

АКАДЕМИЯ НАУК СССР
ЛЕНИНГРАДСКИЙ ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ

МАТЕМАТИЧЕСКИЕ
МЕТОДЫ
ПОСТРОЕНИЯ И АНАЛИЗА
АЛГОРИТМОВ



ЛЕНИНГРАД
«НАУКА»
ЛЕНИНГРАДСКОЕ ОТДЕЛЕНИЕ
1990

Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. 238 с.

В сборнике представлены результаты исследований сотрудников лаборатории теории алгоритмов Ленинградского института информатики и автоматизации АН СССР, а также специалистов, сотрудничавших с этой лабораторией. Работы связаны в основном с разработкой и анализом алгоритмов для обработки знаний, анализа изменений и сигналов и для систем компьютерной алгебры.

Ответственные редакторы

д-р физ.-мат. наук А. О. СЛИСЕНКО
канд. физ.-мат. наук С. В. СОЛОВЬЕВ

Рецензенты:

д-р физ.-мат. наук Ю. В. МАТИЯСЕВИЧ,
д-р техн. наук Л. В. ЧЕРНЫШЕВА

Редактор издательства

Т. И. СУШКОВА

РЕАЛИЗАЦИЯ СИСТЕМЫ СИМВОЛЬНЫХ ВЫЧИСЛЕНИЙ МИНИСАК НА ЯЗЫКЕ ФОРТ

1. Введение

В основу данной реализации положена известная система символьных вычислений САК-2 [1], предназначенная для работы с полиномами от многих переменных над конечными полями. Алгоритмическое наполнение системы САК-2 содержит свыше 500 алгоритмов (процедур и функций), реализующих различные действия над полиномами и связанными с ними структурами. Все эти алгоритмы представлены в виде исходных текстов на алгоритмическом языке Альдес, который относится к классу алголо-подобных бестиповых языков. Система САК-2 включает транслятор, переводящий текст с языка Альдес в стандартный Фортран. Текст этого транслятора дается в двух аутентичных вариантах — на языке Фортран и на языке Альдес. Комбинируя использование Альдес-транслятора системы САК-2 и стандартного транслятора с языка Фортран, можно перевести все алгоритмическое наполнение системы в библиотеку загрузочных модулей данной ЭВМ.

Дальнейшая работа пользователя с системой выглядит следующим образом. Программист пишет программу на языке Альдес, в которой имеются обращения к тем или иным модулям из алгоритмического наполнения. Транслируя эту программу и затем присоединяя к ней необходимые модули из алгоритмического наполнения, можно получить рабочую программу, которая загружается в память и используется для расчетов.

Описанный подход приемлем при использовании больших ЭВМ, но совершенно не годится для средних персональных ЭВМ класса ЕС-1840 из-за своих высоких требований к оперативной памяти. Например, на ЕС ЭВМ средний объем рабочей программы при использовании системы САК-2 составляет около 400 К байт, не считая памяти, необходимой для размещения рабочих значений программы во время счета. На наш взгляд, такое «разбухание» рабочей программы связано, с одной стороны, с двухступенчатой

трансляцией через Фортран в качестве промежуточного языка и, с другой — несовершенством исходного Альдес-транслятора.

В разрабатываемой автором версии системы САК-2 для персональных ЭВМ, которая получила название МИНИСАК, в качестве промежуточного языка выбран не Фортран, а Форт [2] и сам Альдес-транслятор переписан на этом языке с применением особой техники трансляции, позволившей резко сократить его объем. Исходный вариант транслятора (1500 строк на языке Альдес) в двоичном коде на ЕС ЭВМ составляет 420 К байт и требует для своей работы отрезка оперативной памяти размером 500 К, в то время как Альдес-транслятор системы МИНИСАК (800 строк на языке Форт) в оттранслированном виде занимает 25 К байт и вместе с поддерживающей его Форт-системой [3] требует отрезка оперативной памяти менее 100 К байт.

Как известно, каждый транслятор содержит в той или иной форме три основных компонента: лексический анализатор, синтаксический анализатор и генератор кода. Выбор языка Форт в качестве инструментального средства существенно повлиял на способ решения этих задач при создании Альдес-транслятора системы МИНИСАК. Далее описываются технологические аспекты реализации с точки зрения использования этого языка.

2. Лексический анализатор

Задачей лексического анализатора является выделение лексем языка из представленного входного текста. Поскольку в данном случае транслятор является расширением Форт-системы (т. е. надстраивается над ней), то наиболее естественное решение состоит в непосредственном использовании текущего входного потока Форт-системы в качестве входа транслятора. При таком подходе нижний уровень лексического анализатора выглядит достаточно компактно:

```
: КОНЕЦ—ТЕКСТА ( С : ЛИТЕРА——Т : ПРИЗНАК)  
      IF — 1 EXIT THEN QUERY 0;  
: ВВЕСТИ—ЛИТЕРУ ( ——) TIB >IN@ + C@ HERE!  
      CI >IN +!;  
: ПРИНЯТЬ—ЛИТЕРУ ( ——) 1 ALLOT ВВЕСТИ—ЛИТЕРУ;  
: ВЕРНУТЬ—ЛИТЕРУ ( ——) —1 >IN +!;
```

Слово КОНЕЦ—ТЕКСТА вызывает ввод очередной строки при исчерпании текущей, ВВЕСТИ—ЛИТЕРУ выбирает очередную литеру из текущей строки и помещает ее на вершину словаря по адресу HERE. Слово ПРИНЯТЬ—ЛИТЕРУ продвигает на единицу указатель вершины словаря, защищая тем самым находящуюся там последнюю введенную литеру, и вводит следующую. Таким образом, в результате исполнения этого слова (точнее, соответствующей операции) несколько раз подряд и далее испол-

нения слова ВЕРНУТЬ—ЛИТЕРУ непосредственно под вершиной словаря будет сформировано внешнее представление очередной лексемы. Если перед началом такой последовательности действий поместить на стек текущее значение указателя вершины словаря и затем отвести один байт под счетчик длины HERE 1 ALLOT, то по ее завершении можно получить на вершине словаря текстовую строку со счетчиком, которая удовлетворяет требованиям Форт-системы и является внешним представлением данной лексемы:

HERE OVER — 1 — OVER C! DP!

С помощью специальной таблицы, зависящей от принятой системы кодирования, лексический анализатор определяет класс (один из четырех) каждой вводимой литеры: буква, цифра, спецзнак, пусто. Распознавание очередной лексемы начинается с первой литеры, имеющей непустой класс, и продолжается по-разному в зависимости от него.

Если первая литера оказалась буквой, то выбираются все следующие за ней буквы и цифры; так распознается идентификатор. Если первая литера — цифра, то выбираются все последующие цифры; так распознается число. Наконец, если первая литера оказалась спецзнаком, то из входного потока выбирается еще одна литера и полученные две литеры сравниваются с образцами двухлитерных индикантов, имеющихся в языке. При отсутствии соответствующего образца вторая литера сформированной лексемы возвращается обратно во входной поток и данная лексема рассматривается как однолитерный индикант.

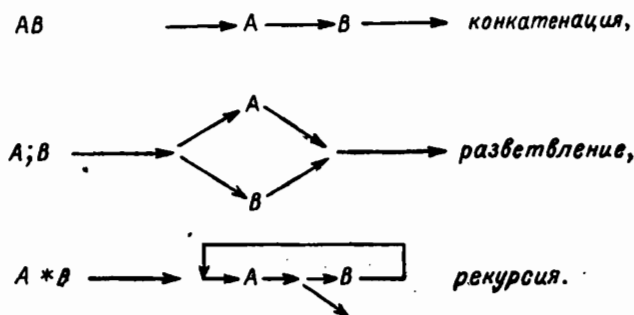
Для лексем — идентификаторов и индикантов — выполняется поиск в специальных таблицах, которые представлены списками слов и определены через стандартное Форт-слово VOCABULARY. Если идентификатор не найден в таблице КЛЮЧЕВЫЕ—СЛОВА, то он возвращается как лексема ИДЕНТИФИКАТОР. Если индикант не найден в таблице ИНДИКАНТЫ, то выдается сообщение об ошибке — недопустимой литере во входном потоке. Если же поиск оказался успешным, то исполняется найденная словарная статья, которая может вернуть специальный лексический класс данного ключевого слова или индиканта или выполнить какое-либо иное действие. Именно таким образом, например, осуществляется распознавание текстовых строк и комментариев, которые в языке Альдес начинаются с двухлитерного индиканта «⌘» (», заканчиваются однолитерным индикантом«) и внутри должны быть «уравновешены» по использованию левых и правых скобок. Словарная статья для слова ⌘ (в списке слов ИНДИКАНТЫ выбирает из входного потока все последующие литеры (вызывая при его исчерпании ввод следующей порции текста) до тех пор, пока не будет считано уравновешенное скобочное выражение. Ясно, что включать эти действия в общую схему лексического анализатора нецелесообразно.

3. Синтаксический анализатор

В практике построения трансляторов уже стало традицией строить синтаксический анализатор автоматически по грамматике контекстно-свободной составляющей входного языка [4]. Этот подход применен и в данной реализации, однако в целях достижения максимальной компактности анализатора грамматика языка задавалась не в традиционной форме Бэкуса—Наура, а в виде регулярных выражений.

Определим три операции над любыми множествами цепочек из лексем нашего языка, включая пустое множество. Операция конкатенации множеств A и B , записываемая как AB , определяет множество всех цепочек вида xu , где $x \in A$ и $u \in B$. Операция разветвления между множествами A и B , записываемая как $A; B$, определяет множество, совпадающее либо с A , либо с B (эта операция имеет практический смысл в том случае, если множества A и B не пересекаются). Наконец, операция рекурсии, записываемая как A^*B , определяет бесконечное множество цепочек $A; ABA; ABAABA; \dots$. В частном случае, если левый операнд рекурсии — пустое множество, то операция A^* означает множество цепочек (составленных из элементов множества A), включающее пустую цепочку — повторение A нуль и более раз. Если же правый операнд рекурсии оказывается пустым множеством, то запись A^* означает повторение элементов множества A один или более раз.

В графической форме введенные операции над множествами можно представить следующим образом:



Каждый из представленных графов имеет один вход и один выход. Процесс порождения элементов множества, определяемого каждой из перечисленных операций, протекает так. В качестве текущей цепочки берется пустая цепочка и осуществляется прохождение через данный граф от его входа к выходу. Прохождение через вершину, соответствующую множеству — операнду данной операции, сопровождается выбором какого-нибудь элемента из этого множества и приписыванием его справа к текущей цепочке.

По достижении конца данного графа текущая цепочка представляет собой один из элементов результирующего множества.

Регулярным выражением называется правильное скобочное выражение, в котором в качестве операций используются введенные выше три операции над множествами, а в качестве операндов — обозначения множеств или регулярные выражения. Будем записывать определения множеств через регулярные выражения следующим образом:

МНОЖЕСТВО : РЕГУЛЯРНОЕ ВЫРАЖЕНИЕ.

Тогда, например, синтаксис выражения в языке Альдес можно задать так:

ВЫРАЖЕНИЕ : (* «ЗНАК—ОПЕРАЦИИ» ОПЕРАНД)

* («ЗНАК—ОПЕРАЦИИ»; «=»).

ОПЕРАНД : «ЧИСЛО»; «ИДЕНТИФИКАТОР» («(

(ВЫРАЖЕНИЕ * «,»;) «)»;

«СТРОКА»; « (» (ВЫРАЖЕНИЕ;) «)».

Здесь «ЧИСЛО», «ИДЕНТИФИКАТОР», «СТРОКА», «(», «)», «=», «,» и «ЗНАК — ОПЕРАЦИИ» обозначают лексемы языка Альдес и одновременно одноэлементные множества цепочек, состоящих из одной такой лексемы. Пустое множество обозначается отсутствием соответствующего операнда. В теории трансляций множества в определенном выше смысле называются нетерминалами, а лексемы, из которых составляются цепочки языка, — терминалами. Если ввести дополнителное обозначение [A] для часто встречающегося разветвления (A;), то правило для операнда будет еще короче:

ОПЕРАНД: «ЧИСЛО»; «ИДЕНТИФИКАТОР» [« (» [ВЫРАЖЕНИЕ* «,»] «)»];

«СТРОКА»; « (» [ВЫРАЖЕНИЕ] «)».

Данное правило говорит, что операндом выражения может быть один из четырех объектов: число, идентификатор, за которым может следовать список выражений через запятую, заключенный в круглые скобки (что соответствует указателю функции со списком фактических параметров или переменной с индексами), строка и выражение в круглых скобках. Если выражение внутри скобок отсутствует, то конструкция () рассматривается как представление специального объекта — пустого списка, который также может быть операндом выражения. Правило для выражения определяет его через рекурсию от операнда, которому может предшествовать несколько знаков одноместной операции, используемых ноль или более раз и знака двухместной операции или равенства. То, что знак равно имеет особый лексический класс, связано с его использованием в других конструкциях, например:

ПРИСВАИВАНИЕ : «ИДЕНТИФИКАТОР» [« (»
ВЫРАЖЕНИЕ * «,» «)»]
«=» ВЫРАЖЕНИЕ.

Здесь выражение справа от знака равно представляет источник присваивания, а конструкция слева — получатель, который может быть либо простой переменной, представленной одним идентификатором, либо переменной с индексами, и тогда после идентификатора следует непустой список индексов через запятую, заключенный в круглые скобки. Все знаки операций имеют один лексический класс; распознавание одноместных и двухместных операций, которые представляются одним и тем же знаком (например, минусом), происходит по месту их использования в соответствии с приведенным правилом.

Полный синтаксис языка Альдес задается с помощью 12—15 правил, аналогичных приведенным выше. Если вернуться к графической интерпретации регулярных выражений, то этот набор правил задает некоторый ориентированный граф с одним входом и одним выходом. Процесс распознавания цепочки лексем на принадлежность языку, определяемому данной грамматикой, состоит в прохождении через этот граф от его начала к концу с отождествлением каждой очередной подпоследовательности лексем из представленной цепочки с элементом множества, указанного в вершине, через которую выполняется прохождение. Здесь существенным оказывается соблюдение принципа однозначности при разветвлении (множества — операнды разветвления не должны пересекаться) и завершаемости рекурсии (при обходе любого цикла в графе должно иметь место продвижение по анализируемой цепочке хотя бы на одну лексему).

Рассматривая процесс анализа как прохождение по графу, можно внести в этот граф дополнительные элементы: пометить дуги графа именами специальных процедур, которые будем называть семантиками, с тем, чтобы при прохождении по отмеченной дуге автоматически выполнялся вызов соответствующей семантики. В момент исполнения семантики синтаксический анализатор «помнит» характеристики последней принятой лексемы: ее лексический класс, внешнее представление и т. д. Эти значения могут быть использованы в семантике как параметры. Семантики в пределах одного правила могут передавать информацию друг другу через глобальные переменные или, учитывая возможность рекурсии, через стек. В этом случае комплекс семантик в рамках одного определения можно рассматривать как одну многовходовую процедуру, собственные данные которой располагаются на стеке. Обозначая семантики через идентификаторы со знаком вопроса, перепишем синтаксические правила для выражения, дополнив их именами семантик, исполняемых по ходу разбора:

ВЫРАЖЕНИЕ : ?Ф1 (* (?1МЕСТН «ЗНАК—ОПЕРАЦИИ») ОПЕРАНД) * (?2МЕСТН «ЗНАК—ОПЕРАЦИИ» ; ?2МЕСТН «=») ?Ф2.

ОПЕРАНД : ?ЧИСЛО «ЧИСЛО»; ?ИД «ИДЕНТИФИКАТОР» (?ИД1 « (» [ВЫРАЖЕНИЕ ?СЧЕТЧИК] * «.»] ?ИД2 «)»; ?ИД3); ?СТРОКА «СТРОКА»; « (» (?ПУСТ«)»; ВЫРАЖЕНИЕ «)»).

Применяя известную технику преобразования инфиксных формул к обратной польской форме с использованием отдельного стека операций, можно задать эти действия внутри введенных семантик и тем самым превратить данный анализатор в транслятор (или интерпретатор) арифметических выражений. Элементами вспомогательного стека операций являются пары значений: исполнительный код данной операции (на этом уровне одноместные и двухместные операции с одинаковым внешним представлением должны различаться) и ее приоритет. Семантика ?Ф1, с которой начинается распознавание выражения, кладет на стек операций некоторый ограничитель (например, число нуль); он должен быть меньше приоритета любой операции. Семантика ?1МЕСТН проверяет, что текущая лексема является допустимым знаком одноместной операции (если это не так, то выдается сообщение об ошибке), находит исполнительный код данной операции и кладет его на стек операций вместе с максимальным приоритетом (обычно 9). Семантика ?2МЕСТН аналогично семантике ?1МЕСТН проверяет, что текущая лексема является допустимым знаком двухместной операции, находит ее исполнительный код и приоритет (число в диапазоне от 2 до 8), а затем кладет их на стек операций, выталкивая оттуда все операции с не меньшим приоритетом. Вытолкнутые операции исполняются или компилируются. Наконец, семантика ?Ф2, завершающая распознавание формулы, кладет на стек фиктивную операцию с приоритетом 1, который должен быть меньше приоритета любой операции, но больше ограничителя семантики ?Ф1, выталкивая при этом все операции с не меньшим приоритетом. В результате на вершине стека операций останется только эта операция и ограничитель, положенный семантикой ?Ф1, которые удаляются со стека.

Семантики, стоящие в правой части правила для операнда выражения, программируют (или исполняют) соответствующие действия над значениями. Например, если ?ЧИСЛО, ?ИД и другие семантики для операнда выводят внешнее представление текущей лексемы в выходной поток, а описанное выше выталкивание операции состоит в том, что в выходной поток выводится обозначение ее исполнительного кода, то данный анализатор является чистым преобразователем инфиксных формул к обратной польской форме.

Использование Форта в качестве инструментального языка программирования в описываемой системе позволяет очень просто строить синтаксический анализатор по записи грамматики входного языка. Если структурные элементы, из которых строятся эти правила (названия лексем-терминалов, множеств-нетерминалов, семантик, скобки, двоеточие, точка, точка с запятой и звездочка), рассматривать как отдельные слова, т. е. разделять пробелами, то на такую запись можно смотреть как на текст на языке Форт, задающий требуемый синтаксический анализатор. Скобки и операции над множествами надо рассматривать как структуры управления, аналогично разветвлениям и циклам языка Форт,

а каждое правило для нетерминала считать аналогом определения через двоеточие. Использование имени нетерминала в правой части правила приводит к компиляции вызова данного слова; его исполнение состоит в распознавании фрагмента цепочки в соответствии с заданным синтаксисом.

Применение языка Форт позволяет существенно оптимизировать механизм передач управления в такой структуре. Дело в том, что нетерминал может не только распознать определяемый его синтаксисом фрагмент цепочки от текущего места, но и отвергнуть этот фрагмент, если он не удовлетворяет заданному синтаксису. Если такое отвержение происходит после продвижения по цепочке хотя бы на одну лексему, то работа анализатора прекращается с выдачей сообщения об ошибке: очередная лексема не подходит по синтаксису данной конструкции. Если же продвижение по цепочке лексем не произошло из-за того, что уже первая лексема не подходит для данного нетерминала, то ошибки нет, и нужно перейти к следующей по порядку альтернативе в разветвлении, текущей альтернативой которого является данный нетерминал. Отвержение возникает в том случае, если данная альтернатива была последней. Таким образом, для каждого нетерминала возможны два завершения: принятие, при котором произошло продвижение по входной цепочке лексем в соответствии с заданным синтаксисом, и непринятие, при котором продвижение не происходит. Оптимизация таких вызовов состоит в использовании упрощенного механизма исключительных ситуаций: при непринятии возврат управления происходит по ссылке на следующую альтернативу, которая компилируется вслед за вызовом данного нетерминала, а при принятии — по адресу возврата плюс 2, чтобы обойти эту ссылку. При каждом обращении к программе нетерминала формируется свой счетчик принятых лексем; в случае нормального завершения счетчик нетерминала, вызвавшего данный, продвигается на число принятых им лексем; при выходе по непринятию осуществляется контроль того, что текущий счетчик принятых лексем равен нулю.

С этой точки зрения лексемы-терминалы, используемые в правых частях правил, рассматриваются как нетерминалы с такой программой: если текущая лексема совпадает с данным терминалом, то она принимается с продвижением счетчика принятых лексем на единицу, если нет, — то не принимается.

При обнаружении синтаксической ошибки из-за непринятия последним опробованным терминалом текущей лексемы можно выдать программисту дополнительную информацию о том, какая именно лексема ожидалась в данном месте. Это один из тех терминалов, которые проверялись после принятия предыдущей лексемы. Например, при анализе Альдес-программы ТЕСТ. $X + 1 = 2..$ выдается сообщение:

ЛЕКСЕМА «+» НЕ ПОДХОДИТ; ОЖИДАЛАСЬ ОДНА
ИЗ ЛЕКСЕМ: «=» «(» «.» «..».

Такое усовершенствование транслятора заметно повышает его удобство для программиста.

Наконец, программы семантик должны исполняться не в момент прохождения через соответствующий вызов, а в момент принятия очередного терминала из входной цепочки. Каждое разветвление в грамматике должно «очищать» очередь семантик, ожидающих исполнения, а скомпилированный вызов семантики — ставить ее в конец этой очереди. В момент принятия терминала накопившиеся семантики исполняются, и вся очередь вновь очищается.

Реализация описанного механизма с подробными комментариями занимает примерно 8 экранов на языке Форт; к качеству внутреннего стека программы нетерминалов используют стек возвратов, предоставляя стек данных в полное распоряжение семантик. Некоторым недостатком такого решения является необходимость иметь необычайно большой стек возвратов (до 400 байт и больше) в зависимости от глубины вложенности для анализируемых конструкций языка.

4. Генератор кода

Результатом работы транслятора является некоторый текст, который, как и в случае записи грамматики входного языка в регулярных выражениях, можно считать текстом на языке Форт, поскольку он состоит из слов, разделенных пробелами. По существу этот выход транслятора представляет собой запись синтаксического дерева входной Альдес-программы, где каждая вершина — конструкция языка Альдес — представлена специальным словом или группой слов.

Будем обозначать специальные слова, соответствующие конструкциям языка Альдес, Форт-словами, начинающимися со знака вопроса. Тогда, например, Альдес-текст $X = F(1, A)$ переходит в последовательность слов:

?LIT 1 A F ?TO X .

Слово ?LIT рассматривает следующее как запись числовой константы, значение которой должно быть положено на стек. Следующее слово A, обозначающее переменную в Альдес-программе, в данном Форт-тексте обозначает словарную статью, исполнение которой кладет на стек значение данной переменной. Аналогично слово F, соответствующее некоторой функции с двумя параметрами, обозначает словарную статью, построенную для этой функции; ее исполнение снимает со стека два значения (параметры) и кладет на стек результат. Служебное слово ?TO рассматривает следующее как имя словарной статьи для переменной и генерирует присваивание этой переменной значения, которое снимается со стека.

Порождение выходного текста осуществляют семантики, выполняемые в процессе синтаксического анализа. Однако для

основных единиц трансляции — алгоритмов — прямое порождение невозможно, поскольку информация, которую желательно помещать при начале алгоритма (число локальных переменных в его теле т. п.), становится известной только по достижении его конца. В силу этого факта порождаемый семантиками текст направляется в специальный буфер (он представляет собой последовательность ссылок на текстовые фрагменты), который освобождается по завершении трансляции каждого алгоритма. Вместе с этим текстом в качестве параметров к слову ?DEF, начинающему определение алгоритма, выводятся: число локальных переменных, список их имен с указанием дополнительных атрибутов, число параметров, глубина вложенности циклов и т. д.

Применение языка Форт позволило организовать порождающую часть транслятора очень компактным образом за счет широкого использования механизма динамической идентификации, как правило, недоступного или неэффективного в других языках. Его основная идея в применении к данной задаче состоит в следующем. Таблица идентификации, т. е. статический контекст при трансляции программы, представляется обычным списком слов, определенным через VOCABULARY. Каждая статья в этом списке, соответствующая какому-либо идентификатору в программе, содержит в своем поле параметров вход в еще один список статей — свой тип. Оказалось необходимым различать 8 разных типов: процедуры, функции, программы, константы, локальные и глобальные переменные и массивы. Каждый тип содержит статьи для действий периода компиляции, которые можно выполнять над идентификаторами, относящимися к данному типу; при этом в качестве одного из параметров каждой такой процедуры передается адрес статьи для идентификатора. Имена статей действий в списках-типах частично пересекаются; все эти списки базируются на один и тот же исходный, в котором определены дополнительные действия так, чтобы поиск любого действия из объединения всех типов всегда заканчивался успешно, выдавая либо «настоящую» статью из данного типа, либо «запасную» статью с тем же именем из базового списка, если в данном типе такая статья отсутствует.

Такой подход позволяет существенно сокращать объем действий, который необходимо запрограммировать в семантиках для анализа конкретной ситуации. Пусть, например, «нагруженное» семантиками правило для присваивания выглядит следующим образом:

ПРИСВАИВАНИЕ : ?ПРИСВ0 «ИДЕНТИФИКАТОР»
 (?ПРИСВ1 « (» (ВЫРАЖЕНИЕ ?ИНДЕКС) * «, » «)»
 ?ПРИСВ3) «=» ВЫРАЖЕНИЕ ?ПРИСВ4 .

Тогда семантика ?ПРИСВ0 ищет данный идентификатор в текущей таблице идентификации и возвращает адрес его статьи, либо, если это впервые встретившийся идентификатор, создает новую статью с типом «локальная переменная» (язык Альдоэ,

как Фортран, разрешает не описывать локальные переменные). Семантика ?ПРИСВ1 исполняется в том случае, если вслед за идентификатором во входном тексте идет открывающая круглая скобка. Эта ситуация соответствует присваиванию значения элементу массива. Вместо проверки того, что данный идентификатор описан как массив, семантика ?ПРИСВ1 исполняет специальную процедуру НАЧ—МАСС, поиск которой осуществляется динамически в типе данного идентификатора. Для локального или глобального массивов этот поиск вернет «настоящую» процедуру, которая сбросит в нуль счетчик индексов в последующем выражении:

: НАЧ—МАСС (A—A, 0) 0 ; ,

который будет увеличиваться на единицу при каждом исполнении семантики ?ИНДЕКС:

: ?ИНДЕКС (K—K + 1) 1 + ; .

Для всех остальных типов идентификатора поиск процедуры НАЧ—МАСС закончится в базовом списке слов, в котором процедура с этим именем выдает сообщение о недопустимом индексировании данного идентификатора:

: НАЧ—МАСС (A—) CR .« НЕДОПУСТИМОЕ
ИНДЕКСИРОВАНИЕ »
DUP « ТИП» ВЫП ». >NAME ». ABORT ; .

Здесь слово ВЫП осуществляет поиск процедуры ТИП в списке слов, который извлекается из статьи с адресом A для данного идентификатора, и исполняет ее. Каждый тип содержит такую процедуру, которая выдает адрес текстовой строки с именем типа в родительном падеже, чтобы его удобнее было объединять с другими словами в сообщениях на русском языке. Например, для локальной переменной такое определение выглядит следующим образом:

: ТИП (A—A1) DROP «ЛОКАЛЬНОЙ ПЕРЕМЕННОЙ» ; .

В результате исполнение вышеприведенной процедуры НАЧ—МАСС для локальной переменной X выдает сообщение:

НЕДОПУСТИМОЕ ИНДЕКСИРОВАНИЕ
ЛОКАЛЬНОЙ ПЕРЕМЕННОЙ X

и закончит работу транслятора через слова ABORT. Если же таким образом реализованные проверки прошли успешно, то к моменту исполнения семантики ?ПРИСВ2 на стеке находится адрес статьи для данного идентификатора локального или глобального массивов и накопившийся счетчик индексов. Семантика ?ПРИСВ2 осуществляет поиск и исполнение процедуры КОН—МАСС, которая проверяет совпадение числа индексов в данном применении с описанием массива.

Семантика ?ПРИСВ3 выполняется в том случае, если вслед за идентификатором сразу следует знак присваивания. Она должна проверить допустимость присваивания. Для этого она осуществляет поиск и исполнение процедур АДР в контексте данного идентификатора:

: ?ПРИСВ2 (A—A) DUP « АДР» ВЫП ;

Для локальной и глобальной переменных эта процедура очевидна:

: АДР (A—) DROP ; ,

а для всех остальных типов она состоит в выдаче сообщения об ошибке, например:

НЕДОПУСТИМОЕ ИСПОЛЬЗОВАНИЕ ГЛОБАЛЬНОГО МАССИВА МТК

(здесь МТК — идентификатор массива) и программируется аналогично вышеприведенному «запасному» варианту процедуры НАЧ—МАСС. Завершающая присваивание семантика ?ПРИСВ4 порождает текст

?ТО А ,

где А — имя статьи, соответствующей переменной или массиву.

Хотя язык Альдес является бестиповым, тем не менее некоторый контроль типов значений в нем необходим. В языке различаются выражения для целых значений, списков, булевских значений и адресов. Учет этих различий и своеобразный контроль типов выполняются через упрощенный механизм запросов [4]. Каждая конструкция в начале своего программирования выдает запросы на программирование своим подконструкциям по их завершении программирует собственные действия в зависимости от полученного внешнего запроса. Для передачи запросов сверху—вниз, от конструкций к подконструкциям, и ответов снизу—вверх, от подконструкций к объемлющим конструкциям, используются специальные стеки.

В данной реализации используются 4 запроса: (ПУСТ) — значение не требуется, (НЕМЕДЛ) — значение (обычно, число) должно быть вычислено во время трансляции, (АДР) — запрос на вычисление адреса и (ЗНАЧ) — запрос на вычисление значения. В рассмотренном выше присваивании семантики ?ПРИСВ1 и ?ПРИСВ3 выдают запрос (ЗНАЧ) на значения выражений, входящих в индексы и в правую часть присваивания. Семантики ?ИНДЕКС, ?ПРИСВ3 и ?ПРИСВ4 проверяют то, что тип значения, вычисляемого запрограммированным выражением, допустим в данной конструкции (число для индекса, число или список для правой части присваивания).

5. Синтез рабочей программы

Сгенерированный в результате трансляции Альдес-программы Форт-текст записывается во внешнюю память стандартным для языка Форт-образом — в виде Форт-экранов. Их трансляция с целью получения исполняемой рабочей программы выполняется синтезирующей частью транслятора, которая содержит определения специальных Форт-слов ?TO, ?DEF и других, порождаемых в выходном тексте анализирующей частью. В окончательном виде рабочая программа представляет собой законченный программный продукт, построенный как замкнутая Форт-система без текстового интерпретатора. Двоичный модуль содержит собственное Форт-ядро, включающее адресный интерпретатор и реализацию в машинных кодах ряда базовых операций, за которым следует шитый код [5] — результат трансляции исходных алгоритмов. Объем ядра — около 1.5 К байт, и это единственный машинно-зависимый компонент системы.

Трансляцию ядра из исходного текста в машинный код выполняет небольшое расширение над встроенным Форт-ассемблером — неизменяемым компонентом развитой Форт-системы [5]. В результате трансляции, помимо собственно двоичного кода ядра, строится список точек входа в него с соответствующими адресами. Эти значения используются в синтезирующей части для генерации ссылок в ядро из создаваемого шитого кода.

Отдельные подсистемы алгоритмического наполнения хранятся в виде оттранслированных с языка Альдес Форт-текстов в описанных выше соглашениях. Их можно добавлять в рабочую программу по мере надобности, транслируя синтезирующей частью. Общий объем рабочего модуля, содержащего все алгоритмическое наполнение, составляет около 75 К байт. Поскольку это превышает стандартный размер адресного Форт-пространства — 64 К байт, то здесь используется свернутый шитый код, в котором все адреса хранятся в виде значений, деленных на два. Это сразу увеличивает диапазон адресов до 128 К байт при условии, что в адресный интерпретатор добавляется команда соответствующего увеличения каждой извлекаемой ссылки.

Скомпилированный рабочий код может быть исполнен путем передачи ему управления из внешней Форт-системы как «чужому» модулю по стандартным соглашениям о связях. При этом внешняя Форт-система обеспечивает связь рабочего модуля с внешним окружением, взаимодействие с программистом и различные диалоговые средства отладки.

Литература

1. *Collins G.* The SAC-2 computer algebra system//Lect. Notes Comp. Sci. 1985. Vol. 204. P. 34, 35.
2. *FORTH-83 Standard.* Mountain View: FORTH Standards Team. 1983.
3. *Баранов С. Н.* Система Форт-ЕС/ЛИИАН, препринт № 1. Л., 1987.
4. *Алгол-68.* Методы реализации. Л., 1976.
5. *Баранов С. Н., Ноздрунов Н. Р.* Язык Форт и его реализации. Л., 1988.

МАШИННО-НЕЗАВИСИМОЕ ОПИСАНИЕ КЛАССА ЗАПРОСОВ, ПОДДЕРЖИВАЕМЫХ В РЕАЛЬНОЕ ВРЕМЯ

В статье [1] дается модель баз данных, удобных для работы с непроцедурными языками описания данных высокого уровня. Эти языки позволяют не использовать язык запросов как таковой, описывая любой желаемый вычислимый результат путем задания характеристик выходных данных. Модель является достаточно общей.

В настоящей статье исследуется класс таких запросов к базам данных типа [1], которые могут поддерживаться определенными типами вычислительных машин в реальное время, т. е. по мере поступления информации о некоторых изменениях в базе данных такая машина находится в постоянной готовности за ограниченное константой число шагов работы выдать ответ на заданный запрос. При этом число шагов работы машины между порциями информации об изменениях в базе данных также ограничено константой. Изменения, вносимые, согласно одной такой порции, в базу данных, имеют локальный характер. Информация о каждом из них задается вектором фиксированной длины.

Основной результат работы — машинно-независимое описание класса запросов к базам данных, поддерживаемых в реальное время. Описание дается на синтаксическом уровне, т. е. установлено, какие операции с данными и в каком порядке нужно разрешить при формулировке запросов, чтобы получить весь класс запросов, ответы на которые можно без задержек неограниченно долго поддерживать на машинах некоторого достаточно широкого класса по мере внесения изменений в базу данных.

1. Модель баз данных

Прежде всего определим, что мы будем понимать под базой данных.

О п р е д е л е н и е 1. Мультимножеством называется целочисленная функция f , заданная на некотором множестве X . Если $x \in X$, то $f(x)$ называется кратностью элемента x в мультимножестве f . Будем допускать мультимножества с отрицатель-

ными кратностями элементов. Если кратность элемента мультимножества равна нулю, то считается, что этот элемент не принадлежит данному множеству. Мультимножества считаются равными, если они содержат одни и те же элементы с одними и теми же кратностями. Элементы с нулевой кратностью при сравнении мультимножеств не учитываются. Мультимножество называется пустым, если в нем нет элементов с ненулевой кратностью.

Через T_n будем обозначать класс финитных (конечных, заданных явным перечислением) мультимножеств кортежей, состоящих из n целых чисел. Класс T_0 естественно отождествить с целыми числами, так как T_0 — мультимножества, содержащие лишь один пустой кортеж с равными кратностями. Пустой элемент T_0 отождествляется с числом 0.

Пустое мультимножество типа T_n будем обозначать через 0_n . Для мультимножеств естественным образом определены операции сложения, вычитания и умножения на целое число, обозначаемые знаками $+$, $-$ и $\cdot$. Эти операции сводятся к соответствующим операциям над кратностями элементов мультимножеств. Мультимножество, состоящее из единственного элемента x с кратностью k , будем обозначать через $k \{x\}$.

О п р е д е л е н и е 2. Типом базы данных будем называть кортеж r вида $\langle r_1, \dots, r_l \rangle$, где $r_1, \dots, r_l$ — целые неотрицательные числа. Число l называется количеством компонент базы данных. Состоянием базы данных типа $r = \langle r_1, \dots, r_l \rangle$ будем называть кортеж $\langle s_1, \dots, s_l \rangle$, где $s_i \in T_{r_i}$ при $i = 1, \dots, l$.

Если f принадлежит классу T_n при $n > 0$, то через $[f]_k$ будем обозначать такое мультимножество кортежей класса T_{n-1} , что $[f]_k(x) = f(k, x)$. Здесь неопределенные значения функций отождествляются с нулевыми. Мультимножество $[f]_k$ называется срезом мультимножества f по компоненте k .

О п р е д е л е н и е 3. Мультимножество f' будем называть локальным изменением мультимножества f , если f' отличается от f кратностью не более чем одного элемента t . Любое целое число как элемент T_0 при этом естественно считать локальным изменением любого другого целого числа.

Кодом локального изменения f' мультимножества f будем называть такой кортеж $\langle t, k \rangle$, что $f' = f + k \{t\}$. Кодом локального изменения f' элемента f из множества T_0 (целых чисел), следовательно, является разность $f' - f$.

Состояние базы данных s' типа r будем называть локальным изменением состояния базы данных s типа r , если мультимножество s'_i — локальное изменение мультимножества s_i для каждого i от 1 до n , где $r = \langle r_1, \dots, r_n \rangle$.

О п р е д е л е н и е 4. Кодом локального изменения $s' = \langle s'_1, \dots, s'_n \rangle$ состояния базы $s = \langle s_1, \dots, s_n \rangle$ типа $\langle r_1, \dots, r_l \rangle$ будем называть кортеж $\langle \alpha_1, \dots, \alpha_l \rangle$, где α_i — код локального изменения s'_i мультимножества s_i при $i = 1, \dots, l$.

Пусть $c_1, \dots, c_k$ — коды локальных изменений состояния базы данных типа r . Через $c_1 \parallel \dots \parallel c_k$ будем обозначать сцепление

кортежей $c_1, \dots, c_k$, т. е. выписанные подряд составляющие их числа.

Пусть s — состояние базы данных типа r , c — код локального изменения состояния базы данных типа r . Тогда через $s * c$ будем обозначать локальное изменение s' состояния s с кодом c . Запись $s * c_1 * \dots * c_k$ служит сокращением для записи:

$$(\dots (s * c_1) * \dots) * c_k.$$

Через Λ_r будем обозначать состояние базы данных типа r , все компоненты которого пусты.

Введенные выше понятия типа и состояния базы данных достаточно полно отражают ситуацию, имеющую место в реальных системах реляционных баз данных, если учесть, что все практически используемые данные можно закодировать целыми числами. Мультимножества, помимо того, что в реальных базах данных они полезны сами по себе, здесь позволяют проще описать исследуемый класс запросов.

2. Машина с индексным доступом

Определим модель абстрактной вычислительной машины, которая может за один шаг работы выполнять операцию равнодоступной адресной машины или некоторое элементарное действие, выполняемое обычно при работе реальных программ ЭВМ с данными, имеющими так называемую индексно-последовательную организацию.

Описываемая абстрактная машина, называемая в дальнейшем машиной с индексным доступом (*ИМ*), состоит из памяти, устройства управления, устройства ввода и вывода информации. Память представляет собой потенциально бесконечную систему одинаковых ячеек. Каждая ячейка однозначно определяется ее адресом, представляющим собой упорядоченную пару целых чисел. Содержимое ячейки с адресом $\langle a, b \rangle$ будем обозначать через $[a, b]$.

Работа машины представляет собой последовательность шагов, пронумерованных натуральными числами — моментами времени. При каждой такой работе в каждый момент времени каждая ячейка содержит целое число. В начальный момент времени все ячейки содержат нули. В процессе работы *ИМ* устройство управления содержит некоторую не меняющуюся программу. Программа — это конечная последовательность команд, описываемых ниже. Каждая команда представляет собой пару *CODE OP*, где *CODE* — код операции, *OP* — операнд или серия операндов. При описании операндов используем следующие соглашения.

Компонентой адреса будем называть целое число или запись вида (k_1, k_2) , где k_1, k_2 — целые числа. Во втором случае запись (k_1, k_2) означает то число, которое находится в ячейке с адресом $\langle k_1, k_2 \rangle$. Компоненты адреса будем обозначать буквой a с индексами. Число, обозначаемое компонентой a , будем записывать в виде $[a]$.

Операндом данных будем называть целое число или запись вида (a_1, a_2) , где a_1, a_2 — компоненты адреса. Во втором случае запись (a_1, a_2) означает целое число, находящееся в ячейке, адрес которой задан компонентами a_1 и a_2 . Операнды данных будем обозначать буквой x . Буквой i будем обозначать номера команд программы.

В каждый момент времени устройство управления *IAM* находится в определенном состоянии. Состояние — это номер выполняемой команды программы. Выполнение команды состоит в некотором изменении содержимого ячеек памяти и состояния устройства управления. При этом могут вовлекаться в работу устройства ввода и вывода. Если номер выполняемой команды на очередном шаге работы не изменился, то к следующему шагу он увеличится на единицу. Последней должна быть команда, всегда изменяющая состояние устройства управления (команда перехода *JUMP*, см. ниже).

Приведем список команд *IAM*.

1. Команда *LOAD* x помещает число, обозначаемое операндом x , в ячейку с адресом $\langle 0, 0 \rangle$ — аккумулятор. Старое содержимое аккумулятора стирается.

2. Команда *STORE* (a_1, a_2) помещает содержимое аккумулятора в ячейку, адрес которой задается компонентами a_1, a_2 . Старое содержимое этой ячейки стирается.

3. Команды сложения *ADD* x , вычитания *SUBT* x , умножения *MULT* x , деления *DIV* x выполняют соответствующие действия, беря первый аргумент из аккумулятора, а в качестве второго аргумента — число, обозначаемое операндом x . Результат операции помещается в аккумулятор. При делении остаток отбрасывается. Деление на 0 дает 0.

4. Команда нахождения следующей занятой ячейки *NEXT* (a_1, a_2) i помещает в аккумулятор такое наименьшее целое число k , что $k \geq [a_2]$ и $[[a_1], k] \neq 0$. Команда нахождения предыдущей занятой ячейки *PREV* (a_1, a_2) i помещает в аккумулятор такое наибольшее целое число k , что $k \leq [a_2]$ и $[[a_1], k] \neq 0$. Если указанное число не найдено, то содержимое аккумулятора не меняется и управление передается команде с номером i , т. е. число i становится новым состоянием устройства управления.

5. Команды безусловного перехода *JUMPi*, перехода по нулю *JZEROi*, перехода по положительному числу *JGTZi* изменяют номер выполняемой команды на i в следующих случаях: *JUMP* — всегда, *JZERO* — при нулевом содержимом аккумулятора, *JGTZ* — при положительном содержимом аккумулятора. В остальных случаях выполняется следующая команда.

6. Команда *READ* (a_1, a_2) читает очередное число с помощью устройства ввода и помещает его в ячейку, адрес которой задается компонентами a_1 и a_2 .

Машина не имеет специальной команды вывода. Меняющиеся выходные данные постоянно находятся в ячейках с фиксированными адресами. Работа ведется в режиме *on—line*, при котором

к моменту ввода очередной порции данных готово значение вычисляемой функции на введенном к этому моменту начальном отрезке входных данных. Таким образом, *IAM* приспособлена для вычисления целочисленных функций на целочисленных последовательностях.

3. Запросы и их поддержка

Запросом типа $r \rightarrow p$ будем называть отображение, ставящее в соответствие состояниям базы данных типа r непустые рекурсивно-перечислимые множества состояний базы данных типа p . Множественность результата запроса будем трактовать как возможность нескольких различных ответов. На запросах естественным образом определен частичный порядок. Запрос f типа $r \rightarrow p$ считается не менее определенным, чем запрос g того же типа, если для любого состояния базы s типа r множество $f(s)$ является подмножеством множества $g(s)$.

Запрос типа $r \rightarrow \langle 0 \rangle$ будем называть скалярным запросом. Скалярный запрос состояниям базы данных ставит в соответствие множества целых чисел. В дальнейшем будем рассматривать вычисление на *IAM* в основном скалярных запросов. Вычисление других запросов можно свести к вычислению скалярных. Действительно, ответ на запрос (состояние базы) можно накопить в закодированном виде в памяти и выдать любую ее часть, введя во входную базу дополнительную структуру, указывающую, какой элемент запроса необходимо выводить. Тем не менее для доказательства понадобится временно зафиксировать следующее определение.

О п р е д е л е н и е 5. Будем считать, что ячейка машины содержит представление элемента у класса T_i , если:

- 1) при $i = 0$ эта ячейка содержит целое число y ;
- 2) при $i > 0$ и пустом x эта ячейка содержит число 0;
- 3) при $i > 0$ и непустом x эта ячейка содержит число $l > 0$, и любая ячейка с адресом $\langle l, k \rangle$ содержит представление среза $[x]_k$.

Будем считать, что машина сохраняет в процессе работы представление элемента типа T_i в ячейке c , если $i = 0$, или при $i > 0$;

1) содержимое l ячейки c , не равное нулю, не меняется, если хотя бы одна ячейка с адресом вида $\langle l, k \rangle$ имеет ненулевое содержимое;

2) для нового ненулевого содержимого l ячейки c все ячейки с адресами вида $\langle l, k \rangle$ содержат нули;

3) машина сохраняет содержимое ячеек с адресами $\langle l, k \rangle$, пока ненулевое содержимое ячейки c есть l .

Подчеркнем, что представление элемента типа T_0 всегда сохраняется в любой ячейке *IAM*.

Пусть M — машина типа *IAM*, $x_1, \dots, x_k$ — последовательность целых чисел, $\langle p_1, \dots, p_n \rangle$ — тип базы данных. Через $M(x_1, \dots, x_k)_{\langle p_1, \dots, p_n \rangle}$ обозначим кортеж $\langle s_1, \dots, s_n \rangle$ элементов

классов $T_{p_1}, \dots, T_{p_n}$ соответственно, представления которых содержатся в ячейках с адресами $\langle 0, 1 \rangle, \dots, \langle 0, n \rangle$ соответственно к моменту выполнения машиной M $k+1$ -й операции *READ*.

О п р е д е л е н и е 6. Машина M типа *IAM* поддерживает запрос φ типа $r \rightarrow p$, если для любой цепочки кодов изменений $c_1, \dots, c_k$ базы данных типа r

$$M(c_1 \| \dots \| c_k) \in \varphi(\Lambda_r * c_1 * \dots * c_k)$$

и для любого элемента $x \in \varphi(s)$ найдется такая цепочка кодов изменений $c_1 \dots c_k$ базы данных типа r , что

$$s = \Lambda_r * c_1 * \dots * c_k \quad \text{и} \quad x = M(c_1 \| \dots \| c_k).$$

Данная машина M непрерывно поддерживает указанный запрос, если она сохраняет в ячейках с адресами $\langle 0, i \rangle$ при $i = 1, \dots, |p|$ элементы типов T_{p_i} в процессе всей своей работы.

Заметим, что в силу данных определений любой скалярный запрос может поддерживаться только непрерывно.

Дополним предыдущее определение. Будем считать, что машина M поддерживает запрос φ в реальное время, если число шагов между последовательными выполнениями команды *READ* ограничено сверху константой.

4. Средства формулировки запросов

Через O^n будем обозначать кортеж из n нулей.

О п р е д е л е н и е 7. Исходными запросами называются следующие:

1) запросы типа $\langle 0, 0 \rangle \rightarrow \langle 0 \rangle$: функции $+$, $-$, $\cdot$, $/$, выполняющие операции сложения $(x + y)$, вычитания $(x - y)$, умножения $(x \cdot y)$, вычисления целой части частного $[x/y]$, причем $[0/0]$ полагается равным 0;

2) запрос типа $\langle \quad \rangle \rightarrow \langle 0 \rangle$: константа $\underline{1}$, отображающая пустой кортеж в целое число 1;

3) запрос типа $\langle 0 \rangle \rightarrow \langle 0 \rangle$: функция *abs*, отображающая целые числа в их абсолютные величины;

4) запрос I_i^r типа $r \rightarrow r_i$, где $r = \langle r_1, \dots, r_n \rangle$, $i \leq n$, отображающий кортежи вида $(x_1, \dots, x_n)$ в x_i , где x_i имеет тип T_{r_i} ;

5) запросы N_n , P_n и K_n типа $\langle T_n, 0^n \rangle \rightarrow \langle 0 \rangle$, где $n > 0$, отображающие кортеж $\langle x, t \rangle$ в целое число:

$K_n(x, t)$ — кратность кортежа t в мультимножестве x , т. е. $x(t)$;

$$N_n(x, t, t_0) = \begin{cases} \min \{k | k > t_0, K(x, t, k) > 0\}, \\ \text{если такое } k \text{ существует,} \\ t_0 \text{ иначе,} \end{cases}$$

$$P_n(x, t, t_0) = \begin{cases} \max \{k | k < t_0, K(x, t, k) > 0\}, \\ \text{если такое } k \text{ существует,} \\ t_0 \text{ иначе;} \end{cases}$$

6) запрос G_n типа $\langle T_n, 0^{n+2} \rangle \rightarrow \langle T_n \rangle$, отображающий кортеж вида $\langle x, t, k \rangle$ в мультимножество $x + k \{t\}$.

Множество исходных запросов будем в дальнейшем обозначать буквой B .

О п р е д е л е н и е 8. Пусть h — запрос типа $p \rightarrow q$, g — запрос типа $q \rightarrow r$. Тогда суперпозицией запросов g и h называется запрос $g \circ h$ типа $p \rightarrow r$, определяемый равенством:

$$g \circ h(s) = g(h(s)),$$

где g в правой части применяется ко всем элементам $h(s)$ с объединением результатов.

Пусть h — запрос типа $p \rightarrow q$, g — запрос типа $p \rightarrow r$. Тогда конкатенацией запросов g и h называется запрос $g \parallel h$ типа $p \rightarrow q \parallel r$, определяемый равенством:

$$g \parallel h(s) = g(s) \parallel h(s),$$

где конкатенация в правой части применяется к всевозможным парам элементов $g(s)$ и $h(s)$.

Множество $\{\circ, \parallel\}$, состоящее из операций суперпозиции и конкатенации запросов, будем обозначать буквой S .

О п р е д е л е н и е 9. Операцией непараметризованной одно-временной рекурсии над запросами называется отображение R^0 , ставящее в соответствие состоянию с базы данных типа $\langle T_k \rangle$ и запросу h типа $\langle 0^{n+1}, T_k \rangle \rightarrow \langle T_k \rangle$ наиболее определенный запрос f типа $r \rightarrow \langle T_k \rangle$, удовлетворяющий следующим условиям:

$$\left. \begin{aligned} c \in f(\Lambda_r), \\ h(t_1, k_1, \dots, t_n, k_n, f(x_1, \dots, x_n)) \subset f(x_1 + k_1 \{t_1\}, \dots, \\ \dots, x_n + k_n \{t_n\}), \end{aligned} \right\} \quad (1)$$

где h применяется к множеству $f(x)$ поэлементно. Через $R_c(f)$ будем обозначать множество R_c для всех возможных c .

Последнее определение нуждается в обосновании своей корректности: следует доказать, что функция f существует и единственна.

Д о к а з а т е л ь с т в о. Соотношения (1) нетрудно переформулировать в виде:

$$c \in f(\Lambda_n), \quad (2)$$

если $r \in h(t_1, k_1, \dots, t_n, k_n, y)$ и $y \in f(x_1, \dots, x_n)$, то

$$z \in f(x_1 + k_1 \{t_1\}, \dots, x_n + k_n \{t_n\}). \quad (3)$$

Заметим, что множество истинных предложений вида $z \in h(t_1, k_1, \dots, t_n, k_n, y)$ перечислимо (в силу определения понятия запроса). Тогда предложения (2) и (3) определяют исчисление, порождающее перечислимое множество предложений вида $r \in f(x_1, \dots, x_n)$. Нетрудно видеть, что, положив $f(x)$ равным $\{z \mid \vdash z \in f(x_1, \dots, x_n)\}$, получим требуемый минимальный запрос.

5. Характеризация класса запросов, поддерживаемых в реальное время

Для формулировки основного результата введем следующие сокращения. Пусть X — некоторое множество запросов, O — множество операций или операция над запросами. Через OX обозначим множество результатов однократного применения операций O к элементам X , через O^*X — множество результатов многократного применения операций O к элементам X и самим элементам X .

Т е о р е м а. Множество запросов, непрерывно поддерживаемых машинами типа IAM в реальное время, равно множеству $T = S^*(RS^*B \cup S^*B)$, другими словами, множеству запросов, получаемых из исходных многократными применениями операций суперпозиции, конкатенации и непараметризованной примитивной рекурсии, причем последняя операция применяется «невложженно», т. е. не применяется к запросам, содержащим результаты ее применения.

Доказательство теоремы основывается на нескольких приведенных ниже леммах. Обозначим множество запросов, непрерывно поддерживаемых IAM в реальное время, через R_{IAM} . Таким образом, теорема утверждает, что $T = R_{IAM}$. Для ее доказательства, кроме понятия поддержки запроса, потребуется понятие вычисления запроса.

О п р е д е л е н и е 10. Запросы типа $r \rightarrow \langle T_i \rangle$ будем называть однокомпонентными. Запрос f типа $\langle r_1, \dots, r_n \rangle \rightarrow \langle r_{n+1} \rangle$ называется сильно вычислимым, если найдутся такие целые неотрицательные числа $i \leq n+1$ и k , а также машина M типа IAM , что $r_{n+1} = r_i$ и машина M , начав работу с представлениями элементов $x_1, \dots, x_n, x_{n+1}$ ($x_{n+1} \in \varnothing_{r_{n+1}}$) типа $T_{r_1}, \dots, T_{r_n}, T_{r_{n+1}}$ в ячейках с адресами $\langle 0^{n+1}, 1 \rangle, \dots, \langle 0, n+1 \rangle$ соответственно, не более чем через k шагов выполняет команду $READ$, имея в ячейке $\langle 0, n+1 \rangle$ представление элемента $f(x_1, \dots, x_n) = x_i$ типа $T_{r_{n+1}}$, причем представления элементов в ячейках с адресами $\langle 0, 1 \rangle, \dots, \langle 0, n \rangle$ сохраняются в процессе работы неизменными.

Л е м м а 1. Все однокомпонентные запросы из S^*B сильно вычислимы.

Доказательство ведется индукцией по построению класса S^*B . Сильная вычислимость запросов $+$, $-$, $\circ$, $|/|$, $\underline{1}$, abs очевидна, так как они выполняются тривиальными программами и работают лишь с целыми числами, представления которых всегда сохраняются. Запрос I_i сильно вычислим программой, состоящей лишь из команды $READ$. Программы, сильно вычисляющие запросы N_n , P_n и K_n , нетрудно построить, так как их результаты — целые числа. В первых двух случаях следует использовать соответственно команды $NEXT$ и $PREV$. Нетрудно также построить программу, сильно вычисляющую запрос G_n .

Представление результата этой программой обеспечивается в ячейке с адресом $\langle 0, 1 \rangle$. Таким образом, все исходные запросы сильно вычислимы.

Класс однокомпонентных запросов из S^*B можно построить из класса исходных запросов с помощью операции композиции, ставящей в соответствие функциям $h, g_1, \dots, g_k$ функцию f , определяемую равенством:

$$f(x) = h(g_1(x), \dots, g_k(x)).$$

Если запросы $h, g_1, \dots, g_k$ сильно вычислимы, то можно построить программу, сильно вычисляющую запрос f . Действительно, программы $g_1, \dots, g_k$ можно переделать так, чтобы они, не мешая друг другу, могли последовательно выполняться, накапливая в различных ячейках требуемые изменения входных данных. Затем модифицированная программа для f , используя исходные данные и информацию об их изменениях, вырабатывает требуемый результат. Лемма доказана.

Лемма 2. $RS^*B \subseteq T$.

Доказательство. В силу леммы 1 достаточно доказать, что если f — сильно вычисляемый запрос, то $R_c(f)$ — запрос, поддерживаемый в реальное время. Программа для поддержки запроса f начинает работу с генерации в памяти представления исходной константы C . Затем циклически выполняются команды чтения кода изменения состояния базы и модифицированная программа сильного вычисления f , вносящая в представление результата запроса $R_c(f)$ необходимые изменения. В итоге в зависимости от порядка внесения изменений машина порождает все возможные элементы значения запроса.

Лемма 3. Множество T замкнуто относительно операций S .

Доказательство. Нетривиальной частью доказательства следует считать доказательство замкнутости T относительно операции суперпозиции. Последняя замкнутость следует из того замечания, что машину, поддерживающую запрос в реальное время, можно модифицировать таким образом, чтобы она выдавала последовательность кодов изменений результата этого запроса.

Лемма 4. Любой запрос, непрерывно поддерживаемый в реальное время, представим в виде суперпозиции запросов из S^*B и RS^*B .

Доказательство состоит из арифметизации IAM . Прежде всего следует модифицировать программу IAM , вычисляющую заданный запрос, чтобы все передачи управления назад (на предшествующие команды) были возможны лишь непосредственно после серии команд $READ$, вводящей код изменения состояния базы данных. Затем можно добиться того, чтобы все эти передачи управления назад вели к первой команде программы. Все содержимое памяти IAM можно считать представлением мультимножества пар целых чисел, т. е. элемента класса T_2 . Таким образом, можно считать, что машина поддерживает запрос типа $r \rightarrow T_2$. По модифицированной программе машины нетрудно

построить такой запрос f и константу c , что поддерживаемый запрос будем иметь вид $R_c(f)$, а f будет принадлежать классу S^*B .

Завершает доказательство леммы 4 построение таких запросов g_i типа $T_2 \rightarrow p_i$, что поддерживаемый запрос h типа $r \rightarrow \langle p_1, \dots, p_k \rangle$ представляется в виде:

$$h = \langle g_1, \dots, g_k \rangle \circ R_c(f)$$

Запрос g_i по содержимому памяти (элементу типа T_2) находит элемент типа T_{p_i} , представление которого содержится в ячейке с адресом $\langle 0, i \rangle$.

Трудность в построении запроса g_i с помощью оператора R состоит в том, что не все локальные изменения состояния памяти приводят к локальным изменениям представлений элементов T_{p_i} . Для преодоления этого препятствия достаточно модифицировать исходную машину так, чтобы, кроме предложенных нами представлений мультимножеств, она содержала в памяти представления, основанные на спаривающих функциях Клини, при которых вся информация о представляемом множестве размещается в одном «слое» памяти, а место для хранения кратности каждого кортежа определено однозначно. Это можно сделать, поскольку исходная машина непрерывно поддерживает запрос и, следовательно, вносит в его результат лишь локальные изменения, за которыми сама в состоянии проследить, пометив каким-либо способом элементы результирующей информации.

Д о к а з а т е л ь с т в о теоремы непосредственно следует из лемм 2, 3 и 4.

В заключение заметим, что при удалении из определения *IAM* команд *PREV* и *NEXT*, а из исходных запросов P_n и N_n основная теорема остается истинной. Машины *IAM* в этом случае превращаются в одну из разновидностей равнодоступных адресных машин.

Литература

1. Бельтюков А. П. Базы данных, ориентированные на работу с помощью непроцедурного языка//Синтез программ: Тезисы докладов школы-семинара. Устинов, 1985, с. 57—59.

КАЧЕСТВЕННОЕ ИЗУЧЕНИЕ ОДНОГО КЛАССА СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ

1. Введение

Статья посвящена математическому моделированию специальных этапов вычислительных процессов, которые образуют группу задач для некоторой мультипрограммной операционной системы (ОС). Рассматриваемые этапы характеризуются интенсивным информационным обменом между процессором и совокупностью периферийных устройств, состав которых в процессе работы не изменяется. Каждому устройству поставлена в соответствии задача ОС, запускаемая на счет при срабатывании устройства и в свою очередь по завершении обработки полученных данных запускающая устройство. Такая ситуация весьма характерна для измерительно-вычислительных и управляющих систем. Отличительными чертами сетей массового обслуживания (СМО), возникающих при моделировании описанных систем, являются: цикличность маршрутов отдельных заявок, постоянная (или слабо варьирующаяся) длительность исполнения отдельных работ в монопольном для данной заявки режиме. Как показано в работе, для систем с двумя заявками постоянство этих длительностей может совмещаться в зависимости от дисциплины как с детерминированным, так и со случайным поведением системы. В данной работе для качественного изучения этих систем используются результаты эргодической теории в сочетании с более элементарными методами. При рассмотрении динамических систем, возникающих в ходе анализа СМО, в тех случаях, когда это облегчает исследование, ограничимся рассмотрением наборов параметров этих систем, находящихся в общем положении.

* Я признателен М. И. Гордину, указавшему мне на возможность изучения СМО с помощью теории динамических систем и оказавшему помощь в процессе работы над статьей.

2. Описание класса исследуемых систем

Рассмотрим состоящую из трех приборов замкнутую СМО, в которой обслуживаются две заявки (рис. 1). Обслуживание заявки с номером i ($i \in \{1, 2\}$) состоит в циклическом исполнении работ p_i, a_i , первая из которых выполняется на обслуживающем приборе Π , а вторая — на обслуживаемом приборе A_i . Определив таким образом работы и маршрут каждой из заявок, для полного описания алгоритма работы СМО следует задать трудоемкости каждой из работ и дисциплину обслуживания прибором Π , где имеет место конкуренция заявок. Предположим, что каждая из работ имеет постоянную трудоемкость $T(c)$, где $c \in \{a_1, a_2, p_1, p_2\}$. Как правило, каждая работа в любой момент времени либо не выполняется вовсе, либо выполняется с единичной скоростью. Такая система может быть задана посредством наложения ограничения на совместную динамику заявок, индивидуальная динамика каждой из которых представляется движением с единичной скоростью по размеченной ориентированной окружности, длины дуг которой равны трудоемкостям работ (рис. 2). Пространство состояний системы двух заявок при отсутствии конкуренции в приборе Π являлось бы прямым произведением их пространств состояний (двумерным тором) с соответствующим законом движения. Учет взаимодействия заявок, т. е. дисциплины обслуживания их прибором Π , приводит к необходимости рассматривать более сложные пространства состояний и законы движения (векторные поля) на них. Ниже рассматриваются системы, в которых обслуживание заявок прибором Π подчиняется одной из следующих дисциплин: FCFS (First come first served) — обслуживание в порядке поступления заявок и LCFS (Last come first served) — обслуживание в порядке, обратном порядку поступления заявок, с прерыванием обслуживания заявки и сохранением полученного ею обслуживания. Насколько известно автору, впервые излагаемый подход был применен для исследования СМО в [1]. Подход к доказательству теоремы 1 в несколько более общем случае, чем рассмотренный в статье, был намечен в [2].

Обозначения. В работе будут встречаться динамические системы следующих трех типов: FCFS, LCFS и St (тип St соответствует отсутствию конкуренции в приборе Π или, при другой интерпретации, наличию у каждой заявки своего такого

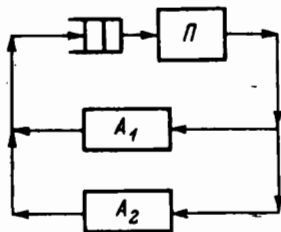


Рис. 1.

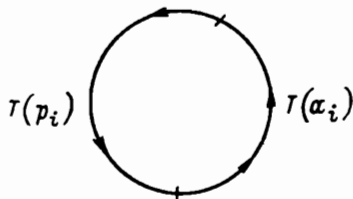


Рис. 2.

прибора). Конкретная система задается типом и набором $(T(a_1), T(p_1), T(a_2), T(p_2)) \in R_+^4$ длительностей исполнения отдельных работ. Обозначается такая система через $\theta(T(a_1), T(p_1), T(a_2), T(p_2))$, где $\theta \in \{FCFS, LCFS, St\}$. Пространство состояний системы обозначается через T_θ^2 . Для типа St укажем сразу, что под T_θ^2 подразумевается двумерный тор, у которого фиксировано его представление в виде произведения двух окружностей (см. рис. 2), т. е. проекции на каждую из них. Предполагается, что окружности снабжены ориентацией, метрикой и разметкой. Соответствие между состоянием системы и состояниями ее компонент (заявок) устанавливается при помощи проекций. Динамика системы St задается векторным полем на T_θ^2 , проектирующимся в описанные выше единичные поля скоростей на сомножителях (так называемый простейший поток на торе). Для остальных систем пространство состояний и динамические системы на них будут описаны ниже. Для этих систем, тесно связанных с двумерным тором, будут, как и для системы St , существовать проекции на пространство состояний отдельных заявок.

3. Траектории динамических систем FCFS и их зависимость от параметров

Рассмотрим случай, когда в приборе Π используется дисциплина $FCFS$. Пространство состояний СМО с двумя заявками и такой дисциплиной представляет собой двумерный тор, из которого вырезана внутренность прямоугольника $LK_1O''K_2$ (рис. 3). Числа $T(a_i), T(p_i), i \in \{1, 2\}$ — это трудоемкости работ i -й заявки, исполняемых соответственно в приборах A_i и Π . В прямоугольнике $O'O''O''$ следует мысленно отождествить каждую точку его верхней стороны $O'O''$ с лежащей под ней точкой нижней стороны OO'' , а каждую точку левой стороны OO' — с лежащей на одной с ней высоте точкой правой стороны $O''O''$. При этом, в частности, совпадут точки, обозначенные одинаковыми буквами. Результат отождествления сторон — двумерный тор. Введем на торе оси координат OO' и OO'' , вычисляемых соответственно по модулю $T(a_2) + T(p_2)$ и по модулю $T(a_1) + T(p_1)$. Движение точек во внутренности указанного пространства и на отрезках K_1O'' и K_2O' осуществляется вдоль интегральных кривых указанного на рис. 3 векторного поля, все векторы которого

имеют единичные проекции на обе оси. Движение на отрезках K_1L и K_2L имеет только одну ненулевую проекцию вектора скорости, причем на K_1L — это проекция на ось OO' , а на K_2L — это проекция на OO'' . Динамику в точке L определим таким образом, чтобы вектор скорости имел единичную проекцию на OO'' и нулевую проекцию на OO' .

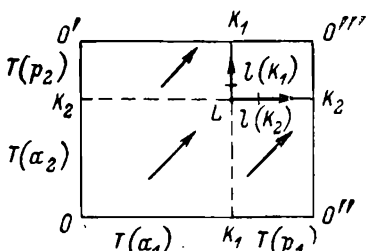


Рис. 3.

З а м е ч а н и е 1. Векторное поле на пространстве состояний задает отвечающую ему полугруппу сдвигов вдоль траектории векторного поля $\{\theta^t\}$, $t \in R_+$. Обычно $\{\theta^t\}$ называют полупотоком.

З а м е ч а н и е 2. Необходимость доопределения динамики в точке L обусловлена тем, что дисциплины в теории массового обслуживания не определяют логику обслуживания при одновременном появлении событий [3].

Заданная таким образом система $FCFS(T(a_1), T(p_1), T(a_2), T(p_2))$ полностью определяется значениями параметров. Заметим, что рассматриваемая динамическая система необратима, т. е. для произвольной точки однозначно определено лишь ее «будущее» и, быть может, отрезок «прошлого» (до попадания исходящей из данной точки обращенной во времени траектории системы $St(T(a_1), T(p_1), T(a_2), T(p_2))$ в прямоугольник $LK_1O''K_2$). Ниже будем исследовать вопрос о том, как заданный набор чисел определяет характер траекторий в описанной динамической системе и периоды этих траекторий. Как известно [4], в системе $St(T(a_1), T(p_1), T(a_2), T(p_2))$ при рациональном отношении чисел $T(a_1) + T(p_1)$ и $T(a_2) + T(p_2)$ (через p/q будем обозначать несократимое представление этого отношения) все траектории периодичны. Таким образом, если в системе $St(T(a_1), T(p_1), T(a_2), T(p_2))$ существует хотя бы одна периодическая траектория, не задевающая замкнутый прямоугольник $LK_1O''K_2$, то существует целое семейство таких траекторий. Все они имеют одинаковый период $T = p(T(a_2) + T(p_2)) = q(T(a_1) + T(p_1))$. Если же траекторий, не задевающих $LK_1O''K_2$, нет, то предельное поведение любой траектории совпадает с поведением одной из точек K_1 или K_2 . Проанализируем возможные типы предельного поведения этих точек. Траектория точки K_1 при первом своем возвращении может пересечь отрезок LK_1 (здесь и ниже см. рис. 3), а траектория точки K_2 — отрезок LK_2 . Назовем этот случай предельным поведением типа 1. Имеется возможность того, что траектории обеих точек K_1 и K_2 попадают при первых своих возвращениях на один и тот же отрезок LK_1 (или на LK_2). Это — предельное поведение типа 2. Наконец, предельным поведением типа 3 назовем такое предельное поведение точек K_1 и K_2 , когда они лежат на одной траектории. Заметим, что примеры систем $FCFS$ с предельным поведением типов 2 и 3 строятся легко. Докажем, что только при таких наборах чисел $T(a_1), T(p_1), T(a_2), T(p_2)$, когда $(T(a_1) + T(p_1))/(T(a_2) + T(p_2))$ рационально, в $FCFS$ имеет место предельное поведение типа 1. Для доказательства необходимо понятие специального представления полупотока. Рассмотрим преобразование T_1 на множестве M_1 , $f \geq 0$ — функция на M_1 . Пусть M — пространство, точками которого служат пары (x, s) , где $x \in M_1$, $0 \leq s \leq f(x)$. Пару вида $(x, f(x))$ отождествим с парой $(I_2, x, 0)$. Введем полупоток $\{\theta^t\}$ на M , под действием которого (x, s) движется вертикально вверх с единичной скоростью до достижения графика функции f ,

после чего мгновенно перескакивает в точку $(T_1x, 0)$ и продолжает свое движение вверх. Формально полупоток задается формулой:

$$\theta(x, s) = \left(T_1^n x, s + t - \sum_{k=0}^{n-1} f(T_1^k x) \right),$$

где n однозначно определяется из неравенства:

$$\sum_{k=0}^{n-1} f(T_1^k x) \leq s + t < \sum_{k=0}^n f(T_1^k x).$$

О п р е д е л е н и е 1. Полупоток $\{\theta^t\}$ называется специальным полупотоком, построенным по преобразованию T_1 и функции f ; а T_1 — базисным преобразованием полупотока. Полупоток допускает специальное представление, если он изоморфен (в естественном смысле) специальному полупотоку.

З а м е ч а н и е 3. Обычно множество M_1 наделено некоторой дополнительной структурой (измеримо или является топологическим пространством или пространством с мерой), а T_1 эту структуру сохраняет. Тогда и полупоток в легко уточняемом смысле сохраняет эту структуру. Нам придется иметь дело с ситуацией, когда M_1 — отрезок, T_1 и f — кусочно-линейные функции, угловые коэффициенты которых равны 0 или 1. Подробное описание нужных конструкций в ситуации, когда T_1 — сохраняющее меру обратимое преобразование, хорошо известно [6]. Обобщение на необратимые преобразования достаточно очевидно. Несколько сложнее обстоит дело с топологическими вопросами. Рассматриваемые полупотоки и преобразования оказываются, как правило, разрывными. Более педантичное рассмотрение этих вопросов требует введения специальных потоков над некоторыми (уже непрерывными) преобразованиями компактных пространств (как правило, вполне несвязных). Этими преобразованиями «накрываются» в естественном смысле появляющиеся ниже «перекладывания отрезков». При этом топологическую часть теории перекладываний приходится вновь доказывать для этих накрывающих преобразований. В статье используется путь компромиссов, чтобы воспользоваться результатами о перекладываниях (см. замечание 4).

Перейдем к доказательству. На рис. 3 видно, что для любой точки динамической системы имеется ее прообраз на разрезе $O'O''$, такой, что данная точка может быть получена из своего прообраза действием потока динамической системы St . Кроме того, каждая точка «угла» $O'O''$ под действием системы $FCFS$ снова когда-нибудь пересечет $O'O''$. Отсюда следует, что $O'O''$ может быть выбрано базисным множеством для специального представления динамической системы $FCFS$. График базисного преобразования (или преобразования последования) специального представления изображен на рис. 4, б. Базисное преобразование на $O'O''$ — букете окружностей может быть сопоставлено преобразованию на

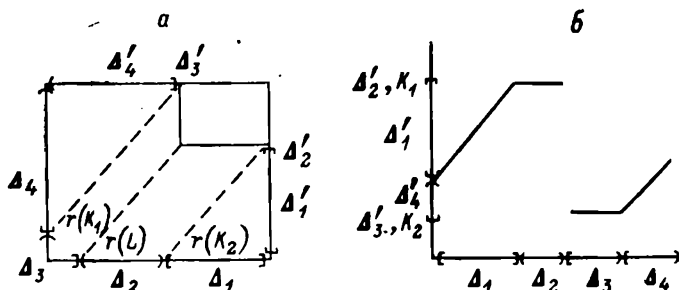


Рис. 4.

ориентированной окружности с длиной, равной длине отрезка $O'O''$, которую будем обозначать через $\mathbb{O}$. Введем отображение $O'O'' \rightarrow \mathbb{O}$ таким образом, чтобы оно сохранило метрические отношения на $O'O''$ (на $\mathbb{O}$ длина отрезков вводится в направлении ориентации, и начало координат соответствует точке O' (O'')). Тогда базисное преобразование на $O'O''$ после указанного в определении специального полупотока отождествления эквивалентно в смысле изучения асимптотического поведения базисному преобразованию на $\mathbb{O}$, если на последней действуют следующие преобразования: на дуге $(r(K_1))' O'$ ($r(K_2))'$ сдвиг на дугу длины $\alpha = \min(T(a_1) + T(p_1), T(a_2) + T(p_2))$; дуга $(r(K_1))'$ ($r(L))'$ переходит в точку K_1' , а дуга $(r(L))'$ ($r(K_2))'$ переходит в точку K_2' . Образ точки y под действием сдвига определяется как $f(y) = |\alpha + y|_{\text{mod } \beta}$, где $\beta = T(a_1) + T(p_1) + T(a_2) + T(p_2)$. Предположим, что предельный тип поведения точек K_1 и K_2 первый, т. е. траектория точки K_1 попадает в точку $l(K_1)$, а точки K_2 — в точку $l(K_2)$. В силу этого предположения существует такое n , что $(l(K_2))' = f^n(K_2')$ или $(l(K_1))' = f^n(K_1')$, причем $\forall i < n f^i(K_1') \in (r(K_1))' (r(L))' (r(K_2))'$, где $(r(K_1))' (r(L))' (r(K_2))'$ — соответствующая дуга $\mathbb{O}$. Предположим для определенности $f^n(K_1') = (l(K_1))'$. Так как $\|(l(K_1))' (l(K_2))'\| < \|K_1 K_2\|$, где $\|$ — длина отрезка, $f^{-n}((l(K_2))') \in K_1 D' K_2'$ и, следовательно, либо $(l(K_2))' = K_2'$, либо существует $i < n$, такое, что или $f^i(K_1') = (l(K_1))'$, или $f^i(K_2') = (l(K_2))'$, что противоречит выбору n .

Однако и при рациональном отношении $(T(a_1) + T(p_1))/(T(a_2) + T(p_2))$ не всегда возможен первый тип предельного поведения K_1 и K_2 (а следовательно, не всегда существует семейство периодических траекторий с периодом $T = \text{НОК}(T(a_1) + T(p_1), T(a_2) + T(p_2))$). Дополнительным условием существования такого типа предельного поведения траекторий точек K_1 и K_2 является то, что между ними можно вписать прямоугольник $LK_1 O'' K_2$. Это означает, что длина отрезка между прообразами этих точек на полуинтервале $O'O''$ должна быть равна $T(p_1) + T(p_2)$. Это возможно в том случае, если площадь, покрываемая полосой между траекториями точек K_1 и K_2 , меньше или равна площади поверхности соответствующего $\mathbb{T}_{3t}^2$, т. е. если $T(T(p_1) +$

$+ T(p_2)) \leq (T(a_1) + T(p_1))(T(a_2) + T(p_2))$, где T — период, следовательно:

$$T \leq \frac{(T(a_1) + T(p_1))(T(a_2) + T(p_2))}{T(p_1) + T(p_2)}.$$

Таким образом, доказано следующее:

Теорема 1. Для динамической системы $FCFS(T(a_1), T(p_1), T(a_2), T(p_2))$ верно следующее: 1) если отношение $(T(a_1) + T(p_1)) / (T(a_2) + T(p_2))$ рационально и НОК $(T(a_1) + T(p_1), T(a_2) + T(p_2)) \leq \frac{(T(a_1) + T(p_1))(T(a_2) + T(p_2))}{T(p_1) + T(p_2)}$, то у системы имеются только предельные периодические траектории, период которых вычисляется как НОК $(T(a_1) + T(p_1), T(a_2) + T(p_2))$; 2) если отношение $(T(a_1) + T(p_1)) / (T(a_2) + T(p_2))$ иррационально или если оно рационально, но НОК $(T(a_1) + T(p_1), T(a_2) + T(p_2)) > \frac{(T(a_1) + T(p_1))(T(a_2) + T(p_2))}{T(p_1) + T(p_2)}$, то имеет место или предельное поведение типа 2, или предельное поведение типа 3.

Можно доказать следующее.

Утверждение 1. Существует сходящийся алгоритм, классифицирующий типы предельного поведения на T_{FCFS}^2 и вычисляющий периоды предельных траекторий.

4.5 Траектории динамической системы LCFS и их зависимость от параметров

Рассмотрим случай, когда обслуживание прибором P производится в соответствии с дисциплиной $LCFS$. Пространство состояний такой системы с двумя заявками представляет собой двумерный тор, из которого вырезан прямоугольник $LK_1O''K_2$ с последующей заклейкой этого прямоугольного отверстия двумя геометрически равными вырезанному прямоугольниками. Один из этих прямоугольников подклеен сторонами K_1L и $O''K_2$ и имеет край LK_2 , но лишен края $O''K_1$, а другой подклеен к LK_2 и $O''K_1$ и имеет край $O''K_2$, но лишен края LK_1 . Будем называть эти прямоугольники соответственно верхним и нижним листами. Изображение на рис. 5 представляет собой развертку, полученную, как и выше, разрезанием тора с дважды заклеенным прямоугольником по окружностям, первая из которых проходит через линию вклейки $O''K_1$ нижнего листа, а вторая — через линию вклейки $O''K_2$ верхнего листа. Как и ранее, введем на торе координатные оси OO' и OO'' . Движение на построенном объекте определяется стандартным потоком на части, оставшейся от обычного тора, а на вклейках может быть описано следующим образом: на верхнем листе проекция вектора скорости на OO' равна 0, а проекция на OO'' равна 1. На нижнем листе проекция вектора скорости на OO' равна 1, а проекция на OO'' равна 0. В определенной таким образом динамической системе поле в точке L совпадает

[illegible]

Рис. 5.

Нетрудно проверить, что существует мера, сохраняемая потоком в $LCFS$. Такой мерой является обычная площадь с учетом того, что прямоугольник $LK_1O''tK_2$ представлен в системе дважды.

З а м е ч а н и я 4. В *LCFS* поведение точки K_2 отличается от согласующегося со здравым смыслом поведения рассматриваемой СМО в соответствующем состоянии. В самом деле, работа p_1 завершена, однако заявка 1 остается в приборе П до тех пор, пока завершится работа p_2 , и лишь затем обе заявки покидают прибор П. Такое определение связано с нашим намерением воспользоваться известными результатами, относящимися к топологической динамике и эргодической теории «перекладываний отрезков», и позволяет обойтись без модификации этих результатов, в которых все рассматриваемые отрезки считаются содержащими свои левые концы и не содержащими правые (можно, разумеется, поменять их ролями одновременно для всех интервалов). Ценой усложнения формулировок результатов и модификации доказательств можно, по-видимому, получить симметричную форму нужных результатов, которая сняла бы проблемы, связанные с неестественностью определения динамики угловых точек прямоугольника $LK_1O''tK_2$. Предпочтительнее, однако, модифицировать в одной точке динамику нашей системы. В вопросах же, допускающих пренебрежение множествами меры 0, произведенная модификация поведения СМО вообще не играет роли (см. замечание 3).

В последующих рассуждениях существенная роль отводится перекладываниям отрезков, поэтому приведем определение перекладывания и ряд результатов, относящихся к ним. Пусть $M = [0, 1]$; $\xi = (\Delta_1, \dots, \Delta_r)$ — разбиение M на r , $2 \leq r \leq \infty$ непесекающихся полуинтервалов, занумерованных слева направо; $\pi = (\pi_1, \dots, \pi_r)$ — некоторая перестановка чисел $1, \dots, r$.

О п р е д е л е н и е 2 [5]. Преобразование $\theta : M \rightarrow M$, являющееся сдвигом на каждом из полуинтервалов Δ_i , $1 \leq i \leq r$, и такое, что Δ_i переставляется в соответствии с перестановкой π , т. е. полуинтервалы $\Delta'_i = \theta \Delta_i$ примыкают друг к другу в порядке $\Delta'_{\pi_1}, \dots, \Delta'_{\pi_r}$, называется переключиванием, соответствующим перестановке π и разбиению ξ . Перестановка π называется приводимой, если $\pi(\{1, 2, \dots, j\}) = \{1, 2, \dots, j\}$ при некотором j , $1 \leq j \leq r$. Поток называется строго эргодическим, если нормиро-

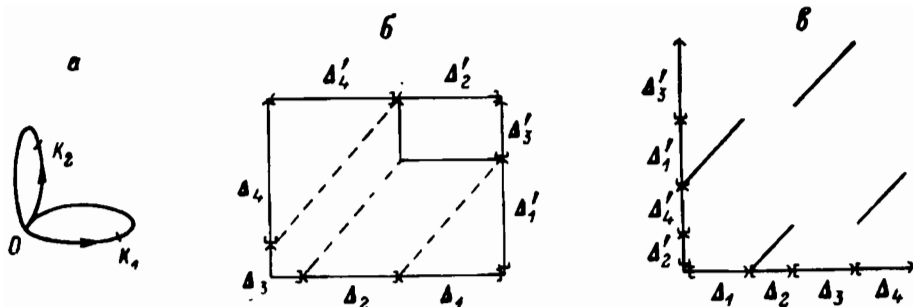


Рис. 6.

ванная инвариантная относительно потока борелевская мера единственна.

Т е о р е м а 2 [5, 7]. Следующие свойства перекладывания θ эквивалентны: 1) θ — апериодично (θ не имеет периодических точек); 2) θ — топологически транзитивно (θ имеет всюду плотную траекторию); 3) θ — минимально (все траектории всюду плотны); 4) траектории точек разрыва θ бесконечны и для разных точек разрыва не пересекаются между собой.

Будем задавать всякое перекладывание парой (λ, π) , где λ — вектор $\lambda = (\lambda_1, \dots, \lambda_r)$, $\lambda_i \geq 0$, состоящий из длин представляемых полуинтервалов, а π — перестановка. Обозначим это перекладывание $\theta_{\lambda, \pi}$.

Т е о р е м а В и ч а—М а з у р а [8, 9]. Пусть $r \geq 2$ и перестановка π — неприводима. Тогда множество $\lambda \in R_+^r$, для которых $\theta_{\lambda, \pi}$ не строго эргодично, имеет нулевую меру Лебега.

Перейдем к *LCFS*. На рис. 6, а изображен букет ориентированных окружностей, который на рис. 5 изображается как OO' и OO'' . Ориентация задается проекцией векторного поля. Из рис. 5 очевидно, что этот букет окружностей является секущей для *LCFS* ($T(a_1)$, $T(p_1)$, $T(a_2)$, $T(p_2)$). Как видно из рис. 5, $O'OO''$ находится в каноническом соответствии с секущей на рис. 6. Поэтому в качестве базисного множества для специального представления потока $\{\theta^t\}$ можно взять полуинтервал $O'OO''$. Преобразы точек K_1 , L , K_2 на $O'OO''$ в *LCFS* задают разбиение $O'OO''$ на полуинтервалы (рис. 6, б). Этот же рисунок иллюстрирует переход полуинтервалов Δ_i , $i \leq 4$ в полуинтервалы Δ'_i . Значение функции f специального представления в точке $y \in \Delta_i$ равно времени перехода y в $y' \in \Delta'_i$. На рис. 6, в приведен график базисного автоморфизма специального представления $\{\theta^t\}$. Из этого рисунка видно, что базисным автоморфизмом *LCFS* является перекладывание отрезков, а перестановка $\pi(\{1, 2, 3, 4\}) = \{3, 1, 4, 2\}$ — неприводима. Отсюда, по теореме Вича—Мазура, следует, что базисный автоморфизм специального потока $\{\theta^t\}$, построенного по *LCFS*, строго эргодичен для почти всех по мере Лебега на R_+^r наборов чисел $T(a_1)$, $T(p_1)$, $T(a_2)$, $T(p_2)$. Для *LCFS* нетрудно проверить следующие факты: 1) если базисный

автоморфизм специального потока $\{\theta_t^I\}$ строго эргодичен, то и поток $\{\theta_t\}$ строго эргодичен; 2) если базисный автоморфизм специального потока $\{\theta_t^I\}$ минимален, то и поток $\{\theta_t^I\}$ минимален. Таким образом, из теоремы Вича—Мазура и сделанных замечаний вытекает следующая теорема.

Т е о р е м а 3. Для почти всех наборов чисел $T(a_1)$, $T(p_1)$, $T(a_2)$, $T(p_2)$ по мере Лебега на R_+^4 поток $\{\theta_t^I\}$ на $\mathbb{T}_{LCFS}^2$ минимален, строго эргодичен и единственная сохраняемая им мера — нормированная площадь.

З а м е ч а н и е 5. Пребывание заявок в состоянии исполнения каждого из возможных сочетаний работ назовем дискретным состоянием. Будем различать дискретное состояние, когда выполняется работа p_1 , а исполнение работы p_2 начато, но прервано на время исполнения работы p_1 , от дискретного состояния, когда выполняется работа p_2 , а исполнение работы p_1 начато, но прервано на время исполнения работы p_2 . Вероятности пребывания системы в различных дискретных состояниях, представляющие практический интерес, могут быть рассчитаны по следующим формулам (нумерация состояний дана рис. 5):

$$\begin{aligned} P_I &= \frac{T(a_1) T(a_2)}{(T(a_1) + T(p_1))(T(a_2) + T(p_2)) + T(p_1) T(p_2)}, \\ P_{II} &= \frac{T(a_1) T(p_2)}{(T(a_1) + T(p_1))(T(a_2) + T(p_2)) + T(p_1) T(p_2)}, \\ P_{III} &= \frac{T(a_2) T(p_1)}{(T(a_1) + T(p_1))(T(a_2) + T(p_2)) + T(p_1) T(p_2)}, \\ P_{IV} &= P_V = \frac{T(p_1) T(p_2)}{(T(a_1) + T(p_1))(T(a_2) + T(p_2)) + T(p_1) T(p_2)}. \end{aligned}$$

Интересно, что эти же формулы соответствуют СМО с дисциплиной $LCFS$ и экспоненциально распределенными временами исполнения работ, если средние значения этих времен совпадают со значениями параметров рассматриваемой нами системы.

Заключение

Приемы, связанные с изучением специального представления, могут быть полезны при изучении других вариантов систем в случае двух заявок. Удастся проанализировать системы с приоритетной дисциплиной обслуживания в приборе П (см. [3]). Пространство состояний системы с двумя заявками сходно с изображенным на рис. 5. Однако в этом случае вырезанный прямоугольник $LK_1O''tK_2$ без края $O''K_1$ заклеен геометрически равным ему прямоугольником, подклеенным к сторонам K_1L , K_2L , $O''K_2$, а векторное поле на нем имеет единичную проекцию на OO'' и нулевую на OO' .

Т е о р е м а 4. Для наборов попарно несоизмеримых чисел $T(a_1)$, $T(p_1)$, $T(a_2)$, $T(p_2)$ в описанной динамической системе имеется единственная предельная периодическая траектория.

Изучению поддается существенный с точки зрения теории СМО случай, когда дисциплина обслуживания в приборе П — разделение времени. С учетом обычного для теории СМО допущения, заключающегося в том, что время переключения с работы на работу стремится к нулю, пространством состояний такой системы является обычный тор, динамика на всей поверхности которого, кроме прямоугольника $LK_1O''tK_2$, определяется как в $St(T(a_1), T(p_1), T(a_2), T(p_2))$, а на указанном прямоугольнике векторное поле направлено так же, как в St , но имеет значения проекций вектора скорости на обе оси, равные 0,5.

Т е о р е м а 5. Для наборов попарно несоизмеримых чисел $T(a_1), T(p_1), T(a_2), T(p_2)$ поток на пространстве состояний этой системы строго эргодичен и сохраняет обычную нормированную площадь, взятую с учетом удвоения площади прямоугольника $LK_1O''K_2$.

Перенос полученных результатов на СМО с тремя и более заявками приводит к непреодолимым в данный момент трудностям.

Литература

1. Вольперт А. Б., Гордин М. И. Об одном классе математических моделей динамики аппаратно-программных средств измерительно-вычислительных комплексов//Процессорные средства электрических измерений. Л., 1984, с. 60—75.
2. Gordin M. I. Ergodic properties of a class of queuing systems//Тез. 1-го Всемирного конгресса общества математической статистики и теории вероятностей им. Бернулли. Т. 2. М., 1986, с. 546.
3. Башарин Г. П., Толмачев А. Л. Теория сетей массового обслуживания и ее применение к анализу информационно-вычислительных систем//Итоги науки и техники: Теория вероятностей, математическая статистика, теоретическая кибернетика. Т. 21. М., 1983, с. 3—120.
4. Арнольд В. И. Дополнительные главы теории обыкновенных дифференциальных уравнений. М., 1978.
5. Вершик А. М., Корнфельд И. П. Периодические аппроксимации и их приложения: Эргодические теоремы, спектральная и энтропийная теория для действий общих групп//Итоги науки и техники: Современные проблемы математики. Фундаментальные направления. Т. 2. М., 1985, с. 70—89.
6. Вершик А. М. Траекторная теория//Там же, с. 89—106.
7. Kean M. Interval exchange transformations//Math. Z. 1975. Vol. 141, N 1, P. 25—31.
8. Veech W. A. Gauss measures for transformations on the space of interval exchange maps//Ann. Math. 1982. Vol. 115, N 1, P. 201—242.
9. Masur H. Interval exchange transformations and measured foliations//Ann. Math. 1982. Vol. 115, N 1, P. 169—200.

ПЛАНИРОВАНИЕ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ВЫВОДА В АТТРИБУТНЫХ КС-ГРАММАТИКАХ

1. Введение

К числу ключевых проблем создания экспертных систем (ЭС) относится проблема планирования вычислений при поиске ответов на такие запросы пользователя, которые требуют синтеза программ на основе содержимого базы знаний (БЗ).

В работе [1] рассмотрен подход к представлению знаний на основе формализма атрибутивных грамматик. В рамках этого подхода оказывается возможным построить эффективные алгоритмы планирования вычислений за счет того, что планирование сводится к поиску вывода в контекстно-свободной (КС) грамматике. При этом возможно решение ряда дополнительных задач, в частности таких, как анализ корректности запроса пользователя и реализация функций подсказки по вариантам задания недостающих данных при некорректном запросе, задача автоматического синтеза алгоритмической избыточности в целях обеспечения семантической надежности вычислений и ряд других.

Предлагаемый вариант построения алгоритмов планирования вычислений является альтернативой традиционному подходу на основе методов логического вывода в исчислениях предикатов.

2. Выразительные возможности атттрибутивных грамматик с КС-ядром

Аттрибутивной грамматикой с КС-ядром принято называть пятерку вида [2]:

$$G_A = \langle V_T, V_N, P, S, At \rangle,$$

где V_T — множество терминальных символов, V_N — множество нетерминальных символов, P — множество КС-правил вывода (подстановки) вида $Y_i \rightarrow \alpha_j$, где $Y_i \in V_N$, $\alpha_j \in (V_T \cup V_N)^*$, S — аксиома, $S \in V_N$, At — атрибутивная компонента грамматики G_A . Не вдаваясь в детали возможных заданий атрибутивной компоненты At , отметим, что в нее входят множество символов

атрибутов, правила сопоставления атрибутов символам грамматики из алфавита $V_T \cup V_N$, а также правила вычисления значений атрибутов в каждом правиле вывода множества P .

Выразительные возможности атрибутивных грамматик определяются следующим набором утверждений.

Утверждение 1. Пусть G_B — двухуровневая грамматика А. ван Вейгардена [3, 4]. По любой G_B -грамматике может быть построена эквивалентная ей атрибутная грамматика G_A с КС-ядром.

Утверждение 2. По любой формальной грамматике G произвольного вида может быть построена эквивалентная ей G_B -грамматика.

Следствие. По любой формальной грамматике произвольного вида может быть построена эквивалентная ей атрибутная грамматика G_A с КС-ядром.

Первое из утверждений доказывается путем указания конструктивного способа построения грамматики G_A по грамматике G_B , второе доказано в работе [5], следствие является транзитивным замыканием утверждений 2 и 1.

Из следствия вытекает, что с помощью G_A -грамматики с КС-ядром можно задать любой рекурсивно-перечислимый язык. Это означает, что по своим выразительным возможностям методы представления знаний на основе формализма G_A -грамматик с КС-ядром не уступают предикатным языкам. Однако преимущества такого описания по сравнению с предикатными языками обусловлены тем фактом, что существуют эффективные алгоритмы поиска вывода в грамматиках с КС-ядром. Именно эти алгоритмы и составляют существо предлагаемых далее процедур планирования вычислений. Заметим, что в большинстве случаев при описании процедурной компоненты БЗ можно ограничиться частными случаями КС-грамматик, например такими, как $LL(k)$ - или $LR(k)$ -грамматиками [6] вплоть до автоматных грамматик, что еще более упрощает задачу обеспечения эффективности планировщика вычислений.

3. Компоненты и структура описания процедурных баз знаний

При формализации семантики предметной области с процедурной компонентой необходимо предусматривать средства описания знаний следующих типов: о вычислимости одних множеств характеристик через другие и о структуре этих знаний в виде вычислительных моделей (ВМ); о структуре связей на множестве ВМ; о программах, реализующих компоненты ВМ.

В модели процедурных БЗ для описания перечисленных компонент будем использовать следующие базовые понятия.

1) Модель задачи (МЗ), которая задается именем, указанием множеств имен входов и выходов, спецификацией входов и выходов и ссылкой либо на ВМ, в которую данная МЗ погружена, либо

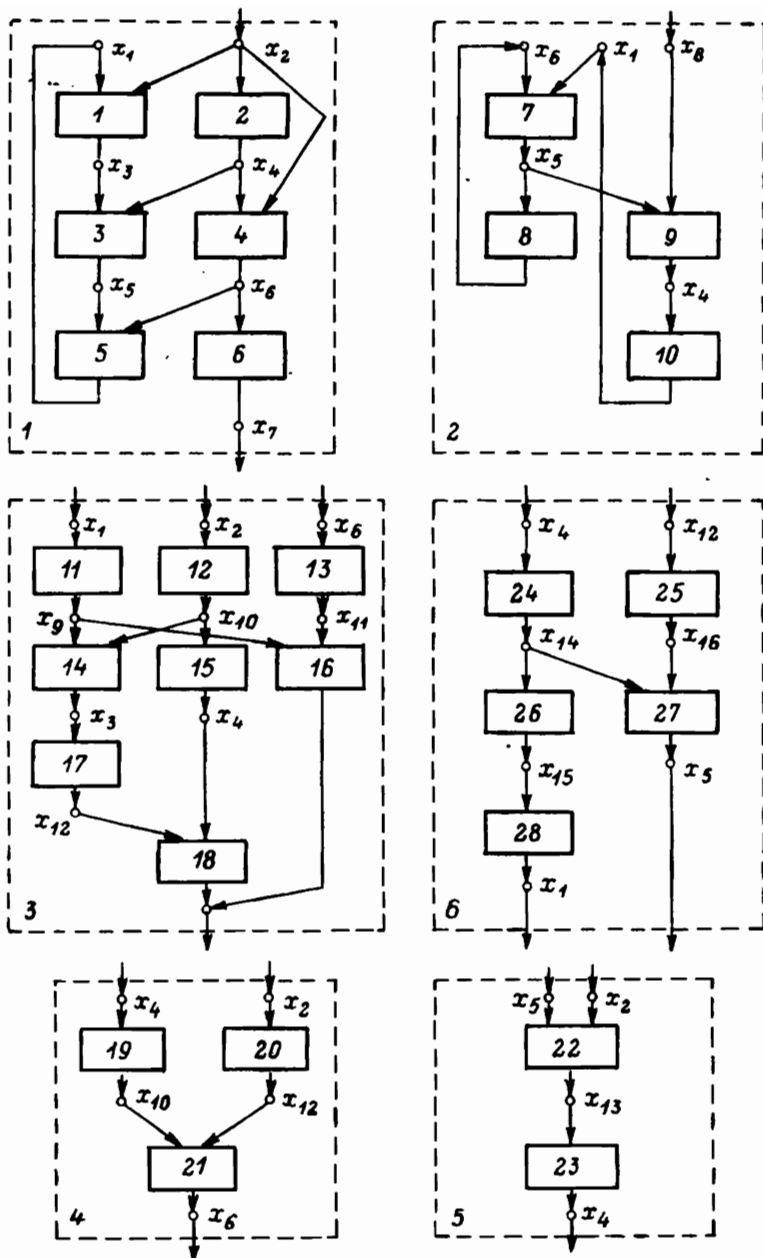


Рис. 1. Структура процедурной компоненты БЗ с указанием номеров моделей задач и связей между ними.

№ модели задачи МЗ	Спецификация связи	№ модели задачи МЗ	Спецификация связи	№ модели задачи МЗ	Спецификация связи	№ модели задачи МЗ	Спецификация связи
1	ВМ3	8	f_3	15	f_5	22	f_9
2	ВМ3	9	ВМ5	16	f_6	23	f_7
3	ВМ3	10	ВМ6	17	f_7	24	f_8
4	ВМ4	11	f_2	18	ВМ6	25	f_5
5	f_1	12	f_4	19	f_8	26	f_2
6	f_2	13	f_5	20	f_8	27	f_9
7	ВМ3	14	f_6	21	f_9	28	f_4

на программный модуль, который является программной реализацией этой МЗ.

2) Вычислительная модель, которая характеризуется множеством потенциальных входов X и выходов Y , множеством МЗ, входящих в состав ВМ, описанием структуры ВМ на множестве МЗ, а также таблицей связей МЗ.

3) Реализация МЗ, задаваемая именем процедуры, множеством формальных параметров входов и выходов, а также текстом программы решения задачи на некотором языке.

Этих компонент достаточно для описания знаний всех ранее указанных типов. Что касается декларативной компоненты БЗ и организации работы с ними, то эти вопросы относительно хорошо исследованы, а их подключение к процедурной компоненте связано с решением обычных проблем системного программирования.

На рис. 1 и в таблице приведен пример описания структуры процедурной компоненты БЗ в терминах введенных базовых понятий. В таблице содержится информация о связях МЗ с другими ВМ или реализациями соответствующих МЗ. Ее и будем называть таблицей связей МЗ.

4. Формальное описание базы знаний

Для формального описания БЗ будем использовать аппарат атрибутивных грамматик с КС-ядром. С помощью таких грамматик, как уже было показано, можно задать любой рекурсивно-перечислимый язык.

Сопоставим каждой ВМ атрибутивную грамматику G_A следующим образом. Множеству X потенциальных входов ВМ поставим в соответствие множество терминальных символов $V_T = \{x_1, x_2, \dots, x_m\}$, $x_i \in X$, множеству Y — множество нетерминальных символов $V_N = \{Y_1, Y_2, \dots, Y_n\}$. Множеству МЗ, входящих в ВМ, поставим в соответствие множество атрибутов $\{\langle \text{МЗ}.i \rangle\}$, $i \in I(\text{ВМ})$, где $I(\text{ВМ})$ — индексное множество МЗ, входящих в ВМ.

Пусть $\langle \text{МЗ}.i \rangle$, $i \in I(\text{ВМ})$ — некоторая модель задачи из ВМ. Она характеризует отношение вычислимости:

$$y_k = \langle \text{МЗ}.i \rangle (x_{i_1}, x_{i_2}, \dots, x_{i_r}). \quad (1)$$

Запишем это отношение в виде следующего правила подстановки с атрибутом:

$$Y_k \langle \varphi_{k_s} \rangle \rightarrow Y_{i_1} Y_{i_2} \dots Y_{i_r} \langle M3.i \rangle, \quad \varphi_{k_s} = \langle M3.i \rangle, \quad (2)$$

где Y_k — нетерминал, сопоставленный величине y_k , а $Y_{i_1}, Y_{i_2}, \dots, Y_{i_r}$ — нетерминалы, сопоставленные аргументам $x_{i_1}, x_{i_2}, \dots, x_{i_r}$ вычислительной модели. Выражение (2) означает, что Y_k выводимо (в нашем случае вычислимо) из величин, отвечающих нетерминалам $Y_{i_1}, Y_{i_2}, \dots, Y_{i_r}$ с помощью функции φ_{k_s} , которая в данном случае отвечает преобразованию, задаваемому $\langle M3.i \rangle$. Порядок следования символов в подстановке (2) должен совпадать с порядком следования аргументов в формуле (1). Кроме того, каждой величине из множества потенциальных входов поставим в соответствие безатрибутную подстановку $Y_i \rightarrow x_i$, что означает, что соответствующий потенциальный вход может быть и исходным данным.

Далее подстановки вида (2) будем записывать в виде:

$$Y_k \rightarrow \langle M3.i \rangle Y_{i_1} Y_{i_2} \dots Y_{i_r}, \quad (3)$$

имея в виду, что символ $\langle M3.i \rangle$ является атрибутом. Это оказывается удобным в дальнейшем при алгоритмизации процессов планирования вычислений. Итак, основные компоненты ВМ описаны в терминах грамматики G_A (ВМ).

Для каждой ВМ из БЗ может быть сформулирована задача вида: дано X_k , найти Z_l , где $X_k \subset X$ (ВМ), $Z_l \subset Z$ (ВМ). Не каждая из таких задач разрешима. Неразрешимость здесь обусловливается возможной недостаточностью исходных данных для получения результатов. Поэтому для любой задачи в рамках конкретной ВМ необходимо решать следующие подзадачи: 1) корректно ли поставлена задача; 2) если не корректно, то каких данных не хватает для разрешимости; 3) если задача корректна, то как найти план ее решения.

Сформулированные вопросы должны решаться в процессе функционирования систем формирования ответов на запросы, т. е. ответы на эти вопросы — функция средств системы управления БЗ. Однако поскольку рассматривается концепция единой алгоритмической основы для представления знаний и методов работы с ними, то задачу формализации и представления знаний необходимо решать с учетом удобства решения тех задач, которые традиционно относятся к системе управления БЗ.

Эффективные алгоритмы решения этих подзадач могут быть получены при использовании алгебраического подхода к заданию языка, в котором грамматики рассматриваются как генераторы формальных степенных рядов в некоммутативных переменных из алфавита терминальных символов [7—9]. При этом язык задается в виде систем уравнений от переменных — нетерминалов, а КС-грамматике с n нетерминалами соответствует система из n уравнений с положительными коэффициентами, которая имеет един-

ственное решение в виде n степенных рядов. Каждое такое решение называют синтаксическим классом грамматики. Уравнения для языка получаются на основе представления грамматики в векторно-матричном виде [7]:

$$Y = AY + F, \quad (4)$$

где Y — вектор нетерминалов грамматики, A и F — соответственно матрица и вектор цепочек в алфавите $V_T \cup V_N$, операция произведения понимается как операция конкатенации цепочек символов грамматики, а сложение — как теоретико-множественное объединение цепочек. Покажем, каким образом можно получить подобное формальное описание на примере BM_1 , структура которой представлена на рис. 1. Для $G_A(BM_1)$ имеем:

$$V_T = \{x_1, x_2, \dots, x_6\}, \quad V_N = \{Y_1, Y_2, \dots, Y_7\},$$

$$P = \{Y_1 \rightarrow \langle M3.5 \rangle Y_5 Y_6, \quad Y_3 \rightarrow \langle M3.1 \rangle Y_1 Y_2, \quad Y_4 \rightarrow \langle M3.2 \rangle Y_2,$$

$$Y_5 \rightarrow \langle M3.3 \rangle Y_3 Y_4, \quad Y_6 \rightarrow \langle M3.4 \rangle Y_2 Y_4, \quad Y_7 \rightarrow \langle M3.6 \rangle Y_6,$$

$$Y_1 \rightarrow x_1, \quad Y_2 \rightarrow x_2, \quad Y_3 \rightarrow x_3, \quad Y_4 \rightarrow x_4, \quad Y_5 \rightarrow x_5, \quad Y_6 \rightarrow x_6\}$$

В векторно-матричной форме грамматика $G_A(BM_1)$ имеет такой вид:

$$Y = \begin{bmatrix} \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \langle M3.5 \rangle Y_5 & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset \langle M3.1 \rangle Y_1 & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset \langle M3.2 \rangle & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset \langle M3.3 \rangle Y_3 & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset \langle M3.4 \rangle Y_4 & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \langle M3.6 \rangle & \emptyset \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \\ Y_6 \\ Y_7 \end{bmatrix} + \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ \emptyset \end{bmatrix}. \quad (5)$$

В выражении (5) символ $\emptyset$ означает нуль алгебры формальных степенных рядов по отношению к операции конкатенации. Принцип формирования матрицы A из этого примера улавливается очень просто, а вектор F составляется на основе подстановок из множества P , которые не содержат справа нетерминалов.

5. Планирование вычислений

Рассмотрим обоснование и сам алгоритм планирования вычислений в пределах одной ВМ. Этот алгоритм основывается на некоторых свойствах матричных итераций в грамматике, заданной в форме (4).

Высотой цепочки терминалов будем называть высоту дерева вывода этой цепочки [5]. Обозначим символом $X^{(1)}$ вектор всех терминальных цепочек, выводимых в грамматике за один шаг. Пусть

$$X^{(k+1)} = A(X^{(k)})X^{(k)} + X^{(k)}, \quad X^{(1)} = F, \quad k = 1, 2, \dots \quad (6)$$

Свойства матричных итераций вида (6) формулируются в следующих теоремах.

Т е о р е м а 1. Перечисление всех терминальных цепочек грамматики $G_A(ВМ)$ с КС-ядром задается итерациями (6).

С л е д с т в и е. Если Y_i — конечный (нерекурсивный) синтаксический класс грамматики $G_A(ВМ)$, то $X_i^{(k)} = X_i^{(k+1)}$, причем $k \leq n$.

Теорема 1 доказывается методом математической индукции. Заметим, что следствие дает лишь необходимое условие.

Конструктивный метод выделения пустых (непроизводящих) нетерминалов дает следующая теорема.

Т е о р е м а 2. Пусть R_k — число координат вектора $X^{(k)}$, имеющих значение $\emptyset$. Если $R_{k+1} = R_k$ для некоторого $k < n$, то $R_{k+l} = R_k$ для любого $l = 1, 2, \dots$.

Теорема 2 доказывается индукцией по l . Практическое ее значение в том, что с помощью содержащегося в ней результата можно построить эффективный алгоритм анализа корректности запроса пользователя на решение задачи.

Общая схема алгоритма планирования вычислений изображена на рис. 2. Прежде чем дать его краткую характеристику, заметим, что для каждого блока алгоритма имеется эффективная алгоритмизация. Здесь же излагаются лишь самые общие идеи этой алгоритмизации.

Планирование начинается с выполнения подалгоритма «Управление синтезом плана вычислений», цель которого — по входному заданию построить редуцированную грамматику для используемой ВМ. Редукция состоит в том, что в множестве V_T остаются только символы, соответствующие входным данным, а в множестве V_n — только так называемые активные нетерминалы. Покажем, каким образом они определяются.

Введем два бинарных отношения. Одно из них определим на декартовом произведении $V_n \times M$, где M — множество МЗ рассматриваемой ВМ. В него включаются все пары $\langle Y_i, M3.J \rangle$, в которых Y_i соответствует выходу модели МЗ. J . Обозначим это отношение и его матрицу смежности символом MY . Второе отношение определим на декартовом произведении $M \times V_n$. В него включим те пары $\langle M3.J, Y_l \rangle$, для которых Y_l соответствует входу модели задачи МЗ. J . Это отношение и его матрицу смежности обозначим символом YM .

Назовем активными нетерминалы, входящие в транзитивное замыкание композиции отношений $YM \circ MY$, построенное для того подмножества $Y^{(1)}$ из V_n , которое соответствует искомым величинам. Транзитивное замыкание строится с помощью конечного числа умножений вида: $M^{(k)} = MY \cdot Y^{(k)}$, $Y^{(k+1)} = YM \cdot M^{(k)}$, причем $1 \leq k \leq n$, $Y^{(1)}$ — вектор, составленный из компонент множества $Y^{(1)}$, а итерации продолжаютсЯ до тех пор, пока на двух последующих шагах не совпадут множества ненулевых компонент векторов $Y^{(k)}$ и $Y^{(k+1)}$. Нетерминал $Y \in V_n$ будет

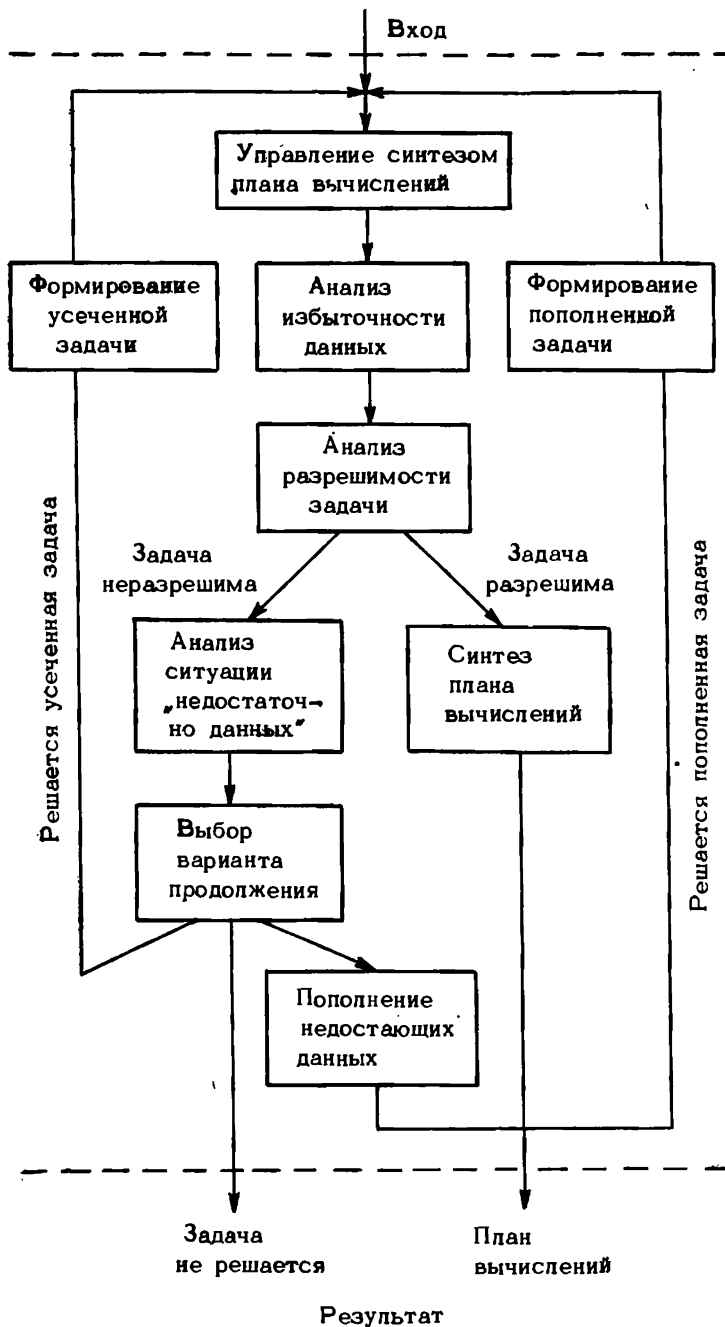


Рис. 2. Схема алгоритма планирования вычислений.

активным, если ему соответствует величина x рассматриваемой ВМ, которая потенциально может участвовать в некоторой схеме вычислений для получения искоемых величин.

Второй шаг редукции грамматики G_A (ВМ) состоит в удалении из описывающей ее матрицы строк и столбцов, отвечающих «неактивным нетерминалам». Аналогичное выполняется по отношению к векторам X и F в представлении (4).

Пусть V_n^a — множество активных нетерминалов, V_n^{bx} — множество нетерминалов, отвечающих входным данным задачи, а V_n^{bxy} — выходным данным. Очевидно, $V_n^{bxy} \subset V_n^a$, а $V_n^{bx} \setminus V_n^a$ задает множество тех данных, которые не будут использованы в схеме решения задачи. Эти данные являются избыточными, их поиск осуществляется на втором шаге планирования вычислений.

Анализ разрешимости поставленной задачи осуществляется путем выполнения матричных итераций в редуцированной грамматике G_A^p (ВМ) с использованием теоремы 2.

При наличии некорректности постановки задачи планировщик по специальному алгоритму, базирующемуся на совместном использовании матричного представления грамматики и матриц смежности YM и MY , устанавливает все возможные способы доопределения исходных данных, которые обеспечивают разрешимость задачи.

В случае корректности постановки задачи осуществляется построение плана вычислений на основе матричных итераций вида (6) в редуцированной грамматике G_A^p (ВМ). Покажем это на примере задачи, сформулированной для ВМ1 (см. рис. 1), исходная грамматика которой имеет представление (5). Рассмотрим задачу, в которой заданы величины x_2, x_5 , а найти требуется величины x_3 и x_6 . Для нее $V_n^a = \{Y_1, Y_2, Y_3, Y_4, Y_5, Y_6\}$, $V_T^p = \{x_2, x_5\}$, а представление G_A^p (ВМ) имеет вид:

$$Y = \begin{bmatrix} \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \langle M3.5 \rangle Y_5 \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset & \langle M3.1 \rangle Y_1 & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset & \langle M3.2 \rangle & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \langle M3.3 \rangle Y_3 & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \langle M3.4 \rangle Y_2 & \emptyset & \emptyset \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \\ Y_6 \end{bmatrix} + \begin{bmatrix} \emptyset \\ x_2 \\ \emptyset \\ \emptyset \\ x_5 \\ \emptyset \end{bmatrix}.$$

Прежде чем решать поставленную задачу, сделаем замечание относительно уравнения (6). Если некоторая терминальная цепочка появляется в итерации с номером k , то далее она будет появляться вновь и в каждой последующей итерации. Чтобы

исключить повторение, достаточно вместо (6) использовать такую схему итераций:

$$\begin{aligned}\Delta X^{(k+1)} &= A(\Delta X^{(k)})X^{(k+1)} + A(X^{(k)})\Delta X^{(k)}, \\ X^{(k+1)} &= X^{(k)} + \Delta X^{(k+1)},\end{aligned}\quad (7)$$

при этом $X^{(1)} = F$, $X^{(2)}$ и $\Delta X^{(2)}$ должны быть получены из уравнения (6), а итерации по схеме (7) — выполняться для $k = 3, 4, \dots$.

В примере $X^{(1)} = F = \langle \emptyset, x_2, \emptyset, \emptyset, x_5, \emptyset \rangle^T$, после первой итерации по уравнению (6) получаем:

$$\begin{aligned}\Delta X^{(2)} &= \langle \emptyset, \emptyset, \emptyset, \langle \text{МЗ. 2} \rangle x_2, \emptyset, \emptyset \rangle^T, \\ X^{(2)} &= \langle \emptyset, x_2, \emptyset, \bar{x}_4, x_5, \emptyset \rangle^T, \\ \bar{x}_4 &= \langle \text{МЗ. 2} \rangle x_2,\end{aligned}\quad (8)$$

а $\bar{x}_4$ следует рассматривать как метасимвол грамматики $\mathcal{B}_A$ (ВМ1). Первая итерация по схеме (7) дает:

$$\begin{aligned}\Delta X^{(3)} &= \langle \emptyset, \emptyset, \emptyset, \emptyset, \emptyset, \langle \text{МЗ. 4} \rangle x_2 \bar{x}_4 \rangle^T, \\ X^{(3)} &= \langle \emptyset, x_2, \emptyset, \bar{x}_4, x_5, \bar{x}_6 \rangle^T, \\ \bar{x}_6 &= \langle \text{МЗ. 4} \rangle x_2 \bar{x}_4.\end{aligned}\quad (9)$$

Далее последовательно получаем:

$$\begin{aligned}\Delta X^{(4)} &= \langle \langle \text{МЗ. 5} \rangle x_5 \bar{x}_6, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset \rangle^T, \\ X^{(4)} &= \langle \bar{x}_1, x_2, \emptyset, \bar{x}_4, x_5, \bar{x}_6 \rangle^T, \\ \bar{x}_1 &= \langle \text{МЗ. 5} \rangle x_5 \bar{x}_6,\end{aligned}\quad (10)$$

$$\begin{aligned}\Delta X^{(5)} &= \langle \emptyset, \emptyset, \langle \text{МЗ. 1} \rangle \bar{x}_1 x_2, \emptyset, \emptyset, \emptyset \rangle^T, \\ X^{(5)} &= \langle \bar{x}_1, x_2, \bar{x}_3, \bar{x}_4, x_5, \bar{x}_6 \rangle^T, \\ \bar{x}_3 &= \langle \text{МЗ. 1} \rangle \bar{x}_1 x_2.\end{aligned}\quad (11)$$

На пятой итерации на позициях с номерами 3 и 6 в векторе $X^{(5)}$ появились выражения, отличные от символа $\emptyset$, так что итерации на этом можно прекращать. План вычислений задается последовательностью формул (8)—(11).

6. Многоуровневая схема планирования вычислений

Итерации по уравнению (1) или по схеме (7) определяют план вычислений в пределах одной ВМ. Необходимость дальнейшей детализации плана вычислений определяется на основании связей МЗ каждой ВМ с другими ВМ или реализациями МЗ, описанных таблицей связей МЗ (см. таблицу).

Алгоритм планирования вычислений в этой ситуации в принципиальном отношении прост. Пусть получен некоторый план вы-

числений в пределах конкретной ВМ (см. разд. 5). Дальнейшая детализация плана связана с последовательным анализом формул, составляющих уже полученный план. В каждую из этих формул входит, и притом только одно, имя МЗ (имя МЗ — это выражение $MZ.i$, где i — номер задачи). Для него по таблице связей МЗ определяется либо имя ВМ, в которой должна детализироваться эта МЗ, либо имя процедуры, являющейся ее реализацией. В последнем случае на место имени МЗ в полученном плане вычислений подставляется имя процедуры, формальными параметрами (входами) которой являются имена соответствующих аргументов МЗ, а выходом — левая часть анализируемой формулы плана вычислений. В первом же случае формулируется новая задача, аналогичная рассмотренной в разд. 5 применительно к той ВМ, которая поставлена в соответствие рассматриваемой МЗ в таблице связей. Такой процесс продолжается до тех пор, пока на место всех имен МЗ в плане вычислений не будут подставлены имена их реализаций.

Поясним суть этой части алгоритма планирования вычислений на примере детализации плана (8)—(11). В нем для соотношений (8)—(10) будут сформулированы соответственно такие новые задачи: 1) дано x_2 , найти x_4 (для ВМ.3); 2) дано x_2, x_4 , найти x_6 (для ВМ.4); 3) дано x_1, x_2 , найти x_3 (для ВМ.3). Что касается формулы (10), то для входящей в нее МЗ.5 имеется реализация (см. таблицу), каковой является процедура с именем f_1 . Решение этих задач выполняется по уже изложенной схеме.

Заключение

Предлагаемый алгоритм планирования вычислений обладает рядом дополнительных особенностей. Во-первых, план вычислений получается в ярусно-параллельной форме, что достаточно удобно в связи с активным развитием ЭВМ с параллельными вычислениями. Во-вторых, если для некоторых вычислений БЗ позволяет получить несколько различных алгоритмов, то все они будут автоматически синтезированы в рамках рассмотренного подхода. Это означает, что с помощью предложенной схемы может решаться проблема алгоритмической избыточности для преодоления трудностей создания устойчивого к сбоям ЭВМ, ошибкам алгоритмиста и программиста программного обеспечения, а также некоторые вопросы верификации алгоритмов и программ. Заметим, что в том примере, который был рассмотрен, на очередной (шестой) итерации был бы получен вектор:

$$\Delta X^{(6)} = \langle \emptyset, \emptyset, \emptyset, \emptyset, \bar{x}_5 = \langle MZ.3 \rangle \bar{x}_3 \bar{x}_4, \emptyset \rangle^T,$$

т. е. было бы получено значение $\bar{x}_5$, которое при некоторых условиях может рассматриваться как контрольное соотношение для проверки всей цепочки вычислений от исходных данных x_2, x_5 до результата x_3 .

Литература

1. Городецкий В. И., Дрозжин В. В., Юсупов Р. М. Многоуровневые атрибутные грамматики для моделирования сложных структурно-динамических систем//Изв. АН СССР. Техн. кибернетика. 1986. № 1. С. 165—168.
2. Кнут Д. Е. Семантика контекстно-свободных языков//Семантика языков программирования. М., 1980, с. 137—161.
3. Маркотти М., Ледгард Х., Бохман Г. Формальные описания языков программирования//Семантика языков программирования. М., 1980, с. 9—136.
4. Пересмотренное сообщение об АЛГОЛе-68//Под ред. А. ван Вейнгардена. М., 1979.
5. Братчиков И. Л. Синтаксис языков программирования. М., 1975.
6. Льюис П., Розенкранц Д., Стирнз Р. Теоретические основы проектирования компиляторов. М., 1979.
7. Хомский Н., Шютценберже М. П. Алгебраическая теория контекстно-свободных языков//Киберн. сб. Нов. сер. 1966. Вып. 3. С. 118—161.
8. Rosenkrantz D. Matrix equations and normal forms of context-free grammars//J. ACM. 1967. Vol. 14. P. 501—507.
9. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. М., 1978.

СТАТИСТИЧЕСКИЙ МЕТОД СИНТЕЗА СМЕШАННОГО АЛГОРИТМА, ОПТИМАЛЬНОГО ПО УСТОЙЧИВОСТИ

1. В настоящее время создано большое количество библиотек и пакетов программ, вследствие чего для решения одной и той же (с точки зрения математической постановки) задачи нередко имеется несколько программных версий, реализующих различные алгоритмы. Выбор одной из них может подчиняться различным требованиям в зависимости от того, какие качества алгоритма наиболее важны для пользователя: устойчивость к погрешностям исходных данных, точность, быстрота исполнения и т. д. При этом для различных исходных данных задачи лучшими по какому-либо из вышеперечисленных критериев могут оказываться различные программы. Поэтому имеет смысл разбить области исходных данных на такие подмножества, принадлежность каждому из которых означала бы предпочтение определенного алгоритма, и, таким образом, на всей области данных действовал бы смешанный (комбинированный) алгоритм. Кроме того, желательно, чтобы структура разбиения (и, следовательно, проверка принадлежности элементам этого разбиения) была достаточно простой. Более подробно и формализованно эти вопросы рассмотрены в работе [1], в которой в качестве критерия предпочтения алгоритма принята точность. В настоящей статье предлагается способ выбора одного из конкурирующих алгоритмов в зависимости от подмножества, куда попадают исходные данные задачи, т. е. способ построения смешанного алгоритма на всей области данных. При этом под стохастической мерой неустойчивости будем понимать, грубо говоря, отношение степени разброса результата работы алгоритма к степени разброса входных данных, ограничиваясь случаями, когда последний мал.

2. Уточним понятие степени неустойчивости.

О п р е д е л е н и е 1. Пусть f — вещественнозначная процедура-функция, действующая в области параметров $G \subset \mathbb{R}^n$, $x = (x_1, \dots, x_n) \in G$, $\xi_1, \dots, \xi_n$ — независимые случайные величины, такие, что $E\xi_i = 0$, $D\xi_i = 1$ ($i = 1, \dots, n$).

Локальной степенью неустойчивости f в точке x назовем:

$$U_f(x) = \lim_{\sigma \rightarrow 0} \frac{\sqrt{Df(x_1 + \sigma \xi_1, \dots, x_n + \sigma \xi_n)}}{\sigma}.$$

З а м е ч а н и е 1. U_f — функция $G \rightarrow \mathbb{R}^+$.

З а м е ч а н и е 2. Случай неодинаковых дисперсий приращений легко может быть сведен к рассмотренному с помощью замены переменных.

О п р е д е л е н и е 2. Пусть $\|\cdot\|$ — некоторая норма в пространстве функций, заданных на G . Глобальной степенью неустойчивости f в области G назовем величину $\|U_f\|$.

П р и м е р ы. В качестве нормы $\|\cdot\|$ можно рассмотреть норму пространства непрерывных функций $C: \|U_f\| = \sup_{x \in G} U_f(x) —$

тогда глобальная неустойчивость в области имеет смысл максимальной локальной неустойчивости, либо норму пространства L_1 :

$\|U_f\| = \int_G U_f(x) dx / \text{mes}(G)$ — и тогда глобальная неустойчивость

имеет смысл усредненной локальной неустойчивости и т. п.

З а м е ч а н и е 3. Понятия степени неустойчивости можно определить не только для процедур-функций, но и для процедур общего вида, которые можно трактовать как отображение некоторой области параметров $G \subset \mathbb{R}^n$ на некоторую область параметров $H \subset \mathbb{R}^m$.

З а м е ч а н и е 4. Более устойчивым (в точке или в области) считается алгоритм, обладающий меньшей (локальной или глобальной) степенью неустойчивости.

3. Л е м м а. Если f дифференцируема в окрестности точки x и для достаточно малых σ случайный вектор $\sigma \xi$ принадлежит этой окрестности, то $U_f(x) = |(\text{grad } f)(x)|$.

Д о к а з а т е л ь с т в о. Пусть $\|\cdot\|_2$ — евклидова норма в $\mathbb{R}^2$. Если f дифференцируема и $\xi = (\xi_1, \dots, \xi_n)$, то, почти наверное, при $\sigma \rightarrow 0$

$$f(x + \sigma \xi) = f(x) + \sigma \sum_{j=1}^n \frac{\partial f}{\partial x_j}(x) \xi_j + \sigma(\sigma^2 \|\xi\|_2^2).$$

Учитывая, что остаточный член — это случайная функция аргумента σ , равномерно интегрируемая по вероятностной мере в окрестности точки $\sigma = 0$, при $\sigma \rightarrow 0$) имеем

$$\mathbb{E} f^2(x + \sigma \xi) = f^2(x) + \sigma^2 |(\text{grad } f)(x)|^2 + \sigma(\sigma^2),$$

$$(\mathbb{E} f(x + \sigma \xi))^2 = f^2(x) + \sigma(\sigma^2),$$

откуда

$$Df(x + \sigma \xi) = \sigma^2 |(\text{grad } f)(x)|^2 + \sigma(\sigma^2).$$

4. **О п р е д е л е н и е 3.** Пусть f_1 и f_2 — алгоритмы, реализующие вычисление функции f в области G , $S \subset G$. Смешанным алгоритмом назовем

$$f_S(x) = \begin{cases} f_1(x), & x \in S, \\ f_2(x), & x \in G \setminus S. \end{cases}$$

Область S назовем областью предпочтения алгоритма f_1 .

В терминах введенных определений задача построения наиболее устойчивого в области G смешанного алгоритма, т. е. алгоритма, имеющего минимальную глобальную степень неустойчивости, переформулируется следующим образом: пусть f_1, f_2 — те же, $\|\cdot\|$ — некоторая норма в пространстве функций $G \rightarrow \mathbb{R}$. Требуется построить область $S \subset G$ такую, чтобы $\|U_{f_S}\|$ была минимальна.

Как говорилось ранее, S должна иметь достаточно простую структуру, чтобы число операций для проверки принадлежности $x \in S$ было ограничено некоторой величиной, не зависящей от x . Эта величина может задаваться пользователем. Строгое определение сложности структуры приводится в работе [1].

5. Ограничимся рассмотрением примера построения области S вида $[a, b] \times [c, d]$. Рассмотрим функцию $f(x_1, x_2): G \rightarrow \mathbb{R}$ и две процедуры-функции f_1 и f_2 , реализующие вычисление f с некоторыми погрешностями, которые в нашем примере моделируются искусственным добавлением к значению функции небольших возмущений. Прямоугольник G разбивается на $N \times N$ одинаковых прямоугольников Π_{ij} вида $[a_i, a_{i+1}] \times [b_j, b_{j+1}]$, где

$$a_j = a + \frac{b-a}{N}(j-1), \quad j = 1, \dots, N,$$

$$b_j = c + \frac{d-c}{N}(j-1), \quad j = 1, \dots, N,$$

Область S строится в виде объединения $NRT \leq N \times N$ прямоугольников Π_{ij} . Тогда проверка $x = (x_1, x_2) \in S$ состоит в проверке некоторого количества неравенств типа: $x_1 \geq a_i, x_1 \leq a_{i+1}, x_2 \geq b_j, x_2 \leq b_{j+1}$. Это количество проверок неравенств во всяком случае $\leq 4NRT$ и может быть уменьшено с учетом того, что некоторые прямоугольники Π_{ij} , входящие в S , могут иметь общие стороны. Как уже отмечалось, число проверок может быть ограничено величиной, заданной пользователем. Пусть эта величина задана и равна K . Приведем общую схему алгоритма поиска области S такой, чтобы $\|U_{f_S}\|$ была минимальна, среди всех областей вида $\cup \Pi_{ij}$, для которых проверка принадлежности $x \in S$ требует не более K проверок неравенств для любого $x \in G$.

Шаг 1. Вычисляются глобальные степени неустойчивости $\|U_{f_1}\|$ и $\|U_{f_2}\|$ в каждом прямоугольнике Π_{ij} ($i, j = 1, \dots, N$); формируются соответствующие массивы $\alpha[i, j] = \|U_{f_1}\|_{\Pi_{ij}}$ и $\beta[i, j] = \|U_{f_2}\|_{\Pi_{ij}}$. Рассматриваются два варианта нормы

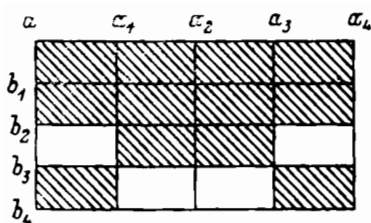


Рис. 1.

$\|\cdot\|$: максимальная в прямоугольнике Π_{ij} и усредненная по прямоугольнику Π_{ij} степени неустойчивости. Нахождение максимума и усреднения производится по случайной выборке $\{x_i\}_{i=1}^{NP}$ из прямоугольника Π_{ij} , состоящей из NP точек. Максимальная степень неустойчивости с учетом леммы вычисляется по формуле:

$$\|U_{f_1, 2}\|_{\Pi_{ij}} = \max_{i=1, \dots, NP} U_{f_1, 2}(x_i) = \max_{i=1, \dots, NP} |(\text{grad } f_{1, 2})(x_i)|,$$

средняя:

$$\|U_{f_1, 2}\|_{\Pi_{ij}} = \sum_{i=1}^{NP} U_{f_1, 2}(x_i) / NP = \sum_{i=1}^{NP} |(\text{grad } f_{1, 2})(x_i)| / NP.$$

Вычисляется также массив:

$$\text{gamma}[i, j] = \alpha[i, j] - \beta[i, j].$$

Очевидно, алгоритм f_1 предпочтителен в тех прямоугольниках Π_{ij} , где $\text{gamma}[i, j] \leq 0$.

Шаг 2. Если разбиение $\{\Pi_{ij}\}_{i, j=1}^N$ области G слишком мелкое и, следовательно, можно ожидать, что число проверок окажется явно большего порядка, чем заданное ограничение K , то производится укрупнение разбиения с шагом step объединением в один прямоугольник $\text{step} \times \text{step}$ соседних Π_{ij} . Для нового разбиения вычисляется аналогичный массиву $\text{gamma}[i, j]$ массив для сравнительной характеристики неустойчивости f_1 и f_2 . Элементы его получаются усреднением $\text{gamma}[i, j]$ по всем Π_{ij} , составляющим прямоугольник нового разбиения. За прямоугольниками нового разбиения и соответствующим массивом можно без ущерба для дальнейших рассуждений сохранить обозначения Π_{ij} и $\text{gamma}[i, j]$ соответственно, где $i, j = 1, \dots, M$; $M = \lfloor N/\text{step} \rfloor$.

Шаг 3. Формируется массив $z[i, j] = \begin{cases} 1, & \text{gamma}[i, j] \leq 0 \\ 0, & \text{gamma}[i, j] > 0 \end{cases}$; $i, j = 1, \dots, M$. Массиву z ставится в соответствие область $S_z = \bigcup_{i, j: z[i, j]=1} \Pi_{ij}$, которая является областью предпочтения f_1 .

Шаг 4. Подсчитывается число проверок неравенств для установления принадлежности области S_z . Используется способ проверки принадлежности по вертикальным или горизонтальным слоям разбиения, предполагающий меньшее число проверок неравенств, чем при проверке принадлежности каждому по отдельности $\Pi_{ij} \subset S_z$. Например, проверка принадлежности $x = (x_1, x_2) \in S_z$, (область S_z изображена на рис. 1 и состоит из 12 прямоугольников Π_{ij}) осуществляется по следующему правилу:

$$\begin{aligned} & (x_2 \in [a, b_2] \text{ and } x_1 \in [a, a_4]), \\ & \text{or } (x_2 \in [b_2, b_3] \text{ and } x_1 \in [a_1, a_3]), \\ & \text{or } (x_2 \in [b_3, b_4] \text{ and } (x_1 \in [a, a_1] \text{ or } x_1 \in [a_3, a_4])). \end{aligned}$$

Проверка принадлежности в данном случае производится по горизонтальным слоям; число проверок неравенств равно 14. Если полученное число не превосходит заданного K , то S_z — искомая область. Вычисляется соответствующая суммарная характеристика неустойчивости смешанного алгоритма:

$$\text{sum}_z = \sum_{i, j=1}^M z[i, j] \times \text{gamma}[i, j] = \sum_{i, j: \Pi_{ij} \subset S_z} \text{gamma}[i, j].$$

Шаг 5. Если число проверок неравенств для S_z более K , то ищется массив y и соответствующая область S_y более простой структуры (число проверок $\leq K$), имеющая в то же время минимальную характеристику $\text{sum}_y = \sum_{i, j: \Pi_{ij} \subset S_y} \text{gamma}[i, j]$. В настоя-

щем примере поиск ведется либо полным перебором всех массивов $y[i, j]$ ($i, j = 1, \dots, M$) со значениями 0 и 1, либо перебором некоторой случайной выборки из числа таких массивов. Для каждого из них вычисляется sum_y и число проверок неравенств для S_y ; из всех S_y , удовлетворяющих ограничению на сложность проверки принадлежности, искомой областью предпочтения алгоритма f_1 является область, имеющая минимальную характеристику sum_y .

6. Численный эксперимент. Рассмотрим функцию $f(x_1, x_2) = x_1^2 + x_2$ в прямоугольнике $G = [-1.0, 1.0] \times (-0.2, 0.8]$. Пусть имеются два алгоритма f_1 и f_2 приближенного вычисления f соответственно с ошибками δ_1 и δ_2 , и поведение ошибок может быть описано выражениями:

$$\delta_1(x_1, x_2) = 0.01 \sin(4x_1) + 0.001 \cos(8x_2),$$

$$\delta_2(x_1, x_2) = 0.001 \cos(8x_1) + 0.01 \sin(2x_2).$$

Область G разбивается на 16 одинаковых прямоугольников, в каждом из которых вычисляется усредненная глобальная степень неустойчивости для f_1 и f_2 . Вычисляются также средние глобальные степени неустойчивости f_1 и f_2 во всей области G (они обозначены U_1 и U_2). Для f_1 (а также для f_2) формируется массив z , определяющий область S_1 предпочтения f_1 (или S_2 для f_2) и соответствующий смешанный алгоритм. Для проверки принадлежности S_1 и S_2 требуется проверить соответственно 12 и 8 неравенств. Проверку принадлежности в обоих случаях экономнее осуществлять по горизонтальным слоям. Вычисляется средняя глобальная степень неустойчивости смешанного алгоритма U_{mix} .

Если требуется, чтобы принадлежность S_1 и S_2 определялась с помощью меньшего числа проверок неравенств, то строятся упрощенные области (они соответствуют массиву y), для которых требуется проверить 4 неравенства. Для смешанного алгоритма, соответствующего упрощенным областям, также вычисляется средняя глобальная степень неустойчивости. Результаты работы программы показаны на рис. 2, где контуром обведены области

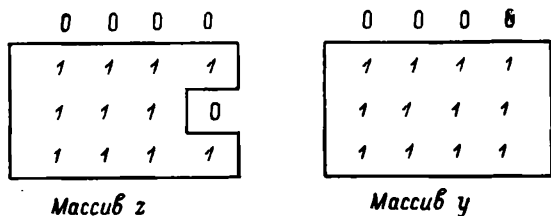


Рис. 2.

предпочтения первого алгоритма. В частности, глобальные (средние) степени неустойчивости первого и второго алгоритмов соответственно равны 1.483490 и 1.491946. При ограничении на число проверяемых неравенств, равном 12, неустойчивость смешанного алгоритма равна 1.477987, а при ограничении, равном 4, она составляет 1.478347.

Литература

1. *Ляшенко Н. Н., Евневич Е. Л.* Статистические задачи выбора и синтеза оптимальных алгоритмов // Зап. науч. семин. ЛОМИ. 1988. Т. 166. С. 72—90.

ИСПОЛЬЗОВАНИЕ И АВТОМАТИЧЕСКИЙ СИНТЕЗ ДИФФЕРЕНЦИАЛЬНЫХ КОРРЕКТОРОВ

Данная работа посвящена рассмотрению системных и содержательных аспектов автоматизации выбора и построения оптимальных процедур обработки данных (например, сигналов). Предлагается использовать представление преобразований в виде композиции стандартного преобразования и корректора, адаптируемого к частному классу задач. Применение и синтез корректоров иллюстрируются на примере задачи мультипликативной фильтрации.

В работе используются следующие обозначения: $\mathbb{R}$ — множество действительных чисел, sq — оператор возведения в квадрат, $\mathcal{S}$ — тождественное отображение на обусловленном множестве функций, $\odot$ — поэлементное умножение значений, $e(t) = t$ ($t \in \mathbb{R}$), $*$ — знак свертки последовательностей.

1. Введение

При проектировании компьютерных систем обработки данных часто возникает необходимость снабдить пользователя средствами оптимизации используемых им преобразований. Так, решая задачу фильтрации сигналов на фоне помех, приходится выбирать оптимальные или близкие к ним фильтры с помощью некоторых исходных (априорных или статистических) данных о шумах; занимаясь селекцией определенных деталей изображения, строят оптимальные (допустимые) селекторы и т. п. При этом за достижение оптимальности приходится платить значительным увеличением библиотеки процедур обработки и сложностью реализации самих средств оптимального выбора процедур.

Вообще говоря, среди стратегий поведения разработчиков существуют две крайние тенденции: первая состоит в стремлении к универсальности охвата средств обработки в ущерб разнообразию решаемых задач (например, только фильтрация, но зато всевозможными способами), вторая — в выборе канонических реализаций методов решения при большом разнообразии решаемых

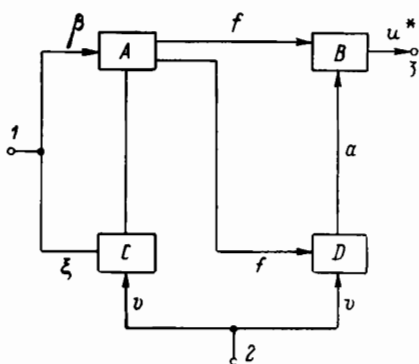


Рис. 1.

Суть подхода состоит в следующем. Пусть для определенности решается задача фильтрации сигнала U , искаженного помехой ξ с законом взаимодействия $\oplus$ (распространенные случаи: $U + \xi$, $U\xi$, $U(1 + \xi)$). Предположим, что в нашем распоряжении имеются некоторые предварительные статистические сведения о характере шума или же возможность в течение некоторого времени наблюдать чистый шум. Тогда предлагаемый способ обработки может быть изображен схемой (рис. 1), которая предусматривает два этапа работы.

На первом этапе наблюдаемый чистый шум поступает на вход 1, а на вход 2 подается эталонный искусственный сигнал v . Блок C осуществляет их взаимодействие по закону $\oplus$, а блок A осуществляет основное преобразование (например, фильтрацию) по некоторому заранее выбранному алгоритму. Этот алгоритм ориентирован на довольно широкий класс помех и в данном конкретном случае может быть далек от оптимального, поэтому он нуждается в коррекции. Результат фильтрации f поступает на вход блока D , на другой вход того же блока подается эталонный сигнал. Блок D приближенным образом строит оператор, переводящий f в v . Оператор может выбираться из конечно-параметрического семейства, тогда построение оператора сводится к вычислению вектора коэффициентов a . На этом первый этап заканчивается. Будем считать, что произведена настройка корректора (исправляющего отображения). Заметим, что вместо чистого шума на первом этапе на вход 1 можно подавать искусственный сигнал, сгенерированный в соответствии с заданными сведениями о распределениях.

На втором этапе происходит собственно фильтрация. На вход 1 подается зашумленный сигнал β . Он фильтруется блоком A , а результат фильтрации f подается на вход корректора B . Блок D передает в B вектор коэффициентов a (или текст процедуры при непараметрическом задании оператора). Корректор применяет исправляющий оператор к сигналу f и выдает в качестве оконча-

ных задач. Можно стремиться сразу к обоим целям, увеличивая громоздкость создаваемой системы, но, приняв ограничения на ее сложность, мы вынуждены идти на определенный компромисс между двумя крайностями.

В данной работе описывается подход к построению систем обработки, который позволяет добиться значительной гибкости с точки зрения оптимизации не в ущерб компактности системы и широте круга преобразований.

тельного результата сигнал U^* , принимаемый нами за статистическую оценку истинного сигнала U (выход $\mathcal{Z}$).

Тот же подход может применяться для решения других задач, например классификации, косвенных измерений, прогнозирования и т. д. Пользуясь подходящей системой коррекции, можно значительно уменьшить круг основных преобразований без существенного проигрыша в качестве обработки. Основные проблемы, разумеется, состоят в выборе корректирующих операторов и построении алгоритмов настройки. Здесь возникает задача идентификации операторов, рассматривавшаяся с различных точек зрения исследователями, работавшими в области автоматического выбора моделей (см., например, [1]).

2. Формальный аспект

Довольно широкий класс корректирующих операторов может быть описан следующим образом. Пусть H — нормированное функциональное пространство, M_j — операторы из H в H ($j = 1, \dots, n$). Набор операторов M_j будем называть порождающим набором, а в качестве семейства корректоров сначала рассмотрим класс:

$$Q = \left\{ \sum_{j=0}^{n-1} a_j M_j \mid a_j \in \mathbb{R} \right\}. \quad (1)$$

Если $L \in Q$ и $v = Lf$, то

$$v = \sum_{j=0}^{n-1} a_j M_j f = \sum_{j=0}^{n-1} a_j f_j, \quad \text{где } f_j = M_j f. \quad (2)$$

Таким образом, отыскание корректора состоит в линейном разложении эталона U_0 по системе $\{f_j\}$. Если, например, $M_j = \frac{d^j}{dt^j}$, то корректирующее преобразование имеет вид:

$$U_0 = a_0 f + a_1 \frac{d}{dt} f + \dots + a_{n-1} \frac{d^{n-1}}{dt^{n-1}} f,$$

т. е. является дифференциальным оператором с постоянными коэффициентами. Если $n = 3$, $M_0 = \mathcal{E}$, $M_1 = \text{sqr}$, $M_2 = \frac{d}{dt}$, то

$$v = a_0 f + a_1 f^2 + a_2 \frac{d}{dt} f$$

и корректор представляет собой нелинейный дифференциальный оператор. Полагая $n = 4$, $M_0 = \mathcal{E} \odot \frac{d}{dt}$, $M_1 = \frac{d}{dt} \odot e$, $M_2 = \frac{d}{dt}$, $M_3 = \frac{d^2}{dt^2}$, получаем:

$$v = a_0 f f' + (a_1 t + a_2) f' + a_3 f'' \text{ и т. п.}$$

Заметим, что сама коррекция в описанном случае проводится довольно быстро, в то время как настройка оказывается более

емкой по времени и не может быть (хотя бы частично) проделана заранее, поскольку нуждается в знании f .

Метод, основанный на использовании класса (1), назовем прямой коррекцией. Наряду с этим рассмотрим обратную коррекцию, основанную на разложении:

$$f = \sum_{j=1}^n b_j v_j, \quad v_j = M_j v_0 \quad (3)$$

и решении уравнения (3) относительно неизвестной функции v . Очевидно, такой подход приводит к увеличению сложности коррекции и в то же время к упрощению (ускорению) настройки, так как система v_j известна заранее и все предварительные вычисления, зависящие только от нее (например, обращение матрицы метода наименьших квадратов и т. п.), могут также быть проделаны предварительно.

Сделанные нами замечания определяют области предпочтения двух подходов. Удачной была бы такая ситуация, в которой из разложения (3) простым способом можно получить разложение (2), тогда появилась бы возможность соединить достоинства обоих подходов. Интересно, что в ряде случаев такая возможность имеется.

Рассмотрим несколько утверждений о связи прямого и обратного способов коррекции.

Т е о р е м а 1. Если M_j — линейные операторы, то необходимым условием совместного существования представлений (2) и (3) является условие: v — неподвижная точка оператора

$$\sum_{j,k=0}^{n-1} c_{j,k} M_j M_k,$$

где $c_{j,k} \in \mathbb{R}$.

Д о к а з а т е л ь с т в о. Если $f = \sum_j b_j M_j v$ и $v = \sum_k a_k M_k f$, то в силу линейности M_j

$$v = \sum_k a_k M_k \left(\sum_j b_j M_j U_0 \right) = \left(\sum_{k,j} b_j a_k M_j M_k \right) v.$$

Теперь достаточно положить $c_{j,k} = b_j a_k$. $\square$

Т е о р е м а 2. Если S — линейный оператор и $M_j = S^j$, то необходимым условием совместного существования представлений (2) и (3) является условие: v — неподвижная точка оператора $\sum_{r=0}^{2n-2} p_r S^r$.

Если это условие выполняется, то достаточным условием восстановления a по b является разрешимость линейной системы $a * b = p$ относительно a_j .

Д о к а з а т е л ь с т в о. Утверждение очевидным образом вытекает из теоремы 1. $\square$

З а м е ч а н и е 2.1. Из теоремы 2 вытекает простой алгоритм проверки «обратимости». Если v принадлежит классу решений уравнений

$$\left(\sum_{r=0}^{2n-2} p_r S^r - \mathcal{E} \right) v = 0$$

и нам известны коэффициенты b_k в разложении (3), то первый шаг состоит в вычислении величин $a_0, \dots, a_{n-1}$ по правилам:

$$a_0 = 1/b_0, \quad a_{m+1} = \frac{1}{b_0} \left(p_{m+1} - \sum_{j=0}^m a_j b_{m+1-j} \right).$$

Второй шаг заключается в подстановке полученных значений в $n-2$ соотношения:

$$\sum_{j=s}^{n-1} a_j b_{n+s-1-j} = p_{n+s-1} \quad (s = 1, \dots, n-2). \quad (4)$$

Если (4) выполняются, то a являются искомыми решениями.

П р и м е р 1. Пусть $S = \frac{d}{dt}$, тогда представление (3) при $n = 2$ имеет вид: $f = b_0 v + b_1 v'$, а представление (2): $v = a_0 f + a_1 f'$. Из обратимости вытекает, что эталон v является решением некоторого однородного дифференциального уравнения второго порядка с постоянными коэффициентами. Пусть $(p_0^{-1})v + p_1 v' + p_2 v'' = 0$, тогда достаточным условием обратимости будет соотношение:

$$\frac{p_1 b_1}{b_0} - \frac{p_0 b_1^2}{b_0^2} = p_2$$

(см. замечание 1). $\square$

3. Эксперименты по мультипликативной фильтрации

На основе изложенного выше подхода авторы проводили эксперименты по коррекции мультипликативных фильтров. Цель экспериментов состояла в сравнении различных корректоров фильтров. Исходный «идеальный» сигнал представлял собой лоренцеву кривую:

$$S(t) = (R^2 + v^2 t^2)^{-\frac{1}{2}}, \quad R = 25 \text{ (м)}, \quad v = 13 \text{ (м/с)}, \quad t \in [0, 80] \text{ (с)}.$$

Использовался гауссовский некоррелированный шум, мультипликативно взаимодействовавший с «идеальным» сигналом, имевшим стандартное отклонение 0.2. Зашумленный сигнал подвергался предварительному пятикратному сглаживанию среднеквадратическим фильтром с прямоугольным окном, равным 5. Результатом являлся сглаженный сигнал F .

Рассматривались два вида корректировки фильтров: прямое восстановление (разложение «идеального» сигнала по определенному базису) и обратное восстановление. Для решения поставлен-

Результаты экспериментов корректировки фильтров

Способ корректировки	Среднеквадратическая ошибка
Прямое восстановление	
Линейное разложение:	
1-го порядка $S = a_1F + a_2F'$	0.0422
2-го порядка $S = a_1F + a_2F' + a_3F''$	0.0422
Нелинейное $S = a_1F + a_2F'^2 + a_3F'$	0.0300
Обратное восстановление	
Рекуррентный метод 1-го порядка $F = a_1S + a_2S'$	0.0433
Итерационный метод:	
1-го порядка $F = a_1S + a_2S'$ 2 итерации	0.0431
2-го порядка $F = a_1S + a_2S' + a_3S''$ 2 итерации	0.0282

ной задачи использовались следующие методы: вычисление производной от дискретной функции с помощью приближенной формулы для пяти узлов; обращение матрицы; квадратическое разложение по заданному базису; решение дифференциальных уравнений методом Эйлера (рекуррентным) и итерационным.

Результаты проведенных экспериментов сведены в табл. 1. В качестве критерия оценки рассматриваемых корректоров выбрана среднеквадратическая ошибка восстановления. Для каждого способа восстановления приведен исходный «идеальный» сигнал I и восстановленный после предварительной фильтрации 2 (рис. 2—5, $I_{\text{сиг}}$ — интенсивность сигнала).

Сравнительный анализ на основании приведенных ошибок восстановления позволяет предпочесть итерационный метод при обратном восстановлении сигнала, когда предварительно сглаженный сигнал раскладывается по базису, включающему вторую производную «идеального» сигнала (ошибка восстановления равна 0.0282). Графический материал, дающий возможность оценить качественную похожесть восстановленного и идеального сигнала, ранжирует опробованные методы так же, как и величина ошибки восстановления.

Коротко о структуре программного обеспечения, поддерживавшего проведение описанных экспериментов. Основная программа содержит альтернативный вызов модулей (подпрограмм), соответствующих выбранному способу корректировки:

sch1 — последовательность вызовов процедур для рекуррентного способа восстановления;

sch2 — обеспечение итерационного метода решения задачи;

sch3 — решение задачи прямого восстановления сигнала.

Среди наиболее важных используемых процедур отметим следующие:

sumbsig — генерация исходного идеального сигнала;

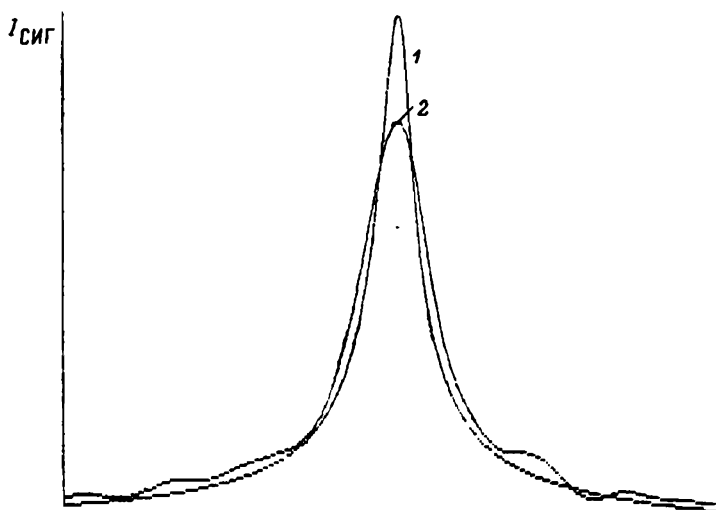


Рис. 2.

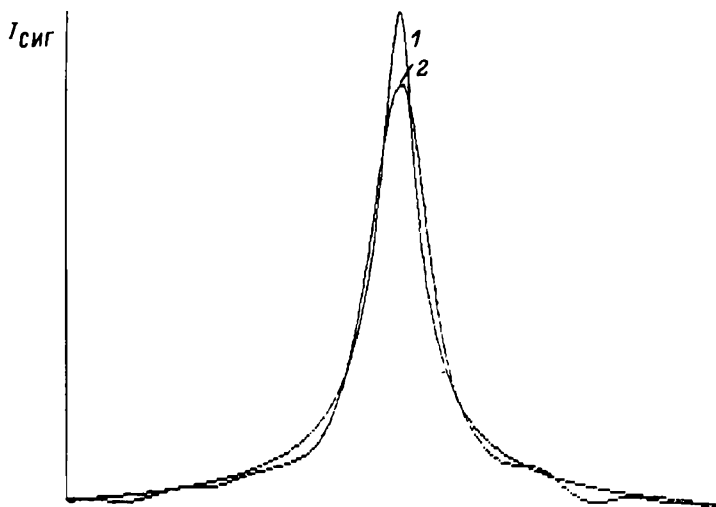


Рис. 3.

noisegen — генерация шума заданного вида и указанных параметров;

sigoper — вычисление зашумленного сигнала по заданному типу взаимодействия между идеальным сигналом и шумом;

filtr — обеспечение многократной среднеквадратической фильтрации (предварительной) зашумленного сигнала;

basform — формирование базиса разложения (является вспомогательной для процедуры вычисления коэффициентов разложения);

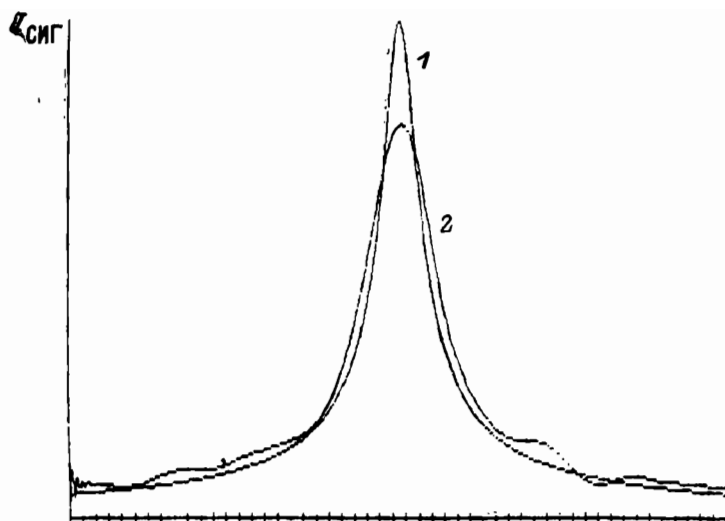


Рис. 4.

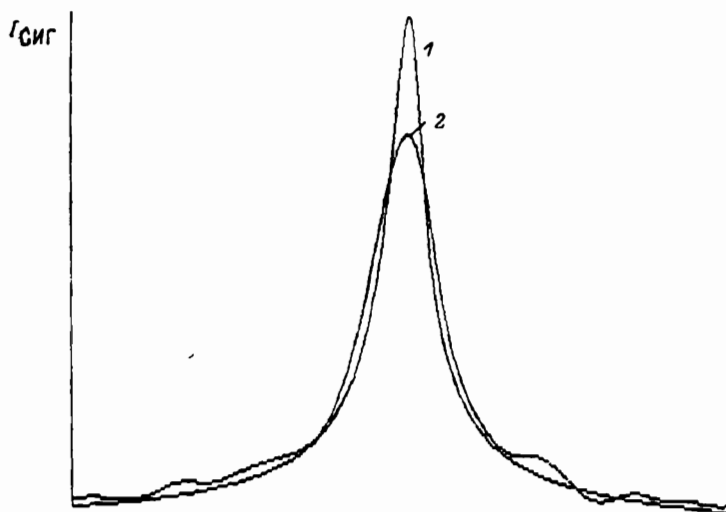


Рис. 5.

inver2 — обращение матрицы (используется процедурой surfit);

surfit — среднеквадратическое разложение по базису;

resrec — обратное восстановление рекуррентным методом;

iterrec — обратное восстановление итерационным методом;

rightrec — прямое восстановление.

Программа и подпрограммы реализованы на языке Pascal в системе TURBO—Pascal на персональном компьютере. Общий

Т а б л и ц а 2

Время работы программ

Название процедуры	Число базисных функций	Время работы, с
sumbsig		4.2
filtr		1.5
basform		0.6
surfit	2	7.0
surfit	3	13.0
recrec	2	4.2
iterrec	2	20.0
iterrec	3	30.0
rightrec	2	1.4
rightrec	3	1.8

объем исходного текста составлял 46 192 байта. Код занимал 17 728 байтов, данные — 35 936 байтов (программа рассчитана на работу с сигналами, имеющими до 256 точек отсчета; число базисных функций не должно превышать 4). В табл. 2 приводится время работы некоторых процедур.

Литература

1. Химмельблау Д. Исследование процессов статистическими методами. М., 1973.

ПРЕДСТАВЛЕНИЕ ЗНАНИЙ ОБ ИЗМЕРЯЕМЫХ ВЕЛИЧИНАХ: ТЕОРЕТИКО-ГРУППОВОЙ ПОДХОД

1. Общая постановка задачи

Одним из основных источников информации о мире является процесс измерения различных величин. Поэтому существенным элементом общей постановки задачи представления знаний является задача представления знаний об измеряемых величинах. Эти знания можно разделить на формализованные, т. е. собственно результаты измерений и информацию, полученную при обработке результатов измерений, и неформализованные — знания, выражающие опыт и интуицию специалистов. Как представлять эти знания? Применительно к формализованным знаниям, казалось бы, особой проблемы нет: достаточно хранить все результаты измерений с подробным описанием соответствующей измерительной процедуры. Но для многих экспериментальных установок (радиотелескопов, ускорителей и т. д.) поток измерительной информации настолько велик (мегабиты и даже гигабиты в секунду), что даже хранить все результаты измерений не представляется возможным, не говоря уже о том, чтобы их использовать. Возникает задача «сжатия», компактификации измерительной информации. Возможны различные виды сжатия: например, вместо массива данных хранить те или иные статистические характеристики этого массива (или, если имеется априорная модель исследуемого объекта с неопределенными параметрами, параметры модели, определенные по результатам измерений). Какую форму компактификации (представления знаний) выбрать? Аналогичный вопрос возникает и при представлении неформализованных знаний: как их лучше представлять, т. е. какую форму представления знаний выбрать, чтобы облегчить их хранение и последующее использование?

Если измерительная система ориентирована на решение конкретной прикладной задачи (например, составляет часть АСУ технологическим процессом), то при выборе формы представления знаний естественно исходить из критерия эффективности решения этой прикладной задачи. Но в большинстве случаев круг задач,

в которых в принципе могут быть использованы полученные знания, заранее неизвестен, поэтому неясен и критерий оптимальности, в соответствии с которым можно было бы выбрать оптимальное представление знаний. Таким образом, задача выбора наилучшего представления знаний относится к классу задач оптимизации в условиях неопределенных критериев оптимальности. В статье описан подход к решению этого класса задач, основанный на использовании симметрий задачи (анонсированный в [1, 2]).

2. Основные идеи теоретико-группового подхода

Рассмотрим простейшую ситуацию, при которой возникает необходимость в сжатии измерительной информации. Например, имеются данные $x_1, \dots, x_n$ многократного измерения одной и той же величины x . В результате сжатия необходимо n оценок истинного значения этой величины заменить одной оценкой. В случае, если известен закон распределения погрешности $x_i - x$, то в качестве такой оценки необходимо использовать наиболее вероятное значение x , т. е. в статистических терминах значение, полученное с помощью метода максимального правдоподобия:

$$\prod_{i=1}^n f(x_i - x) \rightarrow \max_x,$$

где f — плотность распределения погрешности. Заметим, что в реальных вычислениях используют равносильную формулу:

$$\Sigma \psi(x_i - x) \rightarrow \min, \quad (1)$$

где $\psi = -\ln f$, а решение этой минимизационной задачи обычно осуществляется за счет решения уравнения, которое получается при приравнивании производной нулю:

$$\Sigma \psi'(x_i - x) = 0 \quad (2)$$

(штрих означает производную). В частности, в случае нормального закона $\psi(x) = x^2$, и решение уравнения (2) — среднее арифметическое $x = 1/n \Sigma x_i$.

Однако в реальных измерительных ситуациях точный вид закона распределения погрешности неизвестен. Такие ситуации называются робастными, а методы вычисления оценки x по значениям $\{x_i\}$ — робастными методами. Опыт применения различных робастных методов показывает, что наиболее эффективными являются так называемые M -методы, которые состоят в использовании выражения (1) с некоторой заранее заданной четной функцией ψ . Какую ψ выбирать?

Традиционная постановка оптимизационных задач состоит в том, чтобы выбрать функционал J и искать ψ , для которого $J(\psi) \rightarrow \min$. Но выбор J в данном случае достаточно произволен, а если для другого функционала $\tilde{J}$ будет оптимальной другая функция $\tilde{\psi}$, то какую использовать: ψ или $\tilde{\psi}$? Чтобы показать, как можно использовать принципы симметрии для выбора ψ , сформулируем задачу выбора ψ в математических терминах.

О п р е д е л е н и е 1. Пусть ψ — произвольная четная непрерывная функция, монотонно не убывающая при $x > 0$, непрерывно дифференцируемая при $x \neq 0$ и отличная от константы. М-методом, соответствующим ψ , назовем отображение (вообще говоря, многозначное), которое набору $x_1, \dots, x_n$ сопоставляет множество всех решений уравнения $\sum \psi'(x_i - x) = 0$.

З а м е ч а н и е 1. Ограничение гладкими функциями ψ связано с тем, что обычно в качестве ψ берут $-\ln f$ для стандартных плотностей вероятности, которые описываются функциями, гладкими при $x \neq 0$. В принципе можно было бы рассмотреть и более общий случай непрерывных ψ , определяя М-метод как отображение $x_1, \dots, x_n \rightarrow \arg \min_x \sum \psi(x_i - x)$. Но так как цель настоящей статьи — продемонстрировать новый подход, то ограничимся изложением наиболее простой ситуации (гладкой ψ), в которой рассуждения, связанные с использованием этого подхода, достаточно просты и наглядны.

З а м е ч а н и е 2. Возможность многозначности отображения вполне реальна: например, для $\psi(x) = |x|$ и $x_1 < x_2 < x_3 < x_4$ множество решений — весь интервал $[x_2, x_3]$.

З а м е ч а н и е 3. Предположения о монотонности функции ψ и о том, что $\psi \neq \text{const}$, соответствуют (если вспомнить, что $\psi = -\ln f$) вполне естественному допущению, что большая погрешность имеет меньшую вероятность.

Напомним, что отношением (частичного) предпорядка называется произвольное транзитивное отношение. Отношение предпорядка обозначается обычно через $\leq$ или $\preceq$. При этом отношение « $a \preceq b$ и $b \preceq a$ » обозначается обычно через $a \sim b$, отношение « $a \preceq b$ и не $a \sim b$ » — через $a < b$.

О п р е д е л е н и е 2. Пусть A — произвольное множество. Критерием оптимальности на множестве A назовем отношение частичного предпорядка $\preceq$ на A . Будем считать, что a лучше b (в смысле данного критерия), если $a \succ b$, и что a равноценно b , если $a \sim b$. Элемент $a \in A$ назовем оптимальным (в смысле критерия $\preceq$), если $a \succeq b$ для всех $b \in A$.

З а м е ч а н и е 4. Ограничимся в дальнейшем М-методами, удовлетворяющими некоторым естественным условиям. Для их формулировки необходимы некоторые вспомогательные обозначения.

О б о з н а ч е н и е. Пусть a — М-метод, соответствующий функции ψ . Тогда М-метод, соответствующий функции $\tilde{\psi}$, где $\tilde{\psi}(x) = \psi(\lambda x)$, будем обозначать через $\lambda(a)$.

О п р е д е л е н и е 3. Критерий оптимальности на множестве всех М-методов назовем корректным, если выполнены следующие условия: а) если $a \preceq b$, $\lambda > 0$, то $\lambda(a) \preceq \lambda(b)$; б) критерий выделяет единственный оптимальный метод.

К о м м е н т а р и й. Условие а) означает, что результат сравнения двух методов не меняется при замене единиц, в которых выражаются измеренные значения x_i ; условие б) означает, что

критерий достаточно сильный: если бы критерий не позволял выделить единственный оптимальный М-метод, то среди семейства методов, равноценных с точки зрения выбранного критерия, можно было бы провести дальнейший отбор по какому-то другому показателю; если такой комбинированный критерий не удовлетворяет условию б), то можно провести дальнейший отбор, и т. д.

Эти два условия естественны, но на первый взгляд кажутся очень слабыми. В самом деле, существует огромное число различных критериев оптимальности, удовлетворяющих условиям а), б). Однако что касается выбора оптимального метода, то здесь произвол гораздо меньше. Точнее, имеет место следующая теорема.

Т е о р е м а 1. Для любого корректного критерия оптимальности найдется вещественное число p такое, что оптимальный М-метод соответствует функции $\psi(x) = |x|^p$.

З а м е ч а н и е 5. Численные эксперименты с различными критериями оптимальности, проведенные в 70-е годы и в начале 80-х годов [3—5], привели к аналогичному выводу об оптимальности оценки с $\psi(x) = |x|^p$ (ее называют еще p -оценкой).

Итак, одного только требования инвариантности относительно некоторой группы симметрии (в рассматриваемом случае группы масштабных преобразований) достаточно для того, чтобы произвол в выборе ψ сузить до возможности выбора произвольного значения одного параметра p . Тем самым проиллюстрирована эффективность теоретико-группового подхода.

3. Общая формулировка теоретико-группового подхода

Пусть задано множество A , элементы которого в дальнейшем будем называть методами представления знаний, и на A задана группа преобразований G .

О п р е д е л е н и е 4. Критерий оптимальности на множестве A назовем корректным, если выполнены следующие условия: а) если $a \lesssim b$ и $g \in G$, то $ga \lesssim gb$; б) критерий выделяет единственный оптимальный метод.

О п р е д е л е н и е 5. Метод представления знаний a назовем G -инвариантным, если $ga = a$ при всех $g \in G$.

О с н о в н а я л е м м а. Для любого корректного критерия оптимальности оптимальный метод G -инвариантен.

В силу этой леммы для нахождения оптимального метода представления знаний достаточно описать все инвариантные методы.

4. Применение теоретико-группового подхода к формализованным знаниям

1. В разд. 2 приведен пример применения рассматриваемого подхода к простейшему случаю, когда точное знание состоит в точном знании одного вещественного параметра исследуемого объекта.

2. Естественным обобщением этой ситуации является случай, когда для описания объекта достаточно знать конечное число измеряемых параметров, т. е. когда имеется конечное число измерительных процедур, результаты которых позволяют однозначно описать объект. На этот случай легко обобщается описанный в разд. 2 l^p -метод компактификации измерительной информации, носящий название робастной регрессии [3, 6].

3. Принципиально более сложная ситуация возникает в том случае, когда конечного числа измерений недостаточно, т. е. когда имеются измерительные процедуры, для описания которых в свою очередь необходимо задать значения одного или нескольких параметров; при этом результаты измерений, соответствующие различным значениям параметров, вообще говоря, независимы. В этом случае для задания объекта необходимо задать функции, описывающие зависимость измеряемой величины от этих параметров (например, яркости от координат при описании астрономических источников, сигнала от времени при описании динамических систем и т. д.).

Рассмотрим для примера простейший случай функции одной переменной. Эту функцию необходимо восстановить по результатам измерений. Поскольку их количество конечно, речь идет о приближенном описании. Обычно выбирают некоторое семейство базисных функций $f(c, x)$, $\dim c = m$ и ищут искомую функцию $f(x)$ в виде $f(x) = \sum a_i f(c^{(i)}, x)$. Какое семейство базисных функций выбирать? Для простоты анализа рассмотрим случай однозначных комплексно-аналитических функций.

О п р е д е л е н и е 6. Пусть $f, g: C^m \otimes C \rightarrow C$ — однозначные аналитические функции. Будем считать, что они эквивалентны (или порождают одно семейство), если $g(c, x) = \lambda(c) f(c'(c), x)$, где λ и c' — аналитические функции, $\lambda \neq 0$ и отображение $c'(c)$ взаимно однозначно; m -мерным семейством назовем класс эквивалентности по этому отношению.

П р и м е ч а н и е. Эквивалентные $f(c, x)$ и $g(c, x)$ порождают одно и то же множество линейных комбинаций.

Пусть $G = \{x \rightarrow ax + b\}$.

З а м е ч а н и е 6. $x \rightarrow ax$ соответствует изменению единицы измерения, $x \rightarrow x + b$ — изменению начала отсчета.

Т е о р е м а 2 [1, 2]. При $m = 0$ не существует корректных критериев оптимальности на множестве всех семейств. При $m = 1$ для любого корректного критерия оптимальности всякая комбинация функций оптимального семейства является либо многочленом, либо дробно-рациональной функцией, либо суммой экспонент, либо тригонометрическим полиномом, либо произведением экспоненты на синусоиду, либо линейной комбинацией этих функций.

Д о к а з а т е л ь с т в о основано на использовании основной леммы.

Тем самым получено обоснование обычно используемых аппроксимирующих семейств.

4. Можно рассмотреть еще более сложный случай, когда для описания измерительной процедуры необходимо задать произвольную функцию. Например, если объект исследования — физическое поле, то для экспериментального исследования уравнения эволюции необходимо произвольным образом задать начальное поле $f(x)$. В этом случае теоретико-групповой подход также позволяет обосновать обычно используемые модели, в частности все основные фундаментальные физические уравнения [7].

5. Теоретико-групповой подход позволяет описать не только оптимальный способ задания самих оценок, но и оптимальный способ описания области неопределенности: наилучшим описанием этой области является описание в виде эллипсоида [1, 2, 8].

5. Применения теоретико-группового подхода к неформализованным знаниям

Утверждения, составляющие неформализованные знания, характеризуются тем, что у эксперта нет абсолютной уверенности ни в их истинности, ни тем более в их ложности. Поскольку наиболее распространенная форма представления информации в ЭВМ — вещественные числа, то степень уверенности обычно представляется числом от 0 до 1. При этом необходимо решить следующие вопросы: как лучше всего сопоставлять степень уверенности нечеткому утверждению и как по степеням уверенности отдельных утверждений рассчитать степени уверенности в их логической комбинации? В силу основной леммы поиск оптимального метода представления знаний сводится к поиску метода, инвариантного относительно некоторой группы симметрии G . В данном случае (в отличие от разд. 2 и 4) нет естественной группы симметрии. Оказывается, однако, что достаточно предположить [9] существование группы симметрии, при которой все степени уверенности, промежуточные между 0 и 1, равносильны, как уже обнаруживается возможность ограничения класса функций преобразования степеней уверенности конечно-параметрическим семейством таких функций. Аналогично использование групп симметрии позволяет найти оптимальное представление для таких наиболее распространенных экспертных утверждений об измеряемых величинах, как « x примерно равна a с точностью порядка σ » [10].

6. Доказательства

Доказательство теоремы 1.

Определение 7. М-метод a назовем масштабно-инвариантным, если $\lambda(a) = a$ для всех $\lambda > 0$.

Лемма 1. Для любого корректного критерия оптимальности оптимальный М-метод масштабно-инвариантен.

Это частный случай основной леммы, доказываемой ниже.

Л е м м а 2. М-методы, соответствующие функциям $\psi(x)$ и $\bar{\psi}(x)$, совпадают в том и только в том случае, когда $\psi(x) = b\bar{\psi}(x) + c$ для некоторых вещественных чисел b и c , $b \neq 0$.

Д о к а з а т е л ь с т в о. Нетрудно доказать, что если $\bar{\psi} = b\psi + c$, то соответствующие М-методы совпадают. Пусть теперь М-методы совпадают. Докажем сначала, что если отношение $\psi'(x)/\psi'(y)$ — рациональное число, т. е. $\psi'(x)/\psi'(y) = p/q$, где p, q — целые, $p \geq 0, q > 0$, то $\bar{\psi}'(x)/\bar{\psi}'(y) = \psi'(x)/\psi'(y)$. В самом деле, так как $\psi'(x)/\psi'(y) = p/q$, то $q\psi'(x) - p\psi'(y) = 0$. Значит, для $x_1 = \dots = x_q = 0, x_{q+1} = \dots = x_{q+p} = x + y$ будет $\sum \psi'(x_i - x) = 0$. Так как М-методы, соответствующие ψ и $\bar{\psi}$, совпадают, то и $\sum \bar{\psi}'(x_i - x) = 0$, т. е. $q\bar{\psi}'(x) - p\bar{\psi}'(y) = 0$, откуда $\bar{\psi}'(x)/\bar{\psi}'(y) = p/q$.

Разберем теперь два случая:

- 1) $\psi(x) = k(x) + C$,
- 2) $\psi(x) \neq k(x) + C$.

В первом случае $\psi'(x)/\psi'(y) = 1$ при всех $x, y > 0$, поэтому $\bar{\psi}'(x)/\bar{\psi}'(y) = 1$, т. е. $\bar{\psi}'(x) = \text{const}$, откуда $\bar{\psi}(x) = \bar{k}(x) + \bar{C}$ для некоторых $\bar{k}$ и $\bar{C}$, и для этого случая лемма доказана.

Во втором случае $\psi'(x) \neq \text{const}$. Следовательно, есть значения, при которых $\psi'(x) \neq 0$ (иначе было бы $\psi'(x) \equiv 0$). Возьмем произвольную точку x с $\psi'(x) \neq 0$. Одно из двух: либо в некоторой окрестности этой точки $\psi'(x) \equiv \text{const}$, либо в сколь угодно малой окрестности этой точки x существуют точки $\bar{x}$ с $\psi'(\bar{x}) \neq \psi'(x)$. В первом случае, поскольку $\psi'(x) \neq \text{const}$, можно взять одну из границ интервала, на котором $\psi'(\bar{x}) = \psi'(x)$, и она также будет обладать нужным свойством. Итак, в обоих случаях найдется точка y , в которой $\psi'(y) \neq 0$, и в сколь угодно малой окрестности ее есть точки $\bar{y}$ с $\psi'(\bar{y}) \neq \psi'(y)$.

Покажем, что для всех x будет $\psi'(x)/\psi'(y) = \bar{\psi}'(x)/\bar{\psi}'(y)$. Если это можно доказать, то тогда $\bar{\psi}'(x) = \text{const } \psi'(x)$ и, значит, $\bar{\psi}(x) = \text{const } \psi(x) + \text{const}_1$, т. е. лемма будет доказана.

В самом деле, пусть x — произвольная точка. В случае, если отношение $\psi'(x)/\psi'(y)$ рационально, искомое равенство уже доказано. Осталось рассмотреть случай, когда отношение $\psi'(x)/\psi'(y)$ иррационально. Возьмем произвольное натуральное n . В силу выбора y в 2^{-n} -окрестности точки y найдется точка $\bar{y}$ с $\psi'(\bar{y}) \neq \psi'(y)$. По определению М-метода функция $\psi(x)$ непрерывно дифференцируема, поэтому $\psi'(x)$ непрерывна, и, следовательно, при z между y и $\bar{y}$ ее значения образуют целый интервал; стало быть, и отношение $\psi'(x)/\psi'(z)$ принимает всевозможные значения из некоторого интервала. В частности, найдется точка y_n на этом интервале (и тем самым в 2^{-n} -окрестности точки y), для которой отношение $\psi'(x)/\psi'(y_n)$ рационально, и, значит, $\bar{\psi}'(x)/\bar{\psi}'(y_n) = \psi'(x)/\psi'(y_n)$. Переходя к пределу $n \rightarrow \infty$, получим искомое равенство. Лемма доказана.

Докажем теперь саму теорему. В силу лемм 1 и 2 для функции $\psi(x)$, соответствующей оптимальному М-методу, при всех $\lambda > 0$ найдутся $b(\lambda)$ и $c(\lambda)$ такие, что

$$\psi(\lambda x) = b(\lambda) \psi(x) + c(\lambda). \quad (3)$$

Докажем, что функции $b(\lambda)$ и $c(\lambda)$ однозначно определены и дифференцируемы при $\lambda > 0$. В самом деле, так как $\psi(x) \neq \text{const}$, то найдутся x и y такие, что $\psi(x) \neq \psi(y)$. Тогда, вычитая равенства (3) для x и для y , получим:

$$b(\lambda) = (\psi(\lambda x) - \psi(\lambda y)) / (\psi(x) - \psi(y)),$$

где правая часть однозначно определена и гладко зависит от λ , а $c(\lambda) = \psi(\lambda x) - b(\lambda) \psi(x)$.

Так как зависимость b и c от λ гладкая, то можно продифференцировать обе части равенства (3) по λ и положить $\lambda = 1$, в результате получим: $x\psi'(x) = b\psi(x) + c$, где $b = db/d\lambda$, $c = dc/d\lambda$. В случае, если $b = 0$, будет $\psi(x) = c \ln x + c_1$, что противоречит предположению о непрерывности ψ в нуле. Значит, $b \neq 0$, откуда

$$\begin{aligned} d\psi/(b\psi + c) &= dx/x, \\ b^{-1} \ln(\psi + c/b) &= \ln x + c_1, \\ \psi(x) &= -c/b + \exp(c_1) x^{1/b}. \end{aligned}$$

Следовательно, в силу леммы 2 М-метод, соответствующий ψ , совпадает с I^p -методом, где $p = b^{-1}$. Теорема доказана.

З а м е ч а н и е 7. Если отказаться от условия непрерывности $\psi(x)$ в нуле, то дополнительно возникнет возможность $\psi(x) = \ln(x)$. Этот случай, однако, неинтересен, так как при этом условие $\sum \psi(x_i - x) \rightarrow \min$ описывает в точности $x = x_1, \dots, x_n$, т. е. здесь сжатие информации происходит за счет выбора произвольной оценки из числа результатов измерений.

Д о к а з а т е л ь с т в о о с н о в н о й л е м м ы (методом «от противного»). Пусть a — оптимальный метод для корректного критерия оптимальности $\lesssim$, $g \in G$ и $ga \neq a$. Поскольку a — оптимальный метод, то $a \gtrsim ga$, а так как a — единственный оптимальный метод, то $a > ga$. Так как $\gtrsim$ — корректный критерий, то он G -инвариантен, в частности $g^{-1}a > g^{-1}ga = a$, что противоречит оптимальности a . Противоречие завершает доказательство леммы.

Литература

1. Крейнвич В. Я. Об одном общем подходе к описанию неопределенностей в измерительной технике//Тез. докл. 3-й Всес. совещ. по теор. метрологии. Л., ВНИИМ, 1986, с. 187—188.
2. Крейнвич В. Я., Козленко В. Я. Оптимизация в условиях неопределенных критериев//Тез. докл. 4-й Всес. конф. «Применение методов матем. логики». Ч. 2. Таллин, 1986, с. 126—128.
3. Стогов Г. В., Макишанов А. В., Мусаев А. А. Устойчивые методы обработки результатов измерений//Зарубеж. радиоэлектрон. 1982. № 9. С. 3—46.

Eckblom H. Some observations on robust estimation//Nord. Tidskr. Inform. 1974. Vol. 14. P. 22—32.

Forsythe A. B. Robust estimation of straight line regression by minimising p -th power regression//Technometrics. 1972. Vol. 14. P. 159—170.

Кириллова И. С., Крейнович В. Я. Выбор 1-метода определения параметра сдвига на основе критерия применимости//Метрологическое обеспечение приборостроения. Л., ВНИИЭП, 1984, с. 91—97.

Finkelstein A. M., Kreinovich V. Ya., Zapatin R. R. Fundamental physical equations, uniquely determined by their symmetry groups//Lect. Notes Math. 1986. Vol. 1214. P. 159—170.

Солопченко Г. Н., Крейнович В. Я. Аппроксимация областей неопределенности эллипсоидами при решении обратных задач в измерительной технике//Тез. докл. 4-й Всес. симп. «Методы теории идентификации в задачах измерит. техн. и метрологии». Новосибирск, 1985, с. 75—76.

Крейнович В. Я. Семантика итеративного метода С. Ю. Маслова//Вопр. кибернетики. Вып. 131. М., 1987, с. 30—62.

Крейнович В. Я., Резник Л. К. Методы и модели формализации априорной информации в измерительных процедурах//Анализ и формализация вычислительного эксперимента. Л., ВНИИМ, 1986, с. 37—41.

БЕЗБАЗИСНЫЙ ГАРМОНИЧЕСКИЙ АНАЛИЗ И ИНВАРИАНТНЫЕ АППРОКСИМАЦИИ

Методы гармонического анализа, как известно, занимают значительное место в общем арсенале средств изучения процессов. Однако, несмотря на тщательную разработанность многих подходов от далеко идущих обобщений до быстрых алгоритмов, слабым местом большинства методик классификации, фильтрации, оценивания и т. п. является произвольность выбора базисов разложения.

В настоящей работе конструктивно решается задача о наилучшем приближении данной функции в L_1 , L_2 и M (см. обозначения в разд. 2) периодической функцией, период которой находится в заданном диапазоне. Рассматриваются различные обобщения этой задачи на теоретико-групповом уровне.

1. Постановка задачи

Основная задача работы состоит в отыскании функций, инвариантных относительно действия заданной группы на аргумент и наилучшим образом аппроксимирующих выделенную функцию f в метриках L_1 , L_2 или в равномерной метрике. Рассматривается также вопрос о наилучшем приближении f суммой заданного числа компонент, инвариантных относительно различных групп. Наибольший интерес с точки зрения приложений, по-видимому, представляют группы сдвигов. В этом случае приходится иметь дело с выделением периодических компонент. Однако, как показано в разд. 4 и 6, существуют практические задачи, требующие изучения других групп. Прежде всего это задачи уменьшения числа переменных в моделях, решающих правилах и т. п., задачи учета априорной информации в симметриях. Зачастую группа, определяющая тип симметрии, не известна точно, но имеется информация о классе, которому она принадлежит. В простейшем случае это указание на границы промежутка, содержащего период искомой периодической аппроксимации. Таким образом, встает задача оптимального приближения функцией, инвариантной относительно одной из групп класса.

Наконец, отметим, что практические соображения нередко приводят к дискриминации тех или иных подмножеств области определения исходной функции. В подобных случаях естественно определять метрики типа L_1 , L_2 с помощью подходящим образом выбранных весов или, более общо, мер.

2. Вспомогательные сведения

В работе используются следующие обозначения. $\mathbb{R}$ — множество действительных чисел; $\mathbb{R}_0^+$ — множество неотрицательных действительных чисел; $\mathbb{R}^n$ — n -мерное арифметическое пространство; $\mathbb{Z}$ — множество целых чисел; $\mathbb{Z}^+$ — множество натуральных чисел; $\mathbb{Z}_m$ — кольцо вычетов по модулю m ; 1_S — индикатор (характеристическая функция) множества S ; НОК (a, b) — наименьшее общее кратное, а НОД (a, b) — наибольший общий делитель двух натуральных чисел a и b ; mes_k — k -мерная мера Лебега; $\mathcal{P}$ — множество выпуклых компактов в $\mathbb{R}^n$; $\mathfrak{S}$ — единичная сфера в $\mathbb{R}^n$; $\text{Sf}(K, \theta)$ — значение опорной функции компакта $K \subset \mathbb{R}^n$ в точке $\theta \in \mathfrak{S}$; $\mathcal{H}_T$ — линейное подпространство T -периодических функций в гильбертовом пространстве $L_2(X, \mu)$, где X — множество с σ -алгеброй $\mathcal{T}$, а μ — мера; $\text{pr}(f | \mathcal{H})$ — проекция элемента f гильбертова пространства на подпространство $\mathcal{H}$; $\mathcal{H}_T \oplus \mathcal{H}_u$ — векторная сумма подпространств; $\text{Ang}(u, v)$ — угол между элементами гильбертова пространства в промежутке $[0, \pi]$; $\mathcal{P}(S)$ — линейная оболочка множества S ; G, G_j — группы, действующие на X ; G_x — орбита элемента x ; M, M_j — множества представителей орбит групп G и G_j (предполагается, что $M, M_j \in \mathcal{T}$); v_x — условные распределения на орбитах, т. е. такие нормированные на G_x меры, что для любого $A \in \mathcal{T}$

$$\mu(A) = \int_M v_x(A \cap G_x) \mu_0(dx),$$

где μ_0 — мера на $\mathcal{T}|_M$ (на сужении $\mathcal{T}$); $L_1(X, \mu)$ — пространство суммируемых по мере μ функций $f: X \rightarrow \mathbb{R}$; $\mathcal{M}(X)$ — пространство ограниченных на X функций с равномерной нормой; $\text{Med}(g | v_x)$ — медиана функции g относительно меры v_x .

В разд. 3 будут необходимы хорошо известные вспомогательные утверждения, которые назовем леммами.

Л е м м а 1. Если $\mathcal{P}$ — нормированная мера на Y , а f — функция из $L_2(Y, \mathcal{P})$, то константа $c_0 = \int_Y f(x) \mathcal{P}(dx)$ минимизирует функцию r , задаваемую формулой:

$$r(c) = \int_Y (f(x) - c)^2 \mathcal{P}(dx).$$

Это утверждение легко вытекает из равенства $r(c) = r(c_0) + (c - c_0)^2$.

Л е м м а 2. Если $\mathcal{P}$ — нормированная мера на Y , а $f \in L_2(Y, \mathcal{P})$, то $\text{Med}(f | \mathcal{P})$ минимизирует

$$s(c) = \int_Y |f(x) - c| \mathcal{P}(dx).$$

Утверждение непосредственно вытекает из определения медианы.

Л е м м а 3. Если f — ограниченная функция на Y , то константа $c_0 = \frac{1}{2} \left(\sup_Y f + \inf_Y f \right)$ минимизирует

$$g(c) = \sup_Y |f(x) - c|.$$

Утверждение очевидно.

З а м е ч а н и е 1. В ряде случаев будем рассматривать периодические функции не только на $\mathbb{R}$ или $\mathbb{Z}$, но и на отрезках $[0, D]$ или $\{1, \dots, n\}$. Уточним понятие T -периодичности функции h на множестве $S \subset \mathbb{R}$ следующим образом:

$$\forall x (x, x+T \in S \Rightarrow h(x) = h(x+T)).$$

3. Математическое решение основных задач

Сформулируем и докажем основные утверждения, используемые в дальнейшем для построения алгоритмов аппроксимации. Первое из них связано с квадратичной метрикой.

Т е о р е м а 1. Пусть $|f| \leq r$, где r — некоторая G -инвариантная функция из $L_2(X, \mu)$. Тогда формула

$$h(x) = \int_{G_x} f(z) v_x(dz)$$

задает G -инвариантную функцию, ближайшую к f в $L_2(X, \mu)$.

Д о к а з а т е л ь с т в о. Во-первых, заметим, что

$$\begin{aligned} |h(x)| &= \left| \int_{G_x} f(z) v_x(dz) \right| \leq \int_{G_x} |f(z)| v_x(dz) \leq \\ &\leq \int_{G_x} r(z) v_x(dz) = r(x) v_x(G_x) = r(x), \end{aligned}$$

поэтому $h \in L_2(X, \mu)$. Далее, для любого элемента $g \in G$

$$h(gx) = \int_{G_{gx}} f(z) v_{gx}(dz) = \int_{G_x} f(z) v_x(dz) = h(x),$$

так что h является G -инвариантной. Наконец, по лемме 1 функция h является наилучшим приближением f в $L_2(G_x, v_x)$ среди всех констант, т. е. для любой G -инвариантной функции u из L_2 :

$$\int_{G_x} (f(z) - h(z))^2 v_x(dz) \leq \int_{G_x} (f(z) - u(z))^2 v_x(dz).$$

Проинтегрировав левую и правую части по мере μ_0 на M , получим:

$$\int_X (f(x) - h(x))^2 \mu(dx) \leq \int_X (f(x) - u(x))^2 \mu(dx). \quad \square$$

Второе утверждение рассматривает аппроксимации в L_1 .

Т е о р е м а 2. Пусть $|f| \leq r$, где r — некоторая G -инвариантная функция из $L_1(X, \mu)$.

Тогда формула

$$h(x) = \text{Med}(f|_{G_x}, \nu_x)$$

задает G -инвариантную функцию, ближайшую к f в $L_1(X, \mu)$.

Д о к а з а т е л ь с т в о. Очевидно,

$$|h(x)| = |\text{Med}(f|_{G_x}, \nu_x)| \leq \text{Med}(|f|_{G_x}, \nu_x) \leq \text{Med}(r|_{G_x}, \nu_x) = r(x),$$

откуда следует, что $h \in L_1(X, \mu)$. Поскольку

$$h(gx) = \text{Med}(f|_{G_x}, \nu_x) = \text{Med}(f|_{G_x}, \nu_x) = h(x),$$

то h является G -инвариантной. Отсюда в свою очередь вытекает, что h постоянная на G_x и в силу леммы 2 минимизирует

$$\int_{G_x} |f(z) - h(z)| \nu_x(dz)$$

в классе констант на G_x . Остается повторить последнее рассуждение из доказательства теоремы 1.

Третье утверждение относится к задаче равномерной аппроксимации.

Т е о р е м а 3. Пусть $|f| \leq r$, где r — некоторая G -инвариантная функция из $\mathcal{M}(X)$.

Тогда формула

$$h(x) = \frac{1}{2} \left(\sup_{z \in G_x} f(z) + \inf_{z \in G_x} f(z) \right).$$

задает G -инвариантную функцию, ближайшую к f в $\mathcal{M}(X)$.

Д о к а з а т е л ь с т в о. Так как

$$\begin{aligned} |h(x)| &\leq \frac{1}{2} \left(\sup_{z \in G_x} |f(z)| + \inf_{z \in G_x} |f(z)| \right) \leq \\ &\leq \frac{1}{2} \left(\sup_{z \in G_x} r(z) + \inf_{z \in G_x} r(z) \right) = r(x), \end{aligned}$$

то $h \in \mathcal{M}(X)$.

G -инвариантность h доказывается рассуждениями, аналогичными доказательствам теорем 1 и 2. Оптимальность следует из леммы 3.

Теперь перейдем к задаче приближения f в L_2 суммами вида $h = h_1 + \dots + h_k$, где h_j является G_j -инвариантной, причем G_j коммутативна.

Обозначим через $G = \bigcap_{j=1}^k G_j$, $G_0 = \bigoplus_{j=1}^k G_j$, H_j — линейное подпространство G_j -инвариантных функций, H — пространство G -инвариантных функций, $H_0 = \mathcal{L}(H_1 \oplus \dots \oplus H_k)$.

В общем случае всегда $H_0 \subset H$, но $\dim H_0$ может быть меньше, чем $\dim H$. Рассматривая индикаторы $e_x^j = \mathbb{1}_{G_x}$ для $x \in M_j$, получаем ортогональный базис H_j . Но объединение множеств $U_j = \{e_x^j \mid x \in M_j\}$ является, вообще говоря, зависимой системой. Изучая пересечения пространств H_j , можно исключить лишние элементы из $\bigcup_{j=1}^k U_j$ и спроектировать f на линейную оболочку полученного множества. Таков один из возможных путей решения задачи.

В теоремах 4 и 5 рассмотрим более подробно реализацию этого подхода для $k = 2$ и групп сдвигов. В результате анализа станут достаточно ясными соотношения между линейными подпространствами компонент аппроксимации и появятся некоторые алгоритмы вычисления компонент. К сожалению, эти алгоритмы не являются достаточно эффективными (с точки зрения временной сложности), поэтому заслуживают рассмотрения, быть может, менее прямые и прозрачные, но более экономные в вычислительном отношении подходы. Один из них продемонстрирован в теореме 6.

Итак, начнем с частного случая, в котором $k = 2$; G_1, G_2 — группы сдвигов на $\mathbb{Z}$ с периодами T_1 и $T_2 \in \mathbb{Z}^+$ ($\text{НОД}(T_1, T_2) = 1$), Q — плотность μ .

Т е о р е м а 4. Пусть $f \in L_2(\mathbb{Z}, \mu)$. G_1, G_2 — группы сдвигов на $\mathbb{Z}$, кратных T_1 и T_2 соответственно, T_1 и T_2 взаимно просты. Тогда отыскание наилучшего в L_2 приближения функции f суммами $h_1 + h_2$, где h_j является G_j -инвариантной (T_j -периодичной), сводится к проектированию f на подпространство, порожденное $T_1 + T_2 - 1$ векторами $e_0^1, \dots, e_{T_1-1}^1, e_0^2, \dots, e_{T_2-2}^2$.

Д о к а з а т е л ь с т в о. Очевидно, в качестве M_j можно взять множество $\{0, 1, \dots, T_j - 1\}$ ($j = 1, 2$). Пусть G — группа сдвигов на kT_1T_2 ($k \in \mathbb{Z}$), G_0 — группа всех сдвигов на $\mathbb{Z}$. Поскольку $H_0 \subset H$ и H — подпространство T_1T_2 -периодических функций, то искомое приближение достаточно вычислить на множестве $\{0, 1, \dots, T_1T_2 - 1\}$. Заметим, что $\{e_l^1 \mid 0 \leq l < T_1\}$, $\{e_l^2 \mid 0 \leq l < T_2\}$ — базисы H_1 и H_2 соответственно. Так как

$$\sum_{l=0}^{T_1-1} e_l^1 = \sum_{l=0}^{T_1-1} e_l^2 = 1, \quad \text{то} \quad \sum_{l=0}^{T_1-1} e_l^1 - \sum_{l=0}^{T_2-1} e_l^2 = 0,$$

т. е. объединение базисов — зависимая система. В силу максимальности $G_0 \dim(H_1 \cap H_2) = 1$. Исключаем один вектор $e_{T_2-1}^2$ из списка и получаем базис $e_0^1, \dots, e_{T_1-1}^1, e_0^2, \dots, e_{T_2-2}^2$ из $T_1 + T_2 - 1$ элементов.

Более общий случай с произвольным НОД (T_1, T_2) можно свести к рассмотренному факторизацией, учитывая, что $\mathcal{H}_{T_1} \cap \mathcal{H}_{T_2} = \mathcal{H}_{\text{НОД}(T_1, T_2)}$, где $\mathcal{H}_T$ — пространство T -периодических функций. Результатом явится теорема.

Т е о р е м а 5. Если $f \in L_2(Z, \mu)$, G_1, G_2 — группы сдвигов на Z , кратных T_1 и T_2 соответственно, то отыскание наилучшего в L_2 приближения функции f суммами $h = h_1 + h_2$ (где $h_j \in \mathcal{H}_{T_j}$) сводится к проектированию f на подпространство, порожденное $T_1 + T_1 - \tau$ векторами $e_0^1, \dots, e_{T_1-1}^1, e_0^2, \dots, e_{T_2-\tau}^2$ ($\tau = \text{НОД}(T_1, T_2)$).

З а м е ч а н и е 2. Тот факт, что из объединения базисов

$$\{e_s^1 | s \in \{0, \dots, T_1 - 1\}, \{e_s^2 | s \in \{0, \dots, T_2 - 1\}\}$$

можно отбросить τ последних элементов, можно было бы установить и непосредственным выводом уравнений, связывающих элементы различных базисов:

$$\sum_{s=1}^{T_j/\tau} e_{s\tau+u}^j = e_u^0,$$

где $j = 1, 2$; $u \in \{0, \dots, \tau - 1\}$; e_u^0 — базисный элемент в $\mathcal{H}_\tau$ ($e_u^0(x) = \mathbb{1}_{\{x, x \equiv u \pmod{\tau}\}}$). Приравнявая для каждого u суммы по различным j , имеем:

$$\sum_{s=1}^{T_1/\tau} e_{s\tau+u}^1 = \sum_{s=1}^{T_1/\tau} e_{s\tau+u}^2 \quad (u = 0, \dots, \tau - 1). \quad \square$$

С л е д с т в и е 1. Искомая аппроксимация h из теоремы 5 имеет вид:

$$h = \sum_{k=1}^{T_1} e_k^{[T_1]} a_k + \sum_{k=1}^{T_2-\tau} e_k^{[T_2]} a_{k+T_1}, \quad (1)$$

где вектор $\mathbf{A} = (a_k)_{k=1}^{k=r}$ ($r = T_1 + T_2 - \tau$) является решением линейной системы $\mathbf{CA} = \mathbf{R}$, $\mathbf{C} = \mathbf{B}^T \mathbf{Q} \mathbf{B}$, $\mathbf{R} = \mathbf{B}^T \mathbf{Q} \mathbf{F}$, $\mathbf{B}$ — матрица порядка $n \times r$ (n — число элементов носителя $\mathbb{Q}$), элементы $\mathbf{B}$ при $j \leq T_1$ имеют вид $b_{ij} = 1$, если $(i \equiv j) \pmod{T_1}$, и 0 — в противном случае; при $j > T_1$ $b_{ij} = 1$, если $(i \equiv j - T_1) \pmod{T_2}$, и 0 — в противном случае; $\mathbf{Q}$ — диагональная матрица $n \times n$ с элементами $Q(j)$; $\mathbf{F}$ — вектор размерности n с элементами $f(j)$.

Заметим, что в силу диагональности матрицы $\mathbf{Q}$

$$c_{ij} = \sum_{k=1}^n Q(k) b_{ki} b_{kj}, \quad p_j = \sum_{k=1}^n Q(k) f(k) b_{kj}.$$

Матрица $\mathbf{C}$ имеет блочный вид:

$$\mathbf{C} = \left(\begin{array}{c|c} \mathbf{C}^{(11)} & \mathbf{C}^{(12)} \\ \hline \mathbf{C}^{(21)} & \mathbf{C}^{(22)} \end{array} \right),$$

при этом $C^{(21)} = (C^{(12)})^T$, $C^{(11)}$ диагональна, ее элементы $c_{ii}^{(11)} =$
 $= \sum_{j=0}^{\theta/T_1-1} Q(i+jT_1)$; $C^{(22)}$ также диагональна с элементами

$$c_{ii}^{(11)} = \sum_{j=0}^{\theta/T_2-1} Q(i+jT_2).$$

Здесь $\theta = \text{НОК}(T_1, T_2)$.

Компоненты вектора P для $j \leq T_1$ имеют вид:

$$p_j = \sum_{(k \equiv j) \bmod T_1} Q(k) f(k),$$

а для $j > T_1$ они задаются формулой:

$$p_j = \sum_{(k \equiv j-T_1) \bmod T_2} Q(k) f(k). \quad \square$$

З а м е ч а н и е 3. Первая сумма в правой части (2) является T_1 -периодической функцией, а вторая — T_2 -периодической, так что формула (1) дает одно из возможных разложений. Ясно, однако, что существуют другие разложения. Все семейство разложений может быть описано с помощью линейных комбинаций векторов, исключенных нами из базиса подпространства $\mathcal{H}_T$, (см. теорему 5 и замечание 2).

Докажем теперь теорему, дающую более удобный в чисто вычислительном отношении способ аппроксимации суммой двух компонент и сводящий задачу к отысканию одиночных аппроксимаций.

Т е о р е м а 6. Пусть $f \in L_2(Z, \mu)$, для $T \in \mathbb{Z}^+ \mathcal{H}_T$ — линейное пространство T -периодических функций, $T_1, T_2 \in \mathbb{Z}^+$, $\tau = \text{НОД}(T_1, T_2)$, $\mathcal{H} = \mathcal{L}(\mathcal{H}_{T_1} \oplus \mathcal{H}_{T_2})$, $u = \text{pr}(f | \mathcal{H}_\tau)$, $u_j = \text{pr}(f - u | \mathcal{H}_{T_j})$ ($j = 1, 2$),

$$s_j = \frac{(f - u) u_j}{\|u_j\|},$$

$$c_j = s_j + s_{3-j} \sqrt{\frac{\|f - u\|^2 - s_j^2}{\|f - u\|^2 - s_{3-j}^2}},$$

тогда справедливо представление:

$$\text{pr}(f | \mathcal{H}) = c_1 u_1 + c_2 u_2 + u, \quad (2)$$

причем, очевидно, $c_j u_j$, $u \in \mathcal{H}_{T_j}$ ($j = 1, 2$).

Д о к а з а т е л ь с т в о. Из построения u (с учетом того, что $\mathcal{H}_\tau = \mathcal{H}_{T_1} \cap \mathcal{H}_{T_2}$) вытекает свойство $f - u \perp \mathcal{H}_\tau$, откуда в свою очередь

$$\text{pr}(f - u \perp \mathcal{H}) = p_1 + p_2,$$

где $p_j \in \mathcal{H}_{T_j}$ и $p_j = c_j u_j$, где $c_j \geq 0$. Если $f = u$, утверждение очевидно. Предположим, что $f \neq u$, и обозначим $\alpha_j = \text{Ang} \langle p_j, f - u \rangle$, тогда

$$\alpha_j \in \left[0, \frac{\pi}{2}\right], \quad t_j = \cos \alpha_j = \frac{s_j}{\|f - u\|}$$

и, кроме того,

$$\|p_j\| \sin(\alpha_1 + \alpha_2) = \|f - u\| \sin \alpha_{3-j},$$

отсюда

$$\begin{aligned} \|p_j\| &= \|f - u\| \frac{\sqrt{1 - t_{3-j}^2}}{\sqrt{1 - t_j^2} t_{3-j} + \sqrt{1 - t_{3-j}^2} t_j} = \\ &= s_j + s_{3-j} \sqrt{\frac{\|f - u\|^2 - s_j^2}{\|f - u\|^2 - s_{3-j}^2}}. \quad \square \end{aligned}$$

З а м е ч а н и е 4. Как уже было сказано в замечании 3, представление проекции $\text{rg}(f | \mathcal{H})$ в виде суммы функций из $\mathcal{H}_{T_1}$ и $\mathcal{H}_{T_2}$ не однозначно. В формуле (2) третье слагаемое u может быть разбито в свою очередь на два слагаемых $u = \lambda u + (1 - \lambda) u$, где $\lambda \in \mathbb{R}$, и в качестве компонент искомой аппроксимации взяты функции $h_1 = c_1 u_1 + \lambda u$, $h_2 = c_2 u_2 + (1 - \lambda) u$.

В конкретных приложениях встречаются три различных предпочтения формы представления $\text{rg}(f | \mathcal{H})$:

- а) $\lambda = 1$ — присоединение u к $c_1 u_1$;
- б) $\lambda = 1/2$ — минимизация суммы квадратов норм $\|h_1\|^2 + \|h_2\|^2$, обычно играющих роль энергии;
- в) отдельная запись слагаемого u (в случае компьютерных вычислений — отдельное хранение в памяти).

З а м е ч а н и е 5. Анализ пересечений подпространств $\mathcal{H}_{T_1}$, ..., $\mathcal{H}_{T_k}$ позволяет обобщить метод, описываемый теоремой 6, на случай k -компонентного приближения.

4. Следствия из основных теорем

Все задачи, перечисленные во введении и в разд. 1, могут быть решены с помощью теорем 1—6.

1. **Периодические функции на $\mathbb{R}$.** Пусть $f \in L_2(\mathbb{R}, \mu)$, где μ абсолютно непрерывна по мере Лебега и задается плотностью $Q: \mathbb{R} \rightarrow \mathbb{R}_+^*$. Задача отыскания T -периодической функции $h \in L_2(\mathbb{R}, \mu)$, наилучшим образом приближающей f , согласно теореме 1 решается формулой:

$$h(x) = \sum_{k \in \mathbb{Z}} f(x + kT) Q^*(x + kT), \quad (3)$$

если в качестве X взять $\mathbb{R}$, а в качестве группы G — группу сдвигов, кратных T , $Q^*(x + kT) = Q(x + kT) / \sum_{k \in \mathbb{Z}} Q(x + kT)$.

Если нас интересует приближение в L_1 , то решение по теореме 2 задается формулой:

$$h(x) = \inf \left\{ z \mid \sum_{k: f(x+kT) < z} Q^*(x+kT) \geq \frac{1}{2} \right\}. \quad (4)$$

Для равномерной аппроксимации по теореме 3

$$h(x) = \frac{1}{2} \left(\sup_{k \in \mathbb{Z}} f(x+kT) + \inf_{k \in \mathbb{Z}} f(x+kT) \right). \quad (5)$$

2. Периодические функции на отрезке. Выберем в задачах разд. 4.1 плотность вида $Q(x) = \mathbb{1}_{[0, D]}$, $D > 0$. Тогда формулы (3) и (4) дадут решение задач о T -периодической аппроксимации на $[0, D]$ (см. замечание 1).

3. Периодические функции на $\mathbb{Z}$ и $\{1, \dots, n\}$. Формулы (3)—(5) остаются справедливыми в случае, если $X = \mathbb{Z}$, $T \in \mathbb{Z}^+$. Для функций на $\{1, \dots, n\}$ в L_2 с равномерным весом

$$h(x) = C_x \sum_{k \in \mathbb{Z}} f(x+kT),$$

где

$$-\frac{x}{T} < k \leq \frac{n-x}{T}, \quad C_x = \left(\left[\frac{n-x}{T} \right] - \left[-\frac{x}{T} \right] \right)^{-1}.$$

Для функций на $\{1, \dots, n\}$ в L_1 с равномерным весом

$$h(x) = \inf \left\{ z \mid \text{card} \{k \mid f(x+kT) < z\} \geq \frac{n}{2} \right\}.$$

4. Единичная окружность. Если $X = \{e^{i\theta} \mid \theta \in [0, 2\pi[\}$, G — группа сдвигов на X , задаваемых аргументами вида $\theta = k\alpha$, где $k \in \mathbb{Z}$, $\alpha = 2\pi/p$, $p \in \mathbb{Z}^+$, то приходим к задаче аппроксимации 2π -периодической функции функцией с меньшим периодом. В L_2 с равномерным весом решение имеет вид:

$$h(e^{i\theta}) = \frac{1}{p} \sum_{k=1}^p f(e^{i(\theta+k\alpha)}),$$

в общем случае

$$h(e^{i\theta}) = \left(\sum_{k=1}^p f(e^{i(\theta+k\alpha)}) Q(e^{i(\theta+k\alpha)}) \right) / \sum_{k=1}^p Q(e^{i(\theta+k\alpha)}).$$

Соответствующие изменения претерпевают формулы (4) и (5).

5. Кольцо вычетов. Дискретным аналогом задачи из разд. 4 является случай $X = \mathbb{Z}_m$, G — аддитивная подгруппа $\mathbb{Z}_m$.

6. Функции меньшего числа переменных. В задачах оптимизации управления многопараметрическими системами часто возникает необходимость аппроксимировать функцию $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ функцией, не зависящей от некоторых переменных. Эта проблема сводится к изучению случая $X = \mathbb{R}^n$, G — группа всех сдвигов по фиктивным переменным. Решения

сразу следуют из теорем 1—3. Так, для L_2 с равномерным на $[0; 1]^n$ весом $\mathbb{1}_{[0; 1]^n}$ имеем:

$$h(x) = \underbrace{\int_0^1 \dots \int_0^1}_{k} f(x_1, \dots, x_k) dx_1, \dots, dx_k,$$

если $x_1, \dots, x_k$ — фиктивные переменные. Для L_1

$$\begin{aligned} h(x_1, \dots, x_k, x_{k+1}, \dots, x_n) = \\ = \inf \left\{ z \mid \text{mes}_k \{ (x_1, \dots, x_k) \mid f(x_1, \dots, x_n) < z \} \geq \frac{1}{2} \right\}. \end{aligned}$$

Для пространства $\mathcal{M}$

$$\begin{aligned} h(x_1, \dots, x_k, x_{k+1}, \dots, x_n) = \\ = \frac{1}{2} \left(\sup_{0 \leq x_1 \dots x_k \leq 1} f(x_1, \dots, x_n) + \inf_{0 \leq x_1 \dots x_k \leq 1} f(x_1, \dots, x_n) \right). \end{aligned}$$

7. Периодические множества. В задачах растровой оптики [1, 2] приходится восстанавливать периодические множества (растры), искаженные шумами. Эта задача сводится к уже рассмотренным и к замене множеств их индикаторами и соответствующим выбором группы (очень часто это группа сдвигов на плоскости с двумя образующими).

8. Симметричные выпуклые множества. Аппроксимация выпуклого компакта K в $\mathbb{R}^n$ центрально-симметричным выпуклым компактом K_0 в метрике Хаусдорфа сводится к равномерной аппроксимации опорной функции $Sf(K, \square)$ четной функцией на единичной сфере. При этом квадратичная аппроксимация соответствует приближению в квадратичной метрике на $\mathcal{C}$. Таким образом, в качестве группы G можно взять группу, порожденную отображением $\alpha \mapsto -\alpha$ ($\alpha \in G$). Использование более богатых подгрупп сдвигов приводит к вычислению аппроксимаций K выпуклыми компактами с поворотной симметрией заданного порядка. Так, формула

$$K_0 = \frac{1}{p} \bigoplus_{i=1}^p \mathcal{R}_0^{i/p}(K),$$

где $p \in \mathbb{Z}^+$, $\alpha = 2\pi/p$, $\mathcal{R}_0^\theta$ — поворот на угол θ вокруг начала, $K \in \mathcal{C}(\mathbb{R}^2)$, $\bigoplus$ — сложение по Минковскому, задает наилучшее квадратическое приближение K с условием поворотной симметрии порядка p и равномерным по углу (изотропным) весом.

Аналогичным образом можно изучать аксиальные симметрии и симметрии относительно аффинных многообразий более высоких размерностей.

9. Четные функции. Наилучшее приближение функции $f: \mathbb{R} \rightarrow \mathbb{R}$ четной функцией соответствует выбору $X = \mathbb{R}$,

$G = \{x \mapsto x, x \mapsto -x\}$. При квадратичной оптимизации решением является функция:

$$h(x) = \frac{Q(x)f(x) + Q(-x)f(-x)}{Q(x) + Q(-x)},$$

где $Q = \partial\mu/\partial \text{mes}_1$. Если плотность Q сама является четной, то функция h совпадает с так называемой четной частью f :

$$h(x) = \frac{1}{2} (f(x) + f(-x)).$$

То же решение (6) получаем для оптимизации в $\mathcal{M}$, а если Q четна, то оно является решением в L_1 .

10. Суммы конечного числа периодических функций. Предположим, что $f: \mathbb{Z} \rightarrow \mathbb{R}$ и требуется приблизить f в $L_2(\mathbb{Z}, \mu)$ суммой $h_1 + h_2$, где h_j имеет период $T_j \in \mathbb{Z}$ ($j = 1, 2$). Обозначим $\tau = \text{НОД}(T_1, T_2)$.

Как показано в теореме 6, для вычисления аппроксимации следует найти $u = \text{рг}(f| \mathcal{H}_\tau)$, $u_1 = \text{рг}(f - u| \mathcal{H}_{T_1})$, $u_2 = \text{рг}(f - u| \mathcal{H}_{T_2})$. Заметим, что $u \in \mathcal{H}_{T_1} \cap \mathcal{H}_{T_2}$, поэтому в силу линейности проекции

$$u_j = \text{рг}(f| \mathcal{H}_{T_j}) - \text{рг}(u| \mathcal{H}_{T_j}) = \text{рг}(f| \mathcal{H}_{T_j}) - u.$$

Отсюда видно, что за один просмотр массива значений f можно накопить суммы, необходимые для вычисления проекций f на $\mathcal{H}_{T_1}$, $\mathcal{H}_{T_2}$ и $\mathcal{H}_\tau$ (см. алгоритм 6 в разд. 5), после чего легко вычисляются все необходимые коэффициенты.

11. Интервал периодов. Задача наилучшего среднеквадратического приближения $f \in L_2(\{1, \dots, n\}, \mu)$ периодической функцией с периодом $T \in [T_1, T_2]$ сводится к испытанию подряд периодов $T_1, T_1 + 1, \dots, T_2$. Соответствующие вычисления можно выполнить за один просмотр массива значений f (см. алгоритм 1). Вообще говоря, если среди периодов имеются кратные, то можно более экономно вычислять суммы, группируя их в удобные блоки. Однако практически такая возможность возникает редко.

5. Алгоритмы

Из теоремы 1 нетрудно извлечь алгоритм среднеквадратического приближения функцией на $\mathbb{Z}$ с заданным периодом per . Рассмотрим вначале случай, когда вес Q является индикатором множества $\{1, \dots, n\}$.

А л г о р и т м 1

- | | |
|--------------------------------|--|
| 1. Ввод n, per ; | 5. КЦ i ; |
| 2. Ввод $f[i]$ ($i = 1, n$); | 6. НЦ $j = 1, n$; |
| 3. НЦ $i = 1, \text{per}$; | 7. $k \leftarrow (j - 1) \bmod \text{per} + 1$; |
| 4. $S[i] \leftarrow 0$; | 8. $S[k] \leftarrow S[k] + f[j]$; |

- | | |
|---|--|
| 9. КЦ j ; | 16. $h[l] \leftarrow S[k]$; |
| 10. НЦ $m = 1$, per; | 17. КЦ l ; |
| 11. $\text{norm} \leftarrow \text{trunc}((n -$ | 18. $\text{dist} \leftarrow 0$; |
| $- m/\text{per}) - \text{trunc}(-m/\text{per})$; | 19. НЦ $t = 1, n$; |
| 12. $S[m] \leftarrow S[m]/\text{norm}$; | 20. $\text{dist} \leftarrow \text{dist} +$ |
| 13. КЦ m ; | $+ \text{sqr}(h[t] - f[t])$; |
| 14. НЦ $l = 1, n$; | 21. КЦ t . |
| 15. $k \leftarrow (l - 1) \bmod \text{per} + 1$; | |

Здесь шаги 1 и 2 описывают ввод исходных данных, 3—5 — инициализацию массива $S[\dots]$, предназначенного для хранения значений аппроксимации на периоде, шаги 6—13 осуществляют вычисленные аппроксимации на $\{1, \dots, \text{per}\}$, причем 6—9 накапливают необходимые суммы, а 10—13 предназначены для нормирования сумм. Остальные шаги алгоритма являются факультативными: на отрезке 14—17 происходит полное восстановление аппроксимации $h[\dots]$ на множестве $\{1, \dots, n\}$, на отрезке 18—21 — вычисление $\|f - h\|^2$.

Если веса произвольны и равны нулю вне $\{1, \dots, n\}$, то вычисления немного усложняются.

А л г о р и т м 2

- | | |
|---|--|
| 1. Ввод n , per; | 12. НЦ $m = 1$, per; |
| 2. Ввод $f[i]$, $Q[i]$ ($i = 1, n$); | 13. $S[m] \leftarrow S[m]/\text{nor}[m]$; |
| 3. НЦ $i = 1$, per; | 14. КЦ m ; |
| 4. $S[i] \leftarrow 0$; | 15. НЦ $l = 1, n$; |
| 5. $\text{por}[i] \leftarrow 0$; | 16. $k \leftarrow (l - 1) \bmod \text{per} + 1$; |
| 6. КЦ i ; | 17. $h[l] \leftarrow S[k]$; |
| 7. НЦ $j = 1, n$; | 18. КЦ l ; |
| 8. $k \rightarrow (j - 1) \bmod \text{per} + 1$; | 19. $\text{dist} \leftarrow 0$; |
| 9. $S[k] \leftarrow S[k] + f[j] *$ | 20. НЦ $t = 1, n$; |
| $* Q[j]$; | 21. $\text{dist} \leftarrow \text{dist} + \text{sqr}(h[t] -$ |
| 10. $\text{por}[k] \leftarrow Q[j]$; | $- f[t]) * Q[t]$; |
| 11. КЦ j ; | 22. НЦ t . |

Теорема 2 дает способ построения алгоритма приближения $f[\]$ функцией $h[\]$ с периодом per в L_1 .

Для аппроксимации с равномерным весом предназначен алгоритм 3, а алгоритм 4 применим к общей ситуации.

А л г о р и т м 3

- | | |
|--|---|
| 1. Ввод n , per; | 10. $\text{sort}(k, R[k])$; |
| 2. Ввод $f[i]$ ($i = 1, n$); | 11. $m \leftarrow R[k] \bmod 2$; |
| 3. НЦ $i = 1, n$; | 12. $\text{if odd}(R[k]) \text{ then } S[k] \leftarrow$ |
| 4. $k \leftarrow (i - 1) \bmod \text{per} + 1$; | $\leftarrow p[k, m + 1]$; |
| 5. $l \leftarrow (i - 1) \bmod \text{per}$; | 13. $\text{else } S[k] \leftarrow (p[k, m] +$ |
| 6. $p[k, l] \rightarrow f[i]$; | $+ p[k, m + 1]) * 0.5$; |
| 7. $R[k] \rightarrow l$; | 14. КЦ k ; |
| 8. КЦ i ; | 15. НЦ $j = 1, n$; |
| 9. НЦ $k = 1$, per; | 16. $k \leftarrow (j - 1) \bmod \text{per} + 1$; |

17. $h[j] \leftarrow S[k]$;
 18. КЦ;
 19. $\text{dist} \leftarrow 0$;
 20. НЦ $t = 1, n$;

21. $\text{dist} \leftarrow \text{dist} + \text{abs}(h[t] - f[t])$;
 22. КЦ t .

Здесь процедура $\text{sort}(k, m)$ осуществляет сортировку отрезка длины m k -й строки массива $p[]$ и записывает результат в ту же строку. На отрезке 15—18 происходит полное восстановление компоненты, а шаги 19—22 предназначены для вычисления $\|h - f\|$ в L_1 . Вспомогательный массив $p[]$ имеет размеры $[1 \dots \text{per}, 0 \dots n \text{ div per} + 1]$.

А л г о р и т м 4

1. Ввод n, per ;	15. $w[j] \leftarrow w[j] * 0.5$;
2. Ввод $f[i], Q[i] (i = 1, n)$;	16. КЦ j ;
3. НЦ $j = 1, \text{per}$;	17. НЦ $k = 1, \text{per}$;
4. $w[j] \leftarrow 0$;	18. $\text{sort } 2(k, R[k])$;
5. КЦ j ;	19. $a \leftarrow 0; m \leftarrow 0$;
6. НЦ $i = 1, n$;	20. while $a < w[k]$ do 21—22;
7. $k \rightarrow (i - 1) \bmod \text{per} + 1$;	21. $m \leftarrow m + 1$;
8. $l \rightarrow (i - 1) \text{ div per}$;	22. $a \leftarrow a + z[k, m]$;
9. $R[k] \leftarrow l$;	23. $S[k] \rightarrow (p[k, m - 1] * z[k, m - 1] + p[k, m] * z[k, m]) / (z[k, m - 1] + z[k, m])$;
10. $p[k, l] \leftarrow f[i]$;	24. КЦ k ;
11. $z[k, l] \leftarrow Q[i]$;	25. Шаги 15—22 алгоритма 3.
12. $w[k] \leftarrow w[k] + Q[i]$;	
13. КЦ i ;	
14. НЦ $j = 1, \text{per}$;	

Процедура $\text{sort } 2$ в алгоритме 4 сортирует строку $p[]$, производя соответствующую перестановку строки $z[]$. В алгоритме предполагается, что на $\{1, \dots, n\}$ $Q[i] > 0$.

Теорема 3 дает я простой способ периодической равномерной аппроксимации.

А л г о р и т м 5

1. Ввод n, per ;	12. $\text{dist} \leftarrow 0$;
2. Ввод $f[i] (i = 1, n)$;	13. НЦ $k = 1, \text{per}$;
3. НЦ $i = 1, \text{per}$;	14. $h[k] \leftarrow (b[k] + a[k]) * 0.5$;
4. $a[i] \leftarrow f[i]$;	15. $\text{dist} \leftarrow \max(\text{dist}, (b[k] - a[k]) * 0.5)$;
5. $b[i] \leftarrow f[i]$;	16. КЦ k ;
6. КЦ i ;	17. НЦ $m = \text{per} + 1, n$;
7. НЦ $j = \text{per} + 1, n$;	18. $l \leftarrow (m - 1) \bmod \text{per} + 1$;
8. $k \rightarrow (j - 1) \bmod \text{per} + 1$;	19. $h[m] \leftarrow h[l]$;
9. $a[k] \leftarrow \min(a[k], f[j])$;	20. КЦ m .
10. $b[k] \leftarrow \max(b[k], f[j])$;	
11. КЦ j ;	

Шаги 3—11 алгоритма 5 предназначены для вычисления минимальных и максимальных значений f на орбитах (классах вычетов), 12—16 — для вычисления начального отрезка аппрокси-

мации длиной per и расстояния от h до f в метрике μ . На участке 17—20 происходит полное восстановление аппроксимации.

Рассмотрим алгоритм 6, предназначенный для выделения компонент среднеквадратической аппроксимации суммой двух периодических функций и основанный на теореме 6. Заметим, что алгоритм 1 мог бы быть использован для параллельного выделения компонент с заданным списком периодов. Обозначим такую параллельную модификацию для трех компонент через сопр и приведем текст алгоритма 6.

А л г о р и т м 6

- | | |
|---|--|
| 1. Ввод n , per 1, per 2; | 17. $SC1 \leftarrow SC1 + \Delta * u1[i]$; |
| 2. Ввод $f[i]$ ($i = 1, n$); | 18. $SC2 \leftarrow SC2 + \Delta * u2[i]$; |
| 3. $\text{per} 3 \leftarrow \text{НОД}(\text{per} 1, \text{per} 2)$; | 19. КЦ i ; |
| 4. $H1, H2, H3 \leftarrow \text{comp}(f, n, \text{per} 1, \text{per} 2, \text{per} 3)$; | 20. $S1 \leftarrow SC1/\text{SQRT}(N1)$; |
| 5. $N\Delta \leftarrow 0, N1 \leftarrow 0, N2 \leftarrow 0, SC1 \leftarrow 0, SC2 \leftarrow 0$; | 21. $S2 \leftarrow SC2/\text{SQRT}(N2)$; |
| 6. КЦ $i = 1, n$; | 22. $A1 \leftarrow \Delta - \text{SQR}(S1)$; |
| 7. $k1 \leftarrow (i - 1) \bmod \text{per} 1 + 1$; | 23. $A2 \leftarrow \Delta - \text{SQR}(S2)$; |
| 8. $k2 \leftarrow (i - 1) \bmod \text{per} 2 + 1$; | 24. $C1 \leftarrow S1 + S2 * \text{SQRT}(A1/A2)$; |
| 9. $k3 \leftarrow (i - 1) \bmod \text{per} 3 + 1$; | 25. $C2 \leftarrow S2 + S1 * \text{SQRT}(A2/A1)$; |
| 10. $u[i] \leftarrow H3[k3]$; | 26. $\text{dist} \leftarrow 0$; |
| 11. $u1[i] \leftarrow H1[k1] - u[i]$; | 27. НЦ $j = 1, n$; |
| 12. $u2[i] \leftarrow H2[k2] - u[i]$; | 28. $A \leftarrow u[j] * 0.5$; |
| 13. $\Delta \leftarrow f[i] - H3[i]$; | 29. $h1 \leftarrow C1 * u1[j] + A$; |
| 14. $N\Delta \leftarrow N\Delta + \text{SQR}(\Delta)$; | 30. $h2 \leftarrow C2 * u2[j] + A$; |
| 15. $N1 \leftarrow N1 + \text{SQR}(u1[i])$; | 31. $\text{dist} \leftarrow \text{dist} + \text{SQRT}(f[j] - h1[j] - h2[j])$; |
| 16. $N2 \leftarrow N2 + \text{SQR}(u2[i])$; | 32. КЦ j . |

Здесь НОД — функция, реализующая алгоритм Эвклида вычисления наибольшего общего делителя; $H1, H2, H3$ — компоненты (однокомпонентной задачи) с периодами $\text{per} 1, \text{per} 2, \text{per} 3$ соответственно. Задача решается для веса, равномерного на $\{1, \dots, n\}$, однако возможна простая модификация алгоритма (см., например, алгоритм 2), делающая его пригодным для любой положительной на $\{1, \dots, n\}$ весовой функции.

В соответствии с замечанием 5 можно было бы построить алгоритм, по структуре сходный с алгоритмом 6, для решения k -компонентной задачи.

Все перечисленные алгоритмы могут быть использованы для параллельного решения задачи со списком периодов и последующим выбором периодов, соответствующим наилучшим аппроксимациям (по величине dist).

6. Применение инвариантных аппроксимаций

Многообразие задач, связанных с выделением периодичностей (или более общо — симметрий различного рода), хорошо известно специалистам. Тем не менее перечислим несколько направлений,

в которых описываемый здесь подход, по-видимому, особенно эффективен.

При решении задач классификации сигналов часто оказывается, что характерные компоненты периодичны или почти периодичны, причем период лежит в довольно узких пределах. К тому же нередко специфические черты таких компонент описываются довольно жесткими соотношениями между спектральными составляющими. В этом случае естественно традиционный спектральный анализ заменить выделением компонент, основанным на алгоритмах разд. 5. Особенно эффективным в вычислительном отношении этот подход окажется в случаях, когда характерные составляющие раскладываются в медленно сходящийся ряд Фурье (изломы, акустические щелчки, пилообразные импульсы и т. п.).

Статистическая обработка результатов выделения компонент (в простейшем случае усреднение) позволяет строить базисы решающих правил классификации без промежуточного использования произвольных базисов. Алгоритмы инвариантной аппроксимации могут служить фильтрами в тех случаях, когда полезный сигнал априори обладает некоторыми свойствами симметрии.

При построении многокомпонентных моделей измерительных систем, при оптимизации статистических предикторов по сложности и в других аналогичных задачах принятый здесь подход позволяет строить наилучшие в различных смыслах приближения функциями меньшего числа переменных (см. разд. 4.6). Заслуживает внимания такого рода подход и в применении к минимизации числа признаков при распознавании образов. Наконец, аппроксимация множеств фигурами с заданными свойствами симметрии представляет значительный интерес в статистике случайных множеств и технологии обработки изображений (в частности, растровой оптике).

Литература

1. *Фотоэлектрические преобразователи информации*/Под ред. Л. А. Преснухина. М., 1974.
2. *Гренандер У. Лекции по теории образов*. Т. 1. М., 1979.

ЯВНЫЙ МЕТОД РЕШЕНИЯ ИНТЕГРАЛЬНЫХ УРАВНЕНИЙ С ОПЕРАЦИЕЙ ПЕРЕКЛЮЧЕНИЯ

Исследование нелинейных интегральных уравнений в настоящее время привлекает внимание многих исследователей. Это связано как с разнообразием возникающих математических проблем, так и с широтой области их приложений.

По постановке задач и методам их решения настоящая работа примыкает к исследованиям автора, результаты которых опубликованы в [3—6]. Здесь рассматривается метод построения формул обращения для операторов, описанных в работе [3]. Приведем вначале некоторые ситуации, в которых эти операторы могли бы найти применение.

Представим себе систему автоматического регулирования, состоящую из двух блоков: управляющего и управляемого. Управляемый блок 1 (рис. 1) может находиться в различных состояниях, описываемых параметром z . В зависимости от состояния z управляющий блок 2 формирует управляющий сигнал $g(z)$. Функция g определяет закон управления.

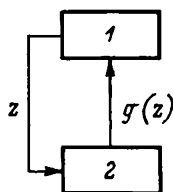
Рассматриваемая система должна удовлетворять двум требованиям: легкости перестройки закона управления g в пределах некоторого класса G и отсутствию сильных ограничений на сложность функций из класса G . Выполнение этих требований, как правило, сопряжено со значительными трудностями, поскольку синтез систем с заданными достаточно сложными характеристиками «вход—выход» — технически нетривиальная задача. С другой стороны, известно, что намного проще формирование временных сигналов, даже значительной сложности.

Рассмотрим структуру управляющего блока (рис. 2), которая позволяет свести задачу получения сложных характеристик к выработке временных сигналов определенной формы. Генератор 3 вырабатывает сигнал $f(t)$, поступающий в преобразователь 4, характеристика которого $J(p, t)$ имеет зону насыщения (рис. 3). Электровакуумные и полупроводниковые приборы с подобными характеристиками широко распространены (см. [1, 2]). Блок 4 преобразует сигналы z и $f(t)$ в сигнал

$$F(t, z) = J(f(t), z) = S(z) \wedge f(t).$$

Рис. 1. Система автоматического регулирования.

1 — управляемый блок; 2 — управляющий.



Независимо от преобразователя блок переключения 1 определяет величины $A(z)$ и $B(z)$, представляющие собой соответственно моменты включения и выключения сигнала $F(t, z)$. Интегратор 2 вырабатывает управляющий сигнал:

$$\int_{A(z)}^{B(z)} F(t, z) dt = g(z),$$

откуда

$$\int_{A(z)}^{B(z)} S(z) \wedge f(t) dt = g(z). \quad (1)$$

Варьируя временной сигнал f , можно задавать различные законы управления, не меняя других параметров системы. Характер связи между g и f зависит от функций A и B . Ниже будет показано, что довольно сложные законы g можно получать с помощью подходящих функций f при довольно простых A и B . В плане приложений нас будут интересовать в основном линейные возрастающие функции A и B , так как они легко технически реализуемы. В математическом отношении их линейность используется не в полной мере. Дальнейшие рассуждения будут основываться на представлении функций A и B в виде $s\omega(z) + z$ ($z > \gamma \in [-\infty, +\infty)$), где s — действительное число, ω — положительная неубывающая непрерывно дифференцируемая функция, $\omega' + 1 > 0$, $\omega(\gamma+) = 0$ при конечном γ . Класс таких функций обозначим Y . Очевидно, что любая линейная неубывающая функция обладает этими свойствами.

Рассмотрим задачу отыскания функции f по заданным функциям g, A, B . Введем функцию $\psi(f_{g, A, B})$, являющуюся мерой сложности реализации сигнала $f_{g, A, B}$. Величина $\sup_{g \in G} \psi(f_{g, A, B})$

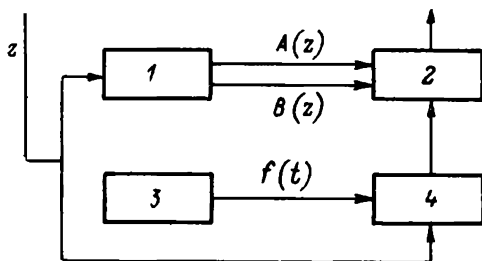


Рис. 2. Схема управляющего блока.

1 — блок переключения; 2 — интегратор;
3 — генератор; 4 — преобразователь.

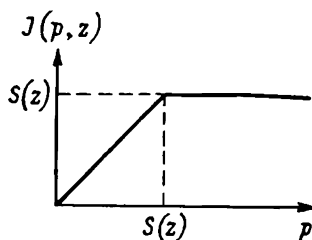


Рис. 3.

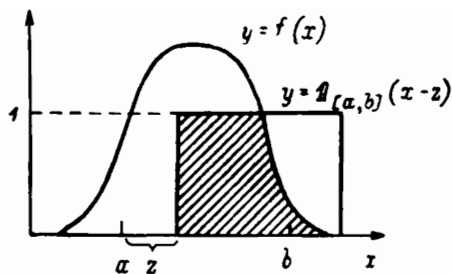


Рис. 4.

характеризует сложность управления для класса G . При проектировании системы в качестве A и B естественно выбирать функции $A_0(z)$ и $B_0(z)$, минимизирующие сложность управления:

$$\begin{aligned} \sup_{g \in G} \psi(f_g, A_0, B_0) &= \\ &= \inf_{A, B \in Y} \sup_{g \in G} \psi(f_g, A, B). \end{aligned}$$

Положим $A(z) = a\omega(z) + z$, $B(z) = b\omega(z) + z$, $S(z) = 1$, тогда уравнение (1) можно представить в виде:

$$\int_R \mathbf{1}_{[a, b]} \left(\frac{t-z}{\omega(z)} \right) \wedge f(t) dt = g(z). \quad (2)$$

Будем искать неотрицательные решения уравнения (2) при $z \in [\gamma, +\infty[$, $\gamma \in \bar{R}$.

Необходимость решать уравнения вида (2) возникает, например, при проектировании систем оптических фильтров, являющихся частью оптических датчиков перемещений. На пути плоского светового потока ставятся две прилегающие друг к другу пластины с отверстиями — прозрачными участками. Величина светового потока, проходящего через пересечение отверстий, определяется площадью их пересечения, которая зависит от формы отверстий и взаимного сдвига фильтров. Пусть в выбранной системе координат нижние края отверстий обоих фильтров лежат на оси OX , а верхние края определяются уравнениями $y = \mathbf{1}_{[a, b]}(x)$ и $y = f(x)$. Тогда площадь пересечения $g(z)$ равна (рис. 4)

$$\int_R \mathbf{1}_{[a, b]}(x-z) \wedge f(x) dx = g(z).$$

При проектировании систем оптических фильтров требуется по заданной форме отверстий первого фильтра найти такую форму отверстий второго фильтра, чтобы площадь пересечения отверстий обоих фильтров заданным образом зависела от их взаимного сдвига.

В работе сформулированы необходимые и достаточные условия существования неотрицательного решения уравнения (2), описана структура класса всех решений и указан способ построения любого решения. Кроме того, выделены некоторые интересные в прикладном отношении частные случаи, для которых сформулированы простые достаточные условия существования решения.

Пусть $\beta > \gamma$, C_β — множество функций из $C[\gamma, +\infty[$ с носителем $[\beta, +\infty[$, C_β^+ — множество неотрицательных функций

из C_β , $\mathbb{1}_A$ — индикатор (характеристическая функция) множества A , $\bar{R}$ — расширенная действительная ось, $E(f)$ — множество значений функции f , $f \circ g$ — композиция функций f и g .

Рассмотрим уравнение:

$$\int_R \mathbb{1}_{[a, b]} \left(\frac{x-z}{\omega(z)} \right) \wedge f(x) dx = g(z), \quad (3)$$

где $z \in]\gamma, +\infty[$, f — неизвестная функция из C_β^+ , $\gamma \in \bar{R}$, $b > a > \gamma$.

Л е м м а 1. Уравнение (3) имеет решение из C_β^+ , тогда и только тогда, когда имеется решение из C_β^+ , не превосходящее единицы.

Д о к а з а т е л ь с т в о. Положим

$$f^*(x) = \begin{cases} f(x), & f(x) \leq 1, \\ 1, & f(x) > 1. \end{cases}$$

Оператор в левой части (1) принимает одинаковые значения на f и f^* , откуда следует утверждение леммы.

Т е о р е м а 1. Пусть ω — непрерывно дифференцируемая функция, $\omega > 0$, $\omega' \geq 0$, $a\omega' + 1 > 0$, $\omega(\gamma+) = 0$ для $\gamma \in R$.

Для того чтобы уравнение (3) имело решение из класса C_β^+ , необходимо и достаточно, чтобы выполнялись условия: а) g непрерывно дифференцируема на $]\gamma, +\infty[$, б) $g \in C_{H^{-1}}(\beta)$, в) $0 \leq g \leq 1$, где

$$\Phi = \sum_{i=0}^{[Q_t^{-1}(\beta)]} W \circ u_i \prod_{j=0}^{i-1} V \circ u_j.$$

Здесь

$$u_0 = I, \quad u_1 = u = (a\omega + I) \circ H^{-1}, \quad \dots, \quad u_n = u_{n-1} \circ u,$$

$$H = b\omega + I, \quad V = \frac{a\omega' \circ H^{-1} + 1}{H' \circ H^{-1}}, \quad W = \frac{g' \circ H^{-1}}{H' \circ H^{-1}},$$

Q_t — убывающая непрерывная интерполяционная функция для функции $q_t(n) = u_n(t)$.

Д о к а з а т е л ь с т в о основывается на ряде лемм.

Л е м м а 2. Если в условиях теоремы уравнение (3) имеет решение из C_β^+ , то функция g непрерывно дифференцируема на $]\gamma, +\infty[$ и f^* удовлетворяет функциональному уравнению,

$$f^*(t) = f^*(u(t)) V(t) + W(t), \quad t \in]\gamma, +\infty[. \quad (4)$$

Д о к а з а т е л ь с т в о. Пусть f — решение из C_β^+ , тогда f^* построенное по f , тоже решение из C_β^+ и $0 \leq f^* \leq 1$. Тогда уравнение (3) можно представить в виде:

$$\int_{a\omega(z)+z}^{b\omega(z)+z} f^*(x) dx = g(z), \quad z \in]\gamma, +\infty[. \quad (5)$$

Так как левая часть непрерывно дифференцируема (в силу непрерывности f^* и непрерывной дифференцируемости ω), то g не-

прерывно дифференцируема. Дифференцирование (5) дает нам равенство:

$$f^*(b\omega(z) + z)(b\omega'(z) + 1) - f^*(a\omega(z) + z)(a\omega'(z) + 1) = g'(z), \quad (6)$$

откуда, полагая $t = H(z)$ и выражая $f^*(t)$, получим равенство (4). По условию теоремы 1 для $\gamma \in R$ $\omega(\gamma+) = 0$, поэтому $H(\gamma+) = \gamma$. Из определения H следует, что $H(+\infty) = +\infty$.

Л е м м а 3. Если в условиях теоремы уравнение (3) имеет решение из C_β^+ , то $g \in C_{H^{-1}(\beta)}$.

Д о к а з а т е л ь с т в о. Из леммы 2 следует, что g непрерывна на $[\gamma, +\infty[$. Кроме того, промежуток интегрирования в левой части уравнения (5) не пересекается с носителем функции f^* , если $H(z) < \beta$. В силу возрастания функций H и H^{-1} последнее неравенство эквивалентно неравенству $z < H^{-1}(\beta)$. Таким образом, $g(z) = 0$ для $z < H^{-1}(\beta)$, откуда $g \in C_{H^{-1}(\beta)}$.

Л е м м а 4. Если в условиях теоремы 1 уравнение (3) имеет решение из C_β^+ с условием $f^* \leq 1$, то оно имеет вид $f^* = \varphi$ и $0 \leq \varphi \leq 1$.

Д о к а з а т е л ь с т в о. Покажем, что область значений функции u содержится в области определения этой функции, т. е. $u(t) > \gamma$. Функция

$$u(t) = a\omega(H^{-1}(t)) + H^{-1}(t) \xrightarrow{t \rightarrow \gamma+} \gamma,$$

так как $H(\gamma+) = \gamma$, $H^{-1}(\gamma+) = \gamma$, $\omega(\gamma+) = 0$. Поскольку функции H и H^{-1} , а следовательно, и функция u возрастают, то $u(t) > \gamma$. Тем самым доказано существование композиций $u_n = u_{n-1} \circ u$ для всех n . Справедливо неравенство $u(t) < t$ для всех t , так как

$$\begin{aligned} u(t) &= u(H(z)) = a\omega(H^{-1}(H(z))) + H^{-1}(H(z)) = \\ &= a\omega(z) + z < b\omega(z) + z = H(z) = t. \end{aligned}$$

Возьмем произвольное $t > \beta$. В силу неравенства $u(t) < t$ последовательность $t_n = u_n(t)$ монотонно убывает. Как было показано, $u(t) > \gamma$, поэтому либо $t_n \xrightarrow{n} \gamma$, либо $t_n \xrightarrow{n} d > \gamma$. Допустим $t_n \xrightarrow{n} d > \gamma$, тогда $u(t_n) = u(u_n(t)) = u_{n+1}(t) = t_{n+1} \xrightarrow{n} d$. Функция u непрерывна (как композиция непрерывных функций), откуда следует $u(d) = \lim_n u(t_n) = d$, что приводит к противоречию с предположением теоремы $u(t) < t$ при $t = d$, т. е. $u_n(t) \xrightarrow{n} \gamma$.

Таким образом, для любого $t > \beta$ существует $k \in N$ такое, что $u_{k+1}(t) < \beta \leq u_k(t)$ и $f^*(u_{k+1}(t)) = 0$. По формуле (4)

$$\begin{aligned} f^*(t) &= f^*(u(t))V(t) + W(t) = (f^*(u_2(t))V(u(t)) + \\ &+ W(u(t)))V(t) + W(t) = \sum_{i=0}^{k(t)} W(u_i(t))V(u_{i-1}(t)) \dots V(u_0(t)). \end{aligned}$$

Введем функцию $q_t(n) = u_n(t)$. Очевидно, эту функцию можно интерполировать непрерывной функцией $Q_t(y)$ так, чтобы $q_t(n) = Q_t(n)$. Неравенство $u_{k+1}(t) < \beta \leq u_k(t)$ представим с помощью введенных обозначений $Q_t(k+1) < \beta < Q_t(k)$. Из непрерывности Q_t следует, что существует такое число $y_0 (k \leq y_0 < k+1)$, что $Q_t(y_0) = \beta$ и $Q_t(k+1) < Q_t(y_0) \leq Q_t(k)$, откуда $k(t) = [y_0] = [Q_t^{-1}(\beta)]$.

Так как $f^* \in C_\beta^+$ и $f^* \leq 1$, то $0 \leq f^* = \varphi \leq 1$.

Перейдем к доказательству достаточности.

Л е м м а 5. Если выполнены условия а), б), в) и предположения теоремы 1, то $\varphi \in C_\beta^+$.

Д о к а з а т е л ь с т в о. Обозначим $B = \{t_k \mid Q_{t_k}^{-1}(\beta) = k\}$. Функция φ непрерывна на $[y, H(+\infty)] \setminus B$. Докажем, что φ непрерывна в точках множества B . Очевидно, что φ непрерывна слева:

$$\varphi(t_k+) - \varphi(t_k) = W(H^{-1}(u_k(t_k))) \prod_{j=0}^k V(u_j(t_k)).$$

Числитель выражения $W(H^{-1}(u_k(t_k)))$ равен

$$\begin{aligned} g'(H^{-1}(u_k(t_k))) &= g'(H^{-1}(Q_{t_k}(k))) = \\ &= g'(H^{-1}(Q_{t_k}(Q_{t_k}^{-1}(\beta)))) = g'(H^{-1}(\beta)) = 0, \end{aligned}$$

откуда функция φ непрерывна в точке t_k .

Наконец, по условию б) для $t < \beta$ функция $\varphi(t) = 0$, поэтому $\text{supp } \varphi \subset [\beta, +\infty]$, что вместе с условием $\varphi \geq 0$ из в) влечет $\varphi \in C_\beta^+$.

Л е м м а 6. Если выполнены условия а), б), в) и предположения теоремы 1, то φ — решение уравнения (3) из C_β^+ .

Д о к а з а т е л ь с т в о. По лемме 5 функция $\varphi \in C_\beta^+$. Кроме того, φ по построению удовлетворяет уравнению (4), а следовательно, и эквивалентному уравнению (6). Исходя из этого и учитывая, что по условию в) $0 \leq \varphi \leq 1$, получим:

$$\begin{aligned} &\frac{d}{dz} \int_R \mathbb{1}_{[a, b]} \left(\frac{x-z}{\omega(z)} \right) \wedge \varphi(x) dx = \\ &= \frac{d}{dz} \int_{a\omega(z)+z}^{b\omega(z)+z} \varphi(x) dx = \varphi(b\omega(z)+z)(b\omega'(z)+1) - \\ &\quad - \varphi(a\omega(z)+z)(a\omega'(z)+1) = g'(z), \end{aligned}$$

откуда

$$\int_R \mathbb{1}_{[a, b]} \left(\frac{x-z}{\omega(z)} \right) \wedge \varphi(x) dx = g(z) + C. \quad (7)$$

Так как $\varphi \in C_\beta^+$, то для $z < H^{-1}(\beta)$ левая часть (7) равна нулю. В силу условия б) при $z < H^{-1}(\beta)$ функция $g(z) = 0$. Откуда $C = 0$ и (7) превращается в (3).

Опишем класс всех решений уравнения (3). Для любой функции h обозначим $A_h(y) = \{t \mid h(t) = y\}$. Для произвольного замкнутого множества $M \subset]\gamma, +\infty[$ примем:

$$S(M) = \{\psi \mid \psi \in C] \gamma, +\infty[\& A_\psi(0) \supset \overline{M}^c\}.$$

Теорема 2. В условиях теоремы 1 класс всех решений уравнения (3) имеет вид:

$$T = \{\varphi + s^2 \mid s \in S(A_\varphi(1))\}.$$

Доказательство. Обозначим через T_0 множество всех решений уравнения (3) из C_β^+ . По теореме 1 множество $T_0 \neq \emptyset$. Докажем, что $T = T_0$.

Возьмем $f \in T_0$. Тогда по лемме 1 можно построить $f^* \in T_0$, а по лемме 4 — функцию $f^* = \varphi$, поэтому функция $s_0 = f - f^*$ обладает следующими свойствами: $s_0 \geq 0$, откуда следует, что s_0 представима в виде $s_0 = s^2$, и $s_0 \in C_\beta$, откуда вытекает, что $s_0 \in C] \gamma, +\infty[$; если $\varphi(t) \neq 1$, то $s_0(t) = 0$, т. е. если $t \notin A_\varphi(1)$, то $t \in A_s(0)$. Таким образом, $A_\varphi^c(1) \subset A_s(0)$. Так как множество $A_s(0)$ замкнуто вследствие непрерывности s , то $A_\varphi^c(1) \subset A_s(0)$. Откуда по определению символа $S(M)$ получим $s \in S(A_\varphi(1))$. Итак, показано, что $f = f^* + s_0 = \varphi + s^2$, т. е. $f \in T$.

Пусть $f \in T$, т. е. $f = \varphi + s^2$, где $s \in S(A_\varphi(1))$. Тогда если $t \in A_\varphi^c(1)$, то $s(t) = 0$, откуда $\underline{f}(t) = \varphi(t)$, $\overline{f}(t) \leq 1$ и $f^*(t) = \underline{f}(t) = \overline{f}(t) = \varphi(t)$. Если же $t \notin A_\varphi^c(1)$, то $t \in A_\varphi(1)$, $\varphi(t) = 1$, $f(t) = 1 + s^2(t) \geq 1$, $f^*(t) = 1 = \varphi(t)$. Таким образом, $f^* = \varphi$. По теореме 1, если выполнены условия а), б), в), то $\varphi \in T_0$, тогда по лемме 1 $f \in T_0$.

З а м е ч а н и е 1. Из леммы 4 вытекает, что решение, подчиненное условию $0 \leq f \leq 1$, единственно.

З а м е ч а н и е 2. Из теоремы 2 следует, что решение единственно в том и только в том случае, когда $A_\varphi^0(1) = \emptyset$.

З а м е ч а н и е 3. Если в предположениях теоремы 1 $g' \geq 0$, то $\varphi \geq 0$.

З а м е ч а н и е 4. Если в предположениях теоремы 1 $\text{supp } g \subset [z_1, z_2]$, то $\text{supp } \varphi \subset [H(z_1), H(z_2)]$.

Доказательство. Из доказательства теоремы 1 следует, что

$$\int_{a\omega(z)+z}^{b\omega(z)+z} \varphi(t) dt = g(z).$$

Так как $\varphi \geq 0$, то для $z \in]-\infty, z_1[\cup]z_2, +\infty[$ $\varphi(t) = 0$ на $[a\omega(z) + z, b\omega(z) + z]$. Следовательно, $\text{supp } \varphi \subset [b\omega(z_1) + z_1, a\omega(z_2) + z_2] \subset [H(z_1), H(z_2)]$.

З а м е ч а н и е 5. Пусть справедливы предположения теоремы 1 и, кроме того, выполнены условия: $\gamma > 0$, $\omega' \leq D$, $\text{supp } g \subset [z_1, z_2]$, $g'(z) \leq C/z^p$, где $p > 1$, $C = (aD(aD +$

+ 1) γ^p)/(($aD + 1$) $^{l+2} - 1$), l — целое число, такое, что: $u_{l+1}(H(z_2)) < \beta$. Тогда $\varphi \leq 1$.

Доказательство. Из возрастания ω следует, что $H' = b\omega' + 1$. Возрастание H^{-1} и условие $H(\gamma+) = \gamma$ приводят к неравенству $H^{-1} > \gamma$. Поэтому

$$\begin{aligned}\varphi(t) &= \sum_{i=0}^{[Q_t^{-1}(\beta)]} W(u_i(t)) \prod_{j=0}^{i-1} V(u_j(t)) = \\ &= \sum_{i=0}^{[Q_t^{-1}(\beta)]} \frac{g'(H^{-1}(u_i(t)))}{H'(H^{-1}(u_j(t)))} \prod_{j=0}^{i-1} \frac{a\omega'(H^{-1}(u_j(t))) + 1}{H'(H^{-1}(u_j(t)))} \leq \\ &\leq \sum_{i=0}^{[Q_t^{-1}(\beta)]} \frac{C(aD + 1)^{i-1}}{(H^{-1}(u_i(t)))^p} \leq \frac{C}{\gamma^p} \sum_{i=0}^{[Q_t^{-1}(\beta)]} (aD + 1)^{i-1}.\end{aligned}$$

Следствие 1. Пусть $b > a > 0$, $\beta > 0$. Для того чтобы уравнение

$$\int_0^{+\infty} \mathbb{1}_{[a, b]} \left(\frac{x}{z} \right) \wedge f(x) dx = g(z), \quad z \in]0, +\infty[\quad (8)$$

имело решение из C_β^+ , необходимо и достаточно, чтобы выполнялись условия: а) g непрерывно дифференцируема на $]0, +\infty[$; б) $g \in C_{\beta/b}$; в) $0 \leq \varphi \leq 1$, где

$$\varphi = \frac{1}{b} \sum_{i=0}^{\left[\frac{\ln(\beta/t)}{\ln \kappa} \right]} \kappa^i g'(\kappa^i t/b), \quad \kappa = a/b.$$

Класс всех решений этого уравнения имеет вид:

$$T = \{\varphi + s^2 \mid s \in S(A_\varphi(1))\}.$$

Доказательство. Так как для любого числа q $\mathbb{1}_{[a, b]}(x) = \mathbb{1}_{[a+q, b+q]}(x + q)$, то левая часть уравнения (8) может быть представлена следующим образом:

$$\int_0^{+\infty} \mathbb{1}_{[a-1, b-1]} \left(\frac{x}{z} - 1 \right) \wedge f(x) dx,$$

и уравнение примет вид:

$$\int_0^{+\infty} \mathbb{1}_{[a-1, b-1]} \left(\frac{x-z}{z} \right) \wedge f(x) dx = g(z).$$

Откуда следует, что уравнение (8) является частным случаем уравнения (3) при $\omega(z) = z$, $\gamma = 0$.

С л е д с т в и е 2. Пусть $b > a$ и $\Delta = b - a$. Для того, чтобы уравнение

$$\int_R 1_{[a, b]}(x - z) \wedge f(x) dx = g(z), \quad z \in R, \quad (9)$$

имело решение из C_{β}^+ , необходимо и достаточно, чтобы выполнялись условия: а) g непрерывно дифференцируема на R ; б) $g \in C_{\beta-b}$; в) $0 \leq \varphi \leq 1$, где

$$\varphi(t) = \sum_{i=0}^{\left[\frac{t-\beta}{\Delta} \right]} g'(t - b - i\Delta).$$

Класс всех решений из C_{β}^+ имеет вид:

$$T = \{\varphi + s^2 \mid s \in S(A_{\varphi}(1))\}.$$

Это утверждение является следствием теорем 1 и 2 при $\omega(z) = z$, $\gamma = -\infty$.

Условия а) и б) теоремы 1 практически легко проверяемы, труднее проверить условие в). В частных случаях, рассмотренных в следствиях 1 и 2, можно указать простые достаточные признаки справедливости в).

З а м е ч а н и е 6. Если $g' \leq b - a$, то в следствии 1 $\varphi \leq 1$.

Д о к а з а т е л ь с т в о. Поскольку $g' \geq 0$, то $\varphi \geq 0$. Так как $g' \leq b - a$, то

$$\varphi(t) \leq \frac{1}{b} \sum_{i=0}^{\infty} \kappa^i g'(\kappa^i t / b) \leq \frac{b-a}{b} \sum_{i=0}^{\infty} \kappa^i = \frac{b-a}{b} \frac{1}{1-\kappa} = 1.$$

З а м е ч а н и е 7. Если $g \in C_{\beta/b}$, $g' \leq \frac{c}{z}$, то в следствии 1 $\varphi \leq 1$. Здесь

$$C = \begin{cases} \beta, & \text{если } \kappa e < 1, \\ -\beta \kappa \ln \kappa, & \text{если } \kappa e > 1. \end{cases}$$

Д о к а з а т е л ь с т в о. Так как $g' \geq 0$, то $\varphi \geq 0$. С другой стороны,

$$\varphi(t) \leq \frac{1}{b} \sum_{i=0}^{u(t)} \kappa^i \frac{C b}{\kappa^i t} = \frac{C}{t} (u(t) + 1) \leq \frac{C}{t} \left(\frac{\ln(\beta/t)}{\ln \kappa} + 1 \right).$$

Обозначим $h(t) = \frac{C}{t} \left(\frac{\ln(\beta/t)}{\ln \kappa} + 1 \right)$. Очевидно, что функция $h(t)$ в точке $t_0 = \beta \kappa e$ достигнет максимального значения, поэтому если $\kappa e \leq 1$, то $t_0 < \beta$ и точка t_0 не попадает в промежуток $[\beta, +\infty[$, на котором функция φ отлична от нуля. Поэтому справедлива оценка $\varphi(t) \leq h(t) \leq h(\beta) = 1$. Если же $\kappa^2 e > 1$, то $t_0 > \beta$ и $\varphi(t) \leq h(t) \leq h(t_0) = 1$.

З а м е ч а н и е 8. Если $g \in C_{\beta/b}$, $g'(z) \leq \frac{C}{z^p}$, где $p > 1$, то в следствии 1 $\varphi \leq 1$. Здесь $C = \beta^p / b^{p-1}$.

Доказательство.

$$\begin{aligned}\varphi(t) &\leq \frac{1}{b} \sum_{i=0}^{u(t)} \kappa^i \frac{C}{\left(\frac{\kappa^i t}{b}\right)^p} = \frac{Cb^{p-1}(\kappa^{u(t)}(1-p) - 1)}{(\kappa^{1-p} - 1)t^p} \leq \\ &\leq \frac{Cb^{p-1} \left(\kappa \left(\frac{\ln(\beta/t)}{\ln \kappa} - 1 \right) (1-p) - 1 \right)}{(\kappa^{1-p} - 1)t^p}.\end{aligned}$$

Обозначим последнее выражение $h(t)$. Так как $h' < 0$, то функция h убывает и $\varphi(t) \leq h(t) \leq h(\beta) \leq 1$.

З а м е ч а н и е 9. Пусть $\beta > b + \Delta$. Если $g \in C_{\beta-b}$, $g'(z) \leq \frac{C}{z^p}$, где $p > 1$, то в следствии 2 $\varphi \leq 1$. Здесь $C = \Delta(p-1) \times (\beta - b - \Delta)^{p-1}$.

Доказательство. Так как $g' \geq 0$, то $\varphi \geq 0$. Кроме того,

$$\begin{aligned}\varphi(t) &\leq \sum_{i=0}^{\left[\frac{t-\beta}{\Delta}\right]} \frac{C}{(t-b-i\Delta)^p} \leq C \int_0^{\left[\frac{t-\beta}{\Delta}\right] + 1} \frac{dy}{(t-b-y\Delta)^p} = \\ &= -C \int_{t-b}^{t-b-\Delta\left[\frac{t-\beta}{\Delta}\right]} \frac{du}{\Delta u^p} \leq \frac{C}{\Delta(p-1)} \frac{1}{(\beta-b-\Delta)^{p-1}} \leq 1.\end{aligned}$$

В качестве примера рассмотрим систему автоматического регулирования с законом управления

$$g(z) = \begin{cases} \left(1 - \frac{2}{z}\right)^2, & z \in [2; 3], \\ 0, & z \in [0; 2] \end{cases}$$

и диапазоном состояний $[0; 3]$. Пусть $G = \{g\}$. Для удобства анализа, разумеется, можно продолжить g на R с помощью того же аналитического выражения.

Если система описывается уравнением

$$\int_R \mathbf{1}_{[1; 2]}(x-z) \wedge \varphi(x) dx = g(z), \quad z \in R, \quad (10)$$

то, учитывая реальный диапазон состояний $[0; 3]$, достаточно найти решение на промежутке $[1; 5]$. По следствию 2 решение системы имеет вид:

$$\varphi(t) = \sum_{i=0}^{\left[\frac{t-4}{4}\right]} g'(t-2-i) = \begin{cases} 0, & t < 4, \\ 4 \frac{t-4}{(t-2)^3}, & 4 \leq t < 5. \end{cases}$$

Если же система описывается уравнением

$$\int_0^{+\infty} \mathbf{1}_{[1; 2]} \left(\frac{x}{z} \right) \wedge \varphi(x) dx = g(z), \quad z \in]0; +\infty[, \quad (11)$$

то достаточно найти решение на промежутке $[0; 6]$.

По следствию 1 получим решение системы:

$$\varphi(t) = \sum_{i=0}^{\left[\frac{\ln t}{\ln 2}\right]-2} \frac{1}{2^i} g' \left(\frac{t}{2^{i+1}} \right) = \begin{cases} 0, & t < 4, \\ 16 \frac{t-4}{t^3}, & 0 \leq t < 6. \end{cases}$$

Введение той или иной меры сложности, позволяющей предпочесть одно решение другому, зависит от способа реализации сигнала. Например, если синтез сигнала основан на сложении синусоидальных гармоник, то мерой сложности может служить наименьшее количество гармоник, достаточное для воспроизведения закона управления с заданной точностью ε . Поскольку

$$\left| \int_{\gamma}^{+\infty} \mathbb{1}_{[a, b]} \left(\frac{x-z}{\omega(z)} \right) \wedge \varphi(x) dx - \int_{\gamma}^{+\infty} \mathbb{1}_{[a, b]} \left(\frac{x-z}{\omega(z)} \right) \wedge h(x) dx \right| \leq \\ \leq (b-a) \sup_z \omega(z) \|\varphi - h\|_2,$$

где $\|\cdot\|_2$ — норма в пространстве $L_2([a\omega(c) + c; b\omega(d) + d])$, $[c, d]$ — диапазон состояний, то указанная точность может быть достигнута при выполнении условия:

$$\|\varphi - \varphi_n\|_{L_2} \leq \frac{\varepsilon}{(b-a) \sup_z \omega(z)} = \delta,$$

где φ — решение уравнения, φ_n — аппроксимирующая функция, равная отрезку ряда Фурье, состоящему из n первых гармоник на $\text{supp } \varphi$, и нулю вне $\text{supp } \varphi$. Введем меру сложности следующего вида:

$$\psi(\varphi) = \inf \{n + 1 \mid \|\varphi - \varphi_n\|_{2,0} \leq \delta\},$$

где $\|\cdot\|_{2,0}$ — норма в пространстве $L_2([a\omega(c) + c, b\omega(d) + d] \cap \text{supp } \varphi)$. Полагая $\varepsilon = 3 \cdot 10^{-2}$ для системы, описываемой уравнением (10), $\delta = 3 \cdot 10^{-2}$. Мера сложности реализации сигнала в этом случае равна 2. Для системы, определяемой уравнением (11), $\delta = 1.5 \cdot 10^{-2}$ и мера сложности равна 20. Таким образом, при проектировании следует предпочитать первую систему.

Литература

1. Бройде А. М., Тарасов Ф. И. Справочник по электровакуумным и полупроводниковым приборам. Ростов, 1962.
2. Лавриненко В. Ю. Справочник по полупроводниковым приборам. Киев, 1963.
3. Ляшенко Т. В. Об одном специальном классе нелинейных интегральных уравнений. I//Вестн. ЛГУ. 1979. № 1. С. 33—42.
4. Ляшенко Т. В. Об одном специальном классе нелинейных интегральных уравнений. II//Вестн. ЛГУ. 1979. № 13. С. 20—26.
5. Ляшенко Т. В. Об одном специальном классе нелинейных интегральных уравнений. III//Вестн. ЛГУ. 1980. № 1. С. 31—35.
6. Ляшенко Т. В. О некоторых приложениях нелинейных интегральных уравнений с операцией переключения//Вестн. ЛГУ. 1981. № 1. С. 40—44.

АЛГОРИТМ АНАЛИЗА СТРУКТУРЫ ГРУППОВЫХ ИСТОЧНИКОВ СИГНАЛОВ

1. Введение

В статье проводится анализ подходов к решению следующей задачи. Пусть в точке $(0, R)$ на плоскости расположен скалярный акустический приемник, получающий сигнал от группового источника, состоящего из n движущихся компонент, причем закон перемещения k -й компоненты имеет вид:

$$x_k(t) = v(t - \tau_k), \quad y_k(t) = 0.$$

Излучение k -й компоненты в точке приема делает вклад $p_k A (\text{dist}_k(t)) Q_k(t)$, где p_k — интенсивность компоненты, Q_k — нормированный шум, излучаемый компонентой, $\text{dist}_k(t)$ — расстояние между точками $(x_k(t), y_k(t))$ и $(0, R)$, $A(z) = z^{-1/2}$.

В результате воздействия группового источника приемник воспринимает сигнал:

$$s(t) = \sum_{k=1}^n p_k A (\text{dist}_k(t)) Q_k(t). \quad (1)$$

Основной вопрос заключается в оценивании неизвестного числа компонент n по отрезку наблюдаемого сигнала s для $t \in [0, T]$ при естественных предположениях о шумах Q_k .

Описываем основные способы формализации задачи, перечень аналитических трудностей, возникающих при ее решении, и возможные пути их преодоления. При построении алгоритма авторами избран эмпирический подход, основанный на результатах машинных экспериментов с модельными и реальными сигналами от акустических источников. В частности, таким образом выбраны некоторые процедуры фильтрации, являющиеся составной частью нашего метода. Эти процедуры, по-видимому, не оптимальны, и соответствующие задачи оптимизации еще ждут своего решения, однако для многих прикладных ситуаций являются допустимыми (в точном понимании этого термина).

Наконец, отметим, что, несмотря на эмпирическое происхождение некоторых звеньев алгоритма, их выбор все же основан на

ряде аналитических соображений и гипотез, приводимых нами в дальнейших разделах.

2. Варианты представления задачи

Выражение (1) удобно преобразовать, представив его в виде:

$$s(t) = 1_{[0, T]}(t) \sum_{k=1}^n \rho_k B(\gamma(t - \tau_k)) Q_k(t), \quad (2)$$

где 1_M — индикатор множества M , $\rho_k = \rho_k R^{-1}$, $[B(z) = (1 + z^2)^{-\frac{1}{2}}$, $\gamma = (v/R)^2$.

Наряду с сигналом s , рассмотрим его «идеальные» огибающие:

$$u_1(t) = 1_{[0, T]}(t) \sum_{k=1}^n \rho_k D(\gamma(t - \tau_k)) \quad (3)$$

или

$$u_2(t) = 1_{[0, T]}(t) \sum_{k=1}^n \rho_k^2 D^2(\gamma(t - \tau_k)), \quad (4)$$

где D — некоторое известное преобразование B . Они могут быть получены с помощью фильтров, устраняющих мультипликативные составляющие Q_k и в то же время сохраняющих аддитивную структуру сигнала s (мультипликативно-аддитивные фильтры). Если соответствующая фильтрация проведена, то задача сводится к отысканию n из соотношения (3) или (4).

Пусть

$$f(x) = \sum_{k=1}^n \rho_k \delta(x - \tau_k), \quad (5)$$

тогда

$$u(t) = \int_{\mathbb{R}} B(\gamma(t - x)) f(x) 1_{[0, T]}(t) dx, \quad (6)$$

откуда видно, что наша задача требует решения уравнения Фредгольма 1-го рода с ядром $B(\gamma(t - x)) 1_{[0, T]}(t)$, известным лишь с точностью до параметра γ с неизвестной функцией f вида (5). Если в нашем распоряжении имеется дополнительный метод уточнения γ , то основная проблема состоит в регуляризации уравнения. Если же, как это чаще бывает, известен лишь диапазон значений γ : $\gamma \in [\gamma_1, \gamma_2]$, то задача может быть сведена к решению уравнения:

$$u(t) = \int_{\mathbb{R}} \int_{\gamma_1}^{\gamma_2} B(\gamma(t - x)) 1_{[0, T]}(t) g(\gamma, x) d\gamma dx \quad (7)$$

с неизвестной функцией g вида:

$$g(\gamma, x) = \delta(\gamma - \gamma_0) \sum_{k=1}^n \rho_k \delta(x - \tau_k).$$

3. Мультипликативно-аддитивная фильтрация

Отображение, сопоставляющее сигналу (2) аппроксимацию сигнала (3), назовем мультипликативно-аддитивным фильтром. Рассмотрим несколько реализаций таких фильтров. Заметим прежде всего, что

$$s^2(t) = \mathbb{1}_{[0, T]}(t) \sum_{k, l=1}^n \rho_k \rho_l L_{k, l}(t) Q_k(t) Q_l(t),$$

где $L_{kl}(t) = B(\gamma(t - \tau_k)) B(\gamma(t - \tau_l))$.

Л е м м а 1. Пусть F — линейный ограниченный оператор из $C[0, T]$ в $C[0, T]$ со свойствами: 1) $\|F\| \leq 1$; 2) для $j \in \{1, \dots, m\}$, набора $\varphi_j \in C[0, T]$, $k \neq l$, $\|F(\varphi_j Q_k Q_l)\| \leq \varepsilon$; 3) существует такая константа c , что $\|F(\varphi_j (Q_k^2 - c))\| \leq \varepsilon$. Если $\|Q_k\| \leq q_m$ и L_{kl} аппроксимируются полиномами $P_{kl} = \sum_{j=1}^m a_{jkl} \varphi_j$ с оценками $\|L_{kl} - P_{kl}\| \leq \theta$, $|a_{jkl}| \leq A_j$, то

$$Fs^2 = c^2 \sum_{k, l=1}^n \rho_k^2 F(B^2(\gamma(t - \tau_k)) - H, \quad (8)$$

где

$$\|H\| \leq n^2 \left(\varepsilon \sum_{j=1}^m A_j + \theta q^2 \right) + \theta nc. \quad (9)$$

Д о к а з а т е л ь с т в о.

$$Fs^2 = \sum_{k, l=1}^n \rho_k \rho_l F(L_{kl} Q_k Q_l).$$

Для $k \neq l$

$$\begin{aligned} |F(L_{kl} Q_k Q_l)| &\leq |F(L_{kl} - P_{kl}) Q_k Q_l| + |F(P_{kl} Q_k Q_l)| \leq \\ &\leq q^2 \theta + \sum_{j=1}^m |a_{jkl}| |F(\varphi_j Q_k Q_l)| \leq q^2 \theta + \varepsilon \sum_{j=1}^m A_j. \end{aligned} \quad (10)$$

Если $k = l$, то

$$F(L_{kl} Q_k Q_l) = FB^2(\gamma(\square - \tau_k) Q_k^2) = cFB^2(\gamma(\square - \tau_k)) + J,$$

где $J = FB^2(\gamma(\square - \tau_k))(Q_k^2 - c)$. При этом [символ $\square$ означает место для постановки независимой переменной].

Далее

$$\begin{aligned} \|J\| &\leq \|F(B^2(\gamma(\square - \tau_k) - P_{kk})(Q_k^2 - c))\| + \|F(P_{kk}(Q_k^2 - c))\| \leq \\ &\leq \theta(q^2 + c) + \varepsilon \sum_{j=1}^m A_j. \end{aligned}$$

Собирая вместе полученные оценки, приходим к (8) и (9)

Л е м м а 2. Пусть $\tau \geq 0$, тогда

$$b(\tau) = \sup_{t \in \mathbb{R}} B(t - \tau) B(t + \tau) = \begin{cases} \frac{1}{\tau^2 + 1}, & \tau \leq 1, \\ \frac{1}{2\tau}, & \tau > 1. \end{cases} \quad (11)$$

Д о к а з а т е л ь с т в о. Дифференцирование функции $c(t) = B(t - \tau) B(t + \tau)$ показывает, что для $\tau \leq 1$ она имеет единственный максимум при $t = 0$, а для $\tau > 1$ — два максимума при $t = \pm \sqrt{\tau^2 - 1}$. В первом случае

$$b(\tau) = B(-\tau) B(\tau) = B^2(\tau) = (1 + \tau^2)^{-1}.$$

Во втором случае

$$\begin{aligned} b(\tau) &= B(\sqrt{\tau^2 - 1} - \tau) B(\sqrt{\tau^2 - 1} + \tau) = \\ &= (4\tau^2(\tau - \sqrt{\tau^2 - 1})(\tau + \sqrt{\tau^2 - 1}))^{-\frac{1}{2}} = (4\tau^2)^{-\frac{1}{2}} = \frac{1}{2\tau}. \end{aligned}$$

Л е м м а 3.

$$\left| \frac{d}{dx} L_{kl}(x) \right| \leq L_{kl}(x).$$

Д о к а з а т е л ь с т в о. Дифференцирование дает:

$$\frac{d}{dx} L_{kl}(x) = -L_{kl}(x) ((t - \tau) B^2(t - \tau) + (t + \tau) B^2(t + \tau)).$$

Остается заметить, что

$$\sup_x |xB^2(x)| = \frac{1}{2}.$$

Л е м м а 4. Если оператор F обладает свойством

$$|F(\varphi Q_k Q_l)| \leq \varepsilon (c_1 \sup |\varphi| + c_2 \sup |\varphi^1|)$$

для $k \neq l$ и если для любого k $\tau_{k+1} - \tau_k > 2/\gamma$, то оценка H в лемме 1 может быть заменена оценкой порядка $n \ln n$.

Д о к а з а т е л ь с т в о. Так же, как и в лемме 1,

$$FS^2 = \sum_{k, l=1}^k \rho_k \rho_l F(L_{kl} Q_k Q_l).$$

Для $k \neq l$

$$\begin{aligned} |F(L_{kl} Q_k Q_l)| &\leq c_1 \varepsilon \sup(L_{kl}) + c_2 \varepsilon \sup\left(\frac{d}{dx} L_{kl}\right) \leq \\ &\leq \varepsilon (c_1 + \gamma c_2) \sup(L_{kl}) \leq \varepsilon (c_1 + c_2 \gamma) |\tau_k - \tau_l|. \end{aligned}$$

Поскольку $\tau_k - \tau_l \geq 2|k - l|/\gamma$, то

$$|F(L_{kl} Q_k Q_l)| \leq \frac{\gamma(c_1 + \gamma c_2)\varepsilon}{2|k - l|},$$

поэтому

$$\begin{aligned} \left| \sum_{k, l=1}^n \rho_k \rho_l F(L_{kl} Q_k Q_l) \right| &= 2 \left| \sum_{\substack{k, l=1 \\ k < l}}^n \rho_k \rho_l F(L_{kl} Q_k Q_l) \right| \leq \\ &\leq 2 \sum_{\substack{k, l=1 \\ k < l}}^n \rho^2 \frac{\gamma(c_1 + \gamma c_2)\varepsilon}{2(l - k)} = \rho^2 \gamma (c_1 + \gamma c_2) \varepsilon \sum_{k < l} \frac{1}{l - k}, \quad \rho_i \leq \rho. \end{aligned}$$

Остается заметить, что последняя сумма равна:

$$\sum_{k=1}^{n-1} \frac{n-k}{k} = n \sum_{k=1}^{n-1} \frac{1}{k} - n + 1 \sim n \ln n.$$

С помощью несложных вычислений можно было бы получить оценки для огибающих типа (3), используя подходящие процедуры сглаживания. В частности, роль таких процедур с успехом выполняют супремальные оконные фильтры (или более общо — квантильные), а также фильтры $F_{\max}$, основанные на сплайн-аппроксимациях по экстремумам (с отбраковкой выбросов или без нее).

4. Аналитические предпосылки алгоритма

Рассмотрим идеализированный вариант задачи (5), получаемый заменой $[0, T]$ на $\mathbb{R}$:

$$u(t) = \int_{\mathbb{R}} B(\gamma(t-x)) f(x) dx.$$

Очевидно, здесь применим метод, основанный на преобразовании Фурье:

$$u^*(p) = \frac{1}{\gamma} B^*\left(\frac{p}{\gamma}\right) f^*(p),$$

где $*$ означает фурье-образ. Согласно (4), функция f^* представляет собой тригонометрический полином:

$$f^*(p) = \sum_{k=1}^n \rho_k e^{-ip\tau_k}.$$

В принятой нами модели B является четной, поэтому B^* вещественна. Если B^* медленно меняется, то она может быть выделена из u^* выбором подходящей процедуры демодуляции. Деление на выделенную функцию и применение обратного преобразования Фурье дает сигнал, по структуре особенностей (экстремумов) которого, очевидно, легко определяется число n .

Таким образом, два связанных между собой допущения — суммируемость временной огибающей на всей вещественной оси и медленное изменение B^* — позволяют использовать сравнительно простой алгоритм выделения компонент. К сожалению, оба эти допущения в действительности не имеют места. Во-пер-

вых, $B(\gamma t) = (1 + \gamma^2 t^2)^{-\frac{1}{2}}$ не принадлежит $L_1(\mathbb{R}, dx)$. Преобразование Фурье $B(\gamma t)$, формально подсчитанное, равно:

$$\int_{-\infty}^{\infty} \frac{e^{-ipt}}{\sqrt{1 + \gamma^2 t^2}} dt = 2 \int_0^{\infty} \frac{\cos pt}{\sqrt{1 + \gamma^2 t^2}} dt = \frac{2}{\gamma} K_0\left(\frac{p}{\gamma}\right),$$

где $K_m(x)$ — бesselевы функции от мнимого аргумента второго рода, $K_0(x) \sim \ln \frac{x}{2}$ при $x \rightarrow 0$. Отсюда видно, что второе допущение о «медленном» изменении огибающей фурье-образа от $B(\gamma t)$ так же не выполняется.

Напишем выражение для фурье-образа сигнала:

$$s(t) = \mathbb{1}_{[0, T]}(t) \sum_{k=1}^n \rho_k \frac{1}{\sqrt{1 + \gamma^2 (t - \tau_k)^2}},$$

предположив, что интервал наблюдения $[0, T]$ достаточно велик и «информативная» часть сигнала $s(t)$ сконцентрирована около точки $t = T/2$. Точнее говоря, предположим, что величины $\varepsilon_k = (T/2 - \tau_k)/T$ достаточно малы. Обозначая $\tau_k - \frac{T}{2}$ через τ'_k , имеем:

$$\begin{aligned} s^*(p) &= \int_0^T s(t) e^{-ipt} dt = \sum_{k=1}^n \rho_k e^{-i \frac{T}{2} p} \int_{-\frac{T}{2}}^{\frac{T}{2}} \frac{e^{-ipt}}{\sqrt{1 + \gamma^2 (t - \tau'_k)^2}} dt = \\ &= \sum_{k=1}^n \rho_k e^{-i \tau'_k p} \left[\left(2 \int_0^{\infty} \frac{\cos pt}{\sqrt{1 + \gamma^2 t^2}} dt - 2 \int_{\frac{T}{2}}^{\infty} \frac{\cos pt}{\sqrt{1 + \gamma^2 t^2}} dt \right) + \right. \\ &\quad \left. + \left(\int_{\frac{T}{2}}^{\frac{T}{2}} \frac{e^{ipt}}{\sqrt{1 + \gamma^2 t^2}} dt - \int_{\frac{T}{2}}^{\frac{T}{2} + \tau'_k} \frac{e^{-ipt}}{\sqrt{1 + \gamma^2 t^2}} dt \right) \right] = \\ &= \sum_{k=1}^n \rho_k e^{-i p \tau'_k} \{ A(p) + A_k(p) \}. \end{aligned} \quad (12)$$

Из (12) видно, что в отличие от «идеальной» схемы, функции $A(p) + A_k(p)$, стоящие в сумме (12) при $e^{-i p \tau'_k}$, различны для разных k , хотя и содержат общее слагаемое:

$$\begin{aligned} A(p) &= 2 \int_0^{\infty} \frac{\cos pt}{\sqrt{1 + \gamma^2 t^2}} dt - 2 \int_{T/2}^{\infty} \frac{\cos pt}{\sqrt{1 + \gamma^2 t^2}} dt = \\ &= \frac{2}{\gamma} K_0\left(\frac{p}{\gamma}\right) - 2 \int_{T/2}^{\infty} \frac{\cos pt}{\sqrt{1 + \gamma^2 t^2}} dt. \end{aligned}$$

Теоретическое исследование влияние «довесков»

$$A_k(p) = \int_{\frac{T}{2} - \tau'_k}^{\frac{T}{2}} \frac{e^{ipt}}{\sqrt{1 + \gamma^2 t^2}} dt - \int_{T/2}^{\frac{T}{2} + \tau'_k} \frac{e^{-ipt}}{\sqrt{1 + \gamma^2 t^2}} dt$$

на отклонение от «идеальной» схемы является довольно сложной задачей и в полной мере нами не проводилось. Здесь еще раз уместно напомнить, что результаты нашей работы носят эмпирический характер, и, как нам кажется, в процессе эксперимента нам удалось сконструировать преобразование, позволяющее в достаточной мере исключить влияние «довесков» $A_k(p)$. Конечно, сразу бросается в глаза, что

$$|A_k(p)| \leq \frac{1}{\gamma} \ln \frac{\frac{T}{2} + \tau'_k}{\frac{T}{2} - \tau'_k},$$

т. е. за счет увеличения интервала наблюдения $A_k(p)$ можно сделать сколь угодно малыми равномерно по k . Но дело в том, что, следуя «идеальной» схеме, нам надо разделить фурье-образ исходного сигнала на его огибающую, являющуюся в «идеальной» схеме фурье-образом «эталонного сигнала» $B(\gamma t) = (1 + \gamma^2 t^2)^{-1/2}$. Оказывается, что после выполнения указанного деления, влияние «довесков» $A_k(p)$, по крайней мере при удалении от точки $p = 0$, является довольно значительным. Более подробно о влиянии $A_k(p)$ и нашей попытке его исключить будет сказано при описании эмпирического алгоритма.

5. Описание алгоритма

Перейдем к описанию самого алгоритма. Пусть, как и выше (см. (12)), $s^*(p)$ — фурье-образ нашего сигнала — огибающей, полученной после фильтрации (рис. 1).

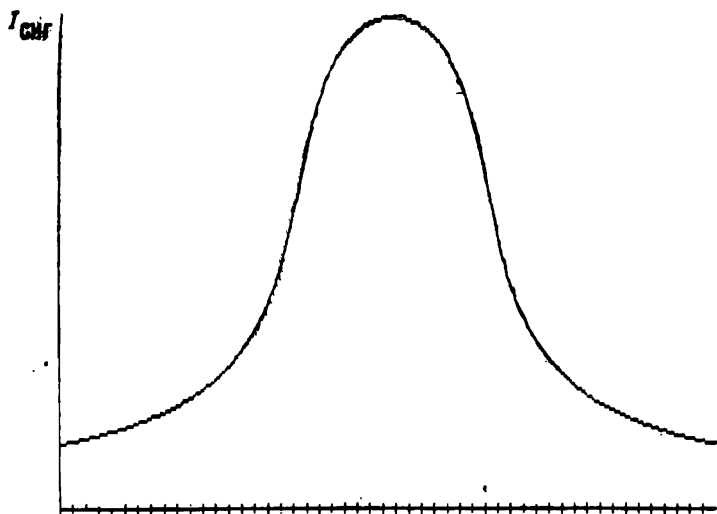


Рис. 1. Огибающая исходного сигнала от 10-компонентного источника.

Шаг 1 — выделение «оггибающей» $|s^*(p)|$. «Оггибающая» $\sigma(p)$ строится путем применения к $|s^*(p)|$ фильтрации, основанной на интерполяции по локальным экстремумам (в данном случае максимумам). Обозначив, как в разд. 3, указанное преобразование через $F_{\max}$, имеем:

$$\sigma(p) = F_{\max} |s^*(p)|, \quad l(p) = \frac{s^*(p)}{\sigma(p)}.$$

Шаг 2 — построение преобразования, «отфильтровывающего» отклонения от «идеальной» схемы, в частности влияние «довесков» $A_k(p)$. При сравнении графиков функций $\operatorname{Re}(l(p))$ и $\operatorname{Re} \sum_{k=1}^n \rho_k e^{-i\tau_k p}$ для конкретных сигналов сразу бросаются в глаза существенные отличия, которые следует отнести за счет влияния «довесков» $A_k(p)$: функция $f(p) = \operatorname{Re} \sum_{k=1}^n \rho_k e^{-i\tau_k p}$ является высокочастотной модуляцией, центрированной относительно вещественной оси, в том смысле, что $F_{\max}(f(p)) = F_{\max}(-f(p))$, т. е. верхняя и нижняя оггибающие у $f(p)$ симметричны относительно вещественной оси. У $\operatorname{Re}(l(p))$ высокочастотная модуляция имеет место лишь на некотором промежутке $[-M, M]$, причем $\operatorname{Re}(l(p))$ не является центрированной.

После сравнения достаточно большого количества вышеупомянутых графиков авторы пришли к следующей эмпирической гипотезе относительно характера отклонения нашей схемы от «идеальной». Предполагается, что влияние «довесков» $A_k(p)$ имеет следующий вид:

$$\frac{s^*(p)}{\sigma(p)} = l(p) = \left(\sum_{k=1}^n \rho_k e^{-i\tau_k p} \right) \mathbb{1}_{[-M, M]}(p) \varphi(p) + \psi(p), \quad (13)$$

где $\varphi(p)$ — положительная функция, медленно меняющаяся на интервале $[M, M]$, а $\psi(p)$ — низкочастотная по сравнению с $\sum_{k=1}^n \rho_k e^{-i\tau_k p}$ модуляция. Исходя из (13), на следующем шаге алгоритма определим функцию $\psi(p)$.

Полагаем:

$$\operatorname{Re} \psi(p) = \frac{1}{2} (F_{\max}(\operatorname{Re}(l(p))) - F_{\max}(-\operatorname{Re}(l(p)))),$$

$$\operatorname{Im} \psi(p) = \frac{1}{2} (F_{\max}(\operatorname{Im}(l(p))) - F_{\max}(-\operatorname{Im}(l(p)))).$$

Теперь функция $\tilde{l}(p) = l(p) - \psi(p)$ является центрированной (центрированы ее Re и Im). Выделение множителя $\varphi(p)$ можно провести, используя, например, интегральные фильтры, так как

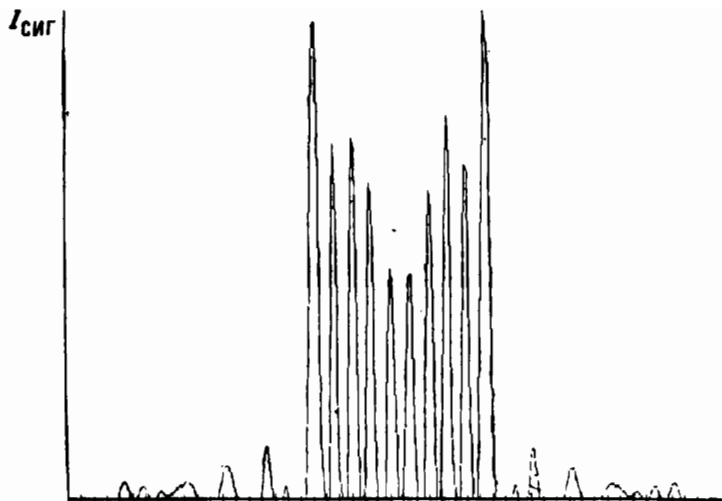


Рис. 2. Результат выполнения третьего шага алгоритма.

$\sum_{k=1}^n \rho_k e^{-i\tau_k p}$ — высокочастотная модуляция, а $\varphi(p)$ медленно меняется на $[-M, M]$. Поскольку можно считать, что

$$\frac{1}{2h} \int_{-h}^h e^{i p \tau_k} e^{-i p \tau_l} dp = \delta_{kl},$$

где δ_{kl} — символ Кронекера, а h — окно фильтрации, которое можно выбрать не слишком большим из-за высокочастотности

$\sum_{k=1}^n \rho_k e^{-i\tau_k p}$, имеем:

$$\begin{aligned} F_{sq}(I)(p_0) &= \frac{1}{2h} \int_{p_0-h}^{p_0+h} |I(p)|^2 dp \approx \\ &\approx \frac{1}{2h} |\varphi(p_0)|^2 \int_{p_0-h}^{p_0+h} \left(\sum_{k=1}^n \rho_k e^{-i\tau_k p} \right) \left(\sum_{k=1}^n \rho_k e^{i\tau_k p} \right) dp = |\varphi(p_0)|^2 \sum_{k=1}^n \rho_k^2. \end{aligned}$$

Таким образом, разделив $I(p)$ на $F_{sq}(I)(p)$, согласно (13), получим:

$$u(p) = \frac{I(p)}{F_{sq}(I)(p)} = c \sum_{k=1}^n \rho_k e^{-i\tau_k p} \mathbb{1}_{[-M, M]}(p),$$

где $c = \left(\sum_{k=1}^n \rho_k^2 \right)^{-1/2}$.

Шаг 3 — обратное преобразование Фурье. Вычисляем аналог функции f из (5) (рис. 2):

$$u^*(p) = \left(c \sum_{k=1}^n \rho_k e^{-i\tau_k p} \right) \mathbb{I}_{[-M, M]}(p)^* = c \left(\sum_{k=1}^n \rho_k \delta(t - \tau_k) \right) * \frac{1}{t} \sin Mt = \\ = c \sum_{k=1}^n \rho_k \frac{\sin M(t - \tau_k)}{t - \tau_k}. \quad (14)$$

Шаг 4 — оценка числа компонент. Результатом работы алгоритма считается количество выходов функции (14) за некоторый эмпирически выбранный уровень, что соответствует выделению главного максимума каждого из слагаемых в (14).

Описанный алгоритм реализован авторами в виде диалоговой системы на языке Turbo—Pascal IBM PC XT. Для выбора подходящих параметров фильтров и величины порога существенно использовались средства машинной графики.

Литература

1. Тихонов А. Н., Арсенин В. Я. Методы решения некорректных задач. М., 1979.

ОБ ОДНОМ ОБОБЩЕНИИ ИНТЕРВАЛЬНОГО АНАЛИЗА И ЕГО ПРИМЕНЕНИИ ДЛЯ ОЦЕНКИ МНОЖЕСТВА ЗНАЧЕНИЙ ФУНКЦИИ

К задаче отыскания хорошей верхней и нижней оценки значений функции при заданной области изменения аргументов возможен целый ряд подходов. Один из них предоставляет интервальный анализ [1—12]. Возникнув из сугубо практических потребностей, связанных с организацией машинных вычислений с гарантированной точностью, интервальный анализ является развитой теорией, применяемой не только для построения вычислительных алгоритмов, но и для получения чисто теоретических результатов.

Существенным преимуществом применения интервального анализа к задаче оценивания функции является простота реализации полученных алгоритмов на ЭВМ. Известен целый ряд пакетов программ для интервальных вычислений. Среди них можно отметить Interval [13], пакет АЛГОЛ-программ для ЭВМ Wirtoughs B5500 [14], систему Triplex [15], а также отечественную разработку для ЭВМ БЭСМ-6 [16]. Достаточно полный обзор вопросов реализации интервальных вычислений можно найти в статье А. Г. Яковлева, помещенной в монографии [2] в качестве добавления.

Одной из первых работ, в которой рассматривается указанная задача, является монография [1], послужившая основой для большинства дальнейших исследований в данной области. На русском языке систематическое изложение основ интервального анализа содержится в книге [12], а также в монографии [2], перевод которой вышел в свет в период подготовки настоящей статьи.

Алгоритмы оценки функции, основанные на указанных работах, как будет показано, наряду с достоинствами, обладают некоторыми серьезными недостатками, что ограничивает область их применения. Ниже будет предложено обобщение интервального анализа, позволяющее получить алгоритм с существенно более широкой областью использования.

Помимо задачи, которой посвящена настоящая работа, предложенное обобщение может быть использовано в ряде других разде-

лов интервального анализа. В частности, можно отметить, что применение его при построении теории производной [17, 12] и интеграла [18, 12] интервальной функции обещает быть перспективным.

1. Определения и обзор известных результатов

Рассмотрим задачу оценивания функции в постановке, принятой при использовании методов интервального анализа. Пусть вещественная функция n переменных $f(x)$, $x \in R^n$ задана в символьном виде, т. е. представлена выражением T , которое построено из функций f_i , взятых из фиксированного множества $\Phi = \{f_1, \dots, f_k\}$, переменных $x_1, \dots, x_n$, $(x_1, \dots, x_n) = x$ и вещественных констант. Обозначим это $f = \text{Sp}(T, f_1, \dots, f_k)$. Пусть, кроме того, задано условие $P(x)$, определяющее область в R^n . Необходимо отыскать такие значения B_1 и B_2 , что $P(x) \Rightarrow B_1 \leq f(x) \leq B_2$, причем желательно, чтобы величина

$$B_2 - \sup_{x \in M} f(x) + \inf_{x \in M} f(x) - B_1,$$

где $M = \{x | P(x)\}$, была возможно меньшей.

Стандартный интервальный анализ позволяет решить задачу в случае, когда $P(x)$ имеет вид:

$$a_1 \leq x_1 \leq b_1 \& \dots \& a_n \leq x_n \leq b_n, \quad a_i, b_i \in R, \quad a_i \leq b_i.$$

Задачу в указанной постановке с таким $P(x)$ будем обозначать Z_1 . В качестве Φ чаще всего [5, 7, 9, 14, 15] рассматривается множество $\{+, -, \cdot, /\}$. Это вызвано практической важностью алгоритмов оценивания рациональных функций. Иногда [6, 11, 13] Φ дополняется функциями x^a , $\exp$, $\ln$, $\sin$, $\cos$, $\arcsin$, $\arccos$ и т. д. Функции из Φ будем называть базовыми. Обозначим:

$$\Omega^n = \{([a_1, b_1], \dots, [a_n, b_n]) | a_i, b_i \in R, a_i \leq b_i\} \cup \{\Lambda\}.$$

Ω^n представляет собой множество замкнутых n -мерных параллелепипедов, среди которых есть и вырожденные. Символом Λ обозначен пустой параллелепипед. Далее в качестве синонима слова «параллелепипед» будем использовать «интервал».

С целью решения задачи Z_1 для функции $f(x)$, $x \in R^n$ и интервала $I \in \Omega^n$ строится интервальное расширение $F(I)$, удовлетворяющее свойству:

$$x \in I \Rightarrow f(x) \in F(I). \quad (1)$$

Для базовой функции $f(x)$, $x \in R^s$ положим:

$$F(I) = \{y | \exists x \in I \& f(x) = y\},$$

где $I \in \Omega^s$. При этом ограничим значения аргумента таким образом, чтобы $F(I) \in \Omega^1$. Например, при определении интервального деления I_1/I_2 полагаем, что $0 \notin I_2$.

Для расширений указанных выше базовых функций легко указать явное выражение через границы интервалов, например:

$$\begin{aligned} [a_1, b_1] + [a_2, b_2] &= [a_1 + a_2, b_1 + b_2], \\ [a_1, b_1] [a_2, b_2] &= [\min(a_1 a_2, a_1 b_2, a_2 b_1, b_1 b_2), \\ &\quad \max(a_1 a_2, a_1 b_2, a_2 b_1, b_1 b_2)], \\ \exp([a, b]) &= [e^a, e^b]. \end{aligned} \quad (2)$$

З а м е ч а н и е 1. Здесь и далее одними и теми же символами обозначены разные функции, например действительное и интервальное сложения. Конкретный смысл каждый раз определяется из контекста.

З а м е ч а н и е 2. Естественно считать, что для любой F $F(\Lambda) = \Lambda$, поэтому при определении интервальных функций случай $I = \Lambda$ специально не оговаривается.

Для небазовой функции $f = \text{Sp}(T, f_1, \dots, f_k)$ ее расширением является интервальная функция, задаваемая выражением T' , которое получается из T заменой всех f_i на F_i , т. е. $F = \text{Sp}(T', F_1, \dots, F_k)$. Для корректности определения необходимо, чтобы в ходе вычисления интервальной функции F для любых возможных значений аргументов не возникало недопустимых интервальных операций, например деления на интервал, содержащий 0.

О п р е д е л е н и е 1. Будем считать, что f имеет интервальное расширение F на интервале $I \in \Omega^n$ (в базисе $\{f_1, \dots, f_k\}$), и записывать $f \in A_1[I]$, если: а) $f = \text{Sp}(T, f_1, \dots, f_k)$; б) для любой функции g , являющейся частью f в том смысле, что выражение, определяющее g , входит в запись f (запишем это $g < f$), и для любого $I' \subset I$, $I' \subset \Omega^n$ имеет место $G(I') \subset \Omega^1$, где G — расширение для g . (Условие замкнутости).

З а м е ч а н и е 3. Если параллелепипед вырожден в одну точку $x = (x_1, \dots, x_n)$, т. е. $I = ([x_1, x_1], \dots, [x_n, x_n])$, то очевидно выполняется $F(I) = [f(x), f(x)]$, что и дает право функцию F называть интервальным расширением f . Любое действительное число x отождествляется с интервалом $[x, x]$, что позволяет, в частности, в качестве аргументов интервальных функций рассматривать действительные числа.

Построенное выше расширение в отличие от других будем называть естественным. По построению очевидно, что для естественного расширения выполняется свойство (1), что и дает простейший алгоритм решения задачи Z_1 .

Заметим, что оценка существенно зависит от формы записи функции. Например, пусть $f(x) = x(10 - x)$, $g(x) = 10x - x^2$, $I = [3, 5]$. Тогда

$$\begin{aligned} F([3, 5]) &= [3, 5](10 - [3, 5]) = [3, 5][5, 7] = [15, 35], \\ G([3, 5]) &= 10[3, 5] - [3, 5]^2 = [30, 50] - [9, 25] = [5, 41]. \end{aligned}$$

Заметим, что

$$\inf_{x \in I} f(x) = 21, \quad \sup_{x \in I} f(x) = 25.$$

О п р е д е л е н и е 2. Диаметром параллелепипеда I называется величина $q(I)$, такая, что: а) $q(I) = b - a$, если $I \in \Omega^1$, $I = [a, b]$; б) $q(I) = \max_{i=1, \dots, n} q(I_i)$, если $I \in \Omega^n$, $n > 1$, $I = I_1 \times \dots \times I_n$.

О п р е д е л е н и е 3. Будем считать, что F удовлетворяет условию Липшица-1 на $I \in \Omega^n$ (обозначим это $F \in L_{p_1}[I]$), если

$$\exists L \forall I' \ I' \subset I \ \& \ I' \in \Omega^n \Rightarrow q(F(I')) \leq Lq(I').$$

Обозначим через $H(f, I)$ интервал

$$\left[\inf_{x \in I} f(x), \sup_{x \in I} f(x) \right].$$

Из (1) следует, что интервальное равенство можно записать так:

$$F(I) = H(f, I) + E(F, I), \quad (3)$$

где $E(F, I) \in \Omega^1$.

Это равенство служит определением интервала $E(F, I)$. Положим $\omega(F, I) = q(E(F, I))$. Величина $\omega(F, I)$ характеризует точность оценки функции f на интервале I . В явном виде

$$\omega(F, I) = B(F(I)) - \sup_{x \in I} f(x) + \inf_{x \in I} f(x) - A(F(I)),$$

где $F(I) = [A(F(I)), B(F(I))]$.

Т е о р е м а 1. Если $f \in A_1[I]$ и $F \in L_{p_1}[I]$, $I \in \Omega^n$, то

$$\exists K \forall I' \ I' \subset I \ \& \ I' \in \Omega^n \Rightarrow \omega(F, I') \leq Kq(I'), \quad (4)$$

т. е. ошибка оценки функции линейно зависит от диаметра параллелепипеда, на котором производится оценка.

З а м е ч а н и е 4. Теоремы 1—3 приводятся без доказательств ввиду того, что утверждения, сформулированные в них, хорошо известны в интервальном анализе. Близкие по формулировкам теоремы доказываются в работах [1, 2, 6, 12].

Существует два пути повышения точности оценивания функции. Первый предусматривает получение расширений, отличных от естественного, но обладающих оценками ошибки, лучшими, чем (4). Второй путь предложен в [1] и основан на разбиении параллелепипеда на части и получении оценок для каждой из этих частей. Если ошибка хотя бы линейно зависит от диаметра, делая размеры каждой части исходного параллелепипеда все меньше, то в принципе можно получить сколь угодно точную оценку рассматриваемой функции.

О п р е д е л е н и е 4. Методы оценки функции, основанные на расширении F_0 , которое обладает свойством

$$\exists L \forall I' \ I' \subset I \ \& \ I' \in \Omega^n \Rightarrow \omega(F_0, I') \leq Lq^s(I'),$$

будем называть методами порядка s , а F_0 — расширением порядка s на I .

Интервальное расширение, дающее квадратичную оценку точности и называемое формой с серединным значением (MV -формой), широко рассматривается в литературе [1, 6, 8, 11, 12]. Его использование основано на следующих теоремах.

Т е о р е м а 2. Пусть функция $f(x_1, \dots, x_n)$ имеет непрерывные частные производные $\partial f / \partial x_i \equiv D_i f$ на интервале $I \in \Omega^n$, т. е. $f \in C^1(I)$. Пусть, кроме того, $D_i f \in A_1[I]$ и $D_i F$ обозначает естественное расширение $D_i f$. Положим

$$F_{MV}(I) = f(m) + \sum_{i=1}^n D_i F(I)(I_i - m_i), \quad (5)$$

где $m = (m_1, \dots, m_n)$ — центральная точка интервала I , а $I = I_1 \times \dots \times I_n$. Тогда выполняется

$$x \in I \Rightarrow f(x) \in F_{MV}(I).$$

Правая часть (5) и называется формой с серединным значением.

Т е о р е м а 3. В условиях предыдущей теоремы и если, кроме того, $\forall i D_i F \in Lp_1[I]$, то

$$\exists L \forall I' \quad I' \subset I \ \& \ I' \in \Omega^n \Rightarrow \omega(F_{MV}, I') \leq Lq^2(I').$$

В работе [10] предлагаются интервальные расширения более высокого порядка (3—6). Их построение основано на аппроксимации функции полиномами. Практическое использование этих расширений возможно лишь в случае оценивания функций одного аргумента.

Рассмотрим разбиение интервала на части [1, 5, 11, 12]. Будем считать, что f непрерывна на I . Пусть F — некоторое расширение f . Обозначим

$$F_k(I) = \bigcup_{i_1, \dots, i_n=1}^k F(I_{i_1}, \dots, I_{i_n}),$$

где $I_{i_1}, \dots, I_{i_n}$ — параллелепипеды равного размера, полученные разбиением исходного на k^n частей. Заметим, что в силу непрерывности $f F_k(I) \in \Omega^1$. Тогда для расширения F первого порядка имеем:

$$\begin{aligned} \omega(F_k, I) &\leq \max_{i_1, \dots, i_n=1, \dots, k} \omega(F, I_{i_1}, \dots, I_{i_n}) \leq \\ &\leq Lq(I_{i_1}, \dots, I_{i_n}) = Lq(I)/k, \end{aligned}$$

откуда очевидно, что для получения точности ε необходимо произвести объем вычислений $p = O(1/\varepsilon^n)$. Для метода порядка s та же оценка имеет вид $p = O(1/\varepsilon^{n/s})$, что показывает весьма высокую трудоемкость алгоритма, особенно для функций большого числа аргументов. Тем не менее различные дополнительные соображения [5, 11] позволяют построить весьма совершенный алгоритм, приведенный в работе [11]. Его сложность, по нашим оценкам, составляет $O(\ln^{n/s}(1/\varepsilon))$.

2. Недостатки существующих методов

У алгоритмов оценки функций, основанных на стандартном интервальном анализе, можно выделить два недостатка. Первый — принципиальная ограниченность интервала, на котором производится оценка. На практике весьма часто встречается ситуация, когда некоторый аргумент изменяется в промежутке $[a, \infty)$ или $(-\infty, a]$. Второй, наиболее существенный, недостаток состоит в ограниченности применения полученных алгоритмов. Дело в том, что существование всех интервальных расширений, рассмотренных выше, зависит от условия, которое не может быть проверено до начала работы алгоритма. Например, при использовании естественного расширения для оценки функции на I необходимо, чтобы $f \in A_1[I]$, однако выполнение условия б) определения 1 устанавливается лишь в процессе работы алгоритма. Это тем более плохо, что при $f \notin A_1[I]$ может иметь место:

$$\forall i \ f \in A_1[I_i],$$

где $I = \bigcup_{i=1}^s I_i$.

Пример 1. Пусть $f(x) = 1/(x^2 - 2x + 1.8)$, $I = [0, 1]$. Положив $g(x) = x^2 - 2x + 1.8$, заметим, что для выполнения условия замкнутости необходимо, чтобы $0 \notin G(I)$. Но так как $G([0, 1]) = [0, 1]^2 - 2 \cdot [0, 1] + 1.8 = [-0.2, 2.8]$, то $f \notin A_1[[0, 1]]$. Тем не менее, положив $I_1 = [0, 0.5]$ и $I_2 = [0.5, 1]$ имеем:

$$G([0, 0.5]) = [0.8, 2.05] \text{ и } G([0.5, 1]) = [0.05, 1.8],$$

откуда, учитывая очевидное свойство естественного расширения $I' \subset I \Rightarrow F(I') \subset F(I)$, получаем:

$$f \in A_1[[0, 0.5]] \text{ и } f \in A_1[[0.5, 1]].$$

Если при использовании алгоритмов с дроблением исходного параллелепипеда (а именно они являются единственно допустимыми с точки зрения точности оценки) встретится ситуация $f \notin A_1[I]$, то нельзя заранее сказать, существует ли разбиение $I = \bigcup_i I_i$ такое, что $\forall i \ f \in A_1[I_i]$. В этом случае приходится

пытаться оценивать функции на все более мелких разбиениях без гарантии конечного успеха. Аналогичная ситуация наблюдается и при расширениях, отличных от естественного.

В принципе можно было бы выбрать Φ таким образом, чтобы условие замкнутости выполнялось автоматически. При этом Φ может быть таким: $\Phi = \{+, -, \cdot, \exp, \sin, \cos, x^\alpha (\alpha > 0)\}$. Однако невозможность включения таких функций, как $\ln$, $\lg$, а главное / (деление), делает такой вариант неприемлемым.

Далее будет предложена модификация интервального анализа, позволяющая избавиться от ограниченности интервалов, на которых производится оценка. Эта модификация также позволит включить в множество Φ практически все функции, встречающиеся в качестве базовых в различных приложениях. Условие замкнутости при этом будет выполняться автоматически.

3. Обобщение интервального анализа

Основная идея обобщенного интервального анализа (ОИА) состоит в следующем. Будем рассматривать расширения действительных функций не на множество параллелепипедов, а на множество

$$\bar{\Omega}^n = \{([a_1, b_1], \dots, [a_n, b_n]) \mid a_i, b_i \in \hat{R}\} \cup \{\Lambda\},$$

где $\hat{R} = R \cup \{\infty\}$.

Если $b \geq a$, то $[a, b]$ — обычный интервал, если $b < a$, то $[a, b]$ есть $]-\infty, b[\cup [a, +\infty[$. В виде $[a, \infty]$, $[\infty, a]$ и $[\infty, \infty]$ записываются соответственно бесконечные интервалы $[a, +\infty[$, $] -\infty, a]$ и $] -\infty, +\infty[$. Элементы $\bar{\Omega}^n$ будем в дальнейшем называть обобщенными параллелепипедами (обобщенными интервалами). Заметим, что $\Omega^n \subset \bar{\Omega}^n$. Таким образом, под обобщенным параллелепипедом понимаем декартово произведение обобщенных одномерных интервалов.

Пусть для $x = (x_1, \dots, x_n)$ задано условие:

$$P(x) = x_1 \in [a_1, b_1] \& \dots \& x_n \in [a_n, b_n],$$

где $[a_i, b_i] \in \bar{\Omega}^1$.

Если функция f задана в символьном виде (в базисе $\Phi = \{f_1, \dots, f_k\}$), то задача отыскания $B_1, B_2 \in \hat{R}$ таких, что

$$P(x) \Rightarrow f(x) \in [B_1, B_2],$$

где $[B_1, B_2] \in \bar{\Omega}^1$, назовем задачей Z_2 .

Подобно случаю стандартного интервального анализа (СИА) при решении Z_2 для функции f и обобщенного интервала I будем строить расширение $\bar{F}$ на множестве обобщенных параллелепипедов так, чтобы выполнялось условие:

$$x \in I \Rightarrow f(x) \in \bar{F}(I), \quad I \in \bar{\Omega}^n. \quad (6)$$

Расширение строится аналогично случаю СИА, т. е. для базовых функций:

$$\bar{F}(I) = \{y \mid \exists x \ x \in I \& f(x) = y\},$$

где $I \in \bar{\Omega}^s$.

Ниже выпишем равенства, позволяющие явно вычислять значения расширений для некоторых наиболее часто употребляемых функций. Эти равенства достаточно просты, хотя и несколько более громоздки, чем в случае СИА (ср. с (2)).

Введем следующие обозначения: $I_1 = [a_1, b_1]$, $I_2 = [a_2, b_2]$, $\Omega_1^1 = \{[\infty, b] \mid b \in R\}$, $\bar{\Omega}_r^1 = \{[a, \infty] \mid a \in R\}$, $\bar{\Omega}_d^1 = \{[a, b] \mid a, b \in R \& a > b\} \cup \{[\infty, \infty]\}$.

Отметим, что любой интервал $I \in \bar{\Omega}_d^1$ естественным образом представим в виде $I = I' \cup I''$, где $I' \in \bar{\Omega}_r^1$, $I'' \in \bar{\Omega}_l^1$. Для опре-

деленности представим $[\infty, \infty]$ как $[\infty, 0] \cup [0, \infty]$. При вычислениях по указанным ниже формулам будем формально полагать, что] для $c \in \widehat{R}$ $c + \infty = \infty + c = -\infty = 1/0 = \infty$, $1/\infty = 0$, и считать, что участие $c \in \widehat{R}$ в записи неравенства предполагает $c \neq \infty$. Положим также для $c < 0$ и $d > 0$ или $d = \infty \min (... , c \cdot \infty, ...) = \max (... , d \cdot \infty, ...) = \infty$. Кроме того,

$$-[a, b] = [-b, -a];$$

$$I_1 + I_2 = \begin{cases} [a_1 + a_2, b_1 + b_2], & \text{если } (I_1, I_2 \in \Omega^1 \cup \overline{\Omega}_l^1 \cup \overline{\Omega}_r^1) \vee \\ & \vee ((I_1 \in \Omega^1 \vee I_2 \in \Omega^1) \& a_1 + a_2 > b_1 + b_2), \\ [\infty, \infty] & \text{в остальных случаях,} \end{cases}$$

$$I_1 - I_2 = I_1 + (-I_2),$$

$$[a, b]^{-1} = \begin{cases} \Lambda, & \text{если } a = b = 0, \\ [1/b, 1/a] & \text{в остальных случаях,} \end{cases}$$

$$I_1 \cdot I_2 = \begin{cases} [\min(a_1 a_2, a_1 b_2, b_1 a_2, b_1 b_2), \max(a_1 a_2, a_1 b_2, b_1 a_2, b_1 b_2)], & \text{если } I_1, I_2 \in \Omega^1 \cup \overline{\Omega}_r^1, \\ -(-I_1 \cdot I_2), & \text{если } I_1 \in \overline{\Omega}_l^1, \\ -(I_1 \cdot (-I_2)), & \text{если } I_2 \in \overline{\Omega}_l^1, \\ I_1' \cdot I_2 \cup I_1'' \cdot I_2, & \text{если } I_1 \in \overline{\Omega}_d^1, I_1 = I_1' \cup I_1'', \\ I_1 \cdot I_2' \cup I_1 \cdot I_2'', & \text{если } I_2 \in \overline{\Omega}_d^1, I_2 = I_2' \cup I_2'', \end{cases}$$

$$I_1/I_2 = I_1 \cdot I_2^{-1},$$

$$\exp([a, b]) = \begin{cases} [e^a, e^b] & \text{если } b \geq a, \\ [0, e^b] \cup [e^a, \infty], & \text{если } a > b, \\ [0, e^b], & \text{если } a = \infty \& b \in R, \\ [e^a, \infty], & \text{если } a \in R \& b = \infty, \\ [0, \infty], & \text{если } a = b = \infty. \end{cases} \quad (7)$$

Вообще говоря, следует ограничиться рассмотрением лишь тех значений аргументов, при которых $\overline{F}(I) \in \overline{\Omega}^1$. В частности, $\exp([a, b]) \notin \overline{\Omega}^1$, если $a > b$. Как избежать этого ограничения, показано ниже. Заметим лишь, что замкнутость не имеет места для значительно более узкого по сравнению с СИА класса функций.

Для небазовой функции расширение в смысле ОИА строится аналогично случаю СИА, т. е. как суперпозиция расширений базовых функций.

О п р е д е л е н и е 5. Будем считать, что для f существует интервальное расширение $\overline{F}$ на интервале $I \in \overline{\Omega}^n$ в смысле ОИА (в базе $\{f_1, \dots, f_k\}$), и записывать $f \in A_2[I]$, если: а) $f = \text{Sp}(T, f_1, \dots, f_k)$; б) $g < f \Rightarrow (\forall I' I' \subset I \& I' \in \overline{\Omega}^n \Rightarrow \overline{G}(I') \in \overline{\Omega}^1)$. (Условие замкнутости).

Отметим два очевидных свойства. Пусть $I \in \Omega^n$, тогда

$$f \in A_1[I] \Rightarrow \bar{f} \in A_2[I] \quad \text{и} \quad \bar{F}(I) = F(I).$$

Как отмечалось выше, весьма желательно, чтобы условие б) выполнялось для всех базовых функций и для всех интервалов $I \in \bar{\Omega}^n$. Нетрудно проверить, что оно выполняется для функций $\Phi_1 = \{+, -, \cdot, /, \sin, \cos, \operatorname{tg}, \operatorname{ctg}, \ln, x^\alpha \text{ (если } R \setminus \{0\} \subset \operatorname{dom}(x^\alpha)), \operatorname{abs}\}$. Особую важность имеет тот факт, что в случае $\Phi = \{+, -, \cdot, /\}$ алгоритм, основанный на ОИА, применим к любой функции $f = \operatorname{Sp}(T, +, -, \cdot, /)$, что не имело места в случае СИА.

Из числа функций, используемых в качестве базовых в большинстве приложений, условию б) определения 5 не удовлетворяют лишь $\exp$, а также функция x^α , если она не определена для отрицательных чисел (например, $x^{1/2}$). Тем не менее существует возможность включения названных функций в множество базовых без нарушения условия замкнутости. Рассмотрим эту возможность на примере функции $\exp$. Пусть $\exp < f$ и $\exp$ входит в выражение, определяющее f , в виде $\exp(g(x))$. Тогда, для того чтобы $f \in A_2[I]$, необходимо $\bar{G}(I) \notin D$, где $D = \{[a, b] \mid a, b \in R, a > b\}$, что непосредственно видно из (7). Однако множество $\exp([a, b])$, где $[a, b] \in D$ можно аппроксимировать обобщенным интервалом $[0, \infty]$ либо обобщенным интервалом $[e^a, e^b]$. Переопределим интервальное расширение в смысле ОИА для функции $\exp$, заменив вариант $a > b$ в (7) либо на $[e^a, e^b]$, либо на $[0, \infty]$. Нетрудно видеть, что в этом случае расширение $\exp$ замкнуто в смысле ОИА. Аналогичная процедура применима и для x^α , когда $\operatorname{dom}(x^\alpha) \cap R_{e^-} = \emptyset$.

Рассмотрим пример функции, которая не может быть оценена средствами СИА, однако легко оценивается при использовании ОИА.

Пример 2. Пусть

$$f(x, y) = \frac{x}{y \operatorname{tg} \frac{\pi x}{4} + 1}, \quad 1 \leq x \leq 3, \quad y \geq 2.$$

$$\begin{aligned} \bar{F}([1, 3], [2, \infty]) &= [1, 3]/([2, \infty] \operatorname{tg}((\pi/4)[1, 3]) + 1) = \\ &= [1, 3]/([2, \infty][1, -1] + 1) = [1, 3]/[3, -1] = \\ &= [1, 3] [-1, 1/3] = [-3, 1]. \end{aligned}$$

Отметим, что известны и другие обобщения интервального анализа. В статье [18] (см. также [12]) приводятся расширения СИА для работы с бесконечными интервалами. Допустимы интервалы $(-\infty, a]$, $[a, +\infty)$ и $(-\infty, +\infty)$. Однако арифметические интервальные операции в том виде, в котором они определены в названной работе, не являются замкнутыми.

В другом обобщении [17] (см. также [12]) построена система, замкнутая относительно арифметических операций. Однако тот факт, что СИА дополняется лишь бесконечными и полубесконеч-

ными интервалами, приводит к слишком грубой оценке множества значений функции. В частности, считается, что если I_1 и I_2 — обычные интервалы и $0 \in I_2$, то $I_1/I_2 = (-\infty, +\infty)$. В работах [17, 18] не рассматриваются расширения для функций, не являющихся рациональными.

Наиболее близким к введенному в настоящей работе является обобщение СИА, приведенное в [19], где содержится определение интервальной арифметики. Если не принимать во внимание некоторые частности, эта арифметика подобна той, которой посвящен разд. 3. Однако в работе [19] автор ограничивается рассмотрением лишь одномерного случая, причем только для рациональных функций.

Следует также упомянуть обобщение СИА, приведенное в [20]. Множество Ω^n пополняется множеством интервалов $[a, b]$, в которых $b < a$. При этом смысл, придаваемый им, не имеет ничего общего со смыслом интервалов, вводимых в настоящей статье. Основной целью обобщения в [20] является упрощение формулировок и доказательств утверждений, обычно рассматриваемых в СИА.

4. Оценка точности

Рассмотрим точность оценки множества значений функции $f(x): \hat{R}^n \rightarrow \hat{R}$ при $x \in I$, $Z \in \bar{\Omega}^n$. При этом будем считать, что f удовлетворяет следующему условию:

$$\forall I' \quad I \subset I' \text{ \& } I' \in \Omega^n \Rightarrow \{y \mid \exists x \in I' \text{ \& } f(x) = y\} \in \bar{\Omega}^1.$$

О п р е д е л е н и е 6. Диаметром обобщенного интервала I назовем величину $q(I)$, такую, что:

$$a) \quad \bar{q}([a, b]) = \begin{cases} \operatorname{arctg} b - \operatorname{arctg} a, & \text{если } b \geq a \vee (a \in R \text{ \& } b = \infty), \\ \operatorname{arctg} b - \operatorname{arctg} a + \pi & \text{в остальных случаях;} \end{cases}$$

$$б) \quad \bar{q}(I) = \max_{i=1, \dots, n} \bar{q}(I_i), \text{ если } I = I_1 \times \dots \times I_n.$$

(Полагаем, что $\operatorname{arctg}(\infty) = \pi/2$).

З а м е ч а н и е 5. Здесь и далее для отображения числовой прямой на отрезок выбрана функция $y = \operatorname{arctg} x$. Вообще говоря, вместо арктангенса можно было бы взять любую функцию $g: R \rightarrow [a, b]$, лишь бы она была монотонной и достаточно гладкой.

О п р е д е л е н и е 7. Будем считать, что F удовлетворяет условию Липшица-2 на $I \in \bar{\Omega}^n$ ($\bar{F} \in L_{p_2}[I]$), если

$$\exists L \quad \forall I' \quad I \subset I' \text{ \& } I' \in \bar{\Omega}^n \Rightarrow \bar{q}(F(I')) \leq \bar{L}q(I').$$

Введем функцию $\oplus$, такую что

$$[a, b] \oplus [c, d] = [\operatorname{tg}(c + \operatorname{arctg} a), \operatorname{tg}(d + \operatorname{arctg} b)], \quad (8)$$

где $[a, b] \in \bar{\Omega}^1$, $[c, d] \in \Omega^1$. (Считаем, что $\operatorname{tg}(\pi/2) = \operatorname{tg}(-\pi/2) = \infty$.) Через $\bar{H}(f, I)$, $I \in \bar{\Omega}^n$ обозначим обобщенный интервал $\{y \mid \exists x \in I \text{ \& } f(x) = y\}$. Учитывая (6), можно записать:

$$\bar{F}(I) = \bar{H}(f, I) \oplus \bar{E}(\bar{F}, I), \quad (9)$$

где $\bar{E}(\bar{F}, I) \in \bar{\Omega}^1$.

Это равенство (аналог (3) в случае СИА) служит определением интервала $\bar{E}$. Величина $\bar{\omega}(\bar{F}, I) = q(\bar{E}(\bar{F}, I))$ характеризует ошибку при оценивании f на обобщенном интервале I средствами ОИА.

Т е о р е м а 4. Пусть $I \in \bar{\Omega}^n$, $f \in A_2[I]$, $\bar{F} \in L_{p_2}[I]$, тогда ошибка оценки $\bar{\omega}$ линейно зависит от диаметра I в смысле ОИА.

Действительно, если $\bar{F} \in L_{p_2}[I]$, то

$$\forall I' \quad I' \subset I \text{ \& } I' \in \bar{\Omega}^n \Rightarrow \bar{q}(\bar{F}(I')) \leq \bar{Lq}(I'),$$

но из (8) и (9) видно, что $\bar{\omega}(\bar{F}, I') \leq \bar{q}(\bar{F}(I'))$, следовательно, $\bar{\omega}(\bar{F}, I') \leq \bar{Lq}(I')$.

Отметим одно неприятное обстоятельство. В случае СИА условие Липшица-1 выполняется для подавляющего большинства функций, которые тем самым попадают под действие теоремы 1. Условие Липшица-2 значительно сильнее ограничивает применение теоремы 4 (аналога теоремы 1). И хотя можно показать, что если $f \in A_1[I]$, $I \in \Omega^n$, то $F \in L_{p_1}[I] \Leftrightarrow F \in L_{p_2}[I]$, тем не менее условие Липшица-2 часто не выполняется в окрестности точек $x \in \hat{R}^n \setminus R^n$. В качестве иллюстрации отметим, что $\nmid \notin L_{p_2}[I]$, если $I = [a, b] \times [c, d]$, $a > b$, $c > d$.

Построенное расширение F действительной функции f на множестве $\bar{\Omega}^n$ по аналогии с СИА назовем естественным. Помимо него, можно предложить и другие расширения, одно из которых рассмотрено в следующем разделе. Теорема 5 связывает $\bar{\omega}(F, I)$ и $\omega(F, I)$ — величины, отражающие точность оценки в смысле СИА и ОИА.

О п р е д е л е н и е 8. Пусть $\bar{F}$ — некоторое расширение f . Будем называть его расширением порядка s на $I \in \bar{\Omega}^n$ (в смысле ОИА), если

$$\exists L \quad \forall I' \quad I' \subset I \text{ \& } I' \in \bar{\Omega}^n \Rightarrow \bar{\omega}(\bar{F}, I') \leq \bar{Lq}^s(I'). \quad (10)$$

Методы оценки, основанные на таком $\bar{F}$, будем называть методами порядка s (в смысле ОИА).

Т е о р е м а 5. Зафиксируем $I \in \Omega^n$. Пусть F — некоторое расширение f в смысле ОИА, удовлетворяющее (6) и определенное для всех $I' \subset I$, $I' \subset \Omega^n$ так, что $F(I') \in \bar{\Omega}^1$. Тогда F — расширение порядка S в смысле ОИА в том и только в том случае, если оно — расширение порядка S в смысле СИА.

Л е м м а. Пусть $I_0 \in \Omega^n$, тогда

$$а) \forall I'_0 \ I'_0 \subset I_0 \ \& \ I'_0 \in \Omega^n \Rightarrow \bar{q}(I'_0) \leq q(I'_0),$$

$$б) \exists k \ \forall I'_0 \ I'_0 \subset I_0 \ \& \ I'_0 \in \Omega^n \Rightarrow (I'_0) \leq k \bar{q}(I'_0).$$

Докажем лемму для случая $n = 1$. Заметим, что $\bar{q}([a, b]) = \arctg b - \arctg a = (b - a)/(1 + c^2)$, где $c \in [a, b]$, поэтому

$$\bar{q}([a, b]) \leq b - a = q([a, b]),$$

$$\bar{q}([a, b]) \geq (b - a)/(1 + \max^2(|a|, |b|)) = (b - a)/k = q([a, b])/k.$$

$$q([a, b]) = (b - a)/(1 + \max^2(a, b)) = (b - a)/k = q([a, b])/k.$$

Для $n > 1$ утверждение леммы непосредственно следует из рассмотренного случая $n = 1$. Заметим, что константа $k = k(I_0)$ своя для каждого I_0 .

Доказательство теоремы. Зафиксируем $I_1 = F(I)$, $I_1 \in \Omega^1$. Пусть $\exists L \ \forall I' \ I' \subset I \ \& \ I' \in \Omega^n \Rightarrow \bar{\omega}(F, I') \leq L \bar{q}^s(I')$. Положим $H(F, I') = [a, b]$, $E(F, I') = [c_1, d_1]$, $\bar{E}(F, I') = [c_2, d_2]$. Исходя из (3), (8), (9), имеем:

$$b + d_1 = \operatorname{tg}(d_2 + \arctg b),$$

$$a + c_1 = \operatorname{tg}(c_2 + \arctg a).$$

Кроме того,

$$\begin{aligned} \omega(F, I') &= d_1 - c_1 = (d_1 + b) - b + a - (a + c_1) = \\ &= q([b, b + d_1]) + q([a + c_1, a]), \end{aligned}$$

но так как $[b, b + d_1] \in I_1$ и $[a + c_1, a] \in I_1$, то, принимая во внимание доказанную лемму,

$$\begin{aligned} \omega(F, I') &\leq k(I_1) (\bar{q}([b, b + d_1]) + \bar{q}([a + c_1, a])) = \\ &= k(I_1) (\arctg(b + d_1) - \arctg b + \arctg a - \arctg(a + c_1)) = \\ &= k(I_1) (d_2 + \arctg b - \arctg b + \arctg a - c_2 - \arctg a) = \\ &= k(I_1) (d_2 - c_2) = k(I_1) \bar{\omega}(F, I') \leq L k(I_1) \bar{q}^s(I'), \end{aligned}$$

но $\bar{q}(I') \leq q(I')$, следовательно,

$$\omega(F, I') \leq k(I_1) L q^s(I').$$

В одну сторону утверждение теоремы доказано. В другую сторону доказательство проводится аналогично. Доказанная теорема показывает эквивалентность методов, основанных на стандартном и на обобщенном интервальном анализе, в случае оценки функции на обычных интервалах.

5. Квадратичный метод

Предлагается метод второго порядка для оценки функции на обобщенном интервале. Метод является аналогом формы с серединым значением.

Функции $u(I)$, $I \in \bar{\Omega}^n$ и $\text{atg}(k, x)$, $k, x \in \hat{R}^n$ определим следующими равенствами (будем считать, что $\text{arctg}(\infty) = \pi/2$):

$$U([a, b]) = \begin{cases} [\text{arctg } a, \text{arctg } b], & \text{если } b \geq a \vee (b = \infty \ \& \ a \in R), \\ [\text{arctg } a, \text{arctg } b + \pi], & \text{если } b < a, \\ [-\pi/2, \text{arctg } b], & \text{если } a = \infty, \end{cases}$$

$$U((a_1, b_1], \dots, [a_n, b_n]) = (U([a_1, b_1]), \dots, U([a_n, b_n])).$$

Если $k, x \in \hat{R}$, то

$$\text{arctg}(k, x) = \begin{cases} \text{arctg } x, & \text{если } x \geq k \vee k = \infty \vee x = \infty, \\ \pi + \text{arctg } x, & \text{если } x < k. \end{cases}$$

Если $k, x \in \hat{R}^n$, $k = (k_1, \dots, k_n)$, $x = (x_1, \dots, x_n)$, то $\text{atg}(k, x) = (\text{atg}(k_1, x_1), \dots, \text{atg}(k_n, x_n))$.

Пусть необходимо оценить функцию f на $I \in \bar{\Omega}^n$. Построим функцию g на $U(I)$. Зафиксируем $k_1 \in \hat{R} : k_1 \notin H(f, I)$ и $k_2 \in \hat{R}^n : k_2 \notin I$. Точку k_1 можно выбрать на основе любой грубой оценки f на I . Положим $g(y) = \text{atg}(k_1, f(\text{tg } y))$, где $y \in U(I)$. Здесь и далее для интервала $I_0 = [a, b]$, $a \leq b$, $b - a < \pi$, будем считать $\text{tg}(I_0) = [\text{tg } a, \text{tg } b]$ и для вектора $x = (x_1, \dots, x_n)$ — $\text{tg } x = (\text{tg } x_1, \dots, \text{tg } x_n)$. Предположим, что $g \in C^1[U(I)]$, $\forall i \ D_i g \in A_1[U(I)]$, $D_i G \in Lp_1[U(I)]$, где $D_i G$ — естественное расширение для $D_i g$ в смысле СИА. Тогда по теоремам 2 и 3 для функции g на $U(I)$ существует форма с серединным значением G_{MV} . Можно записать для любого $I' \subset I$, $I' \in \bar{\Omega}^n$:

$$G_{MV}(U(I')) = g(m(U(I'))) + \sum_{i=1}^n D_i G(U(I')) R_i(U(I')),$$

где для интервала $I = ([a_1, b_1], \dots, [a_n, b_n])$

$$m(I) = ((b_1 + a_1)/2, \dots, (b_n + a_n)/2),$$

$$R_i(I) = [-(b_i - a_i)/2, (b_i - a_i)/2].$$

Положим по определению для $I' \subset I$, $I' \in \bar{\Omega}^n$

$$\bar{F}_{MV}(I') = \text{tg}(G_{MV}(U(I'))). \quad (11)$$

Следующая теорема показывает, что форма (11) (назовем ее NMV -формой) дает квадратичный (в смысле ОИА) метод оценки функции.

Теорема 6. Пусть форма F_{MV} определена на $I \in \bar{\Omega}^n$, тогда:

1) для любого I' , $I' \subset I$, $I' \in \bar{\Omega}^n$ и для любого $x \in I'$ $f(x) \in \bar{F}_{MV}(I')$;

2) существует константа L такая, что для любого $I' \subset I$, $I' \in \bar{\Omega}^n$ $\bar{\omega}(\bar{F}_{MV}, I') \leq Lq^2(I')$.

Доказательство. 1) По определению $g(y)$ имеем $f(x) = \text{tg}(g(y))$, где $y \in U(I)$, причем

$$y = \text{atg}(k_2, x) + v, \quad v = (v_1, \dots, v_n), \quad v_i \in \{0, -\pi\}, \quad (12)$$

но $g(y) \in G_{MV}(U(I'))$ и, следовательно,

$$f(x) = \operatorname{tg} g(y) \in \operatorname{tg} G_{MV}(U(I')) = \bar{F}_{MV}(I').$$

2) Можно заметить, что $q(\bar{E}(\bar{F}_{MV}, I')) = q(E(G_{MV}, U(I')))$ и, кроме того, $q(U(I')) = \bar{q}(I')$, поэтому

$$\begin{aligned} \omega(\bar{F}_{MV}, I') &= q(\bar{E}(\bar{F}_{MV}, I')) = q(E(G_{MV}, U(I'))) \leq \\ &\leq Lq^2(U(I')) = L\bar{q}^2(I'). \end{aligned}$$

По ходу построения формы $\bar{F}_{MV}$ были сделаны предположения о свойствах функции g . Исходя из определения g , имеем:

$$Dig(y) = Dif(x)(1 + x_1^2)/(1 + f^2(x)),$$

где x связан с y соотношением (12). Отсюда для каждой конкретной функции f можно проверить условия, которым должна удовлетворять соответствующая ей функция g .

6. Алгоритм

Пусть необходимо оценить множество значений функции f на обобщенном интервале I_0 . Ниже будет представлен набросок алгоритма, который решает эту задачу. Он получен модификацией алгоритма Мура [11] на случай ОИА. При этом некоторые полезные детали, снижающие вычислительную сложность алгоритма, для простоты опущены.

Будем считать, что для функции f и любого интервала $I' \subset I_0$, $I' \in \Omega^n$ выполняется условие:

$$\{y \mid \exists x \in I' \ \& \ f(x) = y\} \in \bar{\Omega}^1.$$

Пусть, кроме того, для f имеется расширение $\bar{F}$, удовлетворяющее условию монотонности по включению: $I_1 \subset I_2 \Rightarrow \bar{F}(I_1) \subset \bar{F}(I_2)$.

Это условие является обобщением условия (6) и выполняется для большинства известных интервальных расширений, в том числе для рассмотренных в данной работе.

Для данного ε необходимо найти a и b такие, что $\bar{H}(f, I_0) \subset [a, b]$, т. е. решить задачу Z_2 , причем если считать, что $[a, b] = F_p(I_0)$, то должно выполняться $\bar{\omega}(F_p, I_0) \leq \varepsilon$.

Построим алгоритм для нахождения a . Тогда b находится применением этого же алгоритма к функции $-f$. Алгоритм состоит из двух основных частей. Первая часть реализует поиск интервала $\bar{F}(I)$ по интервалу $I \subset I_0$. Организация таких вычислений для некоторых интервальных расширений рассмотрена выше. Вторая часть — дробление исходного интервала I_0 на части I_i , $I_0 = \bigcup_i I_i$ с таким расчетом, чтобы минимизировать количество применений первой части алгоритма, необходимых для достижения данной точности оценивания ε .

Будем считать, что $\bar{F}(I_0) \neq [\infty, \infty]$, и выберем точку $k \notin \bar{F}(I_0)$. Левую границу обобщенного интервала $\bar{F}(I)$ обозначим $A\bar{F}(I)$.

Для $c_1, c_2, k \in \hat{R}, c_1 \neq k, c_2 \neq k$ будем считать, что c_2 больше или равно c_1 относительно k , и записывать это в виде $c_2 \overset{k}{\geq} c_1$, если 1. $k = \infty$ & $c_2 \geq c_1$, либо 2. $k, c_1, c_2 \in R$ & $(k < c_1 \leq c_2 \vee c_1 \leq c_2 < k \vee c_2 < k < c_1)$, либо 3. $k \in R$ & $c_1 = \infty$ & $c_2 < k$, либо 4. $k \in R$ & $c_2 = \infty$ & $(c_1 > k \vee c_1 = \infty)$.

Последовательность $\{c_i\}_{i=1}^m, c_i \in \hat{R}$ назовем k -упорядоченной, если для любых $i, j, j > i$ выполняется $c_j \overset{k}{\geq} c_i$.

В ходе работы алгоритма будет поддерживаться список list. В нем будут храниться пары $(I_i, A\bar{F}(I_i))$, где $I_i \subset I_0$. Первоначально список list содержит лишь пару $(I_0, A\bar{F}(I_0))$. Повторяющимся шагом алгоритма является раскрытие головной пары в списке list.

Перед началом раскрытия список всегда удовлетворяет двум свойствам: 1) пары, содержащиеся в списке, k -упорядочены по значениям своих вторых элементов; 2) объединение всех первых элементов пар, содержащихся в списке list, есть I_0 .

Текущим приближением A_t к значению $A\bar{H}(f, I_0)$ будет являться второй элемент головной пары списка list. Действительно, коль скоро выполняется свойство 2 и для любой пары $(I, A\bar{F}(I))$ из списка list $A_t \overset{k}{\leq} A\bar{F}(I)$, то $A_t \overset{k}{\leq} A\bar{H}(f, I_0)$. Здесь через $A\bar{H}(f, I)$ обозначена левая граница обобщенного интервала значений функции f на интервале I .

Раскрытие головной пары включает следующие действия: 1) проверку условия окончания работы алгоритма (см. ниже); если условие выполнено, то алгоритм заканчивает работу со значением второго элемента головной пары списка list; 2) изъятие из списка головной пары, обозначенной $(I_1, A\bar{F}(I_1))$; 3) преобразование I_1 . Пусть $I_1 = I_{s,1} \times \dots \times I_{1,n}$, где все $I_{i,t}$ — одномерные обобщенные интервалы. Выберем $I_{1,s}$ таким образом, чтобы $\bar{q}(I_{s,s}) = \bar{q}(I_1)$, разделим $I_{1,s}$ на два интервала $I_{2,s}$ и $I_{3,s}$ так, чтобы $\bar{q}(I_{2,s}) = \bar{q}(I_{3,s})$. Положим $I_2 = I_{1,1} \times \dots \times I_{2,s} \times \dots \times I_{1,n}$ и $I_3 = I_{1,1} \times \dots \times I_{3,s} \times \dots \times I_{1,n}$. Теперь $I_1 = I_2 \cup I_3$; 4) нахождение $A\bar{F}(I_2)$ и $A\bar{F}(I_3)$ с помощью расширения $\bar{F}$, т. е. применения первой части алгоритма; 5) включение пары $(I_2, A\bar{F}(I_2))$ и $(I_3, A\bar{F}(I_3))$ в список list таким образом, чтобы он остался k -упорядоченным по значениям вторых элементов пар.

Рассмотрим вопрос прекращения работы алгоритма. Для головной пары списка list $(I_1, A\bar{F}(I_1))$ имеем: $A\bar{F}(I_1) \overset{k}{\leq} A\bar{H}(f, T_0)$.

Если $\bar{F}$ является интервальным расширением порядка s с константой L (см. (10)), то

$$\bar{q}([A\bar{F}(I_1), A\bar{H}(f, I_0)]) \leq L\bar{q}^s(I_1).$$

Это соотношение дает условие прекращения итераций алгоритма — достаточно сделать интервал, соответствующий головной паре, таким, что $\bar{q}(I_1) \leq (2L)^{1/8}$.

Если константа L неизвестна (а именно так чаще всего и бывает на практике), вопрос окончания вычислений становится сложным, и его рассмотрение выходит за рамки настоящей работы.

Построенный выше алгоритм позволяет снизить объем вычислений за счет быстрой локализации точек, где значения функции близки к $\overline{AH}(f, I_0)$ и $\overline{BH}(f, I_0)$. Дробление исходного интервала, полученное в ходе работы алгоритма, мельче вблизи этих точек, что дает возможность исключить из рассмотрения те части исходного параллелепипеда, на которых значения функции заведомо далеки от границ интервала $\overline{H}(f, I_0)$.

Литература

1. Moore R. E. Interval analysis. Englewood Cliffs. 1966.
2. Алефельд Г., Херцбергер Ю. Введение в интервальные вычисления. М., 1987.
3. Шокин Ю. И. Интервальный анализ. Новосибирск, 1981.
4. Interval mathematics/Ed. K. Nickel. Lect. Notes Comput. Sci. Vol. 29. 1975.
5. Moore R. E. On computing the range of rational function on n variables over a bounded region//Computing. 1976. Vol. 16, N 1, 2. P. 1—15.
6. Caprani O., Madsen K. Mean value forms in interval analysis//Computing 1980. Vol. 25, N 2. P. 147—154.
7. Ratschek H., Schröder G. Centered forms for functions in several variables//J. Math. Analysis Applic. 1981. Vol. 82, N 2. P. 543—552.
8. Rall L. B. Mean value and Taylor forms in interval analysis//SIAM J. Math. Analys. 1983. Vol. 14, N 2. P. 223—238.
9. Rall L. B. Representations of intervals and optimal error bounds//Math. Comput. 1983. Vol. 41, N 163. P. 219—227.
10. Cornelius H., Lohner R. Computing the range of values of real functions with accuracy higher then second order//Computing. 1984. Vol. 33, N 3, 4. P. 331—347.
11. Asaithambi N. S., Shen Zhen, Moore R. E. On computing the range of values/Computing. 1982. Vol. 28, N 3. P. 225—237.
12. Калмыков С. А., Шокин Ю. И., Юлдашев З. Х. Методы интервального анализа. Новосибирск, 1986.
13. Yohe J. M. Software for interval arithmetic: a reasonably portable package//ACM Trans. Math. Software. 1979. Vol. 5, N 1. P. 50—63.
14. Good D. I., London R. L. Computer interval arithmetic: definition and proof of correct implementation//J. Assoc. Comput. Machinery. 1970. Vol. 17, N 4. P. 603—612.
15. Cole A. J., Morrison R. A system for interval arithmetic//Software — Practice and Experience. 1982. Vol. 12, N 4. P. 341—350.
16. Роголев А. Н., Шокин Ю. И. Пакет интервальных операций для ЭВМ БЭСМ-6. Новосибирск, 1981.
17. Sendov B. Some topics of segment analysis//Interval mathematics/Ed. K. Nickel. N. Y.: Acad. Press. 1980, p. 203—222.
18. Caprani O., Madsen K., Rall L. B. Integration of interval functions//SIAM J. Math. Analys. 1981. Vol. 12, N 3. P. 321—341.
19. Laveuve S. E. Definition einer Kahan-Arithmetik und ihre Implementierung//Interval mathematics/Ed. K. Nickel. Lect. Notes Comput. Sci. Vol. 29. 1975, p. 236—245.
20. Kaucher E. Interval analysis in the extended interval space IR//Fundamentals of numerical analysis/Ed. G. Alefeld, R. D. Grigorieff. Vol. 2. Wien etc., 1980.

К ОЦЕНИВАНИЮ ПАРАМЕТРА СДВИГА ОДНОГО СЕМЕЙСТВА РАСПРЕДЕЛЕНИЙ

1. Введение

В 1963 г. вышло интересное сообщение М. Кендалла [1], посвященное исследованиям Д. Бернулли метода максимального правдоподобия. Это сообщение содержит в себе также работы самого Д. Бернулли [2] и его оппонента Л. Эйлера [3]. Из работ [2, 3] видно, что у истоков одного из самых распространенных статистических методов оценивания — метода максимального правдоподобия — стоял Д. Бернулли, хотя рассматриваемая им задача носила очень частный характер: по реализациям независимых случайных величин $X_1, X_2, \dots, X_n$, подчиняющихся вероятностному закону с плотностью

$$p(x|\theta) = \frac{2}{\pi} \sqrt{1 - (x - \theta)^2}, \quad |x - \theta| \leq 1,$$

оценить параметр сдвига θ , $|\theta| < \infty$.

В 1970 г. Л. Н. Большев предложил автору рассмотреть эту задачу, но в более общей постановке, а именно по реализациям независимых случайных величин $X_1, X_2, \dots, X_n$, распределение вероятностей которых принадлежит семейству $\{p_k(x|\theta)\}$, $|\theta| < \infty$,

$$p_k(x|\theta) = \begin{cases} \frac{\Gamma(2k)}{\Gamma(k)\Gamma(k)} \frac{1}{2^{k-1}} [1 - (x - \theta)^2]^{k-1}, & |x - \theta| \leq 1, \\ 0, & |x - \theta| > 1, \end{cases} \quad (1)$$

оценить параметр сдвига θ при условии, что k — заданное число из интервала $[1; 2]$. Семейство (1) является довольно богатым. В частности, при $k = 1$ оно содержит все равномерные распределения с носителями вида $\theta - 1 \leq x \leq \theta + 1$. При $k = 3/2$ (случай Д. Бернулли) график плотности $p_{3/2}(x|\theta)$ представляет собой верхнюю дугу эллипса с параметрами $a = 1$ и $b = 2/\pi$, так что в этом случае касательные к графику плотности в точках $x = \theta - 1$ и $x = \theta + 1$ перпендикулярны оси абсцисс. Предлагалось, следуя идеям Д. Бернулли, воспользоваться методом макси-

мального правдоподобия для получения наиболее правдоподобной оценки $\hat{\theta}$, которую для случая $k = 3/2$ и рекомендовал Д. Бернулли в работе [2].

Итак, пусть

$$L(\theta) = \prod_{i=1}^n p_k(X_i | \theta)$$

— функция правдоподобия, построенная по наблюдениям $X_1, X_2, \dots, X_n$, и пусть $\hat{\theta}$ — оценка максимального правдоподобия параметра θ , т. е. $L(\hat{\theta}) = \max_{|\theta| < \infty} L(\theta)$. Оценка $\hat{\theta}$ ищется при единственном условии совместимости: $\max_i |X_i - \theta| \leq 1$, т. е. $0 \leq X_{(n)} - X_{(1)} \leq 2$, где $X_{(1)} \leq X_{(2)} \leq \dots \leq X_{(n)}$ — вариационный ряд, построенный по наблюдениям $X_1, X_2, \dots, X_n$. Вместо $L(\theta)$ удобнее рассматривать $\ln L(\theta)$, причем

$$\ln L(\theta) = (k-1) \sum_{i=1}^n \ln [1 - (X_i - \theta)^2] + n \ln \frac{\Gamma(2k)}{\Gamma(k) \Gamma(k) 2^{2k-1}}. \quad (2)$$

Будем искать $\max \ln L(\theta)$ из уравнения:

$$\frac{d}{d\theta} \ln L(\theta) = 0. \quad (3)$$

Из уравнений (2) и (3) получаем уравнение:

$$\sum_{i=1}^n \frac{X_i - \theta}{1 - (X_i - \theta)^2} = 0. \quad (4)$$

Как видно, это уравнение не зависит от k . Решение его и есть оценка $\hat{\theta}$, которую предлагал Д. Бернулли. Можно показать, что $\hat{\theta}$ удовлетворяет соотношению:

$$\hat{\theta} = \frac{\sum_{i=1}^n \left\{ \frac{1}{1 - (X_i - \hat{\theta})^2} X_i \right\}}{\sum_{i=1}^n \frac{1}{1 - (X_i - \hat{\theta})^2}}. \quad (5)$$

Точнее говоря, уравнение (5) есть (4), разрешенное относительно θ . Соотношение (5) удобно использовать для нахождения $\hat{\theta}$ с помощью итераций. Далее, наряду с Бернулли задачу оценивания θ рассматривал также Эйлер [3], который вместо (5) предложил оценку θ^* , удовлетворяющую соотношению:

$$\theta^* = \frac{\sum_{i=1}^n \{ [1 - (X_i - \theta^*)^2] X_i \}}{\sum_{i=1}^n [1 - (X_i - \theta^*)^2]}. \quad (6)$$

Очевидно, что оценки Бернулли $\hat{\theta}$ и Эйлера θ^* отличаются тем, что в оценке Бернулли приписываются большие веса наблюдениям, которые близки к концам интервала $[\theta - 1; \theta + 1]$, в то время как в оценке Эйлера большие веса приписываются наблюдениям, лежащим около θ . Мне было предложено сравнить их с естественной оценкой $\bar{X}_n = (X_1 + \dots + X_n)/n$. В дальнейшем можно считать, что $\theta = 0$. В таком случае $\hat{\theta}$, θ^* и $\bar{X}_n$ суть оценки нуля.

2. Арифметическое среднее

Очевидно, что $EX_i = 0$, откуда следует, что $\bar{X}_n$ является несмещенной оценкой нуля, причем $DX_i = EX_i^2$. Чтобы вычислить DX_i , найдем EX_i^{2m} . Заметим, что $EX_i^{2m+1} = 0$ при любом натуральном m .

Итак, имеем ($\theta = 0$):

$$\begin{aligned} EX_i^{2m} &= \frac{\Gamma(2k)}{\Gamma(k)\Gamma(k)} \left(\frac{1}{2}\right)^{2k-1} \int_{-1}^1 x^{2m} (1-x^2)^{k-1} dx = \\ &= \frac{\Gamma(2k)!}{\Gamma(k)\Gamma(k)} \left(\frac{1}{2}\right)^{2k-1} B\left(m + \frac{1}{2}, k\right) = \frac{\Gamma(k)\Gamma\left(m + \frac{1}{2}\right)}{\Gamma(k)\Gamma\left(m + k + \frac{1}{2}\right)} \left(\frac{1}{2}\right)^{2k-1}. \end{aligned} \quad (7)$$

Из (7) получаем:

$$DX_i = EX_i^2 = \frac{\sqrt{\pi}}{2^{2k}} \frac{\Gamma(2k)}{\Gamma(k)\Gamma\left(k + \frac{3}{2}\right)}. \quad (8)$$

В частности, если $k = 3/2$, т. е. в случае, рассмотренном Бернулли и Эйлером, имеем $DX_i = 1/4$. Из (8) следует, что

$$D\bar{X}_n = \frac{1}{n} \frac{\sqrt{\pi}}{2^{2k}} \frac{\Gamma(2k)}{\Gamma(k)\Gamma\left(k + \frac{3}{2}\right)}, \quad (9)$$

откуда следует, что

$$\begin{aligned} D\bar{X}_n &= \frac{1}{3n} \quad \text{при } k = 1, \quad D\bar{X}_n = \frac{1}{4n} \quad \text{при } k = \frac{3}{2}, \\ D\bar{X}_n &= \frac{1}{5n} \quad \text{при } k = 2. \end{aligned} \quad (10)$$

Кроме того, согласно центральной предельной теореме, при любом $k \in [1; 2]$ и любом x

$$\lim_{n \rightarrow \infty} P \left\{ \bar{X}_n \leq x \sqrt{\frac{1}{n} \frac{\sqrt{\pi}}{2^{2k}} \frac{\Gamma(2k)}{\Gamma(k)\Gamma\left(k + \frac{3}{2}\right)}} \right\} = \Phi(x),$$

где $\Phi(x)$ — функция распределения стандартного нормального закона.

3. Оценка Эйлера θ^* ($\theta = 0$)

Из (6) имеем:

$$\begin{aligned} \theta^* \sum_{i=1}^n [(1 - X_i^2) + 2X_i\theta^* - \theta^{*2}] &= \\ &= \sum_{i=1}^n \{[(1 - X_i)^2 + 2X_i\theta^* - \theta^{*2}] X_i\}. \end{aligned} \quad (11)$$

Обозначим $\bar{X}_n^k = \frac{1}{n} \sum_{i=1}^n X_i^k$. Очевидно, что $P. \lim_{n \rightarrow \infty} \bar{X}_n = 0$ и

$P. \lim_{n \rightarrow \infty} \bar{X}_n^3 = 0$ и, кроме того, ($\theta = 0$)

$$P. \lim_{n \rightarrow \infty} \bar{X}_n^2 = EX_i^2 = \begin{cases} \frac{1}{3}, & \text{если } k = 1, \\ \frac{1}{4}, & \text{если } k = \frac{3}{2}, \\ \frac{1}{5}, & \text{если } k = 2. \end{cases} \quad (12)$$

Здесь $P. \lim_{n \rightarrow \infty} \bar{X}_n = 0$ означает, что $\bar{X}_n$ сходится к 0 по вероятности, т. е. для любых положительных ε и δ найдется такое $n_0(\varepsilon, \delta)$, что для всех $n > n_0(\varepsilon, \delta)$ выполняются неравенства:

$$P\{|\bar{X}_n^2| < \delta\} > 1 - \varepsilon. \quad (13)$$

Уравнение (13) есть уравнение третьей степени, поэтому имеется по крайней мере один вещественный корень. Так как из (12) следует, что

$$P. \lim_{n \rightarrow \infty} (1 - 3\bar{X}_n^2) = 1 - 3EX_i^2 \geq 0,$$

то, переходя в (13) к пределу по n , получим уравнение:

$$(1 - 3EX_i^2) \tilde{\theta}^* = (\tilde{\theta}^*)^2,$$

корни которого суть:

$$\tilde{\theta}_1^* = 0, \quad \tilde{\theta}_2^* = \sqrt{1 - 3EX_i^2}, \quad \tilde{\theta}_3^* = -\sqrt{1 - 3EX_i^2}, \quad (14)$$

т. е. $\tilde{\theta}_i^*$ не являются случайными.

Очевидно, что интересующие нас корни θ_i^* уравнения (12) лежат не очень далеко от корней $\tilde{\theta}_i^*$, так как $P. \lim \theta_i^* = \tilde{\theta}^*$. Возвращаясь еще раз к уравнению (13), получаем:

$$\sqrt{n} \tilde{\theta}_1^* = \frac{\sqrt{n} [(\bar{X}_n - \bar{X}_n^3) - 3\bar{X}_n \theta_1^{*2}]}{1 - 3\bar{X}_n^2 - \theta_1^{*2}}. \quad (15)$$

Очевидно, что числитель (15) асимптотически нормально распределен с нулевым средним и дисперсией $E(X_i - X_i^3)^2$, в то время как

$$P. \lim_{n \rightarrow \infty} (1 - 3\bar{X}_n^2 - \theta_1^{*2}) = 1 - 3EX_i^2 = \begin{cases} 0, & \text{если } k = 1, \\ \frac{1}{4}, & \text{если } k = \frac{3}{2}, \\ \frac{2}{5}, & \text{если } k = 2. \end{cases} \quad (16)$$

Итак, если $k = 1$, то

$$\theta_1^* = \sqrt[3]{-\bar{X}_n + \bar{X}_n^3 + 3\bar{X}_n\theta_1^{*2} + \theta_1^*(1 - 3\bar{X}_n^2)},$$

откуда

$$n^{1/6}\theta_1^* = \sqrt[3]{-\sqrt{n}(\bar{X}_n - \bar{X}_n^3) + 3\theta_1^{*2}\sqrt{n}\bar{X}_n + \sqrt{n}(1 - 3\bar{X}_n^2)\theta_1^*}.$$

Учитывая, что $P. \lim_{n \rightarrow \infty} \theta_1^* = 0$, $P. \lim_{n \rightarrow \infty} \theta_1^{*2} = 0$, получаем:

$$P. \lim_{n \rightarrow \infty} \theta_1^{*2}\sqrt{n}\bar{X}_n = 0, \quad P. \lim_{n \rightarrow \infty} \sqrt{n}(1 - 3\bar{X}_n^2)\theta_1^* = 0$$

и, следовательно, имеем:

$$\begin{aligned} \lim_{n \rightarrow \infty} P\{n^{1/6}\theta_1^* < x\} &= \lim_{n \rightarrow \infty} P\{\sqrt{n}\theta_1^{*3} < x^3\} = \\ &= \lim_{n \rightarrow \infty} P\{-\sqrt{n}(\bar{X}_n - \bar{X}_n^3) < x^3\} = \Phi\left(\frac{x^3}{\sqrt{E(X_i - X_i^3)^2}}\right). \end{aligned} \quad (17)$$

Учитывая, что $E(X_i - X_i^3)^2 = EX_i^2 - 2EX_i^4 + EX_i^6$, из (7) получаем:

$$E(X_i - X_i^3)^2 = \begin{cases} \frac{8}{105}, & \text{если } k = 1, \\ \frac{5}{64}, & \text{если } k = \frac{3}{2}, \\ \frac{8}{105}, & \text{если } k = 2. \end{cases} \quad (18)$$

Таким образом, из (17) и (18) следует, что при $k = 1$ статистика $n^{1/6}\theta_1^*$ асимптотически распределена при $n \rightarrow \infty$ как корень кубический из нормально распределенной случайной величины с нулевым средним и дисперсией $8/105$. Отсюда с помощью (16) сразу же вытекает:

$$E(n^{1/6}\theta_1^*)^2 = n^{1/3}E\theta_1^{*2} \cong 3 \sqrt{\frac{105}{8}} \int_{-\infty}^{\infty} \frac{1}{\Phi}\left(\sqrt{\frac{105}{8}}x^3\right) x^4 dx < \infty,$$

т. е. при $k = 1$

$$E\theta_1^{*2} = O\left(\frac{1}{n^8}\right). \quad (19)$$

Здесь $\Phi(x) = \Phi'(x)$.

Если же $1 < k \leq 2$, то $E(1 - 3X_i^2) > 0$ и статистика $\sqrt{n} \theta_1^*$ асимптотически нормально распределена при $n \rightarrow \infty$ с нулевым средним и стандартным отклонением $\sqrt{E(X_i - X_i^3)^2 / E(1 - 3X_i^2)}$. В частности, из (16) и (18) получаем:

$$\frac{\sqrt{E(X_i - X_i^3)^2}}{1 - 3EX_i^2} = \begin{cases} \frac{\sqrt{5/64}}{1/4} = \frac{\sqrt{5}}{2}, & \text{если } k = 3/2, \\ \frac{\sqrt{8/105}}{2/5} = \sqrt{10/21}, & \text{если } k = 2. \end{cases} \quad (20)$$

Сравнив (20) и (10), получим, что в случаях $k = 3/2$ и $k = 2$ оценка $\bar{X}_n$ лучше оценки θ_1^* Эйлера (в смысле минимума квадратичного риска). В случае же $k = 1$ оценка Эйлера лучше оценки $\bar{X}_n$, что вполне естественно, ибо при $k = 1$ имеем равномерное распределение.

4. Оценка $\hat{\theta}$ Бернулли (наиболее правдоподобная оценка)

Очевидно, что $X_{(n)} - 1 \leq \hat{\theta} \leq X_{(1)} + 1$, причем если $1 \leq k \leq 2$, то $L(X_{(n)} - 1) = L(X_{(1)} + 1) = 0$. Рассмотрим оценку $T = 1/2 (X_{(1)} + X_{(n)})$. Очевидно, что $ET = 0$ и, кроме того,

$$DT = 2 \left[\frac{\Gamma(k) \Gamma(k+1)}{\Gamma(2k)} \right]^{2/k} \left[\Gamma\left(\frac{2}{k} + 1\right) - \Gamma^2\left(\frac{1}{k} + 1\right) \right] \times \\ \times \frac{1}{n^{2/k}} (1 + o(1)). \quad (21)$$

Из (21) следует, что при больших n

$$DT \sim \begin{cases} 2/n^2, & \text{если } k = 1, \\ 1/18 (3\pi/2)^{4/3} [\Gamma(1/3) - \Gamma^2(2/3)] n^{-4/3}, & \text{если } k = 3/2, \\ 2/3 (1 - \pi/4) 1/n, & \text{если } k = 2. \end{cases} \quad (22)$$

Так как $DX_{(n)} = DX_{(1)} = O(n^{-2/k})$, то $D\hat{\theta} = O(n^{-2/k})$. Учитывая это, а также сравнивая (22) и (10), приходим к выводу, что оценка $\hat{\theta}$ Бернулли лучше оценок $\bar{X}_n$ и θ_1^* . Очевидно, что при $1 \leq k \leq 2$ разумно пользоваться простой оценкой $T = (X_{(1)} + X_{(n)})/2$.

5. Равномерное распределение

Сначала остановимся на случае $k = 1$, когда $X_1, X_2, \dots, X_n$ — независимые случайные величины, равномерно распределенные на интервале $\theta - 1 \leq x \leq \theta + 1$, $|\theta| < \infty$. В этом случае в качестве оценки параметра θ нужно взять (см., [5 — 8]) ста-

тистику Ллойда [4] $T = (X_{(1)} + X_{(n)})/2$, которая является несмещенной оценкой для θ , причем

$$DT = \frac{2}{(n+1)(n+2)}.$$

Теперь сделаем замечание к случаю, когда $X_1, X_2, \dots, X_n$ суть независимые случайные величины, равномерно распределенные на интервале $[-\theta; \theta]$, $\theta > 0$. Здесь θ является параметром масштаба, а плотность вероятности случайной величины X_i есть

$$p(x|\theta) = \begin{cases} 1/2\theta, & |x| \leq \theta, \\ 0, & |x| > \theta. \end{cases}$$

В статистической литературе (см., например, [4—8]) в качестве оценки параметра масштаба θ рекомендуется выбрать статистику

$$W = \frac{n+1}{2(n-1)} (X_{(n)} - X_{(1)}),$$

которая является несмещенной оценкой для θ , причем

$$DW = \frac{2\theta^2}{(n-1)(n+2)}.$$

Статистика W есть функция от достаточной статистики $(X_{(1)}, X_{(n)})$, которая не является полной статистикой в задаче оценивания параметра масштаба θ . В связи с этим рассмотрим следующую процедуру. Пусть $Y_1 = |X_1|$, $Y_2 = |X_2|$, ..., $Y_n = |X_n|$. Очевидно, что $Y_1, Y_2, \dots, Y_n$ суть независимые случайные величины, равномерно распределенные на интервале $[0; \theta]$. Далее, пусть $Y_{(1)} \leq Y_{(2)} \leq \dots \leq Y_{(n)}$ — вариационный ряд, построенный по случайным величинам $Y_1, Y_2, \dots, Y_n$. Очевидно, что $Y_{(n)}$ — полная достаточная статистика в задаче оценивания параметра масштаба θ , причем плотность вероятности $h(y)$ статистики $Y_{(n)}$ задается формулой:

$$h(y) = \begin{cases} ny^{n-1}\theta^{-n}, & \text{если } 0 \leq y \leq \theta, \\ 0, & \text{в противном случае.} \end{cases}$$

Ясно также, что $Y_{(n)} = \max(|X_{(1)}|, |X_{(n)}|)$. Легко убедиться в том, что $EY_{(n)} = n/(n+1) \theta$, откуда следует, что несмещенной оценкой для параметра масштаба θ будет статистика:

$$t = \frac{n+1}{n} Y_{(n)} = \frac{n+1}{n} \max(|X_{(1)}|, |X_{(n)}|),$$

причем

$$Dt = Et^2 - (Et)^2 = \frac{\theta^2}{n(n+2)}.$$

Сравнивая дисперсии Dt и DW оценок t и W , получаем:

$$\frac{Dt}{DW} = \frac{n-1}{2n} = \frac{1}{2} \left(1 - \frac{1}{n}\right),$$

т. е. дисперсия Dt нелинейной (как функции от порядковых статистик $X_{(1)}, X_{(2)}, \dots, X_{(n)}$) несмещенной оценки t почти в 2 раза меньше дисперсии оценки W .

В заключение отметим, что основные результаты сообщения неоднократно приводились Л. И. Большевым и автором во время чтения лекций по математической статистике, обсуждались с коллегами на семинарах.

Литература

1. *Kendall M. G.* Studies in the history of probability and statistics. XI. Daniel Bernoulli on maximum likelyhood//*Biometrika*. 1961. Vol. 48, N 1, 2. P. 1—18.
2. *Bernoulli D.* The most probable choice between several discrepant observations and the formation therefrom of the most likely induction//*Biometrika*. 1961. Vol. 48, N 1, 2. P. 3—13.
3. *Euler L.* Observations on the foregoing dissertation of Bernoulli//*Biometrika*. 1961. Vol. 48, N 1, 2. P. 13—18.
4. *Lloyd E. H.* Least-squares estimation of location and scale parameters using order statistics//*Biometrika*. 1952. Vol. 39. P. 88—95.
5. *Кендалл М. Дж., Стьюарт А.* Статистические выводы и связи. М., 1973.
6. *Дейвид Г.* Порядковые статистики. М., 1979.
7. *Закс Ш.* Теория статистических выводов. М., 1975.
8. *Рао С. Р.* Линейные статистические методы и их применения. М., 1968.

СТАТИСТИЧЕСКИЙ АНАЛИЗ ОДНОЙ ФИЗИЧЕСКОЙ МОДЕЛИ, ИСПОЛЪЗУЕМОЙ В СПЕКТРОСКОПИИ

Повышение разрешающей способности спектральных приборов является одной из актуальнейших задач экспериментальной физики. Хорошо известно, что спектральные линии уширяются благодаря затуханию колебаний атомов, их беспорядочному тепловому движению, столкновениям между собой, приводящим к срыву колебаний, и влиянию аппаратной функции прибора. При этом математическое описание процесса расширения линии одно и то же и при классическом и при квантово-механическом подходах.

Пренебрегая очень малым в видимой части спектра естественным уширением линий, обусловленным затуханием колебаний атомов (неопределенностью в энергии стационарных состояний при квантово-механическом описании), можно выделить три основных эффекта, подлежащих тщательному изучению: а) доплеровское уширение, сопровождающее излучение атомов, находящихся в тепловом движении, б) лоренцево уширение, обусловленное взаимодействием атомов, и в) уширение, связанное с аппаратной функцией прибора [1].

Наблюдаемая на выходе спектроскопа линия возникает в результате совместного действия всех этих факторов, что затрудняет извлечение информации об исходном спектре, т. е. понижает разрешающую способность системы. Однако статистическая обработка результатов наблюдений может ее повысить. Так, статистическими методами проверки гипотез можно выбрать теоретическую модель уширения линий, адекватную эксперименту, и оценить параметры этой модели. Это позволит при решении обратной задачи аккуратнее выделить полезную информацию. Знание параметров модели уширения линий позволяет не только находить физические параметры пламени спектроскопа (концентрацию электронов, постоянную ван-дер-ваальсовского взаимодействия и др.), но и конструировать более совершенные приборы.

Эта работа посвящена задаче статистического разделения эффектов, обусловленных доплеровским, лоренцевым и аппаратными уширениями линий в рамках одной физической модели спектро-

скопа, а также построению статистического критерия для проверки согласия выбранной модели с экспериментальными данными.

1. Математической моделью линейного физического эксперимента, как правило, служит интегральное преобразование:

$$(Tu)(x) = \int_{-\infty}^{\infty} k(x-y)u(y)dy \quad (1)$$

полезного «сигнала» u в наблюдаемый Tu .

Физический смысл ядра преобразования k раскрывается при подстановке вместо u функции δ ($T\delta$)(x) = $k(x)$. Так, в оптическом эксперименте $k(x)$ характеризует распределение яркости изображения точечного источника, которое, вообще говоря, уже не является точечным. Ядро $k(x)$ называется импульсной переходной функцией преобразования, а если преобразование осуществляется прибором — аппаратной функцией этого прибора. Очевидно, при последовательно осуществляемых преобразованиях вида (1) импульсная переходная функция композиции будет представлять собой свертку переходных функций компонент. Предположим, что экспериментатор имеет гипотезу H_0 относительно вида переходной функции $k = f * g * h$ спектрального прибора, согласно которой

$$f(x|a, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{(x-a)^2}{2\sigma^2}\right\}, \quad \begin{matrix} |x| < \infty, \\ |a| < \infty, \sigma > 0 \end{matrix} \quad (2)$$

отражает доплеровское уширение спектральных линий, всегда сопровождающее излучение атомов, находящихся в тепловом движении,

$$g(x|b, L) = \frac{1}{\pi L} \frac{1}{1 + \frac{(x-b)^2}{L^2}}, \quad |x| < \infty, |b| < \infty, L > 0 \quad (3)$$

характеризует их лоренцево уширение, обусловленное взаимодействием атомов, а

$$h(x|c, R) = \frac{|1-R^2|}{2\pi} \frac{1}{1-2R\cos(x-c)+R^2}, \quad \begin{matrix} |x| < \infty, \\ |c| < \infty, |R| < \infty \end{matrix} \quad (4)$$

является аппаратной функцией, характерной для периодической структуры — дифракционной решетки (см., например, [2]).

Пусть H_0 верна. Поставим задачу статистического разделения этих трех эффектов, ведущего к повышению разрешающей способности прибора.

З а м е ч а н и е 1. Так как $h(x|c, R) = h(x|c + \pi, -R)$ и при $R = 0$ $h(x|c, R) = h(x|c, \frac{1}{R})$, то без ограничения общности

можно считать, что $0 \leq R \leq 1$. При таком предположении (4) принимает вид:

$$h(x|c, R) = \frac{1-R^2}{2\pi} \frac{1}{1-2R \cos(x-c) + R^2},$$

$$|x| < \infty, \quad |c| < \infty, \quad 0 \leq R \leq 1.$$

Замечание 2. Если $R = 1$, то функцию (4) естественно считать суммой δ -функций Дирака:

$$h(x|c, 1) = \sum_{m=-\infty}^{+\infty} \delta(x - c - 2m\pi).$$

Замечание 3. Функции f и g можно рассматривать как плотности вероятностей на числовой прямой $|x| < \infty$; точно так же h — плотность вероятности на отрезке $-\pi \leq x \leq \pi$.

Замечание 4. Рассмотрим свертку $J(x|b, c; L, R)$ функций g и h на единичной окружности:

$$J(x|b, c; L, R) = \int_{-\infty}^{\infty} g(y|b, L) h(x-y|c, R) dy.$$

Пользуясь определением (4), можно убедиться в справедливости формулы:

$$J(x|b, c; L, R) = h(x|b+c, Re^{-L}). \quad (5)$$

2. Пусть $I(x|a, b, c; \sigma, L, R)$ — тройная свертка функций f , g и h на единичной окружности. Так как $I = f * g * h = f * (g * h) = f * J$, а $J = g * h$ выражается в терминах h (см. (5)), то достаточно исследовать свертку $f * h$. Из формул (2) и (4) имеем:

$$f * h = \int_{-\infty}^{\infty} f(y|a, \sigma) h(x-y|c, R) dy.$$

Эта функция периодична с периодом 2π . Ее разложение в ряд Фурье имеет вид:

$$f * h = \frac{1}{2\pi} + \frac{1}{\pi} \sum_{n=1}^{\infty} R^n e^{-n^2 \sigma^2 / 2} \cos[n(x-a-c)]. \quad (6)$$

Отсюда и из формулы (5) следует, что ряд Фурье для тройной свертки $f * g * h$ получится из формулы (6) в результате замены c на $b+c$ и R — на Re^{-L} :

$$I(x|a, b, c; \sigma, L, R) = f * g * h =$$

$$= 1/2\pi + 1/\pi \sum_{n=1}^{\infty} (Re^{-L})^n e^{-n^2 \sigma^2 / 2} \cos[n(x-a-b-c)]. \quad (7)$$

3. Из формулы (7) следует, что при справедливости гипотезы H_0 по экспериментальным реализациям I функции I можно оценить лишь функции от параметров: $a+b+c$, σ и Re^{-L} .

Для разделения этих параметров, т. е. для оценки каждой из величин a, b, c, R, L в отдельности, нужны специальные эксперименты.

Предположим, что сумма $a + b + c$ известна. Полагая $y = x - a - b - c$, получим из (7) новую функцию:

$$I_0(y|\sigma, L, R) = \frac{1}{2\pi} + \frac{1}{\pi} \sum_{n=1}^{\infty} (Re^{-L})^n e^{-n^2\sigma^2/2} \cos(ny)$$

и соответствующую ей экспериментальную реализацию:

$$\hat{I}_0 = \hat{I}_0(y + a + b + c).$$

Пусть $c_0, c_1, c_2, \dots$ — коэффициенты Фурье для функции $\hat{I}_0$, т. е.

$$\hat{I}_0(y) = \frac{c_0}{2\pi} = \frac{1}{\pi} \sum_{n=1}^{\infty} c_n \cos(ny). \quad (8)$$

В таком случае, полагая $\alpha = \log(Re^{-L})$ и $\beta = \log e^{-\sigma^2/2}$, а также $l_k = \log c_k$, имеем:

$c_0 = 1 + \xi_0$, $c_k = (Re^{-L})^k (e^{-\sigma^2/2})^{k^2} (1 + \xi_k)$, $k = 1, 2, \dots, n$,
(в виде множителей $1 + \xi_k$ записаны случайные погрешности, возникающие из-за ошибок эксперимента), или после логарифмирования и сохранения лишь главных членов от $\log(1 + \xi_k)$:

$$l_0 = \log c_0 = \xi_0,$$

$$l_k = \log c_k = k\alpha + k^2\beta + \xi_k, \quad k = 1, 2, \dots, n.$$

Предположим, что все ξ_i независимы, распределены одинаково и имеют нулевые средние значения (последнее предположение означает, что систематические ошибки отсутствуют). В этом случае для оценки неизвестных α и β разумно воспользоваться методом наименьших квадратов. Приближенные значения $\hat{\alpha}$ и $\hat{\beta}$ для неизвестных α и β по этому методу определяются как решение системы уравнений:

$$\begin{aligned} \sum_{k=1}^n kl_k &= \hat{\alpha} \sum_{k=1}^n k^2 + \hat{\beta} \sum_{k=1}^n k^3, \\ \sum_{k=1}^n k^2 l_k &= \hat{\alpha} \sum_{k=1}^n k^3 + \hat{\beta} \sum_{k=1}^n k^4. \end{aligned}$$

В явном виде это решение выражается формулами:

$$\begin{aligned} \hat{\alpha} &= \frac{12 [2(2n+1)(3n^2+3n-1)\lambda_1 - 15n(n+1)\lambda_2]}{n(n^2-1)(n+2)(3n^2+3n+2)}, \\ \hat{\beta} &= \frac{60 [-3n(n+1)\lambda_1 + 2(2n+1)\lambda_2]}{n(n^2-1)(n+2)(3n^2+3n+2)}, \end{aligned} \quad (9)$$

где

$$\lambda_1 = \sum_{k=1}^n kl_k, \quad \lambda_2 = \sum_{k=1}^n k^2 l_k.$$

Как случайные величины оценки $\hat{\alpha}$ и $\hat{\beta}$ ведут себя следующим образом:

а) они лишены систематических погрешностей: $E\hat{\alpha} = \alpha$, $E\hat{\beta} = \beta$;

б) их дисперсии (квадраты средних квадратичных уклонений) выражаются формулами:

$$E(\hat{\alpha} - \alpha)^2 = \frac{24(2n+1)(3n^2+3n-1)\sigma^2}{n(n^2-1)(n+2)(3n^2+3n+2)}, \quad \left(= O\left(\frac{1}{n^3}\right)\right),$$

$$E(\hat{\beta} - \beta)^2 = \frac{120(2n+1)\sigma^2}{n(n^2+1)(n+2)(3n^2+3n+2)}, \quad \left(= O\left(\frac{1}{n^5}\right)\right).$$

Кроме того,

$$E(\hat{\alpha} - \alpha)(\hat{\beta} - \beta) = -\frac{180n(n+1)\sigma^2}{n(n^2-1)(n+2)(3n^2+3n+2)}, \quad \left(= O\left(\frac{1}{n^4}\right)\right).$$

Здесь $\sigma^2 = E\xi_k^2$ — дисперсия случайных ошибок эксперимента.

Для оценки неизвестного σ^2 можно воспользоваться формулой:

$$\sigma^2 \approx \hat{\sigma}_1^2 = \frac{1}{n-2} \sum_{k=1}^n (l_k - k\hat{\alpha} - k^2\hat{\beta})^2.$$

4. Проверим согласие теоретической формулы и эксперимента. Для проверки гипотезы H_0 вычислим еще несколько коэффициентов Фурье для эмпирической формулы (8), например $c_{n+1}, \dots, c_{n+m}$. Рассмотрим разности:

$$\begin{aligned} \Delta_{n+r} &= \log c_{n+r} - (n+r)\hat{\alpha} - (n+r)^2\hat{\beta} = \\ &= l_{n+r} - (n+r)\hat{\alpha} - (n+r)^2\hat{\beta}, \quad r = 1, 2, \dots, m, \end{aligned}$$

где $\hat{\alpha}$ и $\hat{\beta}$ — ранее вычисленные оценки по формуле (9) (без использования $c_{n+1}, c_{n+2}, \dots, c_{n+m}$). Пусть $A = \|a_{ij}\|$ — квадратная матрица, элементы которой суть $a_{ij} = 1/\sigma^2 E\Delta_{n+i}\Delta_{n+j}$, $i, j = 1, 2, \dots, m$. В таком случае квадратичная форма $\Delta^T A^{-1} \Delta$, где $\Delta = (\Delta_{n+1}, \Delta_{n+2}, \dots, \Delta_{n+m})^T$, может быть использована для построения нового приближенного значения для σ^2 :

$$\sigma^2 \approx \hat{\sigma}_2^2 = \frac{1}{m+1} (\Delta^T A^{-1} \Delta + l_0^2),$$

где $l_0 = \log c_0$.

Отношение

$$\frac{\hat{\sigma}_1^2}{\hat{\sigma}_2^2} = \frac{(m+1) \sum_{k=1}^n (l_k - k\hat{\alpha} - k^2\hat{\beta})^2}{(n-1) (\Delta^T A^{-1} \Delta + l_0^2)} = F$$

может быть использовано как статистика критерия в задаче проверки гипотезы H_0 . Статистика F при справедливости H_0 , т. е. в случае согласия теории и эксперимента, распределена по закону F с $n-2$ и $m+1$ степенями свободы (см., например, [3]).

В заключение автор выражает признательность В. Г. Воинову за полезные советы при подготовке настоящей работы.

Литература

1. Фриш С. Э. Оптические спектры атомов. М., Л., 1963.
2. Фриш С. Э. Техника спектроскопии. Л., 1936.
3. Никулин М. С. F-распределение, его свойства и связь с другими вероятностными распределениями // Мардиа К., Земрош П. Таблицы F-распределений и распределений, связанных с ними. М., 1984.

БИНОМИАЛЬНАЯ АСИМПТОТИКА

1. Постановка задачи

Под системой (a, b) в дальнейшем понимается упорядоченная система двух образующих коммутативного кольца A с единицей e , а под состоянием c_N^n — произведение $a^{N-n}b^n$, где $0 \leq n \leq N$. Разрежение кратности k означает переход к системе (a^k, b^k) . Рассматривая N как дискретное время, будем называть эволюцией всякую начинающуюся с e последовательность состояний, каждое из которых получается умножением предшествующего на a или b .

Поскольку любое из этих двух умножений порождает поток сдвигов пространства состояний, эволюцию можно интерпретировать как траекторию динамической системы, попеременно управляемой двумя данными потоками. Переходы такой системы удобно представлять сетью Паскаля—Гальтона (рис. 1), а эволюцию — бесконечной ломаной, исходящей из вершины сети (рис. 2). Если в нарушение симметрии эволюцию a^N считать эталонной, а b^N — возмущенной, то произвольную эволюцию следует трактовать как возмущаемую, вообще говоря, беспорядочными сбоями вида $d = b - a$.

Здесь нас будут интересовать эволюции, которые при больших значениях N оказываются в определенном смысле нечувствительными к сбоям. В связи с этим отправной объект изучения — вариацию v_N^n — определим как разность соседних положений подвижного конца N -звенной ломаной: $v_N^n = c_N^n - c_N^{n-1}$ ($1 \leq n \leq N$). Чтобы иметь возможность судить об асимптотическом поведении

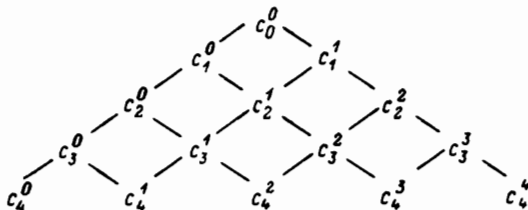


Рис. 1. Пространство состояний.

эволюции при возрастании N , будем предполагать, что в A задана кольцевая преднорма, т. е. ненулевое отображение $a \rightarrow |a|$ кольца A в $\mathbb{R}$, для которого при любых a и b из A и целых неотрицательных n выполнены условия:

$$|a - b| \leq |a| + |b|, \quad |ab| \leq |a| |b|, \quad |na| = n|a|.$$

Стандартным рассуждением устанавливаются такие свойства преднормы, как неотрицательность, симметричность, неравенство $1 \leq |e|$ и оба неравенства треугольника.

Всюду ниже β — фиксированное положительное число и $s = 1 + \beta$. По определению, система (a, b) устойчива, если ограничена двойная последовательность $N^s |v_N^a|$. Подобное стягивание сети переходов (рис. 3) влечет «конфинальность» всех эволюций и, в частности, содержит в себе требование ограниченности последовательности $N^s |v_N^a|$. Это (более слабое по сравнению с устойчивостью системы) условие устойчивости эволюции a^N означает ее достаточно быстрое сближение с эволюцией $a^{N-1}b$, получаемой из эталонной единичным сбоем. Из устойчивости эталонной эволюции a^N в свою очередь вытекает конечность суммы $S = \sum_N |v_N^a|$.

В основе следующего определения — некоторое усиление отмеченного свойства: будем считать, что система подчинена условию захвата, если эта сумма строго меньше единицы. Эти условия так или иначе характеризуют скорость убывания вариации со временем. Более подробную информацию о поведении эволюций при больших N можно будет извлечь из разложения вариации по степеням возмущения d , если, конечно, это разложение окажется асимптотическим. Напомним соответствующее определение. Пусть

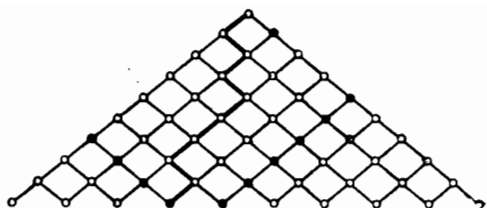


Рис. 2. Эволюция.

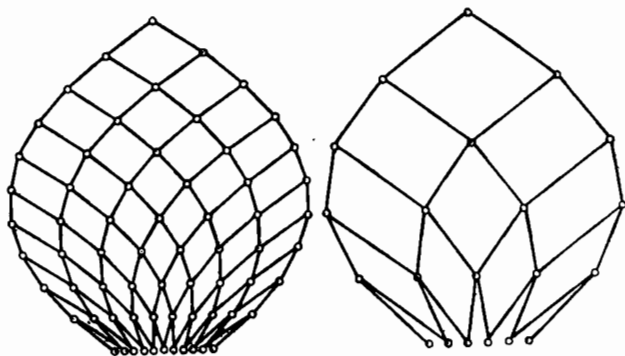


Рис. 3. Фрагмент устойчивой системы до и после разрезания.

X — произвольное направленное множество, $a(x)$, $a_p(x)$ ($p = 1, 2, \dots$) — функции на X со значениями в A . Выражения $a(x) \sim a_p(x)$ образуют последовательность асимптотических формул относительно шкалы сравнения $H_p(x)$ ($x \in X$), если можно указать числовую последовательность C_p такую, что при любом фиксированном p $|a(x) - a_p(x)| \leq C_p H_p(x)$ равномерно по $x \in X$. Соотношение

$$a(x) \sim \sum_{r \geq 0} b_r(x),$$

где $b_r(x)$ — также A -значные функции на X , называется асимптотическим разложением в шкале $H_p(x)$, если выражения

$$a(x) \sim \sum_{r=0}^{p-1} b_r(x)$$

образуют последовательность асимптотических формул относительно этой шкалы.

В задачу работы входит выявление связи между устойчивостью системы и возможностью асимптотического представления эволюции комбинациями высоких степеней эталонного элемента (предполагаемых доступными вычислению) и начальных степеней либо возмущения d , либо собственно элемента b в зависимости от того, что удобнее в конкретном приложении. Кроме того, работа ставит целью найти признак устойчивости и асимптотической представимости, не требующий вычисления неограниченно растущих степеней возмущенного элемента b или возмущения d .

Приведем основной результат, доказательство которого, разбитое для удобства на ряд промежуточных утверждений, излагается в последующих разделах.

Т е о р е м а. Равносильны следующие утверждения:

- а) система устойчива;
- б) эталонная эволюция устойчива и после некоторого разрежения оказывается выполненным условие захвата;
- в) при $0 \leq m \leq n \leq N$ и $N \rightarrow \infty$ соотношение

$$c_N^n - c_N^m \sim \sum_{r \geq 0} \left(\binom{n}{r} - \binom{m}{r} \right) d^r a^{N-r}$$

является асимптотическим разложением в шкале $(n - m) N^{-1-\beta p}$, в частности (для $m = 0$, $n = N$) биномиальное разложение

$$b^N \sim \sum_{r \geq 0} \binom{N}{r} d^r a^{N-r}$$

является асимптотическим в шкале $N^{-\beta p}$ («ньютонова» асимптотика);

г) при $0 \leq m \leq n \leq N$ и $N \rightarrow \infty$ выражения

$$c_N^n - c_N^m \sim \sum_{r=0}^{p-1} \left(\prod_{q=0}^{p-1} \frac{n-q}{r-q} - \prod_{q=0}^{p-1} \frac{m-q}{r-q} \right) c_N^r$$

(дроби с нулевым знаменателем заменяются единицей) образуют последовательность асимптотических формул относительно шкалы $(n - m) N^{-1-\beta p}$, в частности (для $m = 0$, $n = N$) выражения

$$b^N \sim \sum_{r=0}^{p-1} c_N^r \prod_{q=0}^{p-1} \frac{N-q}{r-q}$$

образуют последовательность асимптотических формул относительно шкалы $N^{-\beta p}$ («лагранжева» асимптотика).

Таким образом, искомый признак входит в теорему в качестве условия б) — одновременно необходимого и достаточного.

В следующем разделе безотносительно к перечисленным здесь условиям проводятся построения предварительного характера.

2. Алгебра Винера—Лорана

Обозначим через FA алгебру формальных степенных рядов

$$F(X) = \sum_r a_r X^{-r} \quad (r \in \mathbb{Z}, a_r \in A)$$

над кольцом A , состоящую из рядов с конечным числом ненулевых коэффициентов при положительных степенях X и обладающую единицей $E = eX^0$.

Предложение 1. Справедливы следующие утверждения:

а) при любом a из A элемент $eX - aE$ алгебры FA обратим, причем произвольная натуральная степень обратного элемента R_a имеет вид:

$$R_a^n = R^n(a; X) = \sum_{r \geq 0} \binom{r+n-1}{n-1} a^r X^{-r-n}; \quad (1)$$

б) при любом b из A элемент R_b алгебры FA допускает представление

$$R_b = R_b(X) = R(b; X) = R(b^k; X^k) \sum_{r=1}^k b^{k-r} X^{-r-1} \quad (2)$$

с произвольным натуральным параметром k ;

в) для любых a и b из A имеет место «резольвентное тождество» $R_a - R_b = (a - b) R_a R_b$;

г) семейство $R_a (dR_a)^r$ ($r = 0, 1, 2, \dots$) элементов алгебры FA суммируемо к элементу R_b .

Доказательство.

а) Непосредственная проверка умножением показывает, что

$$(eX - aE) R_a = (eX - aE) \sum_{r \geq 0} a^r X^{-r-1} = E,$$

т. е. $R_a = (eX - aE)^{-1}$; далее, согласно известному свойству биномиальных коэффициентов,

$$\begin{aligned}(eX - aE) R_a^{n+1} &= (eX - aE) \sum_{r \geq 0} \binom{r+n}{n} a^r X^{-r-n-1} = \\ &= \sum_{r \geq 0} \left(\binom{r+n}{n} - \binom{r+n-1}{n} \right) a^r X^{-r-n} = R_a^n,\end{aligned}$$

т. е. для произвольного натурального n $R_a R_a^n = R_a^{n+1}$ и $(R_a)^n = R_a^n$.

б) Чтобы убедиться в справедливости равенства, достаточно умножить на $eX - bE$ его правую часть:

$$R(b^k; X^k) \left(\sum_{r=1}^k b^{k-r} X^{r-1} \right) (eX - bE) = R(b^k; X^k) (eX^k - b^k E) = E.$$

в) К резольвентному тождеству приходим, умножая на $R_a R_b$ обе части равенства $R_b^{-1} - R_a^{-1} = (a - b) E$.

г) Записывая резольвентное тождество в виде $R_b = R_a + dR_a R_b$, а затем итерируя его, находим разложение:

$$R_b = \sum_{r=0}^{q-1} (dR_a)^r R_a + (dR_a)^q R_b.$$

Заметив, что порядок формального ряда R_a^q равен q , делаем вывод о суммируемости семейства $(dR_a)^r R_a$ к элементу R_b .

Предложение 2. Пусть $F_{ab} = R_a^{-1} R_b$, $F_{ba} = R_b^{-1} R_a$, a и n — произвольные натуральные числа. Выполнено тождество

$$\begin{aligned}\sum_{k \geq 0} \binom{k+n-1}{n-1} \left(b^k - \sum_{r=0}^{m-1} \binom{k}{r} d^k a^{k-r} \right) X^{-k-n} = \\ = d^m R_a^{m+n} F_{ab}^n T_{nm}(F_{ba}),\end{aligned}$$

в котором $T_{nm}(X)$ — полином, определяемый формулой:

$$T_{nm}(X) = \sum_{r=0}^{n-1} \binom{r+m-1}{m-1} X^r.$$

Доказательство. Будем рассматривать каждую траекторию (рис. 2) как элементарный исход в схеме случайного блуждания, приписывая вероятность p умножению на a и дополнительную вероятность q — умножению на b . Поскольку всякая траектория с необходимостью пересекает один из экранов $a^m b^r$ ($r = 0, 1, 2, \dots$) или $a^r b^n$ ($r = 0, 1, \dots$), причем соответствующие вероятности пересечений равны $p^m T_{nm}(q)$ и $q^n T_{mn}(p)$, для любых

неотрицательных и взаимно дополнительных до единицы чисел p и q оказывается справедливым равенство:

$$p^m T_{nm}(q) + q^n T_{mn}(p) = 1.$$

Ввиду целочисленности участвующих в нем многочленов его можно рассматривать как функциональное тождество в алгебре FA :

$$(E - Y)^n T_{mn}(Y) + Y^m T_{nm}(E - Y) = E \quad (Y \in FA).$$

При $Y = dR_a$ оно переходит в следующее обобщение резольвентного тождества:

$$R_b^n - R_a^n T_{mn}(dR_a) = d^m R_a^{m+n} F_{ab}^n T_{nm}(F_{ba}),$$

из которого последнее получается при $m = n = 1$. Найдем разложение левой части этого тождества в ряд Лорана. Используя явный вид многочлена T_{mn} и разложение (1) для R_a^n , имеем:

$$\begin{aligned} R_a T_{mn}(dR_a) &= \sum_{r=0}^{m-1} \sum_{j \geq 0} \binom{r+n-1}{n-1} \binom{j+r+n-1}{r+n-1} d^r a^j X^{-j-r-n} = \\ &= \sum_{r=0}^{m-1} \sum_{k \geq r} \binom{k+n-1}{n-1} \binom{k}{r} d^r a^{k-r} X^{-k-n}. \end{aligned}$$

Следовательно, левая часть обобщенного резольвентного тождества представима рядом:

$$\sum_{k \geq 0} \binom{k+n-1}{n-1} \left(b^k - \sum_{r=0}^{m-1} \binom{k}{r} d^r a^{k-r} \right) X^{-k-n},$$

где, как обычно, нулевая степень любого элемента кольца A (в том числе и нулевого) принимается равной единице, а отрицательная его степень, взятая с нулевым коэффициентом, считается равной нулю. Тем самым требуемое соотношение установлено.

Обозначим через WA множество тех элементов W алгебры FA , для которых конечна сумма $\|F\| = \sum_r |a_r|$.

Предложение 3. Подмножество WA алгебры FA является его подалгеброй (алгебра Винера—Лорана), а функция $\|F\|$ обладает всеми необходимыми свойствами преднормы в кольце WA с единицей E , к которым добавляются следующие (связанные с наличием в WA дополнительной структуры) свойства:

- при любых a из A и W из WA элемент aW принадлежит алгебре WA и $\|aW\| \leq \|a\| \|W\|$;
- при любых натуральных r, k выполнено равенство:

$$\|W(X^k) e X^r\| = \|W(X)\|; \quad (3)$$

в). если W_p — суммируемое к W семейство элементов WA и $\sum_p \|W_p\| < \infty$, то W — также элемент WA , причем $\|W\| \leq \sum_p \|W_p\|$.

Доказательство. Действительно, пусть элементы $U(X) = \sum_r a_r X^r$, $V(X) = \sum_r b_r X^r$ принадлежат WA . Тогда, по свойствам преднормы в кольце A ,

$$\|U - V\| = \sum_r |a_r - b_r| \leq \sum_r (|a_r| + |b_r|) = \|U\| + \|V\|,$$

$$\|UV\| = \sum_r \left| \sum_{p+q=r} a_p b_q \right| \leq \sum_r \sum_{p+q=r} |a_p| |b_q| = \|U\| \|V\|,$$

$$\|aU\| = \sum_r |aa_r| \leq \sum_r |a| |a_r| = |a| \|U\|,$$

$$\|nU\| = \sum_r |na_r| = \sum_r n |a_r| = n \|U\|.$$

Поскольку равенство (3) совершенно очевидно, остается проверить утверждение в). Пусть $W_p(X) = \sum_q a_{pq} X^q$, тогда $W(X) = \sum_q \left(\sum_p a_{pq} \right) X^q$, где внутренняя сумма содержит конечное число ненулевых слагаемых. Следовательно:

$$\sum_p \|W_p\| = \sum_{p,q} |a_{pq}| \geq \sum_q \left| \sum_p a_{pq} \right| = \|W\|.$$

Предложение 4. Пусть $1 \leq n \leq N$ и $i-1, j$ — произвольные натуральные числа. Если элементы F_{ab} , $d^i R_a^{i+j} a^{N-n}$ алгебры FA принадлежат подалгебре WA , то

$$n^j \left\| v_{N-i}^{n-1} - \sum_{r=1}^{i-1} \binom{n-1}{r-1} d^r a^{N-r} \right\| \leq \|F_{ab}\|^{j+1} \|d^i R_a^{i+j} a^{N-n}\| \prod_{r=0}^{j-1} (i-r).$$

Доказательство. Заметим прежде всего, что $\|F_{ab}\| = \|E + dR_b\| = |e| + \|dR_b\| \geq 1$, а также, что

$$F_{ab}^i T_{ji}(F_{ba}) = \sum_{r=0}^{j-1} \binom{r+i-1}{i-1} F_{ab}^{i-r}.$$

Отсюда вытекает оценка:

$$\|F_{ab}^j T_{ji}(F_{ba})\| \leq \|F_{ab}\|^j \sum_{r=0}^{j-1} \binom{r+i-1}{i-1} = \|F_{ab}\|^j \binom{i+j-1}{j-1}.$$

Умножив на da^s ($s = 0, 1, 2, \dots$) обе части тождества из предложения 2, получим неравенство:

$$\begin{aligned} \left| \binom{k+n-1}{n-1} da^s b^k - \sum_{r=0}^{m-1} \binom{k}{r} d^{r+1} a^{s+k-r} \right| &\leq \\ &\leq \binom{m+n-1}{n-1} \|F_{ab}\|^n \|d^{m+1} R_a^{m+n} a^s\|, \end{aligned}$$

из которого заменой n на $j+1$, k на $n-1$, m на $i-1$ и s на $N-n$ легко находим требуемую оценку.

3. Сравнение эволюций

В заключительном разделе проводится доказательство основной теоремы по схеме а) $\Rightarrow$ б) $\Rightarrow$ в) $\Rightarrow$ г) $\Rightarrow$ а) и на относительно простом примере демонстрируется техника ее применения.

Предложение 5. Если система (a, b) устойчива, то сумма

$$S_k = \sum_{N \geq 1} |b^k (a^k)^{N-1} - (a^k)^N|$$

стремится к нулю с ростом k .

Доказательство. По определению устойчивости системы (a, b) для некоторого положительного R равномерно по n и N ($1 \leq n \leq N$) выполнено неравенство $N^s |v_N^n| \leq R$. Следовательно:

$$\begin{aligned} \sum_{N \geq 1} |b^k (a^k)^{N-1} - (a^k)^N| &= \sum_{N \geq 1} |c_{Nk}^k - c_{Nk}^0| = \\ &= \sum_{N \geq 1} \left| \sum_{n=1}^k v_{Nk}^n \right| \leq R \left(\sum_{N \geq 1} N^{-s} \right) k^{-\beta} \rightarrow 0, \end{aligned}$$

что и требовалось.

Устойчивость эталонной эволюции a^N , как уже отмечалось при введении этого понятия, является тривиальным следствием устойчивости системы. Поэтому предложение 5 устанавливает импликацию а) $\Rightarrow$ б) для первых двух утверждений основной теоремы. Чтобы доказать импликацию б) $\Rightarrow$ в), используем следующие две простые оценки.

Предложение 6. Если эволюция a^N устойчива, так что $N^s |da^{N-1}| \leq R$ при всех натуральных N , то для произвольных натуральных m, N справедливо неравенство:

$$N^{sm} |d^m a^{N-1}| \leq m^{sm} R^m. \quad (4)$$

Доказательство. Целое неотрицательное число $N-1$ можно представить в виде $N-1 = (n-1)m + r$, где n — нату-

ральное число и $0 \leq r \leq m-1$. Тогда, очевидно, $N \leq mn$ и, следовательно:

$$\begin{aligned} N^{sm} |d^m a^{N-1}| &= N^{sm} |(da^{n-1})^{m-1} da^{n+r-1}| \leq \\ &\leq m^{sm} (n^s |da^{n-1}|)^{m-1} n^s |da^{n+r-1}| \leq \\ &\leq m^{sm} R^{m-1} (n+r)^s / da^{n+r-1} \leq m^{sm} R^m. \end{aligned}$$

Предложение 7. Для произвольных положительных p, q и любого натурального m выполнено неравенство:

$$\sum_{r \geq 0} \binom{r+m-1}{m-1} (r+p)^{-m-q} \leq \left(\frac{1}{p}\right)^q \left(\frac{1}{p} + \frac{1}{q}\right)^m. \quad (5)$$

Доказательство. Для положительных t обозначим $u(t) = te^t (e^t - 1)^{-1} \leq 1 + t$. Очевидное неравенство $\Gamma(v+q) \leq q^{v-m} \Gamma(m+q)$ ($0 \leq v \leq m$) дает:

$$\begin{aligned} \Gamma(m+q) \sum_{r \geq 0} \binom{r+m-1}{m-1} (p+r)^{-m-q} &= \\ &= \int_0^\infty e^{-pt} t^{q-1} u^m(t) dt \leq \int_0^\infty e^{-pt} t^{q-1} (1+t)^m dt = \\ &= \sum_{v \geq 0} \binom{m}{v} \Gamma(v+q) p^{-v-q} \leq \Gamma(m+q) p^{-q} \sum_{v \geq 0} \binom{m}{v} p^{-v} q^{v-m} = \\ &= \Gamma(m+q) \left(\frac{1}{p}\right)^q \left(\frac{1}{p} + \frac{1}{q}\right)^m. \end{aligned}$$

Предложение 8. Пусть $F_{ab} \in \mathbb{W}A$, эволюция a^N устойчива, так что $N^s |v_N^1| \leq R$ при всех натуральных N, v — произвольное натуральное число и μ — такое отличное от единицы натуральное число, что $2v \leq \beta\mu$. Тогда равномерно по n ($1 \leq n \leq N$):

$$N^v \left| v_N^n - \sum_{r=1}^{\mu-1} \binom{n-1}{r-1} d^r a^{N-r} \right| \leq c(\mu, v),$$

где

$$c(\mu, v) = e(2R\mu^s)^\mu \|F_{ab}\|^{v+1} \prod_{r=0}^{v-1} (\mu+r).$$

Доказательство. Обозначим $p = N - n + 1 \geq 1$, $q = \beta\mu - v \geq v$, $m = \mu + v$. Последовательно применяя формулу (1) и оценки (4) и (5), находим:

$$p^v \|d^\mu R_a^m a^{p-1}\| = p^v \sum_{r \geq 0} \binom{r+m-1}{m-1} |d^\mu a^{r+p-1}| \leq$$

$$\begin{aligned} &\leq (R\mu^s)^\mu p^\nu \sum_{r \geq 0} \binom{r+m-1}{m-1} (p+r)^{-m-q} \leq \\ &\leq (R\mu^s)^\mu p^{\nu-q} \left(\frac{1}{p} + \frac{1}{q}\right)^m \leq (R\mu^s)^\mu \left(1 + \frac{1}{\nu}\right)^{\mu+\nu}. \end{aligned}$$

Поскольку $N \leq np$, из предложения 4 следует, что

$$\begin{aligned} &N^\nu \left| v_N^n - \sum_{r=1}^{\mu-1} \binom{n-1}{r-1} d^r a^{N-r} \right| \leq \\ &\leq p^\nu \|d^\mu R_a^m a^{p-1}\| \|F_{ab}\|^{\nu+1} \prod_{r=0}^{\nu-1} (\mu+r) \leq \\ &\leq (R\mu^s)^\mu \left(1 + \frac{1}{\nu}\right)^\mu e \|F_{ab}\|^{\nu+1} \prod_{r=0}^{\nu-1} (\mu+r). \end{aligned}$$

Предложение 9. Пусть $F_{ab} \in \mathbb{W}A$, эволюция a^N устойчива, так что $N^s |v_N| \leq R$, p — произвольное натуральное число, $\mu = \mu(p)$ — наименьшее целое число, удовлетворяющее неравенству $2\beta p + 4 \leq \beta\mu$, наконец $2\nu = 2\nu(p)$ — наименьшее четное число, принадлежащее сегменту $[2\beta p + 2, \beta\mu]$. Тогда при $1 \leq n \leq N$

$$N^{1+\beta p} \left| v_N^n - \sum_{r=1}^{p-1} \binom{n-1}{r-1} d^r a^{N-r} \right| \leq C_p,$$

где «пустая» сумма заменяется нулем, а $C_p = C(\mu, \nu) + \sum_{r=p}^{\mu-1} R r^{sr+\nu}$.

Доказательство. Очевидно, $p \leq \mu - 1$. Согласно предложению 8 и оценке из предложения 6:

$$\begin{aligned} &N^{1+\beta p} \left| v_N^n - \sum_{r=1}^{p-1} \binom{n-1}{r-1} d^r a^{N-r} \right| \leq N^\nu \left| v_N^n - \sum_{r=1}^{\mu-1} \binom{n-1}{r-1} d^r a^{N-r} \right| + \\ &+ N^{1+\beta p} \sum_{r=p}^{\mu-1} \binom{N-1}{r-1} |d^r a^{N-r}| \leq C(\mu, \nu) + \sum_{r=p}^{\mu-1} \frac{(r^s R)^r}{(r-1)!} g_r(N), \end{aligned}$$

где $g_r(N) = 0$ при $N < r$, а при $r \leq N$ $g_r(N) = N(N-1) \dots (N-r+1) N^{\beta p} (N-r+1)^{-sr}$.

При любом фиксированном r последовательность $g_r(N)$, где $N = r, r+1, r+2, \dots$, монотонно убывает. Действительно, положим $n = N - r + 1 \leq N$, тогда

$$g_r(N) = \frac{\left(1 + \frac{1}{n}\right)^r}{1 + \frac{r}{n}} \left(\frac{1 + \frac{1}{n}}{1 + \frac{1}{N}}\right)^{\beta p} \left(1 + \frac{1}{n}\right)^{\beta(r-p)} g_r(N+1) \geq g_r(N+1)$$

(каждый из трех сомножителей не меньше единицы). Поэтому

$$\sum_{r=p}^{\mu-1} \frac{(r^s R)^r}{(r-1)!} g_r(N) \leq \sum_{r=p}^{\mu-1} \frac{(r^s R)^r}{(r-1)!} g_r(r) \leq \sum_{r=p}^{\mu-1} R^r r^{s r + v},$$

и предложение доказано.

Предложение 10. Пусть для некоторого натурального k система (a^k, b^k) подчинена условию захвата $S_k < 1$, а эталонная эволюция a^N устойчива. Тогда $F_{ab} \in \mathbb{W}A$, причем

$$\|F_{ab}\| \leq |e| + S(k) (1 - S_k)^{-1} \sum_{r=0}^{k-1} |b|^r,$$

где через $S(k)$ обозначена сумма (сходящегося) ряда $\sum_{r \geq 0} |v_{rk+1}|$.

Доказательство. Обозначив через d_k разность $b^k - a^k$, заметим вначале, что

$$S_k = \sum_{N \geq 1} |d_k(a^k)^{N-1}| = \|d_k R(a^k; X)\|.$$

Согласно п. г) (предложения 1, в котором a, b, d заменены соответственно на a^k, b^k, d_k , семейство формальных рядов $dR(a^k; X)(d_k R(a^k; X))^r$ ($r = 0, 1, 2, \dots$) суммируемо к $dR(b^k; X)$. Поэтому на основании п. в) предложения 3 и неравенства $S_k < 1$ заключаем, что

$$\begin{aligned} \|dR(b^k; X)\| &\leq \sum_{r \geq 0} \|dR(a^k; X)(d_k R(a^k; X))^r\| \leq \\ &\leq \|dR(a^k; X)\| \sum_{r \geq 0} S_k^r = S(k) (1 - S_k)^{-1}. \end{aligned}$$

Наконец, используя представление (2) и равенство (3), находим следующую оценку:

$$\begin{aligned} \|dR_b\| &\leq \sum_{r=1}^k \|dR(b^k; X^k) b^{k-r} X^{r-1}\| \leq \\ &\leq \|dR(b^k; X)\| \sum_{r=1}^k |b|^{k-r} \leq S(k) (1 - S_k)^{-1} \sum_{r=0}^{k-1} |b|^r. \end{aligned}$$

Остается учесть соотношение:

$$\|F_{ab}\| = \|E + dR_b\| = |e| + \|dR_b\|.$$

Предложение доказано.

Предложение 11. Если эталонная эволюция устойчива и после некоторого разрежения системы оказывается выполненным условие захвата, то соотношение

$$c_N^n - c_N^m \sim \sum_{r \geq 0} \left(\binom{n}{r} - \binom{m}{r} \right) d^r a^{N-r} \quad (0 \leq m \leq n \leq N)$$

является асимптотическим разложением в шкале $(n - m) N^{-1-\beta p}$.

Доказательство. Условия доказываемого предложения совпадают с условиями предыдущего, поэтому $F_{ab} \in WA$ и может быть применено предложение 9, в силу которого при $1 \leq q \leq N$ и произвольном натуральном p

$$\left| v_N^q - \sum_{r=1}^{p-1} \binom{q-1}{r-1} d^r a^{N-r} \right| \leq C_p N^{-1-\beta p}.$$

Следовательно, равномерно по m, n , подчиненным указанному в условии ограничению, выполняется оценка:

$$\begin{aligned} & \left| c_N^n - c_N^m - \sum_{r=0}^{p-1} \left(\binom{n}{r} - \binom{m}{r} \right) d^r a^{N-r} \right| = \\ & = \left| \sum_{q=m+1}^n v_N^q - \sum_{r=1}^{p-1} \sum_{q=m+1}^n \binom{q-1}{r-1} d^r a^{N-r} \right| \leq \\ & \leq \sum_{q=m+1}^n \left| v_N^q - \sum_{r=1}^{p-1} \binom{q-1}{r-1} d^r a^{N-r} \right| \leq C_p (n - m) N^{-1-\beta p}, \end{aligned}$$

в отношении которой должно быть сохранено соглашение о «пустой» сумме. Итак, предложение 11, а вместе с ним истинность импликации б) $\Rightarrow$ в) теоремы доказаны.

Предложение 12. Если соотношение

$$c_N^n - c_N^m \sim \sum_{r \geq 0} \left(\binom{n}{r} - \binom{m}{r} \right) d^r a^{N-r} \quad (0 \leq m \leq n \leq N)$$

является асимптотическим разложением в шкале $(n - m) N^{-1-\beta p}$, то выражения

$$c_N^n - c_N^m \sim \sum_{r=0}^{p-1} \left(\prod_{q=0}^{p-1} \frac{n-q}{r-q} - \prod_{q=0}^{p-1} \frac{m-q}{r-q} \right) c_N^r$$

(дроби с нулевым знаменателем заменяются единицей) образуют последовательность асимптотических формул относительно этой шкалы.

Доказательство. Фиксируя произвольное натуральное p и $N \geq p - 1$, рассмотрим две функции на $\mathbb{C}^3$:

$$F(x, y, z) = \sum_{r=0}^{p-1} \binom{z}{r} (y-x)^r x^{N-r},$$

$$G(x, y, z) = \sum_{r=0}^{p-1} x^{N-r} y^r \prod_{q=0}^{p-1} \frac{z-q}{r-q}.$$

При $n = 0, 1, 2, \dots, p-1$ очевидно равенство:

$$\prod_{q=0}^{p-1} \frac{n-q}{r-q} = \delta_n^r,$$

поэтому для таких значений n

$$F(x, y, n) = \sum_{r=0}^n \binom{n}{r} (y-x)^r x^{N-r} = x^{N-n} y^n,$$

$$G(x, y, n) = \sum_{r=0}^{p-1} x^{N-r} y^r \delta_n^r = x^{N-n} y^n$$

и, поскольку F и G — полиномы степени $p-1$ по z , они совпадают. В частности, теперь уже при любом целом неотрицательном n однородные полиномы $F(x, y, n)$ и $G(x, y, n)$ степени N совпадают как функции двух комплексных переменных, причем коэффициенты первого из них, очевидно, целые. Следовательно, коэффициенты второго также целые, и эти полиномы совпадают как функции от элементов произвольного коммутативного кольца с единицей, в котором оказывается справедливым следующее тождество Ньютона—Лагранжа:

$$\sum_{r=0}^{p-1} \binom{n}{r} (y-x)^r x^{N-r} = \sum_{r=0}^{p-1} x^{N-r} y^r \prod_{q=0}^{p-1} \frac{n-q}{r-q} \quad (N \geq p-1).$$

В применении к кольцу A с $x = a$, $y = b$ и $0 \leq n \leq N$ оно принимает вид:

$$\sum_{r=0}^{p-1} \binom{n}{r} d^r a^{N-r} = \sum_{r=0}^{p-1} c_N^r \prod_{q=0}^{p-1} \frac{n-q}{r-q}.$$

При этом (если считать, что $0c_N' = 0$ для любого N) ограничение на N снимается, так как при $0 \leq n \leq N \leq p-1$ значения левой части

$$\sum_{r=0}^n \binom{n}{r} d^r a^{N-r} = a^{N-n} b^n = c_N^n$$

равно значению правой:

$$\sum_{r=0}^{p-1} c_N^r \delta_n^r = c_N'.$$

По определению асимптотического разложения, выражения

$$c_N^n - c_N^m \sim \sum_{r=0}^{p-1} \left(\binom{n}{r} - \binom{m}{r} \right) d^r a^{N-r}$$

образуют последовательность асимптотических формул относительно шкалы $(n-m)N^{-1-\beta p}$. Преобразуя их правые части посредством тождества Ньютона—Лагранжа, приходим к требованию заключения.

Доказанное предложение устанавливает импликацию $v) \Rightarrow g)$ теоремы. Истинность импликации $g) \Rightarrow a)$ очевидна. Действительно согласно условию $g)$ с $p=1$ и $m=n-1$, последовательность $N^s |v_N^n| = N^{1+\beta} |c_N^n - c_N^m|$; $N=1, 2, \dots$ ограничена равномерно по $n \leq N$, а это и есть условие $a)$ устойчивости системы.

Теорема доказана полностью. Ее применение проиллюстрируем вычислением итераций оператора

$$(Bf)(x) = \int_{\mathbb{R}} b(x-t) f(t) dt$$

с сильно осциллирующим ядром $b(t) = (1/\pi) \sin^2(1/t)$, который будем рассматривать в пространстве $C(\mathbb{R})$ ограниченных непрерывных функций на $\mathbb{R}$ с равномерной нормой. Исходя из соотношения $b(t) \sim (1/\pi)(1+t^2)^{-1}$ ($t \rightarrow \infty$), возьмем в качестве эталонного ядра $a(t)$ его правую часть. Обозначив через A интегральный оператор с ядром a , а через D — разность $B-A$, проверим устойчивость системы (A, B) . Согласно неравенству Коши:

$$\begin{aligned} \|D\|^2 &= \left(\frac{1}{\pi} \int_{\mathbb{R}} \left| \sin^2 x - \frac{x^2}{1+x^2} \right| \frac{dx}{x^2} \right)^2 \leq \\ &\leq \frac{1}{\pi^2} \int_{\mathbb{R}} \frac{((1+x^2) \sin^2 x - x^2)^2}{x^6} dx \int_{\mathbb{R}} \frac{x^2 dx}{(1+x^2)^2} = \frac{7}{60}, \\ \left(\int_{\mathbb{R}} t^2 |b(t) - a(t)| dt \right)^2 &= \left(\frac{1}{\pi} \int_{\mathbb{R}} \left| \sin^2 x - \frac{x^2}{1+x^2} \right| \frac{dx}{x^4} \right)^2 \leq \\ &\leq \frac{1}{\pi^2} \int_{\mathbb{R}} \frac{((1+x^2) \sin^2 x - x^2)^2}{x^8} dx \int_{\mathbb{R}} \frac{dx}{(1+x^2)^2} = \frac{41}{315}. \end{aligned}$$

Далее, учитывая самовоспроизводимость ядра $a_n(t)$ при итерациях оператора A и используя, например, формулу Тейлора с интегральным остаточным членом, нетрудно получить неравенство:

$$\begin{aligned} \|DA^{N-1}\| &\leq \frac{1}{2} \int_{\mathbb{R}} t^2 |b(t) - a(t)| dt \int_{\mathbb{R}} |a_{N-1}'(t)| dt \leq \\ &\leq \frac{1}{2} \sqrt{\frac{41}{315}} \frac{3\sqrt[3]{3}}{2\pi(N-1)^2} \leq 1/2\pi(N-1)^2, \end{aligned}$$

означающее устойчивость эталонной эволюции A^N с показателем $\beta = 1$. Остается проверить, выполнено ли условие захвата для какого-либо натурального k . Уже при $k = 1$ оценка

$$\sum_1^\infty \|DA^{N-1}\| = \|D\| + \sum_1^\infty \|DA^m\| \leq \sqrt{\frac{7}{60}} + \frac{\pi}{12} \leq \frac{2}{3}$$

гарантирует это выполнение с достаточным запасом. Следовательно, при больших значениях N и, например, при $p = 2$ для итерации B^N получаем представление в виде суммы:

$$B^N = (1 - N)A^N + NA^{N-1}B + O(N^{-2}),$$

слагаемые которой легко вычисляются при любом N .

Рассмотренная задача имеет чисто иллюстративный характер и, вероятно, может быть решена без использования биномиальной асимптотики. Представление о применении последней к более содержательным задачам дает следующий результат.

Пусть X — сепарабельное гильбертово пространство, M — алгебра ограниченных знакопеременных борелевских мер на X со сверткой в качестве умножения и полной вариацией в качестве нормы, μ и ν — центрированные вероятностные меры из M с невырожденным корреляционным оператором D .

Рассмотрим задачу аппроксимации свертки μ^N неограниченно растущей кратности N целочисленными линейными комбинациями свертков вида $\mu^n \nu^{N-n}$, $0 \leq n < p$ (кратности μ в которых ограничены) для случая, когда мера μ абсолютно непрерывна по мере ν , предполагаемой гауссовой. Введем следующие обозначения: F_s — спектральная функция положительного оператора D (разложение единицы); β , u , v — вспомогательные параметры, определяемые соотношениями:

$$\beta = \frac{1}{2} \frac{r-1}{r+1}, \quad u = \frac{1}{2} - \beta, \quad v = \frac{1}{2} + \beta,$$

где r — фиксированное число, большее единицы. Далее, T — непрерывный положительный оператор, такой, что функция $t(s) = s^{-3r} \operatorname{tr}(F_s D T)$ ограничена на $\mathbb{R}^+$, $|x|_T = \sqrt{(Tx, x)}$; наконец,

$$c = \frac{4 \exp(-3/2) + 1}{3\sqrt[3]{2\pi}} \leq 0.252$$

— абсолютная постоянная.

Справедливо следующее утверждение.

Если плотность $f(x) = (d\mu/d\nu)(x)$ такова, что при любых x, y из X $|f(x) - f(y)| \leq (g(x) + g(y)) |x - y|_T$, где функция g суммируема с квадратом по мере ν , то либо при любом натуральном N выполнено неравенство

$$\|\mu^N - \nu^N\| + N^{-\beta} R \zeta(1 + \beta) \geq 1,$$

(в котором $R = (a/u)^u (b/v)^v$; $a = 2\sqrt{2} (\sup_t \int g^2(x) \nu(dx))^{1/2}$; а ζ — функция Римана), либо при любом натуральном p имеет место асимптотическое соотношение:

$$\mu^N = \sum_{n=0}^{p-1} \mu^n \nu^{N-n} \prod_{q=0}^{p-1} \frac{N-q}{n-q} + O(N^{-\beta p}),$$

в формулах коэффициентов которого дроби с нулевым знаменателем опускаются.

Метод, исследованный в настоящей работе, позволяет получить доказательство этой и аналогичных ей теорем об аппроксимациях сверток в других нормах, равно как и на других, отличных от X , метрических группах.

ОБ ИМПРИМИТИВНОСТИ ОДНОГО КЛАССА S-КОЛЕЦ

1. Введение

Ряд нерешенных проблем теории сложности вычислений связан с распознаванием изоморфизма конечных алгебраических и комбинаторных объектов. Наиболее трудной среди них является проблема изоморфизма графов, которой эквивалентна проблема изоморфизма объектов в категории всех конечных алгебраических систем [1]. Последовательное применение теоретико-групповой техники [2, 3] привело к построению алгоритма, распознающего изоморфизм двух произвольных n -вершинных графов за $O(n^{\sqrt{n/\log n}})$ шагов [4].

В проблеме изоморфизма значительно меньший прогресс достигнут в определении сложности идентификации объектов, отличных от графов. Так, в настоящее время сложность наилучшего алгоритма, проверяющего изоморфизм групп порядка n , заданных таблицами Кэли, не превосходит $O(n^{\log n})$ [5]. Эта оценка является следствием того, что каждая группа порядка n обладает множеством образующих, состоящим из не более чем $\log n$ элементов. Аналогичные соображения приводят к алгоритмам субэкспоненциальной сложности, проверяющим изоморфизм латинских квадратов, аффинных плоскостей и некоторых других комбинаторных объектов [5].

Промежуточное положение между графами, с одной стороны, и группами и конфигурациями, с другой, занимают турниры, т. е. графы, у которых каждой неупорядоченной паре различных вершин соответствует единственное ориентированное ребро. Как указано в [6], изоморфизм двух n -вершинных турниров можно проверить за время $O(n^{\log n})$. Теоретико-групповая часть этого алгоритма использует тот факт, что группа автоморфизмов произвольного турнира разрешима. В основе его комбинаторной части лежит вариант процедуры наивной классификации вершин, вырабатывающий по графу Γ клеточное кольцо $\Sigma(\Gamma)$ следующим образом [7].

Раскрасим упорядоченные пары вершин графа Γ в различные цвета, соответствующие парам одинаковых вершин, ребрам и не-ребрам. Уточним раскраску с таким расчетом, чтобы пары оди-

накового цвета оказались принадлежащими одинаковому числу треугольников с фиксированными цветами сторон. Итеративное применение таким образом определенного уточнения приведет к цветному графу, у которого множества одноцветных упорядоченных пар вершин индуцируют подграфы $\Gamma_1, \dots, \Gamma_r$. Можно показать [7], что матрицы смежности этих подграфов порождают клеточное кольцо $\Sigma(\Gamma)$, содержащее, в частности, матрицу смежности графа Γ .

Рассмотрим возможную схему построения группы автоморфизмов турнира Γ , аналогичную [6]. В ней наиболее простым оказывается случай, когда кольцо $\Sigma(\Gamma)$ не является клеткой, т. е. вершины турнира Γ после уточнения раскраски разбиваются на более чем один цветной класс. Действительно, в этом случае достаточно рекурсивно применить алгоритм к турнирам, порожденным вершинами цветных классов, и воспользоваться затем техникой Бабаи—Лакса. Заметим, что возможность последнего обусловливается разрешимостью полученных групп.

Случай, когда кольцо $\Sigma(\Gamma)$ оказывается клеткой, приводит к рассмотрению двух подслучаев в зависимости от примитивности $\Sigma(\Gamma)$. Импримитивность клетки $\Sigma(\Gamma)$ означает, что один из базисных графов Γ_i представляется в виде объединения вершинно-непересекающихся турниров [7]. Это обстоятельство снова позволяет применить алгоритм рекурсивно.

Описанная схема сводит задачу построения группы автоморфизмов произвольного турнира к соответствующей задаче для тех турниров Γ , у которых кольцо $\Sigma(\Gamma)$ является примитивной клеткой. Естественным образом возникающая при этом проблема классификации последних оказывается в некотором смысле проще описания всех примитивных клеток, поскольку клеточные кольца турниров обладают следующим дополнительным свойством. Пусть A — базисная матрица кольца $\Sigma(\Gamma)$. Тогда, по определению клеточного кольца [7], матрица A^t , транспонированная к A , также является базисной матрицей кольца $\Sigma(\Gamma)$. Нетрудно проверить, что если Γ — турнир и A — базисная матрица, отличная от единичной, то $A \neq A^t$. В настоящей работе делается первый шаг в изучении колец с таким свойством — рассматриваются клеточные кольца, индуцированные турнирами Кэли.

Турнир Кэли группы G строится следующим образом. Пусть H — подмножество элементов из G такое, что $H \cap H^{-1} = \emptyset$. Вершинами строящегося турнира будут все элементы из G ; ориентированное ребро (g_1, g_2) получается из пары $g_1, g_2 \in G$, для которой $g_1 \cdot g_2^{-1} \in H$. Клеточное кольцо турнира Кэли оказывается S -кольцом над G (или в другой терминологии — кольцом Шюра).

2. Основные определения

Фиксированной будем считать группу G порядка n . Ее групповое кольцо $R(G)$ состоит из формальных сумм вида $\sum c_g g$, где $c_g \in \mathbb{Z}$, называемых величинами. Операции сложения и

умножения в кольце $R(G)$ определяются естественным образом: если $U = \sum c_g g$, $V = \sum c'_g g$, то

$$U + V = \sum (c_g + c'_g) g, \quad UV = \sum_{g, h} (c_g c'_h) gh.$$

Кольцо $R(G)$ интерпретируется как модуль над $\mathbb{Z}$, если для $d \in \mathbb{Z}$ положить $dU = \sum (dc_g) g$.

Величина $\sum c_g g$ называется простой, если $c_g \in \{0, 1\}$ для всех $g \in G$. Если $U \subseteq G$, то через $\underline{U}$ обозначим простую величину $\sum_{g \in U} g$.

О п р е д е л е н и е [8]. Подкольцо Σ кольца $R(G)$ называется S -кольцом над G , если выполнены следующие условия:

а) $1 \in \Sigma$ (1 — единичный элемент в G);

б) существует базис кольца Σ , состоящий из простых величин (называемых базисными), т. е. $\Sigma = \langle \underline{U}_0, \underline{U}_1, \dots, \underline{U}_r \rangle$, где

$$\underline{U}_0 = \{1\} \text{ и } \sum_{i=0}^r \underline{U}_i = \underline{G};$$

в) если $U = \sum c_g g \in \Sigma$, то $U^{(-1)} = \sum c_g g^{-1} \in \Sigma$ и $dU \in \Sigma$ для $d \in \mathbb{Z}$.

Из условия б) следует, что для каждого $g \in G$ имеется единственная базисная величина $\underline{U}_i$, для которой $g \in U_i$. Эта величина обозначается также через $\underline{U}_g$.

В дополнение к операциям из в) каждое S -кольцо замкнуто относительно циклического умножения, определяемого следующим образом: если $U = \sum c_g g$ и $V = \sum c'_g g$, то $U \circ V = \sum (c_g c'_g) g$. Для простых величин циклическое умножение удовлетворяет правилу:

$$U \circ U' = \underline{U \cap U'}.$$

Можно показать, что если Σ — S -кольцо над G и $f: \mathbb{Z} \rightarrow \mathbb{Z}$ — произвольная функция, то $\sum f(c_g) g \in \Sigma$, коль скоро $\sum c_g g \in \Sigma$ [8]. Отсюда следует, что если $U \in \Sigma$, то и сумма U^+ всех элементов из G , встречающихся в U с ненулевыми коэффициентами, также принадлежит Σ . Заметим, что если U — простая величина, то $U^+ = U$.

Пусть $U = \sum c_g g \in \Sigma$ и $m \in \mathbb{Z}$. Положим $U^{(m)} = \sum c_g g^m$.

Л е м м а Ш у р а—В и л а н д а [8]. Пусть G — абелева группа, Σ — S -кольцо над G и $m \in \mathbb{Z}$ взаимно просто с n . Тогда если $U \in \Sigma$, то и $U^{(m)} \in \Sigma$. Более того, если U — базисная величина, то и $U^{(m)}$ — базисная величина.

Величина $\hat{U} = \left(\sum_{(m, n)=1} U^{(m)} \right)^+$ называется следом величины U . Каждое S -кольцо Σ над G содержит величины $\underline{U}_0$ и $\underline{G}$, называемые тривиальными. Если Σ содержит нетривиальную простую величину $\underline{U}$, для которой $U \leq G$, т. е. U — подгруппа группы G , то Σ называется импримитивным S -кольцом, а величина $\underline{U}$ — вырожденной. Не содержащее вырожденных величин S -кольцо

называется примитивным. В таком кольце $U = \{1\}$ и $U = G$ являются единственными подгруппами, для которых $\bar{U} \in \Sigma$.

Обозначим через f_p (p — простое число) функцию, связывающую с целым числом его наименьший неотрицательный вычет по модулю p . Тогда $f_p[U] = \Sigma f_p(c_g) g \in \Sigma$, если $U = \Sigma c_g g \in \Sigma$. Тот факт, что у величин $U, V \in R(\bar{G})$ соответствующие коэффициенты сравнимы по модулю p , будем отражать с помощью записи $U \equiv V \pmod{p}$. Ясно, что $\bar{U} \equiv f_p[U] \pmod{p}$.

Л е м м а Ш у р а [9]. Пусть Σ — примитивное S -кольцо над абелевой группой G , p — простой делитель n и $U \in \Sigma$. Тогда $U^{(p)} \equiv d \cdot 1 \pmod{p}$ для некоторого подходящего целого числа d .

Впервые S -кольца были введены И. Шуром [9] для изучения групп перестановок, содержащих регулярные подгруппы. Пусть Γ — группа перестановок на множестве A и G — подгруппа Γ , регулярно действующая на A . От Γ -действия на A можно перейти к Γ -действию на G , для которого $g^h = gh$ при $g, h \in G$ (через g^h обозначен образ элемента g относительно перестановки, соответствующей h). Обозначим через $1 = U_0, \dots, U_r$ орбиты Γ_1 -действия на G , где Γ_1 — подгруппа группы Γ , оставляющая на месте единицу группы G . Можно показать, что элементы $U_0, U_1, \dots, U_r$, рассматриваемые как простые величины из $R(\bar{G})$, порождают S -кольцо над G . Получаемые таким образом S -кольца получили название шуровых. Следует отметить, что не каждое S -кольцо является шуровым [8].

Исследования Шура и его учеников, связанные с S -кольцами, концентрировались на изучении свойства примитивности. Наиболее глубокий результат здесь принадлежит Виланду, который показал, что S -кольцо над абелевой группой, имеющей по крайней мере одну циклическую силовскую подгруппу, не может быть примитивным, если порядок группы — составной [8]. В этой связи возникает естественный вопрос: должно ли быть импримитивным S -кольцо над абелевой группой, порядок которой не равен степени простого числа? В общем случае ответ на этот вопрос отрицательный, как показывает пример S -кольца над $\mathbb{Z}_{pq} \times \mathbb{Z}_{pq}$, порожденного базисными величинами $\{1\}, \{x, x^2, \dots, x^{pq-1}, y, y^2, \dots, y^{pq-1}\}, \{x^i y^j : i, j = 1, \dots, pq-1\}$, где p, q — различные простые числа, а x, y — различные образующие циклических подгрупп порядка pq [8].

В приведенном примере для каждой базисной величины U было выполнено соотношение $\bar{U} = \bar{U}^{(-1)}$. Как показано в разд. 3, это обстоятельство является существенным по крайней мере для данного примера. Поэтому естественно желание переформулировать поставленный выше вопрос для S -колец над абелевыми группами, удовлетворяющих следующему дополнительному условию: г) если $U \neq 1$ — базисная величина, то $U \neq U^{(-1)}$.

При выполнении условия г) S -кольца будем называть нечетными. Такое название объясняется прежде всего тем, что в таких кольцах число базисных величин нечетно. Другое объяснение со-

стоит в том, что именно такие S -кольца получаются в результате применения конструкции Шура к группам перестановок нечетного порядка, обладающим регулярной подгруппой. Отметим наконец, что нечетные S -кольца возникают в результате применения к турнирам Кэли варианта процедуры наивной классификации вершин, рассмотренного во введении.

3. Нечетные S -кольца над $\mathbb{Z}_{pq} \times \mathbb{Z}_{pq}$

Пусть $G = G_p \times G_q$ (G_p и G_q — элементарные абелевы группы порядков p^2 и q^2 соответственно, где p, q — различные нечетные простые числа), а Σ — нечетное S -кольцо над G . Обозначим через M_p совокупность нетривиальных базисных величин $\underline{U}$, для которых $\underline{U} \circ \underline{G}_p \neq 0$. Аналогично определим множество базисных величин $\underline{M}_q$.

Для $g \in G$ положим $g^* = \{g, g^2, \dots, g^s\}$, где $s = |g| - 1$. Множество $U \subseteq G_p - \{1\}$ назовем p -замкнутым, если $g^* \subseteq U$ для каждого $g \in U$. Заменяя в последнем определении p на q , получим определение q -замкнутого множества.

Л е м м а 1. $M_p \cap M_q = \emptyset$.

Д о к а з а т е л ь с т в о. Пусть, вопреки утверждению леммы, найдется базисная величина $\underline{U}$ в S -кольце Σ , принадлежащая множеству $M_p \cap M_q$. Тогда можно выбрать такие элементы $g, h \in U$, что $g \in G_p$ и $h \in G_q$. Поскольку p и q — различные простые числа, то, по китайской теореме об остатках, найдется число t , удовлетворяющее сравнениям: $t \equiv 1 \pmod{q}$, $t \equiv p - 1 \pmod{p}$. Следовательно, $U^{(t)} \ni h^t = h \in U$, т. е. $U^{(t)} \cap U \neq \emptyset$. Но по лемме Шура—Виланда $\underline{U}^{(t)}$ — базисная величина кольца Σ и, значит, $\underline{U} = \underline{U}^{(t)}$.

С другой стороны, $\underline{U} = \underline{U}^{(t)} \ni g^t = g^{-1}$. Таким образом, $g, g^{-1} \in U$, что противоречит нечетности S -кольца Σ .

Л е м м а 2. Пусть $\underline{U}$ — базисная величина S -кольца Σ .

Тогда:

- а) если $\underline{U} \notin M_p \cup M_q$, то $\dot{\underline{U}} = \sum_i \underline{g_i} \underline{V_i} = \sum_j \underline{U_j} \underline{h_j^*}$, где $\underline{V_i}$ — q -замкнуто, $\underline{U_j}$ — p -замкнуто и $\underline{G}_p \circ \dot{\underline{U}} = \underline{G}_q \circ \dot{\underline{U}} = 0$;
 б) если $\{r_1, r_2\} = \{p, q\}$ и $\underline{U} \in \overline{M}_{r_1}$, то

$$\underline{U} = \sum_{i \in I} \underline{g_i} (1 + \underline{V_i}) + \sum_{j \in J} \underline{h_j} \underline{U_j},$$

где $I \cap J = \emptyset$ и $\underline{V_i}, \underline{U_j}$ — r_2 -замкнуты, $\underline{U} \circ \underline{G}_{r_1} = \{g_i : i \in I\}$;

в) в обозначениях б), если Σ — примитивно, то

$$|V_i| \equiv r_2 - 1 \pmod{r_2} (i \in I), \quad |U_j| \equiv 0 \pmod{r_2} (j \in J).$$

Д о к а з а т е л ь с т в о. Для доказательства а) достаточно проверить, что если $g \in G_p$, $h \in G_q$ и $gh \in U$, то коэффициент, с которым $g^i h^j$ входит в $\dot{\underline{U}}$, отличен от 0 при $i = 1, \dots, p - 1$,

$j = 1, \dots, q - 1$. Но, по китайской теореме об остатках, можно выбрать такое целое число t , что $t \equiv i \pmod{p}$, $t \equiv j \pmod{q}$. По определению следа, $\underline{U}^{(t)} \circ \dot{U} = \underline{U}^{(t)}$ и, значит, все элементы из $\underline{U}^{(t)}$ встречаются в $\dot{U}$ с ненулевыми коэффициентами. Это относится, в частности, и к элементу $g^i h^j = g^t h^t \in \underline{U}^{(t)}$, что завершает доказательство а).

Заметим, что в) есть непосредственное следствие утверждения б) и леммы Шура, и потому для завершения доказательства леммы достаточно проверить справедливость утверждения б). Оно в свою очередь выполняется, если вместе с каждым элементом gh ($g \in G_p$, $h \in G_q$) множество U содержит каждый элемент вида gh^i , $i = 1, \dots, q - 1$ (здесь, не умаляя общности, считаем, что $p = r_1$ и $q = r_2$). Но из условия $\underline{U} \in M_p$ следует, что найдется элемент $\underline{g} \in U \cap G_p$. Поэтому если определить число t_i условиями $t_i \equiv 1 \pmod{p}$ и $t_i \equiv i \pmod{q}$, $i = 1, \dots, q - 1$, то $\underline{U}^{(t_i)} = \underline{U}$, так как $\underline{U}^{(t_i)} \ni \underline{g}^{t_i} = \underline{g} \in U$, а $\underline{U}^{(t_i)}$ — базисная величина по лемме Шура—Виланда. Таким образом, $gh^i = g^{t_i} h^{t_i} \in \underline{U}^{(t_i)} = \underline{U}$, $i = 1, \dots, q - 1$, что и требовалось доказать.

В отличие от лемм 1 и 2, справедливых в более общем случае, в доказательстве следующих утверждений существенно используются ограничения на порядки групп G_p и G_q .

Л е м м а 3. Пусть Σ — примитивно и $\underline{U}$ — его базисная величина. Тогда $\underline{U} \circ (\underline{G}_p + \underline{G}_q) \neq 0$.

З а м е ч а н и е. Утверждение леммы означает, что совокупность базисных величин примитивного S -кольца Σ исчерпывается множеством $\{1\} \cup M_p \cup M_q$.

Д о к а з а т е л ь с т в о. Пусть, вопреки утверждению леммы, найдется базисная величина $\underline{U}$, для которой $\underline{U} \circ (\underline{G}_p + \underline{G}_q) = 0$. Тогда из леммы 2, а) следует, что $\dot{U} = \Sigma g_i^* \underline{V}_i$. В силу q -замкнутости простая величина $\underline{V}_i$ может быть представлена в виде:

$$\underline{V}_i = \sum_{j=1}^{m_i} h_j^*.$$

В силу выбора U каждый элемент h_j отличен от 1 и потому $|V_i| = m_i (q - 1)$. Поскольку $V_i \subseteq G_q - 1$, то $m_i (q - 1) \leq q^2 - 1$, откуда вытекает неравенство:

$$m_i \leq q + 1. \quad (1)$$

По выбору величины U справедливо равенство $\underline{U} \circ \underline{G}_q = 0$ и, значит, по лемме Шура, $|V_i| = qa_i$ для некоторого натурального числа a_i . Таким образом, $m_i (q - 1) = qa_i$ и потому m_i делится на q . Последнее утверждение вместе с неравенством (1) приводит к тому, что $m_i = q$. Поскольку $|G_q| = q^2$, то $\underline{G}_q = 1 + \sum_{j=1}^{q+1} \omega_j^*$,

где $\omega_j \in G_q$ и $\omega_j^* \cap \omega_k^* = \Phi$ при $j \neq k$. Следовательно, найдется такой элемент $\omega_i \in G_q$, что $V_i = G_q - \omega_i^* - 1$.

Рассмотрим базисную величину $\underline{U}_{g_i}$. По лемме 2, б), применяемой для $r_1 = p$, получим $\underline{U}_{g_i} = \underline{g_i} (1 + \tilde{V}_i) + \beta_i$, где β_i — некоторая простая величина группового кольца $R(G)$, в которую все элементы вида $g_i h$ ($h \in G_q$) входят с нулевыми коэффициентами. Множество $\tilde{V}_i$ непусто и q -замкнуто; поэтому $|\tilde{V}_i|$ делится на $q - 1$. Но $V_i \cup \tilde{V}_i \subseteq G_q - 1$ и $V_i \cap \tilde{V}_i = \Phi$, так как $\underline{U}_{g_i} \circ \underline{U} = 0$. С другой стороны, исходя из доказанного выше, $V_i = G_q - \omega_i^* - 1$, и, следовательно, $\tilde{V}_i = \omega_i^*$.

Применяя аналогичное рассуждение к представлению величины $\underline{U}$ в виде $\underline{U} = \sum_j \underline{U_j} h_j^*$ (см. лемму 2, а)), получим $U_j = G_p - \Phi_j^* - 1$ и $U_{h_j} = (1 + \Phi_j^*) h_j + \gamma_j$ для некоторой простой величины $\gamma_j \in \bar{R}(G)$, в которую все элементы вида gh_j ($g \in G_p$) входят с нулевыми коэффициентами. Таким образом, выполнены следующие равенства:

$$\underline{U} = \sum_i \underline{g_i} (\underline{G_q} - \underline{\omega_i^*} - 1) = \sum_j (\underline{G_p} - \Phi_j^* - 1) \underline{h_j^*}, \quad (2)$$

$$\underline{U}_{g_i} = (1 + \omega_i^*) \underline{g_i} + \beta_i, \quad \underline{U}_{h_j} = (1 + \Phi_j^*) \underline{h_j} + \gamma_j, \quad (3)$$

где $g_i, \Phi_j \in G_p, \omega_i, h_j \in G_q, \beta_i, \gamma_j \in R(G)$.

Предположим, что найдется элемент ω_i ($i \neq 1$), для которого $\omega_1 \neq \omega_i$. Тогда $g_1 \omega_i$ входит в $\underline{U}$ с ненулевым коэффициентом и потому в силу (2) для некоторого j $\omega_i^* = h_j^*$. Снова используя (2), заключаем, что $\Phi_j^* = g_i^*$. Подставив в первое из равенств (3) значение h_j^* вместо ω_i^* и Φ_j^* вместо g_i , получим: $\underline{U}_{g_i} = (1 + h_j^*) \Phi_j^* + \beta_i$. Отсюда и из второго неравенства (3) следует, что $\underline{U}_{g_i} \circ \underline{U}_{h_j} \neq 0$, так как $h_j \Phi_j^* \in U_{g_i} \cap U_{h_j}$, что противоречит лемме 1. Поэтому $\omega_i^* = \omega_1^*$ для всех i и аналогично $\Phi_j^* = \Phi_1^*$ для всех j . Таким образом, $\underline{U} = (\underline{G_p} - \Phi_1^* - 1)$, $(\underline{G_q} - \underline{\omega_1^*} - 1)$ и равенства (3) можно представить следующим образом:

$$\underline{U_g} = (1 + \omega_1^*) \underline{g} + \beta_g, \quad \underline{U_h} = (1 + \Phi_1^*) \underline{h} + \gamma_h, \quad g \in G_p - \Phi_1^* - 1, \quad (4)$$

$$h \in G_q - \omega_1^* - 1.$$

Первое из равенств (4) и лемма 2, б), примененная к базисной величине U_{ω_1} , показывают, что $\underline{U}_{\Phi_1} = (1 + \Phi_1^*) \underline{\omega_1} + \gamma'$, где $(\gamma')^+ = \gamma' \cdot \gamma' \in R(G)$ (здесь использовался тот факт, что по лемме 1 $\underline{U}_{\Phi_1} \circ \underline{U_g} = 0$ для всех $g \in G_p$). Аналогично с помощью второго из неравенств (4) устанавливается, что $\underline{U}_{\Phi_1} = (1 + \omega_1^*) \underline{\Phi_1} + \beta'$, где $\beta' \in R(G)$ и $(\beta')^+ = \beta'$. Отсюда следует, что $\underline{U}_{\Phi_1} \circ \underline{U}_{\Phi_1} \neq 0$, так как $\Phi_1 \Phi_1 \in U_{\omega_1} \cap U_{\Phi_1}$, и потому $\underline{U}_{\Phi_1} = \underline{U}_{\Phi_1}$ вопреки лемме 1. Полученное противоречие завершает доказательство леммы.

Основной результат представляется следующим утверждением.

Т е о р е м а. Не существует примитивных нечетных S -колец над группой $\mathbb{Z}_{pq} \times \mathbb{Z}_{pq}$, где p, q — различные нечетные простые числа.

Д о к а з а т е л ь с т в о. Пусть $\{r_1, r_2\} = \{p, q\}$. Элемент $g \in G_{r_1}$ назовем r_2 -полным, если $\underline{U_{gh}} \in M_{r_1}$ для всех $h \in G_{r_2}$. Для доказательства теоремы достаточно проверить следующее утверждение: если Σ — примитивное нечетное S -кольцо над G , то в G существуют q -полные и p -полные элементы. Обозначим его (*).

Действительно, пусть (*) доказано и g, h — p -полный и q -полный элементы соответственно. Тогда $\underline{U_{gh}} \in M_p \cap M_q$, что противоречит лемме 1. и доказывает требуемое утверждение.

Для доказательства (*) выберем произвольную базисную величину $\underline{U}$ из M_p . Тогда по лемме 2, б)

$$\underline{U} = \sum_{i \in I} \underline{g_i(1 + V_i)} + \sum_{j \in J} \underline{h_j U_j}, \quad (5)$$

где U_j и V_i — q -замкнутые простые величины. Если $J \neq \emptyset$, то по лемме 2, в) $|U_j| = q(q-1)$ для всех $j \in J$. Отсюда следует, что $\underline{U_{h_j}} = \underline{h_j(G_q - U_j)} + \beta$, где β — простая величина из $R(G)$ и, следовательно, элемент h_j является q -полным.

Если $J = \emptyset$, то по (5) $\underline{U} = \sum_{i \in I} \underline{g_i(1 + V_i)}$. Не умаляя общности, можно считать, что $V_i \neq G_q$ при $i \in I$ (в противном случае имеется q -полный элемент). Таким образом, $\underline{U} = \sum_{i \in I} \underline{g_i(1 + h_i^*)}$

для некоторых $h_i \in G_q$ по лемме 2, в).

По нечетности Σ имеем неравенство $g_i \neq g_j^{-1}$ при $i, j \in I$. Отсюда, используя лемму 3, заключаем, что $\underline{U \cdot U}$ есть линейная комбинация базисных величин из M_p . Если при этом $h_i^* \neq h_j^*$ для некоторых $i, j \in I$, то элемент $\underline{g_i g_j}$ является q -полным, поскольку $\underline{U U} = \underline{g_i g_j G_q} + \beta''$, где β'' — величина из $R(G)$ с отрицательными коэффициентами.

В силу произвольности выбора базисной величины $\underline{U} \in M_p$ заключаем, что в Σ нет q -полных элементов только в том случае, когда каждая базисная величина $\underline{U} \in M_p$ имеет вид

$$\underline{U} = \sum_i \underline{q_i(1 + h^*)},$$

где $h = h(U) \in G_q$. Это, однако, противоречит примитивности S -кольца Σ , поскольку $U \subseteq G_p \times (1 + h^*) = \tilde{G}(U) < G$. Тем самым доказано, что в G имеются q -полные элементы. Аналогично проверяется существование в G p -полных элементов. Таким образом, утверждение (*) доказано.

Литература

1. Земляченко В. Н., Корнеев Н. М., Тышкевич Р. И. Проблема изоморфизма графов//Зап. науч. семин. ЛОМИ. 1982. Т. 118. С. 83—158.
2. Babai L. Monte Carlo algorithms in graph isomorphism testing//Preprint, Univ. Toronto, 1979.
3. Лакс Ю. Изоморфизм графов с ограниченными степенями вершин может быть установлен за полиномиальное время//Киберн. сб. Нов. сер. 1985. Вып. 22. С. 72—101.
4. Babai L., Kantor W., Luks E. M. Computational complexity and the classification of finite simple groups//Proc. 24-th Ann. Symp. Found. Comput. Sci. N. Y.; London. 1983, p. 162—171.
5. Miller G. L. On the $n \log n$ isomorphism technique//Proc. 10-th ACM Symp. Th. Comput. N. Y.; London. 1978, p. 51—58.
6. Babai L., Luks E. M. Canonical labelling of graphs//Proc. 15-th ACM Symp. Th. Comput. N. Y.; London. 1983, p. 171—183.
7. Weistfeiler B. On construction and identification of graphs//Lect. Notes Math. 1976. Vol. 558.
8. Wielandt H. Finite permutation groups. N.—Y., 1964.
9. Shur I. Zur Theorie der einfach transitiven Permutationsgruppen//Press. Akad. Wiss. phys.-math. Kl. Berlin, 1933, S. 598—623.

ОБ УСЛОВИЯХ ПОЛНОЙ КОГЕРЕНТНОСТИ В ЗАМКНУТЫХ КАТЕГОРИЯХ

Теоремы когерентности, согласно С. Маклейну [1], это теоремы о коммутативности всех диаграмм того или иного класса. Наличие таких теорем позволяет обходиться без вычислений при проверке коммутативности, инвариантным образом определять операции в категориях и т. д.

Большое внимание уделялось изучению проблемы когерентности в замкнутых и, в частности, в симметрических моноидальных замкнутых категориях (СМЗК), к которым относятся категории векторных пространств над полями, векторных расслоений, модулей над кольцами и т. д.

Большой интерес вызывают диаграммы так называемых канонических естественных преобразований, т. е. естественных преобразований, построенных из выделенных в структуре СМЗК, при помощи функторов $\otimes$, $[,]$ (внутреннего hom -функтора) и композиции. Для СМЗК Дж. Келли и С. Маклейном была доказана ограниченная теорема когерентности, грубо говоря, утверждающая, что если в диаграмму канонических естественных преобразований не входят выражения вида $[A, I]$, где I — выделенный объект (для векторных пространств это основное поле), то диаграмма коммутативна [1]. При нарушении этого условия диаграммы канонических естественных преобразований в СМЗК могут быть некоммутиативны. В категории $\mathcal{F}$ форм (shapes) и канонических морфизмов (свободной СМЗК с одним образующим) следующая диаграмма не будет коммутативной (см. рисунок).

$$\begin{array}{ccc}
 [[[A, I], I], I] & \xrightarrow{1} & [[[[A, I], I], I]] \\
 \searrow \pi(\langle \pi(e_C) \rangle) & & \swarrow \pi(e_C) \\
 & [A, I] &
 \end{array}$$

(*)

здесь $\pi = \pi_{ABC} : \text{Hom}(A \otimes B, C) \rightarrow \text{Hom}(A, [B, C])$ — изоморфизм сопряженности, $e = e_{AB} : [A, B] \otimes A \rightarrow B$ — «вычи-

© С. В. Соловьев, 1990

слительный гомоморфизм», $c = c_{AB} : A \otimes B \rightarrow B \otimes A$ — коммутативность тензорного произведения, $\langle h \rangle = e \cdot (1 \otimes h)$.

Диаграмма (*) не будет коммутативна не только в $\mathcal{F}$, но и в некоторых конкретных СМЗК, например в категории векторных пространств над любым полем I . В то же время если A — конечномерное пространство, то (*) коммутативна, и, таким образом, рассматриваемая диаграмма коммутативна в СМЗК конечномерных векторных пространств.

Целью данной работы является получение некоторых условий коммутативности всех диаграмм канонических естественных преобразований в данной СМЗК.

Как будет показано, коммутативность диаграммы (*) в СМЗК V в совокупности с еще одним условием более специального характера является необходимой и достаточной для коммутативности всех диаграмм канонических естественных преобразований в V . Более сильное (достаточное) условие состоит в том, что $\pi(ec) : A \rightarrow [[A, I], I]$ является изоморфизмом.

В работе широко используются результаты [2] и некоторые идеи структурной теории доказательств, приспособленные к рассматриваемой ситуации, в особенности известный метод понижения глубины формул в пропозициональном исчислении. Применительно к декартово замкнутым категориям этот метод рассматривался автором в [3]; см. также [4].

1. Приведем некоторые сведения, которые необходимы для понимания работы, и дадим формулировку основных результатов.

Как известно, СМЗК может рассматриваться как упорядоченный набор: $\langle V, I, \otimes, [,], a, b, c, \pi \rangle$, где V — категория, $I \in Ob(V)$, $\otimes : V \times V \rightarrow V$ и $[,] : V^{op} \times V \rightarrow V$ — бифункторы; $a = a_{ABC} : (A \otimes B) \otimes C \rightarrow A \otimes (B \otimes C)$, $b = b_A : A \otimes I \rightarrow A$, $c = c_{AB} : A \otimes B \rightarrow B \otimes A$, $\pi = \pi_{ABC} : Hom_V(A \otimes B, C) \rightarrow Hom_V(A, [B, C])$ — естественные по A, B, C изоморфизмы.

Часто рассматриваются также естественные гомоморфизмы:

$$e = e_{AB} = \pi_{[A, B] AB}^{-1}(1_{[A, B]} : [A, B] \otimes A \rightarrow B, \\ d = d_{AB} = \pi_{AB (A \otimes B)}(1_{A \otimes B}) : A \rightarrow [B, A \otimes B]$$

(естественность e по A и d по B понимается в обобщенном смысле из [5]). Данные подчиняются ряду соотношений [2], например, $c \cdot c = 1$, $c^{-1} = c$.

Пусть I — категория, единственным объектом которой является I , а единственным морфизмом $1_I : I \rightarrow I$. Пусть $I : V \rightarrow I$ — постоянный функтор.

Канонические функторы в V — это функторы, которые могут быть получены из 1_V и I при помощи композиции с $\otimes$ и $[,]$. Иначе говоря, они представляются осмысленными выражениями, построенными из символов $1_V, \otimes, [,], I$, включая в случае необходимости также скобки. Канонические естественные преобразования — это естественные преобразования, которые пред-

ставляются осмысленными выражениями, построенными из $a, b, c, a^{-1}, b^{-1}, \pi, \pi^{-1}$ при помощи канонических функторов и композиции. Можно убедиться, что категория, объектами которой являются канонические функторы, а морфизмами — канонические естественные преобразования, является СМЗК [1, 2].

Напомним, что естественное преобразование $h: F \rightarrow G$, где F, G — многоместные функторы, состоит из семейства морфизмов (компонент h) и графа Γh , ребра которого указывают, какие пары аргументов функторов F, G должны быть равны при рассмотрении компонент; по отношению к этим парам аргументов должны выполняться также условия естественности [5].

Например, для $e: [1_V, 1_V] \otimes 1_V \rightarrow 1_V$ граф имеет вид:

$$\begin{array}{c} [1_V, 1_V] \otimes 1_V \rightarrow 1_V \\ \hline \begin{array}{c} | \quad | \quad | \\ \hline | \quad | \quad | \end{array} \end{array}$$

Отметим, что граф Γh обладает достаточно специфическими свойствами: в частности, каждая его компонента связности представляет собой пару вершин, соединенных ребром. Аргументы, соединенные ребром, будем называть сопряженными.

По определению, два естественных преобразования $h, h': F \rightarrow G$ равны тогда и только тогда, когда: 1) $\Gamma h = \Gamma h'$ и 2) для любого выбора аргументов функторов F, G , согласованного с $\Gamma h = \Gamma h'$ (с одинаковыми аргументами, соединенными ребрами графа), соответствующие компоненты h и h' совпадают. В частности, совпадение графов является необходимым условием равенства канонических естественных преобразований.

В уже упоминавшейся работе Келли—Маклейна [1] рассматривается, при каких условиях на канонические функторы (точнее, на представляющие их выражения) совпадение графов канонических естественных преобразований $h, h': F \rightarrow G$ будет достаточным условием равенства $h = h'$ в любой СМЗК.

В наших теоремах 1 и 2 рассматриваются условия, которым должна удовлетворять СМЗК для того, чтобы из равенства графов следовало равенство канонических естественных преобразований $h, h': F \rightarrow G$ (без ограничений на функторы F, G).

Т е о р е м а 1. Если в СМЗК V $\pi(ec): 1_V \rightarrow [[1_V, I], I]$ изоморфизм, то для любых канонических естественных преобразований $h, h': F \rightarrow G$, где $\Gamma h \rightarrow \Gamma h', h = h'$.

Т е о р е м а 2. Для того чтобы в СМЗК V для любой пары канонических естественных преобразований $h, h': F \rightarrow G$ с одним и тем же графом $\Gamma h = \Gamma h'$ имело место равенство $h = h'$, необходимо и достаточно выполнение следующих двух условий: а) $\pi(ec): [1_V, I] \rightarrow [[[1_V, I], I], I]$ и $\pi(\langle \pi(ec) \rangle): [[[1_V, I], I], I] \rightarrow [1_V, I]$ — взаимно обратные изоморфизмы (или, что эквивалентно*, диаграмма (*) коммутативна); б) если $f, g: F \rightarrow G$ — канонические естественные преобразования с одним и тем же графом $\Gamma f = \Gamma g$, то $f([p, I]) = g([p, I]) \Rightarrow f(p) = g(p)$,

* Поскольку $\pi(\langle \pi(ec) \rangle) \pi(ec) = 1$.

где p обозначает пару сопряженных аргументов, соответствующую произвольному ребру графа $\Gamma f = \Gamma g$.

Посмотрим, как связаны теоремы 1 и 2. Из условия теоремы 1 следуют оба условия теоремы 2. Действительно, если $\pi(ec) : 1_V \rightarrow \rightarrow [[1_V, I], I]$ — изоморфизм, то и $\pi(ec) : [1_V, I] \rightarrow [[1_V, I], [I], I]$ — изоморфизм. $\pi(\langle \pi(ec) \rangle)$ обратный к нему, так как $\pi(\langle \pi(ec) \rangle) \cdot \pi(ec) = 1$. Это дает а).

Что касается условия б), то импликация $f(p) = g(p) \Rightarrow f([p, I]) = g([p, I])$ имеет место в любой СМЗК. В свою очередь $f([p, I]) = g([p, I]) \Rightarrow f([[p, I], I]) = g([[p, I], I])$. Далее легко доказать, что, рассматривая композицию $f([[p, I], I])$ и $g([[p, I], I])$ с изоморфизмами, которые можно получить из $k = \pi(ec)$ и k^{-1} (они зависят от вида F и G расположения сопряженных аргументов и их ко- или контравариантности) можно вернуться к $f(p)$ и $g(p)$. Например, если $f(p), g(p) : F(p) \rightarrow G(p)$, причем p ковариантен, то $f([p, I], I), g([p, I], I) : F([p, I], I) \rightarrow G([p, I], I)$ и легко доказать, что $G(k^{-1}) f([p, I], I) = F(k) f$, и аналогично для g . А это дает $f([p, I], I) = g([p, I], I) \Rightarrow f(p) = g(p)$, откуда $f([p, I]) = g([p, I]) \Rightarrow f(p) = g(p)$.

Как будет видно из дальнейшего, условие теоремы 1 не следует из а) & б).

Условие б) играет роль «моста», позволяющего перейти от более сильного условия теоремы 1 к более слабому условию а) теоремы 2. Заметим, что с алгебраической точки зрения условие теоремы 1 можно трактовать как естественную изоморфность пространства и второго сопряженного к нему, а условие а) теоремы 2 — как естественную изоморфность первого и третьего сопряженных пространств.

2. Придадим теперь теореме 2 равносильную, но более «синтаксическую» форму, что позволит перенести в категорную ситуацию идеи теории доказательств, существенно используемые дальше.

Приведем, в основном следуя [2], описание категории форм (shapes) и канонических морфизмов (allowable natural transformations between shapes).

Формы определяются индуктивно. Символы I и I суть формы, если A и B суть формы, то $(A \otimes B)$, $[A, B]$ — формы. Все символы I , которые входят в форму, называются переменными (они считаются различными для разных вхождений), символы I называются константами. Если дана СМЗК V , то каждая форма A определяет канонический функтор $|A|_V$: переменные заменяются на функтор 1_V , константы на функтор I , $\otimes$ и $[,]$ также понимаются как функторы из структуры V . Переменные в A называются ко- или контравариантными, в зависимости от ко- или контравариантности соответствующего аргумента функтора $|A|_V$.

Типом будем называть выражение вида $A \rightarrow B$, где A, B — формы. Форма будет называться простой, если она не имеет вида $C \otimes D$. Всякая форма является тензорным произведением простых форм.

Графом ξ типа $A \rightarrow B$ ($\xi : A \rightarrow B$) называется граф, вершинами которого являются вхождения 1 в A и B и который обладает следующими свойствами: 1) в нем нет изолированных вершин; 2) каждая компонента связности представляет собой пару вершин, соединенных ребром; 3) если вершины связаны ребром и обе лежат в A или B , то они имеют противоположную вариантность; 4) если же одна вершина лежит в A , а другая — в B , то их вариантности совпадают.

Если $\xi : A \rightarrow B$ и $\eta : C \rightarrow D$ — графы, то графы $(\xi \otimes \eta) : A \otimes C \rightarrow B \otimes D$ и $[\xi, \eta] : [B, C] \rightarrow [A, D]$ определяются просто как объединение соответствующих графов. Композиция графов определяется более сложно [1], но нам точное определение не понадобится; можно отметить, что формы и графы в качестве морфизмов образуют СМЗК. Определим индуктивно класс формальных канонических морфизмов, канонические морфизмы будут определяться путем его факторизации. Для любых форм A, B, C формальными каноническими морфизмами являются:

$$a_{ABC} : (A \otimes B) \otimes C \rightarrow A \otimes (B \otimes C), \quad a_{ABC}^{-1} : A \otimes (B \otimes C) \rightarrow (A \otimes B) \otimes C,$$

$$b_A : A \otimes I \rightarrow A, \quad b_A^{-1} : A \rightarrow A \otimes I,$$

$$c_{AB} : A \otimes B \rightarrow B \otimes A, \quad 1_A : A \rightarrow A.$$

Их графы определяются очевидным образом.

Если $f : A \rightarrow B$, $g : C \rightarrow D$ — формальные канонические морфизмы, то и $(f \otimes g) : (A \otimes B) \rightarrow (C \otimes D)$, $[f, g] : [B, C] \rightarrow [A, D]$ — формальные канонические морфизмы. Если $f : A \otimes B \rightarrow C$ — формальный канонический морфизм, то $\pi_{ABC}(f) : A \rightarrow [B, C]$ — формальный канонический морфизм; аналогично, если $f : A \rightarrow [B, C]$ — формальный канонический морфизм, то и $\pi_{ABC}^{-1}(f) : A \otimes B \rightarrow C$ — формальный канонический морфизм. Наконец, если $f : A \rightarrow B$ и $g : B \rightarrow C$ — формальные канонические морфизмы, то их композиция $(g \cdot f) : A \rightarrow C$ — формальный канонический морфизм. Во всех случаях, кроме композиции [1], преобразование графов определяется очевидным образом. Формальные канонические морфизмы рассматриваются просто как синтаксические выражения. Следует отметить, что по записи формального канонического морфизма $f : A \rightarrow B$ можно однозначно установить, какие переменные в индексах $a, a^{-1}, b, b^{-1}, \dots, 1$ «отождествляются» с данной переменной (парой сопряженных переменных) в $A \rightarrow B$.

Определим также операцию подстановки формы вместо пары сопряженных переменных в формальный канонический морфизм. Пусть $f : A \rightarrow B$ — формальный канонический морфизм с графом Γf . Пусть C — форма, а p обозначает пару сопряженных переменных (по отношению к графу Γf). Через $f_p \{C\} : A_p \{C\} \rightarrow B_p \{C\}$ будем обозначать формальный канонический морфизм, полученный заменой p в A и B на C и заменой на C также соответствующих переменных в формах, входящих в выражение f

в качестве индексов. В Γf соответствующее ребро заменяется на «пучок» ребер $C \stackrel{\text{=====}}{\longrightarrow} C$.

Категорию $\mathcal{F}$ получим, факторизуя множество формальных канонических морфизмов по наименьшему отношению эквивалентности, обеспечивающему: естественность всех морфизмов по каждой паре сопряженных переменных; категорные свойства (ассоциативность композиции, свойство единиц, функториальность $\otimes$ и $[,]$), а также выполнение аксиом СМЗК для $a, a^{-1}, b, b^{-1}, c, \pi, \pi^{-1}$. Известно, что это отношение разрешимо [6]. Категория, объектами которой являются формы, а морфизмами — классы эквивалентности формальных канонических морфизмов по этому отношению, будет свободной СМЗК с единственным образующим 1. Формальные канонические морфизмы, рассматриваемые с точностью до указанной выше эквивалентности (обозначим ее просто через $=$), будут называться каноническими морфизмами. Само отношение $=$ будет называться также равенством. Все соотношения, определяющие $=$, инвариантны относительно подстановки форм вместо сопряженных переменных, поэтому $f = g \Rightarrow f \downarrow_p^C = g \downarrow_p^C$.

Пусть КЕП (V) — описанная выше категория канонических функторов и канонических естественных преобразований. Она является СМЗК [2]. Имеется единственный функтор $F_V : \mathcal{F} \rightarrow \text{КЕП}(V)$, сохраняющий структуру СМЗК и переводящий форму 1 в функтор 1_V . Значение $F_V(A)$ — это не что иное, как функтор $|A|_V$, рассмотренный выше. Он переводит $a, a^{-1}, b, b^{-1}, c, \pi, \pi^{-1}$ в соответствующие естественные преобразования категории КЕП (V) , канонический морфизм $f : A \rightarrow B$ — в КЕП $F_V(f) : |A|_V \rightarrow |B|_V$.

Определим отношение $\sim_V$ условием $f \sim_V g \Leftrightarrow F_V(f) = F_V(g)$. Очевидно, $\sim_V$ — отношение эквивалентности на канонических морфизмах. Фактор-категория $\mathcal{F}/\sim_V$ (категория, объекты которой совпадают с объектами $\mathcal{F}$, а морфизмами являются классы эквивалентности канонических морфизмов по $\sim_V$) также будет СМЗК, однако в отличие от $\mathcal{F}$ — не свободной.

Выше было показано, что условия теоремы 2 следует из условия теоремы 1. Поэтому достаточно доказать теорему 2. Из всего сказанного ясно, что теорема 2 эквивалентна следующей теореме.

Т е о р е м а 2'. $f \sim_V g$ для всех канонических морфизмов $f, g : A \rightarrow B$ с одним и тем же графом тогда и только тогда, когда выполняются следующие два условия: а) $\pi(ec) : [1, I] \rightarrow [[1, I], I]$ и $\pi(\langle \pi(ec) \rangle) : [[[1, I], I], I] \rightarrow [1, I]$ — взаимно обратные изоморфизмы в $\mathcal{F}/\sim_V$; б) для любых канонических морфизмов h, h' с одним и тем же графом $\xi_{h_p} \{[p, I]\} \sim_V \sim_V h_p \{[p, I]\} \Rightarrow h \sim_V h'$, где p обозначает переменные произвольной сопряженной пары.

З а м е ч а н и е 1. Здесь можно легко показать, что из условий а) и б) теоремы 2 не следует условие теоремы 1. В самом деле, легко указать такое отношение $\sim$, что в $F/\sim$ выполнены

и а) и б). Однако морфизм $\pi(ec) : 1 \rightarrow [[1, I], I]$ не имеет обратного, так как вообще не существует канонических морфизмов из $[[1, I], I]$ в 1.

Прежде всего сформулируем некоторые факты, необходимые при доказательстве.

1) Теорема когерентности Келли—Маклейна. Пусть $f, g : A \rightarrow B$ — канонические морфизмы, и $\Gamma f = \Gamma g$. Если формы A, B не содержат подформ вида $[C, D]$, где D постоянна, а C не постоянна, то $f = g$.

2) Когерентность центральных морфизмов. Как обычно, центральными морфизмами в $\mathcal{F}$ называются морфизмы, которые получаются из $a, a^{-1}, b, b^{-1}, c, 1$ посредством применений $\otimes, [,]$ и композиции (без использования π и π^{-1}).

Если $f, g : A \rightarrow B$ — центральные морфизмы и $\Gamma f = \Gamma g$, то $f = g$.

3) Устранимость сечения (в алгебраической формулировке). Всякий канонический морфизм $f : A \rightarrow B$ является центральным или имеет один из видов: $f = y(h \otimes g)x$, где x, y — центральные морфизмы, h и g нетривиальны (не имеют в качестве области и кообласти тензорного произведения 1); $f = y(\pi(h))$, где y — центральный морфизм; $f = g(\langle h \rangle \otimes 1)x$, где x — центральный морфизм.

4. Перейдем к доказательству теоремы. Доказательство необходимости тривиально. Пусть $f \sim g$ для всех канонических морфизмов $f, g : A \rightarrow B$ с одним и тем же графом. (Здесь и далее будем писать $\sim$ вместо $\sim_V$, поскольку категорию V можно считать фиксированной). Это влечет за собой а), поскольку а) эквивалентно коммутативности диаграммы (*). Если графы Γf и Γg равны до подстановки, то они равны и после подстановки, таким образом, левая и правая части эквивалентности в б) будут истинными, следовательно, б) также необходимо. Доказательство достаточности занимает всю последующую часть работы. Ввиду его сложности, приведем краткий план.

i) Опираясь на идею понижения глубины формул, заимствованную из теории доказательств, покажем, что в доказательстве достаточности можно ограничиться рассмотрением канонических морфизмов, тип которых имеет специальный вид (справа от стрелки имеется не более одного вхождения $\otimes$ или $[,]$, в то же время все простые тензорные сомножители слева от стрелки содержат не более двух вхождений $\otimes$ или $[,]$). Такие типы называются далее 2-типами.

ii) Используя результаты [2], рассматриваем, какую структуру имеют пары канонических морфизмов $f, g : A \rightarrow B$, где $A \rightarrow B$ 2-тип, $\Gamma f = \Gamma g$, $f \not\sim g$ и f и g имеют минимальный ранг (грубо говоря, их тип имеет минимальную длину) в классе пар канонических морфизмов, обладающих соответствующими свойствами, если этот класс непуст.

iii) В итоге удастся показать, что тип такой минимальной пары содержит слева от стрелки тензорный сомножитель вида

$[[1, I], I]$ или вида $[[1, 1], I]$, а справа от стрелки стоит I . Но это ведет к противоречию, поскольку, применяя после перестановки тензорных сомножителей изоморфизм π и используя условие а) теоремы 2 (условие б) также используется в этой и в предыдущей части доказательства), удастся получить пару неэквивалентных канонических морфизмов меньшего ранга. Таким образом, класс пар неэквивалентных канонических морфизмов $f, g: A \rightarrow B$, имеющих один и тот же граф, должен быть пустым, что доказывает теорему.

5. Символами p, q, r будем обозначать пары сопряженных переменных. При записи соответствующего типа (в предположении, что граф фиксирован) обе сопряженные переменные будем обозначать также соответствующим символом.

Л е м м а 1. Пусть $h, h': A \rightarrow B$ — канонические морфизмы, $\Gamma h = \Gamma h'$. Пусть p — произвольная пара сопряженных переменных. Тогда для любой формы C $h \sim h' \Rightarrow h_p \{C\} \sim h'_p \{C\}$.

Д о к а з а т е л ь с т в о. Графы $\Gamma(h_p \{C\})$ и $\Gamma(h'_p \{C\})$ очевидно совпадают. Компоненты $F_V(h_p \{C\})$ и $F_V(h'_p \{C\})$ могут рассматриваться как компоненты $F_V(h)$ и $F_V(h')$; равенство соответственных компонент $F_V(h)$ и $F_V(h')$ влечет за собой и равенство компонент $F_V(h_p \{C\})$, $F_V(h'_p \{C\})$. По определению отношения $\sim$, получаем $h_p \{C\} \sim h'_p \{C\}$. $\square$

Л е м м а 2. Пусть $f: A \rightarrow B$, $g: B \rightarrow C$ — некоторые канонические морфизмы, а переменные сопряженной пары p входят только в f (только в g). Тогда для любой формы D $(gf)_p \{D\} = g(f_p \{D\})$ (соответственно $(gf)_p \{D\} = (g_p \{D\}) f$).

Д о к а з а т е л ь с т в о. Утверждение следует из определения подстановки и свойств композиции [2]. $\square$

Л е м м а 3. Существует единственный канонический морфизм $h_0: a \rightarrow [[a, p], p]$ и единственный канонический морфизм $g_0: [[q, q], a] \rightarrow a$. При этом $g_0 \cdot h_0 \sim 1_a$.

Д о к а з а т е л ь с т в о. Существование морфизма легко проверяется. Например, $g_0 = e((1_a \otimes \pi(c_{q1} b_q)) b_a^{-1})$, $h_0 = \pi(e_{ap} \times c_{a[a, p]})$. По теореме Келли—Маклейна g_0, h_0 единственны. По этой же теореме $g_0 h_0 = 1_a$, так как тип этой композиции $a \rightarrow a$ (тем более $g_0 h_0 \sim 1_a$). $\square$

Обозначим через $h_0(A)$, $g_0(A)$ стрелки $(h_0)_a \{A\}$ и $(g_0)_a \{A\}$, где A — произвольная форма:

$$h_0(A): A \rightarrow [[A, p], p], \quad g_0(A): [[q, q], A] \rightarrow A.$$

Через $h_0^*(A)$, $g_0^*(A)$ будем обозначать канонические морфизмы, полученные из $h_0(A)$, $g_0(A)$ подстановкой A вместо p и q соответственно:

$$h_0^*(A): A \rightarrow [[A, A], A], \quad g_0^*(A): [[A, A], A] \rightarrow A.$$

Л е м м а 4. $g_0^*(A) h_0^*(A) \sim 1_A$.

Д о к а з а т е л ь с т в о. По лемме 1. $\square$

Л е м м а 5. Для любых канонических морфизмов $f_1, f_2: A \rightarrow B$, $f_1 \sim f_2 \Leftrightarrow h_0(B) f_1 \sim h_0(B) f_2$.

Доказательство. Очевидно, $f_1 \sim f_2 \Rightarrow h_0(B) \times f_1 \sim h_0(B) \times f_2$. Пусть $h_0(B) f_1 \sim h_0(B) f_2$. Это влечет $(h_0(B) \times f_1)_p \{B\} \sim (h_0(B) f_2)_p \{B\}$ ($i = 1, 2$). По лемме 2, $(h_0(B) \times f_1)_p \{B\} \sim h_0^*(B) f_i$ ($i = 1, 2$). Имеем:

$$\begin{aligned} h_0(B) f_1 \sim h_0(B) f_2 &\Rightarrow h_0^*(B) f_1 \sim h_0^*(B) f_2 \Rightarrow \\ &\Rightarrow g_0^*(B) h_0^*(B) f_1 \sim g_0^*(B) h_0^*(B) f_2 \Rightarrow 1_{Bf_1} \sim 1_{Bf_2} \Leftrightarrow f_1 \sim f_2. \end{aligned}$$

Использована лемма 4. $\square$

Л е м м а 6. Для любых канонических морфизмов $f_1, f_2 : A \rightarrow B$ существуют канонические морфизмы $f'_1, f'_2 : A \otimes [B, p] \rightarrow p$ такие, что $f_1 \sim f_2 \Leftrightarrow f'_1 \sim f'_2$.

Доказательство. Заметим, что $h_0(B) \cdot f_i$ имеет тип $A \rightarrow [[B, p], p]$. Можно взять:

$$f'_i = \pi^{-1}(h_0(B) f_i) : A \otimes [B, p] \rightarrow p \quad (i = 1, 2).$$

По лемме 5, и так как π^{-1} — изоморфизм (в том числе в $F/\sim$), $f_1 \sim f_2 \Leftrightarrow f'_1 \sim f'_2$. $\square$

6. Л е м м а 7. Существуют единственные канонические морфизмы:

$$\begin{aligned} h_1 : [p, b] \otimes [a, p] &\rightarrow [a, b], \quad h_2 : [b, p \otimes c] \otimes [p, a] \rightarrow [b, a \otimes c], \\ h_3 : [b, c \otimes p] \otimes [p, a] &\rightarrow [b, c \otimes a], \quad h_4 : [b, [p, c]] \otimes [a, p] \rightarrow [b, [a, c]], \\ h_5 : [p, [b, c]] \otimes [a, p] &\rightarrow [a, [b, c]], \quad h_6 : [b, [c, p]] \otimes [p, a] \rightarrow [b, [c, a]], \\ h_7 : [b \otimes p, c] \otimes [a, p] &\rightarrow [b \otimes a, c], \quad h_8 : [p \otimes b, c] \otimes [a, p] \rightarrow [a \otimes b, c], \\ h_9 : [[b, c], p] \otimes [p, a] &\rightarrow [[b, c], a], \quad h_{10} : [[b, p], c] \otimes [a, p] \rightarrow [[b, a], c], \\ h_{11} : [[p, b], c] \otimes [p, a] &\rightarrow [[a, b], c] \end{aligned}$$

и $g_1, \dots, g_{11}$ типов $B_i \rightarrow B_i \otimes [q, q]$ соответственно (где $B_1 = [a, b]$, $B_2 = [b, a \otimes c]$, ..., $B_{11} = [[a, b], c]$ соответственно, т. е. B_i — форма, стоящая справа от стрелки в типе h_i), такие, что $h_i g_i \sim 1_{B_i}$ ($i = 1, \dots, 11$).

Доказательство. Аналогично лемме 3. $\square$

Обозначим через A_i форму, стоящую слева от стрелки в типе h_i . Например, $A_1 = [p, b] \otimes [a, p]$, $A_2 = [b, p \otimes c] \otimes [p, a]$ и т. д.

Пусть A, B, C — произвольные формы. Через $h_i(A, B, C)$, $g_i(A, B, C)$, $A_i(A, B, C)$, $B_i(A, B, C)$ обозначим $(h_i)_{a, b, c} \{A, B, C\}$, $(g_i)_{a, b, c} \{A, B, C\}$, $(A_i)_{a, b, c} \{A, B, C\}$, $(B_i)_{a, b, c} \{A, B, C\}$ соответственно ($i = 1, \dots, 11$). Если $i = 1$, то третий «аргумент» в действительности фиктивный:

$$\begin{aligned} h_1(A, B, C) &: [p, B] \otimes [A, p] \rightarrow [A, B], \\ g_1(A, B, C) &: [A, B] \rightarrow [A, B] \otimes [q, q], \\ h_2(A, B, C) &: [B, p \otimes C] \otimes [p, A] \rightarrow [B, A \otimes C], \\ g_2(A, B, C) &: [B, A \otimes C] \rightarrow [B, A \otimes C] \otimes [q, q] \end{aligned}$$

$$h_i(A, B, C) : A_i(A, B, C) \rightarrow B_i(A, B, C),$$

$$g_i(A, B, C) : B_i(A, B, C) \rightarrow B_i(A, B, C) \otimes [q, q].$$

Глубиной формы D будем называть число вхождений $\otimes$ и $[\cdot, \cdot]$ в D . Ее примарной глубиной будем называть максимум глубин входящих в ее состав простых тензорных сомножителей. Глубину и примарную глубину обозначим через $d(D)$ и $dp(D)$ соответственно.

Пусть D — простая форма и $d(D) > 2$. Рассмотрим структуру D более детально. Легко видеть, что имеются только следующие возможности (в (1) — (11) ниже A, B, C — формы, такие, что $d(A) \geq 1$):

- 1) $D = [A, B]$ $d(B) \geq 1$, 2) $D = [B, A \otimes C]$, 3) $D = [B, C \otimes A]$,
- 4) $D = [B, [A, C]]$, 5) $D = [A, [B, C]]$, 6) $D = [C, [B, A]]$,
- 7) $D = [B \otimes A, C]$, 8) $D = [A \otimes B, C]$, 9) $D = [[B, C], A]$,
- 10) $D = [[B, A], C]$, 11) $D = [[A, B], C]$.

Отметим, что если D имеет вид, рассмотренный в ii), то $D = B_i(A, B, C)$ ($1 \leq i \leq 11$). В этих случаях $A_i(A, B, C)$ имеет соответственно вид:

- 1) $[p, B] \otimes [A, p]$, 2) $[B, p \otimes C] \otimes [p, A]$, 3) $[B, C \otimes p] \otimes [p, A]$,
- 4) $[B, [p, C]] \otimes [A, p]$, 5) $[p, [B, C]] \otimes [A, p]$,
- 6) $[C, [B, p]] \otimes [p, A]$, 7) $[B \otimes p, C] \otimes [A, p]$,
- 8) $[p \otimes B, C] \otimes [A, p]$, 9) $[[B, C], p] \otimes [p, A]$,
- 10) $[[B, p], C] \otimes [A, p]$, 11) $[[p, B], C] \otimes [p, A]$.

Л е м м а 8. Для любой простой формы D , такой, что $d(D) = dp(D) > 2$ имеются i ($1 \leq i \leq 11$) и формы A, B, C такие, что $D = B_i(A, B, C)$ и $dp(A_i(A, B, C)) < dp(D)$.

Д о к а з а т е л ь с т в о. Найдется i ($1 \leq i \leq 11$), такое, что $D = B_i(A, B, C)$ и $d(A) \geq 1$ (а также $d(B) \geq 1$, если $i = 1$). Легко проверяется, что $dp(A_i(A, B, C)) < dp(B_i(A, B, C)) = dp(D)$. $\square$

Через $h_i^*(A, B, C)$, $q_i^*(A, B, C)$, $A_i^*(A, B, C)$, $B_i^*(A, B, C)$ обозначим канонические морфизмы и формы, полученные из $h_i(A, B, C)$, ..., $B_i(A, B, C)$ подстановкой A вместо переменных p, q (p — в A_i и h_i , q — в B_i g_i).

Легко видеть, что $A_i^*(A, B, C) = B_i^*(A, B, C) \otimes [A, A]$ ($i = 1, \dots, 11$). Таким образом, имеем:

$$h_i^*(A, B, C) : B_i(A, B, C) \otimes [A, A] \rightarrow B_i(A, B, C),$$

$$g_i^*(A, B, C) : B_i(A, B, C) \rightarrow B_i(A, B, C) \otimes [A, A].$$

Л е м м а 9. Для любого $i = 1, \dots, 11$ $h_i^*(A, B, C)$ $q_i^*(A, B, C) \sim 1_{B_i(A, B, C)}$.

Д о к а з а т е л ь с т в о. По лемме 1 и лемме 7. $\square$

Л е м м а 10. Пусть $f_1, f_2 : S \rightarrow T$ — канонические морфизмы и среди простых тензорных сомножителей S имеется форма $D = B_i(A, B, C)$ для некоторых форм A, B, C и числа i ($1 \leq i \leq 11$). Пусть h — канонический морфизм, полученный из $h_i(A, B, C) : A_i(A, B, C) \rightarrow B_i(A, B, C)$ тензорным домножением на единичные морфизмы так, чтобы была определена композиция $f_j h$ ($j = 1, 2$). Тогда $f_1 \sim f_2 \Leftrightarrow f_1 h \sim f_2 h$.

Д о к а з а т е л ь с т в о. Аналогично лемме 5. $\square$

Л е м м а 11. Пусть $f_1, f_2 : S \rightarrow T$ — канонические морфизмы. Тогда существуют канонические морфизмы $f'_1, f'_2 : S' \rightarrow T$, такие, что $dp(S') \leq 2$ и $f_1 \sim f_2 \Leftrightarrow f'_1 \sim f'_2$.

Д о к а з а т е л ь с т в о. Индукция по $dp(S)$. База: $dp(S) \leq 2$ (тривиальный случай).

Индукционный переход: если $dp(A) > 2$, то имеются простые тензорные сомножители $D_1, \dots, D_n$, где $dp(D_j) \geq 2$. По лемме 8 для всякого D_j имеются число i ($1 \leq i \leq 11$) и формы A, B, C , такие, что $D_j = B_i(A, B, C)$ и $dp(A_i(A, B, C)) < dp(B_i(A, B, C)) = dp(D_j)$. Теперь можно рассмотреть композиции f_1, f_2 с подходящими «расширениями» $h_i(A, B, C)$ (полученными домножением на единицы, если это необходимо). Беря композиции f_1, f_2 с этими морфизмами для каждого D_j (порядок несуществен, так как D_j — различные тензорные сомножители), получим некоторые канонические морфизмы $\tilde{f}_1, \tilde{f}_2 : \tilde{S} \rightarrow T$, где $\tilde{f}_1 \sim \tilde{f}_2 \Leftrightarrow f_1 \sim f_2$ (по лемме 10) и $dp(\tilde{S}) < dp(S)$. Теперь можно применить предположение индукции. $\square$

Л е м м а 12. Пусть $f_1, f_2 : S \rightarrow T$ — некоторые канонические морфизмы. Тогда имеются канонические морфизмы $f'_1, f'_2 : S' \rightarrow b$, где b — переменная, $dp(S') \leq 2$ и $f_1 \sim f_2 \Leftrightarrow f'_1 \sim f'_2$.

Д о к а з а т е л ь с т в о. По лемме 6 и лемме 11. $\square$

7. Пусть в типе $S \rightarrow T$ форма T имеет вид $a, [a; b]$ или $a \otimes b$, а простые тензорные сомножители S имеют вид $a, [a, b], [la, b], cl, [a \otimes b, cl], [a, b \otimes cl], [a, [b, cl]]$, где a, b — переменные или I . Тогда тип $S \rightarrow T$ будет называться 2-типом. Будем также называть 2-типом всякий тип $S' \rightarrow T'$, такой, что имеются центральные морфизмы $S \rightarrow S'$ и $T' \rightarrow T$, где $S \rightarrow T$ есть 2-тип в смысле, описанном выше. Канонические морфизмы $f : S \rightarrow T$, где $S \rightarrow T$ 2-тип, будут называться 2-морфизмами.

З а м е ч а н и е 2. По лемме 12 для любых канонических морфизмов f_1, f_2 имеются 2-морфизмы f'_1, f'_2 , такие, что $f_1 \sim f_2 \Leftrightarrow f'_1 \sim f'_2$.

Обозначим через $\mathcal{B}$ класс пар 2-морфизмов с одним и тем же графом. Будем исследовать свойства пересечений $\mathcal{W} \cap \mathcal{B}$ и $\mathcal{W}_0 \cap \mathcal{B}$, где $\mathcal{W}$ есть класс пар $f_1, f_2 : S \rightarrow T$ канонических морфизмов с одним и тем же графом, таких, что $f_1 \neq f_2$, и $\mathcal{W}_0$ порождает $\mathcal{W}$ [2] (см. ниже). Увидим, что $\mathcal{W} \cap \mathcal{B}$ содержится в подклассе $\mathcal{W}$, порожденном $\mathcal{W}_0 \cap \mathcal{B}$ (тем же путем, как в [2]).

Напомним определения. $\mathcal{W}_0$ — это класс тех пар (f_1, f_2) канонических морфизмов, которые удовлетворяют следующим условиям:

они имеют один и тот же тип, один и тот же граф и могут быть записаны при помощи операции $\langle \rangle$ следующим образом:

$$f_1 = S \xrightarrow{x} ([B, C] \otimes A) \otimes D \xrightarrow{\langle h_1 \rangle \otimes 1} C \otimes D \xrightarrow{g_1} T,$$

$$f_2 = S \xrightarrow{x'} ([B', C'] \otimes A') \otimes D' \xrightarrow{\langle h_2 \rangle \otimes 1} C' \otimes D' \xrightarrow{g_2} T,$$

где x, x' — центральные морфизмы, h_1, h_2, g_1, g_2 — некоторые канонические морфизмы, и при этом:

- 1) формы B и B' не являются постоянными;
- 2) Γh_1 и Γh_2 не могут быть представлены в виде графов канонических морфизмов вида $g(\langle f \rangle \otimes 1)u$;
- 3) $[B, C]$ соответствует некоторому простому тензорному сомножителю A' (через посредство изоморфизма $x'x^{-1}$);
- 4) $[B', C']$ соответствует простому сомножителю A через посредство $x(x')^{-1}$;
- 5) ни f_1 , ни f_2 не могут быть записаны в виде центральных морфизмов, тензорного произведения или результата применения π к какому-либо каноническому морфизму.

Здесь $\mathscr{W}$ есть наименьший класс пар канонических морфизмов, удовлетворяющий следующим условиям:

- $\mathscr{W}1$) $\mathscr{W}_0$ содержится в этом классе;
- $\mathscr{W}2$) если $(f_1, f_2 : T \rightarrow S)$ содержится в этом классе и $u : T' \rightarrow T, v : S \rightarrow S'$ — центральные, то $(vf_1u, vf_2u : T' \rightarrow S')$, содержится в нем;

$\mathscr{W}3$) если по крайней мере одна из пар $(f_1, f'_1 : A \rightarrow C)$ и $(f_2, f'_2 : B \rightarrow D)$ содержится в этом классе (причем если (f_i, f'_i) не содержится в нем, тогда $f_i = f'_i$), то и $(f_1 \otimes f_2, f'_1 \otimes f'_2 : A \otimes B \rightarrow C \otimes D)$ содержится в нем;

$\mathscr{W}4$) если $(f_1, f_2 : A \otimes B \rightarrow C)$ содержится в этом классе, то и $(\pi(f_1), \pi(f_2) : A \rightarrow [B, C])$ содержится в нем;

$\mathscr{W}5$) если по крайней мере одна из пар $(f_1, f'_1 : A \rightarrow B)$ и $(f_2, f'_2 : C \otimes D \rightarrow E)$ содержится в этом классе (если (f_i, f'_i) в нем содержится, тогда $f_i = f'_i$), то $(f_2 \cdot (\langle f_1 \rangle \otimes 1); f'_2 \cdot (\langle f'_1 \rangle \otimes 1) : ([B, C] \otimes A) \otimes D \rightarrow E)$ содержится в нем.

З а м е ч а н и е 3. Класс $\mathscr{W}$ не изменится, если в $\mathscr{W}3 - \mathscr{W}5$ рассматривать только случай, когда f_i, f'_i — нетривиальны, поскольку если один из них тривиален, т. е. имеет тип $(I \otimes \dots) \otimes I \rightarrow (I \otimes \dots) \otimes I$, то можно применить $\mathscr{W}2$.

В [2] показано, что $f_1 \neq f_2$ (где $f_1, f_2 : A \rightarrow B$ и $\Gamma f_1 = \Gamma f_2$) тогда и только тогда, когда $(f_1, f_2) \in \mathscr{W}$. Следовательно, если $f_1 \sim f_2$, то $(f_1, f_2) \in \mathscr{W}$.

Л е м м а 13. Пусть $(f, g) \in \mathscr{W} \cap \mathscr{B}$. Тогда f, g могут быть представлены в одном из видов, рассмотренных в $\mathscr{W}1 - \mathscr{W}5$, где $(f_1, f'_1), (f_2, f'_2) \in \mathscr{B}$ (и, таким образом, по крайней мере одна из пар $(f_1, f'_1) (f_2, f'_2) \in \mathscr{W} \cap \mathscr{B}$).

Д о к а з а т е л ь с т в о. Легко проверить, что если тип f и g есть 2-тип и имеет один из видов, рассмотренных в $\mathscr{W}3 - \mathscr{W}5$ (случаи $\mathscr{W}1, \mathscr{W}2$ тривиальны), то типы f_1, f'_1, f_2, f'_2 необходимо являются 2-типами. Например, если $(([B, C] \otimes A) \otimes D \rightarrow E$

есть 2-тип, то $C \otimes D \rightarrow E$ и $A \rightarrow B$ суть 2-типы (действительно, вид $C \otimes D$, E и A автоматически подпадает под требуемый определением 2-тип, и легко видеть, рассматривая возможные виды $[B, C]$, что B есть a , $[a, b]$ или $a \otimes b$ и, следовательно, $A \rightarrow B$ также удовлетворяет определению 2-типа). Остальные случаи рассматриваются еще проще.

Следуя [2], введем понятие ранга формы, типа и канонического морфизма. Ранг определяется следующими правилами: $r(1) = 1$, $r(I) = 0$, $r(S \otimes T) = r(S) + r(T)$, $r([S, T]) = r(S) + r(T) + 1$. Если имеем тип $S \rightarrow T$, то ранг $r(S \rightarrow T) = r(S) + r(T)$; $r(f)$, где $f: S \rightarrow T$ есть $r(S \rightarrow T)$. Морфизм $h: S \rightarrow T$ называется тривиальным, если $r(h) = 0$.

Л е м м а 14. Если $x: A \rightarrow B$ — центральный морфизм, то $r(A) = r(B)$.

Тип $A \rightarrow B$ будем называть чистым, если в A , B нет подформ вида $C \otimes D$, где одна из форм, C или D , — постоянна.

Если $S \rightarrow T$ — тип, то имеются центральные морфизмы $x: S' \rightarrow S$, $x': T \rightarrow T'$, такие, что $S' \rightarrow T'$ — чистый тип.

Будем называть 2-тип $S \rightarrow T$ $\sim$ -минимальным, если он чистый и имеются канонические морфизмы $f_1, f_2: S \rightarrow T$, где $\Gamma f_1 = \Gamma f_2$, такие, что $f_1 \not\sim f_2$, но для всех 2-типов $S' \rightarrow T'$, где $r(S' \rightarrow T') < r(S \rightarrow T)$, и канонических морфизмов $f'_1, f'_2: S' \rightarrow T'$, таких, что $\Gamma f'_1 = \Gamma f'_2$, имеет место $f'_1 \sim f'_2$. Пара канонических морфизмов (f_1, f_2) также будет называться $\sim$ -минимальной.

Из условий а), б) теоремы 2' следует, что не существует минимальных 2-типов и пар канонических морфизмов и, следовательно, все канонические морфизмы одного типа с одинаковыми графами $\sim$ -эквивалентны.

Изучим теперь структуру $\sim$ -минимальных типов и пар (здесь не предполагается, что а) и б) обязательно выполнены).

Л е м м а 15. Если (f, g) является $\sim$ -минимальной парой, то $(f, g) \in \mathcal{W}_0 \cap \mathcal{B}$.

Д о к а з а т е л ь с т в о. Очевидно, $f \not\sim g$ влечет $f \neq g$. Следовательно, $(f, g) \in \mathcal{W} \cap \mathcal{B}$. Если $(f, g) \notin \mathcal{W}_0$, то имеются центральные изоморфизмы u, v , такие, что пара (ufv, ugv) имеет одно из представлений $\mathcal{W}3$ — $\mathcal{W}5$. Легко проверяется (принимая во внимание замечание 3), что в этом случае ранг канонических морфизмов f_1, f_1, f_2, f_2 , рассмотренных в $\mathcal{W}3$ — $\mathcal{W}5$, меньше, чем ранг f и g . Это противоречит гипотезе, что (f, g) есть $\sim$ -минимальная пара.

Л е м м а 16. Если $(f, g: A \rightarrow B)$ есть $\sim$ -минимальная пара, то B есть переменная или I .

Д о к а з а т е л ь с т в о. По определению класса $\mathcal{W}_0$, f, g не имеют вида « $\otimes$ », « π » или «центрального». Теорема об устранении сечения приводит теперь к тому, что B не может иметь вид $B_1 \otimes B_2$ или $[B_1, B_2]$. $A \rightarrow B$ — чистый 2-тип, и, следовательно, остаются только две возможности: B есть переменная или I . $\square$

9. В этом разделе покажем, что в действительности B должно совпадать с I . Это будет следовать из условия б) теоремы 2'.

Чтобы доказать это, воспользуемся методом исключения переменных, а также понижения глубины формул, заимствованным из теории доказательств.

Пусть A — форма, p — переменная в A . Запишем это в виде $A(p)$. Определим канонический морфизм $K_{A(p)}$ рекурсивно следующим образом. Если p — ковариантна (контравариантна) в $A(p)$, то $K_{A(p)} : A(I) \otimes p \rightarrow A(p)$ ($K_{A(p)} : A(p) \otimes p \rightarrow I$) соответственно. Здесь $A(I) = A_p \{I\}$. Используем рекурсию по процессу построения A . Пусть $A = p$. Положим $K_p = b_p c_{Ip} : I \otimes p \rightarrow p$.

Если $A \neq p$, то A может иметь один из видов:

$$A_1(p) \otimes A_2, A_1 \otimes A_2(p), [A_1(p), A_2], [A_1, A_2(p)],$$

где p — ко- или контравариантна. Ниже x будет обозначать подходящий центральный изоморфизм.

Пусть $A = A_1 \otimes A_2(p)$ и переменная p — ковариантна. Тогда

$$K_A = (A_1 \otimes A_2(I)) \otimes p \xrightarrow{a_1} A_1 \otimes (A_2(I) \otimes p) \xrightarrow{1 \otimes K_{A_2}} A_1 \otimes A_2(p).$$

Если p контравариантна в A_2 , то

$$K_A = (A_1 \otimes A_2(p)) \otimes p \xrightarrow{a} A_1 \otimes (A_2(p) \otimes p) \xrightarrow{1 \otimes K_{A_2}} A_1 \otimes A_2(I).$$

Подобным образом определяется K_A для $A = A_1(p) \otimes A_2$ (вместо a будет другой центральный изоморфизм).

Пусть $A = [A_1(p), A_2]$ и p — контравариантна в A (и ковариантна в A_1).

Рассмотрим композицию:

$$K_{\bar{A}} = ([A_1(p), A_2] \otimes p) \otimes A_1(I) \xrightarrow{x} [A_1(p), A_2] \otimes (A_1(I) \otimes p) \xrightarrow{\langle K_{A_1} \rangle} A_2.$$

Теперь

$$K_A = \pi(K_{\bar{A}}) = \pi(e(1 \otimes K_{A_1})x).$$

Пусть p — ковариантна в A и контравариантна в A_1 . Рассмотрим композицию:

$$K_{\bar{A}} = ([A_1(I), A_2] \otimes p) \otimes A_1(p) \xrightarrow{x} [A_1(I), A_2] \otimes \otimes (A_1(p) \otimes p) \xrightarrow{\langle K_{A_1} \rangle} A_2$$

и положим $K_A = \pi(K_{\bar{A}}) = \pi(e(1 \otimes K_{A_1})x)$, как выше (x — центральный изоморфизм).

Пусть $A = [A_1, A_2(p)]$. Если p контравариантна в A и A_2 , то возьмем

$$K_{\bar{A}} = ([A_1, A_2(p)] \otimes p) \otimes A_1 \xrightarrow{x} ([A_1, A_2(p)] \otimes A_1) \otimes \otimes p \xrightarrow{e \otimes 1} A_2(p) \otimes p \xrightarrow{K_{A_2}} A_2(I)$$

и

$$K_A = \pi(K_{\bar{A}}) = \pi(K_{A_2}(e \otimes 1)x).$$

Если p ковариантна в A и A_2 , то положим:

$$\begin{aligned} K_{\bar{A}} &= ([A_1, A_2(I)] \otimes p) \otimes A_1 \xrightarrow{x} ([A_1, A_2(I)] \otimes A_1) \otimes \\ &\otimes p \xrightarrow{e \otimes 1} A_2(I) \otimes p \xrightarrow{K_{A_2}} A_2(p) \end{aligned}$$

и

$$K_A = \pi(K_{\bar{A}}) = \pi(K_{A_2}(e \otimes 1)x).$$

Л е м м а 17. Пусть $y(p) : A(p) \rightarrow A'(p)$ — центральный изоморфизм. Тогда, если p ковариантна в A , имеем:

$$\begin{aligned} K_{A'} : A'(I) \otimes p &\rightarrow A'(p) = y(p) K_A (y^{-1}(I) \otimes 1) = \\ &= A'(I) \otimes p \xrightarrow{y^{-1}(I) \otimes 1} A(I) \otimes p \xrightarrow{K_A} A(p) \xrightarrow{y} A'(p). \end{aligned}$$

Если p контравариантна в A , то

$$\begin{aligned} K_{A'} : A'(p) \otimes p &\rightarrow A'(I) = y(I) K_A (y^{-1} \otimes 1) = \\ &= A'(p) \otimes p \xrightarrow{y^{-1} \otimes 1} A(p) \otimes p \xrightarrow{K_A} A(I) \xrightarrow{y(I)} A'(I). \end{aligned}$$

Д о к а з а т е л ь с т в о. По определению K_A . $\square$

Л е м м а 18. Пусть p является простым тензорным сомножителем $A(p)$. Тогда $K_A : A(I) \otimes p \rightarrow A(p)$ — центральный изоморфизм.

Д о к а з а т е л ь с т в о. По определению K_A . $\square$

Л е м м а 19. Пусть $f : B \otimes p \rightarrow A(p)$ — центральный изоморфизм. Тогда существует $f_0 : B \rightarrow A(I)$, такой, что $f = K_A \cdot (f_0 \otimes 1) = B \otimes p \xrightarrow{f_0 \otimes 1} A(I) \otimes p \xrightarrow{K_A} A(p)$.

Д о к а з а т е л ь с т в о. Очевидно, p — простой тензорный сомножитель $A(p)$. В качестве f_0 можно взять $(f_p \{I\}) b^{-1} : B \rightarrow A(I)$. Теперь используем лемму 18 и когерентность центральных морфизмов. $\square$

Л е м м а 20. Пусть $f : A(p) \otimes p \rightarrow C$ ($f : B \otimes p \rightarrow A(p)$) — некоторый канонический морфизм. Тогда

$$f = f_0 \cdot K_A = A(p) \otimes p \xrightarrow{K_A} A(I) \xrightarrow{f_0} C$$

(соответственно $f = K_A (f_0 \otimes 1) = B \otimes p \xrightarrow{f_0 \otimes 1} A(I) \otimes p \xrightarrow{K_A} A(p)$).

Д о к а з а т е л ь с т в о индукцией по рангу f .

База: пусть $r(f) = 2$. В этом случае f имеет тип вида $B \otimes p \rightarrow A(p)$ с формой $A(p)$, изоморфной p , и постоянной B . Очевидно, f — центральный изоморфизм, и можно применить лемму 19.

Индукционный переход: рассмотрим несколько случаев. В силу устранимости сечения f является центральным или имеет один из видов: $f = y(h \otimes g)x$ с центральными x и y и нетривиальными h и g ; $f = y(\pi(h))$ с центральным y ; $f = g((h) \otimes 1)x$.

Если f — центральный изоморфизм, можно применить лемму 19. Рассмотрим остальные случаи. (Если рассматривается не оговоренная особо специализация вида f , то она легко может быть получена путем использования подходящих центральных изоморфизмов).

I. $f = y(h \otimes g)x$, где x, y — центральные изоморфизмы.

I.1. $f = B \otimes p \xrightarrow{x} B_1 \otimes (B_2 \otimes p) \xrightarrow{h \otimes g} A_1 \otimes A_2(p) \xrightarrow{y} A(p)$.

По предположению индукции, $g = K_{A_2}(g_1 \otimes 1)$ для некоторого $g_1: B_2 \rightarrow A_2(I)$, здесь $K_{A_2}: A_2(I) \otimes p \rightarrow A_2(p)$.

Имеем также $y(I) = y_p\{I\}: A_1 \otimes A_2(I) \rightarrow A(I)$. Теперь

$$\begin{aligned} f &= y(h \otimes g)x = y(h \otimes K_{A_2}(g_1 \otimes 1))x = y(1 \otimes K_{A_2})(h \otimes (g_1 \otimes 1))x = \\ &= y(1 \otimes K_{A_2})a(y^{-1}(I) \otimes 1)(y(I) \otimes 1)a^{-1}(h \otimes (g_1 \otimes 1))x = \\ &= K_A(y(I) \otimes 1)a^{-1}(h \otimes (g_1 \otimes 1))x. \end{aligned}$$

В последнем равенстве использован тот факт, что $(1 \otimes K_{A_2})a = K_{A_1 \otimes A_2}$ (по определению K_A) и $y(K_{A_1 \otimes A_2}(y^{-1}(I) \otimes 1)) = K_A$ (по лемме 17). Используя естественность a^{-1} и когерентность центральных изоморфизмов (что дает $a^{-1}x = (x_1 \otimes 1)$ для некоторого центрального x_1), получаем

$$\begin{aligned} K_A(y(I) \otimes 1)a^{-1}(h \otimes (g_1 \otimes 1))x &= K_A((y(I)(h \otimes g_1)) \otimes 1)a^{-1}x = \\ &= K_A((y(I)(h \otimes g_1) \otimes 1)(x_1 \otimes 1)) = K_A((y(I)(h \otimes g)) \otimes 1). \end{aligned}$$

В качестве f_0 можно взять $y(I)(h \otimes g_1)x_1$.

I.2. $f = A(p) \otimes p \xrightarrow{x} A_1 \otimes (A_2(p) \otimes p) \xrightarrow{h \otimes g} C_1 \otimes C_2 \xrightarrow{y} C$. Отметим, что $x = a(x_1 \otimes 1)$, где $x_1: A(p) \rightarrow A_1 \otimes A_2(p)$.

По предположению индукции $g = g_1 K_{A_2}$. Теперь

$$\begin{aligned} f &= g(h \otimes g)x = y(h \otimes (g_1 K_{A_2}))a(x_1 \otimes 1) = \\ &= y(h \otimes g_1)(1 \otimes K_{A_2})a(x_1 \otimes 1) = y(h \otimes g_1)K_{A_1 \otimes A_2}(x_1 \otimes 1) = \\ &= y(h \otimes g_1)x_1(I)x_1^{-1}(I)K_{A_1 \otimes A_2}(x_1 \otimes 1) = y(h \otimes g_1)(x_1(I)K_A \end{aligned}$$

(лемма 17; как выше, $x_1(I) = (x_1)p\{I\}$). Можно взять $f_0 = y(h \otimes g_1)x_1(I)$.

II. $f = y\pi(h)$, где y — центральный изоморфизм.

II.1. $f = A(p) \otimes p \xrightarrow{\pi(h)} [C_1, C_2] \xrightarrow{y} C$, $h: (A(p) \otimes p) \otimes C_1 \rightarrow C_2$; можно считать, что $h = (A(p) \otimes p) \otimes C_1 \xrightarrow{x_1} (A(p) \otimes C_1) \otimes p \xrightarrow{h_1} C_2$ ($x_1 = a^{-1}(1 \otimes c)a$). По предположению индукции $h_1 = h_2 K_{A \otimes C_1}$. По определению K_A и ввиду когерентности центральных изоморфизмов $K_{A \otimes C_1} = (K_A \otimes 1_{C_1})x_1^{\dagger}$. Следовательно, $h = h_2(K_A \otimes 1_{C_1})$, $\pi(h) = \pi(h_2(K_A \otimes 1_{C_1})) = \pi(h_2)K_A$ ввиду естественности π . Таким образом, $f = y\pi(h_2)K_A$ и можно положить $f_0 = y\pi(h_2)$.

II.2. $f = B \otimes p \xrightarrow{\pi(h)} [A_1, A_2(p)] \xrightarrow{y} A(p)$ (p ковариантно входит в A_2). Здесь $h: (B \otimes p) \otimes A_1 \rightarrow A_1(p)$. Очевидно, h

можно рассматривать как композицию:

$$h = (B \otimes p) \otimes A_1 \xrightarrow{x_1} (B \otimes A_1) \otimes p \xrightarrow{h_1} A_2(p) (x_1 = a^{-1} (1 \otimes c) a).$$

Применяя предположение индукции, имеем:

$$h_1 = K_{A_2}(h_2 \otimes 1_p), \quad (h_2: B \otimes A_1 \rightarrow A_2(I), \quad K_{A_2}: A_2(I) \otimes p \rightarrow A_2(p)).$$

Таким образом,

$$\begin{aligned} h &= k_{A_2}(h_2 \otimes 1_p) x_1, \quad \pi(h) = \pi(K_{A_2}(h_2 \otimes 1_p) x_1) = \pi(K_{A_2}(e(\pi(h_2) \otimes \\ &\otimes 1_{A_1})) \otimes 1_p) x_1) = (\text{заметим, что } h_2 = \pi^{-1}(\pi(h_2)) = e(\pi(h_2) \otimes 1_{A_1})) = \\ &= \pi(K_{A_2}((e \otimes 1_p)((\pi(h_2) \otimes 1_{A_1}) \otimes 1_p) x_1)) = (\text{ввиду естественности} \\ &\pi \text{ и } x_1) = \pi(K_{A_2}(e \otimes 1_p) \bar{x}_1 ((\pi(h_2) \otimes 1_p) = (\bar{x}_1 \text{ получено выше} \\ &\text{заменой } B \text{ на } [A_1, A_2(p)] \text{ в } x_1) = K_{[A_1, A_2(p)]}(\pi(h_1) \otimes 1_p), \\ f &= yK_{[A_1, A_2(p)]}(\pi(h_2) \otimes 1_p) = yK_{[A_1, A_2]}(y^{-1}(I) \otimes 1_p) \times \\ &\times ((y(I) \pi(h_2)) \otimes 1_p) = K_A((y(I) \pi(h_2)) \otimes 1_p) \end{aligned}$$

(лемма 17). В качестве f_0 можно взять $y(I) \pi(h_2)$.

II.3. $f = B \otimes p \xrightarrow{\pi(h)} [A(p), A_2] \xrightarrow{y} A(p)$ (p контравариантно в A_1), $h: (B \otimes p) \otimes A_1(p) \rightarrow A_2$. Можно считать, что h есть композиция:

$$h = (B \otimes p) A_1(p) \xrightarrow{x} (B \otimes A_1(p)) \otimes p \xrightarrow{h_1} A_2,$$

$h_1 = h_2 K_{B \otimes A_1}$ по индукционному предположению.

Здесь $h_2: B \otimes A_1(I) \rightarrow A_2$, $K_{B \otimes A_1}: (B \otimes A_1(p)) \otimes p \rightarrow B \otimes A_1(I)$, $\pi(h) = \pi(h_2 K_{B \otimes A_1} x)$.

По определению $K_{B \otimes A_1} = (1_B \otimes K_{A_1}) a$. Таким образом:

$$\begin{aligned} \pi(h_2(1_B \otimes K_{A_1})) &= (\text{как в II. 2, } h_2 = e(\pi(h_2) \otimes 1_{A_1})) = \\ &= \pi(e(\pi(h_2) \otimes 1_{A_1})(1 \otimes K_{A_1}) ax) = \pi(e(1 \otimes K_{A_1})(\pi(h_2) \otimes \\ &\otimes (1_A \otimes p)) ax) = \pi(\langle K_{A_1} \rangle a \bar{x} ((\pi(h_2) \otimes 1_{A_1}) \otimes 1_p)) = \end{aligned}$$

(здесь используется естественность a и x ; $\bar{x}$ получается из x

$$\begin{aligned} \text{заменой } B \text{ на } [A_1, A_2]) &= \pi(\langle K_A \rangle a \bar{x})(\pi(h_2) \otimes 1_p) = \\ &= (\text{по определению } K) = K_A(\pi(h_2) \otimes 1_p). \end{aligned}$$

Можно положить $f_0 = \pi(h_2)$.

III. $f = g(\langle h \rangle \otimes 1) x$.

III.1. $f = A(p) \otimes p \xrightarrow{x} ([B_1, C_1] \otimes A_1) \otimes D \xrightarrow{(h) \otimes 1} C_1 \otimes D \xrightarrow{g} C$.

III.1.1. Контравариантное вхождение p лежит в D . В этом случае ковариантное вхождение p также лежит в D (из рассмотрения графов f, g, h следует, что оно не может лежать в A_1 ; ясно, что оно не может лежать также в $[B_1, C_1]$). Имеем

$$\begin{aligned} f &= A(p) \otimes p \xrightarrow{x} ([B_1, C_1] \otimes A_1) \otimes (D_1(p) \otimes p) \xrightarrow{(h) \otimes 1} C_1 \otimes \\ &\otimes (D_1(p) \otimes p) \xrightarrow{g} C. \end{aligned}$$

Применяя предположение индукции g , имеем:

$$\begin{aligned} g &= g_1(1_{C_1} \otimes K_{D_1}); f = g_1(1_{C_1} \otimes K_{D_1})(\langle h \rangle \otimes 1)x = \\ &= g_1(\langle h \rangle \otimes 1_{D_1(I)})(1 \otimes K_{D_1})x = g_1(\langle h \rangle \otimes 1_{D_1(I)})(1 \otimes K_{D_1})aa^{-1}x = \\ &\quad (\text{заметим, что } g = (ga)a^{-1} = (g_1(1_{C_1} \otimes K_{D_1})a)a^{-1} = \\ &= g_1(K_{C_1 \otimes D_1})a^{-1}) = g_1(\langle h \rangle \otimes 1_{D_1(I)})K_{C_1 \otimes D_1}(x_1 \otimes 1) = \\ (\text{здесь } x_1 - \text{центральный изоморфизм, } x_1: A(p) \rightarrow ([B_1, C_1] \otimes A_1) \otimes \\ &\otimes D_1(p)) = g_1(\langle h \rangle \otimes 1_{D_1(I)})x_1(I)x_1^{-1}(I)K_{C_1 \otimes D_1}(x_1 \otimes 1) = \\ &= (\text{по лемме 17}) = g_1(\langle h \rangle \otimes 1_{D_1(I)})x_1(I)K_A. \end{aligned}$$

Можно взять $g_1(\langle h \rangle \otimes 1_{D_1(I)})x_1(I)$ в качестве f_0 .

III.1.2. Контравариантное вхождение p лежит в A_1 . В этом случае ковариантное вхождение также лежит в A_1 (рассматриваем графы f, g, h). Имеем:

$$f = A(p) \otimes p \xrightarrow{x} ([B_1, C_1] \otimes (A'_1(p) \otimes p)) \otimes D \xrightarrow{\langle h \rangle \otimes 1} C_1 \otimes D \xrightarrow{g} C.$$

Здесь $h'_1: A_1(p) \otimes p \rightarrow B_1$. Применяя к h индукционное предположение, получаем $h = h_1 \cdot K_{A'_1}$. Поскольку $\langle h \rangle = e(1 \otimes h)$, имеем:

$$\begin{aligned} \langle h \rangle &= e(1 \otimes (h_1 K_{A'_1})) = e(1 \otimes h_1)(1 \otimes K_{A'_1}) = \langle h_1 \rangle(1 \otimes K_{A'_1}), \\ f &= g(\langle h \rangle \otimes 1)x = g(\langle h_1 \rangle(1 \otimes K_{A'_1}) \otimes 1)x = \\ &= g(\langle h_1 \rangle \otimes 1)((1 \otimes K_{A'_1}) \otimes 1)x = \\ &= g(\langle h_1 \rangle \otimes 1)x(I)x^{-1}(I)((1 \otimes K_{A'_1}) \otimes 1)x = g(\langle h_1 \rangle \otimes 1)x(I)K_A. \end{aligned}$$

(Равенство $x^{-1}(I)((1 \otimes K_{A'_1}) \otimes 1)x = K_A$ следует из определения K_A).

Можно положить $g(\langle h_1 \rangle \otimes 1)x(I) = f_0$.

III.1.3. Контравариантное вхождение p лежит в C_1 . В этом случае ковариантное вхождение лежит в D (рассматриваем графы f, g, h). Имеем:

$$\begin{aligned} f &= A(p) \otimes p \xrightarrow{x} ([B_1, C_1(p)] \otimes A_1) \otimes (D_1 \otimes p) \xrightarrow{\langle h \rangle \otimes 1} C_1(p) \otimes \\ &\otimes (D_1 \otimes p) \xrightarrow{g} C. \end{aligned}$$

Используя другие центральные изоморфизмы, f можно представить в виде:

$$\begin{aligned} f &= A(p) \otimes p \xrightarrow{x'} ([B_1, C_1(p)] \otimes A_1) \otimes p \otimes D_1 \xrightarrow{(\langle h \rangle \otimes 1) \otimes 1} (C_1(p) \otimes \\ &\otimes p) \otimes D_1 \xrightarrow{g_1} C. \end{aligned}$$

Здесь $g_1: (C_1(p) \otimes p) \otimes D_1 \rightarrow C$, $g_1 = g_2 z = (C_1(p) \otimes p) \otimes D_1 \xrightarrow{z} (C_1(p) \otimes D_1) \otimes p \xrightarrow{g_2} C$, $g_2 = g'_2 K_{C_1 \otimes D_1} z = g'_2(K_{C_1} \otimes 1)$ (по

определению K). Как и выше, $\langle h \rangle \otimes 1_p = e(1 \otimes h) \otimes 1_p$,

$$\begin{aligned} f &= g'_2(K_{C_1} \otimes 1_{D_1})(((e(1 \otimes h)) \otimes 1_p) \otimes 1_{D_1})x' = \\ &= g'_2(K_{C_1}(e(1 \otimes h) \otimes 1_{D_1})x' = g'_2((K_{C_1}(e \otimes 1_p)((1 \otimes h) \otimes 1_p)) \otimes 1_{D_1})x' = \\ &= g'_2((K_{C_1}(e \otimes 1_p)yy^{-1}((1 \otimes h) \otimes 1_p)) \otimes 1_{D_1})x' = \\ &(\text{здесь } y: ([B_1, C_1] \otimes p) \otimes B_1 \rightarrow ([B_1, C_1] \otimes B_1) \otimes p) \\ &= g'_2(e(K_{[B_1, C_1]} \otimes 1_{B_1})y^{-1}((1 \otimes h) \otimes 1_p)) \otimes 1_{D_1})x' = \\ &(\text{по определению } K \text{ и } \pi) \\ &= g'_2(e(K_{([B_1, C_1] \otimes B_1)})((1 \otimes h) \otimes 1) \otimes 1_{D_1})x' = \\ &(\text{ввиду естественности } K \text{ по аргументу } B_1) \\ &= g_2(e(1 \otimes h))(K_{([B_1, C_1] \otimes A_1)})x' = g_2e(1 \otimes h)K_A. \end{aligned}$$

Можно положить $g'_2e(1 \otimes h)$ как f_0 .

III.1.4. Контравариантное вхождение p лежит в B_1 (в B_1 оно ковариантно). В этом случае p лежит в A_1 (рассматриваем графы).

Можно предположить (в случае необходимости можно использовать подходящие центральные изоморфизмы), что

$$f = A(p) \otimes p \xrightarrow{x} ([B_1(p), C_1] \otimes (A_1 \otimes p)) \otimes D \xrightarrow{(h) \otimes 1} C_1 \otimes D \xrightarrow{g} C.$$

Здесь $h: A_1 \otimes p \rightarrow B_1(p)$.

Применив предположение индукции к h , получаем:

$$\begin{aligned} h &= A_1 \otimes p \xrightarrow{h_1 \otimes 1_p} B_1(I) \otimes p \xrightarrow{K_{B_1}} B_1(p), \\ f &= A_1(p) \otimes p \xrightarrow{x} ([B_1(p), C_1] \otimes (A_1 \otimes p)) \otimes D \rightarrow \\ &\xrightarrow{(1 \otimes (h_1 \otimes 1)) \otimes 1} ([B_1(p), C_1] \otimes (B_1(I) \otimes p)) \otimes D \xrightarrow{(1 \otimes K_{B_1}) \otimes 1} \\ &\rightarrow ([B_1(p), C_1] \otimes B_1(p)) \otimes D \xrightarrow{e \otimes 1} C_1 \otimes D \xrightarrow{g} C. \end{aligned}$$

По определению K $e(1 \otimes K_{B_1})y = \pi^{-1}(K_{[B_1(p), C_1]})$, $y: ([B_1(p), C_1] \otimes p) \otimes B_1(I) \rightarrow ([B_1(p), C_1] \otimes ([B_1(I) \otimes p]))$. Таким образом:

$$\begin{aligned} f &= g(e \otimes 1)((1 \otimes K_{B_1}) \otimes 1)((1 \otimes (h_1 \otimes 1_p)) \otimes 1)x = \\ &= g(((e(1 \otimes K_{B_1})y(y^{-1}(1 \otimes (h_1 \otimes 1_p)))) \otimes 1_D)x = \\ &= g(\pi^{-1}(K_{[B_1(p), C_1]})(y^{-1}(1 \otimes (h_1 \otimes 1_p)))) \otimes 1_D)x = \\ &= g(e(K_{[B_1(p), C_1]} \otimes 1_{B_1(I)})(y^{-1}(1 \otimes (h_1 \otimes 1_p)))) \otimes 1_{D_1})x = \\ &= g(e(K_{[B_1(p), C_1] \otimes B_1(I)})(a(1 \otimes (h_1 \otimes 1_p)))) \otimes 1_D)x = \\ &= g(e(1 \otimes h)((K_{[B_1(p), C_1] \otimes A_1})a^{-1}) \otimes 1_D)x = \\ &= g(e(1 \otimes h))K_A. \end{aligned}$$

Можно положить $f_0 = g(e(1 \otimes h))$.

III.2. $f = B \otimes p \xrightarrow{x \otimes 1_p} ([B_1, C_1] \otimes B_2) \otimes D \otimes p \xrightarrow{(h) \otimes 1} ((C_1 \otimes D) \otimes p) \xrightarrow{g} A(p)$. Применяя предположение индукции к g ,

получаем $g = K_{A(p)}(g_1 \otimes 1)$. Следовательно, $f = K_{A(p)}((g_1 \langle h \rangle x) \otimes \otimes 1_p)$. Можно взять $f_0 = g_1 \langle h \rangle x$. $\square$

10. Л е м м а 21. Пусть $f_1, f_2 : A(p) \rightarrow p$ — некоторые канонические морфизмы, $f_1 \sim f_2$. Тогда имеются канонические морфизмы $g_1, g_2 : A(I) \rightarrow I$, такие, что $g_1 \sim g_2$ (в доказательстве этой леммы используется условие б) теоремы).

Д о к а з а т е л ь с т в о. Положим $h_i = \pi^{-1}(f_i([p, I]))$, $i = 1, 2$. По условию б) и поскольку π^{-1} — изоморфизм, $f_1 \sim f_2 \Rightarrow h_1 \sim h_2$, $h_1, h_2 : A([p, I]) \otimes p \rightarrow I$. Применяя лемму 20, имеем: $h_i = g_i^* K_{A([p, I])}$, $g_i^* : A([I, I]) \rightarrow I$, $h_1 \sim h_2 \Rightarrow g_1^* \sim g_2^*$. В качестве g_i можно взять композицию $g_i^* x$, где x — подходящее расширение изоморфизма $\pi(b_i) : I \rightarrow [I, I]$, $x : A(I) \rightarrow A([I, I])$. $\square$

Л е м м а 22. Если пара $(f_1, f_2 : S \rightarrow T)$ является $\sim$ -минимальной, то $T = I$.

Д о к а з а т е л ь с т в о. Если $T \neq I$, то T есть переменная, и $S \rightarrow T$ в действительности имеет вид $S(p) \rightarrow p$. По лемме 21, $f_1 \sim f_2 \Rightarrow g_1 \sim g_2$ для некоторых $g_1, g_2 : S(I) \rightarrow I$. При этом $S(I) \rightarrow I$ есть 2-тип, если $S(p) \rightarrow p$ — 2-тип. Очевидно, ранг $r(S(I) \rightarrow I)$ меньше, чем $r(S(p) \rightarrow p)$. $\square$

11. Если $(f_1, f_2 : S \rightarrow I)$ является $\sim$ -минимальной парой, то она принадлежит $\mathcal{W}_0 \cap \mathcal{B}$ (лемма 15), и, следовательно, f_1, f_2 имеют следующий вид:

$$\left. \begin{aligned} f_1 &= S \xrightarrow{x} ([B, C] \otimes A) \otimes D \xrightarrow{\langle h \rangle \otimes 1} C \otimes D \xrightarrow{g} I, \\ f_2 &= S \xrightarrow{x'} ([B', C'] \otimes A') \otimes D' \xrightarrow{\langle h' \rangle \otimes 1} C' \otimes D' \xrightarrow{g'} I. \end{aligned} \right\} \quad (\alpha)$$

Здесь $S \rightarrow I$ это чистый 2-тип, $[B, C]$, $[B', C']$ являются его простыми тензорными сомножителями и, следовательно (отметим, что, согласно определению $\mathcal{W}_0$, формы B и B' не являются постоянными), B и B' могут иметь один из видов $p, q \otimes p, [p, a]$, а C, C' — один из видов $d, [d, b]$ или $d \otimes b$. Здесь p, q — переменные, а b, a, d — переменные или I .

Как показывает следующая лемма, лишь один из этих случаеввозможен.

Л е м м а 23. Если $f : S \rightarrow T$ — канонический морфизм, T имеет вид a или $a \otimes b$ (a, b — переменные или I), а один из простых тензорных сомножителей S имеет вид $[C, D]$, где C — не постоянная форма, то f имеет тип « $\langle \rangle$ ».

Д о к а з а т е л ь с т в о. Очевидно, f не может быть центральным изоморфизмом, f также не может быть типа « π », так как в этом случае справа от стрелки будет стоять $[E, F]$. Следовательно, f может быть лишь типа « $\otimes$ » или « $\langle \rangle$ ». Теперь используем индукцию по числу простых сомножителей S , которые не являются постоянными.

База: если в S только один сомножитель, а именно $[C, D]$, то f нельзя представить в виде « $\otimes$ ».

Индукционный переход: предположим, что

$$f = S \xrightarrow{x} E \otimes F \xrightarrow{f_1 \otimes g_1} E' \otimes F' \xrightarrow{y} T.$$

Поскольку y — центральный морфизм, а T есть a или $a \otimes b$, E' и F' центрально изоморфны переменным или I . Не теряя общности, можно предположить, что они — переменные или I . Сомножитель $[B, C]$ есть простой сомножитель E или F . Следовательно, предположение индукции применимо к f_1 или g_1 . Рассмотрим, например, первый случай, когда f_1 есть композиция:

$$f_1 = E \xrightarrow{z} ([E_1, E_2] \otimes E_3) \otimes E_4 \xrightarrow{\langle f'_1 \rangle \otimes 1} E_2 \otimes E_4 \xrightarrow{f'_1} E'.$$

Но отсюда следует, что и f имеет представление в виде « $\langle \rangle$ »:

$$\begin{aligned} f &= S \xrightarrow{x'} ([E_1, E_2] \otimes E_3) \otimes (E_4 \otimes F) \xrightarrow{\langle f'_1 \rangle \otimes 1} E_2 \otimes (E_4 \otimes F) \rightarrow \\ &\xrightarrow{a} (E_2 \otimes E_4) \otimes F \xrightarrow{f'_1 \otimes g_1} E' \otimes F' \xrightarrow{y} T. \quad \square \end{aligned}$$

Л е м м а 24. Если $(f_1, f_2 : S \rightarrow I) \in \mathcal{W}_0$. (тем более, если это $\sim$ -минимальная пара), то $[B, C]$ и $[B', C']$ в (α) имеют вид $[[p, b], c]$ и $[[p', b'], c']$ соответственно, где p, p' — переменные, а b, c, b', c' — переменные или I .

Д о к а з а т е л ь с т в о. Согласно определению $\mathcal{W}_0$, h и h' в (α) не имеют вида « $\langle \rangle$ ». Следовательно, по лемме 23, B и B' не могут быть вида a или $a \otimes a'$, где a, a' — переменные или I . Это влечет за собой (отметим, что $S \rightarrow I$ есть 2-тип), что B и B' имеют вид $[a, b]$, где a, b — переменные или I . Но a не может быть константой, поскольку имелся бы изоморфизм $\pi(b) : I \rightarrow [a, b]$, поэтому, используя композицию f_1, f_2 с результатом домножения этого изоморфизма на подходящие единицы, можно было бы получить пару (f'_1, f'_2) меньше ранга, такую, что $f'_1 \approx f'_2$. Теперь, поскольку $S \rightarrow I$ есть 2-тип, формы C и C' автоматически суть переменные или I . $\square$

12. Рассмотрим граф $\xi : S_1 \rightarrow S_2$, где $S_1 \rightarrow S_2$ — некоторый тип. Все переменные, входящие в $S_1 \rightarrow S_2$, рассматриваются как различные в соответствии с порядком их вхождений. Пусть $T_1 \rightarrow T_2$ — другой тип, построенный из некоторых переменных, входящих в $S_1 \rightarrow S_2$. Будем называть его совместимым с ξ , если имеется подграф ξ' графа ξ , $\xi' : T_1 \rightarrow T_2$. Это условие логически эквивалентно условию, что если переменная v входит в $T_1 \rightarrow T_2$, то переменная v' , сопряженная с v относительно ξ , также входит в $T_1 \rightarrow T_2$ и v, v' имеют соответствующие вариантности в $T_1 \rightarrow T_2$.

З а м е ч а н и е 4. Если дан тип $T_1 \rightarrow T_2$ и существует граф ξ' , то он однозначно определяется по ξ . Очевидно, что отношение совместимости типа с графом транзитивно в том смысле, что если тип $T_1 \rightarrow T_2$ совместим с ξ и $\xi' : T_1 \rightarrow T_2$ — соответствующий подграф ξ , то всякий тип, совместимый с ξ' , совместим с ξ .

Вернемся к рассмотрению $\sim$ -минимальной пары (f_1, f_2) (см. (α)).

Пусть S_1 — тензорное произведение всех простых тензорных сомножителей S , за исключением $[B, C]$ и $[B', C']$, т. е. $[[p, b], c]$ и $[[p', b'], c']$. Порядок сомножителей несуществен. Как и раньше, все переменные рассматриваются как различные.

Пусть A_0 — тензорное произведение всех общих простых тензорных сомножителей A и A' ; D_0 — тензорное произведение всех общих простых сомножителей D и D' ; E_1 — тензорное произведение всех общих простых сомножителей D и A' ; E_2 — тензорное произведение всех общих простых сомножителей A и D' .

Легко видеть, что A_0, D_0, E_1, E_2 не имеют общих простых сомножителей, и формы A, A', D, D', S_1 соответственно центрально изоморфны $(A_0 \otimes E_2) \otimes [[p', b'], c']$, $(A_0 \otimes E_1) \otimes [[p, b], c]$, $E_1 \otimes D_0, E_2 \otimes D_0$; $((A_0 \otimes E_1) \otimes E_2) \otimes D_0$.

Не теряя общности, можно считать (если необходимо, применяя композицию некоторых морфизмов с центральными изоморфизмами), что

$$\left. \begin{aligned} f_1 &= (S_1 \otimes [[p, b], c]) \otimes [[p', b'], c'] \xrightarrow{x} ([p, b], c] \otimes ((A_0 \otimes E_2) \otimes \\ &\quad \otimes [[p', b'], c']) \otimes E_1 \otimes D_0 \xrightarrow{\langle h \rangle \otimes 1} (c \otimes E_1) \otimes D_0 \xrightarrow{g} I, \\ f_2 &= (S_1 \otimes [[p, b], c]) \otimes [[p', b'], c'] \xrightarrow{x'} ([p', b'], c'] \otimes ((A_0 \otimes E_1) \otimes \\ &\quad \otimes [[p, b], c]) \otimes E_2 \otimes D_0 \xrightarrow{\langle h' \rangle \otimes 1} (c' \otimes E_2) \otimes D_0 \xrightarrow{g'} I. \end{aligned} \right\} \quad (\beta)$$

Здесь $h: (A_0 \otimes E_2) \otimes [[p', b'], c'] \rightarrow [p, b]$,

$h': (A_0 \otimes E_1) \otimes [[p, b], c] \rightarrow [p', b']$.

Л е м м а 25. Пусть ξ — граф f_1, f_2 .

Рассмотрим следующие типы морфизмов:

1) $A_0 \otimes [[p', b'], I] \rightarrow [p, b]$, 2) $A_0 \otimes [[p, b], I] \rightarrow [p', b']$,

3) $c \otimes E_1 \rightarrow I$, 4) $c' \otimes E_2 \rightarrow I$, 5) $D_0 \rightarrow I$,

6) $E_1 \otimes [[p, b], c] \rightarrow [[p, b], I]$, 7) $E_2 \otimes [[p', b'], c'] \rightarrow [[p', b'], I]$.

Эти типы совместимы с ξ .

Д о к а з а т е л ь с т в о может быть получено из рассмотренных графов h, h', g, g' . Например, если конец ребра графа лежит в A_0 , то другой конец — это p, b, p', b' или лежит в A_0 (рассматриваем графы h_1, h_2 , принимая во внимание, что E_1 и E_2 не имеют общих переменных, даже если их рассматривать с точностью до сопряженности).

Граф ξ определяет графы:

$\xi_1: A_0 \otimes [[p', b'], I] \rightarrow [p, b]$,

$\dots$

$\xi_7: E_2 \otimes [[p', b'], c'] \rightarrow [[p', b'], I]$.

Л е м м а 26. Пусть h_1, h_2 — канонические морфизмы с одним и тем же графом одного из типов:

$$\begin{aligned}(A_0 \otimes E_2) \otimes [[p', b'], c'] &\rightarrow [p, b], \\ (A_0 \otimes E_1) \otimes [[p, b], c] &\rightarrow [p', b'], \quad c \otimes (E_1 \otimes D_0) \rightarrow I, \\ c' \otimes (E_2 \otimes D_0) &\rightarrow I.\end{aligned}$$

Тогда $h_1 \sim h_2$.

Д о к а з а т е л ь с т в о. Ранг $r(h_1) = r(h_2) < r(S \rightarrow T)$.

Кроме того, (f_1, f_2) является $\sim$ -минимальной парой, следовательно, $h_1 \sim h_2$.

Л е м м а 27. Пусть существует канонический морфизм $f: S_1 \otimes S_2 \rightarrow T$. Пусть типы $S_1 \rightarrow I$ и $S_2 \rightarrow T$ совместимы с графом Γf . Тогда существуют канонические морфизмы $h_1: S_1 \rightarrow I$ и $h_2: S_2 \rightarrow T$, графы которых определяются Γf .

Д о к а з а т е л ь с т в о. Индукцией по рангу $S_1 \otimes S_2 \rightarrow T$.

База: если $r(S_1 \otimes S_2 \rightarrow T) = 0$, то лемма тривиальна.

Индукционный переход: если $r(S_1 \otimes S_2 \rightarrow T) > 0$, то можно использовать устранимость сечения.

Если f — центральный изоморфизм, то S_1 — постоянная форма. (Каждая переменная в S_1 связана ребром в графе с некоторой переменной этой же формы в силу условий леммы, но каждая переменная в $S_1 \otimes S_2$ связана также с переменной в T ввиду центральности f . Следовательно, в S_1 вообще нет переменных). Легко видеть, что тогда имеются два центральных изоморфизма $h_1: S_1 \rightarrow I$ и $h_2: S_2 \rightarrow T$.

Пусть f имеет вид:

$$S_1 \otimes S_2 \xrightarrow{\pi(g)} [T_1, T_2] \xrightarrow{y} T.$$

Предположение индукции применимо к $(S_1 \otimes S_2) \otimes T_1 \rightarrow T_2$ ($S_1 \rightarrow I$ и $S_2 \otimes T_1 \rightarrow T_2$ удовлетворяют условиям леммы). Если $h'_1: S_1 \rightarrow I$ и $h'_2: S_2 \otimes T_1 \rightarrow T_2$ получены, то можно положить $h_1 = h'_1$, $h_2 = y\pi(h'_2)$.

Пусть f имеет вид:

$$S_1 \otimes S_2 \xrightarrow{x} \bar{S}_1 \otimes \bar{S}_2 \xrightarrow{g_1 \otimes g_2} T_1 \otimes T_2 \xrightarrow{y} T$$

(x, y — центральные изоморфизмы). Пусть S_{11} — тензорное произведение общих простых тензорных сомножителей S_1 и $\bar{S}_1$, S_{12} — такое произведение для S_1 и S_2 ; аналогично определяем S_{22} и $\bar{S}_{21}$. Легко проверить, что типы $\bar{S}_1 \rightarrow T_1$, $S_{11} \rightarrow I$, $\bar{S}_{21} \rightarrow T_1$ и $S_2 \rightarrow T_2$, $S_{12} \rightarrow I$, $S_{22} \rightarrow T_2$ соответственно удовлетворяют условиям леммы (рассматриваем графы $\Gamma g_1: \bar{S}_1 \rightarrow T_1$, $\Gamma g_2: \bar{S}_2 \rightarrow T_2$), и можно применить индукционное предположение (заметим, что g_1, g_2 нетривиальны). Если стрелки $h_{11}: S_{11} \rightarrow I$, $h_{22}: S_{22} \rightarrow T_2$, $h_{21}: S_{21} \rightarrow T_1$, $h_{12}: S_{12} \rightarrow I$ уже получены, можно получить h_1 и h_2 применением $\otimes$ и композицией с центральными изоморфизмами.

Пусть f имеет вид:

$$S_1 \otimes S_2 \xrightarrow{x} ([E, F] \otimes \bar{S}_1) \otimes \bar{S}_2 \xrightarrow{(h_1) \otimes 1} F \otimes \bar{S}_2 \xrightarrow{h_2} T,$$

где $h_1: S_{11} \otimes S_{21} \rightarrow E$, $h_2: F \otimes (S_{12} \otimes S_{22}) \rightarrow T$ и S_{11} , S_{12} , S_{21} , S_{22} определены так же, как выше.

Если $[E, F]$ — простой тензорный сомножитель S_1 , то $S_{11} \rightarrow E$, $S_{21} \rightarrow I$, $F \otimes S_{12} \rightarrow I$, $S_{22} \rightarrow T$ совместимы с графом Γf : $S_1 \otimes S_2 \rightarrow T$. Если $[E, F]$ — простой тензорный сомножитель S_2 , то $S_{21} \rightarrow E$, $S_{11} \rightarrow I$, $F \otimes S_{22} \rightarrow T$, $S_{12} \rightarrow I$ совместимы с Γf . (Это следует из рассмотрения возможного расположения сопряженных переменных с учетом совместимости типов $S_1 \rightarrow I$ и $S_2 \rightarrow T$ с Γf).

Предположение индукции обеспечивает существование канонических морфизмов соответствующих типов и с соответствующими графами. Морфизмы типов $S_1 \rightarrow I$ и $S_2 \rightarrow T$ можно построить из них, применяя $\otimes$, $\langle \rangle$ и композицию. $\square$

Л е м м а 28. Существуют канонические морфизмы типов 3)—7) с графами ξ_3 — ξ_7 .

Д о к а з а т е л ь с т в о. Применив леммы 26 и лемму 24 к g и g' в (β) , получим морфизмы $l_3: c \otimes E_1 \rightarrow I$, $l_4: c' \otimes E_2 \rightarrow I$, $l_5: D_0 \rightarrow I$, т. е. морфизмы типов 3) и 5). Морфизмы типов 6), 7) можно получить из l_3 — l_5 применением $\langle \rangle$, π и композиции с центральными изоморфизмами:

$$l_6 = \pi(l_6^-), \text{ где } l_6^- = (E_1 \otimes [[p, b], c]) \otimes [p, b] \xrightarrow{ca} ([p, b], c] \otimes [p, b]) \otimes E_1 \xrightarrow{e \otimes 1} c \otimes E_1 \xrightarrow{l_3} I,$$

$$l_7 = \pi(l_7^-), \text{ где } l_7^- = (E_2 \otimes [[p', b'], c']) \otimes [p', b'] \xrightarrow{ca} ([p', b'], c'] \otimes [p', b']) \otimes E_2 \xrightarrow{e \otimes 1} c' \otimes E_2 \xrightarrow{l_4} I. \quad \square$$

Л е м м а 29. Существуют канонические морфизмы

$$l_1: A_0 \otimes [[p', b'], I] \rightarrow [p, b],$$

$$\text{и } l_2: A_0 \otimes [[p, b], I] \rightarrow [p', b'].$$

Д о к а з а т е л ь с т в о. Рассмотрим $h: (A_0 \otimes E_2) \otimes [[p', b'], c'] \rightarrow [p, b]$. Так как тип $c' \otimes E_2 \rightarrow I$ совместим с Γf (и, следовательно, с Γh), c' связана ребром графа с переменной в E_2 (если c' — переменная). Если c' — переменная, можно применить лемму 27 к $h_c \{I\}: (A_0 \otimes (E_2)_c \{I\}) \otimes [[p', b'], I] \rightarrow [p, b]$ и типам $A_0 \otimes [[p', b'], I] \rightarrow [p, b]$ и $(E_2)_c \{I\} \rightarrow I$. Получим, в частности, $l_1: A_0 \otimes [[p', b'], I] \rightarrow [p, b]$ (если $c' = I$, то можно применить лемму 27 без подстановки), $l_2: A_0 \otimes [[p, b], I] \rightarrow [p', b']$ получается из $h: (A_0 \otimes E_1) \otimes [[p, b], c] \rightarrow [p', b']$ аналогично. $\square$

Графы l_1 и l_2 в предыдущей лемме определяются однозначно графами Γh , $\Gamma h'$ и, следовательно, графом $\Gamma f = \Gamma f'$.

13. Теперь можно завершить доказательство теоремы. Напомним, что

$$l_1: A_0 \otimes [[p', b'], I] \rightarrow [p, b], l_2: A_0 \otimes [[p, b], I] \rightarrow [p', b'],$$

$$l_3: c \otimes E_1 \rightarrow I, l_4: c' \otimes E_2 \rightarrow I, l_5: D_0 \rightarrow I,$$

$$l_6: E_1 \otimes [[p, b], c] \rightarrow [[p, b], I], l_7: E_2 \otimes [[p', b'], c'] \rightarrow [[p', b'], I].$$

Рассмотрим h, h', g, g' в (β) . По лемме 26, имеем:

$$h \sim (l_1 (1_{A_0} \otimes l_7)) a, h' \sim (l_2 (1_{A_0} \otimes l_6)) a,$$

$$g \sim b (l_3 \otimes l_5), g' \sim b (l_4 \otimes l_5),$$

$$\text{и } f_1 \otimes b (l_3 \otimes l_1) ((l_1 (1_{A_0} \otimes l_7) a) \otimes 1) x,$$

$$f_2 \sim b (l_4 \otimes l_5) ((l_2 (1_{A_0} \otimes l_6) a) \otimes 1) x'$$

(x, x' — центральные изоморфизмы из (β)).

Можно получить канонический морфизм типа $(S_1 \otimes [[p, b], c]) \otimes [[p', b'], c'] \rightarrow I$ (и тем же графом, что и $\Gamma f_1 = \Gamma f_2$) из l_1 и l_2 соответственно.

Положим:

$$f_i = e (1 \otimes l_i) y_i: (A_0 \otimes [[p, b], I]) \otimes [[p', b'], I] \rightarrow I \quad (i = 1, 2),$$

где y_1 и y_2 — центральные изоморфизмы,

$$y_1: (A_0 \otimes [[p, b], I]) \otimes [[p', b'], I] \rightarrow$$

$$\rightarrow [[p, b], I] \otimes (A_0 \otimes [[p', b'], I]),$$

$$y_2: (A_0 \otimes [[p, b], I]) \otimes [[p', b'], I] \rightarrow [[p', b'], I] \otimes (A_0 \otimes [[p, b], I]).$$

Из f_0 легко получить канонический морфизм типа $(S_1 \otimes [[p, b], c]) \otimes [[p', b'], c'] \rightarrow I$ (и с тем же графом, что и f_1, f_2). Можно положить:

$$\bar{f}_i = (((e (1 \otimes l_i) y_i) ((1 \otimes l_6) \otimes l_7)) \otimes l_5) z,$$

где

$$z: (S_1 \otimes [[p, b], c]) \otimes [[p', b'], c'] \rightarrow$$

$$\rightarrow ((A_0 \otimes (E_1 \otimes [[p, b], c])) \otimes (E_2 \otimes [[p', b'], c'])) \otimes D_0$$

есть центральный изоморфизм.

Л е м м а 30. $b (l_3 \otimes l_5) ((l_1 (1_{A_0} \otimes l_7) a) \otimes 1) x = ((e (1 \otimes l_1) y_1) b (((1 \otimes l_6) \otimes l_7) \otimes l_5)) z,$

$$b (l_4 \otimes l_5) ((l_2 (1_{A_0} \otimes l_6) a) \otimes 1) x' =$$

$$= ((e (1 \otimes l_2) y_2) b (((1 \otimes l_6) \otimes l_7) \otimes l_5)) z.$$

Д о к а з а т е л ь с т в о. Используя естественность рассматриваемых морфизмов и определения l_1 — l_7 , имеем (следует учесть, что $y_1 = a (c \otimes 1)$):

$$((e (1 \otimes l_1) y_1) b (((1 \otimes l_6) \otimes l_7) \otimes l_5)) z =$$

$$= ((e (1 \otimes l_1) a (c \otimes 1) b (((1 \otimes l_6) \otimes l_7) \otimes l_5)) z =$$

$$= b ((e (1 \otimes l_1) a (c \otimes 1) ((1 \otimes l_6) \otimes l_7)) \otimes l_5) z =$$

$$= b ((e (1 \otimes l_1) (l_6 \otimes (1 \otimes l_7)) a (c \otimes 1)) \otimes l_5) z =$$

$$= b ((e (l_6 \otimes 1) (1 \otimes l_1 (1 \otimes l_7)) a (c \otimes 1)) \otimes l_5) z =$$

(см. определения

$$= b((\pi^{-1}(\pi(l_6^-))(1 \otimes l_1(1 \otimes l_7))a(c \otimes 1)) \otimes l_5)z = \\ = b(l_6^-(1 \otimes l_1(1 \otimes l_7))a(c \otimes 1)) \otimes l_5)z =$$

(см. определение l_6^-)

$$= b(l_3(e \otimes 1)ca(1_{E_1} \otimes [[p, b], c] \otimes l_1(1 \otimes l_7))a(c \otimes 1))l_5)z =$$

$$= b(l_3 \otimes l_5)((e(1_{[[p, b], c]} \otimes l_1(1 \otimes l_7))) \otimes 1_{E_1})caa(c \otimes 1)z =$$

$$b(l_3 \otimes l_5)((e(1 \otimes l_1(1 \otimes l_7)a)) \otimes 1_{E_1}((1 \otimes a^{-1}) \otimes 1))caa(c \otimes 1)z.$$

Ввиду когерентности центральных изоморфизмов $((1 \otimes a^{-1}) \otimes 1)caa(c \otimes 1)z = x$. По определению операции $\langle \rangle$, $e(1 \otimes l_1(1 \otimes l_7)a) = \langle l_1(1 \otimes l_7)a \rangle$.

Таким образом, имеем:

$$((e(1 \otimes l_1) \psi) b(((1 \otimes l_6) \otimes l_7 \otimes l_5))z = b(l_3 \otimes l_5)(\langle l_1(1 \otimes l_7)a \rangle \otimes 1)x.$$

Второй случай рассматривается аналогично. $\square$

Таким образом, $f_i \sim f_i^0(((1 \otimes l_6) \otimes l_7) \otimes l_5)z$ ($i = 1, 2$) и ясно, что если $f_1 \sim f_2$, то и $f_1^0 \sim f_2^0$. Так как (f_1, f_2) — $\sim$ -минимальная пара, f_1^0, f_2^0 имеют тип $(A_0 \otimes [[p, b], I]) \otimes [[p', b'], I] \rightarrow I$, то сомножители E_1, E_2 и D_0 в действительности отсутствуют, c, c' суть I и (f_1^0, f_2^0) также $\sim$ -минимальная пара.

Рассмотрим сомножитель $[[p', b'], I]$. Если b' — константа I , т. е. сомножитель имеет вид $[[p, I], I]$, то можно применить π и перейти к композиции результата этого применения с $k^{-1} = \pi(\langle \pi(ec) \rangle) : [[[p, I], I], I] \rightarrow [p, I]$, являющимся изоморфизмом в V . В результате получаем пару $(k^{-1}\pi(f_1^0), k^{-1}\pi(f_2^0)) : (A_0 \otimes [[p, b], I] \rightarrow [p', I])$ меньшего ранга, чем (f_1^0, f_2^0) , и такую, что $k^{-1}\pi(f_1^0) \sim k^{-1}\pi(f_2^0)$. Это противоречит минимальности (f_1^0, f_2^0) .

Если b' — переменная, то ее можно заменить (вместе с сопряженной) на $[b', I]$. Тогда $(f_i^0)_{b'} : \{[b', I]\} : (A_0 \otimes [[p, b], I]) \otimes [[p', [b', I]], I] \rightarrow I$ ($i = 1, 2$) не являются $\sim$ -эквивалентными по условию б) теоремы.

Форма $[[p', [b', I]], I]$ изоморфна $[[p' \otimes b', I], I]$. Применив соответствующий изоморфизм, затем π и взяв композицию результата с k^{-1} , получим:

$$(k^{-1}f_1^0(1 \otimes \tau), k^{-1}f_2^0(1 \otimes \tau)) : ((A_0)_{b'} \{[b', I]\} \otimes [[p, b], I]) \rightarrow [p' \otimes b', I].$$

Здесь $\tau : [[p' \otimes b', I], I] \rightarrow [[p', [b', I]], I]$. Видно, что $k^{-1}f_1^0(1 \otimes \tau) \sim k^{-1}f_2^0(1 \otimes \tau)$, но тип этих морфизмов еще не есть 2-тип. Применив π^{-1} , получили два неэквивалентных морфизма:

$$\pi^{-1}(k^{-1}f_1^0(1 \otimes \tau)), \pi^{-1}(k^{-1}f_2^0(1 \otimes \tau)) : ((A_0)_{b'} \{[b', I]\} \otimes$$

$$\otimes [[p, b]] \otimes (p \otimes b')) \rightarrow I.$$

Воспользовавшись леммой 20, чтобы исключить переменную b' , можно получить два неэквивалентных морфизма:

$$f_1^*, f_2^* : ((A_0)_{b'} \{[I, I]\} \otimes [[p, b], I] \otimes p' \rightarrow I.$$

Заменяя $[I, I]$ на I (эти формы изоморфны), получим неэквивалентные морфизмы:

$$f_1^{**}, f_2^{**} : ((A_0)_{b'}, \{I\} \otimes [[p, b], I] \otimes p' \rightarrow I.$$

Их тип есть 2-тип; они имеют меньший ранг, чем f_1^0, f_2^0 . Противоречие. $\square$

Литература

1. Kelly G. M., Mac Lane S. Coherence in closed categories//J. Pure Appl. Alg. 1971. Vol. 1. P. 97—140.
2. Voreadou R. Coherence and non-commutative diagrams in closed categories//Mem. Amer. Math. Soc. 1977. Vol. 182. P. 1—93.
3. Бабаев А. А., Соловьев С. В. Теорема когерентности для канонических морфизмов в декартово-замкнутых категориях//Зап. науч. семин. ЛОМИ. 1979. Т. 88. С. 3—29.
4. Soloviev S. V. On decreasing the formula's depth in proof theory and category theory//8-th International Congr. of Log., Methodol. and Phil. Sci. Vol. 5, Pt. 1. Moscow, 1987, p. 70—74.
5. Eilenberg S., Kelly G. M. A generalisation of the functorial calculus//J. Alg. 1966. Vol. 3. P. 366—374.

ТЕОРЕМА ДВОЙСТВЕННОСТИ ДЛЯ ЧАСТИЧНО УПОРЯДОЧЕННЫХ МНОЖЕСТВ: АЛГОРИТМЫ

В работе описываются эффективные алгоритмы решения задачи о покрытии данным количеством цепей (антицепей) максимально возможного числа элементов конечного частично упорядоченного множества.

1. Основные результаты

Пусть Y — конечное частично упорядоченное множество (КЧУМ). Обозначим через R_k (соответственно Q_k) наибольшее количество элементов в его подмножестве, являющемся объединением k цепей (соответственно антицепей), где $k = 0, 1, 2, 3, \dots$. Положим $x_k = R_k - R_{k-1}$, $y_k = Q_k - Q_{k-1}$.

Т е о р е м а 1 [1—3] (теорема двойственности).

1) $x_1 \geq x_2 \geq x_3 \geq \dots$, $y_1 \geq y_2 \geq y_3 \geq \dots$;

2) диаграмма Юнга $\lambda(Y)$ с длинами строк $x_1, x_2, \dots$ совпадает с диаграммой Юнга с длинами столбцов $y_1, y_2, \dots$.

С теоремой двойственности связаны следующие вычислительные задачи.

З а д а ч а YOUNGDIAGRAM (Y). По данному КЧУМ из n элементов построить диаграмму Юнга $\lambda(Y)$.

З а д а ч а CHAINSYSTEM (Y, k). Найти максимальную (относительно общего числа элементов) систему из k цепей в Y .

В настоящей работе получены следующие результаты.

Т е о р е м а 2. Задачи CHAINSYSTEM (Y, k) (для всех k — от 1 до n) и YOUNGDIAGRAM (Y) можно решить за время $O(n^4)$.

Разумеется, вторая часть этого утверждения следует из первой. Соответствующий алгоритм изложен в п. 2. Он последовательно решает задачи CHAINSYSTEM (Y, k) для $k = 1, 2, \dots$.

Задача YOUNGDIAGRAM (Y) может быть, кроме того, решена с помощью следующего рекурсивного алгоритма.

Теорема 3. Пусть $\{M_1, \dots, M_k\}$ — множество всех максимальных элементов КЧУМ Y . Тогда:
если среди диаграмм $\lambda(Y \setminus \{M_i\})$ есть хотя бы две различные, то $\lambda(Y)$ есть их объединение;
иначе $\lambda(Y)$ получается из диаграммы $\lambda(Y \setminus \{M_i\})$ добавлением клетки в k -ю строку.
 (Утверждается, в частности, что указанные операции автоматически приводят к построению множества клеток, являющегося диаграммой Юнга).

Хотя описанная рекурсивная процедура дает в наихудшем случае экспоненциальную временную сложность (при неограниченной памяти), она представляет интерес в силу своей простоты. Кроме того, эта процедура может трактоваться и как независимое определение функционала $Y \mapsto \lambda(Y)$.

Чтобы не дублировать вычисления величин, многократно возникающих на различных разветвлениях рекурсии, можно рассмотреть дистрибутивную решетку 2^Y порядковых идеалов КЧУМ Y и индуктивно, руководствуясь теоремой 3, построить отображение (по терминологии [4] — рост) $I \mapsto \lambda(I)$ решетки 2^Y в множество диаграмм Юнга (граф Юнга). Таким образом, за $N = \text{card}(2^Y)$ шагов, на каждом из которых производится простейшая процедура из теоремы 3, можно вычислить значения отображения λ на всех N идеалах КЧУМ Y .

Задача построения системы из данного числа цепей, покрывающей наибольшее количество элементов, во многом аналогична задаче о максимальном потоке, хотя и не сводится к ней непосредственно. Неудивительно поэтому, что, как и в теории потоков в сетях, ключевую роль играет здесь идея «увеличивающего пути», сходная с форд-фалкерсоновской. Конкретизируем.

Каждую систему цепей (дизъюнктных, что далее каждый раз специально не оговаривается) ω можно рассматривать как набор ребер графа отношения порядка. Пусть $\mathfrak{M}$ — некоторый (быть может, замкнутый) путь в этом графе, такой, что его направление согласуется с ориентацией ребер, не входящих в ω , и не согласуется (противоположно) с ориентацией входящих в ω ребер. Образует множество ребер $\omega \Delta \mathfrak{M}$ («симметрическую разность»), включив в него ребра, покрываемые либо системой ω , либо путем $\mathfrak{M}$. Построенное множество может (хотя и необязательно) также представлять собой набор цепей. Описанная схема является основной для алгоритмов из теоремы 2.

Введем обозначение: $H_s(\omega) = N - ks$, где N — общее количество элементов, покрываемых системой ω ; k — количество цепей в этой системе; $s = 0, 1, 2, \dots$.

Теорема 4 (в [4] без доказательства). Если $H_s(\omega) < \max H_s$, то существует такой путь $\mathfrak{M}$, что $\omega' = \omega \Delta \mathfrak{M}$ — система цепей, для которой $H_s(\omega) < H_s(\omega')$.

Теорема 5. Путь $\mathfrak{M}$ (см. теорему 4) может быть построен за время $O(n^3)$.

В изложении теоремы двойственности и смежных результатов в работе [3] опущено техническое доказательство леммы 7 (об увеличивающем пути). Этот пробел будет ликвидирован в ходе доказательства теоремы 4.

2. Доказательство теоремы 4 и леммы 7 [3]

Следуя [3], введем вспомогательную сеть NW_s . Ее вершинами являются всевозможные пары вида (A, i) , где $A \in Y$, $i = 0, 1, \dots, s$, а также две выделенные вершины — источник N_α и сток N_ω . Ребра (дуги) сети NW_s имеют вид $((A, i), (B, i+1))$, где $A < B$, либо вид $(N_\alpha, (A, 0))$ или $((A, s), N_\omega)$. В каждой вершине сети имеется ограничение ≤ 1 на величину (целочисленного) потока (пропускная способность). С произвольной системой цепей $\omega = \{\omega_1, \dots, \omega_k\}$ можно связать поток $\Pi_s(\omega)$ в описанной сети. Этот поток насыщает все дуги вида $((P_{i-1}, j-1), (P_i, j))$, где P_{i-1} и P_i — две последовательные вершины некоторой цепи $P_0 P_1 \dots P_l$, входящей в систему ω ; при этом должны быть выполнены условия $1 \leq j \leq i \leq j+l-s$. Кроме указанных дуг, поток $\Pi_s(\omega)$ насыщает дуги вида $(N_\alpha, (P_i, 0))$, $0 \leq i \leq l-s$ и $((P_i, s), N_\omega)$, $s \leq i \leq l$. Нетрудно вычислить величину потока $\Pi_s(\omega)$, которая равна как раз $H_s(\omega)$. Из условия теоремы 4 и даже из более слабого условия леммы 7 [3] следует, что в сети NW_s существует увеличивающий (по отношению к потоку $\Pi_s(\omega)$, в смысле Форда—Фалкерсона) путь $\mathfrak{N}$. На основе этого пути и будет строиться искомый (см. теорему 4) путь $\mathfrak{M}$.

(Можно с самого начала считать, что система ω не содержит цепей из менее чем s элементов; иначе подобную цепь можно было бы удалить из ω , и значение функционала H_s увеличилось бы).

Пусть $\mathfrak{M} = M_1 M_2 \dots M_D$ — некоторый путь в Y , т. е. элементы M_i и M_{i+1} сравнимы и не совпадают для $i = 1, \dots, D-1$. Через $\Psi_{\mathfrak{M}}(i)$ будем обозначать «направление» ребра $M_i M_{i+1}$, т. е. $+1$, если $M_i < M_{i+1}$, и -1 , если $M_i > M_{i+1}$. Если путь $\mathfrak{M}$ замкнут, то считаем, что $M_{D+1} = M_1$, и соответственно определяем $\Psi_{\mathfrak{M}}(D)$. Если $\mathfrak{N}$ — путь в графе NW_s , то положим $\Psi_{\mathfrak{N}} = \Psi_{\mathfrak{M}}$, где $\mathfrak{N}$ — проекция $\mathfrak{M}$ на Y .

Вернемся к основной линии доказательства. Увеличивающий путь $\mathfrak{N} = N_\alpha N_1 N_2 \dots N_D N_\omega$ по определению обладает следующими свойствами.

1°. Если $\Psi_{\mathfrak{N}}(i) = 1$, то дуга $N_i N_{i+1}$ ненасыщенная, т. е. по ней поток $\Pi_s(\omega)$ не проходит. Если $\Psi_{\mathfrak{N}}(i) = -1$, то дуга $N_{i+1} N_i$ насыщенная.

2°. Если $\Psi_{\mathfrak{N}}(i) = \Psi_{\mathfrak{N}}(i+1) = 1$, то вершина N_{i+1} ненасыщенная.

Пусть W — множество вершин, покрываемых системой ω , $M_i = \text{pr}_Y N_i$, $\mathfrak{M} = \text{pr}_Y \mathfrak{N} = M_1 \dots M_D$, $\Psi = \Psi_{\mathfrak{M}} = \Psi_{\mathfrak{N}}$, $\alpha = 1/2 (\Psi(1) + \Psi(D-1))$. Начнем модифицировать путь $\mathfrak{N}$ (авто-

матически меняя по ходу дела $\mathfrak{M}$, Ψ и т. д.) согласно следующему алгоритму.

L1. Положить $i_0 = 0$, $i^0 = D + 1$.

L2. Если нет такого i , для которого $i_0 < i < i^0$, вершина N_i ненасыщенна и $M_i \in \mathcal{W}$, то перейти к L4A.

L3. Пусть такое i есть; $M_i \in \omega_j \in \omega$, $N_i = (M_i, J)$. Поток $\Pi_s(\omega)$ проходит через вершины вида (M_i, J') , где индекс J' пробегает некоторый интервал Δ в натуральном ряду; в этот интервал число J не входит. Если J лежит правее Δ , перейти к L3A; если левее — к L3B.

L3A. Пусть $\omega_j = P_0 P_1 \dots P_t$, $M_i \approx P_t$. Видоизменим путь $\mathfrak{N}$, переопределив $N_{i+1} = (P_{t+1}, J + 1)$, $N_{i+2} = (P_{t+2}, J + 2)$, ..., $N_{i+s-J} = (P_{t+s-J}, s)$, $D = i + s - J$. Новый путь не длиннее имевшегося и удовлетворяет условиям $1^\circ - 2^\circ$. Положить $i^0 = i$, $j^0 = j$. Перейти к L2.

L3B. Аналогично L3A модифицировать $\mathfrak{N}$. Положить $i_0 = i$, $j_0 = j$. Перейти к L2.

L4A. Если $i^0 \neq D + 1$, то, игнорируя равенство $\mathfrak{M} = \text{rg} \mathfrak{N}$, заменить конечный отрезок пути $\mathfrak{M}$ (см. L3A) $M_{i^0} M_{i^0+1} \dots M_D$ (или, что то же, $P_t \dots P_{t+s-J}$) на $P_t \dots P_1 P_0$.

L4B. Если $i_0 \neq 0$, то аналогично L4A модифицировать начало $\mathfrak{M}$.

L5. Конец. Алгоритм конечен, так как после каждого прохождения цикла разность $i^0 - i_0$ уменьшается и не может стать отрицательной.

Теперь для модифицированного пути $\mathfrak{M}$ имеет место лемма. Лемма 1.

1.1. $\sum_{i=1}^{D-1} \Psi(i) \geq 1 + \alpha(s - 1)$;

1.2. $\Psi(i) = -1 \Rightarrow \exists j: (M_i \text{ и } M_{i+1} \text{ — соседние вершины цепи } \omega_j)$;

1.3. $\Psi(1) = -1 \Rightarrow M_1 \text{ — минимальный элемент некоторой цепи } \omega_{j_0}$;

1.4. $\Psi(D - 1) = -1 \Rightarrow M_D \text{ — максимальный элемент некоторой цепи } \omega_{j_0}$;

1.5. $\Psi(i - 1) = \Psi(i) = 1 \Rightarrow M_i \notin \mathcal{W}$.

Доказательство. Утверждение 1.2 следует из 1° , 1.3 и 1.4 — из характера модификаций на шагах L4A и L4B, 1.5 — из 1° , 2° и того, что в алгоритме реализовался переход $L2 \rightarrow L4A$. Докажем 1.1. Для исходного пути $\mathfrak{M}$ справедливо равенство $\sum \Psi(i) = s = 1 + \alpha(s - 1)$, которое сохраняется вплоть до L4A. В случае модификации пути на шаге L4A число $\Psi(D - 1)$ становится равным -1 , а α — равным 0. Сумма из 1.1 уменьшается на $s - J + t$ (см. L3A, L4A). Чтобы теперь гарантировать 1.1, нужно проверить, что $s - J + t \leq s - 1$, т. е. $J \geq t + 1$. Последнее неравенство в точности соответствует условию, при котором происходит переход $L3 \rightarrow L3A$. Итак,

1.1 справедливо и после L4A. Аналогично доказывается, что 1.1 выполняется и после L4Б. $\square$

К условиям 1.1—1.5 можно добавить еще два:

$$1.6. M_{i_1} = M_{i_2} = M \Rightarrow M \in W,$$

$$1.7. M_{i_1} = M_{i_2} \Rightarrow M_{i_1+1} \neq M_{i_2+1}.$$

Иначе говоря, путь $\mathfrak{M}$ можно видоизменить так, чтобы он не содержал реберных самопересечений (1.7), а также вершинных самопересечений вне множества W (1.6). Правда, теперь возможен случай замкнутого пути $\mathfrak{M}$. При этом будем считать, что $\alpha = 0$, а условия 1.3 и 1.4 — игнорировать. Возможность включения в список условий 1.6, 1.7 обусловлена тем, что при наличии самопересечения одного из указанных типов путь $\mathfrak{M}$ распадается на два пути (один из них — замкнутый), причем оба эти пути удовлетворяют условиям 1.2—1.5, и хотя бы один из них (по принципу Дирихле) — неравенству 1.1. Повторяя в случае надобности эту процедуру, придем к пути, удовлетворяющему 1.1—1.7; сохраним для него обозначение $\mathfrak{M}$.

Л е м м а 2. Пусть система цепей w и путь $\mathfrak{M}$ (замкнутый или незамкнутый) таковы, что выполняются условия 1.1—1.7. Тогда симметрическая разность $w' = w \Delta \mathfrak{M}$ является системой цепей, причем $H_s(w') > H_s(w)$.

Поскольку выше было показано, что в условиях теоремы 4 (или леммы 7 [3]) такой путь $\mathfrak{M}$ всегда существует, то утверждение этой теоремы (леммы) вытекает из леммы 2.

Д о к а з а т е л ь с т в о. То, что $w' = w \Delta \mathfrak{M}$ является системой дизъюнктных цепей, обеспечивается условиями 1.2—1.7; соответствующую рутинную проверку опускаем. Количество цепей в w' равно $k + \alpha$. Чтобы получить из 1.1 оценку $H_s(w') > H_s(w)$, заметим, что $H_s(w') - H_s(w) = \sum \Psi(i) - \alpha s + \alpha$. Действительно (см. определение $H_s(w)$), как раз те ребра, для которых $\Psi(i) = 1$, добавляются к системе w , а те, для которых $\Psi(i) = -1$, исключаются из нее; поскольку нас в действительности интересуют не ребра, а вершины, появляется довесок $+\alpha$; слагаемое $-\alpha s$ возникает из-за изменения на α числа цепей в системе. $\square$

3. Доказательство теоремы 5

Полиномиальный алгоритм для решения задачи построения увеличивающего пути можно было бы построить непосредственно на основе доказательства теоремы 4. Такой алгоритм был бы, однако, заведомо неоптимален по порядку и, кроме того, весьма расточителен относительно памяти. Рассмотрим другой подход, прямо основанный на лемме 2. Задача построения пути $\mathfrak{M}$, удовлетворяющего 1.1—1.7, сводится, как будет показано ниже, к задаче поиска положительного цикла в некоторой вспомогательной сети $IG(w)$, отличной от NW_s и зависящей от w , которая играет роль, аналогичную «инкрементальной графу» из потоковых алгоритмов [5].

Тип ребра	Стоимость
OM , где $M \in Y$, $M \notin W$	$-\frac{1}{2}(s-1)$
MO , где $M \in Y$, $M \notin W$	$-\frac{1}{2}(s-1)$
$O(M, +)$, где M — максимальный элемент одной из цепей системы w	$+\frac{1}{2}(s-1)$
$(M, -)O$, где M — минимальный элемент одной из цепей системы w	$+\frac{1}{2}(s-1)$
$(M_2, \beta)(M_1, -)$, где $M_1 < M_2$ — два последовательных элемента одной из цепей w , $\beta \in \{+, -\}$	-1
M_1M_2 , где $M_1 < M_2$; $M_1, M_2 \in W$	$+1$
$M_1(M_2, +)$, где $M_1 \notin W$, $M_2 \in W$, $M_1 < M_2$	$+1$
$(M_1, -)M_2$, где $M_1 \in W$, $M_2 \notin W$, $M_1 < M_2$	$+1$
$(M_1, -)(M_2, +)$, где $M_1, M_2 \in W$, $M_1 < M_2$	$+1$

Множество вершин графа (сети) $IG(w)$ состоит из выделенной вершины O , всех элементов КЧУМ Y , не покрываемых системой w , а также всевозможных пар вида (M, β) , где $M \in W$, $\beta \in \{+, -\}$; в дальнейшем будет видно, что некоторые из этих вершин без ущерба для конструкции можно удалить из $IG(w)$.

Теперь опишем множество ребер ориентированного графа $IG(w)$, сопровождая его указаниями на значения стоимости (цены), сопоставляемой каждому ребру.

Стоимостью простого (ориентированного) пути в графе $IG(w)$ называется сумма стоимостей входящих в него ребер. Каждый такой путь может быть спроектирован на Y (отбрасываются компоненты β и вершина O). Непосредственной проверкой можно убедиться в справедливости следующего результата, в расчете на который, собственно, и конструировался граф $IG(w)$.

Л е м м а 3. Проекция простого замкнутого ориентированного пути в $IG(w)$, стоимость которого положительна, удовлетворяет условиям 1.1—1.7. Всякий путь в Y , удовлетворяющий 1.1—1.7, может быть получен подобным проектированием. $\square$

Завершим доказательство теоремы 5. Если $\text{card } Y = n$, то в графе $IG(w)$ не более $2n$ вершин. Поиск положительного цикла в этом графе может быть осуществлен с помощью алгоритма Флойда (см., например, [5]) за время $O((2n)^3)$. Проектирование этого цикла на Y и модификация системы цепей (см. лемму 2) требуют меньшего по порядку времени.

З а м е ч а н и е. Если в графе $IG(w)$ нет положительного цикла, то этот факт будет установлен в процессе работы алгоритма Флойда. В этом случае можно будет сделать вывод: значение $H_s(w)$ максимально среди всех систем из k , $k-1$ и $k+1$ цепей, а значит (см. теорему 4), и вообще среди всех систем цепей.

Иными словами, за время $O(n^3)$ можно увеличить значение функционала H_s либо установить, что такое увеличение невозможно.

4. Доказательство теоремы 2

Найти системы из $k = 1, 2, 3, \dots$ цепей в Y , покрывающие максимальное, т. е. равное R_k , количество элементов (такие системы будем называть k -максимальными), можно с помощью следующего алгоритма:

$s := n; \quad k := 0; \quad w := \emptyset;$

repeat

if применить алгоритм из теоремы 5 (см. также замечание в п. 3);

if увеличивающий путь существует

then begin модифицировать w и соответственно k ;

 запомнить w как k -максимальную систему

end

else $s := s - 1$

until w покрывает Y .

Для доказательства этого покажем, что после каждого прохождения цикла справедливы следующие утверждения:

а) система w является k -максимальной;

б) $x_{k+1} - 1 \leq s \leq x_k$ (условимся, что $x_0 = +\infty$).

В начальный момент это очевидно. Пусть а) и б) справедливы после очередного шага. Возможны два случая. Если $x_{k+1} \leq s \leq x_k$, то $R_{k-1} - (k-1)s = R_k - x_k - ks + s \leq R_k - ks = H_s(w)$ и $R_{k+1} - (k+1)s = R_k + x_{k+1} - ks - s \leq R_k - ks = H_s(w)$, т. е. увеличить H_s переходом даже к $(k \pm 1)$ -максимальным системам нельзя. Значит, в соответствии с алгоритмом параметр s уменьшается на 1. После этого по-прежнему выполняются условия (А) (система w не изменилась) и б) (так как по предположению $x_{k+1} \leq s$). Второй случай: $x_{k+1} - 1 = s$. Как и раньше, $R_{k-1} - (k-1)s \leq H_s(w)$, но зато теперь $R_{k+1} - (k+1)s = H_s(w) + 1$. Это означает, что увеличивающий путь есть, причем модифицированная система будет обязательно $(k+1)$ -максимальной. Утверждение (А), тем самым, справедливо, так же как и б): $x_{k+2} - 1 \leq x_{k+1} - 1 = s \leq x_{k+1}$. Итак, доказано (см. а)), что все системы цепей w , получаемые в ходе работы алгоритма, будут максимальными.

При каждом прохождении цикла целочисленная величина $H_s(w)$, равная в начальный момент нулю, увеличивается (либо за счет модификации w , либо за счет изменения s) и не может превзойти n . Отсюда и из теоремы 5 следует, что время работы приведенного алгоритма оценивается величиной порядка $O(n^4)$. $\square$

5. Доказательство теоремы 3

Как показано в [3], удаление экстремального элемента из КЧУМ Y приводит к удалению одной клетки из диаграммы Юнга $\lambda(Y)$ (доказательство основано на теореме 4 настоящей работы).

Отсюда вытекает первое утверждение теоремы 3 (разветвление «то»). Предположим теперь, что $\lambda(Y \setminus \{M_1\}) = \dots = \lambda(Y \setminus \{M_k\}) = \lambda$, $\lambda(Y) = \lambda \cup \{A\}$. Необходимо таким образом, показать, что клетка A расположена в k -й строке.

Пусть ω — система из $k - 1$ дизъюнктивных цепей в КЧУМ Y , покрывающая максимальное количество элементов. Хотя бы один из элементов $M_1, \dots, M_k$ не принадлежит ни одной цепи системы ω . Следовательно, удаление этого элемента не изменит значение функционала R_{k-1} . Отсюда заключаем, что клетка A не может располагаться в первых $k - 1$ строках.

Остается доказать, что A не может быть расположена ниже k -й строки. Предположим противное. Это означает, что удаление любого из элементов M_i не меняет функционала R_k . Иначе говоря, для произвольного $i \in \{1, \dots, k\}$ существует система $\omega^{(i)}$ из k цепей в Y , покрывающая R_k элементов и не содержащая M_i . Как показано в [3] (теорема 2), $\exists l: R_k + Q_l = n + kl$, т. е. максимальная система из l антицепей пересекается с любой максимальной системой из k цепей по kl элементам (и эти две системы покрывают все множество Y). Обозначим описанную систему антицепей через $v = \{v_1, v_2, \dots, v_l\}$. Как отмечено в [1, 4], систему v можно считать упорядоченной в следующем смысле:

$$(p \in v_i \ \& \ q \in v_j \ \& \ p < q) \Rightarrow i < j,$$

т. е. антицепи «располагаются друг под другом». Ясно, что при этом те из элементов M_i , которые покрываются системой v , можно считать принадлежащими антицепи v_i (иначе можно просто переместить такой элемент в эту антицепь).

Возьмем теперь произвольный максимальный элемент M_i . Так как M_i не покрывается системой $\omega^{(i)}$, но $\omega^{(i)}$ и v вместе покрывают Y , то M_i покрывается системой v и, значит, $M_i \in v_l$. Таким образом, антицепь v_l содержит все элементы M_i и, следовательно, только их (напомним: $\{M_1, \dots, M_k\}$ — множество всех максимальных элементов КЧУМ Y). Как уже отмечалось, системы v и $\omega^{(i)}$ пересекаются по kl элементам, т. е. каждая антицепь, входящая в систему v (и, в частности, антицепь v_l), пересекается со всеми цепями, входящими в $\omega^{(i)}$. Отсюда следует, что v_l покрывается системой $\omega^{(i)}$; но $M_i \in v_l$, в то время как $M_i \notin \omega_j^{(i)}$. Полученное противоречие завершает доказательство теоремы 3. $\square$

6. Связь с классическими задачами комбинаторной оптимизации

Цепь (антицепь) частично упорядоченного множества можно определять как клику (независимое множество) в графе отношения сравнимости. Такой подход позволяет рассматривать сформулированные в п. 1 задачи как конкретизации (для графов сравнимости) традиционных задач о покрытиях и раскрасках. Ниже основные результаты настоящей работы будут прокомментированы с этих позиций, что потребует небольшого изменения стиля и смещения некоторых акцентов.

Пусть Y — граф с n вершинами. Положим:

$R_k = \max \{\text{card } A : A \subset Y, A \text{ покрывается } k \text{ кликами}\},$

$Q_l = \max \{\text{card } B : B \subset Y, B \text{ покрывается } l \text{ независимыми подмножествами}\}, k = 0, 1, 2, \dots, l = 0, 1, 2, \dots$. В терминах величин R_k и Q_l могут быть выражены такие классические характеристики графа, как хроматическое число $\chi(Y) = \min \{l : Q_l = n\}$, кликовое число R_1 , число независимости Q_1 . Задача о наименьшем покрытии (кликами) связана с вычислением характеристики $\delta(Y) = \min \{k : R_k = n\}$.

Почти очевидно неравенство $R_k + Q_l \leq n + kl$ (клика и «антиклика» — независимое множество — не могут иметь более одного общего элемента). Отсюда

$$R_k \leq \min_l (n + kl - Q_l), \quad Q_l \leq \min_k (n + kl - R_k). \quad (1)$$

В частности, при $k = 1$ получаем:

$$R_1 \leq \min_l (n + l - Q_l) = \min \{l : Q_l = n\} = \chi(Y)$$

и аналогично $Q_1 \leq \delta(Y)$. Разумеется, оба эти неравенства хорошо известны (и тривиальны); хотелось лишь подчеркнуть, что они являются следствиями более общих неравенств (1).

Основной результат работ [1—3] может быть интерпретирован как теорема о превращении оценок (1) в равенства в том случае, когда Y является графом сравнимости; ранее было известно, что для таких графов $R_1 = \chi(Y)$ (тривиально) и $Q_1 = \delta(Y)$ (теорема Дилуорса). Теперь воспользуемся следующим элементарным фактом.

Л е м м а 4. Пусть натуральные числа $R_1, R_2, R_3, \dots$ и $Q_1, Q_2, Q_3, \dots$ таковы, что

$$R_k = \min_l (n + kl - Q_l), \quad Q_l = \min_k (n + kl - R_k). \quad (2)$$

Тогда существует такая диаграмма Юнга, что числа $R_1, R_2 - R_1, R_3 - R_2, \dots$ — длины ее строк, а числа $Q_1, Q_2 - Q_1, Q_3 - Q_2, \dots$ — длины ее столбцов.

(Верно и обратное утверждение: если R_k и Q_l определять с помощью некоторой диаграммы Юнга, то выполняется (2)).

Сначала доказывается монотонность последовательностей $\{R_k\}$, $\{Q_l\}$, $\{R_{k+1} - R_k\}$, $\{Q_{l+1} - Q_l\}$, а затем и основное утверждение леммы. $\square$

Лемма 4 показывает, что обращение неравенств (1) в равенства (для графов сравнимости) — это утверждение, эквивалентное теореме 1. Остается открытой следующая проблема: охарактеризовать (конструктивно) графы, для которых справедлива теорема двойственности (т. е. по существу (2)). Этот класс графов содержит все графы сравнимости, а также дополнительные к ним «графы несравнимости», но не исчерпывается указанными типами. Пример: граф с множеством вершин $\{1, 2, 3, 4, 5, 6, 7\}$ и множеством ребер $\{12, 23, 34, 45, 56, 67, 17, 14, 26, 36, 47\}$.

Различными авторами интенсивно изучался, в том числе и в алгоритмическом аспекте, близкий по свойствам класс совершенных графов (см., например, [6] и приведенную там библиографию).

В наших терминах совершенным является граф, для которого, как и для всех его подграфов, выполняется равенство $R_1 = \chi(Y)$. Теорема двойственности для совершенных графов, вообще говоря, неверна (и из нее не вытекает «совершенство»). Полиномиальные алгоритмы решения традиционных задач о покрытиях и раскрасках в случае совершенного графа были разработаны Грётшелем, Ловасом и Шрийвером в начале 1980-х годов [6]. Эти алгоритмы можно применить, конечно, и в случае графов сравнимости, хотя хорошо известны и значительно более простые методы. Автору не известны, однако, работы, в которых были бы построены (например, для этого частного случая) эффективные алгоритмы решения наиболее общей задачи — определения максимального числа элементов, покрываемых данным количеством цепей (антицепей, клик, независимых множеств). Этим и мотивована настоящая публикация.

Автор признателен А. М. Вершику, а также Д. Ю. Григорьеву и А. О. Слисенко за внимание, проявленное к этой работе, и поддержку.

Литература

1. *Greene C., Kleitman D.* The structure of Sperner k -families//J. Comb.Theory (A). 1976. Vol. 20. P. 41—68.
2. *Greene C.* Some partitions associated with a partially ordered set//J. Comb. Theory (A). 1976. Vol. 20. P. 69—79.
3. *Фомин С. В.* Конечные частично упорядоченные множества и диаграммы Юнга//ДАН СССР. 1978. Т. 243, № 5. С. 1144—1147.
4. *Фомин С. В.* Обобщенное соответствие Робинсона—Шенстеда—Кнута//Дифференциальная геометрия, группы Ли и механика. VIII//Зап. науч. семин. ЛОМИ. 1986. Т. 155. С. 156—175.
5. *Кристофидес Н.* Теория графов: Алгоритмический подход М., 1978.
6. *Lovasz L.* An algorithmic theory of numbers, graphs, and convexity. Philadelphia, 1986.

ВЫЧИСЛЕНИЕ ГРУППЫ ГАЛУА НАД ФУНКЦИОНАЛЬНЫМ ПОЛЕМ ХАРАКТЕРИСТИКИ НУЛЬ С АЛГЕБРАИЧЕСКИ ЗАМКНУТЫМ ПОЛЕМ КОНСТАНТ ЗА ПОЛИНОМИАЛЬНОЕ ВРЕМЯ

Введение

В настоящей работе описывается алгоритм полиномиальной сложности для построения образующих группы Галуа поля разложения многочлена над полем Ω в предположении, что поле K_1 является конечно-порожденным расширением поля рациональных чисел $\mathbb{Q}$, а поле Ω — конечно-порожденным расширением алгебраического замыкания K_1 поля K_1 .

Задача вычисления группы Галуа является одной из важных задач вычислительной алгебры. Ей всегда уделялось много внимания различными алгебраистами. Первый алгоритм для построения группы Галуа был предложен еще в прошлом веке Кронекером [2]. В последние годы с развитием теории сложности вычислений появилось много других алгоритмов для этой задачи, см., например, [13, 16, 7]. Однако все построенные до настоящего времени алгоритмы в общем случае имели экспоненциальную сложность относительно длины исходных данных. Исключение составляет лишь случай многочленов над конечным полем, когда группа Галуа циклическая. Под сложностью вычисления, как это принято, понимается число необходимых для получения ответа элементарных шагов алгоритма, рассматриваемое как функция от длины записи входа задачи. В качестве понятия алгоритма в данном контексте можно использовать, например, машину Тьюринга, адресную машину и т. п. [1, 5]. Если сложность вычисления оценивается сверху полиномом от длины входа, то задача имеет полиномиальную сложность, или, что то же самое, решается за полиномиальное время. Если же для времени работы алгоритма имеется лишь достижимая оценка сверху экспоненциальной функцией от длины входных данных, то считается, что он имеет экспоненциальную сложность. Алгоритмы, имеющие экспоненциальную сложность, являются неэффективными в худшем слу-

чае. Когда для задачи с ранее известными для ее решения алгоритмами лишь экспоненциальной сложности удастся найти алгоритм, работающий в полиномиальное время, то это можно рассматривать как принципиальный шаг на пути к построению действительно эффективного алгоритма.

Перейдем к более подробной формулировке основного результата. Пусть поле алгебраических чисел $k = \mathbb{Q}[\theta]$, многочлен $h \in \mathbb{Q}[Z]$ (в дальнейшем X, Y, Z обозначают независимые переменные) является минимальным для элемента θ . Поле $K_1 = k(t_1, \dots, t_l, \eta_1)$, где элементы $t_1, \dots, t_l$ (считаем $l \geq 0$) алгебраически независимы над k , а η_1 — алгебраический элемент над $k(t_1, \dots, t_l)$ с минимальным многочленом $\varphi_1 \in k(t_1, \dots, t_l)[Z]$. Далее, пусть $t_{l+1}, \dots, t_{n+1}$ (считаем $n \geq l$) алгебраически независимы над полем K_1 , элемент η_2 алгебраичен над полем $K_1(t_{l+1}, \dots, t_{n+1})$, $\varphi_2 \in K_1(t_{l+1}, \dots, t_{n+1})[Z]$ — минимальный многочлен для η_2 , поле $K = K_1(t_{l+1}, \dots, t_{n+1}, \eta_2)$. Наконец, пусть $f \in K[Y]$ — не обязательно неприводимый многочлен.

Многочлен $f \in K[Y]$ может быть представлен в виде:

$$f = \frac{1}{b} \sum_{0 \leq m \leq \deg_Y f} \sum_{0 \leq r < \deg_h h} \sum_{0 \leq j < \deg_{\varphi_1} \varphi_1} \sum_{0 \leq i < \deg_{\varphi_2} \varphi_2} b_{ijrm} \eta_1^i \eta_2^j \theta^r Y^m,$$

где $b, b_{ijrm} \in \mathbb{Z}[t_1, \dots, t_{n+1}]$ для всех i, j, r, m , причем степень многочлена b и модули его коэффициентов выбираются минимально возможными. Под длиной записи целого числа понимаем количество разрядов в двоичном представлении этого числа (один разряд отводится для знака). Через $l(b)$ (соответственно $l(b_{ijrm})$) обозначим максимум длин записей коэффициентов многочлена b (соответственно b_{ijrm}) при мономах от $t_1, \dots, t_{n+1}$; положим $l(f) = \max_{i, j, r, m} \{l(b_{ijrm}), l(b)\}$. Длины записей или размеры $L(b), L(b_{ijrm})$ многочленов b, b_{ijrm} определим согласно формулам:

$$L(b) = \left(1 + \max_{1 \leq \alpha \leq n+1} \deg_{t_\alpha}(b)\right)^{n+1} l(b),$$

$$L(b_{ijrm}) = \left(1 + \max_{1 \leq \alpha \leq n+1} \deg_{t_\alpha}(b_{ijrm})\right)^{n+1} l(b_{ijrm}).$$

Степень относительно t_α элемента f определим по формуле

$$\deg_{t_\alpha} f = \max_{i, j, r, m} \{\deg_{t_\alpha}(b_{ijrm}), \deg_{t_\alpha}(b)\}.$$

Наконец, под длиной записи или размером $L(f)$ многочлена f будем понимать величину:

$$(1 + \deg_Y f)^{n+1} \left(1 + \max_{1 \leq i \leq n+1} \deg_{t_i} f\right)^{n+1} (1 + \deg_Z \varphi_1 \deg_Z \varphi_2 \deg_Z h) l(f).$$

Таким образом, $L(b), L(b_{ijrm}), L(f)$ по смыслу есть число двоичных разрядов, достаточных для записи всех целых коэффициентов многочленов b, b_{ijrm}, f соответственно. Аналогичным образом определяются длины записей принадлежащих $\mathbb{Z}$ коэффи-

циентов элементов $\mathbb{Q}[Z]$, $k(t_1, \dots, t_l)[Z]$, $K_1(t_{l+1}, \dots, t_{n+1})[Z]$, а также степени относительно t_i элементов из $k(t_1, \dots, t_l)[Z]$, $K_1(t_{l+1}, \dots, t_{n+1})[Z]$; например, определены $l(h)$, $l(\varphi_1)$, $l(\varphi_2)$, $\deg_{t_i} \varphi_1$, $1 \leq i \leq l$, $\deg_{t_i} \varphi_2$, $1 \leq i \leq n+1$. Положим

$$L(h) = (1 + \deg_z h) l(h),$$

$$L(\varphi_1) = (1 + \deg_z \varphi_1) \left(1 + \max_{1 \leq i \leq l} \deg_{t_i} \varphi_1\right)^l (1 + \deg_z h) l(\varphi_1),$$

$$L(\varphi_2) = (1 + \deg_z \varphi_2) \left(1 + \max_{1 \leq i \leq n+1} \deg_{t_i} \varphi_2\right)^{n+1} \times \\ \times (1 + \deg_z h \deg_z \varphi_1) l(\varphi_2).$$

В дальнейшем, не умаляя общности, будем считать, что степени рассматриваемых элементов удовлетворяют неравенствам:

$$\deg_{t_i} \varphi_1 < d_1, \quad 1 \leq i \leq l, \quad \deg_{t_i} \varphi_2 < d_1, \quad 1 \leq i \leq n+1, \quad \deg_z \varphi_1 < d_1, \\ \deg_z \varphi_2 < d_1, \quad \deg_{t_i} f < d_2, \quad 1 \leq i \leq n+1, \quad \deg_{\gamma} f < d, \quad \deg_z h < d_3$$

и для длин записей их коэффициентов справедливы неравенства:

$$l(\varphi_1) < M_1, \quad l(\varphi_2) < M_1, \quad l(f) < M_2, \quad l(h) < M_3.$$

Таким образом, $L(h) \leq M_3 d_3$, $L(\varphi_1) \leq d_1^{l+1} d_3 M_1$, $L(\varphi_2) \leq d_1^{n+3} d_3 M_1$, $L(f) \leq (dd_2)^{n+1} d_1^2 d_3 M_2$, причем величины в правых частях этих неравенств меньше некоторого полинома от соответствующих величин, стоящих в левых частях этих неравенств (при подходящем выборе h , φ_1 , φ_2 , f). Это означает, что с точностью до полиномиальной эквивалентности [1] за $L(\varphi_1)$, $L(\varphi_2)$, $L(h)$, $L(f)$ можно взять значения в левых частях приведенных неравенств.

Основная теорема. Группа Галуа G поля разложения многочлена f над полем $\Omega = \bar{K}_1(t_{l+1}, \dots, t_{n+1}, \eta_2)$ реализуется как подгруппа симметрической группы степени $\deg_{\gamma} f$. Систему образующих группы G , состоящую не более чем из $(\deg_{\gamma} f)^2$ подстановок, можно построить за полиномиальное от $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(f)$ время.

Простейший случай этой теоремы получается, когда поле $\Omega = \bar{\mathbb{Q}}(t_1)$ — здесь и в дальнейшем черта над полем обозначает его алгебраическое замыкание. Уже в этом случае в качестве G может получиться произвольная конечная группа.

Как следствие отметим, что основная теорема позволяет вычислить за полиномиальное время группу Галуа композита полей разложения многочленов f_1 , f_2 над полем Ω . Действительно, длина записи произведения $L(f_1 f_2)$ оценивается сверху полиномом от $L(f_1)$, $L(f_2)$, $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$.

Метод доказательства теоремы не обобщается на поля ненулевой характеристики или на поля с незамкнутыми полями кон-

стант, поскольку он существенно использует аппарат теории аналитических функций, например теорему Римана о монодромии.

З а м е ч а н и е 1. Неприводимость многочленов h , φ_1 , φ_2 из условия теоремы может быть проверена с помощью алгоритма из [7, гл. 1] за полиномиальное время. Многочлен f может быть разложен на неприводимые над K множители также за полиномиальное от $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(f)$ время согласно [7, гл. 1]. При этом существенно, что в определении $L(f)$ взят множитель $(1 + \deg_Y f)^{n+1}$, а не $1 + \deg_Y f$. Последнее поясняется еще и тем, что если рассматриваются многочлены f из $K[Y]$, у которых одновременно степени относительно t_i , где $1 \leq i \leq n+1$, и Y меньше d_0 , то естественно считать длиной их записи величину порядка $d_0^{n+2} d_1^2 d_3 M_2$, и тогда $L(f)$ оказывается полиномиальным от этой величины.

З а м е ч а н и е 2. Если в формулировке основной теоремы степени d , d_1 , d_2 заменить на величину $\mathcal{P}(dd_1d_2)$, где $\mathcal{P}$ обозначает некоторый полином, степень d_3 — на $\mathcal{P}(dd_1d_2d_3)$, длины записей целых коэффициентов M_1 , M_2 , M_3 — на величину $(M_1 + M_2 + M_3 + n)\mathcal{P}(dd_1d_2d_3)$, то утверждение теоремы не изменится, т. е. время будет полиномиальным от $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(f)$ в старом смысле. Этим замечанием будем пользоваться и в дальнейшем. Положим $M = (M_1 + M_2 + M_3 + n)$ и $d_4 = dd_1d_2d_3$.

Опишем теперь содержание работы по разделам, из которых первый и второй являются подготовительными. В них решается задача построения римановой поверхности $\mathcal{W}$ поля алгебраических функций от одной переменной. Более точно, обозначим через K' поле констант поля алгебраических функций $K'(x, y)$ и $k = K' \cap \mathbb{Q}$, причем минимальный многочлен $\Phi \in K'[X, Y]$, задающий соотношение $\Phi(x, y) = 0$, неприводим над $\bar{K}'$. В разд. 1 формулируется теорема 1.1, согласно которой, если фиксировано вложение $k \subset \mathbb{C}$ и рассматривается его продолжение до вложения $K' \subset \mathbb{C}$, то разветвленное накрытие проективных комплексных кривых $\mathcal{W} \rightarrow \mathbb{P}^1(\mathbb{C})$, соответствующее вложению полей $\mathbb{C}(x) \subset \mathbb{C}(x, y)$, топологически не зависит от продолжения вложения $K' \subset \mathbb{C}$.

Эта теорема показывает, что приводимая в разд. 1, 2 конструкция топологически инвариантна; в дальнейшем теорема нигде не используется, поэтому ее доказательство опускается. Далее в разд. 1 строится вложение полей $K' \subset \mathbb{C}$ некоторым специальным образом, чтобы точки ветвления из $\mathbb{P}^1(\mathbb{C})$ отображения $\mathcal{W} \rightarrow \mathbb{P}^1(\mathbb{C})$ были достаточно далеки друг от друга.

В разд. 2 строится собственно разветвленное накрытие $\mathcal{W} \rightarrow \mathbb{P}^1(\mathbb{C})$ и согласованные относительно этого накрытия триангуляции комплексных кривых $\mathcal{W}$ и $\mathbb{P}^1(\mathbb{C})$. В качестве непосредственного следствия получаем, что геометрический род поля алгебраических функций от одной переменной может быть вычислен за полиномиальное время. Вычисление рода является

самостоятельной задачей. Оно сводится к нахождению индекса ветвления e в точке ветвления, а эта задача сводится к построению начального отрезка ряда Пюизе алгебраической функции y . Однако ранее эти три задачи не удавалось решить за полиномиальное время [12]. Используя метод из разд. 2, можно доказать нужный для решения этих задач результат: коэффициент при $(x - a)^{N/e}$ в ряде Пюизе вычисляется за время, полиномиальное от длины записи исходных данных и от N^{r+1} , где r — степень трансцендентности поля констант над примитивным подполем.

Следует подчеркнуть, что в случае, если поле $\Omega = \bar{K}_1(t_1)$, следуем идеям классического алгоритма для вычисления группы Галуа над $\mathbb{C}(z)$ как группы монодромии алгебраической функции [6, 9]. Здесь основная трудность — реализовать алгоритм за полиномиальное время (см. разд. 1, 2).

В разд. 3 решается задача построения группы Галуа в случае, если поле K имеет степень трансцендентности 1 над полем констант (алгебраическое замыкание поля констант в этом разделе есть $\bar{k}(t_1, \dots, t_n)$). Результат разд. 2 позволяет здесь непосредственно построить группу Галуа, если поле K чисто трансцендентно над полем констант. Общий случай сводим к чисто трансцендентному при помощи сифт-алгоритма [4, 11] для построения образующих подгрупп симметрической группы. Кроме того, в разд. 3 описывается алгоритм для разложения многочленов над полем Ω , который использует и обобщает метод из [7, гл. 1] на случай полей с алгебраически замкнутым полем констант.

Наконец, в разд. 4 вычисляется группа Галуа в общем случае и завершается доказательство основной теоремы. Здесь описаны два сведения. Сначала общий случай с неприводимым многочленом f сводится к рассмотрению нескольких (точнее полиномиального числа от длины записи исходных данных) случаев, когда поле K имеет степень трансцендентности 1 над полем констант. Затем описывается, как алгоритм для приводимого многочлена f сводится к рассмотренному случаю неприводимого f .

В настоящей работе постоянно используются результаты о том, что значения элементарных функций могут быть вычислены с заданной точностью за полиномиальное время [10], а также, что корни многочлена с комплексными коэффициентами могут быть отделены друг от друга и вычислены с заданной точностью за полиномиальное время [15].

Обозначения типа $a \leq b^{\mathcal{P}}(c)$, $a \leq 2^{b^{\mathcal{P}}(c)}$ эквивалентны тому, что существует полином $\mathcal{P} \in \mathbb{Z}[X]$ с неотрицательными коэффициентами, для которого справедливы написанные неравенства. Если необходимо зафиксировать полином $\mathcal{P}$, то пишем $a \leq bP_i(c)$, $a \leq 2^{bP_i(c)}$, где $\mathcal{P} = P_i$, i — индекс. В дальнейшем будем неоднократно пользоваться такими обозначениями, не оговаривая их специально. Все полиномы $\mathcal{P}$ и P_i , которые встречаются ниже, легко могут быть найдены эффективно.

1. Построение гомоморфизма с предписанными свойствами, задающего расширение поля скаляров

Здесь поле k такое же, что и во введении, а поле $K = k(t_1, \dots, t_n)[\eta](x)$, где $\eta = \eta_1$ — алгебраический элемент над $k(t_1, \dots, t_n)$ с минимальным многочленом $\varphi = \varphi_1$ и $x = t_{n+1}$ в обозначениях из введения. Будем считать, кроме того, без ограничения общности, что многочлены $h \in \mathbb{Z}[Z]$, $\varphi \in \mathbb{Z}[\theta][t_1, \dots, t_n][Z]$ и φ , рассматриваемый как многочлен от $t_1, \dots, t_n, Z$, абсолютно неприводим, т. е. неприводим в кольце $\bar{\mathbb{Q}}[t_1, \dots, t_n, Z]$ (если это не так, то на основании алгоритма из [7, гл. 1, § 3] можно найти абсолютно неприводимый множитель многочлена φ и изменить элемент θ и поле k). Обозначим через K' поле $k(t_1, \dots, t_n)[\eta]$ и рассмотрим поле алгебраических функций $K'(x, y)$, где элемент y удовлетворяет соотношению алгебраической зависимости $\Phi(x, y) = 0$, причем $\Phi \in K'[X, Y]$ — абсолютно неприводимый многочлен, т. е. Φ неприводим в кольце $\bar{K}'[X, Y]$. Многочлен $\Phi(x, Y) = \Phi(t_{n+1}, Y)$ в этом разделе играет ту же роль, что и многочлен f из введения, длина записи $L(\Phi) = L(\Phi(x, Y))$ определяется подобно $L(f)$. Кроме того, будем считать, что $\deg_y \Phi > 1$, исключая тривиальный для нас случай, когда $y \in k'(x)$, и что $\Phi \in \mathbb{Z}[\theta][t_1, \dots, t_n][\eta][X, Y]$. Зафиксируем некоторое вложение поля k в $\mathbb{C}$ и в дальнейшем будем отождествлять k с подполем в $\mathbb{C}$ при помощи этого вложения $k \subset \mathbb{C}$.

Пусть V — определенная над полем K' гладкая проективная кривая, поле рациональных функций над K' на которой совпадает с $K'(x, y)$ (в [8] V является кривой в $\mathbb{P}^r(\bar{K}')$ для некоторого r). Под комплексной римановой поверхностью поля $K'(x, y)$ будем подразумевать всякую комплексную алгебраическую кривую W , которая получается из V расширением поля скаляров до $\mathbb{C}$. Расширение скаляров определяется вложением полей $K' = k(t_1, \dots, t_n)[\eta] \rightarrow \mathbb{C}$, тождественным на k . Разным таким вложениям соответствуют, вообще говоря, неизоморфные алгебраические кривые W , однако топологически все они эквивалентны. Справедлив следующий более сильный результат.

Т е о р е м а 1.1. Пусть вложению полей $K'(x) \subset K'(x, y)$ соответствуют при двух расширениях поля скаляров K' до $\mathbb{C}$ над k морфизмы проективных комплексных алгебраических кривых $p_i: W_i \rightarrow \mathbb{P}^1(\mathbb{C})$, $i = 1, 2$. Тогда существуют гомеоморфизмы $\gamma: \mathbb{P}^1(\mathbb{C}) \rightarrow \mathbb{P}^1(\mathbb{C})$ и $\gamma_1: W_1 \rightarrow W_2$, такие что $\gamma \circ p_1 = p_2 \circ \gamma_1$. (Здесь рассматривается классическая топология).

Т е о р е м а 1.1 показывает, что описываемая ниже конструкция топологически инвариантна. В дальнейшем эта теорема не используется, поэтому ее доказательство опускается.

З а м е ч а н и е. Известное автору доказательство теоремы 1.1 не обобщается на случай, если в условии теоремы рассматриваются расширения скаляров с K' до $\mathbb{C}$ над $\mathbb{Q}$.

Основной целью этого и следующего разделов является описание алгоритма для построения комплексной римановой поверх-

ности поля $K'(x, y)$, работающего в полиномиальное от $L(h)$, $L(\varphi)$, $L(\Phi)$ время. Более точно, алгоритм будет строить некоторое вложение полей $K' \rightarrow \mathbb{C}$, определяющее вложение $\mathbb{C}(x) \rightarrow \mathbb{C} \otimes_{K'} K'(x, y)$ и соответствующее отображение $p: W \rightarrow \mathbb{P}^1(\mathbb{C})$, которое, согласно теореме 1.1, топологически не зависит от расширения поля скаляров. Алгоритм находит точки ветвления отображения p и строит некоторые триангуляции T_1 и T_2 кривых $\mathbb{P}^1(\mathbb{C})$ и W соответственно. При этом для каждого симплекса $s' \subset W$ из триангуляции T_2 образ $p(s')$ является симплексом из триангуляции T_1 , все точки ветвления отображения p из $\mathbb{P}^1(\mathbb{C})$ (соответственно W) являются вершинами триангуляции T_1 (соответственно T_2), и если $s \subset \mathbb{P}^1(\mathbb{C})$ — симплекс из триангуляции T_1 , отличный от точки ветвления, то $p^{-1}(s) = \bigcup_{1 \leq i \leq \deg_Y \Phi} s_i$, где s_i — попарно различные симплексы из триангуляции T_2 и $\dim s_i = \dim s$, $1 \leq i \leq \deg_Y \Phi$.

В настоящей разделе описывается алгоритм для построения вложения $K \subset \mathbb{C}$, такого, что точки ветвления из $\mathbb{P}^1(\mathbb{C})$ отображения $p: W \rightarrow \mathbb{P}^1(\mathbb{C})$ достаточно далеки друг от друга. Прежде всего при помощи замены переменных, задающей автоморфизм кривой $\mathbb{P}^1(\mathbb{C})$, добьемся, чтобы точка $\infty = (0:1)$ стала неразветвленной для отображения p . Для построения нужного автоморфизма вычислим дискриминант относительно Y многочлена Φ как определитель матрицы Сильвестра многочленов Φ и $\partial\Phi/\partial Y$ [2]. Здесь и в дальнейшем определители вычисляются в полиномиальное время на основе алгоритма из [14], см. также [7, гл. 1] и лемму 1.1. Тогда этот дискриминант $0 \neq D = D(t_1, \dots, t_n, \eta, X) \in K'[X]$ и $\deg_X D \leq (2 \deg_Y \Phi) - 1 \deg_X \Phi$. Перебирая числа $1, 2, \dots$, найдем целое число $a \leq \deg_X(D) + 1$, такое, что $D(t_1, \dots, t_n, \eta, a) \neq 0$. Точка $(a:1)$ неразветвлена для отображения p [8, гл. 2, § 5]. Искомым автоморфизмом, при котором $\infty \mapsto (a:1)$, будет $X \mapsto aX/(X+1)$. Заменяем $\Phi(X, Y)$ на многочлен $(X+1)^{\deg_X \Phi} \Phi(aX/(X+1), Y)$ (см. замечание 2 из введения).

Без ограничения общности и для удобства будем считать, что старшие коэффициенты $lc_Z(h)$, $lc_Z(\varphi)$ и $lc_Y(\Phi)$ многочленов h , φ при Z и Φ при Y равны 1, иначе, согласно замечанию 2 из введения, можно заменить $\theta \mapsto lc_Z(h) \theta$, $\eta \mapsto lc_Z(\varphi) \eta$, $y \mapsto (lc_Y \Phi(x) y)$. Отметим, что поле $K'(x, y) = K'(x, (lc_Y \Phi(x) y))$, и поэтому отображение p , построенное по новому многочлену Φ , эквивалентно отображению p , построенному по старому многочлену Φ (новое p отличается от старого на изоморфизм новой и старой кривых W). В частности, точка $\infty \in \mathbb{P}^1(\mathbb{C})$ неразветвлена для нового отображения p .

Разложим в полиномиальное время на основании алгоритма из [7, гл. 1] многочлен D на неприводимые $D = \lambda \prod_i D_i^{e_i}$, где $D_i \in \mathbb{Z}[\theta][t_1, \dots, t_n, \eta][X]$ — неприводимые многочлены в $K'[X]$, $1 \leq e_i \in \mathbb{Z}$, $0 \neq \lambda \in K'$. Вычислим произведение

$\Delta = \prod_i D_i$. Отметим, что $\Delta \in \mathbb{Z}[\theta][t_1, \dots, t_n, \eta][X]$ в силу того, что старшие коэффициенты h и φ равны 1. Далее найдем $\Delta_0 = \Delta_0(t_1, \dots, t_n, X) = N_{K'(X)/k(t_1, \dots, t_n)(X)}(\Delta) \in \mathbb{Z}[\theta][t_1, \dots, t_n][X]$ — норму [2] из поля $K'(X)$ в поле $k(t_1, \dots, t_n)(X)$ многочлена Δ (норма вычисляется как определитель матрицы $k(t_1, \dots, t_n)(X)$ -линейного отображения $K'(X) \rightarrow K'(X)$). Вычислим дискриминанты δ_0 многочлена Δ_0 относительно X и δ_1 — многочлена $\varphi = \varphi(t_1, \dots, t_n, Z)$ относительно Z и найдем их произведение $\delta_3 = \delta_0 \delta_1 \in \mathbb{Z}[\theta][t_1, \dots, t_n]$. Выберем последовательно целые числа $b_1, \dots, b_n$, такие, что $1 \leq b_i \leq \deg_{t_i}(\delta_3) + 1$ и $\delta_3(b_1, \dots, b_i, t_{i+1}, \dots, t_n) \neq 0$. Элемент b_i находим перебором, после того как найдены $b_1, \dots, b_{i-1}$. Согласно построению и свойствам дискриминанта, многочлены $\Delta_1(X) = \Delta_0(b_1, \dots, b_n, X) \in \mathbb{Z}[\theta][X]$ и $\varphi(b_1, \dots, b_n, Z) \in \mathbb{Z}[\theta][Z]$ не имеют кратных корней.

Далее необходимы следующие две леммы.

Л е м м а 1.1. Пусть A — квадратная матрица размера $s \times s$ с коэффициентами $a_{\beta\gamma}$ из кольца $\mathbb{Z}[\{X_{ij}\}_{1 \leq i \leq v, 1 \leq j \leq \mu_i}]$, где все элементы X_{ij} алгебраически независимы над $\mathbb{Z}$. Пусть далее степени $\deg_{X_{ij}}(a_{\beta\gamma}) < r_i$ для всех $\beta, \gamma, 1 \leq i \leq v, 1 \leq j \leq \mu_i$ и длины записей $l(a_{\beta\gamma}) < N$ для всех β, γ . Тогда мы имеем неравенства $\deg_{X_{ij}}(\det A) < sr_i$ для всех $1 \leq i \leq v, 1 \leq j \leq \mu_i$ и $l(\det A) < s(\log_2 s + N + \sum_{1 \leq i \leq v} \mu_i \log_2 r_i)$.

Д о к а з а т е л ь с т в о. Неравенства $\deg_{X_{ij}}(\det A) < sr_i$ очевидны. Оценка для $l(\det A)$ вытекает из того факта, что коэффициент при каждом из мономов в $\det A$ есть сумма не более $s!$ $(\prod_{1 \leq i \leq v} r_i^{\mu_i})^s$ коэффициентов подобных членов, получающихся после вычисления $\det A$, и каждый из коэффициентов этих подобных членов по модулю меньше 2^{sN} .

Л е м м а 1.2. Пусть $\Omega = \mathbb{Z}[\{X_{ij}\}_{1 \leq i \leq v, 1 \leq j \leq \mu_i}]$ — кольцо многочленов из леммы 1.1, пусть $H, \Psi \in \Omega[Z]$, причем многочлен Ψ неприводим и старший коэффициент $0 \neq \text{lc}_Z \Psi = \Psi_0 \in \Omega$, далее, пусть имеют место оценки $\deg_{X_{ij}} H < s_i, \deg_{X_{ij}} \Psi < r_i$ для $1 \leq i \leq v, 1 \leq j \leq \mu_i$; $\deg_Z H < s, \deg_Z \Psi < r$; $l(H) < N'', l(\Psi) < N'$. Обозначим через $H_1 \in \Omega[Z]$ остаток от деления многочлена $\Psi_0^{(\deg_Z(H) - \deg_Z(\Psi) + 1)} H$ на Ψ . Тогда справедливы следующие неравенства на степени $\deg_Z H_1 < r, \deg_{X_{ij}} H_1 < sr_i + s_i$ для всех $1 \leq i \leq v, 1 \leq j \leq \mu_i$ и на длину записи $l(H_1) < N'' + \log_2 s + \sum_{1 \leq i \leq v} \mu_i \log_2 s_i + s(1 + N' + \log_2 r + \sum_{1 \leq i \leq v} \mu_i \log_2 r_i)$.

Д о к а з а т е л ь с т в о. Положим $H^{(0)} = H$ и $H^{(i+1)} = \Psi_0 H^{(i)} - (\text{lc}_Z H^{(i)}) \Psi$, если $\deg_Z H^{(i)} \geq \deg_Z \Psi$. Тогда многочлен $H^{(t)}$, являющийся конечным членом последовательности

$H^{(0)}, H^{(1)}, \dots$, совпадает с многочленом H_1 . По индукции получаем, что $\deg_{x_{ij}} H^{(\nu)} < \nu r_i + s_i$ и, следовательно, $\deg_{x_{ij}} H_1 < < sr_i + s_i$. Также по индукции доказывается, что модули коэффициентов из $\mathbb{Z}$ многочлена $H^{(\nu)}$ не превосходят $2^{N''+\nu+\nu N'} sr^\nu \times \times \prod_{1 \leq i \leq \nu} (s_i^{\mu_i} r_i^{\mu_i \nu})$, и, следовательно, $l(H_1)$ удовлетворяет требуемому неравенству.

Будем считать, что $\deg_x \Phi < d_2$, $\deg_{t_i} \Phi < d_2$, $1 \leq i \leq n$, $\deg_y \Phi < d$, $l(\Phi) < M_2$ (многочлен Φ здесь играет роль f , см. введение) и напомним, что $\phi = \phi_2$. Тогда в силу лемм 1.1 и 1.2 имеем (приводим здесь даже более слабые неравенства) $\deg_x D < < 2dd_2$, $\deg_{t_i} D < 2dd_2 d_1$, $1 \leq i \leq n$, и $l(D) < (M_1 + M_2 + M_3 + + (n+1) \log_2 d_2) \mathcal{P}(dd_1 d_3)$, поскольку D получается вычислением определителя матрицы Сильвестра дискриминанта с последующим приведением результата по mod ϕ и mod h . Согласно [7, гл. 1], для многочленов D_i будут справедливы оценки $\deg_x D_i < 2dd_2$, $\deg_{t_j} D_i < d_2 \mathcal{P}(dd_1)$, $1 \leq j \leq n$ и $l(D_i) < (M_1 + + M_2 + M_3 + (n+1) d_2) \mathcal{P}(dd_1 d_3)$. Эти оценки получаются на основании лемм 1.1 и 1.2 и конструкции теоремы 1.1 [7]. Далее, опять по леммам 1.1, 1.2 для многочленов Δ и Δ_0 справедливы те же самые неравенства и для δ_0 выполнено $\deg_{t_i} \delta_0 < d_2^2 \mathcal{P}(dd_1)$, $1 \leq i \leq n$ и $l(\delta_0) < (M_1 + M_2 + M_3 + (n+1) d_2) \mathcal{P}(dd_1 d_3)$. Аналогично доказывается, что $\deg_{t_i} (\delta_1) < 2d_1^2$, $1 \leq i \leq n$ и $l(\delta_1) < (M_1 + M_3 + n) \mathcal{P}(d_1 d_3)$. Следовательно, для многочлена δ справедливы оценки $l(\delta) \leq (M_1 + M_2 + M_3 + (n+1) d_2) \times \times \mathcal{P}(dd_1 d_3)$, $\deg_{t_i} \delta < d_2^2 \mathcal{P}(dd_1)$ для всех $1 \leq i \leq n$.

Обозначим $\delta_2 = \delta_2(t_1, \dots, t_n) = \text{lc}_x \Delta_0 = N_{K'/K}(t_1, \dots, t_n) (\text{lc}_K \Delta)$. При подстановке в матрицу Сильвестра для δ_0 нуля многочлена $\delta_2(t_1, \dots, t_n)$ в ней образуется нулевой столбец. Следовательно, $\delta_2(b_1, \dots, b_n) \neq 0$.

В дальнейшем будем неоднократно пользоваться следующей леммой.

Л е м м а 1.3. Пусть $\psi = \sum_{0 \leq i \leq m} \psi_i Z^i \in \mathbb{C}[Z]$ — многочлен с комплексными коэффициентами $\psi_0, \dots, \psi_m$, причем степень $\deg \psi = m$ и $z_1, \dots, z_m$ — корни многочлена ψ . Тогда справедливы следующие утверждения.

(i) $|z_i| < \max \left\{ \sum_{0 \leq i \leq m-1} |\psi_i|/|\psi_m|, 1 \right\} = C$ для всех $1 \leq i \leq m$.

(ii) Если $\psi_0 \neq 0$, то $|z_i| > |\psi_0|/(C^{m-1} |\psi_m|)$, в частности, если $0 \neq \psi_0 \in \mathbb{Z}$, то $|z_i| > 1/(C^{m-1} |\psi_m|)$, $1 \leq i \leq m$.

(iii) Если $z_i \neq z_j$ — два различных корня многочлена ψ и дискриминант R многочлена ψ отличен от нуля, то $|z_i - z_j|^2 > > |R|/(|\psi_m|^{2m-1} m^m (2C)^m (m-1)^{-2})$. В частности, если $\psi \in \mathbb{Z}[Z]$, то вместо $|R|$ в последнем неравенстве можно взять 1.

(iv) Обозначим $N = N(a_0, \dots, a_{m-1}) = \prod_{1 \leq i \leq m} \left(\sum_{0 \leq j < m} a_j z_i^j \right)$, где

$a_0, \dots, a_{m-1} \in \mathbb{C}$. Тогда $\left| \sum_{0 \leq j < m} a_j z_i^j \right| > |N(a_0, \dots, a_m)| \left(m \max_i |a_i| \times \right. \\ \times C^{m-1} m^{-1}$ для всех $1 \leq i \leq m$. В частности, если $\psi \in \mathbb{Z}[Z]$ неприводим, то в этом неравенстве вместо $|N(a_0, \dots, a_{m-1})|$ можно взять $|\psi_0|^{-m+1}$ при $(a_0, \dots, a_{m-1}) \neq (0, \dots, 0)$.

Доказательство. Неравенства п. (i) и (ii) следуют из формул Виета, а неравенство п. (iii) из свойств дискриминанта. Утверждение п. (iv) вытекает из утверждения п. (i).

На основании леммы 1.3 (iv), полагая $\psi = h$, получаем, что $|\delta_j(b_1, \dots, b_n)| > 2^{-MP_1(d_4)}, j = 0, 1, 2, 3$ (напомним: $M = M_1 + M_2 + M_3 + n, d_4 = dd_1 d_2 d_3$). Заметим, что длины записей коэффициентов $l(\delta_j(b_1 + t_1, \dots, b_n + t_n)) < M\mathcal{P}(d_4)$. Поэтому существует такой полином P_2 , что если $|x_i| < 2^{-MP_2(d_4)}, 1 \leq i \leq n$, то $|\delta_j(b_1 + x_1, \dots, b_n + x_n)| > 2^{-MP_1(d_4)-1}, j = 0, 1, 2, 3$.

Пусть $q_1, \dots, q_n$ — n первых простых чисел. Положим $r = \left[\left(\lfloor \sqrt{q_n} \rfloor + 1 \right) / \log_2 \left(1 + 2^{-MP_1(d_4)} / \max_{1 \leq i \leq n} b_i \right) \right] + 1$, здесь $\lfloor \cdot \rfloor$ обозначает целую часть числа. В силу выбора r существуют такие целые r_i , что $b_i < e^{(r_i/r)} \sqrt[r]{q_i} < b_i + 2^{-MP_1(d_4)}, 1 \leq i \leq n$. Вычислим все r_i . Обозначим $\alpha_i = e^{(r_i/r)} \sqrt[r]{q_i}$. Пусть $x_i, 1 \leq i \leq \deg_X \Delta_0$ — все корни, учитывая кратности, многочлена $\Delta_0(\alpha_1, \dots, \alpha_n, X)$. Модули коэффициентов многочлена $\Delta_0(\alpha_1, \dots, \alpha_n, X)$ оцениваются сверху величиной $2^{M\mathcal{P}(d_4)}$, а $|\text{lc}_X \Delta_0(\alpha_1, \dots, \alpha_n, X)| > 2^{-M\mathcal{P}(d_4)}$ согласно только что изложенному. По лемме 1.3 (i), (iii) имеем $|x_i| < 2^{M\mathcal{P}(d_4)}$ для всех i , и если $x_i \neq x_j$, то $|x_i - x_j| > 2^{-MP_1(d_4)}$. Аналогично доказывается, что для модулей разностей корней многочлена $\varphi(\alpha_1, \dots, \alpha_n, Z)$ справедливы такие же оценки снизу, а для самих корней этого многочлена имеют место оценки сверху такие же, как и для x_i .

Положим α равным некоторому фиксированному корню многочлена $\varphi(\alpha_1, \dots, \alpha_n, Z)$. Корень α задается эффективно своим приближением с точностью $(1/3) 2^{-MP_1(d_4)}$. Определяем вложение $K' \rightarrow \mathbb{C}$ над полем k формулами $t_i \rightarrow \alpha_i, 1 \leq i \leq n, \eta \rightarrow \alpha$. Элементы $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ алгебраически независимы над k согласно теореме Линдемана [3], поэтому действительно получаем вложение полей. Через $\Phi_1(X, Y)$ обозначим многочлен, который получается подстановкой в Φ элементов $\alpha_1, \dots, \alpha_n, \alpha$ вместо $t_1, \dots, t_n, \eta$, и через y' — корень многочлена $\Phi_1(x, Y) \in \mathbb{C}(x)[Y]$. Таким образом, определено поле алгебраических функций $\mathbb{C}(x, y')$ над $\mathbb{C}$ (напомним, что Φ неприводим над $\bar{K}'$ и, следовательно, Φ_1 неприводим над $\mathbb{C}$).

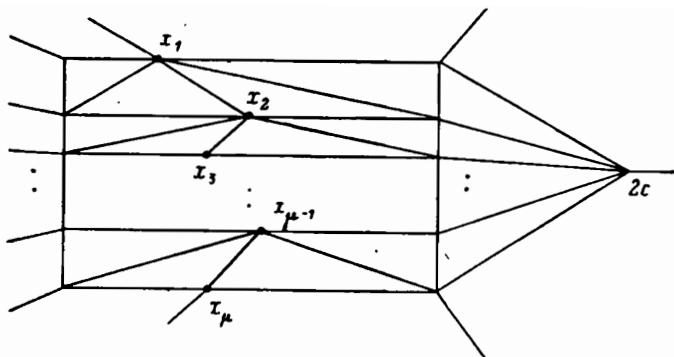
В дальнейшем потребуется еще оценка снизу $|\text{lc}_X \Delta(\alpha_1, \dots, \alpha_n, \alpha)| > 2^{-M\mathcal{P}(d_4)}$. Она получается из леммы 1.3 (iv) при $z_i = \alpha, \psi = \varphi(\alpha_1, \dots, \alpha_n, Z)$ с учетом, что $|N| = |\text{lc}_X \Delta_0| \times |(\alpha_1, \dots, \alpha_n)| > 2^{-M\mathcal{P}(d_4)}$ согласно изложенному выше.

2. Построение римановой поверхности поля алгебраических функций

Перейдем теперь к конструкции триангуляции T_1 комплексной сферы $\mathbb{P}^1(\mathbb{C})$. Положим $v = \deg_X \Delta_0 (\deg_X (\Delta_0) - 1)$. Вычислим значения $\arg(x_i - x_j)$ при $x_i \neq x_j$ с точностью $1/(2v) \leq \leq 1/4$. Обозначим эти приближенные значения в порядке возрастания через $0 \leq \psi_1 \leq \psi_2 \leq \dots \leq \psi_v < 2\pi$, кроме того, для удобства положим $\psi_0 = 0, \psi_{v+1} = 2\pi$. Найдем такое $0 \leq i_0 \leq v$, что $\psi_{i_0+1} - \psi_{i_0} > 5/v$, и вычислим число $a \in \mathbb{C}$, такое, что $|\arg(a) - (\psi_{i_0} + \psi_{i_0+1})/2| < 1/(2v)$, кроме того, $a = a_1 + \sqrt{-1}a_2$, $a_1, a_2 \in \mathbb{Z}$ и $l(a_1), l(a_2) < \mathcal{P}(\log_2 v)$. Сделаем замену переменных $X \rightarrow aX$, т. е. вместо многочлена $\Phi(X, Y)$ будем рассматривать многочлен $\Phi(aX, Y)$. Корни многочлена $\Delta_0(\alpha_1, \dots, \alpha_n, aX)$ суть $a^{-1}x_i$, $1 \leq i \leq \deg_X \Delta_0$, поэтому $|\operatorname{Im}(a^{-1}x_i - a^{-1}x_j)| = |a^{-1}| |x_i - x_j| |\sin(\arg(x_i - x_j) - \arg(a))| > |a^{-1}| |x_i - x_j| \times \times \sin(1/2v) > 2^{-MP_4(d_4)}$. Оставим за многочленом $\Phi(aX, Y)$ прежнее обозначение $\Phi(X, Y)$ и в дальнейшем будем считать без ограничения общности, что $|\operatorname{Im}(x_i - x_j)| > 2^{-MP_4(d_4)}$ для любых двух различных корней x_i и x_j многочлена $\Delta_0(\alpha_1, \dots, \alpha_n, X)$. Для удобства сделаем еще одну замену переменных $X \mapsto \rightarrow X + \sqrt{-1}b$, $b \in \mathbb{Q}$, чтобы вновь полученный многочлен $\Delta(\alpha_1, \dots, \alpha_n, \alpha, X + \sqrt{-1}b)$ имел корни как с положительными, так и с отрицательными мнимыми частями. Такое число b всегда можно найти, в силу того что отображение p имеет по крайней мере две различные точки ветвления в $\mathbb{P}^1(\mathbb{C})$. При этом выберем b так, чтобы $l(b) < M\mathcal{P}(d_4)$. Если необходимо, восстановим $l_{\Sigma}(\Phi) = 1$.

Всякий корень многочлена $\Delta(\alpha_1, \dots, \alpha_n, \alpha, X)$ является корнем многочлена $\Delta_0(\alpha_1, \dots, \alpha_n, X)$. Поэтому можно считать, что x_j , $1 \leq j \leq \deg_X \Delta = \mu$ являются корнями многочлена $\Delta(\alpha_1, \dots, \alpha_n, \alpha, X)$. Найдем приближенные значения всех корней многочлена $\Delta(\alpha_1, \dots, \alpha_n, \alpha, X)$ с точностью до $(1/3) 2^{-MP_4(d_4)}$, а также некоторое целое число c , такое, что $c - 1 > \max_{1 \leq j \leq \mu} |x_j| > > c - 3$. Согласно доказанному, $|c| < 2^{MP(d_4)}$. Через $[a, b]$ будем обозначать замкнутый отрезок с концами a, b , далее $|a, b| = [a, b] \setminus \{a\}$.

В качестве вершин триангуляции $\mathbb{P}^1(\mathbb{C})$ возьмем точку $\infty \in \mathbb{P}^1(\mathbb{C})$, а также следующие точки из $\mathbb{C} \subset \mathbb{P}^1(\mathbb{C})$: $2c$, $c + \sqrt{-1} \operatorname{Im} x_j$, x_j , $-c + \sqrt{-1} \operatorname{Im} x_j$ для всех $1 \leq j \leq \mu$. Будем считать без ограничения общности, что $\operatorname{Im} x_1 > \operatorname{Im} x_2 > \dots > \operatorname{Im} x_\mu$. В качестве ребер (одномерных симплексов) триангуляции возьмем теперь (см. рисунок) отрезки прямых $[2c, c + \sqrt{-1} \operatorname{Im} x_j]$, $[c + \sqrt{-1} \operatorname{Im} x_j, x_j]$, $[x_j, -c + \sqrt{-1} \operatorname{Im} x_j]$ для всех $1 \leq j \leq \mu$, $[x_j, x_{j+1}]$, $[x_j, c + \sqrt{-1} \operatorname{Im} x_{j+1}]$, $[x_j, -c + \sqrt{-1} \operatorname{Im} x_{j+1}]$, $[c + \sqrt{-1} \operatorname{Im} x_j, c + \sqrt{-1} \operatorname{Im} x_{j+1}]$, $[-c + \sqrt{-1} \operatorname{Im} x_j, -c + \sqrt{-1} \operatorname{Im} x_{j+1}]$ для всех $1 \leq j \leq \mu - 1$



и лучи, соединяющие точку ∞ и точки $2c$, $c + \sqrt{-1} \operatorname{Im} x_1$, $c + \sqrt{-1} \operatorname{Im} x_{\mu}$, x_1 , x_{μ} , $-c + \sqrt{-1} \operatorname{Im} x_j$ для всех $1 \leq j \leq \mu$ (луч, соединяющий точку ∞ с точкой $\gamma \in \mathbb{C}$ есть по определению множество $\{t\gamma : t \geq 1, t \in \mathbb{R}\} \cup \{\infty\}$). После определения вершин и ребер, двумерные симплексы триангуляции определяются однозначно (см. рисунок).

Перейдем к построению триангуляции T_2 кривой W . Под разрезом B_j , $1 \leq j \leq \mu$ сферы $\mathbb{P}^1(\mathbb{C})$ будем понимать объединение отрезков $[2c, c + \sqrt{-1} \operatorname{Im} x_j] \cup [c + \sqrt{-1} \operatorname{Im} x_j, x_j]$. После того как сделаны все разрезы B_j , $1 \leq j \leq \mu$, к системе открытых множеств в классической топологии сферы $\mathbb{P}^1(\mathbb{C})$ по определению добавляются множества $\{z: d_1 < \operatorname{Re} z < d_2 \text{ \& } \exists z_1 \in B_j (\operatorname{Im} z_1 \leq \operatorname{Im} z < \operatorname{Im} z_1 + \varepsilon \text{ \& } \operatorname{Re} z = \operatorname{Re} z_1)\}$ для всех $1 \leq j \leq \mu$, $\operatorname{Re} x_j < d_1 < d_2 < 2c$, $\varepsilon > 0$ и множества $\{z: |z - 2c| < \varepsilon \text{ \& } \arg(c + \sqrt{-1} \operatorname{Im} x_{\mu}) < \arg(2c - z) \leq \arg(c - \sqrt{-1} \operatorname{Im} x_1) \text{ или } z = 2c\}$ для всех $0 < \varepsilon < 1$ (функция $\arg$ здесь принимает значения в промежутке $]-\pi, \pi]$). Положим $U = \mathbb{C} \setminus \left(\bigcup_{1 \leq j \leq \mu} B_j \cup \{2c\} \right)$ — это открытое односвязное подмножество в $\mathbb{P}^1(\mathbb{C})$. Тогда прообраз $p^{-1}(U) = \bigcup_{1 \leq i \leq \deg_Y \Phi} W^{(i)}$, где $W^{(i)}$ — открытые

в классической топологии попарно непересекающиеся подмножества W , такие, что ограничение p на $W^{(i)}$ является гомеоморфизмом $p_i: W^{(i)} \rightarrow U$. Отметим, что множество $W^{(i)}$ полностью определяется значением $y'(p_i^{-1}(2c + 1)) = \xi_i$, т. е. корнем многочлена $\Phi_1(2c + 1, Y)$. Алгебраическая риманова поверхность W получается некоторым склеиванием $\deg_Y \Phi$ экземпляров сферы $\mathbb{P}^1(\mathbb{C})$ с разрезами B_j , $1 \leq j \leq \mu$, вдоль разрезов B_j . Уточним теперь способ склейки.

Обозначим через $\tilde{\mathbb{P}}^1(\mathbb{C})$ сферу $\mathbb{P}^1(\mathbb{C})$ с разрезами B_j , $1 \leq j \leq \mu$, а через $\bar{W}^{(i)}$ — i -й экземпляр сферы $\tilde{\mathbb{P}}^1(\mathbb{C})$, $1 \leq i \leq \deg_Y \Phi$. Будем считать, что $W \supset \bar{W}^{(i)} \supset W^{(i)}$. Через $q_i: \tilde{\mathbb{P}}^1(\mathbb{C}) \rightarrow W$ обозначим непрерывную функцию на $\tilde{\mathbb{P}}^1(\mathbb{C})$, которая совпадает с p_i^{-1} на подмножестве U . Такая функция q_i

существует и единственна в силу определения топологии в $\tilde{\mathbb{P}}^1(\mathbb{C})$. Множество $\overline{W}^{(i)} = q_i(\tilde{\mathbb{P}}^1(\mathbb{C}))$. При аналитическом продолжении функции $y_i = y' \circ p_i^{-1}: U \rightarrow \mathbb{C}$ по замкнутому пути, идущему из точки $2c + 1$ вдоль отрезков $[2c + 1, 2c]$, $[2c, c + \sqrt{-1} \operatorname{Im} x_m]$, $[c + \sqrt{-1} \operatorname{Im} x_m, x_m + \varepsilon]$ (концы отрезков указаны в порядке следования точек на пути), где ε — достаточно малое число, затем по окружности радиуса ε , обходящей в положительном направлении (против часовой стрелки) точку x_m , и обратно по только что упомянутым отрезкам в точку $2c + 1$, получаем некоторую функцию $y_j = y' \circ p_j^{-1}$ для подходящего $1 \leq j \leq \deg_Y \Phi$, поскольку при аналитическом продолжении сохраняется соотношение $\Phi_1(x, y') = 0$. В таком случае в множествах $W^{(i)}$ и $W^{(j)}$ отождествляются точки $q_i(x_m)$ и $q_j(x_m)$ и верхний замкнутый край разреза B_m в $W^{(i)}$ склеивается с нижним открытым краем разреза B_m в $W^{(j)}$. Последнее эквивалентно тому, что если $z \in B_m$, то всякая окрестность точки $q_i(z)$ имеет непустое пересечение с $W^{(j)}$. Описанными отождествлениями при всевозможных i, m исчерпываются все склеивания между множествами $\overline{W}^{(i)}$ и, следовательно, задается риманова поверхность W (ср. [6, 9]).

З а м е ч а н и я. 2.1. Вместо рассмотренного выше замкнутого пути с началом в точке $2c + 1$ можно взять любой другой гомотопный ему замкнутый путь на поверхности $\mathbb{P}^1(\mathbb{C}) \setminus \{x_1, \dots, x_\mu, \infty\}$ [6, 9].

З а м е ч а н и е 2.2. Вместо точек x_m , являющихся корнями дискриминанта $\Delta(\alpha_1, \dots, \alpha_n, \alpha, X)$, можно взять в описанной конструкции любое другое подмножество $\mathbb{C}$, содержащее множество точек ветвления отображения p [6, 9].

Выберем путь, используя замечание 1 специальным образом. Пусть $\chi_m \in \mathbb{Q}[\sqrt{-1}]$ — вычисленные с точностью до $(1/3)2^{-MP_*(d_*)}$ приближенные значения корней x_m , $1 \leq m \leq \mu$. Положим $\varepsilon_0 = (1/2)2^{-MP_*(d_*)}$. Будем строить аналитическое продолжение вдоль пути Γ_m , идущего по отрезкам $[2c + 1, 2c]$, $[2c, c + \sqrt{-1} \operatorname{Im} \chi_m]$, $[c + \sqrt{-1} \operatorname{Im} \chi_m, \chi_m + \varepsilon_0]$, затем обходящего квадрат Q_m с вершинами $\chi_m + \varepsilon_0 + \sqrt{-1}\varepsilon_0$, $\chi_m - \varepsilon_0 + \sqrt{-1}\varepsilon_0$, $\chi_m - \varepsilon_0 - \sqrt{-1}\varepsilon_0$, $\chi_m + \varepsilon_0 - \sqrt{-1}\varepsilon_0$, начиная с точки $\chi_m + \varepsilon_0$ в направлении против часовой стрелки, и возвращающегося назад в точку $2c + 1$ по указанным только что отрезкам. Носитель пути Γ_m обозначим $\operatorname{Supp} \Gamma_m = \Gamma_m([0, 1])$. Будем также считать, что $\Gamma_m: [0, 1] \rightarrow \mathbb{C}$ — кусочно-линейное отображение и $\operatorname{card}(\Gamma_m^{-1}(z)) \leq 2$ для всякого $z \in \operatorname{Supp} \Gamma_m$, причем $\operatorname{card}(\Gamma_m^{-1}(z)) = 1$, если $z \in Q_m \setminus \{\chi_m + \varepsilon_0\}$.

Для построения аналитического продолжения необходимы следующие леммы.

Л е м м а 2.1. Пусть $a \in \operatorname{Supp} \Gamma_m$ и пусть $\omega = \sum_{i \geq 0} \omega_i(x - a)^i$ — разложение в степенной ряд некоторой функции ω , такой, что $\Phi_1(x, \omega) = 0$ и $R = \min_{1 \leq m \leq \mu} |a - x_m|$. Тогда справедливы сле-

дующие оценки на коэффициенты степенного ряда $|\omega_i| < 2^{MP_s(d_s)} \left(\frac{3}{4}R\right)^{-i}$ для всех $i \geq 0$.

Доказательство. Согласно интегральной формуле Коши $\omega_i = (1/(2\pi \sqrt{-1})) \int_0 \omega(z) dz/(z-a)^{i+1}$, где интеграл берется по окружности O радиуса $(3/4)R$ с центром в точке a . Следовательно, $|\omega_i| < \max_{z \in O} |\omega(z)| (3R/4)^{-i}$. Пусть

$$\Phi(X, Y) = \sum_i \Phi_i(t_1, \dots, t_n, \eta) Y^i,$$

$$\Phi_i(t_1, \dots, t_n, \eta) \in \mathbb{Z}[\theta][t_1, \dots, t_n, \eta].$$

Тогда по лемме 1.3 (i) выполнено $\max_{z \in O} |\omega(z)| < \max_{z \in O} \sum_i |\Phi_i(\alpha_1, \dots, \alpha_n, \alpha, z)| < 2^{MP_s(d_s)}$ в соответствии с установленными выше верхними оценками на $|\alpha_i|$, $1 \leq i \leq n$, $|\alpha|$ и тем, что $|z| < 4c$, если $z \in O$. Лемма доказана.

Лемма 2.2. Пусть $z \in \mathbb{C}$ — такое число, что $\min_{1 \leq m \leq \mu} |z - x_m| > (1/4)\varepsilon_0$, $|z| < 4c$, и пусть (см. выше) $y_i(z)$, $1 \leq i \leq \deg_Y \Phi$ — все корни многочлена $\Phi_1(z, Y) \in \mathbb{C}[Y]$. Тогда для любых различных индексов i, j имеет место неравенство:

$$|y_i(z) - y_j(z)| > 2^{-MP_s(d_s)} = 3\varepsilon_1.$$

Здесь $3\varepsilon_1$ — обозначение.

Доказательство. Имеем:

$$|y_i(z) - y_j(z)|^2 = |\Delta(\alpha_1, \dots, \alpha_n, \alpha, z)| \prod_{\substack{1 \leq \beta < \gamma \leq \deg_Y \Phi \\ (\beta, \gamma) \neq (i, j), (j, i)}} (y_\beta(z) - y_\gamma(z)) \times \\ \times (lc_X \Delta)(\alpha_1, \dots, \alpha_n, \alpha)^{2\mu-1} > 2^{-MP_s(d_s)}$$

согласно верхним оценкам $|y_\beta(z)|$, $|y_\gamma(z)|$, $|(lc_X \Delta)(\alpha_1, \dots, \alpha_n, \alpha)| < 2^{M^{\mathcal{P}}(d_s)}$ (см. лемму 1.3 (i)), а также нижней оценке $|\Delta(\alpha_1, \dots, \alpha_n, \alpha, z)| = |(lc_X \Delta)(\alpha_1, \dots, \alpha_n, \alpha)| \prod_{1 \leq m \leq \mu} |z - x_m| > 2^{-M^{\mathcal{P}}(d_s)}$, в которой используется неравенство $|(lc_X \Delta)(\alpha_1, \dots, \alpha_n, \alpha)| > 2^{-M^{\mathcal{P}}(d_s)}$, установленное в конце разд. 1.

Лемма 2.3. Пусть $g = Z^m + \sum_{0 \leq i < m} g_i Z^i$ — многочлен степени $m \geq 1$ с комплексными коэффициентами g_i , причем $|g_i| < N$, $0 \leq i < m$, где $N \geq 1$. Далее, пусть $\psi = \sum_{0 \leq i \leq s} \psi_i Z^i$ — также многочлен с комплексными коэффициентами ψ_i , $0 \leq i \leq s$, $\deg \psi = s$, причем $|\psi_i| < \varepsilon' = \min \{ \max \{ 10m(N+1), N_1 \}^{m-s} / (10(m+s)(s+1)), (\varepsilon/(2m))^m ((N+1)m^{-s}(s+1)^{-1}) \}$ для всех $0 \leq i \leq s$, где $N_1 > 2 + \sum_{0 \leq i < m} |g_i|$ и $0 < \varepsilon \leq 1$ — произвольные числа.

Обозначим через z_i , $1 \leq i \leq m$ корни многочлена g . Тогда можно так упорядочить корни $\tilde{z}_i$ многочлена $g_1 = g + \psi$, что для всех

$1 \leq i \leq m$ будет выполнено $|z_i - \tilde{z}_i| < \varepsilon$ и, если $s > m$, для всех $m < i \leq s$ будет справедливо $|\tilde{z}_i| > N_1$.

Доказательство. Пусть $N_2 = \max \{10m(N+1), N_1\}$. Покажем, что в круге, ограниченном окружностью O радиуса N_2 с центром в нуле, содержится ровно m нулей многочлена $g_1 = g + \psi$. Действительно, число нулей многочлена g_1 в этом круге равно $(1/(2\pi V\sqrt{-1})) \int_O g'_1(z) dz/g_1(z)$ и, следовательно, заключено между числами $N_2 \min_{z \in O} |g'_1(z)/g_1(z)|$ и $N_2 \max_{z \in O} |g'_1(z)/g_1(z)|$. Если $z \in O$, то

$$\begin{aligned} |g'_1(z)/g_1(z)| &= \left| \left(\sum_{m < i \leq s} i(\psi_i/(1+\psi_m)) z^{i-m} + m + \right. \right. \\ &+ \sum_{0 \leq i < m} i((g_i + \psi_i)/(1+\psi_m)) z^{i-m} \Big) / \left(z \left(\sum_{m < i \leq s} (\psi_i/(1+\psi_m)) z^{i-m} + \right. \right. \\ &+ 1 + \sum_{0 \leq i < m} ((g_i + \psi_i)/(1+\psi_m)) z^{i-m} \Big) \Big| \leq (m+2|s-m|sN_2^{s-m}\varepsilon' + \\ &+ 2m(N+1)/N_2)/((1-2|s-m|N_2^{s-m}\varepsilon' - 2(N+1)/N_2)N_2) \leq \\ &\leq (m+2/5)/((1-2/(5m))N_2) < (m+1)/N_2. \end{aligned}$$

Таким образом, число корней многочлена g_1 в рассматриваемом круге меньше $m+1$. Аналогично можно оценить снизу $|g'_1(z)/g_1(z)| \geq (m-2/5)/(N_2(1+2/(5m))) > (m-1)/N_2$, т. е. число корней в рассматриваемом круге больше $m-1$ и, значит, равно m .

В круге радиуса N_1 с центром в нуле содержится не больше m корней многочлена g_1 , так как $N_2 \geq N_1$. Корни z_i многочлена g по модулю не превосходят $1 + \sum_{0 \leq i < m} |g_i|$. Следовательно, доказав первую часть утверждения леммы, покажем, что в круге радиуса N_1 с центром в нуле есть ровно m корней, и этим завершим доказательство леммы.

Поскольку отображение, которое ставит в соответствие набору чисел $u_1, \dots, u_n$ их элементарные симметрические функции, конечно, а потому и открыто в классической топологии [8], то для любого многочлена $q \in \mathbb{C}[Z]$ степени n с корнями $u_1, \dots, u_n$ и любого $\varepsilon > 0$ существует $\varepsilon'' > 0$, такое, что если $q_1 \in \mathbb{C}[Z]$, $\deg q_1 \leq n$ и модули коэффициентов q_1 не превосходят ε'' , то $\deg(q+q_1) = n$, и можно так упорядочить корни $\tilde{u}_1, \dots, \tilde{u}_n$ многочлена $q+q_1$, что будут выполняться неравенства $|u_i - \tilde{u}_i| < \varepsilon$ для всех $1 \leq i \leq n$.

Пусть $A = \{z \in \mathbb{C}: |z - z_i| \leq \varepsilon/(2m), 1 \leq i \leq m\}$ и $A = \bigcup_{j \in J} A_j$, где A_j — компоненты связности A , каждая из которых

является объединением не более чем m кругов радиуса $\varepsilon/(2m)$. Пусть $0 \leq t \leq 1$. Покажем теперь, что если $z \notin A$, то $(g + t\psi)(z) \neq 0$. Предположим противное. Тогда $(g + t\psi)(z) = 0$ и $|z| < (N+1)m$. Следовательно, $|t\psi(z)| < (\varepsilon/(2m))^m$. С другой стороны, $|t\psi(z)| = |g(z)| = \prod_{1 \leq i \leq m} |z - z_i| > (\varepsilon/(2m))^m$, что при-

водит к противоречию и доказывает наше утверждение. Из сформулированного выше утверждения о непрерывной зависимости корней многочлена от коэффициентов вытекает, что число корней (учитывая их кратности) многочлена $g + t\psi$, содержащихся в компоненте связности A_j , не зависит от t при $0 < t \leq 1$. Кроме того, из интегральной формулы для количества нулей аналитической функции в области следует, что при t , близких к нулю, это число совпадает с числом корней многочлена g в компоненте A_j . Поэтому число корней многочлена $g + \psi$ в A_j также совпадает с числом корней многочлена g в A_j . Отсюда вытекает, что можно так упорядочить корни $\tilde{z}_j$ многочлена $g + \psi$, что будет выполнено $|z_i - \tilde{z}_i| \leq \max_{j \in J} \text{diam } A_j \leq 2m(\varepsilon/(2m)) = \varepsilon$, $1 \leq i \leq m$, где

$\text{diam } A_j$ обозначает диаметр A_j . В действительности имеют место строгие неравенства $|z_i - \tilde{z}_i| < \varepsilon$, поскольку неравенства на $|\psi_i|$ строгие, что завершает доказательство леммы.

Л е м м а 2.4. Пусть $A = (a_{ij})$ и $B = (b_{ij})$ — квадратные матрицы порядка s , причем $a_{ij}, b_{ij} \in \mathbb{C}[Z]$, $\deg a_{ij} < m$, $\deg b_{ij} < m$, модули коэффициентов многочленов a_{ij} не превосходят N , где $N \geq 1$, а модули коэффициентов многочленов b_{ij} не превосходят $\varepsilon_2 = \varepsilon / ((2m)^s s! N^{s-1})$ для некоторого числа $0 < \varepsilon \leq 1$. Тогда модули коэффициентов многочлена $\det(A + B) - \det(A)$ не превосходят ε .

Д о к а з а т е л ь с т в о. Раскладывая каждую строку определителя $\det(A + B)$ в сумму строки из матрицы A и строки из матрицы B и представляя тем самым $\det(A + B)$ в виде суммы 2^s определителей, получим, что сумма модулей коэффициентов многочлена $\det(A + B) - \det(A)$ не превосходит $\sum_{1 \leq i \leq s} \binom{s}{i} \varepsilon_2^i N^{s-i} \times$

$\times m^s s! < (2m)^s \varepsilon_2 N^{s-1} s! = \varepsilon$, откуда и следует утверждение леммы.

Обозначим через $\tilde{\Phi}$ некоторый многочлен из $\mathbb{Q}[\sqrt{-1}][X, Y]$, такой, что $\deg_Y \tilde{\Phi} = \deg_Y \Phi$, $\deg_X \tilde{\Phi} = \deg_X \Phi$, $\text{lc}_Y \tilde{\Phi} = 1$. Пусть $\tilde{D} = \tilde{D}(X) \in \mathbb{Q}[\sqrt{-1}][X]$ — дискриминант многочлена $\tilde{\Phi}$ относительно Y и $\tilde{x}_i \in \mathbb{C}$, $1 \leq i \leq \deg \tilde{D}$ — корни многочлена $\tilde{D}$. При фиксированном $z \in \mathbb{C}$ через $\tilde{y}_j(z)$, $1 \leq j \leq \deg_Y \tilde{\Phi}$ будем обозначать корни многочлена $\tilde{\Phi}(z, Y) \in \mathbb{Q}[\sqrt{-1}, z][Y]$ (ср. лемму 2.2). Здесь заранее не предполагаем, что $y_j(z)$ при фиксированном j является аналитической функцией или даже непрерывной функцией от z . Пусть, наконец, $\sum_{i \geq 0} \tilde{\omega}_i (x - a)^i$ — разложение в степенной ряд (считаем, что это разложение существует) в точке $a \in \text{Supp } \Gamma_m$ функции $\tilde{\omega}$, такой, что $\tilde{\Phi}(x, \tilde{\omega}) = 0$. Дополним еще $x_1, \dots, x_n$ до семейства x_j , $1 \leq j \leq \deg_X D = \mu_1$, корней с кратностями дискриминанта $D(\alpha_1, \dots, \alpha_n, \alpha, X)$ многочлена $\Phi_1(X, Y)$.

Л е м м а 2.5. Существует такой полином P_7 , что если модули коэффициентов многочлена $\Phi_1 - \tilde{\Phi}$ меньше $\varepsilon_3 = 2^{-M^2 P_7(d_i)}$,

то справедливы следующие утверждения.

(i) Можно так упорядочить корни $\tilde{x}_i$ многочлена $\tilde{D}$, что для всех $1 \leq i \leq \mu_1$ будет выполнено $|x_i - \tilde{x}_i| < \varepsilon_0/8 = (1/16) \times \times 2^{-MP_*(d_*)}$ (определение ε_0 см. выше) для всех $i > \mu_1$ будет выполнено $|\tilde{x}_i| > 4c + 2$.

(ii) Для любого $z \in \mathbb{C}$, такого, что $\min_{1 \leq m \leq \mu} |z - x_m| > \varepsilon_0/4$ и $|z| < 4c + 2 < 2^{MP_*(d_*)}$, можно так упорядочить значения $\tilde{y}_j(z)$, что будут выполнены неравенства $|y_j(z) - \tilde{y}_j(z)| < < (1/3) 2^{-MP_*(d_*)} = \varepsilon_1$ (здесь P_6 и ε_1 из леммы 2.2) для всех $1 \leq j \leq \deg_Y \Phi_1 = \deg_Y \tilde{\Phi}$.

(iii) Пусть функции ω и $\tilde{\omega}$ (разложение для $\tilde{\omega}$ здесь существует в силу (i)), такие, что $\omega_0 = y_j(a)$, $\tilde{\omega}_0 = \tilde{y}_j(a)$ для некоторого $1 \leq j \leq \deg_Y \Phi$. Положим $s = 2M(P_6(d_*) + P_5(d_*)) + 10$. Тогда для любого $0 \leq i \leq s$ выполняется неравенство $|\omega_i - \tilde{\omega}_i| < < (12(s+1))^{-1} 2^{-M((P_*(d_*) + P_*(d_*) + 2)s + P_*(d_*))} = \varepsilon_4$. (определение P_5 см. в лемме 2.1).

Доказательство. Пункты (i) и (ii) следуют непосредственно из лемм 2.2, 2.3, 2.4 (при этом в определении ε_3 можно было бы взять в показателе M , а не M^2). Радиус сходимости R степенного ряда для функции ω не меньше $2\varepsilon_0/3 = (1/3) 2^{-MP_*(d_*)}$ согласно определению Γ_m и тому, что на окружности круга сходимости должна быть точка ветвления алгебраической функции или ее полюс или полюс с ветвлением. Следовательно, согласно п. (i), радиус сходимости $\tilde{R}$ степенного ряда для $\tilde{\omega}$ не меньше $R - (1/8) \varepsilon_0 \geq (13/16) R \geq (13/24) \varepsilon_0$. Теперь, как и в лемме 2.1, можно записать:

$$\omega_i - \tilde{\omega}_i = (1/2\pi \sqrt{-1}) \int_0 (\omega(z) - \tilde{\omega}(z)) dz / (z - a)^{i+1}$$

$$\text{и } |\omega_i - \tilde{\omega}_i| \leq \max_{z \in O} |\omega(z) - \tilde{\omega}(z)| (3R/4)^{-i}.$$

Согласно леммам 2.2, 2.3, 2.4, существует такой полином P_7 , что если модули коэффициентов многочлена $\Phi_1 - \tilde{\Phi}$ меньше ε_3 , то выполняются утверждения п. (i) и (ii) и, кроме того, $|y_j(z) - \tilde{y}_j(z)|^s (2/\varepsilon_0)^s < \varepsilon_4$ при $\min_{1 \leq m \leq \mu} |z - x_m| > \varepsilon_0/4$ и $|z| < 4c + 2$ (отметим, что множитель M^2 возникает в показателе степени за счет возведения величины порядка $2^{-MP_*(d_*)}$ в степень s). В таком случае также выполнено $\max_{z \in O} |\omega(z) - \tilde{\omega}(z)| (3R/4)^{-i} < \varepsilon_4$ для всех $0 \leq i \leq s$. Действительно, $(\omega - \tilde{\omega})$ — непрерывная функция в круге $\{z : |z - a| \leq R - \varepsilon_0/8\}$. Далее, $|\omega(a) - \tilde{\omega}(a)| < (\varepsilon_0/2)^s \varepsilon_4 < \varepsilon_1$, и если $|\omega(z^{(1)}) - \tilde{\omega}(z^{(1)})| > (3R/4)^i \varepsilon_4 \geq (\varepsilon_0/2)^s \varepsilon_4$ для некоторого $z^{(1)}$, такого, что $|z^{(1)} - a| < R - \varepsilon_0/8$, то, согласно лемме 2.1, имеем $|\omega(z^{(1)}) - \tilde{\omega}(z^{(1)})| > 2\varepsilon_1$. Тогда для некоторой точки $z^{(2)}$, такой, что $|z^{(2)} - a| < R - \varepsilon_0/8$, справедливо равенство $|\omega(z^{(2)}) - \tilde{\omega}(z^{(2)})| = 3\varepsilon_1/2$, что невозможно в силу п. (ii).

Полученное противоречие завершает доказательство леммы.

Л е м м а 2.6 (Гензеля). Пусть элементы $a, \tilde{\omega}, \tilde{\omega}_i, \tilde{\Phi}, \varepsilon_3$ такие же, как в лемме 2.5, число $a \in \mathbb{Q}[\sqrt{-1}]$, длина записи $l(a) < M\mathcal{P}(d_4)$, модули коэффициентов многочлена $\Phi_1 - \tilde{\Phi}$ меньше ε_3 и $l(\tilde{\Phi}) < M^2\mathcal{P}(d_4)$. Пусть, далее, $\xi \in \mathbb{C}$ — корень многочлена $\tilde{\Phi}(a, Y)$, такой, что $\tilde{\omega}_0 = \xi$. Тогда $\tilde{\omega}_i \in \mathbb{Q}[\sqrt{-1}, \xi]$ для всех $i \geq 0$ и $l(\tilde{\omega}_i) < M^2\mathcal{P}(d_4(i-1))$ (длина записи $l(\tilde{\omega}_i)$ определяется относительно разложения по базису $\{\xi^j, \sqrt{-1}\xi^j\}$, $0 \leq j < \deg_Y \tilde{\Phi}(a, Y)$, см. введение). Элемент $\tilde{\omega}_i \in \mathbb{Q}[\sqrt{-1}, \xi]$ можно найти за полиномиальное от d_4, i и M время.

Д о к а з а т е л ь с т в о. То, что $\tilde{\omega}_i \in \mathbb{Q}[\sqrt{-1}, \xi]$, вытекает непосредственно из процесса построения элементов ω_i по лемме Гензеля. Значение $(\partial\tilde{\Phi}/\partial Y)(a, \xi) \neq 0$ и $l((\partial\tilde{\Phi}/\partial Y)(a, \xi)) < M^2\mathcal{P}(d_4)$. В кольце $\mathbb{Q}[\sqrt{-1}, \xi][[X-a]][Y]$ многочленов от Y над кольцом формальных степенных рядов от $X-a$ над полем $\mathbb{Q}[\sqrt{-1}, \xi]$ имеет место равенство:

$$\tilde{\Phi} = \left(Y - \xi - \sum_{i \geq 1} \tilde{\omega}_i (X-a)^i \right) \left(\tilde{\Phi}(a, Y)/(Y - \xi) + \sum_{i \geq 1} g_i (X-a)^i \right),$$

где $g_i \in \mathbb{Q}[\sqrt{-1}, \xi][Y]$ и $\deg g_i < \deg_Y \tilde{\Phi}(a, Y) - 1$ для всех $i \geq 1$. Пусть $\tilde{\Phi} = \sum_{i \geq 0} \tilde{\Phi}_i (X-a)^i$, где $\tilde{\Phi}_i \in \mathbb{Q}[\sqrt{-1}][Y]$.

Тогда $(Y - \xi)g_i - (\tilde{\Phi}(a, Y)/(Y - \xi))\tilde{\omega}_i = \tilde{\Phi}_i + \sum_{\beta+\gamma=i, \beta, \gamma < i} g_\beta \tilde{\omega}_\gamma$ для всех $i \geq 1$. Следовательно, коэффициенты многочленов g_i и $\tilde{\omega}_i$ являются неизвестными системы линейных уравнений, получающейся приравниванием коэффициентов при одинаковых степенях Y в левой и правой частях последнего равенства. Матрица этой системы есть матрица Сильвестра для результата многочленов $Y - \xi, \tilde{\Phi}(a, Y)/(Y - \xi)$. Определитель ее равен $\pm (\partial\tilde{\Phi}/\partial Y)(a, \xi)$. Предположим, что $l(g_i), l(\tilde{\omega}_i) < M^2 \times \times P_9(d_4(i-1))$, завершим доказательство леммы индукцией по i (см. [7]). Здесь существенно, что выбран $P_9(d_4(i-1))$, а не $P_9(d_4 i)$, поскольку $l(g_\beta \tilde{\omega}_\gamma) < M^2 P_9(d_4(i-2))$. После решения линейной системы получим $l(g_i), l(\tilde{\omega}_i) < M^2 (P_9(d_4(i-2)) + \mathcal{P}(d_4) \log_2 i) < M^2 P_9(d_4(i-1))$ при подходящем выборе полинома P_9 .

Опишем теперь алгоритм построения аналитического продолжения вдоль пути Γ_m алгебраической функции, удовлетворяющей уравнению $\Phi_1(x, Y) = 0$. Положим $t_0 = 0, a_0 = 2c + 1$ и $\xi^{(0)}$ равным некоторому корню многочлена $\Phi_1(a_0, Y)$, причем корень задается своим приближением $\xi^{(0)}$ с точностью $(1/5)\varepsilon_1 = (1/15) \times \times 2^{-MP_9(d_4)}$. Пусть уже построены точки $t_i \in [0, 1], a_i \in \in \text{Supp } \Gamma_m$, такие, что $\Gamma_m(t_i) = a_i$, и построено приближение ξ_i с точностью $\varepsilon_i/5$ корня $\xi^{(i)}$ многочлена $\Phi_1(a_i, Y)$ для некоторого $i \geq 0$. Если $a_i = 2c + 1$ и $i > 0$, то процесс построения заканчивается. В противном случае построим t_{i+1}, a_{i+1} и $\xi^{(i+1)}, \xi^{(i+1)}$.

Пусть $\rho = \min_{1 \leq m \leq \mu} |a_i - \chi_m|$ (напомним, что χ_m — приближение к χ_m с точностью $(1/3) 2^{-MP \cdot (d_4)}$). В качестве $t_{i+1} \in [0, 1]$ и $a_{i+1} \in \text{Supp } \Gamma_m$ возьмем такие элементы, что

$$\Gamma_m(t_{i+1}) = a_{i+1} \in \mathbb{Q}[\sqrt{-1}], (\rho - (2\varepsilon_0/3))/4 \leq |a_{i+1} - a_i| \leq \\ \leq (\rho - (2\varepsilon_0/3))/2, l(a_{i+1}) < M\mathcal{P}(d_4) \text{ и}$$

$$\Gamma_m([t_i, t_{i+1}]) \subset \{z: |z - a_i| < (\rho - (2\varepsilon_0/3))/2\},$$

причем, если можно взять, согласно этим условиям, $a_{i+1} = 2c + 1$ или эти условия не выполнимы на данном шаге, то берем $a_{i+1} = 2c + 1$, $t_{i+1} = 1$ (на последнем шаге может не выполняться лишь условие $|a_{i+1} - a_i| \geq (\rho - (2\varepsilon_0/3))/4$). Для построения $\xi^{(i+1)}$ найдем многочлен $\tilde{\Phi} \in \mathbb{Q}[\sqrt{-1}][X, Y]$, такой, что модули коэффициентов многочлена $\tilde{\Phi} - \Phi_1$ меньше ε_3 (см. лемму 2.5) и $l(\tilde{\Phi}) < M^2\mathcal{P}(d_4)$. Вычислим с точностью $\varepsilon_1/5$ корни многочлена $\tilde{\Phi}(a_i, Y)$. Среди этих приближенных значений корней по лемме 2.2 и 2.5 (ii) найдется единственное (обозначим его через ξ), такое, что $|\xi - \xi^{(i)}| < 7\varepsilon_1/5$. Соответствующий приближению ξ корень многочлена $\tilde{\Phi}(a_i, Y)$ обозначим через ξ . Разложим многочлен $\tilde{\Phi}(a_i, Y)$ на неприводимые множители над полем $\mathbb{Q}(\sqrt{-1})$ с помощью алгоритма из [7, гл. 1] и среди этих множителей найдем тот, корнем которого является элемент ξ и тем самым зададим поле $\mathbb{Q}[\xi, \sqrt{-1}]$. С помощью леммы 2.6 найдем сумму $\sum_{0 \leq j \leq s} \tilde{\omega}_j (X - a_i)^j$, где $\tilde{\omega}_j \in \mathbb{Q}[\xi]$, $\tilde{\omega}_0 = \xi$ и число s имеют тот же

смысл, что и в леммах 2.5, 2.6. Далее, вычислим $\tilde{\omega}_j \in \mathbb{Q}[\sqrt{-1}]$, такие, что $|\tilde{\omega}_j - \tilde{\omega}_j| < \varepsilon_4$ (см. лемму 2.5 (iii)) и $l(\tilde{\omega}_j) < M^2\mathcal{P}(d_4)$, $0 \leq j \leq s$. Приближенные значения $\tilde{\omega}_j$ для $\tilde{\omega}_j$ можно найти в полиномиальное время, вычислив сначала с достаточной степенью точности элемент ξ , поскольку длины записей $l(\tilde{\omega}_j)$ ограничены сверху (см. лемму 2.6). Наконец, найдем сумму $\sigma = \sum_{0 \leq j \leq s} \tilde{\omega}_j \times$

$\times (a_{i+1} - a_i)^j \in \mathbb{Q}[\sqrt{-1}]$. Вычислим также приближенные значения корней многочлена $\Phi_1(a_{i+1}, Y)$ с точностью до $\varepsilon_1/5$. Покажем, что среди этих приближенных значений существует единственное (обозначим его через $\xi^{(i+1)}$), такое, что $|\sigma - \xi^{(i+1)}| < 6\varepsilon_1/5$. Действительно,

$$\sigma - \xi^{(i+1)} = \sum_{0 \leq j \leq s} (\tilde{\omega}_j - \tilde{\omega}_j) (a_{i+1} - a_i)^j + \sum_{0 \leq j \leq s} (\tilde{\omega}_j - \omega_j) (a_{i+1} - a_i)^j + \\ + \sum_{j > s} \omega_j (a_{i+1} - a_i)^j + \left(\sum_{j > 0} \omega_j (a_{i+1} - a_i)^j - \xi^{(i+1)} \right), \quad (2.1)$$

где $\tilde{\omega}_j$ и ω_j такие же, как в лемме 2.5 при $a = a_i$, $\omega_0 = \xi^{(i)}$, $\tilde{\omega}_0 = \xi$. Согласно определению $\tilde{\omega}_j$ и по леммам 2.5 и 2.1, модули первого, второго и третьего слагаемых в левой части равенства (2.1) не превосходят соответственно $\varepsilon_1/4$, $\varepsilon_1/4$ и $\varepsilon_1/2$. Модуль четвертого слагаемого для всех, кроме одного, приближений корней будет

больше $14\varepsilon_1/5$, а для одного, именно для $\xi^{(i+1)}$, — меньше $\varepsilon_1/5$, что и доказывает наше утверждение. В качестве $\xi^{(i+1)}$ возьмем однозначно соответствующий приближению $\xi^{(i+1)}$ корень многочлена $\Phi_1(a_{i+1}, Y)$. Тогда

$$\left| \xi^{(i+1)} - \sum_{j \geq 0} \omega_j (a_{i+1} - a_i)^j \right| \leq \left| \xi^{(i+1)} - \bar{\xi}^{(i+1)} \right| + \\ + \left| \bar{\xi}^{(i+1)} - \sum_{j \geq 0} \omega_j (a_{i+1} - a_i)^j \right| \leq 2\varepsilon_1/5.$$

Поэтому $\xi^{(i+1)} = \sum_{i \geq 0} \omega_i (a_{i+1} - a_i)^i$ по лемме 2.2. Последнее равенство означает, что $\xi^{(i+1)}$ является значением в точке a_{i+1} требуемого аналитического продолжения вдоль части пути Γ_m исходной ветви алгебраической функции y' , которая задавалась разложением в степенной ряд в окрестности точки $2c + 1$. Закончено описание алгоритма для аналитического продолжения и тем самым построения римановой поверхности отображения p и триангуляций T_1 и T_2 .

Время работы алгоритма построения аналитического продолжения на одном шаге при переходе от $t_i, a_i, \xi^{(i)}$ к $t_{i+1}, a_{i+1}, \xi^{(i+1)}$ оценивается сверху полиномом от $L(\Phi), L(\varphi), L(h)$. Остается только оценить общее число шагов при построении аналитического продолжения вдоль пути Γ_m .

Пусть $J \subset \{1, 2, \dots, \mu\}$ — подмножество индексов, таких, что $\operatorname{Re} \chi_j \geq \chi_m + \varepsilon_0$ для $j \in J$, и пусть $\chi'_j = \operatorname{Re} \chi_j + \sqrt{-1} \operatorname{Im} \chi_m$ — проекция точки χ_j на отрезок $[\chi_m + \varepsilon_0, c + \sqrt{-1} \operatorname{Im} \chi_m]$. Без ограничения общности будем считать, перенумеровав, если необходимо, точки χ_i , что J — начальный отрезок натурального ряда (или J пусто) и что $\operatorname{Re} \chi_{j-1} \leq \operatorname{Re} \chi_j$ для $j-1, j \in J$. Пусть $V_j = [\chi'_j - \varepsilon_0, \chi'_j + \varepsilon_0]$. Число точек a_i на каждом из отрезков V_j , а также на сторонах квадрата Q_m ограничено константой, поскольку $|a_{i+1} - a_i| \geq (\rho - (2\varepsilon_0/3))/4 \geq \varepsilon_0/6$. Рассмотрим теперь некоторый отрезок $[\chi'_{j-1} + \varepsilon_0, \chi'_j - \varepsilon_0]$, и пусть этому отрезку принадлежат точки a_i при $\beta \leq i \leq \gamma$, причем $\operatorname{Re} \chi_j - \varepsilon_0 \geq \operatorname{Re} a_\beta > \operatorname{Re} a_{\beta+1} > \dots > \operatorname{Re} a_\kappa \geq \operatorname{Re} (\chi_j + \chi_{j-1})/2 > \operatorname{Re} a_{\kappa+1} > \dots > \operatorname{Re} a_\gamma \geq \operatorname{Re} \chi_{j-1} + \varepsilon_0$. Положим $a_\beta = a_\beta + (\varepsilon_0/6)$. Тогда по индукции доказывается, что $\operatorname{Re} a_\beta - \operatorname{Re} a_i \geq (5/4)^{i-\beta} (\varepsilon_0/6)$ при $\beta \leq i \leq \kappa$. Аналогично доказывается, что при $\kappa < i \leq \gamma$ выполнено неравенство $\operatorname{Re} a_i - \operatorname{Re} \chi_{j-1} - (2\varepsilon_0/3) \leq (3/4)^{i-\kappa-1} (\operatorname{Re} (\chi_j - \chi_{j-1}) + (2\varepsilon_0/3))/2$. Следовательно, на отрезке $[\chi'_{j-1} + \varepsilon_0, \chi'_j - \varepsilon_0]$ содержится не более $O(1 + |\log_2 \varepsilon_0| + |\log_2 \operatorname{Re} (\chi'_j - \chi'_{j-1})|) \leq M\mathcal{P}(d_4)$ точек a_i , для которых $\operatorname{Re} a_i > \operatorname{Re} a_{i+1}$. Аналогичным образом рассматриваются случаи точек a_i , для которых $\operatorname{Re} a_{i+1} > \operatorname{Re} a_i$ (когда проходим этот отрезок в обратном направлении), а также случаи отрезков $[\chi_m + \varepsilon_0, \chi'_1 - \varepsilon_0]$, $[\chi'_1 + \varepsilon_0, c + \sqrt{-1} \operatorname{Im} \chi_m]$, $[\chi_m + \varepsilon_0, c + \sqrt{-1} \operatorname{Im} \chi_m]$ (если такие промежутки включаются в множество $\operatorname{Supp} \Gamma_m \setminus \left(\bigcup_{j \in J} V_j \right)$), $[c + \sqrt{-1} \operatorname{Im} \chi_m, 2c]$, $[2c, 2c + 1]$.

В результате общее число шагов ограничено $M\mathcal{P}(d_4)$. Этим завершается доказательство того, что алгоритм, приведенный в настоящем разделе, работает в полиномиальное от $L(\Phi)$, $L(\varphi)$, $L(h)$ время.

С л е д с т в и е. Род g римановой поверхности поля алгебраических функций $K'(x, y)$ может быть вычислен в полиномиальное время.

Д о к а з а т е л ь с т в о. Нами была построена триангуляция T_2 римановой поверхности, и теперь достаточно воспользоваться формулой Эйлера $2 - 2g = e_0 - e_1 + e_2$, где e_i — число i -мерных симплексов триангуляции, $0 \leq i \leq 2$.

3. Основная теорема для полей степени трансцендентности один над полем констант

Рассмотрим случай из предыдущего раздела. Вычислим группу Галуа G поля разложения E многочлена $\Phi(x, Y) \in \bar{K}'(x)[Y]$ над полем $\bar{K}'(x)$. Построенное в разд. 1 вложение полей $K' \rightarrow \mathbb{C}$ продолжается до вложения алгебраического замыкания $\bar{K}' \rightarrow \mathbb{C}$ ($\bar{K}'$ будем отождествлять с его образом в $\mathbb{C}$), и при этом в композиции полей $E \subset \mathbb{C}(x)$ справедливо равенство $E \cap \mathbb{C}(x) = \bar{K}'(x)$. Действительно, если $z \in E$, то $\psi(z, x) = 0$ для некоторого неприводимого многочлена $\psi \in \bar{K}'[Z, X]$, и равенство $\psi(z, x) = 0$ для $z \in \mathbb{C}$ возможно, если только $\psi \in \bar{K}'[Z]$ — линейный многочлен, что и требовалось проверить. Следовательно, группа G совпадает с группой Галуа поля разложения $E^{(1)} = E \subset \mathbb{C}(x)$ многочлена $\Phi_1(x, Y)$ над полем $\mathbb{C}(x)$ (напомним, что Φ_1 получается из Φ подстановкой $\alpha_1, \dots, \alpha_n, \alpha$ вместо $t_1, \dots, t_n, \eta$ соответственно). Последняя в свою очередь совпадает с группой монодромии [6, 9] алгебраической функции $y'(x)$, являющейся корнем многочлена $\Phi_1(x, Y)$. Пусть ξ_i , $1 \leq i \leq \deg_Y \Phi$ — все различные корни многочлена $\Phi_1(2c+1, Y)$ (корни задаются своими приближениями, вычисленными в разд. 1) и $y_i|_U = y' \circ p_i^{-1} : U \rightarrow \mathbb{C}$ — аналитические функции, такие, что $y_i(2c+1) = \xi_i$ и $\Phi_1(x, y_i) = 0$ (см. разд. 2). Пусть $y_j|_U$ — функция, которая получается при аналитическом продолжении функции $y_i|_U$ вдоль пути Γ_m . Напомним, что в разд. 2 был найден индекс j , такой, что $\xi_j = y_j(2c+1)$. Обозначим $j = \sigma_m(i)$. Тогда σ_m задает подстановку симметрической группы S_γ степени $\gamma = \deg_Y \Phi$. Группа монодромии функции y' порождается всеми σ_m , $1 \leq m \leq \mu = \deg_x \Delta$ [6, 9]. Таким образом, вычислена группа Галуа $G = \langle \sigma_m : 1 \leq m \leq \mu \rangle \subset S_\gamma$ за полиномиальное от $L(\Phi)$, $L(\varphi)$ и $L(h)$ время.

В дальнейшем потребуются алгоритм для разложения многочленов над полем с алгебраически замкнутым полем констант. Пусть теперь $k, \theta, h, K_1, \eta_1, \varphi_1, K_2, \eta_2, \varphi_2, K, f, \Omega$ такие же, как во введении. Ближайшей целью является описание алгоритма для разложения многочлена f над полем Ω , работающего в полино-

миальное от $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(f)$ время. В частности, этот алгоритм позволяет проверять неприводимость многочлена над полем Ω .

Подобно тому, как это было в разд. 1, будем считать без ограничения общности, что $\varphi_1 \in k[t_1, \dots, t_l][Z]$, $\varphi_2 \in k[t_1, \dots, t_l, \eta_1, t_{l+1}, \dots, t_{n+1}][Z]$, $f \in k[t_1, \dots, t_{n+1}, \eta_1, \eta_2][Z]$ и старшие коэффициенты $lc_Z(h)$, $lc_Z(\varphi_1)$, $lc_Z(\varphi_2)$, $lc_Y(f)$ равны 1. Построим примитивный элемент η расширения $K \supset k(t_1, \dots, t_{n+1})$ и минимальный многочлен $\varphi \in k[t_1, \dots, t_{n+1}][Z]$ для элемента η на основе конструкции из [7, гл. 1, § 3]. Элемент η выбирается в виде $\eta_2 + \beta\eta_1$, где $0 \leq \beta < \deg \varphi_1 \deg \varphi_2$, $\gamma \in \mathbb{Z}$, поэтому $lc_Z \varphi = 1$. Многочлен φ , а также выражения для η_1 и η_2 через η строятся в полиномиальное от $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(f)$ время при помощи решения систем линейных уравнений над полем $k(t_1, \dots, t_{n+1})$. Пользуясь алгоритмом из [7, гл. 1, § 3], разложим φ , рассматриваемый как многочлен от $t_{l+1}, \dots, t_{n+1}$, Z , на абсолютно неприводимые множители над полем $k(t_1, \dots, t_l)$. Этот алгоритм дает на выходе некоторый абсолютно неприводимый множитель $\bar{\varphi} = \bar{\varphi}(t_{l+1}, \dots, t_{n+1}, Z)$ многочлена φ (все такие множители сопряжены), а также подполе $k(t_1, \dots, t_l)[\eta_3] \subset k(t_1, \dots, t_l)$, порожденное коэффициентами $\bar{\varphi}$; для η_3 строится минимальный многочлен $\varphi_3 \in k[t_1, \dots, t_l][Z]$, $lc_Z \varphi_3 = 1$; получаем также выражения для коэффициентов многочлена $\bar{\varphi}$ через η_3 . В дальнейшем будем считать, что η является также корнем $\bar{\varphi}$. Время работы алгоритма полиномиально от $L(h)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(f)$.

Л е м м а 3.1. В подходящем композите полей $\overline{k(t_1, \dots, t_l)}$ и K имеет место равенство $\overline{k(t_1, \dots, t_l)} \cap K = k(t_1, \dots, t_l)[\eta_3]$, кроме того, $\deg_Z \varphi = \deg_Z \bar{\varphi} \deg_Z \varphi_3$.

Д о к а з а т е л ь с т в о. Число различных вложений поля $k(t_1, \dots, t_l)[\eta_3]$ в $k(t_1, \dots, t_l)$ над $k(t_1, \dots, t_l)$ совпадает с числом $\deg_Z \varphi / \deg_Z \bar{\varphi}$ абсолютно неприводимых множителей многочлена φ , поскольку все эти множители сопряжены над $k(t_1, \dots, t_l)$, откуда и следует последнее утверждение. Обозначим $K_0 = K \cap k(t_1, \dots, t_l)$. Элементы $\eta_i \eta_j^i$, $0 \leq i < \deg_Z \varphi_3$, $0 \leq j < \deg_Z \bar{\varphi}$ порождают как линейное пространство над $k(t_1, \dots, t_{n+1})$ поле $K[\eta_3] \supset K$. Поскольку их число $\deg_Z \varphi_3 \deg_Z \bar{\varphi} = \deg_Z \varphi$, то $K[\eta_3] = K$ и $k(t_1, \dots, t_l)[\eta_3] \subset K_0$. Следовательно, $\deg_Z \bar{\varphi} \leq [K : K_0(t_{l+1}, \dots, t_{n+1})] \leq [K : k(t_1, \dots, t_{n+1})[\eta_3]] = \deg_Z \bar{\varphi}$. Отсюда вытекает, что $K_0 = k(t_1, \dots, t_l)[\eta_3]$.

Разложим многочлен f на неприводимые множители над полем K , пользуясь алгоритмом из [7, гл. 1], и в дальнейшем без ограничения общности будем считать, что f неприводим над K . Сделаем в многочлене f замену переменной $Y \mapsto Y + \beta\eta$, где $\beta \in \mathbb{Z}$ с таким расчетом, чтобы выполнялось НОД, $(f(Y + \beta\eta), f'(Y + \beta\eta)) = 1$ для всех вложений σ поля Ω в $\bar{\Omega}$ над $\bar{K}_0(t_{l+1}, \dots, t_{n+1})$. Для этого вычислим $D(Z)$ -дискриминант относительно Y нормы $N(f(Y + \eta Z)) = N_{\bar{K}_0(t_{l+1}, \dots, t_{n+1}, \eta, Y, Z) / \bar{K}_0(t_{l+1}, \dots, t_{n+1}, Y, Z)} \times$

$\times (f(Y + \eta Z))$ из поля $\bar{K}_0(t_{l+1}, \dots, t_{n+1}, \eta, Y, Z)$ в поле $\bar{K}_0(t_{l+1}, \dots, t_{n+1}, Y, Z)$ многочлен $f(Y + \eta Z)$ (здесь Z — новая переменная). Норма и дискриминант вычисляются за полиномиальное время (см. [14] и леммы 1.1, 1.2). Отметим, что $D(Z) \neq 0$ и $\deg_Z D(Z) \leq 2(\deg_Z \bar{\varphi} \deg_Y f)^2$, поэтому перебором можно найти $\beta \in \mathbb{Z}$, $0 \leq \beta \leq 2(\deg_Z \bar{\varphi} \deg_Y f)^2$, такое, что $D(\beta) \neq 0$, и это β будет искомым. В дальнейшем без ограничения общности будем считать, что $\text{НОД}(f, f^\sigma) = 1$ в кольце $\bar{K}[Y]$ для всех вложений $\sigma: \Omega \rightarrow \bar{\Omega}$ над $\bar{K}_0(t_{l+1}, \dots, t_{n+1})$.

Разложим на абсолютно неприводимые множители над $\bar{K}_0$ многочлен $N(f(Y)) \in K_0[t_{l+1}, \dots, t_{n+1}, Y]$, пользуясь алгоритмом из [7, гл. 1, § 3]. Пусть g — один из этих абсолютно неприводимых множителей и $K_0[\eta_4]$ — поле, порожденное коэффициентами g над K_0 , $\varphi_4 \in k[t_1, \dots, t_l, \eta_3][Z]$ — минимальный многочлен для η_4 над K_0 , причем $\text{lc}_Z \varphi_4 = 1$. Тогда многочлен φ_4 неприводим над K , так как $K \cap \bar{k}(t_1, \dots, t_l) = K_0$, и $\bar{f} = \text{НОД}(g, f)$ (здесь НОД берется в кольце $K[\eta_4][Y]$) является неприводимым над $\Omega = \bar{K}_0(t_{l+1}, \dots, t_{n+1}, \eta_2)$ множителем многочлена f . Действительно, $\text{НОД}(g, f^\sigma) \neq 1$ для некоторого вложения $\sigma: \Omega \rightarrow \bar{\Omega}$ над $\bar{K}_0(t_{l+1}, \dots, t_{n+1})$, следовательно, $\bar{f} = \text{НОД}(g, f) \neq 1$, поскольку $g^{\sigma^{-1}} = g$. Предположим, что $\bar{f} = f^{(1)}f^{(2)}$, где $f^{(1)}, f^{(2)} \in \Omega[Y]$, $\text{НОД}(f^{(1)}, f^{(2)}) = 1$. Тогда $\text{НОД}(N(f^{(1)}), N(f^{(2)})) = 1$ в силу того, что $\text{НОД}(f, f^\sigma) = 1$ для всех вложений $\sigma: \Omega \rightarrow \bar{\Omega}$ над $\bar{K}_0(t_{l+1}, \dots, t_{n+1})$. Откуда вытекает, что $\text{НОД}(g, Nf^{(1)}) = 1$ или $\text{НОД}(g, Nf^{(2)}) = 1$, т. е. один из многочленов $f^{(1)}$ или $f^{(2)}$ является константой, и $\bar{f}$ неприводим над Ω , что и доказывает наше утверждение. Все неприводимые над Ω множители многочлена f сопряжены с $\bar{f}$, более точно — они совпадают с $\bar{f}^\tau$, где τ пробегает все вложения $K[\eta_4] \rightarrow \bar{K}$ над K . Описанный алгоритм для разложения многочлена f над полем Ω работает в полиномиальное от $L(f)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(h)$ время. Кроме того, степени и длины записей коэффициентов полученных многочленов удовлетворяют следующим неравенствам: $l(\varphi) < (M_1 + M_3 + n) \mathcal{P}(d_1 d_3)$, $\deg_{t_i}(\varphi) < \mathcal{P}(d_1)$; $l(\varphi_3), l(\bar{\varphi}) < (M_1 + M_3 + n) \mathcal{P}(d_1 d_3)$, $\deg_{t_i}(\varphi_3), \deg_{t_i}(\bar{\varphi}) < \mathcal{P}(d_1)$; $l(\varphi_4), l(\bar{f}) < (M_1 + M_2 + M_3 + (n+1)d_2) \times \times \mathcal{P}(dd_1 d_3)$, $\deg_{t_i} \varphi_4, \deg_{t_i} \bar{f} < d_2 \mathcal{P}(dd_1)$ для всех $1 \leq i \leq n+1$. Эти оценки получаются на основании [7, гл. 1] и лемм 1.1, 1.2.

В дальнейшем будем считать, что многочлен f неприводим над Ω (общий случай будет рассмотрен в разд. 4). Пользуясь алгоритмом из [7, гл. 1, § 3], сделаем замену переменных $Y \mapsto Y + \beta\eta$, $\beta \in \mathbb{Z}$ таким образом, чтобы корень ζ многочлена $f(Y + \beta\eta)$ был примитивным элементом расширения $K_0(t_{l+1}, \dots, t_{n+1}, \eta, \zeta) \supset k(t_1, \dots, t_{n+1})$. Снова без ограничения общности будем считать, что для корня ζ многочлена f выполнено $K_0(t_{l+1}, \dots, t_{n+1}, \eta, \zeta) = k(t_1, \dots, t_{n+1})[\zeta]$ и при этом вычислено выражение для элемента $\eta = \eta(t_1, \dots, t_{n+1}, \zeta)$ в поле $k(t_1, \dots, t_{n+1})[\zeta]$, длина

записи которого оценивается сверху полиномом от $L(f)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(h)$. Более того, справедливы следующие неравенства: $l(\eta(t_1, \dots, t_{n+1}, \xi)) < (M_1 + M_2 + M_3 + (n+1)d_2) \mathcal{P}(dd_1d_3)$, $\deg_{t_i} \eta(t_1, \dots, t_{n+1}, \xi) < d_2 \mathcal{P}(dd_1)$ для всех $1 \leq i \leq n$.

Перейдем к описанию алгоритма для вычисления группы Галуа поля разложения f над полем $\overline{k(t_1, \dots, t_n)(t_{n+1}, \eta)}$, при условии, что f неприводим над этим полем, а многочлен $\bar{f}$ неприводим над полем $\overline{k(t_1, \dots, t_n)(t_{n+1})}$. Это условие проверяется за полиномиальное от $L(f)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(h)$ время с помощью описанного выше алгоритма разложения на неприводимые над полем Ω (в качестве Ω здесь надо взять другие поля $\overline{k(t_1, \dots, t_n)(t_{n+1}, \eta)}$ и $\overline{k(t_1, \dots, t_n)(t_{n+1})}$). Будем считать, что $f \notin \overline{k(t_1, \dots, t_n)}[Z]$, так как иначе группа Галуа единичная. Найдем многочлен $\Phi(t_{n+1}, Y) = M_{\overline{k(t_1, \dots, t_n)(t_{n+1}, \eta, Y)}/\overline{k(t_1, \dots, t_n)(t_{n+1}, Y)}} f$ (ср. выше). Многочлен $\Phi \in K_0(t_{l+1}, \dots, t_n)[Y]$ неприводим над полем $\overline{k(t_1, \dots, t_n)(t_{n+1})}$, поскольку $\Phi(t_{n+1}, \xi) = 0$, элемент ξ примитивный для расширения $\overline{k(t_1, \dots, t_n)(t_{n+1}, \eta, \xi)} \supset \supset \overline{k(t_1, \dots, t_n)(t_{n+1})}$ и $\deg_Y \Phi = \deg_Y f \deg_Z \bar{f} = [k(t_1, \dots, t_n)(t_{n+1}, \eta, \xi) : k(t_1, \dots, t_n)(t_{n+1})]$. Обозначим $t_{n+1} = x$ и вычислим на основе алгоритма из разд. 1, 2 группу Галуа $\tilde{G}_1$ поля разложения $\tilde{E}_1$ многочлена $\Phi(x, Y) \in K_0(t_{l+1}, \dots, t_n)(x)[Y]$ над полем $\overline{k(t_1, \dots, t_n)(x)}$ (обозначения G_1 и E_1 без тильды будут использованы ниже). Дополнительно будем считать, что точка $c \in \mathbb{Z}$ (напомним, что $2c$ — одна из вершин триангуляции T_1 , см. разд. 2) обладает тем свойством, что многочлен $\bar{\Phi}(t_{l+1}, \dots, t_n, 2c+1, Z) \in \overline{k(t_1, \dots, t_n)}[Z]$ не имеет кратных корней. Такую новую точку $c \in \mathbb{Z}$ можно найти перебором, вычислив дискриминант $(D\bar{\Phi})(t_{l+1}, \dots, t_{n+1})$ многочлена $\bar{\Phi}$ относительно Z и взяв в качестве c наименьшее целое γ , такое, что $(D\bar{\Phi})(t_{l+1}, \dots, t_n, 2\gamma+1) \neq 0$ и γ больше старого значения c , определенного в алгоритме из разд. 2. При таком изменении c алгоритм построения $\tilde{G}_1$ по-прежнему будет работать в полиномиальное от $L(f)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(h)$ время.

Напомним, что при вложении $K \rightarrow \mathbb{C}$, построенном в разд. 1 (в нашем случае $K = K_0(t_{l+1}, \dots, t_n)$), элементы $t_1, \dots, t_n, \eta_3$ переходят соответственно в $\alpha_1, \dots, \alpha_n, \alpha$. Обозначим через $\bar{\Phi}_1$ многочлен, который получается из $\bar{\Phi}$ подстановкой $\alpha_1, \dots, \alpha_n, \alpha$ вместо $t_1, \dots, t_n, \eta_3$. Пусть $\bar{a} = \bar{a}(x)$ — корень многочлена $\Phi_1(x, Y)$, рассматриваемый как аналитическая функция на U (см. разд. 2). Тогда значение $\bar{a}_0 = \bar{a}(2c+1)$ полностью определяет $\bar{a}$. Далее, согласно лемме 1.3 (i), (iii), корень $\bar{a}_0$ многочлена $\Phi_1(2c+1, Y)$ задается своим приближением с точностью до $\varepsilon_5 = 2 - (M_1 + M_3 + n + 1) P_{1,0}(d_1 d_3)$. Вычислив это приближение, тем самым зафиксируем $\bar{a}_0$ и $\bar{a}$. Обозначим через $f_1(x, Y)$ и $\Phi_1(\bar{x}, Y)$ многочлены, которые получаются из f и Φ соответственно подстановкой вместо $t_1, \dots, t_n, \eta_3, \eta$ элементов $\alpha_1, \dots, \alpha_n, \alpha, \bar{a}$. Всякий корень многочлена $f_1(2c+1, Y)$ является корнем многочлена

$\Phi_1(2c+1, Y)$. Согласно лемме 1.3 (i), (iii), расстояния между различными корнями многочлена $\Phi_1(2c+1, Y)$ не меньше $2^{-MP_{1,1}(d_1)} = \varepsilon_6$. Вычислив корни многочленов $\Phi_1(2c+1, Y)$, $f_1(2c+1, Y)$ с точностью до $\varepsilon_6/6$ и заново упорядочив при необходимости корни ξ_i , $1 \leq i \leq \deg_Y \Phi$ и многочлена $\Phi_1(2c+1, Y)$, без ограничения общности будем считать, что ξ_i , $1 \leq i \leq \leq \deg_Y f_1$ являются корнями многочлена $f_1(2c+1, Y)$. Обозначим через $\tilde{G}_2$ подгруппу в $\tilde{G}_1$, состоящую из всех элементов σ , таких, что $\sigma(\eta) = \eta$.

Л е м м а 3.2. Группа $\tilde{G}_2$ совпадает с группой Галуа поля разложения $\tilde{E}_1$ многочлена $\Phi(x, Y)$ над $\overline{k(t_1, \dots, t_n)}(x)$. Всякий элемент $\sigma \in \tilde{G}_2$ переводит множество $\{1, 2, \dots, \deg_Y f_1\}$ в себя, и, следовательно, определен гомоморфизм из $\tilde{G}_2$ в симметрическую группу степени $\deg_Y f_1$ по формуле $\sigma \rightarrow \sigma|_{\{1, \dots, \deg_Y f_1\}}$ (здесь вертикальная черта означает ограничение подстановки на подмножество индексов). Образ $\tilde{G}$ группы $\tilde{G}_2$ при этом гомоморфизме совпадает с группой Галуа поля разложения $\tilde{E}$ многочлена $f \in \overline{k(t_1, \dots, t_n)}(t_{n+1}, \eta)[Y]$ над полем $\overline{k(t_1, \dots, t_n)}(t_{n+1}, \eta)$.

Д о к а з а т е л ь с т в о. Первое утверждение леммы следует из основной теоремы теории Галуа [2]. Рассмотрим далее коммутативную диаграмму вложений полей:

$$\begin{array}{ccc} \overline{k(t_1, \dots, t_n)}(t_{n+1}) & \subset & \overline{k(t_1, \dots, t_n)}(t_{n+1})[\xi], \\ \cap & & \cap \\ \overline{k(t_1, \dots, t_n)}(t_{n+1}, \eta) & \subset & \overline{k(t_1, \dots, t_n)}(t_{n+1}, \eta)[\xi] \subset \tilde{E} \subset \tilde{E}_1. \end{array}$$

Этой диаграмме изоморфна аналогичная диаграмма, в которой $t_1, \dots, t_n, \eta, t_{n+1}$ заменены соответственно на $\alpha_1, \dots, \alpha_n, \bar{a}, x$; ξ — на некоторый корень y_j многочлена $f_1(x, Y)$; $\tilde{E}$ и $\tilde{E}_1$ — на поля разложения F и F_1 многочленов f_1 и Φ_1 над $\overline{k(\alpha_1, \dots, \alpha_n)}(x, \bar{a})$ и $\overline{k(\alpha_1, \dots, \alpha_n)}(x)$ соответственно. Поле F_1 порождается над $\overline{k(\alpha_1, \dots, \alpha_n)}(x)$ функциями y_i , $1 \leq i \leq \deg_Y \Phi_1$, и элемент $\sigma \in \tilde{G}_1$ действует по правилу $\sigma(y_i) = y_{\sigma(i)}$ или $\sigma(\xi_i) = \xi_{\sigma(i)}$, где значение $\xi_i = y_i(2c+1)$ полностью определяет функцию y_i .

Группа $\tilde{G}_2 = \{\sigma \in \tilde{G}_1 : \sigma \bar{a} = \bar{a}\}$ отождествляется с группой Галуа поля F над $\overline{k(\alpha_1, \dots, \alpha_n)}(x, \bar{a})$. Всякий элемент $\sigma \in \tilde{G}_2$ оставляет инвариантными коэффициенты многочлена $f_1(x, Y)$ и, следовательно, переводит множество корней этого многочлена в себя, т. е. $\sigma(\{1, 2, \dots, \deg_Y f_1\}) = \{1, 2, \dots, \deg_Y f_1\}$. Последнее утверждение леммы следует из того, что группы Галуа расширений $\tilde{E} \supset \overline{k(t_1, \dots, t_n)}(t_{n+1}, \eta)$ и $F \supset \overline{k(\alpha_1, \dots, \alpha_n)}(x, \bar{a})$ изоморфны, а также из того, что всякий элемент $\sigma \in \tilde{G}_2$ индуцирует автоморфизм $F \rightarrow F$ над $\overline{k(\alpha_1, \dots, \alpha_n)}(x, \bar{a})$, который задается ограничением $\sigma|_{\{1, \dots, \deg_Y f_1\}}$, и, наоборот, всякий ав-

гоморфизм $F \rightarrow F$ над $\bar{k}(\alpha_1, \dots, \alpha_n)(x, \bar{a})$ может быть продолжен до автоморфизма $F_1 \rightarrow F_1$ над $\bar{k}(\alpha_1, \dots, \alpha_n)(x, \bar{a})$.

В силу леммы 3.2 теперь достаточно построить систему образующих группы $\tilde{G}_2$, и после этого, взяв их ограничения на множество $\{1, 2, \dots, \deg_X f_1\}$, получим систему образующих искомой группы $\tilde{G}$.

Л е м м а 3.3. Для элемента $\sigma \in \tilde{G}_1$ условие, что $\sigma \in \tilde{G}_2$, можно проверить в полиномиальное от $L(f)$, $L(\Phi_1)$, $L(\Phi_2)$, $L(h)$ время.

Д о к а з а т е л ь с т в о. Элемент $\bar{a} = \eta(\alpha_1, \dots, \alpha_n, x, y_j)$ для некоторого $1 \leq j \leq \deg_X f_1$, где $\eta(t_1, \dots, t_{n+1}, \zeta)$ — выражение для η в поле $k(t_1, \dots, t_{n+1}, \zeta)$. При этом $\bar{a}_0 = \eta(\alpha_1, \dots, \alpha_n, 2c+1, \xi_j)$. Пусть $\eta(t_1, \dots, t_{n+1}, \zeta) = (1/u) \sum_i u_i \zeta^i$, где $u, u_i \in k[t_1, \dots, t_{n+1}]$ (ср. введение). Без ограничения общности будем считать, что $|u(\alpha_1, \dots, \alpha_n, 2c+1)| > 2^{-M^{\mathcal{P}}(d)}$, при необходимости изменив c , как выше, и $\alpha_1, \dots, \alpha_n$ в разд. 1, полагая там $\delta_3 = \delta_0 \delta_1 u(t_1, \dots, t_{n+1}, 2c+1)$. Равенство $\alpha = \sigma(\alpha)$ эквивалентно $\eta(\alpha_1, \dots, \alpha_n, 2c+1, \xi_j) = \eta(\alpha_1, \dots, \alpha_n, 2c+1, \xi_{\sigma(j)})$. Вычисляя значения α_0 и $\eta(\alpha_1, \dots, \alpha_n, 2c+1, \xi_i)$, $1 \leq i \leq \deg_X f_1$ с точностью ϵ_b , согласно лемме 1.3, можно найти индекс j , а затем установить, верно ли, что $\eta(\alpha_1, \dots, \alpha_n, 2c+1, \xi_j) = \eta(\alpha_1, \dots, \alpha_n, 2c+1, \xi_{\sigma(j)})$. Это завершает доказательство леммы.

Для построения группы $\tilde{G}_2$ воспользуемся теперь сифт-алгоритмом [4, 11]. Пусть задана подгруппа A симметрической группы степени v и пусть $A_i = \{\sigma \in A : \sigma(j) = j, 1 \leq j \leq i\}$ — стабилизатор элементов $1, \dots, i$ в подгруппе A . Сифт-алгоритм по заданной системе образующих группы A за полиномиальное от v и числа образующих s время строит последовательно системы представителей $\sigma_i^{(j)}$, $1 \leq i \leq \kappa_j$ левых смежных классов A_j/A_{j+1} , $0 \leq j \leq v-1$. Каждый элемент $\sigma \in A$ однозначно представляется в виде $\sigma_{i_1}^{(1)} \sigma_{i_2}^{(2)} \dots \sigma_{i_{v-1}}^{(v-1)}$, и такое представление для каждого $\sigma \in A$ может быть найдено за полиномиальное от v и s время. Порядок группы A , равный $\prod_{1 \leq j \leq v} \kappa_j$, также может быть найден за полиномиальное время. Наконец, если задана подгруппа $B \subset A$, такая, что индекс $(A:B) \leq \mathcal{P}(v)$, и принадлежность $\sigma \in B$ можно распознать за время T , то, пользуясь сифт-алгоритмом, можно построить систему образующих группы B , содержащую не больше v^2 элементов за полиномиальное от v, s, T время [4, 11]. Пользуясь последним результатом, на основании леммы 3.3 найдем систему образующих группы $\tilde{G}_2$ за полиномиальное от $L(f)$, $L(\Phi_1)$, $L(\Phi_2)$, $L(h)$ время. Этим закончено описание алгоритма для вычисления группы Галуа поля разложения f над $\bar{k}(t_1, \dots, t_n)(t_{n+1}, \eta)$ при условии, что f неприводим над этим полем, а $\bar{\varphi}$ — над $\bar{k}(t_1, \dots, t_n)(t_{n+1})$.

4. Вычисление группы Галуа в общем случае основной теоремы

Сначала предположим, что многочлен f неприводим над полем Ω . Вычисление группы Галуа G поля разложения многочлена f над полем $\Omega = \overline{k(t_1, \dots, t_l)(t_{l+1}, \dots, t_{n+l}, \eta)}$ сведем к вычислению групп Галуа для нескольких случаев из разд. 3. Именно элементы $t_{l+1}, \dots, t_n$ можно заменить на линейные формы $S_{l+1}, \dots, S_n$ от $t_{l+1}, \dots, t_{n+1}$ с коэффициентами из $\mathbb{Z}$, такие, что $S_{l+1}, \dots, S_n, t_{n+1}$ линейно независимы, и вычислить группу Галуа $\tilde{G}$ поля разложения f над полем $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1}, \eta)} = \tilde{\Omega}$ согласно описанному в разд. 3 алгоритму. Всякая такая группа Галуа $\tilde{G}$ естественным образом вкладывается в G . Ниже будет показано, что можно выбрать достаточный набор семейств линейных форм $\{S_{l+1}, \dots, S_n\}$, из которых по крайней мере для одного из семейств $\{S_{l+1}, \dots, S_n\}$ группа $\tilde{G}$ будет совпадать с G , следовательно, многочлен f неприводим над $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1}, \eta)}$ и многочлен $\tilde{f}$ неприводим над полем $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1})}$. Вычислив, согласно описанному выше алгоритму, все группы $\tilde{G}$, соответствующие тем семействам $\{S_{l+1}, \dots, S_n\}$, для которых f и $\tilde{f}$ неприводимы соответственно над $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1}, \eta)}$ и $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1})}$, а затем, вычислив порядки $\tilde{G}$ с помощью сифт-алгоритма, найдем группу $\tilde{G}$ наибольшего порядка, которая будет совпадать с G .

Обозначим при фиксированных линейных формах $S_{l+1}, \dots, S_n$ поля $\overline{k(t_1, \dots, t_l)(t_{l+1}, \dots, t_{n+1})} = \Omega_1$, $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1})} = \tilde{\Omega}_1$, через E (соответственно $\tilde{E}$) — поле разложения многочлена f над полем Ω (соответственно $\tilde{\Omega}$). Аналогично через E_1 (соответственно $\tilde{E}_1$) обозначим поле разложения многочлена $Nf = \Phi$ (см. разд. 3), рассматриваемого как многочлен от Y , над полем Ω_1 (соответственно $\tilde{\Omega}_1$).

Л е м м а 4.1. Предположим что группы Галуа G_1 и $\tilde{G}_1$ расширений соответственно $E_1 \supset \Omega_1$ и $\tilde{E}_1 \supset \tilde{\Omega}_1$ совпадают. Тогда совпадают также группы Галуа G и $\tilde{G}$ расширений $E \supset \Omega$ и $\tilde{E} \supset \tilde{\Omega}$ соответственно и, кроме того, многочлен $\tilde{f}$ неприводим над полем $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1})}$.

Д о к а з а т е л ь с т в о. Поля $\tilde{E}$, $\tilde{\Omega}$, $\tilde{E}_1$, $\tilde{\Omega}_1$, $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)(t_{n+1})}$ получаются взятием композита с полем $\overline{k(t_1, \dots, t_l, S_{l+1}, \dots, S_n)}$ полей E , Ω , E_1 , Ω_1 , $\overline{k(t_1, \dots, t_l)(t_{l+1}, \dots, t_{n+1})}$ соответственно, поэтому лемма следует непосредственно из теории Галуа [2].

Предположим теперь, что для фиксированного набора линейных форм $S_{l+1}, \dots, S_n$ группы Галуа G_1 и $\tilde{G}_1$ из формулировки леммы 4.1 не совпадают. Это означает, что существует некоторый

элемент $\omega \in (E_1 \cap \overline{K_0(S_{l+1}, \dots, S_n)}) \setminus \overline{K_0(t_{l+1}, \dots, t_{n+1})}$ (напомним, что $\overline{K_0} = \overline{k(t_1, \dots, t_l)}$). Домножив при необходимости ω на подходящий ненулевой элемент из $\overline{K_0}[S_{l+1}, \dots, S_n]$, будем считать в дальнейшем, что ω — целый элемент над $\overline{K_0}[S_{l+1}, \dots, S_n]$ (см. [8]). Обозначив через B (соответственно B_1) целое замыкание кольца $\overline{K_0}[t_{l+1}, \dots, t_{n+1}, \zeta]$ (соответственно $\overline{K_0}[S_{l+1}, \dots, S_n, \omega]$) в поле E_1 (соответственно в поле частных кольца $\overline{K_0}[S_{l+1}, \dots, S_n, \omega]$), положим $B_2 = \overline{K_0}[t_{l+1}, \dots, t_{n+1}, \zeta]$. Обозначим через V, V_1, V_2 аффинные многообразия, определенные над полем $\overline{K_0}$, кольца регулярных функций на которых совпадают соответственно с B, B_1, B_2 , и пусть $\rho: V \rightarrow \mathbf{A}^{n-l+1}(\overline{K_0})$, $\rho_2: V_2 \rightarrow \mathbf{A}^{n-l+1}(\overline{K_0})$ и $\rho_1: V_1 \rightarrow \mathbf{A}^{n-l}(\overline{K_0})$ — морфизмы аффинных многообразий, двойственные вложениям $\overline{K_0}$ -алгебр $\overline{K_0}[S_{l+1}, \dots, S_n, t_{n+1}] \subset B$, $\overline{K_0}[S_{l+1}, \dots, S_n, t_{n+1}] \subset B_2$, $\overline{K_0}(S_{l+1}, \dots, S_n) \subset B_1$. Обозначим через μ, μ_1, μ_2 степени расширений полей рациональных функций $[\overline{K_0}(V): \overline{K_0}(t_{l+1}, \dots, t_{n+1})]$, $[\overline{K_0}(V_1): \overline{K_0}(S_{l+1}, \dots, S_n)]$, $[\overline{K_0}(V_2): \overline{K_0}(t_{l+1}, \dots, t_{n+1})]$ соответственно и через W, W_1, W_2 — подмножества в $\mathbf{A}^{n-l+1}(\overline{K_0})$, $\mathbf{A}^{n-l}(\overline{K_0})$, $\mathbf{A}^{n-l+1}(\overline{K_0})$ соответственно, такие, что для всякой точки ω из W, W_1, W_2 соответственно число элементов прообраза $\rho^{-1}(\omega)$, $\rho_1^{-1}(\omega)$, $\rho_2^{-1}(\omega)$ меньше соответственно μ, μ_1, μ_2 .

В следующей лемме утверждения, касающиеся W_1 , справедливы в предположении, что $G_1 \neq \tilde{G}_1$ (чтобы W_1 было определено), а утверждения о W и W_2 — без этого предположения.

Л е м м а 4.2.

(i) W, W_1, W_2 — замкнутые в топологии Зарисского подмножества $\mathbf{A}^{n-l+1}(\overline{K_0})$, $\mathbf{A}^{n-l}(\overline{K_0})$, $\mathbf{A}^{n-l+1}(\overline{K_0})$ соответственно;

(ii) $W \subset W_2$;

(iii) $W \supset W_1 \times \mathbf{A}^1(\overline{K_0})$, если отождествить $\mathbf{A}^{n-l}(\overline{K_0}) \times \mathbf{A}^1(\overline{K_0}) = \mathbf{A}^{n-l+1}(\overline{K_0})$ при помощи изоморфизма колец $\overline{K_0}[S_{l+1}, \dots, S_n] \otimes \overline{K_0} K_0[t_{n+1}] = \overline{K_0}[S_{l+1}, \dots, S_n, t_{n+1}]$;

(iv) размерность W_1 равна $n - l - 1$ и, следовательно, размерность W равна $n - l$.

Д о к а з а т е л ь с т в о. (i) Морфизмы ρ, ρ_1, ρ_2 являются конечными, а многообразия $\mathbf{A}^{n-l+1}(\overline{K_0})$, $\mathbf{A}^{n-l}(\overline{K_0})$ — нормальными. Утверждение п. (i) следует, например, из [8, гл. 2, § 5].

(ii) Пусть число элементов $\rho_2^{-1}(\omega)$ равно μ_2 , т. е. $\omega \notin W_2$. Обозначим через $\tau: B \rightarrow \overline{K_0}$ некоторое продолжение гомоморфизма $\overline{K_0}[S_{l+1}, \dots, S_n, t_{n+1}, \zeta] \rightarrow \overline{K_0}$, соответствующего точке ω . Образы при гомоморфизме τ элементов $\sigma(\zeta)$, $\sigma \in G_1$ попарно различны. Следовательно, все гомоморфизмы $\tau \circ \sigma$, $\sigma \in G_1$ также попарно различны. Это означает, что $\rho^{-1}(\omega)$ состоит из $\text{card } G_1 = \mu$ элементов, т. е. $\omega \notin W$, что и доказывает утверждение п. (ii).

(iii) Имеем следующие включения колец $\bar{K}_0 [S_{l+1}, \dots, S_n, t_{n+1}] \subset B_1 [t_{n+1}] \subset B$. Следовательно, морфизм ρ можно разложить в композицию морфизмов $V_1 \xrightarrow{\rho_2} V_1 \times A^1(\bar{K}_0) \xrightarrow{\rho_2 \times \text{id}} \xrightarrow{\rho_2 \times \text{id}} A^{n-l}(\bar{K}_0) \times A^1(\bar{K}_0) = A^{n-l+1}(\bar{K}_0)$ (здесь ρ_3 — обозначение первого морфизма, а второй — совпадает с $\rho_2 \times \text{id}$, где id — тождественное отображение $A^1(\bar{K}_0)$). Многообразие $V_1 \times A^1(\bar{K}_0)$ — нормальное, следовательно, $\text{card } \rho_3^{-1}(v) \leq [\bar{K}_0(V) : \bar{K}_0(V_1 \times A^1(\bar{K}_0))] = \mu_3$ (здесь μ_3 обозначает степень) для всякой точки $v \in V_1 \times A^1(\bar{K}_0)$ согласно [8, гл. 2, § 5]. Поэтому если $\omega \in W_2$, то $\text{card } \rho^{-1}(\omega) \leq \mu_3 \text{card } \rho_2^{-1}(\omega) < \mu_3 \mu_2 = \mu$, что и доказывает утверждение п. (iii).

(iv) Рассмотрим некоторое вложение полей $\bar{K}_0 \rightarrow \mathbb{C}$ и многообразия $V_1(\mathbb{C})$, $W_1(\mathbb{C})$, определенные над $\mathbb{C}$ и получающиеся из V_1 , W_1 при помощи расширения основного поля $\bar{K}_0$ до $\mathbb{C}$ [8, гл. 5]; пусть далее $\rho_1(\mathbb{C}) : V_1(\mathbb{C}) \rightarrow A^{n-l}(\mathbb{C})$ — морфизм, получающийся из ρ_1 расширением поля $\bar{K}_0$ до $\mathbb{C}$. Достаточно доказать, что $\dim W_1(\mathbb{C}) = n - l - 1$.

Множество $W_1(\mathbb{C})$ есть множество точек $\omega \in A^{n-l}(\mathbb{C})$, таких, что $\text{card } \rho_1(\mathbb{C})^{-1}(\omega) < \mu_1$. Следовательно, $\rho_1(\mathbb{C}) : V_1(\mathbb{C}) \setminus (\rho_1(\mathbb{C})^{-1}(W_1(\mathbb{C}))) \rightarrow A^{n-l}(\mathbb{C}) \setminus W_1(\mathbb{C})$ — накрытие в классической топологии [8, гл. 2, § 5]. Поскольку покрываемое пространство связно [8, гл. 8] и степень накрытия $\mu_1 > 1$ (поскольку $\omega \notin \bar{K}_0 [S_{l+1}, \dots, S_n]$), то база накрытия $A^{n-l}(\mathbb{C}) \setminus W_1(\mathbb{C})$ не является односвязной. Это возможно только в том случае, если $\dim W_1(\mathbb{C}) = n - l - 1$ (см. [8]), что завершает доказательство леммы.

Множество W_2 совпадает с множеством нулей дискриминанта $\text{Res}_Y(\Phi, \partial\Phi/\partial Y) \in \bar{K}_0 [t_{l+1}, \dots, t_{n+1}]$, поскольку старший коэффициент $\text{lc}_Y \Phi = 1$. Степени $\deg_{t_i} \text{Res}_Y(\Phi, \partial\Phi/\partial Y)$ для всех $l+1 \leq i \leq n+1$ ограничены сверху $d_2 P_{12}(dd_1 d_3)$ согласно леммам 1.1, 1.2. Следовательно, множество W_2 , а также и W , по лемме 2.6 (ii), имеет не более $d_2 P_{12}(dd_1 d_3)$ неприводимых компонент размерности $n - l$. Определим теперь $\{S_{l+1}^{(j)}, \dots, S_n^{(j)}\}$, $1 \leq j \leq (n - l) d_2 P_{12}(dd_1 d_3) + 1$ как базис пространства $\mathcal{L}_j$ линейных форм S от $t_{l+1}, \dots, t_{n+1}$, таких, что $S(1, j, j^2, \dots, j^{n-l}) = 0$, более точно, возьмем $S_{l+i}^{(j)} = j^i t_{l+1} - t_{l+i+1}$, $1 \leq i \leq n - l$. Обозначим через $\bar{K}_0[\mathcal{L}_j]$ алгебру полиномиальных функций с коэффициентами из $\bar{K}_0$ от линейных форм из пространства $\mathcal{L}_j$.

Предположим теперь, что $G_1 \neq \tilde{G}_1$ для каждого семейства линейных форм $\{S_{l+1}^{(j)}, \dots, S_n^{(j)}\}$, $1 \leq j \leq (n - l) d_2 P_{12}(dd_1 d_3) + 1$. Согласно лемме 4.2 (iii), (iv), для каждого j существует отличный от константы из $\bar{K}_0$ неприводимый многочлен $\Psi_j \in \bar{K}_0[\mathcal{L}_j]$, множество нулей которого содержится в W . Далее, из установ-

ленной только что оценки на число неприводимых компонент размерности $n - l$ в W следует, что существуют различные индексы $1 \leq j_0 < \dots < j_{n-l} \leq (n - l) d_2 P_{12} (dd_1 d_3) + 1$ и отличный от константы из $\bar{K}_0$ неприводимый многочлен $\Psi \in \bar{K}_0 [\mathcal{L}_{j_0}] \cap \dots \cap \bar{K}_0 [\mathcal{L}_{j_{n-l}}]$, множество нулей которого содержится в W . Но, с другой стороны, $\bar{K}_0 [\mathcal{L}_{j_0}] \cap \dots \cap \bar{K}_0 [\mathcal{L}_{j_{n-l}}] = \bar{K}_0 [\mathcal{L}_{j_0} \cap \dots \cap \mathcal{L}_{j_{n-l}}] = \bar{K}_0 [\{0\}] = \bar{K}_0$. Первое из этих равенств следует из общего факта, что пересечение двух алгебр полиномиальных функций на пространствах линейных форм совпадает с алгеброй полиномиальных функций на пересечении пространств, второе равенство справедливо в силу выбора $\mathcal{L}_j$, поскольку определитель Вандермонда $\det (j_{\beta}^{\gamma})_{0 \leq \gamma, \beta \leq n-l} \neq 0$. В результате получено противоречие $\Psi \in \bar{K}_0$. Следовательно, по крайней мере для одного из наборов $\{S_{i+1}^{(j)}, \dots, S_n^{(j)}\}$ группа $G_1 = \bar{G}_1$, и тогда, по лемме 4.1, группа $G = \bar{G}$ и многочлен $\bar{f}$ неприводим над $\bar{k}(t_1, \dots, t_l, S_{i+1}^{(j)}, \dots, S_n^{(j)}(t_{n+1}))$. Таким образом, построен искомый набор семейств $\{S_{i+1}^{(j)}, \dots, S_n^{(j)}\}$, $1 \leq j \leq (n - l) d_2 P_{12} (dd_1 d_3) + 1$ и тем самым завершено доказательство основной теоремы из введения для случая, когда многочлен f неприводим.

Рассмотрим наконец общий случай, когда многочлен f может быть приводимым. Разложив f на неприводимые множители $f = \prod_i f_i$, $\text{lc}_Y f_i = 1$ над полем K , согласно [7, гл. 1, § 3], без ограничения общности будем считать, что f не содержит кратных множителей, т. е. все f попарно различны. Далее, каждый из многочленов f_i разложим на неприводимые множители над полем Ω согласно описанной выше конструкции $f_i = \prod f_{im}$, $\text{lc}_Y f_{im} = 1$. Обозначим через $\varphi^{(im)}, y_s^{(im)}, G^{(im)}, G_1^{(im)}, \tilde{G}^{(im)}, \tilde{G}_1^{(im)}, \tilde{G}_2^{(im)}, E^{(im)}, W^{(im)}$ и т. п. объекты, соответствующие многочлену f_{im} и аналогичные объектам $\varphi, y_s, G, G_1, \tilde{G}, \tilde{G}_1, \tilde{G}_2, E, W$ и т. п., соответствующим f (эти объекты могут зависеть также от j , если рассматривается семейство $\{S_{i+1}^{(j)}, \dots, S_n^{(j)}\}$). Через $\varphi_4^{(i)} \in k(t_1, \dots, t_l) [\eta_3] [Z]$ обозначим многочлен, корни которого $\eta_4^{(im)}$ обладают тем свойством, что поле $k(t_1, \dots, t_{n+1}) [\eta, \eta_4^{(im)}]$ совпадает с полем, порожденным коэффициентами многочлена $f_{im} \in k(t_1, \dots, t_{n+1}) [Y]$ над $K = k(t_1, \dots, t_{n+1}) [\eta]$ (многочлен $\varphi_4^{(i)}$ аналогичен φ_4 , см. выше). Как и раньше, можно считать, что корень $\zeta^{(im)}$ многочлена f_{im} является примитивным для расширения $k(t_1, \dots, t_{n+1}, \eta_4^{(im)}, \eta_3, \eta, \zeta^{(im)}) \supset k(t_1, \dots, t_{n+1}, \eta_4^{(im)})$ для всех i, m и что построены выражения элементов η, η_3 в поле $k(t_1, \dots, t_{n+1}) \times [\eta_4^{(im)}, \zeta^{(im)}]$.

Подобно тому, как это было показано для неприводимого многочлена f , доказываем, что число неприводимых компонент

размерности $n - l$ в многообразии $\bigcup_{i, m} W^{(im)}$ не превосходит $d_2 P_{12} (dd_1 d_3)$. Далее доказывается, как и выше, что предположение о том, что для каждого семейства линейных форм $\{S_{l+1}^{(j)}, \dots, S_n^{(j)}\}$, $1 \leq j \leq (n - l) d_2 P_{12} (dd_1 d_3) + 1$ существуют i, m , такие, что $G_1^{(im)} \neq \tilde{G}_1^{(im)}$, приводит к противоречию. Следовательно, по крайней мере для одного из таких семейств выполнено $G_1^{(im)} = \tilde{G}_1^{(im)}$ для всех i, m . Тогда, по лемме 4.1, справедливо $G^{(im)} = \tilde{G}^{(im)}$ и многочлены $\bar{\Phi}^{(im)}$ неприводимы над полем $\bar{k}(t_1, \dots, t_l, S_{l+1}^{(j)}, \dots, S_n^{(j)})$ (t_{n+1}). Кроме того, это семейство $\{S_{l+1}^{(j)}, \dots, S_n^{(j)}\}$ характеризуется тем свойством, что $\prod_{i, m} \text{card}(\tilde{G}_1^{(im)})$ для него максимально. Следовательно, это семейство можно найти за полиномиальное время.

Пусть обозначения $G, G_1, \tilde{G}, \tilde{G}_1, E, E_1, \tilde{E}, \tilde{E}_1, F, F_1, \bar{a}, D, \Delta$ сохраняют тот же смысл, что и раньше (здесь многочлены f и Φ могут быть приводимыми).

Л е м м а 4.3. Если при фиксированном семействе $\{S_{l+1}^{(j)}, \dots, S_n^{(j)}\}$ группы $G_1^{(im)} = \tilde{G}_1^{(im)}$ для всех i, m , то группы $G_1 = \tilde{G}_1$ и $G = \tilde{G}$.

Д о к а з а т е л ь с т в о. Лемма доказывается индукцией по числу пар индексов i, m из следующего общего факта. Пусть $H_0 \subset H_1$ и $H_0 \subset H_2$ — расширения Галуа и $H_0 \subset H$ — расширение полей, такие, что для групп Галуа справедливы равенства $\text{Gal}(H_1/H_0) = \text{Gal}(HH_1/H)$ и $\text{Gal}(H_2/H_0) = \text{Gal}(HH_2/H)$ (здесь HH_1 и HH_2 — композиты полей). Тогда $\text{Gal}(H_1H_2/H_0) = \text{Gal}(HH_1H_2/H)$. Это утверждение является непосредственным следствием теории Галуа. Лемма доказана.

Построим и зафиксируем теперь некоторый гомоморфизм полей $k(t_1, \dots, t_{n+1}, \eta_3, \{\eta_4^{(im)}\}_{i, m}, \eta) \rightarrow k(\alpha_1, \dots, \alpha_n)(x, \bar{a})$, при котором $t_i \mapsto \alpha_i$, $1 \leq i \leq l$; $t_{n+1} \mapsto x$; $S_l^{(i)} \mapsto \alpha_i$, $l + 1 \leq i \leq n$; $\eta_3 \mapsto \alpha$; $\eta \mapsto \bar{a}$ (ср. разд. 1, 3); $\eta_4^{(im)} \mapsto \alpha^{(im)}$ для всех i, m . Обозначим $D^{(im)} = D^{(im)}(X) = \text{Res}_Y(\Phi_1^{(im)}(X, Y), ((\partial \Phi_1^{(im)} / \partial Y)(X, Y)))$ — дискриминант относительно Y многочлена $\Phi_1^{(im)}$, и пусть $x_s^{(im)}$, $1 \leq s \leq \deg_x D^{(im)}$ — все корни многочлена $D^{(im)}$. Согласно изложенному алгоритму, каждая образующая группы $\tilde{G}_1^{(im)}$ соответствует некоторому корню $x_s^{(im)}$. Обозначим эту образующую через $\sigma_s^{(im)}$.

Л е м м а 4.4. (i) Группа $\tilde{G}_1$ совпадает с подгруппой декартова произведения $\prod_{i, m} \tilde{G}_1^{(im)}$, порожденной системой образующих $\{(\sigma^{(im)})_{i, m} \in \prod_{i, m} \tilde{G}_1^{(im)} : \exists z \in \mathbb{C} (\sigma^{(im)} \neq 1 \Rightarrow \exists s (\sigma^{(im)} = \sigma_s^{(im)} \& x_s^{(im)} = z))\}$.

(ii) Группа $\tilde{G}_2$ совпадает с подгруппой в $\tilde{G}_1$, состоящей из таких элементов $\sigma = (\sigma^{(im)})_{i,m}$, что $\sigma^{(im)}(\bar{a}) = \bar{a}$ для всех индексов i, m . Кроме того, $\tilde{G}_2 \subset \prod_{i,m} \tilde{G}_2^{(im)}$.

(iii) Группа $\tilde{G}$ совпадает с образом группы $\tilde{G}_2$ при естественном гомоморфизме $\prod_{i,m} \tilde{G}_2^{(im)} \rightarrow \prod_{i,m} \tilde{G}^{(im)}$, индуцированном описанными выше гомоморфизмами ограничения подстановок на подмножество индексов $\tilde{G}_2^{(im)} \rightarrow \tilde{G}^{(im)}$.

Доказательство. (i) Каждый элемент $\sigma \in \tilde{G}_1$ определяет перестановку корней многочлена $\Phi_1^{(im)}$ для всех i, m и, следовательно, некоторый элемент $(\sigma^{(im)})_{i,m} \in \prod_{i,m} \tilde{G}_1^{(im)}$. Таким

образом, определено вложение $\tilde{G}_1 \rightarrow \prod_{i,m} \tilde{G}_1^{(im)}$. Множество точек

ветвления расширения $F_1 \supset \overline{k(\alpha_1, \dots, \alpha_n)}(x)$ содержится в множестве точек $\{x_s^{(im)}\}_{s,i,m}$. Это вытекает из того, что множество точек ветвления композита расширений совпадает с объединением множества точек ветвления этих расширений; поле F_1 есть композит полей $\overline{k(\alpha_1, \dots, \alpha_n)}(x, y_r^{(im)})$ для всех r, i, m ; и множество точек ветвления расширения $\overline{k(\alpha_1, \dots, \alpha_n)}(x, y_r^{(im)}) \supset \overline{k(\alpha_1, \dots, \alpha_n)}(x)$ содержится в множестве $\{x_s^{(im)}\}$ $1 \leq s \leq \deg_x D^{(im)}$.

Пусть ζ_0 — примитивный элемент для расширения $F_1 \supset \overline{k(\alpha_1, \dots, \alpha_n)}(x)$. Группу Галуа поля $F_1 = \overline{k(\alpha_1, \dots, \alpha_n)}(x, \zeta_0)$ над $\overline{k(\alpha_1, \dots, \alpha_n)}(x)$ можно построить (однако, может быть, не за полиномиальное время), применяя алгоритм из разд. 1—3 к этому расширению полей. Согласно замечанию 2 из разд. 2, в качестве вершин триангуляции в $\mathbb{P}^1(\mathbb{C})$ можно взять вместо точек x_m точки $x_s^{(im)}$ для всех s, i, m . При аналитическом продолжении функции $y_r^{(im)}$ вдоль пути, обходящего вершину триангуляции z , получаем функцию $\sigma(y_r^{(im)})$, где образующая $\sigma \in \tilde{G}_1$ соответствует z . Но, с другой стороны, результат этого продолжения есть $\sigma_s^{(im)}(y_r^{(im)})$, если $z = x_s^{(im)}$ для некоторого s , и $y_r^{(im)}$ — в противном случае. Отсюда и вытекает утверждение п. (i).

(ii), (iii). Следуют непосредственно из теории Галуа (см. лемму 3.2).

По построению аналогично тому, как это было выше для неприводимого f , если две точки $x_s^{(im)}$ и $x_c^{(ab)}$ различны, то $|x_s^{(im)} - x_c^{(ab)}| > 2^{-M^{\mathcal{P}}(d_*)}$. Поэтому, вычислив $x_s^{(im)}$ с достаточной точностью, найдем все совпадающие среди них. Далее, применяя описанный выше алгоритм вычисления группы Галуа для неприводимого многочлена, на основании лемм 4.3 и 4.4 вычислим группу Галуа G поля разложения многочлена f в общем случае за полиномиальное от $L(f)$, $L(\varphi_1)$, $L(\varphi_2)$, $L(h)$ время.

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М., 1979.
2. Ван дер Варден Б. Л. Алгебра. М., 1976.
3. Гельфонд А. О. Трансцендентные и алгебраические числа. М., 1952.
4. Земляченко В. Н., Корнеев Н. М., Тышкевич Р. И. Проблема изоморфизма графов//Зап. науч. семин. ЛОМИ. 1982. Т. 118. С. 83—158.
5. Слисенко А. О. Сложностные задачи теории вычислений//УМН. 1981. Т. 36, № 6. С. 21—103.
6. Чеботарев Н. Г. Теория алгебраических функций. М.; Л., 1948.
7. Чистов А. Л. Алгоритм полиномиальной сложности для разложения многочленов и нахождение компонент многообразия в субэкспоненциальное время// Зап. науч. семин. ЛОМИ. 1984. Т. 137. С. 124—188.
8. Шафаревич И. Р. Основы алгебраической геометрии. М., 1972.
9. Abhyankar S. Coverings of algebraic curves//Amer. J. Math. 1957. Vol. 79, N 4. P. 825—856.
10. Analytic Computational Complexity//Ed. J. E. Trans. N. Y.: Acad. Press, 1976, p. 151—176.
11. Furst M., Hopcroft J., Luks E. Polynomial time algorithms for permutation groups//21-st Sump. Found. Comput. Sci. N. Y.; London, 1980, p. 36—41.
12. Kung H. T., Traub J. F., All algebraic functions can be computed fast//J. Assoc. Comput. Mach. 1978. Vol. 25, N 2. P. 245—260.
13. Landau S., Muller G. L. Solvability by radicals is in polynomial time//Proc. 15-th ACM Symp. Theory Comput. N. Y.; London, 1983, p. 140—151.
14. McLellan M. T. The exact solution of systems of linear equations with polynomial coefficients//J. Assoc. Comput. Mach. 1973. Vol. 20, N 4. P. 563—588.
15. Pinkert J. R. An exact method for finding the roots of a complex polynomial//ACM Trans-Math. Software. 1976. Vol. 2, N 4. P. 335—350.
16. Zassenhaus H. On the van der Varden criterion for the group of an equation//Leat. Not. Comp. Sci. 1979. Vol. 72. P. 95—107.

ОГЛАВЛЕНИЕ

<i>Баранов С. Н.</i> Реализация системы символьных вычислений МИНИСАК на языке ФОРТ	3
<i>Бельтюков А. П.</i> Машинно-независимое описание класса запросов, поддерживаемых в реальное время	16
<i>Вольперт А. Б.</i> Качественное изучение одного класса систем массового обслуживания	26
<i>Городецкий В. И., Тараканов А. О.</i> Планирование вычислений на основе вывода в атрибутных КС-грамматиках	37
<i>Евневич Е. Л.</i> Статистический метод синтеза смешанного алгоритма, оптимального по устойчивости	49
<i>Колесникова О. Н., Ляшенко Н. Н.</i> Использование и автоматический синтез дифференциальных корректоров	55
<i>Крейнович В. Я.</i> Представление знаний об измеряемых величинах: теоретико-групповой подход	64
<i>Ляшенко Н. Н.</i> Безбазисный гармонический анализ и инвариантные аппроксимации	73
<i>Ляшенко Т. В.</i> Явный метод решения интегральных уравнений с операцией переключения	88
<i>Ляшенко Н. Н., Федоров С. И.</i> Алгоритм анализа структуры групповых источников сигналов	99
<i>Нестеров В. М.</i> Об одном обобщении интервального анализа и его применении для оценки множества значений функции	109
<i>Никулин М. С.</i> К оцениванию параметра сдвига одного семейства распределений	125
<i>Никулин М. С.</i> Статистический анализ одной физической модели, используемой в спектроскопии	133
<i>Полищук В. И.</i> Биномиальная асимптотика	138
<i>Пономаренко И. Н.</i> Об импримитивности одного класса S-колец	154
<i>Соловьев С. В.</i> Об условиях полной когерентности в замкнутых категориях	163
<i>Фомин С. В.</i> Теорема двойственности для частично упорядоченных множеств: алгоритмы	190
<i>Чистов А. Л.</i> Вычисление группы Галуа над функциональным полем характеристики нуль с алгебраически замкнутым полем констант за полиномиальное время	200
Рефераты	234

РЕФЕРАТЫ

УДК 518.682

Баранов С. Н. Реализация системы символьных вычислений МИНИСАК на языке Форт//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 3—15.

Описывается подход, позволивший «втиснуть» довольно развитую систему символьных вычислений в габариты средней персональной ЭВМ. Основой реализации послужит язык Форт и автоматизированное построение синтаксического анализатора. В работе обсуждаются технологические аспекты реализации, связанные с использованием этих инструментальных средств. Библ. 5 назв.

УДК 519.5

Бельтюков А. П. Машинно-независимое описание класса запросов, поддерживаемых в реальное время//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 16—25.

В статье исследуется класс запросов к базам данных, которые могут поддерживаться определенными типами вычислительных машин в реальное (т. е. ограниченное константой) время. Число шагов работы машины между порциями информации об изменениях в базе данных также ограниченных константой. Изменения в базе имеют локальный характер, информация о них задается вектором фиксированной длины. Основным результатом работы — машинно-независимое описание класса запросов к базе данных, поддерживаемых в реальное время. Описание дается на синтаксическом уровне. Библ. 1 назв.

УДК 681.3.06: 681.518.3

Вольперт А. Б. Качественное изучение одного класса систем массового обслуживания//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 26—36.

Рассматривается класс сетей массового обслуживания с постоянными временами, в которых обслуживаются две заявки. Показано, что для сетей, в которых обслуживание производится в соответствии с дисциплиной LCFS, характерны такие свойства, как обратимость, строгая эргодичность и топологическая транзитивность, а для сетей, в которых обслуживание производится в соответствии с дисциплиной FCFS, имеет место единственная периодическая траектория. Библ. 9 назв., ил. 6.

УДК 519.5

Городецкий В. И., Тараканов А. О. Планирование вычислений на основе вывода в атрибутивных КС-грамматиках//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 37—48.

Развивается подход к построению алгоритмов планирования вычислений на основе поиска вывода в контекстно-свободных (КС) грамматиках, являющийся альтернативой традиционному подходу, базирующемуся на методах исчисления предикатов. Библ. 9 назв.

УДК 519.95 + 519.6

Евневич Е. Л. Статистический метод синтеза смешанного алгоритма, оптимального по устойчивости//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 49—54.

Описан метод автоматического анализа алгоритмов на степень неустойчивости по отношению к колебаниям входных данных. Рассматриваются вопросы синтеза оптимальных по устойчивости комбинированных алгоритмов. Библ. 1 назв., ил. 2.

УДК 621 + 519.24

Колесникова О. Н., Ляшенко Н. Н. Использование в автоматический синтез дифференциальных корректоров//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 55—63.

Описан метод автоматического синтеза фильтров с помощью дифференциальной коррекции, а также его программная реализация. Рассматриваются результаты машинных экспериментов. Библ. 1 назв., ил. 7, табл. 2.

УДК 519.7 + 512.54 + 519.2

Крейн ович В. Я. Представление знаний об измеряемых величинах: Теоретико-групповой подход//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 64—72.

В статье показано, что в условиях, когда на множестве исследуемых объектов действует некоторая группа симметрии и можно предполагать, что неизвестный критерий оптимальности инвариантен относительно ее действия, оптимальный метод представления знаний также инвариантен относительно нее. Это дает общий подход к представлению знаний в условиях априорной неопределенности, который иллюстрируется на примере выбора робастного метода в математической статистике, выбора оптимального базиса для представления функций и т. д. Библ. 10 назв.

УДК 517.5 + 519.6 + 681.3

Ляшенко Н. Н. Безбазисный гармонический анализ и инвариантные аппроксимации//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 73—87.

В работе рассматриваются алгоритмы приближения периодическими функциями, а также функциями, обладающими другими свойствами симметрии. Характерная особенность постановок основных задач состоит в отсутствии задания какого-либо базиса для параметризации аппроксимирующих классов. Библ. 2 назв.

УДК 517.94

Ляшенко Т. В. Явный метод решения интегральных уравнений с операцией переключения//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 88—98.

Нелинейные интегральные операторы с операцией переключения применимы для описания многих технических систем. В работе дана достаточно общая методика поиска аналитических решений. Приводятся явные формулы обращения для широкого класса операторов. Библ. 6 назв., ил. 4.

УДК 621.391

Ляшенко Н. Н., Федоров С. И. Алгоритмы анализа структуры групповых источников сигналов//Математические методы построения и анализа алгоритмов. Л.: Наука. 1990. С. 99—108.

В работе рассмотрены алгоритмы анализа пространственной структуры источников акустического излучения (задача счета), а также вопросы программной реализации и прикладные аспекты. Библ. 1 назв., ил. 2.

Нестеров В. М. Об одном обобщении интервального анализа и его применении для оценки множества значений функций//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 109—124.

Рассматривается задача отыскания верхней и нижней оценки множества значений функций при заданной области изменения ее аргументов. Дается краткий обзор методов решения задачи, базирующихся на применении интервального анализа. Указываются их недостатки. Предлагается обобщение интервального анализа, позволяющее работать с бесконечными интервалами. Приводятся методы оценки функции, основанные на обобщенном интервальном анализе, а также оценка их эффективности. Библ. 20 назв.

УДК 519.281

Никуллин М. С. К оценке параметра сдвига одного семейства распределений//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 125—132.

Проводится сравнение статистических оценок максимального правдоподобия Эйлера среднего арифметического для семейства распределений с параметром сдвига, рассмотренного в работе Д. Кендалла [1]. Библ. 8 назв.

УДК 519.281

Никуллин М. С. Статистический анализ одной физической модели, используемой в спектроскопии//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 133—137.

Статья посвящена задаче статистического разделения эффектов, обусловленных доплеровским, лоренцевым и аппаратным уширением спектральных линий в рамках одной физической модели спектрографа, а также построению статистического критерия для проверки согласия выбранной модели с экспериментальными данными. Библ. 3 назв.

УДК 517.9

Полещук В. И. Биномиальная асимптотика//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 138—153.

Пусть a^N и b^N — «эталонная» и «возмущенная» полугруппы степеней двух перестановочных элементов нормированного кольца (не обязательно алгебры). Предлагается необходимый и достаточный признак устойчивости, использующий лишь конечное число элементов «возмущенной» полугруппы. Из устойчивости следует асимптотическая предельность высоких степеней элемента b целочисленными линейными комбинациями мономов, содержащих начальные его степени. Приводятся асимптотические формулы с оценками граничных констант. Библ. 1 назв., нл. 3.

УДК 518.5

Пономаренко И. Н. Об импримитивности одного класса S-колец//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 154—162.

Анализ сложности алгоритмов наивной классификации для проверки изоморфизма к изученным свойствам S-колец (колец Шура). Для турниров Кэли соответствующие S-кольца обладают дополнительным свойством, отражающим отсутствие самоспаренных орбит у фиксатора группы перестановок нечетного порядка. Основной результат работы состоит в доказательстве импримитивности таких S-колец над группой $Z_{pq} \times Z_{pq}$. Библ. 9 назв.

УДК 512.58

Соловьев С. В. Об условиях полной когерентности в замкнутых категориях//Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 163—169.

В работе доказано, что все диаграммы канонических естественных преобразований в симметрической моноидальной замкнутой категории коммутативны тогда и только тогда, когда: а) для любого объекта A этой категории $[[[A, 1], 1], 1]$ канонически изоморфен $[A, 1]$; б) $f([p, 1]) \simeq g([p, 1]) \Rightarrow f(p) \simeq g(p)$ для любых двух канонических естественных преобразований f, g . Показано, что достаточным условием коммутативности всех диаграмм является каноническая изоморфность A и $[[[A, 1], 1], 1]$. Здесь $[,]$ — внутренний гом-функтор. Эти результаты дополняют известную теорему когерентности Келли — Маклейна и позволяют в ряде случаев обходиться без вычислений при проверке коммутативности диаграмм. Библ. 5 назв., нл. 1.

Фомин С. В. Теорема двойственности для частично упорядоченных множеств: алгоритмы // Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 190—199.

В работе описываются эффективные алгоритмы решения задачи о покрытии данным количеством цепей (антицепей) максимально возможного числа элементов конечного частично упорядоченного множества. Библ. 6 назв.

УДК 518.5 + 512.46

Чистов А. Л. Вычисление группы Галуа над функциональным полем характеристистики нуль с алгебраически замкнутым полем констант за полиномиальное время // Математические методы построения и анализа алгоритмов. Л.: Наука, 1990. С. 200—232.

В работе описывается алгоритм полиномиальной сложности для построения образующих группы Галуа поля разложения многочлена над функциональным полем характеристики нуль с алгебраически замкнутым полем констант. При этом группа Галуа задается как подгруппа симметричной группы перестановок корней, поле констант является алгебраическим замыканием конечно-порожденного расширения поля рациональных чисел, функциональное поле — конечно-порожденное расширение поля констант, сам многочлен имеет коэффициенты в конечно-порожденном расширении поля рациональных чисел. Библ. 16 назв.

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ
ПОСТРОЕНИЯ И АНАЛИЗА
АЛГОРИТМОВ**

*Утверждено к печати
Ленинградским институтом информатики
и автоматизации АН СССР*

*Художник И. П. Кремлев
Технический редактор Л. И. Каряева
Корректоры А. Х. Салтанова и Г. И. Суворова
ИБ № 44040*

Сдано в набор 23.10.89. Подписано к печати 22.02.90.
М-18075. Формат 60×90^{1/16}. Бумага книжно-журнальная.
Гарнитура литературная. Печать высокая.
Усл. печ. л. 15.00. Усл. кр.-отт. 15.24. Уч.-изд. л. 16.34.
Тираж 2450. Тип. зак. № 2051 Цена 2 р. 70 к.

Ордена Трудового Красного Знамени издательство «Наука»,
Ленинградское отделение.

- 199034, Ленинград, В-34, Менделеевская лин., 1.

Набрано в типографии № 6 ордена Трудового Красного Знамени издательства
«Машиностроение» при Государственном комитете СССР по печати.
193144, Ленинград, ул. Монсеенко, 10.

Ордена Трудового Красного Знамени Первая типография
издательства «Наука».

199034, Ленинград, В-34, 9 лин., 12.

**КНИГИ ИЗДАТЕЛЬСТВА «НАУКА»
МОЖНО ПРЕДВАРИТЕЛЬНО ЗАКАЗАТЬ
В МАГАЗИНАХ ЦЕНТРАЛЬНОЙ КОНТОРЫ «АКАДЕМКНИГА»,
В МЕСТНЫХ МАГАЗИНАХ КНИГОТОРГОВ
ИЛИ ПОТРЕБИТЕЛЬСКОЙ КООПЕРАЦИИ.**

*Для получения книг почтой
заказы просим направлять по адресу:*

- 117393 Москва, ул. Академика Пилюгина, 14, корп. 2, магазин «Книга — почтой» Центральной конторы «Академкнига»;
197345 Ленинград, Петрозаводская ул., 7, магазин «Книга — почтой» Северо-Западной конторы «Академкнига»

*или в ближайший магазин «Академкнига»,
имеющий отдел «Книга — почтой»:*

- 480091 Алма-Ата, ул. Фурманова, 91/97 (Книга — почтой);
370001 Баку, Коммунистическая ул., 51 («Книга — почтой»);
232600 Вильнюс, ул. Университето, 4;
690088 Владивосток, Океанский пр., 140 («Книга — почтой»);
320093 Днепропетровск, пр. Гагарина, 24 («Книга — почтой»);
734001 Душанбе, пр. Ленина, 95 («Книга — почтой»);
375002 Ереван, ул. Туманяна, 31;
664033 Иркутск, ул. Лермонтова, 289 («Книга — почтой»);
420043 Казань, ул. Достоевского, 53 («Книга — почтой»);
252030 Киев, ул. Ленина, 42;
252142 Киев, пр. Вернадского, 79;
252025 Киев, ул. Осипенко, 17;
277012 Кишинев, пр. Ленина, 148 («Книга — почтой»);
343900 Краматорск Донецкой обл., ул. Марата, 1 («Книга — почтой»);
660049 Красноярск, пр. Мира, 84;
443002 Куйбышев, пр. Ленина, 2 («Книга — почтой»);
191104 Ленинград, Литейный пр., 57;
199164 Ленинград, Таможенный пер., 2;

194064 Ленинград, Тихорецкий пр., 4;
220012 Минск, Ленинский пр., 72 («Книга — почтой»);
103009 Москва, ул. Горького, 19а;
117312 Москва, ул. Вавилова, 55/7;
630076 Новосибирск, Красный пр., 51;
630090 Новосибирск, Морской пр., 22 («Книга — почтой»);
142284 Протвино Московской обл., ул. Победы, 8;
142292 Пущино Московской обл., МР «В», 1 («Книга — почтой»);
620151 Свердловск, ул. Мамина-Сибиряка, 137 («Книга — почтой»);
700000 Ташкент, ул. Ю. Фучика, 1;
700029 Ташкент, ул. Ленина, 73;
700070 Ташкент, ул. Шота Руставели, 43;
700185 Ташкент, ул. Дружбы народов, 6 («Книга — почтой»);
634050 Томск, наб. реки Ушайки, 18;
450059 Уфа, ул. Р. Зорге, 10 («Книга — почтой»);
450025 Уфа, ул. Коммунистическая, 49;
720001 Фрунзе, бульв. Дзержинского, 42 («Книга — почтой»);
310078 Харьков, ул. Чернышевского, 87 («Книга — почтой»).