МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 510.67

Дудаков Сергей Михайлович

Выразительная сила языков первого порядка для конечных алгебраических систем над бесконечными универсумами

Автореферат
диссертации на соискание учёной степени
доктора физико-математических наук.

01.01.06 — математическая логика, алгебра и теория чисел

Москва — 2007

Диссертация выполнена на кафедре информатики Тверского государственного университета.

Научный консультант:

доктор физико-математических наук, профессор М.А.Тайцлин

Официальные оппоненты:

доктор физико-математических наук, профессор А.Л.Семёнов
доктор физико-математических наук, профессор А.В.Чагров
доктор физико-математических наук, профессор В.Г.Дурнев

Ведущая организация:

Санкт-Петербургское Отделение Математического Института
им.В.А.Стеклова РАН

Защита диссертации состоится 28 сентября 2007 г. на заседании диссертационного совета Д.501.001.84 в Московском государственном университете имени М.В.Ломоносова по адресу: 119991, Российская Федерация, Москва, ГСП-1, Ленинские горы, Московский государственный университет имени М.В.Ломоносова, Механико-математический факультет, ауд.14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 28 августа 2007 г.

Ученый секретарь диссертационного совета
Д.501.001.84 при МГУ
доктор физико-математических наук,
профессор В.Н.Чубариков

Общая характеристика работы

Актуальность. В настоящее время средства и методы математической логики находят всё более широкое применение при проектировании и анализе программного обеспечения ЭВМ. Одним из наиболее тесно связанных с информатикой разделом математической логики является теория языков первого порядка. Особенно интенсивно развивается теория языков для конечных алгебраических систем. Это обусловлено тем, что такие языки широко используются в системах управления базами данных, где служат средством извлечения информации из баз данных. Сейчас типичной моделью базы данных является предложенная Э.Коддом реляционная модель, в которой база данных мыслится как собрание конечного числа конечных таблиц[1]. Таким образом, состояние базы данных является конечной алгебраической системой некоторой фиксированной сигнатуры, которая называется *сигнатурой базы данных*. Мы будем называть эти алгебраические системы *состояниями*. В качестве языка запросов, с помощью которого происходит извлечение информации, используются различные стилизации языка логики предикатов первого порядка.

Хорошо известно, что не всякое свойство алгебраических систем может быть выражено формулами первого порядка. Например, если сигнатура базы данных содержит только один одноместный предикатный символ P, то невозможно записать в этой сигнатуре формулу первого порядка, выделяющую среди состояний в точности те, в которых количество элементов P является чётным. Другой пример: для двухместного предиката E, задающего граф, невозможно написать формулу, которая будет истинной тогда и только тогда, когда этот граф является связным[2].

Обычно, элементы состояний выбираются из фиксированного множества, называемого *универсумом*. Им могут быть множество натуральных чисел, множество всех слов некоторого алфавита или множество действительных чисел. Поскольку размер отношений состояния хоть и конечен, но потенциально не ограничен, то универсум должен быть бесконечным. Множество элементов универсума, которые входят в хотя бы

[1] Codd E.F. A relational model for large shared data banks. // Communications of the ACM, V.13, 1970. P.377–387.

Codd E.F. Relational completeness of data base sublanguages. // Database Systems (ed. Rustin R.), Prentice-Hall, 1972. P.33–64.

[2] Aho A.V., Ullman J.D. Universality of data retrieval languages. // Proc. of 6th Symp. on Principles of Programming Languages, 1979. P.110–120.

одно отношение состояния, называется активной областью состояния.

Так как не всякое свойство конечных алгебраических систем может быть выражено формулой языка первого порядка сигнатуры этих систем, то активно ведётся поиск методов увеличения выразительной силы. Один из путей состоит в следующем[3]. Обычно, на универсуме, элементы которого хранятся в таблицах, определены какие-либо стандартные отношения, образующие сигнатуру универсума. Для числовых множеств такими отношениями являются сложение и умножение, порядок и т.д. На множестве слов используется конкатенация и лексикографический порядок. Таким образом, универсум тоже является алгебраической системой, но, в отличие от состояния, бесконечной.

Возможно, что если при построении формул первого порядка использовать не только отношения сигнатуры базы данных, но и отношения универсума (такие формулы называются расширенными), то можно будет выразить какие-то свойства, которые невозможно выразить, используя только отношения сигнатуры базы данных (такие формулы называют ограниченными). Разумеется, для сравнения имеет смысл рассматривать только формулы, истинность которых определяется исключительно отношениями сигнатуры базы данных, а не способом связи между этими отношениями и отношениями универсума. Иначе говоря, истинность формул, которые используются для сравнения выразительной силы, не должна зависеть от способа вложения состояния в универсум, формулы должны сохранять свою истинность при произвольных изоморфизмах состояния внутри универсума. Такие формулы называются $=$-инвариантными[4]. Если для некоторого универсума любая $=$-инвариантная расширенная формула эквивалентна ограниченной, то говорят, что для универсума имеет место коллапс к равенству. Коллапс к равенству означает, что используемые в расширенных формулах отношения универсума не позволяют выразить никаких новых свойств состояния по сравнению с ограниченными формулами.

В результате возникло новое направление исследований в теории моделей — теория конечных алгебраических систем, вложенных в бесконечные.

[3]Kanellakis P., Kuper G. Revesz P. Constraint query languages. // Journal of computer and system sciences, V.51, 1995. P.26–52.

[4]Chandra A., Harel D. Computable queries for relational databases. // Journal of compuer and system sciences, V.21(2), 1980. P.156–178.

Одним из главных вопросов этого направления является задача сравнения выразительной силы ограниченных и расширенных языков.

Ю.Ш.Гуревич указал свойство состояний, которое нельзя выразить, используя только отношения сигнатуры базы данных, но можно, если добавить к ним произвольный линейный порядок. Таким образом, для любых упорядоченных универсумов не выполняется коллапс к равенству.

Естественно рассматривать следующую задачу: какие отношения можно добавить к отношению линейного порядка, чтобы ещё увеличить выразительную силу языка? Поскольку мы будем сравнивать выразительную силу расширенного языка с выразительной силой языка с порядком, то нужно рассматривать не только $=$-инвариантные формулы, но и те, истинность которых зависит от отношений сигнатуры базы данных и способа упорядочения её элементов. Такие формулы должны сохранять истинность при произвольных сохраняющих порядок изоморфизмах состояний внутри универсума. Эти формулы называют *$<$-инвариантными*[5].

Ряд универсумов обладает следующим свойством: всякая расширенная $<$-инвариантная формула эквивалентна некоторой *$<$-ограниченной* (то есть формуле с использованием отношений сигнатуры базы данных и порядка). Такое свойство универсума называют *коллапсом к порядку*[6]. Известно[6], что это верно для арифметики Пресбургера, теории действительных чисел, коммутативных групп и других теорий. С другой стороны, имеются неразрешимые теории, в которых это не выполняется, например, арифметика натуральных чисел со сложением и умножением.

Свойства коллапса могут быть выражены в виде множества формул первого порядка сигнатуры универсума. Поэтому свойствами коллапса обладают не только универсумы, но и их элементарные теории.

В связи с этими исследованиями в разных работах сформулировано много открытых вопросов, в частности:

1) возможна ли эффективная трансляция $<$-инвариантных формул в $<$-ограниченные[6]?

2) все ли разрешимые теории обладают свойством коллапса к порядку[6]?

[5] Hull R., Yap C.K. The format model, a theory of database organization. // Journal of the ACM, № 31, 1984. P.518–537.

[6] Belegradek O.V., Stolboushkin A.P., Taitslin M.A. Extended order-generic queries. // Annals of Pure and Applied Logic 97, 1999. P.85–125.

3) верно ли то же самое для обогащений арифметики Пресбургера[7]?

4) верно ли, что для коллапса к порядку необходимо наличие бесконечного множества без независимой формулы[8]?

В указанных работах предложено много достаточных условий для коллапса к порядку: отсутствие независимой формулы, первое и второе свойства изолированности, первое и второе свойства псевдоконечной однородности, сводимость и ограниченность. Однако взаимоотношения между этими свойствами оставались во многом неясными. Было установлено только, что из отсутствия независимой формулы следуют сводимость и ограниченность, из сводимости и ограниченности следует второе свойство изолированности, а из первого (второго) свойства изолированности следует первое (второе) свойство псевдоконечной однородности. Известно также, что первые свойства изолированности и псевдоконечной однородности не совпадают друг с другом. Поэтому в ([6]) также поднят вопрос о том, как соотносятся вышеперечисленные свойства между собой.

Цели работы.

1) Установить, имеет ли место коллапс к порядку в семёновских обогащениях[9] арифметики Пресбургера.

2) Установить, существуют ли разрешимые теории, в которых коллапса к порядку нет.

3) Исследовать случайный граф на предмет свойства коллапса.

4) Установить связь между сводимостью, изолированностью, псевдоконечной однородностью и коллапсом к порядку.

5) Установить, имеются ли сводимые обогащения арифметики Пресбургера с независимой формулой.

6) Разработать методы эффективной трансляции для расширенных $<$-инвариантных формул в $<$-ограниченные.

[7]Тайцлин М.А. Ограниченные псевдоконечная однородность и изолированность. // Вестник Тверского государственного университета, серия «Прикладная математика», Тверь: Тверской государственный университет, 2003. 2(1). С.5—15.

[8]Baldwin J., Benedikt M. Stability theory, permutations of indiscernibles, and embedded finite models. // AMS Trans., 352(11), 2000. С.4937–4969.

[9]Семёнов А.Л. Логические теории одноместных функций на натуральном ряде. // Изв. АН СССР, 47(3), 1983. С.623–658.

Методы исследования. В диссертации используются методы математической логики, в частности, теории моделей.

Научная новизна и основные положения, выносимые на защиту. Все полученные в работе результаты являются новыми. Наиболее существенными из них являются следующие:

1) В обогащениях Семёнова арифметики Пресбургера имеет место коллапс к порядку.

2) Коллапс к порядку имеет место в предикатных обогащениях начального фрагмента нестандартных моделей арифметики Пресбургера.

3) Среди упорядочений случайного графа существуют разрешимые.

4) Для неупорядоченного случайного графа коллапс к равенству имеет место тогда и только тогда, когда сигнатура базы данных является монадической.

5) Свойство сводимости, второе свойство псевдоконечной однородности и второе свойство изолированности эквивалентны. Каждое из них влечёт свойство коллапса к порядку.

6) Первое свойство изолированности является менее общим чем второе. Первое свойство псевдоконечной однородности является менее общим чем второе или эквивалентно ему.

7) Если теория имеет эффективно сводимые модели, то она имеет эффективно тотально сводимые модели.

8) Если теория имеет эффективно I-сводимую модель и тип неразличимого множества I рекурсивен, то возможно выполнение эффективной трансляции расширенных $<$-инвариантных формул в $<$-ограниченные.

9) Эффективная трансляция расширенных $<$-инвариантных формул в $<$-ограниченные возможна для арифметики Пресбургера, её эффективных семёновских обогащений, для теории действительных чисел.

10) Существуют разрешимые обогащения арифметики Пресбургера, в которых нет коллапса к порядку.

11) Существуют обогащения арифметики Пресбургера, в которых есть коллапс к порядку, но всякое бесконечное множество имеет независимую формулу.

Теоретическая и практическая ценность. Работа носит теоретический характер. Полученные результаты отвечают на множество открытых вопросов, опубликованных в печати. Предложенные методы уже использованы другими авторами для получения новых результатов в этой и смежных областях.

Материалы диссертации могут использоваться при чтении специальных курсов студентам, обучающимся математике и математическим основаниям информатики.

Результаты диссертации могут найти практическое применение при анализе языков запросов для систем управления базами данных.

Апробация работы. Содержание диссертации многократно излагалось на семинаре «Теоретические основы информатики», проходящем в Тверском государственном университете, семинарах МГУ по математической логике под руководством академика РАН С.И.Адяна и профессора В.А.Успенского, семинаре ПОМИ РАН по математической логике под руководством члена-корреспондента РАН Ю.В.Матиясевича. Доклад, посвящённый одному из разрабатываемых в диссертации вопросов, был сделан на международной конференции по теоретической информатике CSR-2006 [8] (Санкт-Петербург, июнь 2006) и опубликован в сборнике научных трудов «Computer Science — Theory and Applications» (Lecture Notes in Computer Science).

Публикации. Содержание диссертации опубликовано в ведущих рецензируемых журналах, рекомендованных ВАК: «Математические заметки» [1] и [4], «Известия РАН. Серия математическая» [2], «Успехи математических наук» [3], «Вестник Новгородского государственного университета» [7], «Фундаментальная и прикладная математика»[10]. Кроме того, имеются публикации в журнале «Вестник Тверского государственного университета» [5, 9] и других изданиях [6].

Список публикаций приведён в конце автореферата. Все работы, кроме [3], выполнены без соавторов. В [3] автору принадлежит последняя часть седьмого параграфа (теорема 7.5 и предшествующие определения)

[10]Дудаков С.М. Достаточные условия эффективной трансляции локально генерических запросов // Фундаментальная и прикладная математика (в печати)

и параграфы 8, 9, 10 целиком.

Структура диссертации. Диссертация содержит 176 страниц, состоит из введения, шести глав основной части, заключения, списка литературы и предметного указателя. Список литературы содержит 46 наименований.

Краткое содержание работы

В главе 1 приводятся общие определения, используемые в дальнейшем, а также основные результаты предыдущих авторов. В частности, напоминаются определения *изолированности* и *псевдоконечной однородности*.

Система $(\mathfrak{A}, I)$ обладает *первым (вторым) свойством псевдоконечной однородности*, если выполнено следующее:

1) I — неразличимая в системе $\mathfrak{A}$ (в системе $(\mathfrak{A}, I)$) последовательность;

2) для любой специальной системы $(\mathfrak{A}', I') \equiv (\mathfrak{A}, I)$, любых псевдоконечных в $\mathfrak{A}'$ (в $(\mathfrak{A}, I)$) множеств $D_1, D_2 \subseteq I'$, любых конечных множеств $E_1, E_2 \subseteq |\mathfrak{A}'|$, если существует элементарное в $\mathfrak{A}'$ (в $(\mathfrak{A}', I')$) отображение $h : D_1 \cup E_1 \to D_2 \cup E_2$, то оно может быть продолжено на любой элемент $\mathsf{x} \in |\mathfrak{A}'|$, если система $(\mathfrak{A}', D_1, D_2, h)$ (система $(\mathfrak{A}', I', D_1, D_2, h)$) является ω-насыщенной.

Теория T обладает *первым (вторым) свойством псевдоконечной однородности*, если она имеет модель $\mathfrak{A}$, в которой есть множество I такое, что $(\mathfrak{A}, I)$ обладает первым (вторым) свойством псевдоконечной однородности.

Система $(\mathfrak{A}, I)$ обладает *первым (вторым) свойством изолированности*, если выполнено следующее:

1) I — неразличимая в алгебраической системе $\mathfrak{A}$ (в системе $(\mathfrak{A}, I)$) последовательность;

2) для любой специальной алгебраической системы $(\mathfrak{A}', I') \equiv (\mathfrak{A}, I)$, любого псевдоконечного в $\mathfrak{A}'$ (в $(\mathfrak{A}', I')$) множества $D \subseteq I'$, любого конечного множества $E \subseteq |\mathfrak{A}'|$ и любого элемента $\mathsf{x} \in |\mathfrak{A}'|$ тип $\mathrm{tp}(\mathsf{x}/(D \cup E))$ изолируется в системе $\mathfrak{A}'$ (в системе $(\mathfrak{A}', I')$) типом $\mathrm{tp}(\mathsf{x}/G)$ для некоторого счётного множества $G \subseteq D \cup E$.

Последнее означает, что тип $\mathrm{tp}(\mathsf{x}/(D \cup E))$ является единственным типом в $\mathfrak{A}'$ (в $(\mathfrak{A}', I')$) над множеством $D \cup E$, который является расширением типа $\mathrm{tp}(\mathsf{x}/G)$. Теория T обладает *первым (вторым) свойством* и з о л и р о в а н н о с т и, если она имеет модель $\mathfrak{A}$, в которой есть множество I такое, что $(\mathfrak{A}, I)$ обладает первым (вторым) свойством изолированности.

В ([6,7]) показано, что из первого (второго) свойства изолированности следует первое (второе) свойство псевдоконечной однородности, из любого свойства псевдоконечной однородности следует коллапс к порядку.

Глава 2. Термально изолированные множества

Основным методом изучения свойства коллапса в данной главе являются т е р м а л ь н о и з о л и р о в а н н ы е неразличимые множества. Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ, I — неразличимое в $\mathfrak{A}$ последовательность. Пусть $\mathcal{T}$ — множество всех термов одной переменной сигнатуры Σ. Назовём множество I термально изолированным в $\mathfrak{A}$, если для любых термов $t_1(x), t_2(x) \in \mathcal{T}$ имеет место один из двух случаев:

1) существует константа $M_{t_2} \in \omega$, и для всех $\mathsf{x} \in I$ выполнено $t_2(\mathsf{x}) \leqslant \leqslant M_{t_2}$;

2) для любых элементов $\mathsf{x}, \mathsf{y} \in I$ таких, что $\mathsf{x} < \mathsf{y}$, выполнено $t_1(\mathsf{x}) < < t_2(\mathsf{y})$.

Такие множества можно построить для любых теорий, являющихся обогащениями арифметики Пресбургера (теорема 2.3):

> *Пусть $\mathfrak{L}^* = (\omega, 0, 1, \leqslant, +, \ldots)$ какое-либо обогащение арифметики Пресбургера счётной сигнатуры. Тогда существует элементарное расширение $\mathfrak{A} \succ \mathfrak{L}^*$, в котором существует неразличимое термально изолированное множество I.*

Доказывается теорема при помощи построения последовательности «всё более удовлетворяющих условию» множеств, после чего применяется стандартный способ построения неразличимых множеств с помощью теоремы компактности и теоремы Рамсея.

Важный класс разрешимых обогащений арифметики Пресбургера найден А.Л.Семёновым ([9]). Одноместная функция f на множестве натуральных чисел называется с о г л а с о в а н н о й с о с л о ж е н и е м, если она удовлетворяет следующим условиям:

1) для любого натурального $\mathfrak{n}$ значение $f(x)$ периодично по модулю $\mathfrak{n}$ для всех x, начиная с некоторого;

2) для всякой неограниченной конечной суммы

$$S(x) = \sum_i \mathfrak{a}_i f(x + \mathfrak{b}_i)$$

существует такое $\mathfrak{s}'_S \in \omega$, что либо $S(x + \mathfrak{s}'_S) > f(x)$ для всех $x \in \omega$, либо $S(x + \mathfrak{s}'_S) < -f(x)$ для всех $x \in \omega$;

3) f строго возрастает.

Алгебраическая система $\mathfrak{L}_{SF} = (\omega, 0, 1, \leqslant, +, f)$, где функция f согласована со сложением, называется арифметикой Семёнова.

Для систем $\mathfrak{L}_{SF}$ доказывается теорема 2.4:

Пусть $\mathfrak{A}'$ — специальная модель $\mathrm{Th}(\mathfrak{L}_{SF})$, $I' \subseteq \mathfrak{A}'$ — неразличимая термально изолированная в $\mathfrak{A}'$ последовательность, $D \subseteq I'$ — псевдоконечное множество в $\mathfrak{A}'$, и $E \subseteq |\mathfrak{A}'|$ — конечное множество, $\mathsf{x} \in \mathfrak{A}'$. Тогда тип $\mathrm{tp}(\mathsf{x}/F)$, где $F = D \cup E$, изолируется типом $\mathrm{tp}(\mathsf{x}/G)$ для некоторого счётного $G \subseteq F$.

В доказательстве термальная изолированность используется при построении G. Далее используется результат А.Л.Семёнова о приведении любой формулы к экзистенциальному виду. После показывается, что любая истинная формула следует из бескванторной формулы с константами из G.

Как следствие получается теорема 2.5:

Теория системы $\mathfrak{L}_{SF}$ обладает свойством коллапса к порядку.

Другой пример использования термально изолированных множеств — предикатные обогащения нестандартных моделей арифметики Пресбургера.

Пусть теория $T = \mathrm{Th}(\omega, 0, 1, \leqslant, +, (P_i)_i)$, где P_i — произвольные предикаты, допускает элиминацию кванторов. Пусть $\mathfrak{A} \succ (\omega, 0, 1, \leqslant, +)$ — элементарное строгое расширение арифметики Пресбургера. Изучается теория $T' = \mathrm{Th}(\mathfrak{A}, (P_i)_i)$. Отмечается следующее свойство (лемма 2.6):

Теория T' допускает элиминацию кванторов.

Доказательство использует элиминацию кванторов в исходной теории T.

Доказывается, что элементы термально изолированного неразличимого множества ведут себя как линейно независимые элементы над полем рациональных чисел (лемма 2.7), и, используя это, получается теорема 2.8:

Пусть $\mathfrak{B}$ — произвольная модель T'. Пусть I — произвольное термально изолированное неразличимое множество в $\mathfrak{B}$, все элементы которого больше $\omega^{\mathfrak{B}}$. Тогда система $(\mathfrak{B}, I)$ обладает первым свойством изолированности.

Отсюда легко следует теорема 2.9:

Пусть теория $T = \mathrm{Th}(\omega, 0, 1, \leqslant, +, (P_i)_i)$, где P_i — произвольные предикаты, допускает элиминацию кванторов. Пусть $\mathfrak{A} \succ$ $\succ (\omega, 0, 1, \leqslant, +)$ — элементарное (строгое) расширение арифметики Пресбургера. Тогда в теории $T' = \mathrm{Th}(\mathfrak{A}, (P_i)_i)$ имеет место коллапс к порядку.

Глава 3. Случайный граф

Случайным[11] называется граф $\mathfrak{G} = (V, E)$, обладающий следующим свойством. Для любых четырёх конечных множеств вершин A_1, A_2, A_3, A_4, для которых $A_1 \cap A_2 = A_3 \cap A_4 = \varnothing$, существует вершина x такая, что

1) $(\mathsf{x}, \mathsf{y}) \in E$ для любой вершины $\mathsf{y} \in A_1$;

2) $(\mathsf{x}, \mathsf{y}) \notin E$ для любой вершины $\mathsf{y} \in A_2$;

3) $(\mathsf{y}, \mathsf{x}) \in E$ для любой вершины $\mathsf{y} \in A_3$;

4) $(\mathsf{y}, \mathsf{x}) \notin E$ для любой вершины $\mathsf{y} \in A_4$.

Ранее показано[12]: в упорядоченном случайном графе коллапса к порядку нет, теория дискретно упорядоченного случайного графа неразрешима.

Легко получается следующий результат (теорема 3.2):

Теория случайного графа $\mathrm{Th}(\mathfrak{G})$ не обладает свойством коллапса к равенству, если сигнатура базы данных содержит хотя бы один двухместный предикатный символ.

Чтобы показать, что плотное упорядочение случайного графа может быть разрешимо, используется счётность множества $\mathbb{Q}$ рациональных чисел. Занумеровав их натуральными числами, по индукции строится отношение E из определения случайного графа таким образом, чтобы элемент

[11] Rado R. Universal graphs and universal functions. // Acta Arith., № 9, 1964. P.331–340.

[12] Benedict M., Dong G., Libkin L., Wong L. Relational expressive power of constraint query languages. // Proc. 15th ACM Symp. on Principles of Database Systems, 1996. P.5–16.

х, удовлетворяющий пунктам 1)–4), существовал на любом непустом открытом интервале. Таким образом доказываются следствие 3.3.1:

> *Система* $(\mathbb{Q}, E)$ — *случайный граф.*

и теорема 3.4:

> *Теория системы* $(\mathbb{Q}, E, \leqslant)$ *допускает эффективную элиминацию кванторов.*

Далее рассматриваются монадические состояния на неупорядоченном случайном графе. Сначала замечается, что можно ограничиться рассмотрением лишь таких состояний, в которых различные предикаты не пересекаются. После чего доказывается основная теорема 3.6:

> *Если свойство* $\mathcal{S}$ *конечных алгебраических систем не может быть выражено ограниченными формулами, то оно не может быть выражено и формулами расширенной сигнатуры на случайном графе.*

Для доказательства непосредственно используются игры Эренфойхта.

Глава 4. Сводимые теории

Формула первого порядка $\varphi(\bar{x}, \bar{y})$ сигнатуры (Σ, P) называется с в о д и м о й в системе $(\mathfrak{A}, I)$ (или просто I-сводимой), где I — неразличимая в $\mathfrak{A}$ последовательность, если существует бескванторная порядковая формула $\psi_\varphi(\bar{x}, \bar{z})$ такая, что в системе $(\mathfrak{A}, I)$ истинна следующая (Σ, P)-формула

$$(\forall \bar{y})(\exists \bar{z} \in P)(\forall \bar{x} \in P)(\varphi(\bar{x}, \bar{y}) \leftrightarrow \psi_\varphi(\bar{x}, \bar{z})).$$

Система $(\mathfrak{A}, I)$ называется I - с в о д и м о й, если каждая формула сигнатуры Σ является I-сводимой. Теория $\mathrm{Th}(\mathfrak{A})$ в этом случае тоже называется с в о д и м о й. Сводимость называется э ф ф е к т и в н о й, если построение формулы ψ_φ по формуле φ может быть выполнено алгоритмически. Сводимость называется т о т а л ь н о й, если сводимой является каждая формула сигнатуры (Σ, P). Теория T называется (эффективно, тотально) сводимой, если существует (эффективно, тотально) сводимая система $(\mathfrak{A}, I)$, где $\mathfrak{A} \models T$.

Система $(\mathfrak{A}, I)$ называется м а л о й, если $\mathfrak{A}$ является $|I|^+$-насыщенной. Ранее показано, что если теория сводима, то существует сводимая малая её модель.

Главный результат первой части данной главы — теорема 4.20:

Каждая малая I-сводимая алгебраическая система является тотально I-сводимой.

Для доказательства (параграфы 4.2–4.4) используется механизм вспомогательных формул первого порядка — обобщённых (k, l)-формул (k и l — натуральные числа). Показывается возможность некоторых преобразований выполнимых обобщённых (k, l)-формул, при которых они остаются выполнимыми. Доказывается, что для выполнимых обобщённых (k, l)-формул k не может быть сколь угодно большим. После этого показывается, что все P-ограниченные кванторы могут вынесены в начало формулы и используются ранее доказанные в работах ([8,7]) теоремы.

Ввиду того, что все перечисленные построения выполняются эффективно, если только исходная сводимость была эффективной, получается следствие 4.20.1:

Каждая малая эффективно I-сводимая алгебраическая система является тотально эффективно I-сводимой.

Ещё одно следствие — теорема 4.21:

Если тип неразличимой последовательности I в эффективно I-сводимой системе $(\mathfrak{A}, I)$ является рекурсивным и система $(\mathfrak{A}, I)$ является малой, то тип I в системе $(\mathfrak{A}, I)$ тоже рекурсивен (в частности, теория системы $(\mathfrak{A}, I)$ разрешима).

И, наконец, используя результаты, полученные другими авторами, имеем теорему 4.22:

Если теория T сводима, то теория T обладает вторым свойством изолированности, и, следовательно, в теории T имеет место коллапс к порядку.

Вторая часть этой главы посвящена доказательству обратного результата. В начале вводится вспомогательный механизм различающих пар и доказываются вспомогательные теоремы 4.23 и 4.24, основной результат которых — для сводимости элементарных расширений системы необходимо и достаточно, чтобы для каждой формулы количество различающих пар было ограничено.

Используя эти результаты, доказывается лемма 4.25 о том, что для несводимых теорий в специальных элементарных расширениях их моделей существуют псевдоконечные множества с определёнными свойствами совместности формул над ними. Из этого получается теорема 4.26:

Пусть теория не имеет сводимых моделей, тогда она не обладает ни первым, ни вторым свойством псевдоконечной однородности.

В качестве итога всей главы формулируются теорема 4.27:

Если теория обладает первым (вторым) свойством псевдоконечной однородности, то она обладает вторым свойством изолированности.

и теорема 4.28:

Для любой теории T следующие утверждения эквивалентны:

1) *T обладает вторым свойством псевдоконечной однородности;*
2) *T обладает вторым свойством изолированности;*
3) *T является сводимой.*

Эти результаты очень интересны по двум причинам. Во-первых, свойства сводимости и псевдоконечной однородности изначально были предложены разными людьми независимо, и велась дискуссия о том, какое из свойств является более общим. Во-вторых, для первых свойств изолированности и псевдоконечной однородности эквивалентности нет: существуют теории, обладающие первым свойством псевдоконечной однородности, но не имеющие первого свойства изолированности.

Глава 5. Автоматные системы и их обобщения

Пусть $\mathfrak{L} = (\omega, 0, 1, \leqslant, +)$ — обычная арифметика Пресбургера. Добавим в сигнатуру новые одноместный функциональный и одноместный предикатный символы. Полученную сигнатуру будем обозначать $\Sigma_R^A = (0, 1, <, +, 4^x, R)$. Обогатим систему $\mathfrak{L}$ до системы $\mathfrak{L}_R$ сигнатуры Σ_R^A. Значением функционального символа будет степень по основанию 4: 4^x, а значением предиката R — множество значений гиперэкспоненты по основанию 4. Точнее, определим функцию $H_4(x)$ следующим образом: $H_4(0) = 0$, $H_4(x+1) = 4^{H_4(x)}$. Эта функция — *гиперэкспонента* по основанию 4, а множество её значений и будет нашим предикатом R: $R = \{H_4(x) : x \in \omega\}$. По индукции доказывается теорема 5.1:

Для каждого натурального $\mathfrak{p} > 1$ значение $H_4(x)$ является константой по модулю $\mathfrak{p}$, начиная с некоторого x.

Используя эту теорему, далее доказывается теорема 5.3:

> *В теории T_R любая формула эквивалентна экзистенциальной формуле, матрица которой является булевой комбинацией предикатов делимости для термов вида $v + \mathfrak{a}$ и сравнений сумм вида*
> $$\mathfrak{c} + \sum_v (\mathfrak{a}_v 4^v + \mathfrak{b}_v v),$$
> *где $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ — константы, а v — переменные из формулы.*

Для доказательства используется метод последовательного выноса кванторов существования из-под знака отрицания.

Обогатим сигнатуру Σ_R^A константой $\mathfrak{h}$ и обозначим полученную сигнатуру $\Omega_\mathfrak{h}$: $\Omega_\mathfrak{h} = (0, 1, \leqslant, +, 4^x, R, \mathfrak{h})$. Будем рассматривать алгебраические системы сигнатуры $\Omega_\mathfrak{h}$:

$$\mathfrak{D}_\mathfrak{h} = ([0; \mathfrak{h}], 0_\mathfrak{h}, 1_\mathfrak{h}, \leqslant_\mathfrak{h}, +_\mathfrak{h}, 4^x_\mathfrak{h}, R_\mathfrak{h}, \mathfrak{h}_\mathfrak{h}) \text{ —}$$

начальные фрагменты системы $\mathfrak{L}_R$, ограниченные числом $\mathfrak{h} \in R$. Отношения $\leqslant_\mathfrak{h}$ и $R_\mathfrak{h}$ — обычные ограничения отношений $\leqslant$ и R на множество $[0; \mathfrak{h}]$. Отношение $+_\mathfrak{h}$ будет ограничением с насыщением обычного сложения, то есть $a +_\mathfrak{h} b = a + b$, если $a + b < \mathfrak{h}$, иначе — $a +_\mathfrak{h} b = \mathfrak{h}$. Аналогично ограничивается экспонента. Главным результатом является лемма 5.4:

> *Для каждой формулы φ сигнатуры $\Omega_\mathfrak{h}$ можно построить формулу $\psi(\mathfrak{h}, \mathfrak{h}_1)$ сигнатуры Σ_R^A такую, что*
> $$\mathfrak{D}_\mathfrak{h} \models \varphi \Leftrightarrow \mathfrak{L}_R \models \psi(\mathfrak{h}, \mathfrak{h}_1).$$
> *Здесь $\mathfrak{h}_1$ — элемент R, непосредственно предшествующий $\mathfrak{h}$. Более того, можно считать, что все кванторы формулы ψ ограничены константой $\mathfrak{h}$, и значение каждого встречающегося в ней терма превосходит $\mathfrak{h}$ не более чем в два раза.*

Далее, в лемме 5.5, показывается, что построенная формула ψ эквивалентна линейным неравенствам для $\mathfrak{h}$. Доказывается лемма аналогично теореме 5.3, только вместо появления новых кванторов оказывается возможным определить значения переменных с помощью явных термов. Отсюда получается теорема 5.6:

Значение любой формулы на конечной алгебраической системе вида $\mathfrak{D}_\mathfrak{h}$ эквивалентно булевой комбинации линейных неравенств для $\mathfrak{h}$.

В дальнейшем рассматриваются состояния вида $\mathfrak{D}_\mathfrak{h}$. Свойство состояний, которое исследуется на предмет выразимости:

«Состояние является одной из систем вида $\mathfrak{D}_\mathfrak{h}$, порядки $\leqslant_\mathfrak{h}$ и $\leqslant$ согласованы, и количество элементов предиката $R_\mathfrak{h}$ чётно.» (1)

Здесь $\leqslant$ — порядок универсума. Очевидно, что если какая-то формула выражает указанное свойство, то она является $<$-инвариантной, так как свойство свойство (1) не меняется при сохраняющих порядок $\leqslant$ изоморфизмах состояния внутри универсума. Первые два утверждения этого свойства формулами первого порядка выразить можно (лемма 5.7). Из теоремы 5.6 следует теорема 5.8:

Свойство (1) *нельзя выразить формулами первого порядка сигнатуры* $(\Omega_\mathfrak{h}, \leqslant)$ *ни в каком универсуме.*

Далее рассматривается обогащение арифметики Пресбургера двухместным предикатом $\sqsubseteq$, предложенное в ([7]). Каждое натуральное число может быть разложено единственным образом в сумму различных степеней двойки, и $x \sqsubseteq y$ означает, что x — степень двойки, которая входит в разложение y. Если x не является степенью двойки, то $x \not\sqsubseteq y$ для любого y. По любой формуле данной системы $\mathfrak{L}_\sqsubseteq = (\omega, 0, 1, \leqslant, +, \sqsubseteq)$ может быть построен конечный автомат, распознающий истинность формулы, если ему на вход подать двоичные записи значений переменных. Поэтому данная система называется а в т о м а т н о й[13]. Система эта изоморфна идеалу Фреше счётной атомной булевой алгебры, в которой атомы упорядочены по типу натуральных чисел. Оказывается, существует формула φ, обладающая следующим свойством (леммы 5.9 и 5.10):

Если любую систему вида $\mathfrak{D}_\mathfrak{h}$ вложить в систему $\mathfrak{L}_\sqsubseteq$, то формула φ будет определять функцию, которая по каждому элементу множества $R_\mathfrak{h}$ даёт уникальный атом.

[13]Blumensath A., Graedel E. Automatic structures. // Proc. 15th IEEE Symp. on Logic in Computer Science, 2000. P.51–62.

Поэтому можно выразить чётность $R_{\mathfrak{h}}$ (теорема 5.11), поскольку существует формула, выделяющая любое конечное множество атомов:

> *Свойство* (1) *может быть записано в системе* $\mathfrak{L}_{\sqsubseteq}$ *в виде расширенной формулы.*

Таким образом нами доказана теорема 5.12:

> *В автоматной системе* $\mathfrak{L}_{\sqsubseteq}$ *коллапса к порядку нет.*

Это даёт ответы на открытые вопросы из статей ([6]) и ([7]) (теорема 5.13):

> *Существуют дискретно упорядоченные универсумы с разрешимой теорией, которые увеличивают выразительную силу языка логики предикатов с порядком. Более того, такие универсумы есть среди обогащений арифметики Пресбургера.*

Полученному результату можно придать более общую форму и сформулировать достаточные условия, при которых коллапса к порядку в теории нет (теорема 5.14):

Пусть в теории T сигнатуры Σ линейный порядок является дискретным и полным, и имеются две формулы $\varphi(\bar{x}, \bar{y})$ и $\psi(\bar{x}, \bar{z})$, которые обладают следующими свойствами.

1) *Длина набора $\bar{x}$ в обеих формулах одинакова.*
2) *Существует определимое в теории T множество H, и для любых $\bar{y}_1 \neq \bar{y}_2$ существует $\bar{x} \in H$, для которого*
$$\varphi(\bar{x}, \bar{y}_1) \not\equiv \varphi(\bar{x}, \bar{y}_2).$$
3) *Для любого конечного $K \subseteq H$ и любого $L \subseteq K$ существует $\bar{z}_{KL}$, для которого*
$$(\forall \bar{x} \in K)(\bar{x} \in L \leftrightarrow \psi(\bar{x}, \bar{z}_{KL})).$$

Тогда теория T не обладает свойством коллапса к порядку.

Далее рассматриваются обобщения $\mathfrak{L}_{\sqsubseteq}$. В $\mathfrak{L}_{\sqsubseteq}$ атомы образуют множество $U = \{2^i : i \in \omega\}$. Если взять бесконечное подмножество $U^* \subseteq U$, то можно определить отношение $\sqsubseteq^*$: $x \sqsubseteq^* y \Leftrightarrow x \sqsubseteq y \wedge x \in U^*$. Если существует константа n такая, что для любых $a_1, a_2, \ldots, a_n$ — подряд идущих атомов U, хотя бы один из них входит в U^*, то такое U^* и соответствующее ему отношение $\sqsubseteq^*$ назовём *плотными*, в противном случае — *редкими*.

Замечая, что если отношение $\sqsubseteq^*$ плотно, то с помощью него можно определить $\sqsubseteq$, мы доказываем теорему 5.15:

> *Если отношение $\sqsubseteq^*$ плотно, то в системе $(\omega, 0, 1, \leqslant, +, \sqsubseteq^*)$ коллапса к порядку нет.*

Сложнее доказать результат для редких отношений $\sqsubseteq^*$ (теорема 5.16):

> *Если отношение $\sqsubseteq^*$ является редким, то система $(\omega, 0, 1, \leqslant, +, \sqsubseteq^*)$ обладает свойством коллапса к порядку.*

Для этого строятся элементарные расширения, в которых есть термально изолированные множества I специального вида. Затем, используя игры Эренфойхта, доказывается, что построенные системы являются I-сводимыми. Отсюда следует коллапс к порядку.

Формула $\varphi(\bar{x}, \bar{y})$ называется *независимой* на множестве X, если следующее утверждение выполняется для любого натурального числа N: «существуют наборы $\bar{a}_1, \ldots, \bar{a}_N \in X$ длины $|\bar{x}|$ и для любого $K \subseteq \{1, \ldots, N\}$ существует набор $\bar{b}_K$ длины $|\bar{y}|$ такой, что для любого $i = 1, \ldots, N$ выполнено $i \in K \Leftrightarrow \varphi(\bar{a}_i, \bar{b}_K)$.»

Несмотря на коллапс к порядку в системе $(\omega, 0, 1, \leqslant, +, \sqsubseteq^*)$, имеет место теорема 5.23:

> *В системе $(\omega, 0, 1, \leqslant, +, \sqsubseteq^*)$ на каждом бесконечном множестве есть независимая формула.*

Этот результат опровергает гипотезу из статьи ([8]) о том, для коллапса к порядку необходимо существование бесконечного определимого множества, на котором не было бы независимой формулы.

Глава 6. Эффективная трансляция

Пусть Ω — сигнатура базы данных. Формулу сигнатуры $(\Omega, P, \leqslant)$, в которой все кванторы ограничены по P, а других вхождений P нет, назовём *P-формулой*. *Активной* называется формула, все кванторы которой ограничены активной областью.

Методом последовательного преобразования доказывается лемма 6.1:

Пусть φ — P-формула, а множество I — интерпретация символа P — является плотно упорядоченным множеством без концевых элементов. Тогда φ эквивалентна относительно конечных состояний над I активной $<$-ограниченной формуле.

Способ преобразования является эффективным (следствие 6.1.1).

Используя аналогичный метод, доказывается и лемма 6.2:

Пусть система $(\mathfrak{A}, I)$ сигнатуры (Σ, P) является тотально I-сводимой. Тогда всякая расширенная формула эквивалентна в области I формуле вида $(\exists \bar{c} \in P)(\psi(\bar{c}) \wedge \theta(\bar{c}))$, где формула ψ — в сигнатуре (Σ, P), а θ является P-формулой.

Для эффективной сводимости имеет место следствие 6.2.2:

Если система $(\mathfrak{A}, I)$ является малой и эффективно I-сводимой, то по всякой расширенной формуле можно эффективно построить эквивалентную ей в области I формулу вида $(\exists \bar{c} \in$ $\in P)(\psi(\bar{c}) \wedge \theta(\bar{c}))$.

Используя эти леммы и следствия, доказывается теорема 6.3:

Пусть система $(\mathfrak{A}, I)$ эффективно I-сводима и тип последовательности I рекурсивен. Тогда по всякой $<$-инвариантной формуле φ в сигнатуре (Ω, Σ) эффективно строится эквивалентная ей активная формула φ' в сигнатуре $(\Omega, \leqslant)$.

Для практического применения теоремы 6.3 формулируются её более слабый аналог — теорема 6.5:

Пусть теория T сигнатуры Σ полна и разрешима. Пусть $\mathfrak{A}$ — любая модель T с неразличимым множеством I, на котором нет независимой формулы и тип которого рекурсивен. Тогда по всякой $<$-инвариантной формуле φ в сигнатуре (Ω, Σ) эффективно строится эквивалентная ей активная формула φ' в сигнатуре $(\Omega, \leqslant)$.

Множество I без последнего элемента назовём почти неразличимым в алгебраической системе $\mathfrak{A}$, если для каждой формулы $\psi(\bar{x})$ существует $M_\psi \in I$ такое, что для любых двух одинаково упорядоченных наборов $\bar{\mathsf{x}}_1 \in I$ и $\bar{\mathsf{x}}_2 \in I$, все элементы которых больше M_ψ, выполнено

$\mathfrak{A} \models \psi(\bar{\mathrm{x}}_1) \leftrightarrow \psi(\bar{\mathrm{x}}_2)$. Говоря другими словами, последовательность является почти неразличимой, если каждое условие неразличимости выполняется для всех достаточно больших её элементов. Множество формул, выполняющихся на всех возрастающих последовательностях достаточно больших элементов, назовём типом этой последовательности. Почти неразличимую последовательность, на которой нет независимой формулы или выполняется условие эффективной сводимости назовём трансляционным множеством.

Используя понятие трансляционного множества, предыдущую теорему можно ещё более упростить (теорема 6.7):

> *Пусть T — полная разрешимая теория. Пусть в некоторой модели $\mathfrak{A}$ теории T существует трансляционное множество I, тип которого рекурсивен. Тогда по каждой $<$-инвариантной расширенной формуле может быть эффективно построена эквивалентная $<$-ограниченная формула.*

Особенно легко находить трансляционные множества для квази-о-минимальных теорий (теорема 6.8):

> *Пусть T — полная квази-о-минимальная разрешимая теория. Пусть в некоторой модели $\mathfrak{A}$ теории T существует почти неразличимое множество I. Тогда I — трансляционное множество.*

Используя теоремы 6.7 и 6.8, обнаруживается, что существуют способы эффективной трансляции расширенных формул в эквивалентные им $<$-ограниченные для многих классических теорий. Нужно только указать соответствующее трансляционное множество. Это решает два открытых вопроса из статьи ([6]).

Теорема 6.10:

> *Существует алгоритм, который по любой $<$-инвариантной в арифметике Пресбургера расширенной формуле строит эквивалентную ей активную $<$-ограниченную формулу.*

Трансляционным является множество факториалов: $I = \{x! : x \in \omega\}$.

Теорема 6.12:

> *Существует алгоритм, который по любой $<$-инвариантной в теории действительных чисел расширенной формуле строит эквивалентную ей активную $<$-ограниченную формулу.*

Трансляционным является множество степеней двойки, где показателями являются факториалы натуральных чисел: $I = \{2^{x!} : x \in \omega\}$.

Теорема 6.17:

> *Существует алгоритм, который по любой $<$-инвариантной в системе $\mathfrak{L}_{SF}$ (с эффективно согласованной со сложением функцией f) расширенной формуле строит эквивалентную ей активную $<$-ограниченную формулу.*

В доказательстве для согласованной со сложением функции f определяется «гиперфункция» F: $F(x+1) = f(F(x)!)$, и показывается, что трансляционным является множество $I = \{F(x!) : x \in \omega\}$.

Более сложное доказательство для арифметики Семёнова получается, в частности, из-за того, что арифметика Семёнова, в отличие от двух предыдущих теорий, не является квази-о-минимальной (теорема 6.18):

> *Теория систем $\mathfrak{L}_{SF}$ не является квази-о-минимальной.*

Следовательно, для $\mathfrak{L}_{SF}$ теорема 6.8 неприменима.

В заключении ещё раз перечисляются основные полученные результаты и формулируются некоторые открытые проблемы, отражающие возможные направления дальнейших исследований в данной области.

Автор выражает огромную благодарность научному консультанту профессору М.А.Тайцлину за обсуждение полученных результатов.

Автор благодарит руководителей семинаров, на которых были представлены результаты работы, академика РАН С.И.Адяна, профессора В.А.Успенского, члена-корреспондента РАН Ю.В.Матиясевича и профессора В.П.Оревкова, а также участников этих семинаров.

Список публикаций автора по теме диссертации

[1] Дудаков С.М. Трансляционный результат для расширений арифметики Пресбургера одноместной функцией, согласованной со сложением // Матем. заметки, №76(3), 2004, С.362–371.

[2] Дудаков С.М. Трансляционная теорема для теорий I-сводимых алгебраических систем // Изв. РАН. Серия матем., №68(5), 2004. С.67–90.

[3] Дудаков С.М., Тайцлин М.А. Трансляционные результаты для языков запросов в теории баз данных. // Успехи математических наук, №61:2(368), 2006. С.3–66.

[4] Дудаков С.М. Псевдоконечная однородность, изолированность и сводимость // Матем. заметки, №81(4), 2007, С.515–527.

[5] Дудаков С.М. Выразительная сила языков запросов первого порядка для баз данных на неупорядоченном случайном графе. // Вестник НовГУ. №34, 2005. С.51–57.

[6] Дудаков С.М. Трансляционная теорема в предикатных обогащениях начального фрагмента нестандартных моделей арифметики Пресбургера. // Сложные системы: обработка информации, моделирование и оптимизация, ТвГУ, Тверь, 2002. С.24–37.

[7] Дудаков С.М. Разрешимая теория без трансляционной теоремы. // Вестник ТвГУ, серия «Прикладная математика», №6(12), 2005. С.23–26.

[8] Dudakov S.M. Isolation and reducibility properties and the collapse result. // Proc. of intern. conf. CSR-2006 (Computer Sciences in Russia, Санкт-Петербург, июнь 2006). LNCS 3967, Springer, 2006. P.171–177.

[9] Дудаков С.М. Трансляционная теорема и автоматные системы // Вестник ТвГУ, серия «Прикладная математика», №4(21), 2006. С.5–35.