МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 510.652

ЭФФЕКТИВНАЯ ТРАНСЛЯЦИЯ РАСШИРЕННЫХ $<$-ИНВАРИАНТНЫХ ФОРМУЛ В $<$-ОГРАНИЧЕННЫЕ[1]

Дудаков С.М.
Кафедра информатики

Поступила в редакцию 03.07.2008, после переработки 02.08.2008.

Данная работа продолжает исследования по языкам запросов к базам данных. Ранее установлено, что во многих разрешимых теориях имеет место коллапс к порядку: каждая $<$-инвариантная формула эквивалентна некоторой $<$-ограниченной, но вопрос о возможности эффективного нахождения этой формулы почти не исследовался. Используя полученные нами ранее результаты, мы предлагаем метод эффективной трансляции для широкого класса теорий, который включает арифметику Семенова и теорию действительных чисел.

This paper continues investigations in the database query languages. It is known that for many decidable theories the collapse result holds: each locally generic query is equivalent to some restricted query. But till now the problem of the effective construction of this query is almost unexplored. We use our earlier results to construct a method of effective translation. The method is rather general, for example it is applicable to the Semenov arithmetic and the real number theory.

Ключевые слова: коллапс к порядку, формула первого порядка.
Keywords: collapse result, first-order formula.

1. Введение

Задача, которая решается в данной работе, проистекает из теории баз данных (БД). БД — конечная совокупность конечных таблиц. Таблицы можно считать конечными отношениями, названия которых образуют конечную сигнатуру Ω, а элементы таблиц берутся из какого-либо фиксированного множества A. Хотя количество таблиц и количество элементов в каждой из них конечно, но эти количества потенциально неограниченны, поэтому A следует считать бесконечным. Таким образом, БД можно считать алгебраической системой $\mathfrak{D}$ сигнатуры Ω, носитель которой — конечное подмножество A. Для извлечения информации из БД, как правило, используются языки первого порядка. В простейшем случае запросы являются замкнутыми формулами. Хорошо известно, что не всякое свойство

[1] Работа выполнена при финансовой поддержке РФФИ, проекты 07-01-00637 и 08-01-00241.

алгебраических систем может быть записано такими формулами. Например, если сигнатура БД содержит только один одноместный предикатный символ P, то невозможно записать в этой сигнатуре формулу первого порядка, выделяющую в точности те БД, в которых количество элементов P является чётным.

Один из путей, который помог бы преодолеть это ограничение, состоит в следующем. Обычно над множеством A, элементы которого используются для построения $\mathfrak{D}$, определены какие-либо стандартные отношения, образующие сигнатуру Σ. Например, если $A = \omega$, то над ω в качестве таких отношений можно использовать операции сложения и умножения. Таким образом, элементы, составляющие $\mathfrak{D}$, являются элементами некой алгебраической системы $\mathfrak{A}$ сигнатуры Σ. Возможно, что если в формулах использовать не только отношения из Ω, но и из Σ (такие формулы называются расширенными), то можно будет записать какие-то свойства, которые нельзя записать формулами в сигнатуре Ω (ограниченными). Разумеется, речь должна идти не о связи отношений из Ω и Σ, а только о свойствах отношений из Ω. Более точно, значение формулы не должно меняться при произвольных изоморфизмах $\mathfrak{D}$ внутри $\mathfrak{A}$. Такие формулы называются $=$-инвариантными. Как известно, в некоторых случаях этот метод действительно приводит к увеличению выразительной силы языка. Например, Ю.Ш.Гуревичем показано, что отношение линейного порядка уже само по себе увеличивает выразительные возможности.

Интересно, что во многих случаях использование других отношений кроме порядка не приводит к дальнейшему росту выразительной силы языка. Для этого нужно рассматривать $<$-ограниченные формулы (т.е. формулы в сигнатуре $(\Omega, \leqslant)$) и $<$-инвариантные формулы (т.е. формулы не меняющие своей истинности при произвольных сохраняющих порядок изоморфизмах БД). Как известно, (см., например, [10, 9, 8, 12, 2]) для многих разрешимых теорий выполняется следующее утверждение (коллапс к порядку): для любой модели $\mathfrak{A}$ такой теории любая $<$-инвариантная в ней формула эквивалентна некоторой $<$-ограниченной. Однако до сих пор оставался практически неисследованным вопрос об эффективности такого преобразования. Единственный результат в этой области относится к теории упорядоченных абелевых групп с делением (см. [11]).

Результаты работы [3] дали нам возможность разработать весьма общий алгоритм такой трансляции сразу для большого класса теорий, куда входят, например, арифметика Семенова и арифметика действительных чисел.

Во втором параграфе мы даём основные определения. В третьем — приводим достаточные условия эффективной трансляции и даем схему алгоритма, который эту трансляцию осуществляет. Далее мы показываем, как полученные результаты можно применить к перечисленным выше теориям.

2. Основные определения

Основные понятия теории моделей можно найти, например, в [5]. Пусть Σ — произвольная предикатная сигнатура, не содержащая символа P, а P — одноместный предикатный символ.

Определение 1 (P-ограниченная формула, [8]). *Формула первого порядка φ сигнатуры (Σ, P) называется* P-ограниченной, *если она или не содержит символа P (то есть является формулой в сигнатуре Σ), или построена из P-ограниченных* *формул с помощью булевых связок и P-ограниченных кванторов, т.е. кванторов видов $(\forall x \in P)$ и $(\exists x \in P)$.*

Теперь определим свойство I-сводимости.

Определение 2 (I-сводимость, [8])**.** *Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ с носителем A. Пусть I — плотно упорядоченное множество без концевых элементов в $\mathfrak{A}$, которое является неразличимой в $\mathfrak{A}$ последовательностью.*

Система $\mathfrak{A}$ обладает свойством I-сводимости*, если для любой P-ограниченной формулы $\varphi(\bar{x},\bar{y})$ существует бескванторная порядковая формула $\psi_\varphi(\bar{z},\bar{y})$ такая, что для любого набора $\bar{m} \in A$ существует набор $\bar{c}_\varphi(\bar{m}) \in I$ такой, что*

$$(\mathfrak{A}, I) \models (\forall \bar{y} \in P)(\varphi(\bar{m},\bar{y}) \leftrightarrow \psi_\varphi(\bar{c}_\varphi(\bar{m}),\bar{y})).$$

I-сводимость мы будем называть эффективной, если формула ψ_φ строится по формуле φ эффективно.

Как доказано в [12] (см. также [8]), для I-сводимости системы достаточно, чтобы условие I-сводимости выполнялось лишь для формул сигнатуры Σ.

Определение 3 (Независимая формула, [8])**.** *Формула $\varphi(\bar{x},\bar{y})$ называется* независимой *в теории T, если в теории T следующее утверждение выполняется для любого натурального числа N:*

существуют наборы $\bar{a}_1,\ldots,\bar{a}_N$ длины $|\bar{x}|$ и для любого $K \subseteq \{1,\ldots,N\}$ существует набор $\bar{b}_K$ длины $|\bar{y}|$ такой, что для любого $i = 1,\ldots,N$

$$i \in K \Leftrightarrow \varphi(\bar{a}_i,\bar{b}_K).$$

Неформально это означает, что можно найти сколь угодно большие конечные множества наборов, из которых формула способна выделить произвольное подмножество. В [8] показано, что из отсутствия в теории независимой формулы следует I-сводимость некоторых её моделей.

Определение 4 (Тотальная I-сводимость, см. также [8, 12])**.** *Пусть I — плотно упорядоченное множество без концевых элементов в системе $\mathfrak{A}$ сигнатуры Σ, являющееся неразличимой в $\mathfrak{A}$ последовательностью.*

Алгебраическая система $\mathfrak{A}$ называется тотально I-сводимой*, если для любой формулы $\varphi(\bar{x},\bar{y})$ сигнатуры (Σ, P) (не обязательно P-ограниченной) существует бескванторная порядковая формула $\psi_\varphi(\bar{z},\bar{y})$ такая, что для любого $\bar{m} \in A$ существует набор $\bar{c}_\varphi(\bar{m}) \in I$ такой, что*

$$(\mathfrak{A}, I) \models (\forall \bar{y} \in P)(\varphi(\bar{m},\bar{y}) \leftrightarrow \psi_\varphi(\bar{c}_\varphi(\bar{m}),\bar{y})).$$

Пусть T — теория сигнатуры Σ. Пусть Ω — конечная предикатная сигнатура, не имеющая общих символов с Σ за исключением порядка $<$. При рассмотрении моделей сигнатуры $\Sigma \cup \Omega$, мы всегда считаем, что отношения порядка Σ и Ω согласованы, следовательно, противоречий не возникает.

Определение 5 (Коллапс к порядку, [10, 9])**.** *Формулу первого порядка в сигнатуре (Σ, Ω) мы называем* расширенной*, в сигнатуре $(\leqslant, \Omega)$ —* $<$-ограниченной*.*

Если $\mathfrak{A}$ *— модель* T*,* $\mathfrak{B}$ *— интерпретация символов из* Ω *над* $\mathfrak{A}$*, то* $\mathfrak{B}$ *называется* состоянием *в* $\mathfrak{A}$*. Состояние* $\mathfrak{B}$ *называется* конечным*, если интерпретации всех символов из* Ω *конечны. Формула называется* $<$-инвариантной относительно конечных состояний *(или просто* $<$-инвариантной*), если для любого конечного состояния* $\mathfrak{B}$ *из истинности запроса в* $(\mathfrak{A}, \mathfrak{B})$*, следует его истинность в* $(\mathfrak{A}, \mathfrak{C})$ *для любого* $<$*-изоморфного* $\mathfrak{B}$ *состояния* $\mathfrak{C}$*. Если каждая* $<$*-инвариантная расширенная формула эквивалентна на конечных состояниях некоторой* $<$*-ограниченной формуле, то это свойство теории называется* коллапсом к порядку.

В работах [9, 8, 12] даны достаточные признаки наличия в тех или иных теориях коллапса к порядку. Однако важная задача об эффективности трансляции исследована пока только для теории упорядоченных абелевых групп с делением [11]. Наша работа восполняет этот существенный пробел. Мы формулируем достаточно общие условия, при которых перевод формул из расширенной сигнатуры в $<$-ограниченную выполняется эффективно, и параллельно указываем алгоритмы трансляции. В качестве завершения мы применяем полученные результаты к некоторым классическим теориям, которые наиболее широко используются на практике: арифметике Семенова и арифметике действительных чисел.

3. Достаточные условия эффективной трансляции

Итак, мы считаем, что имеется алгебраическая система сигнатуры Σ и сигнатура ограниченных формул — Ω.

Определение 6. Активная область *состояния* $\mathfrak{B}$ *— множество всех таких* $a \in \mathfrak{A}$*, которые участвуют хотя бы в одном отношении* Ω*. Активную область состояния мы обозначаем с помощью* adom*. Очевидно, что* adom *определяется некоторой формулой сигнатуры* Ω*. Формула, в которой все кванторы являются* adom*-ограниченными, называется* активной*.*

Формула в сигнатуре $(\Omega, P, \leqslant)$, в котором все кванторы ограничены по множеству P, а других вхождений P нет, мы называем P-формулой.

Лемма 1. *Пусть* φ *—* P*-формула, а множество* I *— интерпретация символа* P *— является плотно упорядоченным множеством без концевых элементов. Тогда* φ *эквивалентна относительно конечных состояний в* I *активной формуле в сигнатуре* Ω*.*

Доказательство. Расширим сигнатуру, добавив константы для наименьшего и наибольшего элемента активной области: a_0 и a_m соответственно. Очевидно, что их можно определить с помощью adom-ограниченных кванторов.

Разобьем в формуле φ каждый P-ограниченный квантор на два: по множеству adom и по множеству $P \setminus \mathrm{adom}$ (будем обозначать последнее множество с помощью $\overline{\mathrm{adom}}$):

$$(\exists x \in P)\chi \equiv (\exists x \in \mathrm{adom})\chi \vee (\exists x \in \overline{\mathrm{adom}})\chi;$$

$$(\forall x \in P)\chi \equiv (\forall x \in \mathrm{adom})\chi \wedge (\forall x \in \overline{\mathrm{adom}})\chi.$$

Приведем полученную формулу к предваренному виду. Пусть теперь формула φ имеет вид

$$\varphi \sim (\mathsf{Q}_1 x_1 \in \mathrm{adom}^{\varepsilon_1}) \ldots (\mathsf{Q}_k x_k \in \mathrm{adom}^{\varepsilon_k})\varphi'(\bar{x}),$$

где $\mathrm{adom}^{\varepsilon_i}$ означает adom или $\overline{\mathrm{adom}}$. Пусть $\bar{u}$ — переменные формулы φ', связанные кванторами по adom, $\bar{v}$ — переменные, связанные кванторами по $\overline{\mathrm{adom}}$.

Наша задача — обратной индукцией по l доказать, что формулы

$$(\mathtt{Q}_l x_l \in \mathrm{adom}^{\varepsilon_l}) \ldots (\mathtt{Q}_k x_k \in \mathrm{adom}^{\varepsilon_k}) \varphi'(\bar{x})$$

эквивалентны формулам вида

$$\bigvee_j (\exists \bar{c}_j \in \mathrm{adom})(\chi_j(\bar{c}_j, \bar{v}) \wedge \theta_j(\bar{c}_j, \bar{u})), \tag{1}$$

где формулы χ_j являются конъюнкциями атомных порядковых формул и не содержат переменных $\bar{u}$, а формулы θ_j содержат только adom-ограниченные кванторы и не содержат переменных $\bar{v}$.

Базис индукции ($l = k + 1$) получается тривиально — достаточно привести φ' к дизъюнктивной нормальной форме, и заметить, что для любого $v \in \overline{\mathrm{adom}}$ все атомные формулы сигнатуры Ω ложны, а неравенства вида $u < v$ и $v < u$ эквивалентны формулам

$$(\exists c \in \mathrm{adom})(c < v \wedge c = u) \quad \text{и} \quad (\exists c \in \mathrm{adom})(v < c \wedge c = u)$$

соответственно.

Предположим, что для $l + 1$ наше утверждение доказано. Чтобы сделать индукционный шаг мы должны доказать, что формулы вида

$$(\exists x_l \in \mathrm{adom}^{\varepsilon_l}) \left(\bigvee_j (\exists \bar{c}_j \in \mathrm{adom})(\chi_j(\bar{c}_j, \bar{v}) \wedge \theta_j(\bar{c}_j, \bar{u})) \right),$$

$$(\forall x_l \in \mathrm{adom}^{\varepsilon_l}) \left(\bigvee_j (\exists \bar{c}_j \in \mathrm{adom})(\chi_j(\bar{c}_j, \bar{v}) \wedge \theta_j(\bar{c}_j, \bar{u})) \right)$$

тоже эквивалентны формулам вида (1).

В первом случае, если $x_l \in \mathrm{adom}$, то квантор существования вносится под знак дизъюнкции, а переменная x_l просто включается в множество переменных $\bar{c}$:

$$\bigvee_j (\exists x_l \in \mathrm{adom})(\exists \bar{c}_j \in \mathrm{adom})(\chi_j(\bar{c}_j, \bar{v}) \wedge \theta_j(\bar{c}_j, \bar{u})).$$

Если квантор существования ограничен по $\overline{\mathrm{adom}}$, то точно так же формула будет эквивалентна

$$\bigvee_j (\exists x_l \in \overline{\mathrm{adom}})(\exists \bar{c}_j \in \mathrm{adom})(\chi_j(\bar{c}_j, \bar{v}) \wedge \theta_j(\bar{c}_j, \bar{u})),$$

а последняя формула эквивалентна

$$\bigvee_j (\exists \bar{c}_j \in \mathrm{adom})(((\exists x_l \in \overline{\mathrm{adom}}) \chi_j(\bar{c}_j, \bar{v})) \wedge \theta_j(\bar{c}_j, \bar{u})),$$

поскольку x_l входить в θ_j не может.

Чтобы доказать утверждение для квантора всеобщности, достаточно доказать, что отрицание формул вида

$$\bigvee_j (\exists \bar{c}_j \in \mathrm{adom})(\chi_j \wedge \theta_j)$$

эквивалентно формулам такого же вида. В самом деле:

$$\neg \bigvee_j (\exists \bar{c}_j \in \mathrm{adom})(\chi_j(\bar{c}_j, \bar{v}) \wedge \theta_j(\bar{c}_j, \bar{u})) \equiv$$
$$\equiv \bigwedge_j (\forall \bar{c}_j \in \mathrm{adom})(\neg\chi_j(\bar{c}_j, \bar{v}) \vee \neg\theta_j(\bar{c}_j, \bar{u})).$$

Напомним, что формулы χ_j содержат только неравенства.

Неравенства вида $v_i < v_j$ можно вынести из-под квантора всеобщности.

Для каждого v_i выполнено в точности одно из трех неравенств:

$$v_i < a_0; \quad a_0 < v_i < a_m; \quad a_m < v_i.$$

Добавим к формуле дизъюнкции таких неравенств для каждого v_i и раскроем скобки. В первом случае все неравенства вида $v_i < c$ истинны, а $c < v_i$ — ложны, в последнем — наоборот. Поэтому достаточно рассмотреть случай, когда $a_0 < v_i < a_m$.

В этом случае для любого v_i существуют ближайшие к нему элементы $y_{1i}, y_{2i} \in \mathrm{adom}$: $y_{1i} < v_i < y_{2i}$, а формула

$$(\forall \bar{c}_j \in \mathrm{adom})(\neg\chi_j \vee \neg\theta_j)$$

эквивалентна такой:

$$(\exists \bar{y}_1, \bar{y}_2 \in \mathrm{adom})\Bigg(\bigwedge_i y_{1i} < v_i < y_{2i} \wedge$$
$$\wedge (\forall y \in \mathrm{adom}) \left(\bigwedge_i (y < y_{2i} \vee y_{1i} < y) \right) \wedge$$
$$\wedge (\forall \bar{c}_j \in \mathrm{adom})(\neg\chi'_j \vee \neg\theta_j) \Bigg),$$

где формула χ'_j получается из χ_j заменой неравенств вида $v_i < c$ на $y_{1i} < c$, а неравенств $c < v_i$ — на $c < y_{2i}$.

Осталось внести неравенства вида $v_i < v_j$, $a_0 < v_i < a_m$ и т.д. внутрь квантора существования и мы снова получим формулу нужного нам вида.

Итак мы доказали наше утверждение по индукции. Когда мы выполним последний шаг, в формуле больше не останется кванторов по $\overline{\mathrm{adom}}$. $\square$

Следствие 1. *Способ трансляции P-формул в активные формулы является эффективным.*

Напомним, что мы считаем неразличимую последовательность I интерпретацией одноместного предикатного символа P.

Лемма 2. *Пусть система $\mathfrak{A}$ является тотально I-сводимой. Тогда всякая расширенная формула эквивалентна в области I формуле вида*

$$(\exists \bar{c} \in P)(\psi(\bar{c}) \wedge \theta(\bar{c})), \tag{2}$$

где формула ψ — в сигнатуре (Σ, P), а формула θ является P-формулой.

Доказательство. Рассмотрим произвольную формулу φ. Разобьем в формуле φ каждый квантор на два: по P и по дополнению P:

$$(\exists x)\chi \equiv (\exists x \in P)\chi \vee (\exists x \notin P)\chi.$$

Приведем φ к предваренному виду:

$$(\mathsf{Q}_1 x_1 \in^{\varepsilon_1} P) \ldots (\mathsf{Q}_k x_k \in^{\varepsilon_k} P)\varphi'(\bar{x}),$$

где φ' — бескванторная формула. Так как мы рассматриваем только состояния в I, то из $x \notin P$ автоматически следует $\neg S(\ldots, x, \ldots)$, если $S \in \Omega$. Следовательно, можно считать, что все переменные, входящие в формулы вида $S(\cdots)$, где $S \in \Omega$, связаны ограниченными по P кванторами. Пусть $\bar{u}$ — переменные формулы φ', связанные кванторами по P, $\bar{v}$ — переменные, связанные кванторами по дополнению P.

Наша задача — индукцией по количеству кванторов доказать, что формулы

$$(\mathsf{Q}_l x_l \in^{\varepsilon_l} P) \ldots (\mathsf{Q}_k x_k \in^{\varepsilon_k} P)\varphi'(\bar{x})$$

эквивалентны формулам вида

$$(\exists \bar{c} \in P)(\psi(\bar{c}, \bar{v}) \wedge \theta(\bar{c}, \bar{u})),$$

где формула ψ — в сигнатуре Σ, а θ — P-формула. Кроме того, ψ содержит только переменные $\bar{c}$ и $\bar{v}$, а θ — только $\bar{c}$ и $\bar{u}$.

Базис индукции — бескванторная формула $\varphi'(\bar{u}, \bar{v})$. Для каждого символа $R_j \in \Sigma$, который входит в указанную формулу, согласно условию I-сводимости, выполняется

$$(\forall \bar{u} \in P)(R_j(\bar{u}, \bar{v}) \leftrightarrow \chi_j(\bar{c}_j, \bar{u}))$$

для некоторых $\bar{c}_j \in I$ и порядковой формулы χ_j. Следовательно,

$$\varphi'(\bar{u}, \bar{v}) \equiv (\exists \bar{c}_1, \ldots, \bar{c}_m \in P) \left(\left(\bigwedge_j (\forall \bar{w} \in P)(R_j(\bar{w}, \bar{v}) \leftrightarrow \chi_j(\bar{c}_j, \bar{w})) \right) \wedge \varphi''(\bar{u}, \bar{c}_1, \ldots, \bar{c}_m) \right),$$

где формула φ'' получена из φ' заменой всех формул $R_j(\bar{u}, \bar{v})$ на $\chi_j(\bar{c}_j, \bar{u})$.

Теперь докажем, что отрицание формулы вида

$$(\exists \bar{c} \in P)(\psi(\bar{c}, \bar{v}) \wedge \theta(\bar{c}, \bar{u}))$$

эквивалентно формуле такого же вида.

$$\neg(\exists\bar{c}\in P)(\psi(\bar{c},\bar{v})\wedge\theta(\bar{c},\bar{u}))\equiv(\forall\bar{c}\in P)(\neg\psi(\bar{c},\bar{v})\vee\neg\theta(\bar{c},\bar{u})).$$

Согласно свойству тотальной I-сводимости, существует $\bar{d}\in I$ и порядковая формула χ такие, что

$$(\forall\bar{w}\in P)(\neg\psi(\bar{w},\bar{v})\leftrightarrow\chi(\bar{d},\bar{w})).$$

Следовательно,

$$\begin{aligned}(\forall\bar{c}\in P)(\neg\psi(\bar{c},\bar{v})\vee\neg\theta(\bar{c},\bar{u}))\equiv&\\ \equiv(\exists\bar{d}\in P)(((\forall\bar{w}\in P)(\neg\psi(\bar{c},\bar{v})\leftrightarrow\chi(\bar{d},\bar{w})))\wedge&\\ \wedge(\forall\bar{c}\in P)(\chi(\bar{d},\bar{c})\vee\neg\theta(\bar{c},\bar{u}))),&\end{aligned}$$

что и требовалось.

Теперь при добавлении новых кванторов, мы можем считать, что они перестановочны с первой группой кванторов, следовательно, кванторы по P относятся только к формулам θ, так как ψ не содержит $\bar{u}$, а кванторы по дополнению P — только к ψ, так как θ не содержит $\bar{v}$.

Следовательно, формула φ эквивалентна в состояниях над I формуле вида (2). $\square$

Следствие 2. *В I-сводимой системе $\mathfrak{A}$ всякая расширенная формула эквивалентна в области I формуле вида* (2).

Доказательство. Как известно, если система $\mathfrak{A}$ является I-сводимой, то существует система $(\mathfrak{B},J)$ — элементарное расширение $(\mathfrak{A},I)$ — и плотно упорядоченное множество $J'\subseteq J$ такие, что система $\mathfrak{B}$ является тотально J'-сводимой (см. [3]). Следовательно, в $(\mathfrak{B},J')$ любая формула эквивалентна в J' некоторой формуле вида (2). Но так как I имеет тот же тип, что и J', и тоже плотно упорядочено, то формула

$$(\exists\bar{c}\in P)(\psi(\bar{c})\wedge\theta(\bar{c}))$$

будет истинна на состоянии $\mathfrak{C}_1$ в J' в системе $\mathfrak{B}$ тогда и только тогда, когда она будет истинна на изоморфном ему состоянии $\mathfrak{C}_2$ в I в системе $\mathfrak{A}$. $\square$

Следствие 3. *Если система $\mathfrak{A}$ является эффективно I-сводимой, то по всякой расширенной формуле можно эффективно построить эквивалентную ей в области I формулу вида* (2).

Доказательство. Если система $\mathfrak{A}$ является эффективно I-сводимой, то и тотальное J'-сведение из предыдущего следствия осуществляется эффективно (см. [3]), то есть порядковая формула χ для любой формулы находится эффективно, следовательно, и все построение эффективно. $\square$

Теорема 1. *Пусть система $\mathfrak{A}$ эффективно I-сводима и тип последовательности I рекурсивен. Тогда по всякой $<$-инвариантной формуле φ в сигнатуре (Σ,Ω) эффективно строится эквивалентная ей активная формула φ' в сигнатуре $(\Omega,\leqslant)$.*

Доказательство. Так как формула $<$-инвариантная, то, передвигая активную область состояния в I, мы не меняем истинности формулы.

Согласно следствию 3, в I по формуле φ эффективно строится формула вида

$$(\exists \bar{c} \in P)(\psi(\bar{c}) \wedge \theta(\bar{c}))$$

эквивалентная φ относительно состояний в I. Так как тип I рекурсивен, то формула $\psi(\bar{c})$ для $\bar{c} \in I$ эквивалентна некоторой порядковой формуле χ, причем χ по ψ строится эффективно. Следовательно,

$$(\exists \bar{c} \in P)(\psi(\bar{c}) \wedge \theta(\bar{c})) \equiv (\exists \bar{c} \in P)(\chi(\bar{c}) \wedge \theta(\bar{c})).$$

Итак, мы построили P-формулу эквивалентную исходной для состояний над I. Теперь согласно лемме 1 и следствию 1, она может быть эффективно перетранслирована в активную $<$-ограниченную формулу. Но активная $<$-ограниченная формула сохраняет свою истинность (или ложность) при произвольных передвижениях активной области, как и исходная. Значит они эквивалентны для любых состояний. □

4. Приложения к классическим теориям

Лемма 3. *Если теория T сигнатуры Σ полна, разрешима и не имеет независимой формулы, то любая ее модель $\mathfrak{A}$ с неразличимым множеством I является эффективно I-сводимой.*

Доказательство. Как известно (см. [8]), в условиях леммы модель $\mathfrak{A}$ является I-сводимой. Нам нужно доказать, что для любой формулы $\psi(\bar{x}, \bar{y})$ сигнатуры Σ эффективно строится порядковая формула $\chi(\bar{c}, \bar{y})$, для которой

$$(\forall \bar{x})(\exists \bar{c} \in P)(\forall \bar{y} \in P)(\psi(\bar{x}, \bar{y}) \leftrightarrow \chi(\bar{c}, \bar{y})).$$

Рассмотрим произвольную формулу $\psi(\bar{x}, \bar{y})$. Будем последовательно проверять истинность следующей последовательности формул:

$$(\exists \bar{b}_1, \ldots, \bar{b}_m) \bigwedge_{K \subseteq \{1, \ldots, m\}} (\exists \bar{a}) \bigwedge_{i=1}^{m} (\psi(\bar{a}, \bar{b}_i) \leftrightarrow i \in K) \tag{3}$$

для $m = 1, 2, 3, \ldots$. Так как в теории независимой формулы нет, то для некоторого m формула (3) окажется ложной. Таким образом, максимальная длина согласованной (когерентной) последовательности (см. [8, 4]) может быть эффективно найдена. Следовательно, и формула χ может быть эффективно построена. □

Теорема 2. *Пусть теория T не имеет независимой формулы. Пусть T имеет модель $\mathfrak{A}$, в которой существует неразличимая последовательность I, имеющая рекурсивный тип. Тогда по всякой $<$-инвариантной формуле φ в сигнатуре (Σ, Ω) эффективно строится эквивалентная ей формула φ' в сигнатуре $(\Omega, \leqslant)$.*

Доказательство. Следует из леммы 3 и теоремы 1 □

Для применения полученных результатов к конкретным теориям нам будет полезно следующее определение.

Определение 7. *Последовательность I без последнего элемента назовем* почти неразличимой *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 $\bar{x}_1 \in I$ и $\bar{x}_2 \in I$, все элементы которых больше M_ψ, выполнено*

$$\mathfrak{A} \models \psi(\bar{x}_1) \leftrightarrow \psi(\bar{x}_2).$$

Говоря другими словами, последовательность является почти неразличимой, если каждое условие неразличимости выполняется для всех достаточно больших ее элементов. Множество формул, выполняющихся на всех возрастающих последовательностях достаточно больших элементов, назовем типом этой последовательности.

Лемма 4. *Если I — почти неразличимая последовательность в $\mathfrak{A}$, то существует модель $\mathfrak{B} \equiv \mathfrak{A}$ и неразличимая в $\mathfrak{B}$ последовательность J, которая имеет тот же тип, что и I.*

Доказательство. Следует из теоремы компактности. □

Теорема 3. *Пусть T — полная разрешимая теория без независимой формулы. Пусть в некоторой модели $\mathfrak{A}$ теории T существует почти неразличимая последовательность I, тип которой рекурсивен. Тогда по каждой $<$-инвариантной расширенной формуле может быть эффективно построена эквивалентная $<$-ограниченная формула.*

Доказательство. Следует из предыдущей леммы и теоремы 2. □

Для удобства мы будем называть множество I, удовлетворяющее условиям теоремы *трансляционным множеством.*

5. Теория действительных чисел

В теории действительных чисел любая формула эквивалентна булевой комбинации алгебраических неравенств с целыми коэффициентами (см., например, [1]). Пусть

$$I = \{2^{n!} : n \in \omega\}.$$

Лемма 5. *I — трансляционное множество в стандартной модели* $(\mathbb{R}, +, \times, <)$.

Доказательство. Рассмотрим произвольную формулу $\psi(\bar{y})$. Мы можем считать, что $\psi(\bar{y})$ составлено из алгебраических неравенств с помощью булевых связок, и что все коэффициенты в неравенствах (включая свободные члены) по модулю не меньше единицы. Пусть L — сумма всех модулей коэффициентов и показателей степеней переменных из ψ. Пусть целое число $N > L + 2\log_2 L$ и $M_\psi = 2^{(N+1)!}$. Пусть набор переменных $\bar{y} \in I$ упорядочен по возрастанию и $y_n = 2^{m!}$ $(m \geqslant N+1)$.

Далее мы будем рассматривать только многочлены, которые получаются из многочленов, составляющих ψ, отбрасыванием слагаемых и делением на переменные. Мы не будем об этом специально упоминать.

Индукцией по количеству переменных в нетривиальном многочлене, докажем, что его значение по модулю не меньше 1. Для констант это следует из нашего допущения.

Рассмотрим многочлен с n переменными:

$$\sum_{j=0}^{k} p_j(y_1, \dots, y_{n-1}) y_n^j$$

Пусть $p_k(y_1, \dots, y_{n-1}) > 0$. Тогда по индукционному предположению

$$p_k(y_1, \dots, y_{n-1}) \geqslant 1$$

и

$$\sum_{j=0}^{k} p_j(y_1, \dots, y_{n-1}) y_n^j \geqslant y_n^k - \sum_{j=0}^{k-1} |p_j(y_1, \dots, y_{n-1})| y_n^j. \tag{4}$$

Далее получаем, что $y_n^j \leqslant 2^{m! \cdot (k-1)}$, $k \leqslant L$ и

$$|p_j(y_1, \dots, y_{n-1})| \leqslant L y_{n-1}^L \leqslant L 2^{(m-1)! \cdot L}.$$

Подставляя эти оценки в (4) получим:

$$2^{m! \cdot k} - L \cdot L 2^{(m-1)! \cdot L} \cdot 2^{m! \cdot (k-1)} \geqslant 2^{m! \cdot (k-1)} (2^{m!} - L^2 \cdot 2^{(m-1)! \cdot L}) \geqslant \\ \geqslant 2^{m! \cdot (k-1)} (2^{m!} - 2^{(m-1)! \cdot N}) \geqslant 1.$$

Точно так же, если $p_k(y_1, \dots, y_{n-1}) < 0$, то $p_k(y_1, \dots, y_{n-1}) \leqslant -1$ и

$$\sum_{j=0}^{k} p_j(y_1, \dots, y_{n-1}) y_n^j \leqslant -1.$$

Следовательно,

$$\sum_{j=0}^{k} p_j(y_1, \dots, y_{n-1}) y_n^j > 0 \leftrightarrow \\ \leftrightarrow \bigvee_{j=0}^{k} \left(p_j(y_1, \dots, y_{n-1}) > 0 \wedge \bigwedge_{i=j+1}^{k} p_i(y_1, \dots, y_{n-1}) = 0 \right). \quad \square$$

Теорема 4. *Существует алгоритм, который по любой $<$-инвариантной в теории действительных чисел расширенной формуле строит эквивалентную ей активную $<$-ограниченную формулу.*

Доказательство. Теория действительных чисел о-минимальна. Из этого следует, что независимой формулы нет. Тогда существование алгоритма следует из предыдущей леммы и теоремы 3. $\square$

6. Арифметика Семенова

Следующие определения введены А.Л.Семеновым в работах [6, 7].

Определение 8 (Согласованность со сложением, [7]). *Одноместная функция f на множестве натуральных чисел называется* согласованной со сложением, *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*

$$S(x) = \sum_i \mathfrak{a}_i f(x + \mathfrak{b}_i) \tag{5}$$

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.*

Функция называется эффективно согласованной со сложением, *если период в пункте 1) эффективно находится по $\mathfrak{n}$, по сумме (5) можно эффективно определить, является ли она ограниченной, и если не является, то константа $\mathfrak{s}'_S$ эффективно находится по S.*

Примерами согласованных со сложением функций являются показательная функция $\mathfrak{c}^x$ или факториал $x!$.

Обогащение арифметики Пресбургера

$$\mathfrak{L}_{SF} = (\omega, 0, 1, <, +, f),$$

в котором функция f согласована со сложением, предложено А.Л.Семеновым в [6, 7]. Там же показано, что для случая эффективной согласованности теории таких обогащений разрешимы.

В [7] показано, что если функция f является согласованной со сложением и не определима с помощью сложения, то для всякого $\mathfrak{c} \in \omega$ существует $\mathfrak{s}_\mathfrak{c} \in \omega$ такое, что для всех $x \in \omega$

$$f(x + \mathfrak{s}_\mathfrak{c}) \geqslant \mathfrak{c} f(x) + \mathfrak{c}x,$$

откуда следует, что f растет не медленнее, чем показательная функция. В частности, существует такое $\mathfrak{s}_2 \in \omega$, что

$$f(x + \mathfrak{s}_2) \geqslant 2f(x). \tag{6}$$

Из вышесказанного следует, что для всякой неограниченной суммы $S(x)$ вида (5) существует константа $\mathfrak{s}_S \in \omega$ такая, что для всех x выполнено

$$f(x - \mathfrak{s}_S) \leqslant |S(x)| \leqslant f(x + \mathfrak{s}_S). \tag{7}$$

Если функция согласована со сложением эффективно, то все указанные константы: $\mathfrak{s}_\mathfrak{c}$, $\mathfrak{s}_2$ и $\mathfrak{s}_S$, можно эффективно найти.

В теории системы $\mathfrak{L}_{SF}$ определима обратная к f функция:

$$f^{-1}(x) = y \iff (f(0) \geqslant x \wedge y = 0) \vee (f(y) \leqslant x \wedge \forall z(f(z) \leqslant x \to z \leqslant y)).$$

Здесь мы для удобства полагаем, что если $f(0) = \mathfrak{n}$, то $f^{-1}(x) = 0$ при $x \leqslant \mathfrak{n}$.

Мы будем рассматривать произвольную эффективно согласованную со сложением функцию f. В дальнейшем мы считаем, что такая функция зафиксирована.

Для любого $\mathfrak{p}$ функция f периодична по модулю $\mathfrak{p}$ для достаточно больших аргументов. Пусть $g(\mathfrak{p})$ означает максимальный из периодов по модулям $1, 2, \ldots, \mathfrak{p}$.

Поскольку f периодична по любому модулю, начиная с некоторого аргумента, то если рассматривать вектор остатков

$$\bar{h}(\mathsf{x}) = (f(\mathsf{x}) \bmod 1,\ f(\mathsf{x}) \bmod 2,\ f(\mathsf{x}) \bmod 3,\ \ldots)$$

при $\mathsf{x} \equiv 0 \pmod{1, 2, \ldots, m}$, то он имеет некоторый предел при $\mathsf{x} \to \infty$, $m \to \infty$. Пусть $\bar{h}_0$ — этот предел.

Покажем, как построить трансляционное множество I. Будем строить его элементы по очереди. В качестве первого элемента возьмем нуль: $\mathsf{x}_0 = 0$.

Предположим, что элементы $\mathsf{x}_0, \ldots, \mathsf{x}_{m-1}$ построены. Покажем, как построить x_m.

Договоримся об обозначениях. С помощью букв ε, η, θ будем обозначать непустые конечные последовательности целых чисел из диапазона $[-m; 0]$, длина которых не превосходит m. Будем также считать, что на множестве этих последовательностей задан следующий порядок: меньшими считаем последовательности меньшей длины, а при равной длине те, которые меньше лексикографически:

$$(0) < (-1) < \cdots < (-m) < (0, 0) < (0, -1) < \cdots$$
$$\cdots < (0, -m) < (-1, 0) < \cdots < (-m, \ldots, -m).$$

Сначала определим числа l^{ε}:

- $l^0 = m$;
- $l^{\varepsilon, i-1} = g(l^{\varepsilon, i})$;
- $l^{\varepsilon, i, 0} = l^{\varepsilon, i}$.

Теперь определим *векторы остатков* r^{ε}, которые будут иметь длины l^{ε} соответственно:

- $r^0 = (0, \ldots, 0)$;
- $r^{\varepsilon, i-1} = (0, \ldots, 0)$;
- $r^{\varepsilon, i, 0} \equiv r^{\varepsilon, i} - \bar{h}_0[l^{\varepsilon, i}]$ по модулям $1, \ldots, l^{\varepsilon, i}$.

Здесь с помощью $\bar{h}_0[l^{\varepsilon, i}]$ мы обозначили первые $l^{\varepsilon, i}$ компонент вектора $\bar{h}_0$.

Наконец, определим числа $\mathsf{x}_m^{\varepsilon}$ обратной индукцией по ε при нашем упорядочении, с помощью $|\varepsilon|$ мы обозначаем длину последовательности ε:

- $\mathsf{x}_m^{\varepsilon, 0}$ при $|\varepsilon, 0| = m$ полагаем бóльшими $f(\mathsf{x}_{m-1})$ и при этом, если $\varepsilon_1 < \varepsilon_2$, то $\mathsf{x}_m^{\varepsilon_1, 0} > f(\mathsf{x}_m^{\varepsilon_2, 0})$. Кроме того, $\mathsf{x}_m^{\varepsilon, 0}$ должны быть равны $r^{\varepsilon, 0}$ по модулям $1, \ldots, l^{\varepsilon, 0}$;

- $\mathsf{x}_m^{\varepsilon,-m}$ при $|\varepsilon,-m|<m$ полагаем бо́льшими всех $f(\mathsf{x}_m^{\eta})$, где $\eta>(\varepsilon,-m)$. Кроме того, $\mathsf{x}_m^{\varepsilon,-m}$ должны быть равны $r^{\varepsilon,-m}$ по модулям $1,\ldots,l^{\varepsilon,-m}$;

- Остальные $\mathsf{x}_m^{\varepsilon,i}$, где $|\varepsilon,i|<m$, вычисляем, используя рекуррентное соотношение:
$$\mathsf{x}_m^{\varepsilon,i}=f(\mathsf{x}_m^{\varepsilon,i-1})+\mathsf{x}_m^{\varepsilon,i,0}. \tag{8}$$

Полагаем $\mathsf{x}_m=\mathsf{x}_m^0$.

Прежде всего покажем, что наше построение возможно, то есть что числа с нужными остатками от деления существуют.

Лемма 6. *Существуют сколь угодно большие числа равные r^{ε} по модулям $1,\ldots,l^{\varepsilon}$.*

Доказательство. Используем индукцию по ε при нашем упорядочении. Для r^0 и $r^{\varepsilon,i-1}$ это очевидно: годятся достаточно большие факториалы.

Что касается $r^{\varepsilon,i,0}$, то достаточно вспомнить, что $f(k!)$ будет равно $\bar{h}_0[l^{\varepsilon,i}]$ по модулям $1,\ldots,l^{\varepsilon,i}$ для достаточно больших k. По индукционному предположению, существует бесконечно много x равных $r^{\varepsilon,i}$ по модулям $1,\ldots,l^{\varepsilon,i}=l^{\varepsilon,i,0}$. Но тогда числа $\mathsf{x}-f(k!)$ будут равны $r^{\varepsilon,i,0}=r^{\varepsilon,i}-\bar{h}_0[l^{\varepsilon,i}]$ по модулям $1,\ldots,l^{\varepsilon,i,0}$. $\square$

Нужно заметить, что построенные векторы остатков r^{ε} будут для различных m отличаться только своей длиной.

Покажем, что такое построение гарантирует несколько свойств множества I.

Лемма 7. *x_m все равны нулю по любому модулю $\mathfrak{p}$, начиная с некоторого m.*

Доказательство. Рассмотрим построение любого x_m при большом m. Из построения будет понятно, каким именно должно быть m. Очевидно, что нам будет достаточно показать, что все $\mathsf{x}_m^{\varepsilon}$ будут равны r^{ε} по модулям $1,\ldots,l^{\varepsilon}$.

Используем обратную индукцию по ε при нашем упорядочении.

Значение $f(\mathsf{x}_m^{\varepsilon,i-1})$ равно $\bar{h}_0[l^{\varepsilon,i}]$ по модулям $1,\ldots,l^{\varepsilon,i}$, так как $\mathsf{x}_m^{\varepsilon,i-1}$ равно нулю по модулям $1,\ldots,g(l^{\varepsilon,i})=l^{\varepsilon,i-1}$ (по индукционному предположению).

Значение $\mathsf{x}_m^{\varepsilon,i,0}$ равно $r^{\varepsilon,i,0}$ по модулям $1,\ldots,l^{\varepsilon,i}=l^{\varepsilon,i,0}$ (по индукционному предположению). Отсюда сразу получается
$$\mathsf{x}_m^{\varepsilon,i}=f(\mathsf{x}_m^{\varepsilon,i-1})+\mathsf{x}_m^{\varepsilon,i,0}\equiv\bar{h}_0[l^{\varepsilon,i}]+r^{\varepsilon,i,0}=\bar{h}_0[l^{\varepsilon,i}]+(r^{\varepsilon,i}-\bar{h}_0[l^{\varepsilon,i}])=r^{\varepsilon,i}$$
по модулям $1,\ldots,l^{\varepsilon,i}=l^{\varepsilon,i,0}$. $\square$

Следствие 4. *Если $\mathsf{x}\in I$, то x^{ε} будут константами по любому модулю, начиная с некоторого x.*

Лемма 8. *Если $\varepsilon_1<\varepsilon_2$ и $\mathsf{x}\in I$, то $\mathsf{x}^{\varepsilon_1}>f(\mathsf{x}^{\varepsilon_2})$, начиная с некоторого x.*

Доказательство. Тривиально следует из построения $\mathsf{x}_m^{\varepsilon}$. $\square$

Лемма 9. *Пусть $\mathsf{x}_1,\mathsf{x}_2\in I$, $\mathsf{x}_1<\mathsf{x}_2$. Тогда $\mathsf{x}_1^{\varepsilon}<\mathsf{x}_2^{\eta}$ для любых достаточно больших x_1 и x_2.*

Доказательство. Базовые константы при построении x_2^η берутся большими $f(\mathsf{x}_1)$. А при построении остальных x_2^η используются только функция f, которая монотонно возрастает, и сложение. Следовательно, x_2^η будет только больше. С другой стороны, x_1^ε будет, наоборот, не больше x_1. □

7. Эффективная трансляция для арифметики Семенова

В дальнейших построениях мы будем часто использовать термы одной переменной следующего вида:

$$t(x) = \sum_i \beta_i f(x^{\varepsilon_i} + \mathfrak{a}_i) + \sum_i \gamma_i x^{\eta_i}. \tag{9}$$

Докажем главное для нас утверждение о термах вида (9).

Лемма 10. *Для всякого неограниченного терма $t(x)$ вида (9) существует константа $\mathfrak{b}_t$, существует последовательность θ_t, и для всех $\mathsf{x} \in I$, начиная с некоторого, выполнено*

$$\mathsf{x}^{\theta_t} - \mathfrak{b}_t \leqslant f^{-1}(|t(\mathsf{x})|) \leqslant \mathsf{x}^{\theta_t} + \mathfrak{b}_t.$$

При этом θ_t и $\mathfrak{b}_t$ могут быть эффективно найдены по t.

Доказательство. Для удобства будем полагать $t(\mathsf{x})$ положительным. Противоположный случай получается заменой $t(\mathsf{x})$ на $-t(\mathsf{x})$.

Будем считать, что терм t не содержит подобных членов и все коэффициенты не равны нулю.

Далее выполняем следующие действия:

1) Если x^θ для наименьшего θ входит в терм t только линейно, то заменим его по формуле (8).

2) Рассмотрим $s^\theta(x)$ — подсумму t вида

$$s^\theta(\mathsf{x}^\theta) = \sum_{\varepsilon_i = \theta} \beta_i f(x^\theta + \mathfrak{a}_i) \tag{10}$$

для наименьшего θ. Если сумма $s^\theta(x)$ ограничена, то убираем ее из рассмотрения и возвращаемся к пункту 1).

Поскольку ограниченная сумма s^θ без подобных членов должна содержать не меньше двух слагаемых, а на шаге 1) добавляется не более одного слагаемого вида $\beta f(\mathsf{x}^\theta + \mathfrak{a})$, то этот процесс рано или поздно прекратится.

В результате получим, что

$$t(x) = s^\theta(x^\theta) + \delta(x),$$

где сумма s^θ вида (10) неограничена, а все слагаемые из $\delta(\mathsf{x})$ имеют порядок не больший x^θ (см. лемму 8). Согласно неравенству (7), существует константа $\mathfrak{s}_{s^\theta}$ и для любого x выполнено

$$f(x - \mathfrak{s}_{s^\theta}) \leqslant s^\theta(x) \leqslant f(x + \mathfrak{s}_{s^\theta}).$$

Можем выбрать x настолько большим, чтобы выполнялось

$$s^\theta(\mathsf{x}^\theta) \geqslant f(\mathsf{x}^\theta - \mathfrak{s}_{s^\theta}) \geqslant 2|\delta(\mathsf{x})|.$$

Тогда будем иметь

$$\frac{1}{2}f(\mathsf{x}^\theta - \mathfrak{s}_{s^\theta}) \leqslant \frac{1}{2}s^\theta(\mathsf{x}^\theta) \leqslant t(\mathsf{x}) \leqslant \frac{3}{2}s^\theta(\mathsf{x}^\theta) \leqslant \frac{3}{2}f(\mathsf{x}^\theta + \mathfrak{s}_{s^\theta}).$$

Учитывая, что f растет не медленнее экспоненты, а f^{-1}, соответственно, не быстрее логарифма, получаем для любого x

$$f^{-1}\left(\frac{1}{2}f(x - \mathfrak{s}_{s^\theta})\right) \geqslant x - \mathfrak{s}_{s^\theta} - \mathfrak{c}$$

и

$$f^{-1}\left(\frac{3}{2}f(x + \mathfrak{s}_{s^\theta})\right) \leqslant x + \mathfrak{s}_{s^\theta} + \mathfrak{c}$$

для некоторой константы $\mathfrak{c}$. Тогда $\mathfrak{b}_t = \mathfrak{s}_{s^\theta} + \mathfrak{c}$. □

Следствие 5. *Если $t_1(x)$ и $t_2(x)$ — два неограниченных терма вида* (9), $\mathsf{x}_1, \mathsf{x}_2 \in I$ *и* $\mathsf{x}_1 < \mathsf{x}_2$, *то* $t_1(\mathsf{x}_1) < t_2(\mathsf{x}_2)$, *начиная с некоторого* x_1.

Доказательство. Следует из леммы 10 и леммы 9. □

Лемма 11. *Для любого терма $t(x)$ вида* (9) *при* $\mathsf{x} \in I$ *для любого натурального* $\mathfrak{p}$ *значение* $t(\mathsf{x})$ *является константой по модулю* $\mathfrak{p}$ *начиная с некоторого* x.

Доказательство. Очевидно, что все сводится к определению остатков от деления чисел вида $f(\mathsf{x}^\varepsilon + \mathfrak{a})$. Напомним, что остатки от деления x^ε равняются r^ε (следствие 4). Следовательно, остатки от деления $f(\mathsf{x}^\varepsilon + \mathfrak{a})$ определяются в силу периодичности f. □

Лемма 12. I — *трансляционное множество в системе* $\mathfrak{L}_{SF}$.

Доказательство. Будем считать, что $\bar{x}$ — переменные, принимающие значения из I, а $\bar{y}$ — произвольные переменные. Напомним, что каждая формула в системе $\mathfrak{L}_{SF}$ эквивалентна экзистенциальной формуле

$$(\exists \bar{u})\psi(\bar{u}, \bar{\mathsf{x}}, \bar{\mathsf{y}}), \tag{11}$$

матрицу $\psi(\bar{u}, \bar{\mathsf{x}}, \bar{\mathsf{y}})$ которой составляют предикаты делимости и сравнения разделенных (см.[2]) термов, то есть неравенства вида

$$\underbrace{\sum_j (\mathfrak{a}_j f(u_{k_j} + \mathfrak{d}_j) + \mathfrak{b}_j u_{k_j})}_{(*)} - \sum_i t_i(\mathsf{x}_i) - r(\bar{\mathsf{y}}) \geqslant 0. \tag{12}$$

Здесь термы $t_i(\mathsf{x}_i)$ будут иметь вид (9). Терм $r(\bar{\mathsf{y}})$ может иметь какой угодно вид, для нас это не важно. Кроме ранее определенных операций мы в r будем допускать операции $\lfloor v \rfloor_I$ и $\lceil v \rceil_I$, означающие ближайшие к v слева и справа соответственно элементы I. Мы покажем, с одной стороны, как определить истинность формулы на больших $\bar{\mathsf{x}}$, когда $\bar{\mathsf{y}}$ в формуле нет (т.е. что множество I является почти неразличимым рекурсивного типа). С другой стороны, продемонстрируем, что формула является сводимой при достаточно больших x.

Мы сделаем это в два этапа. Сначала мы удалим кванторы, получив формулу вида

$$\sum_i t_i(\mathsf{x}_i) - r(\bar{\mathsf{y}}) \geqslant 0,$$

а затем покажем, как определить ее истинность для достаточно больших $\mathsf{x} \in I$, и докажем ее сводимость.

Без ограничения общности мы можем считать, что $\bar{u}$ и $\bar{\mathsf{x}}$ упорядочены по убыванию.

Если терм t_i ограничен по модулю, то его можно исключить из неравенств с помощью подстановки вместо него всевозможных значений и объединением получаемых формул с помощи дизъюнкции.

В дальнейшем будем считать, что все термы $t_i(\mathsf{x}_i)$ неограничены. Согласно следствию 5, мы можем для любого $\mathfrak{m}$ найти константу $M_{\mathfrak{m}}$ такую, что если все $\mathsf{x}_i > M_{\mathfrak{m}}$, то

$$\mathfrak{m}\left|\sum_{i>1} t_i(\mathsf{x}_i)\right| < t_1(\mathsf{x}_1).$$

Возьмем $\mathfrak{m} = 8$. Тогда для $\mathsf{x}_i > M_8$ получим

$$\frac{7}{8}t_1(\mathsf{x}_1) \leqslant \sum_i t_i(\mathsf{x}_i) \leqslant \frac{9}{8}t_1(\mathsf{x}_1). \tag{13}$$

Дальнейшие рассуждения будут сходны с доказательством теоремы 3 из [2]. Если для некоторого u_k термы вида $f(u_k + \mathfrak{d})$ не встречается в ψ, то элиминация квантора производится как в арифметике Пресбургера.

Напомним, что $u_1 > u_2 > \cdots > u_m$. Разобьем сумму $(*)$ на две части: $S(u_1)$ содержит все слагаемые вида $\mathfrak{a}_j f(u_1 + \mathfrak{d}_j)$, $s(\bar{u})$ — все остальное. Если сумма $S(u_1)$ ограничена по модулю, то она заменяется константами с последующим объединением полученных формул с помощью дизъюнкции.

Если $S(u_1)$ неограничена, то будем считать, что она положительна. Тогда существуют константы $\mathfrak{s}_S$ и $\mathfrak{s}^*$ такие, что

$$f(u_1 - \mathfrak{s}_S) \leqslant S(u_1) \leqslant f(u_1 + \mathfrak{s}_S) \tag{14}$$

и $f(u_1 - \mathfrak{s}_S) > 4|s(\bar{u})|$ при $u_1 > u_2 + \mathfrak{s}^*$. При $u_2 < u_1 \leqslant u_2 + \mathfrak{s}^*$ квантор по u_1 удаляется так же — подстановкой и дизъюнкцией. При $u_1 > u_2 + \mathfrak{s}^*$ получаем

$$|s(\bar{u})| < \frac{1}{4}f(u_1 - \mathfrak{s}_S) \leqslant \frac{1}{4}S(u_1).$$

Для x_1 возможны три ситуации:

$$\mathsf{x}_1^{\theta_{t_1}} \geqslant f^{-1}(8|r(\bar{\mathsf{y}})|) + \mathfrak{b}_{t_1} + 1,$$

$$\mathsf{x}_1^{\theta_{t_1}} \leqslant f^{-1}\left(\frac{1}{8}|r(\bar{\mathsf{y}})|\right) - \mathfrak{b}_{t_1} - 1$$

или
$$f^{-1}\left(\frac{1}{8}|r(\bar{\mathsf{y}})|\right) - \mathfrak{b}_{t_1} - 1 \leqslant \mathsf{x}_1^{\theta_{t_1}} \leqslant f^{-1}(8|r(\bar{\mathsf{y}})|) + \mathfrak{b}_{t_1} + 1.$$

Рассмотрим по очереди все три случая.

1) Пользуясь леммой 10, получаем
$$|t_1(\mathsf{x}_1)| \geqslant f(f^{-1}(|t_1(\mathsf{x}_1)|)) \geqslant f(\mathsf{x}_1^{\theta_{t_1}} - \mathfrak{b}_{t_1}) \geqslant$$
$$\geqslant f(f^{-1}(8|r(\bar{\mathsf{y}})|) + 1) \geqslant 8|r(\bar{\mathsf{y}})|.$$

Так как $|t_1(\mathsf{x}_1)| \geqslant 8|r(\bar{\mathsf{y}})|$, то, учитывая (13),
$$\frac{3}{4}t_1(\mathsf{x}_1) \leqslant \sum_i t_i(\mathsf{x}_i) + r(\bar{\mathsf{y}}) \leqslant \frac{5}{4}t_1(\mathsf{x}_1).$$

При
$$u_1 + \mathfrak{s}_S + \mathfrak{s}_2 < \mathsf{x}_1^{\theta_{t_1}} - \mathfrak{b}_{t_1} \leqslant f^{-1}(t_1(\mathsf{x}_1))$$
получаем, пользуясь (6) и (14):
$$S(u_1) + s(\bar{u}) \leqslant \frac{5}{4}S(u_1) \leqslant \frac{5}{4}f(u_1 + \mathfrak{s}_S) = \frac{5}{8} \times 2f(u_1 + \mathfrak{s}_S + \mathfrak{s}_2 - \mathfrak{s}_2) \leqslant$$
$$\leqslant \frac{5}{8}f(u_1 + \mathfrak{s}_S + \mathfrak{s}_2) < \frac{5}{8}f(f^{-1}(t_1(\mathsf{x}_1))) \leqslant \frac{5}{6} \times \frac{3}{4}t_1(\mathsf{x}_1) \leqslant$$
$$\leqslant \frac{5}{6}\left(\sum_i t_i(\mathsf{x}_i) + r(\bar{\mathsf{y}})\right),$$
то есть неравенство (12) ложно.

Если же
$$u_1 - \mathfrak{s}_S - \mathfrak{s}_2 > \mathsf{x}_1^{\theta_{t_1}} + \mathfrak{b}_{t_1} + 1 \geqslant f^{-1}(t_1(\mathsf{x}_1)) + 1,$$
аналогично получаем:
$$S(u_1) + s(\bar{u}) \geqslant \frac{3}{4}S(u_1) \geqslant \frac{3}{4}f(u_1 - \mathfrak{s}_S) \geqslant \frac{3}{4} \times 2f(u_1 - \mathfrak{s}_S - \mathfrak{s}_2) \geqslant$$
$$\geqslant \frac{3}{2}f(f^{-1}(t_1(\mathsf{x}_1)) + 1) \geqslant \frac{6}{5} \times \frac{5}{4}t_1(\mathsf{x}_1) \geqslant \frac{6}{5}\left(\sum_i t_i(\mathsf{x}_i) + r(\bar{\mathsf{y}})\right),$$
то есть (12) истинно.

При
$$\mathsf{x}_1^{\theta_{t_1}} - \mathfrak{b}_{t_1} - \mathfrak{s}_S - \mathfrak{s}_2 \leqslant u_1 \leqslant \mathsf{x}_1^{\theta_{t_1}} + \mathfrak{b}_{t_1} + \mathfrak{s}_S + \mathfrak{s}_2 + 1$$
переменную u_1 можно заменить термами вида $\mathsf{x}_1^{\theta_{t_1}} + \mathfrak{f}$ и взять дизъюнкцию получаемых формул. Заметим только, что вновь возникающие термы от x_1 будут иметь требуемый вид.

2) Пользуясь леммой 10, получаем

$$|t_1(\mathsf{x}_1)| \leqslant f(f^{-1}(|t_1(\mathsf{x}_1)|)+1) \leqslant f(\mathsf{x}_1^{\theta_{t_1}} + \mathfrak{b}_{t_1} + 1) \leqslant \\ \leqslant f\left(f^{-1}\left(\frac{1}{8}|r(\bar{\mathsf{y}})|\right)\right) \leqslant \frac{1}{8}|r(\bar{\mathsf{y}})|.$$

Имеем

$$\frac{7}{8}t_1(\mathsf{x}_1) + r(\bar{\mathsf{y}}) \leqslant \sum_i t_i(\mathsf{x}_i) + r(\bar{\mathsf{y}}) \leqslant \frac{9}{8}t_1(\mathsf{x}_1) + r(\bar{\mathsf{y}})$$

и из-за $8|t_1(\mathsf{x}_1)| \leqslant |r(\bar{\mathsf{y}})|$ получаем

$$\frac{3}{4}r(\bar{\mathsf{y}}) \leqslant \sum_i t_i(\mathsf{x}_i) + r(\bar{\mathsf{y}}) \leqslant \frac{5}{4}r(\bar{\mathsf{y}}).$$

Рассматривается аналогично случаю 1), но вместо $f^{-1}(t_1(\mathsf{x}_1))$ берем $f^{-1}(r(\bar{\mathsf{y}}))$. Заботиться о нужном виде новых термов здесь нет необходимости.

3) Имеем

$$f^{-1}\left(\frac{1}{8}|r(\bar{\mathsf{y}})|\right) - \mathfrak{b}_{t_1} - 1 \leqslant \mathsf{x}_1^{\theta_{t_1}} \leqslant f^{-1}(8|r(\bar{\mathsf{y}})|) + \mathfrak{b}_{t_1} + 1.$$

Учитывая, что для достаточно больших значений $r(\bar{\mathsf{y}})$ может существовать не более одного элемента I, удовлетворяющего этому неравенству, получим, что либо x_1 равняется одному из конечного множества значений (при малых $r(\bar{\mathsf{y}})$), либо x_1 равен одному из двух ближайших к

$$f^{-1}(8r(\bar{\mathsf{y}})) + \mathfrak{b}_{t_1} + 1$$

элементов I. Заменяя x_1 на указанные значения мы избавимся от x_1 в формуле под кванторами.

Таким образом, можно удалить все кванторы из формулы (11). В результате останутся неравенства вида

$$\sum_i t_i(\mathsf{x}_i) + r(\bar{\mathsf{y}}) \geqslant 0$$

и предикаты делимости вида $Q_j(t_k(\mathsf{x}_k))$ и $Q_j(r(\bar{\mathsf{y}}))$.

Доказательство почти неразличимости и рекурсивности типа I (это случай, когда $r(\bar{\mathsf{y}}) = \mathrm{const}$) легко получается из следствия 5 и леммы 11.

Для доказательства сводимости снова рассматриваем указанные три случая и выписываем явные неравенства для каждого x_i. □

Теорема 5. *Существует алгоритм, который по любой $<$-инвариантной в системе $\mathfrak{L}_{SF}$ расширенной формуле строит эквивалентную ей активную $<$-ограниченную формулу.*

Доказательство. Следует из леммы и теоремы 3. □

Список литературы

[1] Верещагин Н.К., Шень А. Языки и исчисления. М.: МЦНМО, 2000.

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

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

[4] Дудаков С.М., Тайцлин М.А. Трансляционные результаты для языков запросов в теории баз данных // Успехи математических наук, №61:2(368), 2006. С.2–65.

[5] Кейслер Г., Чен Ч.Ч. Теория моделей. М.: Мир, 1977.

[6] Семенов А.Л. О некоторых расширениях арифметики сложения натуральных чисел // Изв. АН СССР, 43(5), 1979. С.1175–1195.

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

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

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

[10] 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.

[11] Stolboushkin A.P., Taitslin M.A. Linear vs. order constraint queries over relational databases // Proc. 15th ACM Symp. on Principles of Database Systems, 1996. P.17–27.

[12] Taitslin M.A. A general condition for collapse results // Annals of Pure and Applied Logic. 2001. 113. P.323–330.