22. Свойства элементарных теорий: полнота, алгоритмическая разрешимость. Метод элиминации кванторов для доказательства алгоритмической разрешимости некоторых теорий (общий алгоритм). Основные этапы метода элиминации кванторов для доказательства алгоритмической разрешимости теории целых чисел с отношениями делимости (алгоритм Пресбургера)

Билеты 14

Теория T заданной сигнатуры σ называется *полной*, если для любого предложения $A \in Sent(\sigma)$ либо A, либо $\neg A$ принадлежит теории T ($Sent(\sigma)$ – множество предложений сигнатуры σ). Любая структурная теория полна (любому предложению структурной теории можно дать истинностную оценку, т.е. сказать, истинно оно или ложно). Полнота аксиоматических теорий не гарантируется. Например, теория групп не полна, так как предложение, выражающее коммутативность группы, и его отрицание не являются следствием групповых аксиом, поскольку в математике имеются как примеры коммутативных, так и некоммутативных групп.

Теория $T \subseteq Sent(\sigma)$ называется *алгоритмически разрешимой*, если существует алгоритм, который по любому предложению $A \in Sent(\sigma)$ отвечает на вопрос, принадлежит ли предложение A теории T.

Для ответа на этот вопрос используется *метод элиминации кванторов*. Пусть Th – теория сигнатуры σ, $A, B \subseteq Sent(\sigma)$. A и B равносильный в рамках теории Th (обозначение $A \overset{Th}{\equiv} B$), если $Th \cup \{A\} \vDash B$ и $Th \cup \{B\} \vDash A$. В случае, если $Th = Th_{ax} = Th(G, \Gamma)$ – аксиоматическая теория, то $A \overset{Th}{\equiv} B \Leftrightarrow \Gamma \cup \{A\} \vDash B,\ \Gamma \cup \{B\} \vDash A$. Метод применим к таким теориям, для которых возможен элементарный шал элиминации.

Пусть $A = \exists x[A_1(x) \& \dots \& A_n(x)]$, $A_1(x), \dots, A_n(x)$ – бескванторные формулы. Шаг элиминации состоит в том, чтобы найти такую бескванторную формулу B, что $A \overset{Th}{\equiv} B$. Формализуем алгоритм. Дано: $A \in Sent(\sigma)$, Th – теория сигнатуры Γ. Вопрос: $A \overset{?}{\in} Th$.

Алгоритм элиминации кванторов

1. Привести все самые внутренние кванторы к квантору ∃ с помощью двойных отрицаний и законов де Моргана.
2. Привести области действия кванторов к виду ДНФ
3. Распределить кванторы существования ∃ по слагаемым ДНФ
4. Для каждого слагаемого выполнить элементарный шаг элиминации кванторов
5. Повторить шаги (1)-(4), если это необходимо

Если в результате применения алгоритма A превратилось в истину ($A \to 1$), то она принадлежит теории Th, если $A \to 0$, то не принадлежит.

Арифметика Пресбургера

$\langle \mathbb{N}, 0, +, -, S \rangle$, $S(x) = x + 1$, $\sigma_z = \langle 0,1, +, -, <, D_2, D_3, \dots \rangle$ - сигнатура арифметики, где D_i – предикат делимости, т.е. $D_m(x) =$ "x делится на m без остатка". $Th(Z, \sigma_z)$.

Китайская теорема об остатках. Если натуральные числа $m_1, m_2, \dots, m_k$ попарно взаимно просты, то для любых целых $r_1, r_2, \dots, r_k$ таких, что $0 \le r_i < m_i$ при всех $\forall i = 1, \dots, k$ найдётся число N, которое при делении на m_i даёт остаток r_i при всех $\forall i = 1, \dots, k$.

Введем обозначение $M_i = \frac{M}{m_i}$, где M_i – произведение всех чисел, кроме m_i, m_i и M_i – взаимно простые. Тогда существуют u_i и v_i такие, что $m_i u_i + M_i v_i = 1$ (по теореме Безу). Домножим на r_i, получим $m_i u_i r_i + M_i v_i r_i = r_i$. Рассмотрим слагаемое $M_i v_i r_i$ (оно делится на все числа m_i): $M_i v_i r_i \ mod\, m_j = \begin{cases} 0, & j \neq i \\ r_i, & j = i \end{cases}$. $K = \left(\sum_{i=1}^{k} M_i v_i r_i\right) mod\, M$.

Рассмотрим процесс элиминации кванторов в рамках данной теории. $kx = \underbrace{x + x + \dots + x}_{k}$ – может быть реализовано умножение на константу. Возможные атомарные формулы: $(r < S)$, $(r = S)$, $D_m(r)$, $\neg(r < S)$, $\neg(r = S)$, $\neg D_m(r)$.

$$\neg(r = S) = (r < S) \vee (S < r), \qquad \neg(r < S) = (S < r + 1), \qquad (r = S) = (r < S + 1) \,\&\, (S - 1 < r),$$

$$D_m(r) = \bigvee_{i=1}^{m-1} D_m(r - i)$$

Осталось два типа формул $(r < S)$ и $D_m(r)$. Используем $\forall x[\dots \vee \dots] = \neg\exists[\neg \dots \&\neg \dots]$, $\exists[\dots \& \dots]$. Атомарные формулы называются $(kx < t)$ – ограничением сверху, $(t < kx)$ – ограничением снизу.

$(t_1 < k_1 x) \,\&\, (t_2 < k_2 x) = (t_1 k_2 < t_2 k_1) \,\&\, (t_2 < k_1 x) \vee (t_2 k_1 < t_1 k_2) \,\&\, (t_1 < k_1 x) \vee (t_1 k_2 = t_2 k_1) \,\&\, (t_1 < k_1 x)$, предполагается, что t_1 и t_2 – термы, не содержащие x. Необходимо отделить t.

$D_m(kx - t) = \bigvee_{i=0}^{m-1} D_m(kx - i) \,\&\, D_m(t - i)$. Под каждым квантором есть атомарная формула, в которой i – некоторое конкретное число. $D_m(kx - i) = \bigvee_{i=0}^{m-1} D_m(x - j) \,\&\, \underbrace{D_m(kj - i)}_{\text{всегда либо 0, либо 1}}$, где k – конкретное число, а j – неизвестное.

$D_m(x - i) = D_{q_1}(x - i) \,\&\, D_{q_2}(x - i) \,\&\, \dots \,\&\, D_{q_n}(x - i)$, $m = q_1 q_2 \dots q_n$, $q_i = p_j^j$, p_j – простое. Разложим m на простые множители. Пусть $D_{p^a}(x - i_1) \,\&\, D_{p^b}(x - i_2) = \underbrace{D_{p^a}(i_2 - i_1)}_{\text{всегда либо 0, либо 1}} \,\&\, D_{p^b}(x - i_2)$ и предположим, что $a \le b$,

тогда $D_{q_1}(x - i_1) \,\&\, D_{q_2}(x - i_2) \,\&\, \dots \,\&\, D_{q_k}(x - i_k) = D_Q(x - K)$, где $q_1, q_2, \dots, q_k$ – попарно взаимно простые числа,

$i_1, i_2, \dots, i_k$ – остатки, следовательно нужно найти число x, ведь по КТО найдется такое K, $K < Q = q_1, q_2, \dots, q_k$, $k \ mod \ q_j = i_j$.

Элементарный шаг элиминации применяем к одному из следующих видов:

$$\left.\begin{array}{c} \exists x(kx < t) \\ \exists x(t < kx) \\ \exists x D_m(x - i) \\ \exists x(kx < t) \ \ D_m(x - i) \\ \exists x(t < kx) \ \ D_m(x - i) \end{array}\right\} = 1$$

$$\exists x(k_1 x < t_1) \ \& \ (t_2 < k_2 x)$$

$$\exists x(k_1 x < t_1) \ \& \ (t_2 < k_2 x) \ \& \ D_m(x - i)$$

Рассмотрим последнее:

$$\exists x[(k_1 x < t_1) \ \& \ (t_2 < k_2 x) \ \& \ D_m(x - i)] = \exists x\big[(k_1 k_2 x < t_1 k_2) \ \& \ (k_1 t_2 < k_1 k_2 x) \ \& \ D_{k_1 k_2 m}(k_1 k_2 x - k_1 k_2 i)\big] \overset{x' = k_1 k_2 x}{=}$$

$$= \exists x'\big[(x' < t_1 k_2) \ \& \ (k_1 t_2 < x') \ \& \ D_{k_1 k_2 m}(x' - k_1 k_2 i)\big] \overset{M = k_1 k_2 m, \ \ k = k_1 k_2 i}{=}$$

$$= D_M(k_1 t_2 < k + 1) \ \& \ (k_1 t_2 + 1 < k_2 t_1) \vee D_m(k_1 t_2 - k + 2) \ \& \ (k_1 t_2 + 2 < k_2 t_1) \vee \dots$$

$$\vee D_m(k_1 t_2 - k + m) \ \& \ (k_1 t_2 + m < k_2 t_1)$$

Рассмотрим предпоследнее:

$$\exists x[(k_1 x < t_1) \ \& \ (t_2 < k_2 x)] = \exists x[(k_1 k_2 x < k_2 t_1) \ \& \ (k_1 t_2 < k_1 k_2 x)] \overset{x' = k_1 k_2 x}{=} \exists x'\big[(x' < k_2 t_1) \ \& (k_1 t_2 < x') \ \& D_{k_1 k_2}(x')\big]$$