Об эффективности алгоритмов машинного обучения для некоторых классов булевых функций

Архипова А. Н. (Москва, МГУ им. М. В. Ломоносова)

a.n.arkhipova@yandex.ru

В работе [1] рассматривается Probably Approximately Correct Model (PAC-модель) для изучения эффективности алгоритмов машинного обучения, в которой предполагается задание распределения на множестве примеров и целью познающего является нахождение гипотезы, аппроксимирующей целевую функцию с заранее заданной точностью. В работе доказывается неэффективность работы алгоритма Персептрон на классе линейных пороговых функций и эффективность на классе вложенных функций. При доказательстве первого факта использовались определение и свойства функции Хастада, построение которой можно найти в статье [2].

Таким образом, косвенно утверждается непринадлежность функции Хастада классу вложенных функций. В данной работе получено прямое доказательство данного факта.

Утверждение 1. *$F(f)$ — функция Хастада не лежит в множестве NF_n, где NF_n — множество вложенных функций от n переменных, $n = 2^m$, $m \geqslant 3$.*

Использование класса пороговых функций для определения эффективности работы различных алгоритмов приводит к необходимости изучения некотрых их свойств и взаимосвязей.

Пусть

$$\rho^{'}(f^{'}, f^{''}) = \min_{l_{\vec{\omega}^{'},\sigma^{'}} \to f^{'}, l_{\vec{\omega}^{''},\sigma^{''}} \to f^{''}} \rho(l^{'}, l^{''}),$$

где $l_{\vec{\omega},\sigma} \to f(x_1, \ldots, x_n)$ — линейная форма, задающая пороговую функцию f (линейной формой называется функция вида $l_{\vec{\omega},\sigma}(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i\omega_i - \sigma, \omega_i \in Z, i = 1, \ldots, n; \sigma \in Z$).

Утверждение 2. *Для любой тройки функций вида*

$$f_1 : x_1 + 2x_2 + 4x_3 + \ldots + 2^{i-1}x_i \geqslant \sum_{j=1}^{i-1} 2^{j-1}, i \geqslant 4,$$

$$f_2 : x_1 \geqslant 1,$$

$$f_3 : x_i \geqslant 1$$

нарушается неравенство треугольника для функции ρ'*, то есть*

$$\rho'(f', f'') > \rho'(f', f''') + \rho'(f'', f''').$$

Благодарю моего научного руководителя Ирматова Анвара Адхамовича за ценные рекомендации и советы.

Список литературы

[1] Servedio R. A. On PAC Learning Using Winnow, Perceptron and a Perceptron-Like Algorithm.

[2] Hastad J. On the size of weigts for threshold gates.

О конечной порожденности исчисления высказываний с произвольными операциями вывода

Боков Г. В. (Москва, МГУ им. М. В. Ломоносова)

bokovgrigoriy@gmail.com

Важным свойством классического исчисления высказываний [1] является существование конечного множества аксиом, из которых выводимы все тавтологии этого исчисления. Данное свойство называют конечно-порожденностью исчисления. При расширении понятия исчисления обычно требуется, чтобы данное свойство сохранялось. Так в 1949 г. Л. Хенкин [2] показал, что расширенный фрагмент исчисления высказываний, содержащий классическую импликацию, конечно-порожден относительной операции *modus ponens*: если выводимо A и $A \to B$, то B выводимо. В данной работе вводиться в рассмотрение расширенный фрагмент исчисления высказываний с произвольными модусными операциями [3] и доказываются необходимые и достаточные условия конечно-порожденности такого исчисления.

Пусть A — некоторое множество и $U = \{u_1, u_2, \ldots, u_n, \ldots\}$ — счетный алфавит переменных u_n, значениями которых являются элементы a из A. Обозначим через P_A множество всех функций $f(u_{i_1}, \ldots, u_{i_n})$ со значениями в A, где $i_j < i_{j'}$ при $j < j'$, $j, j' = 1, \ldots, n$, $n \in \mathbb{N}$. Эти функции являются отображениями вида $f : A^n \to A$, где $A^n = \underbrace{A \times \ldots \times A}_{n}$. Такие функции иногда называют функциями $|A|$-значной логики.

Множество переменных U будем интерпретировать, как переменные высказывания, а множество A — как значения, которые могут принимать высказывания. В такой интерпретации функции из множества P_A можно рассматривать как логические связки над высказываниями. Если $|A| = 2$, то элементами множества A будут 1 и 0, которые интерпретируются стандартным образом, как истина и ложь. Для произвольного множества A обобщим понятие истины и лжи следующим образом. Пусть ρ — произвольный предикат на A, то есть отображение $\rho : A \to E_2$, где $E_2 = \{0, 1\}$. Тогда множество $\mathbb{T} = \{a \in A \mid \rho(a) = 1\}$ будем интерпретировать, как множество истинных значений, а множество $\mathbb{F} = \{a \in A \mid \rho(a) = 0\}$ — как мно-

жество ложный значений. Пару $(\mathbb{T}, \mathbb{F})$, порожденную предикатом ρ, будем называть *истинностным разбиением* множества A.

Каждый предикат ρ порождает естественный гомоморфизм nat_ρ множества P_A в множество всех функций двузначной логики P_2 [4]. Этот гомоморфизм каждой функции $f(x_1, \ldots, x_n)$ из P_A сопоставляет такую функцию $f_\rho(x_1, \ldots, x_n)$ из P_2, что для любого набора $\langle \sigma_1, \ldots, \sigma_n \rangle \in E_2^n$ и любого $\sigma_0 \in E_2$ выполнено

$$f_\rho(\sigma_1, \ldots, \sigma_n) = \sigma_0 \Leftrightarrow f(\hat{\sigma}_1, \ldots, \hat{\sigma}_n) \subseteq \hat{\sigma}_0,$$

где $\hat{\sigma}_i = \mathbb{T}$, при $\sigma_i = 1$, и $\hat{\sigma}_i = \mathbb{F}$, при $\sigma_i = 0$, $i = 0, 1, \ldots, n$.

Пусть $\Sigma \subseteq P_A$ — конечное множество функций и $X \subseteq U$ — множество переменных, тогда обозначим через $\Phi_\Sigma(X)$ множество всех формул над логическими связками из Σ и множеством переменных X. Когда $X = U$ множество $\Phi_\Sigma(X)$ будем для краткости обозначать через Φ_Σ. Каждой формуле $\mathfrak{F} \in \Phi_\Sigma$ можно однозначно сопоставить функцию $f_\mathfrak{F} \in P_A$ [4]. В этом случае говорят, что формула $\mathfrak{F}$ выражает функцию $f_\mathfrak{F}$. Формулу $\mathfrak{F}$ из Φ_Σ будем называть *тавтологией*, то есть тождественно истинной, относительно истинностного разбиения $(\mathbb{T}, \mathbb{F})$, если $f_\mathfrak{F}(i_1, \ldots, i_m) \in \mathbb{T}$, при любых значениях $i_1, \ldots, i_m$ из A, где m — это арность функции $f_\mathfrak{F}$. Обозначим через Th множество всех тавтологий в Φ_Σ.

Определим понятие модусной операции. Пусть $\mathfrak{F}_0, \mathfrak{F}_1, \ldots, \mathfrak{F}_m$ различные формулы из $\Phi_\Sigma(\{x_1, \ldots, x_n\})$, тогда набор $\langle \mathfrak{F}_1, \ldots, \mathfrak{F}_m; \mathfrak{F}_0 \rangle$ задает модусную операцию на Φ_Σ, определенную схемой:

$$\frac{\mathfrak{F}_1(x_1, \ldots, x_n), \ldots, \mathfrak{F}_m(x_1, \ldots, x_n)}{\mathfrak{F}_0(x_1, \ldots, x_n)}.$$

Классическим примером модусной операци является операция *modus ponens*:

$$\frac{x_1, x_1 \to x_2}{x_2}.$$

Множество всех модусных операций на Φ_Σ обозначим через $\mathcal{M}_\Sigma$. Нас будут интересовать не все модусные операции, а лишь те $\omega \in \mathcal{M}_\Sigma$, которые тавтологии переводят в тавтологии $\omega : \mathrm{Th} \to \mathrm{Th}$. Такие операции назовем допустимыми [5] на Th. Множество всех допустимых на Th операций обозначим через O_{Th}.

Множество тавтологий Th и множеств допустимых на Th операций $\Omega \subseteq O_{\mathrm{Th}}$ образуют алгебраическую систему (Th, Ω), которую будем называть *исчислением высказываний*.

Пусть $\Omega \subseteq O_{\mathrm{Th}}$ — произвольное множество допустимых на Th модусных операций, тогда на Th можно определить оператор замыкания, порожденный операциями из Ω [6]. Этот оператор будем обозначать через $[\cdot]_\Omega$. Для произвольного $M \subseteq \mathrm{Th}$ и $\mathfrak{A} \in \mathrm{Th}$ формулу $\mathfrak{A} \in [M]_\Omega$ назовем выводимой из множества формул M и обозначим это через $M \vdash_\Omega \mathfrak{A}$. Множество тавтологий Th будем называть конечно-порожденным относительно множества операций Ω, если существует такое конечное множество $M \subseteq \mathrm{Th}$, что $[M]_\Omega = \mathrm{Th}$. Исчисление высказываний (Th, Ω) конечно-порождено, если множество Th конечно-порождено относительно множества операций Ω.

Пусть $X \subseteq U$ некоторое множество переменных, тогда обозначим через $\mathcal{M}_\Sigma(X) \subseteq \mathcal{M}_\Sigma$ множество всех операций над переменными из X:

$$\mathcal{M}_\Sigma(X) = \{\omega \in \mathcal{M}_\Sigma \mid \omega = \langle \mathfrak{F}_1, \ldots, \mathfrak{F}_m; \mathfrak{F}_0 \rangle, \mathfrak{F}_i \in \Phi_\Sigma(X),\ i = 0, 1, \ldots, m\}.$$

Будем говорить, что операция $\omega = \langle \mathfrak{F}_1, \ldots, \mathfrak{F}_m; \mathfrak{F}_0 \rangle \in \mathcal{M}_\Sigma(\{x_1, \ldots, x_n\})$ выводима из множества операций $\Omega \subseteq \mathcal{M}_\Sigma$, если существует такое конечное множество тавтологий $M \subseteq \mathrm{Th}$, что для любых формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{B}_1, \ldots, \mathfrak{B}_m \in \Phi_\Sigma$ из выполнения условия $\mathfrak{B}_i = \mathfrak{F}_i(\mathfrak{A}_1, \ldots, \mathfrak{A}_n) \in \mathrm{Th}, i = 1, \ldots, m$ следует выводимость

$$M,\ \mathfrak{B}_1, \ldots, \mathfrak{B}_n \vdash_\Omega \mathfrak{F}_0(\mathfrak{A}_1, \ldots, \mathfrak{A}_n).$$

Выводимость операции ω из множества операций Ω обозначим через $\Omega \vdash \omega$.

Определим несколько классов функций. Функцию $f(x_1, \ldots, x_n) \in P_A$ назовем *линейной* (*монотонной*) относительно предиката ρ, если $f_\rho = \mathrm{nat}_\rho(f) \in P_2$ является линейной (монотонной) булевской функцией. Множество всех линейных и монотонных относительно ρ функций в P_A обозначим соответственно через L_ρ и M_ρ. Функцию $f(x_1, \ldots, x_n, y) \in P_A$ назовем *импликативной* относительно предиката ρ, если для функции $f_\rho = \mathrm{nat}_\rho(f) \in P_2$ выполнено

$$f_\rho(\sigma_1, \ldots, \sigma_n, \sigma_0) = 0 \Leftrightarrow \sigma_0 < \sigma_i,\ i = 1, \ldots, n,$$

где $\sigma_i \in E_2$. Множество всех импликативных относительно ρ функций в P_A обозначим через I_ρ.

Теорема. *Для любого множества A, любого предиката ρ на A и каждого конечного множества логических связок $\Sigma \subseteq P_A$ существуют такие конечные множества допустимых на* Th *операций $\Omega_L(\Sigma),\ \Omega_M(\Sigma),\ \Omega_I(f),\ f \in \Sigma$, что для произвольного конечного множества операций $\Omega \subseteq O_{\mathrm{Th}}$ исчисление (Th, Ω) конечно-порождено тогда и только тогда, когда выполнено хотя бы одно из условий*

1. $\Sigma \subseteq L_\rho,\ 1 \in [nat_\rho(\Sigma)]$ *и* $\Omega \vdash \Omega_L(\Sigma)$;
2. $\Sigma \subseteq M_\rho,\ 1 \in [nat_\rho(\Sigma)]$ *и* $\Omega \vdash \Omega_M(\Sigma)$;
3. *Найдется такая функция* $f \in [\Sigma] \cap I_\rho$, *что* $\Omega \vdash \Omega_I(f)$;
3. $\mathrm{Th} = \varnothing$.

Список литературы

[1] Новиков П. С. Элементы математической логики. — М.: Наука, 1973.

[2] Henkin L. Fragments of the propositional calculus // J. Symb. Logic. — 1949. 14. — P. 42–82.

[3] Циткин А. И. О допустимых правилах интуиционистской логики высказываний // Матем. сб. — 1977. 102 (144): 2.

[4] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

[5] Минц Г. Е. Допустимые и производные правила // Записки научных семинаров ЛОМИ АН СССР. — 1968. 8. — С. 189–191.

[6] Кон П. Универсальная алгебра. — М.: Мир, 1968.

Об алгоритмической неразрешимости проблемы выразимости пропозициональных исчислений

Боков Г. В. (Москва, МГУ им. М. В. Ломоносова)

bokovgrigoriy@gmail.com

В работе рассматривается проблема выразимости и полноты пропозициональных исчислений с модусными операциями вывода с точки зрения их алгоритмической неразрешимости. Доказаны достаточные условия алгоритмической неразрешимости проблемы выразимости пропозициональных исчислений с одной модусной операцией вывода. Для случая конечнопорожденных исчислений с одной модусной операцией вывода получены достаточные условия алгоритмической неразрешимости проблемы полноты.

1. Введение

Проблема выразимости пропозициональных исчислений впервые была поставлена Тарским в 1946 году на конференции по проблемам математики, посвященной двухсотлетию Принстонского университета [16]. Пусть Th некоторое множество формул, которое назовем тавтологиями, и Ω — конечное множество допустимых правил над тавтологиями. Пара (Th, Ω) образует исчисление. Проблема выразимости состоит в описании всех таких пар (L, M) конечных подмножеств Th, для которых все формулы множества M можно выразить из формул множества L посредством правил Ω [4].

В 1949 году Линиал и Пост [14] опубликовали короткую заметку, в которой без доказательства сформулировали гипотезу об алгоритмической неразрешимости проблемы полноты для классического исчисления высказываний над связками $\{\vee,\ \neg\}$ с единственной операций:

$$\frac{\overline{x},\ x \vee y}{y}.$$

Доказательство данного результата постепенно было восстановлено последующими авторами. Первым в этом направлении был Дэвис [11], который в 1958 году опубликовал первый вариант доказательства теоремы Линиала и Поста, далее в 1963 году Синглетари [15]

и в 1964 — Интема [17] завершили доказательство. Следует отметить, что они использовали эквивалентную систему связок $\{\rightarrow,\ \neg\}$ и обычную операцию *modus ponens*. Независимо от них в 1958 году Харроп [13] построил конечную систему аксиом над бинарными связки $\{\circ,\ \rightarrow\}$ и конечное множество правил вывода, для которых проблема выразимости алгоритмически неразрешима.

В 1963 году Глэдстоун [12] обобщил результат Линиала и Поста на случай произвольной конечной системы связок, из которых выразима импликация. Для этого он рассмотрел операцию аналог *modus ponens*:

$$\frac{x,\ F_{\rightarrow}(x,y)}{y},$$

где $F_{\rightarrow}(x,y)$ — формула, выражающая импликацию, и показал, что существует конечное множество аксиом, для которых проблема выразимости алгоритмически неразрешима.

Независимо от результата Линиала и Поста в том же 1963 году Кузнецов [5] доказал алгоритмическую неразрешимость целого класса задач для исчислений высказываний с операцией *modus ponens*, куда входит проблема эквивалентности, проблема полноты и выразимости. В отличии от других авторов, которые в основном использовали для доказательства алгоритмической неразрешимости однородные продукции Поста, Кузнецов свел поставленные алгоритмические проблемы исчисления высказываний к вопросу рекурсивной отделимости двух множеств тавтологий.

В 2009 автором работы независимо от Глэдстоуна, Синглетари и Интема была доказана теорема Линиала и Поста для тавтологий над связками $\{\&,\ \vee,\ \rightarrow,\ \neg\}$ с операцией *modus ponens* [1].

2. Основные понятия

Пусть $E_2 = \{0, 1\}$. Через P_2 обозначим множество всех булевских функций [10]. Элементы множества P_2 будем обозначать прописными латинскими буквами $f, g, h, \ldots$, возможно, с индексами. Число существенных переменных функции $f \in P_2$ обозначим через $\varkappa(f)$. На множестве P_2 определим оператор замыкания $[\cdot]$, порожденный операцией суперпозиции [10]. Множество $Q \subseteq P_2$ — замкнуто, если $[Q] = Q$.

Будем считать, что имеется некоторый счетный универсум переменных $\mathcal{U}$, элементы которого будем обозначать прописными латинскими буквами $x, y, z, \ldots$, возможно, с индексами. Если множество переменных $\mathcal{U}$ интерпретировать, как переменные высказывания, принимающие только значения истина и ложь, то функции из P_2 можно рассматривать как логические связки над данными переменными. Определим понятие формулы. Пусть $\Sigma \subseteq P_2$ — конечное множество функций и $X \subseteq \mathcal{U}$ — некоторое множество переменных, тогда формулой над логическими связками из Σ и множеством переменных X назовем слово (конечную последовательность) в алфавите $\Sigma \cup X$, которое определяется следующим образом. Слово $x \in X$ является формулой. Если слова $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ — формулы и $f \in \Sigma$ — логическая связка арности n, тогда слово $f\mathfrak{A}_1 \ldots \mathfrak{A}_n$ является формулой. Обозначим через $\Phi_\Sigma(X)$ множество всех формул над логическими связками из Σ и множеством переменных X. Когда $X = \mathcal{U}$ множество $\Phi_\Sigma(X)$ будем для краткости обозначать через Φ_Σ. Элементы множества Φ_Σ будем обозначать строчными готическими буквами $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$, возможно, с индексами. Под равенством формул из $\Phi_\Sigma(X)$ будем понимать равенство соответствующих слов в алфавите $\Sigma \cup X$.

Формула $\mathfrak{A} \in \Phi_\Sigma(X)$ является подформулой формулы $\mathfrak{B} \in \Phi_\Sigma(X)$, если найдутся такие слова $\alpha_1, \alpha_2 \in (\Sigma \cup X)^*$, что $\mathfrak{B} = \alpha_1 \mathfrak{A} \alpha_2$. Собственными будем называть такие подформулы $\mathfrak{A}$ формулы $\mathfrak{B}$, для которых $\mathfrak{A}$ не совпадает с $\mathfrak{B}$. Определим понятие глубины подформулы $\mathfrak{A} \in \Phi_\Sigma(X)$ формулы $\mathfrak{B} \in \Phi_\Sigma(X)$. Если $\mathfrak{A}$ совпадает с $\mathfrak{B}$, то глубина $\mathfrak{A}$ равна нулю. Пусть $\mathfrak{A}$ собственная подформула в $\mathfrak{B}$ и $\mathfrak{C}$ — минимальная подформула в $\mathfrak{B}$, для которой $\mathfrak{A}$ является собственной подформулой, тогда, если глубина $\mathfrak{C}$ равна $n \in \mathbb{N}$, то глубина $\mathfrak{A}$ равна $n + 1$. Глубину подформулы $\mathfrak{A}$ формулы $\mathfrak{B}$ будем обозначать через $d_{\mathfrak{B}}(\mathfrak{A})$.

Будем говорить, что формула $\mathfrak{A} \in \Phi_\Sigma$ зависит от переменного $x \in \mathcal{U}$, если x является подформулой в $\mathfrak{A}$. Зависимость формулы $\mathfrak{A}$ от переменной x обозначим через $\mathfrak{A}(x)$, зависимость от переменных $x_1, \ldots, x_n$ — через $\mathfrak{A}(x_1, \ldots, x_n)$.

Каждой формуле $\mathfrak{F} \in \Phi_\Sigma$ однозначно сопоставим функцию из $[\Sigma \cup \{x\}]$ [10], где $x \in P_2$ — тождественная функция. Поскольку каждую логическую связку из Σ можно интерпретировать как соот-

ветствующую ей функцию, то по аналогии с определением формулы можно определить понятие *интерпретации формулы*. Каждая переменная задает тождественную функцию из P_2, которую будем обозначать тем же символом; если формулам $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$ уже сопоставлены функции $f_1, \ldots, f_m$, то формуле $f\mathfrak{A}_1 \ldots \mathfrak{A}_m$ сопоставим функцию g равную функции $f(f_1, \ldots, f_m)$. Итак, каждой формуле $\mathfrak{F}$ из Φ_Σ можно сопоставить функцию из P_2, которую будем обозначать через $f_\mathfrak{F}$. В этом случае будем говорить, что формула $\mathfrak{F}$ выражает функцию $f_\mathfrak{F}$.

Формулу $\mathfrak{F}$ из Φ_Σ будем называть *тавтологией* или тождественно истинной, если $f_\mathfrak{F}(i_1, \ldots, i_m) = 1$, при любых значениях $i_1, \ldots, i_m$ из E_2, где m — это арность функции $f_\mathfrak{F}$. Обозначим через Th множество всех тавтологий в Φ_Σ:

$$\mathrm{Th} = \{\mathfrak{F} \in \Phi_\Sigma \mid f_\mathfrak{F} \equiv 1\}.$$

На множестве формул Φ_Σ определим понятие модусной операции [8]. Пусть $\mathfrak{F}_0, \mathfrak{F}_1, \ldots, \mathfrak{F}_m$ различные формулы из $\Phi_\Sigma(\{x_1, \ldots, x_n\})$, тогда набор $\langle \mathfrak{F}_1, \ldots, \mathfrak{F}_m; \mathfrak{F}_0 \rangle$ задает операцию $\omega : \Phi_\Sigma^m \to \Phi_\Sigma$, определенную следующим образом:

$$\omega(\xi_1, \ldots, \xi_m) = \xi_0 \Leftrightarrow \exists x_1, \ldots, x_n \in \Phi_\Sigma \left(\bigwedge_{i=0}^{m} \xi_i = \mathfrak{F}_i(x_1, \ldots, x_n) \right),$$

где $\xi_0, \xi_1, \ldots, \xi_m \in \Phi_\Sigma$. Обозначим правую часть условия через $R_\omega(\xi_0, \xi_1, \ldots, \xi_m)$, тогда операцию ω можно записать в виде λ-функции [9]:

$$\omega(\xi_1, \ldots, \xi_m) = \lambda_{\xi_1, \ldots, \xi_m}\big(\xi_0 \mid R_\omega(\xi_0, \xi_1, \ldots, \xi_m)\big).$$

Следуя [2, 8] такие операции будем обозначать в виде схемы:

$$\frac{\mathfrak{F}_1(x_1, \ldots, x_n), \ldots, \mathfrak{F}_m(x_1, \ldots, x_n)}{\mathfrak{F}_0(x_1, \ldots, x_n)}.$$

Классическим примером модусной операци является операция *modus ponens*:

$$\frac{x_1, x_1 \to x_2}{x_2}.$$

Множество всех модусных операций на Φ_Σ обозначим через $\mathcal{M}_\Sigma$. Элементы множества $\mathcal{M}_\Sigma$ будем обозначать прописной греческой буквой ω, а множества элементов из $\mathcal{M}_\Sigma$ — строчной греческой буквой Ω, возможно, с индексами.

Нас будут интересовать не все модусные операции, а лишь те $\omega \in \mathcal{M}_\Sigma$, которые тавтологии переводят в тавтологии $\omega : \mathrm{Th} \to \mathrm{Th}$. Такие операции назовем допустимыми [7] на Th. Множество всех допустимых на Th операций обозначим через O_{Th}.

Кроме того определим на множестве Th операцию подстановки. Пусть $\mathfrak{A}$ — тавтология, содержащая переменное высказывание x, а $\mathfrak{B}$ — произвольная формула из Φ_Σ. Тогда, если заменить в $\mathfrak{A}$ все вхождения x на $\mathfrak{B}$, то полученная формула $\mathfrak{A}(\mathfrak{B})$ тоже будет тавтологией. В этом случае будем говорить, что из $\mathfrak{A}$ выводима $\mathfrak{A}(\mathfrak{B})$. Операцию будем записывать в виде схемы:

$$\frac{\mathfrak{A}(x)}{\mathfrak{A}(\mathfrak{B})}.$$

Данную операцию можно опустить, если предполагать, что каждая тавтология задает не одну, а множество формул, получающихся из данной применением операции подстановки к всевозможных переменным данной тавтологии. Пользуясь свойством перестановочности операции подстановки относительно любой модусной операции, далее будем опускать явное применение операции подстановки.

Множество тавтологий Th и множество допустимых операций Ω образуют алгебраическую систему (Th, Ω), которую будем называть пропозициональным исчислением. Пусть $\Omega \subseteq O_{\mathrm{Th}}$ — произвольное множество допустимых на Th модусных операций, тогда на Th можно определить оператор замыкания, порожденный операциями из Ω [3]. Этот оператор будем обозначать через $[\cdot]_\Omega$ или просто через $[\cdot]$, когда множество Ω фиксировано[1].

Несложно проверить, что для любого множество модусных операций $\Omega \subseteq \mathcal{M}_\Sigma$ оператор $[\cdot]_\Omega$ является алгебраических операторо замыкания [3].

[1]Во избежание увеличения количества обозначений, операторы замыкания для множеств различной природы имеют одно и тоже обозначение $[\cdot]$.

Множество тавтологий $M \subseteq \mathrm{Th}$ называется замкнутым относительно множества операций Ω, если $[M]_\Omega = M$ и полным, если $[M]_\Omega = \mathrm{Th}$. Для произвольного $M \subseteq \mathrm{Th}$ и $\mathfrak{A} \in \mathrm{Th}$ формулу $\mathfrak{A} \in [M]_\Omega$ назовем выводимой из множества формул M и будем обозначать это через $M \vdash_\Omega \mathfrak{A}$ или просто через $M \vdash \mathfrak{A}$, если множество Ω фиксировано. Множество тавтологий Th будем называть конечно-порожденным относительно множества операций Ω, если существует такое конечное множество $M \subseteq \mathrm{Th}$, что $[M]_\Omega = \mathrm{Th}$. Исчисление высказываний (Th, Ω) конечно-порождено, если множество Th конечно-порождено относительно множества операций Ω.

Каждую формулу из Φ_Σ можно представлять в виде ориентированного дерева, листьям которого приписаны переменные из $\mathcal{U}$, а внутренним вершинам — элементы множества Σ. Каждой позиции в этом дереве соответствует, с одной стороны, элемент множества $\Sigma \cup \mathcal{U}$, с другой — подформула из Φ_Σ. Введем функции ψ и η для задания соответственно символа и подформулы данной формулы в данной позиции. Позиции в формуле будем задавать словами над множеством $\mathbb{N}$.

Отображение ψ сопоставляет каждой формуле $\mathfrak{F} \in \Phi_\Sigma$ отображение $\psi_\mathfrak{F} : \mathbb{N}^* \to \Sigma \cup \mathcal{U} \cup \{\bot\}$, где $\bot$ — символ, не принадлежащий $\Sigma \cup \mathcal{U}$. Если $\mathfrak{F} \in \mathcal{U}$, то

$$\psi_\mathfrak{F}(\alpha) = \begin{cases} \mathfrak{F}, & \text{если } \alpha = \Lambda, \\ \bot, & \text{иначе.} \end{cases}$$

Если $\mathfrak{F} = f(\mathfrak{F}_1, \ldots, \mathfrak{F}_k)$, то

$$\psi_\mathfrak{F}(\alpha) = \begin{cases} f, & \text{если } \alpha = \Lambda, \\ \psi_{\mathfrak{F}_i}(\beta), & \text{если } \alpha = i\beta,\ 1 \leqslant i \leqslant k, \\ \bot, & \text{иначе.} \end{cases}$$

Отображение η сопоставляет каждой формуле $\mathfrak{F} \in \Phi_\Sigma$ отображение $\eta_\mathfrak{F} : \mathbb{N}^* \to \Phi_\Sigma \cup \{\bot\}$. Если $\mathfrak{F} \in \mathcal{U}$, то

$$\eta_\mathfrak{F}(\alpha) = \begin{cases} \mathfrak{F}, & \text{если } \alpha = \Lambda, \\ \bot, & \text{иначе.} \end{cases}$$

Если $\mathfrak{F} = f(\mathfrak{F}_1, \ldots, \mathfrak{F}_k)$, то

$$\eta_{\mathfrak{F}}(\alpha) = \begin{cases} \mathfrak{F}, & \text{если } \alpha = \Lambda, \\ \psi_{\mathfrak{F}_i}(\beta), & \text{если } \alpha = i\beta,\ 1 \leqslant i \leqslant k, \\ \perp, & \text{иначе.} \end{cases}$$

Несложно заметить, что отображения ψ и η связаны соотношением. Для любой формулы $\mathfrak{F} \in \Phi_\Sigma$ и любого слова $\alpha \in \mathbb{N}^*$ выполнено $\psi_{\mathfrak{F}}(\alpha) = \psi_{\eta_{\mathfrak{F}}(\alpha)}(\Lambda)$.

Введем на множестве формул Φ_Σ отношение $\leqslant$. Пусть $\mathfrak{A} \in \Phi_\Sigma(\{x_1, \ldots, x_n\})$ и $\mathfrak{B} \in \Phi_\Sigma$, тогда положим

$$\mathfrak{A} \leqslant \mathfrak{B} \rightleftharpoons \exists C_1, \ldots, C_n \in \Phi_\Sigma\Big(\mathfrak{A}(C_1, \ldots, C_n) = \mathfrak{B}\Big).$$

Следует сделать несколько замечаний по поводу отношения $\leqslant$. Если формула $\mathfrak{B}$ получена из формулы $\mathfrak{A}$ с помощью операции подстановки, то $\mathfrak{A} \leqslant \mathfrak{B}$. В ряде последующих утверждений данной работы возникнет необходимость в выделении из конкретного множества тавтологий тех тавтологий, которые являются в некотором плане минимальными относительно $\leqslant$. Легко заметить, что множество тавтологий Th не содержит минимальных элементов, поскольку любая тавтология сравнима с формулой, полученной из данной переименованием переменных без отождествления. Назовем такие формулы эквивалентными. Поскольку исходное множество переменных $\mathcal{U}$ счетное, то каждая тавтология имеет счетное число эквивалентных ей тавтологий. Формула, полученная из данной переименованием переменных без отождествления, всегда из нее выводится с помощью операции подстановки и наоборот, поэтому далее будем предполагать, что мы работаем не с конкретной тавтологией, а с целым классом тавтологий, эквивалентных данной.

Формулы $\mathfrak{A}, \mathfrak{B} \in \Phi_\Sigma(\{x_1, \ldots, x_n\})$ будем называть совместными и писать $\mathfrak{A} \simeq \mathfrak{B}$, если существуют такие $C_1, \ldots, C_n, D_1, \ldots, D_n \in \Phi_\Sigma$, что

$$\mathfrak{A}(C_1, \ldots, C_n) \equiv \mathfrak{B}(D_1, \ldots, D_n).$$

Множество формул $M \subseteq \Phi_\Sigma(X)$ назовем разрешимым в тавтологиях, если существует такое отображение $\sigma : X \to \Phi_\Sigma$, что для любой формулы $\mathfrak{F} \in M$ выполнено $\sigma\mathfrak{F} \in \mathrm{Th}$.

Пусть $M \subseteq \Phi_\Sigma(X)$ и $\mathfrak{F}_i, \mathfrak{G}_i \in \Phi_\Sigma(X),\ i = 1, \ldots, k,\ k \geqslant 1$. Рассмотрим систему уравнений

$$M \vDash \begin{cases} \mathfrak{F}_1 = \mathfrak{G}_1 \\ \quad \ldots \\ \mathfrak{F}_m = \mathfrak{G}_m \end{cases} \qquad (*)$$

Множество формул M в уравнении играет роль области определения. Решением уравнения (*) будем называть такое отображение $\sigma\colon X \to \Phi_\Sigma$, которое будем называть подстановкой, что множество формул $\sigma M = \{\sigma\mathfrak{F} \mid \mathfrak{F} \in M\}$ разрешимо в тавтологиях и для каждого $i = 1, \ldots, k$ выполнено тождество $\sigma\mathfrak{F}_i \equiv \mathfrak{G}_i$, где $\equiv$ означает синтаксическое совпадение формул. Система (*) разрешима, если она имеет решение.

Рассмотрим произвольную модусную операцию $\omega = \langle \mathfrak{F}_1, ..., \mathfrak{F}_m; \mathfrak{F}_0 \rangle$, где $\mathfrak{F}_i \in \Phi_\Sigma(X^n),\ i = 1, \ldots, m$, и $X^n = \{x_1, \ldots, x_n\}$, которая задается соотношением:

$$\omega(\xi_1, \ldots, \xi_m) = \xi_0 \rightleftharpoons \exists x_1, \ldots, x_n \in \Phi_\Sigma \left(\bigwedge_{i=0}^{m} \xi_i = \mathfrak{F}_i(x_1, \ldots, x_n) \right).$$

Разрешающим уравнением аргумента ξ_p операции $\omega(\xi_1, \ldots, \xi_m)$ будем называть уравнение:

$$\mathfrak{F}_1, \ldots, \mathfrak{F}_m \vDash \mathfrak{F}_0 = \mathfrak{F}_p.$$

Обозначим его через $\mathcal{E}_p$.

Разрешающим графом аргумента ξ_p операции $\omega(\xi_1, \ldots, \xi_m)$ назовем граф $G_p = (V_p, E_p)$, где $V_p \subseteq X_n \times \mathbb{N}^l$, где $l \in \mathbb{N}$ такое максимальное число, для которого существует такое слово $\alpha \in \mathbb{N}^l$, что либо $\psi_{\mathfrak{F}_0}(\alpha) \neq \perp$, либо $\psi_{\mathfrak{F}_p}(\alpha) \neq \perp$. Определим множества V_p и E_p следующим образом. Пара $(x, \alpha) \in V_p$ тогда и только тогда, когда найдется такое слово β, для которого либо $\psi_{\mathfrak{F}_0}(\beta\alpha) = x$ и $\psi_{\mathfrak{F}_p}(\beta) \in X^n$, либо $\psi_{\mathfrak{F}_0}(\beta) \in X^n$ и $\psi_{\mathfrak{F}_p}(\beta\alpha) = x$. Пара $\big((x, \alpha), (y, \beta)\big) \in E_p$ тогда и только тогда, когда найдется такое слово γ, что либо $\alpha = \Lambda$ и тогда $\psi_{\mathfrak{F}_0}(\gamma) = x,\ \psi_{\mathfrak{F}_p}(\gamma\beta) = y$, либо $\beta = \Lambda$ и тогда $\psi_{\mathfrak{F}_0}(\gamma\alpha) = x,\ \psi_{\mathfrak{F}_p}(\gamma) = y$.

Определим отношение эквивалентности $\sim_p$ на множестве вершин V_p разрешающего графа G_p. Отношение $\sim_p$ строится конструктивно. Для каждого $(x,\alpha) \in V_p$ положим $(x,\alpha) \sim_p (x,\alpha)$, а для $(x,\alpha),\ (y,\beta) \in V_p$ положим $(x,\alpha) \sim_p (y,\beta)$ тогда и только тогда, когда найдутся такие эквивалентные вершины $(x',\alpha'),\ (y',\beta') \in V_p$, что либо $\big((x',\alpha'),(x,\alpha)\big),\ \big((y',\beta'),(y,\beta)\big) \in E_p$, либо $\big((x,\alpha),(x',\alpha')\big),\ \big((y,\beta),(y',\beta')\big) \in E_p$. Не сложно проверить, что эквивалентные вершины принадлежат одной связной компоненте графа G_p.

Аргумент ξ_p операции $\omega(\xi_1,\dots,\xi_m)$ будем называть перестановочным, если его разрешающее уравнение $\mathcal{E}_p$ имеет решение и найдутся такие неэквивалентные вершины $(x,\alpha),(y,\beta) \in V_p$ разрешающего графа G_p из одной ациклической компоненты связности, такие различные переменные $z_1,\dots,z_{q-1} \in X^n$, не принадлежащие $\mathfrak{F}_0$ и $\mathfrak{F}_p$, и такие различные $i_1,\dots,i_q \in \overline{m} \setminus \{p\}$, что

$$x, z_1 \in \mathfrak{F}_{i_1};\ z_1, z_2 \in \mathfrak{F}_{i_2};\ \dots\ z_{q-1}, y \in \mathfrak{F}_{i_q}.$$

Расширением операции $\omega = \langle \mathfrak{F}_1,\dots,\mathfrak{F}_m;\mathfrak{F}_0\rangle$, где $\mathfrak{F}_i \in \Phi_\Sigma(X),\ i = 1,\dots,m$, назовем всякую операцию $\omega' = \langle \mathfrak{G}_1,\dots,\mathfrak{G}_{m'};\mathfrak{G}_0\rangle$, для которой $\mathfrak{G}_1,\dots,\mathfrak{G}_{m'}$ разрешимы в тавтологиях, $\mathfrak{G}_i \not\equiv \mathfrak{G}_j$ для любых $1 \leqslant i < j \leqslant m$ и существует такая подстановка $\sigma : X \to \Phi_\Sigma$, что $\mathfrak{G}_0 \equiv \sigma\mathfrak{F}_0$ и для каждого $i \in \overline{m'}$ найдется такое $j \in \overline{m}$, что $\mathfrak{G}_i \equiv \mathfrak{F}_j$. Расширение ω' будем называть собственным, если для всякого множества тавтологий $M = \{\mathfrak{A} \in \mathrm{Th} \mid \exists i,\ 0 \leqslant i \leqslant m',\ \mathfrak{G}_i \leqslant \mathfrak{A}\}$ замыкания $[M]_{\{\omega\}}$ и $[M]_{\{\omega'\}}$ совпадают.

3. Алгоритмическая неразрешимость проблемы выразимости

Теорема 1. *Если $[\Sigma] = P_2$ и существует собственное расширение операции $\omega \in O_{\mathrm{Th}}$, имеющее перестановочный аргумент, то проблема выразимости для исчисления $(\mathrm{Th},\{\omega\})$ алгоритмически не разрешима.*

Доказательство утверждений.

Для начала докажем вспомогательные леммы.

Лемма 1. [Об унифицирующей подстановке] *Пусть* $M \subseteq \Phi_\Sigma(X),\ \mathfrak{F}_i, \mathfrak{G}_i \in \Phi_\Sigma(X),\ i = 1, \ldots, k,\ k \geqslant 1$. *Если система уравнений*

$$M \vDash \begin{cases} \mathfrak{F}_1 = \mathfrak{G}_1 \\ \ldots \\ \mathfrak{F}_m = \mathfrak{G}_m \end{cases} \qquad (*)$$

имеет решение, то существует такая подстановка $\sigma^* : X \to \Phi_\Sigma(X)$, *что для любого решения* σ' *этой системы существует такая подстановка* $\sigma : X \to \Phi_\Sigma$, *что* $\sigma' = \sigma\sigma^*$.

Доказательство. Опишем допустимые эквивалентные преобразования системы (*), каждое из этих преобразований не изменяет множества решений системы.

1) Если для некоторого i формулы $\mathfrak{F}_i, \mathfrak{G}_i$ имеют вид $\mathfrak{F}_i = f(\mathfrak{A}_1, \ldots, \mathfrak{A}_n)$ и $\mathfrak{G}_i = g(\mathfrak{B}_1, \ldots, \mathfrak{B}_m)$ соответственно, где n и m — арности логических связок f и g. Если $f \neq g$, то система несовместна и, следовательно, не имеет решения. Если же $f = g$, то заменяем уравнение $\mathfrak{F}_i = \mathfrak{G}_i$ системы (*) на группу уравнений $\mathfrak{A}_1 = \mathfrak{B}_1, \ldots, \mathfrak{A}_n = \mathfrak{B}_n$.

2) Если $\mathfrak{F}_i$ совпадает с $\mathfrak{G}_i$, то уравнение $\mathfrak{F}_i = \mathfrak{G}_i$ удаляется.

3) Если для некоторого i одна из формул $\mathfrak{F}_i, \mathfrak{G}_i$ является переменной x. Для определенности будем считать, что $\mathfrak{F}_i \equiv x$, случай, когда $\mathfrak{G}_i \equiv x$ рассматривается аналогично. Если переменное x не принадлежит $\mathfrak{G}_i$, то подставим формулу $\mathfrak{G}_i$ вместо x во все оставшиеся уравнения системы. Если $\mathfrak{G}_i$ содержит x, то система (*) не совместна.

Преобразование 1), в случае применения к уравнениям максимально возможной глубины, уменьшает число уравнений данной, либо большей глубины, поэтому его можно применить лишь конечное число раз. Преобразование 2) уменьшает число уравнений, поэтому оно также применимо лишь конечное число раз. Преобразование 3) уменьшает число переменных x имеющих явное выражение $x = \mathfrak{B}$, через остальные переменные системы и имеющих более одного вхождения в систему, поэтому оно применимо лишь конечное число раз.

Таким образом, процесс применения к системе уравнений (*) преобразований 1)–3) обрывается за конечное число раз. Результирующая система, к которой эти преобразования применимы, может иметь

лишь вид $x_1 = \mathfrak{A}_1, \ldots, x_n = \mathfrak{A}_n$, где $\mathfrak{A}_i \in \Phi_\Sigma\big(X \setminus \{x_1, \ldots, x_n\}\big)$, $i = 1, \ldots, n$.

Выберем в качестве σ^* такую подстановку, что σ^* отображает переменные x_i в формулы $\mathfrak{A}_i$, $i = 1, \ldots, n$, а на остальных переменных из X совпадает с тождественным отображением. Поскольку $\sigma^*(x_i) \equiv \sigma^*\mathfrak{A}_i$ для каждого $i = 1, \ldots, n$, то σ^* — решение системы уравнений (*).

Предположим, что σ' — решение системы уравнений (*), тогда $\sigma'(x_i) \equiv \sigma'\mathfrak{A}_i$ для каждого $i = 1, \ldots, n$, поэтому $\sigma'(x_i) = \sigma'\mathfrak{A}_i = \sigma'\sigma^*(x_i)$ для каждого $i = 1, \ldots, n$, на остальных переменных $\sigma^*(x) = x$, поэтому $\sigma'(x) = \sigma'\sigma^*(x)$. Следовательно, $\sigma' = \sigma'\sigma^*$. Лемма доказана.

Системы продукций Поста

Однородная система продукции Поста — это тройка $T = \langle A, V, l\rangle$, где $A = \{a_1, \ldots, a_n\}$ — конечный алфавит; $V = \{v_1, \ldots, v_n\}$ — множество пар вида $v_i = (a_i, \alpha_i)$, где $a_i \in A$ и $\alpha_i \in A^*$ не пустое слово для каждого $i = 1, \ldots, n$; $l \geqslant 1$ — натуральное число.

Будем говорить, что T применима к слову $\xi \in A^*$, если $|\xi| \geqslant l$, и не применима в противном случае. Система T функционирует детерминировано следующим образом, на каждом такте стираются первые l букв входного слова ξ, а к оставшемуся слову справа приписывается слово α_i, соответствующее первой букве a_i слова ξ. Результатом применения T к слову $\xi = a_i x y$, где $|a_i x| = l$, будем называть слово $y\alpha_i$. Факт применимости T будем обозначать через $a_i x y \xrightarrow{T} y\alpha_i$.

Вычислением системы T на входном слове ξ назовем цепочку слов $\xi \xrightarrow{T} \xi_1 \xrightarrow{T} \xi_2 \xrightarrow{T} \ldots$.

Будем называть слово $\eta \in A^*$ T-продукцией слова $\xi \in A^*$ и писать $\xi \overset{T}{\Longrightarrow} \eta$, если он может быть получено из ξ на каком-либо шаге вычисления, то есть существует конечная последовательность слов $\xi_1, \ldots, \xi_s \in A^*$ такая, что $\xi_1 = \xi, \xi_s = \eta$ и $\xi_i \xrightarrow{T} \xi_{i+1}$, $i = 1, \ldots, s-1$. Таким образом, $\xi \overset{T}{\Longrightarrow} \xi$ и из того, что $\xi \overset{T}{\Longrightarrow} \eta \xrightarrow{T} \zeta$, следует $\xi \overset{T}{\Longrightarrow} \zeta$.

Если последовательность T-продукций слова $\xi \in A^*$ конечна, то будем говорить, что система T останавливается на входном слове ξ, и записывать это через $T(\xi)\downarrow$. Для каждой однородной системы про-

дукции Поста $T = \langle A, V, l\rangle$ поставим вопрос о разрешимости проблемы остановки этой системы: существует ли алгоритм, который по любому наперед заданному слову $\xi \in A^*$ устанавливает, конечно или бесконечно множество его T-продукций, то есть останавливается ли T на слове ξ или нет. Известно, что проблема остановки однородных систем продукций Поста алгоритмически неразрешима [6].

Чтобы доказать алгоритмическую неразрешимость проблемы выразимости пропозиционального исчисления, сведем к ней проблему остановки однородных систем продукций Поста. Для этого по каждой системе продукций Поста T и каждому входному слову ξ построим такую систему тавтологий $\Gamma(T, \xi)$, что $T(\xi)\downarrow$ тогда и только тогда, когда из $\Gamma(T, \xi)$ посредством операции ω выразимо некоторое фиксированное множество тавтологий Υ.

Кодирование слов тавтологиями

Поскольку множество логических связок Σ полно, то в замыкании содержится функции конъюнкция, дизъюнкция и отрицание. Обозначим соответствующие формулы через $x \wedge y,\ x \vee y$ и $\neg$ соответственно. Будем считать, что формулы $x \wedge y,\ x \vee y \in \Phi_\Sigma(\{x, y\})$, а $\neg x \in \Phi_\Sigma(\{x\})$. Если $\circ \in \{\wedge,\ \vee\}$, то расстановку скобок

$$(x_1 \circ (x_2 \circ \ldots \circ (x_{n-1} \circ x_n)))$$

будем считать стандартной и сокращенно обозначать данную формулу через

$$x_1 \circ x_2 \circ \ldots \circ x_{n-1} \circ x_n.$$

Если не оговорено противного, то будем считать, скобки в формулах расставлены стандартным образом.

Определим своего рода кодирование, сопоставив каждой букве алфавита A некоторую тавтологию однозначным образом. Для этого введем уникальную переменную $v \in \mathcal{U}$, которую будем использовать только в кодах букв и нигде иначе. Кодом буквы a_i будем считать тавтологию

$$\underbrace{v \vee \ldots \vee v}_{i} \vee \neg v,$$

которую обозначим через $\overline{a_i},\ i = 1, \ldots, n$.

Далее, произвольному непустому слову $\xi = c_1 \dots c_s$ над алфавитом A сопоставим класс всех тавтологий вида $\overline{c_1} \wedge \dots \wedge \overline{c_s}$, с произвольной расстановкой скобок между конъюнкциями. Произвольного представителя этого класса обозначим через $\overline{\xi}$, которого будем называть кодом слова ξ. Таким образом каждый представитель одного класса кодирует одно и тоже слово.

Для слова $\xi = c_1 \dots c_s$ обозначим формулу $\overline{c_1} \wedge \dots \wedge \overline{c_s}$ со стандартной расстановкой скобок между конъюнкциями через $\overrightarrow{\xi}$, а формулу

$$((\overline{c_1} \wedge \overline{c_2}) \wedge \dots) \wedge \overline{c_s}$$

через $\overleftarrow{\xi}$. В силу введенных обозначений и замечания о расстановке скобок, для любой буквы a и слова ξ формула $\overline{a} \wedge \overrightarrow{\xi}$ совпадает с формулой $\overrightarrow{a\xi}$, а формула $\overleftarrow{\xi} \wedge \overline{a}$ совпадает с формулой $\overleftarrow{\xi a}$. Для всякого слова $\xi = b_1 \dots b_s$ формулу $\overline{b_1} \wedge \dots \wedge \overline{b_s} \wedge \overline{x}$ обозначим через $\overrightarrow{\xi x}$. В силу соглашений о скобках, для любых слов ξ и η формула $\overrightarrow{\xi}\,\overrightarrow{\eta}$ совпадает с формулой $\overrightarrow{\xi\eta}$.

Преобразование операции вывода

Пусть ω — модусная операция из условия теоремы. Пусть $\omega' = \langle \mathfrak{F}_1, \dots, \mathfrak{F}_m; \mathfrak{F}_0 \rangle$, где $\mathfrak{F}_i \in \Phi_\Sigma(X),\ i = 0, 1, \dots, n$, собственное расширение операции ω с перестановочным аргументом p, тогда разрешающее уравнение

$$\mathfrak{F}_1, \dots, \mathfrak{F}_m \vDash \mathfrak{F}_0 = \mathfrak{F}_p \qquad (*)$$

аргумента p имеет решение. По лемме 1 существует решение $\sigma\colon X \to \Phi_\Sigma(X)$, тогда $\sigma\mathfrak{F}_0 \equiv \sigma\mathfrak{F}_p$. Обозначим через X' множество всех переменных, содержащихся в формулах $\mathfrak{F}_i,\ i = 1, \dots, m$, и пусть $\sigma' = \sigma|_{X'}$ ограничение подстановки σ на переменные X', то есть на переменных их X' σ' ведет себя также, как и подстановка σ, а на остальных переменных совпадает с тождественной подстановкой. Тогда $\sigma'\mathfrak{F}_0 \equiv \sigma'\mathfrak{F}_p$, если $\mathfrak{F}_0 \in \Phi_\Sigma(X')$, иначе $\sigma'\mathfrak{F}_0 \leqslant \sigma'\mathfrak{F}_p$. Без ограничения общности будем считать, что $\mathfrak{F}_0$ не имеет уникальных переменных, то есть $X' = X$.

Поскольку p перестановочный элемент операции ω', то найдутся такие неэквивалентные вершины $(x, \alpha), (y, \beta) \in V_p$ разрешающего

графа G_p из одной ациклической компоненты связности, такие различные переменные $z_1, \ldots, z_{q-1} \in X^n$, не принадлежащие $\mathfrak{F}_0$ и $\mathfrak{F}_p$, и такие различные $i_1, \ldots, i_q \in \overline{m} \setminus \{p\}$, что

$$x, z_1 \in \mathfrak{F}_{i_1};\ z_1, z_2 \in \mathfrak{F}_{i_2};\ \ldots\ z_{q-1}, y \in \mathfrak{F}_{i_q}.$$

Поскольку $\mathfrak{F}_1, \ldots, \mathfrak{F}_m$ разрешимы в тавтологиях и σ — унифицирующее решение уравнения (*), то $\sigma\mathfrak{F}_1, \ldots, \sigma\mathfrak{F}_m$ также разрешимы в тавтологиях, поэтому существует такая подстановка $\widetilde{\sigma}\colon X^n \to \Phi_\Sigma(\{u\})$, что $\widetilde{\sigma}\sigma\mathfrak{F}_i \in \mathrm{Th}$ для каждого $i = 1, \ldots, m$. Обозначим подстановку $\widetilde{\sigma}\sigma$ через $\widehat{\sigma}$.

Рассмотрим компоненту связности K, содержащую вершины $(x, \alpha), (y, \beta) \in V_p$. Сопоставим каждому классу эквивалентности этой компоненты относительно отношения $\sim_p$ новую уникальную переменную. Поскольку компонента K не имеет циклов, то найдется класс эквивалентности, не содержащий вершин (z, d), для которых переменное z входит в формулу $\mathfrak{F}_0$. Сопоставим этой компоненте переменное w_1. Рассмотрим класс эквивалентности инцидентный первому классу. Из определения эквивалентности $\sim_p$ следует, что такой класс единственный. Сопоставим этой компоненте переменное w_2. Далее по аналогии, рассматриваем класс, отличный от первого и инцидентный второму, если он существует, то он единственный и сопоставим ему переменное w_3. И так далее, пока не встретим класс эквивалентности, не содержащий вершин (z, d), для которых переменное z входит в формулу $\mathfrak{F}_p$. Пусть этой компоненте сопоставили переменное w_k. Тем самым классы эквивалентности компоненты K образуют цепь длины k.

Из свойства разрешающего графа G_p для любых двух вершин (x', α') и (y', β') из одной компоненты связности выполнено $\eta_{\sigma(x')}(\alpha') \equiv \eta_{\sigma(y')}(\beta')$. Поэтому найдется такое слово γ, что для любой вершины (z, δ) из компоненты K выполнено $\eta_{\widetilde{\sigma}(z)}(\delta\gamma) = u$. Для каждой вершины (z, δ) из класса, соответствующего переменной w_i, заменим в формуле $\widehat{\sigma}(z)$ переменное u в позиции $\delta\gamma$ на переменное w_i. Проделаем такую процедуру для каждого $i = 1, \ldots, k$. Пусть при этом переменным x и y сопоставили переменные w_μ и w_ν соответственно. Поскольку вершины $(x, \alpha), (y, \beta)$ не эквивалентны, то $\mu \neq \nu$. Для определенности будем считать, что $\mu < \nu$ и $\nu - \mu = r$. Рассмотрим

новые уникальные переменные $x_1, \ldots, x_n$, где $n = \lceil \frac{\mu-1}{r} \rceil + \lceil \frac{k-\nu+1}{r} \rceil + 1$. Обозначим остаток от деления $\mu - 1$ на r через r'. Заменим переменное w_i на x_j, где $j = \lceil \frac{i+r'}{r} \rceil$, для каждого $i = 1, \ldots, k$. Пусть $\lceil \frac{\mu+r'}{r} \rceil = s$, тогда $\lceil \frac{\nu+r'}{r} \rceil = s + 1$.

Поскольку переменные $z_1, \ldots, z_{q-1}$ не принадлежат $\mathfrak{F}_0$ и $\mathfrak{F}_p$, то $\sigma(z_i) = z_i,\ i = 1, \ldots, q-1$. Поэтому найдется такие слова $\gamma_1, \ldots, \gamma_{q-1}$, что $\eta_{\widehat{\sigma}(z_i)}(\gamma_i) = u,\ i = 1, \ldots, q-1$. Для каждой переменной z_i заменим в формуле $\widehat{\sigma}(z_i)$ переменное u в позиции γ_i на переменное x_s. Проделаем такую процедуру для каждого $i = 1, \ldots, q-1$.

Подстановку, полученную указанными преобразованиями из подстановки $\widehat{\sigma}$, обозначим через $\overline{\sigma}$. Без ограничения общности будем считать, что $q = 1$, $n = 4$ и $s = 2$, остальные случаи рассматриваются по аналогии. Тогда $\overline{\sigma}\mathfrak{F}_p \in \Phi_\Sigma(\{x_1, x_2, x_3, u\})$, $\overline{\sigma}\mathfrak{F}_0 \in \Phi_\Sigma(\{x_2, x_3, x_4, u\})$, $\overline{\sigma}\mathfrak{F}_{i_1} \in \Phi_\Sigma(\{x_2, x_3, u\})$, остальные тавтологии $\overline{\sigma}\mathfrak{F}_j \in \Phi_\Sigma(\{x_1, x_2, x_3, x_4, u\})$. Заметим, что i_1 не совпадает с p. Обозначим тавтологию $\overline{\sigma}\mathfrak{F}_p$ через $\langle x_1, x_2, x_3 \rangle$, тавтологию $\overline{\sigma}\mathfrak{F}_0$ через $\langle x_2, x_3, x_4 \rangle$, тавтологию $\overline{\sigma}\mathfrak{F}_{i_1}$ через $x_2 \to x_3$, оставшиеся тавтологии объединим в одну группу, которую обозначим через H. Формула $x \to y$ является аналогом импликации, поэтому далее будем применять к ней понятия посылки и заключения, аналогичные стандартной импликации.

Поскольку операция ω будучи примененной к тавтологиям $\langle x_1, x_2, x_3 \rangle,\ x_2 \to x_3, \mathrm{H}$ всегда на выходе даст тавтологию $\langle x_2, x_3, x_4 \rangle$, то тем самым имеется модусная операция, заданная схемой

$$\frac{\langle x_1, x_2, x_3 \rangle,\ x_2 \to x_3, \mathrm{H}}{\langle x_2, x_3, x_4 \rangle},$$

которая является собственным расширением операции ω.

Получение систем тавтологий $\Gamma(T, \xi)$ и Υ

Пусть $T = \langle A, V, l \rangle$ — однородная система продукций Поста, где $A = \{a_1, \ldots, a_n\}$ — конечный алфавит, $V = \{v_1, \ldots, v_n\}$ — множество пар вида $v_i = (a_i, \alpha_i)$, $a_i \in A$ и $\alpha_i \in A^*$ не пустое слово для каждого $i = 1, \ldots, n$, $l \geqslant 1$ и $\xi \in A^*$ произвольное слово. Тогда возьмем в качестве $\Gamma(T, \xi)$ множество тавтологий:

(1) $\langle x, \overline{\xi}, \mathfrak{B}_\xi \rangle$

(2) $\overrightarrow{a_i \alpha x} \to x \wedge \overrightarrow{\alpha_i}$, для всех $\alpha \in A^*,\ |\alpha| = l-1,\ 1 \leqslant i \leqslant n$

(3) $\overrightarrow{a_i \alpha} \to \overrightarrow{\alpha_i}$, для всех $\alpha \in A^*,\ |\alpha| = l-1,\ 1 \leqslant i \leqslant n$

(4) $\overrightarrow{\alpha} \to x$, для всех $\alpha \in A^*,\ |\alpha| \leqslant l-1$

(5) $x \to x$,

(6) $(x \wedge (\overline{a} \wedge y)) \wedge z \to ((x \wedge \overline{a}) \wedge y) \wedge z$, для всех $\alpha \in A$

(7) $(x \wedge \overline{a}) \wedge y \to x \wedge (\overline{a} \wedge y)$, для всех $\alpha \in A$

где $\mathfrak{B}_\xi$ — формула, определяемая по следующему правилу. Если $|\xi| < l$, то $\mathfrak{B}_\xi = x$, если $|\xi| = l$ и a_i первая буква слова ξ, то $\mathfrak{B}_\xi = \overrightarrow{\alpha_i}$, если же $|\xi| > l$ и $\xi = a_i \xi' \eta$, где $|\xi'| = l-1$, то $\mathfrak{B}_\xi = \overrightarrow{\eta} \wedge \overrightarrow{\alpha_i}$. И добавим в него множество тавтологий H. Обозначим множество тавтологий H, (2), (3), (4), (5), (6), (7) через Γ_T и множество тавтологий H, (5), (6), (7) — через R.

В качестве Υ возьмем множество состоящее из тавтологии $\langle x, x, x \rangle$.

Свойства выводимых из $\Gamma(T, \xi)$ тавтологий

Тот факт, что для формул $\mathfrak{A}$ и $\mathfrak{B}$ существует такая последовательность формул $\mathfrak{A}_0, \ldots, \mathfrak{A}_k$, где $k \geqslant 1$, для которой выполнено $M \vdash \mathfrak{A}_{i-1} \to \mathfrak{A}_i,\ i = 1, \ldots, k$, будем обозначать для краткости через $M \vdash \mathfrak{A} \Rightarrow \mathfrak{B}$, где M — некоторое множество тавтологий.

Лемма 2. *Для любых* $\xi, \beta, \zeta \in A^+$ $R \vdash (\overleftarrow{\xi} \wedge \overrightarrow{\beta}) \wedge \overrightarrow{\zeta} \Rightarrow \overleftarrow{\xi\beta} \wedge \overrightarrow{\zeta}$.

Доказательство. Доказывать будем индукцией по длине слова β. Если $|\beta| = 1$, тогда формула $(\overleftarrow{\xi} \wedge \overrightarrow{\beta}) \wedge \overrightarrow{\zeta}$ совпадает с $\overleftarrow{\xi\beta} \wedge \overrightarrow{\zeta}$, следовательно, $R \vdash (\overleftarrow{\xi} \wedge \overrightarrow{\beta}) \wedge \overrightarrow{\zeta} \Rightarrow \overleftarrow{\xi\beta} \wedge \overrightarrow{\zeta}$ по формуле (5). Пусть теперь $\beta = a\delta$, где $|\delta| \geqslant 1$, тогда в R выводима следующая цепочка импликаций:

$$(\overleftarrow{\xi} \wedge (\overline{a} \wedge \overrightarrow{\delta})) \wedge \overrightarrow{\zeta} \xrightarrow{(6)} (\overleftarrow{\xi a} \wedge \overrightarrow{\delta}) \wedge \overrightarrow{\zeta} \xrightarrow{\text{IH}} \overleftarrow{\xi\beta} \wedge \overrightarrow{\zeta}.$$

Первая импликация есть подстановочный вариант формулы (6), а вторая получена на основе предположения индукции.

Следствие 1. *Для любых* $\xi, \beta \in A^+$ $R \vdash \overrightarrow{\xi} \wedge \overrightarrow{\beta} \Rightarrow \overleftarrow{\xi} \wedge \overrightarrow{\beta}$.

Лемма 3. *Для любых* $\xi, \beta \in A^+$ $R \vdash \overleftarrow{\xi} \wedge \overrightarrow{\beta} \Rightarrow \overrightarrow{\xi\beta}$.

Доказательство. Доказывать будем индукцией по длине слова ξ. Если $|\xi| = 1$, то есть $\xi = a$, тогда формула $\overleftarrow{\xi} \wedge \overrightarrow{\beta}$ совпадает с $\overrightarrow{\alpha\beta}$, следовательно, $R \vdash \overleftarrow{\xi} \wedge \overrightarrow{\beta} \Rightarrow \overrightarrow{\alpha\beta}$ по формуле (5). Если $|\xi| = 2$, то есть $\xi = ab$, тогда $R \vdash \overleftarrow{\xi} \wedge \overrightarrow{\beta} \Rightarrow \overrightarrow{\alpha\beta}$ по формуле (7). Пусть теперь $\xi = \delta a$, где $|\delta| > 1$, тогда в R выводима следующая цепочка импликаций:

$$(\overleftarrow{\delta} \wedge \overline{a}) \wedge \overrightarrow{\beta} \xrightarrow{(7)} \overleftarrow{\delta} \wedge \overrightarrow{a\beta} \xRightarrow{\text{IH}} \overrightarrow{\xi\beta}.$$

Первая импликация есть подстановочный вариант формулы (7), а вторая получена на основе предположения индукции.

Следствие 2. *Для любых* $\xi, \beta \in A^+$ $R \vdash \overrightarrow{\xi} \wedge \overrightarrow{\beta} \Rightarrow \overrightarrow{\xi\beta}$.

Лемма 4. *Если* $\xi \xrightarrow{T} \beta$, *то* $\Gamma_T \vdash \overrightarrow{\xi} \Rightarrow \overrightarrow{\beta}$.

Доказательство. Поскольку T применима к ξ, то $|\xi| \geqslant l$. Если $|\xi| = l$ и $\xi = a_i\delta$, то $\beta = \alpha_i$ и по формуле (3) имеем $\Gamma_T \vdash \overrightarrow{a_i\delta} \Rightarrow \overrightarrow{\alpha_i}$. Если же $|\xi| > l$ и $\xi = a_i\delta\zeta$, $|\delta| = l - 1$, то $\beta = \zeta\alpha_i$ и в Γ_T выводима цепочка:

$$\overrightarrow{a_i\delta\zeta} \xrightarrow{(2)} \overrightarrow{\zeta} \wedge \overrightarrow{\alpha_i} \xRightarrow{\text{Сл 2}} \overrightarrow{\zeta\alpha_i},$$

где Сл 2 есть применение следствия 2. Тем самым доказали, что $\Gamma_T \vdash \overrightarrow{\xi} \Rightarrow \overrightarrow{\beta}$.

Для произвольного множества тавтологий M обозначим через $\langle M \rangle$ множество состоящее из тавтологий H, из тавтологий $\mathfrak{A}$, для которых существуют такие формулы $\mathfrak{B}_1, \ldots, \mathfrak{B}_m \in M$, что $\omega(\mathfrak{B}_1, \ldots, \mathfrak{B}_m) = \mathfrak{A}$, а также из тавтологий $\mathfrak{A}$, для которых существуют такая формула $\mathfrak{B} \in M$ и подстановка σ, что $\mathfrak{A} = \sigma\mathfrak{B}$.

Положим $\Gamma_0 = \Gamma(T, \xi)$ и $\Gamma_{n+1} = \langle \Gamma_n \rangle$, тогда $[\Gamma(T, \xi)]_\omega = \cup_{n \geqslant 0} \Gamma_n$. Покажем теперь, что из формул множества $\Gamma(T, \xi)$ до некоторого шага N вычислений системы T на входном слове ξ мы не можем вывести ни одну формулу вида $\langle \mathfrak{A}, \overline{\beta}, \mathfrak{B} \rangle$ никак иначе, кроме как пользуясь формулами (2) и (3), гарантирующими, что слово β, кодируемое

формулой $\overline{\beta}$, является продукцией системы T на входном слове ξ. Для начала докажем следующую лемму, утверждающую, что только формулы определенного вида выводимы из системы $\Gamma(T, \xi)$.

Лемма 5. *Пусть система продукций T, будучи примененной к слову $\xi \in A^*$, не остановилась за N шагов своей работы, тогда для любого $n \leqslant N$ множество Γ_n состоит лишь из подстановочных вариантов формул из Γ_T и формул вида $\langle x, \overline{\beta}, y\rangle$, где $\overline{\beta}$ — код слова $\beta \in A^*$.*

Доказательство. Докажем лемму индукцией по n. Все формулы из $\Gamma(T, \xi)$ имеют указанный вид, поэтому для Γ_0 утверждение верно. Пусть оно верно для всех $n' < n$, докажем его для n. Поскольку операция подстановки не меняет вид формул, рассмотрим только операцию ω. Пусть формула $\mathfrak{C} \in T_n$ получена из формул $\mathfrak{B}_1, \ldots, \mathfrak{B}_m \in T_{n-1}$. По выбору подстановки $\overline{\sigma}$ формулы $\mathfrak{B}_1, \ldots, \mathfrak{B}_m$ есть подстановочные варианты формул $\langle x, y, z\rangle,\ x \to y$ и формул H. Поскольку $\mathrm{H} \subseteq \Gamma_n$ и формулы $\langle x, y, z\rangle,\ x \to y$ сами не совместны, а также не совместны ни с одно формулой из H, то можно ограничиться только рассмотрением подстановочных вариантов формул $\langle x, y, z\rangle,\ x \to y$.

Итак, пусть формула $\mathfrak{C}$ получена из формул $\langle \mathfrak{A}, \mathfrak{B}, \mathfrak{C}\rangle,\ \mathfrak{B} \to \mathfrak{C} \in T_{n-1}$, тогда по предположению индукции $\mathfrak{B}$ является формулой вида $\overline{\beta}'$, где $\overline{\beta}'$ — подстановочный вариант кода слова $\beta \in A^*$, а $\mathfrak{B} \to \mathfrak{C}$ — есть подстановочный вариант формулы из Γ_T. Возможны следующие случаи

1) Формула $\mathfrak{B} \to \mathfrak{C}$ получена из (2), (3), (5), (6) или (7). Во всех случаях, если посылка импликации имеет вид $\overline{\beta}'$, то и заключение имеет тот же вид.

2) Формула $\mathfrak{B} \to \mathfrak{C}$ получена из (4). Этот случай не возможен, поскольку формула $\mathfrak{B}$ была бы подстановочным вариантом формулы $\overline{\beta}$ для некоторого слова β, длина которого меньше l, что означало бы остановку системы T, чего не может быть по выбору N.

Лемма доказана.

Из описанного в лемме 5 вывода формул из $\Gamma(T, \xi)$ непосредственно следует утверждение.

Следствие 3. *Если из $\Gamma(T, \xi)$ выводима формула вида $\langle \mathfrak{A}, \overline{\beta}', \mathfrak{B}\rangle$, где $\overline{\beta}'$ — подстановочный вариант кода слова $\beta \in A^*$, то найдутся та-*

кие формулы $\mathfrak{C}$ *и* $\mathfrak{D}$*, для которых формула* $\langle \mathfrak{C}, \overline{\beta}, \mathfrak{D} \rangle$ *выводима из* $\Gamma(T, \xi)$.

Лемма 6. *Пусть система продукций* T*, будучи примененной к слову* $\xi \in A^*$*, не остановилась за* N *шагов своей работы, тогда для любого* $n \leqslant N$ *и любого слова* $\beta \in A^*$*, если* $\langle \mathfrak{A}, \overline{\beta}, \mathfrak{B} \rangle \in T_n$*, для некоторых формул* $\mathfrak{A}$ *и* $\mathfrak{B}$*, то* $\xi \overset{T}{\Longrightarrow} \beta$.

Доказательство. Докажем лемму индукцией по n. Если $n = 0$, то $\langle \mathfrak{A}, \overline{\beta}, \mathfrak{B} \rangle$ может совпадать только с $\langle x, \overline{\xi}, \mathfrak{B}_\xi \rangle$, и при этом $\xi \overset{T}{\Longrightarrow} \xi$. Пусть утверждение леммы верно для всех $n' < n$, докажем его для n.

Если $\langle \mathfrak{A}, \overline{\beta}, \mathfrak{B} \rangle$ получена из формулы $\langle \mathfrak{C}, \overline{\delta}', \mathfrak{D} \rangle$ с помощью операции подстановки, то из-за особенностей кодирования $\overline{\delta}'$ неминуемо совпадает с $\overline{\beta}$. Тогда по предположению индукции $\xi \overset{T}{\Longrightarrow} \beta$.

Если $\langle \mathfrak{A}, \overline{\beta}, \mathfrak{B} \rangle$ получена из формул $\langle \mathfrak{C}, \mathfrak{D}, \overline{\beta} \rangle, \mathfrak{D} \to \overline{\beta} \in T_{n-1}$ и H с помощью операции ω. Согласно лемме 5 и следствию 3 можно считать, что $\mathfrak{D}$ имеет вид $\overline{\delta}$ для некоторого слова $\delta \in A^*$. Тогда по предположению индукции $\xi \overset{T}{\Longrightarrow} \delta$. Возможны следующие случаи

1) Формула $\overline{\delta} \to \overline{\beta}$ получена с помощью подстановки из (2) или (3). Тогда $\delta \xrightarrow{T} \beta$ и, следовательно, $(\xi \overset{T}{\Longrightarrow} \beta) = (\xi \overset{T}{\Longrightarrow} \delta \xrightarrow{T} \beta)$.

2) Формула $\overline{\delta} \to \overline{\beta}$ получена с помощью подстановки из (4). Этот случай не возможен, поскольку слово δ имело бы длину меньшую чем l, что означало бы остановку системы T, чего не может быть по выбору N.

3) Формула $\overline{\delta} \to \overline{\beta}$ получена с помощью подстановки из (5), (6) или (7). Тогда $\overline{\delta}$ и $\overline{\beta}$ коды одного и того же слова β и, следовательно, $\xi \overset{T}{\Longrightarrow} \beta$.

Лемма доказана.

Сведение проблемы остановки к проблеме выразимости

Лемма 7. *Для всякой однородной системы продукций Поста* $T = \langle A, V, l \rangle$ *и произвольного слова* $\xi \in A^*$ $T(\xi) \downarrow$ *тогда и только тогда, когда* $\langle x, x, x \rangle \in [\Gamma(T, \xi)]_{\{\omega\}}$.

Доказательство. Докажем прямое утверждение. Пусть $T(\xi) \downarrow$, тогда найдется такое слово $\beta \in A^*$, длина которого меньше l. Значит,

либо $\xi = \beta$, либо по лемме 4 $\Gamma_T \vdash \overrightarrow{\xi} \Rightarrow \overrightarrow{\beta}$. Из формулы (4) имеем $\Gamma_T \vdash \overrightarrow{\beta} \Rightarrow x$, поскольку система $\Gamma(T, \xi)$ содержит тавтологию $\overrightarrow{\xi}$, то с помощью операции ω можно выразить формулу $\langle \beta, x, x \rangle$, откуда, однократным применением операции ω к формулам $\langle \beta, x, x \rangle$ и (5), выражаем искомую тавтологию $\langle x, x, x \rangle$.

Докажем обратное утверждение. Пусть $\langle x, x, x \rangle \in [\Gamma(T, \xi)]_{\{\omega\}}$, но T не остановилась на слове ξ. Тогда по лемме 5 $[\Gamma(T, \xi)]_{\{\omega\}}$ не содержит тавтологии $\langle x, x, x \rangle$, чего быть не может. Лемма доказана.

Доказательство теоремы 1

Предположим противное, то есть существует алгоритм A, решающий задачу выразимости конечных систем тавтологий. Рассмотрим произвольную однородную систему продукций Поста $T = \langle A, V, l \rangle$ и слово $\xi \in A^*$. Так как система $\Gamma(T, \xi)$ конечна, то с помощью алгоритма A можно проверить, выразима ли из нее формула $\langle x, x, x \rangle$ или нет. По лемме 7 имеем: если $\langle x, x, x \rangle$ выразима из $\Gamma(T, \xi)$ с помощью операции ω, то система T, будучи примененной к слову ξ, остановится, если же $\langle x, x, x \rangle$ не выразима из $\Gamma(T, \xi)$ с помощью операции ω, то система T не остановится на слове ξ. Это означает, что алгоритм A позволяет решить проблему остановки для однородной системы продукции Поста Σ. В силу алгоритмической неразрешимости последней получаем противоречие. Теорема доказана.

4. Алгоритмическая неразрешимость проблемы полноты

Рассмотрим произвольную модусную операцию $\omega \in \mathcal{M}_\Sigma$, удовлетворяющую условию теоремы 1 и образованное ей исчисление $(\mathrm{Th}, \{\omega\})$. Пусть $\Gamma(T, \xi)$ — множество тавтологий, определенное в предыдущем разделе. Обозначим множество формул $\{\mathfrak{A} \in \Phi_\Sigma \mid \langle x, y, z \rangle \leqslant \mathfrak{A}\}$ через T_ω, тогда справедлива следующая лемма.

Лемма 8. *Если множество тавтологий T_ω полно в $(\mathrm{Th}, \{\omega\})$, то для всякой однородной системы продукций Поста $T = \langle A, V, l \rangle$ и произвольного слова $\xi \in A^*$ система T остановится на входном слове ξ тогда и только тогда, когда множество тавтологий $\Gamma(T, \xi)$ полно в $(\mathrm{Th}, \{\omega\})$.*

Поскольку проблема остановки однородных систем продукций поста алгоритмически неразрешима, то как следствие из этой леммы имеем следующую теорему.

Теорема 2. *Для любой полной системы логических связок* Σ *и любой модусной операции* $\omega \in O_{\mathrm{Th}}$*, имеющей собственное расширение с перестановочным аргументом, существует исчисление* $(\mathrm{Th}, \{\omega\})$*, для которого проблема полноты алгоритмически не разрешима.*

Доказательство леммы 8.

Докажем прямое утверждение. Пусть $T(\xi)\downarrow$, тогда по лемме 7 из множества $\Gamma(T,\xi)$ с помощью операции ω выразима тавтология $\langle x,x,x\rangle$. Доказательства также следует, что помимо $\langle x,x,x\rangle$ выразима и тавтология $\langle x,y,z\rangle$. С помощью операции подстановки можем получить включение $T_\omega \subseteq [\Gamma(T,\xi)]_\omega$. Поскольку множество T_ω полно, то и множество $\Gamma(T,\xi)$ также полно в $(\mathrm{Th}, \{\omega\})$.

Докажем обратное утверждение. Поскольку $\Gamma(T,\xi)$ полно в $(\mathrm{Th}, \{\omega\})$, то $\langle x,x,x\rangle \in [\Gamma(T,\xi)]_{\{\omega\}}$, тогда, снова применяя лемму 7, получаем $T(\xi)\downarrow$. Лемма доказана.

Список литературы

[1] Боков Г. В. Проблема полноты в исчислении высказываний // Интеллектуальные системы. — 2009. Т. 13. Вып. 1–4. — С. 165–181.

[2] Гильберт Д., Бернайс П. Логические исчисления и формализация арифметики. — М.: Наука, 1979.

[3] Кон П. Универсальная алгебра. — М.: Мир, 1968.

[4] Кудрявцев В. Б. Функциональные системы. — М.: Изд-во МГУ, 1982.

[5] Кузнецов А. В. Неразрешимость общих проблем полноты, разрешимости и эквивалентности для исчислений высказываний // Алгебра и логика. — 1963. Т. 2. № 4. — С. 47–66.

[6] Мальцев А. И. Алгоритмы и рекурсивные функции. — М.: Наука, 1965.

[7] Минц Г. Е. Допустимые и производные правила // Записки научных семинаров ЛОМИ АН СССР. — 1968. 8. — С. 189–191.

[8] Циткин А. И. О допустимых правилах интуиционистской логики высказываний // Матем. сб. — 1977. 102 (144): 2.

[9] Шенфилд Д. Математическая логика. — М.: Наука, 1975. — С. 314–323.

[10] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

[11] Davis M. Computability and unsolvability. — New York: McGraw-Hill, 1958. — P. 137–142.

[12] Gladstone M. D. Some Ways of Constructing a Propositional Calculus of Any Required Degree of Unsolvability // Transactions of the American Mathematical Society. — 1965. Vol. 118. — P. 192–210.

[13] Harrop R. On the existence of finite models and decision procedures // Proceedings of the Cambridge Philosophical Society. — 1958. Vol. 54. — P. 1–16.

[14] Linial S., Post E. L. Recursive unsolvability of the deducibility, Tarski's comleteness, and independence of axioms problems of the propositional calculus (abstract) // Bulletin of the American Mathematical Society. — 1949. Vol. 55. — P. 50.

[15] Singletary W. E. A complex of problems proposed by Post // Bulletin of the American Mathematical Society. — 1964. Vol. 70. N 1. — P. 105–109.

[16] Address at the Princeton University bicentennial conference on problems of mathematics (December 17–19, 1946) / by Alfred Tarski // The Bulletin of Symbolic Logic. — 2000. Vol. 6. N 1.

[17] Yntema M. K. A detailed argument for the Post-Linial theorems // Notre Dame J. of Formal Logic. — 1964. Vol. 5. N 1. — P. 37–50.

Построение синхронизирующих деревьев

Гасанов Э. Э., Дин А. А. (Москва, МГУ им. М. В. Ломоносова)
el_gasanov@mail.ru

В данной работе рассматривается известная проблема синхронизации сигнала, возникающая при производстве электронных схем (чипов). Она состоит в том, чтобы от некоторой точки чипа (источника) до некоторых других точек чипа (стоков) сигнал доходил одновременно. В чипах в качестве источника выступает выход генератора периодических сигналов, определяющих тактовую частоту чипа, а в качестве стоков — управляющие входы регистров, которые определяют состояние чипа в каждый момент времени. Одновременность поступления сигнала гарантирует одномоментность изменения состояния чипа через равные промежутки времени. Эта задача решалась как для чисто производственных алгоритмов [1], так и на модельных объектах [2, 3]. В данной работе используется модель, предложенная в [3].

В качестве модели мы будем рассматривать ориентированные деревья с корнем, каждая вершина которых лежит на плоской целочисленной решетке, каждое ребро соединяет две соседние вершины целочисленной решетки (то есть каждое ребро имеет длину 1, а степень инцидентности каждой вершины не более 4), и все ребра направлены от корня к концевым вершинам, при этом *корень* — это вершина, в которую не входит ни одно ребро, а из *концевых вершин* не исходит ни одного ребра. На рисунке 1 приведен пример такого дерева, причем корень дерева помечен треугольником, а концевые вершины помечены жирными точками. Ориентация ребер на рисунке не приведена, так как после фиксации корня она определяется однозначно.

Полустепенью исхода вершины дерева назовем число ребер, исходящих из вершины.

Задержкой вершины дерева назовем ее полустепень исхода, *задержкой пути* в дереве — сумму задержек всех вершин пути, а *задержкой до концевой вершины* дерева — задержку пути, ведущего от корня к этой концевой вершине. Такое определение задержки продиктовано технологическими особенностями распространения сигналов в

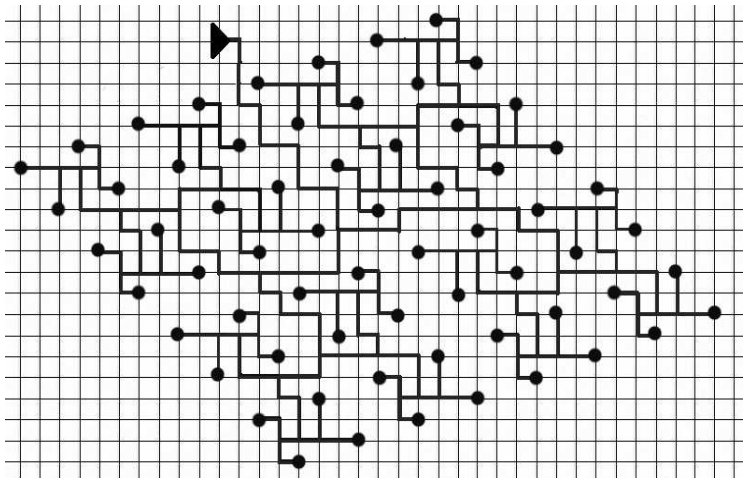


Рис. 1. Пример построенного синхронизирующего дерева для конфигурации $K \in \mathcal{K}_4$.

чипах. Понять эти особенности может помочь следующая «водная» интерпретация. Представим, что в каждой вершине стоит насос, а каждое исходящее ребро это каналы, данным насосом заполняемые. Насос включается, если заполнен канал, соответствующий входному ребру вершины, поэтому насосы, соответствующие концам исходящих ребер включатся только тогда, когда заполнятся каналы, соответствующие данным ребрам. А время заполнения каналов пропорционально их количеству.

Конфигурацией назовем множество точек плоской целочисленной решетки, одна из которых называется *источником*, а остальные точки конфигурации называются *стоками*. На рисунке 1 приведен пример конфигурации, причем источник помечен треугольником, а стоки — жирными точками.

Основная задача: для заданной конфигурации точек K построить дерево A, корень которого совпадает с источником, множество концевых вершин которого содержит множество стоков конфигурации K и задержка до всех концевых вершин дерева, являющихся стоками конфигурации, одинакова. Дерево A, построенное для конфигурации

K и обладающее данными свойствами, будем называть *синхронизирующим* и обозначать $A(K)$.

Неформально, синхронизирующее дерево позволяет доставлять сигнал от источника за одинаковое время до каждого из стоков. На рисунке 1 приведен пример синхронизирующего дерева, для определенной ранее конфигурации.

Отметим, что в синхронизирующем дереве могут быть концевые вершины не совпадающие со стоками.

Расстоянием между двумя точками плоскости $a = (x_a, y_a)$ и $a' = (x_{a'}, y_{a'})$ назовем число $\rho(a, a') = |x_a - x_{a'}| + |y_a - y_{a'}|$.

$r(K) = \min\limits_{a,a' \in K,\ a \neq a'} \rho(a, a')$ — минимальное расстояние между любыми двумя разными точками конфигурации K.

Для натурального m введем следующий класс конфигураций

$$\mathcal{K}_m = \{K : r(K) \geqslant m\}.$$

Конфигурацию точек, для которой невозможно построить синхронизирующее дерево, будем называть *ловушкой*.

В работе [3] было показано, что в классах $\mathcal{K}_1$ и $\mathcal{K}_2$ существуют ловушки, и что для любой конфигурации из $\mathcal{K}_n$, где $n \geqslant 5$, существует синхронизирующее дерево. Оставался открытым вопрос для конфигураций из $\mathcal{K}_3$ и $\mathcal{K}_4$. Результаты данной работы позволяют получить окончательные ответы на данные вопросы.

Теорема 1. *В классе $\mathcal{K}_3$ существует ловушка.*

Теорема 2. *Для любой конфигурации $K \in \mathcal{K}_4$ можно построить синхронизирующее дерево.*

Идея доказательства теоремы 2 основывается на следующем алгоритме построения синхронизирующих деревьев, схематически изображенном на рис. 2.

1) Соединяются по четыре соседних стока в одно синхронизирующее поддерево, с подкорнем в некоторой точке решетки. В случае если стоков оказывается меньше, то в нужном месте добавляем «фиктивное» ребро для сохранения симметрии.

2) Далее первый раз отражаем схему соединения относительно прямой на которой лежат 2 соседних соединенных стока поддерева,

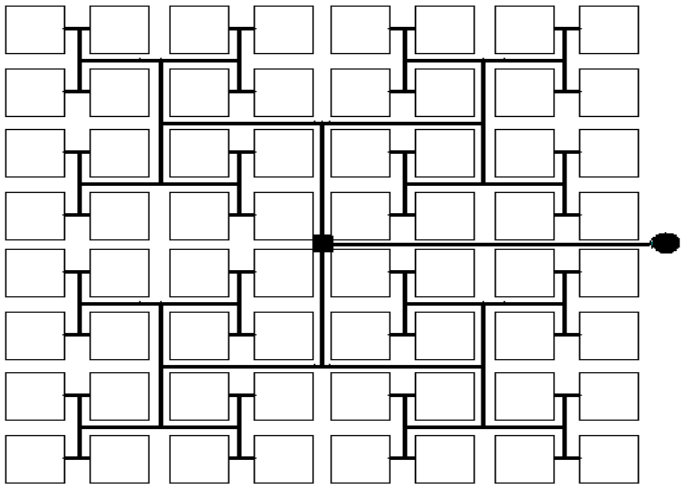


Рис. 2. Схема соединения поддеревьев.

и второй раз относительно прямой перпендикулярной первой прямой. И соединяем отображенной схемой соседние стоки.

3) Соединяются два соседних подкорня, от которых были построены поддеревья доставляющие сигналы в предыдущем шаге одно поддерево. В случае если в каких-то поддеревьях не хватает стоков, то в соответствующих местах добавляются для сохранения симметрии «фиктивные» ребра.

4) Повторяется 2-й шаг, до тех пор пока не будет уложено дерево для всех точек конфигурации.

Дерево, приведенное на рис. 1, является деревом, построенным по данному алгоритму.

Список литературы

[1] Pavisic I., Lu A., Zolotykh A. A., Gasanov E. E. Method in integrating clock tree synthesis and timing optimization for an integrated circuit design / United States Patent: 6,550,044. — April 15, 2003

[2] Sherwani N. A. Algorithms for VLSI Physical Design Avtomation. — Kluwer Academic Publishers, 1993.

[3] Гасанов Э. Э., Проворова А. Л. О синтезе синхронизирующих деревьев // Материалы IX Международной конференции «Интеллектуальные системы и компьютерные науки» (23–27 октября 2006 г.) Т. 1, часть 1. — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 89–92.

Представления элементов частично-упорядоченных алгебраических систем фрагментами

Грунский И. С., Максименко И. И. (Донецк, ИПММ НАН Украины)

iim@bank-prsp.dn.ua

Введение

Одной из важнейших проблем теории дискретных систем является анализ поведения объекта (автомата, помеченного графа) посредством проведения с ним экспериментов [1, 2].

В работах [1, 3] был введен и обоснован подход к исследованию контрольных и распознающих экспериментов в классах автоматов Мили на основе их представления специальными окрестностями в метрических пространствах автоматов. Для бэровской метрики, отражающей близость автоматов по поведению, были найдены [3] конструктивные критерии существования контрольных экспериментов.

Данный метод использован в [4] для неструктурированных объектов и их дескрипторов.

В настоящей статье этот подход распространен на алгебраические системы специального вида, обобщающие классы автоматов Мили и помеченных графов.

1. Основные понятия и определения

Рассмотрим алгебраическую систему вида $(\mathbf{A}, \leqslant, \mathrm{n})$, где $\mathbf{A}$ — счетное множество объектов, $\leqslant$ — предпорядок и $n : \mathbf{A} \to \mathbf{N}^+ \cup \{\infty\}$ — невозрастающая функция сложности.

Два объекта A и B эквивалентны ($A \cong B$), если одновременно $A \leqslant B$ и $B \leqslant A$. Каждый объект A однозначно определяется множествами фрагментов $Fr(A) = \{B \in \mathbf{A} | \mathrm{B} \leqslant \mathrm{A}\}$ и кофрагментов $CoFr(A) = \{B \in \mathbf{A} | \mathrm{B} \not\leqslant \mathrm{A}\}$. Объект A с конечной сложностью $n(A)$ назовем финитным и инфинитным в противном случае. Объект C является разделяющим для объектов A и B ($C \in S(A, B)$), если выполнено одно из условий ($C \leqslant A$ и $C \not\leqslant B$) или ($C \not\leqslant A$ и $C \leqslant B$).

Систему $(\mathbf{A}, \leqslant, \mathrm{n})$ назовем финитно разделимой, если для любых двух неэквивалентных объектов существует финитный объект, их разделяющий.

На множестве объектов введем «расстояние» между объектами β аналогично «бэровской» метрике [3], полагая $\beta(A, B) = 0$, если $A \cong B$ и $\beta(A, B) = 1/r$, где $r = inf\{n(C)|C \in S(A, B)\}$ в противном случае. Через $LimF$ обозначим множество предельных объектов [4] для $F \subseteq \mathbf{A}$.

Пару объектов $(A, B) \in Fr(A_0) \times CoFr(A_0)$ назовем представлением для произвольных $A_0 \in \mathbf{A}$ и $F \subseteq \mathbf{A}$, если для любого $C \in F$ из включения $(A, B) \in Fr(C) \times CoFr(C)$ вытекает $C \cong A_0$.

Система $(\mathbf{A}, \leqslant, \mathrm{n})$ сильно непредставима, если для всякого объекта $A \in \mathbf{A}$ не существует представление относительно A и $\mathbf{A}$.

Систему $(\mathbf{A}, \leqslant, \mathrm{n})$ назовем линейно упорядоченной, если $\mathbf{A}$ — линейно упорядочено.

Система $(\mathbf{A}, \leqslant, \mathrm{n})$ всюду плотна, если для любых объектов A, B из соотношения $A < B$ вытекает существование объекта C, для которого $A < C < B$.

Введем алгебраические системы объектов вида $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$, где $\leqslant$ — предпорядок, $\nabla, \triangle$ — идемпотентные, коммутативные и ассоциативные всюду определенные бинарные операции, $\mathrm{n} : \mathbf{A} \to \mathbf{N}^+ \cup \{\infty\}$ — неубывающая функция сложности, и справедливы следующие аксиомы:

1. для любых двух объектов A и B выполнены соотношения $A \leqslant A\nabla B$ и $A\triangle B \leqslant A$;

2. для любых объектов $A_1, A_2, B \in \mathbf{A}$ из $A_1 \leqslant B, A_2 \leqslant B$ следует $A_1 \nabla A_2 \leqslant B$;

3. для любых объектов $A_1, A_2, B \in \mathbf{A}$ из $A_1 \not\leqslant B, A_2 \not\leqslant B$ вытекает $A_1 \triangle A_2 \not\leqslant B$;

4. для любых двух объектов $A, B \in \mathbf{A}$ полагаем, что $n(A\nabla B) = max(n(A), n(B))$ и $n(A\triangle B) = min(n(A), n(B))$.

Назовем алгебраическую систему $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$ локально замкнутой, если для всякого $A \in \mathbf{A}$ множества $Fr(A)$ и $CoFr(A)$ замкнуты относительно счетного числа операций ∇ и $\triangle$ соответственно.

Введем операцию $\odot$ над парами объектов $(A_1, B_1), (A_2, B_2) \in \mathbf{A^2}$, полагая $(A_1, B_1) \odot (A_2, B_2) = (A_1 \nabla A_2, B_1 \triangle B_2)$.

2. Представимость алгебраических систем вида $(\mathbf{A}, \leqslant, \mathrm{n})$

Имеет место следующий критерий сильной непредставимости:

Утверждение 1. *Пусть дана линейно упорядоченная система* $(\mathbf{A}, \leqslant, \mathrm{n})$. *Система сильно непредставима тогда и только тогда, когда она является всюду плотной.*

В работе [4] был получен метрический критерий существования финитных представлений неструктурированных объектов. Для произвольных алгебраических систем подобный критерий в общем случае не выполнен:

Теорема 2. *Дана финитно разделимая алгебраическая система* $(\mathbf{A}, \leqslant, \mathrm{n})$. *Если для произвольных* $A_0 \in \mathbf{A}$ *и* $F \subseteq \mathbf{A}$ *существует финитное представление, тогда* $A_0 \notin limF$. *Обратное утверждение неверно.*

3. Представимость алгебраических систем вида $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$

Алгебраическая структура систем вида $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$ описана в

Утверждение 3. *Алгебраическая система вида* $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$ *является верхней полурешеткой, но не решеткой в общем случае.*

Справедливо

Утверждение 4. *Для локально замкнутых алгебраических систем* $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$ *существует представление для всякого* $A_0 \in \mathbf{A}$ *и произвольного множества* $F \subseteq \mathbf{A}$.

Для финитно разделимых и локально замкнутых алгебраических систем вида $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$ справедлив метрический критерий финитной представимости:

Теорема 5. *Финитное представление для* $A_0 \in \mathbf{A}$ *и множества* $F \subseteq \mathbf{A}$ *существует тогда и только тогда, когда* $A_0 \notin LimF$.

Алгебраическая структура представлений в финитно разделимых и локально замкнутых алгебраических системах $(\mathbf{A}, \leqslant, \nabla, \triangle, \mathrm{n})$ описывается следующей

Теорема 6. *1. Множество представлений для фиксированных A_0 и F является идемпотентной и коммутативной полугруппой относительно операции $\odot$.*

2. Множество финитных представлений для фиксированных A_0 и F является идемпотентной и коммутативной полугруппой относительно операции $\odot$.

Заключение

В данной работе обобщен метрический критерий представимости, полученный ранее авторами для классов автоматов Мили [1, 3] и классов неструктурированных объектов [4].

Список литературы

[1] Грунский И. С., Козловский В. А. Синтез и идентификация автоматов. — Киев.: Наукова думка, 2004.

[2] Бородай С. Ю. Эксперименты в эффективно заданных классах автоматов: Автореферат канд. физ.-мат. наук; 01.01.09 / СГУ. — Саратов, 1997.

[3] Максименко И. И. Эксперименты в финитно-определенных метрических пространствах автоматов: Автореферат канд. физ.-мат. наук; 01.01.09 / СГУ — Саратов, 2000.

[4] Максименко И. И. Финитные представления неструктурированных объектов // Труды института прикладной математики и механики. — 2009. Т. 19. — С. 162–167.

Решетка замкнутых классов самодвойственных функций трехзначной логики

Жук Д. Н. (Москва, МГУ им. М. В. Ломоносова)

zhuk@intsys.msu.ru

В работе описывается решетка замкнутых классов трехзначной логики, которые вкладываются в предполный класс самодвойственных функций. Также в работе описаны различные свойства этой решетки: выделены все конечно-порожденные и предикато-описуемые классы; найдены мощности надрешеток и подрешеток для всех классов.

Введение

В работах [1, 2] Э. Пост описал все замкнутый классы двузначной логики. Их оказалось счётное количество, причем все они конечно-порождены. Но в 1959 году было показано, что уже в трехзначной логике континуум замкнутых классов. С. В. Яблонский [4] описал все предполные классы трехзначной логики. Оказалось [5, 7], что во всех предполных классах кроме предполного класса линейных функций континуум замкнутых подклассов.

В настоящей работе исследуется структура замкнутых классов в предполном классе самодвойственных функций. Важные результаты в этой области были получены С. С. Марченковым. Он описал многие замкнутые классы [6], а также доказал, что решетка замкнутых классов самодвойственных функций континуальна [7]. Но несмотря на континуальность, автору удалось в явном виде описать структуру всех замкнутых классов самодвойственных функций. С помощью этого описания, в работе доказываются различные свойства полученной решетки. В частности выделяются все конечно-порожденные и предикатно-описуемые классы, найдены мощности подклассов и надклассов для каждого замкнутого класса.

Описание решетки замкнутых классов

Пусть $\mathbb{N} = \{1, 2, 3, \dots\}$ — множество всех натуральных чисел, $\mathbb{N}_0 = N \cup \{0\}$, $E_k = \{0, 1, 2, \dots, k-1\}$, P_k — множество всех функ-

ций k-значной логики, R_k — множество всех отношений или предикатов k-значной логики. В работе предикаты будем изображать в виде матриц, в которых столбцам соответствуют наборы, на которых предикат принимает значение 1. Для $S \subseteq R_k$ через $Pol(S)$ обозначим множество всех функций из P_k, сохраняющих каждый предикат из множества S.

Пусть $m \in \mathbb{N}$, $n \in \mathbb{N}_0$, $A_1, \ldots, A_m \subseteq \{1, 2, \ldots, n\}$, $A_1 \cup \ldots \cup A_m = \{1, 2, \ldots, n\}$. (В случае, если $n = 0$ имеем $A_1 = A_2 = \ldots = A_m = \varnothing$). Тогда предикат $\pi_{A_1,\ldots,A_m} \in R^{m+n}$ определяется следующим соотношением:

$$\pi_{A_1,\ldots,A_m}(x_1, \ldots, x_m, y_1, \ldots, y_n) = 1$$

точно тогда, когда выполняются следующие условия:

1) $x_i \in \{0, 1\}$ для любого $i \in \{1, \ldots, m\}$;

2) $(x_i = 1) \vee (y_j \in \{0, 1\})$ для любых $i \in \{1, \ldots, m\}$, $j \in A_i$;

3) хотя бы одно из значений $x_1, \ldots, x_m, y_1, \ldots, y_n$ отлично от нуля.

Через Π_n^m обозначим множество всех таких предикатов. Пусть $\Pi^l = \bigcup\limits_{3 \leqslant m+n \leqslant l} \Pi_n^m, \Pi_l = \bigcup\limits_{n \leqslant l, m+n \geqslant 3} \Pi_n^m, \Pi = \bigcup\limits_{l} \Pi^l$.

На множестве Π определяется рефлексивное и транзитивное бинарное отношение $\lesssim$ [9]. При этом доказывается, что для любого $\rho \in \Pi_n^m$ выполняется $\{\sigma \in \Pi | \sigma \lesssim \rho\} \subseteq \Pi^{m+n}$.

Пусть $\sigma : E_3 \longrightarrow E_3$, $\sigma(0) = 1$, $\sigma(1) = 0$, $\sigma(2) = 2$. Каждому предикату ρ сопоставим предикат ρ^*, двойственный относительно замены нуля на единицу:

$$\rho^*(x_1, \ldots, x_n) := \rho(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)).$$

Для $S \subseteq R$ положим $S^* := \{\rho | \rho^* \in S\}$.

Будем говорить, что множество $F \subseteq \Pi$ замкнуто относительно отношения $\lesssim$, если

$$\forall \rho \in F, \forall \rho' \in \Pi \; (\rho' \lesssim \rho \implies \rho' \in F).$$

Пусть $F \subseteq \Pi$, положим

$$Clone(F) = Pol\left(F \cup \left\{ \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \end{pmatrix} \right\}\right),$$

$$Clone^*(F) = Pol\left(F^* \cup \left\{\begin{pmatrix}0&1&2\\1&2&0\end{pmatrix}, \begin{pmatrix}1&1&0&0&0\\0&1&0&1&2\end{pmatrix}\right\}\right).$$

Теперь определим семейство замкнутых классов Υ.

Семейство Υ. Пусть $F \subseteq \Pi$ непусто и замкнуто относительно отношения $\lesssim$, тогда $Clone(F), Clone^*(F) \in \Upsilon$. Других замкнутых классов в семействе Υ нет.

Теорема 1. *Пусть $F_1, F_2 \subseteq \Pi$ непусты и замкнуты относительно отношения $\lesssim$, тогда $Clone(F_1) \subseteq Clone(F_2) \Longleftrightarrow F_1 \supseteq F_2$.*

Следствие. *Пусть $F_1, F_2 \subseteq \Pi$ непустые и замкнутые относительно отношения $\lesssim$, причём $F_1 \neq F_2$, тогда $Clone(F_1) \neq Clone(F_2)$.*

Определим некоторые предикаты, которые понадобятся нам в дальнейшем:

$$\rho_{+1} = \begin{pmatrix}0&1&2\\1&2&0\end{pmatrix}, \ \rho_T = \begin{pmatrix}0&1&2\\1&0&2\end{pmatrix}, \ \rho_N = \begin{pmatrix}0&1&1&1\\0&0&1&2\end{pmatrix},$$

$$\rho_W = \begin{pmatrix}0&0&1&1&1\\0&1&0&1&2\end{pmatrix}, \ \rho_Q = \begin{pmatrix}0&0&0&0&1&1&1\\0&0&1&1&0&1&1\\0&1&0&1&1&0&1\end{pmatrix},$$

$$\rho_L(x_1, x_2, x_3) = 1 \Longleftrightarrow x_1 + x_2 = 2x_3 (mod\ 3),$$

$$\rho_{L2}(x_1, x_2, x_3, x_4) = 1 \Longleftrightarrow (\forall i\ x_i \in \{0,1\}) \wedge (x_1 + x_2 = x_3 + x_4 (mod\ 2)),$$

$$\rho_{\vee,n}(x_1, \ldots, x_n) = 1 \Longleftrightarrow$$
$$\Longleftrightarrow (\forall i\ x_i \in \{0,1\}) \wedge ((x_1 = 1) \vee (x_2 = 1) \vee \ldots \vee (x_n = 1)),$$

$$\rho_{\wedge,n}(x_1, \ldots, x_n) = 1 \Longleftrightarrow$$
$$\Longleftrightarrow (\forall i\ x_i \in \{0,1\}) \wedge ((x_1 = 0) \vee (x_2 = 0) \vee \ldots \vee (x_n = 0)),$$

$$\rho_{=,01}(x_1, x_2, x_3) = 1 \Longleftrightarrow$$
$$\Longleftrightarrow (x_1 = 1) \vee ((x_1 = 0) \wedge (x_2, x_3 \in \{0,1\}) \wedge (x_2 = x_3)),$$

$$\rho_{=,10}(x_1, x_2, x_3) = 1 \Longleftrightarrow$$
$$\Longleftrightarrow (x_1 = 0) \vee ((x_1 = 1) \wedge (x_2, x_3 \in \{0,1\}) \wedge (x_2 = x_3)),$$

$$\rho_{=,012}(x_1,x_2,x_3)=1 \Longleftrightarrow (x_1=1)\vee((x_1=0)\wedge(x_2=x_3)),$$
$$\rho_{=,102}(x_1,x_2,x_3)=1 \Longleftrightarrow (x_1=0)\vee((x_1=1)\wedge(x_2=x_3)),$$

Определим ещё два семейства замкнутых классов:
Семейство Θ.

$$\mathbf{S}=Pol\left(\{\rho_{+1}\}\right),\ \mathbf{S_0}=Pol\left(\{\rho_{+1},(0)\}\right),\ \mathbf{SL}=Pol\left(\{\rho_{+1},\rho_L\}\right),$$
$$\mathbf{1S}=[\{(x+1)(mod 3)\}],\ \mathbf{SL_0}=Pol\left(\{\rho_{+1},\rho_L,(0)\}\right),$$
$$\mathbf{T}=Pol\left(\{\rho_{+1},\}\right),\ \mathbf{C}=Pol\left(\left\{\rho_{+1},\begin{pmatrix}0 & 1\end{pmatrix}\right\}\right),$$
$$\mathbf{D}=Pol\left(\left\{\rho_{+1},\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right\}\right),\ \mathbf{M}=Pol\left(\left\{\rho_{+1},\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 1\end{pmatrix}\right\}\right),$$
$$\mathbf{DM}=\mathbf{D}\cap\mathbf{M},\ \mathbf{DN}=Pol\left(\{\rho_{+1},\rho_N,\rho_N^*\}\right),$$
$$\mathbf{TD}=\mathbf{T}\cap\mathbf{D},\ \mathbf{TM}=\mathbf{T}\cap\mathbf{M},\ \mathbf{TN}=\mathbf{DN}\cap\mathbf{T},$$
$$\mathbf{L}=Pol\left(\{\rho_{+1},\rho_{L2}\}\right),\ \mathbf{TL}=\mathbf{L}\cap\mathbf{T},\ \mathbf{C_2}=\mathbf{L}\cap\mathbf{M},$$
$$\mathbf{TC_2}=\mathbf{C_2}\cap\mathbf{T},\ \mathbf{O}=[\{x\}].$$

Семейство Φ. Для $n\geqslant 2$

$$\mathbf{a_n}=Pol\left(\{\rho_{+1},\rho_{\vee,n}\}\right),\ \mathbf{A_n}=Pol\left(\{\rho_{+1},\rho_{\wedge,n}\}\right),$$
$$\mathbf{a_nM}=\mathbf{a_n}\cap\mathbf{M},\ \mathbf{A_nM}=\mathbf{A_n}\cap\mathbf{M},$$
$$\mathbf{a_nN}=Pol\left(\{\rho_{+1},\rho_{\vee,n},\rho_N\}\right),\ \mathbf{A_nN}=Pol\left(\{\rho_{+1},\rho_{\wedge,n}\rho_N^*\}\right),$$
$$\mathbf{a}_\infty=\bigcap_n\mathbf{a_n},\ \mathbf{A}_\infty=\bigcap_n\mathbf{A_n},$$
$$\mathbf{a}_\infty\mathbf{M}=\bigcap_n\mathbf{a_nM},\ \mathbf{A}_\infty\mathbf{M}=\bigcap_n\mathbf{A_nM},$$
$$\mathbf{a}_\infty\mathbf{N}=\bigcap_n\mathbf{a_nN},\ \mathbf{A}_\infty\mathbf{N}=\bigcap_n\mathbf{A_nN},$$
$$\mathbf{aP}=Pol\left(\{\rho_{+1},\rho_Q\}\right),\ \mathbf{AP}=Pol\left(\left\{\rho_{+1},\rho_Q^*\right\}\right),$$
$$\mathbf{aPN}=Pol\left(\{\rho_{+1},\rho_Q,\rho_N\}\right),\ \mathbf{APN}=Pol\left(\left\{\rho_{+1},\rho_Q^*,\rho_N^*\right\}\right),$$
$$\mathbf{aP_1}=Pol\left(\{\rho_{+1},\rho_Q,\rho_W,\}\right),\ \mathbf{AP_1}=Pol\left(\left\{\rho_{+1},\rho_Q^*,\rho_W^*\right\}\right).$$
$$\mathbf{aP_n}=\mathbf{aP_1}\cap Pol(\pi_{\{1,2,\ldots,n\}}),\mathbf{AP_n}=\mathbf{AP_1}\cap Pol(\pi^*_{\{1,2,\ldots,n\}}),\ \text{где } n\geqslant 2.$$

$$\mathbf{aP}_\infty = \bigcap_n \mathbf{aP_n},\ \mathbf{AP}_\infty = \bigcap_n \mathbf{AP_n},$$
$$\mathbf{aQ} = Pol\left(\{\rho_{+1}, \rho_{=,01}\}\right),\ \mathbf{AQ} = Pol\left(\{\rho_{+1}, \rho_{=,10}\}\right),$$
$$\mathbf{aW} = Pol\left(\{\rho_{+1}, \rho_{=,012}\}\right),\ \mathbf{AW} = Pol\left(\{\rho_{+1}, \rho_{=,102}\}\right).$$

Теорема 2. *Множество* $\Upsilon \cup \Theta \cup \Phi$ *содержит все замкнутые классы, которые вкладываются в* $Pol\left(\{\rho_{+1}\}\right)$.

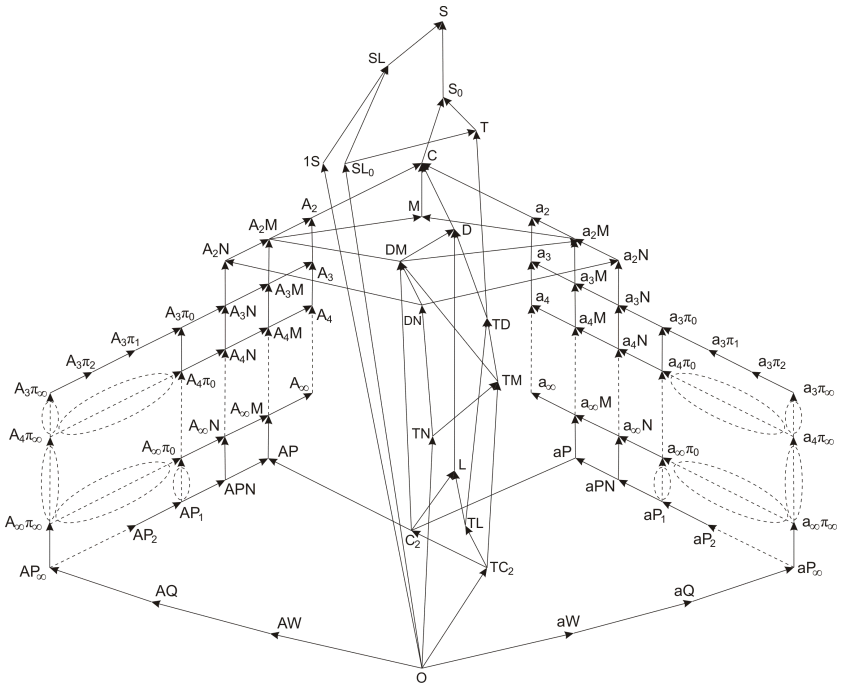


Рис. 1. Структура замкнутых классов.

Попарная вложимость замкнутых классов друг в друга для семейств Θ и Φ схематично изображена на рис. 1 в виде графа, где замкнутым классам соответствуют вершины графа. Две вершины графа M_1 и M_2 соединены сплошным ребром, причём M_1 расположена выше M_2, точно тогда, когда $M_2 \subset M_1$, и не существует замкнутого

класса M', такого что $M_2 \subset M' \subset M_1$. Две вершины графа M_1 и M_2 соединены пунктиром, причём M_1 расположена выше M_2, точно тогда, когда $M_2 \subset M_1$ и существует бесконечная последовательность замкнутых классов $K_1 \supset K_2 \supset K_3 \supset \ldots$, такая что $K_1 \subset M_1$; $\bigcap\limits_i K_i = M_2$; если $M_2 \subset M' \subset M_1$, то $M' = K_i$ для какого-то i. В некоторых других случаях пунктирное ребро между двумя вершинами помещается в пунктирный эллипс. Это означает, что вложимость этих классов не подходит под предыдущие два случая.

Также на рис. 1 изображены некоторые замкнутые классы из семейства Υ. Для $n \geqslant 3$ положим

$$\begin{gathered}
\mathbf{a_n\pi_0} = Clone(\Pi^n \cap \Pi_0),\ \mathbf{A_n\pi_0} = Clone^*(\Pi^n \cap \Pi_0),\\
\mathbf{a_n\pi_\infty} = Clone(\Pi^n),\ \mathbf{A_n\pi_\infty} = Clone^*(\Pi^n),\\
\mathbf{a_\infty\pi_0} = Clone(\Pi_0),\ \mathbf{A_\infty\pi_0} = Clone^*(\Pi_0),\\
\mathbf{a_\infty\pi_\infty} = Clone(\Pi),\ \mathbf{A_\infty\pi_\infty} = Clone^*(\Pi),\\
\mathbf{a_3\pi_1} = Clone(\pi_{\{1\},\{1\}}),\ \mathbf{A_3\pi_1} = Clone^*(\pi_{\{1\},\{1\}}),\\
\mathbf{a_3\pi_2} = Clone(\pi_{\{1\},\varnothing}),\ \mathbf{A_3\pi_2} = Clone^*(\pi_{\{1\},\varnothing}).
\end{gathered}$$

Свойства семейств Θ, Φ и Υ

Замкнутый класс $M \subseteq P_3$ называется конечно-порожденным, если существует конечное множество $M_0 \subseteq M$, такое что $M = [M_0]$. Замкнутый класс $M \subseteq P_3$ называется предикатно-описуемым, если существует конечное множество $S \subseteq R$, такое что $M = Pol(S)$. Как следует из предыдущей главы, все замкнутые классы в семействах Θ и Φ конечно-порождены. Положим

$$\rho_1 < \rho_2 \Longleftrightarrow \rho_1 \lesssim \rho_2 \wedge \neg(\rho_2 \lesssim \rho_1).$$
$$Bound(F) := \{\rho \in \Pi | \rho \notin F, \forall \sigma \in \Pi(\sigma < \rho \Longrightarrow \sigma \in F)\}.$$

Теорема 3. *Пусть $F \subseteq \Pi$, F — непусто и замкнуто относительно отношения $\lesssim$, тогда $Clone(F)$ конечно-порожден точно тогда, когда множество $Bound(F)$ конечно.*

Следствие. *Пусть $F \subseteq \Pi$, F — непусто и замкнуто относительно отношения $\lesssim$, $|F| < \infty$, тогда $Clone(F)$ конечно-порожден.*

Теорема 4. *Замкнутый класс $M \in \Theta \cup \Phi$ предикатно-описуем точно тогда, когда*

$$M \notin \{\mathbf{a}_\infty, \mathbf{A}_\infty, \mathbf{a}_\infty\mathbf{M}, \mathbf{A}_\infty\mathbf{M}, \mathbf{a}_\infty\mathbf{N}, \mathbf{A}_\infty\mathbf{N}, \mathbf{aP}_\infty, \mathbf{AP}_\infty\}.$$

Теорема 5. *Пусть $F \subseteq \Pi$, F — непусто и замкнуто относительно отношения $\lesssim$, тогда $Clone(F)$ предикатно-описуем точно тогда, когда F конечно.*

Пусть M_1, M_2 — замкнутые классы из $\Upsilon \cup \Phi \cup \Theta$, причём $M_1 \subset M_2$, тогда будем говорить, что M_1 — подкласс M_2, а M_2 — надкласс M_1. Следующие теоремы описывают мощность множества подклассов и надклассов для замкнутых классов из $\Upsilon \cup \Phi \cup \Theta$.

Теорема 6. *Пусть $F \subseteq \Pi$ — непусто и замкнуто относительно отношения $\lesssim$, тогда мощность множества подклассов $Clone(F)$ континуальна тогда и только тогда, когда $F \neq \Pi$. Мощность множества подклассов $\mathbf{A}_\infty\pi_\infty = Clone(\Pi)$ конечна.*

Теорема 7. *Пусть $M \in \Theta \cup \Phi$, тогда мощность множества подклассов M*

- *счётна, если $M \in \{\mathbf{aP}, \mathbf{aPN}, \mathbf{aP_1}, \mathbf{aP_2}, \mathbf{aP_3}, \ldots, \mathbf{AP}, \mathbf{APN}, \mathbf{AP_1}, \mathbf{AP_2}, \mathbf{AP_3}, \ldots\}$,*
- *континуальна, если $M \in \{\mathbf{S}, \mathbf{S_0}, \mathbf{C}, \mathbf{M}, \mathbf{a}_\infty, \mathbf{A}_\infty, \mathbf{a}_\infty\mathbf{M}, \mathbf{A}_\infty\mathbf{M}, \mathbf{a}_\infty\mathbf{N}, \mathbf{A}_\infty\mathbf{N}\}$, либо $M \in \bigcup\limits_{n \geqslant 2} \{\mathbf{a_n}, \mathbf{A_n}, \mathbf{a_n}\mathbf{M}, \mathbf{A_n}\mathbf{M}, \mathbf{a_n}\mathbf{N}, \mathbf{A_n}\mathbf{N}\}$,*
- *конечна в остальных случаях.*

Теорема 8. *Пусть $F \subseteq \Pi$ — непусто и замкнуто относительно отношения $\lesssim$, тогда мощность множества надклассов $Clone(F)$ континуальна, если F содержит бесконечное подмножество, состоящее из попарно несравнимых предикатов; конечна, если F — конечно; и счётна в остальных случаях.*

Следствие. *Для $n \geqslant 3$ мощность множества надклассов $\mathbf{a_n}\pi_\infty$ конечна.*

Теорема 9. *Пусть $M \in \Theta \cup \Phi$, тогда мощность множества надклассов M*

- *счётна, если* $M \in \{\mathbf{a}_\infty, \mathbf{A}_\infty, \mathbf{a}_\infty\mathbf{M}, \mathbf{A}_\infty\mathbf{M}, \mathbf{a}_\infty\mathbf{N}, \mathbf{A}_\infty\mathbf{N}, \mathbf{aP}, \mathbf{aPN}, \mathbf{aP_1}, \mathbf{aP_2}, \mathbf{aP_3}, \ldots, \mathbf{AP}, \mathbf{APN}, \mathbf{AP_1}, \mathbf{AP_2}, \mathbf{AP_3}, \ldots\}$,
- *континуальна, если* $M \in \{\mathbf{aP}_\infty, \mathbf{AP}_\infty, \mathbf{aQ}, \mathbf{AQ}, \mathbf{aW}, \mathbf{AW}, \mathbf{C_2}, \mathbf{TC_2}, \mathbf{O}\}$,
- *конечна в остальных случаях.*

Условно говоря, из этих теорем и следствия следует, что континуум замкнутых классов расположен на рис. 1 вблизи точки $\mathbf{a}_\infty\pi_\infty$, так как для любого $n \geqslant 3$ мощность множества надклассов $\mathbf{a_n}\pi_\infty$ конечна и для любого $m \geqslant 1$ мощность множества надклассов $\mathbf{aP_m}$ счётна.

Список литературы

[1] Post E. Determination of all closed systems of truth tables // Bull. Amer. Math. Soc. — 1920. 26. 427.

[2] Post E. Two-Valued Iterative Systems of Mathematical Logic. — Princeton: Princeton Univ. Press, 1941.

[3] Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. Т. 127. № 1. — С. 44–46.

[4] Яблонский С. В. О функциональной полноте в трехзначном исчислении // Докл. АН СССР. — 1954. 95. — С. 1153–1155.

[5] Demetrovics J., Hannak L. The number of reducts of preprimial algebra // Algebra Universalis. — 1983. Vol. 16. N 1. — P. 178–185.

[6] Марченков С. С., Деметрович Я, Ханнак Л. О замкнутых классах самодвойственных функций в P_3 // Методы дискретного анализа и решении комбинаторных задач. — 1980. 34. — С. 38–73.

[7] Марченков С. С. О замкнутых классах самодвойственных функций многозначной логики // Проблемы кибернетики. — 1983. 40. — С. 261–266.

[8] Бондарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста I-II // Кибернетика. — 1969. 3. 1–10. 5. 1–9.

[9] Жук Д. Н. Решетка замкнутых классов самодвойственных функций трехзначной логики. М.: Изд-во МГУ, 2011.

О некоторых аспектах теоремы Римана — Роха на конечных графах

Иванов И. О. (Москва, МГУ им. М. В. Ломоносова)

truefet@gmail.com

В своей работе [1] Matthew Baker и Serguei Norine спроецировали хорошо известную теорему Римана — Роха на графы, рассматривая на них целочисленные дивизоры. При этом они установили связь своей теории с несколько изменённой Chip-Firing Game, введённой Biggs'ом в [2]. Biggs в своих работах [3, 4, 5] проводит связь этой игры с хроматическим числом графа и полиномом Tutte, характеризующим степень связности графа. В [6] была доказана теорема Римана — Роха для дивизоров с рационально-значными элементами.

Данная работа посвящена необходимости нахождения эффективного алгоритма, находящего выигрышную стратегию, либо утверждающего, что её не существует. Этот же алгоритм поможет в нахождении размерности линейной оболочки дивизора, введённой в [1].

Теорема 1. *Существует алгоритм, который решает Chip-Firing Game для дивизора на полном графе с n вершинами за $2n^2 + 1$ операцию.*

Теорема 2. *Существует алгоритм, который решает Chip-Firing Game для дивизора на полном двудольном графе с n и m вершинами в долях соответственно за $2n^2 + 5n + 3mn + m + 1$ операций.*

Благодарю моего научного руководителя Ирматова Анвара Адхамовича за ценные рекомендации и советы.

Список литературы

[1] Baker M., Norine S. Riemann-Roch and Abel-Jacobi theory on a finite graph.

[2] Biggs N. Algebraic potential theory of graphs.

[3] Biggs N. Chip-firing and the critical group of a graph.

[4] Biggs N. The Tutte polynomial as a growth function.

[5] Biggs N., Winkler P. Chip-firing and the chromatic polynomial.

[6] James R., Miranda R. A Riemann-Roch theorem for edge-weighted graphs.

О сложности тестирования логических устройств на некоторые типы неисправностей

Икрамов А. А. (Москва, МГУ им. М. В. Ломоносова)

melan44@mail.ru

В статье рассматриваются сложности тестирования на разнотипные неисправности. Для некоторых классов получены точные значения, для других верхние и нижние оценки. Также рассмотрен случай для почти всех булевых функций на класс инверсных неисправностей и нижняя оценка для перепутываний не более двух переменных

Определение. Неисправностью назовем отображение $\varphi\colon E_2^n \to Q$, где $Q \subset E_2^n$ и $\exists \alpha \in E_2^n\colon \varphi(\alpha) \neq \alpha$.

Определение. Проверяющим тестом для класса неисправностей Φ и функции $f \in P_2(n)$ назовем $T \subset E_2^n$ такое, что $\forall \varphi \in \Phi \quad \exists\, \alpha \in T\colon f(\varphi(\alpha)) \neq f(\alpha)$.

Определение. Сложностью тестирования функции $f \in P_2(n)$ на класс неисправностей Φ назовем $L(f, \Phi) = \min |T|$ среди всех проверяющих тестов T.

Определение. Сложностью тестирования класса неисправностей Φ для $P_2(n)$ назовем величину $L(n, \Phi) = \max_{f \in P_2(n)} L(f, \Phi)$.

Определение. Классом инверсных неисправностей F_{in}^2 назовем множество всех $\varphi_\sigma\colon \varphi_\sigma(\alpha) = \alpha \oplus \sigma$, $\sigma \in E_2^n \setminus \{0\}$. Через $F_{in}^2(p)$ обозначим класс таких φ_σ, что $||\sigma|| = p$.

Теорема 1. *Для почти всех* $f \in P_2(n) \quad L(f, F_{in}^2(1)) = 1$.

Доказательство. Рассмотрим произвольный набор $\tilde{\alpha} \in E_2^n$. Все наборы $\tilde{\beta}$, находящиеся от него на расстоянии 1 по Хеммингу, образуют шар, в который рассматриваемая неисправность может перевести данный набор. Если $f(\tilde{\alpha}) \neq f(\tilde{\beta})$ для всех таких $\tilde{\beta}$, то набор $\tilde{\alpha}$ является тестовым для данной функции. Оценим количество функций, у которых существует такой набор. Число наборов, у которых нужно зафиксировать значения равно $n + 1$. Теперь возьмем другие $n + 1$ наборов, связанных требованием на расстояние. Чтобы генерируемые здесь функции не совпали, мы вычеркнем из возможных значений на предыдущих $n+1$ наборе то значение, что зафиксировали на предыдущем шаге. Получим $2^{n+1} - 1$ значений на них. Таким образом, на

каждом последующем шаге мы генерируем различные функции. Посчитаем их общее количество:

$$\sum_{k=1}^{t(n)} 2^{2^n-k(n+1)} \cdot (2^{n+1}-1)^{k-1} = 2^{2^n-n-1} \sum_{k=0}^{t(n)-1} \left(\frac{2^{n+1}-1}{2^{n+1}}\right)^k \to_{n\to\infty}$$

$$\to 2^{2^n-n-1} \cdot \frac{1}{1-\frac{2^{n+1}-1}{2^{n+1}}} = 2^{2^n-n-1} \cdot 2^{n+1} = 2^{2^n}.$$

Здесь $t(n)$ — число возможных разбиений булева куба на шары радиуса 1. Это число равно числу кодов Хемминга, исправляющих одну ошибку, то есть $t(n) = 2^{n-[\log_2 n]-1}$. Таким образом, почти все булевы функции имеют тестовый набор на $F^2_{in}(1)$.

Определение. Классом неисправностей типа конъюнктивных слипаний $S^2_{\&}$ назовем класс разбиений множества переменных X^n и значением переменной x_i будет являться минимальное значение из всех переменных ее множества.

Определение. Классом неисправностей типа конъюнктивных слипаний $S^2_{\vee}$ назовем класс разбиений множества переменных X^n и значением переменной x_i будет являться максимальное значение из всех переменных ее множества.

В [1] даются нижняя и верхняя оценки: $n-1 \leqslant L(n, S^2_{\vee} \cup F^2_{in}(1)) \leqslant n$ (Предложение 18). Докажем следующее:

Теорема 2. $\forall n \geqslant 2 \quad L(n, S^2_{\vee} \cup F^2_{in}(1)) = n.$

Доказательство. Рассмотрим функцию $x_1 \& x_2 \& \ldots \& x_n$. Каждый набор слоя $n-1$ проверяет эту функцию на слипание переменной, равной на нем 0, с остальными переменными. Значит, достаточно $n-1$ набора, чтобы проверить на все неисправности типа слипания (оставшаяся переменная, которая среди всех взятых наборов принимает значение 1, уже проверена на слипание, так как все остальные от нее отделены). Однако, эта оставшаяся переменная не проверена на инверсию. Следовательно, необходимо добавить оставшийся набор из слоя $n-1$ для проверки на инверсию (либо набор из всех единиц). Таким образом, сложность тестирования этой функции равна n.

По принципу двойственности верно следующее утверждение (возьмем функцию $x_1 \vee x_2 \vee \ldots \vee x_n$):

Теорема 3. $\forall n \geqslant 2 \quad L(n, S^2_{\&} \cup F^2_{in}(1)) = n.$

Так как имеем $L(n, S^2_{\vee}) = n - 1$ (доказано в [1]), то по принципу двойственности верно $L(n, S^2_{\vee}) = n - 1$. Значит, очевидна оценка $L(n, S^2_{\vee} \cup S^2_{\&}) \leqslant 2(n-1)$. Докажем, что здесь верно равенство:

Теорема 4. $\forall n \geqslant 3 \quad L(n, S^2_{\vee} \cup S^2_{\&}) = 2(n-1).$

Доказательство. Рассмотрим функцию $(x_1 \vee x_2 \vee \ldots \vee x_n) \oplus x_1 \& x_2 \& \ldots \& x_n$. Для тестирования на все виды слипания нужно по $n-1$ набору со слоев 1 и $n-1$. Так как в этом случае они не пересекаются, то получаем равенство.

Из теорем 2, 3, 4 получаем следствие:

Теорема 5. $\forall n \geqslant 2 \quad 2n - 2 \leqslant L(n, S^2_{\vee} \cup S^2_{\&} \cup F^2_{in}(1)) \leqslant 2n - 1.$

Определение. Перестановка s множества индексов переменных из X^n называется неисправностью типа перепутывания кратности $p = \sum_{i=1}^{n} \mathrm{sign}|s(i) - i|$, если $p > 0$.

Обозначим класс неисправностей типа перепутывания над алгеброй логики через W^2. Класс таких неисправностей кратности p — через $W^2(p)$.

Теорема 6. $L(n, W^2(2)) \geqslant n - 1.$

Доказательство. Построим следующую функцию: пусть она всюду равна 1, кроме следующих наборов: в слое $n-1$ набор $(1, \ldots, 1, 0)$, в слое $n-2$ набор $(1, \ldots, 1, 0, 0)$ и так далее до слоя 1 с набором $(1, 0, \ldots, 0)$. Тогда эти наборы будут тестовыми (их $n-1$): каждый проверяет уникальную неисправность (для набора из слоя i перестановку переменных x_i и x_{i+1}, которую никакие другие наборы не проверяют. Следовательно, сложность тестирования на перепутывание не более двух переменных не меньше $n-1$.

Выражаю благодарность за помощь в написании работы своему научному руководителю Кудрявцеву Валерию Борисовичу.

Список литературы

[1] Кудрявцев В. Б., Гасанов Э. Э., Долотова О. А., Погосян Г. Р. Теория тестирования логических устройств. — М.: Физматлит, 2006.

Декомпозиция графа по средней плотности

Магомедов А. М., Магомедов М. А. (Махачкала)

magomedtagir1@yandex.ru

Для заданного графа $G = (V, E)$, где V — множество вершин, E — множество рёбер (допускаются параллельные рёбра и петли), обозначим наибольшую степень вершины через $\Delta(G)$, а наибольшее значение «средней плотности» подграфа $G' = (V', E') \subseteq G$ (отношения числа рёбер $|E'|$ к числу вершин $|V'|$) — через $mad\,(G)$.

В [1, 2] построены алгоритмы вычисления $mad\,(G)$ за время $O(M(|V|, |V| + |E|) \log |V|)$, где $M(a, b)$ — время нахождения минимального разреза в сети с a вершинами и b рёбрами.

Понятие средней плотности графа используется в задачах оптимизации расписаний. Пусть каждому прибору из некоторого заданного множества предписан для обработки набор из двух требований — элементов множества $\{1, 2, \ldots, n\}$ (необязательно различных), над каждым из двух требований прибор должен выполнить операцию единичной длительности; одновременно требование (или прибор) может участвовать разве лишь в одной операции. Если $G = (V, E)$ — граф с множеством вершин $V = \{v_1, \ldots, v_n\}$, где количество рёбер вида (v_i, v_j) в множестве E равно количеству приборов с предписанным набором (i, j), то результат статьи [3] формулируется следующим образом: *построение расписания нечетной длительности* $\Delta(G)$*, где каждый прибор выполняет запланированные операции в последовательные промежутки времени, возможно тогда и только тогда, когда*

$$mad\,(G) \leqslant \lfloor \Delta(G)/2 \rfloor\,. \tag{1}$$

Для $\Delta(G) = 5$ результат был получен ранее в [4].

Здесь и ниже ограничение рассмотрения графами нечетной степени объясняется не только соображениями краткости, но и тем обстоятельством, что рассмотрение для графов четной степени существенно проще (и базируется на классической теореме Петерсена о разбиении связного регулярного графа четной степени на гамильтоновы циклы [5]).

В задачах оптимизации расписаний (и интервальной рёберной раскраски графа) востребованы такие разбиения расписания (графа), где существование решения задачи для всего расписания (графа) равносильно существованию решения соответствующей подзадачи для каждого подрасписания (подграфа) — элемента разбиения.

Пусть $G = (V, E)$ — граф нечетной степени, p_1 и p_2 — нечетные натуральные числа,

$$p_1 + p_2 = \Delta(G) + 1; \quad 3 \leqslant p_i \leqslant \Delta(G) - 2, \quad i = 1, 2.$$

Разбиение множества E на подмножества E_1 и E_2 будем называть *декомпозицией по средней плотности*, если подграфы G_1 и G_2 графа G, порожденные соответственно E_1 и E_2, удовлетворяют условиям: 1) для каждой вершины $v \in V$ равенства $d_{G_i}v = p_i$ и $d_{G_{3-i}}v = p_{3-i} - 1$ равносильны
2) $\Delta(G_i) = p_i$
3) $mad\,(G_i) \leqslant \lfloor p_i/2 \rfloor$; $i = 1, 2$

Теорема. *Декомпозиция графа G по средней плотности существует тогда и только тогда, когда имеет место (1).*

Заметим, что свойство (1) при $\Delta(G) = 3$ является наследуемым и означает, что всякая связная компонента графа G содержит не более одного цикла.

Работа выполнена при финансовой поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» № 2011–1.3.2–111–017/12.

Список литературы

[1] Picard J.-C., Queyranne M. A network flow solution to some nonlinear 0-1 programming problems, with applications to graph theory // Networks. — 1982. V. 12. — P. 141–159.

[2] Goldberg A. V. Finding a maximum density subgraph // Technical Report. — Berkeley / University of California, Computer Science Division, 1984. (Identifier: CSD–84–171).

[3] Магомедов А. М. Непрерывное расписание с двухэлементными предписаниями // Известия Саратовского университета. Новая серия. Сер. «Математика. Механика. Информатика». — 2011. Т. 11. Вып. 2. — С. 113–119.

[4] Сапоженко А. А., Магомедов А. М. Условия существования непрерывных расписаний длительности пять // Вестник МГУ. Сер. «Вычислительная математика и кибернетика». — 2010. Т. 34. № 1. — С. 39–44.

[5] Petersen J. Die theorie der regulären graphen // Acta Math. — 1891. 15. — P. 193–220. JBuch. 23.115.

О формулах числа классов эквивалентности и числе пороговых функций

Носов М. В. (Москва, МГУ им. М. В. Ломоносова)

mvnosov@rambler.ru

В работе представлены некоторые формулы числа классов эквивалентности, которые использованы для вывода комбинаторного арифметического выражения, задающего число пороговых функций.

1. Некоторые формулы числа классов эквивалентности

Пусть на конечном множестве M введено отношение эквивалентности, функция $r : M \times M \longrightarrow \{0, 1\}$ определяется следующим образом:

$$r(a,b) = \begin{cases} 1, & \text{если } a \text{ и } b \text{ эквивалентны,} \\ 0, & \text{если } a \text{ и } b \text{ не эквивалентны.} \end{cases}$$

Пусть N — число классов эквивалентности. Справедливы следующие формулы

$$N = \sum_{a \in M} \frac{1}{\sum\limits_{b \in M} r(a,b)},$$

$$N = \sum_{a \in M} \sum_{\beta \subseteq M, \beta \neq \varnothing} \frac{1}{|\beta|} \prod_{b \in \beta} r(a,b) \prod_{b \notin \beta} (1 - r(a,b)),$$

во второй формуле при $\beta = M$ последнее произведение равно 1. Имеют место простые комбинаторные утверждения

Утверждение 1. *Пусть q_i — переменные, $i = 1, \ldots, |M|$, тогда*

$$\sum_{\beta \subseteq M, \beta \neq \varnothing} \frac{1}{|\beta|} \prod_{i \in \beta} q_i \prod_{i \notin \beta} (1 - q_i) = \\ = \sum_{m=1}^{|M|} \left((-1)^{m+1} \left(1 + \frac{1}{2} + \ldots + \frac{1}{m} \right) \left(\sum_{\beta \subseteq M, |\beta| = m} \prod_{i \in \beta} q_i \right) \right).$$

Утверждение 2. *Пусть переменные q_i принимают значения 0 и 1, M — произвольное конечное множество, $m \in \{1, \ldots, |M|\}$, тогда*

$$\sum_{\beta \subseteq M, |\beta|=m} \prod_{i \in \beta} q_i = \frac{1}{m!} \sum_{j=1}^{m} s(m,j)(q_1 + \ldots + q_{|M|})^j,$$

где $s(m,j)$ — числа Стирлинга первого рода.

Таким образом, получаем выражение числа классов эквивалентности

$$N = \sum_{l=1}^{|M|} (-1)^{l+1} \left(\sum_{j=l}^{|M|} \left(1 + \frac{1}{2} + \ldots + \frac{1}{j}\right) \frac{1}{j!} s\,(j,l) \right) \sum_{a \in M} \left(\sum_{b \in M} r\,(a,b) \right)^l.$$

2. Число пороговых функций

Для случая пороговых функций n переменных исследуем величину

$$\sum_{b} r(a,b).$$

Пусть a_i, b_i — целые числа, по модулю не больше любого натурального числа $m_0, m_0 \geqslant (n+1)^{\frac{n+1}{2}}$,

$$f(a,b,x) = (2a_1x_1 + \ldots + 2a_nx_n + 2a_0 + 1)(2b_1x_1 + \ldots + 2b_nx_n + 2b_0 + 1),$$
$$x \in E_2^n, |f(a,b,x)| \leqslant (2m_0(n+1)+1)^2 = k, m = (2k)^k.$$

Пусть M — множество целых точек $[-m_0, m_0]^{n+1}$. Отношение эквивалентности на M: две целые точки эквивалентны, если задаваемые ими пороговые функции равны (точке $a = (a_1, \ldots, a_n)$ соответствует пороговая функция, определяемая знаком выражений $a_1x_1 + \ldots + a_nx_n + a_0$ или $2a_1x_1 + \ldots + 2a_nx_n + 2a_0 + 1$). Известно, что при указанном m_0 приведенное соответствие является сюръективным. Тогда

$$r(a,b) = \prod_{x \in E_2^n} \left(1 - \frac{(-1)^m}{m!} \prod_{j=1}^{m} ((f+1)\ldots(f+k) - j) \right).$$

Аналогично утверждению 2 можно доказать

Утверждение 3. *Пусть q_i — переменные, принимающие значения 0 или 1, $i = 1, \ldots, n$, тогда*

$$\prod_{i=1}^{n}(1-q_i) = \frac{(-1)^n}{n!}\sum_{p=0}^{n} s\left(n+1, p+1\right)\left(q_1 + \ldots + q_n\right)^p .$$

Применяя его к рассматриваемому случаю получаем

$$\sum_b r(a,b) = \frac{1}{2^n!}\sum_{p=0}^{2^n} s\left(2^n+1, p+1\right) \times \\ \times \sum_b \left(\frac{(-1)^m}{m!}\sum_x \prod_{j=1}^{m}\left((f+1)\ldots(f+k)-j\right)\right)^p .$$

Утверждение 4. *Имеет место следующее разложение*

$$\prod_{j=1}^{m}\left((f+1)\ldots(f+k)-j\right)) = \sum_{l=0}^{km} c_l f^l,$$

где

$$c_0 = \sum_{j=0}^{m} s\left(m+1, j+1\right)\left(k!\right)^j, c_{km} = 1,$$

$$c_l = \frac{(-1)^{km}}{(km)!}\sum_{j=0}^{m} s\left(m+1, j+1\right)\left(k!\right)^j \times$$

$$\left(\sum_{p=0}^{km}\left(\frac{(k+p)!}{k!p!}\right)^j \frac{(km)!}{(km-p)!p!}\left(\sum_{i=0}^{km-l} p^i s\left(km+1, l+1+i\right)\right)\right),$$

$$0 < l < km.$$

Доказательство. Запишем с неопределенными коэффициентами

$$\prod_{j=1}^{m}((f+1)\dots(f+k)-j)=\sum_{l=0}^{km}c_l f^l,$$

получаем систему

$$\begin{cases} c_0=\prod_{j=1}^{m}(k!-j) & =\prod_{j=1}^{m}(k!\binom{k}{k}-j)= \\ & =\sum_{j=0}^{m}s(m+1,j+1)(k!\binom{k}{k})^j, \\ c_0+c_1+\dots+c_{km} & =\prod_{j=1}^{m}(k!\binom{k+1}{k}-j)= \\ & =\sum_{j=0}^{m}s(m+1,j+1)(k!\binom{k+1}{k})^j, \\ c_0+2c_1+\dots+2^{km}c_{km} & =\prod_{j=1}^{m}(k!\binom{k+2}{k}^k-j)= \\ & =\sum_{j=0}^{m}s(m+1,j+1)(k!\binom{k+2}{k})^j, \\ & \dots\dots\dots \\ c_0+kmc_1+\dots+(km)^{km}c_{km} & =\prod_{j=1}^{m}(k!\binom{k+km}{k}-j)= \\ & =\sum_{j=0}^{m}s(m+1,j+1)(k!\binom{k+km}{k})^j. \end{cases}$$

Тогда

$$c_l=\frac{\sum_{j=0}^{km}s(m+1,j+1)(k!)^j D_{lj}}{(km)!(km-1)!\dots1!},$$

где D_{lj} — следующий определитель

$$D_{lj}=\begin{vmatrix} 1 & 0\dots0^{l-1} & \binom{k}{k}^j & 0^{l+1}\dots1^{km} \\ 1 & 1\dots1^{l-1} & \binom{k+1}{k}^j & 1^{l+1}\dots1^{km} \\ 1 & 2\dots2^{l-1} & \binom{k+2}{k}^j & 2^{l+1}\dots2^{km} \\ \dots\dots\dots & & & \\ 1 & km\dots(km)^{l-1} & \binom{k+km}{k}^j & (km)^{l+1}\dots(km)^{km} \end{vmatrix}$$

Разложим по первой строке $D_{lj}=D_{1lj}+(-1)^l D_{2lj}$, где первое слагаемое D_{1lj} — следующий определитель

$$D_{1lj}=\begin{vmatrix} 1\dots1^{l-1} & \binom{k+1}{k}^j & 1^{l+1}\dots1^{km} \\ 2\dots2^{l-1} & \binom{k+2}{k}^j & 2^{l+1}\dots2^{km} \\ \dots & \dots & \dots \\ km\dots(km)^{l-1} & \binom{k+km}{k}^j & (km)^{l+1}\dots(km)^{km} \end{vmatrix},$$

второе слагаемое D_{2lj} — следующий определитель

$$D_{2lj} = \begin{vmatrix} 1 & 0 \dots 0^{l-1} & 0^{l+1} \dots 0^{km} \\ 1 & 1 \dots 1^{l-1} & 1^{l+1} \dots 1^{km} \\ 1 & 2 \dots 2^{l-1} & 2^{l+1} \dots 2^{km} \\ \dots\dots\dots & & \\ 1 & km \dots (km)^{l-1} & (km)^{l+1} \dots (km)^{km} \end{vmatrix}.$$

Последний известен

$$D_{2lj} = (-1)^{km}\, s\,(km+1, l+1)\,(km)!\,(km-1)!\,(km-2)! \dots 1!.$$

Первый определитель D_{1lj} разлагаем по l-ому столбцу получаем

$$D_{1lj} = \sum_{i=1}^{km} (-1)^{l+i} \binom{k+i}{k}^j Q_{il},$$

где Q_{il} — определитель

$$Q_{il} = \begin{vmatrix} 1 \dots 1^{l-1} & \binom{k+1}{k})^j & 1^{l+1} \dots 1^{km} \\ 2 \dots 2^{l-1} & \binom{k+2}{k})^j & 2^{l+1} \dots 2^{km} \\ \dots\dots\dots & & \\ km \dots (km)^{l-1} & \binom{k+km}{k})^j & (km)^{l+1} \dots (km)^{km} \end{vmatrix}.$$

Эти определители известны, получаем

$$D_{1lj} = \sum_{i=1}^{km} (-1)^{l+i} \binom{k+i}{k}^j \frac{(km)! \dots 1!}{((km-l)!l!)} S_{km-l}(1, \dots, i-1, i+1, \dots, km),$$

где $S_{km-l}(1, \dots, i-1, i+1, \dots, km)$ результат подстановки в элементарный симметрический многочлен степени $km-l$ от $km-1$ переменных указанных чисел. Эта величина находится, пользуясь соотношением

$$S_d(1, \dots, i-1, i+1, \dots, km) = S_d(1, \dots, i-1, i, i+1, \dots, km) - iS_{d-1}(1, \dots, i-1, i+1, \dots, km).$$

Арифметические преобразования приводят к сформулированному результату.

Из этого утверждения получаем

$$\left(\sum_b r(a,b)\right)^l = \left(\frac{1}{2^n!}\sum_{p=0}^{2^n} s(2^n+1,p+1)\sum_b \left(\frac{(-1)^m}{m!}\sum_{q=0}^{km} c_q(\sum_x f^q)\right)^p\right)^l.$$

Выражение во внутренних скобках

$$\sum_x f^q = \sum_x (2a_1x_1 + \ldots + 2a_nx_n + 2a_0 + 1)^q \times$$
$$\times (2b_1x_1 + \ldots + 2b_nx_n + 2b_0 + 1)^q = \sum_x \sum_{\beta\subset\{1,\ldots,n\},|\beta|\leqslant q}$$
$$\sum_{\substack{j_0,j_i,\in\beta,\\ j_0+\sum_{i\in\beta} j_i = q-|\beta|}} \left(\frac{q!}{j_0!\prod_{i\in\beta}(j_i+1)!}(2a_0+1)^{j_0}\prod_{i\in\beta}(2a_i)^{j_i+1}\prod_{i\in\beta}x_i\right)(\cdot)$$

Значит

$$\sum_{q=0}^{km} c_q\left(\sum_x f^q\right) = \sum_{q=0}^{km}\sum_x \sum_{\beta_1,\beta_2\subset\{1,\ldots,n\}} \sum_{\substack{j_{10},j_{1i},\in\beta_1,j_{20},j_{2i},\in\beta_2,\\ j_{10}+\sum_{i\in\beta_1} j_{1i} = q-|\beta 1|\\ j_{20}+\sum_{i\in\beta_2} j_{2i} = q-|\beta 2|}}$$
$$\frac{c_q(q!)^2 2^{n-|\beta_1\cup\beta_2|}}{j_{10}!j_{20}!\prod_{i\in\beta_1}(j_{1i}+1)!\prod_{i\in\beta_2}(j_{2i}+1)!}$$
$$(2a_0+1)^{j_{10}}\prod_{i\in\beta 1}(2a_i)^{j_{1i}+1}(2b_0+1)^{j_{20}}\prod_{i\in\beta 2}(2b_i)^{j_{2i}+1}.$$

Введем множество

$$\Gamma = \Bigg\{ (\beta_1, \beta_2, j_{10}, \{j_{1i}, i \in \beta_1\}, j_{20}, \{j_{2i}, i \in \beta_2\}, q) \mid$$

$$\beta_1, \beta_2 \subset \{1, \dots, n\}, j_{10} + \sum_{i \in \beta_1} j_{1i} + |\beta_1| = q, j_{20} + \sum_{i \in \beta_2} j_{2i} + |\beta_2| = q,$$

$$j_{10}, j_{1i} \in Z, i \in \beta_1, j_{20}, j_{2i} \in Z, i \in \beta_2,$$

$$j_{10} \geqslant 0, j_{1i} \geqslant 0, i \in \beta_1, j_{20} \geqslant 0, j_{2i} \geqslant 0, i \in \beta_2, 0 \leqslant q \leqslant km \Bigg\},$$

элементы которого можно перенумеровать $l = 1, \dots, |\Gamma|$. Перепишем формулу

$$\sum_{q=0}^{km} c_q \left(\sum_x f^q \right) = \sum_{l=1}^{|\Gamma|} w(l) 2^{n - |\beta_1(l) \cup \beta_2(l)|} (2a_0+1)^{j_{10}(l)} \prod_{i \in \beta 1(l)} (2a_{1i})^{j_{1i}(l)+1} \times$$

$$(2b_0 + 1)^{j_{20}(l)} \prod_{i \in \beta 2(l)} (2b_{2i})^{j_{2i}(l)+1},$$

$$w(l) = \frac{c_q(l) \left(q\,(l)!\right)^2}{j_{10}\,(l)! j_{20}\,(l)! \prod_{i \in \beta_1(l)} (j_{1i}(l)+1)! \prod_{i \in \beta_2(l)} (j_{2i}(l)+1)!}.$$

Тогда

$$\sum_b \left(\sum_{q=0}^{km} c_q \left(\sum_x f^q \right) \right)^p =$$

$$= \sum_b \Bigg(\sum_{\nu_1, \dots, \nu_{|\Gamma|}, \nu_1 + \dots + \nu_{|\Gamma|} = p} \frac{p!}{\nu_1!, \dots, \nu_{|\Gamma|}!} 2^{pn - \sum_{i=1}^{|\Gamma|} |\beta_1(i) \cup \beta_2(i)| \nu_i} \times$$

$$\prod_{i=1}^{|\Gamma|} \left(w(i)^{\nu_i}\right) (2a_0 + 1)^{\sum_{i=1}^{|\Gamma|} \nu_i j_{10}(i)} \prod_{d \in \beta_1(i)} (2a_d)^{\sum_{i=1}^{|\Gamma|} ((j_{1d}(i)+1)\nu_i)} \times$$

$$(2b_0 + 1)^{\sum_{i=1}^{|\Gamma|} \nu_i j_{20}(i)} \prod_{d \in \beta_2(i)} (2b_d)^{\sum_{i=1}^{|\Gamma|} ((j_{2d}(i)+1)\nu_i)} \Bigg).$$

Получаем выражение числа пороговых функций

$$N_n = \sum_{l=1}^{(2m_0+1)^{(n+1)}} (-1)^{l+1} \left(\sum_{j=l}^{(2m_0+1)^{(n+1)}} \left(1 + \frac{1}{2} + \ldots + \frac{1}{j}\right) \frac{1}{j!} s(j,l) \right) \times$$

$$\sum_{a} \left(\frac{1}{2^n!} \sum_{p=0}^{2^n} \frac{(-1)^{mp} s(2^n+1, p+1)}{(m!)^p} \times \right.$$

$$\left. \sum_{\nu_1,\ldots,\nu_{|\Gamma|}, \nu_1+\ldots+\nu_{|\Gamma|}=p} \frac{p!}{\nu_1!,\ldots,\nu_{|\Gamma|}!} 2^{pn-\sum_{i=1}^{|\Gamma|}|\beta_1(i)\cup\beta_2(i)|\nu_i} \times \right.$$

$$\prod_{i=1}^{|\Gamma|} \left(w(i)^{\nu_i}\right) (2a_0+1)^{\sum_{i=1}^{|\Gamma|} j_{10}(i)\nu_i} \prod_{d\in\beta_1(i)} (2a_d)^{\sum_{i=1}^{|\Gamma|}(j_{1d}(i)+1)\nu_i} \times$$

$$\left(\sum_{b_0=-m_0}^{b_0=m_0} (2b_0+1)^{\sum_{i=1}^{|\Gamma|}\nu_i j_{20}(i)} \right) \times$$

$$\left. \prod_{d\in\beta_2(i)} \left(\sum_{b_d=-m_0}^{b_d=m_0} (2b_d)^{\sum_{i=1}^{|\Gamma|}(j_{2d}(i)+1)\nu_i} \right) \right)^l.$$

Появившиеся степенные суммы известны

$$\sum_{i=-m}^{i=m} (2i)^h = \frac{2^h\left(1+(-1)^h\right)}{h+1} \sum_{i=0}^{h+1} \binom{d+1}{i} B_i (m+1)^{h+1-i},$$

$$\sum_{i=-m}^{i=m} (2i+1)^h = \frac{1+(-1)^h}{h+1} \sum_{i=0}^{h+1} \binom{d+1}{i} \times$$

$$\times B_i \left((2m+1)^{h+1-i} - 2^h (m+1)^{h+1-i} \right) + (2m+1)^h.$$

Подстановка выражений сумм через числа Бернулли, возведение в степень и вновь суммирование степеней приводит к сложному представлению числа пороговых функций через комбинаторные символы.

Интегральная формула числа пороговых функций

Носов М. В. (Москва, МГУ им. М. В. Ломоносова)

mvnosov@rambler.ru

Пусть F пороговая функция от n переменных, $a = (a_0, a_1, \ldots, a_n)$, $x = (x_1, \ldots, x_n)$. Известно, что её можно задать функцией $f_1(a, x)$, где

$$f_1(a,x) = a_1x_1 + \ldots + a_nx_n + a_0,$$
$$a_0, a_1, \ldots, a_n \in \mathbf{Z},$$
$$|a_i| \leqslant P, i = 1, \ldots, n,$$
$$P = \left[(n+1)^{\frac{n+1}{2}} + 1\right].$$

Очевидно, тогда F можно задать функцией

$$f(a,x) = 2a_1x_1 + \ldots + 2a_nx_n + 2a_0 + 1,$$

при этом разделяющая гиперплоскость не проходит через вершины куба, то есть принимает целые значения вне интервала $(-1, 1)$. Очевидно,что можно определить функцию $G(a, x)$, которая обеспечит «поразрядные» действия в нижеприведенных формулах. В выражении

$$\sum_{b,x} (f(a,x)f(b,x)G(b,x))$$

коэффициенты при $G(b, x)$ — целые положительные числа, если плоскости с направляющими векторами a и b определяют точку x в полупространствах одного знака, в противном случае — целые отрицательные. По модулю коэффициенты не превосходят величины $(2(n+1)P)^2$.Если при фиксированном значении b и всех векторах x, коэффициенты положительны, то это значит, что плоскости, определяемые векторами a и b, делят вершины куба одинаково. Имеет место следующее очевидное утверждение. Если на конечном множестве M введено отношение эквивалентности $\sim$, тогда

$$|M/\sim| = \sum_{x \in M} \frac{1}{\sum\limits_{y \in M} (x \sim y)}.$$

Обозначим через B множество всех целых точек куба $[-P,P]^{(n+1)}$

Утверждение. *Число пороговых функций задается формулой*

$$N_n = \int_0^1 \sum_{a\in B} \left(e^{2\pi i\left(\sum_{b\in B, x\in E_2^n}(f(a,x)f(b,x)G(b,x))\right)t} \right) \cdot$$

$$\cdot \left(\sum_{j=1}^{|B|} \frac{1}{j} \sum_{\substack{\beta\in B,\\ |\beta|=j}} \prod_{b\in\beta} \prod_{x\in E_2^n} \sum_{l=1}^{P} e^{-2\pi i l G(b,x)t} \cdot \right.$$

$$\left. \prod_{b\notin\beta} \left(\sum_{\substack{\gamma\subset E_2^n,\\ |\gamma|\geqslant 1}} \prod_{x\in\gamma} \left(\sum_{l=1}^{P} e^{-2\pi i l G(b,x)t} \right) \prod_{x\notin\gamma} \left(\sum_{l=1}^{P} e^{2\pi i l G(b,x)t} \right) \right) \right) dt.$$

О сложности распознавания дискретных образов плоских фигур

Павлов М. В. (Москва, МГТУ «Станкин»)

anhromanio@gmail.com

Замкнутое множество точек действительной плоскости (плоская фигура) при отображении на целочисленный квадрат порождает дискретный образ фигуры. При действии на данную фигуру движениями из заданного класса K возникает набор дискретных образов, интерпретируемый как множество единиц булевскрй функции. Под сложностью распознавания фигуры относительно данного класса движений понимается сложность реализации этой функции схемой из функциональных элементов. Указано множество фигур, для которого описание сложности относительно вращений экспоненциональна как функция от размеров целочисленного квадрата.

Некоторые линейные оценки сложности для рассматриваемого подхода были получены в [1]. Подход связанный с построением соответствующих графов изучен в [2].

Плоской **фигурой** будем называть замкнутое подмножество действительной плоскости $\mathbb{R}^2$. Введем понятие дискретнго изображения фигуры.

Пусть фигура Φ на $\mathbb{R}^2$ находится внутри квадрата B_n размером $n \times n$. Углы квадрата расположены в точках $(0,0)(0,n)(n,n)(n,0)$, и квадрат разбит на n^2 клеток с границами на целочисленной решетке. Пусть $\sigma_{i,j}$ — параметр, такой что если в клетке (i,j) без границы есть точки фигуры, то $\sigma_{i,j} = 1$, иначе $\sigma_{i,j} = 0$. Получившийся набор $\sigma_{i,j}$,$1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n$, будем называть изображением фигуры.

Будем говорить, что клетка (i,j) закрашивается, если $\sigma_{i,j}$ меняет значение с 0 на 1, и раскрашивается, если с 1 на 0.

Рассмотрим класс движений K. Пусть $K(\Phi)$ — множество фигур, получаемых из Φ с помощью движений из K и лежащих внутри квадрата B_n. Множество изображений каждой фигуры из $K(\Phi)$ обозначим $H(\Phi, K)$. В этом множестве не более 2^{n^2} элементов. Рассмотрим такую булеву функцию $f_{\Phi,K}(x_{1,1}, x_{1,2}, \ldots, x_{n,n-1}, x_{n,n})$ от n^2 переменных, что $f_{\Phi,K}(\sigma_{1,1}, \ldots, \sigma_{n,n}) = 1 \Longleftrightarrow (\sigma_{1,1}, \ldots, \sigma_{n,n}) \in H(\Phi, K)$. Будем

говорить, что $f_{\Phi,K}$ распознает образ фигуры Φ при заданном классе движений K.

Пусть $L(f)$ — минимальная сложность реализации функции f в базисе $(\vee, \wedge, \neg)$ функциональных элементов [4].

Пусть задана последовательность K_n классов движений, $n = 1, 2, \ldots$. Нас интересует поведение $L_{\{K_n\}}(n) = \max\limits_{\Phi \subset B_n} L(f_{\Phi,K_n})$ при $n \to \infty$.

Далее для каждого $n = 1, 2, \ldots$ в качестве K_n будем брать вращение вокруг точки, принадлежащей квадрату B_n. Возьмем клетку $([\frac{n}{2}]+1, [\frac{n}{2}]+1)$ нашего квадрата. Выберем в ней точку O_n так, что расстояние до правой границы клетки $\frac{1}{4}$, а до верхней $\frac{1}{2}$.

Теорема. *Существует последовательность фигур $\{\Phi_1, \Phi_2, \ldots\}$ для последовательности классов $\{K_n\}$, что $L(f_{\Phi_n,K_n}) \gtrsim \frac{2^k}{k}$, где $k = [\frac{n}{4}]$.*

Построение фигуры

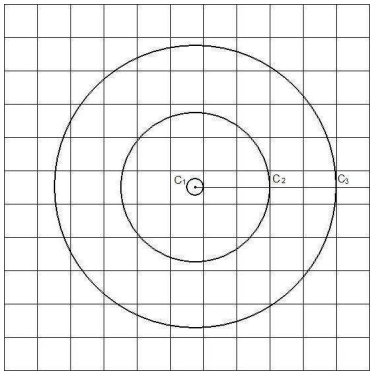


Рис. 1. Окружности C_i.

Фиксируем n. Обозначим точку O_n как O. Проведем окружности $C_1, C_2, \ldots, C_k$ с центрами в O и с радиусами $\frac{1}{4}, \frac{9}{4}, \ldots, \frac{1}{4}+2(k-1)$. При $k = [\frac{n}{4}]$ они помещаются в квадрате, так как $2+2(k-1) \leqslant [\frac{n}{2}]$, причем C_i касается левой границы клетки $([\frac{n}{2}]+1, [\frac{n}{2}]+2i)$, и никакие из этих окружностей не пересекают ее.

Проведем горизонтальный луч из точки O вправо. Для точек на окружностях введем координату φ, равную угловой величине дуги, соединяющей эту точку с точкой пересечения луча и окружности, причем дуга направлена от точки пересечения против часовой стрелки. $\varphi \in [0, 2\pi)$ Пусть $\varphi = 2\pi t$ и $t \in [0, 1)$.

Рассмотрим окружность C_i. Выделим следующее подмножество M_i на ней. Будем считать, что двоичное представление t не оканчивается на периодическую 1. Пусть у двоичного разложения t на i-м месте после запятой стоит единица. Тогда точка с координатой $2\pi t$ принадлежит этому множеству. Таким образом множество M_i состоит из 2^{i-1} дуг и имеет вид

$$M_i = \{\varphi | \frac{2\pi}{2^i}(2j-1) \leqslant \varphi < \frac{2\pi}{2^i}2j, j = 1, 2, 3, \dots 2^{i-1}\}.$$

Положим $M = \bigcup_{i=1}^{k} M_i$.

Пусть заданы двоичные наборы σ_m длиной k, $m = 1, \dots p$. Пусть число s_m $(0 \leqslant s_m < 1)$ в двоичном представлении имеет вид $0, \sigma_m 00 \dots$. Зададим множество дуг на окружности C_i:

$$L_i = \bigcup_{m=1}^{p} \{\varphi | 2\pi s_m < \varphi < 2\pi(s_m + 2^{-k})\},$$

$L = \bigcup_{i=1}^{k} L_i$. Наконец рассмотрим $A = M \bigcap L$.

Пусть $a(i, j, k)$ — дуга окружности C_i, задаваемая угловыми координатами вида

$$2\pi 2^{-k}(j-1) < \varphi < 2\pi 2^{-k} j$$

для тех j, что дуга без концов полностью лежит в A, а точнее для j вида

$$2^{k-i}(2l-1) + v; l = 1, \dots, 2^{i-1}; v = 1, \dots, 2^{k-i}.$$

Проведем касательные через концы дуги. Рассмотрим фигуру $F(i, j, k, \varepsilon_i)$, ограниченную этими касательными, дугой $a(i, j, k)$, и

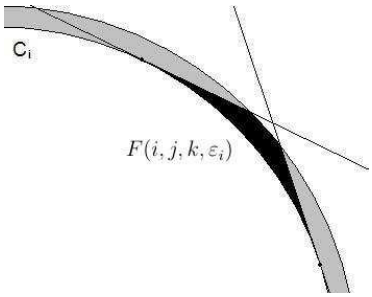


Рис. 2. Фигура $F(i,j,k,\varepsilon_i)$.

окружностью с центром O и радиусом на ε_i большим, чем у C_i, $\varepsilon_i \ll 1$. Таким образом фигура $F(i,j,k,\varepsilon_i)$ целиком содержится в кольце R_i, толщина которого равна ε_i.

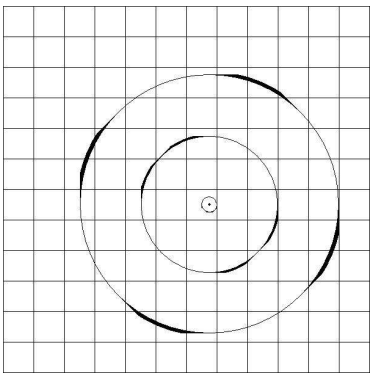


Рис. 3. Пример Ф.

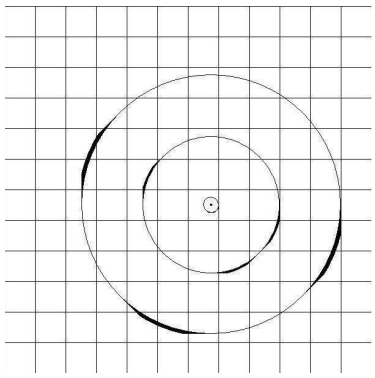


Рис. 4. Другой пример Ф.

Построим такие фигуры для каждой дуги $a(i,j,k) \subset A$ и возьмем их объединение. Пусть $F = \bigcup\limits_{i,j} F(i,j,k,\varepsilon_i)$, $C = \bigcup\limits_{i=1}^{k} C_i$, $\Phi = F \bigcup C$. Таким образом получили искомую фигуру Ф. На рисунке 3 пример фигуры для $n = 12$ и множества всех двоичных наборов длины 3, на рисунке 4 для множества $\{000, 011, 101, 110, 111\}$.

Лемма 1. *Окружности $C_1, C_2, \ldots, C_k$ не проходят через вершины клеток и не касаются других сторон клеток.*

Очевидно, что эти окружности не касаются других сторон клеток, так как радиус имеет вид $\frac{1}{4} + 2(i-1)$, а при касании других сторон клеток радиус должен быть вида $\frac{3}{4} + l$, $\frac{1}{2} + l$ или $\frac{1}{4} + 2k + 1$, где l — целое.

Пусть C_i проходит через вершину угла клетки, а именно через точку с координатами $(x + \frac{1}{4} + l, y + \frac{1}{2} + m)$, где (x, y) — координаты O, l и m — целые. Тогда по теореме Пифагора

$$(\frac{1}{4} + l)^2 + (\frac{1}{2} + m)^2 = (\frac{1}{4} + 2(i-1))^2.$$

Покажем, что уравнение не имеет решений в целых числах. Действительно,

$$l^2 + \frac{l}{2} + \frac{1}{16} + m^2 + m + \frac{1}{4} = \frac{1}{16} + (i-1) + 4(i-1)^2,$$
$$2l^2 + l + \frac{1}{8} + 2m^2 + 2m + \frac{1}{2} = \frac{1}{8} + 2(i-1) + 8(i-1)^2,$$
$$\frac{1}{2} = 2(i-1) + 8(i-1)^2 - (2l^2 + l + 2m^2 + 2m).$$

Правая часть целая, а левая нет, то есть нет решения в целых числах.

Переименуем переменные $x_{i,j}$ функции $f_{\Phi,K}$ следующим образом: $y_i = x_{[\frac{n}{2}]+2i,[\frac{n}{2}]+1}$ при $1 \leqslant i \leqslant k$, а оставшиеся переменные из набора $x_{i,j}$ обозначим через $y_{k+1} \ldots y_{n^2}$.

Напомним, что фигура Φ характеризуется набором параметров $\varepsilon_i, i = 1 \ldots k$, которые задают толщину колец $R_i, i = 1 \ldots k$ с внутренней окружностью C_i, покрывающих фигуру Φ. Пусть $R = \bigcup_{i=1}^{k} R_i$.

Лемма 2. *Существует набор $(\varepsilon_i > 0, i = 1 \ldots k)$ такой, что при вращении Φ вокруг O значения переменных $y_{k+1} \ldots y_{n^2}$ постоянны.*

Из леммы 1 следует, что для каждой окружности C_i существует $\varepsilon_i > 0$ такое, что при увеличении радиуса окружности на ε_i рисунок окружности изменится только на клетке $([\frac{n}{2}] + 2i, [\frac{n}{2}] + 1)$. Таким образом дискретные изображения R_i и C_i отличаются только в клетке $([\frac{n}{2}] + 2i, [\frac{n}{2}] + 1)$.

При таком выборе ε_i: $C \subseteq \Phi \subset R$, а это значит, что Φ при вращении вокруг O может отличаться от излбражения C только на клетках $([\frac{n}{2}]+2i, [\frac{n}{2}]+1)$, которых всего k штук, а на остальных клетках значение то же. Лемма доказана.

Далее посмотрим какие наборы будут получаться на $y_1, \dots y_k$ при вращении фигуры Φ. В силу построения фигуры Φ: $y_i = 1$ только если точка касания C_i со стороной клетки соответствующей y_i при повороте принадлежит A, но не лежит на конце дуги из A.

Лемма 3. *При вращении фигуры* Φ *вокруг* O*, набор переменных* $(y_1, \dots y_k)$ *принимает значения из* $\{\sigma_m\}$ *или* $(0, \dots, 0)$.

В соответствии с перенумерацией переменных функции $f_{\Phi,K}$ перенумеруем сами клетки: $([\frac{n}{2}]+2i, [\frac{n}{2}]+1)$ на i при $1 \leqslant i \leqslant k$, а остальные на $k+1, \dots, n^2$. Пусть Φ повернули на угол φ по часовой стрелке.

Пусть $\frac{\varphi}{2\pi}$ в двоичном представлении имеет вид $0, \sigma \dots$. Тогда если $\sigma \in \{\sigma_m\}$, то точки касания окружностей C_i со сторонами клетки i принадлежат определённому выше множеству дуг L. Только если точка касания со стороной клетки i принадлежит определенному выше A, то $y_i = 1$ по построению фигуры Φ. Если $0, \sigma 000 \dots < \frac{\varphi}{2\pi} < 0, \sigma 111 \dots$, то $(y_1, \dots, y_k) = (\sigma)$. В случае $\sigma \notin \{\sigma_m\}$ получим $(y_1, \dots, y_k) = (0, \dots, 0)$.

Стоит заметить, что для каждого σ_m можно указать φ (например $\varphi = 2\pi \cdot 0, \sigma 1$), такое что при повороте на этот угол $(y_1, \dots, y_k) = (\sigma)$. А это значит, что $(y_1, \dots, y_k) = (0, \dots, 0)$ или $(y_1, \dots, y_k) = (\sigma_m)$ для некоторого m.

Таким образом для множества наборов σ_m получили фигуру Φ, которая при вращении вокруг O имеет такие дискретные изображения, у которых набор переменных $y_1, \dots y_k$ принимает значения σ_m или $(0, \dots, 0)$, а набор $y_{k+1}, \dots y_{n^2}$ постоянен.

Лемма 4. *Если* $g(y_1, \dots, y_k)$ *— подфункция* $f(y_1, \dots, y_k, y_{k+1}, \dots, y_m)$*, то* $L(f) \geqslant L(g) - 3$.

Если g подфункция f, то $g(y_1, \dots, y_k) = f(y_1, \dots, y_k, \tau^{k+1}, \dots, \tau^m)$, для некоторого набора $(\tau^{k+1}, \dots, \tau^m)$. Подставляя в схему функции f вместо $(y_{k+1}, \dots, y_m)$ набор констант $(\tau^{k+1}, \dots, \tau^m)$ получим, что $L(g) \leqslant L(f) + 3$.

Доказательство теоремы

По известным нижним оценкам [3] $L(k) \gtrsim \frac{2^k}{k}$, то есть существует последовательность функций $g_k = g(y_1, \ldots, y_k)$, что $L(g_k) \gtrsim \frac{2^k}{k}$. Возьмем такие функции $g(y_1, \ldots, y_k)$, что $g(0, \ldots, 0) = 1$.

Пусть $[\frac{n}{4}] = k$ и множество единиц функции g_k есть $\{\sigma_m\}$. Построим для $\{\sigma_m\}$ фигуру Φ_n. Тогда g_k будет подфункцией $f_{\Phi_n, K_n}(y_1, \ldots y_{n^2})$, соответствующей фигуре Φ. И по лемме 4: $L(f_{\Phi_n, K_n}) \gtrsim \frac{2^k}{k}$.

Автор выражает благодарность С. В. Алешину, под руководством которого выполнена работа.

Список литературы

[1] Григорьева А. Н. Алгоритм линейной сложности для распознавания изоморфизма плоских изображений // Теория сложности вычислений. 3. Зап. научн. сем. ЛОМИ. — Л.: Наука, 1988. 174. — С. 101–121.

[2] Aleŝin S. V., Ŝćepanović R. L. Brze procedure raspoznavanja oblika. — Beograd, 1992.

[3] Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. — М.: Наука, 1965. Вып. 14. — С. 31–110.

[4] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

Теоретико-возможностные модели матричных игр двух субъектов в двух вариантах теории возможностей

Папилин С. С., Пытьев Ю. П. (Москва, МГУ им. М. В. Ломоносова)

papilin@physics.msu.ru, yuri.pytyev@gmail.com

1. Возможностная модель матричной игры двух субъектов

В игре участвуют два субъекта, «игрок A» и «игрок B». Игроки принимают нечеткие решения $\alpha \in \{1, \ldots, m\}$ и $\beta \in \{1, \ldots, n\}$ независимо друг от друга,

$$\mathrm{p}_i^{\mathrm{A}} \stackrel{\mathrm{def}}{=} \mathrm{P}^{\mathrm{A}}(\alpha = i) \geqslant 0, \max_{1 \leqslant i \leqslant m} \mathrm{p}_i^{\mathrm{A}} = 1, \tag{1}$$

$$\mathrm{p}_j^{\mathrm{B}} \stackrel{\mathrm{def}}{=} \mathrm{P}^{\mathrm{B}}(\beta = j) \geqslant 0, \max_{1 \leqslant j \leqslant n} \mathrm{p}_j^{\mathrm{B}} = 1, \tag{2}$$

есть распределения возможностей решений игроками. Наборы возможностей определяют нечеткие, или фазифицированные, стратегии принятия решений игроков A и B.

Определим матрицу переходных возможностей события W, элементы которой $s_{ij} \stackrel{\mathrm{def}}{=} \mathrm{P}(W|\alpha = i, \beta = j)$ задают зависимость переходной возможности W от решений игроков, тогда *возможность события W как функция нечетких стратегий игроков*

$$\mathrm{P}(W|\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}) = \max_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} s_{ij} \bullet \mathrm{p}_i^{\mathrm{A}} \bullet \mathrm{p}_j^{\mathrm{B}} \stackrel{\mathrm{def}}{=} S(\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}), \tag{3}$$

где $\bullet$ есть операция умножения возможностей: минимум в первом варианте теории возможностей и «обычное» умножение во втором.

Будем считать, что в рассматриваемой игре для игрока A событие W — «выигрыш», а для B — «проигрыш», и поэтому игрок A стремится максимизировать возможность 3, а игрок B — минимизировать.

Максиминную стратегию $\mathrm{p}^{*\mathrm{A}}$ *игрока* A определим как любое решение задачи

$$\min_{\mathrm{p}^{\mathrm{B}}\in\mathcal{P}^{\mathrm{B}}} S(\mathrm{p}^{*\mathrm{A}},\mathrm{p}^{\mathrm{B}}) = \max_{\mathrm{p}^{\mathrm{A}}\in\mathcal{P}^{\mathrm{A}}} \min_{\mathrm{p}^{\mathrm{B}}\in\mathcal{P}^{\mathrm{B}}} S(\mathrm{p}^{\mathrm{A}},\mathrm{p}^{\mathrm{B}}) \stackrel{\mathrm{def}}{=} s_{maxmin}, \tag{4}$$

где s_{maxmin} назовем *максиминной возможностью.*

Множество всех максиминных стратегий по 4 задается условием

$$\min_{1\leqslant j\leqslant n} \max_{1\leqslant i\leqslant m} s_{ij} \bullet \mathrm{p}_i^{*\mathrm{A}} = \min_{1\leqslant j\leqslant n} \max_{1\leqslant i\leqslant m} s_{ij}. \tag{5}$$

Минимаксную стратегию $\mathrm{p}_*^{\mathrm{B}}$ *игрока* B определим как любое решение задачи

$$\max_{\mathrm{p}^{\mathrm{A}}\in\mathcal{P}^{\mathrm{A}}} S(\mathrm{p}^{\mathrm{A}},\mathrm{p}_*^{\mathrm{B}}) = \min_{\mathrm{p}^{\mathrm{B}}\in\mathcal{P}^{\mathrm{B}}} \max_{\mathrm{p}^{\mathrm{A}}\in\mathcal{P}^{\mathrm{A}}} S(\mathrm{p}^{\mathrm{A}},\mathrm{p}^{\mathrm{B}}) \stackrel{\mathrm{def}}{=} s_{minmax}, \tag{6}$$

в которой s_{minmax} назовем *минимаксной возможностью.*

Множество всех минимаксных стратегий $\mathrm{p}_*^{\mathrm{B}}$ в 6 определяется условием

$$\max_{1\leqslant j\leqslant n} ((\max_{1\leqslant i\leqslant m} s_{ij}) \bullet \mathrm{p}_{*j}^{\mathrm{B}}) = \min_{1\leqslant j\leqslant n} \max_{1\leqslant i\leqslant m} s_{ij}. \tag{7}$$

Теорема 1. *В любой одноматричной игре существуют максиминные* $\mathrm{p}^{*\mathrm{A}}$ *и минимаксные* $\mathrm{p}_*^{\mathrm{B}}$ *стратегии, причем максиминная возможность выигрыша и минимаксная возможность проигрыша равны*

$$s_{maxmin} = s_{minmax} \stackrel{\mathrm{def}}{=} s = \min_{1\leqslant j\leqslant n} \max_{1\leqslant i\leqslant m} s_{ij}. \tag{8}$$

Для любых максиминной $\mathrm{p}^{*\mathrm{A}}$ *и минимаксной* $\mathrm{p}_*^{\mathrm{B}}$ *стратегий* $S(\mathrm{p}^{*\mathrm{A}},\mathrm{p}_*^{\mathrm{B}}) = s$*; тройка* $(\mathrm{p}^{*\mathrm{A}},\mathrm{p}_*^{\mathrm{B}},s)$ *есть решение одноматричной игры.*

Четкая стратегия игрока A, в которой $\mathrm{p}_i^{\mathrm{A}} = \begin{cases} 1, & i = i_0, \\ 0, & i \neq i_0, \end{cases}$ $i = 1,\ldots,m$*, является максиминной, если* $\min_{1\leqslant j\leqslant n} s_{i_0 j} = s$.

Четкие максиминные стратегии существуют не для любой матрицы переходных возможностей.

Четкая стратегия игрока B, в которой $\mathrm{p}_j^{\mathrm{B}} = \begin{cases} 1, & j = j_0, \\ 0, & j \neq j_0, \end{cases}$ $j = 1,\ldots,n$*, является минимаксной, если* $\max_{1\leqslant i\leqslant m} s_{ij_0} = s$.

Четкие минимаксные стратегии существуют для любой матрицы переходных возможностей.

В первом и втором вариантах теории возможностей формулировка теоремы выглядит одинаково, включая совпадение цен игры. Условия на множества всех максиминных и всех минимаксных стратегий отличаются операцией умножения возможностей.

2. Возможностная модель биматричной игры

В теории возможностей значения $P(W)$ и $P(\Omega\backslash W)$ не зависят друг от друга однозначно, и модель одноматричной игры не может охарактеризовать ситуацию, в которой игрок A считает «выигрышем» событие W, а игрок B считает «выигрышем» событие $\Omega \setminus W$. Для описания таких ситуаций следует ввести матрицы переходных возможностей W и $\Omega \setminus W$:

$$s_{ij} \stackrel{\text{def}}{=} \mathrm{P}(W|\alpha = i, \beta = j),$$
$$t_{ij} \stackrel{\text{def}}{=} \mathrm{P}(\Omega \setminus W|\alpha = i, \beta = j),$$
$$\max(s_{ij}, t_{ij}) = 1, \quad i = 1, \ldots, m, \quad j = 1, \ldots, n.$$

Соответственно

$$\mathrm{P}(W|\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}) = \max_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}} s_{ij} \bullet \mathrm{p}_i^{\mathrm{A}} \bullet \mathrm{p}_j^{\mathrm{B}} \stackrel{\text{def}}{=} S(\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}), \tag{9}$$

$$\mathrm{P}(\Omega \setminus W|\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}) = \max_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}} t_{ij} \bullet \mathrm{p}_i^{\mathrm{A}} \bullet \mathrm{p}_j^{\mathrm{B}} \stackrel{\text{def}}{=} T(\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}). \tag{10}$$

Для рассматриваемой игры можно поставить две задачи: максимизации и минимизации.

В задаче максимизации цель игрока A — максимизировать $\mathrm{P}(W|\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}})$, а цель игрока B — максимизировать $\mathrm{P}(\Omega \setminus W|\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}})$. *Точка равновесия* в такой задаче — пара стратегий $(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}_*^{\mathrm{B}})$, для которых выполняется условие

$$\forall \mathrm{p}^{\mathrm{A}} \in \mathcal{P}^{\mathrm{A}} \quad S(\mathrm{p}^{\mathrm{A}}, \mathrm{p}_*^{\mathrm{B}}) \leqslant S(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}_*^{\mathrm{B}});$$
$$\forall \mathrm{p}^{\mathrm{B}} \in \mathcal{P}^{\mathrm{B}} \quad T(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}^{\mathrm{B}}) \leqslant T(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}_*^{\mathrm{B}}).$$

В задаче минимизации цель игрока A — минимизировать $\mathrm{P}(\Omega\backslash W)$, а цель игрока B — минимизировать $\mathrm{P}(W)$. *Точка равновесия* — пара стратегий $(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}^{\mathrm{B}}_{*})$, для которых

$$\forall \mathrm{p}^{\mathrm{A}} \in \mathcal{P}^{\mathrm{A}} \quad S(\mathrm{p}^{\mathrm{A}}, \mathrm{p}^{\mathrm{B}}_{*}) \geqslant S(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}^{\mathrm{B}}_{*});$$
$$\forall \mathrm{p}^{\mathrm{B}} \in \mathcal{P}^{\mathrm{B}} \quad T(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}^{\mathrm{B}}) \geqslant T(\mathrm{p}^{*\mathrm{A}}, \mathrm{p}^{\mathrm{B}}_{*}).$$

Теорема 2. *В любой биматричной игре с задачей максимизации существуют точки равновесия. Пара четких стратегий (i^*, j_*) есть точка равновесия тогда и только тогда, когда*

$$\max_{1\leqslant i\leqslant m} s_{ij_*} = s_{i^*j_*}; \quad \max_{1\leqslant j\leqslant n} t_{i^*j} = t_{i^*j_*}.$$

Точки равновесия из четких стратегий могут как существовать, так и не существовать в зависимости от матриц $\{s_{ij}\}$ и $\{t_{ij}\}$ переходных возможностей.

В биматричной игре с задачей минимизации точки равновесия могут как существовать, так и не существовать в зависимости от матриц переходных возможностей. Если точки равновесия существуют, то среди них есть и точки равновесия из четких стратегий. Пара четких стратегий (i^*, j_*) есть точка равновесия тогда и только тогда, когда

$$\min_{1\leqslant j\leqslant n} s_{i^*j} = s_{i^*j_*}; \quad \min_{1\leqslant i\leqslant m} t_{ij_*} = t_{i^*j_*}.$$

Если таких пар нет, то в соответствии с вышесказанным точек равновесия, в том числе из фазифицированных стратегий, в задаче минимизации нет.

В первом и втором вариантах теории возможностей формулировка теоремы выглядит одинаково.

Работа выполнена при финансовой поддержке РФФИ, проект №11–07–00722–а.

Список литературы

[1] Папилин С. С., Пытьев Ю. П. Вероятностные и возможностные модели матричных игр двух субъектов // Математическое моделирование. — 2010. Т. 22. № 12. — С. 10–15.

[2] Пытьев Ю. П. Возможность как альтернатива вероятности. Математические и эмпирические основы, применение. — М.: Физматлит, 2007.

Слабозамкнутые классы линейных булевых функций

Петрова О. А. (Москва, МГУ им. М. В. Ломоносова)

hellga.01@mail.ru

В данной статье рассматриваются пары (f, t), где f — булева функция, t — натуральное число или 0, называемое временной задержкой. На множестве таких пар определяется операция синхронной суперпозиции по аналогии с операцией суперпозиции для булевых функций. Далее рассматриваются первые проекции множетсв пар (f, t) и для них определяется понятие слабой замкнутости по аналогии с замкнутостью для булевых функций.

В данннной статье описываются слабозамкнутые классы множеств, состоящих из линейных функций.

1. Основные понятия из алгебры булевых функций

Введем следующие обозначения.

Множество $\{0, 1\}$ обозначим через E_2, тогда E_2^n — декартово произведение n сомножителей E_2.

Отображение $f : E_2^n \to E_2$ называется булевым.

Пусть $U = \{u_1, u_2, \ldots\}$ — счетный алфавит переменных, принимающих значения из E_2. Тогда отображение f можно интерпретировать как функцию $f(u_{j_1}, \ldots, u_{j_n})$, которая определяется, во-первых, отображением f, а во-вторых, указанием переменных, от которых она зависит. Такие функции и переменные $u_k \in U$, называются также булевыми. Класс всех булевых функций обозначаем C_1.

Будем говорить, что булева функция $f(x_1, \ldots, x_i, \ldots, x_n)$ существенно зависит от переменой x_i, если найдутся два таких набора
$\tilde{\alpha}_1 = (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$ и
$\tilde{\alpha}_2 = (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$,
такие, что значения $f(\tilde{\alpha}_1)$ и $f(\tilde{\alpha}_2)$ различны.

Далее, для обозначения переменных будем иногда использовать латинские буквы x, y, z, возможно, с индексами.

На произвольном множестве булевых функций M можно индуктивно ввести понятие формулы.

1. Пусть $f(x_1, \ldots, x_n)$ — функция из M; тогда выражение $f(x_1, \ldots, x_n)$ является формулой над M.

2. Пусть $f(x_1, \ldots, x_n)$ — функция из M и в строке $G_1, \ldots, G_n$ каждое выражение G_i является либо формулой над M, либо переменной из U, тогда выражение $f(G_1, \ldots, G_n)$ является формулой над M.

Класс всех формул над M обозначается $<M>$.

Далее, каждой формуле A из $<M>$ индуктивно сопоставляется функция из M, называемая суперпозицией над M.

1. Если формула A из $<M>$ является выражением $f(x_1, \ldots, x_n)$ таким, что функция $f(x_1, \ldots, x_n)$ принадлежит M, то A сопоставляем булеву функцию $f(x_1, \ldots, x_n)$, которую называем суперпозицией над M.

2. Пусть формула A имеет вид $f(G_1, \ldots, G_n)$, где $f(x_1, \ldots, x_n)$ есть функция из M, а каждое выражение G_i является либо формулой над M, либо переменной из U. Сопоставим каждому G_i выражение g_i, где g_i — булева функция, если G_i — формула над M, и g_i — переменная u_{j_i}, если G_i — эта переменная. В результате получим выражение $f(g_1, \ldots, g_n)$. Рассмотрим его как функцию $h(y_1, \ldots, y_m)$ от множества переменных $U' = \{y_1, \ldots, y_m\}$, содержащего точно все те переменные, от которых зависит хотя бы одна их функций g_i и f. Эту булеву функцию h сопоставляем выражению $f(G_1, \ldots, G_n)$ и называем суперпозицией над M.

Класс всех суперпозиций над M обозначается $[M]$.

Тройка $(M, <M>, [M])$ называется алгеброй (функциональной системой), порожденной множеством M.

Оператор $[\,]$ обладает следующими свойствами:

$$
\begin{aligned}
&1)\ [M] \supseteq M,\\
&2)\ M_1 \supseteq M_2 \Rightarrow [M_1] \supseteq [M_2],\\
&3)\ [[M]] = [M],
\end{aligned}
$$

и называется замыканием. Множество M называется замкнутым, если $[M] = M$.

Говорят, что множество M_1 выразимо через M_2, если $[M_2] \supseteq M_1$.

Множество $M_1 \subseteq M$ называется полным в M, если $[M_1] = M$. В случае, если множество M_1 конечно, множество M называется конечно порожденным.

Множество $M_1 \subseteq M$ называется предполным в M, если оно является замкнутым, и для любой функции f, такой что $f \in M, f \notin M_1$, верно $[M_1 \cup \{f\}] = M$.

Множество M_1 называется базисом в M, если оно полно в M, но всякое его собственное подмножество уже не полно в M.

Множество $\Sigma(M)$ всех замкнутых подмножеств множества M образует частичный порядок по отношению включения. Этот порядок называется решеткой замкнутых классов в M и представляют в виде графа. Вершинами этого графа являются замкнутые классы булевых функций, вложение которых друг в друга обозначается ребром, ориентированным от более широкого класса к классу, вложенному в него.

Замкнутые множества из $\Sigma(C_1)$ называются классами Поста.

Функция f называется самодвойственной, если верно

$$f(\bar{x}_1, \ldots, \bar{x}_n) = \bar{f}(x_1, \ldots, x_n).$$

Рассмотрим представление булевых функций в базисе

$$\{x_1 \cdot x_2, x_1 + x_2, 0, 1\},$$

которое называется разложением в полиномом Жегалкина.

Булева функция $f(x_1, \ldots, x_n)$, чей полином Жегалкина имеет вид

$$\Sigma a_i x_i + d,$$

называется линейной.

Пусть $c \in E_2$. Говорят, что булева функция $f(x_1, \ldots, x_n)$ сохраняет константу c, если $f(c, \ldots, c) = c$.

Пусть даны два набора $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$, такие, что при любых $i \leqslant n$ верно $\alpha_i \leqslant \beta_i$. Говорят, что набор α предшествует набору β и пишут $\alpha \leqslant \beta$. Булева функция $f(x_1, \ldots, x_n)$ называется монотонной, если для любых наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$ из соотношения $\alpha \leqslant \beta$ следует, что $f(\alpha) \leqslant f(\beta)$.

Булева функция f называется α-функцией, если $f(x,\dots,x)=x$.
Булева функция f называется β-функцией, если $f(x,\dots,x)=1$.
Булева функция f называется γ-функцией, если $f(x,\dots,x)=0$.
Булева функция f называется δ-функцией, если $f(x,\dots,x)=x+1$.

2. Операция синхронной суперпозиции

Рассмотрим пары (f,t), где f — булева функция , t — натуральное число или 0, называемое временной задержкой.

Обозначим

$$C_1' = \{(f,t) \mid f \in C_1, t = 0,1,2\dots\},$$
$$C_1'' = \{(f,t) \mid f \in C_1, t = 1,2\dots\},$$

где C_1 — множество булевых функций.

Будем говорить, что элементы (f_1,t) и (f_2,t) совпадают, если функции f_1 и f_2 совпадают, то есть совпадают их множества существенных переменных, и на любом наборе значений существенных переменых значения функций совпадают.

На произвольном множестве $B \subseteq C_1'$ определим оператор синхронной суперпозиции. Для этого рассмотрим следующие операции.

1. Операция переименования переменных.

Пусть $(f(x_1,\dots,x_i,\dots,x_n),t) \in B$ и y — некоторая переменная.

Тогда результатом применения операции переименования переменной x_i в переменную y к элементу $(f(x_1,\dots,x_i,\dots,x_n),t)$ является элемент $(f(x_1,\dots,y,\dots,x_n),t)$.

2. Операция подстановки.

Для этой операции отождествим каждую переменную x_i с элементом $(x_i,0)$.

Пусть даны элементы множества $B \in C_1''$

$$(f(x_1,\dots,x_n),t_1),(g_1,t_2),\dots,(g_n,t_2).$$

Тогда результатом применения операции подстановки элементов $(g_1,t_2),\dots,(g_n,t_2)$ в элемент $(f(x_1,\dots,x_n),t_1)$ является элемент

$$(f(g_1,\dots,g_n),t_1+t_2),$$

где $f(g_1,\dots,g_n)$ — обычная суперпозиция функций $g_1,\dots,g_n$ и f.

Элемент (F, T) называется синхронной суперпозицией над множеством $B \in C_1''$, если он может быть получен из элементов множества B с помощью операций переименования переменных и подстановки.

Класс всех синхронных суперпозиций над B обозначим через $[B]_{cc}$.

Множество B называется синхронно-замкнутым, если$[B]_{cc} = B$.

Множество B_1 синхронно-выразимо через B_2, если $[B_2]_{cc} \supseteq B_1$.

Множество $B_1 \subseteq B$ называется синхронно-полным в B, если $[B_1]_{cc} = B$.

3. Слабозамкнутые классы булевых функций

Пусть $B \subseteq C_1'$. Одинаковые функции могут входить в B с разными задержками.

Множество булевых функций $M = \{f \in C_1 \mid \exists t \geqslant 0 : (f, t) \in B\}$ называется первой проекцией множества B и обозначается $Pr_1(B)$.

Множество булевых функций M называется слабозамкнутым, если существует синхронно-замкнутое множество $B' \subseteq C_1'$ такое, что $Pr_1 B' = M$.

Множество булевых функций M называется положительно-слабозамкнутым, если существует синхронно-замкнутое множество $B' \subseteq C_1''$ такое, что $Pr_1 B' = M$. Положительно-слабозамкнутое множество является слабозамкнутым.

Все замкнутые классы Поста являются положительно-слабозамкнутыми. Это следует из того, что операция синхронной суперпозиции на объектах (f, t) слабее операции суперпозиции на множестве булевых функций в том смысле, что первая проекция синхронного замыкания $Pr_1([M]_{cc})$ является подмножеством множества $[Pr_1(M)]$. А для любого замкнутого класса Поста P и любого класса M, такого, что $P = Pr_1(M)$ верно

$$P = Pr_1(M) \subseteq Pr_1([M]_{cc}) \subseteq [Pr_1(M)] = [P] = P.$$

То есть все включения обращаются в равенства и $P = Pr_1([M]_{cc})$ для любого M, такого, что $P = Pr_1(M)$.

Существуют также слабозамкнутые классы, не являющиеся замкнутыми классами Поста. Например, рассмотрим множество

$$\tilde{S} = \{(f, 0), (\varphi, t) \mid \varphi \in Y, f \in S, t = 1, 2, \ldots\},$$

где $Y = \{\varphi \mid \varphi(x_1, \ldots, x_n) = \varphi(\bar{x}_1, \ldots, \bar{x}_n)\}$ — множество четных функций, а $S = \{f \mid f(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n)\}$ — множество самодвойственных функций.

Первая проекция множества $\tilde{S}$ $\{f, \varphi \mid \varphi \in Y, f \in S\}$ будет слабозамкнутым классом, так как первая проекция синхронного замыкания множества $\tilde{S}$ будет содержать все четные и самодвойственные функции.

Рассмотрим два замкнутых класса Поста M_1 и M_2, такие, что $M_2 \subseteq M_1$.

Будем говорить, что пара множеств (M_1, M_2) относится к первому типу, если не существует слабозамкнутого множества K, такого что $M_2 \subset K \subset M_1$.

Будем говорить, что пара множеств (M_1, M_2) относится ко второму типу, если не существует положительно-слабозамкнутого множества K, такого что $M_2 \subset K \subset M_1$, но существует слабозамкнутое множество K' (не являющееся положительно-слабозамкнутым), такое что $M_2 \subset K' \subset M_1$.

Будем говорить, что пара множеств (M_1, M_2) относится к третьему типу, если существует положительно-слабозамкнутое множество K, такое что $M_2 \subset K \subset M_1$.

4. Слабозамкнутые классы линейных булевых функций

Все множество линейных функций можно разделить на четыре класса.

– Класс (1): линейные γ-функции, то есть функции, обращающиеся при отождествлении переменных в 0. В данный класс входят константа 0 и функции вида $\Sigma_{i=1}^{2k} x_i$.

– Класс (2): линейные α-функции, то есть функции, обращающиеся при отождествлении переменных в x. В данный класс входят функции вида $\Sigma_{i=1}^{2k+1} x_i$.

– Класс (3): линейные β-функции, то есть функции, обращающиеся при отождествлении переменных в 1. В данный класс входят константа 1 и функции вида $\Sigma_{i=1}^{2k} x_i + 1$.
– Класс (4): линейные δ-функции, то есть функции, обращающиеся при отождествлении переменных в $x + 1$. В данный класс входят функции вида $\Sigma_{i=1}^{2k+1} x_i + 1$.

Лемма 1. *Если слабозамкнутый класс линейных функций содержит хотя бы одну функцию из класса (i), существенно зависящую от двух или более переменных, то данный класс должен содержать целиком весь класс* (i).

Доказательство. Если функция f принадлежит классу (1) и отлична от константы 0, то отождествлением переменных из нее можем получить функцию $x_1 + x_2$. Из пары $(x_1 + x_2, t)$, где t — произвольная задержка, подстановкой в себя можно получить пары вида $(x_1 + \ldots + x_{2^k}, 2^{k-1}t)$, а из данных пар отождествлением переменных можем получить и любую функцию из класса (1) с некоторой задержкой. Следовательно, слабозамкнутый класс, содержащий некоторую функцию из класса (1), отличную от 0, содержит весь класс (1).

Аналогичные рассуждения верны для любой функции из класса (2), отличной от x, для любой функции из класса (3), отличной от константы 1, и для любой функции из класса (4), отличной от $x + 1$. Лемма доказана.

Рассмотрим множества линейных функций, получаемые при различных объединениях классов (1)–(4). Объединение классов (i) и (j) будем обозначать как класс (ij).

Можно заметить, что $(1234) = L_1, (23) = L_2, (12) = L_3, (2) = L_4$, $(24) = L_5$.

Будем говорить, что рассматриваем класс с нулевыми задержками, если приписываем всем функциям из этого класса задержки равные нулю. Будем говорить, что рассматриваем функцию с положительной задержкой, если приписываем функции всевозможные положительные задержки. Будем говорить, что рассматриваем класс с положительными задержками, если приписываем всем функциям из этого класса всевозможные положительные задержки.

Лемма 2. *Слабозамкнутый класс, содержащий класс* (4)*, содержит класс* (2)*.*

Доказательство. Рассмотрим некоторую функцию из класса (4) с произвольной задержкой и рассмотрим синхронную суперпозицию, подставляя эту функцию в себя вместо всех своих аргументов, переименовав некоторым образом переменные. В результате получим функцию из класса (2).

Данная синхронная суперпозиция допустима, так как задержки у объектов, подставляемых в аргументы, одинаковы. Любая функция из класса (2) с произвольной задержкой, кроме тождественной, порождает весь класс (2) с некоторым набором задержек. Таким образом, класс (4) порождает класс (2), и слабозамкнутый класс, содержащий класс (4), должен содержать и класс (2). Лемма доказана.

Следствие из леммы 2. *Классы* $(4), (14), (34), (134)$ *не являются слабозамкнутыми.*

Лемма 3. *Классы* $(1), (3), (13)$ *являются положительно-слабозамкнутыми, а классы* $(124), (234)$ *не являются слабозамкнутыми классами.*

Доказательство. Отождествление переменных переводит функцию из класса (i) в функцию из класса (i).

Классы $(1), (3), (13)$ являются положительно-слабозамкнутыми классами. В качестве задержек достаточно рассмотреть любые положительные числа. Обозначим эти классы соответственно SL_1, SL_2, SL_3.

Класс (124) не является слабозамкнутым, так как при подстановке в функцию из класса (4) функций из класса (1) получим функцию из класса (3).

Аналогично, класс (234) не является слабозамкнутым, так как при подстановке в функцию из класса (4) функций из класса (3) получим функцию из класса (1). Лемма доказана.

Лемма 4. *Класс* (123) *является слабозамкнутым, но не является положительно-слабозамкнутым.*

Доказательство. Класс (123) является слабозамкнутым. Действительно, достаточно рассмотреть функции из классов (1) и (3) с по-

ложительными задержками, а функции из класса (2) с нулевыми задержками. Обозначим этот класс SL_4.

В то же время класс SL_4 не является положительно-слабозамкнутым: в классе (2) есть тождественная функция x, пусть ей приписана положительная задержка t_1, в классе (1) есть функция $x+y$, пусть ей приписана положительная задержка t_2. Подставим тожественную функцию x в себя t_2-1 раз, получим пару $(x, t_1 \cdot t_2)$. Подставим $x+y$ в себя вместо обоих аргументов t_1-1 раз, предварительно переименовав переменные так, чтобы у разных копий были разные переменые. Получим пару $(\Sigma_{i=1}^{2^{t_1-1}} x_i, t_1 \cdot t_2)$. Отождествим все переменные, кроме первых двух, получим пару $(x_1+x_2, t_1 \cdot t_2)$. В классе (3) есть функция x_1+x_2+1 с некоторой задержкой t. Подставим пары $(x, t_1 \cdot t_2), (y+z, t_1 \cdot t_2)$ в пару (x_1+y_1+1, t), получим пару $(x+y+z+1, T)$, первая проекция которой принадлежит классу (4). Лемма 4 доказана.

Введем обозначение: $f_{(1)}=0$, $f_{(2)}=x$, $f_{(3)}=1$, $f_{(4)}=x+1$.

Рассмотрим теперь случай, когда множество кроме прочих содержит функцию $f_{(i)}$ из класса (i).

Обозначим объединение класса (i) и функции $f_{(j)}$ как $(i\bar{j})$.

Множество, состоящее только из функции $f_{(i)}$ обозначим как класс $(\bar{i})$.

Нетрудно видеть, что $(\bar{2}) = O_1, (\bar{3}) = O_2, (\bar{1}) = O_3, (\bar{2}\bar{4}) = O_4$, $(\bar{2}\bar{3}) = O_5, (\bar{1}\bar{2}) = O_6, (\bar{1}\bar{3}) = O_7, (\bar{1}\bar{2}\bar{3}) = O_8, (\bar{1}\bar{2}\bar{3}\bar{4}) = O_9$.

Лемма 5. *Класс* $(\bar{4})$ *пороэюдает класс* $(\bar{2})$*, поэтому если в слабозамкнутый класс входит включен класс* $(\bar{4})$*, то должен быть включен класс* $(\bar{2})$.

Класс $(\bar{1}\bar{4})$ *пороэюдает класс* $(\bar{3})$*, класс* $(\bar{3}\bar{4})$ *пороэюдает класс* $(\bar{1})$*, класс* $(1\bar{4})$ *пороэюдает класс* (3)*, класс* $(3\bar{4})$ *пороэюдает класс* (1)*, класс* $(2\bar{4})$ *пороэюдает класс* (4).

Доказательство. Если дана пара $(x+1, t)$, где t — произвольная задержка, то из нее подстановкой в себя можно получить пару $(x, 2t)$, следовательно, класс $(\bar{4})$ порождает класс $(\bar{2})$.

Из пар $(0, t_1), (x+1), t_2$, где t_1 и t_2 — произвольные задержки, можно получить пару $(1, t_1+t_2)$, а из пар $(1, t_1), (x+1), t_2$, где t_1 и t_2 — произвольные задержки, можно получить пару $(0, t_1+t_2)$, сле-

довательно, класс $(\bar{1}\bar{4})$ порождает класс $(\bar{3})$, а класс $(\bar{3}\bar{4})$ порождает класс $(\bar{1})$.

Из пар $(\Sigma_{i=1}^{2k} x_i, t_1), (x+1, t_2)$, где t_1 и t_2 — произвольные задержки, можно получить пару $(\Sigma_{i=1}^{2k} x_i + 1, t_1 + t_2)$, из пар $(\Sigma_{i=1}^{2k} x_i + 1, t_1), (x + 1, t_2)$, где t_1 и t_2 — произвольные задержки, можно получить пару $(\Sigma_{i=1}^{2k} x_i, t_1 + t_2)$, из пар $(\Sigma_{i=1}^{2k+1} x_i, t_1), (x + 1, t_2)$, где t_1 и t_2 — произвольные задержки, можно получить пару $(\Sigma_{i=1}^{2k+1} x_i + 1, t_1 + t_2)$, следовательно, класс $(1\bar{4})$ порождает класс (3), класс $(3\bar{4})$ порождает класс (1), класс $(2\bar{4})$ порождает класс (4). Лемма доказана.

Лемма 6. *Классы* $(\bar{1}2), (1\bar{2}), (\bar{2}3), (2\bar{3}), (\bar{1}23), (1\bar{2}3), (12\bar{3}), (\bar{1}2\bar{3}), (\bar{1}2\bar{3}4), (1\bar{2}3\bar{4})$ *являются слабозамкнутыми классами, но не являются положительно-слабозамкнутыми классами.*

Доказательство. Класс $(\bar{1}2)$ является слабозамкнутым классом. Для доказательства достаточно рассмотреть класс (2) с нулевыми задержками, а класс $(\bar{1})$ с положительной задержкой. Обозначим этот слабозамкнутый класс SL_5.

Класс SL_5 не является положительно-слабозамкнутым: тождественную функцию $x \in (\bar{2})$ с ненулевой задержкой и константу $0 \in (1)$ с ненулевой задержкой можно синхронизировать, подставив каждую функцию в себя необходимое число раз. После этого, подставляя вместо первых двух переменных функции $x_1 + x_2 + x_3 \in (2)$ тождественные функции, а вместо последней переменной — константу 0, получим функцию $x_1 + x_2$ с некоторой задержкой, и, следовательно, и весь класс (1).

Класс $(2\bar{3})$ является слабозамкнутым классом: рассмотрим класс (2) с нулевой задержкой, а класс $(\bar{3})$ рассмотрим с положительной задержкой. Обозначим этот класс SL_6.

Класс SL_6 не является положительно-слабозамкнутым классом, рассуждения повторяют доказательство аналогичного утверждения для SL_5.

Класс $(\bar{1}2\bar{3})$ является слабозамкнутым классом: рассмотрим класс (2) с нулевыми задержками, класс $(\bar{3})$ с положительной задержкой, класс $(\bar{1})$ с положительной задержкой. Обозначим этот класс SL_7.

Класс SL_7 не является положительно-слабозамкнутым классом, так как из доказательства леммы 6 следует, что класс $(\bar{1}2)$ порождает весь класс (1) в случае положительных задержек.

Классы $(1\bar{2}), (\bar{2}3), (1\bar{2}3)$ являются слабозамкнутыми, так как классы $(1), (3), (13)$ можно рассматривать с положительными задержками, и добавление тождественной функции $x \in (\bar{2})$ с нулевой задержкой не порождает ничего нового. Обозначим эти классы SL_8, SL_9, SL_{10}.

Классы SL_8, SL_9, SL_{10} не являются положительно-слабозамкнутыми. Доказательство данного утверждения аналогично рассмотрению предыдущих случаев (каждый раз сможем получить либо весь класс (2) либо весь класс (4)).

Класс $(12\bar{3})$ является слабозамкнутым. Действительно, достаточно рассмотреть все функции из класса (12) с нулевыми задержками, константу $0 \in (1)$ с положительной задержкой и константу $1 \in (\bar{3})$ с положительной задержкой. Обозначим этот класс SL_{11}.

Класс SL_{11} не является положительно-слабозамкнутым классом. Действительно, синхронизируя тождественную функцию из класса (2) и функцию $x_1 + x_2$ из класса (1) и подставляя их в функцию $y_1 + y_2 + 1 \in (3)$, получим функцию $x + x_1 + x_2 + 1 \in (4)$.

Класс $(\bar{1}23)$ является слабозамкнутым. Рассмотрим все функции из класса (23) с нулевыми задержками, константу 1 с положительной задержкой и константу 0 с положительной задержкой. Обозначим этот класс SL_{12}.

Класс SL_{12} не является положительно-слабозамкнутым классом. Рассмотрение аналогично случаю класса $(12\bar{3})$.

Класс $(\bar{1}2\bar{3}4)$ является слабозамкнутым. Рассмотрим функции из класса (24) с нулевыми задержками, константу 0 с положительной задержкой и константу 1 с положительной задержкой. Обозначим этот класс SL_{13}.

Класс SL_{13} не является положительно-слабозамкнутым классом, так как из доказательства леммы 6 следует, что $(\bar{1}2)$ порождает весь класс (1) в случае положительных задержек.

Класс $(1\bar{2}3\bar{4})$ является слабозамкнутым. Рассмотрим функции из класса (13) с положительными задержками, функцию $x + 1 \in (\bar{4})$ с

нулевой задержкой, тождественную функцию с нулевой задержкой. Обозначим этот класс SL_{14}.

Класс SL_{14} не является положительно-слабозамкнутым, так как из доказательства леммы 6 следует, что класс $(1\bar{2})$ порождает весь класс (2) в случае положительных задержек. Лемма доказана.

Лемма 7. *Классы* $(12\bar{3}4), (\bar{1}234), (\bar{1}3), (\bar{1}\bar{2}3), (1\bar{3}), (1\bar{2}\bar{3}), (\bar{1}24), (2\bar{3}4)$ *не являются слабозамкнутыми.*

Доказательство. Как было показано в доказательстве леммы 3, класс (124) порождает класс (3), следовательно, класс $(12\bar{3}4)$ не является слабозамкнутым.

Аналогично, класс (234) порождает класс (1), следовательно, класс $(\bar{1}234)$ не является слабозамкнутым.

Класс $(\bar{1}3)$ не является слабозамкнутым, так как если рассмотреть $0 \in (\bar{1})$ с нулевой задержкой, то из класса (3) получим функцию из класса (4), а значит и сам класс (4), подставив 0 вместо одной из переменных. Если же рассмотреть 0 с положительной задержкой t_1 и некоторую функцию f из класса (3), отличную от константы 1, с положительной задержкой t_2, то подставляя 0 в себя t_2-1 раз, а f в себя t_1-1 раз получим 0 и некоторую функцию $F \in (3)$ из (являющуюся $t-1$-ой итерацией f) с одинаковыми задержками $t_1 \cdot t_2$. Подставляя в F вместо всех переменных, кроме одной, саму F, а вместо оставшейся переменной функцию 0 с задержкой $t_1 \cdot t_2$ получаем функцию из класса (1). Если же взять все функции из класса (3), отличные от константы, с нулевыми задержками, то получим все функции из класса (2).

Класс $(\bar{1}\bar{2}3)$ тоже не является слабозамкнутым, так как добавление тождественной функции не порождает ничего нового.

Класс $(1\bar{3})$ не является слабозамкнутым, так как если рассмотреть класс $(\bar{3})$ с нулевой задержкой, то из класса (1) получим класс (4). Если же рассмотреть константу $1 \in (\bar{3})$ с положительной задержкой и еще некоторую функцию из класса (1), отличную от константы 0, с положительной задержкой, то получаем функцию из класса (3) (рассуждения аналогичны случаю с классом $(\bar{1}3)$). Если же взять все функции из класса (1), отличные от константы с нулевыми задержками, то получим все функции из класса (2). Следовательно, класс

$(1\bar{2}\bar{3})$ тоже не является слабозамкнутым (так как добавление тождественной функции не порождает ничего нового).

Класс $(\bar{1}24)$ не является слабозамкнутым, так как при подстановке константы $0 \in (\bar{1})$ в некоторую функцию из класса (4) получаем константу $1 \in (3)$.

Класс $(2\bar{3}4)$ не является слабозамкнутым, так как при подстановке константы $1 \in (\bar{3})$ в некоторую функцию из класса (4) получаем константу $0 \in (1)$. Лемма доказана.

Теорема 1. *Классы $L_1 - L_5, O_1 - O_9, SL_1 - SL_{14}$ являются слабозамкнутыми, при этом классы $L_1 - L_5, O_1 - O_9, SL_1 - SL_3$ являются положительно-слабозамкнутыми классами.*

Других слабозамкнутых классов линейных функций не существует.

Доказательство теоремы. Из леммы 1 следует, что слабозамкнутый класс линейных функций, содержащий функции из класса (i), либо содержит весь класс (i), либо содержит только функцию $f_{(i)}$ и никакую другую функцию из класса (i).

Следовательно, слабозамкнутый класс линейных функций имеет один из видов: $(i), (ij), (ijk), (ijkl), (\bar{i}), (\bar{i}j), (\bar{i}jk), (\bar{i}jkl), (\bar{i}\bar{j}), (\bar{i}\bar{j}k), (\bar{i}\bar{j}kl), (\bar{i}\bar{j}\bar{k}), (\bar{i}\bar{j}\bar{k}l), (\bar{i}\bar{j}\bar{k}\bar{l})$, где $i, j, k, l \in \{1, 2, 3, 4\}$.

Из леммы 2 следует, что среди классов вида $(i), (ij), (ijk), (ijkl)$ слабозамкнутыми могут быть только классы $(1), (2), (3), (4), (12), (13), (14), (23), (24), (34), (123), (124), (134), (234), (1234)$.

Из них $(1234) = L_1, (23) = L_2, (12) = L_3, (2) = L_4, (24) = L_5$.

Из лемм 3 и 4 следует, что среди оставшихся классов вида $(i), (ij), (ijk), (ijkl)$ слабозамкнутыми являются только SL_1–SL_4, причем классы SL_1, SL_2, SL_3 являются положительно-слабозамкнутыми.

Из лемм 2 и 5 следует, что среди классов вида $(\bar{i}), (\bar{i}j), (\bar{i}jk), (\bar{i}jkl), (\bar{i}\bar{j}), (\bar{i}\bar{j}k), (\bar{i}\bar{j}kl), (\bar{i}\bar{j}\bar{k}), (\bar{i}\bar{j}\bar{k}l), (\bar{i}\bar{j}\bar{k}\bar{l})$ слабозамкнутыми могут быть только классы $(\bar{1}2), (1\bar{2}), (\bar{1}3), (1\bar{3}), (\bar{2}3), (2\bar{3}), (\bar{1}23), (1\bar{2}3), (12\bar{3}), (\bar{1}\bar{2}3), (1\bar{2}\bar{3}), (\bar{1}2\bar{3}), (\bar{1}24), (2\bar{3}4), (\bar{1}234), (12\bar{3}4), (\bar{1}2\bar{3}4), (1\bar{2}3\bar{4})$.

Из них $(\bar{2}) = O_1, (\bar{3}) = O_2, (\bar{1}) = O_3, (\bar{2}\bar{4}) = O_4, (\bar{2}\bar{3}) = O_5, (\bar{1}\bar{2}) = O_6, (\bar{1}\bar{3}) = O_7, (\bar{1}\bar{2}\bar{3}) = O_8, (\bar{1}\bar{2}\bar{3}\bar{4}) = O_9$.

Из лемм 6 и 7 следует, что среди оставшихся классов слабозамкнутыми являются только классы $SL_5 - SL_1 4$, которые не являются положительно-слабозамкнутыми. Теорема 1 доказана.

Из теоремы 1 следует

Теорема 2. *Справедливы следующие положения.*
а) Пары классов линейных функций (L_5, L_4), (L_5, O_4), (L_4, O_1), (O_i, O_j), *где* O_j *является предполным в* O_i, *относятся к первому типу;*
б) Пары классов $(L_1, L_2), (L_1, L_3), (L_1, L_5), (L_2, L_4), (L_3, L_4), (L_2, O_5)$, $(L_3, O_6), (L_1, O_9)$ *относятся ко второму типу.*

Автор выражает благодарность своему научному руководителю Кудрявцеву В. Б. за помощь в научной деятельности и написании данной статьи.

Список литературы

[1] Кудрявцев В. Б., Блохина Г. Н., Кнап Ж., Кудрявцев В. В. Алгебра логики. — Москва — Любляна, 2006.

[2] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

Слабозамкнутые классы самодвойственных булевых функций

Петрова О. А. (Москва, МГУ им. М. В. Ломоносова)

hellga.01@mail.ru

1. Замыкание относительно операции суперпозиции

Введем следующие обозначения.

Множество $\{0,1\}$ обозначим через E_2, тогда E_2^n — декартово произведение n сомножителей E_2.

Отображение $f : E_2^n \to E_2$ называется булевым.

Пусть $U = \{u_1, u_2, \ldots\}$ — счетный алфавит переменных, принимающих значения из E_2. Тогда отображение f можно интерпретировать как функцию $f(u_{j_1}, \ldots, u_{j_n})$, которая определяется, во-первых, отображением f, а во-вторых, указанием переменных, от которых она зависит. Такие функции и переменные $u_k \in U$, называются также булевыми. Класс всех булевых функций обозначаем C_1.

Далее, для обозначения переменных будем иногда использовать латинские буквы x, y, z, возможно, с индексами.

На произвольном множестве булевых функций M можно индуктивно ввести понятие формулы.

1. Пусть $f(x_1, \ldots, x_n)$ — функция из M; тогда выражение $f(x_1, \ldots, x_n)$ является формулой над M.

2. Пусть $f(x_1, \ldots, x_n)$ — функция из M и в строке $G_1, \ldots, G_n$ каждое выражение G_i является либо формулой над M, либо переменной из U, тогда выражение $f(G_1, \ldots, G_n)$ является формулой над M.

Класс всех формул над M обозначается $<M>$.

Далее, каждой формуле A из $<M>$ индуктивно сопоставляется функция из M, называемая суперпозицией над M.

1. Если формула A из $<M>$ является выражением $f(x_1, \ldots, x_n)$ таким, что функция $f(x_1, \ldots, x_n)$ принадлежит M, то A сопоставляем булеву функцию $f(x_1, \ldots, x_n)$, которую называем суперпозицией над M.

2. Пусть формула A имеет вид $f(G_1, \ldots, G_n)$, где $f(x_1, \ldots, x_n)$ есть функция из M, а каждое выражение G_i является либо формулой над

M, либо переменной из U. Сопоставим каждому G_i выражение g_i, где g_i — булева функция, если G_i — формула над M, и g_i — переменная u_{j_i}, если G_i — эта переменная. В результате получим выражение $f(g_1, \ldots, g_n)$. Рассмотрим его как функцию $h(y_1, \ldots, y_m)$ от множества переменных $U' = \{y_1, \ldots, y_m\}$, содержащего точно все те переменные, от которых зависит хотя бы одна их функций g_i и f. Эту булеву функцию h сопоставляем выражению $f(G_1, \ldots, G_n)$ и называем суперпозицией над M.

Класс всех суперпозиций над M обозначается $[M]$.

Тройка $(M, <M>, [M])$ называется алгеброй (функциональной системой), порожденной множеством M.

Оператор [] обладает следующими свойствами:

$$1)[M] \supseteq M;$$
$$2)M_1 \supseteq M_2 \Rightarrow [M_1] \supseteq [M_2];$$
$$3)[[M]] = [M].$$

и называется замыканием. Множество M называется замкнутым, если $[M] = M$.

Говорят, что множество M_1 выразимо через M_2, если $[M_2] \supseteq M_1$.

Множество $M_1 \subseteq M$ называется полным в M, если $[M_1] = M$. В случае, если множество M_1 конечно, множество M называется конечно порожденным.

Множество $M_1 \subseteq M$ называется предполным в M, если оно является замкнутым, и для любой функции f, такой что $f \in M, f \notin M_1$, верно $[M_1 \cup \{f\}] = M$.

Множество M_1 называется базисом в M, если оно полно в M, но всякое его собственное подмножество уже не полно в M.

Множество $\Sigma(M)$ всех замкнутых подмножеств множества M образует частичный порядок по отношению включения. Этот порядок называется решеткой замкнутых классов в M и представляют в виде графа. Вершинами этого графа являются замкнутые классы булевых функций, вложение которых друг в друга обозначается ребром, ориентированным от более широкого класса к классу, вложенному в него.

Замкнутые множества из $\Sigma(C_1)$ называются классами Поста.

Функция f называется самодвойственной, если верно

$$f(\bar{x}_1, \ldots, \bar{x}_n) = \bar{f}(x_1, \ldots, x_n).$$

Рассмотрим представление булевых функций в базисе

$$\{x_1 \cdot x_2, x_1 + x_2, 0, 1\}$$

которое называется разложением в полиномом Жегалкина.

Булева функция $f(x_1, \ldots, x_n)$, чей полином Жегалкина имеет вид

$$\Sigma a_i x_i + d,$$

называется линейной.

Пусть $c \in E_2$. Говорят, что булева функция $f(x_1, \ldots, x_n)$ сохраняет константу c, если $f(c, \ldots, c) = c$.

Пусть даны два набора $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$, такие, что при любых $i \leqslant n$ верно $\alpha_i \leqslant \beta_i$. Говорят, что набор α предшествует набору β и пишут $\alpha \leqslant \beta$. Булева функция $f(x_1, \ldots, x_n)$ называется монотонной, если для любых наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$ из соотношения $\alpha \leqslant \beta$ следует, что $f(\alpha) \leqslant f(\beta)$.

Булева функция f называется α-функцией, если $f(x, \ldots, x) = x$.

Булева функция f называется β-функцией, если $f(x, \ldots, x) = 1$.

Булева функция f называется γ-функцией, если $f(x, \ldots, x) = 0$.

Булева функция f называется δ-функцией, если $f(x, \ldots, x) = x+1$.

Множество всех самодвойственных булевых функций обозначается D_3.

Множество самодвойственных монотонных булевых функций, обозначается D_2.

Множество булевых функций, сохраняющих константы 0 и 1, обозначается C_4.

Множество самодвойственных булевых функций, сохраняющих константы 0 и 1, обозначается D_1.

Множество самодвойственных линейных булевых функций, обозначается L_5.

Множество самодвойственных линейных булевых функций, сохраняющих константы 0 и 1, обозначается L_4.

Множества D_3, D_2, D_1, L_4, L_5 являются замкнутыми классами относительно операции суперпозиции.

Также замкнутыми классами линейных функций являются следующие классы одноместных функций:

$O_1 = \{x\}, O_4 = \{x, x+1\}$.

2. Операция синхронной суперпозиции

Рассмотрим пары (f, t), где f — булева функция , t — натуральное число или 0, называемое временной задержкой.

Обозначим

$$C_1' = \{(f,t) \mid f \in C_1, t = 0, 1, 2 \ldots\},$$
$$C_1'' = \{(f,t) \mid f \in C_1, t = 1, 2 \ldots\},$$

где C_1 — множество булевых функций.

На произвольном множестве $B \subseteq C_1'$ определим оператор синхронной суперпозиции. Для этого рассмотрим следующие операции.

1. Операция переименования переменных.

Пусть $(f(x_1, \ldots, x_i, \ldots, x_n), t) \in B$ и y — некоторая переменная.

Тогда результатом применения операции переименования переменной x_i в переменную y к элементу $(f(x_1, \ldots, x_i, \ldots, x_n), t)$ является элемент $(f(x_1, \ldots, y, \ldots, x_n), t)$.

2. Операция подстановки.

Для этой операции отождествим каждую переменную x_i с элементом $(x_i, 0)$.

Пусть даны элементы множества $B \in C_1''$

$$(f(x_1, \ldots, x_n), t_1), (g_1, t_2), \ldots, (g_n, t_2).$$

Тогда результатом применения операции подстановки элементов (g_1, t_2),...,(g_n, t_2) в элемент $(f(x_1, \ldots, x_n), t_1)$ является элемент

$$(f(g_1, \ldots, g_n), t_1 + t_2),$$

где $f(g_1, \ldots, g_n)$ — результат подстановки функций $g_1, \ldots, g_n$ вместо аргументов функции f.

Элемент (F, T) называется синхронной суперпозицией над множеством $B \in C_1''$, если он может быть получен из элементов множества B с помощью операций переименования переменных и подстановки.

Класс всех синхронных суперпозиций над B обозначим через $[B]_{cc}$. Множество B называется синхронно-замкнутым, если$[B]_{cc} = B$. Множество B_1 синхронно-выразимо через B_2, если $[B_2]_{cc} \supseteq B_1$. Множество $B_1 \subseteq B$ называется синхронно-полным в B, если $[B_1]_{cc} = B$.

3. Слабозамкнутые классы булевых функций

Пусть $B \subseteq C_1'$. Одинаковые функции могут входить в B с разными задержками.

Множество булевых функций $M = \{f \in C_1 \mid \exists t \geqslant 0 : (f, t) \in B\}$ называется первой проекцией множества B и обозначается $Pr_1(B)$.

Множество булевых функций M называется слабозамкнутым, если существует синхронно-замкнутое множество $B' \subseteq C_1'$ такое, что $Pr_1 B' = M$.

Множество булевых функций M называется положительно-слабозамкнутым, если существует синхронно-замкнутое множество $B' \subseteq C_1''$ такое, что $Pr_1 B' = M$. Положительно-слабозамкнутое множество является слабозамкнутым.

Все замкнутые классы Поста являются положительно-слабозамкнутыми. Это следует из того, что операция синхронной суперпозиции на объектах (f, t) слабее операции суперпозиции на множестве булеых функций в том смысле, что первая проекция синхронного замыкания $Pr_1([M]_{cc})$ является подмножеством множества $[Pr_1(M)]$. А для любого замкнутого класса Поста P и любого класса M, такого, что $P = Pr_1(M)$ верно

$$P = Pr_1(M) \subseteq Pr_1([M]_{cc}) \subseteq [Pr_1(M)] = [P] = P.$$

То есть все включения обращаются в равенства и $P = Pr_1([M]_{cc})$ для любого M, такого, что $P = Pr_1(M)$.

Существуют также слабозамкнутые классы, не являющиеся замкнутыми классами Поста. Например, рассмотрим множество

$$\tilde{S} = \{(f, 0), (\varphi, t) \mid \varphi \in Y, f \in S, t = 1, 2, \ldots\},$$

где $Y = \{\varphi \mid \varphi(x_1, \ldots, x_n) = \varphi(\bar{x}_1, \ldots, \bar{x}_n)\}$ — множество четных функций, а $S = \{f \mid f(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n)\}$ — множество самодвойственных функций.

Первая проекция множества $\tilde{S}$ $\{f, \varphi \mid \varphi \in Y, f \in S\}$ будет слабозамкнутым классом, так как первая проекция синхронного замыкания множества $\tilde{S}$ будет содержать все четные и самодвойственные функции.

Рассмотрим два замкнутых класса Поста M_1 и M_2, такие, что $M_2 \subseteq M_1$.

Будем говорить, что пара множеств (M_1, M_2) относится к первому типу, если не существует слабозамкнутого множества K, такого что $M_2 \subset K \subset M_1$.

Будем говорить, что пара множеств (M_1, M_2) относится ко второму типу, если не существует положительно-слабозамкнутого множества K, такого что $M_2 \subset K \subset M_1$, но существует слабозамкнутое множество K' (не являющееся положительно-слабозамкнутым), такое что $M_2 \subset K' \subset M_1$.

Будем говорить, что пара множеств (M_1, M_2) относится к третьему типу, если существует положительно-слабозамкнутое множество K, такое что $M_2 \subset K \subset M_1$.

4. Слабозамкнутые классы самодвойственных булевых функций

Лемма 1. *Если* $B \subseteq C_1', Pr_1 B = D_1, f \in D_3, f \notin D_1$, *то для произвольного* $t \in N \cup \{0\}$ *выполнено* $D_3 = Pr_1[B \cup \{(f, t)\}]_{cc}$.

Доказательство. Все самодвойственные функции делятся на α- и δ-функции. Класс D_1 содержит все самодвойственные α-функции. Для любой самодвойственной функции f с вектором значений $(f_1, \ldots, f_n)$ существует самодвойственная функция g с набором значений $(g_1, \ldots, g_n) = (\bar{f}_1, \ldots, \bar{f}_n)$, обратным к вектору значений функции f. Сопоставим друг другу такие функции f и g.

Пусть дана пара (f_δ, t), где f является самодвойственной δ-функцией, то есть $f_\delta \in D_3, f_\delta \notin D_1$. Отождествлением переменных функции f_δ из данной пары можно получить пару $(x + 1, t)$. Теперь, для

произвольной самодвойственной δ-функции g рассмотрим соответсвующую α-функцию f, равную отрицанию функции g. В множестве пар B существует пара (f, t_1). Используя операцию подстановки пары (f, t_1) в пару $(x{+}1, t)$ можем получить пару $(g, t{+}t_1)$. Так как рассуждение проведено для произвольной самодвойственной δ-функции g, то подобным образом можем получить все самодвойственные δ-функции с некоторыми задержками. Данное множество в объединении с B в первой проекции даст весь класс D_3. Лемма доказана.

Обозначим $C_4' = \{(f, t) \mid f \in C_4, t = 0, 1, 2 \ldots\}$.

Лемма 2. *Если $B \subseteq C_4'$, то $[Pr_1 B] = Pr_1[B]_{cc}$.*

Доказательство. C_4 — множество всех булевых α-функций. Пусть даны пары (f, t) и (g, t_1), где $f(x_1, \ldots, x_n)$ — α-функция и $g(x_1, \ldots, x_m)$ — α-функция. Отождествлением переменных из данных пар можно получить пары (x, t) и (x, t_1). Применим операцию подстановки n копий элемента (x, t_1) в элемент $(f(x_1, \ldots, x_n), t)$, получим элемент $(f, t + t_1)$. Теперь применим операцию подстановки m копий элемента (x, t) в элемент $(g(x_1, \ldots, x_m), t_1)$, получим элемент $(g, t + t_1)$. Таким образом, мы получили функции f и g с одинаковыми задержками. Применяя данное рассуждение к произвольному множеству $\{(g_1, t_1), \ldots, (g_n, t_n)\} \subseteq B$, можем получить множество $\{(g_1, t_1 + \ldots + t_n), \ldots, (g_n, t_1 + \ldots + t_n)\}$. Следовательно, имея произвольное множество пар $\{(f(x_1, \ldots, x_n), t)(g_1, t_1), \ldots, (g_n, t_n)\} \subseteq B$ всегда можно применить операцию подстановки и получить пару $(f(g_1, \ldots, g_n), t + t_1 + \ldots + t_n)$. Отсюда следует утверждение леммы. Лемма доказана.

Обозначим $D_2' = \{(f, t) \mid f \in D_2, t = 0, 1, 2 \ldots\}$.

Лемма 3. *Если $B \subseteq D_2'$, и существует пара $(f, t) \in B$, такая , что $f \neq x$, то $Pr_1[B]_{cc} = D_2$.*

Доказательство. По лемме 2 так как $D_2 \subset D_1$, то $Pr_1[B]_{cc} = [Pr_1 B]$. Множество $[Pr_1 B]$ является замкнутым множеством монотонных самодвойственных функций, при этом $[Pr_1 B] \neq \{x\}$, так как по условию в $[Pr_1 B]$ есть нетождественная функция f. Единственным замкнутым классом монотонных самодвойственных функций, содержащим нетождественные функции, является D_2. Лемма доказана.

Лемма 4. *Из любой нелинейной самодвойственной функции подстановкой переменных можно получить одну из следующих функций:*

$yz + xy + xz(+1)$
$yz + xy + xz + y + z(+1)$
$yz + xy + xz + x + y(+1)$
$yz + xy + xz + x + z(+1)$.

Доказательство. Используем известный результат: из нелинейной функции при помощи подстановки переменных можно получить нелинейную булеву функцию от двух переменных, либо функцию от трех переменных, x-компонента которой нелинейна.

Применим данный результат к произвольной нелинейной самодвойственной функции. Нелинейных самодвойственных функций от двух переменных не существует. Следовательно, из данной функции при помощи подстановки переменных можно получить нелинейную булеву функцию от трех переменных, x-компонента которой нелинейна. Существует всего шестнадцать самодвойственных функций от трех переменных, они определяются своими значениями на первых четырех наборах. Половина из этих функций являются линейными (x, $x+1$, y, $y+1$, z, $z+1$, $x+y+z$, $x+y+z+1$). Оставшиеся восемь функций являются нелинейными самодвойственными:

$yz + xy + xz$
$yz + xy + xz + y + z$
$yz + xy + xz + x + y$
$yz + xy + xz + x + z$
$yz + xy + xz + 1$
$yz + xy + xz + y + z + 1$
$yz + xy + xz + x + y + 1$
$yz + xy + xz + x + z + 1$.

Лемма доказана.

Теорема 1. *Пары классов* (D_3, D_1), (D_2, O_1), (D_1, D_2), (D_1, L_4), (D_3, L_5) *относятся к первому типу.*

Доказательство. По лемме 1, если рассмотреть множество пар, состоящих из функции из D_1 и некоторой (произвольной) задержки, и добавить к этому множеству пару из функции, не принадлежащей D_1, с некоторой задержкой, то в первой проекции синхронного замы-

кания полученного множества пар получится весь класс самодвойственных функций D_3. Следовательно, пара множеств (D_3, D_1) относится к первому типу.

По лемме 2 первая проекция синхронного замыкания некоторого множества α-функций с произвольными задержками совпадает с замыканием этого множества α-функций относительно операции суперпозиции. Множество D_1 состоит из всех самодвойственных α-функций, следовательно, первая проекция любого синхронно замкнутого множества пар, состоящих их функции из D_1 и некоторой временной является замкнутым классом Поста. Таким образом, пары множеств (D_1, D_2) и (D_1, L_4) относятся к первому типу.

По лемме 3 пара множеств (D_2, O_1) относится к первому типу.

Рассмотрим множество пар, состоящих из линейной самодвойственной функции и некоторой задержки. Среди них существуют пары (x, t_1), $(x_1 + x_2 + x_3, t_0)$, $(x_1 + x_2 + x_3 + 1, t_1)$. Добавим к данному множеству пару, состоящую из нелинейной самодвойственной функции f с некоторой задержкой t.

По лемме 4 из функции f подстановкой переменных можно получить самодвойственную функцию от трех переменных вида $xy+xz+yz+\alpha_1 x+\alpha_2 y+\alpha_3 z+\beta$, где $\alpha_1, \alpha_2, \alpha_3, \beta \in \{0, 1\}$ и $\alpha_1+\alpha_2+\alpha_3 = 0$. Так как у нас есть пары (x, t_1), (y, t_1), (z, t_1), получаемые переименование переменной в паре (x, t_1), то аналогичной подстановкой переменных из пары (f, t) можем получить пару $(xy + xz + yz + \alpha_1 x + \alpha_2 y + \alpha_3 z + \beta, t_1 + t)$.

Переименование переменных получаем пары $(xy + xz + yz + \alpha_2 x + \alpha_3 y + \alpha_1 z + \beta, t_1 + t)$ и $(xy + xz + yz + \alpha_3 x + \alpha_1 y + \alpha_2 z + \beta, t_1 + t)$. Применим операцию подстановки полученных пар в элемент $(x_1 + x_2 + x_3 + \beta, t_\beta)$, получим пару $(xy + xz + yz, t_1 + t_\beta + t)$, где функция $xy + xz + yz$ является α-функцией и базисом класса D_1. К паре $(xy + xz + yz, t_1 + t_\beta + t)$ применимо утверждение леммы 2. Следовательно, из пары $(xy + xz + yz, t_1 + t_\beta + t)$ можем получить множество пар, первой проекцией которого является весь класс D_1.

Далее заметим, что функция $x_1 + x_2 + x_3 + 1$ не принадлежит D_1. А так как выше доказано, что пара множеств (D_3, D_1) относится к первому типу, то можно получить множество пар, первой проекцией которого является весь класс D_3.

Следовательно, пара (D_3, L_5) относится к первому типу. Теорема доказана.

Лемма 5. *Для любого слабозамкнутого класса самодвойственных булевых функций верно точно одно из утверждений:*

1. Данный класс состоит только из α-функций и является замкнутым классом

2. Для каждой α-функции f из данного класса функция, равная отрицанию f, также принадлежит данному классу.

Доказательство. Каждая самодвойственная функция является либо α-функцией, либо δ-функцией.

Из леммы 2 следует, что если слабозамкнутый класс содержит некоторое множество α-функций, то оно содержит замыкание этого множества. И, если данный класс не содержит δ-функций, то выполняется утверждение 1.

Если данный класс содержит хотя бы одну δ-функцию, то в соответствующем множестве пар, состоящих из функции и задержки, кроме множества пар вида (f_α, t), первые проекции которых являются α-функциями, есть хотя бы одна пара (g, t_1), где g — δ-функция. Тогда отождествлением переменных в данном элементе можно получить пару $(x + 1, t_1)$, а после применения операции подстановки в неё элементов (f_α, t) можно получить множество элементов вида $(f_\alpha + 1, t + t_1)$, первой проекцией которого будет множество отрицаний всех α-функций, входящих в рассматриваемый слабозамкнуты класс. Следовательно, в этом случае выполняется утверждение 2.

Лемма доказана.

Теорема 2. *Слабозамкнутыми классами самодвойственных булевых функций являются классы Поста D_3, D_2, D_1, L_5, L_4, O_4, O_1, а также множество D_4, состоящее из всех функций, принадлежащих D_2, и функций, обратных к ним.*

Класс D_4 является положительно-слабозамкнутым.

Доказательство. По лемме 5 любой слабозамкнутый класс самодвойственных булевых функций является либо замкнутым классом α-функций, то есть совпадает с одним из классов D_2, D_1, L_4, O_1, либо распадается на две части: одна часть — замкнутый класс α-функций, вторая часть — множество отрицаний этих α-функций.

Если первая часть совпадает с D_1, то слабозамкнутый класс совпадает с D_3.

Если первая часть совпадает с L_4, то слабозамкнутый класс совпадает с L_5.

Если первая часть совпадает с O_1, то слабозамкнутый класс совпадает с O_4.

Если первая часть совпадает с D_2, то получаем слабозамкнутый класс D_4, состоящий из функций, принадлежащих D_2, и их отрицаний.

Если рассмотреть функции из D_2 со всевозможными четными задержками, а функции, являющиеся отрицаниями функций из D_2, со всевозможными нечетными, то при синхронном замыкании ничего нового не появится.

Следовательно, класс D_4 является положительно-слабозамкнутым классом. Теорема доказана.

Список литературы

[1] Кудрявцев В. Б., Блохина Г. Н., Кнап Ж., Кудрявцев В. В. Алгебра логики. — М.; Любляна, 2006.

О частотных языках на биграммах

Петюшко А. А. (Москва, МГУ им. М. В. Ломоносова)

petsan@newmail.ru

Пусть A ($|A| < \infty$) — конечный алфавит, а $L \subseteq A^*$ — некоторый язык над этим алфавитом.

По каждому слову α языка L можно построить матрицу биграмм $(n(\alpha))_{a,b\in A}$, такую что $n_{ab}(\alpha)$ — это число рядом рядом стоящих букв ab в слове α. В данной статье решается обратная задача — по матрице $n(\alpha)$ установить некоторые свойства языка $L(n(\alpha))$, то есть множества всех слов, имеющих матрицу биграмм $n(\alpha)$. Полученные языки $L(n(\alpha))$ удается классифицировать.

Пример. Пусть $A = \{0, 1\}$, $\alpha = 01011100$.

Тогда матрица биграмм $n(\alpha) = \begin{pmatrix} n_{00}(\alpha) & n_{01}(\alpha) \\ n_{10}(\alpha) & n_{11}(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$.

Рассмотрим сначала результат, касающийся регулярности языка, в котором заданы некоторые ограничения на какое-то подмножество элементов матрицы биграмм.

Теорема 1. *Пусть задан набор $k < \infty$ биграмм $\overline{\beta} = (\beta_1, \ldots, \beta_k)$, где $|\beta_i| = 2, i = 1 \ldots k$, а также набор отрезков $\overline{c} = ([c_1^1, c_2^1], \ldots, [c_1^k, c_2^k])$, где $c_1^i \leqslant c_2^i, c_j^i \in N \cup \{0\}, i = 1 \ldots k, j = 1 \ldots 2$. Тогда язык $L_{\overline{\beta},\overline{c}} = \{\alpha | \quad n_{\beta_i}(\alpha) \in [c_1^i, c_2^i], i = 1 \ldots k\}$ регулярен.*

Более интересный случай, когда мы рассматриваем матрицу биграмм не как абсолютное ограничение, а как задание относительных значений биграмм, то есть языка, в котором сохраняются отношения $n_{ab}(\alpha)/n_{cd}(\alpha) \quad \forall a, b, c, d \in A, n_{cd}(\alpha) > 0$. Для более детального рассмотрения нам потребуется ряд определений.

Определение. Назовем частотным языком на биграммах, заданным матрицей биграмм $n(\alpha)$, следующий язык при $k \in N$:

$$F_{\cup n(\alpha)} = \bigcup_{k=1}^{\infty} L(kn(\alpha)).$$

Построим по матрице $n(\alpha)$ ориентированный граф $G_{n(\alpha)}$ на плоскости. Вершинами у этого графа будут все буквы из алфавита A, при этом ребра будут соответствовать биграммам с учетом их кратностей,

то есть кратность $n_{ab}(\alpha)$ будет порождать $n_{ab}(\alpha)$ ориентированных ребер $a \to b$. Аналогично, кратность $n_{cc}(\alpha)$ будет порождать $n_{cc}(\alpha)$ петель $c \to c$.

Определение. Назовем ориентированный граф эйлеровым, если если выполняются следующие условия: 1) Все вершины, являющиеся начальной или конечной вершиной хотя бы одного ребра, лежат в одной компоненте связности соответствующего неориентированного графа; 2) У всех вершин количество входящих ребер равно количеству исходящих ребер.

Определение. Назовем ориентированный граф почти эйлеровым, если выполняются следующие условия: 1) Все вершины, являющиеся начальной или конечной вершиной хотя бы одного ребра, лежат в одной компоненте связности соответствующего неориентированного графа; 2) У всех вершин, кроме двух, количество входящих ребер равно количеству исходящих ребер. У оставшихся двух вершин разность количества входящих ребер и количества исходящих ребер равна $+1$ и -1 соответственно.

Как показано в [1], в эйлеровом графе существует эйлеров цикл (то есть такой цикл, который содержит все ребра, причем каждое — только один раз), а в почти эйлеровом — эйлеров путь, не являющийся эйлеровым циклом (то есть такой путь, который содержит все ребра, причем каждое — только один раз, и при этом начальная вершина не совпадает с конечной).

Теорема 2. *Пусть задана матрица биграмм $n(\alpha)$. Тогда:*
1) Если ориентированный граф $G_{n(\alpha)}$ является эйлеровым, то в частотном языке $F_{\cup n(\alpha)}$ счетное число слов;
2) Если ориентированный граф $G_{n(\alpha)}$ является почти эйлеровым, то в частотном языке $F_{\cup n(\alpha)}$ конечное ненулевое число слов, имеющих одинаковую длину;
3) Если ориентированный граф $G_{n(\alpha)}$ не является ни эйлеровым, ни почти эйлеровым, то в частотном языке $F_{\cup n(\alpha)}$ нет ни одного слова.

Очевидно, что если выполняются условия 2) или 3) Теоремы 2, то язык $F_{\cup n(\alpha)}$, в котором не более чем конечное число слов, будет регулярным. Поэтому интересен вопрос, когда он будет являться регулярным при условии 1).

Определение. Назовем две ненулевые матрицы n_1 и n_2 одинакового размера неколлинеарными, если не существует ненулевых действительных коэффициентов $c_1, c_2 \in R, (c_1, c_2) \neq (0, 0)$, таких, что верно $c_1 n_1 + c_2 n_2 = 0$.

Теорема 3. *Пусть $A, |A| < \infty$ — некоторый конечный алфавит. Далее, пусть задана матрица биграмм $n(\alpha)$ такая, что соответствующий ей ориентированный граф $G_{n(\alpha)}$ является эйлеровым. Тогда:*
1) Если существует такое разложение $n(\alpha)$ в сумму двух ненулевых неколлинеарных матриц $n(\alpha) = n(\alpha_1) + n(\alpha_2)$ такое, что обе матрицы $n(\alpha_1)$ и $n(\alpha_2)$ задают ориентированные графы $G_{n(\alpha_1)}$ и $G_{n(\alpha_2)}$, которые являются эйлеровыми, то язык $F_{\cup n(\alpha)}$ нерегулярен;
2) В противном случае язык $F_{\cup n(\alpha)}$ регулярен.

Однако данная теорема дает слишком общие условия на матрицу биграмм. Рассмотрим частный, но часто используемый на практике случай двухбуквенного алфавита.

Теорема 4. *Пусть $A = \{0, 1\}$. Далее, пусть задана матрица биграмм $n(\alpha)$ такая, что соответствующий ей ориентированный граф $G_{n(\alpha)}$ является эйлеровым. Тогда:*
1) Язык $F_{\cup n(\alpha)}$ нерегулярен, если $\exists i, i \in \{0, 1\}$ такое, что $n_{ii}(\alpha) > 0$, и при этом $\exists u \neq v, u, v \in \{0, 1\}$ такие, что $n_{uv}(\alpha) > 0$;
2) Язык $F_{\cup n(\alpha)}$ регулярен, если $\exists i, i \in \{0, 1\}$ такое, что $n_{ii}(\alpha) > 0$, и при этом $\forall u, v \in \{0, 1\}, (i, i) \neq (u, v)$ выполняется $n_{uv}(\alpha) = 0$;
3) Язык $F_{\cup n(\alpha)}$ регулярен при $n_{00}(\alpha) = n_{11}(\alpha) = 0$.

Отметим, что для доказательства двух последних теорем напрямую использовалась теорема Клини о представимости регулярных событий в автомате (см. [2]).

Автор выражает благодарность своему научному руководителю, д.ф.-м.н., профессору Бабину Д. Н., за постановку задачи и ценные указания.

Список литературы

[1] Оре О. Теория графов. — М.: Наука, 1980.

[2] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

О двух методах распознавания эквивалентности в алгебраических моделях программ

Подловченко Р. И. (Москва, НИВЦ МГУ им. М. В. Ломоносова)
Захаров В. А. (Москва, МГУ им. М. В. Ломоносова, ф-т ВМК)

rip@vvv.srcc.msu.su, zakh@cs.msu.su

Назначение данной статьи — обратить внимание на один из последних результатов в теории моделей последовательных программ. В ней даётся представление об алгебраических моделях программ, об основных проблемах их теории, условиях, в которых они рассматриваются, и концепциях, лежащих в основе двух практикуемых методов распознавания эквивалентности. Формулируются результаты, полученные этими методами и применимые в программировании.

Алгебраические модели программ введены в [4] как обобщение двух моделей последовательных программ — операторных схем Ляпунова-Янова [3, 6] и дискретных преобразователей Глушкова-Летичевского [1]. Объекты алгебраической модели именуются схемами программ. В теории алгебраических моделей программ основной является проблема эквивалентных преобразований (э.п.) в модели. Она заключается в построении системы э.п., полной в модели, то есть удовлетворяющей требованию: для любых двух эквивалентных схем из этой модели существует конечная цепочка э.п., принадлежащих системе и транслирующая одну из схем в другую. Проблема э.п. рассматривается только в моделях с разрешимой проблемой эквивалентности, то есть предполагается наличие алгоритма, который распознает эквивалентность схем в модели. Таким образом, на первое место в исследованиях выходит проблема эквивалентности в модели.

Алгебраические модели строятся над двумя конечными алфавитами — алфавитом Y операторных символов и алфавитом P логических переменных, принимающих значения 0 и 1. Все алгебраические модели программ имеют общим множество своих объектов — схем программ и отличаются друг от друга отношением эквивалентности между схемами. Эти отношения вводятся единообразно, определяя тем самым всё множество моделей. Существенной является

Теорема 1. *Проблемы эквивалентности и э.п. в любой алгебраической модели программ над Y, P сводятся к одноимённым проблемам в моделях матричных схем над Y, P.*

На основании этой теоремы обе проблемы рассматриваются в моделях матричных схем. Опишем их. Матричная схема над Y, P представляет собой конечный граф с двумя выделенными вершинами — входом без заходящих в него дуг и выходом без исходящих из него дуг; остальные вершины наделены метками из Y; из каждой вершины графа, кроме выхода, исходят дуги в количестве, равном числу наборов значений всех переменных из P (множество таких наборов обозначается X), и помечены различными наборами.

Матричные схемы выполняются на функциях, отображающих множество всех цепочек операторных символов из Y (они называются операторными цепочками) в множество X. Такие функции называются функциями разметки. Выполнение схемы на функции разметки заключается в обходе схемы, который начинается в ее входе с пустой операторной цепочкой и сопровождается приписыванием к текущей операторной цепочке символа, сопоставленного вершине при переходе через нее; при этом выход из вершины происходит по дуге, помеченной тем набором из X, который является значением функции разметки на полученной цепочке. Результатом выполнения схемы считается цепочка, полученная к моменту достижения выхода схемы; иначе результат не определен. Эквивалентность схем определяется выбором двух параметров: отношения эквивалентности ν в множестве операторных цепочек над Y и подмножества L допустимых функций разметки: требуется, чтобы на любой допустимой функции разметки результат выполнения на ней одной из схем был определён, если определён результат выполнения другой, и эти результаты были ν-эквивалентными. С введением такой эквивалентности получается (ν, L)-модель матричных схем над Y, P.

К настоящему времени предложены два метода разрешения эквивалентности в моделях матричных схем — один в [5] и другой в [2]. Оба метода рассматривают сочетаемые маршруты в схемах, сравниваемых на эквивалентность, то есть пути в схемах, начинающиеся в их входах и пролагаемые общей для них допустимой функцией разметки. В терминах сочетаемых маршрутов формулируется

критерий эквивалентности схем. Выделяется семейство упорядоченных моделей: в такой модели любая операторная цепочка не имеет ν-эквивалентных ей подцепочек, а допустимыми являются все функции разметки, сохраняющие своё значение на ν-эквивалентных операторных цепочках. Основанием этому является то, что в таких моделях сочетаемость маршрутов алгоритмически распознаваема, а в матричной схеме любой маршрут прокладывается некоторой допустимой функцией разметки.

Метод в [5] нацелен на распознавание эквивалентности, в процессе которого устанавливаются свойства структуры эквивалентных схем. Последнее необходимо для решения проблемы э.п. Концепция этого метода — осуществить проверку эквивалентности двух схем просмотром сочетаемых маршрутов в них, имеющих конечную длину, которая определяется размерами схем. Доказана

Теорема 2. *Проблема эквивалентности в уравновешенной модели с левым и правым сокращением разрешима за полиномиальное время относительно размеров сравниваемых схем; в такой модели решена и проблема э.п.*

Названные в теореме 2 модели — это частный вид упорядоченных моделей, в которых ν-эквивалентные цепочки равны по длине и сохраняют ν-эквивалентность при сокращении их на ν-эквивалентные префиксы (левая сократимость) и суффиксы (правая сократимость).

Альтернативный подход к построению эффективных алгоритмов решения задачи проверки эквивалентности схем программ предусматривает сведение этой задачи к проблеме пустоты для двухленточных односторонних детерминированных машин (2-DM) специального вида. Для проверки эквивалентности двух матричных схем π_1, π_2 в (ν, L)-модели необходимо построить 2-DM D_ν, описывающую отношение эквивалентности ν операторных цепочек, то есть распознающую все ν-эквивалентные пары операторных цепочек. Доказана

Теорема 3. *Отношение эквивалентности ν операторных цепочек может быть описано 2-DM тогда и только тогда, когда (ν, L)-модель является упорядоченной.*

Далее для пары схем π_1, π_2 и 2-DM D_ν, описывающей отношение эквивалентности ν операторных цепочек, строится комбинированная

2-DM $K(\pi_1, \pi_2, D_\nu)$, которая принимает в качестве входных данных, записанных на ее лентах, пары маршрутов в схемах π_1 и π_2. Устройство комбинированной 2-DM таково, что справедлива

Теорема 4. *Если 2-DM D_ν описывает эквивалентность ν операторных цепочек, то схемы π_1 и π_2 эквивалентны в (ν, L)-модели тогда и только тогда, когда комбинированная машина $K(\pi_1, \pi_2, D_\nu)$*
A: распознает пустое бинарное отношение и
B: в каждом бесконечном прогоне бесконечно часто считывает данные на обеих лентах.

Разрешимость проблемы пустоты для некоторых классов комбинированных машин $K(\pi_1, \pi_2, D_\nu)$ обеспечивает

Теорема 5. *Если эквивалентность ν операторных цепочек описывается 2-DM D_ν, имеющей конечное множество F допускающих состояний, и схемы π_1 и π_2 эквивалентны в (ν, L)-модели, то число состояний комбинированной машины $K(\pi_1, \pi_2, D_\nu)$, достижимых из ее начального состояния, ограничено величиной $2^{O(|F|(|\pi_1|+|\pi_2|))}$.*

Следствие 1. *Если отношение эквивалентности ν операторных цепочек разрешимо за полиномиальное время и описывается 2-DM D_ν, имеющей конечное множество F допускающих состояний, то проблема эквивалентности схем программ в (ν, L)-модели принадлежит классу сложности co-NP.*

Следствие 2. *Если отношение эквивалентности ν операторных цепочек описывается конечной 2-DM D_ν, то проблема эквивалентности схем программ в (ν, L)-модели принадлежит классу сложности NLOG.*

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» 2009–2013 г.г.

Список литературы

[1] Глушков В. М., Летичевский А. А. Теория дискретных преобразователей // Избранные вопросы алгебры и логики. — Новосибирск: Наука, 1973. — С. 5–39.

[2] Захаров В. А. Проверка эквивалентности программ при помощи двухленточных автоматов // Кибернетика и системный анализ. — 2010. № 4. — С. 39–48.

[3] Ляпунов А. А. О логических схемах программ // Проблемы кибернетики. — М.: Физматгиз, 1958. Вып. 1. — С. 46–74.

[4] Подловченко Р. И. Иерархия моделей программ // Программирование. — 1981. № 2. — С. 3–14.

[5] Подловченко Р. И. Об одной методике распознавания эквивалентности в алгебраических моделях программ // Программирование. — 2011. № 6.

[6] Янов Ю. И. О логических схемах алгоритмов // Проблемы кибернетики. — М.: Физматгиз, 1958. Вып. 1. — С. 75–127.

О проверке эквивалентности последовательных и рекурсивных программ на упорядоченных полугрупповых шкалах

Подымов В. В. (Москва, МГУ им. М. В. Ломоносова, ф-т ВМК)

valdus@yandex.ru

Проблема эквивалентности программ в широком смысле формулируется следующим образом: требуется выяснить, имеют ли заданные программы одинаковое поведение. В данной работе в качестве формализации понятия программы используется модель рекурсивных программ, предложенная в заметке [1] и обобщающая модель вычислений последовательных программ.

В работе [2] была предложена методика исследования проблемы эквивалентности линейных унарных рекурсивных программ, семантика которых описывается уравновешенными полугрупповыми шкалами. Цель данного исследования состоит в обобщении этой методики на более широкий класс семантик, описываемых упорядоченными полугрупповыми шкалами.

Считаем заданными конечный алфавит A базовых функций и конечный алфавит C базовых предикатов. Также задан счетно-бесконечный алфавит F заголовков функций, которые могут использоваться в программе. Слово в алфавите $A \cup F$ будем называть термом. Множество всех термов будем обозначать записью $Term$. Терм t будем называть базовым, если $t \in A^*$, и линейным, если он является базовым или представим в виде $t = t'ft''$, где t', t'' — базовые термы, $f \in F$.

Под унарной рекурсивной программой будем понимать систему $\pi = (F_\pi, D, T)$, где $F_\pi \subset F$ — конечное множество заголовков функций, определяемых в программе, $D : F_\pi \times C \to Term$ — описание функций, $T \in Term$ — запрос программы. Унарную рекурсивную программу будем называть линейной, если ее запрос и область значений функции D суть линейные термы. Линейную унарную рекурсивную программу далее будем называть просто программой.

Сложность $|\pi|$ программы $\pi = (F_\pi, D, T)$ определим следующим образом: $|\pi| = |T| + \sum_{f \in F_\pi, c \in C} |D(f, c)|$.

Семантика программы определяется моделью — системой $M = (S, s_0, R, \xi)$, где S — произвольное множество состояний данных, $s_0 \in S$ — начальное состояние, $R : S \times A \to S$ — функция преобразования данных, $\xi : S \to C$ — оценка истинности предикатов на состояниях данных. Наряду с функцией R будем использовать ее расширение R^* с множества A на множество базовых термов: $R^*(s, \lambda) = s$, $R^*(s, ah) = R^*(R(s, a), h)$. Вместо записи $R^*(s_0, h)$ для краткости будем использовать запись $[h]$.

Трассой программы $\pi = (T, F, D)$ будем называть конечную или бесконечную последовательность термов, начинающуюся с запроса программы и такую, что каждый следующий терм получается из предыдущего заменой входящего в него заголовка функции f на терм $D(f, c)$, где c — произвольный базовый предикат. Трассу программы π будем называть ее вычислением в модели $M = (S, s_0, R, \xi)$, если выполнены следующие условия:

1) если она конечна, то оканчивается базовым термом и
2) при замене терма $t'ft''$, $f \in F$, на терм $t'D(f, c)t''$ базовый предикат c определяется по правилу $c = \xi([t'])$.

В заданной модели M у заданной программы π существует ровно одно вычисление. Если вычисление является конечным, то его результатом объявляется состояние данных $[\mathrm{t}]$, отвечающее его последнему терму t. Две программы будем считать эквивалентными в модели M, если их вычисления в этой модели либо оба бесконечны, либо оба конечны и имеют одинаковый результат.

Под шкалой $\mathcal{F} = (S, s_0, R)$ будем понимать множество всех моделей вида $M = (S, s_0, R, \xi)$, где функция ξ произвольна. Программы π_1, π_2 будем считать эквивалентными на шкале $\mathcal{F}$ ($\pi_1 \sim_{\mathcal{F}} \pi_2$), если они эквивалентны в любой модели, определяемой этой шкалой. Шкалу также можно расматривать как ориентированный помеченный граф с выделенным корнем s_0.

Шкалу $\mathcal{F} = (S, s_0, R)$ будем называть полугрупповой, если множество состояний шкалы $[h]$ с операцией $[h_1][h_2] = [h_1h_2]$ образует полугруппу, и упорядоченной, если для любых базовых термов t', t'' верно неравенство $[t't''] \neq [t']$. Для краткости будем отождествлять

полугрупповую шкалу и описываемую ей полугруппу. Упорядоченную полугрупповую шкалу далее будем называть просто шкалой.

Введенные понятия позволяют поставить проблему эквивалентности программ следующим образом: для заданной шкалы $\mathcal{F}$ и заданной пары программ π_1, π_2 проверить выполнимость соотношения $\pi_1 \sim_{\mathcal{F}} \pi_2$.

Будем говорить, что программа $\pi = (F_\pi, D, T)$ представлена в нормальной форме, если $T = f \in F_\pi$, для всех $c \in C$, $f \in F_\pi$ терм $D(f, c)$ либо базовый, либо представим в виде aft, $a \in A$, $f \in F_\pi$, $t \in A^*$, в F_π выделен специальный символ f_{inf} такой, что $D(f_{inf}, c) = af_{inf}$ и все символы F_π, кроме f_{inf}, можно последовательностью замен f на $D(f, c)$ привести к базовым термам. В [2] было показано, что любая программа может быть приведена к нормальной форме за полиномиальное время и с возрастанием сложности программы не более чем в полиномиальное число раз. Поэтому в дальнейшем считаем, что программы уже приведены к нормальной форме.

Четверку $K = (W, U, w^+, w^*)$, где W — конечно порожденный моноид с операцией $*$ и нейтральным элементом e, U — его подмоноид и $w^+, w^* \in W$, будем называть критериальной системой для шкалы $\mathcal{F}$, если

- существует гомоморфизм $\varphi : \mathcal{F} \times \mathcal{F} \to U$ такой, что $w^+ * \varphi(s_1, s_2) * w^* = e \Leftrightarrow s_1 = s_2$,
- уравнение $X * w = e$, где $w \in U * w^*$, имеет не более одного решения относительно X и
- уравнение $w * X = e$, где $w \in w^+ * U$, имеет не более одного решения относительно X.

Пусть теперь заданы программы π_1, π_2, шкала $\mathcal{F}$ и критериальная система K для этой шкалы. Опишем граф совместных вычислений G_{π_1,π_2} программ π_1, π_2.

Вершинами графа являются четверки вида $(G_1, G_2, w, \hat{w})$, где $G_i \in F_{pi_i} \cup \{\lambda\}$, $w \in w^+ * U$, $\hat{w} \in U * w^*$. Произвольной паре термов вида $T_1 = t'_1 f_1 t''_1$, $T_2 = t'_2 f_2 t''_2$, где $t'_i, t''_i \in A^*$, $f_i \in F_{\pi_i} \cup \{\lambda\}$ (если $f_i = \lambda$, то $t''_i = \lambda$), соответствует вершина графа $V_{T_1,T_2} = (f_1, f_2, w^+ * \varphi([t'_1], [t'_2]), \varphi([t''_1], [t''_2]) * w^*)$.

Пусть $Tr_1 = Tr'_1T_1T'_1$, $Tr_2 = Tr'_2T_2T'_2$, где $T_i, T'_i \in Term$ — произвольные трассы программ π_1, π_2, реализуемые в некоторой общей модели (терм T'_i отсутствует, если терм T_i базовый), причем если $T_i = t'_i f_i t''_i$, то $c_i = \xi([t'_i])$. Дуги графа G_{π_1,π_2} описываются четырьмя случаями. Если состояния $[t'_1]$, $[t'_2]$ совпадают или не достижимы друг из друга, то из вершины V_{T_1,T_2} в вершину $V_{T'_1,T'_2}$ исходит дуга, несущая метку (c_1, c_2). Если терм T_1 базовый или состояние $[t'_1]$ достижимо из состояния $[t'_2]$, то из вершины V_{T_1,T_2} в вершину V_{T_1,T'_2} исходит дуга, несущая метку (ε, c_2). Если терм T_2 базовый или состояние $[t'_2]$ достижимо из состояния $[t'_1]$, то из вершины V_{T_1,T_2} в вершину $V_{T'_1,T_2}$ исходит дуга, несущая метку (c_1, ε). Во всех остальных случаях из вершины V_{T_1,T_2} не исходит никаких дуг.

Корнем графа объявляется вершина (f_1, f_2, w^+, w^*), где f_i — запрос программы π_i. Для простоты формулировок далее считаем, что граф G_{π_1,π_2} содержит только вершины, достижимые из корня.

В графе G_{π_1,π_2} особо выделяются опровергающие вершины и опровергающие циклы. Опровергающая вершина — вершина вида $(\lambda, \lambda, w, \hat{w})$, где $w * \hat{w} \neq e$. Опровергающий цикл — цикл, третьи компоненты всех вершин которого лежат в одном из множеств $U_\prec$, $U_\succ$, где $U_\prec = \{w^+ * \varphi(s_1, s_2) | s_1 \prec s_2\}$, $U_\succ = \{w^+ * \varphi(s_1, s_2) | s_2 \prec s_1\}$ (здесь запись $s' \prec s''$ означает, что состояние s'' достижимо из состояния s' на шкале $\mathcal{F}$).

Теорема 1. *$\pi_1 \sim_{\mathcal{F}} \pi_2$ тогда и только тогда, когда в графе G_{π_1,π_2} нет опровергающих вершин и опровергающих циклов.*

Теорема 2. *Если шкала $\mathcal{F}$ имеет критериальную систему K, то $\pi_1 \sim_{\mathcal{F}} \pi_2$ тогда и только тогда, когда граф G_{π_1,π_2} не содержит опровергающих вершин и опровергающих циклов и его размер ограничен величиной $2^{O(n)}$, где $n = |\pi_1| + |\pi_2|$.*

Теорема 3. *Если шкала $\mathcal{F}$ имеет критериальную систему $K = (W, U, w^+, w^*)$, моноид W является группой и проблемы достижимости состояний шкалы и равенства элементов моноида полиномиально разрешимы, то и проблема эквивалентности $\pi_1 \sim_{\mathcal{F}} \pi_2$ разрешима.*

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» 2009–2013 гг.

Список литературы

[1] De Bakker J. W., Scott D. A. Theory of programs. Unpublished notes. — Vienna: IBM Seminar, 1969.

[2] Захаров В. А. Об эффективной разрешимости проблемы эквивалентности линейных унарных рекурсивных программ // Математические вопросы кибернетики. — М.: Наука, 1999. Вып. 8. — С. 255–273.

Алгебраическая характеризация языков, допустимых в отмеченных графах

Пряничникова Е. А. (Донецк, Государственный университет информатики и искусственного интеллекта)

Pryanichnikovae@gmail.com

В теории конечных автоматов одним из важнейших результатов является теорема Клини, в которой утверждается, что класс языков, распознаваемых конечными автоматами, совпадает с классом рациональных языков, представимых регулярными выражениями алгебры Клини [1]. Основная цель данной работы — доказать аналогичную теорему для более широкого класса отмеченных графов и алгебр.

Графом с отмеченными дугами (конечным автоматом) назовем четверку $G = (Q, E, X, \mu)$, где Q — конечное множество вершин; $E \subseteq Q \times Q$ — множество дуг; X — конечное множество отметок дуг; $\mu : E \to X$ — функция отметок дуг.

Графом с отмеченными вершинами назовем четверку $G = (Q, E, X, \mu)$, где Q — конечное множество вершин, $E \subseteq Q \times Q$ — множество дуг; X — конечное множество отметок вершин; $\mu : Q \to X$ — функция отметок вершин.

Полностью отмеченным графом назовем четверку $G = (Q, E, X, \mu)$, где Q — конечное множество вершин, $|Q| = n$; $E \subseteq Q \times Q$ — множество дуг; X — конечное множество отметок; $\mu : Q \cup E \to X$ — функция отметок вершин и дуг.

Путем в графе будем называть конечную последовательность вершин $l = q_1 q_2 \dots q_k$, где $(q_i, q_{i+1}) = e_i \in E$. Вершину q_1 будем называть начальной вершиной пути l, вершину q_k — конечной вершиной пути.

Отметкой пути $l = q_1 q_2 \dots q_k$ в графе с отмеченными дугами будем называть последовательность отметок входящих в этот путь дуг $\mu(e_1)\mu(e_2)\dots\mu(e_{k-1})$. Отметкой пути $l = q_1 q_2 \dots q_k$ в графе с отмеченными вершинами будем называть последовательность отметок вершин $\mu(q_1)\mu(q_2)\dots\mu(q_k)$. Отметкой пути $l = q_1 q_2 \dots q_k$ в полностью отмеченном графе будем называть чередующуюся последовательность отметок вершин и дуг $\mu(q_1)\mu(e_1)\mu(q_2)\mu(e_2)\dots\mu(q_k)$.

Пусть $I \subseteq Q$ — множество начальных вершин графа, $F \subseteq Q$ — множество финальных вершин. Отметки всех путей в отмеченном графе G, начальные вершины которых принадлежат множеству I, а конечные — множеству F, назовем языком, допускаемым графом G, и обозначим $L(G)$.

Пусть X — конечный алфавит; X^* — множество всех слов конечной длины в алфавите X; X^n — множество всех слов длины n в алфавите X; $X^{\geqslant n}$ — множество всех слов конечной длины в алфавите X, длина которых больше или равна n.

Определим на множестве X^* частичную бинарную операцию $\overset{n}{\circ}$ склеивания двух слов с параметром n следующим образом: для всех $w_1, w_2 \in X^*$

$$w_1 \overset{n}{\circ} w_2 = \begin{cases} xyz, & \text{если } w_1 = xy,\ w_2 = yz,\ y \in X^n; \\ \text{не определено} & \text{в противном случае.} \end{cases}$$

Операция $\overset{n}{\circ}$ ассоциативна при любом n, то есть $(2^{X^*}, \overset{n}{\circ})$ и $(2^{X^{\geqslant n}}, \overset{n}{\circ})$ — полугруппы.

Нейтральный элемент по операции $\overset{n}{\circ}$ существует тогда и только тогда, когда она определена на множестве языков, в которых нет слов, длина которых меньше n. Если нейтральный элемент существует, то он равен X^n. Таким образом, полугруппа $(2^{X^*}, \overset{n}{\circ})$ является моноидом только при $n = 0$.

Введем на языках $L, R \subseteq X^*$ следующие операции:

1) $L \cup R = \{w : w \in L \text{ или } w \in R\}$;

2) $L \overset{n}{\circ} R = \{w_1 \overset{n}{\circ} w_2 : w_1 \in L \text{ и } w_2 \in R\}$;

3) $L^{\overset{n}{+}} = \bigcup\limits_{i=1}^{\infty} L^i$, где $L^1 = L$; $L^{i+1} = L^i \overset{n}{\circ} L$ для всех $i \geqslant 1$.

Для характеризации языков, представимых в отмеченных графах, рассмотрим алгебры $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$ и $(2^{X^{\geqslant n}}, \overset{n}{\circ}, \cup, \overset{n}{*}, X^n, \varnothing)$.

Все алгебры $(2^{X^{\geqslant n}}, \overset{n}{\circ}, \cup, \overset{n}{*}, X^n, \varnothing)$ являются полукольцами.

Алгебра $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$ будет иметь единицу по операции $\overset{n}{\circ}$ только в случае, когда $n = 0$ и операция $\overset{n}{\circ}$ совпадает с конкатенацией, а рассматриваемая алгебра является алгеброй регулярных языков. Во всех остальных случаях эти алгебры не будут полукольцами.

Регулярные выражения в алгебре $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$ определим следующим образом:

1) $\varnothing$ является регулярным выражением и представляет язык $L(\varnothing) = \varnothing$;
2) x является регулярным выражением и представляет язык $L(x) = \{x\}$ для всех $x \in \bigcup\limits_{0 \leqslant i \leqslant n+1} X^i$;
3) Если R и Q — регулярные выражения, представляющие языки $L(R)$ и $L(Q)$ соответственно, то выражения $(R \overset{n}{\circ} Q)$, $(R \cup Q)$, $(R^{\overset{n}{+}})$ также являются регулярными, причем $L(R \overset{n}{\circ} Q) = L(R) \overset{n}{\circ} L(Q)$, $L(R \cup Q) = L(R) \cup L(Q)$, $L(R^{\overset{n}{+}}) = (L(R))^{\overset{n}{+}}$.

Теорема 1. *Язык $L \subseteq X^*$ допустим в графе с отмеченными дугами, графе с отмеченными вершинами и полностью отмеченном графе тогда и только тогда, когда он описывается регулярным выражением любой алгебры из семейства $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$.*

Эта теорема в некотором смысле аналогична широко известной теореме Клини для конечных автоматов. В случае, когда $n = 0$ и рассматриваются только графы с отмеченными дугами, теорема 1 совпадает с теоремой Клини.

На основе доказательства теоремы разработаны методы анализа и синтеза языков, представимых в отмеченных графах.

Поскольку для описания одного и того же класса графов можно использовать различные алгебры, представляет интерес вопрос о связи таких алгебр между собой.

Теорема 2. *Для двух алгебр $(2^{X^*}, \overset{n_1}{\circ}, \cup, \overset{n_1}{+}, \varnothing)$ и $(2^{X^*}, \overset{n_2}{\circ}, \cup, \overset{n_2}{+}, \varnothing)$ в случае, когда $n_1 < n_2$, существует такое отображение $\varphi : 2^{X^*} \to 2^{X^*}$, которое является гомоморфизмом. Если $n_2 > n_1$, то гомоморфизма нет.*

Рассматриваемое в теореме отображение является инъекцией, поэтому в случае, когда $n_1 < n_2$, алгебра $(2^{X^*}, \overset{n_1}{\circ}, \cup, \overset{n_1}{+}, \varnothing)$ изоморфно вложима в алгебру $(2^{X^*}, \overset{n_2}{\circ}, \cup, \overset{n_2}{+}, \varnothing)$, причем образ φ является подалгеброй $(2^{X^*}, \overset{n_2}{\circ}, \cup, \overset{n_2}{+}, \varnothing)$, а значит, все рассматриваемые алгебры вхо-

дят в одно квазимногообразие, в которое входит алгебра регулярных языков.

Теорема 3. *Пусть* $\Re(n)$ *— множество всех регулярных выражений алгебры* $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$. *Если* $n_1 < n_2$, *то существует такое отображение* $\psi : \Re(n_1) \to \Re(n_2)$, *которое сохраняет язык регулярного выражения, то есть, если* r *— это регулярное выражение алгебры* $(2^{X^*}, \overset{n_1}{\circ}, \cup, \overset{n_1}{+}, \varnothing)$, $L(r)$ *— язык, представляемый этим регулярным выражением, то* $\psi(r)$ *— это регулярное выражение алгебры* $(2^{X^*}, \overset{n_2}{\circ}, \cup, \overset{n_2}{+}, \varnothing)$ *и* $L(\psi(r)) = L(r)$.

В данной работе рассматриваются языки, допустимые в отмеченных графах: графах с отмеченными дугами, графах с отмеченными вершинами и графах, в которых отмечены и дуги, и вершины. Найдена алгебраическая характеризация таких языков, разработаны методы их анализа и синтеза. Исследованы основные свойства семейства алгебр языков, допустимых в отмеченных графах.

Список литературы

[1] Anderson J. Automata Theory with Modern Applications. — Cambridge: Cambridge University Press, 2006.

[2] Капитонова Ю. В., Летичевский А. А. Математическая теория проектирования вычислительных систем. — М.: Наука, 1988.

Базисы в P-множествах

Родин А. А. (Москва, МГУ им. М. В. Ломоносова)

tyman307@rambler.ru

В работе рассматриваются предполные классы, содержащие все о.-д. функции, в каждом состоянии которых реализуется функция из некоторого замкнутого класса D алгебры-логики (P-множества). Рассматривается задача о существовании базиса в различных P-множествах.

Введение

Через P^2 обозначим множество всех ограниченно-детерминированных функций (автоматных отображений), входные и выходные переменные которых принимают значения из множества бесконечных последовательностей, составленных из нулей и единиц. Будем считать, что на множестве P^2 определена операция суперпозиции[1].

Пусть D — произвольный замкнутый класс Поста [2]. Введем понятие P-множества, порожденного классом D, — это множество всех ограниченно-детерминированных (о.-д.) функций, в каждом состоянии которых реализуется функция алгебры-логики, принадлежащая D. Будем обозначать такое множество через P_D. Очевидно, P-множество можно рассматривать, как самостоятельную функциональную систему, и тогда возникает ряд стандартных для функциональных систем задач. В [1] показано, что в P^2 существует полная система, не содержащая базиса, вместе с тем, в P^2 можно выделить базис. С этой точки зрения интерес представляет аналогичная задача для функциональной системы P_D, порожденной произвольным множеством D.

Целью данной работы является доказательство следующих утверждений.

Теорема 1. *Пусть $0, 1, x \in D$. Тогда в P_D существует полная система, не содержащая базиса.*

Теорема 2. *Пусть $0, 1, x \in D$. Тогда в P_D существует базис.*

Теорема 3. *Пусть порождающее множество D содержит тождественную функцию а.-л. и функцию отрицания. Тогда в P_D существует полная система, из которой нельзя выделить базис.*

Теорема 4. *Пусть порождающее множество D содержит тождественную функцию а.-л. и функцию отрицания. Тогда в P_D существует базис.*

Доказательство теоремы 1

Пусть $\rho = \{\rho_1, \ldots, \rho_d\}$ — множество функций а.-л., которое является базисом в D. Согласно [3], такой базис всегда существует. Обозначим через $R = \{R_1, \ldots, R_d\}$ множество о.-д. функций с одним состоянием, таких, что в состоянии функции R_i реализуется функция а.-л. ρ_i. Очевидно, что тождественные 0 и 1 принадлежат замыканию R.

Зафиксируем произвольное натуральное число m и рассмотрим произвольные 2^m о.-д. функций. Пусть в совокупности они зависят от переменных $x_1, \ldots, x_n$. Каждой функции можно взаимнооднозначно сопоставить двоичный набор длины m. То есть в качестве номера функции будем рассматривать значение этого набора. Обозначим эти о.-д. функции через $f_{00..0}, \ldots, f_{11..1}$.

Рассмотрим схему, изображенную на рис. 1, которая реализует некоторую о.-д. функцию $h(x_1, \ldots, x_n, y_1, \ldots, y_m, z)$. В блоках, обозначенных $F_{00..0}, \ldots, F_{11..1}$, реализуются о.-д. функции $f_{00..0}, \ldots, f_{11..1}$ соответственно. В блоке M_α, где α — двоичный набор длины m, реализуется такая о.-д. функция, что ее значение в первый момент времени равно 1 тогда и только тогда, когда двоичный набор значений входных переменных в первый момент времени равен α, то есть $(y_1(1), \ldots, y_m(1)) = \alpha$. Выход функции в блоке M_α в остальные моменты времени всегда равен 0. Блок M_x реализует о.-д. функцию от одной переменной, которая пропускает значение переменной в первый момент времени и выдает 0 во все последующие моменты. В блоках, обозначенных $\vee$, реализуется дизъюнкция, в блоках $\&$ — конъюнкция, в блоках G_0 — нулевая задержка.

Пусть в первый момент времени набор входных переменных $(y_1(1), \ldots, y_m(1))$ принимает значение α. Это означает, что на выхо-

де блока M_α реализуется единица в первый момент времени, а выход всех остальных блоков $M_\beta, \beta \neq \alpha$ равен нулю в первый момент. Следовательно, в первый момент времени на выходе схемы появляется значение $z(1)$, а в остальные моменты на входы последней дизъюнкции подается только одно значение, отличное от тождественного нуля, это значение функции f_α. Таким образом, начиная со второго момента времени, функция h «работает» как одна из функций $f_{00..0}, \ldots, f_{11..1}$. Какая конкретно функция получится, зависит от значений переменных $y_1, \ldots, y_m$ в первый момент времени.

Проверим, что $h \in P_D$. Для это нужно рассмотреть функции а.-л., которые реализуются в состояниях h. В первый момент реализуется z — тождественная функция а.-л. Во все остальные моменты реализуется функция а.-л., которая также реализуется в одном из состояний о.-д. функции f_α, которая принадлежит P_D. Следовательно, h также принадлежит P_D.

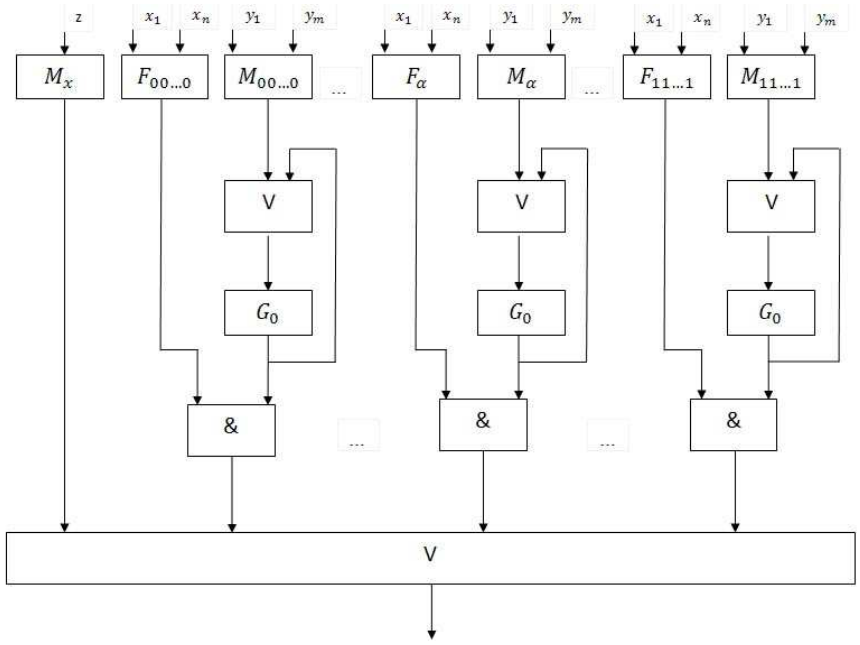


Рис. 1.

Покажем, что $f_{00..0}, \ldots, f_{11..1} \in [h \cup R]$. Рассмотрим произвольную функцию f_α. Пусть в начальном состоянии f_α реализуется функция а.-л. $a(x_1, \ldots, x_n)$. Пусть $A(x_1, \ldots, x_n)$ — истинностная о.-д. функция, в состоянии которой реализуется a. Пусть C_i — тождественный ноль, если i-й разряд набора α равен 0, и C_i — тождественная единица в противном случае, $i \in \{1, \ldots, m\}$. Очевидно, $A, C_i \in R$. Рассмотрим суперпозицию

$$h(x_1, \ldots, x_n, C_1, \ldots, C_m, A(x_1, \ldots, x_n)).$$

Из определения функции h следует, что выход такой суперпозиции совпадает с выходом f_α в любой момент времени. Функцию h будем называть генератором для функций $f_{00..0}, \ldots, f_{11..1}$.

Перенумеруем некоторым образом все функции из $P_D \setminus R$. Это можно сделать, поскольку P_D содержит счетное число функций. Построим нумерацию таким образом, чтобы для любого натурального $m > 0$ функция с номером $2^m + 1$ являлась генератором для всех функций с номерами, не превосходящими 2^m. Будем обозначать функцию с номером $2^m + 1$ через h_m. Рассмотрим бесконечную систему функций

$$N = R \bigcup_{i \geqslant 1} \{h_i\}.$$

Очевидно, система N полна. Предположим, из нее можно выделить базис. Функции из R обязательно должны присутствовать в базисе, поскольку все функции h_m пропускают значение переменной z в первый момент времени. Поскольку базис не может быть конечным, в нем присутствуют хотя бы две функции $h_i, h_j, i < j$. Но, по построению, $h_i \in [R \cup h_j]$. Следовательно, функцию h_i можно исключить из базиса без потери свойства полноты. Следовательно, это не базис. Теорема доказана.

Доказательство теоремы 2

В [1] (С. 175–178) приведен пример базиса в P относительно суперпозиции. Покажем, что конструкция, описанная там, с некоторыми модификациями переносится и на рассматриваемый случай. Для этого нам понадобится понятие F-свойства, введенное в [4].

Пусть $f(x_1, \ldots, x_n)$ — о.-д. функции из P_D. Будем считать, что переменная x_i функции f обладает F-свойством на сверхслове γ, если существуют момент времени t_0 такой, что для любых сверхслов $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n$ значение

$$b = f(b_1, \ldots, b_{i-1}, \gamma, b_{i+1}, \ldots, b_n)$$

таково, что $\gamma(t) = b(t)$ для любого $t > t_0$.

Иначе говоря, если подать сверхслово γ на i-й вход функции f, она постепенно превратится в проводник и будет пропускать переменную x_i.

Введенное понятие позволяет кодировать автомат с помощью ключа, которым является бесконечная последовательность (сверхслово). Периодическое сверхслово можно рассматривать как константную о.-д. функцию. Очевидно, что все константные функции принадлежат P_D, поскольку в каждом состоянии константной о.-д. функции реализуется либо 0, либо 1, и $0, 1 \in D$.

Лемма 1. *Пусть $f(x_1, \ldots, x_n)$ — о.-д. функция из P_D, γ — сверхслово. Существует о.-д. функция $f(x_1, \ldots, x_n, z) \in P_D$ такая, что выполнены следующие условия:*

1) $f'(x_1, \ldots, x_n, \gamma) = f(x_1, \ldots, x_n)$;

2) Переменная z функции h обладает F-свойстом на любой последовательности, отличной от γ.

Рассмотрим следующую схему, реализующую f'. Здесь символом ρ отмечена подсхема, реализующая истинностную о.-д. функцию, в состояниях которой реализуется функция а.-л. $\rho(x_1, x_2) = x_1x_2 \vee \bar{x_1}\bar{x_2}$, символом & обозначена конъюнкция, а символом v функция $v(x_1, x_2, x_3) = x_1x_3 \vee x_2\bar{x_3}$, G_1 — единичная задержка, γ — константная о.-д. функция, реализующая бесконечную последовательность γ.

До тех пор, пока на вход z поступает последовательность γ, на третий вход блока v будет поступать 1, и на выходе системы будет реализовываться значение функции f. Таким образом, первое условие выполнено.

Пусть на вход z подается последовательность γ', отличная от $\gamma, \gamma'(t_0) \neq \gamma(t_0)$. Тогда на третий вход блока v будет поступать значение 0 в любой момент времени, больший t_0. Отсюда следует, что на

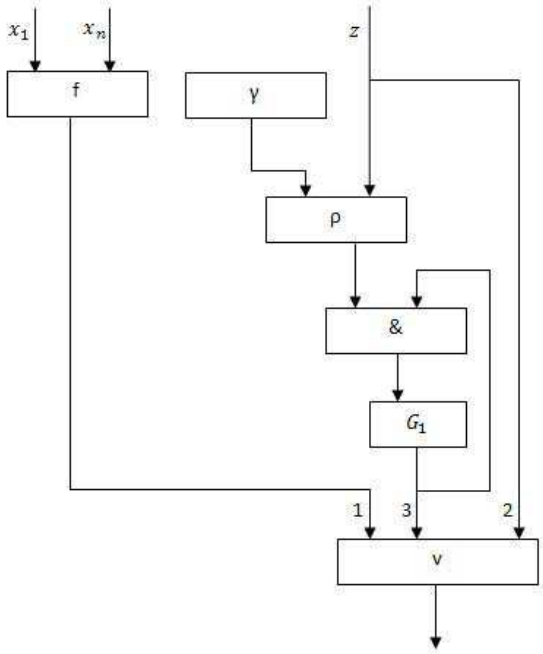


Рис. 2.

выходе схемы будет реализовываться последовательность, отличная от γ' лишь в конечном числе разрядов, что означает справедливость второго условия.

Осталось проверить, что функция f', построенная таким образом, принадлежит P_D. Действительно, если на третий вход блока v поступает значение 1, то на выход функции f' поступает значение f в этот момент времени. Функция а.-л., реализуемая в состоянии функции f, принадлежит D, поскольку $f \in P_D$. Если на третий вход блока v поступает значение 0, то функция f' находится в состоянии, в котором реализуется либо 0, либо 1. То есть, у функции f' достижимы только те состояния, в которых реализуются функции из D. Лемма доказана.

Будем писать $h = K(f, \gamma)$, если h кодирует f с помощью ключа γ.

Для построения базиса рассмотрим систему $N = R \cup \{h_1, h_2 \ldots\}$, описанную в доказательстве теоремы 1. Обозначим через Z_i замыкание множества $R \cup \{h_i\}, i > 0$, через Z_0 обозначим $[R]$.

Пусть Z — конечное множество о.-д. функций. Выберем из этого множества о.-д. функцию, имеющую наибольшее число состояний и обозначим это число через $n(Z)$. Пусть H_n — множество всех периодических последовательностей, у которых длины периодов образуют множество чисел, представимых в виде $p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}$, где все $p_j, j = 1, \ldots, m$ — простые числа, не превосходящие n. Рассмотрим цепочку вложенных множеств

$$Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \ldots$$

Несложно видеть, что из этой цепочки можно выделить бесконечную подцепочку

$$Z_0 \subseteq Z_{i_1} \subseteq Z_{i_2} \subseteq \ldots$$

такую, что для любого натурального j во множестве $Z_{i_j} \setminus Z_{i_{j-1}}$ содержится хотя бы одна константная о.-д. функция C_{i_j}, период которой является простым числом, превосходящим $n(Z_{i_{j-1}})$.

Очевидно, что система $N' = R \cup \{h_{i_1}, h_{i_2} \ldots\}$ также полна. Рассмотрим систему

$$N'' = R \cup \{K(h_{i_1}, C_0), K(h_{i_2}, C_{i_1}), \ldots, K(h_{i_{j+1}}, C_{i_j}) \ldots\},$$

где C_0 — тождественный ноль. Она также полна, поскольку через нее выразима система N'. Покажем, что N'' является базисом. Никакую функцию из R нельзя исключить без потери свойства полноты, поскольку все функции, не принадлежащие R пропускают значение одной из входных переменных в первый момент времени. Рассмотрим множество

$$N''_j = R \cup \{K(h_{i_1}, C_0), K(h_{i_2}, C_{i_1}), \ldots, K(h_{i_j}, C_{i_{j-1}})\}.$$

По построению, оно сохраняет множество бесконечных последовательностей $H_{n(Z_j)}$ [1]. С другой стороны, любая функция $K(h_{i_{k+1}}, C_{i_k}), k > j$ также сохраняет $H_{n(Z_j)}$. Поэтому $N'' \backslash K(h_{i_{j+1}}, C_{i_j})$ неполна для любого j. Следовательно, N'' является базисом. Теорема доказана.

Доказательство теоремы 3

Пусть $\rho = \{\rho_1, \ldots, \rho_d\}$ — множество функций а.-л., которое является базисом в D. Обозначим через $R = \{R_1, \ldots, R_d\}$ множество о.-д. функций с одним состоянием, таких, что в состоянии функции R_i реализуется функция а.-л. ρ_i. Очевидно, что тождественное отрицание принадлежат замыканию R.

Зафиксируем произвольное натуральное число m и рассмотрим произвольные 2^m о.-д. функций. Пусть в совокупности они зависят от переменных $x_1, \ldots, x_n$. Каждой функции можно взаимнооднозначно сопоставить двоичный набор длины m. То есть в качестве номера функции будем рассматривать значение этого набора. Обозначим эти о.-д. функции через $f_{00..0}, \ldots, f_{11..1}$.

Рассмотрим схему, изображенную на рис. 3, которая реализует некоторую о.-д. функцию $h(x_1, \ldots, x_n, y_1, \ldots, y_{2m}, z)$. В блоках, обозначенных $F_{00..0}, \ldots, F_{11..1}$, реализуются о.-д. функции $f_{00..0}, \ldots, f_{11..1}$ соответственно. В блоке M_α, где $\alpha = (\alpha_1, \ldots, \alpha_m)$ — двоичный набор длины m, реализуется такая о.-д. функция, что ее значение в первый момент времени равно 1 тогда и только тогда, когда двоичный набор значений входных переменных в первый момент времени удовлетворяет следующим условиям:

$$y_1(1) + y_2(1) = \alpha_1, \ldots, y_{2m-1}(1) + y_{2m}(1) = \alpha_m.$$

Выход функции в блоке M_α в остальные моменты времени всегда равен 0. Блок M_x реализует о.-д. функцию от одной переменной, которая пропускает значение переменной в первый момент времени и выдает 0 во все последующие моменты. В блоках, обозначенных $\vee$, реализуется дизъюнкция, в блоках $\&$ — конъюнкция, в блоках G_0 — нулевая задержка.

Пусть в первый момент времени двоичный набор $(y_1(1) + y_2(1), \ldots, y_{2m-1}(1) + y_{2m}(1))$ принимает значение α. Это означает, что на выходе блока M_α реализуется единица в первый момент времени, а выход всех остальных блоков $M_\beta, \beta \neq \alpha$ равен нулю в первый момент. Следовательно, в первый момент времени на выходе схемы появляется значение $z(1)$, а в остальные моменты на входы последней дизъюнкции подается только одно значение, отличное от тожде-

ственного нуля, это значение функции f_α. Таким образом, начиная со второго момента времени, функция h моделирует одну из функций $f_{00..0}, \ldots, f_{11..1}$. Какая конкретно функция получится, зависит от значений переменных $y_1, \ldots, y_{2m}$ в первый момент времени.

Проверим, что $h \in P_D$. Для это нужно рассмотреть функции а.-л., которые реализуются в состояниях h. В первый момент реализуется z — тождественная функция а.-л. Во все остальные моменты реализуется функция а.-л., которая также реализуется в одном из состояний о.-д. функции f_α, которая принадлежит P_D. Следовательно, h также принадлежит P_D.

Покажем, что $f_{00..0}, \ldots, f_{11..1} \in [h \cup R]$. Рассмотрим произвольную функцию f_α. Пусть в начальном состоянии f_α реализуется функция а.-л. $a(x_1, \ldots, x_n)$. Пусть $A(x_1, \ldots, x_n)$ — истинностная о.-д. функция, в состоянии которой реализуется a. Пусть о.-д. функции $\varphi_1(x), \ldots, \varphi_{2m}(x)$ определяются следующим образом: $\varphi_{2i-1}(x) = \varphi_{2i}(x) = x$, если i-й разряд набора α равен 0, и $\varphi_{2i-1}(x) = x$, $\varphi_{2i}(x) = \overline{x}$, если i-й разряд набора α равен 0, $i \in \{1, \ldots, m\}$. Очевидно, $A, h_j \in R$. Рассмотрим суперпозицию

$$h(x_1, \ldots, x_n, \varphi_1(x), \ldots, \varphi_{2m}(x), A(x_1, \ldots, x_n)).$$

Из определения функции h следует, что выход такой суперпозиции совпадает с выходом f_α в любой момент времени. Функцию h будем называть генератором для функций $f_{00..0}, \ldots, f_{11..1}$.

Обозначим через S_n множество всех о.-д. функций из P_D, зависящих не более чем от n переменных и имеющих при этом не более n состояний. Количество таких функций конечно, поэтому для каждого множества S_n можно построить генератор h_n.

Рассмотрим бесконечную систему функций

$$N = R \bigcup_{i \geqslant 1} \{h_i\}.$$

Очевидно, система N полна. Предположим, из нее можно выделить базис. Функции из R обязательно должны присутствовать в базисе, поскольку все функции h_m пропускают значение переменной z в первый момент времени. Поскольку базис не может быть конечным,

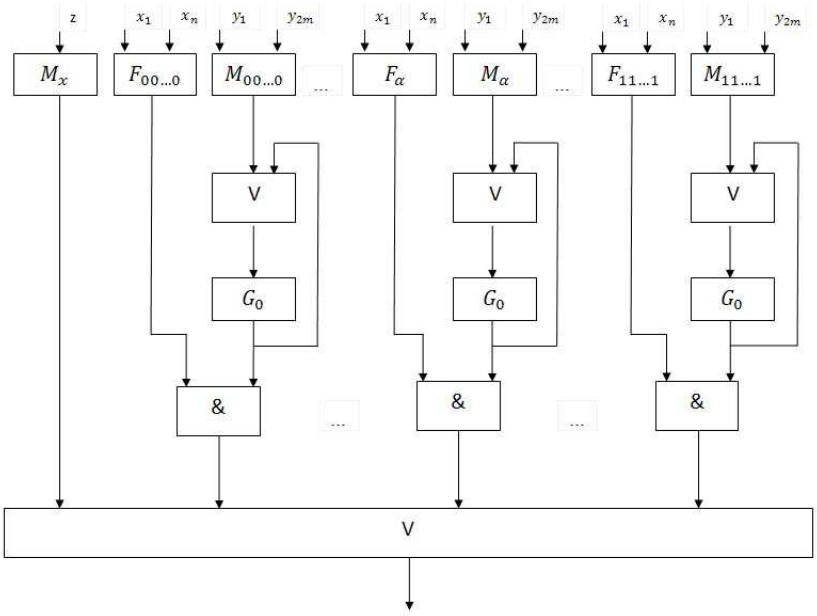


Рис. 3.

в нем присутствуют хотя бы две функции h_i, h_j такие, что j превосходит и количество переменных, и количество состояний функции h_i. Тогда, по построению, $h_i \in [R \cup h_j]$. Следовательно, функцию h_i можно исключить из базиса без потери свойства полноты. Следовательно, это не базис. Теорема доказана.

Доказательство теоремы 4

Для доказательства существования базиса этого нам понадобится обобщение F-свойства. Кодировать автоматы с помощью константных о.-д. функций уже не получится, поскольку они могут не принадлежать P-множеству P_D. Поэтому в качестве ключа будем использовать о.-д. функции, зависящие от одной переменной.

Пусть $f(x_1, \ldots, x_n), \varphi(x)$ — о.-д. функции из P_D. Рассмотрим о.-д. функцию $f'(x_1, \ldots, x_n, y_1, y_2)$, которая реализуется представленной ниже схемой. Здесь символом ρ отмечена подсхема, реализующая ис-

тинностную о.-д. функцию, в состояниях которой реализуется функция а.-л. $\rho(x_1, x_2) = x_1x_2 \vee \bar{x_1}\bar{x_2}$, символом & обозначена конъюнкция, а символом v функция $v(x_1, x_2, x_3) = x_1x_3 \vee x_2\bar{x_3}$, G_1 — единичная задержка, ϕ — о.-д. функция $\varphi(x)$.

Если на вход y_2 подавать значение $\varphi(y_1)$ в каждый момент времени, то на третий вход блока v всегда будет поступать 1, и на выходе системы будет реализовываться значение функции f. Если окажется, что значения последних двух входов не удовлетворяют условию $\varphi(y_1) = y_2$, на третий вход блока v будет поступать 0 и он начнет пропускать значение входа y_2.

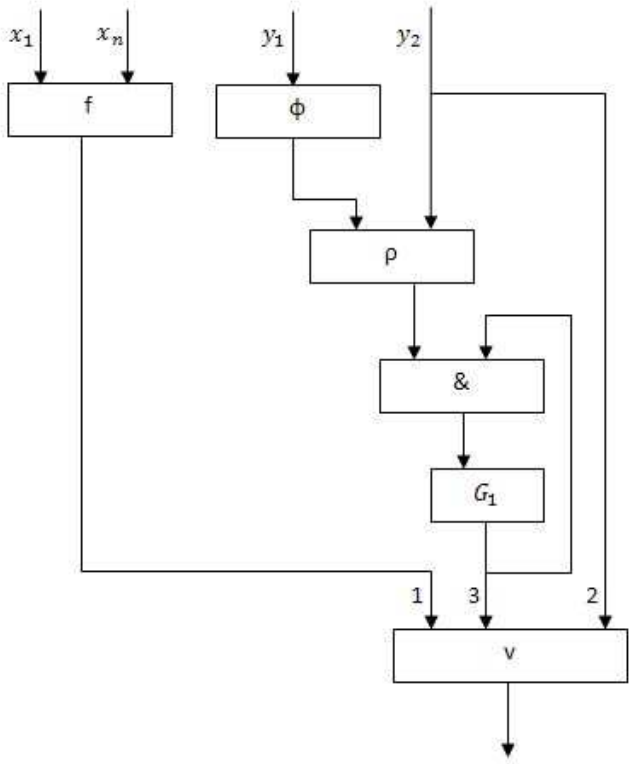


Рис. 4.

Проверим, что функция f', построенная таким образом, принадлежит P_D. Действительно, если на третий вход блока v поступает значение 1, то на выход функции f' поступает значение f в этот момент времени. Функция а.-л., реализуемая в состоянии функции f, принадлежит D, поскольку $f \in P_D$. Если на третий вход блока v поступает значение 0, то на выход функции f' поступает значение φ в этот момент времени. То есть, у функции f' достижимы только те состояния, в которых реализуются функции из D.

Будем говорить, что построенная таким образом функция f' кодирует f с помощью ключа φ и обозначать через $K(f, \varphi)$.

Замечание. В некоторых случаях не обязательно иметь ключ, для того, чтобы «раскодировать» о.-д. функцию. Например, пусть f' кодирует некоторую о.-д. функцию f, где в качестве ключа выступает тождественное отрицание. Для того, чтобы ее «раскодировать» достаточно подставить в последние два входа функции f' тождественные 0 и 1, при этом не обязательно иметь отрицание. Для того, чтобы «взломать» функцию, достаточно подавать на последние два входа значения, удовлетворяющие условию $\varphi(y_1) = y_2$.

Для построения базиса рассмотрим систему $N = R \cup \{h_1, h_2 \ldots\}$, описанную в доказательстве предыдущей теоремы. Выделим из нее бесконечную подсистему $N' = R \cup \{h_{p_1}, h_{p_2} \ldots\}$, где $p_1, p_2, \ldots$ — последовательность всех простых чисел, упорядоченная по возрастанию. Очевидно, N' также полна.

Пусть p — простое число. Обозначим через $g_p(x)$ такую о.-д. функцию, что $g_p(x(t)) = \overline{x(t)}$, если t кратно p и $g_p(x(t)) = x(t)$ в противном случае. Очевидно, g_p имеет p состояний, поэтому $g_p \in R \cup \{h_p\}$. Пусть H_n — множество всех периодических последовательностей, у которых длины периодов образуют множество чисел, представимых в виде $p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}$, где все $p_j, j = 1, \ldots, m$ — простые числа, не превосходящие n.

Рассмотрим систему

$$N_j'' = R \cup \{K(h_{p_1}, g_1), K(h_{p_2}, g_{p_1}), \ldots, K(h_{p_j}, g_{p_{j-1}}) \ldots\},$$

которая также полна. Покажем, что она является базисом.

Никакую функцию из R нельзя исключить без потери свойства полноты, поскольку все функции, не принадлежащие R пропускают значение одной из входных переменных в первый момент времени.

Рассмотрим множество

$$N''_j = R \cup \{K(h_{p_1}, g_1), K(h_{p_2}, g_{p_1}), \ldots, K(h_{p_j}, g_{p_{j-1}})\}.$$

По построению, оно сохраняет множество бесконечных последовательностей H_{p_j}. С другой стороны, любая функция $K(h_{p_{k+1}}, g_{p_k})$, $k > j$ также сохраняет H_{p_j}. Поэтому, $N'' \setminus K(h_{p_{j+1}}, g_{p_j})$ неполна для любого j. Следовательно, N'' является базисом. Теорема доказана.

Автор выражает глубокую благодарность своему научному руководителю проф. В. А. Буевичу за постановку задачи и содействие в ходе выполнения данной работы, а также проф. С. В. Алешину и проф. В. Б. Кудрявцеву за внимание к ней.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

[3] Угольников А. Б. Классы Поста. — М.: Изд-во ЦПИ при мех.-мат. ф-те МГУ, 2008.

[4] Кудрявцев В. Б. О мощности множеств предполных множеств некоторой функциональной системы, связанной с автоматами // Проблемы кибернетики.—М.:Физматгиз,1965. Вып. 13.—С. 45–74.

Быстрый алгоритм построения для k-значных функций полиномов по составному модулю k

Селезнева С. Н. (Москва, МГУ им. М. В. Ломоносова)

selezn@cs.msu.su

Введение

Рассматривается задача проверки полиномиальности k-значных функций (функций над кольцами вычетов по модулю k). Известно, что каждая k-значная функция может быть задана полиномом по модулю k в том и только в том случае, если если k — простое число[1]. Селезневой С. Н. в [2] был предложен практически применимый алгоритм, который по вектору значений k-значной функции $f(x_1, \ldots, x_n)$, где $k = p^m$, p — простое число, $m \geqslant 2$, определяет, задается ли f полиномом по модулю k, и в случае положительного ответа находит ее канонический полином, причем алгоритм имеет битовую сложность $O(N)$, где $N = k^n$ — длина вектора значений функции. Этот алгоритм можно обобщить на случай произвольного составного числа k, при этом его сложность остается такой же.

В настоящей заметке подробно рассматривается случай произвольного составного k. Приведено описание алгоритма, который по вектору значений k-значной функции $f(x_1, \ldots, x_n)$ определяет, задается ли эта функция полиномом по модулю k, в случае положительного ответа строит один из ее полиномов, причем алгоритм имеет битовую сложность $O(N)$, где $N = k^n$ — длина вектора значений функции f.

Основные понятия

Пусть $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$. Функция $f(x_1, \ldots, x_n)$ называется *k-значной*, если $f : E_k^n \to E_k$, где $n = 1, 2, \ldots$.

Множество всех k-значных функций обозначим как P_k, множество всех k-значных функций, зависящих от переменных $x_1, \ldots, x_n$, обозначим как P_k^n.

Пусть $\mathbb{Z}$ — множество целых чисел; $\mathbb{Z}_k = \mathbb{Z}/(k) = \{0, 1, \ldots, k-1\}$ — кольцо вычетов по модулю k, где $k \geqslant 1$.

Функция $f(x_1, \ldots, x_n) \in P_k^n$ *задается полиномом по модулю* k, если найдется такой полином $p(x_1, \ldots, x_n) \in \mathbb{Z}_k[x_1, \ldots, x_n]$, что

$$p(x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

Множество k-значных функций, задающихся полиномами по модулю k, обозначим как Pol_k, и будем называть их полиномиальными.

Известно [1], что $Pol_k = P_k$ тогда и только тогда, когда k — простое число.

Быстрые алгоритмы построения по вектору значений k-значной функции $f(x_1, \ldots, x_n)$ ее полинома по модулю k при простых k предложены Гавриловым Г. П., Сапоженко А. А. (1977 г., [3]) для $k = 2$, Тарannиковым Ю. В. (2004 г.) для произвольного простого числа k. Сложность этих алгоритмов (в алгоритмической модели СФЭ) равна $O(N \log N)$ битовых операций, где $N = k^n$ — длина вектора значений функции.

Мещаниновым Д. Г. (1995 г. [4]) описан алгоритм, проверяющий по вектору значений k-значной функции $f(x_1, \ldots, x_n)$ для $k = p^m$, где p — простое число, $m \geqslant 2$, является ли функция f полиномиальной и в случае положительного ответа строящий какой-то ее полином. Сложность этого алгоритма равна $O(N \log^m N)$ операций, где $N = k^n$ — длина вектора значений функции.

Селезневой С. Н. (2011 г. [2]) предложен алгоритм, проверяющий по вектору значений k-значной функции $f(x_1, \ldots, x_n)$ для $k = p^m$, где p — простое число, $m \geqslant 2$, является ли функция f полиномиальной и в случае положительного ответа строящий ее канонический полином. Сложность этого алгоритма (в алгоритмической модели СФЭ) равна $O(N)$ битовых операций, где $N = k^n$ — длина вектора значений функции. Этот алгоритм обобщается на случай произвольного составного k, и сложность его остается такой же.

В настоящей заметке опишем этот алгоритм для случая произвольного составного числа k.

Алгоритм распознавания полиномиальности и построения полиномов

В качестве алгоритмической модели рассмотрим схемы из функциональных элементов (СФЭ) в некотором полном в P_k базисе. Под

сложностью алгоритма будем понимать число функциональных элементов в соответствующей СФЭ.

Теорема. *Пусть k — составное число. Можно построить детерминированный алгоритм (в алгоритмической модели СФЭ), который для произвольной функции $f(x_1, \ldots, x_n) \in P_k^n$ по вектору ее значений определяет, верно ли, что $f \in Pol_k^n$, и в случае положительного ответа строит какой-то ее полином со сложностью $O(N)$ битовых операций (с числом функциональных элементов $O(N)$), где $N = k^n$ — длина вектора значений функции.*

Доказательство. Опишем алгоритм, который для произвольной функции $f \in P_k^n$ по вектору ее значений определяет, является ли она полиномиальной, и в случае положительного ответа строит какой-то ее полином.

Пусть k — составное число, $k = p_1^{m_1} \cdot \cdots \cdot p_r^{m_r}$, где p_i — попарно различные простые числа, $m_i \geqslant 1$.

Если $r = 1$, то есть $k = p^m$, где p — простое число, $m \geqslant 2$, — воспользуемся алгоритмом из [2].

Пусть $r \geqslant 2$. Тогда кольцо $\mathbb{Z}_k$ есть прямая сумма идеалов, изоморфных кольцам $\mathbb{Z}_{p_i^{m_i}}$.

Шаг 1. Пусть $d_i = p_i^{m_i}$, $i = 1, \ldots, r$.

Пусть $\alpha = (a_1, \ldots, a_n) \in E_k^n$ и $\beta = (b_1, \ldots, b_n) \in E_k^n$. Будем говорить, что наборы α и β *сравнимы по модулю* d_i и обозначать $\alpha = \beta (\mathrm{mod}\ d_i)$, если

$$a_1 = b_1 (\mathrm{mod}\ d_i), \ldots, a_n = b_n (\mathrm{mod}\ d_i).$$

По свойствам полиномов над кольцами вычетов по модулю k если функция $f(x_1, \ldots, x_n) \in Pol_k$, то для любых наборов $\alpha, \beta \in E_k^n$ из того, что $\alpha = \beta (\mathrm{mod}\ d_i)$, следует $f(\alpha) = f(\beta) (\mathrm{mod}\ d_i)$.

Выполним проверку этого необходимого условия полиномиальности для функции $f(x_1, \ldots, x_n)$.

Для этого для каждого i, $i = 1, \ldots, r$, сравниваем значения функции f на наборах, сравнимых по модулю $p_i^{m_i}$. Так как сравнимость наборов по модулю $p_i^{m_i}$ задает отношение эквивалентности на множестве E_k^n, то проверку для каждого i можно выполнить со сложностью

$O(N)$. Значит, сложность шага 1 будет также $O(N)$ битовых операций.

Если хотя бы однажды условие не выполняется, то $f \notin Pol_k$. Иначе, переходим к шагу 2.

Шаг 2. По китайской теореме об остатках сопоставим каждому элементу $a \in E_k$ однозначный набор $(a_1, \ldots, a_r) \in E_{p_1^{m_1}} \times \cdots \times E_{p_r^{m_r}}$, являющийся решением системы сравнений:

$$a = a_i (\mathrm{mod}\ p_1^{m_1}), \ldots, a = a_r (\mathrm{mod}\ p_r^{m_r}).$$

В силу выполненного условия шага 1 функции $f(x_1, \ldots, x_n) \in P_k^n$ сопоставляется набор функций $(f_1, \ldots, f_r) \in P^n_{p_1^{m_1}} \times \cdots \cdot P^n_{p_1^{m_1}}$.

Теперь для каждого i, $i = 1, \ldots, r$, надо проверить задается ли функция $f_i(x_1^i, \ldots, x_n^i) \in P^n_{p_i^{m_i}}$ полиномом по модулю $p_i^{m_i}$ и в случае положительного ответа найти какой-то ее полином.

Воспользуемся известными алгоритмами.

Если $m_i = 1$, то применим алгоритмы построения полиномов при простых p_i (Гаврилов Г. П., Сапоженко А. А. [3], Таранников Ю. В.). Получим вектор коэффициентов полинома функции f_i со сложностью $O(p_i^{m_i n} n)$.

Если $m_i \geqslant 2$, то применим алгоритмы распознавания полиномиальности и построения полиномов при составных $p_i^{m_i}$ (Селезнева С. Н. [2]). Если $f_i \notin Pol_{p_i^{m_i}}$, то $f \notin Pol_k$. Иначе, получим вектор коэффициентов канонического полинома функции f_i со сложностью $O(p_i^{m_i n})$.

Сложность шага 2 равна $O(N)$.

Шаг 3. Если все функции f_i – полиномиальны (каждая по своему модулю), то опять-таки по китайской теореме об остатках по набору коэффициентов $c_1 \in E_{p_1^{m_1}}, \ldots, c_r \in E_{p_r^{m_r}}$ при мономе X в полиномах функций $f_1, \ldots, f_r$ соответственно найдем коэффициент $c \in E_k$ при мономе X в полиноме функции f, являющийся решением системы сравнений:

$$c = c_1 (\mathrm{mod}\ p_1^{m_1}), \ldots, c = c_r (\mathrm{mod}\ p_r^{m_r}).$$

Выполнить шаг 3 можно со сложностью $O(N)$.

Теорема доказана.

Работа поддержана РФФИ, гранты 09–01–00701а, 10–01–00768а.

Список литературы

[1] Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН. — 1958. 51. — С. 5–142.

[2] Селезнева С. Н. Быстрый алгоритм построения для k-значных функций полиномов по модулю k при составных k // Дискретная математика. — 2011. Т. 23. Вып. 3. — С. 3–22.

[3] Гаврилов Г. П., Сапоженко А. А. Сборник задач по дискретной математике. — М.: Наука, 1977.

[4] Мещанинов Д. Г. Метод построения полиномов для функций k-значной логики // Дискретная математика. — 1985. Т. 7. Вып. 3. — С. 48–60.

Порядок функции Шеннона для накопленного ветвления схем из функциональных элементов

Стариков А. О. (Москва, МГУ им. М. В. Ломоносова)

alexey.starikov@mail.ru

Введение

Одной из основных задач синтеза схем из функциональных элементов (СФЭ) является синтез схем, минимальных относительно некоторой заданной характеристики. Для оценки качества конкретных алгоритмов синтеза бывает полезным сопоставление ассимптотики сложности данного алгоритма с функцией Шеннона для минимальной схемы. Ассимптотика функции Шеннона для сложности, представляемой в виде количества элементов в схеме в стандартном базисе, была найдена О. Б. Лупановым в работе [4]. Ассимптотика функции Шеннона для сложности, заданной глубиной схемы в произвольном бесконечном базисе, была найдена О. М. Касим-Заде в работе [5].

Исходя из некоторых свойств практической реализации схем из функциональных элементов [7], имеет смысл рассмотреть характеристику, связанную с топологией соединения элементов схемы. В данной работе исследуется функция Шеннона для сложности, представленной в виде накопленного ветвления, то есть суммарного ветвления провода по пути от входа схемы к её выходу. В качестве базиса рассматривается стандартная система $\{\vee, \&, \neg\}$, дополненная тождественной функцией $\{x\}$.

Как оказалось, методы синтеза Шеннона [1] и Лупанова [4] дают схемы с большим накопленным ветвлением (порядка не меньше $O(2^n)$). При этом построенный автором метод, основанный на «балансировке» совершенной ДНФ с помощью вставок древовидных схем из тождественных функций, дал достаточно хорошую оценку. В работе этот метод используется для получения верхней оценки значения функции Шеннона для накопленного ветвления. Автором получена также нижняя оценка, дающая в совокупности с верхней порядковую оценку $O(n)$, при этом верхняя оценка отличается от нижней

менее чем в два раза. Для доказательства нижней оценки применяются мощностные соображения, приведенные в доказательстве нижней оценки функции Шеннона для количества элементов СФЭ [1].

Основные понятия и результаты

Будем исходить из определения схемы из функциональных элементов как нагруженного ориентированного графа.

Вершины ориентрованного графа, в которые не входит ни одного ребра, называются истоками. Орграф называется ациклическим, если в нем нет ориентированных циклов. В ациклическом орграфе глубиной вершины ν называется максимальное число ребер в ориентированном пути из какого-либо истока в вершину ν. Орграф называется упорядоченным, если для каждой вершины ν_i, в которую входит k_i ребер, задан порядок $e_1, e_2, \ldots, e_{k_i}$ этих ребер.

Систему $Б = \{g_1, g_2, \ldots, g_m\}$, где все g_i — функции алгебры логики, будем называть базисом функциональных элементов. В дальнейшем, как правило, будем подразумевать под базисом функциональных элементов систему $Б_0 = \{\vee, \&, \neg, x\}$. Так как все эти функции симметричны относительно своих переменных, то ребра, входящие в каждую вершину, можно не упорядочивать.

Схемой из функциональных элементов (СФЭ) над базисом $Б$ называется ациклический упорядоченный орграф, в котором:

1) каждому истоку приписана некоторая переменная, причем разным истокам приписаны разные переменные (истоки при этом называются входами схемы, а приписанные им переменные — входными переменными);

2) каждой вершине, в которую входят $k \geqslant 1$ ребер, приписана функция из базиса $Б$, зависящая от k переменных (вершина с приписанной функцией при этом называется функциональным элементом);

3) некоторые вершины выделены как выходы (истоки также могут являтся выходами).

Индукцией по глубине q вершины ν определяется функция f_ν, реализуемая в данной вершине. Если $q = 0$, то есть ν — исток, и ν приписана переменная x_i, то $f_\nu \equiv x_i$. Пусть реализуемые функции уже определены для всех вершин глубины меньшей, чем q_0. Рассмотрим

вершину ν глубины q_0, в которую входят ребра $e_1, e_2, \ldots, e_k$ из вершин $\nu_1, \nu_2, \ldots, \nu_k$, и в этих вершинах реализуются функции $f_1, f_2, \ldots, f_k$. Пусть вершине ν приписана функция $g(x_1, \ldots, x_k)$. Тогда в ν реализуется функция $f_\nu = g(f_1, f_2, \ldots, f_k)$.

Будем говорить, что схема реализует систему функций, реализуемых в ее выходах. Схема реализует данную функцию, если она реализует ее хотя бы на одном из выходов.

Сложностью схемы из функциональных элементов называется число функицональных элементов в схеме. Будем обозначать сложность через L.

Назовем проводом, исходящим из функционального элемента ν, множество вершин $\{\nu_1, \ldots, \nu_F\}$, в которые из элемента ν идут ребра. Ветвлением провода назовем число вершин F в соответствующем ему множестве. Обозначим ветвление провода, исходящего из вершины ν, через $F(\nu)$. Будем считать, что если из ν не выходит ни одного ребра, то $F(\nu) = 1$.

При этом будем считать, что ветвление входов запрещено, то есть для любого истока ν_0 справедливо $F(\nu_0) = 1$.

Пусть $P = (\nu_0, \nu_1, \nu_2, \ldots, \nu_n)$ — путь из истока ν_0 (входной вершины) в выходную вершину v_n. Назовем накопленным ветвлением по пути P величину

$$F(P) = \sum_{i=1}^{n} F(\nu_i).$$

Назовем накопленным ветвлением СФЭ S величину

$$F(S) = \max_{P \text{ — путь из входа в выход}} F(P).$$

Введем функцию Шеннона для накопленного ветвления СФЭ по формуле

$$F(n) = \max_{f \in P_2(n)} \quad \min_{f \text{ реализуется СФЭ } S} \quad F(S).$$

Автором получены следующие оценки функции Шеннона для накопленного ветвления:

Теорема 1. *Для схем из функциональных элементов над базисом* $Б_0 = \{\vee, \&, \neg, x\}$

$$F(n) \lesssim](3 \log_3 2 + 1)n[+] \log_2 n[+ 1.$$

Теорема 2. *Для схем из функциональных элементов над базисом* $Б_0 = \{\vee, \&, \neg, x\}$

$$F(n) \gtrsim 3(\log_3 2)n - 6(\log_3 2)\log_2 n - 3.$$

Из теорем 1 и 2 непосредственно следует

Следствие 1. *Порядок функции Шеннона* $F(n)$ *над базисом* $Б_0$ *равен* $O(n)$.

Кроме того, нижняя оценка функции Шеннона для накопленного ветвления СФЭ существенна:

Следствие 2. *Для почти всех функций из* P_2 *порядок наименьшего накопленного ветвления среди схем из функциональных элементов, реализующих данную функцию, совпадает с порядком функции Шеннона.*

Автор выражает благодарность своему научному руководителю И. В. Кучеренко за постановку задачи и внимание к работе и академику В. Б. Кудрявцеву за ценные советы и замечания.

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2002.

[2] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

[3] Кудрявцев В. Б., Блохина Г. Н., Кнап Ж., Кудрявцев В. В. Алгебра логики. — М.; Любляна: Изд-во мех.-мат. ф-та МГУ, 2006.

[4] Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — М.: Физматгиз, 1963. Вып. 10. — С. 63–97.

[5] Касим-Заде О. М. О глубине булевых функций над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Сер. 1. — 2007. Т. 14. № 1. — С. 45–69.

[6] Sherwani N. A. Algorithms for VLSI Physical Design Automation. Third Edition. — Springer, 1998.

[7] Pillage L. T., Rohrer R. A. Asymptotic waveform evaluation for timing analysis // IEEE Trans. on CAD of Integrated Circuits and Systems. — 1990. 9. № 4. — С. 352–366.

О минимизации сложности представления булевых функций из некоторых классов

Чебурахин И. Ф. (Москва)

cybernetics@mati.ru

Введение

Рассматривается задача реализации булевых функций (БФ) в классе формул и — схем из функциональных элементов (ФЭ) в базисе Жегалкина, а также получения при этом по возможности минимальных значений показателей сложности. От сложности-качества этих схем зависят основные характеристики вычислительных и управляющих систем. Проводимые исследования в этой области свидетельствуют, что получение минимального решения неизбежно предполагает использование алгоритмов переборного характера. Следствием этого является большая трудоемкость поиска такого решения уже для функций небольшой размерности. Это приводит к разработке новых подходов постановки задачи и её решения, заметно отличающихся по трудоёмкости от переборных [1–3].

Символ $\cdot$ (точка) используется для обозначения логического или арифметического умножения [4–6].

1. Булевы функции, базисы, формулы и схемы из ФЭ, показатели сложности

Пусть f ($f^{(n)}$ или $f(X)$) — булева функция, зависящая от n переменных из множества $X = \{x_1, \ldots, x_n\}$. Под базисом G понимаем конечную функционально полную систему БФ (или соответствующих ФЭ), в частности, — $G = \{\&, \oplus, 1\}$ для всех булевых функций. Считаем, что функция $f^{(n)}$ задается формулой $F^{(n)}$ в базисе G. В качестве меры сложности представления функции f формулой F или схемой S из ФЭ определяем соответствующие показатели (дискретные функционалы): $L_a(f, G)$ — суммарное число вхождений символов переменных в формулу F; $L_F(f, G)$ — число базисных подформул в F; $Dep_F(f, G)$ — глубина F; $L_S(f, G)$ — число ФЭ в схеме S; $Dep_S(f, G)$ — глубина схемы S.

По практическим соображениям показатели сложности минимизируем. При представлении БФ в классе формул (включая скобочные) для минимизации показателей сложности используются эквивалентные преобразования, — в классе схем для минимизации числа ФЭ дополнительно применяется ветвление их выходов [4–9].

2. Функциональные уравнения (ФУ)

Напомним определение ФУ типа 1 [4–9]: $f^{(n)} = h(f^{(n-1)}, x_n)$, где $n \geqslant 2$, $f^{(2)}$ — начальная функция, $h^{(2)}$ — функция рекурсии, входящая в базис G или представляемая через базисные функции. Обобщим этот тип ФУ. Для полинома Жегалкина $F^{(n)}$ определяем вектор p повторяемости переменных множества $X = \{x_1, \ldots, x_i, \ldots, x_n\}$ в формуле $F^{(n)}$, то есть $p = (p_1, \ldots, p_i, \ldots, p_n)$, где переменная x_i повторяется в формуле $F^{(n)}$ число p_i раз. Заодно получаем $L_a(F^{(n)}, G) = \sum_{i=1}^{n} p_i$.

Пусть $p_i = \max\{p_1, \ldots, p_i, \ldots, p_n\}$, тогда ФУ типа 1 имеет вид

$$F^{(n)} = \left(\left(x_i \cdot F^{(n-1),1}\right) \oplus F^{(n-1),2}\right), \tag{1}$$

где верхние индексы 1 и 2 — номера соответствующих остаточных подфункций, зависящих от числа $(n-1)$ переменных. На основе этого ФУ строится алгоритм градиентного типа, позволяющий получить требуемую формулу $F^{(n)}$. С помощью (1) получаем верхнюю оценку сложности L_F. На каждом шаге алгоритма для соответствующей переменной x_i $(1 \leqslant i \leqslant n-2)$ применяется не больше двух базисных операций и не более двух остаточных подфункций. Для оставшихся подформул, зависящих от переменных x_{n-1} и x_n, при их представлении может потребоваться не более четырёх базисных функций. Итого, получаем $L_F(F^{(n)}, G) \leqslant 2^n$.

3. Элементарные симметрические полиномы (ЭСП) Жегалкина [7, 8]

Рассмотрим ЭСП Жегалкина $F_i(\mathrm{n})$, где n — число переменных, i — степень полинома, то есть $2 \leqslant n \leqslant N$, $1 \leqslant i \leqslant n$.

$$
\begin{aligned}
&F_1^{(n)}(x_1,\ldots,x_n) = x_1 \oplus \ldots \oplus x_n,\\
&F_2^{(n)}(x_1,\ldots,x_n) = x_1\cdot x_2 \oplus x_1\cdot x_3 \oplus \ldots \oplus x_{n-1}\cdot x_n,\\
&\ldots\\
&F_n^{(n)}(x_1,\ldots,x_n) = x_1\cdot \ldots \cdot x_n.
\end{aligned}
\tag{2}
$$

При $i = 1$ или n получаем классы функций «$\oplus$» и «&» (то есть $F_1^{(n)}$ или $F_n^{(n)}$), для которых получены следующие совпадающие оценки

$L_a(F_1^{(n)}, G)_{\min} = L_a(F_n^{(n)}, G)_{\min} = n$,

$L_F(F_1^{(n)}, G)_{\min} = L_S(F_1^{(n)}, G)_{\min} = L_F(F_n^{(n)}, G)_{\min} =$
$= L_S(F_n^{(n)}, G)_{\min} = n - 1$,

$Dep_F(F_1^{(n)}, G)_{\min} = Dep_S(F_1^{(n)}, G)_{\min} = Dep_F(F_n^{(n)}, G)_{\min} =$
$= Dep_S(F_n^{(n)}, G)_{\min} = \lceil \log_2 n \rceil$.

При помощи ФУ типов 1 или 2 получены и другие оценки показателей сложности, из которых ниже потребуются следующие [4–8]:

$$
\begin{gathered}
L_S(F_2^{(n)}, G)_{\min} = 3n - 5, \qquad L_S(F_3^{(n)}, G)_{\min} = 5n - 13,\\
L_S(F_4^{(n)}, G) = 7n - 25, \qquad L_S(F_5^{(n)}, G) = 9n - 41,\\
L_S(F_6^{(n)}, G) = 11n - 61.
\end{gathered}
\tag{3}
$$

Приводя ФУ (1) к виду $F_i^{(n+1)} = F_i^{(n)} \oplus (x_{n+1}\cdot F_{i-1}^{(n)})$, где $n \geqslant 2$, $2 \leqslant i \leqslant n-1$, удобно записывать ЭСП $F_i^{(n)}$ при помощи таблицы [9].

Для ЭСП Жегалкина $F_i^{(n)}$, где n — число переменных и i — степень полинома, поставим задачу вывода оценки $L_S(F_i^{(n)}, G_3) = L_S(i,n) = U(i,n)$ для $n \geqslant 2$, $1 \leqslant i \leqslant n$. Для имеющихся оценок сложности $U(i,n)$ (3) выполним преобразования, разбивая каждую из них на три алгебраические слагаемые (кроме первой и второй оценок). Итак, из каждой $U(i,n)$, $3 \leqslant i \leqslant n-1$, выделяем первое слагаемое $(n-1)$, затем из оставшегося выражения выделяем произведение $(i-1)\cdot(2n-4)$. Тогда оставшаяся часть — сеточная функция u_i (u_i: 4, 12, 24, 40, …, для значений аргумента i, $3 \leqslant i \leqslant n-1$), получается вычитанием из исходного выражения первых двух слагаемых:

$U(1,n) = L_S(F_1^{(n)}, G) = n - 1$,

$U(2,n) = L_S(F_2^{(n)}, G) = 3n - 5 = (n-1) + (2n-4)$,

$U(3,n) = L_S(F_3^{(n)}, G) = 5n - 13 = (n-1) + 2(2n-4) - 4,$
$U(4,n) = L_S(F_4^{(n)}, G) = 7n - 25 = (n-1) + 3(2n-4) - 12,$
$U(5,n) = L_S(F_5^{(n)}, G) = 9n - 41 = (n-1) + 4(2n-4) - 24,$
$U(6,n) = L_S(F_6^{(n)}, G) = 11n - 61 = (n-1) + 5(2n-4) - 40, \ldots$

Для функции u_i составляем разности первого, второго и далее порядков, пока не получим нулевую строку (если существует). Из того, что разности третьего порядка равны нулю, следует второй порядок для многочлена u_i с неопределенными коэффициентами, то есть

$$u_i = a_0 \cdot i^2 + a_1 \cdot i + a_2. \tag{4}$$

Решаем систему уравнений, получаемую из (4) для $i = 3,\ 4, 5$:

$$a_0 \cdot 5^2 + a_1 \cdot 5 + a_2 = 24,$$
$$a_0 \cdot 4^2 + a_1 \cdot 4 + a_2 = 12,$$
$$a_0 \cdot 3^2 + a_1 \cdot 3 + a_2 = 4.$$

Находим $a_0 = 2$; $a_1 = -6$; $a_2 = 4$. Таким образом, функция $u_i = 2 \cdot i^2 - 6 \cdot i + 4$. С третьей составляющей искомая оценка сложности

$$U(i,n) = L_S(F_i^{(n)}, G) = (n-1) + (i-1) \cdot (2 \cdot n - 4) - (2 \cdot i^2 - 6 \cdot i + 4). \tag{5}$$

Итак, аналитически получена верхняя оценка показателя $L_S(F_i^{(n)}, G)$.

Для оценок (5) высказывается гипотеза, справедливая для показателей $L_S(F_1^{(n)}, G)$, и $L_S(F_n^{(n)}, G)$: значения показателя L_S сложности, получаемые при помощи функционала (5) минимальные.

Список литературы

[1] Журавлев Ю. И. Теоретико-множественные методы в алгебре логики // Проблемы кибернетики. — 1962. № 8.

[2] Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. — 1960. Вып. 3.

[3] Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. — 1959. № 2.

[4] Чебурахин И. Ф. Функциональные уравнения и сложность произвольной булевой функции в разных базисах // 7-я Межд. научн. конф. «Дискретные модели в теории управляющих систем». — М., 2006.

[5] Чебурахин И. Ф. Преобразования функциональных уравнений и показатели сложности булевых функций // Материалы IX Межд. семинара «Дискретная математика и её приложения». — М., 2007.

[6] Чебурахин И. Ф. Математические модели для интеллектуализации синтеза дискретных логических управляющих устройств на основе цифровых интегральных схем // Изв. РАН. ТиСУ. — 2008. № 1.

[7] Чебурахин И. Ф. Показатели сложности симметрических полиномов Жегалкина // Тез. докл. XV Межд. конф. «Проблемы теоретической кибернетики». — Казань, 2008.

[8] Чебурахин И. Ф. Сложность симметрических полиномов Жегалкина // XVII Межд. школа-семинар «Синтез и сложность управляющих систем». — М., 2008.

[9] Чебурахин И. Ф., Цурков В. И. Синтез дискретных логических устройств обработки информации на основе теории агентов // Мехатроника, автоматизация, управление. — 2011. № 3. — С. 27–34.

On five types of stability of multicriteria combinatorial minimin problem

Emelichev V. A. (Belarusian State University)
Karelkina O. V. (University of Turku)
Kuzmin K. G. (Belarusian State University)

emelichev@bsu.by, volkar@utu.fi, kuzminkg@mail.ru

In this work, we address the issue of qualitative characteristics of stability of discrete multicriteria optimization problems (see, e.g. [2]). Analysis of the five most known stability types has been carried out for two multicriteria minimin combinatorial problems: with Pareto and lexicographic principles of optimality. As a result necessary and at the same time sufficient conditions for each stability type are obtained as well as interrelation between these types are revealed.

Let A_i be the i-th row of matrix $A = [a_{ij}] \in \mathbf{R}^{n\times m}$, $n \geqslant 1$, $m \geqslant 2$, T be a non empty system of non empty sets $N_m = \{1, 2, \ldots, m\}$ (called trajectories), i.e. $T \subseteq 2^{N_m} \setminus \{\varnothing\}$, $|T| \geqslant 2$. Let the components of vector-function $f(t, A) = (f_1(t, A_1), f_2(t, A_2), \ldots, f_n(t, A_n))$ be defined on T by minimin criteria (see, e.g. [3])

$$f_i(t, A_i) = \min_{j\in t} a_{ij} \to \min_{t\in T}, \quad i \in N_n.$$

On the set T we define two binary relations of domination

$$t \underset{P,A}{\succ} t' \;\Leftrightarrow\; f(t, A) \geqslant f(t', A) \;\wedge\; f(t, A) \neq f(t', A),$$
$$t \underset{L,A}{\succ} t' \;\Leftrightarrow\; \exists k \in N_n \;\big(f_k(t, A_k) > f_k(t', A_k) \;\wedge$$
$$\wedge\; k = \min\{i \in N_n : f_i(t, A_i) \neq f_i(t', A_i)\}\big).$$

Using these relations we specify the Pareto set and lexicographic set respectively:

$$P^n(A) = \big\{t \in T :\; \forall t' \in T \;\; (t \underset{P,A}{\overline{\succ}} t')\big\},$$
$$L^n(A) = \big\{t \in T :\; \forall t' \in T \;\; (t \underset{L,A}{\overline{\succ}} t')\big\}.$$

Here and further the line over a binary relation means the negation of the relation.

Thus two n-criteria combinatorial problems with minimin criteria arise: the problem $Z_P^n(A)$ of finding the Pareto set $P^n(A)$ and the problem $Z_L^n(A)$ of finding the lexicographic set $L^n(A)$.

Since $2 \leqslant |T| < \infty$ then $\varnothing \neq L^n(A) \subseteq P^n(A)$ for any $A \in \mathbf{R}^{n\times m}$.

Let us put into consideration the Smale set and the Slater set respectively:

$$Sm^n(A) = \{t \in T : \ \forall t' \in T \setminus \{t\} \ \ (t \underset{Sm,A}{\overline{\succ}} t')\},$$
$$Sl^n(A) = \{t \in T : \ \forall t' \in T \setminus \{t\} \ \ (t \underset{Sl,A}{\overline{\succ}} t')\},$$

where $t \underset{Sm,A}{\succ} t' \ \Leftrightarrow \ f(t,A) \geqslant f(t',A)$ and $t \underset{Sl,A}{\succ} t' \ \Leftrightarrow \ f(t,A) > f(t',A)$.

Let us denote for brevity any of the sets $P^n(A)$ or $L^n(A)$ by $M^n(A)$ and a multicriteria problem of finding $M^n(A)$ by $Z_M^n(A)$.

We will investigate the five known (see, e.g., [1]) stability types of the multicriteria problem $Z_M^n(A)$. The problem $Z_M^n(A)$ is called S_1-*stable* if there exists $\varepsilon > 0$ such that for any $A' \in \Omega(\varepsilon)$ we have $M^n(A + A') \subseteq M^n(A)$; S_2-*stable* if there exists $\varepsilon > 0$ such that for any $A' \in \Omega(\varepsilon)$ we have $M^n(A) \cap M^n(A + A') \neq \varnothing$; S_3-*stable* if there exists $\varepsilon > 0$ such that for any $A' \in \Omega(\varepsilon)$ we have $M^n(A) \subseteq M^n(A + A')$; S_4-*stable* if there exists $\varepsilon > 0$ such that for any $A' \in \Omega(\varepsilon)$ we have $M^n(A) = M^n(A + A')$ and S_5-*stable* if there exist $\varepsilon > 0$ and $t^0 \in M^n(A)$ such that for any $A' \in \Omega(\varepsilon)$ we have $t^0 \in M^n(A + A')$. Here $\Omega(\varepsilon) = \{A' \in \mathbf{R}^{n\times m} : \ \|A'\| < \varepsilon\}$ is the set of perturbing matrices $A' = [a'_{ij}]$ with rows A'_i, $i \in N_n$, $\|A'\| = \max\{|a'_{ij}| : \ (i,j) \in N_n \times N_m\}$.

Remark 1. Directly from the given definitions it follows:
1) if the problem $Z_M^n(A)$ is S_1-stable, then it is S_2-stable,
2) if the problem $Z_M^n(A)$ is S_3-stable, then it is S_5-stable,
3) the problem $Z_M^n(A)$ is S_4-stable if and only if it is S_1- and S_3-stable,
4) if the problem $Z_M^n(A)$ is S_5-stable, then it is S_2-stable.

Let us denote $N_i(t, A_i) = \operatorname{Arg\,min}\{a_{ij} : j \in t\}, \ i \in N_n,$ and $V(t, A, I) = \prod\limits_{i\in I} N_i(t, A_i), \ I \subseteq N_n$.

The problem with Pareto principle of optimality

For vector $v = (v_1, v_2, \ldots, v_n) \in \mathbf{R}^n$ and set $I = \{i_1, i_2, \ldots, i_k\} \subseteq N_n$, $i_1 < i_2 < \ldots < i_k$, we introduce notation $v_I = (v_{i_1}, v_{i_2}, \ldots, v_{i_k})$.

We put $P^n(t, A) = \{t' \in P^n(A) : \ f(t, A) \geqslant f(t', A)\}$,

$$I(t, t') = \{i \in N_n : \ f_i(t, A_i) = f_i(t', A_i)\}.$$

Theorem 1. *$Z_P^n(A)$, $n \geqslant 1$, is S_1-stable iff for any trajectory $t \in Sl^n(A)$ and vector $v \in V(t, A, N_n)$ there exists trajectory $t^* \in P^n(t, A)$ such that $v_{I(t,t^*)} \in V(t^*, A, I(t, t^*)$.*

This statement indicates that for any trajectory $t \in Sl^n(A)$ there exists trajectory $t^* \in P^n(t, A)$ which is invariant to small perturbations of problem parameters.

Theorem 2. *$Z_P^n(A)$, $n \geqslant 1$, is S_2-stable for any matrix $A \in \mathbf{R}^{n \times m}$.*

For trajectory $t \in P^n(A)$ we introduce a set $Q(t, A) = \{t' \in T : f(t, A) = f(t', A)\}$.

Theorem 3. *$Z_P^n(A)$, $n \geqslant 1$, is S_3-stable iff for any trajectories $t \in P^n(A)$, $t' \in Q(t, A)$ and any index $i \in N_n$ the inclusion $N_i(t, A_i) \supseteq N_i(t', A_i)$ is valid.*

Condition given above indicates that for any two equivalent trajectories t and t' the equality $V(t, A, N_n) = V(t', A, N_n)$ must hold.

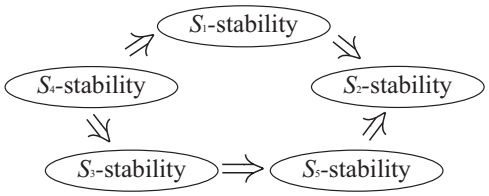
The next result follows from theorems 1 and 3 by virtue of remark 1.

Theorem 4. *$Z_P^n(A)$, $n \geqslant 1$, is S_4-stable iff both statements hold:*
(i) $\forall t \in Sl^n(A)\ \forall v \in V(t, A, N_n)\ \exists t^* \in P^n(t, A)\ \ \big(v \in V(t^*, A, I(t, t^*))\big)$,
(ii) $\forall t \in P^n(A)\ \ \forall t' \in Q(t, A)\ \ \forall i \in N_n\ \ \big(N_i(t, A_i) \supseteq N_i(t', A_i)\big)$.

Theorem 5. *$Z_P^n(A)$, $n \geqslant 1$, is S_5-stable iff there exists trajectory $t^0 \in P^n(A)$ such that for any trajectory $t \in Q(t^0, A)$ and any index $i \in N_n$ the inclusion $N_i(t^0, A_i) \supseteq N_i(t, A_i)$ is valid.*

This condition indicates of the existence of efficient trajectory t^0 such that for all trajectories t equivalent to it the inclusion $V(t^0, A, N_n) \supseteq V(t, A, N_n)$ holds.

Summarizing the results obtained in theorems 1–5 and taking into account remark 1, we conclude that relations between different stability types of the problem $Z_P^n(A)$ are described by the following scheme:



The problem with lexicographic principle of optimality

Let us introduce a set of indexes $M(t) = \{i \in N_n : \ t \in L_i^n(A_i)\}$. It is easy to see that for $t \in L_1^n(A)$ we have $\varnothing \neq M(t) = N_q \subseteq N_n$, where $q = \max\{i \in N_n : t \in L_i^n(A)\} = |M(t)|$.

Theorem 6. *For the problem $Z_L^n(A)$, $n \geqslant 1$, the following statements are equivalent:*
(i) $Z_L^n(A)$ *is S_1-stable,* (ii) $Z_L^n(A)$ *is S_2-stable,*
(iii) $\forall t \in L_1^n(A) \ \ \forall v \in V(t, A, M(t)) \ \ \exists t^* \in L^n(A) \quad \big(v \in V(t^*, A, M(t))\big)$.

Statement (iii) indicates that for any non lexicographic trajectory $t \in L_1^n(A)$ there exists trajectory $t^* \in L^n(A)$ that will not allow trajectory t to become lexicographically optimal under small perturbations.

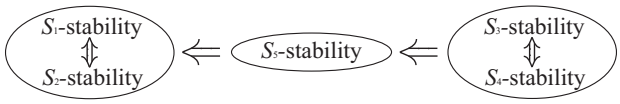
Theorem 7. *For the problem $Z_L^n(A)$, $n \geqslant 1$, the following statements are equivalent:*
(i) $Z_L^n(A)$ *is S_3-stable,* (ii) $Z_L^n(A)$ *is S_4-stable,*
(iii) $\forall t \in L^n(A) \ \ \forall i \in N_n \ \ \forall t' \in L_i^n(A) \quad \big(N_i(t, A_i) \supseteq N_i(t', A_i)\big)$.

Statement (iii) indicates that any trajectory $t \in L^n(A)$ must not be dominated by trajectories $L_i^n(A)$, $i \in N_n$, under small perturbations of problem parameters.

Theorem 8. $Z_L^n(A)$, $n \geqslant 1$, *is S_5-stable iff there exists trajectory $t^0 \in L^n(A)$ such that for any index $i \in N_n$ and any trajectory $t \in L_i^n(A)$ the inclusion $N_i(t^0, A_i) \supseteq N_i(t, A_i)$ is valid.*

This statement indicates of that there exists lexicographically optimal trajectory t^0 which must not be dominated by trajectories $L_i^n(A)$, $i \in N_n$, under small perturbations of problem parameters.

Summarizing the results obtained in theorems 6, 7 and 8, taking into account remark 1, we conclude that the relations between different stability types of the problem $Z_L^n(A)$ are described by the following scheme:



References

[1] Emelichev V. A., Girlich E., Nikulin Yu. V., Podkopaev D. P. Stability and regularization of vector problem of integer linear programming. Optimization. 2002. **51** (4). P. 645–676.

[2] Sergienko I. V., Shilo V. P. Discrete Optimization Problems (in Russian). Kiev: Naukova dumka, 2003.

[3] Tapiero Ch. Risk and Financial Management. 2004. Chichester, John Wiley and Sons Ltd.

On the 2D order curves over finite ring

Skobelev V. V. (Donetsk, IAMM of NAS of Ukraine)

vv_ skobelev@iamm.ac.donetsk.ua

Applications of algebraic models (especially of elliptic curves) in modern cryptography has stimulated research of properties of algebraic curves over arbitrary finite associative-commutative ring $\mathcal{K} = (K, +, \cdot)$ with the unit. In [1] systematically investigated the 2d and the 3d order curves. In the given paper are presented some properties of curves

$$\Gamma : a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0, \qquad (1)$$

where $a_{11}, a_{12}, a_{22}, a_1, a_2, a_0 \in K$ and $(a_{11}, a_{12}, a_{22}) \neq (0, 0, 0)$.

The graph of Γ can be characterized in the following way.

Let $a_{3-i,3-i} \neq 0$ and $a_{ii} = a_{12} = a_i = 0$ where either $i = 1$, or $i = 2$. The graph of Γ is the set of all solutions $(x_0, y_0) \in K^2$ either of equation $a_{22}y^2 + a_2y + a_0 = 0$ $(i = 1)$, or of equation $a_{11}x^2 + a_1x + a_0 = 0$ $(i = 2)$.

Let $a_{3-i,3-i} \neq 0$, $a_{ii} = a_{12} = 0$ and $a_i \neq 0$ where either $i = 1$, or $i = 2$.

Theorem 1. *Let Char* $\mathcal{K} \neq 2$. *If* $i = 1$ *and there exist elements* $b, c \in K\backslash\{0\}$ *such that* $a_{22} = cb^2$ *and* $a_2 = 2cb$ *then the graph of* Γ *is the set of all points* $(x_0, y_0) \in K^2$ *such that* $(w_0, u_0) = (by_0 + 1, x_0)$ *is a solution of equation* $cw^2 + a_1u + (a_0 - c) = 0$. *If* $i = 2$ *and there exist elements* $b, c \in K\backslash\{0\}$ *such that* $a_{11} = cb^2$ *u* $a_1 = 2cb$ *then the graph of* Γ *is the set of all points* $(x_0, y_0) \in K^2$ *such that* $(w_0, u_0) = (bx_0 + 1, y_0)$ *is a solution of equation* $cw^2 + a_1u + (a_0 - c) = 0$.

Let $a_{11} = a_{22} = 0$ and $a_{12} \neq 0$.

Theorem 2. *If* $a_1 = a_2 = 0$ *then the graph of* Γ *is the set of all points* $(x_0, y_0) \in K^2$ *such that* (x_0, y_0) *is a solution of equation* $a_{12}xy + a_0 = 0$. *If* $a_2 \neq 0$ *and there exists an element* $c \in K\backslash\{0\}$ *such that* $a_2 = ca_{12}$ *then the graph of* Γ *is the set of all points* $(x_0, y_0) \in K^2$ *such that* $(u_0, v_0) = (a_{12}y_0 + a_1, x_0 + c)$ *is a solution of equation* $uv + (a_0 - ca_1) = 0$. *If* $a_1 \neq 0$ *and there exists an element* $c \in K\backslash\{0\}$ *such that* $a_1 = ca_{12}$ *then the graph of* Γ *is the set of all points* $(x_0, y_0) \in K^2$ *such that* $(u_0, v_0) = (a_{12}x_0 + a_2, y_0 + c)$ *is a solution of equation* $uv + (a_0 - ca_2) = 0$.

Let $a_{ii} \neq 0$ $(i = 1, 2)$ and $a_j \neq 0$ $(j = 1, 2)$.

Theorem 3. *Let* $Char\, \mathcal{K} \neq 2$ *and there exist elements* $b_1, b_2, c, d \in K\backslash\{0\}$ *such that* $a_{11} = cb_1^2$, $a_{12} = 2cb_1b_2$, $a_{22} = cb_2^2$, $a_1 = db_1$ *and* $a_2 = db_2$. *The graph of* Γ *is the set of all points* $(x_0, y_0) \in K^2$ *such that* $w_0 = b_1x_0 + b_2y_0$ *is a solution of equation* $cw^2 + dw + a_0 = 0$.

Let $a_{ii} \neq 0$, $a_{3-i,3-i} = 0$ and $a_{12} \neq 0$, where either $i = 1$, or $i = 2$. The graph of Γ is the set of all solutions $(x_0, y_0) \in K^2$ either of equation $x(a_{11}x + a_{12}y) + a_1x + a_2y + a_0 = 0$ $(i = 1)$, or of equation $y(a_{22}y + a_{12}x) + a_1x + a_2y + a_0 = 0$ $(i = 2)$.

Let $Char\, \mathcal{K} \neq 2$, $a_{ii} \neq 0$ $(i = 1, 2)$ and either $a_1 = 0$, or $a_2 = 0$. If $a_1 = 0$ and there exist elements $b_1, b_2, c, d \in K\backslash\{0\}$ such that $a_{22} = db^2$, $a_2 = 2dbc$ and $a_0 = dc^2$ then the graph of Γ is the set of all solutions $(x_0, y_0) \in K^2$ of equation $x(a_{11}x + a_{12}y) + d(by + c)^2 = 0$. If $a_2 = 0$ and there exist elements $b_1, b_2, c, d \in K\backslash\{0\}$ such that $a_{11} = db^2$, $a_1 = 2dbc$ and $a_0 = dc^2$ then the graph of Γ is the set of all solutions $(x_0, y_0) \in K^2$ of equation $y(a_{22}y + a_{12}x) + d(bx + c)^2 = 0$.

Canonical form of Γ can be characterized in the following way.

Let

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}, \quad \text{where} \quad A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

Linear operator A annihilates linear form

$$h(x, y) = a_1x + a_2y$$

if and only if $a_1\alpha_{11} + a_2\alpha_{21} = 0$ and $a_1\alpha_{12} + a_2\alpha_{22} = 0$. Thus any linear operator that annihilates linear form $h(x, y)$ is not a bijection.

Theorem 4. *In the result of linear transformation* A *quadric form*

$$f(x, y) = a_{11}x^2 + a_{12}xy + a_{22}y^2$$

can be transformed into the form $g(u, v) = b_{11}u^2 + b_{22}v^2$ *if and only if there exist elements* $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, *such that*

$$2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0,$$

where

$$b_{11} = a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2$$

$$\text{and} \quad b_{22} = a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2.$$

Corollary 1. *In the result of linear transformation A quadric form* $f(x,y)$ *can be transformed into the form* $g(u,v) = b_{11}u^2$ *if and only if there exist elements* $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$ *such that*

$$2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0$$
$$\textit{and} \quad a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0.$$

Corollary 2. *In the result of linear transformation A quadric form* $f(x,y)$ *can be transformed into the form* $g(u,v) = b_{22}v^2$ *if and only if there exist elements* $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$ *such that*

$$2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0$$
$$\textit{and} \quad a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0.$$

Corollary 3. *In the result of linear transformation A quadric form* $f(x,y)$ *can be transformed into the form* $g(u,v) = b_{12}uv$ *if and only if there exist elements* $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$ *such that*

$$a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0$$
$$\textit{and} \quad a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0.$$

Remark. The reason for extraction of equation $b_{12}uv + a_0 = 0$ is the following. Linear form $b_{12}uv + a_0$ in a ring can be transformed by bijection $u = \gamma U + \delta V$, $v = \varphi U + \psi V$ into the form $\gamma\varphi U^2 + \delta\psi V^2$ if and only if there exists elements $\gamma, \delta, \varphi, \psi \in K$ such that, что $\gamma\psi - \delta\varphi \neq 0$ and $b_{12}(\gamma\psi + \delta\varphi) = 0$.

Further investigations can be connected with analysis of non-trivial subclasses of curves.

References

[1] Skobelev V. V., Glazunov N. M., Skobelev V. G. Manifolds over rings. Theory and applications. 2011. Donetsk: IAMM of NAS of Ukraine.