

ИЗУЧЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ ПОТОКАМИ ПЕРВИЧНЫХ ТРЕБОВАНИЙ В ТАНДЕМЕ СИСТЕМ ОБСЛУЖИВАНИЯ С ЦИКЛИЧЕСКИМ АЛГОРИТМОМ С ПРОДЛЕНИЕМ

Кочеганов Виктор Михайлович¹, Зорин Андрей Владимирович²

¹ Национальный исследовательский Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: kocheganol@gmail.com

² Национальный исследовательский Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: andrei.zorine@itmm.unn.ru

Постановка задачи

В данной работе рассматривается сеть (тандем) из двух систем массового обслуживания. В первой из них обслуживаются конфликтные потоки по циклическому алгоритму, а во второй — по алгоритму с промедлением. Данная тандемная сеть подробно описана в работе [1]. Развиваемый там подход позволил представить тандем систем как единую систему массового обслуживания. Напомним существенные моменты из описания системы. На вход обслуживающему устройству поступают четыре входных потока требований: Π_1, Π_2, Π_3 и Π_4 . Требования входного потока Π_j поступают в очередь O_j с неограниченной вместимостью, $j \in \{1, 2, 3, 4\}$. Требования из очереди O_j обслуживаются в порядке поступления. Требования входных потоков Π_1 и Π_3 формируются внешней средой, имеющей всего одно состояние. Каждый из этих потоков является неординарным пуассоновским потоком. Обозначим λ_1 и λ_3 интенсивности потоков групп требований потоков Π_1 и Π_3 соответственно. Производящая функция количества требований в группе по потоку Π_j имеет вид $f_j(z) = \sum_{\nu=1}^{\infty} p_{\nu}^{(j)} z^{\nu}$, $j \in \{1, 3\}$. Предполагается, что $f_j(z)$ сходится для любого $z \in \mathbb{C}$ такого, что $|z| < (1 + \varepsilon)$, $\varepsilon > 0$. После обслуживания, требования из очереди O_1 поступают обратно в систему как требования потока Π_4 . Требования потока Π_4 , в свою очередь, после обслуживания поступают в систему в качестве требований потока Π_2 . Потоки Π_2 и Π_3 конфликтные в том смысле, что их требования не могут быть обслужены одновременно.

Зафиксируем положительные целые числа $d, n_0, n_1, \dots, n_d$. Тогда множество состояний обслуживающего устройства будет выглядеть следующим образом: $\Gamma = \{\Gamma^{(k,r)} : k = 0, 1, \dots, d; r = 1, 2, \dots, n_k\}$. В состоянии $\Gamma^{(k,r)}$ сервер находится в течение неслучайного времени $T^{(k,r)}$. Алгоритм смены состояний учитывает предыдущее состояние прибора, так и длину очереди O_3 в момент принятия решения и формально описан в работе [1].

Для задания процесса обслуживания используются потоки насыщения $\Pi_1^{\text{sat}}, \Pi_2^{\text{sat}}, \Pi_3^{\text{sat}}, \Pi_4^{\text{sat}}$. Число требований в потоке насыщения Π_j^{sat} за время $T^{(k,r)}$

неслучайно и равно $\ell(k, r, j)$, если обслуживающее устройство находится в состоянии $\Gamma^{(k,r)} \in \Gamma$.

Представленная система массового обслуживания может рассматриваться как кибернетическая управляющая система. Схема управляющей системы представлена на рис. 1. На схеме присутствуют следующие блоки: внешняя среда с одним состоянием, входные полюса (входные потоки $\Pi_1, \Pi_2, \Pi_3, \Pi_4$ и потоки насыщения $\Pi_1^{\text{sat}}, \Pi_2^{\text{sat}}, \Pi_3^{\text{sat}}, \Pi_4^{\text{sat}}$), внешняя память (очереди O_1, O_2, O_3, O_4), устройство по переработке внешней памяти (устройства поддержания дисциплин очередей $\delta_1, \delta_2, \delta_3, \delta_4$), внутренняя память (обслуживающее устройство, ОУ), устройство по переработке внутренней памяти (граф переходов из одного состояния ОУ в другое), выходные полюса (выходные потоки $\Pi_1^{\text{out}}, \Pi_2^{\text{out}}, \Pi_3^{\text{out}}, \Pi_4^{\text{out}}$).

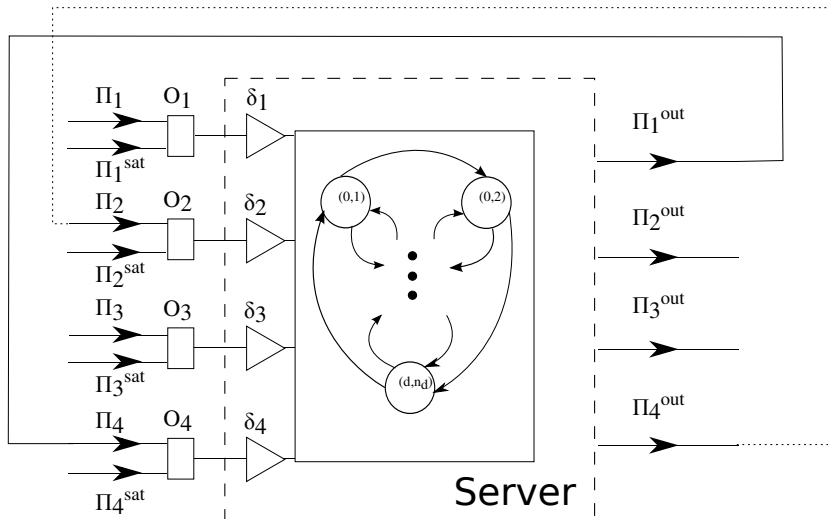


Рис. 1. Схема СМО как управляющей кибернетической системы

В работе [2] были выделены информация, координаты и функция данной системы. Это позволило конструктивно задать последовательности случайных величин и случайных элементов, описывающих дискретную временную шкалу наблюдения и состояния всех блоков схемы. В частности, в качестве дискретной временной шкалы выбрана последовательность $\tau_0 = 0, \tau_1, \tau_2, \dots$ моментов смены состояния обслуживающего устройства. Обозначим через $\Gamma_i \in \Gamma, i = 1, 2, \dots$, состояние обслуживающего устройства в течение времени $(\tau_{i-1}; \tau_i]$ и через $\Gamma_0 \in \Gamma$ — его состояние в момент времени τ_0 , и пусть $\varkappa_{j,i} \in \mathbb{Z}_+$ — количество требований в очереди O_j в момент времени $\tau_i, i \geq 0$. Было доказано, что стохастическая последовательность $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{2,i}, \varkappa_{3,i}, \varkappa_{4,i}); i = 0, 1, \dots\}$ является однородной цепью Маркова. Свойства последовательности $\{(\Gamma_i, \varkappa_{3,i}); i \geq 0\}$ изучены в работах [1, 3].

Основной результат

В данной работе мы рассматриваем последовательность

$$\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{3,i}); i \geq 0\}. \quad (1)$$

Теорема 1. *Стохастическая последовательность (1) при заданном распределении элемента $(\Gamma_0, \varkappa_{1,0}, \varkappa_{2,0}, \varkappa_{3,0}, \varkappa_{4,0})$ является однородной цепью Маркова.*

Теорема 2. *Для того, чтобы марковская цепь (1) имела стационарное распределение, достаточно выполнения неравенства*

$$\min_{\substack{k=1,d \\ j=1,3}} \frac{\sum_{r=1}^{n_k} \ell(k, r, j)}{\lambda_j f'_j(1) \sum_{r=1}^{n_k} T^{(k,r)}} > 1.$$

СПИСОК ЛИТЕРАТУРЫ

- [1] Kochegarov V. M., Zorine A. V. Low-Priority Queue and Server's Steady-State Existence in a Tandem Under Prolongable Cyclic Service // Distributed Computer and Communication Networks. DCCN 2016. Communications in Computer and Information Science (Vishnevskiy V., Samouylov K., Kozyrev D. (eds)). — Cham: Springer, 2016. — V. 678. — Pp. 210–221.
- [2] Кочеганов В. М., Зорин А. В. Вероятностная модель тандема систем массового обслуживания с циклическим управлением с продлением // Теория вероятностей, случайные процессы, математическая статистика и приложения: материалы Междунар. науч. конф., посвящ. 80-летию проф., д-ра физ.-мат. наук Г. А. Медведева, Минск — 23–26 февр. 2015. — Минск: 2015. — С. 94–99.
- [3] Kochegarov V. M., Zorine A. V. Low-priority queue fluctuations in tandem of queueing systems under cyclic control with prolongations // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2015) : материалы Восемнадцатой междунар. науч. конф., 19–22 окт. 2015 г., Москва: / Ин-т проблем упр. им. В. А. Трапезникова Рос. акад. наук; под общ. ред. В. М. Вишневого. — М.: ИПУ РАН — 2015. — С. 517–524.

О РАЦИОНАЛЬНЫХ ЗАДЕРЖКАХ ФУНКЦИЙ k -ЗНАЧНОЙ ЛОГИКИ

Кочергин Алексей Вадимович

ИПМ им. М. В. Келдыша РАН, e-mail: alexeykoch@mail.ru

Изучается обобщенная глубина (задержка) функций k -значной ($k \geq 2$) логики при реализации схемами из функциональных элементов над произвольным конечным базисом. В работе под базисом понимается произвольное множество

функций k -значной логики, такое, что его замыкание относительно операции суперпозиции совпадает с множеством всех функций k -значной логики.

Пусть каждому функциональному элементу Φ_i базиса B соответствует некоторое положительное число t_i . Величину t_i будем называть обобщенной глубиной (или задержкой) элемента Φ_i над базисом B . Под обобщенной глубиной цепи схемы будем понимать сумму обобщенных глубин составляющих ее элементов. Обобщенной глубиной схемы над базисом B , обозначаемой через $T_B(S)$, называется максимальная обобщенная глубина цепи, ведущей от некоторого входа схемы S к ее выходу. Обобщенной глубиной функции (или ее задержкой) f над базисом B будем называть величину $T_B(f) = \min T_B(S)$, где минимум берется по всем схемам S над базисом B , реализующим функцию f . Функцией Шеннона обобщенной глубины над базисом B называется функция $T_B(n)$, определяемая при всех натуральных n равенством $T_B(n) = \max T_B(f)$, где максимум берется по всем функциям k -значной логики f , зависящим от n переменных. Если же для любого функционального элемента Φ_i базиса B величина t_i равна единице, то понятия обобщенной глубины схемы, обобщенной глубины функции, функции Шеннона обобщенной глубины соответственно совпадают с понятиями глубины схемы, глубины функции, функции Шеннона глубины (см., например [1]). Функцию Шеннона глубины будем обозначать через $D_B(n)$.

В работе [1] установлена асимптотика функции Шеннона обобщенной глубины для произвольного базиса функций двузначной ($k = 2$) логики: показано, что для произвольного конечного базиса B функций двузначной логики и любых положительных обобщенных глубин базисных элементов при $n \rightarrow \infty$ выполняется соотношение $T_B(n) \sim \gamma n$, где $\gamma = \min_i (\frac{t_i}{\log_2 m_i})$, t_i — обобщенная глубина элемента Φ_i , а m_i — число существенных переменных у базисной функции f_i , соответствующей элементу Φ_i .

В работе [2] доказано, что для всякого конечного базиса B функций k -значной $k, k \geq 3$, логики существует такая положительная константа α_B , что при $n \rightarrow \infty$ выполняется соотношение $D_B(n) \sim \alpha_B n$. Показано, что константа α_B представляется в виде $\alpha_B = \log_k \lambda_B$, где λ_B является алгебраическим числом. Указан алгоритм нахождения по произвольному конечному базису B функций k -значной логики многочлена с целыми коэффициентами, максимальным действительным корнем которого является число λ_B .

В работе [3] установлено, что при любом натуральном $k, k \geq 3$, для произвольного конечного базиса B функций k -значной логики и любых положительных обобщенных глубин базисных элементов существует такая положительная константа τ_B , что при $n \rightarrow \infty$ выполняется соотношение

$$T_B(n) \sim \tau_B n.$$

Результатами данной работы являются следующие утверждения.

Теорема 1. При любом натуральном k , $k \geq 3$, для всякого конечного базиса B функций k -значной логики и любых положительных рациональных обобщенных глубин базисных элементов константа τ_B из соотношения $T_B(n) \sim \tau_B n$ имеет вид $\tau_B = \log_k \delta_B$, где δ_B является алгебраическим числом.

Теорема 2. Существует алгоритм нахождения по произвольному конечному базису B функций k -значной логики и заданным положительным рациональным обобщенным глубинам базисных элементов многочлена с целыми коэффициентами, максимальным действительным корнем которого является число δ_B .

Работа выполнена при финансовой поддержке Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

СПИСОК ЛИТЕРАТУРЫ

- [1] Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.
- [2] Кочергин А. В. О глубине функций k -значной логики в конечных базисах // Вестник Московского университета. Серия 1. Математика. Механика. — 2013. — № 1. — С. 56–59.
- [3] Кочергин А. В. О задержке функций k -значной логики в конечных базисах // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, 20–25 июня 2016 г.). — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 137–139.

УТОЧНЕНИЕ НИЖНЕЙ ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЯ СТЕПЕНЕЙ

Кочергин Вадим Васильевич¹, Кочергин Дмитрий Вадимович²

¹ МГУ имени М. В. Ломоносова, e-mail: vvkoch@yandex.ru

² МГУ имени М. В. Ломоносова, e-mail: dk@kocherg.in

В работе изучаются возможности уточнения оценок сложности (в первую очередь нижних мощностных оценок) для задачи наискорейшего возведения в степень и некоторых близких к ней задач.

В случае реализации булевых функций в классических моделях вычислений (схемы из функциональных элементов, контактные схемы, формулы и др.) О. Б. Лупановым были установлены (см., например, [1]) асимптотики роста соответствующих функций Шеннона (а также асимптотически точные значения сложности для почти всех функций от заданного числа переменных), которые были позже уточнены С. А. Ложкиным (см., например, [2]).

Рассмотрим возможности аналогичного уточнения оценок схемной (т. е. допускающей возможность многократного использования результатов промежуточных вычислений) сложности для двух неклассических задач, которые единообразно можно описать следующим образом.

Пусть U — свободная полугруппа над конечным алфавитом $\{x_1, \dots, x_k\}$. Тогда элементами полугруппы U являются все конечные слова над этим алфавитом, а произведение uv элементов u и v полугруппы U — это конкатенация слов u и v .

Последовательность S элементов полугруппы U , имеющая вид

$$x_1, x_2, \dots, x_n, \alpha_1, \alpha_2, \dots, \alpha_r,$$

где $\alpha_r = u$ и для каждого t , $1 \leq t \leq r$, найдутся такие i и j , что α_i и α_j лежат в множестве $\{x_1, \dots, x_n, \alpha_1, \dots, \alpha_{t-1}\}$ и $\alpha_t = \alpha_i \alpha_j$, будем называть вычислением элемента u полугруппы U , а число r — длиной вычисления S .

Для произвольного элемента u полугруппы U обозначим через $l(u)$ минимальную длину вычисления элемента u . Наконец, введем функцию Шеннона $l_k(n)$ сложности вычисления элементов свободной полугруппы над k -значным алфавитом равенством $l_k(n) = \max l(u)$, где максимум берется по всем словам длины n над алфавитом мощности k .

Для случая $k \geq 2$ аккуратное применение известных методов дает следующую верхнюю оценку функции Шеннона

$$l_k(n) \leq \frac{n}{\log_k n} \left(1 + (2 + o(1)) \frac{\log_2 \log_2 n}{\log_2 n} \right).$$

Из стандартных мощностных соображений нетрудно получить нижнюю оценку

$$l_k(n) \geq \frac{n}{\log_k n} \left(1 + (1 + o(1)) \frac{\log_2 \log_2 n}{\log_2 n} \right).$$

В работе [3] эта нижняя оценка усилена:

Теорема 1 [3]. Для любого $k \geq 2$ при $n \rightarrow \infty$ справедливо равенство

$$l_k(n) = \frac{n}{\log_k n} \left(1 + (2 + o(1)) \frac{\log_2 \log_2 n}{\log_2 n} \right).$$

При $k = 1$ задача о сложности вычисления элементов свободной полугруппы известна как задача о наискорейшем возведении в степень или в аддитивной постановке — как задача об аддитивных цепочках (см., например, [4, раздел 4.6.3]).

А. Брауэр установил [5] (см. также, например, [4, раздел 4.6.3, теорема D]) верхнюю оценку

$$l(x^n) \leq \log_2 n + \frac{\log_2 n}{\log_2 \log_2 n} \left(1 + (2 + o(1)) \frac{\log_2 \log_2 \log_2 n}{\log_2 \log_2 n} \right),$$

которая вместе с очевидной нижней оценкой $l(x^n) \geq \log_2 n$ дает асимптотику роста величины $l(x^n)$ при $n \rightarrow \infty$.

П. Эрдёш для функции $l_1(n)$ усилил [6] (см. также, например, [4, раздел 4.6.3, теорема E]) нижнюю оценку, показав, что для любого $\varepsilon > 0$ при всех достаточно больших n выполняется неравенство

$$l_1(n) \geq \log_2 n + (1 - \varepsilon) \frac{\log_2 n}{\log_2 \log_2 n}.$$

Эта нижняя оценка состоит из двух слагаемых — первое присутствует в нижней оценке сложности возведения в любую степень и «отвечает» за величину показателя степени, а второе (мощностное) слагаемое имеет место для почти всех показателей степени и «отвечает» за «структуру» числа n .

Попытки несколько увеличить мощностную составляющую наталкиваются на значительные трудности, связанные с тем, что для этой задачи число схем (способов вычислений) сложности не более L оценивается сверху величиной $(cL \log L)^L$, где c — некоторая константа, а не величиной $(cL)^L$ как это обычно бывает при получении мощностных нижних оценок сложности схемных вычислений. В этом направлении получено следующее продвижение.

Теорема 2. Пусть $n \rightarrow \infty$. Тогда

$$l_1(n) - \left(\log_2 n + \frac{\log_2 n}{\log_2 \log_2 n} \right) = O \left(\frac{\log_2 n \log_2 \log_2 \log_2 n}{(\log_2 \log_2 n)^2} \right).$$

В заключение рассмотрим еще одну близкую задачу — задачу о сложности вычисления элементов конечных абелевых групп.

Пусть G — конечная абелева группа, M — произвольное подмножество элементов, порождающее всю группу. Для произвольного элемента $g \in G$ аналогично случаю вычисления элемента свободной полугруппы можно определить величину $L(g, M)$ (подробнее см., например, [7]). Далее полагаем $L(G) = \max L(g, M)$, где максимум берется по всем элементам g и всем порождающим множествам M группы G ; $L_A(n) = \max L(G)$, где максимум берется по всем абелевым группам порядка не более n .

Теорема 3. При $n \rightarrow \infty$ справедливо равенство

$$L_A(n) - \left(\log_2 n + \frac{\log_2 n}{\log_2 \log_2 n} \right) = O \left(\frac{\log_2 n \log_2 \log_2 \log_2 n}{(\log_2 \log_2 n)^2} \right).$$

СПИСОК ЛИТЕРАТУРЫ

- [1] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.
- [2] Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.

- [3] Кочергин В. В., Кочергин Д. В. Уточнение асимптотического поведения сложности сборки слов схемами конкатенации // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2016, № 2. — С. 12–18.
- [4] Кнут Д. Е. Искусство программирования, т. 2. 3-е издание. — М.: Издательский дом «Вильямс», 2000.
- [5] Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — V. 45. — P. 736–739.
- [6] Erdős P. Remarks on number theory, III: On addition chains // Acta Arith. — 1960. — V. 6. — P. 77–81.
- [7] Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. Вып. 4. — М.: Наука, 1992. — С. 178–217.

ПОВЕДЕНИЕ ФУНКЦИИ ШЕННОНА СЛОЖНОСТИ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ В ОДНОМ БЕСКОНЕЧНОМ БАЗИСЕ

Кочергин Вадим Васильевич¹, Михайлович Анна Витальевна²

¹ МГУ имени М. В. Ломоносова, e-mail: vvkoch@yandex.ru

² НИУ ВШЭ, e-mail: anna@mikhaylovich.com

Исследуется задача о сложности реализации функций многозначной логики схемами из функциональных элементов в бесконечном базисе, состоящем из отрицания Поста и всех монотонных функций.

Дадим необходимые определения; недостающие определения можно найти, например, в [1].

Обозначим множество $\{0, 1, \dots, k-1\}$ через E_k . Последовательность

$$\tilde{\alpha}_1 = (\alpha_{11}, \dots, \alpha_{1n}), \tilde{\alpha}_2 = (\alpha_{21}, \dots, \alpha_{2n}), \dots, \tilde{\alpha}_r = (\alpha_{r1}, \dots, \alpha_{rn})$$

наборов из множества E_k^n назовем *возрастающей цепью относительно порядка* $0 < 1 < \dots < k-1$ или просто *цепью*, если все наборы $\tilde{\alpha}_1, \tilde{\alpha}_2, \dots, \tilde{\alpha}_r$ различны и выполняются неравенства

$$\alpha_{ij} \leq \alpha_{i+1,j}, \quad i = 1, \dots, r-1, \quad j = 1, \dots, n.$$

Пусть $f(x_1, \dots, x_n)$ — функция k -значной логики. Упорядоченную пару наборов $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \dots, \beta_n)$, $\tilde{\alpha}, \tilde{\beta} \in E_k^n$, будем называть *обрывом для функции f* , если выполнены условия:

1) $\alpha_j \leq \beta_j$, $j = 1, \dots, n$;

2) $f(\tilde{\alpha}) > f(\tilde{\beta})$.

Под *падением $d_C(f)$ функции f на цепи $C = (\tilde{\alpha}_1, \tilde{\alpha}_2, \dots, \tilde{\alpha}_r)$* будем понимать число обрывов для функции f на парах вида $(\tilde{\alpha}_i, \tilde{\alpha}_{i+1})$.

Снад $d(f)$ функции f определим равенством $d(f) = \max d_C(f)$, где максимум берется по всем цепям C .

Пусть P_k — множество всех функций k -значной логики ($k \geq 2$), M — класс всех функций из P_k , монотонных относительно стандартного порядка $0 < 1 < \dots < k-1$.

Будем рассматривать схемы из функциональных элементов в базисе $B_P^k = M \cup \{N_P^k(x)\}$, где $N_P^k(x)$ — отрицание Поста, т. е. функция $x+1 \pmod k$.

Для произвольной схемы S в базисе B_P^k введем две меры сложности, обозначив через $I_{B_P^k}(S)$ и $L_{B_P^k}(S)$ число элементов в схеме S , которым приписана базисная функция N_P^k и, соответственно, общее число функциональных элементов в схеме S . Для каждой функции f из P_k положим

$$I_{B_P^k}(f) = \min I_{B_P^k}(S), \quad L_{B_P^k}(f) = \min L_{B_P^k}(S),$$

где минимумы берутся по всем схемам S , реализующим функцию f в базисе B_P^k .

В случае $k = 2$ и базиса B_P^2 , состоящего из всех монотонных булевых функций и обычного отрицания, для произвольной булевой функции f А. А. Марковым [2] установлено точное значение величины $I_{B_P^2}(f)$, называемой инверсионной сложностью системы F :

$$I_{B_P^2}(f) = \lceil \log_2(d(f) + 1) \rceil.$$

Этот результат допускает обобщение на случай произвольного k . В работе [3] доказано, что для любой функции k -значной логики f справедливо аналогичное равенство:

$$I_{B_P^k}(f) = \lceil \log_2(d(f) + 1) \rceil.$$

Из этого равенства для меры сложности, характеризующей общее число всех элементов схемы, вытекают следующие оценки:

$$\lceil \log_2(d(f) + 1) \rceil \leq L_{B_P^k}(f) \leq 2 \lceil \log_2(d(f) + 1) \rceil + 1.$$

Перейдем к уточнению этих оценок.

Для произвольного натурального n положим

$$\tau(n) = \begin{cases} 1, & \text{если } 3^r < n \leq 4 \times 3^{r-1} \text{ для некоторого целого } r; \\ 2, & \text{если } 4 \times 3^{r-1} < n \leq 2 \times 3^r \text{ для некоторого целого } r; \\ 3, & \text{если } 2 \times 3^r < n \leq 3 \times 3^r \text{ для некоторого целого } r. \end{cases}$$

Теорема 1. При $k \geq 3$ для любой функции k -значной логики f , удовлетворяющей условию $d(f) \geq 2$, справедливы неравенства

$$\begin{aligned} L_{B_P^k}(f) &\geq 3(\lceil \log_3(d(f) + 1) \rceil - 1) + \tau(d(f) + 1), \\ L_{B_P^k}(f) &\leq 3(\lceil \log_3(d(f) + 1) \rceil - 1) + \tau(d(f) + 1) + 1. \end{aligned}$$

Отметим, что нижняя оценка из теоремы 1 для функции $N_P^k(x)$, удовлетворяющей условию $d(N_P^k) = 1$, не выполняется, так как верны равенства $d(N_P^k) = 1$ и $L_{B_P^k}(N_P^k) = 1$, но $3(\lceil \log_3 2 \rceil - 1) + \tau(2) = 2$.

Стандартным образом определим функцию Шеннона сложности реализации функций k -значной логики схемами в базисе B_P^k :

$$L_{B_P^k}(n) = \max L_{B_P^k}(f),$$

где максимум берется по всем функциям k -значной логики f от n переменных.

Теперь обозначим через $T(k, n)$ величину, на единицу превосходящую значение максимально возможного спада у функций k -значной логики от n переменных. Таким образом,

$$T(k, n) = (k-1)n - \left\lfloor \frac{(k-1)n}{k} \right\rfloor + 1 = (k-2)n + \left\lceil \frac{n}{k} \right\rceil + 1.$$

Наконец, для произвольного натурального n положим

$$\sigma(n) = \begin{cases} -1, & \text{если } n = 1; \\ 0, & \text{если } n = 2^{r+1} - 1 \text{ для некоторого натурального } r; \\ 1, & \text{иначе.} \end{cases}$$

Теорема 2. 1. При $k = 2$ для любого натурального n справедливы равенства

$$L_{B_P^2}(n) = 2 \lceil \log_2 T(k, n) \rceil + \sigma(n) = 2 \lceil \log_2(n+1) \rceil + \sigma(n).$$

2. При $k \geq 3$ для любого натурального $n \geq 4$ для функции Шеннона $L_{B_P^k}(n)$ справедливо равенство

$$L_{B_P^k}(n) = 3(\lceil \log_3 T(k, n) \rceil - 1) + \tau(T(k, n)) + 1.$$

Отметим, что для функции k -значной логики

$$\xi_n(x_1, \dots, x_n) = (x_1 + \dots + x_n + 1)(k-1) \pmod{k}$$

от n переменных, имеющей при фиксированных значениях k и n максимально возможный спад, в условиях теоремы 2 верно равенство

$$L_{B_P^k}(\xi_n) = L_{B_P^k}(n).$$

СПИСОК ЛИТЕРАТУРЫ

- [1] Яблонский С. В. Введение в дискретную математику. 4-е изд. — М.: Высшая школа, 2003.
- [2] Марков А. А. Об инверсионной сложности систем функций // ДАН СССР. — 1957. — Т. 116, № 6. — С. 917–919.
- [3] Кочергин В. В., Михайлович А. В. О минимальном числе отрицаний при реализации систем функций k -значной логики // Дискретная математика. — 2016. — Т. 28, вып. 4. — С. 80–90.

ОБ ОДНОЙ МОДЕЛИ СОКРЫТИЯ ФУНКЦИОНАЛЬНОСТИ СХЕМ И ОЦЕНКАХ СТЕПЕНИ ИХ ЗАЩИЩЁННОСТИ ПРИ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНОЙ РЕАЛИЗАЦИИ «ТИПИЧНЫХ» ФУНКЦИЙ

Ложкин Сергей Андреевич, Павлова Анастасия Федоровна, Данилов Борис Радиславович, Шуплецов Михаил Сергеевич

Московский государственный университет имени М. В. Ломоносова, e-mail: lozhkin@cs.msu.su, nastyapavlova7@gmail.com, brdanilov@gmail.com, shupletsov@cs.msu.ru

В данной статье рассматривается задача информационной защиты структуры и функциональности схем из функциональных элементов (СФЭ), которая связана, в частности, с задачей сокрытия функциональности СБИС на этапе их изготовления. В ней предлагается модель, которая содержит описание методов синтеза асимптотически оптимальных по сложности СФЭ из [1] и способов их защиты от раскрытия функциональности.

В настоящей работе исследуется уровень защищённости СФЭ, построенных указанными методами, от раскрытия их функциональности при сокрытии некоторых локальных соединений. Эти СФЭ строятся с использованием методов обобщённого разложения и универсальных систем функций алгебры логики (ФАЛ) [1].

Синтез защищенных от раскрытия функциональности схем из функциональных элементов

Предлагаемый метод ориентирован на синтез СФЭ в произвольном конечном полном базисе B . При этом общая конструкция асимптотически наилучшего метода [1] синтеза СФЭ Σ_f , которая реализует произвольную ФАЛ $f(x_1, \dots, x_n)$ в базисе B , состоит в следующем.

Сначала ФАЛ $f(x_1, \dots, x_n)$ подвергается (см. [1]) обобщенному разложению по своим последним $(n - q)$ БП $x'' = (x_{q+1}, \dots, x_n)$ на основе некоторой ФАЛ $\phi = \phi(y_1, \dots, y_{2^{n-q}})$, реализуемой схемой формульного типа Φ . После этого каждая из остаточных функций $f_{\sigma''}(x') = f(x', \sigma'')$, где $x' = (x_1, \dots, x_q)$, а σ'' — произвольный набор единичного куба B^{n-q} размерности $(n - q)$, реализуется на основе представления

$$f_{\sigma''} = \psi(g_{\sigma'',1}, \dots, g_{\sigma'',p})$$

с использованием функции $\psi = \psi(y_1, \dots, y_p)$, вычисляемой другой схемой формульного типа Ψ , и построенного на основе селекторного d -компонентного разбиения $D = (Y_1, \dots, Y_d)$ множества булевых переменных (БП) $Y = \{y_1, \dots, y_p\}$ этой функции и соответствующего ему d -компонентного ψ -универсального множества (УМ) ФАЛ $G = G^{(1)} \cup \dots \cup G^{(d)}$ порядка q от БП x' .

Пусть Σ_A — та подсхема схемы Σ_f , в которой реализуются функции множества G , а Σ_B — подсхема, реализующая систему всех функций $f''_\sigma, \sigma'' \in B^{n-q}$, на основе (1), используя выходы схемы Σ_A для снятия соответствующих функций $g_{\sigma,i}$.

Заметим, что вместо любой БП y_i из компоненты Y_s разбиения D может подставляться любая ФАЛ из соответствующего ей подмножества $G^{(s)}$ множества G , причём любые две различные подстановки указанного вида соответствуют реализации различных ФАЛ. Таким образом, разрывая все или часть соединений, связывающих в подсхеме Σ_B входы формул Ψ с выходами блока Σ_A мы получаем одну и ту же схему для целого ряда попарно неэквивалентных исходных схем Σ_f .

Рассмотрим стандартный базис B_0 из ФЭ $\Sigma_\&, \Sigma_\vee$ и Σ_- веса 1, реализующих ФАЛ $x_1x_2, x_1 \vee x_2$ и $\bar{x}_1$ соответственно. Пусть формула $\Psi = \Psi_r$ представляет собой полное r -ярусное двоичное дерево, построенное из блоков Ψ_1 , реализующих ФАЛ $\psi(x_1, x_2, x_3, x_4) = x_1x_3 \vee x_2x_4$, которое получается в результате соединения $(2^r - 1)$ таких блоков через входы x_3, x_4 .

Заметим, что формула Ψ имеет $p = p_r = 2 + 4 + \dots + 2^r + 2^r$ входов и реализует ФАЛ $\psi = \psi_r(y_1, \dots, y_p)$, которая обладает (см. [1]) «геометрическим» (кратности 2) селекторным разбиением своих БП, состоящим из $(2^{r+1} - 1)$ компонент мощности $1, 1, \dots, 2^{r-1}, 2^{r-1}, 2^r$. При этом последняя из указанных компонент состоит из 2^r т. н. основных входов — входов с номерами 3, 4 всех 2^{r-1} блоков Ψ_1 , расположенных в r -ом ярусе дерева формулы Ψ .

Заметим, далее, что при отсоединении основных входов формулы Ψ от выходов схемы Σ_A , на которых реализуются соответствующие данным входам Q различных ФАЛ из ψ -УМ G , число получаемых в результате восстановления данных соединений попарно неэквивалентных схем Σ_f будет равно Q^{2^r} . Отметим, что даже в том специальном случае, когда указанное отсоединение и последующее присоединение основных входов задаётся перестановкой входов 3 и 4 внутри некоторых подсхем Ψ_1 , число вариантов будет равно $2^{2^{r+1}-1}$, если в тех вершинах СФЭ Σ_f , которые соответствуют переставляемым входам, реализуются различные ФАЛ.

На основе описанных выше конструкций с использованием квазиполных деревьев из блоков Ψ_1 доказывается следующее утверждение.

Теорема. *Существует алгоритм, который для произвольной ФАЛ $f(x_1, \dots, x_n)$ строит реализующую её СФЭ Σ_f над стандартным базисом B_0 такую, что*

$$L(\Sigma_f) = \frac{2^n}{n} \left(1 + \frac{2 \log_2 n + O(1)}{n} \right).$$

При этом в схеме Σ_f можно выделить множество S , состоящее из связных непересекающихся одновыходных подсхем глубины, не превосходящей два, с двумя выделенными входами в каждой, такое, что: 1) $|S|$ асимптотически не меньше, чем $\frac{1}{6} 2^n / n$; 2) если q — количество таких подсхем в S , на два выделен-

ных входа которых поступают две различные ФАЛ, то схема Σ' , полученная из СФЭ Σ_f удалением всех дуг, заходящих в выделенные входы указанных подсхем, допускает не менее 2^q попарно не эквивалентных вариантов восстановления (в рамках тех же подсхем и их выделенных входов) удаленных дуг; 3) для почти всех ФАЛ $f(x_1, \dots, x_n)$ число $q = q(n)$ при $n = 1, 2, \dots$ асимптотически равно $|S|$.

Работа выполнена при финансовой поддержке РФФИ, грант № 15-01-07474-а.

СПИСОК ЛИТЕРАТУРЫ

- [1] Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.

О СЛОЖНОСТИ И ГЛУБИНЕ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ СХЕМАМИ, ВЛОЖЕННЫМИ В ЕДИНИЧНЫЙ КУБ

Ложкин Сергей Андреевич¹, Садовников Олег Александрович²,
Довгалюк Екатерина Леонидовна³

¹ МГУ им. М.В. Ломоносова, e-mail: lozhkin@cmc.msu.ru

² МГУ им. М.В. Ломоносова, e-mail: oleg.a.sadovnikov@gmail.com

³ МГУ им. М.В. Ломоносова, e-mail: k3neart@gmail.com

Рассматривается класс схем из функциональных элементов в стандартном базисе из элементов конъюнкции, дизъюнкции и отрицания. Для каждой схемы Σ из данного класса наряду с глубиной $D(\Sigma)$ определим ее размерность $R(\Sigma)$, равную минимальной размерности единичного (булева) куба, допускающего изоморфное вложение Σ . Установлено, что при $n = 1, 2, \dots$ для произвольной функции алгебры логики f от n булевых переменных существует реализующая ее схема Σ_f такая, что $D(\Sigma_f) \leq 2n + o(n)$ и $R(\Sigma_f) \leq n - \log \log n + O(1)$. При этом почти все функции алгебры логики от n переменных, как оказалось, обладают тем свойством, что любая СФЭ, реализующая одну из них и имеющая размерность не больше, чем $n - \log \log n + O(1)$, имеет глубину не меньше, чем $n + \frac{n}{\log \log n} + O(1)$. Тем самым доказано, что для $n = 1, 2, \dots$ почти все функции от n переменных допускают реализацию их схемами рассматриваемого вида, размерность и глубина которых отличаются от минимальных (по всем эквивалентным схемам) значений указанных параметров не более чем на константу и асимптотически не более, чем в 2 раза соответственно. Полученные результаты уточняют оценки, установленные в [5].

Основные определения

Данная работа посвящена исследованию ряда вопросов геометрической реализации схем из функциональных элементов* (СФЭ) над стандартным базисом $B_0 = \{\&, \vee, \neg\}$ в единичном (булевом) кубе B^n , где $B = \{0, 1\}$.

Напомним [4], что граф $\hat{G}$ называется *подразбиением* графа G , если $\hat{G}$ можно получить из G заменой некоторых его ребер на простые цепи, и что два графа считаются *гомеоморфными*, если они имеют изоморфные подразделения.

Будем говорить, что граф G допускает изоморфное (соответственно, гомеоморфное) вложение в граф H , если в графе H существует подграф $\hat{G}$, изоморфный графу G (являющийся, соответственно, подразбиением G).

При этом будем считать, что указанное вложение φ графа G в граф H задается изоморфным (соответственно, гомеоморфным) отображением вершин и ребер графа G в вершины и ребра (соответственно, простые цепи) графа H .

Под изоморфным вложением СФЭ Σ в граф H будем понимать изоморфное вложение в граф H ее графа G , то есть графа, полученного из Σ в результате снятия ориентации с ее ребер и удаления пометок с ее вершин, а также отождествления (удаления) параллельных ребер.

Будем рассматривать куб B^n как граф с 2^n вершинами и $n \cdot 2^{n-1}$ ребрами, соединяющими всевозможные пары соседних вершин, то есть вершин, соответствующих наборам куба, отличающимся ровно в одном разряде. Обозначим через $R(\Sigma)$ минимальную размерность единичного куба, допускающего изоморфное вложение (далее — просто “вложение”) СФЭ Σ , а через $D(\Sigma)$ — ее глубину.

Заметим, что элементы $\&$ и $\vee$ с отождествленными входами (то есть, с параллельными входными дугами) можно рассматривать как одновходовые коммутационные элементы, реализующие тождественные функции алгебры логики. С помощью эквивалентных преобразований СФЭ Σ , связанных с добавлением и удалением коммутационных элементов, можно изменять структуру ее коммутационных подсхем, соединяющих входы Σ и выходы ее функциональных элементов с выходами Σ и входами функциональных элементов. Таким образом можно изменять геометрическую структуру схемы Σ , и, в частности, уменьшить степень ее вершин. При этом, в общем случае, глубина СФЭ Σ может возрасти.

Обычным образом определим размерность $R(f)$ (глубину $D(f)$) ФАЛ f как минимальную размерность (соответственно, глубину) СФЭ, реализующей ФАЛ f , а затем введем связанные с ними функции Шеннона:

$$R(n) = \max_{f \in P_2(n)} R(f), \quad D(n) = \max_{f \in P_2(n)} D(f),$$

где $P_2(n)$ — множество всех ФАЛ от булевых переменных (БП) $X(n) = \{x_1, x_2, \dots, x_n\}$.

*Понятия, которые здесь используются, но не раскрываются, см., например, в [2, 4]

В работе [3] исследовалось поведение функции Шеннона $R(n)$ и было доказано, что

$$n - \log \log n + c_1 \leq R(n) \leq n - \log \log n + c_2,$$

где c_1 и c_2 — некоторые константы. При этом типичное значение глубины схем, построенных при получении верхней оценки для ФАЛ от n булевских переменных (БП) имело при $n = 1, 2, \dots$ экспоненциальный относительно n порядок роста, хотя известно [1], что

$$n - \log \log n + c_3 \leq D(n) \leq n - \log \log n + c_4,$$

где c_3 и c_4 — некоторые константы.

Основные результаты

Теорема 1. *Для любой ФАЛ f от n переменных существует такая реализующая ее СФЭ Σ в стандартном базисе, что*

$$R(\Sigma_f) \leq n - \log \log n + c_5 \text{ и}$$

$$D(\Sigma_f) \leq 2n + \bar{o}(n),$$

где c_5 — некоторая константа. При этом для любой СФЭ Σ , реализующей произвольную ФАЛ f от n переменных и такой, что $R(\Sigma_f) \leq n - \log \log n + c_6$, справедлива следующая нижняя оценка ее глубины:

$$D(\Sigma_f) \geq n + \frac{n}{\log \log n} + c_7,$$

где c_6, c_7 — некоторые константы, причем $c_6 \geq c_7$.

Тем самым устанавливается тот факт, что для произвольной ФАЛ f от n переменных существует такая реализующая ее СФЭ Σ_f , размерность которой отличается от функции Шеннона не более, чем на константу, а глубина асимптотически не больше, чем $2D(n)$.

Работа выполнена при финансовой поддержке РФФИ — грант № 15-01-07474-а.

СПИСОК ЛИТЕРАТУРЫ

- [1] Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. — Вып. 6. — М.: ФИЗМАТЛИТ, 1996. — С. 189–214.
- [2] Ложкин С. А. Лекции по основам кибернетики (учебное пособие). М.: МГУ, 2004.
- [3] Седелев О. Б. Реализация функций алгебры логики схемами из функциональных элементов, вложенными в единичный куб // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2008. — № 1. — С. 44–50.
- [4] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

- [5] Ложкин С. А., Садовников О. А. О сложности и глубине реализации булевых функций схемами, вложенными в единичные кубы // Дискретные модели в теории управляющих систем. IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г. Труды. — М.: МАКС-Пресс, 2015. — С. 145–147.

НОВЫЕ ОЦЕНКИ ФУНКЦИИ ШЕННОНА ДЛИНЫ ЕДИНИЧНОГО ДИАГНОСТИЧЕСКОГО ТЕСТА В НЕКОТОРЫХ БАЗИСАХ

Любич Илья Геннадиевич¹, Романов Дмитрий Сергеевич²

¹ Московский государственный университет имени М. В. Ломоносова, e-mail: Lubi4ig@gmail.com

² Московский государственный университет имени М. В. Ломоносова, e-mail: romanov@cs.msu.ru

Схемы из функциональных элементов (СФЭ, см., например, [2]) — одна из классических моделей дискретных управляющих систем без памяти; анализ функционирования СФЭ при возникновении в них неисправностей традиционно осуществляется с помощью тестового подхода [6]. Пусть на схему S с входами $x_1, x_2, \dots, x_n$, реализующую булеву функцию или систему булевых функций $f(x_1, x_2, \dots, x_n)$, действует источник неисправностей U , способный преобразовать схему S к одной из СФЭ (с такими же входами и выходами, что и у S) некоторого заранее известного списка H конечной длины, содержащего и исходную схему. Множество T входных наборов называется *проверяющим тестом* для схемы S относительно источника неисправностей U тогда и только тогда, когда для любой схемы S_1 из списка H имеет место импликация: если S_2 реализует некоторую булеву функцию или систему булевых функций f_2 , не равную f , то найдется набор $\tilde{\alpha}$ из T такой, что $f_2(\tilde{\alpha}) \neq f(\tilde{\alpha})$. Множество T входных наборов называется *диагностическим тестом* для схемы S относительно источника неисправностей U тогда и только тогда, когда для любых двух схем S_1, S_2 из списка H имеет место импликация: если S_1 и S_2 реализуют неравные булевы функции или системы булевых функций f_1 и f_2 соответственно, то найдется набор $\tilde{\alpha}$ из T такой, что $f_1(\tilde{\alpha}) \neq f_2(\tilde{\alpha})$. Тест минимальной длины называется минимальным, число наборов в тесте T называется длиной теста и обозначается $L(T)$. Источник неисправностей U , способный вызвать поломку не более чем одного элемента схемы, называется *единичным*; тесты относительно такого источника также называются *единичными*. Схема S , при любой неисправности под действием источника неисправностей U реализующая функцию или систему функций, неравную функции или системе функций, реализуемой схемой S в отсутствие неисправностей, называется *тестопригодной* относительно источника неисправностей S . Схема, тестопригодная относительно единичного источника неисправностей, называется *неизбыточной*. Под длиной минимального проверяющего (диагностического)

теста для булевой функции или системы функций f , реализованной с помощью СФЭ в базисе B , относительно источника неисправностей U понимается величина $L_B^{\text{detect}}(U, f)$ ($L_B^{\text{diagn}}(U, f)$), равная минимуму по всем тестопригодным реализующим f СФЭ S в базисе B минимума по всем проверяющим (соответственно диагностическим) тестам T для S относительно U величины $L(T)$. Пусть $\hat{P}_2(n)$ — множество всех булевых функций, существенно зависящих от всех своих n переменных $x_1, x_2, \dots, x_n$. Функцией Шеннона длины проверяющего (диагностического) теста для реализованной с помощью СФЭ в базисе B булевой функции f относительно источника неисправностей U называется величина $L_B^{\text{detect}}(U, n) = \max_{f \in \hat{P}_2(n)} L_B^{\text{detect}}(U, f)$ (соответственно, величина $L_B^{\text{diagn}}(U, n) = \max_{f \in \hat{P}_2(n)} L_B^{\text{diagn}}(U, f)$).

Неисправность в некотором месте схемы (на входе схемы или функционального элемента или на выходе функционального элемента) называется константной, если для каждого входного набора значение, вычисляемое в этом месте, заменяется на какую-то константу. Неисправность в некотором месте схемы называется инверсной, если значение, вычисляемое в этом месте при отсутствии данной неисправности (все остальные неисправности в схеме, если они есть, при этом сохраняются), заменяется на противоположное. Условимся о следующих обозначениях для источников неисправностей в СФЭ. Обозначение для источника неисправностей будет иметь вид X_z^y , где X — это одна или несколько заглавных латинских букв, указывающих на место возможной неисправности (P — неисправности на входах схем, I — неисправности на входах функциональных элементов, O — неисправности на выходах функциональных элементов), y — это название типа неисправности (const, 0, 1 — константные неисправности, константные неисправности типа 0 и константные неисправности типа 1 соответственно, inv — инверсные неисправности), z указывает на число возможных неисправностей (k , если неисправностей не больше k ; нижний индекс отсутствует, если ограничений на число неисправных элементов в схеме нет).

Поведение функций Шеннона длины теста при инверсных неисправностях на выходах элементов в СФЭ изучалось в работах [1, 3–5]. Справедливы следующие утверждения.

Теорема 1. При всяком $n \in \mathbb{N}$ для СФЭ в базисе $B = \{x \& \bar{y}, \bar{x}\}$ имеет место неравенство $L_B^{\text{diagn}}(O_1^{\text{inv}}, n) \leq 2$.

Теорема 2. Существует такая константа $c > 0$, что при всяком $n \in \mathbb{N}$ для СФЭ в базисе $B = \{x \& y, \bar{x}\}$ имеет место неравенство $L_B^{\text{diagn}}(O_1^{\text{inv}}, n) \leq c$.

Авторы выражают благодарность профессору С. А. Ложкину за внимание к работе.

Работа выполнена при поддержке РФФИ (проекты № 15-01-07474-а, № 16-01-00593-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Коваценко С. В. Синтез легкотестируемых схем в базисе Жегалкина для инверсных неисправностей // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2000. — № 2. — С. 45–47.
- [2] Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М. : Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с.
- [3] Редькин Н. П. Единичные проверяющие тесты для схем при инверсных неисправностях элементов // Математические вопросы кибернетики. — Вып. 12. — М. : Физматлит, 2003. — С. 217–230.
- [4] Романов Д. С. Метод синтеза избыточных схем в базисе Жегалкина, допускающих единичные диагностические тесты длины один // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 4. — С. 38–54.
- [5] Романов Д. С. Метод синтеза избыточных схем в стандартном базисе, допускающих единичные диагностические тесты длины два // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2016. — № 3. — С. 56–72.
- [6] Чегис И. А., Яблонский С. В. Логические способы контроля электрических схем // Тр. МИАН СССР. — 1958. — Т. 51. — С. 270–360.

ПЕРЕЧИСЛЕНИЕ РАЗБИЕНИЙ ПРЯМОУГОЛЬНИКА

Магомедов Абдулкарим Магомедович¹, Магомедов Тагир
Абдулкаримович²

¹ Дагестанский университет, e-mail: magomedtagirl1@yandex.ru

² Дагестанский университет, e-mail: tagir.magomedov@gmail.com

Рассматривается «компьютерный» подход к генерации взаимно-рекуррентных формул (в.р.ф.) для перечисления разбиений $w \times h$ -прямоугольника M ($w \cdot h$ четно, $w > 1$, $h > 1$) на 1×2 -прямоугольники («плитки»). Количество таких разбиений будем обозначать через $f(w, h)$.

Для небольших w и h задача была предложена на VI Всероссийской олимпиаде школьников по информатике [1, 2]. Впервые задача исследована в [3, 4], где показано, что для вычисления $f(w, h)$ в случае $w = 2$ достаточно одной рекуррентной формулы ($f(2, h)$ равно h -му числу Фибоначчи), в случае $w = 3$ удается построить систему из двух в.р.ф. В [5] показано, что при $w = 5$ система в.р.ф. состоит из восьми формул.

Ячейку $M_{i,j}$ назовем *точкой ветвления* для разбиения, если 1) первой непокрытой плиткой ячейкой в последовательности $M_{1,1}, \dots, M_{1,w}$;

$\dots; M_{h,1}, \dots, M_{h,w}$ является $M_{i,j}$; 2) ячейки $M_{i,j+1}$ и $M_{i+1,j}$ не покрыты плитками. Понятие *частичного разбиения* (ч.р.) определяется рекурсивно: пустое покрытие считается ч.р. (и обозначается μ_{11}); если $\mu_{i,j}$ — ч.р. с точкой ветвления $M_{i,j}$, то наименьшее разбиение, содержащее $\mu_{i,j}$ и точно одну из двух пар ячеек: $(M_{i,j}, M_{i+1,j})$ и $(M_{i,j}, M_{i,j+1})$, считается ч.р. — потомком $\mu_{i,j}$, если обладает точкой ветвления или же равно полному разбиению.

Рассмотрим ориентированное двоичное дерево T с корнем μ_{11} , вершины v дерева T — ч.р. с описанным выше способом определения потомков. Каждому ч.р. v припишем *дескриптор* $(v_1, \dots, v_w)$, где $v_k = h - \max\{i : M_{i,k} \in v\}$, и индекс $ind_v = \max\{v_1, \dots, v_w\}$. Множество вершин разобьем на классы эквивалентности $F[0], F[1], \dots$: эквивалентными считаются вершины с дескрипторами $\{v_1, \dots, v_w\}$, $\{v_w, \dots, v_1\}$ и $\{v_1 + C, \dots, v_m + C\}$, $C = \text{const}$. Количество различных способов достройки ч.р. v (вершины дерева) из i -го класса эквивалентности до полного разбиения будем называть *перечислением для вершины v* и обозначать $F[i, ind_v]$. Построение двоичного дерева T «сверху вниз — слева направо» условимся завершить, когда для каждой висячей вершины ранее уже построена вершина того же класса эквивалентности; при этом каждую висячую вершину будем называть *терминальной*, а эквивалентную ей вершину с ненулевой полустепенью исхода — *вторично-терминальной*.

Пусть v — вторично-терминальная вершина. Двоичное поддерево с корнем в вершине v будем называть *терминальным поддеревом T_v* , если среди его вершин терминальными являются корень, листья и только они.

Теорема 1. Для любой вторично-терминальной вершины v *перечисление равно сумме перечислений для листьев терминального поддерева T_v* .

Алгоритм компьютерной генерации в.р.ф.: из каждого класса эквивалентности $F[i]$ выбрать по одной вторично-терминальной вершине v , построить для v терминальное поддерево T_v и в соответствии с Теоремой 1 представить перечисление $F[i, ind_v]$ в виде суммы перечислений листьев терминального поддерева T_v .

В следующей теореме, доказанной с привлечением компьютерных подходов, $N(w)$ обозначает количество классов эквивалентности (следовательно, и количество формул в системе в.р.ф. для $w \times h$ -прямоугольника).

Теорема 2. Для $w = 6, \dots, 13$ значения $N(w)$ задаются таблицей:

w	6	7	8	9	10	11	12	13
$N(w)$	10	33	38	142	158	653	709	3050

Если в правой части формулы для вычисления $F[i, k]$ содержится слагаемое $F[j, k]$, то будем говорить, что « j -я формула предшествует i -й формуле», и использовать запись: $F[j] \leftarrow F[i]$. Для организации вычислений по сгенерированному списку в.р.ф. необходимо выполнить *согласование* — отсортировать список таким образом, чтобы для каждой пары формул, для которой определено

условие « $\leftarrow$ », предшествующая формула располагалась ранее по списку. Доказано, что согласование всегда возможно. Более того, справедлива следующая теорема.

Теорема 3. *Согласование списка в.р.ф. выполнимо за время $O(N^2(w))$.*

Отметим, что авторская компьютерная программа, вычислившая, в частности, $f(8, 60) = 540702837469800345466636655620114250126334269081771798953$,

успешно прошла тестирование для известных из литературы примеров: $f(3, 20) = 413403$ [4, с. 379], $f(8, 6) = 4213133$ [2, с. 53], $f(8, 20) = 3547073578562247994$ [2, с. 54].

Работа выполнена при финансовой поддержке отдела математики и информатики ДНЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

- [1] Кирюхин В. М. VI Всероссийская олимпиада школьников по информатике // Информатика и образование. — 1994. — № 3. — С. 47–50.
- [2] Волченков С. Г. Задача «Паркет» // Информатика и образование. — 1994. — № 3. — С. 52–54.
- [3] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. Concrete Mathematics. — Massachusetts : Addison-Wesley, 1994. — 657 p.
- [4] Грэхем Р., Кнут Д., Паташник О. Конкретная математика. Основание информатики. — М. : Мир, 1998. — 703 с.
- [5] Магомедов А. М., Магомедов Т. А. Компьютерный вывод рекуррентных формул разбиения прямоугольника // Тезисы докладов X Белорусской математической конференции. — Минск : Институт математики НАН Беларуси, 2008. — С. 44.

ВЕКТОРНЫЕ ПРОСТРАНСТВА НАД РЕШЕТКАМИ С ЕДИНСТВЕННЫМ БАЗИСОМ

Маренич Евгений Евгеньевич

Московский педагогический государственный университет, e-mail: marenich1@yandex.ru

В работах [1–5] рассматривались векторные пространства над решетками и их свойства. В работах [3, 4] доказан критерий единственности базиса. В работе [2] доказано, что пространства, порожденные столбцами симметрических идемпотентов над нечеткой решеткой, имеют единственный базис. В работе рассматриваются конечнопорожденные векторные пространства над дистрибутивными решетками. Найдены условия, при которых пространство имеет единственный базис над цепями. Рассмотрены свойства столбцовых пространств, порожденных столбцами симметрических идемпотентов, и применены к симметрическим идемпотентам.

Предварительные сведения.

Пусть $L = (L, \wedge, \vee, \leq)$ — дистрибутивная решетка с частичным порядком $\leq$ и решеточными операциями $\vee$ и $\wedge$, L — решетка с нулем $\tilde{0}$ и единицей $\tilde{1}$, $\tilde{0} \neq \tilde{1}$, $L^{m \times n}$ — множество всех (решеточных) матриц размера $m \times n$, элементы которых принадлежат L . Обозначим: $A^{(j)}$ есть j -й столбец матрицы A , $j = 1, 2, \dots, n$; $0_{m \times 1}$ — нулевой столбец, $0_{m \times 1} \in L^{m \times 1}$. На множестве решеточных матриц $L^{m \times n}$ определен частичный порядок $\leq$: $A \leq B$ тогда и только тогда $a_{ij} \leq b_{ij}$, когда для всех i, j , где матрицы $A = (a_{ij})$, $B = (b_{ij})$.

Сложение и умножение матриц определяются как обычно: вместо операции сложения используется операция $\vee$, а вместо операции умножения используется операция $\wedge$. Пусть элемент $\lambda \in L$, матрицы $B = (b_{ij})$, $C = (c_{ij}) \in L^{m \times n}$. Пишем $C = \lambda B$, если $c_{ij} = \lambda \wedge b_{ij}$ для всех индексов i, j . Нечеткой решеткой называется решетка $([0; 1], \wedge, \vee, \leq)$, где $[0; 1]$ — числовой интервал, $\leq$ — обычный частичный порядок на числовом множестве и для любых $a, b \in [0; 1]$

$$a \wedge b = \max\{a, b\}, a \vee b = \min\{a, b\}.$$

Обозначим $Column_L(A)$ пространство над решеткой L , порожденное столбцами матрицы A . Векторами пространства $Column_L(A)$ являются линейные комбинации столбцов матрицы A ,

$$\begin{aligned} Column_L(A) &= Lin_L(A^{(1)}, A^{(2)}, \dots, A^{(n)}) = \\ &= \{\lambda_1 A^{(1)} + \lambda_2 A^{(2)} + \dots + \lambda_n A^{(n)} \mid \lambda_1, \lambda_2, \dots, \lambda_n \in L\}. \end{aligned}$$

Пространство $V = Column_L(A)$ — верхняя полурешетка относительно операции $+$. Если пространство V — решетка, то обозначим $\tilde{\wedge}$ точную нижнюю грань. Если пространство V есть дистрибутивная решетка, то говорим, что V дистрибутивное пространство. Арифметическое пространство $L^{m \times 1}$ — дистрибутивная решетка с решеточными операциями $+$ и $\wedge$. Имеем

$$u \wedge v = (u_{(1)} \wedge v_{(1)}, u_{(2)} \wedge v_{(2)}, \dots, u_{(m)} \wedge v_{(m)})$$

для всех $u, v \in L^{m \times 1}$.

Теорема 1.1. Пространство V является подрешеткой решетки $L^{m \times 1}$ тогда и только тогда, когда $A^{(r)} \wedge A^{(s)} \in V$ для любых столбцов $A^{(r)}, A^{(s)}$.

На множестве V определен частичный порядок $\preceq$: $u \preceq v$ тогда и только тогда, когда $u = \lambda v$ для некоторого элемента $\lambda \in L$, [3]. Элемент $a \in L$ называется $\vee$ -неразложимым, если для любых $b, c \in L$ из равенства $a = b \vee c$ следует, что $a = b$ или $a = c$. Обозначим: $join(V)$ — множество всех $\vee$ -неразложимых векторов пространства V ;

$$J(V) = join(V) - \{0_{m \times 1}\}, MJ(V) = \max\{J(V), \preceq\}, M(V) = \max\{V, \preceq\},$$

где $\max(P, \leq)$ — множество всех максимальных элементов частично упорядоченного множества $\max(P, \leq)$. Базисом пространства V называется конечное

минимальное множество $W \subseteq V$ такое, что $V = \text{Lin}_L(W)$, [1–4]. Пространство может иметь базисы, содержащие разное число векторов. Существует единственный базис, состоящий из V -неразложимых векторов.

Теорема 1.2. [3–4]. Пусть $MJ(V)$ — базис пространства V . Пространство V имеет единственный базис тогда и только тогда, когда

$$MJ(V) \subseteq M(V).$$

Пространства с единственным базисом.

Пусть L — цепь с нулем $\tilde{0}$ и единицей $\tilde{1}$. Если V — ненулевое пространство над решеткой L , то $MJ(V)$ — базис пространства V [2–4].

Теорема 2.1. Пусть $L = \text{Column}_L(A)$, где ненулевые столбцы матрицы $A \in L^{m \times n}$ образуют базис W пространства V такой, что если вектор $w = A^{(i)} \in W$, то $w_{(i)}$ — наибольший элемент столбца w , если вектор $w = A^{(i)} \in W$, то $w_{(i)} > z_{(i)}$ для любого $z \in W, z \neq w$. Тогда W — единственный базис пространства V и $W = MJ(V)$.

Свойства ретрактов

Пусть L — дистрибутивная решетка. Матрица $B \in L^{m \times n}$ называется идемпотентом, если $B = B^2$. Пространство, порожденное столбцами идемпотентной матрицы, называется ретрактом [1, 2].

Теорема 3.1. Матрица $B \in L^{m \times n}$ является идемпотентом тогда и только тогда, когда для любого вектора $v \in V = \text{Column}_L(B)$ справедливо равенство $v = Bv$.

Теорема 3.2. Если B — идемпотент, то ретракт $V = \text{Column}_L(B)$ — решетка и $u \tilde{\wedge} v = B(u \wedge v)$ для любых векторов $u, v \in V$.

Для брауэровых решеток L теорема 3.2 доказана в работе [5].

Следствие 3.1. Каждый ретракт V есть дистрибутивное пространство.

Свойства симметрических идемпотентов.

Пусть L — дистрибутивная решетка с нулем $\tilde{0}$ и единицей $\tilde{1}$, симметрический идемпотент $C \in L^{m \times n}$, ретракт $V = \text{Column}_L(C)$. Обозначим $\text{set}(A)$ множество всех элементов матрицы $A \in L^{m \times n}$.

Теорема 4.1. Справедливы утверждения.

i) Для любых i, j справедливы равенства

$$C^{(i)} \wedge C^{(j)} = c_{ij} C^{(i)}.$$

ii) V — подрешетка решетки $L^{m \times 1}$.

iii) Для всех $j = 1, 2, \dots, m$ справедливы равенства

$$\bigwedge_{i=1}^m C^{(i)} = \bigwedge_{\text{set}(C)} C^{(j)}.$$

Теорема 4.2. *Справедливы утверждения.*

i) Каждый диагональный элемент матрицы C является наибольшим в своей строке и в своем столбце.

ii) Для любых i, j , если $c_{ii} = c_{ij}$, то $C^{(i)} = c_{ii}C^{(j)}$.

Следствие 4.1. *Пусть L — цепь с нулем $\tilde{0}$ и единицей $\tilde{1}$. Тогда каждая строка и каждый столбец матрицы C содержит $\mu = \wedge \text{set}(C)$ — наименьший элемент матрицы C .*

Следствие 4.2. *Пусть L — цепь с нулем $\tilde{0}$ и единицей $\tilde{1}$. Тогда ретракт V имеет единственный базис.*

Следствие 4.3. *Пусть L — цепь с нулем $\tilde{0}$ и единицей $\tilde{1}$, W — базис пространства V , состоящий из столбцов матрицы C . Тогда $W = MJ(V)$.*

СПИСОК ЛИТЕРАТУРЫ

- [1] Kim Ki Hang. Boolean matrix theory and applications. — New York: Marcel Dekker, 1982. — 288 p.
- [2] Kim Ki Hang, Roush F. W. Generalized fuzzy matrices // Fuzzy Sets Systems. — 1980. — No 4. — P. 293–315.
- [3] Маренич Е. Е., Маренич В. Е. Базисы и размерность векторных пространств над решётками // Фундаментальная и прикладная математика. — 2014. — Т. 19, вып.2. — С. 151–169.
- [4] Marenich E. E., Marenich V. E. Bases and dimension of vector spaces over lattices // Journal of Mathematical Sciences. — 2016. — V. 213, № 2. — P. 230–242.
- [5] Marenich V. E. Lattices of matrix rows and matrix columns. Lattices of invariant column eigenvectors // Matrix methods: Theory, Algorithms and Applications Dedicated to the Memory of Gene Golub. Edited by Vadim Olshevsky (University of Connecticut, USA) & Eugene Tyrtyshnicov (Russian Academy Sciences, Russia). — New York: Springer, 2010. — P. 104–116.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И МЕТОДЫ АППАРАТНОЙ ПОДДЕРЖКИ АЛГОРИТМОВ УПРАВЛЕНИЯ ВЗАИМОДЕЙСТВУЮЩИМИ ПРОЦЕССАМИ В ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Мартышкин Алексей Иванович

Пензенский государственный технологический университет, e-mail: alexey314@yandex.ru

Для работы современных вычислительных систем в режиме реального времени все обширнее применяют многопроцессорные (МПС) и многоядерные

структуры, создание которых сопряжено с решением задач управления процессами и ресурсами путем диспетчеризации, эффективность выполнения которой определяется скоростью переключения процессов. Проанализировав методы планирования в многопроцессорных системах [1], выявлено два основных подхода к планированию и диспетчеризации задач: разделение времени и разделение пространства. Достоинство первого метода — автоматическое поддержание балансировки загрузки, второго — отсутствие необходимости перезагрузки кэш-памяти процессорного узла (ПУ) и наличие индивидуальных очередей задач. Детальный анализ показывает, что имеющиеся математические модели МПС отображают реальные процессы грубо, вносят погрешности при оценке вероятностно-временных характеристик, а в ряде случаев приводят к ложным результатам. На рис. 1 показана математическая модель МПС с общим диспетчером задач (ДЗ) без учета приоритетности потока [2].

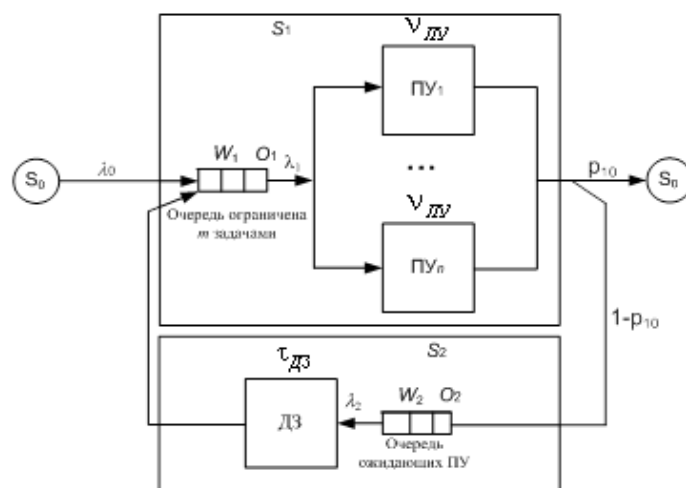


Рис. 1. Математическая модель МПС с общим ДЗ.

Среднее время ожидания задачи в очередях подсистемы «ДЗ–ПУ» рассчитывается по формуле

$$W = \alpha_1 w_1 + \alpha_2 w_2, \quad (1)$$

где α_1 , α_2 — коэффициенты передачи; w_1 , w_2 — время ожидания обслуживания в очереди перед ПУ и перед ДЗ соответственно.

Время ответа в системе с ДЗ и общей очередью задач в МПС равно

$$U = \alpha_1 u_1 + \alpha_2 u_2, \quad (2)$$

где u_1 , u_2 — время ответа от ПУ и от ДЗ соответственно.

Отличие от моделей-аналогов — ДЗ выделен в самостоятельный ресурс и представлен отдельной одноканальной системой массового обслуживания (СМО). На очередь перед ПУ наложено ограничение, в ней может находиться не более m задач на обработку. Также в модели учтены задержки на переключение контекста и перезагрузкой кэш-памяти ПУ.

Математическая модель ДЗ со стратегией разделения в пространстве состоит из n одноканальных СМО ($S_1, \dots, S_n$) (рис. 2) [2].

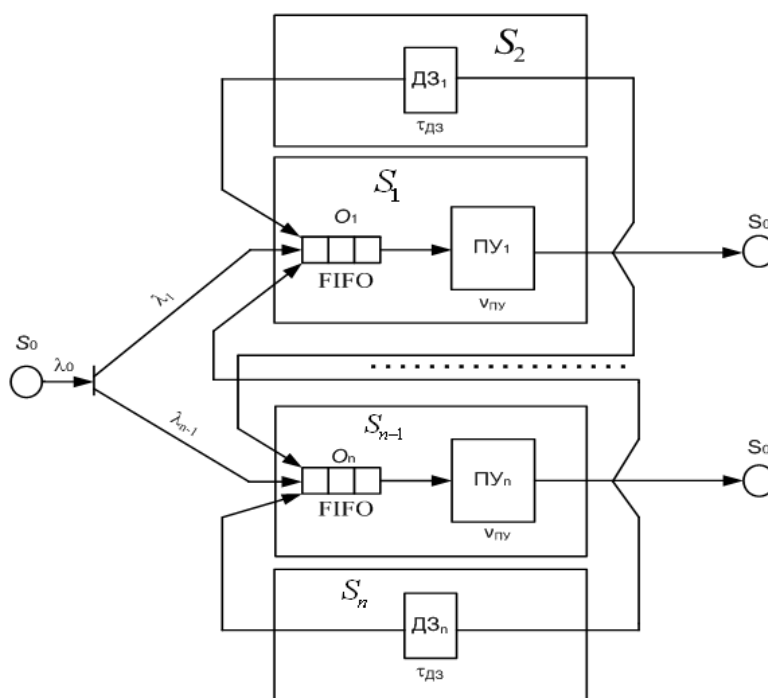


Рис. 2. Математическая модель МПС с индивидуальными ДЗ.

Среднее время ожидания задачи в очередях сети рассчитывается как

$$W = \sum_{i=1}^n \alpha_i w_i, \quad (3)$$

где α_i — коэффициент передачи i -й СМО сети; w_i — время ожидания в очереди перед i -й СМО.

Время ответа в системе с распределенными ДЗ находится по формуле

$$U = \sum_{i=1}^n \alpha_i u_i, \quad (4)$$

где u_i — время ответа подсистемы «ДЗ–ПУ».

Здесь также учтено ограничение длин очередей перед ПУ. Отличие от моделей-аналогов — ДЗ также представлен отдельным устройством. Также в модели учтены задержки на переключение контекста, учтена балансировка загрузки ПУ и связанные с ней временные задержки. На основании моделей проведены эксперименты, характеристики которых соответствуют системам «мягкого» реального времени. Предложенные модели алгоритмов управления взаимодействующими процессами в высокопроизводительных вычислительных системах могут быть положены в организацию аппаратной реконфигурируемой вычислительной системы (РВС). В последние годы все чаще вычислительные системы (ВС) строятся без применения традиционных процессоров в

ПУ. Взамен их для повышения гибкости используются ПЛИС. Данное решение применяется и для аппаратной поддержки ДЗ, входящего в состав РВС, реализованной на ПЛИС, что позволяет достаточно быстро перестраивать устройство под различные типы задач. Подробно описание РВС дано в [3]. Рассмотрим более подробно аппаратную реализацию ДЗ, проектирование которого осуществлено с помощью языка VHDL в САПР Quartus II. Разработанная структура состоит из следующих блоков: модуль генерации задач; модуль для управления очередью задач; модуль очереди хранения задач; процессорный модуль; модуль синхронизации. Моделирование РВС проводилось с помощью ModelSim–Altera 10.0с. Были получены результаты моделирования в виде временных диаграмм функционирования РВС (рис. 3). По результатам моделирования видно, что первым для обслуживания текущей задачи назначен четвертый ПУ, следом назначается третий ПУ, и так далее. Это обусловлено схемой приоритетов от выполнения задач в системе, т. е. от четвертого ПУ к первому.

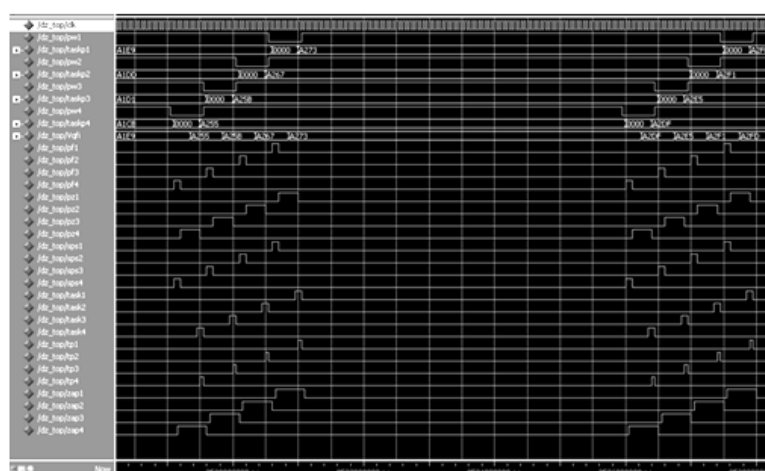


Рис. 3. Полученные диаграммы работы РВС в среде моделирования ModelSim-Altera 10.0с.

На основе выполненного анализа современных методов моделирования ДЗ в МПС разработаны методы математического моделирования подсистемы «ДЗ-ПУ», основанные на приоритетных СМО и системах с ограничением длины очереди с использованием разомкнутых сетей массового обслуживания. Рассмотрена модель РВС. Разработано VHDL описание подсистемы планирования и диспетчеризации задач, что позволяет рассмотреть работу РВС в режиме реального времени. В ходе исследования выявлено, что ДЗ успевает принимать и назначать весь поток поступающих задач. Он не перегружен на всем отрезке времени моделирования и способен обрабатывать более интенсивный входящий поток.

Работа выполнена при поддержке РФФИ (проект № 16-07-00012-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Таненбаум Э., Бос Х. Современные операционные системы. — СПб. : Питер, 2015. — 1120 с.
- [2] Мартышкин А. И. Математическое моделирование диспетчеров задач в многопроцессорных вычислительных системах на основе стохастических сетей массового обслуживания : дис. ... канд. техн. наук: 05.13.18: защищена 18.12.13: утв. 16.06.14 / Мартышкин Алексей Иванович. — Пенза, 2013. — 160 с. — Библиогр. : с. 144-157. — 04201453771.
- [3] Мартенс-Атюшев Д. С., Мартышкин А. И. Разработка реконфигурируемой вычислительной системы для цифровой обработки сигнала // Технические науки — от теории к практике. — 2015. — № 52. — С. 50–58.

НЕКОТОРЫЕ ЗАМКНУТЫЕ КЛАССЫ В P_k И ИХ ГОМОМОРФИЗМЫ В P_d ДЛЯ $d \mid k$

Мещанинов Дмитрий Германович

Национальный исследовательский университет «МЭИ», e-mail: MeshchaninovDG@mpei.ru

Рассматриваются замкнутые классы k -значной логики, содержащие класс L всех линейных по модулю k функций. Наибольшими среди них являются классы $C(d)$ функций, *сохраняющих сравнение по модулю d , $d \mid k$* , т. е. удовлетворяющих условию

$$\text{если } \tilde{a} \equiv \tilde{b} \pmod{d}, \text{ то } f(\tilde{a}) \equiv f(\tilde{b}) \pmod{d}.$$

При $d \neq 1, d \neq k$ классы $C(d)$ являются предполными в P_k [1].

Изучены классы

$$C(d_1, \dots, d_m) = C(d_1) \cap \dots \cap C(d_m).$$

Их решетка по включению полностью описана А. Н. Череповым [2, 3]. Анализировались также классы $R(d)$, $L(d)$ сохранения d -разностей, их решетки [4, 5]. Для $d \neq 1, d \neq k$ выполняются включения $L \subset L(d) \subset R(d) \subset C(d)$.

Функция, удовлетворяющая условию

$$\text{если } \tilde{a} \equiv \tilde{b} \pmod{d}, \text{ то } f(\tilde{a}) = f(\tilde{b}),$$

называется d -периодической.

Определим функции $g_d(\tilde{x})$ и $j(\tilde{x})$. Функция $g_d(\tilde{x})$ принимает значение 1, если $\tilde{x} \equiv \tilde{0} \pmod{d}$, и $g_d(\tilde{x}) = 0$ в остальных случаях. Функция $j(\tilde{x})$ принимает значение 1, если $\tilde{x} = \tilde{0}$, иначе $j(\tilde{x}) = 0$.

Для $d \mid k, e \mid d$ определим $C_e(d)$ как класс всех функций вида

$$f(\tilde{x}) = l(\tilde{x}) + G_e(\tilde{x}) + d \cdot H(\tilde{x}), \quad (1)$$

где $l(\tilde{x}) \in L$, функция G_e является e -периодической, последнее слагаемое правой части кратно d .

Теорема 2. 1. Класс $C_e(d)$ порождается системой $\{x + y, g_e(x, y), dj(x, y)\}$, которая при $d \neq 1, d \neq k, e \neq 1$ образует базис в $C_e(d)$.

2. При фиксированном d классы $C_e(d)$ образуют решетку, изоморфную решетке делителей числа d .

Введем также для $d \mid k$ класс

$$S(d) = [\{1, x + y, xg_d(x)\} \cup \bigcup_{n=1}^{\infty} \{dg_d(x_1, \dots, x_n)\}].$$

Теорема 2. 1. Справедливы включения

$$L \subseteq S(d), S(d) \subseteq C_1(d), S(d) \subseteq R(d).$$

2. При $k = p^2$ и $k = pq$, где p, q простые, справедливо равенство $S(p) = C_1(p) \cap R(p)$ и $S(p)$ является предполным в каждом из классов $C_1(p)$ и $R(p)$.

Эти результаты уточняют строение решетки классов, содержащих L , при $k = 4$ [6], $k = p^2$ [7] и $k = pq$ [5].

Формула (1) для функции f из P_k указывает d -периодическую функцию G_e , принимающую значения из E_d и обладающую многими свойствами функции f (сохранение сравнений и разностей, канонические представления), она аналогична функции d -значной логики. Отображение $f \rightarrow G_e$ оказывается, таким образом, гомоморфизмом замкнутых классов в P_k на замкнутые классы в P_d , что сводит ряд задач в P_k к аналогичным задачам в P_d . Это касается, в частности, условий и формул полиномиальной реализации [8], свойств решетки классов [4, 5, 9].

СПИСОК ЛИТЕРАТУРЫ

- [1] Яблонский С. В. Функциональные построения в k -значной логике // Труды МИАН СССР. — 1958. — Т. 51. — С. 5–142.
- [2] Черепов А. Н. Описание структуры замкнутых классов в P_k , содержащих класс полиномов // Проблемы кибернетики. — Вып. 40. — М.: Наука, 1983. — С. 5–18.
- [3] Черепов А. Н. Надструктура класса сохранения отношений сравнения в k -значной логике по всем модулям-делителям k . — Автореф. дисс. канд. физ.-мат. н. — М., 1986.
- [4] Мещанинов Д. Г. О первых d -разностях функций k -значной логики // Математические вопросы кибернетики. — Вып. 7. — М.: Наука, 1998. — С. 265–280.
- [5] Мещанинов Д. Г. О замкнутых классах k -значных функций, сохраняющих первые d -разности // Математические вопросы кибернетики. — Вып. 8. — М.: Наука, 1999. — С. 219–230.

- [6] Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов // Дискретная математика. — 1997. — Т. 9, вып. 2. — С. 24–39.
- [7] Мещанинов Д. Г. О замкнутых классах полиномов над кольцом Z_k // Труды IX Междунар. конф. «Дискретные модели в теории управляющих систем» (20–22 мая 2015 г.) — М.: МАКС-Пресс, 2015. — С. 161–163.
- [8] Мещанинов Д. Г. Метод построения полиномов для функций k -значной логики // Дискретная математика. — 1995. — Т. 7, вып. 3. — С. 48–60.
- [9] Мещанинов Д. Г. О некоторых свойствах надструктуры класса полиномов в P_k // Матем. заметки. — 1988. — Т. 44, вып. 5. — С. 673–681.

ЛОГИЧЕСКИЕ МЕТОДЫ ВЕРИФИКАЦИИ ПРОГРАММ РАЗВИТИЯ

Михайлов Валерий Юрьевич

Казанский федеральный университет, e-mail: mih@kpfu.ru

В настоящее время программно-целевые методы стали основными в управлении социальными объектами различной природы (регионы, университеты, отрасли и пр.). Центральным элементом этих методов является разработка программы развития (ПР) соответствующего социального объекта (СО) на достаточно долгий период времени. Для компьютерных программ важнейшим вопросом является их верификация, т. е. доказательство их правильности. В теоретическом программировании в таком случае говорят, что программа соответствует своей спецификации, понимая под спецификацией описание решаемой задачи на некотором формализованном языке.

В этой работе мы описываем применение методов верификации программ к ПР, которые, естественно, не являются программами для компьютеров, но часто разработаны столь подробно, что постановка вопроса об их верификации является вполне оправданной и актуальной.

Рассмотрим процесс разработки «правильных» ПР. Для этого мы должны разработать с той или иной степенью подробности модель функционирования СО. Будем представлять ее в виде автомата Бюхи K .

Пусть $P = \langle p_1, p_2, \dots, p_n \rangle$ — список параметров, характеризующих состояние СО в произвольный момент времени. Пусть R_i — интервал изменения параметра p_i . Разобьем интервал R_i на некоторое количество непересекающихся интервалов $r_{ij}, i = 1, \dots, n, j = 1, \dots, m_i$.

Среди параметров P выделим специальный параметр s , означающий количество средств, имеющихся у нас для реализации программы в данном состоянии.

Введем набор элементарных логических переменных. Логическая переменная A_{ij} принимает значение истина тогда и только тогда, когда параметр p_i

принимает значение из интервала $r_{ij}, i = 1, \dots, n, j = 1, \dots, m_i$. Логические переменные, соответствующие параметру s , будем обозначать $S_1, \dots, S_m$.

Множество состояний автомата. Каждое состояние $q(\tilde{A})$ автомата K характеризуется списком элементарных переменных, истинных в данном состоянии. $\tilde{A}$ имеет вид $\langle A_{1j_1}, A_{2j_2}, \dots, A_{nj_n} \rangle$, т. е. из всех переменных $A_{ij}, i = 1, \dots, n$, в этот список попадает только одна переменная A_{ij_i} , которая означает, что в данном состоянии значение параметра p_i находится в интервале r_{ij_i} . Таким образом, множество состояний автомата K конечно $Q = q_0, q_1, \dots, q_k, k \leq m_1 * m_2 * \dots * m_n$.

Множество переходов автомата. Мы должны определить множество доступных для нас действий $D = d_1, \dots, d_s$, выполнение которых в какой-то момент времени t приводит к изменению состояния СО. С каждым действием d_i , свяжем оператор e_i , который может выполняться в каждый момент времени с различной интенсивностью. На практике удобно выделять некоторые параметры e_i явно. Выражение $e_i(b, a_1, a_2, \dots, a_k)$ обозначает оператор e_i , выполняемый с атрибутами $a_1, a_2, \dots, a_k$, на реализацию которого выделена сумма b . Два состояния $q(\tilde{A})$ и $q'(\tilde{A}')$ связаны переходом, помечаемым оператором $e_i(b, a_1, a_2, \dots, a_k)$, если его выполнение в любой период времени в состоянии, в котором истинны переменные $\tilde{A}$, приводит к состоянию, в котором истинны переменные из $\tilde{A}'$.

Начальное состояние автомата. Начальное состояние q_0 автомата K соответствует состоянию СО в начальный период действия ПР. Как правило, это состояние, в котором истинны переменные $A_{11}, A_{21}, \dots, A_{n1}$.

Выделенные (принимающие) состояния. Выделенные состояния автомата K соответствуют состояниям СО, отвечающим всем требованиям ПР, или более широко — требованиям руководства СО с точки зрения устойчивого функционирования СО в будущем.

Траекторией работы автомата K называется конечная или бесконечная последовательность его состояний $c_0, c_1, \dots, c_N, \dots$ такая, что:

- 1) c_0 — начальное состояние,
- 2) состояния c_i и c_{i+1} связаны переходом для каждого i .

Каждая траектория работы автомата K соответствует некоторому сценарию развития СО. Правильный сценарий должен

- 1) начинаться в текущей точке развития;
- 2) либо заканчиваться в некоторой точке, соответствующей выделенному состоянию, либо не заканчиваться, но описывать процесс развития, при котором некоторое выделенное состояние будет повторяться бесконечное число раз;
- 3) удовлетворять определенному дополнительному набору требований, формируемых экспертами по развитию СО данного типа.

Имея правильный сценарий, мы имеем конечный сценарий, по которому легко создается «правильная программа развития» на определенный период

времени, и гарантию выхода СО на траекторию устойчивого развития после окончания реализации соответствующей программы.

Требования к разрабатываемой программе. Мы предлагаем в качестве языка, на котором формулируются требования к правильным сценариям развития, использовать язык логики LTL [1].

Пример. Пусть на сценарий развития накладывается следующее требование: в сценарии должны быть предусмотрены некоторые контрольные точки $o_1, o_2, \dots, o_k$, и в каждой точке o_i параметры развития должны соответствовать определенному набору введенных выше логических переменных $\tilde{A}_i$. К множеству логических переменных автомата K добавим логические переменные $O_1, O_2, \dots, O_k$. Формула $\phi(O_i) = FO_i \& G(O_i \rightarrow XG\neg O_i)$ означает, что переменная O_i будет истинной только в один момент времени. Формула $\psi = \phi(O_1) \& \dots \& \phi(O_k) \& G(O_1 \Rightarrow XFO_2) \& \dots \& G(O_{k-1} \Rightarrow XFO_k)$ означает, что каждая переменных O_i будет истинной только в один момент времени t_i , и момент времени t_{j+1} будет следовать после момента времени $t_j, j = 1, \dots, k-1$. Формула $\gamma = \psi \& G(O_1 \rightarrow \&\tilde{A}_1) \& \dots \& G(O_k \rightarrow \&\tilde{A}_k)$, где $\&\tilde{A}_i$ — есть конъюнкция переменных из списка $\tilde{A}_i$, выражает описанное требование.

Теперь наша задача свелась к следующей: по заданному автомату Бюхи K и заданной формуле ϕ логики LTL найти траектории работы автомата K , на которых формула ϕ будет истинной. Эта задача известна как задача Model Checking и имеет эффективное решение [2].

Таким образом, построение правильной ПР представляет из себя некоторый итерационный процесс, на каждом шаге которого уточняется и усложняется модель развития СО (в виде автомата Бюхи K_i), уточняются и усложняются требования на правильные сценарии развития (в виде формулы ϕ_i логики LTL) и решается задача Model Checking.

Описанный подход был успешно применен при разработке и верификации Программы повышения конкурентоспособности Казанского федерального университета среди ведущих мировых научно-образовательных центров на 2013–2020 гг. [3].

СПИСОК ЛИТЕРАТУРЫ

- [1] Caferra R. Logic for Computer Science and Artificial Intelligence. — John Wiley & Sons. — 2013. — 537]p.
- [2] Карпов Ю. Г. Model Checking. Верификация параллельных и распределенных программных систем. — СПб.: БХВ-Петербург. — 2010. — 460 с.
- [3] Программа повышения конкурентоспособности федерального государственного автономного образовательного учреждения высшего профессионального образования «Казанский (Приволжский) федеральный университет» среди ведущих мировых научно-образовательных центров на 2013–2020

гг. — Казань, 2013. — 61 с. URL: <http://kpfu.ru/cpr/ppk> (дата обращения 12.03.2017).

О СТРОЕНИИ ОДНОГО ЗАМКНУТОГО КЛАССА ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

Михайлович Анна Витальевна

Национальный исследовательский университет «Высшая школа экономики», e-mail: anna@mikhaylovich.com

В работе описаны все замкнутые классы, содержащиеся в классе из примера А. А. Мучника [1] замкнутого класса со счётным базисом.

Пусть $E = \{0, 1, 2\}$, $f : E^n \rightarrow E$, т. е. $f \in P_3$. Обозначим через N_f множество всех наборов из E^n , на которых функция f принимает значение 1.

Множество всех наборов из E^n , которые получаются друг из друга перестановкой компонент, будем называть слоем. Слой из E^n , содержащий e единиц, d двоек и не содержащий нулей, обозначим через $\mathcal{L}(e, d)$. Множество из i наборов из $\{1, 2\}^{i+j}$, содержащих $i + j - 1$ двойку и одну единицу на одном из первых i мест обозначим через $\mathcal{L}(1, i - 1) \times \{2\}^j$.

Для $i = 2, 3, \dots$ обозначим через $g_i(x_1, \dots, x_i)$ такую функцию из P_3 , что $N_{g_i} = \mathcal{L}(1, i - 1)$. Обозначим через $\hat{G}_i$ множество всех функций, полученных из функции g_i перестановкой и переименованием переменных без отождествления и добавлением несущественных переменных.

Для $t, s \in \mathbb{N}$ обозначим через $h_{t,s}(x_1, \dots, x_{t+s})$ такую функцию из P_3 , что $N_{h_{t,s}} = \mathcal{L}(1, t - 1) \times \{2\}^s$. Обозначим через $\hat{H}_t$ объединение функций $h_{t,s}$ для всех $s \geq 1$ и функций, полученных из функций $h_{t,s}$ перестановкой и переименованием переменных без отождествления и добавлением несущественных переменных. Положим

$$G = \bigcup_{i \geq 2} g_i; \quad \hat{G} = \bigcup_{i \geq 2} \hat{G}_i; \quad F = [G]; \quad H_i = \bigcup_{t=1}^i \hat{H}_t; \quad H = \bigcup_{t=1}^{\infty} \hat{H}_t; \quad C_0 = [\{0(x, y)\}].$$

Отметим несколько свойств введённых множеств функций.

1. Для всех $i \geq 2$ выполняется равенство $[\{g_i\}] = \hat{G}_i \cup H_i \cup C_0$.
2. Пусть $2 \leq i_1 < i_2 < \dots < i_s$. Тогда $[\{g_{i_1}, \dots, g_{i_s}\}] = \hat{G}_{i_1} \cup \dots \cup \hat{G}_{i_s} \cup H_{i_s} \cup C_0$.
3. Выполняется равенство $F = \hat{G} \cup H \cup C_0$.
4. Пусть D — бесконечное подмножество натуральных чисел, отличных от единицы. Тогда

$$\left[\bigcup_{i \in D} \{g_i\} \right] = \left(\bigcup_{i \in D} \hat{G}_i \right) \cup H \cup C_0.$$

5. Для всех $i, j \in \mathbb{N}$ выполняется равенство $[\{h_{i,j}\}] = H_i \cup C_0$.

6. Для всех $i \in \mathbb{N}$ выполняется равенство $[H_i] = H_i \cup C_0$.
7. Множество H является замкнутым классом, причём класс H не имеет базиса.

Класс F содержит замкнутые классы четырёх типов:

1. Классы вида

$$F_D^\alpha = \left[\bigcup_{i \in D} \{g_i\} \right],$$

где D — счётное подмножество множества $\mathbb{N} \setminus \{1\}$. Назовём такие замкнутые классы классами типа α . Класс, включающий все классы типа α , сам являющийся классом типа α — это класс F . Предполными классами в классах типа α являются только классы типа α . Из свойств 1 и 4 следует, что класс F_D^α имеет бесконечный базис $\bigcup \{g_i\}$, где объединение берётся по всем $i \in D$.

2. Классы вида

$$F_D^\beta = \left[\bigcup_{i \in D} \{g_i\} \cup H \right],$$

где D — конечное подмножество множества $\mathbb{N} \setminus \{1\}$. Назовём такие замкнутые классы классами типа β . Класс типа β , содержащийся во всех классах типа β — это класс H . Предполными классами в классах типа β являются только классы типа β . Используя свойства 1, 2 и 7, нетрудно показать, что класс F_D^β не имеет базиса.

3. Классы вида

$$F_{D,j}^\gamma = \left[\bigcup_{i \in D} \{g_i\} \cup H_j \right],$$

где D — подмножество множества $2, \dots, j$. Назовём такие замкнутые классы и класс H_1 классами типа γ . Класс типа γ , содержащийся во всех классах типа γ — это класс H_1 . Предполными классами в классах типа γ могут быть только классы типа γ или класс C_0 . Из свойств 2 и 6 следует, что если $j \in D$, то класс $F_{D,j}^\gamma$ имеет конечный базис $\bigcup \{g_i\}$, а если $j \notin D$, то конечный базис $(\bigcup \{g_i\}) \cup h_{j,t}$, где объединение берётся по всем $i \in D$, а $t \in \mathbb{N}$.

4. Класс C_0 . Этот класс содержится во всех вышеперечисленных классах и является предполным для класса H_1 .

Теорема. Все замкнутые подклассы класса F исчерпываются классами типа α , β , γ и классом C_0 . При этом классы типа α имеют счётный базис, классы типа β не имеют базиса, а классы типа γ и класс C_0 имеют конечный базис.

В самом деле, пусть $X \subset F$, $X = [X]$. Если класс X содержит бесконечное подмножество множества G , то $H \subset X$, и, следовательно, X является классом

типа α . Если X содержит только конечное число функций из G , то возможны два случая. Если для некоторого бесконечного множества $D \subset \mathbb{N}$ для любого $i \in D$ существует функция $h_{i,j} \in X$, то $H \subset X$. В этом случае X является классом типа β . Если же существует лишь конечное число индексов i , таких, что найдётся функция $h_{i,j} \in X$, $j \in \mathbb{N}$, то X является классом типа γ . Если же класс X не содержит функций $h_{i,j}$ для всех $i, j \in \mathbb{N}$, то $X = C_0$. Из свойства 3 следует, что других классов нет. Базируемость и конечная порождённость подклассов следует из свойств 1, 2, 4, 6 и 7.

Обозначим через $\mathcal{F}_{\alpha\beta}$ множество всех классов типа α и типа β . Построим биекцию между множеством подмножеств множества $\mathbb{N} \setminus \{1\}$ и множеством классов $\mathcal{F}_{\alpha\beta}$. Пусть $D \subset \mathbb{N} \setminus \{1\}$. Если D — бесконечное множество, то ему соответствует класс $F_D = [\cup\{g_i\}]$, где объединение берётся по всем $i \in D$. Если множество D конечно, то ему соответствует класс $F_D = [(\cup\{g_i\}) \cup H]$, где объединение берётся по всем $i \in D$. Очевидно, что это взаимнооднозначное соответствие, причём $F_{D_1} \subset F_{D_2}$ тогда и только тогда, когда $D_1 \subset D_2$.

Пусть $i \geq 2$, $D \subset \{2, \dots, i\}$, причём $i \in D$. Положим $F_D^s = [(\cup\{g_j\}) \cup H_s]$, где $s \geq i$, а объединение берётся по всем $j \in D$. По определению F_D^s является классом типа γ . Из определения классов типа γ следует, что классы F_D^s , где $s \geq i$, образуют счётную цепь вложенных друг в друга классов. Кроме того, все эти классы содержатся в классе $F_D = [(\cup\{g_j\}) \cup H]$ типа β и для каждого класса типа β существует бесконечное множество последовательно вложенных друг в друга классов типов γ . Отметим, что частичный порядок по включению замкнутых классов типа γ совпадает с частичным порядком по включению множества подмножеств множества $\{2, \dots, s\}$.

СПИСОК ЛИТЕРАТУРЫ

- [1] 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.

МОДЕЛЬ ИНДИВИДУАЛЬНОГО РИСКА В СТРАХОВАНИИ ЗЕРНОВЫХ КУЛЬТУР

Моисеев Александр Владимирович¹, Киндаев Александр Юрьевич²

¹ Пензенский государственный университет, e-mail: moigus@mail.ru

² Пензенский государственный технологический университет, e-mail: ale-kindaeve@yandex.ru

Риск является неотъемлемой частью любого расширенного воспроизводства. В связи с этим механизмы защиты от риска востребованы экономикой, что реализуется через создание страховых фондов. Здесь возникают противоречия между интересами страховщиков и страхователей. Коррелированность убытков в агростраховании при рассмотрении компактных территорий после наступления «неудачного» года позволяет страховщикам увеличивать страховые тарифы,

с чем вполне могут согласиться и страхователи, однако череда «хороших» лет приводит к изменению восприятия риска и, как следствие, требование со стороны страхователей к снижению страховых тарифов. Разрешить данное противоречие можно средствами математического моделирования. Моделирование позволяет проанализировать взаимодействие страховщиков и страхователей.

Моделирование осуществлено на основе предположения нормальности распределения урожайности, кроме этого, рассматривается факт наступления страхового случая и ущерб по отдельно взятым договорам страхования. Итоговая модель получается с использованием формулы полной вероятности.

Вероятность наступления страхового случая

Будем рассматривать классический подход к описанию индивидуальных потерь [1]

$$X = I \cdot Y, \quad (1)$$

где I — индикаторная функция наступления страхового события, Y — размер страхового возмещения после наступления страхового случая. Средний размер страхового возмещения (mean severity) есть математическое ожидание случайной величины X : $m = EX = P\{I = 1\} \cdot EY$.

При реализации страхования урожая сельскохозяйственных культур, согласно [2], в качестве критерия наступления страхового случая ($I = 1$) применяется снижение более чем на долю α урожайности данной культуры от среднего значения урожайности данной культуры в данной местности за предшествующие пять лет

$$\frac{\sum_{K=i-5}^{i-1} U_K - 5 \cdot U_i}{\sum_{K=i-5}^{i-1} U_K} > \alpha, \quad (2)$$

где U_i — урожайность сельскохозяйственной культуры в i -ом году.

Заметим, что урожайность U_i формируется под воздействием многих факторов [3]. Таким образом, на основании центральной предельной теоремы, можно предположить, что случайная величина U имеет нормальное распределение с функцией плотности

$$p_u(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-a)^2}{2\sigma^2}}, \quad (3)$$

где a — математическое ожидание U , σ — стандартное отклонение U .

Исходя из выше сказанного, будем моделировать величину U согласно распределению (3). Вычислим вероятность события $I = 1$ используя (2).

$$P\{I = 1\} = 0,5 - \Phi\left(\frac{\alpha EU}{\sigma U \sqrt{1 + (1 + \alpha)^2}}\right), \quad (4)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt$ — функция Лапласа.

Заметим, что отношение $\frac{\sigma_U}{EU}$ есть коэффициент вариации V урожайности. Таким образом, если взять значение $\alpha = 0,3$, то результат (4) запишется $P\{I = 1\} = 0.5 - \Phi\left(\frac{0.3}{V\sqrt{2.69}}\right)$.

Распределение индивидуальных потерь

Рассмотрим модель распределения ущерба. Будем исходить из того, что если страховой случай наступил, то ущерб определяется величиной [2]:

$$Y = \frac{P}{10} \cdot S \cdot \left(\frac{\sum_{K=i-5}^{i-1} U_K}{5} - U_i \right), \quad (5)$$

где P — средняя цена производителей сельскохозяйственной культуры за 1 тонну, сложившаяся в субъекте РФ за год, предшествующий i -ому году заключения договора страхования; S — посевная площадь под сельскохозяйственной культурой. Если считать величины P и S детерминированными, то распределение величины, заданной формулой (5), определяется случайной величиной $\frac{\sum_{K=i-5}^{i-1} U_K}{5} - U_i$. Для величины Y получим следующие параметры нормального распределения: $a = 0$, $\sigma = \sqrt{\frac{6}{5}} \cdot \frac{P \cdot S}{10} \cdot \sigma_U$. Запишем функцию распределения случайной величины X заданной равенством (1):

$$F_X(x) = P\{0 \leq x\} \cdot P\{I = 0\} + P\{Y \leq x | I = 1\} \cdot P\{I = 1\}. \quad (6)$$

На рисунке 1 представлен график функции распределения индивидуальных потерь (6) при параметрах: $P = 1$ т.руб., $S = 1000$ га, $\sigma_U = 5,25$ ц/га, $V = 0,2904$. Значения параметров по урожайности соответствуют урожайности овса в Башмаковском районе Пензенской области.

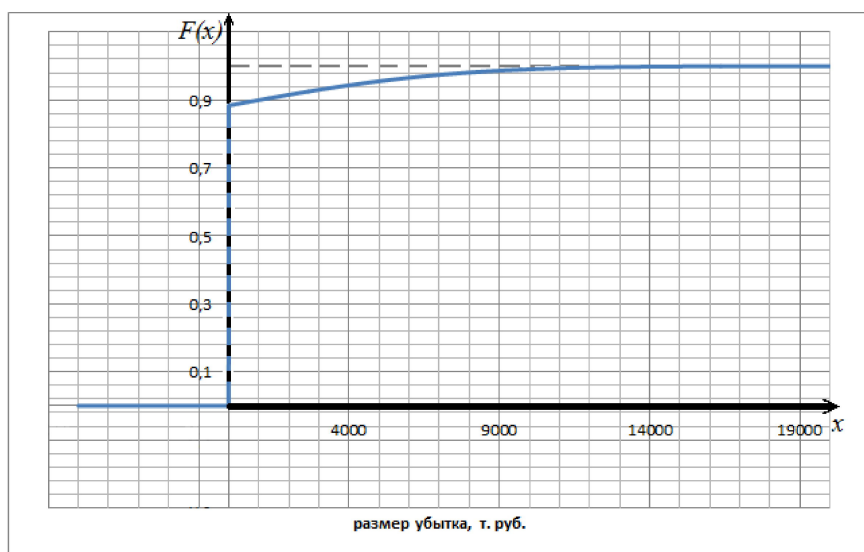


Рис. 1. Функция распределения индивидуального ущерба при страховании овса.

Вопросы моделирования суммарного риска в условиях коррелированности ущерба по отдельным договорам рассмотрены в [4].

Работа выполнена при поддержке РФФИ (проект № 16-36-00275-мол_а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Фалин Г. И., Фалин А. И. Теория риска для актуариев в задачах. — М.: Мир, «Научный мир», 2004. — 240 с.
- [2] Страхование урожая сельскохозяйственных культур и посадок многолетних насаждений с государственной поддержкой: актуарная экспертиза / В. Н. Баскаков, Е. К. Крылова, А. В. Селиванова и др.; по ред. д. ф.-м. н., проф. В. Н. Баскакова. — М.: Янус-К, 2016. — 320 с.
- [3] Посыпанов Г. С., Долгодворов В. Е., Жеруков Б. Х. Растениеводство. — М.: Инфра-М, 2016. — 612 с.
- [4] Киндаев А. Ю., Моисеев А. В. Моделирование страхования в сельском хозяйстве с учетом коррелированности результатов по региону // XXI век: итоги прошлого и проблемы настоящего плюс. — Пенза: ПензГТУ, 2015. — № 3. — С. 175–181.

О РАВЕНСТВЕ ЧИСЕЛ P_4 -УПАКОВКИ И P_4 -ПОКРЫТИЯ В РАСЩЕПЛЯЕМЫХ ГРАФАХ И ИХ РАСШИРЕНИЯХ

Мокеев Дмитрий Борисович

НИУ Высшая Школа Экономики в Нижнем Новгороде, Лаборатория Алгоритмов и Технологий Анализа Сетевых Структур, e-mail: MokeevDB@gmail.com

Граф называется *расщепляемым*, если существует разбиение множества его вершин на клику и независимое множество. Класс расщепляемых графов является наследственным и, следовательно, может быть описан множеством запрещенных графов (минимальных по отношению «быть порожденным подграфом» графов, не принадлежащих данному классу). Множество минимальных запрещённых подграфов для класса расщепляемых графов составляют цикл из 4 вершин, его дополнение и цикл из 5 вершин [1].

Кограф можно охарактеризовать как граф, не содержащий порождённых подграфов, изоморфных P_4 .

Пусть $\mathcal{X}$ — множество графов. Множество попарно непересекающихся порождённых подграфов графа G , изоморфных графам из $\mathcal{X}$, называется $\mathcal{X}$ -упаковкой G . Задача об $\mathcal{X}$ -упаковке состоит в том, чтобы найти $\mathcal{X}$ -упаковку графа наибольшего размера. Размер такой $\mathcal{X}$ -упаковки графа G называется его *числом $\mathcal{X}$ -упаковки* и обозначается $\mu_{\mathcal{X}}(G)$. Множество вершин графа G , покрывающее все порождённые подграфы графа G , изоморфные графам из $\mathcal{X}$, называется *вершинным покрытием G относительно $\mathcal{X}$* или просто $\mathcal{X}$ -покрытием. Задача об $\mathcal{X}$ -покрытии состоит в том, чтобы найти $\mathcal{X}$ -покрытие графа наименьшего размера. Размер такого $\mathcal{X}$ -покрытия графа G называется его *числом $\mathcal{X}$ -покрытия* и обозначается $\beta_{\mathcal{X}}(G)$. Если множество $\mathcal{X}$ состоит из

единственного графа H , то будем говорить об H -упаковках, H -покрытиях и т. п.

Задаче об упаковке графа посвящено немало работ, особенно её алгоритмическим аспектам (см., например, [3, 4]). Известно, что задача поиска мощности максимальной H -упаковки NP-полна для любого графа H , имеющего компоненту связности с тремя или более вершинами. Будучи сформулированы как задачи ЦЛП, задачи о $\mathcal{X}$ -упаковке и $\mathcal{X}$ -покрытии образуют пару двойственных задач. Интерес представляют графы, в которых отсутствует разрыв двойственности, то есть те, в которых $\mu_{\mathcal{X}}(G) = \beta_{\mathcal{X}}(G)$. Это свойство может способствовать эффективному решению этих задач для таких графов.

Цель настоящей работы — описать расщепляемые графы и графы, полученные из расщепляемых с помощью замены вершин кографами, в которых выполняется равенство чисел μ_{P_4} и β_{P_4} .

Некоторые обозначения

Обозначим $V(G)$ множество вершин графа G , а $|G|$ — число вершин в нём. Окрестность вершины v будем обозначать $N(v)$. Будем обозначать $N[v] = N(v) \cup \{v\}$.

Используются стандартные обозначения P_n и C_n для простых путей и простых циклов соответственно.

Далее введём специфические обозначения для некоторых конкретных графов.

Граф *house* — это дополнение графа P_5 .

Граф *rising sun* — это расщепляемый граф, клика которого состоит из 4 вершин, а независимое множество — из 3 вершин. Каждая вершина независимого множества смежна ровно с двумя вершинами клики. Две вершины клики имеют степень 4, а остальные две имеют степень 5. Граф *co-rising sun* является дополнением графа *rising sun*.

Граф *net* — это расщепляемый граф, клика и независимое множество которого состоят из 3 вершин. Каждая вершина клики смежна ровно с одной вершиной независимого множества, каждая вершина независимого множества смежна ровно с одной вершиной клики. Граф S_3 является дополнением графа *net*.

Граф A получен из графа C_4 добавлением двух несмежных вершин. Каждая из них смежна с одной вершиной цикла, причём вершины их окрестностей являются смежными. Граф *co-A* является дополнением A .

Граф *parapluie* получен из графа P_4 заменой одной из его вершин степени 2 графом P_4 . Граф *parachute* является дополнением графа *parapluie*.

Граф $2P_4$ состоит из двух компонент связности, каждая из которых изоморфна P_4 . Граф *co-2P4* является его дополнением.

Зеркально-расщепляемые графы и их расширения

Назовём граф *зеркально-расщепляемым*, если существует такое разбиение множества его вершин на подмножества K_1, K_2, L_1, L_2 , что:

1. $K_1 \cup K_2$ формирует клику в G , а $L_1 \cup L_2$ является независимым множеством G ;
2. для любого $t \in \{1, 2\}$ для любых $x, y \in K_t$ выполняется $N[x] \subseteq N[y]$ или $N[y] \subseteq N[x]$;
3. для любого $t \in \{1, 2\}$ для любых $x, y \in L_t$ выполняется $N(x) \subseteq N(y)$ или $N(y) \subseteq N(x)$.

Теорема 1. *Следующие утверждения равносильны для графа G :*

- G — расщепляемый граф и $\mu_{P_4}(G) = \beta_{P_4}(G)$;
- G не содержит порожденных подграфов, изоморфных графам $C_4, 2P_2, C_5, rising\ sun, co-rising\ sun, S_3, net$;
- G — зеркально-расщепляемый граф.

Операция замены графом H вершины x состоит в следующем:

1. Эта вершина удаляется из графа.
2. К графу добавляется несколько новых вершин, соединённых между собой так, что они порождают подграф, изоморфный H .
3. Каждая новая вершина соединена ребром со всеми вершинами $N(x)$ в исходном графе.

Будем называть *расширением* графа G граф, полученный из G заменой некоторых его вершин произвольными кографами.

Теорема 2. *Следующие утверждения равносильны для графа G :*

- G — расширение расщепляемого графа и $\mu_{P_4}(G) = \beta_{P_4}(G)$;
- G не содержит порожденных подграфов, изоморфных графам $P_5, house, C_5, rising\ sun, co-rising\ sun, S_3, net, A, co-A, parapluie, parachute, 2P_4, co-2P_4$;
- G — расширение зеркально-расщепляемого графа.

Работа выполнена при поддержке РФФИ (проекты № 16-31-00109-мол-а, 17-01-00710-а), гранта Президента РФ МК-4819.2016.1 и Лаборатории Алгоритмов и Технологий Анализа Сетевых Структур Научного Исследовательского Университета Высшей Школы Экономики.

СПИСОК ЛИТЕРАТУРЫ

- [1] Földes S., Hammer P.L. Split graphs // Proceedings of 8th South-Eastern Conference on Combinatorics, graph theory, and computing, Baton Rouge, Louisiana. — 1977. — P. 311–315.
- [2] Hell P. Graph packing // Electronic Notes in Discrete Mathematics. — 2000. — Vol. 5 — P. 170–173.

- [3] Yuster R. Combinatorial and computational aspects of graph packing and graph decomposition // Computer Science Review. — 2007. — Vol. 1. — P. 12–26.

О ПОЛИНОМИАЛЬНОЙ РАЗРЕШИМОСТИ ПРОБЛЕМЫ ЭКВИВАЛЕНТНОСТИ ПРОГРАММ В ПЕРЕГОРОДЧАТЫХ МОДЕЛЯХ НАД ПРОГРЕССИВНЫМИ ПОЛУГРУППАМИ

Молчанов Андрей Эрикович, Подымов Владислав Васильевич

МГУ имени М. В. Ломоносова, e-mail: valdus@yandex.ru

Проблема эквивалентности программ формулируется так: выяснить, имеют ли две программы схожие (эквивалентные) поведения. В [1] предложен алгоритм полиномиального сведения проблемы эквивалентности в перегородчатых моделях программ с процедурами к двум проблемам в моделях программ без процедур с той же семантикой программных операторов: эквивалентности и совместного останова (в терминах [1] — непустоты пересечения). Проблема совместного останова формулируется так: выяснить, существует ли общий контекст работы программ, при котором обе программы успешно завершают выполнение. Эта проблема, насколько нам известно, ранее никем не исследовалась для нетривиальных моделей программ (отличных от конечных автоматов [2]). Нами предлагается метод решения этой проблемы, позволяющий с учётом результатов [1], [3] получить описание полиномиальных алгоритмов решения проблемы эквивалентности для широкого класса перегородчатых моделей программ.

Считаем заданными четыре конечных алфавита: операторов $\mathfrak{O}$, логических условий $\mathfrak{L}$, вызовов (процедур) $\mathfrak{C}$ и возвратов (из процедур) $\mathfrak{R}$. Введём также алфавит действий $\mathfrak{A} = \mathfrak{O} \cup \mathfrak{C} \cup \mathfrak{R}$. Цепочка — это слово в алфавите $\mathfrak{A}$. О-слово — это слово в алфавите $\mathfrak{O}$. Запись $\mathfrak{B}(M)$ обозначает перегородчатую модель программ с процедурами, описанную далее, над моноидом M , порождённым множеством операторов: M — полугруппа с операцией композиции $*$, каждый элемент m которой может быть представлен в виде конечной композиции операторов ($m = o_1 * \dots * o_k = [o_1 \dots o_k]$); $[\lambda]$ — нейтральный элемент M (здесь λ — пустое слово).

Процедура — это конечный ориентированный размеченный граф следующего вида. В графе выделено две вершины: вход и выход. Остальные вершины делятся на преобразователи и процедурные вершины. Каждый преобразователь v помечен оператором $O(v)$. Каждая процедурная вершина u помечена вызовом $C(u)$, возвратом $R(u)$ и натуральным числом $N(u)$ (номером вызываемой процедуры). Вход и выход не помечены. Во вход не входит ни одной дуги. Из выхода не исходит ни одной дуги. Дуги имеют вид $v \xrightarrow{\ell} v'$, где ℓ — метящее дугу логическое условие. Различные дуги, исходящие из одной вершины, помечены различными условиями.

Программа — это конечный набор процедур, упорядоченный натуральными числами. $\pi[i]$ — это i -я процедура программы π .

Выполнение процедуры $\pi[i]$ в контексте $\mu : \mathfrak{A}^* \rightarrow \mathfrak{L}$ состоит в обходе вершин графа $\pi[i]$. На каждом шаге обхода определена текущая вершина v и текущая цепочка h ; в начале обхода v — вход и $h = \lambda$. Если v — выход, то обход процедуры успешно завершается, и цепочка h объявляется результатом обхода. В противном случае определяется новая цепочка g , после чего выбирается дуга $v \xrightarrow{\mu(g)} v'$, и обход продолжается в вершине v' с цепочкой g . Если из v не исходит дуги с требуемой меткой, то обход завершается неуспешно. Если v — вход, то $g = h$. Если v — преобразователь, то $g = h O(v)$. Если v — процедурная вершина, то g определяется так: если π не содержит процедуры с номером $N(v)$, то обход завершается неуспешно; процедура $\pi[N(v)]$ выполняется в контексте μ' , таком что $\mu'(u) = \mu(g C(v) u)$ для любой цепочки u ; если w — результат выполнения $\pi[N(v)]$, то $g = w R(v)$; если выполнение $\pi[N(v)]$ неуспешно, то обход $\pi[i]$ завершается неуспешно. Бесконечное выполнение процедуры $\pi[i]$ неуспешно. Выполнение программы π — это выполнение процедуры $\pi[1]$.

Процедурное разбиение цепочки h над M — это пара, содержащая последовательность вызовов и возвратов $(x_1, \dots, x_m)$ и последовательность элементов M $([h_0], \dots, [h_m])$, такие что $h = h_0 x_1 h_1 x_2 \dots x_m h_m$. $\Phi(M)$ — это множество всех контекстов μ , таких что $\mu(h_1) = \mu(h_2)$ для любых цепочек h_1, h_2 с равными процедурными разбиениями над M . Программы π_1, π_2 эквивалентны в модели $\mathfrak{B}(M)$ (коротко: $\pi_1 \sim_M \pi_2$), если для любого контекста μ из $\Phi(M)$ либо выполнения обеих программ неуспешны, либо оба выполнения успешны и процедурные разбиения результатов этих выполнений над M совпадают. Исследуемая нами вариация проблемы эквивалентности формулируется так: для заданных программ π_1, π_2 и заданного моноида M проверить соотношение $\pi_1 \sim_M \pi_2$.

Моноид M прогрессивен, если для любых о-слов h, g верна импликация $[h] = [hg] \Rightarrow g = \lambda$. Элемент m_2 моноида M достижим из элемента m_1 (коротко: $m_1 \prec m_2$), если $m_1 \neq m_2$ и $\exists m : m_1 * m = m_2$. Критериальная система $(W, w^+, w^*, U, \varphi)$ для моноида M состоит из (критериального) моноида W с нейтральным элементом e и операцией $\circ$, его элементов w^+, w^* и подмоноида U и гомоморфизма $\varphi : M \times M \rightarrow U$, таких что: $m_1 = m_2 \Leftrightarrow w^+ \circ \varphi(m_1, m_2) \circ w^* = e$; любое уравнение $X \circ w \circ w^* = e$ имеет не более одного решения относительно X в классе смежности $w^+ \circ U$; если $w^+ \circ \varphi(m_1, m_2) = w^+ \circ \varphi(m_3, m_4)$, то $m_i \prec m_{3-i} \Leftrightarrow m_{2+i} \prec m_{5-i}$ для $i \in \{1, 2\}$. Далее потребуется такой набор ограничений (*) на моноид M : он прогрессивен; для него существует критериальная система; соотношение $[h_1] \prec [h_2]$ можно проверить за время, полиномиальное относительно размеров h_1, h_2 ; соотношения $w^+ \circ w_{12} = w^+ \circ w_{34}$ и $w^+ \circ w_{12} \circ w^* = w^+ \circ w_{34} \circ w^*$, где $w_{12} = \varphi([h_1], [h_2])$ и $w_{34} = \varphi([h_3], [h_4])$, можно проверить за время, полиномиальное относительно размеров h_1, h_2 ,

h_3, h_4 . Записью $\mathfrak{P}(M)$ обозначим модель программ $\mathfrak{B}(M)$ без процедурных вершин.

Теорема. Если моноид M удовлетворяет условиям (*), то проблема совместного останова программ в модели $\mathfrak{P}(M)$ полиномиально разрешима.

Следствие. Если моноид M удовлетворяет условиям (*), то проблема эквивалентности программ в модели $\mathfrak{B}(M)$ полиномиально разрешима.

Справедливость следствия обосновывается: полиномиальной сводимостью проблемы эквивалентности в $\mathfrak{B}(M)$ к проблемам эквивалентности и совместного останова в $\mathfrak{P}(M)$ [1]; полиномиальной разрешимостью проблемы эквивалентности в $\mathfrak{P}(M)$ [3]; основной теоремой данной работы.

Алгоритм, обосновывающий теорему, строит вершины (v_1, v_2, w) графа Γ , описывающие промежуточные состояния совместного выполнения программ, в котором ими достигнуты вершины v_1, v_2 и накоплены о-слова h_1, h_2 , такие что $w = w^+ \circ \varphi([h_1], [h_2])$. Применяя технику, схожую с используемой в [3], можно описать способ выбора программы, совершающей шаг обхода на каждом шаге совместного выполнения хотя бы в одном контексте из $\Phi(M)$, такой что: по вершине (v_1, v_2, w) можно быстро определить все вершины, описывающие следующий шаг совместного выполнения; достаточно построить лишь полиномиально много вершин графа Γ , чтобы установить осуществимость или неосуществимость совместного останова программ; построение каждой вершины полиномиально по времени.

Примеры моноидов, обладающих свойствами (*) (включая произвольные частично-коммутативные моноиды), можно найти, например, в [3, 4].

Работа выполнена при поддержке РФФИ (проект № 15-01-05742 А).

СПИСОК ЛИТЕРАТУРЫ

- [1] Молчанов А. Э. Разрешимость эквивалентности в двухпараметрических перегорожденных моделях программ // Моделирование и анализ информационных систем. — 2014. — Т. 21, № 4. — С. 104–115.
- [2] Rutledge J. D. On Ianov's program schemata // Journal of the ACM. — 1964. — V. 11, N. 1. — P. 29–35.
- [3] Захаров В. А. Быстрые алгоритмы разрешения эквивалентности пропозициональных операторных программ на упорядоченных полугрупповых шкалах // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2014. — № 4. — С. 29–35.
- [4] Захаров В. А. Быстрые алгоритмы разрешения эквивалентности операторных программ на уравновешенных шкалах // Математические вопросы кибернетики. — 1998. — Т. 7. — С. 303–324.

ОБ АБСТРАКТНОЙ ХАРАКТЕРИЗАЦИИ ГИПЕРГРАФИЧЕСКИХ АВТОМАТОВ

Молчанов Владимир Александрович¹, Хворостухина Екатерина
Владимировна²

¹ Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского,
e-mail: v.molchanov@inbox.ru

² Саратовский Государственный Технический Университет имени Гагарина Ю. А., e-mail:
kalyanew2007@rambler.ru

Основные понятия

В работе исследуется проблема абстрактной характеристики универсальных гиперграфических автоматов, которая формулируется следующим образом: при каких условиях абстрактный автомат $A = (X, S, Y, \delta, \lambda)$ будет изоморфен универсальному автомату $\text{Atm}(H_1, H_2)$ над некоторыми гиперграфами H_1, H_2 ?

Согласно [1] гиперграфом называется алгебраическая система $H = (X, L)$, где X — непустое множество вершин гиперграфа и L — семейство некоторых подмножеств множества X , называемых ребрами гиперграфа. Гиперграф $H = (X, L)$ называется эффективным, если любая его вершина принадлежит некоторому ребру этого гиперграфа.

Пусть p — некоторое натуральное число. Гиперграф H будем называть гиперграфом с p -определимыми ребрами, если в каждом ребре этого гиперграфа найдется по крайней мере $p + 1$ вершина и, с другой стороны, любые p вершин этого гиперграфа содержатся не более, чем в одном ребре.

Например, если рассматривать плоскости [2] как гиперграфы, вершинами которых являются точки, а ребрами — прямые этих плоскостей, то любая проективная плоскость и любая аффинная плоскость с числом точек более четырех являются эффективными гиперграфами с 2-определимыми ребрами.

Следуя [3], под автоматом будем понимать алгебраическую систему $A = (X, S, Y, \delta, \lambda)$, состоящую из множества состояний X , полугруппы входных символов S , множества выходных символов Y , функции переходов $\delta : X \times S \rightarrow X$ и выходной функции $\lambda : X \times S \rightarrow Y$, таких что для любых $x \in X$ и $s, t \in S$ выполняются условия $\delta(x, st) = \delta(\delta(x, s), t)$, $\lambda(x, st) = \lambda(\delta(x, s), t)$.

Изоморфизмом автомата $A = (X, S, Y, \delta, \lambda)$ на автомат $A_1 = (X_1, S_1, Y_1, \delta_1, \lambda_1)$ называется упорядоченная тройка $\gamma = (f, \pi, g)$ биекций $f : X \rightarrow X_1$, $\pi : S \rightarrow S_1$ и $g : Y \rightarrow Y_1$, сохраняющих алгебраическую структуру таких автоматов, т. е. π является изоморфизмом полугруппы S на полугруппу S_1 и для любых значений $s, t \in S, x \in X$ выполняются условия $\pi(s \cdot t) = \pi(s) \cdot \pi(t)$, $f(\delta(x, s)) = \delta_1(f(x), \pi(s))$ и $g(\lambda(x, s)) = \lambda_1(f(x), \pi(s))$.

Автомат $A = (X, S, Y, \delta, \lambda)$ будем называть гиперграфическим автоматом, если множество состояний X и множество выходных символов Y наделены

такими структурами гиперграфов $H_X = (X, L_X)$ и $H_Y = (Y, L_Y)$, что при каждом фиксированном входном сигнале $s \in S$ преобразование $\delta_s : X \rightarrow X$ является эндоморфизмом гиперграфа H_X и отображение $\lambda_s : X \rightarrow Y$ — гомоморфизмом гиперграфа H_X в гиперграф H_Y . Такие автоматы будем также обозначать $A = (H_X, S, H_Y, \delta, \lambda)$.

Для гиперграфов $H_X = (X, L_X)$, $H_Y = (Y, L_Y)$ через $S(H_X, H_Y)$ обозначим полугруппу $\text{End}H_X \times \text{Hom}(H_X, H_Y)$ с бинарной операцией, определяющейся по правилу: $(\varphi, \psi)(\varphi_1, \psi_1) = (\varphi\varphi_1, \varphi\psi_1)$ для пар $(\varphi, \psi), (\varphi_1, \psi_1) \in \text{End}H_X \times \text{Hom}(H_X, H_Y)$.

Важный пример гиперграфического автомата дает алгебраическая система $\text{Atm}(H_X, H_Y) = (H_X, S(H_X, H_Y), H_Y, \delta', \lambda')$ с функциями $\delta'(x, (\varphi, \psi)) = \varphi(x)$, $\lambda'(x, (\varphi, \psi)) = \psi(x)$ (где $x \in X, (\varphi, \psi) \in S(H_X, H_Y)$). Легко проверить, что $\text{Atm}(H_X, H_Y)$ удовлетворяет следующему универсальному свойству: для любого гиперграфического автомата $A = (H_X, S, H_Y, \delta, \lambda)$ существует такой гомоморфизм $\pi : S \rightarrow S(H_X, H_Y)$, что упорядоченная тройка $\gamma = (\Delta_X, \pi, \Delta_Y)$ является гомоморфизмом A в $\text{Atm}(H_X, H_Y)$. По этой причине такой гиперграфический автомат $\text{Atm}(H_X, H_Y)$ называется универсальным гиперграфическим автоматом над гиперграфами H_X, H_Y .

Пусть X — произвольное непустое множество, p — натуральное число и R — $(p+1)$ -арное отношение на множестве X . Согласно [4] отношение R называется p -эквивалентностью на множестве X , если оно удовлетворяет следующим условиям:

(T_1) $(x, \dots, x, x) \in R$ для любого $x \in X$;

(T_2) для любых $1 \leq i_1, \dots, i_p, i_{p+1} \leq p+1$,

$$(x_1, \dots, x_p, x_{p+1}) \in R \implies (x_{i_1}, \dots, x_{i_p}, x_{i_{p+1}}) \in R;$$

(T_3) для любых попарно различных элементов $x_1, \dots, x_{p-1}, x_p \in X$,

$$(x, x_1, \dots, x_{p-1}, x_p), (x_1, \dots, x_{p-1}, x_p, y) \in R \implies (x, x_1, \dots, x_{p-1}, y) \in R.$$

При этом p -эквивалентность R называется квазиполной, если выполняется условие

(T_4) для любых элементов $x_1, \dots, x_p \in X$, удовлетворяющих условию $(x_1, \dots, x_p, x_p) \in R$, найдется такой отличный от всех них элемент $x \in X$, что $(x_1, \dots, x_p, x) \in R$.

Главный результат

Для автомата $A = (X, S, Y, \delta, \lambda)$ на множествах X, Y определим канонические $(p+1)$ -арные отношения R_X, R_Y по следующим формулам: упорядоченный набор $(a_1, a_2, \dots, a_{p+1}) \in X^{p+1}$ (соответственно $(a_1, a_2, \dots, a_{p+1}) \in Y^{p+1}$) в том и только том случае принадлежит отношению R_X (соответственно отношению R_Y), если для любых различных элементов $x_1, x_2, \dots, x_{p+1} \in X$ найдется такой символ $s \in S$, что для каждого $i = \overline{1, p+1}$ выполняется равенство $\delta(x_i, s) = a_i$ (соответственно $\lambda(x_i, s) = a_i$).

Теорема 1. Автомат $A = (X, S, Y, \delta, \lambda)$ в том и только том случае будет изоморфен универсальному гиперграфическому автомату $\text{Atm}(H_1, H_2)$ над некоторыми эффективными гиперграфами с p -определимыми ребрами H_1 и H_2 , если выполняются следующие условия:

- 1) для различных $s, t \in S$, найдется такой элемент $x \in X$, что либо $\delta(x, s) \neq \delta(x, t)$, либо $\lambda(x, s) \neq \lambda(x, t)$;
- 2) канонические отношения R_X и R_Y автомата A являются квазиполными p -эквивалентностями соответственно на множествах X и Y ;
- 3) если для отображений $f_1 : X \rightarrow X$, $f_2 : X \rightarrow Y$ при любых значениях $x_1, x_2, \dots, x_{p+1} \in X$, удовлетворяющих условию $(x_1, x_2, \dots, x_{p+1}) \in R_X$, существуют такие символы $s, t \in S$, что $f_1(x_i) = \delta(x_i, s)$ и $f_2(x_i) = \lambda(x_i, t)$ для всех $i = \overline{1, p+1}$, то найдется такой символ $a \in S$, что $f_1(x) = \delta(x, a)$ и $f_2(x) = \lambda(x, a)$ для всех $x \in X$.

СПИСОК ЛИТЕРАТУРЫ

- [1] Bretto A. Hypergraph theory. An Introduction. — Cham. : Springer, 2013. — 133 p. DOI: 10.1007/978-3-319-00080-0.
- [2] Хартсхорн Р. Основы проективной геометрии. — М. : Мир, 1970. — 161 с.
- [3] Плоткин Б. И., Гринглаз Л. Я., Гварамия А. А. Элементы алгебраической теории автоматов. — М. : Высшая школа, 1994. — 192 с.
- [4] Молчанов А. В. Об определяемости гиперграфических автоматов их выходными функциями // Теоретические проблемы информатики и ее приложений. Саратов. — 1998. — Вып. 2. — С. 74–84.

СЛОЖНОСТЬ ПРОБЛЕМЫ «ВЫПОЛНИМОСТЬ» ДЛЯ БИНАРНЫХ ПРОГРАММ

Мубаракзянов Рустам Гамирович

Казанский (Приволжский) федеральный университет, e-mail: rustam.mubarakzjanov@ekpfu.ru

Вычислительная модель, называемая бинарной программой, хорошо известна [1]. Напомним основные определения.

Детерминированной бинарной программой (БР) P на множестве переменных $X = \{x_0, \dots, x_{n-1}\}$ называется ориентированный ациклический граф с одной начальной вершиной и двумя финальными вершинами. Одна из финальных вершин помечена 0, другая — 1 (назовем ее принимающей). Каждая нефинальная вершина этого графа помечена переменной из X , и из нее выходят ровно две дуги, помеченные 0 и 1. Процесс вычисления детерминированной БР при фиксировании значений переменных из X сводится к следующему. Вычисление начинается в корне s программы. Если переменная, которой помечен s , имеет значение $a \in \{0, 1\}$, то осуществляется переход в сына s по дуге,

помеченной a . Из этой вершины переход осуществляется в зависимости от значения помечающей ее переменной. Так как путь, соответствующий значениям переменных, выбирается однозначно, каждому набору значений переменных можно сопоставить пометку той финальной вершины, в которую приводит вычисление. Эта пометка является значением вычисляемой функции.

Если в определении бинарной программы добавить возможность наличия недетерминированных вершин, т. е. не помеченных никакой переменной, или вероятностных вершин, т. е. помеченных случайными переменными, принимающими значения 0 и 1 с вероятностью $1/2$, получим определения недетерминированной и вероятностной программы соответственно. Вероятностная программа P определяет функцию $c_P : \{0, 1\}^n \rightarrow [0, 1]$, $c_P(x)$ — вероятность того, что P , имея на входе x , достигает принимающую вершину. Программа P вычисляет функцию h , если $c_P(x) > 1/2$ для $h(x) = 1$, и $c_P(x) < 1/2$ для $h(x) = 0$, т. е. вероятность, что P выдает $h(x)$, больше $1/2$ для любого набора значений переменных x . Если эта вероятность больше $1 - \varepsilon$ для некоторого ε , $0 \leq \varepsilon < 1/2$, то вычисление называется вычислением с ограничением на ошибку (ε — ошибка вычисления).

Определим сложность программы P как число ее вершин. В целях получения соотношений между различными классами сложности рассматриваются ограниченные классы бинарных программ [1]. k раз читающая бинарная программа (BPk) — бинарная программа, которая на любом пути вычисления каждую переменную читает не более k раз. Один раз читающая BP ($BP1$) называется упорядоченной (обозначается $OBDD$), если переменные читаются в определенном порядке. $OBDD$ интересны в связи с возможностью их практического использования [2]. Программа BPk называется $kOBDD$, если ее можно разбить на k слоев так, что переменные в каждом слое читаются не более одного раза в соответствии с одним и тем же порядком.

Обозначим классы функций, вычислимых детерминированными, недетерминированными, вероятностными с ограничением на ошибку и вероятностными общего вида бинарными программами полиномиальной сложности $P-BP$, $NP-BP$, $BPP-BP$ и $PP-BP$ соответственно. Для ограниченных классов бинарных программ в обозначениях классов сложности суффикс “ $-BP$ ” заменим соответствующим сокращением. Известны соотношения между классами сложности для $OBDD$ [3, 4].

Классы бинарных программ полиномиальной сложности будем обозначать так же, как и соответствующие классы сложности. Например, вероятностные (без ограничения на ошибку) $OBDD$ полиномиального размера обозначим как $PP-OBDD$. Из контекста будет ясно, для чего используются обозначения: для бинарных программ или для класса сложности.

Назовем бинарную программу уровневой, если для любой ее нефинальной вершины v все пути от корня до v имеют одинаковую длину. Такая програм-

ма может быть разбита на уровни: каждый уровень содержит нефинальные вершины, одинаково удаленные от корня. Шириной уровневой программы называется максимальное число вершин на одном уровне. Если рассматривать BP , ширина которых ограничена некоторой функцией $\omega(n)$, обозначим их $BP^{\omega(n)}$.

При обобщениях $P-OBDD$ важно, чтобы полученные бинарные программы сохраняли свойства, позволяющие эффективно работать с ними. Важной проблемой в теории сложности является сложность задачи «Выполнимость».

Для BP полиномиального размера в классе $NP-BP1$ тест на «Выполнимость» полиномиален. Следовательно, аналогичное утверждение верно $P-BP1$, $NP-OBDD1$. Этот тест осуществляет проход по графу программы в глубину. Так как каждая переменная читается не более одного раза, можно не учитывать значения переменных. Если рассматривать BP константной ширины, то ограничение на полиномиальный размер выполнится.

Обобщим рассмотренные классы сложности.

Класс $P-BP1$ строго включается в $P-BP2$. Для последнего класса, даже для $P-2OBDD^3$, проблема «Выполнимость» NP -полна [5].

Теорема. Для любого целого k и для любой целочисленной функции $\omega(n)$ справедливо следующее $PP-kOBDD^{\omega(n)} \subseteq PP-OBDD^{\omega(n)^{2k}}$.

Идея доказательства состоит в замене наборов состояний уровней исходной $kOBDD$ всех k слоев, находящихся на равном удалении от начала слоя, на один уровень состояний $OBDD$.

Проблема «Выполнимость» NP -полна для $BPP-OBDD$ [6] и, следовательно, для $PP-OBDD$.

СПИСОК ЛИТЕРАТУРЫ

- [1] Wegener I. Branching programs and binary decision diagrams: theory and applications. — SIAM monographs on discrete mathematics and applications. — Philadelphia: SIAM, 2000. — 408 p.
- [2] Bryant R. E. Graph-based algorithms for Boolean function manipulation // IEEE Transact. on Comput. — 1986. — V. 35. — P. 677–691.
- [3] Ablayev F. Randomization and nondeterminism are incomparable for ordered read-once branching programs // Proc. ICALP'97, LNCS 1256. — Springer, 1997. — P. 195–202.
- [4] Ablayev F., Karpinski M., Mubarakzjanov R. On BPP versus $NP \cup coNP$ for ordered read-once branching programs // Theoret. Comput. Sci. — 2001. — V. 264. — P. 127–137.
- [5] Meinel Ch., Theobald T. Algorithms and data structures in VLSI design. — Berlin. : Springer. — 1998. — 267 P.

- [6] Agrawal M., Thierauf T. The satisfiability problem for probabilistic ordered branching programs // Theory Comput. Systems (TOCS). — 2001. — V. 34. — P. 471–487.

О СВОЙСТВАХ НЕКОТОРЫХ ФУНКЦИЙ, СОХРАНЯЮЩИХ ЦЕНТРАЛЬНЫЕ ПРЕДИКАТЫ, В МНОГОЗНАЧНОЙ ЛОГИКЕ

Нагорный Александр Степанович

МГУ имени М. В. Ломоносова, e-mail: anagorny@list.ru

Основные определения

Пусть $k \geq 3$, $E_k = \{0, 1, \dots, k-1\}$. Множество всех конечноместных функций на E_k обозначим через P_k . Элементы множества P_k будем называть k -значными функциями или функциями k -значной логики. Определения операции суперпозиции, замкнутого класса, предполного (максимального) класса, предиката и других основных понятий можно найти, например, в [1].

Предикат, заданный на E_k , назовем *центральным*, если он является вполне рефлексивным, вполне симметричным, отличен от тождественно истинного предиката, и существует такое нетривиальное подмножество $\Delta = \{\delta_1, \delta_2, \dots, \delta_r\}$ множества E_k (называемое *центром*), что предикат является истинным для любого набора, пересекающегося с центром. Класс k -значных функций, сохраняющих минимальный (по числу наборов) 2-местный центральный предикат с центром Δ будем обозначать через C_Δ или $C_{\delta_1, \delta_2, \dots, \delta_r}$, а для класса k -значных функций, сохраняющих одноместный центральный предикат с центром Δ , будем использовать традиционное обозначение T_Δ или $T_{\delta_1, \delta_2, \dots, \delta_r}$.

Обозначим также через $M_{\alpha_1, \alpha_2, \dots, \alpha_k}$ класс k -значных функций, монотонных относительно линейного порядка $\alpha_1 \prec \alpha_2 \prec \dots \prec \alpha_k$, а через $U_{\Delta_1, \Delta_2, \dots, \Delta_l}$ — класс k -значных функций, сохраняющих нетривиальное ($1 < l < k$) разбиение $E_k = \Delta_1 \cup \Delta_2 \cup \dots \cup \Delta_l$.

Наконец, буквой B обозначим *класс Слупецкого* — класс всех функций из P_k , которые либо имеют не более одной существенной переменной, либо принимают не более $k-1$ различных значений.

При любом $k \geq 2$ все классы k -значных функций, перечисленные выше, являются замкнутыми и предполными в P_k (см. [2]). Также отметим, что из теоремы 1 из [3] следует, что с ростом k почти все предполные в P_k классы являются классами функций, сохраняющих центральные предикаты (не менее чем 2-местные).

Наконец, пусть $Im(f)$ есть множество всех значений, которые принимает функция f .

Мы будем пользоваться следующим удобным обозначением. Для любых целых s и t положим $\overline{s, t} = \begin{cases} s, s+1, \dots, t, & \text{если } s \leq t; \\ s, s-1, \dots, t, & \text{иначе.} \end{cases}$

Основные результаты

Всюду далее $k \geq 3$.

Теорема 1. Для любых непустых множеств Δ и E , удовлетворяющих условиям $\Delta \cap E = \emptyset$ и $\Delta \cup E \subset E_k$, справедливо вложение $C_\Delta \cap T_E \subseteq T_{\Delta \cup E}$.

Теорема 2. Пусть $\emptyset \neq E \subset E_k$. Тогда

$$T_E \cap M_{\overline{0,k-1}} \subseteq T_{\overline{0,b}} \cap T_{\overline{a,k-1}} \cap T_{\overline{a,b}}, \quad \text{где } a = \min_{\sigma \in E} \{\sigma\}, \quad b = \max_{\sigma \in E} \{\sigma\}.$$

Теорема 3. Для любого нетривиального разбиения $D = \{\Gamma, \Delta, E\}$ множества E_k выполнено

$$C_\Delta \cap T_{\Gamma \cup E} \cap M_{\Gamma, \Delta, E} \subseteq U_{\Gamma, \Delta \cup E} \cap U_{\Gamma \cup \Delta, E}$$

(здесь $M_{\Gamma, \Delta, E}$ обозначает произвольный класс функций, монотонных относительно любого линейного порядка на E_k , согласно которому $\gamma \prec \delta \prec \varepsilon$ при всех $\gamma \in \Gamma, \delta \in \Delta, \varepsilon \in E$).

Теорема 4. Пусть $D = \{\Delta, E\}$ — нетривиальное разбиение множества E_k . Если $\emptyset \neq E' \subseteq E$, то

$$T_{E'} \cap U_{\Delta, E} \subseteq T_E.$$

Теорема 5. Пусть функция $f \in P_k$ удовлетворяет условию $f \in C_0$. Тогда $f \in T_0$ или существует $\varepsilon \in E_k \setminus \{0\}$ такое, что $\text{Im}(f) \subseteq \{0, \varepsilon\}$.

Теорема 6. Пусть для некоторого целого α ($1 \leq \alpha \leq k-2$) и некоторой функции $f \in P_k$ выполнено $f \in M_{\overline{0,k-1}} \cap C_{\overline{0,\alpha-1}} \cap T_{\overline{\alpha,k-1}}$. Тогда $f \in T_\alpha$ или $\alpha \notin \text{Im}(f)$.

Теорема 7. Пусть мощность множества $\Delta \subseteq E_k$ удовлетворяет неравенствам $1 \leq |\Delta| \leq k-2$ и $\sigma \in E_k \setminus \Delta$. Если $f \in C_\Delta \cap U_{\{\sigma\}, E_k \setminus \{\sigma\}}$, то $f \in T_{\Delta \cup \{\sigma\}}$ или $\sigma \notin \text{Im}(f)$.

Теорема 8. Пусть $f \in P_k$. Если $f \in \bigcap_{\sigma=1}^{k-1} C_\sigma$, то $f \in T_0$ или $0 \notin \text{Im}(f)$.

Теорема 9. Пусть $t \geq 2$ и множества $\Delta_1, \Delta_2, \dots, \Delta_t \subseteq E_k$ таковы, что $\bigcup_{i=1}^t (E_k \setminus \Delta_i) = E_k$ и при всех $i = 1, 2, \dots, t$ справедливо $|\Delta_i| = k-2$. Тогда

$$C_{\overline{1,k-2}} \cap B \subseteq \left(\bigcup_{i=1}^t C_{\Delta_i} \right) \cup T_{0,k-1}.$$

Отметим, что полученные результаты нельзя улучшить (в том смысле, что утверждения теорем перестают быть верными после удаления любого класса из пересечений, стоящих в левых частях включений). Кроме того, автор считает нужным сослаться на свою работу [4], где сформулированы некоторые другие универсальные (справедливые для всех k) свойства функций k -значной логики, сохраняющих центральные предикаты.

Работа выполнена при поддержке РФФИ (проекты №16-01-00593-а и №17-01-00782-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Марченков С. С. Функциональные системы с операцией суперпозиции. — М. : Физматлит, 2004. — 104 с.
- [2] Rosenberg I. G. Über die funktionale Vollständigkeit in den mehrwertigen Logiken // Rozprawy Československe Akad. Věd. N. 80. Praha: Řada Math. Přír. Věd., 1970. — P. 3–93.
- [3] Захарова Е. Ю., Кудрявцев В. Б., Яблонский С. В. О предполных классах в k -значных логиках // ДАН СССР. — 1969. — Т. 186, № 3. — С. 509–512.
- [4] Нагорный А. С. О некоторых пересечениях предполных классов многозначной логики, вложенных в классы C_0 и $C_{0,1,\dots,k-3}$ // Материалы Международного научного семинара «Дискретная математика и ее приложения в экономико-математическом моделировании и информационных технологиях» (Запорожье, 11–13 октября 2012 г.), 2012. — С. 51–52.

ЛЕММА ОБ ИЗОЛИРОВАНИИ: СПЕЦИАЛЬНЫЕ СЕМЕЙСТВА И СЛУЧАЙНОСТЬ

Останин Александр Михайлович

Московский физико-технический институт, e-mail: aleksandr.ostanin@phystech.edu

Пусть A — некоторое n -элементное множество, $\mathcal{F}$ — семейство подмножеств A . Для каждого элемента $x \in A$ вес $w(x)$ выбирается случайно из множества $\{1, 2, \dots, m\}$, а вес элемента $E \in \mathcal{F}$ определяется как $\sum_{x \in E} w(x)$. Если ровно

один элемент $\mathcal{F}$ имеет минимальный вес, то весовая функция w называется *изолирующей* для семейства $\mathcal{F}$. Лемма об изолировании утверждает, что при таких условиях вероятность того, что w — изолирующая функция, не меньше $(1 - \frac{1}{m})^n$ [1]. Далее эту вероятность будем называть *вероятностью изолирования*.

В данной работе мы рассматриваем вопросы, связанные с уточнением леммы для некоторых классов семейств, а также с изучением свойств изолирования семейств случайных подмножеств.

Теорема 1. Пусть $m = 2$, а $\mathcal{F}$ состоит из двухэлементных подмножеств n -элементного множества. Тогда количество изолирующих весовых функций для $\mathcal{F}$ не меньше чем $2(n - 2)$.

Доказательство теоремы 1. Назовем функцию *сильно изолирующей*, если минимальное ребро единственно и имеет вес 2. Докажем, что таких функций не меньше чем $2(n - 2)$, отсюда будет следовать и утверждение теоремы. Двухэлементные множества будем рассматривать как ребра в графе на n вершинах.

Пусть G — минимальный по количеству вершин граф, для которого сильно изолирующих функций меньше, чем $2(n - 2)$. Легко проверить, что тогда

$n > 4$. Тогда G не содержит изолированных вершин, т. к. удаление такой вершины не меняет вероятности изолирования. Также G не содержит вершины u степени $n - 1$, т. к. в противном случае имеется как минимум $2(n - 3)$ сильно изолирующие функции на графе без u , которые можно расширить до сильно изолирующей на всем графе, поставив в u вес 2, а также $(n - 1)$ сильно изолирующая функция, принимающая 1 ровно на u и еще одной вершине — в итоге имеем уже $3n - 7 \geq 2n - 2$ сильно изолирующих функций.

Пусть все степени вершин в G равны 1. Тогда граф является паросочетанием из $k = \frac{n}{2}$ ребер и имеет ровно $\frac{n}{2} \cdot 3^{\frac{n}{2}-1}$ сильно изолирующих функций, что не меньше $2(n - 2)$.

Обозначим $N(x)$ множество соседей вершины x . Выберем вершину u максимальной степени и v произвольную, не соединенную с u . Обозначим $B = N(u) \cap N(v)$, $A = N(u) \setminus B$, $C = N(v) \setminus B$, $D = V(G) \setminus (N(u) \cup N(v) \cup \{u, v\})$. В силу доказанного выше выполнено $|N(u) \cup N(v)| \geq 2$. Явно найдем нужное количество сильно изолирующих функций. В каждом пункте выпишем, какие вершины будут иметь вес 1, остальные будут иметь вес 2.

- $w(u) = w(x) = 1$ для некоторой $x \in A$.
- $w(u) = w(v) = w(x) = 1$ для некоторой $x \in A$.
- $w(v) = w(x) = 1$ для некоторой $x \in C$.
- $w(v) = w(u) = w(x) = 1$ для некоторой $x \in C$.
- $w(v) = w(x) = 1$ для некоторой $x \in B$.
- $w(u) = w(x) = 1$ для некоторой $x \in B$.
- $w(x) = w(y) = 1$, $x \in A \cup B \cup C$, $y \in D$, $(x, y) \in E(G)$.
- $w(x) = w(y) = w(u) = 1$, $x \in A \cup B \cup C$, $y \in D$, $(x, y) \notin E(G)$, $(y, u) \in E(G)$.
- $w(x) = w(y) = w(v) = 1$, $x \in A \cup B \cup C$, $y \in D$, $(x, y) \notin E(G)$, $(y, v) \in E(G)$.

Нетрудно видеть, что в каждом случае получаем сильно изолирующие функции. В первых 6 пунктах их в сумме $2(|A| + |B| + |C|)$, а в последних трех не меньше чем $|D| \cdot |A \cup B \cup C| \geq 2|D|$. Значит, в сумме сильно изолирующих функций не меньше чем $2(|A| + |B| + |C| + |D|) = 2(n - 2)$. **Теорема 1 доказана.**

Случайные семейства подмножеств

Рассмотрим модель, в которой семейство $\mathcal{F}$ из двухэлементных подмножеств выбирается случайно и $m = 2$. Таким образом, в графе на n вершинах с вероятностью p_n независимо выбирается каждое ребро, после этого каждой вершине равновероятно присваивается вес 1 или 2, и по таким расстановкам считается вероятность единственности минимального ребра. Вопрос: для каких последовательностей p_n можно утверждать, что с вероятностью стремящейся к 1 весовая функция неизолирующая для семейства $\mathcal{F}$?

Теорема 2. Если $p_n > 100 \frac{\log n}{n^2}$, то вероятность изолирования в построенном таким образом случайном графе стремится к нулю.

Доказательство теоремы 2.

Лемма. Пусть p_n — вероятность появления каждого ребра в графе на n вершинах. Тогда матожидание количества независимых множеств в нем не больше

$$n \cdot 2^{0.87n} + 2^n \cdot e^{-p_n \cdot \frac{n^2}{32}}.$$

Доказательство леммы.

Матожидание количества независимых множеств найдем, используя линейность матожидания: $\sum_{k=0}^n \binom{n}{k} \cdot (1-p_n)^{\binom{k}{2}}$. Рассмотрим сначала $k < \frac{n}{4}$. Пусть $l = \frac{n}{4}$. Тогда

$$\binom{n}{k} \leq \binom{n}{l} \leq \frac{n^l}{l!} \leq \left(\frac{ne}{l}\right)^l = 2^{l \log \frac{n}{l} + l \log e} = 2^{l \log 4e} \leq 2^{n \cdot 0.87}.$$

Значит, часть суммы при $k < \frac{n}{4}$ можно оценить сверху величиной $n \cdot 2^{0.87n}$.

При $k \geq \frac{n}{4}$ каждое слагаемое вида $(1-p_n)^{\binom{k}{2}}$ не больше, чем то же слагаемое при $k = \frac{n}{4}$. Значит, используя равенство $\sum_{i=1}^n \binom{n}{i} = 2^n$, часть суммы при $k \geq \frac{n}{4}$ можно оценить сверху величиной

$$2^n \cdot (1-p_n)^{\binom{\frac{n}{4}}{2}} \leq 2^n \cdot e^{-p_n \cdot \binom{\frac{n}{4}}{2}} \leq 2^n \cdot e^{-p_n \cdot \frac{n^2}{32}}.$$

Лемма доказана.

Во-первых, если минимальное ребро не будет иметь вес 2, то единицы в графе образуют независимое множество. Значит, вероятность такой ситуации равна матожиданию количества независимых множеств в случайном графе, деленном на 2^n (так как функция ставит единицы в точности в вершины, входящих в выбранное независимое множество). Вероятность такого события по лемме не больше $n \cdot 2^{-0.13n} + e^{-p_n \cdot \frac{n^2}{32}}$. Первое слагаемое стремится к 0. Показатель степени не превосходит $-100 \cdot \frac{\log n}{n^2} \cdot \frac{n^2}{32} = -\frac{100 \log n}{32}$, поэтому второе слагаемое стремится к нулю.

Пусть теперь минимальное ребро имеет вес 2, т.е. оба конца имеют вес 1. Выберем это ребро $\binom{n}{2}$ способами. Тогда в оставшемся графе на $n-2$ вершинах единицы образуют независимое множество. По показанному выше, вероятность такого события не больше $(n-2) \cdot 2^{-0.13(n-2)} + e^{-p_n \cdot \frac{(n-2)^2}{32}}$.

Аналогично выкладке выше, показатель степени не превосходит $-100 \cdot \frac{\log n}{n^2} \cdot \frac{(n-2)^2}{32} \leq -\frac{99}{32} \cdot \log n$.

Отсюда получаем оценку сверху на рассматриваемую вероятность $(n-2) \cdot 2^{-0.13(n-2)} + e^{-\frac{99}{32} \log n}$.

Домножая на $\binom{n}{2}$, получим оценку сверху на искомую вероятность

$$\frac{n(n-1)(n-2)}{2} \cdot 2^{-0.13(n-2)} + \frac{n(n-1)}{2} \cdot \frac{1}{n^{\frac{99}{32}}},$$

что стремится к нулю. Теорема 2 доказана.

СПИСОК ЛИТЕРАТУРЫ

- [1] Ta-Shma N. A simple proof of the Isolation Lemma // Electronic Colloquium on Computational Complexity. — 2015.

О ПРИНАДЛЕЖНОСТИ ЧАСТИЧНЫХ ФУНКЦИЙ РАНГА 2 МАКСИМАЛЬНЫМ МУЛЬТИКЛОНАМ

Пантелеев Владимир Иннокентьевич

Иркутский государственный университет, e-mail: vl.panteleyev@gmail.com

На множестве $E_2 = \{0, 1\}$ определим следующие множества функций:

$$P_{2,n}^{*-} = \{f \mid f : E_2^n \rightarrow 2^{E_2}\}, P_2^{*-} = \bigcup_n P_{2,n}^{*-}$$

$$P_{2,n}^* = \{f \mid f : E_2^n \rightarrow E_2 \cup \{\emptyset\}\}, P_2^* = \bigcup_n P_{2,n}^*$$

Функции из множества P_2^{*-} называются мультифункциями, из P_2^* — частичными функциями. Очевидно, что множество частичных функций вкладывается в множество мультифункций. Заметим, что множество частичных (а значит и мульти-) функций содержит и множество булевых функций. Будем отождествлять одноэлементные множества с элементами этих множеств.

Суперпозиция

$$f(f_1(x_1, \dots, x_m), \dots, f_n(x_1, \dots, x_m))$$

мультифункций $f(x_1, \dots, x_n), f_1(x_1, \dots, x_m), \dots, f_n(x_1, \dots, x_m)$ определяет мультифункцию $g(x_1, \dots, x_m)$ следующим образом:

$$g(\alpha_1, \dots, \alpha_m) = \bigcup_{\beta_i \in f_i(\alpha_1, \dots, \alpha_m)} f(\beta_1, \dots, \beta_n)$$

для любого набора $(\alpha_1, \dots, \alpha_m) \in E_2^m$.

Определения клона, максимального клона предполагаем стандартными. В [1] описаны все 15 максимальных клонов мультифункций.

Описание решетки всех клонов является сложной и нерешенной к настоящему времени задачей. В первую очередь это связано с тем, что данная решетка континуальна.

Вместо описания решетки всех клонов можно поставить для каждой мультифункции вопрос о принадлежности максимальным клоном. Отношение принадлежности максимальным клоном является отношением эквивалентности на множестве всех мультифункций и определяет скелет решетки клонов мультифункций.

Так как число максимальных мультиклонов равно 15, то число классов эквивалентности не больше 2^{15} .

Нахождение точного числа классов можно вести следующим образом: компьютерными экспериментами определять нижнюю оценку, а свойствами функций — верхнюю. При этом стоит заметить, что компьютерный перебор уже при 4-х переменных является не очень эффективным из-за больших временных затрат. С другой стороны и установление общих свойств является нетривиальной задачей.

Одним из возможных решений задачи описания всех классов эквивалентности является рассмотрение специальных подмножеств. Такими подмножествами являются, в частности, булевы и частичные функции.

В [2] показано, что множество булевых функций порождает 18 классов. В каждом классе имеется функция, существенно зависящая не более чем от 4-х аргументов.

При рассмотрении вопроса о принадлежности частичных функций максимальным мультиклонам далее будем рассматривать только такие функции, которые хотя бы на одном наборе возвращают $\emptyset$.

Компьютерный перебор функций, зависящих не более чем от 3 переменных, позволил найти 97 классов. Выборочные исследования функций, зависящих от 4 переменных, добавили еще 2 класса.

Таким образом, с учетом результатов из [2], число классов, порожденных частичными функциями, не меньше 117.

Пусть

$$M_{ij} = \{f \in P_2^* \mid f(0, \dots, 0) = i, f(1, \dots, 1) = j\}.$$

Справедливы следующие утверждения.

Теорема 1. Каждое из множеств M_{00} и M_{11} отношением принадлежности максимальным мультиклонам разбивается на 6 классов.

Теорема 2. Множество M_{10} порождает не менее 5 и не более 7 классов.

СПИСОК ЛИТЕРАТУРЫ

- [1] Пантелеев В. И. Критерий полноты для недоопределенных частичных булевых функций // Вестник НГУ. Серия: Математика, механика, информатика. — 2009. — Т. 9, вып. 3. — С. 95–114.
- [2] Казимиров А. С, Пантелеев В. И. О классах булевых функций, порожденных максимальными мультиклонами // Вестник Бурятского государственного университета. Математика и информатика. — 2015, выпуск 9. — С. 16–22.

ТОЖДЕСТВА В СУПЕРКЛОНАХ

Перязев Николай Алексеевич¹, Шаранхаев Иван Константинович²

¹ Санкт-Петербургский государственный электротехнический университет, e-mail:

nikolai.baikal@gmail.com

² Бурятский государственный университет, e-mail: goran5@mail.ru

Мультиоперации

Пусть A — множество, $n \geq 0$.

— n -местная мультиоперация — $f : A^n \rightarrow 2^A$.

$|A| = k$ — ранг мультиоперации, n — размерность мультиоперации.

M_A^n, M_A — множества n -местных и всех мультиопераций над A ;

— мультиоперации $f \in M_A$, где $A = \{a_0, \dots, a_{k-1}\}$ можно представлять как отображения

$$f : \{2^0, 2^1, \dots, 2^{k-1}\}^n \rightarrow \{0, 1, \dots, 2^k - 1\},$$

получаемых из f при кодировке

$$a_i \rightarrow 2^i; \quad \emptyset \rightarrow 0; \quad \{a_{i_1}, \dots, a_{i_s}\} \rightarrow 2^{i_1} + \dots + 2^{i_s}.$$

— $f = (\alpha_1, \dots, \alpha_{k^n})$ векторная форма n -местной f ,

где $\alpha_i \in \{0, 1, \dots, 2^k - 1\}$ и $\alpha_i = f(2^{i_1}, \dots, 2^{i_n})$, а $(i_1, \dots, i_n)$ есть представление $i - 1$ в системе исчисления по основанию k n -разрядным числом;

— n -местная пустая мультиоперация

$$\theta^n(a_1, \dots, a_n) = \emptyset;$$

— n -местная полная мультиоперация

$$\pi^n(a_1, \dots, a_n) = A;$$

— n -местная мультиоперация проектирования по i аргументу

$$e_i^n(a_1, \dots, a_n) = \{a_i\};$$

— бинарная мультиоперация пересечения

$$f_{\cap}(a, b) = \{a\} \cap \{b\};$$

— разрешимость f по i аргументу

$$(\mu_i f)(a_1, \dots, a_n) = \{a \mid a_i \in f(a_1, \dots, a_{i-1}, a, a_{i+1}, \dots, a_n)\}.$$

Легко видно, что:

$$b \in (\mu_i f)(a_1, \dots, a_{i-1}, c, a_{i+1}, \dots, a_n) \iff c \in f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n);$$

— суперпозиция мультиопераций $f \in M_A^n$ и $f_1, \dots, f_n \in M_A^m$

$$(f * f_1, \dots, f_n)(a_1, \dots, a_m) = \bigcup_{b_i \in f_i(a_1, \dots, a_m)} f(b_1, \dots, b_n).$$

— пересечение f и g

$$(f \cap g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) \cap g(a_1, \dots, a_n);$$

- $f_{\cap} = (e_1^2 * e_1^2, \mu_2 e_1^2);$
- $(f \cap g) = (f_{\cap} * f, g).$

Суперклоном над множеством A называется любое подмножество $R \subseteq M_A$, содержащее все мультиоперации пустые, полные, проектирования и замкнутое относительно суперпозиций и разрешимостей [1].

Полутождества и тождества

- Полутождество суперассоциативности суперпозиции

$$\begin{aligned} ((f * g_1, \dots, g_n) * h_1, \dots, h_m) &\subseteq \\ &\subseteq (f * (g_1 * h_1, \dots, h_m), \dots, (g_n * h_1, \dots, h_m)), \\ \text{если } f &\text{ — унарная мультиоперация, то верно тождество} \\ ((f * g) * h_1, \dots, h_m) &= (f * (g * h_1, \dots, h_m)); \end{aligned}$$

- Полутождество разрешимости суперпозиции

$$\begin{aligned} \mu_i(f^n * g_1^m, \dots, g_n^m) &\subseteq \bigcap_{j=1}^n (\mu_i g_j^m * e_1^m, \dots, e_{i-1}^m, \\ &(\mu_j f^n * \pi^m, \dots, \pi^m, \underbrace{e_i^m}_j, \pi^m, \dots, \pi^m), e_{i+1}^m, \dots, e_m^m), \end{aligned}$$

если f — унарная мультиоперация, то верно тождество

$$\mu_i(f * g^m) = (\mu_i g^m * e_1^m, \dots, e_{i-1}^m, (\mu f * e_i^m), e_{i+1}^m, \dots, e_m^m).$$

- Пусть $f = (1002), g_1 = (13), g_2 = (31), h = (3).$

Тогда

$$\begin{aligned} ((f * g_1, g_2) * h) &= (1), \\ (f * (g_1 * h), (g_2 * h)) &= (3). \end{aligned}$$

Получили строгое включение

$$((f * g_1, g_2) * h) \subset (f * (g_1 * h), (g_2 * h)).$$

- Пусть $f^2 = (501042013), g_1^1 = (465), g_2^1 = (736).$

Тогда

$$\begin{aligned} \mu_1(f^2 * g_1^1, g_2^1) &= (752), \\ (\mu_1 g_1^1 * (\mu_1 f^2 * e_1^1, \pi^1)) \cap (\mu_1 g_2^1 * (\mu_2 f^2 *, \pi^1, e_1^1)) &= (756). \end{aligned}$$

Получили строгое включение

$$\mu_1(f^2 * g_1^1, g_2^1) \subset (\mu_1 g_1^1 * (\mu_1 f^2 * e_1^1, \pi^1)) \cap (\mu_1 g_2^1 * (\mu_2 f^2 *, \pi^1, e_1^1)).$$

Альтернативные определения суперклона

- подстановка g в f по i аргументу

$$\begin{aligned} (f *_i g)(a_1, \dots, a_{n+m-1}) &= \\ &= \bigcup_{b_i \in g(a_i, \dots, a_{i+m-1})} f(a_1, \dots, a_{i-1}, b_i, a_{i+m}, \dots, a_{n+m-1}); \end{aligned}$$

- отождествления i и j аргументов f
 $(\Delta_{i,j}f)(a_1, \dots, a_{n-1}) = f(a_1, \dots, a_{j-1}, a_i, a_{j+1}, \dots, a_{n-1});$

Суперклоном над множеством A называется любое подмножество $R \subseteq M_A$, содержащее все мультиоперации пустые, полные, проектирования и замкнутое относительно подстановок, разрешимостей и отождествлений.

Суперклоном над множеством A называется любое подмножество $R \subseteq M_A$, содержащее все мультиоперации пустые, полные, проектирования и замкнутое относительно подстановок, разрешимостей и пересечения.

Тождества в суперклонах

- $(f \cap (g \cap h)) = ((f \cap g) \cap h);$
- $(f \cap g) = (g \cap f);$
- $\mu_i \theta^n = \theta^n;$
- $\mu_i \pi^n = \pi^n;$
- $\mu_i e_j^n = \mu_j e_i^n = (\pi^1 *_1 (e_i^n \cap e_j^n));$
- $\mu_i \mu_i f = f;$
- $\mu_i (f \cap g) = (\mu_i f \cap \mu_i g);$
- $\mu_i (f^n *_j g^m) = (\mu_i f^n *_j g^m)$
 при $i \in \{1, \dots, j-1, j+m, \dots, n+m-1\};$
- $\mu_i (f^n *_j g^m) = \alpha^{n+m-1}(\mu_i g^m *_i \mu_j f^n)$ для некоторой метаоперации перестановки аргументов α^{n+m-1} при $i \in \{j, \dots, j+m-1\}.$

Суперклоны и мультиклоны

Мультиклоном над множеством A называется любое подмножество $R \subseteq M_A$, содержащее все мультиоперации пустые, полные, проектирования и замкнутое относительно суперпозиций.

Теорема 1. Пусть множество мультиопераций B содержит мультиоперацию e_1^2 и замкнуто относительно разрешимостей. Тогда суперклон и мультиклон, порожденные множеством B , совпадают.

СПИСОК ЛИТЕРАТУРЫ

- [1] Перязев Н. А., Шаранхаев И. К. Теория Галуа для клонов и суперклонов // Дискретная математика. — 2015. — Т. 27, № 4. — С. 79–93.

О ВЕРХНЕЙ ОЦЕНКЕ ОРИЕНТИРУЕМОГО РОДА ПРОСТОГО ГРАФА

Петренюк Владимир Ильич

Кропивницкий технический университет, e-mail: petrenjukvi@rambler.ru

Задача состоит в уточнении верхней оценки ориентируемого рода $\gamma(G)$ графа G , полученного в [3] в результате отождествления упорядоченных k пар

(x_{1j}, x_{1j}) элементов подмножеств X_i множества точек графов G_i ориентируемого рода $\gamma(G_i)$, с приведенными в [1] характеристиками $t_{G_i}(X_i)$ — числом достижимости — и $\theta_{G_i}(X_i)$ или $\partial\theta_{G_i}(X_i)$ подмножеств X_i , а также новой характеристики $ms_{G_i}(X_i)$, $i = 1, 2$. Число достижимости $t_{G_i}(X_i)$, $t_i = t_{G_i}(X_i)$ определяется как наименьшее число клеток s_{ij} , $s_{ij} \in S_{\gamma(G_i)} \setminus f(G)$, на границах которых расположены все элементы непересекающихся между собой подмножеств X_{ij} множества X_i , где минимум берётся по всем различным f -минимальным вложениям графа G_i в поверхность S ориентируемого рода $\gamma(G_i)$, $i = 1, 2$. В [2] описаны две характеристики: $\theta_{G_i}(X_i)$ для циклической и звёздной структур границ множества клеток $\{s_{ij}\}_{j=1}^{t_i}$ и характеристики $\partial\theta_{G_i}(X_i)$ для специальной цепочной структуры множества границ клеток s_{ij} , где $j = 1, \dots, t_{G_i}(X_i)$, $i = 1, 2$. Определим $ms_{G_i}(x_{ij}, s_k)$ как наибольшее число простых звёзд $st_{G_i}(a_m)$, т. е. подграфов, гомеоморфных графу K_4 , с, по меньшей мере, тремя концевыми вершинами x_{ij} графа G_i , расположенными на границе некоторой клетки s_k , $s_k \in S_{\gamma(G_i)} \setminus f(G)$, в которую вкладываются без пересечения рёбер во внутренних точках все $st_{G_i}(a_m)$, при заданом минимальном вложении f графа G_i в ориентируемую поверхность S рода $\gamma(G_i)$, реализующего три упомянутых выше характеристики подмножества X_i , $i = 1, 2$. Будем говорить о вершине x_{ij} как об обладающей, по меньшей мере, двойным доступом, если максимальное число $ms_{G_i}(x_{ij}, s_k)$ не меньше 1, где максимум берётся для всех клеток по всем различным минимальным вложениям f графа G_i в ориентируемую поверхность S рода $\gamma(G_i)$, реализующим три упомянутых выше характеристики подмножества X_i , $i = 1, 2$. Обозначим через $ms_{G_i}(X_i)$ наибольшую сумму чисел $ms_{G_i}(x_{ij})$, где максимум берётся по всем различным точкам x_{ij} графа G_i , $i = 1, 2$. Пусть граф G получен, как указано выше, т. е. в результате отождествления упорядоченных k пар (x_{1j}, x_{2j}) в точку x_j , $j = 1, k$ элементов подмножеств X_i множества точек графов G_i ориентируемого рода $\gamma(G_i)$, где граф G_1 — рода $\gamma(G_1)$, граф G_2 — квазизвезда с плоским связным графом центром R и ребрами-лучами, принадлежащими различным подграфам $H_{j'}$, $H_{j''}$ графа G , гомеоморфным одному из графов множества $\{K_4, K_5, K_5 \setminus e, K_{2,3}, K_{3,3}, K_{3,3} \setminus e\}$. Подграфы $H_{j'}$, $H_{j''}$ образуют своеобразное кольцо или куски кольца вокруг центра R , причём множество вершин этих подграфов содержит, по меньшей мере, две вершины, присоединяющиеся к двум вершинам графа G_1 , а остальные вершины принадлежат графу R и могут принадлежать двум разным подграфам $H_{j'}$, $H_{j''}$ с общим ребром. Обозначим через x число подграфов, гомеоморфных K_4 с двумя вершинами, присоединяющимися к вершинам $x_{1j'}, x_{1j''}$ с двусторонним доступом, $j' \neq j''$, $j', j'' = 1, ms'_1$, где через ms'_1 определим число задействованных в подграфах $H_{j'}$, $H_{j''}$ вершин x_{1j} с, по меньшей мере, двойным доступом.

Теорема 1. Пусть имеют место принятые выше обозначения, граф G_1 — рода $\gamma(G_1)$, граф G_2 — квазизвезда с плоским связным графом-центром R , где

$\gamma(G_1) = g_1$, $t_{G_i}(X_i) = t_i > 0$, $ms_{G_1}(X_1) = ms_1$, $ms'_1 > 1$, $\theta_{G_i}(X_i) = \theta_i > 0$ или $\partial\theta_{G_i}(X_i) = \partial\theta_i > 0$, $i = 1, 2$, и задано φ -преобразование следующим образом:

$\varphi(G_1 + G_2, \sum_{j=1}^k (x_{1j} + x_{2j})) \longrightarrow (G, \{x_j\}_{j=1}^k)$. Тогда имеет место неравенство

$$\gamma(G) \leq \gamma(G_1) + \sum_{i=1}^2 (t_i - (\theta_i + \partial\theta_i) - 1) - ms'_1 + x.$$

Доказательство. Пусть выполняются условия теоремы. Обозначим через f_i минимальные вложения графа G_i , реализующие $t_{G_i}(X_i) = t_i > 0, i = 1, 2$. Положим, что на клетке s_{11} реализован многосторонний доступ к элементам множества X_1 и при обходе границы этой клетки имеется $ms_{G_1}(x_{1j})$ копий точки x_{1j} , $j = 1, \dots, k$. На множестве клеток s_{ij} , $i = 1, 2$, реализуем процедуру преобразования циклической структуры в цепочную, тем самым уменьшая на $\theta_{G_i}(X_i)$ число преобразованных клеток. Когда на преобразованном множестве не будет ни циклов, ни звёзд, состоящих из его элементов, реализуем процедуру преобразования цепочной структуры в нецепочную, тем самым уменьшая на $\partial\theta_{G_i}(X_i)$ число элементов (преобразованных клеток). При помощи дополнительных l_i ручек, $l_i = t_i - (\theta_i + \partial\theta_i) - 1$, приклеенных одним концом к регулярной подклетке клетки s_{i1} , а другим к каждой регулярной подклетке клетки s_{ij} , где $j = 2, \dots, t_i$. Получим клетку s'_i , на границе которой расположены все элементы множеств X_i , $i = 1, 2$, и обозначим через f'_i минимальные вложения графа G_i , реализующие такое расположение. Расположим внутри клетки s'_1 клетку s'_2 так, чтобы $\partial s'_1 \cap \partial s'_2 = \emptyset$. Выполним операцию отождествления пар точек (x_{1j}, x_{2j}) в точку x_j , $j = 1, \dots, k$. Вложим ребра звезд $St_{G_2}(x_{2j})$ в кольцо, разделяющее границы клеток s'_1 и s'_2 , с учётом того, что при обходе границы этой клетки имеется ms'_1 копий тех точек x_{1j} , $j = 1, \dots, k$, которые по меньшей мере одной вершиной принадлежат непересекающимся по рёбрам подграфам, гомеоморфным одному из графов $\{K_4, K_5, K_5 \setminus e, K_{2,3}, K_{3,3}, K_{3,3} \setminus e\}$, а другими вершинами принадлежат графу R . Тогда ms'_1 ручек станут лишними за счёт использования двустороннего доступа к некоторым вершинам указанных графов, где $ms'_1 \leq x$, x — число подграфов, гомеоморфных графу K_4 , обладающих двумя вершинами $x_{2j'}, x_{2j''}$, которые присоединяются к вершинам $x_{1j'}, x_{1j''}$ с, по меньшей мере, двусторонним доступом к ним на $S_{\gamma(G_1)}$. Получим вложение графа G в ориентированную поверхность рода γ ,

$\gamma \leq \gamma(G_1) + \sum_{i=1}^2 (t_i - (\theta_i + \partial\theta_i) - 1) - (ms'_1 - x)$. Поскольку $\gamma(G) \leq \gamma$, то имеет место неравенство теоремы 1. **Теорема 1 доказана.**

Пример. Возьмём графы $K_{3,7}$ и $K_{3,11}$ из числа граф-обструкций для тора и двойного тора соответственно. Пусть граф $G = K_{3,7}$. Пусть граф $G_1 = K_{3,3}$ с множеством вершин $\{1', 2', 3', 4', 5', 6'\}$, $X_1 = \{1', 2', 3'\}$, достижимым на торе, т. е. $t_1 = 1$, и обладающим трёхсторонним доступом, $ms_1 = ms'_1 = 3$. Пусть граф $G_2 = 4K_{1,3}$, причём $X_2 = \{1'', 2'', 3''\}$ и $t_2 = 1$, т. е. множество вершин X_2

имеет число достижимости 1 на некоторой клетке графа $K_{3,3}$, вложенного в тор. Для указанных множеств X_i , $i = 1, 2$, имеем равенство $\theta_i = \partial\theta_i = 0$. В результате отождествления пар вершин $\{(i', i'')\}_{i=1}^6$ в вершины $\{1, 2, 3\}$ получим четыре подграфа, гомеоморфных K_4 , обладающих с графом G_1 тремя общими вершинами, отождествляемых в вершины из $\{2, 5, 6\}$, поэтому $x = 4$. Поскольку $ms_1 = 3$, то тогда род графа $G = K_{3,7}$ не больше $1 + (1 - 1) + (1 - 1) + (4 - 3) = 2$. Для графа $G = K_{3,11}$ имеем $G_1 = K_{3,7}$ рода 2 и $x = 4$, $ms_1 = ms' = 3$. Получим, что род графа $G = K_{3,11}$ не больше $2 + (1 - 1) + (1 - 1) + (4 - 3) = 3$.

СПИСОК ЛИТЕРАТУРЫ

- [1] Петренюк В. И. Две характеристики дуального графа плоского графа // Материалы конференции «Искусственный интеллект – 2004». — 2004. — С. 230–231.
- [2] Петренюк В. И. Обобщенная оценка рода простого графа. // Искусственный интеллект. — 2004. — Т. 4. — С. 34 — 45.
- [3] Петренюк В. И. Оценка рода арех- m -склейки простых графов. // Материалы XV международной конференции «Проблемы теоретической кибернетики». — Казань: «Отечество», 2008. — С. 34.

НЕКОТОРЫЕ ВОПРОСЫ ТЕОРИИ КОНТРОЛЯ И ДИАГНОСТИКИ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Попков Кирилл Андреевич

ИПМ им. М. В. Келдыша РАН, e-mail: kirill-formulist@mail.ru

Введение

Рассматривается задача синтеза легкотестируемых схем, реализующих заданные булевы функции. Пусть имеется схема из функциональных элементов S с одним выходом, реализующая булеву функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \dots, x_n)$. Под воздействием некоторого источника неисправностей один или несколько элементов схемы S могут перейти в неисправное состояние. Ограничимся рассмотрением произвольных и однотипных константных неисправностей на выходах элементов. Описания указанных неисправностей, а также необходимые для дальнейшего изложения определения функций неисправности, проверяющего и диагностического тестов, их длин, полного и единичного тестов и избыточных схем можно найти, например, в работах [1, 2].

Пусть зафиксирован вид неисправностей элементов, B — произвольный функционально полный базис и T — единичный проверяющий тест для некоторой схемы S в базисе B . Введём следующие обозначения: $D_{\text{ЕП}}^B(T)$ — длина

теста T ; $D_{\text{ЕП}}^B(S) = \min D_{\text{ЕП}}^B(T)$, где минимум берётся по всем единичным проверяющим тестам T для схемы S ; $D_{\text{ЕП}}^B(f) = \min D_{\text{ЕП}}^B(S)$, где минимум берётся по всем избыточным схемам S в базисе B , реализующим функцию f ; $D_{\text{ЕП}}^B(n) = \max D_{\text{ЕП}}^B(f)$, где максимум берётся по всем булевым функциям f от n переменных, для которых определено значение $D_{\text{ЕП}}^B(f)$. Функция $D_{\text{ЕП}}^B(n)$ называется *функцией Шеннона* длины единичного проверяющего теста. По аналогии с функциями $D_{\text{ЕП}}^B$ можно ввести функции $D_{\text{ЕД}}^B$, $D_{\text{ПП}}^B$ и $D_{\text{ПД}}^B$ для соответственно единичного диагностического теста, полного проверяющего и полного диагностического тестов, зависящие от T , от S , от f и от n (в определениях функций $D_{\text{ПП}}^B(f)$ и $D_{\text{ПД}}^B(f)$ не требуется предполагать избыточность схем). Так, например, $D_{\text{ПД}}^B(n)$ — функция Шеннона длины полного диагностического теста.

Для удобства над буквой D после символов, обозначающих базис, через точку с запятой будем ставить символы «0, 1», «0» или «1» в случаях, когда в схемах допускаются соответственно произвольные константные неисправности, однотипные константные неисправности типа 0 или типа 1 на выходах элементов.

Полные диагностические тесты

К настоящему времени ни для какого функционально полного конечного базиса B не известны верхние оценки величин $D_{\text{ПД}}^{B;1}(n)$, $D_{\text{ПД}}^{B;0}(n)$ и $D_{\text{ПД}}^{B;0,1}(n)$, по порядку меньшие 2^n . Ранее были также неизвестны нелинейные нижние оценки ни одной этих величин.

В работе автора [3] получены экспоненциальные нижние оценки указанных величин в некоторых базисах (а именно, в базисе $\{|\}$ для величины $D_{\text{ПД}}^{B;1}(n)$, в базисе $\{\downarrow\}$ для величины $D_{\text{ПД}}^{B;0}(n)$ и в любом из базисов $\{|\}$, $\{\downarrow\}$, $\{\&, \neg\}$, $\{\vee, \neg\}$ для величины $D_{\text{ПД}}^{B;0,1}(n)$).

Нижние оценки длин единичных тестов

В работе автора [4] получен ряд константных нижних оценок длин минимальных единичных тестов для схем из функциональных элементов в широких классах базисов при однотипных и произвольных константных неисправностях на выходах элементов. Эти оценки либо являются новыми (теоремы 4, 5), либо обобщают уже имевшиеся оценки (теоремы 1, 3).

Единичные проверяющие тесты для схем в базисе $\{\&, \neg\}$

Выделим пять возможных представлений функции $f(\tilde{x}^n)$:

$$f(\tilde{x}^n) = x_i, \quad (1)$$

$$f(\tilde{x}^n) = 0, \overline{x_i} \text{ или } x_{i_1}^{\sigma_1} \& x_{i_2} \dots \& x_{i_k}, \quad (2)$$

$$f(\tilde{x}^n) = \overline{x_{i_1}} \& \overline{x_{i_2}} \& x_{i_3} \& \dots \& x_{i_k} \text{ или } \underbrace{(\dots ((x_{i_1}^{\sigma_1} \& x_{i_2})^{\sigma_2} \& x_{i_3})^{\sigma_3} \& \dots \& x_{i_k})^{\sigma_k}}_{k-1}, \quad (3)$$

$$f(\tilde{x}^n) = x_{i_1}^{\sigma_1} \& \dots \& x_{i_k}^{\sigma_k}, \quad (4)$$

$$f(\tilde{x}^n) = \underbrace{(\dots ((x_{i_1}^{\sigma_1} \& x_{i_2}^{\sigma_2})^{\delta_1} \& x_{i_3}^{\sigma_3})^{\delta_2} \& \dots \& x_{i_k}^{\sigma_k})^{\delta_{k-1}}}_{k-1}, \quad (5)$$

где $2 \leq k \leq n$ в представлениях (2), (3), (5) и $1 \leq k \leq n$ в представлении (4); $\sigma_1, \dots, \sigma_k, \delta_1, \dots, \delta_{k-1} \in \{0, 1\}$; $i, i_1, \dots, i_k \in \{1, \dots, n\}$, причём индексы $i_1, \dots, i_k$ попарно различны; в представлении (3) хотя бы одно из чисел $\sigma_2, \dots, \sigma_k$ равно 0 и если $k = 2$, то полагаем $x_{i_3} \& \dots \& x_{i_k} \equiv 1$, а в представлении (5) хотя бы одно из чисел $\delta_1, \dots, \delta_{k-1}$ равно 0.

Теорема 1. Для любой булевой функции $f(\tilde{x}^n)$, отличной от тождественной единицы, справедливо равенство

$$D_{\text{ЕП}}^{\{\&, \neg\}; 1}(f) = \begin{cases} 0, & \text{если функция } f \text{ представима в виде (1),} \\ 1, & \text{если функция } f \text{ представима в виде (2),} \\ 2, & \text{если функция } f \text{ представима в виде (3),} \\ 3, & \text{если функция } f \text{ не представима в видах (1)–(3).} \end{cases}$$

Если же $f \equiv 1$, то значение $D_{\text{ЕП}}^{\{\&, \neg\}; 1}(f)$ не определено.

Следствие 1. Для любого $n \geq 2$ справедливо равенство $D_{\text{ЕП}}^{\{\&, \neg\}; 1}(n) = 3$.

Теорема 2. Для любой булевой функции $f(\tilde{x}^n)$, отличной от констант, справедливо равенство

$$D_{\text{ЕП}}^{\{\&, \neg\}; 0}(f) = \begin{cases} 0, & \text{если функция } f \text{ представима в виде (1),} \\ 1, & \text{если функция } f \text{ представима в виде (4), но не в виде (1),} \\ 2, & \text{если функция } f \text{ представима в виде (5),} \\ 3, & \text{если функция } f \text{ не представима в видах (1), (4), (5).} \end{cases}$$

Если же $f \equiv 0$ или $f \equiv 1$, то значение $D_{\text{ЕП}}^{\{\&, \neg\}; 0}(f)$ не определено.

Следствие 2. Для любого $n \geq 2$ справедливо равенство $D_{\text{ЕП}}^{\{\&, \neg\}; 0}(n) = 3$.

Таким образом, для любой булевой функции найдено точное значение длины минимального единичного проверяющего теста для реализующих её избыточных схем из функциональных элементов в базисе $\{\&, \neg\}$ при однотипных константных неисправностях любого из типов 0, 1 на выходах элементов.

Работа выполнена при поддержке программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

СПИСОК ЛИТЕРАТУРЫ

- [1] Редькин Н. П. Надежность и диагностика схем. — М. : Изд-во МГУ, 1992. — 192 с.

- [2] Попков К. А. О единичных диагностических тестах для схем из функциональных элементов в базисе Жегалкина // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2016. — № 3(39). — С. 3–18.
- [3] Попков К. А. Нижние оценки длин полных диагностических тестов для схем и входов схем // Прикладная дискретная математика. — 2016. — № 4(34). — С. 65–73.
- [4] Попков К. А. Нижние оценки длин единичных тестов для схем из функциональных элементов // Препринты ИПМ им. М. В. Келдыша. — 2016. — № 139. — 20 с. URL: <http://library.keldysh.ru/preprint.asp?id=2016-139>

ИДЕМПОТЕНТНЫЕ БИНАРНЫЕ ОТНОШЕНИЯ И ОТНОШЕНИЯ ДОСТИЖИМОСТИ НА ГРАФАХ

Поплавский Владислав Брониславович

Саратовский государственный университет, e-mail: poplavskivb@mail.ru

Рассмотрим алгебру $\langle \mathbf{P}, \cdot, {}^{-1}, {}^c \rangle$ всех бинарных отношений на множестве X , состоящую из множества $\mathbf{P}$ всевозможных подмножеств декартова квадрата $X \times X$, бинарной операции умножения " $\cdot$ ", двух унарных операций: обращения " ${}^{-1}$ " и дополнения " c ", определяемых стандартным образом.

Каждое бинарное отношение $\rho \in \mathbf{P}$, рассматриваемое как подмножество $\rho \subseteq X \times X$, можно считать множеством рёбер ориентированного графа, вершины которого составляют множество X . Будем такой граф обозначать (X, ρ) .

Множество $\mathbf{P}$ всевозможных бинарных отношений на множестве вершин X с операцией умножения образует моноид, т.е. полугруппу $\langle \mathbf{P}, \cdot \rangle$ с единицей, роль которой выполняет диагональное бинарное отношение $\Delta = \{(x, x) | x \in X\}$. При этом неравенство $\rho \subseteq \sigma$ влечёт $\rho \cdot \tau \subseteq \sigma \cdot \tau$, $\tau \cdot \rho \subseteq \tau \cdot \sigma$ для любых $\rho, \tau, \sigma \in \mathbf{P}$, что означает стабильность частично упорядоченного множества $\langle \mathbf{P}, \subseteq \rangle$ относительно умножения.

Операция дополнения, в силу равенств $(\rho \cdot \sigma)^c = \rho^c \cdot \sigma^c$ является анти-изоморфизмом частично упорядоченного моноида, меняющим порядок $\subseteq$ на $\supseteq$.

Обращение бинарных отношений является биективным отображением, сохраняющим порядок $\subseteq$. Однако, для обращения произведений бинарных отношений выполняется тождество: $(\rho \cdot \sigma)^{-1} = \sigma^{-1} \cdot \rho^{-1}$.

Введем обозначение: $\rho^* = (\rho^{-1})^c = (\rho^c)^{-1}$.

Определение 1. Бинарное отношение $\rho \in \mathbf{P}$ называется *первичным идемпотентом*, если $\Delta \not\subseteq \rho = \rho \cdot \rho$, и *вторичным идемпотентом* в противном случае: $\Delta \subseteq \rho = \rho \cdot \rho$.

Любое бинарное отношение $\rho \in \mathbf{P}$ порождает *вторичные идемпотенты* *правого типа*: $\rho^{\mathcal{R}} = (\rho \cdot \rho^*)^*$ и *левого типа*: $\rho^{\mathcal{L}} = (\rho^* \cdot \rho)^*$.

Доказательства следующих двух теорем в случае, когда множество X конечно, можно найти в [1] и [2].

Теорема 1. Пусть ρ — идемпотент полугруппы бинарных отношений P . Идемпотент ρ является первичным идемпотентом тогда и только тогда, когда $\rho \subsetneq \rho^R$ и $\rho \subsetneq \rho^L$, и является вторичным идемпотентом тогда и только тогда $\rho = \rho^R = \rho^L$.

Известно, что полугруппа $\langle P, \cdot \rangle$ бинарных отношений разбивается на непересекающиеся $\mathcal{J}$ — классы Грина, которые в свою очередь разбиваются на $\mathcal{L}$ — и $\mathcal{R}$ — классы. Следующая теорема показывает, что вторичные идемпотенты указывают необходимый признак того, что бинарные отношения порождают один и тот же односторонний идеал, т. е. $\mathcal{L}$ — или $\mathcal{R}$ — класс Грина.

Теорема 2. Если бинарные отношения ρ и σ порождают один и тот же правый главный идеал частичной полугруппы $\langle P, \cdot \rangle$, то $\rho^R = \sigma^R$. Если ρ и σ порождают левый идеал, то это влечет совпадение вторичных идемпотентов левого типа: $\rho^L = \sigma^L$.

Следующие равенства проверяются непосредственно и указывают свойства вторичных идемпотентов.

Теорема 3. Для любого бинарного отношения ρ выполняются равенства:

$$\begin{aligned}\rho^L &= (\rho^*)^R = (\rho^L)^L = (\rho^L)^R, \\ \rho^R &= (\rho^*)^L = (\rho^R)^R = (\rho^R)^L.\end{aligned}$$

Из теорем 2 и 3 следует, что в каждом $\mathcal{L}$ — или $\mathcal{R}$ — классе Грина частичной полугруппы $\langle P, \cdot \rangle$, может находиться только один вторичный идемпотент.

Известно, что вторичные идемпотенты играют важную роль в вопросах разрешимости простейших матричных уравнений, делимости, регулярности матриц и пр. [1,2,3].

В следующем утверждении обсуждается взаимное расположение вторичных идемпотентов и их порождающих бинарных отношений ρ и ρ^* в двусторонних идеалах (J — классах) полугруппы $\langle P, \cdot \rangle$.

Теорема 4. Пусть $(\rho^L)^*$ и ρ^L порождают один и тот же двусторонний идеал полугруппы $\langle P, \cdot \rangle$, тогда бинарные отношения ρ и ρ^* порождают тот же двусторонний идеал. Причём, если $(\rho^L)^*$ и ρ^L порождают один и тот же левый идеал полугруппы $\langle P, \cdot \rangle$, то бинарное отношение ρ порождает тот же левый идеал, и, если $(\rho^L)^*$ и ρ^L порождают один и тот же правый идеал полугруппы $\langle P, \cdot \rangle$, то бинарное отношение ρ^* порождает тот же правый идеал.

Аналогичное утверждение можно сформулировать для $(\rho^R)^*$ и ρ^R , меняя местами слова «левый» и «правый».

Пусть ρ^k обозначает произведение $\rho \cdot \dots \cdot \rho$, содержащее k сомножителей.

Определение 2. Транзитивным бинарным отношением называется бинарное отношение ρ , удовлетворяющее условию $\rho^2 \subseteq \rho$, и называется транзитивно — рефлексивным, если $\Delta \cup \rho^2 \subseteq \rho$.

Транзитивным замыканием бинарного отношения ρ называют бинарное отношение ${}^t\rho = \bigcup_{k=1}^{\infty} \rho^k = \rho \cup \rho^2 \cup \rho^3 \cup \dots$

Транзитивно-рефлексивным замыканием бинарного отношения ρ называют бинарное отношение $\bar{\rho} = \bigcup_{k=0}^{\infty} \rho^k = \Delta \cup \rho \cup \rho^2 \cup \rho^3 \cup \dots$

Транзитивное замыкание бинарного отношения ${}^t\rho$ является для вершин X ориентированного графа (X, ρ) отношением достижимости, т. е. бинарным отношением, которому принадлежат пары различных вершин, соединяемых цепью направленных рёбер графа (X, ρ) . Транзитивно-рефлексивное замыкание бинарного отношения $\bar{\rho}$ получается из графа достижимости $(X, {}^t\rho)$ добавлением петель ко всем вершинам.

Очевидно, что бинарное отношение ρ является транзитивным тогда и только тогда, когда ${}^t\rho = \rho$. Следующее утверждение даёт признаки транзитивности в терминах вторичных идемпотентов.

Теорема 5. Следующие условия эквивалентны:

1. Бинарное отношение ρ является транзитивным;
2. Выполняется неравенство $\rho \subseteq \rho^{\mathcal{L}} \cap \rho^{\mathcal{R}}$;
3. Выполняется неравенство $\bar{\rho} \subseteq \rho^{\mathcal{L}} \cap \rho^{\mathcal{R}}$.

СПИСОК ЛИТЕРАТУРЫ

- [1] Поплавский В. Б. О приложениях ассоциативности дуальных произведений алгебры булевых матриц // Фундаментальная и прикладная математика. — 2011/2012. — Т. 17, вып. 4. — С. 181–192. (Translation: Poplavski V. B. On applications of associativity of dual compositions in the algebra of Boolean matrix // Journal of Mathematical Sciences. Springer, New York. Vol. 191, No. 5 (2013). P. 718–725.)
- [2] Поплавский В. Б. Об идемпотентах алгебры булевых матриц // Изв. Саратов. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. — 2012. — Т. 12, вып. 2. — С. 26–33.
- [3] Schein B. M. Regular elements of the semigroup of all binary relations // Semigroup Forum. — 1976. — V. 13. — Pp. 95–102.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ НЕПОСТОЯННОЙ ИНТЕНСИВНОСТИ ОБСЛУЖИВАНИЯ НА СРЕДНЮЮ ЗАДЕРЖКУ ТРЕБОВАНИЯ В СИСТЕМЕ С ФИКСИРОВАННЫМ РИТМОМ

Пройдакова Екатерина Вадимовна

Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: rev_1@mail.ru

В работе рассматривается система обслуживания m независимых и конфликтных потоков $\Pi_1, \Pi_2, \dots, \Pi_m$ требований в классе циклических алгоритмов с непостоянной интенсивностью обслуживания. Конфликтность означает, что обслуживание потоков происходит в непересекающиеся промежутки времени. Обслуживающее устройство имеет $2m$ состояний $\Gamma^{(1)}, \Gamma^{(2)}, \dots, \Gamma^{(2m)}$ известной длительности $T_1, T_2, \dots, T_{2m}$. В состоянии $\Gamma^{(2j-1)}$, $j = 1, \dots, m$ пропускается только поток Π_j с непостоянной интенсивностью $\mu_j(t) > 0$, $t \in [0, T_{2j-1}]$. В состоянии $\Gamma^{(2j)}$ обслуживается также только поток Π_j , но уже с постоянной интенсивностью μ'_j . Интенсивности определяют среднее число заявок, обслуживающихся в единицу времени. Смена состояний обслуживающего устройства осуществляется по циклическому алгоритму. Такой алгоритм используется потому, что он прост в реализации и часто оказывается квазиоптимальным (близким к оптимальному) при сильной загрузке системы. Потоки $\Pi_1, \Pi_2, \dots, \Pi_m$ считаем пуассоновскими с известными параметрами $\lambda_1, \lambda_2, \dots, \lambda_m$ соответственно. Здесь λ_j определяет среднее число требований, поступающих в единицу времени по потоку Π_j , $j = 1, \dots, m$. По всем входным потокам разрешены неограниченные очереди. Произвольный вид функции интенсивности обслуживания $\mu_j(t)$ в состояниях $\Gamma^{(2j-1)}$, $j = 1, \dots, m$ может быть реализован за счет аппроксимации его кусочно-постоянной функцией. В силу этого, вид функций $\mu_j(t)$ полагаем кусочно-постоянным, с конечным числом ($n > 2$) скачков. Состояние $\Gamma^{(2j-1)}$ длительности T_{2j-1} представлялось в виде объединения n виртуальных состояний $\Gamma^{(2j-1)} = \{\Gamma_1^{(2j-1)}, \Gamma_2^{(2j-1)}, \dots, \Gamma_n^{(2j-1)}\}$, следовательно, оно являлось укрупненным состоянием. Длительности виртуальных состояний $\Gamma_1^{(2j-1)}, \Gamma_2^{(2j-1)}, \dots, \Gamma_n^{(2j-1)}$ известны и равны $T_{2j-1,1}, T_{2j-1,2}, \dots, T_{2j-1,n}$ единиц времени соответственно, причем $T_{2j-1} = T_{2j-1,1} + T_{2j-1,2} + \dots + T_{2j-1,n}$. В каждом из указанных виртуальных состояний интенсивность обслуживания $\mu_j(t)$ последовательно принимала значения $\mu_{j,1}, \mu_{j,2}, \dots, \mu_{j,n}$. Алгоритм смены состояний обслуживающего устройства оставался циклическим. В силу этого, для новой модели можно было применять те же методы исследований, что и в случае системы с постоянной интенсивностью обслуживания, только с учетом увеличения числа состояний обслуживающего устройства. В работах [1–3] автором ранее исследовалась циклическая система, в которой значение интен-

сивности обслуживания в состояниях $\Gamma^{(2j-1)}$, $j = 1, \dots, m$, предполагалось равным постоянной величине.

Имитационное моделирование

Для того, чтобы исследовать влияние непостоянной интенсивности обслуживания на характеристики функционирования циклической управляющей системы, была создана соответствующая имитационная модель. В начале работы имитационной модели задавались следующие входные параметры: m (штук); $T_1, T_2, \dots, T_{2m}$ (единиц времени); λ_j, μ'_j , $j = 1, \dots, m$ (требований в единицу времени). Также задавался вид функций $\mu_j(t)$ интенсивностей обслуживания в состояниях $\Gamma^{(2j-1)}$, $j = 1, \dots, m$.

Моделирование включало в себя два этапа. На первом этапе определялся момент перехода системы в квазистационарный (близкий к стационарному) режим функционирования. На втором этапе моделировалась работа системы в квазистационарном режиме для нахождения численных оценок характеристик системы. В частности, были найдены значения $\widetilde{M\gamma_j}$, $j = 1, \dots, m$ оценок среднего времени ожидания начала обслуживания требования по потокам и оценка γ^* среднего времени ожидания начала обслуживания произвольного требования, где $\gamma^* = \sum \lambda_j \widetilde{M\gamma_j} / \sum \lambda_j$. Основным критерием качества управления конфликтными потоками является среднее время ожидания начала обслуживания произвольной заявки или средняя задержка требования. При моделировании учитывались физические ограничения на некоторые параметры: $T_2 \geq 6$, $T_4 \geq 6$, $T_1 \geq T_2$, $T_3 \geq T_4$ и $T \geq 80$. Предварительно, методом сокращенного перебора, решалась задача оптимизации по критерию $\gamma^* \rightarrow \min$.

В качестве примера, далее рассмотрен случай двух потоков ($m = 2$). При значениях $T_2 = T_4 = 6$, $\mu_1(t) = 1$, $\mu_2(t) = 1$, $\mu'_1 = \mu'_2 = 2$, $\lambda_1 = 0,05$ и $\lambda_2 = 0,4$, минимум оценки γ^* равен 21,56 единиц времени, и он достигается при $T = 80$, $T_1 = 6$, $T_3 = 62$. Данные значения и являются квазиоптимальными (близкими к оптимальным) для случая постоянных интенсивностей обслуживания. Изучим, как повлияет непостоянная интенсивность обслуживания по второму направлению на оценку γ^* , в случае неизменных значений остальных параметров и при квазиоптимальных T , T_1 , T_3 . Максимальное число требований, которое может обслужиться в состоянии $\Gamma^{(3)}$, останется таким же, как при постоянной интенсивности обслуживания ($l_2 = 62$). Ниже, в качестве примера, рассмотрены несколько случаев.

Случай 1. Кусочно-постоянная функция $\mu_2(t)$ интенсивности обслуживания второго потока в состоянии обслуживающего устройства $\Gamma^{(3)}$, имеет четыре точки разрыва и задается следующим образом: $T_{3,1} = 18$, $T_{3,2} = 12$, $T_{3,3} = 14$, $T_{3,4} = 18$, а соответствующие интенсивности обслуживания принимают значения $\mu_{2,1} = 1,5$, $\mu_{2,2} = 1,2$, $\mu_{2,3} = 0,8$, $\mu_{2,4} = 0,6$. Значение оценки γ^* в этом случае равно 18,76 единиц времени.

Случай 2. Кусочно-постоянная функция $\mu_2(t)$ с четырьмя точками разрыва задается следующим образом: $T_{3,1} = 12$, $T_{3,2} = 18$, $T_{3,3} = 14$, $T_{3,4} = 18$, где интенсивности обслуживания принимают последовательно значения $\mu_{2,1} = 1, 2$, $\mu_{2,2} = 1, 5$, $\mu_{2,3} = 0, 8$, $\mu_{2,4} = 0, 6$. Оценка γ^* здесь равна 19,71.

Случай 3. У функции $\mu_2(t)$ четыре точки разрыва, при этом $T_{3,1} = 18$, $T_{3,2} = 14$, $T_{3,3} = 12$, $T_{3,4} = 18$ и $\mu_{2,1} = 0, 6$, $\mu_{2,2} = 0, 8$, $\mu_{2,3} = 1, 2$, $\mu_{2,4} = 1, 5$. Значение оценки γ^* в этом случае равно 22,84 единиц времени.

Таким образом, в случае системы с фиксированным ритмом, очевидно, что наличие непостоянной интенсивности обслуживания даже по одному направлению влияет на такую характеристику, как среднее время ожидания начала обслуживания произвольного требования γ^* . Как было показано выше, за счет введения функциональной зависимости $\mu_2(t)$, можно добиться уменьшения γ^* по сравнению с квазиоптимальным значением, полученным при постоянных интенсивностях обслуживания (в первом случае на 2,8, а во втором случае на 1,85 единиц времени). Можно и ухудшить значения оценки γ^* , подобрав функцию $\mu_2(t)$ определенным образом, например, увеличивая интенсивность обслуживания по потоку ближе к завершению основной фазы обслуживаемого устройства, как в третьем случае.

Работа в рамках госбюджетной темы Н-005-0 «Математическое моделирование и анализ стохастических эволюционных систем и процессов принятия решений».

СПИСОК ЛИТЕРАТУРЫ

- [1] Федоткин М. А., Пройдакова Е. В. Нелинейная модель процесса циклического обслуживания и выходные потоки // Известия высших учебных заведений. Прикладная нелинейная динамика. Издание Саратовского университета. — 2005. — Т. 13, № 3. — С. 48–60.
- [2] Пройдакова Е. В., Федоткин М. А. Определение условий существования стационарного распределения выходных потоков в системе с циклическим управлением // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия Математика. — 2006. — Вып. 1(4). — С. 92–102.
- [3] Пройдакова Е. В. Численное исследование циклической и приоритетной систем управления конфликтными потоками требований // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2013. — № 3(1). — С. 199–205.

ИССЛЕДОВАНИЕ ОПЕРАЦИЙ ПО УПРАВЛЕНИЮ КОНФЛИКТНЫМИ ПОТОКАМИ НЕОДНОРОДНЫХ ТРЕБОВАНИЙ

Рачинская Мария Анатольевна, Федоткин Михаил Андреевич

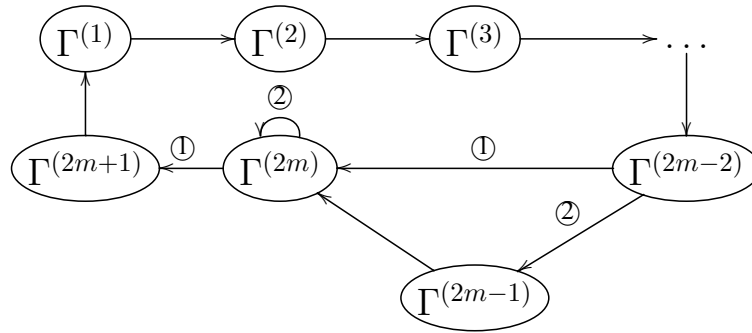
Нижегородский государственный университет им. Н. И. Лобачевского, e-mail:
rachinskaya.maria@gmail.com, fma5@rambler.ru

Описание исследуемой системы

Рассматривается система, на вход которой поступает $m \geq 2$ конфликтных неоднородных потоков $\Pi_1, \Pi_2, \dots, \Pi_m$ с целью получить обслуживание требованиям. Предполагается, что все потоки были сформированы под воздействием внешней среды, что привело к образованию зависимости между последовательными требованиями и скоплению их в группы [1]. Так, поток $\Pi_j, j \in \{1, 2, \dots, m\}$, адекватно аппроксимируется неординарным пуассоновским потоком с параметрами λ_j — интенсивность поступления групп, p_j, q_j и s_j — вероятности поступления группы из одного, двух или трех требований ($p_j + q_j + s_j = 1$). Потоки $\Pi_1, \Pi_2, \dots, \Pi_{m-1}$ являются малоинтенсивными, а поток Π_m обладает большой интенсивностью. Кроме того, выделяется приоритетный поток Π_1 . Изучается система, в которой не происходит потерь требований. Поступая в систему и не получая обслуживание мгновенно, требования становятся в очередь ожидания по соответствующему потоку. Устройство, осуществляющее операцию по обслуживанию требований, также выполняет операцию по управлению потоками. Выделяются состояния $\Gamma^{(1)}, \Gamma^{(2)}, \dots, \Gamma^{(2m+1)}$, в каждом из которых обслуживающее устройство (ОУ) находится в течение промежутка времени заданной длительности $T_1, T_2, \dots, T_{2m+1}$. По истечении такого промежутка принимается решение о смене или продлении текущего состояния. В состояниях вида $\Gamma^{(2j-1)}$ при $j \neq m$ обслуживаются требования потока Π_j с интенсивностью обслуживания μ_j . Переход к обслуживанию следующего потока осуществляется через состояние вида $\Gamma^{(2j)}$, $j \neq m$, которое выделено для безопасного завершения обслуживания потока Π_j . Для обслуживания потока Π_m выделены состояния $\Gamma^{(2m-1)}$ и $\Gamma^{(2m)}$. Интенсивность обслуживания в них одинакова и равна μ_m , но при этом $T_{2m} < T_{2m-1}$. Безопасная переналадка ОУ после обслуживания потока Π_m происходит в состоянии $\Gamma^{(2m+1)}$. Итак, пропускная способность ОУ в состояниях обслуживания характеризуется величинами $l_j = [\mu_j T_{2j-1}]$, $j \in \{1, 2, \dots, m\}$, и $l'_m = [\mu_m T_{2m}]$, где $[x]$ есть целая часть числа x .

Обозначим через $\tau_i > 0, i \in \{0, 1, \dots\}$, случайные моменты, в которые происходит принятие решения о переключении или продлении состояния ОУ. Пусть $\Gamma_i \in \{\Gamma^{(1)}, \Gamma^{(2)}, \dots, \Gamma^{(2m+1)}\}$ — случайное состояние ОУ на промежутке $[\tau_i, \tau_{i+1})$, и $\varkappa_{j,i} \in X = \{0, 1, \dots\}$ — случайное число требований в очереди по потоку

Π_j в момент τ_i . Следующие случайные величины характеризуют поведение системы по потоку Π_j на промежутке $[\tau_i, \tau_{i+1})$: $\eta_{j,i} \in \{0, 1, \dots\}$ — число требований, поступивших в систему, $\xi_{j,i}$ — максимальное число требований, которое может быть обслужено, $\xi'_{j,i} \in Y_j = \{0, 1, \dots, l_j\}$ — число требований, которые реально были обслужены. Здесь $\xi_{j,i} \in \{0, l_j\}$ для $j \neq m$ и $\xi_{m,i} \in \{0, l'_m, l_m\}$. Величина $\xi'_{j,-1} \in \{0, 1, \dots\}$ считает требования потока Π_j , покинувшие систему в промежутке $[0, \tau_0)$. Граф смены состояния ОУ имеет следующий вид:



Здесь переходы ① осуществляются при достижении количеством ожидающих требований потока Π_1 пороговой величины H_1 , т.е. при $\alpha_{1,i} + \eta_{1,i} \geq H_1$, в противном случае осуществляется переход ②.

Модель системы и ее исследование

В [2] доказано следующее утверждение.

Теорема 1. *Последовательность*

$$\{(\Gamma_i, \alpha_{1,i}, \alpha_{m,i}, \xi'_{1,i-1}, \xi'_{m,i-1}); i = 0, 1, \dots\}$$

с начальным распределением вектора $(\Gamma_0, \alpha_{1,0}, \alpha_{m,0}, \xi'_{1,-1}, \xi'_{m,-1})$ является одnorodной цепью Маркова.

Заметим, что при такой модели исследуется динамика работы системы по приоритетному потоку и потоку с большой интенсивностью. Однако аналогичными методами можно изучать функционирование системы по любому потоку Π_j , $j \in \{2, 3, \dots, m\}$, если в качестве состояния выбирать вектор $(\Gamma_i, \alpha_{1,i}, \alpha_{j,i}, \xi'_{1,i-1}, \xi'_{j,i-1})$.

Одной из целей аналитических исследований системы является нахождение условий, при которых в системе существует установившийся стационарный режим функционирования. Обозначим длительность минимального цикла смены состояния ОУ через $T = \sum_{k=1}^{2m+1} T_k - T_{2m-1}$.

Теорема 2. *Для существования стационарного режима системы по потоку Π_1 необходимо и достаточно выполнения неравенства*

$$\lambda_1 T(3s_1 + 2q_1 + p_1) - l_1 < 0.$$

Кроме того, из следующей теоремы определяются легко проверяемые необходимые условия существования стационарного режима по потоку Π_m .

Теорема 3. *При одновременном выполнении условий*

$$\lambda_m T_{2m}(3s_m + 2q_m + p_m) - l'_m > 0,$$

$$\lambda_m T_{2m-1}(3s_m + 2q_m + p_m) - l_m > 0$$

или условий

$$\lambda_m(T + T_{2m-1} - T_{2m})(3s_m + 2q_m + p_m) - l_m > 0,$$

$$\lambda_m(T + T_{2m-1})(3s_m + 2q_m + p_m) - l_m - l'_m > 0$$

стационарного режима системы по потоку Π_m не существует.

На основе полученных результатов построена компьютерная имитационная модель системы. Такая модель позволяет экспериментально определить значения параметров $T_1, T_2, \dots, T_{2m+1}, H_1$, при которых достигается наилучшие значения показателей эффективности исследуемой операции. В качестве основного показателя предлагается выбирать среднее время ожидания произвольным требованием начала обслуживания. Цель оптимального управления в таком случае — обратить показатель эффективности в минимум. Пример подобного имитационного исследования можно найти в [3] для системы, осуществляющей операции по циклическому управлению потоками без обратной связи и обслуживанию требований потоков.

СПИСОК ЛИТЕРАТУРЫ

- [1] Fedotkin M., Rachinskaya M. Parameters estimator of the probabilistic model of moving batches traffic flow // Distributed Computer and Communication Networks, Springer International Publishing, Ser. Communications in Computer and Information Science. — 2014. — V. 279. — P. 154–168.
- [2] Федоткин М. А., Рачинская М. А. Модель функционирования системы управления и обслуживания потоков разной интенсивности и приоритетности // Вестник Волжской государственной академии водного транспорта. — 2016. — № 48. — С. 62–69.
- [3] Федоткин М. А., Рачинская М. А. Имитационная модель циклического управления конфликтными неординарными пуассоновскими потоками // Вестник Волжской государственной академии водного транспорта. — 2016. — № 47. — С. 43–51.

ОБОБЩЕНИЕ ФУНКЦИИ ШЕННОНА ДЛЯ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Редькин Николай Петрович

Московский государственный университет имени М. В. Ломоносова, e-mail: npredkin@mail.ru

В математической кибернетике большое значение придается исследованию сложности управляющих систем, среди которых особое место занимают схемы из функциональных элементов [1, 2]. Для них основная задача в наиболее общем ставится так [1]. Задан некоторый конечный функционально полный базис

$B = \{\varphi_1, \dots, \varphi_k\}$, где $\varphi_1, \dots, \varphi_k$ — какие-то попарно различные булевы функции, реализуемые соответственно функциональными элементами $E_1, \dots, E_k$ данного базиса. Каждому элементу E_i приписано отвечающее ему неотрицательное число $P(E_i)$ — вес этого элемента. Обычно предполагается, что если элемент реализует булеву функцию, существенно зависящую от двух или более переменных, то вес такого элемента больше нуля (хотя следует отметить, что имеются и работы, в которых изучается сложность схем в базисах, содержащих элементы с нулевыми весами, см., например, [3]). В качестве меры сложности схемы принимается сумма весов всех элементов, составляющих эту схему; обозначается сложность схемы S через $L(S)$. Число $L(f) = \min L(S)$, где минимум берется по всем схемам в заданном базисе, реализующим булеву функцию f , называется сложностью (реализации) функции f . Если интересуются сложностью реализации булевых функций из некоторого класса F , то в первую очередь рассматривают функцию Шеннона $L(F) = \max L(f)$, где максимум берется по всем булевым функциям из класса F . В качестве основных задач обычно рассматриваются задачи нахождения (или оценки с той или иной степенью точности) функций Шеннона $L(f)$ и $L(F)$.

Для класса $P_2^{(n)}$ всех булевых функций от n переменных О. Б. Лупанов установил [4], что

$$L(P_2^{(n)}) \sim \rho(B) \frac{2^n}{n}, \quad n \rightarrow \infty,$$

где $\rho(B)$ — так называемый приведенный вес базиса B ($\rho(B) = \min \frac{P(E_i)}{r_i - 1}$, где E_i — элемент базиса B , r_i — число существенных переменных функции φ_i , реализуемой элементом E_i , а минимум берется по всем тем элементам E_i , для которых $r_i \geq 2$).

Чтобы указать, какой базис с отвечающими ему весами элементов имеется в виду, используются обозначения $L_B(f)$ и $L_B(F)$. Базисы B_1 и B_2 считаются различными не только когда они содержат различные (неупорядоченные) наборы функций, но и в случае, когда им отвечает один и тот же набор функций $\varphi_1, \dots, \varphi_k$, но разные наборы $P_1, \dots, P_k$ и $P'_1, \dots, P'_k$ весов элементов.

Рассмотрим теперь обобщенные функции Шеннона $L^*(f)$ и $L^*(F)$, полагая $L^*(f) = \sup L_B(f)$, $L^*(F) = \sup L_B(F)$, где верхние грани берутся по всем функционально полным конечным базисам. Для принятой в данном случае меры сложности схем функции $L^*(f)$ и $L^*(F)$ не определены, поскольку $L_B(f)$ и $L_B(F)$ могут быть сколь угодно большими (при достаточно больших весах элементов базиса). Вместе с тем возможно использование и других критериев сложности схем, при которых обобщенные функции Шеннона приобретают вполне определенный содержательный смысл и представляют несомненный интерес.

Рассмотрим, например, широко распространенный критерий, когда под сложностью схемы подразумевается число элементов в ней. При таком критерии, как нетрудно заметить (см., например, [5, с. 162, 214, 215]) сложность реализации (в любом функционально полном базисе) произвольной булевой функции f от n переменных не превосходит $2^{2^n} - n$ и представляет собой целое число из отрезка $[0, 2^{2^n} - n]$, а потому «sup» в определениях $L^*(f)$ и $L^*(F)$ можно заменить на «max». В таком случае $L^*(f)$ (или $L^*(F)$) представляет собой наименьшее возможное число функциональных элементов, которым можно ограничиться при реализации f (соответственно, самой сложнореализуемой функции из F) схемой в любом конечном функционально полном базисе. Из приведенной выше оценки О. Б. Лупанова при растущем n получаем асимптотику

$$L^*(P_2^{(n)}) \sim \frac{2^n}{n}.$$

Решение вопроса о поведении обобщенной функции Шеннона для индивидуальной булевой функции (или для «жидкого» класса булевых функций, например, симметрических) требует отдельного специального исследования. Такое исследование проведено для конъюнкций, т. е. для последовательности булевых функций $x_1, x_1x_2, \dots, x_1x_2 \dots x_n, \dots$. Выбор такой последовательности представляется вполне закономерным, потому что конъюнкция — это одна из важнейших конкретных (или, как часто говорят, индивидуальных) булевых функций. Она оказывается подходящей, весьма удобной с точки зрения реализации («физическими») элементами и потому часто присутствует в качестве одной из функций базиса (например, классического базиса $\{\&, \vee, \neg\}$, базиса Жегалкина $\{\&, \oplus, 0, 1\}$ и др.). В теории часто используется в ряде важных представлений произвольных булевых функций в нормальных формах, полиномах Жегалкина, многочисленных специальных представлениях. Исследованию сложности реализации конъюнкции посвящены работы ряда авторов [6–9].

Здесь получен следующий результат.

Теорема 1. Для любого натурального $n \geq 3$

$$L^*(x_1 \dots x_n) = 3(n - 1);$$

при $n = 1, 2$ значения $L^*(x_1)$ и $L^*(x_1x_2)$ равны соответственно 0 и 4.

Доказательство подобных утверждений, касающихся сложности реализации булевых функций схемами из функциональных элементов, обычно распадается на две части: получение нижних оценок сложности схем и получение (обычно конструктивное) подходящих верхних оценок. В нашем случае нижняя оценка $L^*(x_1x_2) \geq 4$ следует из [9, утв. 2].

При получении верхней оценки для обобщенной функции Шеннона используется метод расширения базиса, предложенный в [10]. Под расширением базиса B понимается всякий базис B' , $B' \supseteq B$, который включает в себя все функции из B , а также те функции, каждая из которых может

быть получена из какой-то функции базиса B отождествлением переменных. Например, если в B входит функция $f(x_1, x_2, x_3, x_4) = x_1\overline{x_2} \vee x_3\overline{x_4}$, то в расширение B' базиса B могут входить $f(x_1, x_1, x_1, x_1) = x_1\overline{x_1} \vee x_1\overline{x_1} = 0$ (получается отождествлением всех четырех переменных функции f), $f(x_1, x_2, x_2, x_1) = x_1\overline{x_2} \vee x_2\overline{x_1} = x_1 \oplus x_2$ (получается путем отождествлений $x_1 \equiv x_4, x_2 \equiv x_3$) и некоторые другие функции. Очевидно, каждому элементу расширения B' , реализующему отсутствующую в B функцию, можно сопоставить эквивалентную ему (в смысле реализующую ту же самую функцию) схему из одного элемента базиса B' , получающуюся из соответствующего элемента базиса B «склеиванием» некоторых его входов. Отсюда следует, что для произвольной функции f выполняется равенство $L_B(f) = L_{B'}(f)$ и для получения верхних оценок сложности реализации булевых функций схемами над B достаточно получить эти оценки для схем над произвольным (в частности над максимальным по мощности) расширением B' базиса B . Имея в расширении B' более богатый (сравнительно с B) выбор базисных функций проще строить и схемы, достаточно близкие к минимальным. А главное то, что, используя понятие расширения базиса, все бесконечное множество возможных базисов можно разбить на относительно небольшое число (в пределах десятка для известных к настоящему времени примеров) пересекающихся классов, в каждом из которых присутствуют несколько функций, достаточных для реализации конъюнкции со сложностью, позволяющей подтвердить искомую верхнюю оценку сложности реализации конъюнкции.

Еще одной весьма важной для теории и приложений индивидуальной булевой функцией является дизъюнкция $x_1 \vee \dots \vee x_n$, n — натуральное число. Поскольку дизъюнкция $x_1 \vee \dots \vee x_n$ является функцией двойственной к конъюнкции $x_1 \dots x_n$ [2], то из теоремы 1 с использованием «принципа двойственности» [2] легко извлекается:

Теорема 2. Для любого натурального $n \geq 3$

$$L^*(x_1 \vee \dots \vee x_n) = 3(n - 1);$$

при $n = 1, 2$ значения $L^*(x_1)$ и $L^*(x_1 x_2)$ равны соответственно 0 и 4.

СПИСОК ЛИТЕРАТУРЫ

- [1] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М. : Изд-во МГУ, 1984. — 138 с.
- [2] Яблонский С. В. Введение в дискретную математику. — М. : Высшая школа, 2003. — 384 с.
- [3] Нечинорук Э. И. О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики. — 1962. — Вып. 8. — С. 123–160.
- [4] Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.

- [5] Редькин Н. П. Дискретная математика. — М. : Физматлит, 2009. — 264 с.
- [6] Сопруненко Е. П. О минимальной реализации некоторых функций схемами из функциональных элементов // Проблемы кибернетики. — 1965. — Вып. 15. — С. 117–134.
- [7] Горелик Е. С. О сложности реализации элементарных конъюнкций и дизъюнкций в базисе x/y // Проблемы кибернетики. — 1973. — Вып. 26. — С. 27–36.
- [8] Минимальная реализация функции $f = x_1x_2 \dots x_r$ схемами из элементов шепферовского типа / С. В. Новиков, В. Э. Комиссаров, В. П. Супрун // Вестник Белорусского университета. — 1975. — Серия 1, № 2. — С. 13–17.
- [9] Кочергина Г. А. О сложности реализации элементарных конъюнкций и дизъюнкций схемами в некоторых полных базисах // Математические вопросы кибернетики. — 2002. — Вып. 11. — С. 219–246.
- [10] Редькин Н. П. О полных проверяющих тестах для схем из функциональных элементов // Математические вопросы кибернетики. — 1989. — Вып. 2. — С. 198–222.

КАНОНИЧЕСКАЯ ЗАДАЧА ДИСПЕТЧЕРИЗАЦИИ: АНАЛИЗ МАСШТАБИРУЕМОСТИ РЕШАЮЩЕГО АЛГОРИТМА ПРИ РЕАЛИЗАЦИИ НА GPU

Резников Михаил Борисович¹, Федосенко Юрий Семенович²

¹ Волжский государственный университет водного транспорта, e-mail: mirekez@gmail.com

² Волжский государственный университет водного транспорта, e-mail: fds@vgavt.ru

Современная практика решения трудоемких оптимизационных задач заключается в распараллеливании работ на массиве вычислительных ресурсов. Такой подход требует разработки специальных алгоритмов, архитектуры и определяет направление развития как универсальных многоядерных ЦПУ и многопроцессорных комплексов, так и создания специализированных вычислительных систем. Для решения вычислительно сложных прикладных задач дискретной оптимизации наиболее распространенной базой является динамическое программирование. Возникающие в транспортных приложениях задачи данного класса характеризуются NP-трудностью и, соответственно, экспоненциальной зависимостью длительности решения от размерности математической модели. Последнее обстоятельство особенно чувствительно для приложений, непосредственно связанных с оперативным планированием и управлением использованием транспортных средств. Ниже на примере канонической задачи диспетчеризации [1] проведено исследование эффективности организации вычислительных процессов с использованием видеокарты (GPU).

Математическая модель

Рассматривается n -элементный детерминированный поток Z независимых объектов $z_1, z_2, \dots, z_n$. Каждый объект $z_i, i = \overline{1, n}$ подлежит однофазному однократному обслуживанию стационарным процессором P и характеризуется следующими целочисленными параметрами: t_i — момент готовности к обслуживанию, τ_i — длительность обслуживания, a_i — штраф за единицу времени пребывания в системе обслуживания. Не ограничивая общности, полагаем выполняющимися неравенства $0 \leq t_1 \leq \dots \leq t_i \leq \dots \leq t_n$. В начальный момент времени $t = 0$ процессор P свободен и находится в состоянии готовности к выполнению обслуживания объектов потока Z . Обслуживание объекта z_i может быть начато свободным процессором P в любой момент времени t ($t \geq t_i$) и осуществляется без прерываний. Необслуженный объект не может покинуть очередь. Одновременное обслуживание процессором P двух и более объектов и его непроизводительные простои запрещены. Поток Z объектов считается обслуженным в том и только в том случае, если завершены обслуживанием все входящие в него объекты.

Расписание обслуживания ρ потока Z отождествляется с перестановкой $p = (p(1), p(2), \dots, p(k), \dots, p(n))$ множества индексов объектов и считается компактным, т. е. момент t'_k начала обслуживания очередного объекта $z_{p(k)}$ определяется соотношениями $t'_1 = t_{p(1)}, t'_k = \max\{t'_{k-1} + \tau_{p(k-1)}, t_{p(k)}\}$ при $k = \overline{2, n}$. Момент t'_n завершения обслуживания потока Z определяется как момент завершения обслуживания объекта $z_{p(n)}$. Каноническая задача диспетчеризации заключается в построении расписания ρ^* , обеспечивающего минимизацию суммарного штрафа по всем объектам потока Z , т. е.

$$W(p) = \sum_{k=1}^n a_{p(k)}(t'_k - t_{p(k)}) \rightarrow \min. \quad (1)$$

Решение (1) может быть получено на основе формализма динамического программирования (DP). Пусть $W_k^{\min}(t, S)$ — минимальная величина суммарного штрафа при обслуживании подмножества объектов S ($S \subset Z$) процессором P , освободившимся в момент времени t после обслуживания объекта $p(k)$, k — порядковый номер обслуживаемого объекта. В этих обозначениях рекуррентное соотношение динамического программирования имеет вид

$$W_k^{\min}(t, S) = \min_{i \notin S, i=\overline{1, n}} (W_{k+1}^{\min}(t' + \tau_i, S \cup z_i) + a_i(t' - t_i)), \quad (2)$$

и решение задачи (1) будет получено на этапе $W^{\min} = W_0^{\min}(0, \emptyset)$, поскольку $W_n^{\min}(t, S) = 0$. Задача (1) относится к классу NP-трудных в сильном смысле [2], её вычислительная сложность пропорциональна 2^n . Соответственно, при традиционной, однопоточной реализации алгоритма продолжительность θ

построения оптимального расписания ρ^* уже для значений $n > 26$ экспоненциально растет от десяти-пятнадцати минут.

Оценка эффективности распараллеливания решающего алгоритма с использованием GPU

С учетом общего числа состояний (t, S) системы и ограничении t некоторым максимальным моментом времени T вычислительная сложность алгоритма DP оценивается величиной $O(T2^n)$, поскольку в каждом состоянии (t, S) требуется n операций доступа к памяти по случайному адресу RAM. Аналогично записывается и оценка требуемого объема оперативной памяти. Поэтапный расчет значений функции штрафа при k от n до 0 обеспечивает доступность значений $W_{k+1}^{min}(t, S)$ на шаге k . При реализации параллельного расчета выполнение алгоритма DP осуществляется в нескольких независимых вычислительных потоках. Соответственно описанный выше порядок вычислений значений функции штрафа независимо и поочередно для каждого шага k обеспечивает необходимую синхронизацию. При этом граф «операции-операнды» для алгоритма аналогичен графу иерархии состояний системы и требует наличия общей памяти либо интенсивной коммуникации между потоками.

Таким образом, производительность параллельного алгоритма ограничена по памяти (memory limited), поскольку с ростом числа потоков интенсивность обращения к RAM возрастет пропорционально. Для количественной оценки эффективности распараллеливания алгоритм DP был реализован на GPU Nvidia GeForce 680 1GHz с числом ядер 1600 и 4GB RAM DDR5 в среде CUDA, под управлением CPU Intel i5 2GHz. В качестве примера на рис. 1 представлена зависимость длительности θ расчета значений функции штрафа для всех состояний при $T = 32$ и $n = 22$.

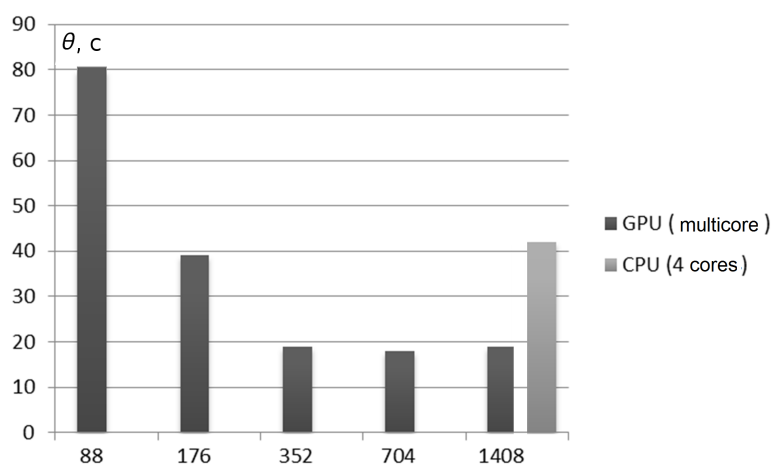


Рис. 1. Время выполнения алгоритма в зависимости от количества ядер.

Из представленных экспериментальных результатов можно сделать следующие выводы: эффект от увеличения количества ядер, вовлеченных в вычислительный процесс, имеет место при их числе до 352 единиц, что составляет

порядка четверти доступных ресурсов; общий выигрыш от использования GPU по сравнению с CPU не более чем двукратный при превосходстве GPU по количеству ядер в два порядка. Заметим при этом, что доступный объем RAM был полностью использован.

Работа выполнена при поддержке РФФИ (проект № 15-07-03141).

СПИСОК ЛИТЕРАТУРЫ

- [1] Коган Д. И., Федосенко Ю. С. Задача диспетчеризации: анализ вычислительной сложности и полиномиально разрешимые подклассы // Дискретная математика. — 1996. — Вып. 3. — С. 135–147.
- [2] Коган Д. И., Федосенко Ю. С. Задачи синтеза оптимальных стратегий обслуживания стационарных объектов в одномерной рабочей зоне процессора // Автоматика и телемеханика. — 2010. — № 10. — С. 50–62.

ОБ АЛГОРИТМЕ ПЕРЕБОРА n -АРНЫХ ГРУППОИДОВ, У КОТОРЫХ КАЖДОЕ ОТНОШЕНИЕ ЭКВИВАЛЕНТНОСТИ ЯВЛЯЕТСЯ ОДНОСТОРОННЕЙ КОНГРУЭНЦИЕЙ

Решетников Артём Владимирович

Национальный исследовательский университет «Московский институт электронной техники», e-mail: a_reshetnikov@hush.com

Пусть (G, f) — частичный n -арный группоид, то есть f — отображение $G' \rightarrow G$, где $G' \subseteq G^n$. Мы говорим, что $G' = \text{dom } f$ — область определения частичной операции f . Для каждого индекса $i \in \{1, \dots, n\}$ и каждого кортежа $\alpha = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in G^{n-1}$ определим на множестве G частичную унарную операцию $\varphi_{i,\alpha}(x) = f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$. Отношение эквивалентности ρ на G назовём R_i -конгруэнцией, или односторонней конгруэнцией, если, каким бы ни был кортеж $\alpha \in G^{n-1}$, отношение ρ является конгруэнцией частичного унара $(G, \varphi_{i,\alpha})$. В случае $\text{dom } f = G^n$ говорим, что (G, f) — n -арный группоид.

Нас интересуют n -арные группоиды G , обладающие следующим свойством: все отношения эквивалентности на G являются односторонними конгруэнциями, и для любого значения i найдётся отношение эквивалентности на G , не являющееся R_i -конгруэнцией. Обозначим класс таких n -арных группоидов через K_n .

Случай $n = 2$ полностью рассмотрен в работе [2], некоторые результаты для случая $n \geq 3$ приведены в статье [3].

Для решения некоторых вопросов были составлены компьютерные программы. Приведём утверждения, лежащие в основе их работы. Понятия *изоморфизма* и *продолжения* считаем известными из теории частичных универсальных алгебр (см., например, главу 1 монографии [1], соответственно §2 и §6, где эти определения даны для частичных бинарных группоидов).

Предложение 1. Пусть для частичного n -арного группоида G существует продолжение до n -арного группоида из класса K_n . Тогда все отношения эквивалентности на G являются односторонними конгруэнциями.

Для произвольной частичной n -арной операции f и подстановки σ из n элементов определим частичную n -арную операцию $f^\sigma(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

Предложение 2. Пусть (G, f) — частичный n -арный группоид. Если отношение эквивалентности $\rho \subseteq G^2$ не является односторонней конгруэнцией для (G, f) , то, каким бы ни было продолжение (G, g) частичного n -арного группоида (G, f) , какой бы ни была подстановка σ из n элементов, ни для какого частичного n -арного группоида, изоморфного (G, g^σ) , отношение ρ не является односторонней конгруэнцией.

СПИСОК ЛИТЕРАТУРЫ

- [1] Ляпин Е. С., Евсеев А. Е. Частичные алгебраические действия. — С.-Петербург: Росс. гос. пед. ун-т им. А. И. Герцена, Образование, 1991. — 163 с.
- [2] Кожухов И. Б., Решетников А. В. Алгебры, у которых все отношения эквивалентности являются конгруэнциями // Фундаментальная и прикладная математика. — 2010. — Т. 16, № 3. — С. 161–192.
- [3] Решетников А. В. Об односторонних конгруэнциях n -арного группоида // Электронные информационные системы. — 2016. — № 1(8). — С. 89–95.

О ТЕСТАХ ДЛЯ СХЕМ ПРИ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

Романов Дмитрий Сергеевич

Московский государственный университет имени М. В. Ломоносова, e-mail: romanov@cs.msu.ru

Схемы из функциональных элементов (СФЭ, см., например, [1]) — одна из классических моделей дискретных управляющих систем без памяти; анализ функционирования СФЭ при возникновении в них неисправностей традиционно осуществляется с помощью тестового подхода [8]. Пусть на схему S с входами $x_1, x_2, \dots, x_n$, реализующую булеву функцию или систему булевых функций $f(x_1, x_2, \dots, x_n)$, действует источник неисправностей U , способный преобразовать схему S к одной из СФЭ (с такими же входами и выходами, что и у S) некоторого заранее известного списка H конечной длины, содержащего и исходную схему. Определения проверяющего и диагностического теста вводятся традиционным образом [1, 6]. Тест минимальной длины называется минимальным, число наборов в тесте T называется длиной теста и обозначается $L(T)$. Источник неисправностей U , способный вызвать поломку

не более чем одного элемента схемы, называется единичным; тесты относительно такого источника также называются единичными. Тесты относительно источника, способного вызвать произвольное число поломок элементов, называются полными. *Нетривиальной* будем называть неисправность СФЭ, при которой меняется распространение сигналов в схеме. Схема S , при любой неисправности (нетривиальной неисправности) под действием источника неисправностей U реализующая функцию или систему функций, неравную функции или системе функций, реализуемой схемой S в отсутствие неисправностей, называется *тестопригодной* (*квазитестопригодной*) относительно источника неисправностей S . Схема, тестопригодная (квазитестопригодная) относительно единичного источника неисправностей, называется *неизбыточной* (*квазинеизбыточной*). Под длиной минимального проверяющего (диагностического) теста для булевой функции или системы функций f , реализованной с помощью СФЭ в базисе B , относительно источника неисправностей U понимается величина $L_B^{\text{detect}}(U, f)$ ($L_B^{\text{diagn}}(U, f)$), равная минимуму по всем тестопригодным реализующим f СФЭ S в базисе B минимума по всем проверяющим (соответственно диагностическим) тестам T для S относительно U величины $L(T)$. Пусть $\hat{P}_2(n)$ — множество всех булевых функций, существенно зависящих от всех своих n переменных $x_1, x_2, \dots, x_n$. *Функцией Шеннона* длины проверяющего (диагностического) теста для реализованной с помощью СФЭ в базисе B булевой функции f относительно источника неисправностей U называется величина $L_B^{\text{detect}}(U, n) = \max_{f \in \hat{P}_2(n)} L_B^{\text{detect}}(U, f)$ (соответственно, величина $L_B^{\text{diagn}}(U, n) = \max_{f \in \hat{P}_2(n)} L_B^{\text{diagn}}(U, f)$).

Неисправность в некотором месте схемы (на входе схемы или функционального элемента или на выходе функционального элемента) называется константной, если для каждого входного набора значение, вычисляемое в этом месте, заменяется на какую-то константу. Неисправность в некотором месте схемы называется инверсной, если значение, вычисляемое в этом месте при отсутствии данной неисправности (все остальные неисправности в схеме, если они есть, при этом сохраняются), заменяется на противоположное. Условимся о следующих обозначениях для источников неисправностей в СФЭ. Обозначение для источника неисправностей будет иметь вид X_z^y , где X — это одна или несколько заглавных латинских букв, указывающих на место возможной неисправности (P — неисправности на входах схем, I — неисправности на входах функциональных элементов, O — неисправности на выходах функциональных элементов), y — это название типа неисправности (const, 0, 1 — константные неисправности, константные неисправности типа 0 и константные неисправности типа 1 соответственно, inv — инверсные неисправности), z указывает на число возможных неисправностей (k , если неисправностей не больше k ; ниж-

ний индекс отсутствует, если ограничений на число неисправных элементов в схеме нет).

Справедливы следующие утверждения.

Теорема 1. При всяком $n \in \mathbb{N}$, $n \geq 2$, для любой булевой функции n переменных существует реализующая ее квазинеизбыточная СФЭ в произвольном конечном полном базисе B , допускающая проверяющий тест длины 3 относительно O_1^{const} . Если при этом B — неприводимая полная в P_2 система функций от не более чем двух переменных, не содержащая констант и отличная от $\{x \& \bar{y}, x \vee \bar{y}\}$, то $L_B^{\text{detect}}(O_1^{\text{const}}, n) = 3$ при $n \geq 3$.

Верхние оценки в теореме 1 получаются незначительными модификациями рассуждений из [6], нижняя следует из работы К. А. Попкова [5].

Теорема 2. Существует такая константа $c > 0$, что при всяком $n \in \mathbb{N}$ для СФЭ в базисе $B' = \{x \& y, x \oplus y, x \sim y\}$ имеют место неравенства $L_{B'}^{\text{detect}}(O_2^{\text{const}}, n) \leq L_{B'}^{\text{diagn}}(O_2^{\text{const}}, n) \leq c$.

Теорема 2 получается применением модифицированной техники, предложенной в работе [7]. С учетом результатов работ [2–4] о поведении функции Шеннона длины проверяющего и диагностического теста относительно кратных константных неисправностей на входах схем оказывается справедливым следующее утверждение.

Теорема 3. При $n \in \mathbb{N}$, $n \rightarrow \infty$ для СФЭ в базисе $B' = \{x \& y, x \oplus y, x \sim y\}$ имеют место асимптотические равенства $L_{B'}^{\text{detect}}(PO_2^{\text{const}}, n) = 2n - 2 \log_2 n + \Theta(1)$, $L_{B'}^{\text{diagn}}(PO_2^{\text{const}}, n) = \Theta(n^2)$.

Отметим, что при моделировании с помощью СФЭ полиномов Жегалкина оказывается справедливым следующий простой факт.

Теорема 4. При всяком $n \in \mathbb{N} \cup \{0\}$ для любой булевой функции $f(x_1, \dots, x_n)$ существует избыточная СФЭ в бесконечном базисе $B^\infty = \{x_1 \& \dots \& x_m, x_1 \oplus x_2, x_1 \sim x_2 \mid m \in \mathbb{N}, m \geq 2\}$ такая, что длина ее минимального полного диагностического теста при инверсных неисправностях на выходах элементов равна 1.

Автор выражает благодарность профессору С. А. Ложкину за внимание к работе.

Работа выполнена при поддержке РФФИ (проекты № 15-01-07474-а, № 16-01-00593-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М. : Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с.
- [2] Носков В. Н. Диагностические тесты для входов логических устройств // Дискретный анализ. — Новосибирск : ИМ СО АН СССР, 1974. — № 26. — С. 72–83.

- [3] Носков В. Н. О сложности тестов, контролирующих работу входов логических схем // Дискретный анализ. — Новосибирск : ИМ СО АН СССР, 1975. — № 27. — С. 23–51.
- [4] Погосян Г. Р. О проверяющих тестах для логических схем. — М. : ВЦ АН СССР, 1982. — 57 с.
- [5] Попков К. А. Нижние оценки длин единичных тестов для схем из функциональных элементов. Препринт № 139 ИПМ им. М. В. Келдыша РАН. — М. : ИПМ им. М. В. Келдыша РАН, 2016. — 20 с.
- [6] Романов Д. С. Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. — 2014. — Т. 26, вып. 2. — С. 100–130.
- [7] Романов Д. С., Романова Е. Ю. Метод синтеза неизбыточных схем, допускающих короткие единичные диагностические тесты при константных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2016. — № 2. — С. 87–102.
- [8] Чегис И. А., Яблонский С. В. Логические способы контроля электрических схем // Тр. МИАН СССР. — 1958. — Т. 51. — С. 270–360.

ОЦЕНКИ ФУНКЦИЙ ШЕННОНА ДЛИН ТЕСТОВ ДЛЯ ЛОГИЧЕСКИХ СХЕМ

Романов Дмитрий Сергеевич

Московский государственный университет имени М. В. Ломоносова, e-mail: romanov@cs.msu.ru

Схемы из функциональных элементов (СФЭ) — одна из классических моделей дискретных управляющих систем без памяти; анализ функционирования СФЭ при возникновении в них неисправностей традиционно осуществляется с помощью тестового подхода (см., напр., [1]). Определения проверяющего и диагностического теста вводятся традиционным образом [1]. Число наборов в тесте T называется длиной теста и обозначается $L(T)$. Источник неисправностей U , способный вызвать поломку не более чем одного элемента схемы, называется единичным; тесты относительно такого источника также называются единичными. Тесты относительно источника, способного вызвать произвольное число поломок элементов, называются полными. *Нетривиальной* будем называть неисправность СФЭ, при которой меняется распространение сигналов в схеме. Схема S , при любой неисправности (нетривиальной неисправности) под действием источника неисправностей U реализующая функцию или систему функций, неравную функции или системе функций, реализуемой схемой S в отсутствие неисправностей, называется *тестопригодной* (*квазитестопригодной*) относительно источника неисправностей S . Схема, тестопригодная

(квазитестопригодная) относительно единичного источника неисправностей, называется *неизбыточной* (квазинеизбыточной). Под длиной минимального проверяющего (диагностического) теста для булевой функции или системы функций f , реализованной с помощью СФЭ в базисе B , относительно источника неисправностей U понимается величина $L_B^{\text{detect}}(U, f)$ ($L_B^{\text{diagn}}(U, f)$), равная минимуму по всем тестопригодным реализующим f СФЭ S в базисе B минимуму по всем проверяющим (соответственно диагностическим) тестам T для S относительно U величины $L(T)$. Пусть $\hat{P}_2(n)$ — множество всех булевых функций, существенно зависящих от всех своих n переменных $x_1, x_2, \dots, x_n$. *Функцией Шеннона* длины проверяющего (диагностического) теста для реализованной с помощью СФЭ в базисе B булевой функции f относительно источника неисправностей U называется величина $L_B^{\text{detect}}(U, n) = \max_{f \in \hat{P}_2(n)} L_B^{\text{detect}}(U, f)$

(соответственно, величина $L_B^{\text{diagn}}(U, n) = \max_{f \in \hat{P}_2(n)} L_B^{\text{diagn}}(U, f)$). Введем обозна-

чения для источников неисправностей в СФЭ. Обозначение для источника неисправностей будет иметь вид X_z^y , где X — это одна или несколько заглавных латинских букв, указывающих на место возможной неисправности (P — на входах схем, I — на входах функциональных элементов, O — на выходах функциональных элементов), y — это название типа неисправности (const, 0, 1 — константные, константные типа 0 и константные типа 1 соответственно, inv — инверсные неисправности), z указывает на число возможных неисправностей (k , если неисправностей не больше k ; нижний индекс отсутствует, если ограничений на число неисправных элементов в схеме нет). Введем обозначения для базисов: $B_0 = \{x \& y, x \vee y, \bar{x}\}$, $B_1 = \{x \& y, x \oplus y, 1\}$, $B' = \{x \& y, x \oplus y, x \sim y\}$, $B_0^\infty = \{\bar{x}\} \cup \bigcup_{i \geq 2} \{x_1 \& \dots \& x_i, x_1 \vee \dots \vee x_i\}$. Приведем

обзор некоторых оценок функций Шеннона длин тестов для СФЭ без введения в схемы дополнительных входов и выходов. $L_{B_1}^{\text{detect}}(IO_1^{\text{const}}, n) \leq n + 4$ [2],

$L_{B_1}^{\text{detect}}(PIO_1^{\text{const}}, n) \leq 3n + 4$ [2], $L_{B_1}^{\text{detect}}(IO_k^{\text{const}}, n) \leq 4 + \sum_{j=1}^{\lfloor \log 2k \rfloor} \binom{n}{j}$ [3]; для про-

извольного полного конечного базиса B : $L_B^{\text{detect}}(O^{\text{const}}, n) \leq 2(2^{\lceil n/2 \rceil} + 2^{\lfloor n/2 \rfloor} + n)$ [4, 5]; $L_{B_0}^{\text{detect}}(I^0, n) = L_{B_0}^{\text{detect}}(I^1, n) \leq O(2^{n/2})$

[6]; $L_{B_0}^{\text{detect}}(O^0, n) = L_{B_0}^{\text{detect}}(O^1, n) \leq n$ [7]; $L_{B_0}^{\text{diagn}}(O_1^0, n) = L_{B_0}^{\text{diagn}}(O_1^1, n) \leq 2n + 1$ [8]; $L_{B_0}^{\text{diagn}}(O_1^0, n) = L_{B_0}^{\text{detect}}(O_1^1, n) \leq 2\lceil \log_2 n + 1 \rceil + 1$ [9]; $L_{B_1}^{\text{diagn}}(O_1^{\text{inv}}, n) \leq n + 1$,

$L_{B_1}^{\text{diagn}}(O^{\text{inv}}, n) \leq 2^{n-2}$ [10]; в произ-

вольном полном базисе B : $L_B^{\text{detect}}(O_1^{\text{const}}, n) \leq n + 3$ [11]. Особый интерес

представляют константные верхние оценки функций Шеннона длины теста:

$L_{B_1}^{\text{detect}}(O_1^{\text{inv}}, n) = 1$ [10]; в произвольном полном базисе B : $L_B^{\text{detect}}(O_1^{\text{inv}}, n) \leq 3$ [12]; $L_{B_0}^{\text{detect}}(O^0, n) = L_{B_0}^{\text{detect}}(O^1, n) = 2$ при $n > 1$ [13]; $L_{B_1}^{\text{detect}}(O_1^1, n) = 1$ [14];

$L_{B_1}^{\text{detect}}(O^0, n) = 1$ [15]; отметим, впрочем, что $L_{\{x|y\}}^{\text{detect}}(O^1, n) \geq n + 1$ [16]; для

произвольного полного базиса B : $2 \leq L_B^{\text{detect}}(O_1^{\text{const}}, n) \leq 4$ [17] (перебор ведется по квазинеизбыточным схемам); найдены примеры полных конечных базисов $\tilde{B}'$, $\tilde{B}''$ таких, что $2 \leq L_{\tilde{B}'}^{\text{detect}}(O^{\text{const}}, n) \leq 4$ [18], $2 \leq L_{\tilde{B}'}^{\text{detect}}(O^{\text{inv}}, n) \leq 4$ [19]; $L_{B_0}^{\text{diagn}}(O_1^0, n) = L_{B_0}^{\text{diagn}}(O_1^1, n) = 2$ [20]; $L_{B_1}^{\text{diagn}}(O_1^{\text{inv}}, n) = 1$ [21]; $L_{B_1}^{\text{diagn}}(O_1^0, n) = 2$ [22]; $L_{B_0}^{\text{diagn}}(O_1^{\text{inv}}, n) = 2$ [23]; $L_{B'}^{\text{diagn}}(O_1^{\text{const}}, n) \leq 22$ [24]; в любом полном базисе B , содержащемся в множестве элементарных конъюнкций с одинаковыми степенями переменных, линейных функций двух переменных и функций, представляющих собой конъюнкцию $x_1 \bar{x}_2$ и некоторой функции, при $n \geq 3$ $L_B^{\text{detect}}(O_1^{\text{const}}, n) \geq 3$ [25]. Работа выполнена при поддержке РФФИ (проекты № 15-01-07474-а, № 16-01-00593-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Редькин Н. П. Надежность и диагностика схем. — М. : Изд-во МГУ, 1992. — 192 с.
- [2] Reddy S. M. Easily testable realization for logic functions // IEEE Trans. Comput. — 1972. — Vol. 21, Iss. 1. — Pp. 124–141.
- [3] Saluja K. K., Reddy S. M. Fault detecting test sets for Reed–Muller canonic networks // IEEE Trans. Comput. — 1975. — Vol. 24, No. 1. — Pp. 995–998.
- [4] Редькин Н. П. О полных проверяющих тестах для схем из функциональных элементов // Вестник Моск. ун-та. Сер. 1. Матем. Мех. — 1986. — № 1. — С. 72–74.
- [5] Редькин Н. П. О полных проверяющих тестах для схем из функциональных элементов // Матем. вопросы киберн. — Вып. 2. — М. : Наука, 1989. — С. 198–222.
- [6] Редькин Н. П. О проверяющих тестах для схем при однотипных константных неисправностях на входах элементов // Изв. вузов. Матем. — 1988. — № 7. — С. 57–64.
- [7] Редькин Н. П. О схемах, допускающих короткие тесты // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 1988. — № 2. — С. 17–21.
- [8] Редькин Н. П. О единичных диагностических тестах для однотипных константных неисправностей на выходах функциональных элементов // Вестник Моск. ун-та. Сер. 1. Матем. Мех. — 1992. — № 5. — С. 43–46.
- [9] Редькин Н. П. О синтезе легкотестируемых схем в одном бесконечном базисе // Вестник Моск. ун-та. Сер. 1. Матем. Мех. — 2007. — № 3. — С. 29–33.
- [10] Коваценко С. В. Синтез легкотестируемых схем в базисе Жегалкина для инверсных неисправностей // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2000. — № 2. — С. 45–47.

- [11] Коляда С. С. Единичные проверяющие тесты для схем из функциональных элементов // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2013. — № 4. — С. 32–34.
- [12] Редькин Н. П. Единичные проверяющие тесты для схем при инверсных неисправностях элементов // Матем. вопросы киберн. — Вып. 12. — М. : Физматлит, 2003. — С. 217–230.
- [13] Бородина Ю. В. О синтезе легкотестируемых схем в случае однотипных константных неисправностей на выходах элементов // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2008. — Т. 63, № 1. — С. 40–44.
- [14] Бородина Ю. В. О схемах, допускающих единичные тесты длины 1 при константных неисправностях на выходах элементов // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2008. — № 5. — С. 49–52.
- [15] Бородина Ю. В., Бородин П. А. Синтез легкотестируемых схем в базисе Жегалкина при константных неисправностях типа «0» на выходах элементов // Дискр. матем. — 2010. — Т. 22, вып. 3. — С. 127–133.
- [16] Бородина Ю. В. Нижняя оценка длины полного теста в базисе $\{x|y\}$ // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2015. — Т. 70, № 4. — С. 49–51.
- [17] Романов Д. С. Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискр. матем. — 2014. — Т. 26, вып. 2. — С. 100–130.
- [18] Романов Д. С. О синтезе схем, допускающих полные проверяющие тесты константной длины относительно произвольных константных неисправностей на выходах элементов // Дискр. матем. — 2013. — Т. 5, вып. 2. — С. 104–120.
- [19] Романов Д. С. О синтезе схем, допускающих полные проверяющие тесты константной длины относительно инверсных неисправностей на выходах элементов // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2015. — № 1. — С. 30–37.
- [20] Попков К. А. О точном значении длины минимального единичного диагностического теста для одного класса схем. — М. : ИПМ им. М. В. Келдыша РАН, 2015. — 20 с.
- [21] Романов Д. С. Метод синтеза избыточных схем в базисе Жегалкина, допускающих единичные диагностические тесты длины один // Изв. высших учебных заведений. Поволжский регион. Физ.-мат. науки. — 2015. — № 4. — С. 38–54.
- [22] Попков К. А. О единичных диагностических тестах для схем из функциональных элементов в базисе Жегалкина. — Москва : ИПМ им. М. В. Келдыша РАН, 2016. — 16 с.

- [23] Романов Д. С. Метод синтеза избыточных схем в стандартном базисе, допускающих единичные диагностические тесты длины два // Изв. высших учебных заведений. Поволжский регион. Физ.-мат. науки. — 2016. — № 3. — С. 56-72.
- [24] Романов Д. С., Романова Е. Ю. Метод синтеза избыточных схем, допускающих короткие единичные диагностические тесты при константных неисправностях на выходах элементов // Изв. высших учебных заведений. Поволжский регион. Физ.-мат. науки. — 2016. — № 2. — С. 87-102.
- [25] Попков К. А. Нижние оценки длин единичных тестов для схем из функциональных элементов. — М. : ИПМ им. М. В. Келдыша РАН, 2016. — 20 с.

ЧИСЛО СУММ И РАЗНОСТЕЙ В АБЕЛЕВЫХ ГРУППАХ

Саргсян Ваге Гнелович

Московский государственный университет имени М. В. Ломоносова, e-mail: vahe_sargsyan@yandex.ru

Пусть G — абелева группа порядка n , а $k \geq 0$ и $l \geq 0$ — целые числа, удовлетворяющие условию $k + l \geq 2$, и $A \subseteq G$. Обозначим $-A = \{-x \mid x \in A\}$, $A + A = \{x_1 + x_2 \mid x_1, x_2 \in A\}$, $A - A = \{x_1 - x_2 \mid x_1, x_2 \in A\}$. Подмножество $A \subseteq G$ называется (k, l) -суммой, если существует подмножество $B \subseteq G$ такое, что $A = \underbrace{B + \dots + B}_k - \underbrace{B - \dots - B}_l$. В частности, $(1, 1)$ -сумма называется раз-

ностью, а $(2, 0)$ -сумма — просто суммой. Семейство (k, l) -сумм в G обозначим через $SS_{k,l}(G)$, а через Z_n — группу по модулю n . В работах [1] и [2] были получены следующие результаты соответственно.

Теорема 1. Пусть p — простое число. Тогда справедливы соотношения $p^2 2^{p/3} = o(|SS_{2,0}|)$ и $|SS_{2,0}(Z_p)| \leq 2^{p/3 + \kappa(p)}$, где $\kappa(p)/p \rightarrow 0$ при $p \rightarrow \infty$, причем $\kappa(p) = o(p(\log \log p)^{2/3}(\log p)^{-1/9})$.

Теорема 2. Пусть p — простое число. Тогда справедливы соотношения $p^2 2^{p/3} = o(|SS_{1,1}(Z_p)|)$ и $|SS_{1,1}(Z_p)| \leq 2^{p/3 + \kappa(p)}$, где $\kappa(p)/p \rightarrow 0$ при $p \rightarrow \infty$, причем $\kappa(p) = o(p(\log \log p)^{2/3}(\log p)^{-1/9})$.

Пусть $D(G)$ — размер наибольшей собственной подгруппы группы G , а $\varphi(n)$ — функция Эйлера. В этой работе доказывается следующая теорема.

Теорема 3. Пусть G — абелева группа порядка n и экспоненты ν , а k, l — неотрицательные целые числа, и $k + l = 2$. Тогда при $n, \nu \rightarrow \infty$ справедливы оценки $\nu \varphi(\nu) 2^{\nu/3} = o(|SS_{k,l}(G)|)$ и $|SS_{k,l}(G)| \leq 2^{n/3 + D(G)/3 + o(n)}$.

Нижняя оценка

Лемма 1. Пусть G — абелева группа. Тогда следующие утверждения эквивалентны: (A) — экспонента группы G делится на d ; (B) — существует подгруппа H группы G такая, что факторгруппа G/H изоморфна циклической группе Z_d .

Лемма 2. Пусть n — натуральное число, а k и l — неотрицательные целые числа, и $k + l = 2$. Тогда справедлива оценка $n\varphi(n)2^{n/3} = o(|SS_{k,l}(Z_n)|)$ при $n \rightarrow \infty$.

Пусть G — абелева группа порядка n и экспоненты ν . В силу леммы 1 существует подгруппа H группы G такая, что факторгруппа G/H изоморфна циклической группе Z_ν . Тогда существует элемент g порядка ν такой, что $G = H \cup (g + H) \cup \dots \cup ((\nu - 1)g + H)$. Для каждого подмножества B факторгруппы G/H $B = \{(b_i + H) \mid b_i \in \{0, g, \dots, (\nu - 1)g\}, i = 1, \dots, |B|\}$ положим $B'(B) = \{b_i \mid b_i \in \{0, g, \dots, (\nu - 1)g\}, i = 1, \dots, |B|\} \subseteq G$. Заметим, что если B_1, B_2 — различны, то различны и подмножества $B'_1(B_1), B'_2(B_2)$. Нетрудно убедиться, что если $B = kA - lA$ для некоторого $A \subseteq G/H$, то $B'(B) = kA'(A) - lA'(A) \subseteq G$. Так как факторгруппа G/H изоморфна циклической группе Z_ν , то в силу леммы 2 получаем нижнюю оценку.

Верхняя оценка

Пусть G — абелева группа порядка n , а $f_i: G \rightarrow \mathbb{R}, i = 1, \dots, m$. Тогда

$$(f_1 * \dots * f_m)(x) = \sum_{x_1 \in G} \dots \sum_{x_{m-1} \in G} f_1(x_1) \dots f_{m-1}(x_{m-1}) f_m(x - x_1 - \dots - x_{m-1}).$$

Пусть $A_1, \dots, A_m$ — непустые подмножества группы G . Обозначим через $A_1(x), \dots, A_m(x)$ характеристические функции соответственно множеств $A_1, \dots, A_m$. Тогда $r(A_1, \dots, A_m, x) = (A_1 * \dots * A_m)(x)$ есть количество наборов $(x_1, \dots, x_m) \in A_1 \times \dots \times A_m$, таких, что $x = x_1 + \dots + x_m$. Положим $S_h(A_1, \dots, A_m) = \{x \in G \mid (A_1 * \dots * A_m)(x) \geq h\}$.

Лемма 3. Пусть G — абелева группа порядка n , а A, B — непустые подмножества группы G , и $h > 0$ такое, что $\sqrt{hn} \leq \min(|A|, |B|)$. Тогда справедлива оценка $|S_h(A, B)| \geq \min(n, |A| + |B| - D(G)) - 3\sqrt{hn}$.

L -гранулой типа смежного класса называется объединение смежных классов группы G по некоторой подгруппе порядка не меньше L .

Пусть L — целое число и $d \in G$, причем $\text{ord}(d) \geq L$, где $\text{ord}(d)$ — порядок элемента d . Рассмотрим подгруппу G , порожденную элементом d , и разобьём каждый её смежный класс на $\lfloor \text{ord}(d)/L \rfloor$ прогрессий вида $\{x + id \mid 0 \leq i \leq L - 1\}$ и одно «остаточное» множество мощности менее L . Для каждого $d \in G$ фиксируем одно такое разбиение. Объединение полученных прогрессий называется L -гранулой типа прогрессии.

Лемма 4. Пусть n — достаточно большое натуральное число, а G — абелева группа порядка n . Тогда в группе G есть не более $2^{3n/L}$ L -гранул обоих типов (прогрессии и смежного класса).

Лемма 5. Пусть n — достаточно велико, и M — множество мощности n , а ρ — вещественное число, меньшее некоторой абсолютной положительной константы. Тогда, число подмножеств множества M , мощности не более ρn , не превосходит $2^{n\sqrt{\rho}}$.

Лемма 6 (гранулирование). Пусть n — достаточно большое натуральное число, G — абелева группа порядка n , и $k > l \geq 0$, $k + l \geq 2$, A — произвольное подмножество группы G , а $\varepsilon \in (0, \frac{1}{2})$, L и L' — положительные числа, удовлетворяющие неравенству $n > L'(4L/\varepsilon)^{4^{2(k+l)+1}(k+l)^2\varepsilon^{-2(k+l)-3}}$. Тогда существует подмножество $A' \subseteq G$ такое, что A' — либо L -гранула типа прогрессии, либо L' -гранула типа смежного класса, $|A \setminus A'| \leq \varepsilon n$, множество $kA - lA$ содержит все элементы $x \in G$ такие, что

$$\underbrace{(A' * \dots * A')}_k * \underbrace{(-A') * \dots * (-A')}_l(x) \geq \varepsilon n^{k+l-1},$$

за исключением не более εn элементов.

Пусть G — абелева группа порядка n , а $k > l \geq 0$, и $k + l = 2$. Положим $L = L' = \lfloor \log n \rfloor$ и $\varepsilon = (\log n)^{-1/8}$. Заметим, что при достаточно большом n такой выбор параметров удовлетворяет условию леммы 6 для случая $k + l = 2$. Для каждого множества $A \subseteq G$, применяя лемму 6, построим множество $A'(A)$. Оценим величину $|SS_{k,l}(G)|$ путем подсчета количества соответствующих пар $(A'(A), kA - lA)$. Пусть A' — гранула типа прогрессии или смежного класса. Для каждого фиксирования A' рассмотрим два случая: $|A'| > n/3 + D(G)/3$ и $|A'| \leq n/3 + D(G)/3$. Пусть $|A'| > n/3 + D(G)/3$. В силу пункта (iii) леммы 6 получим, что множество $kA - lA$ является подмножеством объединения множества $\overline{S_{\varepsilon n}(\underbrace{A', \dots, A'}_k, \underbrace{(-A)', \dots, (-A)'}_l)}$ с некоторым подмножеством группы G мощности, не превышающей εn . В силу леммы 3 при условии $|A'| > n/3 + D(G)/3$ получим, что

$$|\overline{S_{\varepsilon n}(\underbrace{A', \dots, A'}_k, \underbrace{(-A)', \dots, (-A)'}_l)}| \leq n/3 + D(G)/3 + 3n\sqrt{\varepsilon}.$$

Из леммы 5 и того, что множество $kA - lA$ однозначно определяет множество $kA - lA$, получим, что число способов выбора $kA - lA$ при заданном множестве A' мощности, превышающей $n/3 + D(G)/3$, не превосходит $2^{n/3+D(G)/3+4n\sqrt{\varepsilon}}$. Пусть $|A'| \leq n/3 + D(G)/3$. По пункту (ii) леммы 6 следует, что A является подмножеством объединения множества A' с некоторым подмножеством группы G мощности, не превышающей εn . Из леммы 5 и того, что каждое множество $A \subseteq G$ порождает ровно одно множество вида $kA - lA$, следует, что число способов выбора $kA - lA$ при заданном множестве A' мощности, не превышающей $n/3 + D(G)/3$, не превосходит $2^{n/3+D(G)/3+n\sqrt{\varepsilon}}$.

Из вышеизложенного и леммы 4, с учетом того, что $3n/L \leq n\sqrt{\varepsilon}$ при достаточно большом n , получаем $|SS_{k,l}(G)| \leq 2^{n/3+D(G)/3+\bar{o}(n)}$ при $n \rightarrow \infty$.

Работа выполнена при поддержке РФФИ (проект № 16-01-00593-а).
СПИСОК ЛИТЕРАТУРЫ

- [1] Green B., Ruzsa I. Counting sumsets and sum-free sets modulo a prime // *Studia Sci. Math. Hungarica.* — 2004. — Vol. 41. — P. 285–293.
- [2] Саргсян В. Г. Число разностей в группах простого порядка // *Дискретная математика.* — 2013. — Т. 25, вып. 1. — С. 152–158.

О ДЛИНЕ ПОЛИНОМОВ НЕ ВСЮДУ ОПРЕДЕЛЕННЫХ ФУНКЦИЙ k -ЗНАЧНОЙ ЛОГИКИ

Селезнева Светлана Николаевна

Московский государственный университет имени М. В. Ломоносова, e-mail: selezn@cs.msu.su

В работе получена асимптотика длины полиномов не всюду определенных k -значных функций.

Пусть $E_k = \{0, 1, \dots, k-1\}$, где $k \geq 2$ — целое число. Рассматриваем множество $P_k = \{f^{(n)} : E_k^n \rightarrow E_k \mid n = 0, 1, 2, \dots\}$ всех функций k -значной логики, или k -значных функций. Далее считаем, что на множестве E_k задано поле $(E_k; +, \cdot)$ с нулем 0. В этом случае каждая k -значная функция $f \in P_k$ может быть однозначно представлена таким полиномом $P(f)$ относительно операций этого поля, в котором степени всех переменных не выше $(k-1)$ [1, 2]. Длиной $l(P)$ полинома P назовем число его различных слагаемых с ненулевыми коэффициентами, $l(0) = 0$.

Ранее в [3, 4] исследовалась длина полиномов, приближающих k -значные функции с заданной точностью. При этом функция $g(x_1, \dots, x_n) \in P_k$ называется приближением функции $f(x_1, \dots, x_n) \in P_k$ с точностью δ , $0 \leq \delta \leq 1$, если доля наборов значений переменных, в которых функции f и g различаются, не превосходит δ . Считается, что полином $P(g)$ приближает k -значную функцию f с точностью δ , если функция g является приближением функции f с точностью δ . При таком определении исходная функция и ее приближение могут отличаться на произвольных множествах наборов, требование накладывается лишь на мощность этих множеств. В настоящей работе мы рассматриваем более сильное ограничение, а именно, исходная функция обязана быть точно задана на некотором заранее известном множестве наборов E . Такие функции назовем не всюду определенными.

Если $f(x_1, \dots, x_n) \in P_k$ и $E \subseteq E_k^n$, то функцию f вместе с множеством E назовем *не всюду определенной k -значной функцией* с областью определения $E(f) = E$. Функция $g(x_1, \dots, x_n) \in P_k$ называется *доопределением* функции $f(x_1, \dots, x_n) \in P_k$ с множеством E , $E \subseteq E_k^n$, если для каждого набора $\alpha \in E$ верно $g(\alpha) = f(\alpha)$. Полином $P(g)$ доопределяет k -значную функцию f с множеством E , если функция g является доопределением функции f с этим множеством.

В [3, 4] рассматривалась длина полиномов, приближающих функции. Длиной $l^\delta(f)$ функции f с точностью δ называется наименьшая длина среди

всех полиномов, приближающих функцию f с точностью δ . Получены оценки наибольшей длины $l_k^{\delta_n}(n)$ с точностью δ_n среди всех k -значных функций, зависящих от n переменных:

$$\begin{aligned} l_2^{\delta}(n) &= 1 \text{ при } \delta \geq \frac{1}{2} \text{ [3]}, \\ l_k^{\delta}(n) &= 1 \text{ при } \delta \geq \frac{k-1}{k} \text{ [4]}, \\ l_2^{\delta}(n) &\leq \frac{1}{2} \cdot (1 - \delta) \cdot 2^n + o(2^n) \text{ при } 0 < \delta < \frac{1}{2} \text{ [3]}, \\ l_k^{\delta}(n) &\leq \frac{k-1}{k} \cdot (1 - \delta) \cdot k^n + o(k^n) \text{ при } 0 < \delta < \frac{k-1}{k} \text{ [4]}, \\ l_k^{\delta_n}(n) &\sim \frac{k-1}{k} \cdot k^n, \text{ где } \delta_n \geq \left(\frac{k-1}{k}\right)^n, \delta_n \rightarrow 0 \text{ при } n \rightarrow \infty \text{ [4]}, \\ l_2^{q/2^n}(n) &\sim \frac{1}{2} \cdot 2^n, \text{ где } q \geq 1 - \text{целое число [4]}. \end{aligned}$$

В настоящей работе исследуется длина полиномов, доопределяющих функции. Длиной $l^E(f)$ функции f на множестве E называется наименьшая длина среди всех полиномов, доопределяющих функцию f с множеством E . Рассматривается наибольшая длина $l_k^E(n)$ на множестве E среди всех k -значных функций, зависящих от n переменных, и вводится функция Шеннона $l_k^{m(n)}(n) = \max_{E \subseteq E_k^n: |E|=m(n)} l_k^E(n)$.

В работе получены следующие оценки.

Теорема.

1. Если $k \geq 2$ — целое число, $(E_k; +, \cdot)$ — поле, $n \geq 1$, $0 \leq m \leq k^n$, то $l_k^m(n) \leq m$.
2. Если $n \geq 1$, $0 \leq m \leq 2^n$, то $l_2^m(n) = m$.
3. Если $k \geq 3$ — целое число, $(E_k; +, \cdot)$ — поле, $0 \leq m(n) \leq k^n$ при всех $n = 1, 2, \dots$ и $m(n) \rightarrow \infty$ при $n \rightarrow \infty$, то $l_k^{m(n)}(n) \sim m(n)$ при $n \rightarrow \infty$.

Работа поддержана РФФИ (проект № 17-01-00782-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Яблонский С. В. Функциональные построения в k -значной логике // Труды Математического института им. В. А. Стеклова АН СССР. — 1958. — Т. 51. — С. 5–142.
- [2] Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. М.: Изд-во МЭИ, 1997.
- [3] Джавадов Р. М. О сложности приближенного задания функций алгебры логики // Доклады АН СССР. — 1982. — Т. 265, вып. 1. — С. 24–27.
- [4] Селезнева С. Н. О приближении с заданной точностью функций k -значных логик полиномами // Дискретная математика. — 2008. — Т. 20, вып. 2. — С. 32–45.

СЛОЖНОСТЬ СИСТЕМ ФУНКЦИЙ k -ЗНАЧНОЙ ЛОГИКИ В КЛАССЕ ПОЛЯРИЗОВАННЫХ ПОЛИНОМИАЛЬНЫХ ФОРМ

Селезнева Светлана Николаевна¹, Гордеев Михаил Михайлович²

¹ Московский государственный университет имени М. В. Ломоносова, e-mail: selezn@cs.msu.su

² Московский государственный университет имени М. В. Ломоносова, e-mail: gordmisha@gmail.com

В работе получено значение наибольшей сложности систем с m , $m \geq 2$, функциями k -значной логики, зависящими от n переменных, в классе поляризованных полиномиальных форм нечетных $k \geq 3$.

В [1] рассматривались представления функций алгебры логики поляризованными полиномиальными формами (ППФ), которые подходят для программируемых логических матриц (ПЛМ). В [2] получены некоторые оценки длины функций алгебры логики в классе ППФ, и в [3] найдено значение функции Шеннона длины функций алгебры логики в этом классе. В [4] поляризованные полиномиальные формы определены для многозначных логик и получена верхняя оценка функции Шеннона длины функций k -значной логики в этом классе. В [4–12] найдены верхние и нижние оценки длины функций многозначных логик в классе ППФ, однако асимптотика функции Шеннона пока не получена. В [7] рассмотрена задача о сложности представления систем функций k -значных логик в классе ППФ и найдено точное значение функции Шеннона при $k = 2$ и $k = 3$ для систем, содержащих хотя бы две функции. В настоящей работе этот результат обобщается на случай произвольного возможного нечетного k .

Пусть $k \geq 2$ — целое число, $E_k = \{0, 1, \dots, k-1\}$. Рассматривается множество $P_k = \{f^{(n)} : E_k^n \rightarrow E_k \mid n = 0, 1, 2, \dots\}$ всех функций k -значной логики. Пусть на E_k задано поле $(E_k; +, \cdot)$. Поляризованной полиномиальной формой (ППФ) над этим полем по вектору поляризации $\delta = (d_1, \dots, d_n) \in E_k^n$ называется сумма различных произведений различных поляризованных переменных вида $(x_i + d_i)$ в некоторых степенях с ненулевыми коэффициентами. Каждая функция $f \in P_k$, зависящая от n переменных, представима однозначной ППФ $P^\delta(f)$ по каждому вектору $\delta \in E_k^n$ [11, 12, 4]. Сложностью системы ППФ с одним и тем же вектором поляризации называется число различных слагаемых, встречающихся во всех ППФ этой системы. Сложностью системы функций из P_k в классе ППФ называется наименьшая сложность среди всех таких систем ППФ с одним и тем же вектором поляризации, которые представляют все функции этой системы. Функция Шеннона $L_k^{\text{ППФ}}(n, m)$ сложности систем с m функциями из P_k в классе ППФ определяется как наибольшая сложность в классе ППФ среди всех систем из m функций, зависящих от одних и тех же n переменных. В [7] доказано, что $L_2^{\text{ППФ}}(n, m) = 2^n$ и $L_3^{\text{ППФ}}(n, m) = 3^n$ при всех $n \geq 1, m \geq 2$.

Теорема. Если $k \geq 3$ — нечетное число, $(E_k; +, \cdot)$ — поле, то при всех $n \geq 1$, $m \geq 2$ верно равенство $L_k^{\text{ППФ}}(n, m) = k^n$.

Работа частично поддержана РФФИ (проект № 17-01-00782-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Sasao T., Besslich P. On the complexity of mod-2 sum PLA's // IEEE Trans. on Comput. — 1990. — V. 39, No 2. — P. 262–266.
- [2] Супрун В. П. Сложность булевых функций в классе канонических поляризованных полиномов // Дискретная математика. — 1993. — Т. 5, вып. 2. — С. 111–115.
- [3] Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, вып. 3. — С. 323–326.
- [4] Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.
- [5] Селезнева С. Н. О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 117–121.
- [6] Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — Вып. 3. — С. 40–45.
- [7] Селезнева С. Н. Сложность систем функций алгебры логики и систем функций трехзначной логики в классах поляризованных полиномиальных форм // Дискретная математика. — 2015. — Т. 27, вып. 1. — С. 111–122.
- [8] Балюк А. С., Янушковский Г. В. Верхние оценки сложности функций над конечными полями в классах кронекеровых форм // Известия Иркутского государственного университета. Серия: Математика. — 2015. — Вып. 14. — С. 3–17.
- [9] Балюк А. С., Зинченко А. С. Нижняя оценка сложности функций над конечным полем порядка 4 в классе поляризованных полиномов // Известия Иркутского государственного университета. Серия: Математика. — 2016. — Вып. 16. — С. 19–29.
- [10] Балюк А. С., Зинченко А. С. Нижняя оценка сложности пятизначных функций в классе поляризованных полиномов // Дискретная математика. — 2016. — Т. 28, вып. 4. — С. 29–37.

- [11] Яблонский С. В. Функциональные построения в k -значной логике // Труды Математического института им. В. А. Стеклова АН СССР. — 1958. — Т. 51. — С. 5–142.
- [12] Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Изд-во МЭИ, 1997.

ВЕРХНЯЯ ОЦЕНКА ВЕЩЕСТВЕННОЙ СЛОЖНОСТИ КОМПЛЕКСНОГО ДПФ

Сергеев Игорь Сергеевич

ФГУП «НИИ “Квант”», e-mail: isserg@gmail.com

Дискретное преобразование Фурье (ДПФ) играет важнейшую роль в теории и практике быстрых вычислений и цифровой обработки сигналов, см., например, [1, 2].

ДПФ порядка N с примитивным корнем ζ определяется как

$$\text{ДПФ}_{N,\zeta}(\gamma_0, \dots, \gamma_{N-1}) = (\gamma_0^*, \dots, \gamma_{N-1}^*), \quad \gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij}.$$

Чаще всего ДПФ применяется к вещественным или комплексным векторам длины N , равной степени двойки. ДПФ является линейным преобразованием и обычно вычисляется при помощи элементарных линейных операций. Мы исследуем сложность комплексного ДПФ порядка $N = 2^k$ при реализации схемами или неветвящимися программами в линейном алгебраическом базисе вещественных операций: сложения, вычитания, скалярного умножения на произвольные константы.

Теория алгоритмов быстрого преобразования Фурье (БПФ), развитая в середине 20-го века, позволяет вычислить ДПФ любого порядка N со сложностью $O(N \log N)$, см. [1, 2]. Снизу пока известны лишь оценки вида $\Omega(N)$.

Напомним, что любой метод БПФ модифицируется для случая вещественного входного вектора, при этом сложность уменьшается асимптотически вдвое, см. [2, 3]. Поэтому случай вещественных векторов не требует отдельного рассмотрения.

Среди аккуратных верхних оценок сложности ДПФ порядка $N = 2^k$ долгое время (с 1980-х гг.) наилучшей оставалась асимптотическая оценка $4N \log_2 N$ операций. Она достигается на известном методе «БПФ с расщепленным основанием» (split-radix), см., например, [2, 3]. Метод использует около $3N \log_2 N$ аддитивных операций и около $N \log_2 N$ скалярных умножений. Только в середине 2000-х гг. оценка общей вещественной сложности ДПФ порядка $N = 2^k$ была улучшена до $3\frac{7}{9} \cdot N \log_2 N$ [4, 5] (см. также [3]). Этот метод использует чуть больше скалярных умножений: асимптотически $\frac{10}{9} \cdot N \log_2 N$.

Далее, в [6] при помощи компьютерной программы было обнаружено существование вариантов метода с расщепленным основанием меньшей сложности, чем у классической версии, при $N \in \{256, 512\}$. Хотя по сложности найденные схемы уступают схемам [4, 5], в отличие от последних они используют только корни из единицы в качестве множителей. Позже, в [7] предложен еще один метод вычисления ДПФ с меньшим, чем у упомянутых выше схем, числом скалярных умножений, $\frac{11}{12} \cdot N \log_2 N$, и общей сложностью $3\frac{5}{6} \cdot N \log_2 N$.

Любая из перечисленных общих схем (исключая конкретные примеры [6]) строится рекурсивно из базовых подсхем, выполняющих ДПФ малого порядка, по правилу декомпозиции [8]. Следующий результат получен на пути объединения подходящих базовых схем растущего размера.

Теорема. *Комплексное ДПФ порядка $N = 2^k$ реализуется схемой из асимптотически $2,875N \log_2 N$ вещественных операций сложения и вычитания, $0,89375N \log_2 N$ вещественных умножений на константы, таким образом, с общей сложностью асимптотически $3,76875N \log_2 N$ вещественных операций.*

Хотя оценка [4, 5] улучшена совсем незначительно, предположительно она близка к пределу, достижимому схемами типа [8].

Работа выполнена при поддержке РФФИ (проект № 17-01-00485а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов. — М. : Мир, 1989. — 448 с.
- [2] Власенко В. А., Лаппа Ю. М., Ярославский Л. П. Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов. — М. : Наука, 1990. — 180 с.
- [3] Гашков С. Б., Сергеев И. С. Алгоритмы быстрого преобразования Фурье. В сб. «Дискретная математика и ее приложения». V. — М. : Изд-во ИПМ РАН, 2009, 3–23.
- [4] Johnson S. F., Frigo M. A modified split-radix FFT with fewer arithmetic operations // IEEE Trans. Signal Process. — 2007. — V. 55(1). — P. 111–119.
- [5] Lundy T. J., van Buskirk J. A new matrix approach to real FFTs and convolutions of length 2^k // Computing. — 2007. — V. 80. — P. 23–45.
- [6] Haynal S., Haynal H. Generating and searching families of FFT algorithms // J. Satisf., Boolean Modeling and Comput. — 2011. — V. 7. — P. 145–187.
- [7] Zheng W., Li K., Li K. Scaled radix-2/8 algorithm for efficient computation of length- $N = 2^m$ DFTs // IEEE Trans. Signal Process. — 2014. — V. 62(10). — P. 2492–2503.
- [8] Cooley J. W., Tukey J. W. An algorithm for the machine calculation of complex Fourier series // Math. Comp. — 1965. — V. 19. — P. 297–301.

О ПОДОБИИ МАТРИЦЫ ЖОРДАНОВОЙ КЛЕТКЕ НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

Сидоров Сергей Владимирович

Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: sesidorov@yandex.ru,
sergey.sidorov@itmm.unn.ru

1. Предварительные сведения и постановка задачи

Понятие подобных матриц над кольцом целых чисел $\mathbb{Z}$ хорошо известно (см., например, [1]) и является обобщением понятия подобных матриц над полем рациональных чисел $\mathbb{Q}$ (см., например, [2]).

Определение. Говорят, что матрица $A \in \mathbb{Z}^{n \times n}$ подобна над $\mathbb{Z}$ матрице $B \in \mathbb{Z}^{n \times n}$, если существует такая матрица $X \in \mathbb{Z}^{n \times n}$, что $AX = XB$ и $|\det(X)| = 1$.

В определении подобия над $\mathbb{Q}$ требуется только, чтобы $\det(X) \neq 0$.

Поскольку отношение подобия является отношением эквивалентности, то множество $\mathbb{Z}^{n \times n}$ разбивается на классы подобных матриц. Описание классов подобия над $\mathbb{Q}$ было получено Г. Фробениусом во второй половине XIX века. Классы подобных над $\mathbb{Z}$ матриц устроены гораздо сложнее, чем классы подобных матриц над $\mathbb{Q}$. К настоящему времени полное описание всех классов подобия над $\mathbb{Z}$ неизвестно и вряд ли может быть получено. Тем не менее, можно сделать некоторые ограничения, например, рассматривать только те матрицы, все собственные числа которых целые. Для таких матриц можно надеяться на получение полной классификации.

Здесь мы рассматриваем матрицы, имеющие характеристический многочлен $(\lambda_0 - \lambda)^n$, где $\lambda_0 \in \mathbb{Z}$. Все такие матрицы над полем $\mathbb{Q}$ подобны жордановым формам (т.е. блочно-диагональным матрицам с жордановыми клетками на диагонали). Над кольцом $\mathbb{Z}$ это, вообще говоря, неверно (см., например, [3,4,5,6]). Далее мы получим критерий того, когда матрица подобна над $\mathbb{Z}$ одной жордановой клетке.

Известно, что если матрицы A и B подобны над $\mathbb{Z}$, то они подобны и над $\mathbb{Q}$, а также выполняются равенства $\Delta_k(A) = \Delta_k(B)$, $k = 1, \dots, n$, где $\Delta_k(A)$ и $\Delta_k(B)$ — наибольшие общие делители миноров k -го порядка матриц A и B соответственно (см., например, [3,5]). Кроме того (см., например, [4,5]), если все собственные числа матрицы A целые, то она подобна над $\mathbb{Z}$ верхнетреугольной матрице с собственными числами по диагонали.

2. Основной результат

Напомним, что жордановой клеткой $J_n(\lambda_0)$ называется матрица порядка n вида

$$J_n(\lambda_0) = \begin{pmatrix} \lambda_0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_0 \end{pmatrix}.$$

Следующая теорема устанавливает необходимые и достаточные условия, при которых матрица A подобна над $\mathbf{Z}$ жордановой клетке.

Теорема. Матрица $A \in \mathbf{Z}^{n \times n}$ подобна над $\mathbf{Z}$ жордановой клетке $J_n(\lambda_0)$ тогда и только тогда, когда выполняются следующие условия:

1. $\det(A - \lambda E) = (\lambda_0 - \lambda)^n$, $\lambda_0 \in \mathbf{Z}$.
2. $\text{rank}(A - \lambda_0 E) = n - 1$.
3. $\Delta_{n-1}(A - \lambda_0 E) = 1$.

Доказательство. Очевидно, что A и B подобны над $\mathbf{Z}$ тогда и только тогда, когда $A - \lambda_0 E$ и $B - \lambda_0 E$ подобны над $\mathbf{Z}$. Следовательно, необходимость вытекает из равенств $\text{rank}(A - \lambda_0 E) = \text{rank}(J_n(\lambda_0) - \lambda_0 E) = n - 1$, $\Delta_{n-1}(A - \lambda_0 E) = \Delta_{n-1}(J_n(\lambda_0) - \lambda_0 E) = 1$.

Докажем достаточность. Поскольку A подобна над $\mathbf{Z}$ некоторой верхнетреугольной матрице

$$T = \begin{pmatrix} \lambda_0 & t_{12} & t_{13} & \cdots & t_{1,n-1} & t_{1,n} \\ 0 & \lambda_0 & t_{23} & \cdots & t_{2,n-1} & t_{2,n} \\ 0 & 0 & \lambda_0 & \cdots & t_{3,n-1} & t_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_0 & t_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & \lambda_0 \end{pmatrix},$$

то $\Delta_{n-1}(T - \lambda_0 E) = \Delta_{n-1}(A - \lambda_0 E) = 1$. С другой стороны,

$\Delta_{n-1}(T - \lambda_0 E) = t_{12}t_{23} \cdots t_{n-1,n}$, поэтому $t_{12}, t_{23}, \dots, t_{n-1,n} \in \{1, -1\}$. Осталось доказать, что матрицы T и $J_n(\lambda_0)$ подобны над $\mathbf{Z}$. Для этого найдем такую матрицу X , что $TX = XJ_n(\lambda_0)$ и $\det(X) = 1$. Пусть $X = (x_{ij})$ — верхнетреугольная матрица с единицами по диагонали. Тогда условие $TX = XJ_n(\lambda_0)$ с учетом треугольности матриц X и T эквивалентно следующим равенствам:

$$\sum_{k=1}^n t_{ik}x_{kj} = \lambda_0 x_{ij} + \sum_{k=i+1}^{j-1} t_{ik}x_{kj} + t_{ij} = x_{i,j-1} + x_{ij}\lambda_0 \quad (1)$$

для $i = 1, \dots, n$; $j = i, \dots, n$. После небольшого упрощения в равенстве (1) получаем

$$t_{i,i+1}x_{i+1,j} + \sum_{k=i+2}^{j-1} t_{ik}x_{kj} + t_{ij} = x_{i,j-1}, \quad i = 1, \dots, n-2; j = i+2, \dots, n. \quad (2)$$

При $j = i+2$ из равенства (2) получаем

$$t_{i,i+1}x_{i+1,i+2} = x_{i,i+1} - t_{i,i+2}, \quad i = 1, \dots, n-2.$$

При $j = i+3$ из равенства (2) получаем

$$t_{i,i+1}x_{i+1,i+3} = x_{i,i+2} - t_{i,i+2}x_{i+2,i+3} - t_{i,i+3}, \quad i = 1, \dots, n-3.$$

В общем случае при $j = i+s$, $s = 2, \dots, n-1$ из равенства (2) получаем

$$t_{i,i+1}x_{i+1,i+s} = x_{i,i+s-1} - \sum_{k=i+2}^{i+s-1} t_{ik}x_{k,i+s} - t_{i,i+s}, \quad i = 1, \dots, n-s.$$

Таким образом, полагая элементы $x_{12}, x_{13}, \dots, x_{1n}$ произвольными целыми числами и учитывая, что $|t_{i,i+1}| = 1$ для $i = 1, \dots, n-1$, мы последовательно находим элементы каждой наддиагонали матрицы X . **Теорема доказана.**

Следствие. Матрица $A \in \mathbf{Z}^{n \times n}$ подобна над $\mathbf{Z}$ жордановой клетке $J_n(\lambda_0)$ тогда и только тогда, когда A подобна $J_n(\lambda_0)$ над полем рациональных чисел $\mathbf{Q}$ и $\Delta_{n-1}(A - \lambda_0 E) = 1$.

Работа выполнена при поддержке РФФИ (проект № 15-01-06249).

СПИСОК ЛИТЕРАТУРЫ

- [1] Newman M. Integral matrices. — New York and London : Academic Press, 1972. — 224 p.
- [2] Мальцев А. И. Основы линейной алгебры. — М. : Наука, 1970. — 400 с.
- [3] Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел // Известия высших учебных заведений. Математика. — 2006. — № 4. — С. 57–64.
- [4] Сидоров С. В. О подобии матриц с целочисленным спектром над кольцом целых чисел // Известия высших учебных заведений. Математика. — 2011. — № 3. — С. 86–94.
- [5] Сидоров С. В. Выделение эффективно разрешимых классов в задаче подобия матриц над кольцом целых чисел : дис. ... канд. физ.-мат. наук : 01.01.09 : защищена 15.10.15 : утв. 21.03.16 / Сидоров Сергей Владимирович. — Нижний Новгород, 2015. — 121 с. — Библиогр. : с. 109–113.
- [6] Сидоров С. В. О подобии матриц третьего порядка над кольцом целых чисел, имеющих приводимый характеристический многочлен // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2009. — № 1. — С. 119–127.

ЭВОЛЮЦИОННЫЕ МЕТОДЫ В ЗАДАЧАХ ТЕХНИЧЕСКОЙ ДИАГНОСТИКИ

Сперанский Дмитрий Васильевич

Московский государственный университет путей сообщения, e-mail: Speranskiy.DV@gmail.com

Последние 20–25 лет интенсивно ведутся исследования в научном направлении, называемом эволюционными вычислениями [1]. Это направление объединяет разработки математических методов, использующих принципы природных механизмов. В настоящее время методы и технологии, инспирированные природными системами, широко применяются во многих отраслях науки и техники. Их целью является разработка природных алгоритмов, ориентированных на решение различных оптимизационных задач. В статье описывается приложение идей генетических и муравьиных алгоритмов, относящихся к классу эволюционных вычислений, к решению задачи диагностики цифровых устройств. Ниже речь идет о задаче размещения контрольных точек (РКТ) в цифровом устройстве (ЦУ), обеспечивающих повышение его тестопригодности. Последнее означает приспособленность устройства к проведению контроля его технического состояния в процессе эксплуатации, в том числе обнаружения в нем неисправностей.

Известны различные постановки задач РКТ. Все предложенные для решения этих задач методы базируются на предварительном анализе ЦУ, связанном с определением показателей управляемости, наблюдаемости и тестируемости устройства. В ряде известных ныне систем анализа меры для оценки ее показателей определяются путем анализа топологии (структуры) ЦУ [2].

Задача РКТ формулируется следующим образом. В ЦУ, заданном в виде структурной схемы, необходимо разместить заданное число (или не более заданного числа) контрольных точек, обеспечивающих максимальное приращение показателя тестируемости всего ЦУ в целом.

Ниже предложен подход к решению этой задачи, который также подразумевает получение численных значений упомянутых выше показателей ЦУ, но на иной теоретической основе. Соответствующие показатели связаны с оценкой количества информации в узлах ЦУ, появляющейся в процессе его функционирования, и подробно описаны в [3, 4]. Преимущество такого информационного подхода состоит в том, что он базируется только на данных логического моделирования исправного ЦУ на случайной входной последовательности, т. е. не требует значительно более сложного и трудоемкого анализа структурной схемы ЦУ.

Для решения задачи РКТ разработан простой генетический алгоритм (ГА). Исходными данными являются число выводимых контрольных точек, размер популяции, вероятности операторов кроссинговера и мутации, показатели

управляемости, наблюдаемости и тестируемости каждой линии ЦУ, вычисленные по данным логического моделирования ЦУ на случайной входной последовательности.

Перед работой ГА нумеруются все линии схемы ЦУ числами от 1 до L . Хромосома в ГА кодируется двоичным набором длины L , в котором i -й разряд равен 1, если i -я линия ЦУ включается в число выбранных контрольных точек, и i -й разряд равен 0, если соответствующая линия не включается. Таким образом, каждой хромосоме соответствует некоторый набор контрольных точек.

В качестве фитнес-функции для оценки хромосомы в предлагаемом ГА используется значение тестируемости ЦУ с использованием первичных выходов ЦУ, дополненным контрольными точками, определяемыми оцениваемой хромосомой.

Критерием окончания работы ГА может быть использовано либо задаваемое заранее число поколений, генерируемых алгоритмом, либо стабилизация полученного лучшего (с максимальной тестируемостью) решения для нескольких последних поколений. Для селекции хромосом в процессе репродукции используется случайный поиск на основе колеса рулетки. Число запусков рулетки выбирается равным мощности популяции. В качестве оператора кроссинговера используется классический одноточечный. Оператор мутации в описываемом ГА состоит в замене на противоположное значение случайно выбранной позиции хромосомы.

При выполнении оператора кроссинговера могут быть получены хромосомы с числом единиц, отличным от k . Для получения в ней ровно k единиц воспользуемся для простоты следующим приемом коррекции: если хромосома имеет r лишних (недостающих) единиц, то заменим r случайно выбранных таких позиций нулями (единицами).

Теперь рассмотрим еще одну разновидность задачи РКТ, которая может быть решена эволюционным муравьиным алгоритмом [1]. Приведем формулировку этой задачи. Пусть задано ЦУ в виде структурной логической схемы, диагностирование которой осуществляется с помощью заранее зафиксированного теста T . Пусть также задано множество $F = \{f_1, f_2, \dots, f_n\}$ неисправностей ЦУ, которые тестом T не обнаруживаются. Требуется разместить в ЦУ минимальное число контрольных точек, выбранных из заданного множества $P = \{p_1, p_2, \dots, p_m\}$ таким образом, чтобы при подаче теста T на ЦУ по его реакции обнаруживалась каждая неисправность из множества F .

Покажем, что рассматриваемая задача всегда может быть сведена к классической задаче о покрытии множества. Из содержательного смысла задачи ясно, что вывод одной контрольной точки $p_i \in P$ ($i = 1, \dots, m$) позволяет в действительности обнаруживать в общем случае не одну неисправность из множества F , а некоторое подмножество неисправностей $F(p_i) \subset F$. Состав подмножеств неисправностей $F(p_i)$ может быть найден методом логического

моделирования ЦУ с учетом того, что наблюдение реакции ЦУ на тест T ведется на всех ее первичных (штатных) выходах и одном дополнительном выходе, организованном в контрольной точке $p_i \in P$. С использованием приведенных данных построим прямоугольную таблицу, имеющую n строк и m столбцов. Строка с номером i этой таблицы соответствует неисправности $f_i \in F$, а столбец с номером j соответствует подмножеству $F(p_j) \subset F$. Поместим на пересечении i -й строки и j -го столбца этой таблицы, элемент a_{ij} , равный 1 (0), если f_i обнаруживается (не обнаруживается) на выходе j .

Понятно, что выбор множества P контрольных точек должен быть таким, чтобы удовлетворялось равенство $\bigcup_{i=1}^n F(p_i) = F$. Вместе с тем также понятно, что подмножества $F(p_i)$ и $F(p_j)$, где $i \neq j$, могут иметь общие элементы, т. е. $F(p_i) \cap F(p_j) \neq \emptyset$. Последнее означает возможность обнаружения некоторых неисправностей из множества при выборе различных контрольных точек.

Из сказанного выше следует, что решение исследуемой нами задачи РКТ состоит в выборе минимального числа ее столбцов таким образом, чтобы в каждой ее строке находилась по крайней мере одна единица. Очевидно, что это есть классическая задача о покрытии множества.

Иными словами, исследуемая нами задача всегда может быть сведена к классической задаче о покрытии множества, для решения которой известны несколько эффективных эволюционных муравьиных алгоритмов (МА). Сравнение таких МА выполнено, в частности, в работе [5].

СПИСОК ЛИТЕРАТУРЫ

- [1] Скобцов Ю. А., Сперанский Д. В. Эволюционные вычисления. — М. : Национальный открытый университет «ИНТУИТ», 2015. — 326 с.
- [2] Bennets R. G. Design of testable logic circuits. — Addison Wesley Publishing Company, 1984.
- [3] Speranskiy D. V. Testability analysis of discrete devices on information approach base: theory, software, statistical results // Proc. Intern. Conf. "Technical Diagnostics-89". — Prague, 1989. — V. II. — P. 439–442.
- [4] Барашко А. С., Скобцов Ю. А., Сперанский Д. В. Моделирование и тестирование дискретных устройств. — Киев, Наукова думка, 1992. — 286 с.
- [5] Lessing L., Dumitrescu I., Stutzle T. A comparison between ACO algorithms for set covering problem // ANTS'2004, 4th International Workshop on Ant Algorithms and Swarm Intelligence. — Ser. LNCS. — V. 3172. — Springer Verlag, 2004. — P. 1–12.

НЕКОТОРЫЕ СВОЙСТВА АВТОМАТНОГО ЗАМЫКАНИЯ МНОЖЕСТВ БУЛЕВЫХ ФУНКЦИЙ

Сысоева Любовь Николаевна

Национальный исследовательский университет «Высшая школа экономики», e-mail: s-luba@mail.ru

Задача о реализации булевых функций автоматами рассматривалась рядом авторов (см. [1, 2]). В работе [3] рассматривалась реализация булевых функций конечными инициальными автоматами с константными состояниями, получены описания множеств булевых функций максимальной мощности, которые могут быть реализованы одним булевым автоматом с двумя и тремя константными состояниями.

В настоящей работе вводится понятие автоматного замыкания множества булевых функций. Показывается, что существует шесть автоматно-замкнутых классов булевых функций.

Множество всех функций алгебры логики обозначается через P_2 . Пусть $P_2(n)$ — множество всех булевых функций, зависящих от фиксированных переменных $x_1, x_2, \dots, x_n$, $n \geq 1$. Под *булевым автоматом* будем понимать автомат $V = (\{0, 1\}, \{0, 1\}, Q, F, G)$ с произвольным числом входов, входным алфавитом $\{0, 1\}$, выходным алфавитом $\{0, 1\}$, алфавитом состояний Q , функцией перехода G и функцией выхода F . Основные обозначения и определения берутся из [4]. Пусть n — число входов автомата V . Без ограничения общности будем полагать, что входы автомата V занумерованы от 1 до n и на i -й вход автомата V подается значение булевой переменной x_i . Тем самым можно считать, что в каждый момент времени на входы автомата V подается некоторый двоичный набор значений переменных $x_1, x_2, \dots, x_n$ и для любого состояния $q \in Q$ функция выхода $F(q, x_1, x_2, \dots, x_n)$ является булевой функцией от переменных $x_1, x_2, \dots, x_n$. Пусть $\mathcal{A} \subseteq P_2$. Булев автомат V будем называть *автоматом над $\mathcal{A}$* , если для любого состояния q автомата V функция выхода $F(q, x_1, x_2, \dots, x_n)$ содержится в $\mathcal{A}$. Отметим, что функции рассматриваются с точностью до несущественных переменных и переименования переменных.

Пусть $V_{q_1} = (\{0, 1\}, \{0, 1\}, Q, F, G, q_1)$ — инициальный булев автомат с начальным состоянием q_1 и n входами. Пусть $C = (\tilde{\beta}_1, \tilde{\beta}_2, \dots, \tilde{\beta}_{2^n})$ — упорядоченная последовательность всех двоичных наборов длины n , $n \geq 1$. Будем говорить, что *автомат V_{q_1} с последовательностью C реализует булеву функцию $f(x_1, x_2, \dots, x_n)$* , если при последовательной подаче на входы автомата V_{q_1} наборов из C в каждый момент $t = 1, 2, \dots, 2^n$ на выходе автомата V_{q_1} выдается значение $f(\tilde{\beta}_t)$. Будем также говорить, что *функция f реализуется автоматом V_{q_1}* , если для некоторой последовательности наборов C автомат V_{q_1} с последовательностью C реализует f . Обозначим через $P(V_{q_1})$ множество всех булевых функций, реализуемых автоматом V_{q_1} .

Автоматные функции, реализуемые булевыми автоматами, будем называть *двоичными автоматными функциями*. Другими словами, автоматная функция является двоичной, если входным и выходным алфавитом для этой функции является алфавит $\{0, 1\}$. Пусть $\mathcal{A} \subseteq P_2$. Двоичную автоматную функцию $h(x_1, x_2, \dots, x_n)$ будем называть *функцией над $\mathcal{A}$* , если h реализуется некоторым инициальным булевым автоматом над $\mathcal{A}$. Пусть V_{q_1} — некоторый инициальный булев автомат, реализующий двоичную автоматную функцию h , и C — некоторая последовательность подаваемых наборов. Будем говорить, что *функция h с последовательностью подаваемых наборов C реализует булеву функцию $f(x_1, x_2, \dots, x_n)$* , если f реализуется автоматом V_{q_1} с последовательностью подаваемых наборов C . Будем также говорить, что *функция h реализует булеву функцию f* , если для некоторой последовательности наборов C функция h с последовательностью C реализует f .

Для автоматных функций можно стандартным образом определить понятие автоматной формулы, т. е. формулы над системой автоматных функций (см. [4, 5]). Пусть дано некоторое конечное множество булевых функций $\mathcal{A}$. Введем следующее понятие *автоматной формулы над $\mathcal{A}$* индуктивным образом (см. [5]).

1. Базис индукции. Символ любой переменной является автоматной формулой над $\mathcal{A}$, называемой тривиальной формулой.
2. Индуктивный переход. Пусть $h(x_1, x_2, \dots, x_n)$ — двоичная автоматная функция над $\mathcal{A}$ и $\Phi_1, \Phi_2, \dots, \Phi_n$ — автоматные формулы над $\mathcal{A}$. Тогда $h(\Phi_1, \Phi_2, \dots, \Phi_n)$ является автоматной формулой над $\mathcal{A}$.

Понятие *автоматной функции, реализуемой автоматной формулой над $\mathcal{A}$* , определяется стандартным образом.

Пусть C — некоторая последовательность подаваемых наборов, а Φ — автоматная формула над $\mathcal{A}$, реализующая некоторую автоматную функцию $h(x_1, x_2, \dots, x_n)$. Будем говорить, что *булева функция $f(x_1, x_2, \dots, x_n)$ реализуется автоматной формулой Φ с последовательностью подаваемых наборов C* , если f реализуется функцией h с последовательностью подаваемых наборов C . Будем также говорить, что *автоматная формула Φ реализует булеву функцию f* , если для некоторой последовательности наборов C формула Φ с последовательностью C реализует f .

Автоматным замыканием $[\mathcal{A}]_{\mathcal{A}}$ множества булевых функций $\mathcal{A}$ называется множество всех булевых функций, реализуемых автоматными формулами над $\mathcal{A}$. Нетрудно заметить, что $\mathcal{A} \subseteq [\mathcal{A}]_{\mathcal{A}}$.

Основным результатом данной работы является следующая теорема, описывающая все автоматически-замкнутые классы в P_2 .

Теорема 1. Пусть $\mathcal{A} \subseteq P_2$ и $\mathcal{A} \neq \emptyset$.

1. Если $\mathcal{A} \not\subseteq T_0$ и $\mathcal{A} \not\subseteq T_1$, то $[\mathcal{A}]_{\mathcal{A}} = P_2$.

2. Если $\mathcal{A} \subseteq T_0 \setminus T_1$ и $\mathcal{A} \neq \{0\}$, то $[\mathcal{A}]_A = T_0$.
3. Если $\mathcal{A} \subseteq T_1 \setminus T_0$ и $\mathcal{A} \neq \{1\}$, то $[\mathcal{A}]_A = T_1$.
4. Если $\mathcal{A} \subseteq T_{01}$, то $[\mathcal{A}]_A = T_{01}$.
5. Если $\mathcal{A} = \{0\}$, то $[\mathcal{A}]_A = \{0\}$.
6. Если $\mathcal{A} = \{1\}$, то $[\mathcal{A}]_A = \{1\}$.

Автор выражает благодарность доценту Дудаковой О. С. и профессору Колпакову Р. М. за постановку задачи и обсуждение результатов работы.

СПИСОК ЛИТЕРАТУРЫ

- [1] Кузьмин В. А. Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга // Проблемы кибернетики. — Вып. 13. — 1965. — С. 75–96.
- [2] То Суан Зунг Об асимптотических закономерностях сложности автоматов из некоторых классов // Проблемы кибернетики. — Вып. 22. — 1970. — С. 5–44.
- [3] Сысоева Л. Н. Максимальные множества булевых функций, реализуемых инициальным булевым автоматом с двумя или тремя константными состояниями // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, вып. 4. — С. 95–99.
- [4] Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. — М. : Наука, 1985. — 320 с.
- [5] Яблонский С. В. Введение в дискретную математику. — М. : Высшая школа, 2006. — 384 с.

СТРУКТУРА МНОГОИНДЕКСНЫХ ТРАНСПОРТНЫХ МНОГОГРАННИКОВ

Титова Елена Борисовна, Шевченко Валерий Николаевич

Нижегородский государственный университет, e-mail: elena.titova@itmm.unn.ru, shev@vmk.unn.ru

Обозначения: $\mathbf{1}^{p \times q}$ — $p \times q$ -матрица, каждый элемент которой равен 1, E_n — единичная матрица n -го порядка; $\det(A)$ и $\text{perm}(A)$ — определитель и перманент матрицы A , A^T — матрица, транспонированная к A , $A \times B$ — кронекерово произведение матриц A и B (определение и свойства см., например, в [1]).

Предлагаемые тезисы можно рассматривать как продолжение [2, 3].

1. Рассмотрим множество неотрицательных решений системы линейных неравенств:

$$\sum_{j_1=1}^{n_1} x_{j_1 j_2} \leq b_{0 j_2}, \quad \sum_{j_2=1}^{n_2} x_{j_1 j_2} \geq b_{j_1 0}. \quad (1)$$

Переход к равенствам в системе (1) не меняет структуры задачи, но позволяет рассматривать ее как трехиндексную транспортную задачу (см., напр., [4, 5]). Аналогичная процедура разработана авторами для любого k . При переходе к k индексам с s суммированиями при неотрицательных переменных $x_J = x_{j_1 \dots j_k}$ получим следующее рекурсивное задание матрицы многоиндексной транспортной задачи:

$$T_{s,k}(n_1, \dots, n_k) = \left[\frac{T_{s,k-1}(n_1, \dots, n_{k-1}) \times E_{n_k}}{T_{s-1,k-1}(n_1, \dots, n_{k-1}) \times \mathbf{1}^{1 \times n_k}} \right].$$

Матрица $T_{sk}(n_1, \dots, n_k)$ состоит из $\binom{k}{s}$ строчечных блоков, число ее столбцов $\prod_{i=1}^k n_i$, строк $\sigma_{k-s}(n_1, \dots, n_k)$, ранг матрицы $\sum_{i=s}^k \sigma_{k-i}(n_1 - 1, \dots, n_k - 1)$. В [6] получен спектр матрицы $T_{sk}(n_1, \dots, n_k)^\top T_{sk}(n_1, \dots, n_k)$. Отсюда при $n_1 = \dots = n_k = n$ легко выписывается минимальный многочлен

$$\delta(\lambda, T_{sk}(n)) = \lambda \prod_{j=s}^k (\lambda - \binom{j}{s} n^s).$$

В [7] авторами рассматривался рост миноров k -индексных транспортных задач.

2. Рассмотрим матрицу

$$A_{lmn} = \begin{pmatrix} l & l & l \\ m & -n & m \\ n & m & -n \end{pmatrix}$$

и присоединенную к ней

$$A_{lmn}^* = \begin{pmatrix} n^2 - m^2 & l(n+m) & l(n+m) \\ 2mn & -2ln & 0 \\ m^2 + n^2 & l(n-m) & -l(n+m) \end{pmatrix}.$$

Нетрудно видеть, что $\det(A_{lmn}) = 2ln(m+n)$, $\text{perm}(A_{lmn}) = 2lm^2$.

Утверждение 1. Характеристический многочлен матрицы A_{lmn} имеет вид

$$\begin{aligned} \det(\lambda E_3 - A_{lmn}) &= \lambda^3 + \lambda^2(2n-l) + \lambda(n^2 - m^2 - 3nl - lm) + 2ln(n+m) = \\ &= (\lambda + m + n)(\lambda^2 + (n-m-l)\lambda - 2ln). \end{aligned} \quad (2)$$

Обозначим корни многочлена (2) через $\lambda_1, \lambda_2, \lambda_3$. Заметим, что $\lambda_1 = -m-n$ не зависит от l , свободный член во второй скобке не зависит от m , функция $\omega = \det(A_{lmn}) + \text{perm}(A_{lmn}) = 2l(m^2 + n^2 + mn)$ — симметрическая.

Утверждение 2. $\det(A_{lmn}) \text{perm}(A_{lmn}^*) = -2 \text{perm}(A_{lmn}) \det(A_{lmn}^*)$

Мы считаем, что введенная матрица A_{lmn} и рассмотрение перманентов, с ней связанных, даст дополнительные средства для изучения иерархии транспортных задач.

Работа выполнена при поддержке РФФИ (проект № 15-01-06249).

СПИСОК ЛИТЕРАТУРЫ

- [1] Воеводин В. В., Кузнецов Ю. А. Матрицы и вычисления. — М.: Наука, 1984.
- [2] Шевченко В. Н. Циклы в линейном и целочисленном линейном программировании. // Материалы XII Международного семинара «Дискретная математика и ее приложения» — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 277–280.
- [3] Титова Е. Б., Шевченко В. Н. О минимальном многочлене матрицы ограничений многоиндексной транспортной задачи. // Материалы XII Международного семинара «Дискретная математика и ее приложения» — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 271–274.
- [4] Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.
- [5] Раскин Л. Г., Кириченко И. О. Многоиндексные задачи линейного программирования. — М.: Радио и связь, 1982.
- [6] Шевченко В. Н. Характеристические многочлены многоиндексных транспортных задач. // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 83–88.
- [7] Титова Е. Б., Шевченко В. Н. О минорах матрицы ограничений многоиндексных транспортных задач. // Дискретная математика. — 2012. — Т. 24, вып. 4. — С. 147–157.

СИНТЕЗ СТРАТЕГИЙ ОДНОПРОЦЕССОРНОГО ОБСЛУЖИВАНИЯ ПОТОКА ПАКЕТОВ ОБЪЕКТОВ ТРАНСПОРТНОГО ТИПА

Трухина Мария Александровна

Волжский государственный университет водного транспорта, e-mail: mat@vgavt-nn.ru

Строится модель однопроцессорного обслуживания потока пакетов объектов транспортного типа. Формулируются новые модификации задачи синтеза оптимальных стратегий обслуживания и конструируются решающие алгоритмы.

Математическая модель

Процессор P должен выполнить обслуживание потока M объектов, прибывающих в составе пакетов $O(s)$, $s = \overline{1, h}$. В принимаемых ниже обозначениях первый индекс каждого объекта из M совпадает с номером пакета, которому объект принадлежит; второй индекс объекта через порядковый номер

идентифицирует его внутри пакета. Количество объектов в пакете $O(s)$ обозначим $n(s)$, $n(s) \geq 1$. Таким образом, каждый пакет $O(s)$ состоит из объектов $o_{s,1}, o_{s,2}, \dots, o_{s,n(s)}$, подлежащих однократному без прерываний обслуживанию, $s = \overline{1, h}$, а общее количество n таких объектов в потоке M определяется суммой $\sum_{s=1}^h n(s)$.

Для каждого пакета $O(s)$ считается известным момент t_s его поступления в очередь для обслуживания процессором P . Не ограничивая общности рассмотрения, полагаем $0 = t_1 \leq \dots \leq t_s \leq \dots \leq t_h$. В начальный момент времени $t = 0$ процессор считается свободным, находящимся в состоянии готовности к выполнению обслуживания объектов потока M .

Обслуживание каждого объекта реализуется без прерываний. Процессор не может обслуживать два или более объектов одновременно, его непроизводительные простои запрещены. Обслуживание поступающих объектов потока M может выполняться в произвольном порядке. Длительность обслуживания объекта $o_{s,l}$ полагается равной $\tau_{s,l}$, $s = \overline{1, h}$, $l = \overline{1, n(s)}$. Все введенные числовые параметры считаются целочисленными.

Пакет объектов $O(s)$ считается обслуженным, если завершены обслуживанием все входящие в его состав объекты $o_{s,l}$, $s = \overline{1, h}$, $l = \overline{1, n(s)}$.

Момент t_s^f завершения обслуживания пакета $O(s)$ определяется как $\max(t_{s,1}^f, t_{s,2}^f, \dots, t_{s,n(s)}^f)$, где $t_{s,l}^f$ — момент завершения обслуживания объекта $o_{s,l}$, $s = \overline{1, h}$, $l = \overline{1, n(s)}$. За промежуток времени от момента прибытия пакета $O(s)$ до момента завершения обслуживания всех входящих в его состав объектов налагается штраф $F_s(\Delta_s)$, где $\Delta_s = t_s^f - t_s$, $s = \overline{1, h}$. Функция $F_s(\Delta_s)$ именуется функцией индивидуального штрафа по пакету $O(s)$, $s = \overline{1, h}$. Полагая, что все функции $F_s(\Delta_s)$, $s = \overline{1, h}$ являются произвольными неубывающими и принимающими только неотрицательные значения. Удобно считать, что штраф по каждому пакету взимается в момент завершения его обслуживания.

Стратегия обслуживания записывается как произвольная перестановка $S = ((\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_i, \beta_i), \dots, (\alpha_n, \beta_n))$ двойных индексов всех объектов, т.е. элементов совокупности

$$\{(1, 1), (1, 2), \dots, (1, n(1)), (2, 1), (2, 2), \dots, (h, 1), (h, 2), \dots, (h, n(h))\}.$$

При реализации стратегии S первым обслуживается объект из пакета с номером α_1 , имеющий внутренний номер β_1 ; вторым обслуживается объект из пакета с номером α_2 , имеющий внутренний номер β_2 и т.д.; последним обслуживается объект из пакета с номером α_h , имеющий внутренний номер β_h . Реализации стратегий считаем компактными [1], т.е. промежуточный простой процессора возможен только в ситуации более позднего прибытия объекта, подлежащего обслуживанию в качестве следующего. В таком случае при известной стратегии S для каждого объекта $o_{s,l}$ моменты $t_{s,l}^b(S)$ и $t_{s,l}^f(S)$

соответственно начала и завершения обслуживания вычисляются очевидным образом арифметически.

Критерии оценки и задачи оптимизации

В базовой постановке [2] величина штрафа за пребывание пакета $O(s)$, $s = \overline{1, h}$ в системе обслуживания согласно стратегии S определяется линейной функцией $\varphi_s(\Delta_s) = a_s \cdot \Delta_s$, где a_s величина штрафа за единицу времени пребывания пакета в системе обслуживания.

Для оценки стратегий S практически значимыми являются критерии

$$K_1(S) = \sum_{s=1}^h \varphi_s(\Delta_s) \text{ и } K_2(S) = \max \varphi_s(\Delta_s).$$

В случае линейной модели учета мягкого директивного срока $t_s^d, t_s^d > t_s$ завершения обслуживания по пакету $O(s)$ величина штрафа рассчитывается по формуле

$$\varphi_s^d = \begin{cases} a_s(t_s^f - t_s), & \text{при } t_s^f \leq t_s, \\ a_s(t_s^d - t_s) + b_s(t_s^f - t_s^d), & \text{при } t_s^f > t_s, \end{cases}$$

где b_s — величина штрафа за единицу времени превышения директивного срока.

Соответственно аналогичные введенным выше критерии оценки стратегий S имеют вид

$$K_3(S) = \sum_{s=1}^h \varphi_s^d(\Delta_s) \text{ и } K_4(S) = \max \varphi_s^d(\Delta_s).$$

В скалярной постановке задачи оптимизации состоят в нахождении стратегий, синтезируемых по условию $\min_S K_i(S), i = \overline{1, 4}$.

Для сформулированных задач разработаны решающие алгоритмы основывающиеся на идеологии динамического программирования [3, 4] и ветвей и границ [5].

СПИСОК ЛИТЕРАТУРЫ

- [1] Коган Д. И., Федосенко Ю. С. Задача диспетчеризации: анализ вычислительной сложности и полиномиально разрешимые подклассы // Дискретная математика. — 1996. — Т. 8, Вып. 3. — С. 135–147.
- [2] Модели и оптимизационные задачи однопроцессорного обслуживания пакетов объектов / Д. И. Коган, М. А. Трухина, Ю. С. Федосенко, А. В. Шеянов // Автоматика и телемеханика. — 2016. — № 11. — С. 142–157.
- [3] Беллман Р., Дрейфус С. Прикладные задачи динамического программирования. — М. : Наука, 1965. — 460 с.

- [4] Коган Д. И., Федосенко Ю. С. Общая схема динамического программирования в задачах синтеза стратегий обслуживания объектов, поступающих пакетами // Сборник научных трудов международной научно-технической конференции «Информатика и технологии. Инновационные технологии в промышленности и информатике». Московский технологический университет. Физико-технологический институт. — М. : МТУ, 2016. — С. 154–157.
- [5] Сигал И. Х., Иванова А. П. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы. — М. : Физматлит, 2002. — 240 с.

ЭРГОДИЧЕСКИЕ АВТОМАТНЫЕ ОТОБРАЖЕНИЯ С ЗАДЕРЖКОЙ

Тяпаев Ливат Борисович

Саратовский национальный исследовательский государственный университет им. Н. Г. Чернышевского, e-mail: TiapaevLB@info.sgu.ru

Автоматные преобразования слов бесконечной длины над алфавитом $\mathbb{F}_p = \{0, 1, \dots, p-1\}$, где p простое, совпадают с непрерывными в p -адической метрике преобразованиями кольца целых p -адических чисел $\mathbb{Z}_p$. Более того, отображения реализуемые синхронными автоматами удовлетворяют p -адическому условию Липшица с константой равной 1. Характеризация сохраняющих меру и эргодических 1-липшицевых преобразований была получена В. С. Анашиным, см., например, [1]. Автоматные отображения в ракурсе геометрических образов — множеств точек плоскости с рациональными координатами, а также динамических систем — аффинных и ортогональных преобразований геометрических образов, изучались автором ранее, см. [2–6]. Объектом исследования является асинхронно автоматное преобразование (специального типа) кольца $\mathbb{Z}_p$ в контексте p -адической динамики: автоматы рассматриваются как динамические системы на фазовом пространстве $\mathbb{Z}_p$.

Синхронный автомат это шестерка $\mathfrak{A} = (\mathfrak{I}, \mathcal{S}, \mathcal{O}, S, O, s_0)$, где $\mathfrak{I}$ — входной алфавит, $\mathcal{S}$ — множество состояний автомата, $\mathcal{O}$ — выходной алфавит, $S: \mathfrak{I} \times \mathcal{S} \rightarrow \mathcal{S}$ — функция переходов, $O: \mathfrak{I} \times \mathcal{S} \rightarrow \mathcal{O}$ — функция выхода, $s_0 \in \mathcal{S}$ — начальное состояние. *Асинхронный автомат* $\mathfrak{B}$ определяется похожим образом, за исключением функции выхода: $O: \mathfrak{I} \times \mathcal{S} \rightarrow \mathcal{O}^*$. Т. о., синхронные автоматы осуществляют отображения «буква в букву», асинхронные же — «буква в слово». Алфавиты $\mathfrak{I}, \mathcal{O}$ суть конечные множества, однако $\mathcal{S}$ не обязательно конечно. Будем рассматривать достижимые автоматы: любое состояние $s \in \mathcal{S}$ автомата достижимо из начального состояния s_0 после подачи на вход автомата слова $u \in \mathfrak{I}^*$ конечной длины. Положим $\mathfrak{I} = \mathcal{O} = \mathbb{F}_p$.

Каждый автомат $\mathfrak{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0)$ определяет отображение $f_{\mathfrak{A}}$ из кольца целых p -адических чисел $\mathbb{Z}_p$ в себя: слово бесконечной длины

$\alpha = \dots \alpha_{n-1} \dots \alpha_1 \alpha_0$ над алфавитом $\mathbb{F}_p$ рассматривается как целое p -адическое число $x \in \mathbb{Z}_p$, т.е. $x = x(\alpha) = \sum_{i=0}^{\infty} \delta_i(x) \cdot p^i$, где $\delta_i(x) \in \mathbb{F}_p$. Для любого $x \in \mathbb{Z}_p$ положим $\delta_i(f_{\mathfrak{A}}(x)) = O(\delta_i(x), s_i)$, $i = 0, 1, 2, \dots$, где $s_i = S(\delta_{i-1}(x), s_{i-1})$, $i = 1, 2, \dots$. Будем говорить, что отображение $f_{\mathfrak{A}}$ является *автоматным отображением* автомата $\mathfrak{A}$. Аналогичным образом мы можем рассматривать и *асинхронно автоматные отображения*: асинхронный автомат $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0)$ осуществляет преобразование $f_{\mathfrak{B}}$ кольца целых p -адических чисел $\mathbb{Z}_p$. Класс автоматных отображений совпадает с классом 1-липшицевых отображений, см. [1]; класс асинхронно автоматных отображений — нет.

Отображение $f_{\mathfrak{B}}: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ называется *отображением с задержкой n* , $n \in \mathbb{N}$, если данный асинхронный автомат $\mathfrak{B}$ слово $\alpha = \dots \alpha_{n-1} \dots \alpha_1 \alpha_0$ преобразует в слово $\beta = \dots \beta_{n+1} \beta_n$ так, что $O(\delta_i(\alpha_{n-1} \dots \alpha_1 \alpha_0), s_i) = e$, где e пустое слово, $i = 0, 1, 2, \dots, n-1$, $s_i = S(\delta_i(\alpha_{n-1} \dots \alpha_1 \alpha_0), s_{i-1})$, $i = 1, 2, \dots, n-1$; $O(\delta_i(\alpha), s_i) = \delta_i(\beta)$, $i = n, n+1, \dots$. Заметим что, как правило, термин «задержка» («задержка на n тактов») используется в более узком смысле, срав., например, с [7]: а именно, преобразователь с задержкой определяется как автомат, который прочитывает входное слово буква за буквой в течение первых n тактов и печатает пустое слово; после этого автомат выдает входное слово без изменений. В частности, *односторонний сдвиг*, см. [8], определяется асинхронным автоматом с одиночной задержкой.

Динамическая система есть тройка $(\mathbb{S}, \mu, f)$, где $\mathbb{S}$ есть измеримое пространство с мерой μ , а $f: \mathbb{S} \rightarrow \mathbb{S}$ — измеримая функция. Более того, мы будем полагать, что пространство $\mathbb{S}$ метрическое, т.е. $\mathbb{S}$ снабжено метрикой d . Отображение $F: \mathbb{S} \rightarrow \mathbb{S}$ называется *сохраняющим меру*, если $\mu(F^{-1}(S)) = \mu(S)$ для всякого измеримого $S \subset \mathbb{S}$. Сохраняющее меру отображение F называется *эргодическим*, если для каждого измеримого $S \subset \mathbb{S}$ такого, что $F^{-1}(S) = S$, либо $\mu(S) = 1$, либо $\mu(S) = 0$. Тройка $(\mathbb{Z}_p, \mu, f)$, где $f = f_{\mathfrak{B}}$ отображение с задержкой n , суть динамическая система на пространстве $\mathbb{Z}_p$. Элементарными подмножествами в $\mathbb{Z}_p$ являются шары $B_{p^{-k}}(a) = a + p^k \mathbb{Z}_p$, причем $\mathbb{Z}_p$ можно снабдить нормализованной мерой Хаара $\mu = \mu_p: \mu_p(\mathbb{Z}_p) = 1$ и $\mu_p(B_{p^{-k}}(a)) = p^{-k}$. Метрика $d = d_p$ определяется так: $d_p(x, y) = |x - y|_p$, причем $d_p(x, y) \leq \max\{d_p(x, z), d_p(z, y)\}$ для любых $x, y, z \in \mathbb{Z}_p$, т.е. пространство $\mathbb{Z}_p$ есть неархимедово пространство.

Теорема 1. *Отображение $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ с задержкой n является непрерывной функцией.*

Обозначим символом F_k редукцию f по модулю $p^{n \cdot (k-1)}$ на элементах кольца $\mathbb{Z}/p^{n \cdot k} \mathbb{Z}$ для $k = 2, 3, \dots$

Теорема 2. *Отображение $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ с задержкой n сохраняет меру тогда и только тогда, когда число F_k -прообразов точки $x \in \mathbb{Z}/p^{n \cdot (k-1)} \mathbb{Z}$ равно p^n , $k = 2, 3, \dots$*

Пусть $x_0 \in \mathbb{Z}_p$ и существует $r \in \mathbb{N}$ такое, что $f^r(x_0) = x_0$. Число r — длина периода точки x_0 . Орбита точки x_0 есть $\{x_0, x_1, \dots, x_{r-1}\}$, где $x_j = f^j(x_0)$, $0 \leq j \leq r-1$. Такая орбита называется r -циклом. Пусть $\gamma(k)$ есть $r(k)$ -цикл $\{x_0, x_1, \dots, x_{r(k)-1}\}$, $k = 1, 2, 3, \dots$, где $x_j = (f \bmod p^{kn})^j(x_0)$, $0 \leq j \leq r(k) - 1$.

Теорема 3. Пусть отображение $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ с задержкой n сохраняет меру. Тогда f эргодично, если $\gamma(k)$ единственный цикл для всех $k \in \mathbb{N}$.

СПИСОК ЛИТЕРАТУРЫ

- [1] Anashin V., Krennikov A. Applied algebraic dynamics. — Berlin–N. Y.: Walter de Gruyter GmbH & Co., 2009.
- [2] Тяпаев Л. Б. Геометрическая модель поведения автоматов и их неотличимость // Математика. Механика. — 1999. — № 1. — С. 139–143.
- [3] Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сар. ун-та, Нов. серия. Сер. : Математика. Механика. Информатика. — 2006. — Т. 6 № 1-2. — С. 121–133.
- [4] Тяпаев Л. Б. Геометрические образы автоматов и динамические системы // Дискретная математика и ее приложения. Материалы X Международного семинара. — 2010. — С. 510–513.
- [5] Тяпаев Л. Б., Василенко Д. В. Дискретные динамические системы, определяемые геометрическими образами автоматов // Интеллектуальные системы. — 2013. — Т. 17, №1-4. — С. 196–201.
- [6] Тяпаев Л. Б., Матов Д. О. Базисы геометрических образов для динамических систем, определяемых некоторыми классами автоматов // Компьютерные науки и информационные технологии. Материалы Международной научной конференции. — 2009. — С. 201–204.
- [7] Linz P. An introduction to formal languages and automata. — Jones and Bartlett learning, 2011.
- [8] Grigorchuk R. I., Nekrashevich V. V., and Sushchanskii V. I. Automata, dynamical systems, and groups // Proc. Steklov Institute Math. — 2000. — V. 231. — P. 128–203.

ПОСТРОЕНИЕ ИНВАРИАНТНОГО КЛАССА ПРИЗНАКОВ 3D-ИЗОБРАЖЕНИЙ

Федотов Николай Гаврилович, Моисеев Александр Владимирович¹,
Сёмов Алексей Александрович²

¹ Пензенский государственный университет, e-mail: fedotov@pnzgu.ru, moigus@mail.ru

² ООО «КомХэлф», e-mail: matematik_aleksey@mail.ru

В статье рассматривается новый подход к анализу и распознаванию 3D-изображений, основанный на методах и положениях стохастической геометрии

и представляющий собой развитие идей из [1]. В работе [6] представлены практические эксперименты по применению разрабатываемого метода. Математическая модель предлагаемого метода — гипертрейс-преобразование — представлено в [4].

Трейс-матрицы $3TM$ и TM являются удобным инструментом для анализа преобразований распознаваемых объектов, таких как движение и масштабные изменения [1, 2, 3]. Гипертрейс-матрица $3TM$ — 3D-трейс-образ исходного пространственного изображения, который содержит информацию о первоначальном объекте. Аналогично, трейс-матрица TM — 2D-трейс-образ плоского изображения 2D-фигуры сечения, полученного при пересечении плоскости $B(\eta(\omega, \varphi), r)$ исходного 3D-объекта F .

Свойства трейс-матриц в зависимости от операций, применяемых к 2D-изображению сечения, рассмотрены в [1]. Рассмотрим свойства гипертрейс-матриц в зависимости от операций, применяемых к 3D-изображению.

Поворот 3D-изображения в пространстве. В глобальных осях 3D-объекта каждая сканирующая плоскость B будет характеризоваться расстоянием r от начала координат до нее и углами ω и φ ($0 \leq \omega \leq 2\pi, 0 \leq \varphi \leq \pi$), где $\eta = [\cos \omega \cdot \sin \varphi, \sin \omega \cdot \sin \varphi, \cos \varphi]$ — единичный вектор в R^3 , ω — угол между осью $0x$ и проекцией на плоскость $0xy$ прямой $b \subset B$, φ — угол между осью $0z$ и прямой b :

$$B(\eta(\omega, \varphi), r) = \{(x, y, z) : x \cdot \cos \omega \cdot \sin \varphi + y \cdot \sin \omega \cdot \sin \varphi + z \cdot \cos \varphi = r\}.$$

Как было сказано в [4], для учета произвольной неизвестной пространственной ориентации объекта необходимо определить ключевые точки, которые характеризуют уникальные свойства 3D-объекта, независимые от его вращения в пространстве. Им будут соответствовать плоскости, для которых $B(\eta(\delta, \gamma), r) = B'(\eta(\delta', \gamma'), r)$.

Если сканирующую плоскость B в пространстве повернуть относительно прямой d , проходящей через фиксированный северный полюс сферы (первая ключевая точка), на угол π радиан, то она будет параллельна сама себе и ее вектор нормали $\vec{\eta}$ будет направлен в прямо противоположную сторону, так как для любого значения угла δ имеются равенства $B(\eta(\delta, \gamma), r) = B'(\eta(\delta + \pi, \pi - \gamma), r)$ и $\vec{\eta} = -\vec{\eta}'$. Другими словами, плоскостям $B(\eta(\delta, \gamma), r)$ и $B'(\eta(\delta + \pi, \pi - \gamma), r)$ будут соответствовать диаметрально противоположные точки опорной сетки на сфере. Так как вектор нормали плоскости определяет направление порядка следования сечений 3D-объекта сеткой сканирующих плоскостей (элементы матрицы $3TM$ по глубинной оси $0r$), то через каждый интервал длины π по оси 0δ переворачиваются вертикальные столбцы (ось 0γ) и глубинные строки (ось $0r$) гипертрейс-матрицы $3TM$. Заметим, что матрица $3TM$ будет 2π -периодична в направлении горизонтальной оси 0δ .

Перенос 3D-изображения в пространстве. Если происходит сдвиг исходного 3D-изображения на вектор $\{a \cdot \cos \lambda \cdot \sin \beta; a \cdot \sin \lambda \cdot \sin \beta; a \cdot \cos \beta\}$ длины a , то точка (x', y', z') сдвинутого изображения F' будет соответствовать точке (x, y, z) исходного изображения F следующим образом:

$$x' = x + a \cdot \cos \lambda \cdot \sin \beta, y' = y + a \cdot \sin \lambda \cdot \sin \beta, z' = z + a \cdot \cos \beta.$$

При переносе исходного трехмерного изображения произойдет сдвиг строк гипертрейс-матрицы $3TM$ в глубинном направлении на величину $a \cdot (\sin \beta \cdot \sin \gamma \cdot \cos (\delta - \lambda) + \cos \beta \cdot \cos \gamma)$ вверх или вниз в зависимости от знака выражения. При этом вертикальные столбцы и горизонтальные строки матрицы $3TM$ остаются на своём месте и не сдвигаются вдоль осей 0ω и 0φ , так как при сдвиге 3D-изображения угол сканирующей плоскости $B'(\eta(\delta', \gamma'), r')$, соответствующей сканирующей плоскости $B(\eta(\delta, \gamma), r)$ исходного изображения, не изменяется: $\delta' = \delta, \gamma' = \gamma$.

Таким образом, при сдвиге 3D-изображения в гипертрейс-матрице $3TM$ увеличивается или уменьшается количество нулевых элементов в глубинных строках (ось $0r$) в зависимости от его приближения или удаления от глобального начала координат. Поэтому 3D-трейс-образ изображения будет растягиваться вдоль оси $0r$ на число, определяемое вектором переноса.

Операция масштабирования 3D-изображения в пространстве. Если происходит масштабирование исходного 3D-изображения в μ раз, то точка масштабированного изображения F' будет соответствовать точке исходного изображения F следующим образом: $x' = \mu \cdot x, y' = \mu \cdot y, z' = \mu \cdot z$.

Поэтому сканирующей плоскости $B(\eta(\delta, \gamma), r)$ исходного изображения F будет соответствовать сканирующая плоскость $B'(\eta(\delta', \gamma'), r')$ масштабированного изображения F' : $x \cdot \cos \delta' \cdot \sin \gamma' + y \cdot \sin \delta' \cdot \sin \gamma' + z \cdot \cos \gamma' = \frac{r'}{\mu}, \mu \neq 0$. При $r' = \mu \cdot r$ и $\delta' = \delta, \gamma' = \gamma$ сканирующая плоскость $B'(\eta(\delta, \gamma), r')$ совпадет с плоскостью $B(\eta(\delta, \gamma), r)$. При масштабировании в μ раз 3D-изображение будет пересекать больше ($\mu > 1$) или меньше ($\mu < 1$) сканирующих плоскостей (изменяются размеры изображения при сохранении значения шага сканирования). Поэтому в глубинных строках гипертрейс-матрицы $3TM$ изменится количество ненулевых элементов, которые обозначают свойства сечений изображения сеткой плоскостей и 3D-трейс-образ будет расширяться или сужаться в μ раз вдоль оси $0r$. Отметим, что при масштабировании изображения начения элементов гипертрейс-матрицы $3TM$ будут изменяться в зависимости от вида функционала $Hypert$.

Трейс-матрицы $3TM$ и TM являются удобным инструментом для анализа движения распознаваемых объектов и их масштабных изменений. Возможности извлечения различных свойств 3D-объекта описаны в [5, 6].

Применяя при обработке матрицы соответствующие функционалы, которые инвариантны к приведенным выше преобразованиям изображения и изменениям строк гипертрейс- и трейс-матриц, мы будем конструировать признаки,

инвариантные к группе движений и масштабированию 3D-изображения. Строгое математическое описание данных свойств (изменений матрицы в результате движения 3D-изображения) описано выше.

Работа выполнена при поддержке РФФИ (проект № 15-07-04484-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Федотов Н. Г. Теория признаков распознавания образов на основе стохастической геометрии и функционального анализа. — М. : ФИЗМАТЛИТ, 2009. — 304 с.
- [2] Fedotov N. G., Ryndina S. V., Syemov A. A. Trace transform of spatial images // 11th International conference on Pattern Recognition and Image Analasis: New Information technologies (PRIA-11-2013). Conference Proceedings (V. I–II). — Samara: IPSI RAS, 2013. — V. 1. — P. 186–189.
- [3] Fedotov N. G., Ryndina S. V., Syemov A. A. Trace transform of three-dimensional objects: recognition, analysis and database search // Pattern Recognition and Image Analysis. Advances in Mathematical Theory and Applications. — 2014. — Vol. 24, No. 4. — P. 566–574.
- [4] Сёмов А. А. Основные методы построения гипертрейс-матриц // XXI век: итоги прошлого и проблемы настоящего плюс. Серия: технические науки. Информационные технологии. — 2015. — № 03. — С. 69–76.
- [5] Федотов Н. Г., Семов А. А., Моисеев А. В. Минимизация признакового пространства распознавания 3D изображения на основе стохастической геометрии и функционального анализа // Машинное обучение и анализ данных. — 2015. — Т. 1, № 13. — С. 1796–1814.
- [6] Федотов Н. Г., Семов А. А., Моисеев А. В. Интеллектуальные возможности гипертрейс-преобразования: конструирование признаков с заданными свойствами // Машинное обучение и анализ данных. — 2014. — Т. 1, № 9. — С. 1200–1214.

КЛАССИФИКАЦИЯ НА ОСНОВЕ ПРИЗНАКА ФОРМЫ: ПРОБЛЕМЫ И РЕЗУЛЬТАТЫ

Фофанов Вячеслав Борисович, Нагматуллин Тимур Рустэмович

АО «Научно-производственная корпорация “Системы прецизионного приборостроения”», e-mail: viatcheslavfofanov@gmail.com, nagmat12tim@gmail.com

Введение

При визуальной классификации часто используемым признаком является форма объекта. Оптико-электронные системы формируют изображение проекции объекта на плоскость перпендикулярную направлению наблюдения. Поэтому классификация объектов по форме сводится к сравнению формы

их проекций. Следует иметь в виду, что характерные особенности формы сохраняются только на крупномасштабных изображениях.

Для измерения эффективности признака или набора признаков будет применяться средняя вероятность правильной классификации, достигаемая при их использовании.

Определение формы

При визуальной классификации использование формы в качестве признака осуществляется, как правило, на подсознательном уровне. Автоматизация классификации требует формального определения понятие формы. Известно несколько подходов к решению этой задачи. В настоящей работе используется определение формы, предложенное в работах [1, 2]. Пусть D — ограниченное подмножество точек плоскости, лежащих внутри простой замкнутой жордановой кривой, называемое фигурой. Если D — выпуклое множество, то из каждой пересекающей его прямой оно вырезает только одну хорду. Назовем формой выпуклой фигуры D распределение вероятностей P_D длины хорды, вырезаемой D из случайной прямой. Будем говорить, что фигуры A и B имеют одну и ту же форму, если распределения P_A и P_B совпадают. В [2] доказано, что форма фигуры инвариантна к поворотам и параллельным переносам.

Таким образом, сравнение фигур A и B по форме заключается в проверке равенства распределений P_A и P_B . Методы математической статистики позволяют проверить равенство распределений P_A и P_B путем сравнения случайных выборок, полученных из этих распределений. Поэтому в качестве формы фигуры можно рассматривать выборку из длин хорд, вырезанных фигурой из случайных прямых. Пусть $l_A = (l_{A,k})_{1 \leq k \leq n_A}$ и $l_B = (l_{B,k})_{1 \leq k \leq n_B}$ — выборки длин хорд, вырезанных из этих прямых фигурами A и B . Предположение о равенстве распределений P_A и P_B в математической статистике называется гипотезой однородности. Для ее проверки разобьем множество R вещественных чисел на s интервалов. Пусть $m_{A,j}$ и $m_{B,j}$ — количество элементов выборок l_A и l_B соответственно, оказавшихся в j -ом интервале. Известно, что при равенстве распределений P_A и P_B распределение статистики $X_{n_A+n_B}^2$ вида

$$X_{n_A+n_B}^2 = n_A n_B \sum \frac{1}{m_{A,j} + m_{B,j}} \left(\frac{m_{A,j}}{n_A} - \frac{m_{B,j}}{n_B} \right)^2,$$

стремиться при $(n_A + n_B) \rightarrow +\infty$ к распределению χ^2 с $(s - 1)$ степенью свободы. Для проверки гипотезы однородности зададим положительное число α (например, 0.01 или 0.005) и, решив уравнение $P(\chi^2 \geq t_\alpha) = \alpha$ относительно t_α , построим критическую область $[t_\alpha, +\infty[$. Если $X_{n_A+n_B}^2 > t_\alpha$, то гипотеза отвергается. Таким образом, α имеет наглядную содержательную интерпретацию. Она равняется вероятности отвергнуть верную гипотезу.

Наконец, перейдем к описанию формы невыпуклых фигур. Такая фигура может вырезать из пересекающей ее прямой нескольких хорд. Поэтому сопо-

ставим каждой невыпуклой фигуре не одну, а пару случайных величин. Первая случайная величина будет описывать число хорд, вырезаемых фигурой из случайной прямой. Вторая — сумму их длин. Таким образом, формой невыпуклой фигуры назовем распределение двумерной величины.

Пусть θ — дискретная случайная величина со значениями в множестве $\mathbb{Q}$, равная числу хорд, вырезанных проекцией из случайной прямой, λ — случайная величина со значениями в $\mathbb{R}$, равная сумме длин всех хорд, вырезанных проекцией из случайной прямой. Пусть (θ_A, λ_A) и (θ_B, λ_B) — двумерные случайные величины. Очевидно, что два равенства

$$P(\theta_A = k) = P(\theta_B = k), k \in \mathbb{Q}, \quad (1)$$

$$P(\lambda_A \leq b | \theta_A = k) = P(\lambda_B \leq b | \theta_B = k), b \in \mathbb{R}, k \in \mathbb{Q}, \quad (2)$$

эквивалентны равенству

$$P(\theta_A = k, \lambda_A \leq b) = P(\theta_B = k, \lambda_B \leq b), b \in \mathbb{R}, k \in \mathbb{Q}, \quad (3)$$

означающему, что случайные векторы (θ_A, λ_A) и (θ_B, λ_B) имеют одно и то же совместное распределение. Поэтому для проверки равенства (3) достаточно проверить справедливость равенств (1) и (2) изложенными выше методами.

Классификация по форме

Изложенное выше определяет последовательность действий, выполняемых при классификации. Вначале на плоскости с проекцией наблюдаемого объекта требуется построить семейство случайных прямых и получить двумерную выборку. То же самое нужно проделать с проекциями объектов, образующих смесь. Наблюдаемый объект следует отнести к тому классу, в котором число проекций, имеющих ту же форму, что и проекция наблюдаемого объекта, оказалось наибольшим. При неизвестной ориентации наблюдаемого объекта применение решающего правила требует создания конечного набора проекций объектов смеси, обеспечивающего классификацию с заданной эффективностью.

В качестве иллюстрации изложенного подхода приведем оценку эффективности признака формы, полученную при классификации смеси из летательных аппаратов, разделенных на три класса с условными названиями самолеты, вертолеты и беспилотные. В ходе компьютерных экспериментов каждый объект представлялся своей проекцией со случайной ориентацией. Вероятности правильной классификации объектов каждого класса составили 0.75, 1.00 и 0.89. С учетом априорных вероятностей 0.25, 0.50 и 0.25 средняя вероятность правильной классификации равняется 0.91.

Классификация объектов и сегментация изображений

При решении прикладных задач исходной информацией об объектах служат изображения сцены. Поэтому вначале необходимо по изображению определить проекцию объекта и только после этого приступать к его классификации. Получение проекции по изображению сцены называется сегментацией. Сегментация

признается успешной, если форма проекции, полученной по изображению, совпадает с формой проекции, построенной по 3d модели. К сожалению, требования к свойствам изображения, гарантирующим успешную сегментацию, отсутствуют. Однако, для локально однородных сцен зависимость качества сегментации от заметности объекта, измеряемой величиной отношения сигнал/шум, и радиуса корреляции приведена в [3].

СПИСОК ЛИТЕРАТУРЫ

- [1] Fofanov V. B., Zhelezov A. S. Description of the shape of patterns with the help of random chords // 8th International conference on pattern recognition and image analysis: new information technologies (PRIA-8-2007), Yoshkar-Ola, Russian Federation, October 8–12, 2007, V. 2: conference proceedings. Yoshkar-Ola, 2007. Pp. 84–87.
- [2] Fofanov V. B., Zhiznevsky A. N. Concerning the Issue of Object Classification by Form // Research Journal of Applied Sciences. 2015. No. 8. Pp. 371–375.
- [3] Fofanov V. B., Zhiznevsky A. N. Concerning the Issue of Object Classification by Form. Part 2 // Research Journal of Applied Sciences. 2015. No. 8. Pp. 385–390.

О ЛАС-ВЕГАС-МОДЕЛИ АВТОМАТА С КВАНТОВЫМИ И КЛАССИЧЕСКИМИ СОСТОЯНИЯМИ

**Хадиев Камилль Равилевич¹, Ибрагимов Ришат Нариманович²,
Yakaryilmaz Abuzer³, Prusis Krisjanis⁴, Vihrovs Jevgenijs⁵**

¹ University of Latvia, Казанский федеральный университет, e-mail: kamilhadi@gmail.com

² Казанский федеральный университет, e-mail: rishat.ibrahimov@yandex.ru

³ University of Latvia, e-mail: abuzer@lu.lv

⁴ University of Latvia, e-mail: krisjanis.prusis@lu.lv

⁵ University of Latvia, e-mail: jevgenijs.vihrovs@lu.lv

Мы рассматриваем Лас-Вегас-модели квантовых и вероятностных автоматов и улучшаем в два раза известную оценку разницы между количеством состояний для вероятностных и детерминированных моделей. Также мы показываем аналогичную оценку для квантовой модели. Таким образом, практически достигнута максимальная возможная разница с КДА. Кроме того были получены аналогичные результаты для модели OBDD.

Определения

Конечный Лас-Вегас-автомат (ЛВ-ВКА) — это вероятностный автомат, который может выдать результат “accepted”, “rejected” или “don’t know”. При этом, если автомат принимает или отвергает слово (результат “accepted” или “rejected”), то он делает это всегда корректно. Следовательно, множество состояний разбивается на три непересекающихся подмножества: множества принимающих, отвергающих и нейтральных состояний для указанных выше возможных

исходов работы автомата, соответственно. ЛВ-ВКА A может распознать язык L с ограниченной ошибкой $\varepsilon < 1$, если каждое слово из языка L он принимает, а каждое слова не из языка L отвергает, при этом вероятность выдать вердикт “don’t know” меньше или равна ε . Подробное определение можно найти в работе [1]. Аналогичное определение мы можем рассмотреть для квантового конечного Лас-Вегас-автомата ЛВ-ККА, подробное определение можно найти в работе [2].

Для заданного языка L через $DFA(L)$, $LV_\varepsilon(L)$, и $ULV_\varepsilon(L)$ обозначим минимальные размеры ДКА, ЛВ-ВКА и ЛВ-ККА, распознающих язык L , соответственно, где ε — ограниченная ошибка для Лас-Вегас- и квантовых Лас-Вегас-автоматов. Заметим, что в случае точных вычислений $\varepsilon = 0$.

Модель ветвящихся программ OBDD может быть рассмотрена как неоднородный автомат с переменной структурой [4], то есть семейство автоматов $A_1, \dots, A_n, \dots$ для каждой из длины слов, при этом символы входного слова могут читаться в соответствии с заранее заданным порядком θ и функция перехода зависит в том числе от номера считываемого символа. Кроме того количество состояний может зависеть от длины слова. При этом, когда говорят об OBDD, то говорят о вычислении булевых функций. Для функции f и OBDD можно определить меры сложности, аналогичные автоматным: $OBDD(f)$, $LV_\varepsilon - OBDD(f)$, и $ULV_\varepsilon - OBDD(L)$

Вероятностные и квантовые Лас-Вегас-автоматы и OBDD

Применив результаты из коммуникационных вычислений [3, 2], можно получить следующие оценки:

Лемма 1. Для любого регулярного языка L и границы $\varepsilon < 1$ для ЛВ-КВА ЛВ-ККА выполняются следующие неравенства:

$$(DFA(L))^{1-\varepsilon} \leq LV_\varepsilon(L) \text{ и } (DFA(L))^{1-\varepsilon} \leq ULV_\varepsilon(L).$$

Для $\varepsilon = 0.5$ эта нижняя оценка позволяет получить квадратичную разницу в количестве состояний. С точностью до константы этот разрыв достигается [1] с помощью языка $END_k = \{u1v \mid u, v \in \{0, 1\}^* \text{ и } |v| = k - 1\}$: $DFA(END_k) = 2^k$ и $LV_{\varepsilon/2}(END_k) \leq 4 \cdot 2^{k/2}$.

Мы предлагаем новый язык $MXOR_k$, который позволяет улучшить оценку для ЛВ-КВА, и может быть распознан ЛВ-ККА с таким же числом состояний, как и у ЛВ-КВА. Язык $MXOR_k$ для $k > 0$ состоит из слов вида $\{0, 1\}^{<2k} x_1 \{0, 1\}^{2k-1} x_2 \{0, 1\}^{2k-1} \dots x_m \{0, 1\}^{2k-1}$, где $m > 0$, $x_i \in \{0, 1\}$ для $1 \leq i \leq m$, $\bigoplus_{i=0}^m x_i = 1$ и $x_0 = 0$.

Покажем, что для КДА, распознающего $MXOR_k$, потребуется не менее 2^{2k} состояний.

Теорема 1. $DFA(MXOR_k) \geq 2^{2k}$ для любого $k > 0$.

Доказательство. Рассмотрим 2^{2k} классов слов $C_1, \dots, C_{2^{2k}}$. Слово $w \in C_z$, где $(a_0, \dots, a_{2k-1}) = (z)$ — двоичное представление z , тогда и только тогда, когда выполняется условие $\bigoplus_{i \in \{1, \dots, |w|\}, (|w|-i) \bmod 2k=j} w_i = a_j$. Покажем,

что два слова из разных классов не эквивалентны по Майхиллу-Нероуду. $w \in C_z, w' \in C_{z'}, z' \neq z$. Это означает, что для $(a_0, \dots, a_{2k-1}) = (z)$ и $(a'_0, \dots, a'_{2k-1}) = (z')$ существует j такое, что $a'_j \neq a_j$. Без ограничения общности предположим, что $a_j = 1, a'_j = 0$. Рассмотрим слово v длины $|v| = 2k - 1 - j$. Тогда $wv \in MXOR_k$ и $w'v \notin MXOR_k$. **Теорема 1 доказана.**

Далее построим ЛВ-КВА и ЛВ-ККА, распознающий язык $MXOR_k$ с использованием $2 \cdot 2^k$ состояний.

Теорема 2. $LV_{0.5}(MXOR_k), ULV_{0.5}MXOR_k \leq 2 \cdot 2^k$ для $k > 0$.

Доказательство. Построим ЛВ-КВА P с ограниченной ошибкой 0.5. В начале работы автомат равновероятно выбирает один из двух возможных вариантов продолжения вычислений. В дальнейшем работа автомата состоит только из детерминированных переходов. В первом (втором) варианте вычислений предполагается, что x_i расположены на нечетных (четных) позициях. Множество состояний автомата P : $\{(p, s) \mid p \in \{p_0, p_1\} \text{ и } s \in \{s_{(0)}, \dots, s_{(2^k-1)}\}\}$, где (i) — строка длины k . Количество состояний $2 \cdot 2^k$. Первый вариант вычислений начинается в состоянии $(p_1, s_{(0)})$, второй — в состоянии $(p_0, s_{(0)})$. Оба варианта используют одинаковые переходы. Если P в состоянии (p_0, s) , то он всегда переходит в состояние (p_1, s) . Если P в состоянии $(p_1, s_{(i)})$ и следующий входной символ $x \in \{0, 1\}$, то автомат переходит в состояние $(p_1, s_{(j)})$, где (j) получено из i следующим образом: $(j)_k = x \text{ XOR } (i)_1$ и $(j)_l = (i)_{l+1}$ для $1 \leq l < k$. Если автомат заканчивает работу в состоянии (p_0, s) , то результат “don’t know”, так как был осуществлен неправильный выбор пути вычислений. Если P заканчивает работу в состоянии $(p_1, s_{(i)})$, то решение принимается по первому биту (i) : входное слово принимается (отвергается) если $(i)_1 = 1$ ($(i)_1 = 0$). Наконец, слова длины меньше $2k$ никогда не будут приняты, так как первый бит (0) не может быть изменен раньше, чем за $2k$ шагов. Квантовый автомат можно построить аналогично. **Теорема 2 доказана.**

Для OBDD можно показать результат, аналогичный лемме 1 [5, 3].

Рассмотрим булеву функцию $SSA(X)$, где $X \in \{0, 1\}^n$, n — четное. Обозначим через $s(X)$ конкатенацию всех четных бит x_{2i} , для которых $x_{2i-1} = 1$, а через $adr(X)$ — для которых $x_{2i-1} = 0$. Пусть целое $a(X)$ такое, что $(a(X)) = adr(X)$, тогда $SSA(X) = s(X)_{a(X)}$ и $SSA(X) = 0$, если $a(X) > |s(X)|$.

Для этой функции можно доказать следующую теорему по аналогии с доказательствами для автоматов.

Теорема 3. $OBDD(SSA) \geq 2^{n/2 - \log_2 n - 1}$.

$LV_{0.5} - OBDD(SSA), ULV_{0.5} - OBDD(SSA) \leq 2^{n/4 + 3 \log_2 n}$.

Работа выполнена при поддержке ERC Advanced Grant MQC.

СПИСОК ЛИТЕРАТУРЫ

- [1] Hromkovich J., Schnitger G. On the power of Las Vegas for one-way communication complexity, OBDDs, and finite automata // Information and Computation. — 2001. — V. 169. — No. 2. — P. 284–296.
- [2] Klauck H. On quantum and probabilistic communication: Las Vegas and one-way protocols // Proceedings of the thirty-second annual ACM symposium on theory of computing. — ACM, 2000. — P. 644–651.
- [3] Hirvensalo M., Seibert S. Lower bounds for Las Vegas automata by information theory // RAIRO – Theoretical Informatics and Applications. — 2003. — V. 37. — No. 1. — P. 39–49.
- [4] Wegener I. Branching Programs and Binary Decision Diagrams: Theory and Applications. — Philadelphia: SIAM, 2000. — 408 p.
- [5] Sauerhoff M., Sieling D. Quantum branching programs and space-bounded nonuniform quantum complexity // Theoretical Computer Science. — 2005. — V. 334. — No. 1-3. — P. 177–225.

ИЕРАРХИИ ДЛЯ КВАНТОВЫХ И КЛАССИЧЕСКИХ ОДИН РАЗ ЧИТАЮЩИХ УПОРЯДОЧЕННЫХ ВЕТВЯЩИХСЯ ПРОГРАММ

Хадиев Камиль Равилевич¹, Хадиева Алия Ихсановна²

¹ University of Latvia, Казанский федеральный университет, e-mail: kamilhadi@gmail.com

² Казанский федеральный университет, e-mail: aliya.khadi@gmail.com

Мы рассматриваем известную модель ветвящихся программ — OBDD. Подробнее о ней можно прочесть в книге [1]. Эта модель является удобной для вычисления булевых функций. Известно, что классы $LSPACE/poly$ и NC^1 совпадают с классами функций, вычислимых ветвящимися программами, а также OBDD могут рассматриваться как автоматы с переменной структурой. Кроме того, ветвящиеся программы являются хорошей моделью для потоковых алгоритмов, используемых в промышленном программировании. В последние десятилетия исследователи активно рассматривают квантовые OBDD, подробнее о них можно узнать в статье [2]. Одним из вопросов, который интересен для этой модели — это построение иерархии классов сложности. Результаты для детерминированной и недетерминированной OBDD исследовались в статье [3]. В данной работе мы рассмотрим вопрос построения иерархии для вероятностных и квантовых OBDD с ограниченной ошибкой.

OBDD на множестве переменных $X = \{x_1, x_2, \dots, x_n\}$ — это ветвящаяся программа, обладающая следующими свойствами. Ее вершины разбиты на n уровней $1, \dots, n$ таким образом, что для каждого ребра из вершин уровня i ведут только в вершины уровня $(i + 1)$. На каждом уровне i считывается

значение только одной переменной x_{j_i} . На любом пути вычисления каждая переменная считывается один раз. Говорят, что OBDD P читает переменные в порядке $\theta = (j_1, \dots, j_n)$. *Ширина* $w(P)$ OBDD P — это максимум от количества вершин на уровне, взятый по всем уровням P . Говорят, что OBDD $P(X)$ вычисляет булеву функцию $f(X)$ ($f : \{0, 1\}^n \rightarrow \{0, 1\}$), если для любого набора $\nu \in \{0, 1\}^n$ такого, что $f(\nu) = 1$, в $P(X)$ есть путь из начальной вершины в ту из двух финальных вершин, которая помечена символом 1. В противном случае такого пути нет. Вершины последнего уровня называются финальными и помечаются символами из $\{0, 1\}$.

POBDD (вероятностная OBDD) — это OBDD, в которой разрешены вероятностные переходы. QOBDD (квантовая OBDD) — это OBDD, в которой преобразования происходят над квантовым регистром. Квантовый регистр — это вектор комплексных чисел $|\psi\rangle$, для которого верно следующее: $\sum_{i=1}^w ||\psi\rangle[i]||^2 = 1$, где w — ширина QOBDD. Для квантовой OBDD на i -ом уровне применяется одно из унитарных преобразований U_i^0 или U_i^1 , в зависимости от прочитанной переменной. Таким образом, после i -го уровня регистр переходит в состояние $|\psi^i\rangle = |\psi^{i-1}\rangle U_i^{x_{i_j}}$, где $|\psi^0\rangle$ — это начальное состояние. После n -го уровня производится измерение регистра. Вероятность того, что результат на входном наборе будет $z \in \{0, 1\}$, равна $Pr_z = \sum_{i \in Result_z} ||\psi^n\rangle[i]||^2$, где множество $Result_0 \subset \{1, \dots, w\}$, а множество $Result_1 = \{1, \dots, w\} \setminus Result_0$.

Говорят, что POBDD P вычисляет булеву функцию $f(X)$ с ограниченной ошибкой, если существует такая константа $0 < \delta < 0.5$, что для любого набора $\nu \in \{0, 1\}^n$ такого, что $f(\nu) = 1$, в $P(X)$ вероятность выдать ответ 1 не менее, чем $0.5 + \delta$, а для $f(\nu) = 0$ такая вероятность менее чем $0.5 - \delta$. Аналогично для QOBDD R . Обозначим $PWIDTH(f) = \{w = w(P) : \text{POBDD } P \text{ вычисляет } f \text{ с ограниченной ошибкой}\}$ и $QWIDTH(f)$ — аналогичное множество для QOBDD.

Рассмотрим классы **PROBDD** $_d$ и **BQOBDD** $_d$, состоящие из булевых функций, вычисляемых POBDD и QOBDD ширины d с ограниченной ошибкой, соответственно.

Для того чтобы построить иерархии для этих классов, рассмотрим модификацию функции $WS_n(X)$ из работы [4]. Модифицированная функция $WS_n^b(x)$ получена из оригинальной путем добавления фиктивных переменных. Рассмотрим целые положительные n , b , и $X = (x_1, \dots, x_n) \in \{0, 1\}^n$. Пусть $p(b)$ — наименьшее простое число, превосходящее b , при этом функция $s_b(X) = \left(\sum_{i=1}^b i \cdot x_i\right) \bmod p(b)$. Тогда $WS_n^b(x) = x_{s_b(X)+1}$ для $s_b(X) < b$ и $WS_n^b(X) = 0$ иначе. Известно, что для $WS_n^b(X)$ любая POBDD P , вычисляющая ее с ограниченной ошибкой, имеет ширину не менее чем $2^{\Omega(n)}$.

Лемма 1. Для достаточно больших n и b такого, что $const = o(b)$ и $w \in PWIDTH(WS_n^b)$ выполняется: $2^{\Omega(b)} \leq w \leq 2^b$.

Левое неравенство может быть доказано способом, аналогичным методу в работе [4]. Правое следует из того, что для любой функции, зависящей от всех своих переменных, можно построить OBDD ширины 2^n , построив полное бинарное дерево.

Используя свойства $WS_n^n(X)$ докажем иерархию для **ВРОБDD**_d

Теорема 1. Для целых чисел $d = o(2^n)$, $const = o(d)$, выполняется утверждение: **ВРОБDD**_{d^{1/δ}} $\subsetneq$ **ВРОБDD**_d при условии $const = o(\delta)$.

Доказательство. Очевидно, что **ВРОБDD**_{d^{1/δ}} $\subseteq$ **ВРОБDD**_d. Докажем неравенство этих классов. Согласно лемме 1 выполняется $WS_n^{\log d} \in \mathbf{ВРОБDD}_d$. В тоже время любая **ВРОБDD** P , вычисляющая функцию с ограниченной ошибкой, такова, что $w(P) = 2^{\Omega(\log d)} > 2^{(\log d)/\delta} = d^{1/\delta}$, следовательно, $WS_n^{\log d} \notin \mathbf{ВРОБDD}_{d^{1/\delta}}$.

Теорема 1 доказана.

Рассмотрим результаты для **QOBDD**. Для этого обсудим сложностные свойства трех функций: MOD_n^p , $MSW_n^b(X)$, $REQ_n^b(X)$. Булева функция $MOD_n^p(X) = 1$ тогда и только тогда, когда $(\sum_{i=1}^n x_i) \bmod p = 0$. Булева функция $MSW_n^b(X)$ — модификация функции $MSW_n(X)$ из [5]. $MSW_n^b(X) = (r \sim z) \& (x_z \oplus x_{r+n/2})$, где числа $z = s_{b/2}(x_1, \dots, x_{b/2})$, $r = s_{b/2}(x_{b/2+1}, \dots, x_b)$. Определим $REQ_n^b(X)$. Пусть $q(t+1) = b$, $t = \lceil \log_2 q \rceil$. Разобьем первые b переменных на q блоков подряд идущих переменных, обозначим переменные i -го блока $(y_0^i, \dots, y_{t-1}^i, z^i)$. Пусть $bin(y^i) = \sum_{j=0}^t 2^j y_j^i$, $Adr(X, i) = Adr(X, i-1) \oplus bin(y^i)$, $Adr(X, 0) = 0$. $REQ_n^b(X) = 1$ тогда и только тогда, когда $\sum_{i=1}^{q/2} 2^{Adr(x,i)} z^i = \sum_{i=q/2+1}^q 2^{Adr(x,i)} z^i$. Для этих функций выполняется следующее утверждение.

Лемма 2. Для $w \in QWIDTH(REQ_n^b)$ выполняется: $\lfloor b/\lceil \log b + 1 \rceil \rfloor \leq w \leq b^2$.

Для $w \in QWIDTH(MOD_n^p)$ выполняется: $\lfloor \log p \rfloor \leq w \leq O(\log p)$.

Для $w \in QWIDTH(MSW_n^b)$ выполняется: $\lfloor 2^{\Omega(b)} \rfloor \leq w \leq 2^b$ для $const = o(b)$.

Используя эти результаты, можно доказать иерархию для **BQOBDD**_d.

Теорема 2. Для целых d справедливы следующие утверждения:

BQOBDD_{d/δ²} $\subsetneq$ **ВРОБDD**_{d²}, для $d < \log n$, $d > 2$, $const = o(\delta)$.

BQOBDD_{d/ log₂² d} $\subsetneq$ **ВРОБDD**_{d²}, для $d < n$, $d > 2$.

BQOBDD_{d^{1/δ}} $\subsetneq$ **BQOBDD**_d, для $d = o(2^n)$, $const = o(d)$, $const = o(\delta)$.

Работа выполнена при поддержке ERC Advanced Grant MQC.

СПИСОК ЛИТЕРАТУРЫ

- [1] Wegener I. Branching Programs and Binary Decision Diagrams: Theory and Applications. — Philadelphia: Society for Industrial and Applied Mathematics, 2000.
- [2] Ablayev F. On the computational power of probabilistic and quantum branching program / F. Ablayev, A. Gainutdinova, M. Karpinski, C. Moore, C. Pollett // Information and Computation. — 2005. — V. 203. — No. 2. — P. 145–162.

- [3] Ablayev F. Very narrow quantum OBDDs and width hierarchies for classical OBDDs / F. Ablayev, A. Gainutdinova, K. Khadiev, A. Yakaryılmaz // Lobachevskii Journal of Mathematics. — 2016. — V. 37. — № 6. — P. 670–682.
- [4] Savicky P., Zak S. A read-once lower bound and a $(1, +k)$ -hierarchy for branching programs // Theoretical Computer Science. — 2000. — V. 238. — No. 1. — P. 347–362.
- [5] Sauerhoff M. Quantum vs. Classical read-once branching programs // Dagstuhl Seminar Proceedings. — Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.

О СЛОЖНОСТИ МИНИМИЗАЦИИ КВАЗИЦИКЛИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

Чухров Игорь Петрович

Институт автоматизации проектирования РАН, Москва, e-mail: chip@icad.org.ru

Исследуются булевы функции, которые сочетают различные свойства, обеспечивающие экстремальные значения характеристик трудоёмкости минимизации, неприменимость локальных методов сокращения трудоёмкости перебора и невозможность эффективного использования достаточных условий минимальности при применении универсальных методов минимизации.

Для построения и оценки характеристик квазициклических булевых функций используются:

циклические функции экспоненциальной протяжённости,
поясковые функции ограниченной протяжённости,
доминирование множеств в задаче о минимальном покрытии,
достаточные условия минимальности, основанные на независимых семействах множеств.

преобразования функций, сохраняющие метрические свойства множеств вершин в единичном кубе.

Обобщение некоторых понятий на множества элементов позволяет расширить возможности применения методов обоснования минимальности покрытий и получить экстремальные нижние оценки числа структурно разнообразных минимальных комплексов граней для построенных функций. Однако вычислительная эффективность поиска и проверки таких обобщённых свойств, которые имеют не локальный характер, оказывается неприемлемой.

При изложении используются понятия и обозначения для множества булевых функций n переменных P_n , n -мерного единичного куба B^n и задачи о минимальном покрытии конечного множества, которые можно найти в [1–4]. Множество единичных вершин функции $f \in P_n$ в кубе B^n обозначим через N_f .

Протяжённостью функции называется диаметр наибольшей из компонент интервального графа, вершинами которого являются максимальные грани функции, а рёбрами — пары пересекающихся граней.

(i) Булева функция $f \in P_n$ называется *k-циклической* если интервальный граф функции является циклом, максимальная размерность граней равна k и каждое пересечение максимальных граней содержит одну вершину.

Множество вершин, которые содержатся в пересечении двух максимальных граней циклической функции f , обозначим через A_f . Все максимальные грани размерности больше 1 являются ядровыми. Функцию, для которой множество единичных вершин в кубе B^n есть множество собственных вершин ядровых граней $N_f \setminus A_f$, обозначим через W_f .

Протяжённость циклической функции f равна $|S_f| - 1$, где S_f — множество максимальных граней функции. При построении k -циклических функций, обладающих экспоненциальной протяжённостью и определёнными свойствами максимальных граней, используются 1-циклические функции, на которых достигается максимальный порядок протяжённости равный 2^n для функций n переменных [1, стр. 113].

(ii) Функция $f \in P_n$, для которой множество N_f содержит вершины слоёв B_i^n с номерами $i = m - h, \dots, m$ куба B^n , где $0 \leq h \leq m \leq n$, называется *поясковой* и обозначается через $S_{m-h,m}^n(\tilde{x}^n)$. Поясковая функция имеет ограниченную протяжённость при h порядка n , а число максимальных граней может экспоненциально превосходить число единичных вершин функции. Любая максимальная грань поясковой функции входит в некоторый комплекс граней, который является минимальным относительно широкого класса мер сложности [2].

(iii) *Отношение доминирования* в задаче о минимальном покрытии определяется для системы множеств $\langle X, Y \rangle$, где $Y \subseteq 2^X$. Если для множеств $A, B \subset X$ любое семейство множеств $S \subseteq Y$, которое содержит множество A , содержит и множество B , то множество A доминирует множество B . Для сокращения размерности системы множеств [4] используется отношение доминирования только для одноэлементных множеств $A = \{x_A\}$ и $B = \{x_B\}$. При этом для определения отношения доминирования достаточно рассматривать только множества $y \in Y$, а не семейства множеств $S \subseteq Y$, и выполнение условия: если $x_A \in y$, то $x_B \in y$ для любого множества $y \in Y$.

(iv) *Достаточные условия минимальности* покрытия для системы множеств $\langle X, Y \rangle$ определяются на основе нижних границ, вычисляемых по независимому семейству множеств $\mathcal{A} = \{A \mid A \subset X\}$, для которого любое множество $y \in Y$ пересекается не более чем с одним множеством $A \in \mathcal{A}$ [3]. Независимое множество является частным случаем независимого семейства множеств, в котором каждое множество состоит из одного элемента.

Множество квазициклических функций $\mathcal{F}_{n,k} \subset P_n$ определяется по k -циклической функции $f \in P_r$, где $k < r < n$, и поясковым функциям:

$$F_f(\tilde{x}^n) = f(x_1, \dots, x_r) S_{m-h,m}^{n-r}(x_{r+1}, \dots, x_n) \text{ при } k = 1 \text{ и } h < m \leq (n-r)/2,$$

$$F_f(\tilde{x}^n) = f(x_1, \dots, x_r) S_{m-h,m}^{n-r-2}(x_{r+1}, \dots, x_{n-2}) \bar{x}_{n-1} \bar{x}_n \vee W_f(x_1, \dots, x_r) \cdot \\ \cdot \left(S_{m-h,m-h_1}^{n-r-2}(x_{r+1}, \dots, x_{n-2}) x_{n-1} \bar{x}_n \vee S_{m-h_2,m}^{n-r-2}(x_{r+1}, \dots, x_{n-2}) \bar{x}_{n-1} x_n \right)$$

при $k \geq 2$ и $1 \leq h_1 - 1 \leq h_2 < h < m \leq (n-r-2)/2$, где W_f — функция, для которой единичными вершинами в кубе B^r являются собственные вершины ядровых граней функции f .

Теорема 1. В множестве функций $\mathcal{F}_{n,k}$ при определённых значениях параметров k, r, m, h, h_1, h_2 есть функции, которые имеют свойства:

экспоненциальная протяжённость и нет ядровых граней;

число максимальных граней экспоненциально превосходит число единичных вершин функции;

экспоненциальное число доминирующих множеств единичных вершин функции, каждое из которых имеет экспоненциальную мощность;

минимальность комплексов граней основывается достаточными условиями, которые используют семейство независимых множеств экспоненциальной мощности, в котором каждое множество имеет экспоненциальную мощность;

каждая максимальная грань входит в некоторый кратчайший комплекс;

дважды экспоненциальное число кратчайших и минимальных комплексов граней, которые имеют различные множества собственных вершин.

Изучение квазициклических функций позволяет расширить понимание проблем и сложности минимизации булевых функций, к которым применяются алгоритмы использующие переборные схемы.

Работа выполнена при поддержке РФФИ (проект № 16-01-00593-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Васильев Ю. Л., Глаголев В. В. Метрические свойства дизъюнктивных нормальных форм // Дискретная математика и математические вопросы кибернетики. Т. 1. — М.: Наука, 1974. — С. 99–148.
- [2] Чухров И. П. О мерах сложности комплексов граней в единичном кубе // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 6. — С. 77–94.
- [3] Чухров И. П. О доказательстве минимальности покрытий через обобщение понятия независимости // Дискретный анализ и исследование операций. — 2017. — Т. 24, № 2. — С. 102–119.
- [4] Coudert O., Sasao T, Two-level logic minimization // Logic Synthesis and Verification. — Norwell, MA: Kluwer Acad. Publ., 2002. — P. 1–27.

СЛОЖНОСТЬ КОНВЕЙЕРНОЙ РЕАЛИЗАЦИИ ДИСКРЕТНЫХ МАРКОВСКИХ ПРОЦЕССОВ, ЗАДАННЫХ БЛОЧНЫМИ СТОХАСТИЧЕСКИМИ МАТРИЦАМИ

Шалагин Сергей Викторович

Казанский национальный исследовательский технический университет им. А. Н. Туполева — КАИ, e-mail:
Sshalagin@mail.ru

Определены оценки временной и аппаратной сложности конвейерной реализации дискретных стохастических марковских процессов (ДСМП). В качестве базовых элементов определены конечные детерминированные автоматы с множествами входов и состояний заданной размерности. Оценки временной и аппаратной сложности получены, в частности, для ДСМП, задаваемых блочными матрицами: эргодическими стохастическими матрицами, которые включают блоки из ненулевых элементов, размерность которых не превышает заданную.

Для стохастической матрицы размерности l на n имеет место выражение [1]:

$$P_{l \times n} = \sum_{b=1}^B a_b A_b, \quad (1)$$

где $B \leq (n-1) \cdot l + 1$, (a_b) — имплицитный вектор, (A_b) — система стохастических булевых матриц размерности l на n , $b = \overline{1, B}$.

Введем в рассмотрение конечный детерминированный автомат (КДА) вида $A = (X, S, s = \phi(x, s))$, где X, S — множества входов и внутренних состояний, $s = \phi(x, s)$ — автоматная функция, реализующая преобразование вида $S \times X \rightarrow S$.

Стохастическая функция, определенная на основе СМ $P_{l \times n}$ представима (согласно известной методике [2, 3]) структурной схемой, включающей генератор дискретной случайной величины (ДСВ) $X : |X| \leq B$ и КДА вида A , для которого, в общем случае, $|S| = n$, $|X| \leq B$. С целью уменьшения оценок сложности вычисления $s = \phi(x, s)$ актуальна задача снижения верхней границы для значения B , имеющего порядок $O(n \cdot l)$.

Имеет место [4]

Замечание. Для частных случаев СМ, определенных согласно [5, 6], верхняя оценка для значения B может иметь меньшее значение.

СМ $P_{l \times n}$ представима согласно выражению:

$$P_{l \times n} = \left(\hat{P}_{1 \times d}^{(i)} \cdot P'_{d \times n}(i) \right), \quad i = \overline{1, l}, \quad (2)$$

где $n \leq d \cdot l$, $\hat{P}_{1 \times d}^{(i)} = (\hat{p}_1^{(i)} \dots \hat{p}_d^{(i)})$, $P'_{d \times n}(i) = (M_1^{(i)} \dots M_d^{(i)}) \cdot I_d$, $\hat{p}_k^{(i)} = \sum_{j \in D_k} p_{ij}$, $M_k^{(i)} = (p_{ij} / \hat{p}_k^{(i)})_{1 \times (n/d)}$, $j \in D_k$, $k = \overline{1, d}$, I_d — $d \times n$ -матрица, в которой

d -я строка содержит значения «1», а остальные элементы — значения «0», $i = \overline{1, l}$. При этом $P_{l \times n} = (p_{k_1} \dots p_{k_d})$, $i = \overline{1, l}$, $c_k = n \cdot (k-1)/d + 1, n \cdot k/d$, $D_k = [n \cdot (k-1)/d + 1, n \cdot k/d]$, $k = \overline{1, d}$. Согласно [4, 7], имеет место

Утверждение. Для $n \leq d \cdot l$, СМ $P_{l \times n}$ представима согласно (2) на основе генератора ДСВ X' : $|X'| \leq \hat{B}$, КДА вида A_1 : $|S_1| = d$, $|X_1| \leq \hat{B}$, $\hat{B} \leq (d-1) \cdot l + 1$, d генераторов ДСВ $X''_{\hat{X}}$: $|X''_{\hat{X}}| \leq B'$, $\lceil \log_2 \hat{B} \rceil$ мультиплексоров « d в 1» и КДА вида A_2 : $|S_2| = n/d$, $|X_2| \leq \hat{B}'$, $B' \leq (n/d - 1) \cdot l + 1$.

Представляют интерес определенные частные случаи СМ. Например, блочные правые и левые СМ [8], заданные согласно (2) на основе утверждения.

Пусть блочные СМ представимы на основе блоков, состоящих из ненулевых элементов. Размер блоков для блочных правых (П) СМ — $m_2 \times n_1$ и $m_1 \times n_2$, а для блочных левых (Л) — $l_1 \times n_1$ и $l_2 \times n_2$, $l_1 + l_2 = l$, $n_1 + n_2 = n$. В случае представления блочных СМ на основе разложения вида (1) согласно [2, 3], величина $B \leq Q - m + 1$. Причем для ПСМ $Q = l_2 \cdot n_1 + l_1 \cdot n_2$, а для ЛСМ $Q = l_1 \cdot n_1 + l_2 \cdot n_2 + 2$. В случае представления ПСМ на основе утверждения, величина $|S_1| = 2$, $|X_1| = 1$, $|S_2| = n' = \max(n_1, n_2)$, $|X_2| \leq l' \cdot (n' - 1) + 1$, где $l' = \max(l_1, l_2)$. В случае представления ЛСМ на основе утверждения, величина $|S_1| = 2$, $|X_1| \leq 4$, $|S_2| = n'$, $|X_2| \leq l' \cdot (n' - 1) + 1$.

СПИСОК ЛИТЕРАТУРЫ

- [1] Лоренц А. А. Синтез надежных вероятностных автоматов. — Рига: «Зинатне», 1975. — 168 с.
- [2] Поспелов Д. А. Вероятностные автоматы. — М.: «Энергия», 1970. — 88 с.
- [3] Ченцов В. М. Об одном методе синтеза автономного стохастического автомата // Кибернетика. — 1968. — № 3. — С. 32–35.
- [4] Шалагин С. В. Метод разложения стохастических матриц для синтеза конвейерных генераторов дискретных марковских процессов // Вестник технологического университета. — 2015. — Т. 18, № 10. — С. 160–162.
- [5] Захаров В. М., Эминов Б. Ф. Анализ алгоритмов разложения двоично-рациональных стохастических матриц на комбинации булевых матриц // Информационные технологии. — 2008. — № 3. — С. 54–59.
- [6] Кузнецов С. Е., Нурмеев Н. Н., Салимов Ф. И. Задача о минимальном имплицитующем векторе // Математические вопросы кибернетики. — 1991. — Вып. 3. — С. 199–216.
- [7] Шалагин С. В. Конвейерное генерирование дискретных марковских процессов на основе разложения стохастических матриц // «Дискретная математика и ее приложения»: материалы XII Междунар. семинара имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.) / Под. ред. О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 178–181.

- [8] Захаров В. М. и др. К задаче дискриминантного анализа автоматных марковских моделей / В. М. Захаров, Н. Н. Нурмеев, Ф. И. Салимов, С. В. Шалагин, С. Ю. Соколов // Вестник Казанского государственного технического университета им. А. Н. Туполева. — 2001. — № 3. — С. 37–39.

ПОСЛЕДОВАТЕЛЬНАЯ ОЦЕНКА АЛЬТЕРНАТИВ С ПОМОЩЬЮ ОТНОСИТЕЛЬНЫХ АСИМПТОТИЧЕСКИХ ВЕЛИЧИН СРЕДНЕГО ДОХОДА

Шорникова Татьяна Александровна

Пензенский государственный технологический университет, e-mail: shornikovat@mail.ru

Рассмотрим следующую задачу — расчет асимптотической величины среднего дохода, используя системы уравнений для вероятностей перехода из одного состояния в другое. Для этого построим стохастическую модель с использованием случайных процессов на основе выбора с помощью производящей функции различных альтернатив.

Вместо нахождения величин $v_i(n)$ (общий ожидаемый доход после n шагов) путем последовательной оценки альтернатив на каждом шаге сформулируем асимптотическую формулу для $v_i(n)$ и с помощью вычисленных на ее основе величин рассмотрим альтернативы [1].

Используем предложенный подход для дискретных изменений с постоянной оценкой состояний. Другие случаи потребуют лишь незначительных модификаций.

На первом шаге решения задачи сформулируем известное асимптотическое соотношение между $v_i(n)$ и $v_i(n-1)$ [2]:

$$v_i(n) = q_i + \sum_{j=1}^N p_{ij} \cdot [(n-1)g + v_j].$$

Далее используем следующую формулу [2]:

$$v_i(n) = ng + v_i,$$

где q_i — сумма произведений вероятностей перехода на соответствующую экономическую оценку, g — средний доход, взвешенный по предельным вероятностям, показывающим вероятности отдельных состояний после достаточно длительного хода процесса, v_i — одномоментный доход при i -ом состоянии.

Тогда можно записать:

$$ng + v_i = q_i + \sum_{j=1}^N p_{ij} \cdot [(n-1)g + v_j].$$

что при $n = 1$ даст:

$$g + v_i = q_i + \sum_{j=1}^N p_{ij} v_j.$$

Получили N уравнений для $N + 1$ неизвестных $g, v_1, \dots, v_N$.

Для принятия решения достаточно знать соотношения между v_i , т.е. относительные значения общего ожидаемого дохода [3]. Эти соотношения можно определить просто, потребовав лишь постоянства значений разности $v_{i-1} - v_i$. Тогда система уравнений расширяется за счет уравнения $v_N = 0$. Вычисленные v_i будут отличаться от исходных на одну и ту же постоянную величину. Это означает, что разница между ними будет такая же, как и между исходными v_i . Поскольку при выборе альтернатив речь идет о различии их оценок, то можно воспользоваться этими «относительными» v_i . Разницу $v_1 - v_2$ можно интерпретировать, например, как разницу между ожидаемым доходом процесса, вышедшим из состояний 1 и 2.

Определив $g, v_1, \dots, v_N$, выразим относительные асимптотические величины $v_i(n)$.

Перейдем ко второму шагу решения поставленных задач. С помощью величин $g, v_1, \dots, v_N$ можно более просто и однозначно выбирать оптимальную альтернативу [3]. Критерием выбора альтернативы является формула [4]

$$q_i^k + \sum_{j=1}^N p_{ij}^k v_j.$$

При достаточно большом n ее можно заменить формулой [5]

$$q_i^k + \sum_{j=1}^N p_{ij}^k (ng + v_j).$$

Весь процесс решения можно резюмировать следующим образом:

1) с помощью величин p_{ij}, q_i по формуле

$$g + v_i = q_i + \sum_{j=1}^N p_{ij} v_j$$

определяются величины v_i, g ($v_n = 0$).

2) для каждого состояния отыскивается альтернатива, максимизирующая

$$q_i^k + \sum_{j=1}^N p_{ij}^k v_j,$$

где v_j определяются в п.1;

3) найденная альтернатива даст величины q_i^k, p_{ij}^k для повторения шага 1 или 2.

СПИСОК ЛИТЕРАТУРЫ

- [1] Алехина М. А., Логвина О. А. Оценка значимости воздействия в математическом моделировании экологического состояния объекта // Журнал «XXI век: итоги прошлого и проблемы настоящего плюс». — 2016. — № 2 (30). — С. 217–221.
- [2] Шорникова Т. А. Расчет дохода при стохастическом моделировании // Журнал «Обозрение прикладной и промышленной математики». — 2009. — Т. 16, № 5. — С. 951–952.
- [3] Гусынина Ю. С. Математико-статистическое моделирование производственной системы // Сборник научных трудов международной научно-практической конференции «Человек, общество и государство в современном мире»: в 2 томах. — 2016. — С. 241–244.
- [4] Шорникова Т. А. Стохастическое моделирование процессов с помощью производящей функции // Журнал «Модели, системы, сети в экономике, технике, природе и обществе». — 2016. — № 3 (19). — С. 88–98.
- [5] Shornikova T. A., Kalashnikova E. Y., Halitova G. I. Diffusive Markovskiye of transformation in the many-sided corner-measured space // European Researcher. — 2012, Vol. (20). — № 5-1. — Pp. 529–531.

ОЦЕНКИ ФУНКЦИИ ШЕННОНА ДЛЯ ДИНАМИЧЕСКОЙ АКТИВНОСТИ ОРИЕНТИРОВАННЫХ КОНТАКТНЫХ СХЕМ

Шуплецов Михаил Сергеевич

Московский государственный университет имени М. В. Ломоносова, e-mail: shupletsov@cs.msu.ru

Введение

Оценка энергопотребления интегральных схем является одной из важных задач проектирования СБИС. В современных интегральных схемах, построенных на основе КМОП технологий, выделяют как статическое энергопотребление, связанное с рассеянием тепла и поддержанием заданного потенциала в узлах схемы, подключенных к источнику питания, так и динамическое энергопотребление, возникающее при изменении потенциалов в узлах схемы.

Ранее, для анализа статического и динамического энергопотребления интегральных схем в ряде работ были введены специальные функционалы сложности для модели схем из функциональных элементов (СФЭ). Первые подходы к анализу статического энергопотребления для СФЭ были предложены в работе [1], а основные теоретические результаты в этом направлении были получены О. М. Касим-Заде в работах [2,3]. В указанных работах был введен и исследован функционал мощности СФЭ, характеризующий статическое энергопотребление, для которого был установлен порядок роста соответствующей

функции Шеннона в произвольном конечном полном базисе. Оказалось, в частности, что существуют базисы как с линейным, так и с экспоненциальным поведением указанной функции Шеннона. Кроме того, была показана возможность построения для “типичной” функции алгебры логики (ФАЛ) такой реализующей ее СФЭ, сложность которой асимптотически оптимальна, а мощность оптимальна по порядку роста. В свою очередь, для теоретической оценки динамического энергопотребления схем в работе [4] был введен функционал динамической (переключательной) активности для СФЭ. При этом, было доказано, что в произвольном базисе порядок роста функции Шеннона для динамической активности СФЭ не превосходит некоторую линейную функцию, и были предложены методы синтеза, позволяющие для произвольной ФАЛ построить СФЭ в стандартном базисе, сложность которой асимптотически оптимальна, а мощность и динамическая активность оптимальны по порядку роста.

Стоит отметить, что наравне с теоретическими исследованиями разрабатываются различных практические подходы к оценке динамического энергопотребления для конкретных схем. Первые эффективные алгоритмы расчета и оценки динамического энергопотребления конкретных схем были представлены в работе [5]. Обзор основных результатов в этом направлении можно найти в работе [6].

В данной работе введен функционал динамической активности для модели ориентированных контактных схем (ОКС), и установлено точное значение функции Шеннона для динамической активности ОКС. Доказано, что для произвольной ФАЛ от n переменных можно построить такую реализующую ее СФЭ в стандартном базисе, сложность которой асимптотически не больше, чем $\frac{2^n}{n}$, а ее динамическая активность не превосходит значение соответствующей функции Шеннона с точностью до мультипликативной константы.

Основные определения

Пусть $\Sigma = \Sigma(x_1, \dots, x_n; a', a'')$ — произвольная (1,1)-ОКС от булевых переменных (БП) $\tilde{x} = (x_1, \dots, x_n)$, имеющая вход a' и выход a'' . Пусть $V(\Sigma)$ — множество вершин ОКС Σ , отличных от a' и a'' . Тогда для каждой вершины v , $v \in V$, ОКС Σ определим функцию достижимости $g_v(\tilde{x})$ от входа a' до вершины v , которая равна 1 на наборе $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n) \in B^n$, где B^n — единичный n -мерный куб, тогда и только тогда, когда в Σ существует ориентированный путь из вершины a' в вершину v , состоящий из проводящих контактов. Динамической активностью ОКС Σ на паре наборов $\tilde{\alpha}$ и $\tilde{\beta}$ будем называть следующую величину:

$$S(\Sigma, \tilde{\alpha}, \tilde{\beta}) = \sum_{v \in V(\Sigma)} g_v(\tilde{\alpha}) \oplus g_v(\tilde{\beta})$$

Данная величина характеризует число внутренних вершин ОКС Σ достижимость от входа a' до которых изменилась при смене значений, подаваемых на контакты схемы, с набора значений $\tilde{\alpha}$ на набор значений $\tilde{\beta}$. В свою очередь, *динамической активностью* $S(\Sigma)$ ОКС Σ назовем максимальное значение величины $S(\Sigma, \tilde{\alpha}, \tilde{\beta})$ взятое по всем парам наборов $(\tilde{\alpha}, \tilde{\beta})$ из $B^n \times B^n$.

Для произвольной ФАЛ f *динамической активностью* $S^{OKC}(f)$ этой ФАЛ в классе ОКС будем называть минимальную динамическую активность (1,1)-ОКС, реализующих ФАЛ f . Пусть $P_2(n)$ — множество всех ФАЛ от n переменных $x_1, x_2, \dots, x_n$. Функцией Шеннона $S^{OKC}(n)$ для динамической активности ОКС будем, как обычно, называть максимальное значение динамической активности $S^{OKC}(f)$ среди всех ФАЛ $f, f \in P_2(n)$.

Основные результаты

Основными результатами данной работы являются следующие две теоремы.

Теорема 1.

Для функции Шеннона $S^{OKC}(n)$ для динамической активности ОКС выполнено следующее равенство:

$$S^{OKC}(n) = 2(n - 1).$$

Теорема 2. *Существует неотрицательная и стремящаяся к нулю последовательность действительных чисел $\epsilon(1), \epsilon(2), \dots$ такая, что для любого $n, n = 1, 2, \dots$, любая ФАЛ $f, f \in P_2(n)$, может быть реализована некоторой (1,1)-ОКС Σ_f , удовлетворяющей неравенствам*

$$L(\Sigma_f) \leq (1 + \epsilon(n)) \frac{2^n}{n}, \quad S^{OKC}(\Sigma_f) \leq (1 + \epsilon(n)) cn,$$

где c — некоторая положительная константа.

Работа выполнена при поддержке РФФИ (проект № 15-01-07474-а).

СПИСОК ЛИТЕРАТУРЫ

- [1] Вайнцвайг М. Н. О мощности схем из функциональных элементов // Докл. АН СССР. — 1961. — Т. 139, № 2. — С. 320–323.
- [2] Касим-Заде О. М. Об одновременной минимизации сложности и мощности схем из функциональных элементов // Проблемы кибернетики. — М.: Наука, 1978. — Вып. 33. — С. 215–220.
- [3] Касим-Заде О. М. Об одной мере сложности схем из функциональных элементов // Проблемы кибернетики. — М.: Наука, 1981. — Вып. 38. — С. 117–179.
- [4] Ложкин С. А., Шуплецов М. С. О динамической активности схем из функциональных элементов и построении асимптотически оптимальных по сложности схем с линейной динамической активностью // Ученые записки Казанского университета. Серия физико-математические науки, 2014. — Т. 156, кн. 3. — С. 84–97.

- [5] Devadas S., Keutzer K., White J. Estimation of power dissipation in CMOS combinational circuits // Proc. Custom Integrated Circuits Conf. — 1990. — P. 19.7.1–19.7.6.
- [6] Najm F. A survey of power estimation techniques in VLSI circuits (Invited paper) // IEEE Trans VLSI Syst. — 1994. — V. 2, No. 4. — P. 446–455.

ПОСТРОЕНИЕ СМЕШАННЫХ АЛГОРИТМОВ НА БАЗЕ ОДНОГО BUNDLE МЕТОДА

Яруллин Рашид Саматович

Казанский (Приволжский) федеральный университет, e-mail: YarullinRS@gmail.com

В настоящий момент разработано достаточно много различных методов решения задач нелинейного программирования. Каждый из этих методов оптимизации обладает своими недостатками и достоинствами. В связи с этим при решении практических задач с целью ускорения сходимости процесса оптимизации данные методы используются комплексно. А именно, на каждом шаге выбирается такой метод, который при отыскании следующего приближения наиболее эффективен среди всех остальных методов. Алгоритм, который в результате образуется на основе применения различных методов оптимизации, называется смешанным (см., напр., [1–2]). В данной работе предлагается смешанный алгоритм на базе одного bundle метода, в котором предусмотрена возможность периодического отбрасывания отсекающих плоскостей.

Пусть $f(x)$ — выпуклая в n -мерном евклидовом пространстве R_n функция, $\partial f(y)$, $\partial_\eta f(y)$ — субдифференциал и η -субдифференциал функции $f(x)$ в точке $y \in R_n$ соответственно, субградиент функции $f(x)$ удовлетворяет условию Липшица с константой $L > 0$, т. е. для любого $s(x) \in \partial f(x)$, где $x \in R_n$, выполняется

$$\|s(x)\| \leq L.$$

Предполагается, что функция $f(x)$ достигает своего минимального значения в R_n .

Положим $f^* = \min\{f(x) : x \in R_n\}$, $X^* = \{x \in R_n : f(x) = f^*\}$, $X^*(\varepsilon) = \{x \in R_n : f(x) \leq f^* + \varepsilon\}$, где $\varepsilon > 0$, $T = \{0, 1, \dots\}$.

Требуется за конечное число итераций найти точку из множества $X^*(\varepsilon)$.

Опишем сначала вспомогательную процедуру со следующими входными параметрами:

$$\hat{x} \in R_n, \quad \hat{\delta} > 0, \quad \hat{\mu} > 0, \quad \hat{\theta} \in (0, 1), \quad t \in T. \quad (1)$$

$$\pi = Procedure(\hat{x}, \hat{\delta}, \hat{\mu}, \hat{\theta}, t).$$

0. Инициализация стартовых параметров $k = 1$, $x_k = \hat{x}$.

1. Полагается $i = 1$, $x_{k,i} = x_k$,

$$\hat{f}_{k,i}(y) = f(x_{k,i}) + \langle s_{k,i}, y - x_{k,i} \rangle, \quad (2)$$

где $s_{k,i} \in \partial f(x_{k,i})$.

2. Находится точка

$$x_{k,i+1} = \operatorname{argmin}\{\hat{f}_{k,i}(y) + \frac{\hat{\mu}}{2}\|y - x_k\|^2 : y \in R_n\}, \quad (3)$$

вычисляется $\delta_{k,i} = f(x_k) - [\hat{f}_{k,i}(x_{k,i+1}) + \frac{\hat{\mu}}{2}\|x_{k,i+1} - x_k\|^2]$.

3. Если $\delta_{k,i}^2 \leq \hat{\delta}$, то полагается $i(t) = i$, $k(t) = k$, и итерационный процесс прекращается, результатом работы процедуры является точка x_k .

4. Если

$$f(x_{k,i+1}) \leq f(x_k) - \hat{\theta}\delta_{k,i}, \quad (4)$$

то выбирается точка $x_{k+1} \in R_n$ такая, что $f(x_{k+1}) \leq f(x_{k,i+1})$, значение k увеличивается на единицу, и следует переход к п. 1.

5. Выбирается $s_{k,i+1} \in \partial f(x_{k,i+1})$, полагается

$$\hat{f}_{k,i+1}(y) = \max\{\hat{f}_{k,i}(y), f(x_{k,i+1}) + \langle s_{k,i+1}, y - x_{k,i+1} \rangle\}, \quad (5)$$

значение i увеличивается на единицу, и следует переход к п. 2.

Приведем некоторые свойства, касающиеся предложенной процедуры π .

Согласно (1), (5) при $k \geq 1$, $i \geq 1$ выполняется $\hat{f}_{k,i}(y) = \max_{1 \leq j \leq i} \{f(x_{k,j}) + \langle s_{k,j}, y - x_{k,j} \rangle\}$. Функция $\hat{f}_{k,i}(y)$ называется моделью выпуклой функции $f(x)$. Поскольку модель $\hat{f}_{k,i}(y)$ состоит из линейных функций, то функция $\hat{f}_{k,i}(y)$ является выпуклой.

Приведем без доказательства следующий известный результат (см., напр., [3, с. 144]).

Теорема 1. Пусть параметр $\hat{\mu}$ процедуры π задан согласно условию (1) и определенным образом построены точки x_k и $x_{k,i+1}$, $k \geq 1$, $i \geq 1$, из (3), а вектор $\hat{\alpha}_{k,i} = (\hat{\alpha}_1, \dots, \hat{\alpha}_i) \in R_i$ является решением следующей задачи:

$$\min_{\alpha=(\alpha_1, \dots, \alpha_i)} \left\{ \frac{1}{2\hat{\mu}} \left\| \sum_{j=1}^i \alpha_j s_{k,j} \right\|^2 + \sum_{j=1}^i \alpha_j e_{k,j} : \alpha = (\alpha_1, \dots, \alpha_i) \geq 0, \sum_{j=1}^i \alpha_j = 1 \right\},$$

и, кроме того, $\hat{s}_{k,i} = \sum_{j=1}^i \hat{\alpha}_{k,i}[j] s_{k,j}$, $\hat{e}_{k,i} = \sum_{j=1}^i \hat{\alpha}_{k,i}[j] e_{k,j}$. Тогда выполняются следующие утверждения:

$$x_{k,i+1} = x_k - \frac{1}{\hat{\mu}} \hat{s}_{k,i}, \quad \delta_{k,i} = \hat{e}_{k,i} + \frac{1}{2\hat{\mu}} \|\hat{s}_{k,i}\|^2, \quad \hat{s}_{k,i} \in \partial_{\hat{e}_{k,i}} f(x_k).$$

На основе вспомогательной процедуры π построим метод отыскания точки из множества $X^*(\varepsilon)$, где $\varepsilon > 0$, который заключается в следующем.

0. Задается $z_0 \in R_n$, $\mu_0 > 0$, $\delta_0 > 0$, $t = 0$, $\theta \in (0, 1)$.

1. Находится $z_{t+1} = \pi(z_t, \delta_t, \mu_t, \theta, t)$.

2. Задается $\mu_{t+1} \geq \mu_t$, $\delta_{t+1} \leq \delta_t$.

3. Полагается $t = t + 1$, и следует переход к п. 1.

В п. 4, предлагаемой процедуры π , заложена возможность периодического отбрасывания всех отсекающих плоскостей, которая заключается в следующем. В окрестности точек $x_{k,i+1}$ на каждом шаге процедуры π оценивается качество аппроксимации надграфика целевой функции моделью $\hat{f}_{k,i}(x)$. Если при некотором i выполняется неравенство (4), то качество аппроксимации считается достаточно хорошим, и происходит полное обновление модели выпуклой функции за счет отбрасывания отсекающих плоскостей. В противном случае уточняется модель выпуклой функции и отсечения не отбрасываются.

Отметим, что в п. 4 процедуры π при отбрасывании секущих плоскостей задаются основные итерационные точки. В процессе построения этих точек могут использоваться любые релаксационные методы минимизации. Важно отметить, что сходимость всех таких смешанных алгоритмов будет гарантирована сходимостью предложенного bundle метода, причем даже в том случае, когда упомянутые релаксационные методы, включенные в смешанные алгоритмы, являются эвристическими.

Теорема 2. Пусть предложенным методом построена последовательность $\{z_t\}$, $t \in T$, и заданы числа $\varepsilon > 0$, μ_t , δ_t , $t \in T$, такие, что $\delta_t \rightarrow 0$, $\mu_t \rightarrow \infty$, $t \in T$. Тогда найдется номер $t' \in T$, для которого выполнится включение $z_{t'} \in X^*(\varepsilon)$.

Работа выполнена при поддержке РФФИ (проект № 16-31-60014).

СПИСОК ЛИТЕРАТУРЫ

- [1] Заботин И. Я., Яруллин Р. С. Метод отсечений с обновлением аппроксимирующих множеств и его комбинирование с другими алгоритмами // Изв. Иркутского гос. ун-та. Сер. Математика. — 2014. — Т 10. — С. 13–26.
- [2] Зангвилл У. И. Нелинейное программирование. — М. : Сов. радио, 1973. — 312 с.
- [3] Bonnans J., Gilbert J., Lemarechal C., Sagastizabal C. Numerical Optimization: Theoretical and Practical Aspects. — Berlin : Springer-Verlag, 2003. — 490 p.

О ПРЕОБРАЗОВАНИЯХ ДИСКРЕТНЫХ СЛУЧАЙНЫХ ВЕЛИЧИН МНОГОЧЛЕНАМИ

Яшунский Алексей Дмитриевич

ИПМ им. М. В. Келдыша РАН, e-mail: yashunsky@keldysh.ru

Пусть $E_k = \{0, 1, \dots, k-1\}$ и B — некоторое множество функций на E_k , тогда $\langle E_k, B \rangle$ — алгебра, см. [1]. Рассмотрим случайные величины со значениями в множестве E_k . Распределение $\mathbf{p} = (p_0, \dots, p_{k-1})$ такой случайной величины — вектор, лежащий в $(k-1)$ -мерном симплексе, заданном соотношениями $\sum p_i = 1$, $p_i \geq 0$, $i = 0, \dots, k-1$. Соответствующий симплекс будем

далее обозначать $T^{(k)}$. Носителем распределения $\mathbf{p}$ будем называть множество $N(\mathbf{p}) = \{i \in E_k \mid p_i > 0\}$.

Если $f(x_1, \dots, x_n) \in B$ и $X_1, \dots, X_n$ — независимые в совокупности случайные величины, имеющие распределения $\mathbf{p}^{(1)}, \dots, \mathbf{p}^{(n)}$ соответственно, то $f(X_1, \dots, X_n)$ есть случайная величина X с распределением $\mathbf{p}$, для компонент которого выполнены равенства:

$$p_i = \sum_{\substack{\sigma_1, \dots, \sigma_n: \\ f(\sigma_1, \dots, \sigma_n) = i}} p_{\sigma_1}^{(1)} \cdots p_{\sigma_n}^{(n)}.$$

Таким образом, каждая n -арная функция $f \in B$ индуцирует полилинейное отображение $\hat{f} : (T^{(k)})^n \rightarrow T^{(k)}$. Обозначим $\hat{B} = \{\hat{f} \mid f \in B\}$. Тогда $\langle T^{(k)}, \hat{B} \rangle$ есть алгебра вероятностных распределений, индуцированная алгеброй $\langle E_k, B \rangle$.

Пусть $G \subset T^{(k)}$ и пусть $W_B(G)$ — наименьшее по включению топологически замкнутое (относительно топологии, заданной стандартной евклидовой метрикой) множество, содержащее G и замкнутое относительно всех операций $\hat{f}, f \in B$. Тогда $\langle W_B(G), \hat{B} \rangle$ — подалгебра алгебры $\langle T^{(k)}, \hat{B} \rangle$, которую будем называть алгеброй аппроксимируемых распределений, порожденной начальным множеством G и операциями B . В случае, когда множество G состоит из единственного распределения $\mathbf{p}$, вместо $W_B(\{\mathbf{p}\})$ будем писать $W_B(\mathbf{p})$.

В данной работе изучаются свойства множества $W_B(\mathbf{p})$ в случае, когда B — множество всех многочленов $(\text{mod } k)$ над E_k .

Будем далее обозначать через $+$ и $\times$ сложение и умножение $\text{mod } k$, а через $\oplus$ и $\otimes$ — индуцированные ими операции в $T^{(k)}$.

Теорема 1. Пусть $G = \{\mathbf{p} \mid N(\mathbf{p}) = \{0, 1\}\}$ и $B = \{+, \times, 0, 1, \dots, k-1\}$. Тогда $W_B(G) = T^{(k)}$.

Доказательство. Для всех распределений $\mathbf{p} \in T^{(k)}$ покажем индукцией по $|N(\mathbf{p})|$, что $\mathbf{p} \in W_B(G)$. При $|N(\mathbf{p})| = 1$ это следует из $0, 1, \dots, k-1 \in B$.

Пусть задано $\mathbf{p}$, $|N(\mathbf{p})| > 1$, и для любого $\mathbf{q}$, $|N(\mathbf{q})| < |N(\mathbf{p})|$, выполнено $\mathbf{q} \in W_B(G)$. Положим $i = \min N(\mathbf{p})$, $A = \{j \mid j + i \in N(\mathbf{p}), j \neq 0\}$. Тогда $|A| = |N(\mathbf{p})| - 1$, и для любого $\mathbf{q}$ с $N(\mathbf{q}) = A$ имеет место $\mathbf{q} \in W_B(G)$.

Заметим, что $W_B(G) \supseteq \{s \otimes t \mid s \in G, N(t) = A\} = \{r \mid N(r) = A \cup \{0\}\}$. Пусть $\mathbf{i}$ таково, что $N(\mathbf{i}) = \{i\}$, тогда $W_B(G) \supseteq \{\mathbf{i} \oplus r \mid N(r) = A \cup \{0\}\} \ni \mathbf{p}$, что завершает шаг индукции. **Теорема 1 доказана.**

Теорема 2. Пусть $k = p^m$, где p — простое число, B — множество всех многочленов над E_k , и $\mathbf{q}$ таково, что $|N(\mathbf{q})| > 1$. Тогда $W_B(\mathbf{q}) = T^{(k)}$.

Доказательство. Если k — простое число, то утверждение теоремы вытекает из результатов работы [2]. Пусть далее $k = p^m$, $m > 1$.

Пусть $A = \{p \times t \mid t \in E_k\}$. Тогда для любого $a \in A$ при $n \geq m$ выполнено $a^n = 0$. Вместе с тем, множество $E_k \setminus A$ образует конечную группу относительно умножения $\times$, поэтому существует такая степень n_0 , что для любого $b \in E_k \setminus A$

выполнено $b^{n_0} = 1$. Отсюда вытекает, что найдется многочлен $f(x) = x^N \in B$, принимающий значения 0 на множестве A и значение 1 вне его.

Существует естественный гомоморфизм $\varphi : E_{p^m} \rightarrow E_p$, сохраняющий операции $+$ и $\times$. Отметим, что $\varphi(A) = 0 \in E_p$. Определим $\varphi(\mathbf{q})$ как вектор из $T^{(p)}$, j -я компонента которого равна $\sum_{\varphi(i)=j} q_i$. Отметим, что $W_B(\varphi(\mathbf{q})) = T^{(p)}$. Из свойств гомоморфизмов (см. [3]) при этом вытекает, что для любого $\eta \in [0, 1]$ найдется такое распределение $\mathbf{t} \in W_B(\mathbf{q})$, что $\sum_{i \in A} t_i = \eta$. Тогда $\hat{f}(\mathbf{t}) = (\eta, 1 - \eta, 0, \dots, 0) \in W_B(\mathbf{q})$, откуда, в силу произвольности η получаем, что $\{s \mid N(s) = \{0, 1\}\} \subseteq W_B(\mathbf{q})$. Применяя далее теорему 1, получаем доказываемое утверждение. **Теорема 2 доказана.**

В отличие от степеней простых чисел, при прочих значениях k , вообще говоря, невозможно аппроксимировать над E_k произвольное распределение, подставляя в многочлены независимые одинаково распределенные невырожденные случайные величины. Это показывает

Теорема 3. Пусть $k = p_1 p_2$, где p_1, p_2 — простые числа, B — множество всех многочленов над E_k , и пусть

$$K = \{\mathbf{r} \oplus \mathbf{s} \mid N(\mathbf{r}) = \{p_1 \times t \mid t \in E_k\}, N(\mathbf{s}) = \{p_2 \times t \mid t \in E_k\}\}.$$

Тогда $W_B(K) = K$.

Доказательство. Отметим, что K топологически замкнуто, поэтому достаточно показать его замкнутость относительно преобразований распределений, индуцированных многочленами из множества B .

Пусть $Z_1, \dots, Z_n$ — независимые случайные величины с распределениями из множества K . Тогда каждая величина Z_i представляется в виде суммы $Z_i = X_i + Y_i$, где X_i и Y_i — независимые случайные величины с распределениями $\mathbf{r}^{(i)}$, $\mathbf{s}^{(i)}$. При этом имеет место $N(\mathbf{r}^{(i)}) = \{p_1 \times t \mid t \in E_k\}$ и $N(\mathbf{s}^{(i)}) = \{p_2 \times t \mid t \in E_k\}$.

Заметим, что для любых i, j выполнено $X_i \times Y_j = 0$. Пусть теперь $f(x_1, \dots, x_n) \in B$ — некоторый многочлен:

$$f(x_1, \dots, x_n) = \sum_{\sigma=(\sigma_1, \dots, \sigma_n)} \alpha_\sigma x_1^{\sigma_1} \cdots x_n^{\sigma_n}.$$

Тогда $f(Z_1, \dots, Z_n) = \sum_\sigma \alpha_\sigma (X_1 + Y_1)^{\sigma_1} \cdots (X_n + Y_n)^{\sigma_n}$, что, в силу ортогональности X_i и Y_j при всех i, j , преобразуется к виду

$$\sum_\sigma \alpha_\sigma X_1^{\sigma_1} \cdots X_n^{\sigma_n} + \sum_\sigma \alpha_\sigma Y_1^{\sigma_1} \cdots Y_n^{\sigma_n} = f(X_1, \dots, X_n) + f(Y_1, \dots, Y_n).$$

Поскольку множества $\{p_1 \times t \mid t \in E_k\}$ и $\{p_2 \times t \mid t \in E_k\}$ замкнуты относительно преобразований многочленами, получаем, что распределение случайной величины $f(Z_1, \dots, Z_n)$ лежит в множестве K . **Теорема 3 доказана.**

Отметим, что $K \neq T^{(k)}$, таким образом построен пример множества, любое подмножество которого заведомо не позволяет аппроксимировать произвольное распределение.

Автор выражает глубокую признательность О. М. Касим-Заде за внимание к работе.

Работа выполнена при поддержке Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

СПИСОК ЛИТЕРАТУРЫ

- [1] Мальцев А. И. Алгебраические системы. — М.: Наука, 1970.
- [2] Яшунский А. Д. Приближения вероятностных распределений функциями k -значной логики // Препринты ИПМ им. М. В. Келдыша. — 2016. — № 58. — 7 с. — doi:10.20948/prepr-2016-58
- [3] Яшунский А. Д. Конечные системы операций для аппроксимации дискретных вероятностных распределений // Препринты ИПМ им. М. В. Келдыша. — 2017. — № 10. — 7 с. — doi:10.20948/prepr-2017-10

Авторский указатель

S. Lawrencenko, 11

K. Prusis, 250

J. Vihrovs, 250

A. Yakaryilmaz, 250

М. Ф. Аблаев, 13, 16

Ф. М. Аблаев, 13, 16

М. Б. Абросимов, 18, 21

В. Б. Алексеев, 24

М. А. Алехина, 26

А. А. Андрианова, 29

Н. Г. Анищенко, 32

Д. Н. Бабин, 34

А. М. Бабич, 37

М. Ю. Бабич, 39

Г. А. Банару, 42

М. Б. Банару, 42

И. В. Барков, 44

О. Ю. Барсукова, 47

И. Б. Болотин, 32

Л. Н. Бондаренко, 49

А. В. Бухман, 52

А. В. Васильев, 13

С. И. Веселов, 76

В. А. Воблый, 55, 56

А. А. Вороненко, 58, 60

Л. И. Высоцкий, 62

А. Ф. Гайнутдинова, 65

А. Гнатенко, 68

Д. Е. Горбатенко, 71

М. М. Гордеев, 225

С. М. Грабовская, 74

Д. В. Грибанов, 76

Ю. С. Гусынина, 103

Б. Р. Данилов, 145

Е. Л. Довгалюк, 147

О. С. Дудакова, 78

А. А. Евдокимов, 81

Ш. Р. Жайлауова, 84

Л. П. Жильцова, 87

В. В. Жуков, 90

И. Я. Заботин, 92, 95

В. А. Захаров, 68, 84

М. Т. Зиятдинов, 13, 98

А. В. Зорин, 100, 135

А. Ф. Зубков, 103

Р. Н. Ибрагимов, 250

А. В. Ильев, 105

М. А. Иорданский, 108

К. Е. Казаева, 92

А. С. Казимиров, 110

А. Ю. Киндаев, 168

Д. И. Коган, 112, 115, 117

И. Б. Кожухов, 120

И. В. Козин, 122

Р. М. Колпаков, 123

А. В. Колчин, 126

Ю. А. Комбаров, 129

А. В. Корольков, 16

А. Г. Коротченко, 132

С. В. Костин, 18

В. М. Кочеганов, 135

- С. Е. Кочемазов, 71
А. В. Кочергин, 137
В. В. Кочергин, 139, 142
Д. В. Кочергин, 139

С. А. Ложкин, 145, 147
И. Г. Любич, 150

А. М. Магомедов, 152
Т. А. Магомедов, 152
Е. С. Малахова, 60
Е. Е. Маренич, 154
А. И. Мартышкин, 157
А. К. Мелешко, 56
Д. Г. Мещанинов, 161
А. С. Митрошина, 112
В. Ю. Михайлов, 163
А. В. Михайлович, 142, 166
О. В. Моденова, 21
А. В. Моисеев, 168, 244
Д. Б. Мокеев, 171
А. Э. Молчанов, 174
В. А. Молчанов, 177
Р. Г. Мубаракзянов, 179
Т. М. Мухтарова, 29

Т. Р. Нагматуллин, 247
А. С. Нагорный, 182

А. М. Останин, 184

А. Ф. Павлова, 145
В. И. Пантелеев, 187
Н. А. Перязев, 189
В. И. Петренюк, 191
А. О. Петриков, 120
П. Г. Пичугина, 47
В. В. Подымов, 174
С. И. Полюга, 122
К. А. Попков, 194
В. Б. Поплавский, 197
М. А. Посыпкин, 123
Е. В. Пройдакова, 200

А. С. Пудов, 112

М. А. Рачинская, 203
Н. П. Редькин, 205
М. Б. Резников, 209
С. Ю. Реймеров, 110
А. В. Решетников, 212
Д. С. Романов, 150, 213, 216

О. А. Садовников, 147
В. Г. Саргсян, 220
С. Н. Селезнева, 223, 225
А. А. Семенов, 71
И. С. Сергеев, 227
А. А. Сёмов, 244
С. В. Сидоров, 229
Т. Г. Смирнова, 87
В. М. Сморякова, 132
Д. В. Сперанский, 232
Л. Н. Сысоева, 235

Е. Б. Титова, 237
М. А. Трухина, 239
Л. Б. Тяпаев, 242

К. С. Ульянов, 115

В. Р. Фазылов, 29
Ю. С. Федосенко, 112, 115, 117, 209
М. А. Федоткин, 203
Н. Г. Федотов, 244
В. Б. Фофанов, 247

К. Р. Хадиев, 250, 253
А. И. Хадиева, 253
Д. К. Хандурин, 117
Е. В. Хворостухина, 177

А. Ю. Чирков, 76
И. П. Чухров, 256

С. В. Шалагин, 259
И. К. Шаранхаев, 189
М. Л. Шарапова, 49
В. Н. Шевченко, 237

Т. А. Шорникова, 261

О. Н. Шульгина, 95

М. С. Шуплецов, 145, 263

Р. С. Ярулин, 95, 266

А. Д. Яшунский, 268