Секция «Комбинаторный анализ»

ОБОБЩЕННЫЕ МНОГОЧЛЕНЫ МОЦКИНА И ИХ СВОЙСТВА

Л. Н. Бондаренко (Пенза), М. Л. Шарапова (Москва)

В [1] рассматриваются гибридные многочлены Эрмита—Лагерра

$$P_n^{(\alpha)}(x,t) = \sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{x^k t^{n-2k}}{(n-2k)!k!\Gamma(k+\alpha+1)}, \qquad (1)$$

где $[\cdot]$ — целая часть числа, $\Gamma(z)$ — гамма-функция. Их производящая функция $\sum_{n=0}^{\infty} P_n^{(\alpha)}(x,t)\, u^n/n! = (xu^2)^{-\alpha/2} e^{tu} I_\alpha(2u\sqrt{x})$, где $I_\alpha(z)$ — модифицированная функция Бесселя первого рода порядка α.

На базе многочленов (1) в [1] введены s-ассоциированные центральные триномиальные коэффициенты $C_n^{(s)} = P_n^{(s)}(1,1), s = 0,1,\ldots$, удовлетворяющие соотношению $2(n+1)C_n^{(s+1)} = C_{n+2}^{(s)} - C_{n+1}^{(s)}$, а числа $M_n = C_n^{(1)}$ являются известными числами Моцкина [2, 3]. Несмотря на привлекательность этого подхода, для обобщения чисел Моцкина лучше подходит другой путь, базирующийся на следующем понятии.

Определение 1. Многочлены Моцкина $L_n^{(r)}$ порядка $r = 1, 2, \ldots$ зададим выражением

$$L_n^{(r)}(t) = \frac{1}{rn+1} \sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{rn+1}{n-2k} \binom{(r-1)n+2k+1}{k} t^{n-2k}. \qquad (2)$$

Это определение мотивировано тем, что $M_n = L_n^{(1)}(1)$, а числа $M_n^{(2)} = L_n^{(2)}(1)$ [4] являются обобщением чисел Моцкина. Поэтому $M_n^{(r)} = L_n^{(r)}(1)$ назовем числами Моцкина порядка r.

Теорема 1. *Для многочленов $L_n^{(r)}(t)$ справедливо соотношение*

$$L_n^{(r)}(t) = \frac{1}{2^n n!} D_v^{n-1} \left((\sqrt{4v+t^2}+t)^n (v+1)^{rn} \right)\Big|_{v=0}, \; D_v = \frac{\partial}{\partial v}. \quad (3)$$

Доказательство. Применение к равенству (3) формул бинома Ньютона и Лейбница для $(n-1)$-й производной от произведения функций позволяет получить выражение

$$L_n^{(r)}(t) = \frac{(rn)!}{2^n n!} \sum_{k=0}^{n-1} \binom{n-1}{k} \frac{t^{n-2k}}{((r-1)n+k+1)!} 2^k \sum_{i=0}^{n} \binom{n}{i} \prod_{j=0}^{k-1} (i-2j),$$

внутренняя сумма в котором при $k = 0, 1, \ldots, n-1$ равна

$$\sum_{i=0}^{n} \binom{n}{i} \prod_{j=0}^{k-1} (i-2j) = 2^k D_z^k \, (1+\sqrt{z})^n \big|_{z=1} = \frac{2^{n-k} n (n-k+1)!}{(n-2k)!}$$

и обращается в нуль при $k > [n/2]$, что доказывается с помощью гипергеометрических функций и приводит к выражению (2).

Теорема 2. *Производящей функции* $v = F_r(t,u) = \sum_{n=1}^{\infty} L_n^{(r)}(t) u^n$, *описывающей многочлены Моцкина порядка* r, *отвечает обратная функция* $u = F_r^{-1}(t,v) = 2v(\sqrt{4v+t^2}+t)^{-1}(v+1)^{-r}$, *и справедливо рекуррентное соотношение*

$$L_0^{(r)}(t) = 1, \; L_{n+1}^{(r)}(t) = t \left\langle L_n^{(r)}(t) \right\rangle^r + \left\langle L_{n-1}^{(r)}(t) \right\rangle^{2r}, \; n \geq 0, \qquad (4)$$

где $\langle Q_n(t) \rangle^m = \sum_{k_1+\ldots+k_m=n,\, k_i \geq 0} Q_{k_1}(t) \ldots Q_{k_m}(t)$ — *свертка кратности* m *последовательности многочленов* $\{Q_k(t)\}_0^n$ k*-й степени.*

Доказательство. Первое утверждение теоремы 2 вытекает из формулы (3) и теоремы Лагранжа [3]. Применение производящей функции $v = F_r(t,u)$, увеличенной на 1, к выражению для функции $u = F_r^{-1}(t,v)$ дает алгебраическое уравнение для вычисления производящей функции $u^2(v+1)^{2r} + tu(v+1)^r - (v+1) + 1 = 0$. Так как коэффициент при u^n степенного ряда $(v+1)^r$ равен r-кратной свертке $\langle L_n^{(r)}(t) \rangle^r$, то сравнение коэффициентов в этом уравнении при степенях u приводит к рекуррентной формуле (4). Отметим, что при $r = 1$, $t = 1$ записанное уравнение и соотношение (4) соответствуют известным формулам для чисел Моцкина [2].

В [5] изучались перестановки Гесселя—Стенли (ГС-перестановки) порядка r, т. е. перестановки $\sigma = \sigma_1 \ldots \sigma_{rn}$, $r = 1, 2, \ldots$ мультимножества $\{1^r, \ldots, n^r\}$, у которых все буквы, стоящие между любыми двумя вхождениями символа $i \in \{1, \ldots, n\}$ не меньше этого i.

Подслово ГС-перестановки σ порядка r с совпадающими окаймляющими символами, в котором каждый символ повторяется ровно r раз, назовем ГС-подсловом (при $r = 1$ все символы σ являются ГС-подсловами), причем σ имеет n ГС-подслов. Например, перестановка 123332244411 имеет ГС-подслова: $123332244411, 233322, 333, 444$.

Для двух смежных ГС-подслов η_1, η_2 ГС-перестановки порядка r естественно вводится отношение порядка: $\eta_1 < \eta_2$, если окаймляющий символ η_1 меньше окаймляющего символа η_2.

Определение 2. ГС-перестановку σ порядка r будем называть М-перестановкой порядка r, если она обладает свойствами: 1) σ является 312-избегающей ГС-перестановкой порядка r, т. е. не существует тройки индексов $i < j < k$, для которых выполняется неравенство $\sigma_j < \sigma_k < \sigma_i$; 2) в σ отсутствуют три смежных возрастающих ГС-подслова, т. е. нет смежных ГС-подслов η_1, η_2, η_3, для которых $\eta_1 < \eta_2 < \eta_3$.

Отметим, что 312-избегающие обычные перестановки были введены Д. Кнутом, а их свойства описаны, например, в [3].

Пусть $\mathcal{M}_n^{(r)}$ — множество всех М-перестановок порядка r над алфавитом $\{1, \ldots, n\}$. Для каждого слова $\sigma \in \mathcal{M}_n^{(r)}$ определим число подъемов $0 \le \mathrm{rim}(\sigma) \le [n/2]$ всех смежных ГС-подслов выражением $\mathrm{rim}(\sigma) = \#\{i : \eta_i < \eta_j,\ \eta_i, \eta_j - \text{смежные подслова},\ \sigma \in \mathcal{M}_n^{(r)}\}$. Например, для $\sigma = 123344432211 \in \mathcal{M}_4^{(3)}$ имеем $\mathrm{rim}(\sigma) = 0$, а для $\sigma = 111233344422 \in \mathcal{M}_4^{(3)}$ — $\mathrm{rim}(\sigma) = 2$.

Теорема 3. $L_n^{(r)}(t) = \sum_{\sigma \in \mathcal{M}_n^{(r)}} t^{n-2\mathrm{rim}(\sigma)}$, $M_n^{(r)} = L_n^{(r)}(1) = |\mathcal{M}_n^{(r)}|$, *коэффициент при* t^{n-2k} *в* $L_n^{(r)}(t)$ *равен* $\#\{\sigma \in \mathcal{M}_n^{(r)} : \mathrm{rim}(\sigma) = k\}$.

Теорема 3 дает комбинаторную интерпретацию обобщенных чисел Моцкина и коэффициентов многочлена $L_n^{(r)}(t)$.

Работа выполнена при финансовой поддержке первого автора грантом РФФИ (проект 14-01-00273).

Список литературы

1. Blasiak P., Dattoli G., Horzela A., Penson K. A., Zhukovsky K. Motzkin numbers, central trinomial coefficients and hybrid polynomials // Jornal of Integer Sequenses. — 2008. — 11. — Art. 08.1.1. — P. 11.

2. Sloane N. J. A. The on-line encyclopedia of integer sequences. — `http://oeis.org/A001006` — 2015.

3. Стенли Р. Перечислительная комбинаторика. Т. 2. — М.: Мир, 2009.

4. Sloane N. J. A. The on-line encyclopedia of integer sequences. — http://oeis.org/A006605 — 2015.

5. Бондаренко Л. Н., Шарапова М. Л. Параметрические комбинаторные задачи и методы их исследования // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2010. — № 4. — С. 50–63.

ЗАДАЧА ПОИСКА ШИРИНЫ СИМПЛЕКСА, ЗАДАННОГО СИСТЕМОЙ С ОГРАНИЧЕННЫМ СПЕКТРОМ МИНОРОВ

Д. В. Грибанов (Нижний Новгород)

В данной работе рассматривается сложность задачи поиска ширины симплекса заданного целочисленной системой линейных неравенств. Пусть $A \in \mathbb{Z}^{m\times n}$ и $b \in \mathbb{Z}^n$, как $P(A,b)$ обозначим полиэдр заданный системой неравенств $Ax \leq b$, другими словами $P(A,b) = \{x \in \mathbb{R}^n : Ax \leq b\}$. Пусть $\Delta_k(A)$ и $\delta_k(A)$ есть максимальное и минимальное абсолютные значение $k \times k$ миноров матрицы A.

Шириной выпуклого тела P будем называть следующую величину: $\mathrm{width}(P) = \min_{c\in\mathbb{Z}^n\setminus\{0\}}\{\max\{c^\top x : x \in P\} - \min\{c^\top x : x \in P\}\}$. Хинчиным [4] был установлен следующий факт: если P не содержит точек из $\mathbb{Z}^n$, то $\mathrm{width}(P) \leq f(n)$, где величина $f(n)$ зависит только от размерности. Существует много оценок на величину $f(n)$. Наилучшая оценка $O(n^{3/4}\log^c(n))$ дана в работе [6]. Наилучшая оценка для симплексов $O(n\,\log(n))$ дана в работе [1]. Дополнительные результаты о ширине симплксов приведены в работе [5].

В работах [2, 3] приведены аналоги теоремы Хинчина, где дополнительным условием является некоторое ограничение на миноры системы задающей политоп. Приведем один из основных результатов данных работ, верный для симплексов.

Теорема 1. *Пусть $A \in \mathbb{Z}^{(n+1)\times n}$, $b \in \mathbb{Z}$ и $P = P(A,b)$ есть симплекс размерности n. Если* $\mathrm{width}(P) \geq \delta_n(A) - 1$, *то $P \cap \mathbb{Z}^n \neq \emptyset$. Более того, в данном случае существует полиномиальный алгоритм предъявляющий целую точку внутри P.*

Задача подсчета ширины симплекса является NP-трудной, как было показано в работе [8]. В случае же ограниченности миноров

системы, задающей симплекс, сложность задачи становится полиномиальной, что показано в данной работе. Имеет место следующая теорема.

Теорема 2. *Пусть* $A \in \mathbb{Z}^{(n+1)\times n}$, $b \in \mathbb{Z}$ *и* $P = P(A, b)$ *есть симплекс размерности* n. *Если величина* $\max\{\Delta_n(A\,b), \Delta_{n-1}(A)\}$ (*под* $(A\,b)$ *имеется в виду расширенная матрица системы*) *фиксирована, то задача вычисления ширины* P *является полиномиально разрешимой.*

Для симплексов, не имеющих целых точек, условия теоремы 2 можно смягчить, а именно можно избавиться от условий на правую часть системы.

Теорема 3. *Пусть* $A \in \mathbb{Z}^{n\times(n+1)}$, $b \in \mathbb{Z}$ *и* $P = P(A, b)$ *есть симплекс размерности* n, *причем* $P \cap \mathbb{Z}^n = \emptyset$. *Если величина* $\max\{\Delta_n(A), \Delta_{n-1}(A)\}$ *фиксирована, то задача вычисления ширины* P *является полиномиально разрешимой.*

Алгоритм, лежащий в основе данной теоремы, использует алгоритмический результат о разбиении произвольного простого конуса на унимодулярные конуса, принадлежащий А. Ю. Чиркову и упомянутый в монографии [9]. Алгоритм также использует процедуру построения *нормальной диагональной формы Смита* [7], одна из наиболее оптимальных версий данной процедуры приведена в работе [10].

Также в данной работе была исследована задача целочисленной оптимизации на симплексе заданном выпуклой оболочкой точек, образующих матрицу с ограниченными минорами. Было показано существование квази-полиномиального алгоритма в данном случае где под квази-полиномиальным алгоритмом понимается алгоритм со сложностью $O(2^{poly(\log\, n)})$.

Теорема 4. *Пусть* $A \in \mathbb{Z}^{(n+1)\times n}$, $c \in \mathbb{Z}^n$ *и* $P = \mathrm{conv}(A)$ *есть симплекс размерности* n (*под* $\mathrm{conv}(A)$ *будем понимать выпуклую оболочку столбцов матрицы* A). *Если величина* $\Delta_n(A)$ *фиксирована, то для решения задачи* $\max\{c^\top x : x \in P \setminus \mathrm{vert}(P) \cap \mathbb{Z}^n\}$ *существует квази-полиномиальный алгоритм. Более того, если величина, равная сумме* $n \times n$ *миноров матрицы* A *фиксирована, то для решения задачи* $\max\{c^\top x : x \in P \setminus \mathrm{vert}(P) \cap \mathbb{Z}^n\}$ *существует полиномиальный алгоритм.*

Список литературы

1. Banaszczyk W., Litvak A. E., Pajor A., Szarek S.J̇. The flatness theorem for non-symmetric convex bodies via the local theory of Banach spaces // Mathematics of operations research. — 1999. — 24 (3). —

P. 728–750.

2. Gribanov D. V. The flatness theorem for some class of polytopes and searching an integer point // Springer Proceedings in Mathematics & Statistics. Models, Algorithms and Technologies for Network Analysis. — 2013. — 104. — P. 37–45.

3. Gribanov D. V., Veselov S. I. On integer programming with bounded determinants // Optimization Letters. Online first.

4. Khinchine A. A quantitative formulation of Kronecker's theory of approximation // Izvestiya Akademii Nauk SSR Seriya Matematika. — 1948. — 12. — P. 113–122.

5. Haase C., Ziegler G. On the maximal width of empty lattice simplices // Europ. J. Combinatorics. — 2000. — 21. — P. 111-119.

6. Rudelson M. Distances between non-symmetric convex bodies and the MM^* -estimate // Positivity. — 2000. — 4(2). — P. 161–178.

7. Schrijver A. Theory of linear and integer programming. — WileyInterscience series in discrete mathematics. John Wiley & Sons, 1998.

8. Sebö A. An introduction to empty lattice simplexes // Cornuéjols, G., Burkard, R.R., Woeginger, R.E. LNCS. — 1999. — 1610. — P. 400–414.

9. Shevchenko V.N. Qualitative topics in integer linear programming (Translations of Mathematical Monographs). — AMS, 1996.

10. Storjohann A. Near optimal algorithms for computing Smith normal forms of integer matrices // ISSAC'96 Proceedings of the 1996 international symposium on Symbolic and algebraic computation. ACM Press. — 1996. — P. 267–274.

О ВОЗМОЖНЫХ ЗНАЧЕНИЯХ МАКСИМУМА ОТНОСИТЕЛЬНОГО ВЛИЯНИЯ ПЕРЕМЕННЫХ ДЛЯ БУЛЕВЫХ ФУНКЦИЙ

И. В. Грибушин (Москва)

В работе [1] дана нижняя оценка максимального значения влияния переменных булевой функции, что позволяет описать класс булевых функций, на которых достигается минимум максимального влияния переменных. В настоящей работе предложены точные верхняя и нижняя оценки максимального относительного влияния переменных для булевых функций и описан класс функций, на котором достигаются граничные значения.

Рассмотрим булеву функцию $f : \{-1,1\}^n \to \{-1,1\}$ от n переменных. Пусть $[n] := \{1, ..., n\}$.

Определение 1 [2]. Характеристической функцией множества $S \subseteq [n]$ называется: $\chi_S := \prod_{i \in S} x_i, \chi_\emptyset := 1$.

Определение 2 [2]. Пусть x равномерно распределено на пространстве $\{-1,1\}^n$. Коэффициентом Фурье функции f относительно $S \subseteq [n]$ называется: $\hat{f}(S) := \hat{f}_S := \mathbf{E} f(x)\chi_S(x)$.

Из равенства Парсеваля [2] следует, что $\sum_{S \subseteq [n]} \hat{f}(S)^2 = 1$.

Определение 3 [3]. Влиянием i-й переменной на функцию f называется: $Inf_i := \mathbf{Pr}_{x \in \{-1,1\}^n}[f(x) \neq f(x^{\oplus i})]$.

Замечание 1 [1]. $Inf_i(f) = \sum_{i \in S \subseteq [n]} \hat{f}(S)^2$.

Определение 4 [3]. Полным влиянием функции f называется величина $Inf(f) := \sum_{i=1}^{n} Inf_i(f)$.

Определение 5. Функции f и $\tilde{f}$ называются эквивалентными, если они имеют одинаковые множества влияний переменных:

$$\{Inf_i(f) | i \in [n]\} = \{Inf_i(\tilde{f}) | i \in [n]\}.$$

Определение 6. Относительным влиянием i-ой переменной на функцию f называется величина $\tau_i = \frac{Inf_i(f)}{Inf(f)}$.

Определение 7 [4]. f называется τ-регулярной для некоторого $\tau > 0$, если $\forall i \in [n] : Inf_i(f) \leq \tau Inf(f)$.

Из определения 7 имеем:

$$\max_{i \in [n]} Inf_i(f) \leq \tau Inf(f) \Rightarrow \max_{i \in [n]} \frac{Inf_i(f)}{Inf(f)} \leq \tau.$$

Так как для любой τ-регулярной функции имеет смысл рассматривать только наименьшее возможное значение τ, получаем, что $\tau = \max_{i \in [n]} \frac{Inf_i(f)}{Inf(f)}$.

Пусть $a \in \{-1,1\}^n$ — точка на булевом кубе, тогда положим $\delta_a(x) = \{1, \text{если } x = a; -1, \text{в противном случае}\}$.

Обозначим I_f — множество, на котором $f = 1$; $k_1(f) := |I_f|$; $M_+ := \{1\} \times \{-1,1\}^{n-1}$ и $M_- := \{-1\} \times \{-1,1\}^{n-1}$ — множества, на которых $x_1 = 1$ и $x_1 = -1$ соответственно. Пусть $k_+(f) := |M_+ \cap I_f|$ и $k_-(f) := |M_- \cap I_f|$ — количество точек в верхнем и нижнем полугиперпространствах относительно переменной x_1, в которых $f = 1$.

Положим $k'_- := \min(k_-, 2^{n-1} - k_-)$; $k'_+ := \min(k_+, 2^{n-1} - k_+)$; $k'_1(f) := k'_+(f) + k'_-(f)$.

Утверждение 1. *Любая булева функция f может быть представлена в виде*: $f = \sum_{x \in I_f} \delta_x + |I_f| - 1$.

Лемма 1. *Для любой булевой функции f и любого $S \neq \emptyset, \{1\}$ выполнено* : $\left|\hat{f}_S\right| \leq \frac{k'_+ + k'_-}{2^{n-1}}$.

Утверждение 2. *Если k'_1 нечетное, то $\tau \leq \frac{2^{n-1}-1}{2^{n-1}+n-2}$. Равенство достигается тогда и только тогда, когда $Inf_1 = \frac{2^{n-1}-1}{2^{n-1}}$ и $Inf_{i \neq 1} = \frac{1}{2^{n-1}}$.*

Утверждение 3. *Если k'_1 четное, то $\tau \leq \frac{2^{n-2}}{2^{n-2}+n-1}$. Равенство достигается тогда и только тогда, когда $Inf_1 = 1$ и $Inf_{i \neq 1} = \frac{1}{2^{n-2}}$.*

Утверждение 4. *Все возможные значения τ для τ-регулярных булевых функций от не более, чем 3 переменных*: $0, \frac{1}{3}, \frac{3}{7}, \frac{1}{2}, \frac{3}{5}$ *и* 1.

Теорема 1. *Множество возможных значений τ для пороговых функций, существенно зависящих от 4 переменных равно*:

$$\left\{\frac{1}{4}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{5}{12}, \frac{1}{2}, \frac{7}{10}\right\}.$$

Далее везде далее предполагаем, что $n \geq 4$. Оценим относительное влияние переменных τ для любой булевой функции.

Теорема 2. *Относительное влияние переменных любой булевой функции, существенно зависящей от n переменных, не превосходит $\frac{2^{n-1}-1}{2^{n-1}+n-2}$. Для функций, таких, что $k'_1 \neq 1$, относительное влияние меньше $\frac{2^{n-1}-1}{2^{n-1}+n-2}$.*

Определение 8 [5]. Пусть $p : \{-1, 1\}^n \to \mathbf{R}$ — линейный многочлен, $f = \text{sign}(p)$, тогда функция $f : \{-1, 1\}^n \to \{-1, 1\}$ называется пороговой.

Определение 9 [5]. Весом пороговой функции $f = sign(p(x))$, где $p = \sum_{i=1}^n a_i x_i - \theta$ называется величина $w(f) := \sum_{i=1}^n a_i^2 + \theta^2$.

Рассмотрим функции, такие, что $k'_1 = 1$. Все они являются пороговыми. Так как для любой пороговой функции f существует эквивалентная ей монотонная пороговая функция [5], рассматриваемые функции эквивалентны функции вида: $x_1^\delta = x_1 + \delta_{\{-1\} \times \{1\}^{n-1}} + 1$. Обозначим класс таких функций через X_1^δ.

Теорема 3. *Функции из класса X_1^δ имеют вес равный n^2-n+1. Их количество равно $n2^{(n+1)}$.*

Из теорем 2 и 3 следует теорема 4.

Теорема 4. *Среди булевых функций, существенно зависящих от n переменных, равенство $\tau = \frac{2^{n-1}-1}{2^{n-1}+n-2}$ выполнено на функциях из X_1^δ и только на них.*

Автор выражает благодарность своему научному руководителю А. А. Ирматову за внимание к работе и полезные обсуждения.

Список литературы

1. J. Kahn, G. Kalai, N. Linial. The influence of variables on Boolean functions // Proceedings of the 29th Annual Symposium on Foundations of Computer Science (1988). — P. 68–80.

2. R. O'Donnell. Analysis of Boolean functions. — Cambridge: Cambridge University Press, 2014.

3. Ben-Or, N. Linial. Collective coin flipping // Randomness and computation. — 1990. — V. 5. — P. 91–115.

4. I. Diakonikolas, P. Harsha, A. Klivans, R. Meka, P. Raghavendra, R. Servedio, Li-Yang Tan. Bounding the average sensitivity and noise sensitivity of polynomial threshold functions // Proceedings of the 42nd ACM symposium on theory of computing (2010). — 2010. — P. 533–542.

5. S. Muroga. Threshold logic and its applications. — New York: Wiley-Interscience, 1971.

ОПРЕДЕЛЕНИЕ МАТРОИДА КАК ГЕОМЕТРИЧЕСКОЙ КОНФИГУРАЦИИ

А. В. Ильев (Омск), В. П. Ильев (Новосибирск)

Впервые определение конечного матроида было дано в 1935 г. Уитни [1]. В дальнейшем было предложено множество эквивалентных определений матроида (см., например, [2]). Большая часть этих определений относится к следующим двум группам.

Первая группа определений. Матроид определяется как булева решетка 2^U всех подмножеств непустого конечного множества U с выделенным семейством подмножеств.

К этой группе относится данное Уитни определение в терминах независимых множеств. В этом определении выделено непустое семейство $\mathcal{A} \subseteq 2^U$ *независимых множеств*, обладающее свойствами:

$(A1)$ если $A \in \mathcal{A},\ B \subseteq A$, то $B \in \mathcal{A}$;

$(A2)$ для любых $A, B \in \mathcal{A}$ таких, что $|B| = |A| + 1$, существует элемент $b \in B \setminus A$, для которого $A \cup \{b\} \in \mathcal{A}$.

Обозначается матроид обычно как $M = (U, \mathcal{A})$.

Обыкновенный матроид — это пара $M = (U, \mathcal{A})$, где U — непустое конечное множество, $\mathcal{A}$ — непустое семейство его независимых подмножеств, обладающее свойствами $(A1)$, $(A2)$, а также свойствами:

$(A3)$ для любого $u \in U$ выполнено $\{u\} \in \mathcal{A}$;

$(A4)$ для любых $u, v \in U$, если $u \neq v$, то $\{u, v\} \in \mathcal{A}$.

К первой группе относятся также хорошо известные определения матроида в терминах баз, циклов и другие.

Вторая группа определений. Матроид определяется как булева решетка 2^U всех подмножеств непустого конечного множества U с заданным на 2^U отображением.

Наиболее известными определениями второй группы являются определение в терминах ранговой функции и следующее определение в терминах оператора замыкания.

Матроид — это пара $M = (U, \varphi)$, где U — непустое конечное множество, φ — отображение булевой решетки 2^U всех подмножеств множества U в себя, которое ставит в соответствие любому множеству $X \subseteq U$ его замыкание $\overline{X}$ и обладает следующими свойствами:

$(\varphi 1)$ $X \subseteq \overline{X}$ для любого $X \subseteq U$;

$(\varphi 2)$ для любых $X, Y \subseteq U$ если $X \subseteq Y$, то $\overline{X} \subseteq \overline{Y}$;

$(\varphi 3)$ $\overline{\overline{X}} = \overline{X}$ для любого $X \subseteq U$;

$(\varphi 4)$ для любых элементов $u, v \in U$ и любого подмножества $X \subseteq U$ если $u \notin \overline{X}$ и $u \in \overline{X \cup \{v\}}$, то $v \in \overline{X \cup \{u\}}$

Матроид $M = (U, \varphi)$ называется *обыкновенным*, если он, кроме того, обладает свойством $(\varphi 5)$:

$(\varphi 5)$ $\overline{\emptyset} = \emptyset$ и $\overline{\{u\}} = \{u\}$ для любого $u \in U$.

Определение в терминах оператора замыкания часто принимают в качестве определения *комбинаторной геометрии*, отождествляя комбинаторные геометрии и обыкновенные матроиды [3, 4]. Если в этом определении отказаться от условия $(\varphi 5)$, то мы получаем определение *комбинаторной предгеометрии*. Таким образом, комбинаторная предгеометрия и матроид — это один и тот же объект.

Весьма естественно выглядело бы определение комбинаторной геометрии как геометрической конфигурации, т. е. системы поверхностей различного ранга, удовлетворяющих заданным аксиомам инцидентности. Хотя изучению вопросов, связанных с комбинаторны-

ми геометриями, посвящена обширная литература (см., например, [3–7]), нам нигде не удалось найти общего геометрического определения комбинаторной предгеометрии (геометрии), которое было бы эквивалентно определению матроида (обыкновенного матроида).

Мы предлагаем геометрическое определение комбинаторной предгеометрии, эквивалентное определению конечного матроида. Дано также аналогичное определение комбинаторной геометрии.

Комбинаторная предгеометрия — это пара $(U, \mathcal{F})$, где U — непустое конечное множество *точек*, $\mathcal{F}$ — семейство его подмножеств — *поверхностей*, каждой из которых приписан *ранг* $k \in Z_+$, обладающих следующими свойствами:

$(G1)$ поверхность ранга 0 существует;

$(G2)$ никакая поверхность ранга k не лежит в поверхности ранга $k-1$;

$(G3)$ всякая поверхность ранга k и точка, не лежащая на ней, лежат в единственной поверхности ранга $k+1$;

$(G4)$ любые k точек, не лежащие ни в какой поверхности ранга, меньшего k, лежат в единственной поверхности ранга k.

Комбинаторная геометрия — это комбинаторная предгеометрия, для которой выполнено свойство $(G5)$:

$(G5)$ $\emptyset$ и все точки являются поверхностями.

Несложно проверить, что система аксиом $(G1)$–$(G5)$ независима, т. е. любая из них не является следствием остальных аксиом.

Эквивалентность приведенного определения определению обыкновенного матроида вытекает из следующей теоремы.

Теорема. 1) *Пусть* $M = (U, \mathcal{A})$ *— обыкновенный матроид, где* U *– непустое конечное множество его элементов,* $\mathcal{A}$ *— семейство его независимых множеств. Тогда семейство* $\mathcal{F}$*, определенное по правилу*

$$\mathcal{F} = \{F \subseteq U \mid \exists A \in \mathcal{A}\ (F = A \cup \{u \in U \mid A \cup \{u\} \notin \mathcal{A}\})\ \}, \quad (1)$$

обладает свойствами $(G1)$–$(G5)$*, причем имеет место равенство*

$$\mathcal{A} = \{A \subseteq U \mid \forall F \in \mathcal{F}\ (r(F) < |A| \to A \not\subseteq F)\}. \quad (2)$$

2) *Пусть* $(U, \mathcal{F})$ *— комбинаторная геометрия, где* U *— непустое конечное множество точек, а* $\mathcal{F}$ *— семейство ее поверхностей. Тогда семейство* $\mathcal{A}$*, определенное по правилу* (2)*, обладает свойствами* $(A1)$–$(A4)$*, причем имеет место равенство* (1).

Доказана также эквивалентность предложенного нами определения комбинаторной предгеометрии и определения матроида общего вида.

Работа первого автора выполнена при поддержке Программы фундаментальных научных исследований государственных академий наук на 2013-2020 годы, п.I.1.1.3. «Теоретико-модельные и алгебро-геометрические свойства алгебраических систем».

Работа второго автора выполнена при финансовой поддержке РНФ (проект 15-11-10009).

Список литературы

1. Whitney H. On the abstract properties of linear dependence // American Journal of Mathematics. — 1935. — V. 57. — P. 509–533.

2. Welsh D. J. A. Matroid theory. — London: Academic Press, 1976.

3. Айгнер М. Комбинаторная теория. — М.: Мир, 1982.

4. Crapo H. H., Rota G.-C. On the foundations of combinatorial theory. II. Combinatorial geometries. — Cambridge: MIT Press, 1970.

5. Lint J. H. van, Wilson R. M. A course in combinatorics. — New York: Cambridge University Press, 2001.

6. Mason J. H. Matroids as the study of geometrical configurations // Higher combinatorics, ed. by M. Aigner. — Dordrecht: Reidel Publishing Company, 1977. — P. 133–176.

7. White N., ed. Combinatorial geometries. Encyclopedia of mathematics and its applications. V. 29. — Cambridge: Cambridge University Press, 1987.

НЕКОТОРЫЕ ЗАДАЧИ НА МАТРОИДАХ

А. Н. Исаченко (Минск), А. М. Ревякин (Москва)

Определения из теории матроидов можно найти в [1–3].

Наиболее известные оптимизационные задачи на матроидах — задача поиска базы минимального или максимального веса и задача поиска независимого множества максимального или минимального веса на пересечении двух матроидов. Для их решения применяется «жадный» алгоритм и алгоритм поиска решения на пересечении двух матроидов соответственно [1].

В настоящей статье рассматривается задача поиска гамильтонова цикла матроида минимального веса. Напомним, что цикл матроида $M = (S, \Sigma)$, имеющего ранг k, называется гамильтоновым, если он содержит $k + 1$ элемент. Некоторые свойства гамильтоновых циклов приведены в работах [4–7].

Итак, пусть дан матроид $M = (S, \Sigma)$ ранга k без петель с заданными весами элементов $w(e) \geq 0$, $e \in S$. Считаем, что матроид

определён семейством циклов Σ. То есть Σ является семейством подмножеств из 2^S, удовлетворяющее следующим двум условиям:

C1) если $C_1 \neq C_2$, $C_1, C_2 \in \Sigma$, то $C_1 \not\subset C_2$;

C2) если $C_1, C_2 \in \Sigma$ и $z \in C_1 \cap C_2$, то существует $C_3 \in \Sigma$, такое что $C_3 \subseteq (C_1 \cup C_2) \backslash z$.

Ниже используются следующие обозначения: $\mathrm{list}(I)$ — упорядоченный список элементов множества I, $\mathrm{first}(\mathrm{list}(I))$ первый элемент этого списка; $\sigma(I)$ — замыкание множества I в матроиде $M = (S, \Sigma)$, то есть множество элементов из S, включая элементы I, добавление которых к I не изменяет ранг.

Для решения задачи рассмотрим следующий алгоритм.

Первый шаг.

1. Упорядочиваем элементы матроида по неубыванию их весов. Пусть $w(e_1) \leq w(e_2) \leq \cdots \leq w(e_n)$.

2. $I_0 = \emptyset$, $\mathrm{list}(I_0) = S$, $\mathrm{Fam} = \{I_0\}$.

3. Пересчитываем веса элементов $w(e_i) := w(e_i) - w(e_1)$. Полагаем оценку $\xi(I_0)$ множества I_0 и текущий рекорд f^* равными $w(e_1)$.

4. Полагаем $I_1 = \{e_1\}$, $I_2 = \emptyset$, $\mathrm{list}(I_1) := \mathrm{list}(I_0) - \sigma(e_1)$, $\mathrm{list}(I_2) := \mathrm{list}(I_2) - \{e_1\}$.

5. Преобразуем веса элементов из $\mathrm{list}(I_1)$ и $\mathrm{list}(I_2)$ по формуле $w(e) := w(e) - w(\mathrm{first}(\mathrm{list}(I_j)))$, $e \in \mathrm{list}(I_j)$, $j = 1, 2$. Оценки множеств $\xi(I_j) = \xi(I_0) + w(\mathrm{first}(\mathrm{list}(I_j)))$, $j = 1, 2$.

6. Полагаем $\mathrm{Fam} = \{I_1, I_2\}$.

Общий шаг.

1. Среди множеств семейства Fam находим множество I_p с минимальной оценкой. Если таких множеств несколько, берём любое из тех, которые имеют максимальное число элементов. Полагаем рекорд f^* равным $\xi(I_p)$.

2. Если $|I_p| = k$, то есть I_p — база матроида, идём к пункту 5. Если $|I_p| = k + 1$, то I_p искомый гамильтонов цикл. Завершаем работу.

3. Полагаем множества $I_p^1 = I_p \cup \{\mathrm{first}(\mathrm{list}(I_p))\}$, $I_p^2 = I_p$, списки $\mathrm{list}(I_p^1) = \mathrm{list}(I_p) - \sigma(I_p^1)$, $\mathrm{list}(I_p^2) = \mathrm{list}(I_p) - \mathrm{first}(\mathrm{list}(I_p))$, оценки $\xi(I_p^j) = \xi(I_p) + w(\mathrm{first}(\mathrm{list}(I_p^j)))$, $j = 1, 2$.

4. Полагаем $\mathrm{Fam} := (\mathrm{Fam} \setminus \{I_p\}) \cup \{I_p^1, I_p^2\}$. Перенумеровываем множества Fam от 1 до $|\mathrm{Fam}|$. Возвращаемся к пункту 1 общего шага.

5. Добавляя к I_p по одному элементу из $S \backslash I_p$ в порядке неубывания их весов, находим первый элемент e_l из них, для которого $I_p \cup e_l$ является циклом. Полагаем $I_p := I_p \cup e_l$, $\xi(I_p^j) = \xi(I_p) + w(e_l)$ и идём к пункту 1 общего шага.

Нетрудно видеть, что данный алгоритм является реализацией метода ветвей и границ, аналогичной алгоритму Литтла для задачи коммивояжёра. Прямой перенос вариантов алгоритма Литтла невозможен в силу отсутствия у матроидов отношения инцидентности элементов, которое применяется в задаче коммивояжёра на графе для формулирования правила ветвления и пересчета оценок.

Для матроидов правила ветвления принимают самый общий вид, состоящий в выборе на каждой итерации для включения в гамильтонов цикл любого элемента с минимальным весом. Процедура приведения весов заключается в уменьшении всех весов на величину минимального из весов, что приводит к появлению элементов e с $w(e) = 0$. При включении элемента в текущее решение, для соответствующей ветви дерева поиска решения исключаются все элементы, приводящие к образованию циклов с уже имеющимся независимым множеством.

Список литературы

1. Welsh D. J. A. Matroid theory. — London: Acad. Press, 1976.
2. Айгнер М. Комбинаторная теория. — Москва: Мир, 1982.
3. Ревякин А. М., Исаченко А. Н. Криптоморфные системы аксиом, линейная и алгебраическая представимость матроидов // Сборник научных трудов МИЭТ. Посвящается 70-летию профессора А. С. Поспелова. — М.: МИЭТ, 2016. — С. 99–109.
4. Исаченко А. Н., Исаченко Я. А. Периметр матроида и задача коммивояжёра для матроидов // XI Белорусская математическая конференция. Тез. докл. Междунар. науч. конф., Минск, 5–9 ноября 2012 г. — Ч. 4. — Минск: Институт математики НАН Беларуси, 2012. — С. 87–88.
5. Исаченко А. Н., Исаченко Я. А. Свойства гамильтоновых матроидов // Международный конгресс по информатике: информационные системы и технологии. Материалы меджунар. науч. конгресса, Республика Беларусь, Минск, 4–7 нояб. 2013 г. — Минск: БГУ, 2013. — С. 538–541.
6. Исаченко А. Н., Исаченко Я. А. Циклический граф гамильтонова матроида // Дискретная математика, алгебра и их приложения: Тез. докл. Междунар. науч. конф. Минск, 14–18 сентября 2015 г. — Минск: Институт математики НАН Беларуси, 2015. — С. 108–109.
7. Исаченко А. Н., Исаченко Я. А. О некоторых характеризациях матроидов и свойствах гамильтоновых матроидов // Современные информационные технологии и ИТ-образование. — 2015. — Т. 2 (№ 11). — С. 214–219.

ОПТИМАЛЬНАЯ СТРАТЕГИЯ ВЫБОРА ПЕРЕМЕННОЙ ВЕТВЛЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ О СУММЕ ПОДМНОЖЕСТВ МЕТОДОМ ВЕТВЕЙ И ГРАНИЦ

Р. М. Колпаков, М. А. Посыпкин (Москва)

Рассматривается оптимизационная задача о сумме подмножеств, которая может быть сформулирована следующим образом:

$$\begin{array}{l} \text{maximize } f(\tilde{x}) = \sum_{i\in N} x_i w_i, \\ \text{subject to } f(\tilde{x}) = \sum_{i\in N} x_i w_i \le C, \\ x_i \in \{0,1\}, i \in N, \end{array} \tag{1}$$

где $N = \{1, 2, \ldots, n\}$, $C > 0$ и $w_i > 0$ для $i \in N$. Задача о сумме подмножеств является частным случаем задачи о ранце с одним ограничением [1, 2], в котором веса и стоимости предметов совпадают.

Пусть $I \subseteq N$ и пусть θ — некоторое отображение из I в $\{0, 1\}$. Тогда пара (I, θ) однозначным образом определяет следующую оптимизационную подзадачу P задачи (1):

$$\begin{array}{l} \text{maximize } f(x) = \sum_{i\in N} w_i x_i, \\ \text{subject to } f(x) = \sum_{i\in N} w_i x_i \le C, \\ x_i = \theta(i), i \in I, \\ x_i \in \{0,1\}, i \in N \setminus I. \end{array}$$

Переменные x_i для $i \in I$ называются *фиксированными переменными* подзадачи P, а переменные x_i для $i \in N \setminus I$ называются *свободными переменными* этой подзадачи. Элементы пары (I, θ), определяющей подзадачу P, будем обозначать через $I(P)$ и θ_P. Положим также

$$I_0(P) = \{i \in I(P) : \theta_P(i) = 0\}, \quad I_1(P) = \{i \in I(P) : \theta_P(i) = 1\}.$$

Пусть $W = \sum_{i\in N} w_i$. Будем говорить, что для подзадачи P выполнено *условие отрицательного отсева* **C0**, если $\sum_{i\in I(P)} \theta_P(i) w_i > C$. Очевидно, что подзадача, удовлетворяющая условию **C0**, не имеет решений. Будем говорить, что для подзадачи P выполнено *условие положительного отсева* **C1**, если $\sum_{i\in I(P)} (1-\theta_P(i)) w_i \ge W - C$. Очевидно, что подзадача, удовлетворяющая условию **C1**, имеет единственное оптимальное решение. Пусть подзадача P не удовлетворяет ни одному из условий **C0** и **C1**, x_j — некоторая свободная переменная подзадачи P. Тогда подзадачу P можно разбить на две

подзадачи P_0 и P_1, получаемые из P присваиванием переменной x_j значений 0 и 1 соответственно. Процедуру получения подзадач P_0 и P_1 из подзадачи P будем называть *декомпозицией* подзадачи P по переменной x_j. Переменная x_j называется *переменной ветвления* для подзадачи P.

Рассматривается классический метод ветвей и границ (МВГ) для решения задачи о сумме подмножеств, который состоит в последовательном выполнении итераций следующего цикла (в процессе выполнения данной процедуры поддерживаются список подзадач, подлежащих дальнейшему рассмотрению, и текущее рекордное решение задачи).

1. В список подзадач помещается исходная задача (1).

2. Если список подзадач пуст, то алгоритм завершает свою работу, в противном случае выбирается и удаляется из списка одна из подзадач (подзадача P).

3. Если подзадача P удовлетворяет условию **C0**, выполняется переход к шагу 2.

4. Если подзадача P удовлетворяет условию **C1**, вычисляется оптимальное решение z для данной подзадачи. Если значение целевой функции f на данном решении больше текущего рекорда, текущее рекордное решение заменяется на z. Затем выполняется переход к шагу 2.

5. Для подзадачи P выбирается переменная ветвления и призводится декомпозиция подзадачи P по данной переменной на две подзадачи, которые добавляются в список подзадач. Затем выполняется переход к шагу 2.

Сложностью решения задачи о сумме подмножеств МВГ называется число итераций цикла 2–5, выполняемых при решении задачи данным методом. Очевидно, что данная сложность равна числу подзадач (включая исходную задачу), рассмотренных в процессе решения задачи МВГ.

Пусть G — задача вида (1). Под процедурой выбора переменной ветвления для решения этой задачи МВГ будем понимать произвольное отображение φ, которое ставит в соответствие каждой паре (I, θ), где $I \subset N$ и θ — отображение из I в $\{0, 1\}$, некоторое число $\varphi(I, \theta)$ из $N \setminus I$. Под сложностью решения задачи G МВГ с процедурой φ выбора переменной ветвления понимается сложность процедуры решения задачи G МВГ, при выполнении которой на шаге 5 алгоритма в качестве переменной ветвления для декомпозиции подзадачи P выбирается переменная с номером $\varphi(I(P), \theta_P)$. Процедуру выбора переменной ветвления для решения задачи G МВГ будем называть *оптимальной*, если сложность решения задачи G

МВГ с данной процедурой выбора переменной ветвления является минимальной возможной. В общем случае, под процедурой выбора переменной ветвления для МВГ будем понимать произвольное отображение Φ, которое ставит в соответствие каждой тройке (G, I, θ), где G — задача вида (1), $I \subset N$ и θ — отображение из I в $\{0, 1\}$, некоторое число $\Phi(G, I, \theta)$ из $N \setminus I$. Процедуру Φ выбора переменной ветвления для МВГ будем полагать оптимальной, если для любой задачи G вида (1) процедура $\varphi_G(I, \theta) = \Phi(G, I, \theta)$ решения задачи G МВГ является оптимальной. Далее будем без ограничения общности полагать, что для задачи (1) выполняется $w_1 \geq w_2 \geq \ldots \geq w_n$. Рассмотрим процедуру Φ^M выбора переменной ветвления для МВГ такую, что $\Phi^M(G, I, \theta) = \min\{i \mid i \in N \setminus I\}$, тем самым в качестве переменной ветвления для декомпозиции любой подзадачи задачи G данная процедура выбирает свободную переменную x_i с наибольшим значением w_i. Мы называем такую процедуру выбора переменной ветвления *мажоритарной*. В [3] показано, что мажоритарная процедура выбора переменной ветвления может быть более эффективной, чем общераспространенная процедура выбора дробной переменной в качестве переменной ветвления.

Теорема. *Мажоритарная процедура выбора переменной ветвления является оптимальной для решения задачи о сумме подмножеств.*

Работа выполнена при финансовой поддержке РФФИ (проект 15-07-03102).

Список литературы

1. Martello S., Toth P. Knapsack Problems. — John Wiley & Sons Ltd., 1990.

2. Kellerer H., Pfershy U., Pisinger D. Knapsack Problems. — Springer Verlag, 2004.

3. Колпаков Р. М., Посыпкин М. А. Асимптотическая оценка сложности метода ветвей и границ с ветвлением по дробной переменной для задачи о ранце // Дискретн. анализ и исслед. опер. — 2008. — Т. 15, № 1. — С. 58–81.

О СЛОВАХ, ИЗБЕГАЮЩИХ ПОВТОРЫ

Н. В. Котляров (Москва)

Данная статья посвящена некоторым вопросам, связанным с существованием периодических структур в словах из формальных языков. Наиболее простой и хорошо изученной периодической структурой являются квадраты, то есть фрагменты вида xx, где x — произвольное непустое слово. Слово, не содержащее квадратов, называется бесквадратным. Классическим результатом, связанным с квадратами, является работа Акселя Туэ [1], в которой установлено существование как угодно длинных бесквадратными слов над алфавитом из трех букв. С другой стороны, несложно проверить, что не существует бесквадратных слов над алфавитом из двух букв. Поэтому из результатов Туэ следует, что алфавит из трех букв является минимальным алфавитом, над которым существуют как угодно длинные бесквадратные слова. В дальнейшем было получено много различных альтернативных доказательств данного результата Туэ, одно из наиболее изящных доказательств представлено в [2]. Естественным обобщением результата Туэ является работа [3]. В нашей работе рассматривается случай, когда в словах допускаются достаточно "маленькие" квадраты. Подобное допущение рассматривается, например, в работе [4], где доказано существование бесконечного слова над алфавитом из двух букв, которое содержит только 3 различных коротких квадрата. Другие базовые результаты, касающиеся квадратов, получены в работах [5, 6].

Нетрудно заметить, что задача существования сколь угодно длинных слов, не содержащих фрагментов определенного типа, эквивалентна задаче существования бесконечных слов над тем же алфавитом, не содержащих данных фрагментов. Поэтому в работах, посвященных этой тематике, обычно рассматривается эквивалентная задача существования бесконечных слов.

Слово называется сильно бескубным, если оно не содержит фрагментов вида xxa, где x — непустое слово, a — первая буква слова x. Классическим результатом Акселя Туэ для сильно бескубных слов является работа [3], в которой было доказано существование сколь угодно длинных сильно бескубных слов над двухбуквенным алфавитом. В частности, в данной работе приведен пример бесконечного сильно бескубного слова над двухбуквенным алфавитом. Это слово называется в литературе последовательностью Туэ (Туэ—Морса).

Другим естественным обобщением задачи о существовании сколь угодно длинных бесквадратных слов является рассмотрение в качестве "запретных" фрагментов не только квадратов, но и квадратов

с Δ ошибками замещения, то есть фрагментов вида xy, где слово x отличается от слова y ровно на Δ букв. Отметим, что, например, любой фрагмент длины 2 является либо квадратом, либо квадратом с одной ошибкой замещения, поэтому для данной задачи естественно вводить ограничения снизу как на длины "запретных" квадратов, так и на длины "запретных" квадратов с ошибками замещения. По нашим сведениям данная задача еще не рассматривалась в научной литературе, за исключением предыдущих работ автора [7], где было показано существование над алфавитами различных мощностей сколь угодно длинных слов, не содержащих квадратов и квадратов с одной ошибкой, в зависимости от ограничений снизу на длину квадратов. В данной работе рассматривается следующая задача: можно ли построить над двухбуквенным алфавитом как угодно длинное слово, не содержащее квадратов и квадратов с несколькими ошибками при наличии ограничения на длины этих квадратов, и каким при этом должно быть это ограничение? В данной работе доказано, что существует бесконечное слово над алфавитом из двух букв, не содержащее квадратов с не более чем Δ ошибками таких, что их длина превосходит $4\Delta + 4$. Основной результат работы:

Теорема. *Для любого натурального Δ существует бесконечное слово над алфавитом из двух букв, у которого нет факторов, являющихся квадратами с не более Δ ошибками и периодом больше $2\Delta + 2$.*

При доказательстве данной теоремы строится отображение f_g из множества слов над алфавитом из двух букв в множество слов над алфавитом из двух букв по следующему правилу:

$$f_g(a_1a_2...a_{n-1}a_n) = g(a_1a_2)g(a_2a_3)...g(a_{n-1}a_n),$$

$$f_g(a_1a_2...) = g(a_1a_2)g(a_2a_3)...,$$

где g — отображение из слов двухбуквенного алфавита длины 2 в множество слов двухбуквенного алфавитом, которое подобрано так, что образ последовательности Туэ—Морса при отображении f_g обладал бы требуемыми свойствами. В работе представлен примеры такого отображения для всех возможных значений Δ.

Список литературы

1. Thue A. Uber unendliche Zeichenreihen // Norske, Vid. Selsk. Skr. I, Mat. Nat. Kl. Khristiana — 1906. — 7. — S. 1–22.

2. Саломаа А. Жемчужины теории формальных языков. — М.: Мир, 1986.

3. Thue A. Uber die gegenseitige Lage gleicher Teile gewisser Zeichenreihen // Norske, Vid. Selsk. Skr. I, Mat. Nat. Kl. Kristiania. —

1912. — 1. — S. 1–67.

4. Fraenkel A. S., Simpson R. J. How many squares must a binary sequence contain? // Electr. J. Comb. — 1995. — 2.

5. Crochemore M., Ilie L., Rytter. W. Repetitions in strings: algorithms and combinatorics // Theor. Comput. Sci. — 2009. — 410 (50). — P. 5227–5235.

6. Crochemore M., Rytter. W. Squares, cubes, and time-space efficient string searching // Algorithmica. — 1995. — 13 (5). — P. 405–425.

7. Котляров Н. В. О существовании сколь угодно длинных слов, не содержащих квадратов с одной возможной ошибкой замещения // Дискретная математика. — 2015. — Т. 27, вып. 2. — С. 56–72.

ДИСТРИБУТИВНЫЕ ВЕКТОРНЫЕ ПРОСТРАНСТВА НАД РЕШЕТКАМИ И ИХ СВОЙСТВА

Е. Е. Маренич, В. Е. Маренич (Москва)

В работах [1–3] определены векторные пространства над решетками и рассмотрены их свойства. В работах [4, 5] доказан критерий дистрибутивности пространства над двухэлементной решеткой и доказан критерий регулярности булевых матриц конечного (или бесконечного размера) над двухэлементной решеткой. В работе [1] доказан критерий дистрибутивности пространства над двухэлементной решеткой, использующий идентификаторы.

Предварительные сведения. Пусть $(L, \wedge, \vee, \leq)$ — решетка с частичным порядком $\leq$ и решеточными операциями $\vee$ и $\wedge$. Обозначим: $\widetilde{0}$ и $\widetilde{1}$ — наименьший и наибольший элементы решетки; $join(L)$ — множество всех $\vee$-неразложимых элементов решетки L; множество $J(L) = join(L) \setminus \{\widetilde{0}\}$.

Пусть $L^{m\times n}$ — множество всех (решеточных) $m \times n$ матриц. В работе рассматриваются матрицы (и пространства) только над дистрибутивными решетками с $\widetilde{0}$ и $\widetilde{1}$, где $\widetilde{0} \neq \widetilde{1}$. Операции сложения и умножения матриц над решеткой L задаются как обычно: вместо сложения используется операция $\vee$, а вместо умножения – $\wedge$.

Пусть элемент $\lambda \in P$, матрицы $A = (a_{ij})$, $C = (c_{ij}) \in P^{m\times n}$. Будем писать $C = \lambda A$, если $c_{ij} = \lambda \wedge a_{ij}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Матрица $A \in L^{m\times n}$ называется регулярной, если существует матрица $X \in L^{n\times m}$ такая, что $AXA = A$.

Векторным пространством, порожденным множеством векторов $U = \{u_1, u_2, \ldots, u_n\} \subseteq L^{m\times 1}$, называется множество
$Lin(U) = \{\lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n |\ \lambda_1, \lambda_2, \ldots, \lambda_n \in L\}$.

Столбцовое пространство матрицы $A \in L^{m\times n}$ – это пространство $Column_L(A) = Lin(A^{(1)}, A^{(2)}, \ldots, A^{(n)})$, где $A^{(i)}$ — i-й столбец A.

1. *Векторные пространства как решетки.* Пусть L — решетка, $V = Lin_L(U) \subseteq L^{m\times 1}$, где U — множество векторов $\{u_1, u_2, \ldots, u_n\} \subseteq L^{m\times 1}$.

Арифметическое пространство $L^{m\times 1}$ является дистрибутивной решеткой с решеточными операциями $\vee$ и $\wedge$. Пространство V — полурешетка относительно операции $\vee$. Если для любого множества $S \subseteq V$ существует $\vee S$, то V — полная решетка, [6]. В частности, конечные пространства V являются решетками.

Обозначим $\vee$ и $\widetilde{\wedge}$ решеточные операции в решетке V. Для любых векторов $u, v \in V$ справедливы неравенства $u \mathbin{\widetilde{\wedge}} v \leq u \wedge v$. Если для векторов $u, v \in V$ существует наибольшее $\mu \in L$ такое, что $\mu u \leq v$, то обозначим его через $\langle v/u \rangle_V$. Определение и свойства брауэровых решеток даны [6]. Если L — брауэрова решетка, то для любых векторов $u, v \in V$ существует $\langle v/u \rangle_V$.

Теорема 1.1. *Пусть L — брауэрова решетка. Тогда пространство V — решетка и для любых векторов $v, w \in V$*

$$v \mathbin{\widetilde{\wedge}} w = \sum_{r=1}^{n} \left(\langle v/u_r \rangle_V \wedge \langle w/u_r \rangle_V\right) u_r.$$

Теорема 1.2. *Пусть L — цепь с единицей $\widetilde{1}$. Тогда для любых векторов $v, w \in V$ и любого $\lambda \in P$ справедливы равенства:*

$$\lambda(u \mathbin{\widetilde{\wedge}} v) = (\lambda u) \mathbin{\widetilde{\wedge}} v = u \mathbin{\widetilde{\wedge}} (\lambda v) = (\lambda u) \mathbin{\widetilde{\wedge}} (\lambda v).$$

Теорема 1.3. *Пусть L — полная брауэрова решетка. Тогда V — полная решетка.*

2. *Дистрибутивность ретрактов.* Пусть L — решетка, матрица $B \in L^{m\times m}$, пространство $V = Column_L(B)$. Матрица B называется идемпотентом, если $B = B^2$. Пространство V называется ретрактом, если $V = Column_L(B)$ для некоторого идемпотента B.

Теорема 2.1. *Пусть матрица B — идемпотент. Тогда V — решетка и $u \mathbin{\widetilde{\wedge}} v = B(u \wedge v)$ для любых векторов $u, v \in V$.*

Для брауэровых решеток теорема 2.1 доказана в работе [7].

Следствие 2.1. *Каждый ретракт — дистрибутивное пространство.*

Следствие 2.2. *Пусть пространство V — ретракт. Тогда для любых векторов $u, v \in V$ и для любых $\lambda \in L$ справедливы равенства* $\lambda(u\widetilde{\wedge}v) = (\lambda u)\widetilde{\wedge}v = u\widetilde{\wedge}(\lambda v) = (\lambda u)\widetilde{\wedge}(\lambda v)$.

3. *Идентификаторы.* Пусть P — конечная дистрибутивная решетка, пространство $V \subseteq P^{m\times 1}$. Вектор $id(w) \in P^{m\times 1}$ называется идентификатором вектора $w \in J(V)$, если $id(w)$ есть $\vee$-неразложимый вектор решетки $P^{m\times 1}$ такой, что

$$id(w) \le w, \quad id(w) \not\le \sum_{j\in J(V), w\not\le z} z.$$

Каждый идентификатор $id(w)$ имеет только одну ненулевую компоненту, которая является $\vee$-неразложимым элементом решетки P.

Теорема 3.1. *Пространство V дистрибутивно тогда и только тогда, когда V — пространство с идентификаторами.*

Для решетки $P = \{\widetilde{0}, \widetilde{1}\}$ теорема 3.1 доказана в [1].

4. *Дистрибутивные пространства над цепями.* Пусть P — конечная цепь, пространство $V \subseteq P^{m\times 1}$.

Теорема 4.1. *Пространство V дистрибутивно тогда и только тогда, когда для любого вектора $w \in J(V)$*

$$w \not\le \sum_{j\in J(V), w\not\le z} z.$$

5. *Дистрибутивность пространств над нечеткой решеткой.* Нечеткой решеткой называется решетка $L = ([0;1], \vee, \wedge, \le)$, где $[0;1]$ - числовой интервал, $\le$ — обычный ЧП на числовом множестве и для любых $a, b \in [0;1]$: $a \vee b = \max\{a, b\}$, $a \wedge b = \min\{a, b\}$.

Пусть матрица $A \in L^{m\times n}$, пространство $V = Column_L(A)$. Обозначим $Set(A)$ — множество всех элементов матрицы A.

Теорема 5.1. *Пусть P — множество и $\{1\} \cup Set(A) \subseteq P \subseteq [0;1]$. Тогда решетка $U = Column_P(A)$ — подрешетка решетки V.*

Следствие 5.1. *Следующие утверждения равносильны.*

1. *Пространство V дистрибутивно (модулярно).*
2. *Для любого множества P, такого что $\{1\} \cup Set(A) \subseteq P \subseteq [0;1]$, пространство $U = Column_P(A)$ дистрибутивно (модулярно).*

Следствие 5.2. *Пусть матрица $A \in \{\widetilde{0}, \widetilde{1}\}^{m\times n}$. Если пространство $Column_{\{\widetilde{0},\widetilde{1}\}}(A)$ не дистрибутивно (не модулярно), то и пространство $Column_L(A)$ не дистрибутивно (не модулярно).*

Список литературы

1. Kim K. Boolean matrix theory and applications — New York: Marcel Dekker, 1982.

2. Kim K. and Roush F. Generalized fuzzy matrices // Fuzzy Sets Systems. — 1980. — 4. — P. 293–315.

3. Маренич Е. Е., Маренич В. Е. Базисы и размерность векторных пространств над решётками // Фундамент. и прикл. матем. — 2014. — 19:2. — С. 151–169.

4. Зарецкий К. А. Регулярные элементы полугруппы бинарных отношений // Успехи мат. наук. — 1962. — Т. XVII, вып. 3. — С. 177–179.

5. Зарецкий К. А. Полугруппа бинарных отношений // Математический сборник. — 1963. — 61 (103). — С.291–305.

6. Биркгоф Г. Теория решёток. — М.: Наука, 1984.

7. Marenich V. E. Lattices of matrix rows and matrix columns. Lattices of invariant column eigenvectors // Matrix methods: Theory, Algorithms and Applications — 2010. — P. 104–116.

ДИСКРЕТНЫЕ ВЕРСИИ ТЕОРЕМ О НЕПОДВИЖНЫХ ТОЧКАХ

О. Р. Мусин (Москва)

Лемма Шпернера о раскраске вершин триангуляции, доказанная в 1928 году, является дискретным аналогом теоремы Брауэра о неподвижной точке. У леммы большое число приложений. В частности, эта лемма и ее обобщения играют важную роль в теории игр и математической экономике.

Дискретными версиями теоремы Борсука—Улама являются леммы Таккера, Ки Фана и Шашкина. У этих лемм тоже имеются многочисленные приложения.

В наших работах [1–7] получено большое число обобщений классических теорем о неподвижных точках и их дискретных аналогов. Рассмотрим здесь некоторые из них.

Лемма Шпернера утверждает, что *при любой Шпернеровской раскраске вершин триангуляции n-мерного симплекса в $n+1$ цветов найдется ячейка триангуляции, вершины которой покрашены во все цвета.* В работе [3] мы показываем, что вместо симплекса можно взять произвольное многообразие с краем. Более того, на многообразия можно обощить и так называемую “лемму Шпернера для многогранников.”

В этой же работе мы показываем, что леммы Таккера и Фана тоже могут быть обобщены для симплициальных многообразий. В

работе [1] рассматривается класс многообразий со свободным действием инволяции для которых верна теорема Борсука—Улама. (Мы назвали этот класс БУТ.) В [3] доказано, что если многообразие принадлежит этому классу, то для него верны леммы Таккера и Фана. Большая часть этих результатов может быть обобщена для БУТ-пространств, которые рассматриваются в работе [7].

Оказывается, что не обязательно рассматривать триангуляции. Мы показали, см. [2], что вместо триангуляций можно рассматривать "квадрангуляции", то есть разбиения многообразия с краем на параллелипипеды.

В 1990-х годах уральский математик Ю. А. Шашкин опубликовал несколько работ по теме данной статьи. В частности, в 1996 году он опубликовал работу в которой нашел дискретный аналог теоремы о нечетном отображении сфер. Эта работа была опубликована только на русском и в ней рассматривался только двумерный случай, т.е. триангуляция многоугольника. Более того, Ю. А. Шашкин приписал этот результат Ки Фану. Лемма Шашкина действительно может быть выведена из леммы Фана, однако, этот результат новый, а доказательство Шашкина оригинальное.

В работе [4] мы рассматриваем обобщения леммы Шашкина. Сначала доказывается, что вместо сфер в теореме о нечетном отображении могут быть любые БУТ-многообразия. Это позволяет получить лемму Шашкина для триангуляций многообразий из класса БУТ.

В недавней работе [5] мы рассмотрели обобщения леммы Шпернера без предположении, что раскрасска на границе является Шпернеровской, а число цветов m может быть и меньше чем $n+1$. По раскраске на границе мы определи инвариант μ, который равен 1 при Шпернеровской раскраске. Основной результат:
Если $\mu \neq 0$, то верна лемма Шпернера, т.е. найдется симплекс триангуляции, вершины которого покрашены во все m цветов.

Заметим, что если $m = n+1$, то инвариант μ является степенью отображения, а при $m = n$ это инвариант Хопфа. В работе [6] рассматриваются дальнейшие приложения инварианта μ к леммам Шпернера и Кнастера—Куратовского—Мазуркевича (KKM), а также к их "цветным" обобщениям.

Работа выполнена при поддержке гранта NSF DMS–1400876 и гранта РФФИ 15-01-99563

Список литературы

1. Musin O. R. Borsuk–Ulam type theorems for manifolds // Proc. Amer. Math. Soc. — 2012. — 140. — P. 2551–2560.

2. Musin O. R. Sperner type lemma for quadrangulations // Mosc. J. of Combin. and Number Theory. — 2015. — 5 (1). — P. 26–35.

3. Musin O. R. Extensions of Sperner and Tucker's lemma for manifolds // J. of Combin. Theory Ser. A. — 2015. — 132. — P. 172–187.
4. Musin O. R. Generalizations of Tucker–Fan–Shashkin lemmas // arXiv: 1409.8637.
5. Musin O. R. Homotopy invariants of covers and KKM type lemmas // arXiv:1505.07629.
6. Musin O. R. KKM type theorems with boundary conditions, arXiv:1512.04612
7. Musin O. R., Volovikov A. Yu. Borsuk–Ulam type spaces // Mosc. Math. J. — 2015. — 15 (4) — P. 749–766.

ВОКРУГ ЛЕММЫ ОБ ИЗОЛИРОВАНИИ

А. О. Останин, А. Б. Дайняк (Москва)

Пусть A — некоторое n-элементное множество, F — семейство подмножеств A. Пусть для каждого элемента $x \in A$ его вес $w(x)$ выбирается случайно из множества $\{1, 2, \ldots, m\}$, а вес элемента $E \in F$ определяется как $\sum\limits_{x \in E} w(x)$. Если ровно один элемент F имеет минимальный вес, то весовая функция w называется *изолирующей* для семейства F. Лемма об изолировании утверждает, что при таких условиях вероятность того, что w — изолирующая функция, не меньше $(1 - \frac{1}{m})^n$.

В данной работе мы рассматриваем некоторые вопросы, касающиеся уточнения леммы, получения достижимых оценок вероятности единственности множества с минимальным весом и поиска оптимальных конструкций.

Теорема [точная лемма об изолировании для одноэлементных подмножеств]. *Пусть F — система одноэлементных множеств на n-элементном множестве. Тогда вероятность того, что функция w изолирующая, не меньше*

$$\frac{n \cdot \sum\limits_{x=1}^{m-1} x^{n-1}}{m^n}.$$

Эта оценка достигается тогда и только тогда, когда F содержит все n одноэлементных подмножеств.

Доказательство проводится индукцией по n.

Пусть теперь размер множеств в F ограничен снизу некоторым натуральным числом l. Покажем, как получать примеры для таких систем, используя примеры для систем одноэлементных множеств.

Назовем $(n_1, n_2, \ldots, n_l)$-полной системой систему множеств F на $n = n_1 + n_2 + \ldots n_l$ элементах такую, что $V(G) = \cup_{i=1}^{l} V_i$, где $|V_i| = n_i$, и множества в F получаются взятием из каждого V_i по одному элементу. Нетрудно видеть, что в этом случае F будет содержать $n_1 \cdot n_2 \cdot \ldots \cdot n_l$ множеств. Если $n_i \geq 2$ для любого i, то для такой системы вероятность единственности минимального множества равна $\prod_{i=1}^{l} \alpha(n_i)$, где $\alpha(n_i)$ — вероятность единственности минимума для системы из n_i одноэлементных множеств. Поскольку при фиксированном n количество весовых функций одно и то же, мы будем минимизировать количество тех из них, при которых минимум единственнен.

Теорема [асимптотическая оптимальность $(2, n-2)$-полной системы для $l = 2$]. *Для любого натурального n существует натуральное M такое, что при любом $m > M$ количество изолирующих весовых функций для $(2, n-2)$-полной системы меньше, чем количество хороших расстановок для $(x, n-x)$-полной системы при любом $x \in [3; n-3] \cup \{1, n-1\}$.*

Заметим, что для $(2, 2, 2, \ldots, 2)$-полной системы вероятность изолирующей функции ровна $(\frac{m-1}{m})^{\frac{n}{2}}$, что равняется квадратному корню из оценки Та-Шма. Однако, из предыдущей теоремы следует, что такая система не является оптимальной в своем классе, то есть при больших m можно получить меньшую вероятность единственности минимума.

Компьютерный перебор для небольших значений n, m ($n \leq 7, m \leq 5$) позволяет выдвинуть следующую гипотезу.

Гипотеза. *Для систем F множеств на n элементах, составленных из l-элементных подмножеств ($n \geq 2l$), минимум вероятности изолирующей весовой функции достигается на $(2, 2, \ldots, 2, n-2(l-1))$-полной системе.*

Мы доказали эту гипотезу при $l = 2, m = 2$. В таком случае F удобно рассматривать как множество ребер графа на n вершинах. Для проверки гипотезы нужно доказать, что в любом графе на n вершинах количество весовых функций на вершинах, для которых минимальное ребро единственно, не меньше чем $2(n-2)$.

Теорема [точная лемма об изолировании для $m = 2$ и систем двухэлементных подмножеств]. *Количество изолирующих весовых*

функций на вершинах в любом графе на n вершинах не меньше чем $2(n-2)$.

Опишем идею доказательства.

Лемма. *Если в графе m ребер, то количество изолирующих функций не меньше m.*

Если граф полный, то изолирующих функций не меньше чем $\frac{n(n-1)}{2}$.

В противном случае выберем вершины u, v, не соединенные ребром так, чтобы максимизировать $|N(u) \cup N(v)|$. Пусть $A = N(u) \setminus N(v), B = N(u) \cap N(v), C = N(v) \setminus N(u)$, $a = |A|, b = |B|, c = |C|$. В зависимости от размера множества $|A \cup B \cup C|$ возникает несколько случаев, в каждом из которых можно предъявить $2(n-2)$ изолирующих функций.

Приведем также утверждение, согласно которому оценка вероятности в теореме Та-Шма скорее всего недостижима.

Теорема. *Пусть* $m \geq 3$. *Тогда количество изолирующих весовых функций не меньше чем* $(m-1)^n + \frac{a_1}{2}$, *где* a_1 *— количество изолирующих весовых функций, отображающих хотя бы один элемент в единицу.*

Доказательство теоремы состоит в чуть более подробном анализе конструкции Та-Шма.

Список литературы

1. Jukna S. Extremal combinatorics: with applications in computer science. — Springer, 2001.

2. Ta-Shma N. A simple proof of the Isolation Lemma. — 2015.

3. Mulmuley K., Vazirani Umesh., Vazirani Vijay. Matching is as easy as matrix inversion // Combinatorica. — 1987. — 7 (1). — P. 105–113.

4. Valiant L., Vazirani V. NP is as easy as detecting unique solutions // Theoretical Computer Science. — 1986. — 47. — P. 85–93.

МАТРОИДЫ, СВЯЗАННЫЕ С РАЗБИЕНИЯМИ МНОЖЕСТВ, И ИХ СИЛЬНЫЕ ОТОБРАЖЕНИЯ

А. М. Ревякин (Москва), А. Н. Исаченко (Минск)

Используются терминология и обозначения монографии Оксли [1]. Пусть $M = (S, I)$ — матроид на конечном множестве S с с семейством независимых множеств I и ранговой функцией $r(A)$, $A \subseteq S$, и k — натуральное число, $0 < k \leq r(S)$. Подмножество

A множества S называется замкнутым, если $r(A \cup a) > r(A)$ для каждого $a \in S \setminus A$. Семейство $L(M)$ всех замкнутых множеств матроида образует геометрическую решетку. Матроид M_k с семейством независимых множеств $I_k = \{A \subseteq S : A \in I \text{ и } |A| \leq k\}$ называется k-усечением матроида M. Ранговая функция матроида M_k равна $r_k(A) = \min\{k, r(A)\}$. Решетка замкнутых множеств M_k получается из решетки $L(M)$ вычеркиванием всех элементов ранга, большего или равного k, и заменой всех их единственным максимальным элементом решетки. Если некоторый матроид M на множестве S изоморфен $(r(H)-1)$-усечению матроида H на том же множестве S, то говорят, что H есть наращение матроида M. Решетка $L(H)$ замкнутых множеств матроида H получается из решетки $L(M)$ включением уровня новых коатомов, который лежит между старыми коатомами и единичным элементом решетки. Различные наращения матроида N на конечном множестве S, упорядоченные как антицепи булеана, образуют полную решетку, минимальный элемент FM которого называется свободным наращением матроида M. Конструкция свободного наращения и свойств наращений описаны в [2].

Введем нулевой элемент 0 ($0 \notin S$), который соответствует пустому множеству $\emptyset$ и обозначим через $\{\emptyset\}$ матроид с нулевым рангом на одноэлементном множестве $\{0\}$. Пусть матроид $M_0 = M + \{\emptyset\}$ — прямая сумма матроидов M и $\{\emptyset\}$ на множестве $S \cup 0$. Сильным отображением матроида M на множестве S в матроид N на множестве T (обозначение: $M \Rightarrow N$) называется функция $\sigma : S \cup 0 \to T \cup 0$ такая, что $\sigma(0) = 0$, и прообраз каждого замкнутого множества N_0 замкнут в M_0. Слабым отображением матроида M на множестве S в матроид N на множестве T (обозначение: $M \dashrightarrow N$) называется функция $\sigma : S \cup 0 \to T \cup 0$ такая, что $\sigma(0) = 0$ и если A подмножество множества S таково, что отображение $\sigma|A$ является взаимно однозначным на A и $\sigma(A)$ — независимое множество в матроиде N_0, то A — также независимое множество в матроиде M. Основные результаты о слабых и сильных отображениях можно найти в [3–8].

Пусть M^* — матроид, двойственный к матроиду M, а $M \cup N$ — объединение матроидов M и N на одном и том же множестве S. Тогда тождественная функция на $S \cup 0$ индуцирует сильные отображения $M \cup N \Rightarrow M$ и $M \Rightarrow M_k$. Причем, если $M \Rightarrow N$, то $M \dashrightarrow N$ (обратное неверно) и $N^* \Rightarrow M^*$. Для слабых отображений следующие условия эквивалентны: а) тождественная функция на $S \cup 0$ индуцирует $M \dashrightarrow N$; б) каждое независимое множество в N является также независимым в M; в) каждое зависимое множество в M

также зависимо в N; г) каждый цикл из M содержит цикл из N; д) $r_M(A) \geq r_N(A)$ для каждого $A \subseteq S$.

Теорема 1. *Пусть FN — свободное, а N — произвольное наращения матроида M на S. Тогда тождественная функция индуцирует слабое отображение $FN \dashrightarrow N$.*

Теорема 2. *Если $M \wedge N = (M^* \cup N^*)^*$, то $M \Rightarrow M \wedge N$.*

Матроид $M \wedge N$ из теоремы 2 называется произведением матроидов M и N.

Пусть $G = (V, E)$ — связный граф, M — его циклический матроид на E, а $\omega(v)$ — функция, заданная на вершинах графа, со значениями в некотором поле F, не равная тождественно нулю, что $\sum\limits_{v \in V} \omega(v) = 0$. Будем говорить, что двухкомпонентный лес асиметричен, если сумма весов вершин каждой его компоненты связности не равна $0 \in F$.

Теорема 3. *Асиметричные двухкомпонентные леса графа $G = (V, E)$ образуют базы некоторого матроида N на множестве ребер E и тождественная функция на $E \cup 0$ индуцирует сильное отображение циклического матроида M графа G в N.*

Теорема 4. *Пусть $M = (S, I)$ — матроид ранга k, и пусть $S = B \cup R_1 \cup R_2 \cup \ldots \cup R_p$ — разбиение множества S на попарно непересекающиеся подмножества, $r(B) = k$ и семейство I^* содержит все такие подмножества A множества B, что $A \in I$, $|A| = k - p$ и найдутся $a_i \in R_i$, для которых $A \cup \{a_1, \ldots, a_p\} \in I$. Тогда если I^* непусто, то оно образует семейство баз некоторого матроида $M_{R_1,R_2,\ldots,R_p}$ на множестве B и тождественная функция на $B \cup 0$ индуцирует сильное отображение сужения $M \setminus (R_1 \cup R_2 \cup \ldots \cup R_p)$ в матроид $M_{R_1,R_2,\ldots,R_p}$.*

Для p равных 1, 2 и 3 результат, аналогичный теореме 4, ранее получил А. Речки [8]. Приведенные в работе результаты могут быть использованы в приложениях для определения жесткости планарных ферм с удаленными фрагментами [8] и решения задач электротехники [3, 4]. При этом определение жесткости планарных ферм, состоящих из жестких стержней и соединяющих их шарниров, сводится к проверке сильной связности неких специально построенных ориентированных двудольных графов. Следовательно, минимальное число диагональных стержней, которые необходимо добавить для жесткости квадратной фермы, равно минимальному числу дуг в соответствующем сильно связном остовном подграфе двудольного графа.

Список литературы

1. Oxley J. G. Matroid theory. — N.Y.: Oxford University Press, 2006.

2. Ревякин А. М. О наращениях комбинаторных геометрий //Вестн. Моск. ун-та. Мат. Мех. — 1976. — 4. — С. 59–62.

3. Recski A. Matroid theory and its applications in electric network theory and in statics — Budapest: Akad. Kiado, 1989.

4. Revyakin A. M. Matroids // J. Math. Sci. — 2002. — V. 108, N 1. — P. 71–130.

5. Welsh D. J. A. Matroid Theory. — London: Academic Press, 1976.

6. Kung J. P. S. Strong maps // In: Theory of matroids / Ed. White N. — Cambridge Univ. Press. — 1986. — P. 224–253.

7. Kung J. P. S., Nguyen Hien Quang. Weak maps // In: Theory of matroids / Ed. White N. — Cambridge Univ. Press. — 1986. — P. 254–271.

8. Ревякин А. М., Речки А. Сильные и слабые отображения матроидов и их применение // Материалы YIII Международного семинара "Дискретная математика и ее приложения"(2–6 февраля 2004 г.) — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 219–221.

ПАРАТОПИИ ОРТОГОНАЛЬНЫХ СИСТЕМ ТЕРНАРНЫХ КВАЗИГРУПП

П. Н. Сырбу, Д. К. Чебан (Кишинев)

Понятие паратопии введено В. Д. Белоусовым в [1]. Пусть $\Sigma = \{F, E, A, B\}$ — ортогональная система, где A и B — бинарные квазигруппы, определенные на непустом множестве Q, а F и E — бинарные селекторы на Q: $F(x, y) = x$, $E(x, y) = y$, $\forall x, y \in Q$. Если $\theta : Q^2 \to Q^2$ некоторое отображение, то существуют бинарные операции C и D на Q, такие что $\theta(x, y) = (C(x, y), D(x, y))$ $\forall x, y \in Q$. Положим $\theta = (C, D)$. Отображение θ называется паратопией системы Σ, если $\Sigma\theta = \Sigma$. В. Д. Белоусов показал [1], что существуют в точности девять ортогональных систем, состоящих из двух бинарных квазигрупп и бинарных селекторов F и E, которые обладают по крайней мере одной нетривиальной паратопией. Авторы данного сообщения обобщили результат Белоусова на тернарный случай и

полностью описали ортогональные системы, состоящие из трех тернарных квазигрупп и тернарных селекторов, обладающие по крайней мере одной паратопией.

Напомним, что n-арный группоид (Q, A) называется n-арной квазигруппой, если в равенстве $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ каждый элемент множества $\{x_1, x_2, \ldots, x_{n+1}\}$ однозначно определен остальными n элементами. Если (Q, A) является n-арной квазигруппой и $\sigma \in S_n$, то операция ${}^{\sigma}A$, заданная эквивалентностью

$$ {}^{\sigma}A(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}) = x_{\sigma(n+1)} \Leftrightarrow A(x_1, x_2, \ldots, x_n) = x_{n+1} $$

для любых $x_1, x_2, \ldots, x_n, x_{n+1} \in Q$, называется парастрофом (Q, A). Парастроф ${}^{\sigma}A$ называется главным парастрофом, если $\sigma(n + 1) = n + 1$. Операции $A_1, A_2, \ldots, A_n$, арности n, определенные на множестве Q, называются ортогональными, если, для любых $a_1, a_2, \ldots, a_n \in Q$, система уравнений $\{A_i(x_1, x_2, \ldots, x_n) = a_i\}_{i=\overline{1,n}}$ разрешима однозначно. Система n-арных операций $A_1, A_2, \ldots, A_s$, определенных на множестве Q, где $s \geq n$, называется ортогональной если каждые n операций этой системы ортогональны. Для любого отображения $\theta : Q^n \to Q^n$ существуют n единственных n-арных операций $A_1, A_2, \ldots, A_n$, на Q, такие что $\theta((x_1^n)) = (A_1(x_1^n), A_2(x_1^n), \ldots, A_n(x_1^n))$, для любых $(x_1^n) \in Q^n$. Более того, отображение θ биективно тогда и только тогда, когда операции $A_1, A_2, \ldots, A_n$ ортогональны [5]. Операции $E_1, E_2, \ldots, E_n$, где $E_i(x_1, x_2, \ldots, x_n) = x_i$, для любых $x_1, x_2, \ldots, x_n \in Q$, называются n-арными селекторами на Q. n-арные квазигруппы, обладающие ортогональными n-ками парастрофов (главных парастрофов), называются парастрофно-ортогональными (самоортогональными).

Если $\Sigma = \{A_1, A_2, \ldots, A_n, E_1, E_2, \ldots E_n\}$ — ортогональная система, то систему $\{A_1\theta, A_2\theta, \ldots, A_n\theta, E_1\theta, E_2\theta, \ldots, E_n\theta\}$ обозначим через $\Sigma\theta$. Биективное отображение $\theta : Q^n \to Q^n$ называется паратопией системы Σ если $\Sigma\theta = \Sigma$.

Рассмотрим ортогональную систему $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$, где A_1, A_2, A_3 — тернарные квазигруппы определенные на непустом множестве Q и E_1, E_2, E_3 — тернарные селекторы на Q. Пусть $\theta : Q^3 \to Q^3$ — некоторое отображение, $\theta = (B_1, B_2, B_3)$, где B_1, B_2, B_3 являются тернарными операциями на Q и $\theta(x_1^3) = (B_1(x_1^3), B_2(x_1^3), B_3(x_1^3))$, для любых $(x_1^3) \in Q^3$. Если θ является паратопией системы Σ, то $\{A_1, A_2, A_3, E_1, E_2, E_3\} = \{A_1\theta, A_2\theta, A_3\theta, B_1, B_2, B_3\}$, следовательно паратопии системы Σ являются тройками операций Σ.

Мы находим необходимые и достаточные условия того, что тройка операций из Σ задает паратопию системы Σ. Так как селекторы E_1, E_2, E_3 фиксированны, мы рассматриваем тройки операций из Σ со всевозможным расположением селекторов: тройки без селекторов (один возможный случай), тройки с одним селектором и двумя квазигрупповыми операциями (9 возможных случаев, так как селектор E_i может появляться в каждой из трех позиций и $i = 1, 2, 3$), тройки с одной квазигрупповой операцией и двумя селекторами (18 возможных случаев, так как каждые два селектора могут появляться в каждых двух из трех позиций) и тройки из трех селекторов (6 возможных случаев).

Мы доказываем, что тройка операций из Σ задает паратопию системы Σ тогда и только тогда, когда квазигрупповые операции данной системы выражаются друг через друга (с помощью парастрофии и/или суперпозиции) и, в большинстве случаев, одна из квазигруп системы удолетворяет некоторому тождеству. Более того, некоторые из полученных тождеств влекут самоортогональность соответствующей тернарной квазигруппы или некоторых ее бинарных ретрастов.

Отметим что в бинарном случае существование паратопий влечет выполлнение некоторых минимальных тождеств, а именно трех из семи минимальных тождеств из классификации Белоусова-Беннетта [2]. Известно, что выполнение минимальных тождеств в бинарных квазигруппах влечет ортогональность некоторых пар парастрофов данных квазигрупп [2, 3, 6].

При исследовании необходимых и достаточных условий чтобы тройка операций из $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ задавала паратопию системы Σ, получено описание всех паратопий данной системы и найдены все ортогональные системы из трех тернарных квазигрупп и тернарных селекторов, обладающие по крайней мере одной нетривиальной паратопией.

Теорема. *Существует* 153 *ортогональных систем, состоящих из трех тернарных квазигрупп и тернарных селекторов* E_1, E_2, E_3, *обладающих по крайней мере одной нетривиальной паратопией.*

Следствие 1 [4]. *Любая тернарная квазигруппа* (Q, A) *удовлетворяющая одному из тождеств* $A(A,^{(132)} A,^{(123)} A) = E_2$ *или* $A(A,^{(132)} A,^{(123)} A) = E_3$, *является самоортогональной типа* $(\varepsilon, (132), (123))$.

Следствие 2. *Если тернарная квазигруппа* (Q, A) *удовлетворяет тождеству* $A(E_1, A,^{(23)} A) = E_3$ *то, для* $\forall a \in Q$, *его* 1*-ретракт* $B_a(x, y) = A(a, x, y)$ *является самоортогональным.*

Следствие 3. *Если тернарная квазигруппа* (Q, A) *удовлетворяет тождеству* $A(A, E_2, {}^{(13)}A) = E_3$ *то, для* $\forall a \in Q$, *его* 2*-ретракт* $B_a(x, y) = A(x, a, y)$ *вляется самоортогональным.*

Следствие 4. *Если тернарная квазигруппа* (Q, A) *удовлетворяет тождеству* $A(A, {}^{(12)}A, E_3) = E_2$ *то, для* $\forall a \in Q$, *его* 3*-ретракт* $B_a(x, y) = A(x, y, a)$ *вляется самоортогональным.*

Список литературы

1. Белоусов В. Д. Системы ортогональных операций // Матем. сборник. — 1968. — 77 (119). — С. 33–52.

2. Belousov V. Parastrofic-orthogonal quasigroups // Quasigroups and Related Systems. — 2005. — 14. — P. 3–51.

3. Bennett F.E. Quasigroups identities and Mendelsohn designs // Canad. J. Math. — 1989. — 41 (2). — P. 341–368.

4. Evans T. Latin cubes orthogonal to their transposes — a ternary analogue of Stein quasigroups // Aequationes Math. — 1973. — 9. P. 296–297.

5. Сырбу П.Н. Об ортогональных и самоортогональных n-арных операциях // Матем. исслед. — 1987. — 66. — С. 121–129.

6. Syrbu P., Ceban D. On π-quasigroups of type T_1 // Bul. Acad. Stiinte Repub. Mold. Mat. — 2014. — 2. — P. 36–43.

О КОМБИНАТОРНОМ ТОЖДЕСТВЕ HAJNAL—NAGY

С. П. Тарасов (Москва)

Решеточным путем называется путь из шагов $(1, 1), (1, -1)$ по целым точкам двумерной целочисленной решетки. Число шагов пути называется *длиной* пути. *Путем Дика* называется решеточный путь (четной длины), который стартует из начала координат, проходит только по точкам с неотрицательными ординатами и заканчивается на оси абсцисс (но не пересекает ее).

Назовем *профилем* любую конечную $\{0, 1\}$-последовательность. Будем говорить, что решеточный путь *согласован* с профилем $[b_0\, b_1 \ldots]$, $b_i \in \{0, 1\}$, если он не проходит через точки из множества $\{(2i, 0) \mid b_i = 0\}$.

Обозначим $\mathcal{P}[(1^k0^k)^n1] = \mathcal{P}[\underbrace{1^k0^k\ldots1^k0^k}_{n\text{ раз}}1]$ множество всех решеточных путей длины $4kn$, которые начинаются в начале координат и согласованы с профилем $(1^k0^k)^n1$. В [1] высказана гипотеза, что справедливо тождество $|\mathcal{P}[(1^k0^k)^n1]| = |\mathcal{P}[\underbrace{1^k0^k\ldots1^k0^k}_{n\text{ раз}}1]| = 4^{4kn-n}B_n$, где $B_n = \binom{2n}{n}$. Мы показываем справедливость этого тождества для небольших k. Для этого выписывается система уравнений относительно производящих функций соответствующих решеточных путей с ограничениями, которую удается решить для небольших значений k.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 14-01-00641.

Список литературы

1. P. Hajnal P., Nagy G.V. A bijective proof of Shapiro's Catalan convolution // The electronic journal of combinatorics. — 2014. — 21 (2). — P. 2–42.

О МИНИМАЛЬНОМ МНОГОЧЛЕНЕ МАТРИЦЫ ОГРАНИЧЕНИЙ МНОГОИНДЕКСНОЙ ТРАНСПОРТНОЙ ЗАДАЧИ

Е. Б. Титова, В. Н. Шевченко (Нижний Новгород)

Будем использовать следующие обозначения: $\mathbf{1}^{p\times q}$ — $p \times q$-матрица, каждый элемент которой равен 1, E_n — единичная матрица n-го порядка; A — целочисленная $m \times n$-матрица ($m \le n$), $r(A)$ — ее ранг, $A^\top$ — матрица, транспонированная к A, $A \times B$ — кронекерово произведение матриц A и B (определение и свойства см., например, в [1]).

Традиционная мера сложности для многоиндексных транспортных многогранников (Тр) — рост миноров в матрицах ограничений этих задач [2, 3]. Здесь делается попытка в качестве меры сложности рассматривать степень минимального многочлена этой матрицы.

Рассмотрим двухиндексный Тр, являющийся множеством неотрицательных решений системы линейных уравнений:

$$\sum_{j_1=1}^{n_1} x_{j_1 j_2} = b_{0 j_2},\ \sum_{j_2=1}^{n_2} x_{j_1 j_2} = b_{j_1 0}. \tag{1}$$

Ее можно обобщить на случай трехиндексного Тр двумя способами: в первом число суммирований $s = 1$ (планарный Тр) и

$$\sum_{j_1=1}^{n_1} x_{j_1 j_2 j_3} = b_{0 j_2 j_3},\ \sum_{j_2=1}^{n_2} x_{j_1 j_2 j_3} = b_{j_1 0 j_3},\ \sum_{j_3=1}^{n_3} x_{j_1 j_2 j_3} = b_{j_1 j_2 0},$$

во втором число суммирований $s = k - 1 = 2$ (аксиальный Тр) и

$$\sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2} x_{j_1 j_2 j_3} = b_{00 j_3},\ \sum_{j_1=1}^{n_1}\sum_{j_3=1}^{n_3} x_{j_1 j_2 j_3} = b_{0 j_2 0},\ \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3} x_{j_1 j_2 j_3} = b_{j_1 00}.$$

Используя кронекерово произведение систему (1) можно записать в виде:

$$T_{12}(n_1, n_2) = \begin{pmatrix} E_{n_1} \times \mathbf{1}^{1\times n_2} \\ \hline \mathbf{1}^{1\times n_1} \times E_{n_2} \end{pmatrix}.$$

Для матрицы $T_{12}(n_1, n_2)T_{12}^{\top}(n_1, n_2)$ характеристический многочлен имеет вид

$$\det(\lambda E_{n_1+n_2} - T_{12}T_{12}^{\top}) = \lambda(\lambda - n_1)^{(n_2-1)}(\lambda - n_2)^{(n_1-1)}(\lambda - (n_1 + n_2)),$$

для матрицы $T_{12}^{\top}(n_1, n_2)T_{12}(n_1, n_2)$ —

$$\det(\lambda E_{n_1 n_2} - T_{12}^{\top}T_{12}) = \lambda^{(n_1 n_2 - n_1 - n_2 + 1)}(\lambda - n_1)^{(n_2-1)}(\lambda - n_2)^{(n_1-1)}\cdot$$

$$\cdot(\lambda - (n_1 + n_2)),$$

а минимальный многочлен $\delta(\lambda, T_{12}(n_1, n_2))$ для обоих случев совпадает и при $n_1 \neq n_2$ имеет максимальную степень $d_{12}(n_1 \neq n_2) = 4$:

$$\delta(\lambda, T_{12}(n_1, n_2)) = \lambda(\lambda - n_1)(\lambda - n_2)(\lambda - (n_1 + n_2)),$$

при $n_1 = n_2 = n$ — минимальную степень $d_{12}(n_1 = n_2) = 3$:

$$\delta(\lambda, T_{12}(n)) = \lambda(\lambda - n)(\lambda - 2n).$$

При переходе к k индексам (широкий спектр прикладных задач, получаемых таким образом, см., например, в [4]) с неотрицательными переменными $x_J = x_{j_1 \ldots j_k}$ первый блок Тр с s суммированиями имеет вид

$$\sum_{j_1=1}^{n_1} \ldots \sum_{j_s=1}^{n_s} x_{j_1,\ldots,j_k} = b_{0\ldots 0 j_{s+1}\ldots j_k},$$

а соответствующая матрица ограничений имеет вид $T_{I_1}(n_1,\ldots,n_k) = \mathbf{1}^{1\times n_1}\times\ldots\times\mathbf{1}^{1\times n_s}\times E_{n_{s+1}}\times\ldots\times E_{n_k}$. Если рассмотреть все возможные варианты суммирования и лексикографически упорядочить индексы переменных $x_{j_1,\ldots,j_k}$ и правых частей уравнений, то матрица ограничений $T_{sk}(n_1,\ldots,n_k)$ k-индексной задачи с s суммированиями будет иметь следующее рекурсивное задание:

$$T_{s,k}(n_1,\ldots,n_k) = \left[\begin{array}{ccc} T_{s,k-1}(n_1,\ldots,n_{k-1}) & \times & E_{n_k} \\ \hline T_{s-1,k-1}(n_1,\ldots,n_{k-1}) & \times & \mathbf{1}^{1\times n_k} \end{array}\right].$$

Матрица $T_{sk}(n_1,\ldots,n_k)$ состоит из $\binom{k}{s}$ строчечных блоков, число ее столбцов $N = \prod_{i=1}^{k} n_i$, строк $M = \sigma_{k-s}(n_1,...,n_k)$, ранг $r = \sum_{i=s}^{k}\sigma_{k-i}(n_1-1,...,n_k-1)$. В [5] получен характеристический многочлен матрицы $T_{sk}(n_1,\ldots,n_k)^{\top}T_{sk}(n_1,\ldots,n_k)$. Отсюда при $n_1 = \ldots = n_k = n$ легко выписывается минимальный многочлен

$$\delta(\lambda, T_{sk}(n)) = \lambda\prod_{j=s}^{k}(\lambda - \binom{j}{s}n^s).$$

Утверждение 1. *Минимальная степень* $d_{sk}(n_1 = \ldots = n_k \geq 2) = k - s + 2$, *максимальная* $d_{sk}(n_1 \neq \ldots \neq n_k \neq 1) = 1 + \prod_{i=s}^{k}\binom{k}{s}$.

Матрицу T назовем α-модулярой, если в любой базисной системе столбцов все миноры порядка r равны $\pm\alpha$. В таком случае задача проверки пустоты транспортного многогранника имеет эффективный алгоритм. Для $T_{13}(n_1,n_2,n_3)$ свойство α-модулярности доказано в [6].

Утверждение 2. *Матрица* $T_{1k}(n_1,n_2,n_3,2\ldots,2)$ — *α-модулярна.*

Хорошо известно, что для матриц $T_{sk}(n_1,\ldots,n_k)$ при $s \geq 2$ утверждение 2 не верно [2].

Список литературы

1. Воеводин В. В., Кузнецов Ю. А. СМБ. Матрицы и вычисления. — М.: Наука, 1984.

2. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

3. Титова Е. Б., Шевченко В. Н. О минорах матрицы ограничений многоиндексных транспортных задач // Дискретная математика. — 2012. — Т. 24, вып. 4. — С. 147–157.

4. Раскин Л. Г., Кириченко И. О. Многоиндексные задачи линейного программирования. — М.: Радио и связь, 1982.

5. Шевченко В. Н. Характеристические многочлены многоиндексных транспортных задач // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 83–88.

6. Ильичёв А. П. Исследование многогранников многоиндексных транспортных задач: Автореферат дис. канд. физ.-мат. наук. — Горький, 1988.

О НЕЗАВИСИМЫХ СЕМЕЙСТВАХ МНОЖЕСТВ В ЗАДАЧЕ О ПОКРЫТИИ

И. П. Чухров (Москва)

Комбинаторная постановка задачи о покрытии конечного множества заключается в нахождении семейства допустимых подмножеств минимальной сложности, которое содержит все элементы множества.

Системой множеств называется пара $\langle X, Y\rangle$, где X — конечное множество элементов и $Y \subseteq 2^X$ — *семейство* различных множеств.

Множество элементов X, которые содержатся в произвольном семействе множеств $S \subseteq Y$, обозначим через X_S. Будем говорить, что семейство S *покрывает* множество элементов X_S.

Покрытием для системы множеств $\langle X, Y\rangle$ называется любое семейство $S \subseteq Y$, которое покрывает все множество X. Для существования покрытия семейство Y должно покрывать все множество X.

Сложность произвольного семейства множеств $S \subseteq Y$ определяется неотрицательным аддитивным функционалом $C\colon Y \to R^+$, который задает сложность множеств из Y, и соотношением $C(S) = \sum_{y\in S} C(y)$, определяющим сложность семейства S.

Стандартная задача о покрытии $Z = \langle X, Y, C\rangle$ заключается в нахождении семейства $S \subseteq Y$, которое является покрытием X и имеет

минимальную сложность $C(S)$. Сложность минимального покрытия в задаче $Z = \langle X, Y, C\rangle$ обозначим через $C(X, Y)$.

Если сложность любого множества равна 1 и сложность любого семейства равна его мощности, то функционал сложности называется *длиной* и обозначается через l.

Различные оптимизационные задачи для дискретных структур могут быть сформулированы как задачи о покрытии обобщенного вида. При этом может требоваться покрыть заданное подмножество элементов, а система множеств и функционал сложности могут удовлетворять ограничениям, которые порождаются свойствами структур, например, графа, булева куба и т. д. Следующие задачи обобщенного вида могут быть сведены к стандартной задаче о покрытии множества.

(i) Задача $Z_A = \langle A, X, Y, C\rangle$, где $A \subset X$, заключается в нахождении семейства $S \subseteq Y$ минимальной сложности, которое *покрывает* A, т. е. $A = X_S$.

(ii) Задача $\tilde{Z}_A = \langle A, X, Y, C\rangle$, где $A \subset X$, заключается в нахождении семейства $S \subseteq Y$ минимальной сложности, которое *содержит* A, т.е. $A \subseteq X_S$.

(iii) Задача $\tilde{Z}_{A,B} = \langle A, B, X, Y, C\rangle$, где $A \subset X$, $B \subset X$ и $A \cap B$ — пусто, заключается в нахождении семейства $S \subseteq Y$ минимальной сложности, для которого $A \subseteq X_S \subseteq A \cup B$.

Задача минимизации булевых функций относительно аддитивной меры сложности $\mathcal{L}$ в геометрической интерпретации [1] является задачей о покрытии для системы множеств $\langle B^n, G^n\rangle$, где B^n — множество вершин, G^n — множество граней n-мерного единичного куба и сложность комплекса граней равна сумме сложностей граней. Задаче минимизации всюду определенной булевой функции соответствует задача $Z_A = \langle N_f, B^n, G^n, \mathcal{L}\rangle$, а частично определенной булевой функции соответствует задача $\tilde{Z}_{A,B} = \left\langle N_f, N_{\tilde{f}}, B^n, G^n, \mathcal{L}\right\rangle$, где $A = N_f$ и $B = N_{\tilde{f}}$ — множества единичных и неопределенных вершин функции f в кубе B^n соответственно.

В обзорных статьях [2, 3] изложены различные алгоритмические вопросы и подходы к решению задачи о покрытии, которые характерны для многих трудных дискретных оптимизационных задач.

Предлагаемый метод получения нижних оценок длины и сложности минимальных покрытий основан на обобщении понятия независимого множества элементов.

Определение. *Независимым семейством множеств для системы множеств* $\langle X, Y\rangle$ *называется семейство* $\mathcal{A} = \{A \mid A \subset X\}$,

если любое множество $y \in Y$ пересекается не более чем с одним множеством $A \in \mathcal{A}$.

Независимое множество элементов является частным случаем независимого семейства множеств, в котором каждое множество состоит из одного элемента. Независимыми семействами множеств являются семейства, которые соответствуют компонентам связности или состоят из двух множеств: собственных элементов всех ядровых множеств и элементов, которые не содержатся в ядровых множествах.

Лемма 1. *Если $\mathcal{A}$ является независимым семейством для системы множеств $\langle X, Y\rangle$, то для любого аддитивного функционала сложности C выполняется $C(X,Y) \geq \sum\limits_{A\in\mathcal{A}} \tilde{C}(A,X,Y)$, где $\tilde{C}(A,X,Y)$ — сложность минимального покрытия для задачи $\tilde{Z}_A$.*

Лемма 2. *Для задачи $\tilde{Z}_A = \langle A, X, Y, C\rangle$ справедливы оценки*

$$\tilde{l}(A,X,Y) \geq \tilde{l}_{X,Y,A} = \lceil |A|/\Delta_{X,Y,A}\rceil,\ \tilde{C}(A,X,Y) \geq \tilde{C}_{X,Y,A},$$

где $\Delta_{X,Y,A}$ — максимальное число элементов множества A, которые содержатся в одном множестве семейства Y; $\tilde{C}_{X,Y,A}$ — сложность $\tilde{l}_{X,Y,A}$ множеств из Y, которые пересекаются с множеством A и имеют меньшую сложность.

Независимое семейство множеств может быть представлено в виде объединения независимого множества элементов, возможно пустого, и независимого семейства множеств среди которых нет независимых множеств элементов.

Теорема 1. *Если $\{Q\} \cup \mathcal{A}$ является независимым семейством для системы множеств $\langle X, Y\rangle$, где Q — независимое множество и в семействе $\mathcal{A}$ нет независимых множеств, то для аддитивного функционала сложности выполняется*

$$l(X,Y) \geq |Q| + \sum_{A\in\mathcal{A}} \lceil |A|/\Delta_{X,Y,A}\rceil,$$

$$C(X,Y) \geq \sum_{x\in Q} \tilde{C}_{X,Y,\{x\}} + \sum_{A\in\mathcal{A}} \tilde{C}_{X,Y,A}.$$

Оценки теоремы 1, в случае их достижимости, являются достаточными условиями минимальности покрытия и используются при доказательстве следующей теоремы.

Теорема 2. *Для задачи минимизации булевых функций*

(i) при $n \leq 3$ для всех функций длина кратчайшего покрытия совпадает с мощностью максимального независимого множества;

(ii) при $n \geq 5$ существуют функции, для которых длина кратчайшего покрытия больше мощности максимального независимого

множества.

Работа выполнена при финансовой поддержке РФФИ (проект 16-01-00593а).

Список литературы

1. Чухров И. П. О мерах сложности комплексов граней в единичном кубе // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 6. — С. 77–94.

2. Еремеев А. В., Заозерская Л. А., Колоколов А. А. Задача о покрытии: сложность, алгоритмы, экспериментальные исследования // Дискретный анализ и исследование операций. — 2000. — Серия 2, Т. 7, № 2. — С. 22–46.

3. Coudert O., Sasao T. Two-level logic minimization // Logic synthesis and verification — Norwell, MA, USA: Kluwer Academic Publishers — 2002. — P. 1–27.

ЦИКЛЫ В ЛИНЕЙНОМ И ЦЕЛОЧИСЛЕННОМ ЛИНЕЙНОМ ПРОГРАММИРОВАНИИ

В. Н. Шевченко (Нижний Новгород)

Будем использовать следующие бозначения: $\mathbf{Z}$ — кольцо целых чисел, $\mathbf{R}$ — поле вещественных чисел, если $M \subseteq \mathbf{R}$, то M^n — множество n-мерных столбцов x с координатами $x_j \in M$; при $x \in M^n, y \in M^n$ $x \leq y \Leftrightarrow x_j \leq y_j (j = 1, \ldots, n) \Leftrightarrow y \geq x$; $x < y \Leftrightarrow x_j < y_j (j = 1, \ldots, n) \Leftrightarrow y > x$. Аналогично определяется множество $M^{s \times t}$ матриц и отношения $''\geq''$ и $''>''$ на нем. Через $r(A)$ обозначим ранг матрицы A, а через A^T — матрицу, транспонированную к A.

Рассмотрим пару двойственных задач ЛП:

$$\begin{array}{ccccc} \max & & cx & & \\ x & \geq & 0 & \text{и} & \\ Ax & \leq & b & & \end{array} \qquad \begin{array}{ccccc} \min & & ub & & \\ uA & \geq & c & , & \\ u & \geq & 0 & & \end{array}$$

соответствующую этой паре кососимметрическую матрицу

$$K(A) = \begin{pmatrix} 0 & A^T \\ -A & 0 \end{pmatrix},$$

а также окаймляющие ее матрицы

$$K_{00}(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & A^T \\ 0 & -A & 0 \end{pmatrix}, \quad K_{01}(A) = \begin{pmatrix} 0 & c & 0 \\ -c^T & 0 & A^T \\ 0 & -A & 0 \end{pmatrix},$$

$$K_{10}(A) = \begin{pmatrix} 0 & 0 & -b^T \\ 0 & 0 & A^T \\ b & -A & 0 \end{pmatrix}, \; K_{11}(A) = \begin{pmatrix} 0 & c & -b^T \\ -c^T & 0 & A^T \\ b & -A & 0 \end{pmatrix}.$$

Положим при $\mu \in \{0,1\}$, $\nu \in \{0,1\}$ $r_{\mu\nu}(m,n) = r(K_{\mu\nu}(A))$. Хорошо известно [1], что для любой кососимметрической матрицы K множество $C(K) = \{z : z \geq 0, Kz \geq 0, z + Kz > 0\}$ не пусто и что [2] каждый из векторов $z \in C(K_{11})$ решает обе задачи линейного программирования. Отсюда следует, что задача линейного программирования и основная задача теории линейных неравенств — нахождение решения системы линейных неравенств или доказательство его отсутствия — имеют одинаковую сложность. Так же хорошо известно [2], что данный факт не верен для задач целочисленного линейного программирования. Если рассматриваемый вектор z единственный, то обозначим его $z_{opt} = (t; x; u)^T \in \mathbf{Z}^{(m+n+1)\times 1}$. Алгоритмы, вычисляющие $z_{opt}(K_{11})$ по известному $z_{opt}(K_{00})$, назовем циклическими. Будем считать далее, что $r_{00}(m,n)$ остался неизменным.

Для $d \times n$-матрицы B со столбцами b_j $(j = 1, 2, \ldots, n)$ обозначим через $B^{\angle} = \{\sum_{j=1}^{n} b_j y_j \; y_j \geq 0\}$ множество неотрицательных линейных комбинаций ее столбцов и предположим, что $B^{\angle}$ совпадает со множеством решений системы $\sum_{k=1}^{d} a_{ik} x_k \geq 0$ $(i = 1, \ldots, m)$.

Триангуляцией конуса K с узлами из множества B назовем множество $T(B) = \{S_1, \ldots, S_t\}$ таких S_τ, для которых выполнены следующие условия: 1) $S_\tau \subseteq \{1, \ldots, n\}$, 2) $|S_\tau| = r = \operatorname{rank} B(S_\tau)$, 3) $B^{\angle} = \bigcup_{\tau=1}^{t} B^{\angle}(S_\tau)$, 4) $B^{\angle}(S_\tau) \cap B^{\angle}(S_\sigma) = B^{\angle}(S_\tau \cap S_\sigma)$.

Множество $\triangle(T(B)) = \bigcup_{\tau=1}^{t} \Gamma(S_\tau)$ дает пример геометрической реализации d-мерного однородного симплициального комплекса (с. к.). Обозначим через $\triangle_k = \bigcup_{\tau=1}^{t} \Gamma_k(S_\tau)$ $(k = 0, \ldots, d)$ множество k-мерных граней с. к. $\triangle$, положим $f(\triangle) = (f_0(\triangle), \ldots, f_d(\triangle))$, $f_k(\triangle) = |\triangle_k|$ и $f(\lambda, \Delta) = \sum_{k=0}^{d} f_k(\Delta)\lambda^k$.

Следуя [3], представим многочлен $f(\lambda, \Delta)$ в виде

$$f(\lambda, \Delta) = \sum_{k \in \mathbf{Z}_+} \gamma_k(\Delta)\lambda^k (1+\lambda)^{d-k}$$

и назовем целочисленную последовательность $\gamma = (\gamma_0, \gamma_1, \dots)$ (d,n)-реализуемой, если $\gamma_k = \gamma_k(\Delta)$ при $k = 0, 1, \dots, d$ и $\gamma_k = 0$ при $k > d$.

Для любых натуральных чисел a и i существует единственное биномиальное i-разложение числа $a = \binom{a_i}{i} + \binom{a_{i-1}}{i-1} + \dots + \binom{a_j}{j}$, где $a_i > a_{i-1} > \dots > a_j \geq j \geq 1$. Тогда число $a^{<i>} = \binom{1+a_i}{1+i} + \dots + \binom{1+a_j}{1+j}$ называется i-й псевдостепенью числа a.

Теорема 1. 1. *Если найдется такое k, при котором $\gamma_{k+1} > \gamma_k^{<k>}$, то последовательность γ не реализуема ни при каком d.*

2. *Если $\gamma_{k+1} \leq \gamma_k^{<k>}$ при $k = 1, \dots, d-1$ (условия Маколея—Макмюллена—Стенли* [4]*), то последовательность γ — $(2d)$-реализуема.*

Следующая теорема позволяет находить минимальное d, при котором последовательность γ является d-реализуемой.

Теорема 2. *Для d-реализуемости целочисленной последовательности $\gamma = (\gamma_0, \gamma_1, \dots)$ необходимо и достаточно, чтобы выполнялись следующие условия:*
1) $\gamma_0 = 1$, $\gamma_i \geq 0$ *при* $i = 1, \dots, d$ *и* $\gamma_k = 0$ *при целых* $k \geq d$,
2) $\gamma_i \geq \gamma_{d-i} \leq \gamma_{d-i-1}$ *при* $i = 1, \dots, \lfloor \frac{d}{2} \rfloor$ *("овраг")*
3) $\gamma_{i+1} - \gamma_{j-i} \leq (\gamma_i - \gamma_{j+1-i})^{<i>}$ *при* $j = d, \dots, 2d$ *и* $i = 1, \dots, \lfloor \frac{j}{2} \rfloor$.

Следствие 1. $f(\lambda, \Delta) = \sum_{k=0}^{d+1} \gamma_k(\Delta) \lambda^k (1+\lambda)^{d+1-k}$, *где* $\gamma_k(\Delta) = |\{\tau \mid \dim J_\tau = k-1\}|$ — *целое неотрицательное число, не зависящее от порядка следования симплексов* $S_1, \dots, S_t$, $\gamma_0(\Delta) = 1$ *и* $\gamma_{d+1}(\Delta) = 0$.

Таким образом, $\partial\Delta = \bigcup_{i=1}^{m_1} \Gamma(F_i)$, а для остальных граней из Δ несложно доказать, что $\Delta \setminus \partial\Delta = \bigcup_{\tau=1}^{t} [\overline{J_\tau}, S_\tau]$, где объединение дизъюнктно и $\overline{J_\tau}$ — множество вершин симплекса S_τ, дополнительное к J_τ.

Следствие 2. $f(\lambda, \Delta \setminus \partial\Delta) = \sum_{k=0}^{d+1} \gamma_k(\Delta) \lambda^{d+1-k} (1+\lambda)^k$, $f(\lambda, \partial\Delta) = \sum_{k=0}^{\delta} (\gamma_k(\Delta) - \gamma_{d+1-k}(\Delta))(\lambda^k (1+\lambda)^{d+1-k} - \lambda^{d+1-k}(1+\lambda)^k)$.

При небольших d для любых n полученные условия легко проверяемы. То же верно при любых d, если n ограничено сверху полиномом от d. Этим удалось воспользоваться для формулировки следующей гипотезы.

Гипотеза. *Пусть $\Gamma(d,n)$ — множество γ-векторов d-мерных политопов с n вершинами, $\Gamma'(d,n)$ — аналогичное множество для симплициальных политопов, $\Gamma''(d,n)$ — аналогичное множество для простых политопов,* $\mathrm{conv}(M)$ — *выпуклая оболочка множе-*

ства M. Тогда

$$\Gamma(d,n) = \boldsymbol{Z}^d \bigcap \mathrm{conv}(\Gamma'(d,n) \bigcup \Gamma''(d,n)).$$

При $d = 3$ эта гипотеза доказана Штейницем [4].

Список литературы

1. Воеводин В. В., Кузнецов Ю. А. СМБ. Матрицы и вычисления. — М.: Наука, 1984.

2. Схрейвер А. Теория линейного и целочисленного программирования. — М.: Мир, 1991.

3. Шевченко В. Н. О разбиении политопа на симплексы без новых вершин. // Известия ВУЗ. Математика. — 1997. — №12 (427). — С. 89–99.

4. Ziegler G. Lectures on polytopes. — Berlin: Springer-Verlag, 1995.

5. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

Секция «Теория графов»

О ДИСТАНЦИОННЫХ КОДАХ ГРЕЯ

И. С. Быков, А. Л. Пережогин (Новосибирск)

Определим *n-мерный код Грея* как циклическую последовательность всех 2^n бинарных слов длины n такую, что два соседних слова отличаются ровно в одном символе. Любому n-мерному коду Грея соответствует гамильтонов цикл в графе Q_n. *Переходная последовательность* пути $v_1, v_2, \ldots, v_{m+1}$ в Q_n — это слово $T = (\tau_1, \tau_2, \ldots, \tau_m)$ над алфавитом $\{1, 2, \ldots, n\}$ такое, что τ_i — направление ребра (v_i, v_{i+1}) (в случае, если путь замкнутый, считаем слово T циклическим). Необходимое и достаточное условие того, что символьная последовательность является переходной последовательностью гамильтонова цикла (кода Грея) хорошо известно и приводится, например, в [1].

Коды Грея имеют многочисленные практические применения [2]. При этом возникают вопросы о существовании и построении кодов Грея, обладающих заданными свойствами. Одним из таких свойств является локальная равномерность переходной последовательности кода, которая обеспечивает равномерное изнашивание контактов в реальных устройствах, использующих эти коды [3]. Ранее рассматривались следующие параметры равномерности:

• $l_1(G)$ — такое максимальное число, что в каждом подслове длины $l_1(C)$ переходной последовательности кода C все буквы различны; наибольшее значение, которое параметр $l_1(C)$ принимает на множестве всех n-мерных кодов Грея обозначим $l_1(n)$;

• $l_2(G)$ — такое минимальное число, что в каждом подслове длины $l_2(C)$ переходной последовательности кода C встречаются все буквы из алфавита $\{1, 2, \ldots, n\}$; наименьшее значение, которое параметр $l_2(C)$ принимает на множестве всех n-мерных кодов Грея обозначим $l_2(n)$.

Лучшие известные оценки для $l_1(n)$ и $l_2(n)$ [4, 5]:

$$n - \lceil 2.001 \log n \rceil \le l_1(n) \le n - 1;$$

$$n+1 \le l_2(n) \le n+3\lceil \log n \rceil.$$

Другим возможным свойством кода Грея является антиподальность; n-мерный код Грея называется (n,t)-*антиподальным*, если противоположные двоичные слова находятся на расстоянии t в коде. Антиподальные коды Грея изучались в [6, 7]. В частности, в [7] показано, что для любого четного n существует $(n, 2^{n-1})$-антиподальный код Грея.

Рассмотрим класс кодов Грея, со свойством, в некотором смысле обобщающим понятие равномерности и антиподальности. Назовем n-мерный код $\langle d,k\rangle_n$-*дистанционным кодом Грея*, если расстояние Хэмминга между словами, находящимися в коде на расстоянии k, равно d. Далее для краткости такой код будем называть $\langle d,k\rangle_n$-кодом Грея. Справедливы следующие утверждения:

Утверждение. *Код C является $\langle d,d\rangle_n$-кодом тогда и только тогда, когда $l_1(C) \ge d$. В частности, код C является $\langle n-1,n-1\rangle_n$-кодом тогда и только тогда, когда $l_1(C) = n-1$.*

Утверждение. *Если для кода C выполнено $l_2(C) = n+1$, то код C является $\langle n-1,n+1\rangle_n$-кодом.*

Для существования $\langle d,k\rangle_n$-кода необходимо, чтобы d и k были одной четности, а также $d \le k$.

Утверждение. *При $1 < k < 2^n - 1$ не существует $\langle 1,k\rangle_n$-кода Грея.*

Утверждение. *$\langle n,k\rangle_n$-код Грея существует тогда и только тогда, когда n — четное число и $k = 2^{n-1}$.*

Теорема. *Следующие дистанционные коды Грея существуют:*
1) $\langle 2, 2^k - 2^t\rangle_n$ *при* $t < k \le n$;
2) $\langle d, 2^{t+d-1}\rangle_n$ *при четном* d *и* $n \ge d+t$;
3) $\langle d, 2^{t+d-1} - 2^t\rangle_n$ *при четном* d *и* $n \ge d+t$;
4) $\langle d, 2^t d\rangle_n$ *при четном* d *и* $d \le l_1(n-t)$;
5) $\langle d+1, 2^t d\rangle_n$ *при нечетном* d *и* $d \le l_1(n-t)$.

Для улучшения верхней оценки $l_1(n)$ и нижней оценки $l_2(n)$, которые являются тривиальными, особый интерес представляют дистанционные коды Грея при $d = n-1$:

Теорема. *Пусть n — четное число. $\langle n-1,k\rangle_n$-код Грея существует тогда и только тогда, когда существует $\langle n-1,k'\rangle_n$-код Грея, где $k \cdot k' \equiv 1 (\mathrm{mod}\ 2^n)$.*

Доказательство. Пусть $Q_n^{(n-1)}$ — граф на множестве двоичных слов длины n, в котором ребром соединены два слова, расстояние Хэмминга между которыми равно $n-1$. Заметим, что при четном n

существует изоморфизм $\varphi : Q_n^{(n-1)} \to Q_n$:

$$\varphi(v) = \begin{cases} v, \text{если вес } v \text{ четный} \\ \overline{v}, \text{иначе.} \end{cases}$$

Пусть $C = v_0, v_1, v_2, \ldots, v_{2^n-1}$ — $\langle n-1, k\rangle_n$-код Грея. Тогда цикл

$$C' = \varphi(v_0), \varphi(v_k), \varphi(v_{2k}), \ldots, \varphi(v_{(2^n-1)k})$$

является $\langle n-1, k'\rangle_n$-кодом Грея. Теорема доказана.

Следствие. *Пусть n — четное число. Если для некоторых k и k', удовлетворяющих $k \cdot k' \equiv 1(\mod 2^n)$, выполнено $k < n-1$, то $\langle n-1, k'\rangle_n$-код Грея не существует.*

Теорема. *Пусть $k = 2^p(2m+1)$ и $(2m+1) \cdot k' \equiv 1(\mod 2^{n-p})$. Если $\frac{n-2^p}{d} > k'$, то $\langle n-d, k\rangle_n$-код Грея не существует.*

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 14-01-00507).

Список литературы

1. Пережогин А. Л. Об автоморфизмах циклов в n-мерном булевом кубе // Дискретный анализ и исследование операций. — 2007. — Вып. 14. — С. 67–79.

2. Savage C. A Survey of Combinatorial Gray Codes // SIAM Review. — 1996. — Vol. 39. — P. 605–629.

3. Goddyn L., Lawrence G. M., Nemeth E. Gray codes with optimized run lengths // Utilitas Mathematica. — 1988. — Vol. 34. — P. 179–192.

4. Goddyn L., Gvozdjak P. Binary gray codes with long bit runs // The Electronic Journal of Combinatorics. — 2003. — Vol. 10.

5. Быков И. С. О равномерных кодах Грея // Дискретный анализ и исследование операций. — 2016. — Вып. 23. — С. 51–64.

6. Killian C., Savage C., Antipodal Gray Codes // Discrete Mathematics. — 2002. — Vol. 281. — P. 221–236.

7. Chang G. J., Eu S.-P., Yeh C.-H. On the (n, t)-antipodal Gray codes // Theoretical Computer Science. — 2007. — Vol. 374 (1–3). — P. 82–90.

МИНИМАЛЬНЫЕ НОСИТЕЛИ СОБСТВЕННЫХ ФУНКЦИЙ ГРАФОВ ХЭММИНГА

А. А. Валюженич (Новосибирск)

Расстоянием Хэмминга $d(x, y)$ между словами x, y из множества $\{0, 1, \ldots, q-1\}^n$ называется число позиций, в которых x и y различны. *Графом Хэмминга* называется граф, вершины которого — это все слова длины n над алфавитом $\{0, 1, \ldots, q-1\}$, а ребрами графа соединяются вершины на расстоянии Хэмминга 1. Обозначим граф Хэмминга через $H(n, q)$. Хорошо известно, что множество собственных значений матрицы смежности графа $H(n, q)$ — это $\{\lambda_m = n(q-1) - qm | m = 0, 1, \ldots, n\}$. Функция $f : H(n, q) \longrightarrow \mathbb{R}$ называется *собственной функцией* графа $H(n, q)$, отвечающей собственному значению λ, если $Af = \lambda f$, где A — матрица смежности $H(n, q)$. Пусть $f : H(n, q) \longrightarrow \mathbb{R}$. Множество $S(f) = \{x \in H(n, q) | f(x) \neq 0)\}$ называется *носителем функции* f. Для носителя собственной функции известна следующая нижняя оценка:

Теорема [1]. *Пусть* $f : H(n, q) \longrightarrow \mathbb{R}$ *— собственная функция, отвечающая собственному значению* λ_m *и* $f \not\equiv 0$. *Тогда*

$$|S(f)| \geq 2^m (q-2)^{n-m}$$

для $\frac{mq^2}{2n(q-1)} > 2$ *и*

$$|S(f)| \geq q^n (\frac{1}{q-1})^{m/2} (\frac{m}{n-m})^{m/2} (1 - \frac{m}{n})^{n/2}$$

для $\frac{mq^2}{2n(q-1)} \leq 2$.

Из результатов работы [2] следует, что для мощности носителя собственной функции $f : H(n, q) \longrightarrow \{-1, 0, 1\}$, отвечающей собственному значению $\lambda = q(n-m) - n$, выполнена нижняя оценка $|S(f)| \geq 2^m$.

В данной работе найдены минимальные носители собственных функций графов Хэмминга $H(n, q)$ с собственным значением $n(q-1) - q$. Кроме того, получена полная характеризация собственных функций, на которых достигается минимальное значение носителя.

Множество вершин x графа $H(n, q)$, у которых i-ая координата равна k, обозначим через $T_k(i, n)$. В работе доказывается следующая теорема:

Теорема. *Пусть* $f : H(n,q) \longrightarrow \mathbb{R}$ *— собственная функция, отвечающая собственному значению* λ_1*,* $q > 2$ *и* $f \not\equiv 0$*. Тогда* $|S(f)| \geq 2(q-1)q^{n-2}$*.*

Более того, если $|S(f)| = 2(q-1)q^{n-2}$*, то*

$$f(x) = \begin{cases} c, & \text{при } x \in T_k(i,n) \setminus T_m(j,n); \\ -c, & \text{при } x \in T_m(j,n) \setminus T_k(i,n); \\ 0, & \text{иначе;} \end{cases}$$

где $c \neq 0$ *— некоторая константа,* i, j, k, m *— некоторые числа, причем* $i \neq j$*.*

Исследование выполнено при финансовой поддержке Российского научного фонда (проект 14-11-00555).

Список литературы

1. Воробьев К. В, Кротов Д. С. Оценки мощности минимального 1-совершенного битрейда в графе Хэмминга // Дискретн. анализ и исслед. опер. — 2014. — Т. 21, вып. 6. — С. 6–10.

2. Potapov V. N. On perfect 2-colorings of the q-ary n-cube // Discrete Math. — 2012. — V. 312, is. 8. — P. 1269-1272.

ПРОСТАЯ ФОРМУЛА ДЛЯ ЧИСЛА ПОМЕЧЕННЫХ ВНЕШНЕПЛАНАРНЫХ k-ЦИКЛИЧЕСКИХ БЛОКОВ И ИХ АСИМПТОТИЧЕСКОЕ ПЕРЕЧИСЛЕНИЕ

В. А. Воблый (Москва)

Точкой сочленения связного графа называется его вершина, после удаления которой вместе с инцидентными ей ребрами граф становится несвязным. *Блок* — это связный граф без точек сочленения, а также максимальный связный нетривиальный подграф, не имеющий точек сочленения. *Цикломатическим числом* связного графа называется увеличенная на единицу разность между числом ребер графа и числом его вершин. Под k*-циклическим* графом понимается связный граф с цикломатическим числом равным k. *Планарный* граф – это граф, который можно уложить на плоскости без пересечения ребер. *Внешнепланарным* графом называется планарный граф,

если его можно уложить на плоскости так, что все его вершины принадлежат одной грани [1, с. 127, 131].

Теорема. *Для числа $OB(n,k)$ помеченных внешнепланарных k-циклических блоков с n вершинами при $k \geq 1$ и $n \geq k+2$ верна формула*

$$OB(n,k) = \frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!}. \tag{1}$$

Доказательство. В [2] при $k \geq 1$ и $n \geq 3$ выведена формула

$$OB(n,k) = \frac{(n-1)!}{4} \sum_{i=1}^{k} \binom{n+i-3}{2i-2} \frac{(-1)^{k-i}(2i)!}{(2i-1)i!i!}.$$

Выражая биномиальный коэффициент через факториалы и сокращая дробь, получим

$$OB(n,k) = \frac{(n-1)!}{2} \sum_{i=1}^{k} \frac{(-1)^{k-i}(n+i-3)!}{(n-i-1)!(i-1)!i!}.$$

Обозначим правую часть (1) через $f_k(n)$ и используем метод математической индукции.

При $k=1$ верно, что $OB(n,1) = (n-1)!/2 = f_1(n)$. Пусть (1) верна при некотором k, докажем, что она верна при $k+1$. Действительно, имеем

$$OB(n,k+1) = \frac{(n-1)!}{2} \sum_{i=1}^{k+1} \frac{(-1)^{k-i+1}(n+i-3)!}{(n-i-1)!(i-1)!i!} =$$

$$\frac{(n-1)!(n+k-2)!}{2k!(k+1)!(n-k-2)!} - \frac{(n-1)!}{2} \sum_{i=1}^{k} \frac{(-1)^{k-i}(n+i-3)!}{(n-i-1)!(i-1)!i!} =$$

$$\frac{(n-1)!(n+k-2)!}{2k!(k+1)!(n-k-2)!} - \frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!} =$$

$$\frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!} \Big(\frac{(n-1)(n-2)}{k(k+1)} - 1 \Big) =$$

$$\frac{(n-3)!(n+k-2)!}{2(k-1)!k!(n-k-2)!} \frac{(n+k-1)(n-k-2)}{k(k+1)} = f_{k+1}.$$

Доказательство закончено.

Следствие. *Для числа $OB(n,k)$ помеченных внешнепланарных k-циклических блоков с n вершинами при фиксированном $k \geq 1$ и $n \to \infty$ верна асимптотическая формула*

$$OB(n,k) \sim n! \frac{n^{2k-3}}{2(k-1)!k!}.$$

Доказательство. При фиксированном $k \geq 1$ и $n \to \infty$ имеем

$$OB(n,k) = \frac{n!(n+k-2)(n+k-3)...(n-k-1)}{n(n-1)(n-2)2(k-1)!k!} \sim n! \frac{n^{2k-3}}{2(k-1)!k!}.$$

Список литературы

1. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977.

2. Воблый В. А. О числе помеченных внешнепланарных k-циклических блоков // Дискретная математика. — 2016. — Т. 28 (в печати).

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ПЛАНАРНЫХ ПОЛНОБЛОЧНО-КАКТУСНЫХ ГРАФОВ

В. А. Воблый, А. К. Мелешко (Москва)

Планарный граф — это граф, который можно уложить на плоскости без пересечения ребер. Кактусом называется связный граф, в котором нет ребер, лежащих более чем на одном простом цикле [1, с. 93]. Все блоки кактуса — ребра или простые циклы. Полноблочно-кактусный граф — связный граф, у которого все блоки или полные графы, или циклы. Два графа называются гомеоморфными, если их можно получить из одного графа с помощью последовательности подразбиений ребер.

Помеченные полноблочно-кактусные графы перечислены в [2].

Теорема 1. *Для числа PF_n помеченных планарных полноблочно-кактусных графов с n вершинами при $n \geq 3$ верна формула*

$$PF_n = \frac{(n-1)!}{n}[z^{n-1}] \exp\left(nz + \frac{nz^2}{2} + \frac{nz^3}{6} + \frac{nz^3}{2(1-z)}\right).$$

Доказательство. Пусть C_n — число помеченных связных графов с n вершинами, а B_n — число помеченных блоков с n вершинами. Введем производящую функцию: $B(z) = \sum\limits_{n=3}^{\infty} B_n \frac{z^n}{n!}$.

В работе [3] автором было получена формула

$$C_n = \frac{(n-1)!}{n}[z^{n-1}] \exp(nB'(z)), \tag{1}$$

где $[z^i]$ — коэффициентный оператор [4, с. 11].

Обозначая через $\bar{B}(z)$ экспоненциальную производящую функцию для числа блоков помеченных планарных полноблочно-кактусных графов, получим

$$PF_n = \frac{(n-1)!}{n}[z^{-1}] \exp(n\bar{B}'(z))z^{-n}.$$

Из теоремы Понтрягина-Куратовского следует, что граф планарен тогда и только тогда, когда он не содержит подграфов, гомеоморфных полному графу K_5 и $K_{3,3}$. Поэтому в рассматриваемых графах нет блоков-полных графов с числом вершин $n > 4$. Учитывая, что число помеченных циклов с n вершинами равно $(n-1)!/2$, найдем

$$\bar{B}(z) = \sum_{n=2}^{4} \frac{z^n}{n!} + \sum_{n=4}^{\infty} \frac{1}{2}(n-1)!\frac{z^n}{n!},$$

$$\bar{B}'(z) = nz + \frac{nz^2}{2} + \frac{nz^3}{6} + \frac{nz^3}{2(1-z)}. \tag{2}$$

Подставив (2) в (1), получим утверждение теоремы.

Теорема 2. *Для числа PF_n помеченных планарных полноблочно-кактусных графов с n вершинами при $n \to \infty$ верна асимптотическая формула*

$$PF_n \sim cn^{-5/2}a^n n!,$$

где $c \approx 0.1183273421$, $a \approx 4.2534965791$.

Доказательство. Используем теорему Флажоле-Седжвика [5; теорема VIII.8].

Имеем $PF_n = \frac{(n-1)!}{n}[z^n]\Big\{z\Big(\exp\Big(z + \frac{z^2}{2} + \frac{z^3}{6} + \frac{z^3}{2(1-z)}\Big)\Big)^n\Big\} =$

$$= \frac{(n-1)!}{n}F(N,n),$$

где $N = n$, $\lambda = 1$, $a(z) = z$, $b(z) = \exp\left(z + \frac{z^2}{2} + \frac{z^3}{6} + \frac{z^3}{2(1-z)}\right)$.

Очевидно, функции $a(z)$ и $b(z)$ аналитические в точке $z = 0$ и $b(0) = 1$. Функция $b(z)$ имеет положительные коэффициенты, так как $b(z) = \exp(\bar{B}(z))$ и $\bar{B}(z)$ — производящая функция для числа помеченных блоков частного вида. Поскольку $b_2 > 0, b_3 > 0$, имеем НОД$\{j|b_j > 0\} = 1$. Так как $z = 1$ — ближайшая к началу координат особая точка $b(z)$, радиус сходимости R функции $b(z)$ равен 1. Очевидно, $a(z)$ имеет бесконечный радиус сходимости. Таким образом, условия 1-3 теоремы Флажоле-Седжвика выполнены.

Найдем $T = \lim\limits_{x\to 1-0} \frac{xb'(x)}{b(x)} = \lim\limits_{x\to 1-0} \left(x + x^2 + \frac{x^3}{2} + \frac{3x^3}{2(1-x)} + \frac{x^4}{2(1-x)^2}\right) = +\infty$, $0 < \lambda < T$. Уравнение $r\frac{b'(r)}{b(r)} = \lambda$ имеет вид $r + r^2 + \frac{r^3}{2} + \frac{3r^3}{2(1-r)} + \frac{r^4}{2(1-r)^2} = 1$.

Решая это уравнение с помощью Wolfram Mathematica, получим единственный действительный корень $r \approx 0.4471957138$. Вычисляя величину $\sigma = \left(\frac{b'(r)}{b(r)}\right)' + \frac{\lambda}{r^2} = 1 + r + \frac{3r}{1-r} + \frac{3r^2}{(1-r)^2} + \frac{r^3}{(1-r)^3} + \frac{1}{r^2}$, получим $\sigma \approx 11.3671060792$. Также с помощью Wolfram Mathematica вычислим

$$c = \frac{a(r)}{r\sqrt{2\pi\sigma}} = \frac{1}{\sqrt{2\pi\sigma}} \approx 0.1183273421, \quad a = \frac{b(r)}{r} \approx 4.2534965791.$$

Окончательно при $n \to \infty$ имеем асимптотику

$$PF_n = \frac{(n-1)!}{n} F(N, n) \sim \frac{(n-1)!}{n} \frac{1}{\sqrt{2\pi\sigma}} n^{-1/2} \left(\frac{b(r)}{r}\right)^n \sim n! c n^{-5/2} a^n.$$

Доказательство закончено.

Следствие. *Почти все помеченные полноблочно-кактусные графы не являются планарными.*

Доказательство. Известно [2, теорема 3], что для числа F_n помеченных кактусов с n вершинами при $n \to \infty$ верна асимптотическая формула $F_n \sim c_1 n^{-5/2} a_1^n n!$, где $c_1 = 0.1178070871$, $a_1 = 4.261224133$. Следовательно, в силу теоремы 3 имеем

$$\lim_{n\to\infty} \frac{PF_n}{F_n} = \lim_{n\to\infty} \frac{c n^{-5/2} a^n}{c_1 n^{-5/2} a_1^n} = \lim_{n\to\infty} \frac{c}{c_1} \left(\frac{a}{a_1}\right)^n = 0,$$

то есть асимптотически почти все помеченные полноблочно-кактусные графы не являются планарными.

Список литературы

1. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977

2. Воблый В. А., Мелешко А. К. Перечисление помеченных полноблочно-кактусных графов //Дискретный анализ и исследование операций. — 2014. — Т. 21, вып. 2. — С. 24–32.

3. Воблый В. А. Об одной формуле для числа помеченных связных графов // Дискретный анализ и исследование операций. — 2012. — Т. 19, вып. 4. — С. 48–59.

4. Гульден Я., Джексон Д. Перечислительная комбинаторика. — М.: Наука, 1990.

5. Flajolet Ph., Sedgewick R., Analytic combinatorics. — Cambridge University Press, 2009.

ИЗБЫТОЧНОСТЬ КОНСТРУКТИВНЫХ ОПИСАНИЙ ГАМИЛЬТОНОВЫХ ГРАФОВ

М. А. Иорданский (Нижний Новгород)

Рассматриваются обыкновенные, конечные, неориентированные графы. Используется *конструктор* графов, содержащий потенциально бесконечный запас графов. К исходным графам, а также к графам, получаемым из них, применяются бинарные *операции склейки*. При выполнении этих операций производится отождествление изоморфных подграфов $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$ графов-операндов G_1 и G_2. Для результирующего графа G операции склейки графов G_1 и G_2 используется обозначение $G \Leftarrow (G_1 \circ G_2)\tilde{G}$, где $\tilde{G} \subseteq G$ — подграф, полученный в результате отождествления подграфов $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$, называемый *подграфом склейки* [1].

Конструктивные описания графов задаются суперпозициями операций склейки. В качестве исходных графов выбираются элементарные графы, обладающие заданным свойством. Для сохранения результирующими графами характеристического свойства на операции склейки накладывается система ограничений, включающая в себя, в общем случае, ограничения на вид отождествляемых подграфов,их выбор в графах-операндах и способ отождествления [2].

Возможность такого единообразного формулирования условий наследования различных характеристических свойств графов основывается на избыточности, вносимой операциями склейки в задание информации о графах при их конструктивных описаниях. При этом один и тот же граф может быть реализован суперпозициями, обладающими различной избыточностью.

Вершинная избыточность оценивается по формуле

$$I_v^s(G) = \frac{\sum_{i=0}^{q} |V(\tilde{G}_i)|}{|V(G)|},$$

где q — число операций склейки в суперпозиции s, реализующей граф G, $\tilde{G}_i$-подграф склейки i-й операции.

Для оценки реберной избыточности используется формула

$$I_e^s(G) = \frac{\sum_{i=0}^{q} |E(\tilde{G}_i)|}{|E(G)|}.$$

Вершинная избыточность конструктивных описаний эйлеровых графов и (r, s)-деревьев рассматривалась соответственно в работах [3, 4]. В [5] получена оценка реберной избыточности для конструктивных описаний гамильтоновых планарных графов.

В данной работе найдены оценки реберной избыточности конструктивных описаний обыкновенных гамильтоновых графов на основе трех способов, рассмотренных в [6].

Для сохранения свойства гамильтоновости на операции склейки накладываются следующие ограничения.

Лемма. *Если G_1 и G_2 — гамильтоновы графы, то граф $G \Leftarrow (G_1 \circ G_2)\tilde{G}$ также будет гамильтоновым при выполнении любого из следующих условий:*
1) *отождествляемый подграф хотя бы одного из графов-операндов содержит все его вершины;*
2) *каждый отождествляемый подграф содержит концевые вершины гамильтоновых цепей графов-операндов.*

Исходными графами являются простые циклы C_p, $p \geq 3$. Ребра произвольного гамильтонова графа G, $|V(G)| = n$, $|E(G)| = m$ разбиваются на два подмножества: ребра,принадлежащие гамильтонову циклу, и ребра-хорды, не принадлежащие гамильтонову циклу. Хордальное ребро называется *разделяющим*, если его концевые вершины образуют разделяющее множество графа G.

В первом способе синтеза сначала строятся графы $(C_{n_1} \circ C_{n_2})K_2$, $n_1 + n_2 = n$, $n_1, n_2 \geq 3$, каждый из которых реализует гамильтонов

цикл $C_n, n \geq 4$ с одной хордой. Эти графы затем склеиваются в нужном количестве по гамильтонову циклу.

Во втором способе гамильтонов цикл $C_n, n \geq 4$, последовательно склеивается с циклами $C_q, q \geq 3$, по $L_q, q \geq 3$, добавляя к текущему гамильтонову графу по одной хорде.

В третьем способе вначале с помощью операций склейки по K_2 строится n — вершинный гамильтонов граф, все хордальные ребра которого являются разделяющими. Затем полученный граф последовательно склеивается по $(L_{n'} \circ L_{n''})O_0, n', n'' \geq 2$ с циклами $C_p, p \geq 4$, добавляющими в G по две хорды, не являющиеся разделяющими в подграфе, порожденном этими хордами и гамильтоновым циклом.

В каждом методе синтеза, очевидно, используются операции, удовлетворяющие условиям леммы и, следовательно, сохраняющие гамильтоновость графов-операндов.

Пусть $\Im_n$ множество n-вершинных обыкновенных гамильтоновых графов; S_i множестве всех суперпозиций s, реализующих граф $G \in \Im_n$ с использованием i-го способа синтеза, $i \in \overline{1,3}$.

Рассматриваются функции шенноновского типа, характеризующие величину реберной избыточности:

$$\min_{s \in S_i} I_e^s(G) = I_e^i(G), \ \max_{G \in \Im_n} I_e^i(G) = I_e^i(\Im_n), \ i \in \overline{1,3}.$$

Теорема. *Справедливы неравенства*

$$I_e^1(\Im_n) < n - 1, \quad I_e^2(\Im_n) < n/2 - 1,$$

$$I_e^3(\Im_n) \preceq n/4 \quad \textit{при} \quad n \to \infty.$$

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, №4. — С. 35–63.

2. Иорданский М. А. Конструктивная классификация графов // Моделирование и анализ информационных систем. — 2012. — Т. 19, №4. — С. 144–153.

3. Иорданский М. А. Избыточность конструктивных описаний эйлеровых графов // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество. — 2014. — С. 115–116.

4. Иорданский М. А. Избыточность конструктивных описаний (r, s)-деревьев //Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20-22 мая 2015 г. — М.: МАКС Пресс, 2015. — С. 90–91.

5. Иорданский М. А. Избыточность конструктивных описаний гамильтоновых планарных графов // Мат-лы XI международного семинара «Дискретная математика и ее приложения» (МГУ, 18–22 июня 2012 г.) — М. : Изд-во механико-математического ф-та МГУ. — 2012. — С. 285–288.

6. Иорданский М. А. Конструктивные описания гамильтоновых графов //Вестник Нижегородского государственного университета. Математика. — 2012. — №3 (1). — С. 137–140.

АЛГОРИТМ ПОСТРОЕНИЯ AOE-ЦЕПИ В ПЛОСКОМ СВЯЗНОМ 4-РЕГУЛЯРНОМ ГРАФЕ

Т. А. Макаровских, А. В. Панюков (Челябинск)

Для плоского графа G далее через $E(G)$ будем обозначать множество его ребер, представляющих плоские жордановы кривые с попарно непересекающимися внутренностями, гомеоморфные отрезкам. Через $V(G)$ обозначим множество граничных точек этих кривых. Топологическое представление плоского графа $G = (V, E)$ на плоскости S с точностью до гомеоморфизма определяется заданием для каждого ребра $e \in E$ следующих функций [1]: $v_k(e)$, $k = 1, 2$ – вершины, инцидентные ребру e; $l_k(e)$, $k = 1, 2$ – ребра, полученные вращением ребра e против часовой стрелки вокруг вершины $v(k)$; $r_k(e)$, $k = 1, 2$ – ребра, полученные вращением ребра e по часовой стрелке вокруг вершины $v(k)$. Далее будем считать, что все рассматриваемые плоские графы представлены указанными функциями. Пространственная сложность такого представления будет $O(|E| \cdot \log_2 |V|)$.

Определение 1. *Графом переходов* [2] $T_G(v)$ вершины $v \in V(G)$ будем называть граф, вершинами которого являются ребра, инцидентные вершине v, т.е. $V(T_G(v)) = E_G(v)$, а множество ребер – разрешенные переходы между ребрами.

Определение 2. *Системой переходов* [3] T_G будем называть множество $\{T_G(v) \mid v \in V(G)\}$, $T_G(v)$ – граф переходов в вершине v.

Определение 3. Путь $P = v_0, e_1, v_1, ..., e_k, v_k$ в G называется T_G-*совместимым*, если $\{e_i,\ e_{i+1}\} \in E(T_G(v_i))$, $1 \le i \le k-1$.

Определение 4. Пусть для цепи $T = v_0, k_1, v_1, \ldots, k_n, v_n, v_n = v_0$ в графе $G = (V, E)$ в каждой вершине $v \in V$ задан циклический порядок $O^{\pm}(v)$, определяющий систему переходов $A_G(v) \subset O^{\pm}(v)$. В случае, когда $\forall v \in V(G)\ A_G(v) = O^{\pm}(v)$, систему переходов $A_G(v)$ будем называть *полной системой переходов*.

Определение 5. Эйлерову цепь T будем называть A-*цепью* тогда и только тогда, когда она является A_G-совместимой цепью. Таким образом, последовательные ребра в цепи T (инцидентные вершине v) являются соседями в циклическом порядке $O^{\pm}(v)$.

В работе [3] определены некоторые классы графов, для которых распознавание наличия A-цепи требует полиномиального времени.

Рассмотрим плоскость S. Пусть на ней задан плоский эйлеров граф $G = (V, E)$. Пусть f_0 – внешняя грань графа G. Для любого подмножества $H \subset S$ определим $\mathrm{Int}(H)$ как подмножество S, являющееся объединением всех связных компонент множества $S \backslash H$, не содержащих внешней грани f_0. Так, $\mathrm{Int}(G)$ будет представлять объединение всех внутренних граней графа G. Для плоского графа в качестве цикла $O^{\pm}(v)$ далее будем рассматривать соседей при вращении текущего ребра e по или против часовой стрелки относительно вершины v.

Определение 6. Будем говорить, что цикл $C = v_1 e_1 v_2 e_2 \ldots v_k$ в эйлеровом графе G имеет *упорядоченное охватывание* (является OE-цепью), если для любой его начальной части $C_i = v_1 e_1 v_2 e_2 \ldots e_i$, $i \le |E(G)|$ выполнено условие $\mathrm{Int}\,(C_i) \cap G = \emptyset$.

Определение 7. Будем говорить, что цепь является AOE-*цепью*, если она одновременно является OE-цепью и A-цепью.

Теорема 1. *Если в плоском графе G графе существует A-цепь, то существует и AOE-цепь.*

Теорема 2. *В плоском связном 4-регулярном графе G существует AOE-цепь.*

Определение 8. *Рангом ребра* $e \in E(G)$ будем называть значение функции $\mathrm{rank}(e) : E(G) \to N$, определяемую рекурсивно: пусть $E_1 = \{e \in E : e \subset f_0\}$ – множество ребер, ограничивающих внешнюю грань f_0 графа $G(V, E)$, тогда $(\forall e \in E_1)\,(\mathrm{rank}(e) = 1)$; пусть $E_k(G)$ – множество ребер ранга 1 графа $G_k \left(V, E \backslash \left(\bigcup_{l=1}^{k-1} E_l \right) \right)$,

тогда $(\forall e \in E_k)\,(\mathrm{rank}(e) = k)$.

Различные способы вычисления значений функции $\mathrm{rank}(e)$ приведены в работах [1, 4]. Вычислительная сложность определения ранга для всех ребер графа не превосходит $O(|E| \log_2 |V|)$.

Определение 9. Сураф G_k графа G, для которого $E(G_k) = \{e \in E(G) : \mathrm{rank(e)} \geq \mathrm{k}\}$ назовем *суграфом ранга* k.

Предложение 1. *Вершина, инцидентная четырем ребрам, смежным внешней грани, является точкой сочленения.*

Предложение 2. *Внешняя грань суграфа G_k является объединением всех граней ранга k в графе G.*

Из предложений 1 и 2 следует, что в любом плоском графе G можно найти точки сочленения для любого суграфа G_k, $k = 1, 2, ...$ и провести расщепление в этих вершинах таким образом, чтобы в G_k не появились новые грани. В результате получим граф, в котором любой сураф G_k не имеет точек сочленения.

Приведем описание алгоритма, который позволяет построить AOE-цепь в любом плоском связном 4-регулярном графе G, любой сураф G_k которого не имеет точек сочленения.

Алгоритм *AOE*-TRAIL. Вход: $G = (V, E)$; начальная вершина $v \in V(f_0)$. Вывод: $ATrail$ – выходной поток, содержащий построенную алгоритмом AOE-цепь.

`Initiate(`G`, `v_0`);` // Инициализация
`Ranking(`G`);` // Ранжирование
$e = \arg\max_{e \in E(v)} \mathrm{rank}(e)$; $v = v_1(e)$;
`do` {
  `if` $(v \neq v_1(e))$ REPLACE(e);
  $ATrail$ << v << e;
  $\mathrm{mark}(e) =$ `false`; counter++; $v = v_2(e)$;
  `if` $(\mathrm{rank}(r_2(e)) \geq \mathrm{rank}(l_2(e)))$ `then`
    `if` $\mathrm{mark}(r_2(e))$ `then` $e = r_2(e)$ **else** $e = l_2(e)$;
  `else if` $\mathrm{mark}(l_2(e))$ `then` $e = l_2(e)$ `else` $e = r_2(e)$;
} `while(counter` $< |E(G)|$`);`
`Stop`

Теорема 3. *Алгоритм AOE-TRAIL строит AOE-цепь в плоском связном 4-регулярном графе G за время $O(|E(G)| \cdot \log_2 |V(G)|)$.*

Список литературы

1. Панюкова Т. А. Обходы с упорядоченным охватыванием в плоских графах // Дискретный анализ и исследование операций. Сер. 2. — 2006. — Т. 13, № 2. — С. 31–43.

2. Szeider S. Finding paths in graphs avoiding forbidden transitions // Discrete Applied Mathematics. — 2003. — 126. — P. 261–273.

3. Фляйшнер Г. Эйлеровы графы и смежные вопросы. — М.: Мир, 2002.

4. Савицкий Е. А. Использование алгоритма поиска в ширину для определения уровней вложенности ребер плоского графа // Информационные технологии и системы: тр. Третьей междунар. науч. конф. / Челябинск: Изд-во ЧелГУ, 2014. — С. 43–45.

ГРАНИЧНЫЕ КЛАССЫ ГРАФОВ В ЗАМКНУТЫХ СЕМЕЙСТВАХ КЛАССОВ ГРАФОВ

Д. С. Малышев (Нижний Новгород)

В настоящей работе мы рассматриваем только *обыкновенные графы*, т. е. непомеченные неориентированные графы без петель и кратных ребер. Класс графов называется *наследственным*, если он замкнут относительно удаления вершин. Любой наследственный класс может быть задан множеством своих запрещенных порожденных подграфов. Если наследственный класс может быть задан конечным множеством запрещенных порожденных подграфов, то он называется *конечно определенным*. Помимо семейства $\mathbb{H}$ всех наследственных классов мы рассматриваем два его подсемейства. Первое из них — семейство $\mathbb{SH}$ всех *сильно наследственных* классов, т.е. классов, замкнутых относительно удаления вершин и ребер. Второе — семейство $\mathbb{M}$ всех *минорно замкнутых* классов, т.е. сильно наследственных классов, замкнутых еще и относительно стягивания ребер. Любой класс из $\mathbb{SH}$ может быть задан множеством своих запрещенных подграфов. Очевидно, что класс из $\mathbb{SH}$ может быть задан конечным множеством запрещенных подграфов тогда и только тогда, когда он является конечно определенным. Поэтому термин «конечно определенный класс» имеет в семействе $\mathbb{SH}$ такое же значение, что и в семействе $\mathbb{H}$. Согласно известной теореме Н. Робертсона и П. Сеймура [1], любой минорно замкнутый класс может быть задан конечным множеством своих запрещенных миноров.

Пусть Π — какая-либо задача на графах. Наследственный класс с полиномиально разрешимой задачей Π называется Π-*простым*. Наследственный класс с NP-полной задачей Π называется Π-*сложным*. Понятие граничного класса было введено в работе [2] применительно к задаче о независимом множестве и обобщено в работе [3] на случай произвольной задачи на графах из класса NP. Ранее это понятие рассматривалось только в рамках семейства $\mathbb{H}$. Здесь мы распространяем это понятие на другие семейства. Пусть $\mathbb{F} \in \{\mathbb{H}, \mathbb{SH}, \mathbb{M}\}$. Класс $\mathcal{X}$ называется $(\Pi, \mathbb{F})$-*предельным*, если существует такая бесконечная последовательность $\mathcal{X}_1 \supseteq \mathcal{X}_2 \supseteq \ldots$ из Π-сложных классов, каждый из которых принадлежит $\mathbb{F}$, что $\mathcal{X} = \bigcap\limits_{i=1}^{\infty} \mathcal{X}_i$. Минимальный по включению $(\Pi, \mathbb{F})$-предельный класс называется $(\Pi, \mathbb{F})$-*граничным*. Значение этого понятия раскрывает следующая теорема, которая может быть доказана точно также, как и соответствующие утверждения из [2, 3]:

Теорема 1. *Пусть* $\mathbb{F} \in \{\mathbb{H}, \mathbb{SH}\}$. *Конечно определенный класс из* $\mathbb{F}$ *является* Π-*сложным тогда и только тогда, когда он включает какой-нибудь* $(\Pi, \mathbb{F})$-*граничный класс. Минорно замкнутый класс является* Π-*сложным тогда и только тогда, когда он включает какой-нибудь* $(\Pi, \mathbb{M})$-*граничный класс.*

Таким образом, по теореме 1 знание всех граничных классов приводит к полной классификации всех конечно определенных классов (или всех минорно замкнутых) по сложности решения данной задачи. Однако, применительно к семейству $\mathbb{H}$, вопрос получения описания всех граничных классов оказывается сложным для многих задач Π, на настоящее время известен только один пример полного описания множества граничных классов [4]. В работе [5] было доказано, что для реберной задачи о 3-раскраске (задачи 3-PP) совокупность $(3\text{-PP}, \mathbb{H})$-граничных классов является континуальной, что, по-видимому, свидетельствует о принципиальной невозможности получения полного описания множества граничных классов для этой задачи. В семействе $\mathbb{SH}$ вопрос полного описания граничных классов оказывается более простым. Пусть $\mathcal{T}$ — класс всех лесов, каждая компонента связности которых имеет не более трех листьев. Для некоторых задач на графах (например, для задач НМ и ДМ о независимом и о доминирующем множествах) класс $\mathcal{T}$ является единственным граничным в семействе $\mathbb{SH}$ [2, 6]. Однако, совокупность всех $(3\text{-PP}, \mathbb{SH})$-граничных классов остается континуальной [6]. Из теоремы Робертсона—Сеймура следует, что для любой задачи Π множество всех $(\Pi, \mathbb{M})$-граничных классов является не более чем счетным.

Множество планарных графов $\mathcal{P}lanar$ для семейства $\mathbb{M}$ является аналогом класса $\mathcal{T}$ для семейства $\mathbb{SH}$. Именно, для многих задач на графах (например, для задач НМ и ДМ) класс $\mathcal{P}lanar$ является единственным граничным в семействе $\mathbb{M}$ [6].

Было бы интересным найти такие классическую задачу на графах П и (П, $\mathbb{M}$)-граничный класс, что не известны ни (П, $\mathbb{H}$)-граничные, ни (П, $\mathbb{SH}$)-граничные классы. *Нумерацией графа* G называется произвольное инъективное отображение $f_G : V(G) \longrightarrow \overline{1, |V(G)|}$. *Ленточной шириной графа* G называется число $b(G) = \min \max_{(u,v)\in E(G)} |f_G(u) - f_G(v)|$, где минимум берется по всевозможным нумерациям f_G графа G. *Задача о ленточной ширине графа* (кратко, *задача ЛШ*) для заданного графа G состоит в вычислении $b(G)$. *Задача ЛШ*$_{+2}$ для заданного графа G состоит в вычислении такого числа $p(G)$, что $b(G) \leq p(G) \leq b(G) + 2$. Задача ЛШ — классическая NP-трудная задача на графах, задача ЛШ$_{+2}$ также NP-трудна. *Циклическая 1-гусеница* — граф, получаемый добавлением к простому циклу попарно несмежных вершин (возможно, ни одной), каждая из которых смежна ровно с одной из вершин цикла. Минорное замыкание множества всех циклических 1-гусениц обозначается через 1-$\mathcal{C}Caterpillar$.

Теорема 2. *Класс* 1-$\mathcal{C}Caterpillar$ *является* (*ЛШ*$_{+2}$, $\mathbb{M}$)*-граничным.*

Отметим, что на настоящее время для задач ЛШ и ЛШ$_{+2}$ в семействах $\mathbb{H}$ и $\mathbb{SH}$ граничные классы не известны.

Работа выполнена при финансовой поддержке РФФИ (проект 16-31-60008-мол-а-дк), гранта Президента РФ МК-4819.2016.1, лаборатории алгоритмов и технологий анализа сетевых структур, Национальный исследовательский университет «Высшая школа экономики».

Список литературы

1. Robertson N., Seymour P. Graph minors XX: Wagner's conjecture // Journal of Combinatorial Theory, Series B. — 2004. — V. 92, No 2. — P. 325–357.

2. Alekseev V. E. On easy and hard hereditary classes of graphs with respect to the independent set problem // Discrete Applied Mathematics. — 2003. — V. 132, No. 1–3. — P. 17–26.

3. Alekseev V. E., Boliac R., Korobitsyn D. V., Lozin V. V. NP-hard graph problems and boundary classes of graphs // Theoretical Computer Science. — 2007. — V. 389, No 1–2. — P. 219–236.

4. Малышев Д. С. Критические классы графов для задачи о реберном списковом ранжировании // Дискретный анализ и исследование операций. — 2013. — Т. 20, вып. 6. — С. 59–76.

5. Малышев Д. С. Континуальные множества граничных классов графов для задач о раскраске // Дискретный анализ и исследование операций. — 2009. — Т. 16, вып. 5. — С. 41–51.

6. Малышев Д. С. Критические элементы в комбинаторно замкнутых семействах классов графов // Дискретный анализ и исследование операций. — 2016 (направлено в журнал).

О ДИФФЕРЕНЦИАЦИИ ГРАФОВ НА ОСНОВЕ БЫСТРО ВЫЧИСЛЯЕМЫХ ИНВАРИАНТОВ

Б. Ф. Мельников, Н. П. Чурикова (Самара)

Настоящая статья посвящена некоторым частным вопросам, связанным с проблемой построения алгоритмов определения (не) изоморфности двух заданных графов. После нескольких десятилетий работы над данной проблемой многих научных групп недавно (в самом конце 2015 г.) было объявлено об окончании разработки квазиполиномиального (псевдо-полиномиально-временно́го) алгоритма; однако стоит отметить, что публикаций этого алгоритма пока не появилось, вся информация пока ограничивается научно-популярными сайтами вроде [1] с примерно следующим текстом:

> Математик Ласло Бабай из Чикагского университета в США разработал теоретический алгоритм, позволяющий существенно ускорить сравнение графов друг с другом ... Бабай изложил основные моменты своей работы в двух лекциях, а присутствующие на них эксперты в области теории графов пока не нашли ошибок в рассуждениях ученого. Между тем окончательной верификации в математическом сообществе его работа пока не получила.

Итак, информации о возможности практического применения данного алгоритма пока нет. На практике применяются более простые процедуры, от которых ожидается хорошая работа в большинстве случаев. Например, используются эвристики для доказательства, что два графа не изоморфны ([2] и многие другие). Для этого используют различные инварианты, и, как только обнаруживаются два различных значения одного и того же инварианта, приходят к заключению, что графы не изоморфны. В [2] одним из авторов настоящей статьи был предложен один из вариантов проверки двух заданных графов на неизоморфность — а именно, эвристический алгоритм определения конкретной последовательности поверки инвариантов.

В настоящей работе кратко описывается решение одной из задач, необходимых для осуществления этого подхода. Мы рассматриваем два инварианта, для которых ранее были неизвестны такие примеры графов, для которых эти инварианты дают разную дифференциацию (т. е. когда *ровно один* из этих инвариантов показывает их неизоморфность). А именно, мы, во-первых, рассматриваем индекс Рандича — величину

$$\sum_{(v_i,v_j)\in E} \frac{1}{\sqrt{d(v_i)d(v_j)}},$$

где v_i и v_j — две вершины, образующие ребро множества E. Во-вторых, мы также рассматриваем вектор степеней 2-го порядка, определённый и исследованный в [2]. (При этом важно отметить, что, согласно доступной об алгоритме Бабая информации, в этом алгоритме, по-видимому, используются аналогичные инварианты.)

Эвристические алгоритмы, работавшие со случайно сгенерированными графами, содержащими по 10 вершин, не дали ни одного примера, для которых упомянутые нами инварианты дают разную дифференциацию. Однако нами найден пример (по-видимому, ранее подобных примеров опубликовано не было), когда разную дифференциацию для упомянутых нами инвариантов дают два графа, содержащие по 12 вершин; приведём этот пример.

Для графа G_1 матрица смежности следующая:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

При этом приближённое значение индекса Рандича графа G_1 есть 5.79870219113. Вектор степеней второго порядка сначала запишем по порядку вершин графа:

$$[[3,5,7,3],[4,7,3],[4,5,7,5,3],[4,5,3,7,5,3,4],[4,7,7],[3,7,3,3,5,3,4],$$
$$[3,7,5],[5,5,5],[4,5,3,7,3],[4,5,7,3,3],[5,7,7],[5,5,7,7]],$$

после чего проведём сортировку [2]:

$$[[7,5,5,4,4,3,3],[7,5,4,3,3,3,3],[7,5,5,4,3],[7,5,4,3,3],[7,5,4,3,3],$$
$$[7,7,5,5],[7,5,3,3],[7,7,5],[7,7,4],[7,5,3],[7,4,3],[5,5,5]].$$

Для графа G_2 матрица смежности следующая:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

При этом значение индекса Рандича *в точности совпадает* с вычисленным для графа. Вектор степеней второго порядка сразу запишем в отсортированном виде:

$$[[7,5,5,4,3,3,3],[7,5,4,4,3,3,3],[7,5,5,4,3],[7,5,4,3,3],[7,5,4,3,3],$$
$$[7,7,5,3],[7,5,5,3],[7,7,5],[7,5,5],[7,7,3],[7,4,3],[5,5,4]].$$

Как мы видим, он не совпадает с аналогичным вектором графа G_1.

Подробное описание эвристических алгоритмов получения подобных пар графов мы приведём в следующей публикации.

Список литературы

1. Graph-theory breakthrough tantalizes mathematicians // Электронный ресурс: `http://www.nature.com/news/graph-theory-breakthrough-tantalizes-mathematicians-1.18801` (дата публикации 19.11.2015, дата обращения 17.04.2016).

2. Мельников Б. Ф., Сайфуллина Е. Ф. Применение мультиэвристического подхода для случайной генерации графа с заданным вектором степеней // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2013. — № 3 (27). — С. 70–83.

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

Д. Б. Мокеев (Нижний Новгород)

В статье используются традиционные обозначения для простых путей, циклов и полных графов: P_n, C_n, K_n.

Пусть $\mathcal{X}$ — множество графов. Множество попарно непересекающихся порождённых подграфов графа G, изоморфных графам из $\mathcal{X}$, называется $\mathcal{X}$-*упаковкой* G. Множество вершин графа G, покрывающее все порождённые подграфы графа G, изоморфные графам из $\mathcal{X}$, называется $\mathcal{X}$-*покрытием*. Граф называется *кёниговым* относительно $\mathcal{X}$, если в любом его порождённом подграфе наибольшая мощность $\mathcal{X}$-упаковки равна наименьшей мощности $\mathcal{X}$-покрытия [1]. Класс всех кёниговых графов относительно множества $\mathcal{X}$ обозначаем через $\mathcal{K}(\mathcal{X})$. Если множество $\mathcal{X}$ состоит из единственного графа H, то будем говорить об H-упаковках, H-покрытиях и кёниговых графах относительно H.

Класс $\mathcal{K}(\mathcal{X})$ при любом $\mathcal{X}$ является наследственным и, следовательно, может быть описан множеством запрещенных графов (минимальных по отношению «быть порожденным подграфом» графов, не принадлежащих $\mathcal{X}$). Для P_2 такую характеризацию даёт теорема Кёнига вместе с известным критерием двудольности. Кроме этой

классической теоремы автору известны следующие результаты такого рода для обыкновенных графов: в [2] описаны все запрещённые подграфы для класса $\mathcal{K}(\mathcal{C})$, где $\mathcal{C}$ — множество всех простых циклов, в [1, 3] описаны все запрещённые подграфы для классов $\mathcal{K}(P_3)$ и $\mathcal{K}(\{P_3, C_3\})$, а также дано конструктивное описание обоих классов. В [4] описано несколько семейств запрещённых графов для класса $\mathcal{K}(P_4)$ и высказано предположение, что объединение этих семейств образует полное множество запрещенных графов для данного класса.

Граф называется расщепляемым, если существует разбиение множества его вершин на клику и независимое множество. Класс расщепляемых графов также является наследственным. Множество его минимальных запрещённых подграфов составляют $2P_2$, C_4 и P_5.

Цель настоящей работы — дать описание пересечения класса $\mathcal{K}(P_4)$ с классом графов, полученных из расщепляемых с помощью замены вершин кографами. Даётся описание множества минимальных запрещённых графов для этого класса, а так же его структурная характеризация.

Далее порождённый подграф, изоморфный P_4 будем называть *квартетом*.

Обозначим $V(G)$ множество вершин графа G. Окрестность вершины v будем обозначать $N(v)$.

Кографом называется граф, не содержащий квартетов.

Определение. Операция *замены графом H вершины x* состоит в том, что эта вершина удаляется из графа, к графу добавляется несколько новых вершин, соединённых между собой так, что они порождают подграф, изоморфный H. Каждая новая вершина соединена ребром со всеми вершинами $N(x)$ в исходном графе.

Определение. Будем говорить, что граф G является *расширением* графа H, если он может быть получен из H заменой некоторых его вершин произвольными кографами.

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*.

Определение. Пусть H — расщепляемый граф со следующими свойствами:
1) $V(G) = K_1 \cup K_2 \cup L_1 \cup L_2$;
2) $K_1 \cup K_2$ формирует клику в G, а $L_1 \cup L_2$ является независимым множеством G;
3) для любого $t \in \{1, 2\}$ для любых $x, y \in K_t$ выполняется $N(x) \subseteq N(y)$ или $N(y) \subseteq N(x)$;
4) для любого $t \in \{1, 2\}$ для любых $x, y \in L_t$ выполняется $N(x) \subseteq N(y)$ или $N(y) \subseteq N(x)$.

Будем называть такой граф зеркально-расщепляемым.

Теорема. *Следующие утверждения равносильны для связного графа G:*
1) *G является расширением некоторого зеркально-расщепляемого графа;*
2) *G является расширением расщепляемого графа, не содержащего порождённых подграфов rising sun, co-rising sun, S_3, net;*
3) *G не содержит порождённых подграфов C_5, P_5, $\overline{P_5}$, rising sun, co-rising sun, S_3, net, A, co-A, parapluie, parachute, $2P_4$, $\overline{2P_4}$;*
4) *G принадлежит множеству $\mathcal{K}(P_4)$ и является расширением расщепляемого графа.*

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 16-31-00109-мола, 16-01-00599-а), гранта Президента РФ МК-4819.2016.1 и Лаборатории алгоритмов и технологий анализа сетевых структур НИУ ВШЭ, грант правительства РФ (договор 11.G34.31.0057).

Список литературы

1. Алексеев В. Е., Мокеев Д. Б. Кёниговы графы относительно 3-пути // Дискретный анализ и исследование операций. — 2012. — Т. 19, вып. 4. — С. 3–14.

2. Ding G., Xu Z., Zang W. Packing cycles in graphs II // Journal of Combinatorial Theory. Ser. B. — 2003. — Vol. 87. — P. 244–253.

3. Alekseev V. E., Mokeev D. B. König graphs for 3-paths and 3-cycles // Discrete Applied Mathematics. — 2016. — Vol. 204. — P. 1–5.

4. Mokeev D. König Graphs for 4-paths // Models, Algorithms and Technologies for Network Analysis. — 2014. — P. 93–103.

ОБ ОДНОМ ТЕОРЕТИКО-ГИПЕРГРАФОВОМ ПОДХОДЕ РЕШЕНИЯ ЗАДАЧИ О КЛИКАХ

В. А. Перепелица (Запорожье), Д. А. Тамбиева (Черкесск)

Известно, что задача о покрытии графа кликами относится к классу NP-полных (NP-трудных) задач [1]. В этой связи ее решения в научных публикациях ограничивается статистически эффективными и асимптотически точными алгоритмами. В настоящей работе предлагается алгоритм α выделения множества допустимых решений покрытия графа типовыми подграфами различной конфигурации, базирующийся на методологии теории гиперграфов. Для описания обобщенной математической модели указанной задачи используем термин «функциональная единица», под которой понимаем минимальную значимую единицу соответствующую подструктуре некоторой сложной системы.

В структуре системы имеется n функциональных единиц. В теоретико-графовой модели рассматриваемой задачи строим граф $G = (V,\ E)$, в котором $V = \{v_1, v_2,\ ...,\ v_n\}$ — множество вершин, каждая вершина v_i, $i = 1,\ 2,\ ...,\ n$ взаимнооднозначно соответствует i-ой функциональной единице, а $E = \{e_{ij}\}$, $(i,\ j = 1,\ 2,\ ...,\ n)$ — множество ребер, где наличие ребра $e_{ij} = (v_i,\ v_j) \in E$ соответствует вертикальным и/или горизонтальным связям системы между i-ой и j-ой функциональными единицами. Требуется выделить множество допустимых решений покрытия графа $G = (V,\ E)$ типовыми подграфами заданной конфигурации.

Рассмотрим указанный алгоритм для решения задачи покрытия графа 3-кликами (трисочетаниями).

На первом шаге алгоритма осуществляется переход от исходного графа $G = (V,\ E)$ к гиперграфу $H\,(W,\ I)$, на базе которого проводятся все дальнейшие вычисления.

Принцип построения гиперграфа $H\,(W,\ I)$ следующий: вершины графа $G = (V,\ E)$, соответствующие типовому подграфу заданной конфигурации, стягиваются в одну гипервершину гиперграфа

$H(W,\, I)$. Ребро гиперграфа $H(W,\, I)$ строится между двумя гипервершинами в том случае, если пересечение множеств вершин графа $G = (V,\ E)$ образующих эти гипервершины гиперграфа $H(W,\, I)$ пусто.

Условимся, что множество вершин $V = \{v\}$ представляет собой множество натуральных чисел $v = 1,\, 2,\, ...,\, i,\, ...,\, n$. Тогда гипервершины $w \in W$ представляют собой упорядоченные (по возрастанию) тройки $w = (v_1,\, v_2,\, v_3)$, где $v_1 < v_2 < v_3$. Упорядочив множество W этих троек лексикографически, получим последовательность (упорядоченное множество)

$$W = \{w_1,\, w_2,\, ...,\, w_\mu,\, ...,\, w_M\}\,,\ M = |W|\,. \tag{1}$$

Последовательность (1) разбиваем на подпоследовательности $W_1, W_2, ..., W_l, ..., W_L$ следующим образом. Сначала рассмотрим последовательность

$$\left\{v_1^1,\, v_1^2,\, ...,\, v_1^\mu,\, ...,\, v_1^M\right\} \tag{2}$$

первых компонент v_1^μ в гипервершинах $w_\mu = (v_1^\mu,\, v_2^\mu,\, v_3^\mu)$ последовательности (1), т.е. между элементами упорядоченных последовательностей (1) и (2) существует взаимнооднозначное соответствие. Далее заметим, что последовательность (2) состоит из подпоследовательностей одинаковых по значению элементов. Выбрав из каждой такой подпоследовательности по одному представителю, получим упорядоченную по возрастанию последовательность, состоящую из этих представителей:

$$\bar{V} = \{1,\, i_2,\, ...,\, i_l,\, ...,\, i_L\}\,. \tag{3}$$

С учетом обозначения $i_1 = 1$, ряд чисел (3) определяет собой разбиение последовательности (1) на подпоследовательности

$$W_l = \left\{w_\mu = (v_1^\mu,\, v_2^\mu,\, v_3^\mu) : v_1^\mu = i_l,\ i_l \in \bar{V}\right\},\ l = 1,\, L.$$

Этот процесс заканчивается тогда, когда сформируется такая доля W_L, на которой полностью исчерпывается множество гипервершин W, т.е. является пустым подмножество $W \setminus (W_1 \cup W_2 \cup ... \cup W_L) = \emptyset$.

Результат построения гиперграфа $H(W,\, I)$ представляется в виде матрицы смежности A^1 гипервершин $w \in W$.

На втором шаге реализуется специальная процедура отсеивания неперспективных гипервершин, суть которой на первом шаге итерации определяется тем свойством, что всякая гипервершина $w \in W_\chi$, принадлежащая допустимому решению имеет степень $\deg w = n_0 - 1$,

где $n_0 = n/3$. Поэтому если общее количество входящих и исходящих дуг оказывается меньшим, чем приведенная выше оценка, то такую гипервершину будем считать «неперспективной» и «вычеркивается» из матрицы A^1. Последующие шаги процедуры отсеивания предполагает последовательное удаление всех «неперспективных» гипервершин и реализуется на базе матриц преобразования: A^i, B^i, C^i, где i=1, ..., t – шаг итерации.

Последовательность шагов алгоритма α:

$$G(V,E) \to H(W,I) \to \underbrace{A^1 \to B^1 \to C^1}_{1\text{-}я\ итерация} \to \ldots \to$$

$$\to \underbrace{A^{(t-1)} \to B^{(t-1)} \to C^{(t-1)}}_{(t-1)\text{-}я\ итерация} \to \underbrace{A^{(t)} \to B^{(t)} \to C^{(t)}}_{t\text{-}я\ итерация}, \ldots$$

Если $C^{(t-1)} = C^t$, то достигли неподвижной точки, соответствующей множеству допустимых решений задачи о покрытии графа трисочетаниями.

Лемма 1. *Если данный граф содержит единственное допустимое решение, то алгоритм α гарантирует нахождение неподвижной точки размерности n_0, однозначно определяющей это решение. Трудоемкость нахождения допустимого решения в этом случае ограничена сверху полиномом от n.*

Лемма 2. *При выполнении условий леммы 1 на каждой итерации (кроме последней) удаляется хотя бы одно ребро или вершина соответствующего гиперграфа.*

Лемма 3. *Если исходный граф полный, то начальная матрица A^1 представляет собой неподвижную точку.*

Лемма 4. *Если в исходном графе некоторый треугольник принадлежит хотя бы одному допустимому решению, то соответствующая ему гипервершина не будет удалена ни на какой итерации.*

Лемма 5. *Для всякого исходного графа неподвижная точка достигается алгоритмом не более чем за полиномиальное число итераций.*

Лемма 6. *Нижняя оценка размерности неподвижной точки является полином порядка $O\left(n^3\right)$.*

Пусть m — размерность матрицы A^1, тогда с учетом леммы 2 справедлива

Лемма 7. *Для всякой матрицы A^1 количество итераций для достижения неподвижной точки задачи о трисочетаниях не превосходит $O(n^9)$.*

Отметим, что подробное описание алгоритма α и доказательства представленных лемм можно найти в [2].

Список литературы:

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

2. Перепелица В. А., Тамбиева Д. А. Системы с иерархической структурой управления: разработка экономико–математических и инструментальных методов. — М.: Финансы и статистика, 2009.

БУЛЕВО-МАТРИЧНЫЕ ИДЕМПОТЕНТЫ

В. Б. Поплавский (Саратов)

Пусть $\langle \mathbf{B}_{m\times n}, \cup, \cap, ', O, I\rangle$ есть булева алгебра $m \times n$ матриц с элементами из некоторой булевой алгебры $\langle \mathbf{B}, \cup, \cap, ', 0, 1\rangle$. Операции объединения $\cup$, пересечения $\cap$, дополнения $'$ и, следовательно, отношение частичного порядка $\subseteq$ определяются для матриц поэлементно. Матрицы O и I, образованные целиком из нулей 0 и единиц 1 соответственно, дают нуль и единицу такой вторичной булевой алгебры.

Матрицу $C = A \sqcap B \in \mathbf{B}_{m\times k}$ с элементами $C^i_j = \bigcup_{t=1}^{n}(A^i_t \cap B^t_j)$ назовём *конъюнктным произведением* матриц согласованных размеров $A = (A^i_j) \in \mathbf{B}_{m\times n}$ и $B = (B^i_j) \in \mathbf{B}_{n\times k}$. *Дизъюнктное произведение* $A \sqcup B$ определяется дуальным образом: $A \sqcup B = (A' \sqcap B')'$.

Рассмотрим $\mathbf{M}^n(\mathbf{B}) = \bigcup_{m,n\in\langle 1,..,n\rangle} \mathbf{B}_{m\times n}$ - множество булевых матриц всевозможных размеров, начиная с 1×1 по $n \times n$. Пары $\langle \mathbf{M}^n(\mathbf{B}), \sqcap\rangle$ и $\langle \mathbf{M}^n(\mathbf{B}), \sqcup\rangle$ образуют частичные полугруппы относительно частичных, то есть определенных не для каждых пар матриц, бинарных операций. При этом неравенство $A \subseteq B$ влечёт $A \sqcap C \subseteq B \sqcap C$, $C \sqcap A \subseteq C \sqcap B$ и $A \sqcup C \subseteq B \sqcup C$, $C \sqcup A \subseteq C \sqcup B$. Дополнение булевых матриц , в силу равенств $(A \sqcap B)' = A' \sqcup B'$ и $(A \sqcup B)' = A' \sqcap B'$, является изоморфизмом частичных полугрупп $\langle \mathbf{M}^n(\mathbf{B}), \sqcap\rangle$ и $\langle \mathbf{M}^n(\mathbf{B}), \sqcup\rangle$.

Пусть A^T означает транспонирование матрицы A. Заметим, что $(A \sqcap B)^T = B^T \sqcap A^T$ и $(A \sqcup B)^T = B^T \sqcup A^T$. Здесь и далее полагаем, что $A'^T = (A^T)' = (A')^T$.

Символом E будем далее обозначать квадратные единичные матрицы с единицами на главной диагонали и нулями на остальных местах. При этом соответствующий контексту размер матрицы E указывать не будем.

Определение 1. Матрица A называется *первичным* $\sqcap$-*идемпотентом*, если $E \nsubseteq A = A \sqcap A$, и *вторичным* $\sqcap$-*идемпотентом* частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, если $E \subseteq A = A \sqcap A$.

Для частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcup \rangle$ первичные и вторичные $\sqcup$-идемпотенты определяются дуальным образом, то есть матрица $A = A \sqcup A$ называется *первичным* $\sqcup$-*идемпотентом*, если $A \nsubseteq E'$, и *вторичным* $\sqcup$-*идемпотентом*, если $A \subseteq E'$.

Любая булева матрица произвольного размера порождает *вторичные идемпотенты правого типа*: $A^{\mathcal{R}} = A \sqcup A'^T$, $A_{\mathcal{R}} = (A^{\mathcal{R}})'^T = A \sqcap A'^T$ и *левого типа*: $A^{\mathcal{L}} = A'^T \sqcup A$, $A_{\mathcal{L}} = (A^{\mathcal{L}})'^T = A'^T \sqcap A$. Причём матрицы $A^{\mathcal{R}}$ и $A^{\mathcal{L}}$ являются вторичными $\sqcap$-идемпотентами, а $A_{\mathcal{R}}$ и $A_{\mathcal{L}}$ являются вторичными $\sqcup$-идемпотентами [1, 2].

Теорема 1. *Пусть A — идемпотент частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$. Матрица A является первичным $\sqcap$-идемпотентом тогда и только тогда, когда $A \subsetneqq A^{\mathcal{R}}$ и $A \subsetneqq A^{\mathcal{L}}$, и является вторичным $\sqcap$-идемпотентом тогда и только тогда $A = A^{\mathcal{R}} = A^{\mathcal{L}}$.*

Теорема 2. *Если матрицы A и B порождают один и тот же правый главный идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$ (или полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcup \rangle$) то $A^{\mathcal{R}} = B^{\mathcal{R}}$, что равносильно равенству $A_{\mathcal{R}} = B_{\mathcal{R}}$. Если матрицы A и B порождают левый идеал, то это влечет совпадение вторичных идемпотентов левого типа: $A^{\mathcal{L}} = B^{\mathcal{L}}$, $A_{\mathcal{L}} = B_{\mathcal{L}}$.*

Следующие равенства указывают свойства вторичных идемпотентов.

$$A^{\mathcal{L}} = (A_{\mathcal{L}})'^T = (A'^T)^{\mathcal{R}}) = A^{\mathcal{L}} \sqcup A_{\mathcal{L}} = A_{\mathcal{L}} \sqcup A^{\mathcal{L}} =$$
$$= (A^{\mathcal{L}})^{\mathcal{L}} = (A^{\mathcal{L}})^{\mathcal{R}} = (A_{\mathcal{L}})^{\mathcal{L}} = (A_{\mathcal{L}})^{\mathcal{R}},$$
$$A^{\mathcal{R}} = (A_{\mathcal{R}})'^T = (A'^T)^{\mathcal{L}}) = A^{\mathcal{R}} \sqcup A_{\mathcal{R}} = A_{\mathcal{R}} \sqcup A^{\mathcal{R}} =$$
$$= (A^{\mathcal{R}})^{\mathcal{R}} = (A^{\mathcal{R}})^{\mathcal{L}} = (A_{\mathcal{R}})^{\mathcal{R}} = (A_{\mathcal{R}})^{\mathcal{L}}.$$

Свойства $A_{\mathcal{L}}$ и $A_{\mathcal{R}}$ записываются аналогично двойственным образом.

Известно, что вторичные идемпотенты играют главную роль в вопросах разрешимости простейших матричных уравнений, делимости, регулярности матриц, порождаемости односторонних идеалов, поиска транзитивно-рефлексивных замыканий и пр. [1, 2].

Частичная полугруппа $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$ разбивается на непересекающиеся $\mathbf{D}$-классы Грина двусторонних идеалов. В следующем утверждении обсуждается взаимное расположение вторичных $\sqcap$- и $\sqcup$-идемпотентов в двусторонних идеалах ($\mathbf{D}$-классах) частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$.

Теорема 3. *Пусть $A_{\mathcal{L}}$ и $A^{\mathcal{L}}$ порождают один и тот же двусторонний идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, тогда матрицы A и A'^T порождают тот же двусторонний идеал. Причём,если $A_{\mathcal{L}}$ и $A^{\mathcal{L}}$ порождают один и тот же левый идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, то матрица A порождает тот же левый идеал идеал, и, если $A_{\mathcal{L}}$ и $A^{\mathcal{L}}$ порождают один и тот же правый идеал частичной полугруппы $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$, то матрица A'^T порождает тот же правый идеал.*

Аналогичное утверждение можно сформулировать для $A_{\mathcal{R}}$ и $A^{\mathcal{R}}$, меняя местами слова "левый"и "правый".

Заметим, что, учитывая теорему 2, в каждом левом или правом идеале частичной полугруппе $\langle \mathbf{M}^n(\mathbf{B}), \sqcap \rangle$ может находиться только один вторичный $\sqcap$-идемпотент, либо $\sqcup$-идемпотент.

Вторичные $\sqcap$- и $\sqcup$-идемпотенты располагаются достаточно "плотно"в множестве $\mathbf{M}^n(\mathbf{B})$. Так каждый левый или правый идеал частичной полугруппы $\langle \mathbf{M}^3(\{0,1\}), \sqcap \rangle$ порождается либо вторичным $\sqcap$-идемпотентом, либо вторичным $\sqcup$-идемпотентом. Это означает , что любая матрица $\{0,1\}$-матрица (размера с 1×1 по 3×3) может только лишь "элементарными"преобразованиями строк (или столбцов) быть приведена либо к $\sqcap$-идемпотентной матрице с единицами на главной диагонали, либо к $\sqcup$-идемпотентной матрице с нулями на главной диагонали.

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.

2. Поплавский В. Б. Об идемпотентах алгебры булевых матриц // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. — 2012. — Т. 12, вып. 2. — С. 26–33.

О ТРАНЗИЕНТНЫХ ВЗВЕШИВАНИЯХ БЕСКОНЕЧНЫХ СИЛЬНО СВЯЗНЫХ ОРГРАФОВ

С. В. Савченко (Черноголовка)

Пусть $\mathcal{D}$ — счетный орграф и w — его *взвешивание*, т.е. положительная функция на его дугах. Для *взвешенного орграфа* $(\mathcal{D}, w)$ обозначим через $A_w(\mathcal{D})$ его *весовую матрицу смежности*. По определению $A_w(\mathcal{D})(u, v) = w(u, v)$, если (u, v) — дуга в $\mathcal{D}$, и $A_w(\mathcal{D})(u, v) = 0$ в противном случае. Таким образом, если w тождественно равно 1 на дугах $\mathcal{D}$, то $A_w(\mathcal{D})$ совпадает с обычной матрицей смежности орграфа $\mathcal{D}$. Определим ее *"внутренний"спектральный радиус* $\lambda(\mathcal{D}, w)$ как супремум спектральных радиусов конечных главных подматриц в $A_w(\mathcal{D})$ (или, то же самое, весовых матриц смежности конечных взвешенных подорграфов в $(\mathcal{D}, w)$). Мы будем рассматривать только случай, когда $\lambda(\mathcal{D}, w) < \infty$. Тогда, очевидно, будет конечен и супремум $\lambda^{(n)}(\mathcal{D}, w)$ спектральных радиусов главных подматриц порядка n в $A_w(\mathcal{D})$ (или, то же самое, весовых матриц смежности взвешенных подорграфов порядка n в $(\mathcal{D}, w)$). Очевидно, последовательность $\lambda^{(n)}(\mathcal{D}, w)$ не убывает (по n) и сходится к $\lambda(\mathcal{D}, w)$. В работе исследуется поведение величины

$$\Delta^{(n)}(\mathcal{D}, w) = n\big(\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w)\big)$$

и даются ответы на некоторые вопросы, впервые поставленные в [1].

В дальнейшем мы всегда будем считать, что исходный орграф $\mathcal{D}$ является *сильно связным*. В этом случае он содержит по крайней мере один (ориентированный) *цикл* (т.е. сильно связный подорграф, из каждой вершины которого выходит ровно одна дуга) и, следовательно, $\lambda(\mathcal{D}, w) > 0$ для любого взвешивания w, определенного на $\mathcal{D}$. Мы скажем, что множество W вершин в $\mathcal{D}$ является *цикловой трансверсалью*, если орграф $\mathcal{D} - W$ (полученный удалением всех вершин подмножества W из $\mathcal{D}$ вместе с инцидентными им дугами) вообще не имеет никаких циклов.

Взвешивание w назовем *транзиентным*, если бесконечный ряд $\sum\limits_{m=0}^{\infty} A_w^m(\mathcal{D})\lambda(\mathcal{D}, w)^{-m}$ сходится (поэлементно). Множество всех таких взвешиваний орграфа $\mathcal{D}$ обозначим через $\mathcal{T}(\mathcal{D})$. Если ряд расходится, то взвешивание w называется *рекуррентным*. Для конечного орграфа любое его взвешивание рекуррентно. Таким образом, транзиентность w означает, что взвешенный орграф $(\mathcal{D}, w)$ далек по своим рекуррентным (аналитическим) свойствам от конечного

случая. Можно было бы ожидать, что при $w \in \mathcal{T}(\mathcal{D})$ разность $\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w)$ убывает к нулю достаточно медленно. Однако, оказывается, что в классе $\mathcal{T}(\mathcal{D})$ для величины $\Delta^{(n)}(\mathcal{D}, w)$ всегда справедлива следующая альтернатива.

Теорема 1. *При фиксированном $\mathcal{D}$ или для любой положительной функции $g(n)$ найдется взвешивание $w \in \mathcal{T}(\mathcal{D})$ такое, что $\Delta^{(n)}(\mathcal{D}, w) < g(n)$ при каждом $n \geq 1$, или для любого $w \in \mathcal{T}(\mathcal{D})$ существует положительная константа c_w, независящая от n, такая, что $\Delta^{(n)}(\mathcal{D}, w) > c_w$. Последняя альтернатива имеет место тогда и только тогда, когда $\mathcal{D}$ допускает конечную цикловую трансверсаль.*

Заметим, что во втором случае мы также неявно считаем, что орграф $\mathcal{D}$ содержит цикл какой угодно большой длины: иначе в силу теоремы Ван Кира, доказанной в [2], множество $\mathcal{T}(\mathcal{D})$ пусто и, следовательно, и говорить не о чем. Пока мы не в состоянии доказать, что для любого $\mathcal{D}$ с конечной цикловой трансверсалью существует $w \in \mathcal{T}(\mathcal{D})$ такое, что $\Delta^{(n)}(\mathcal{D}, w) < C_w$ при некоторой $C_w > 0$. Однако, можно довольно просто показать, что для любой положительной функции $g(n)$ с $\limsup g(n) = \infty$ всегда найдутся $\mathcal{D}$, все циклы которого проходят через одну вершину, и $w \in \mathcal{T}(\mathcal{D})$ такие, что $\Delta^{(n)}(\mathcal{D}, w) < g(n)$ при бесконечно многих n. Это, в частности, показывает, что для справедливости теоремы 1 множитель n в $\Delta^n(\mathcal{D}, w)$ нельзя, вообще говоря, заменить на n^α, где $0 < \alpha < 1$.

В силу теоремы 1 только при наличии конечной цикловой трансверсали у $\mathcal{D}$ мы можем всегда быть уверенными в том, что достаточно быстрая сходимость $\lambda^{(n)}(\mathcal{D}, w)$ к $\lambda(\mathcal{D}, w)$ влечет хорошие рекуррентные свойства w.

Следствие. *Предположим, что $\mathcal{D}$ допускает конечную цикловую трансверсаль и $\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w) = o(n^{-1})$. Тогда взвешивание w является рекуррентным.*

В приложениях (особенно в теории вероятностей) наиболее важным является понятие *положительной рекуррентности*. По определению, она имеет место тогда и только тогда, когда последовательность $A_w^m(\mathcal{D})\lambda(\mathcal{D}, w)^{-m}$ не сходится к нулю. Замечательно, что в этом случае оба уравнения $A_w(\mathcal{D})\vec{\xi} = \lambda(\mathcal{D}, w)\vec{\xi}$ и $A_w^\top(\mathcal{D})\vec{\eta} = \lambda(\mathcal{D}, w)\vec{\eta}$ имеют положительные решения, скалярное произведение которых конечно.

Гипотеза. *Предположим, что $\mathcal{D}$ допускает конечную цикловую трансверсаль и $\lambda(\mathcal{D}, w) - \lambda^{(n)}(\mathcal{D}, w) = o(n^{-2})$. Тогда взвешивание w является положительно рекуррентным.*

В отличие от рекуррентного случая для транзиентного w матрица $A_w(\mathcal{D})$ не обязана иметь положительные собственные векторы. Для того, чтобы предъявить достаточное условие на $\mathcal{D}$, при котором это справедливо при каждом $w \in \mathcal{T}(\mathcal{D})$, нам понадобится новое определение. Скажем, что последовательность различных вершин $\{v_m\}_{m=0}^{\infty}$ образует *бесконечный вперед путь*, если при любом $m \geq 0$ пара (v_m, v_{m+1}) является дугой в $\mathcal{D}$. Используя идеи доказательства теоремы 1 из [3], можно показать справедливость следующего утверждения.

Предложение. *Пусть $\mathcal{D}$ не содержит бесконечного вперед пути. Тогда для любого $w \in \mathcal{T}(\mathcal{D})$ весовая матрица смежности $A_w(\mathcal{D})$ не имеет положительного собственного вектора.*

Таким образом, как ни странно, транзиентность взвешивания w и наличие у $\mathcal{D}$ некоторых важных свойств конечного орграфа (существование конечной цикловой трансверсали, отсутствие бесконечного вперед пути) влекут плохие спектральные свойства матрицы $A_w(\mathcal{D})$ (достаточно медленная сходимость $\lambda^{(n)}(\mathcal{D}, w)$ к своему пределу $\lambda(\mathcal{D}, w)$, отсутствие положительных собственных векторов). На данный момент мы не имеем простого объяснения этого достаточно противоречивого факта.

Список литературы

1. Seneta E. Finite approximations to infinite non-negative matrices // Mathematical Proceedings of the Cambridge Philosophical Society. — 1967. — V. 63. — P. 983–992.

2. Cyr V. Countable Markov shifts with transient potentials // Proceedings of the London Mathematical Society. — 2011. — V. 103. — P. 923–949.

3. Harris T. E. Transient Markov chains with stationary measures // Proceedings of the American Mathematical Society. — 1957. — V. 8. — P. 937–942.

О КЛИКОВЫХ ПОКРЫТИЯХ РЕБЕР В ГРАФАХ С ОГРАНИЧЕНИЯМИ СТЕПЕНЕЙ ВЕРШИН

С. Н. Селезнева, М. В. Мельник (Москва)

В работе найден критерий единственности тупикового кликового покрытия ребер для графов, в которых степени всех вершин не превышают четырех.

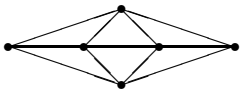
Графом G назовем пару множеств (V, E), где V — множество вершин, E — множество ребер, причем каждому ребру $e \in E$ поставлена в соответствие неупорядоченная пара (v, w) различных вершин, и разным ребрам сопоставлены различные пары вершин. *Степенью* вершины $v \in V$ в графе $G = (V, E)$ назовем величину $d_G(v) = |\{(v, w) \mid w \in V, (v, w) \in E\}|$. Пусть $\Delta(G) = \max\limits_{v \in V} d_G(v)$ обозначает наибольшую степень вершин в графе G.

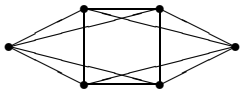
Если $K \subseteq V$, то множество K называется *кликой* в графе $G = (V, E)$, если из $v, w \in K$, $v \neq w$, следует $(v, w) \in E$. Клика K называется *максимальной*, если из $u \in V \setminus K$ следует, что множество $K \cup \{u\}$ не является кликой. Множество максимальных клик $T = \{K_1, \ldots, K_m\}$ называется *кликовым покрытием ребер* (КПР) в графе $G = (V, E)$, если из $(v, w) \in E$ следует, что найдется такой номер j, $1 \leq j \leq m$, что $v, w \in K_j$. КПР называется *тупиковым* КПР (ТКПР), если при удалении из него любой клики оставшееся множество не является КПР. ТПКР называется *кратчайшим*, если оно содержит наименее возможное число клик.

Задача о существовании в произвольном графе $G = (V, E)$ КПР мощности, не превосходящей M, где число M подается на вход алгоритма вместе с графом G, является NP-полной [1].

В работе рассматриваются графы, в которых степени всех вершин не превосходят четырех.

Пусть Γ_α и Γ_β — графы, изображенные ниже.

Γ_α : 

Γ_β : 

Если $G = (V, E)$, и $V' \subseteq V$, то граф $G' = (V', E')$, где $E' = \{(v, w) \in E \mid v, w \in V'\}$, назовем *порожденным* подграфом графа G.

Теорема 1. *В графе $G = (V, E)$ с $\Delta(G) \leq 4$ ТКПР единственно тогда и только тогда, когда этот граф не содержит порожденных подграфов, изоморфных Γ_α или Γ_β.*

Следствие. *В графе $G = (V, E)$ с $\Delta(G) \leq 3$ ТКПР единственно.*

Теорема 2. *Существует полиномиальный алгоритм, который в произвольном графе $G = (V, E)$ с $\Delta(G) \leq 4$ находит его кратчайшее ТКПР.*

Работа частично поддержана РФФИ, грант 16–01–00593-а.

Список литературы

1. Kou L. T., Stockmeyer L. J., Wong C. K. Covering edges by cliques with regard to keyword conflicts and intersection graphs // Comm. ACM. — 1978. — V. 21. — P. 135–138.

ГРАФЫ, НЕ ДОПУСКАЮЩИЕ (a, d)-ДИСТАНЦИОННУЮ АНТИМАГИЧЕСКУЮ РАЗМЕТКУ

М. Ф. Семенюта (Кировоград)

За последние 20 лет появилось большое количество разных типов и подтипов разметок, с которыми можно ознакомится в электронном журнале Д. Галлиана [1]. Будем рассматривать конечные неориентированные графы без кратных ребер и петель. Под весом $w(u)$ вершины u графа $G = (V, E)$, при вершинной разметке f, понимаем сумму меток вершин, смежных с u, то есть $w(u) = \sum_{v \in N(u)} f(v)$, где $v \in V(G)$, а $N(u)$ — множество смежности вершины u.

Будем называть (a, d)-дистанционной антимагической разметкой графа $G = (V, E)$ порядка n такую биекцию $f : V(G) \to \{1, 2, \ldots, n\}$, для которой множество всех вершинных весов образует арифметическую прогрессию a, $a+d$, $a+2d$, $\ldots$, $a+(n-1)d$ с первым членом a и разностью d, где a, d — фиксированные неотрицательные целые числа и $a \geq 1$, $d \geq 0$. Граф G, допускающий такую разметку, называют (a, d)-дистанционным антимагическим графом.

С. Арумугам и Н. Камачи, предложившие данную разметку, получили несколько базовых результатов [2]. Установили необходимое условие существования (a, d)-дистанционной антимагической разметки графа, доказали, что цикл C_n будет (a, d)-дистанционным антимагическим графом только при нечетном n и $d = 1$, а граф C_{2n}^{+} является $(2n + 2, 1)$-дистанционным антимагическим графом. Следующий шаг сделан в работе [3], где исследуются на дистанционную антимагичность цепи P_n при $2 \leq n \leq 15$, дизъюнктивное объединение изоморфных копий цикла C_n и графы с порядком меньшим 6. Для (a, d)-дистанционного антимагического графа множества смежности любых двух вершин не должны быть равными [2]. Это дает

возможность установить те типы графов, которые не допускают данной разметки. К ним относятся некоторые мультидольные графы, также графы, содержащие не меньше двух висячих ребер, смежных одной и той же вершине. Следующие теоремы расширяют семейство таких графов.

Теорема 1. *Если граф G содержит цикл $abcd$ с $\deg a = \deg c = 2$, то G не является (a, d)-дистанционным антимагическим графом.*

Доказательство. В графе G множества смежности $N(a) = \{b, d\}$ и $N(c) = \{b, d\}$ совпадают. Из этого следует, что для него не существует (a, d)-дистанционной антимагической разметки. Теорема доказана.

Теорема 2. *Если $a \leq 2$, то корона $P_n \circ P_1$ не допускает $(a, 1)$-дистанционной антимагической разметки для $n \geq 2$.*

Доказательство. Обозначим $V(P_n \circ P_1) = \{u_1, u_2, u_3, \ldots, u_n, v_1, v_2, \ldots, v_n\}$ множество вершин короны $P_n \circ P_1$, где $\{u_1, u_2, \ldots, u_n\}$ и $\{v_1, v_2, \ldots, v_n\}$ — множество вершин копии P_n и n копий P_1, соответственно. Допустим, что существует (a, d) - дистанционная антимагическая разметка f короны $P_n \circ P_1$. Запишем веса вершин, полученные при наличии разметки f

$$w(v_i) = f(u_i),$$

$$w(u_1) = f(v_1) + f(u_2),\ w(u_2) = f(v_2) + f(u_1) + f(u_3),\ \ldots,$$

$$w(u_n) = f(v_n) + f(u_{n-1}),$$

где $i = 1, 2, \ldots, n$.

Найдем суму весов всех вершин:

$$\sum_{i=1}^{n} w(u_i) + \sum_{i=1}^{n} w(v_i) = 2an + dn(2n - 1)$$

или

$$2\sum_{i=1}^{n} f(u_i) + n(2n + 1) - (f(u_1) + f(u_n)) = 2an + dn(2n - 1)$$

(d не может принимать значения 1 или 2.)

Пусть $d = 1$, тогда

$$2\sum_{i=1}^{n} f(u_i) = 2an - 2n + (f(u_1) + f(u_n)).$$

Так как $f(u_1) + f(u_n) \leq 4n - 1$, получим

$$2\sum_{i=1}^{n} f(u_i) \leq 2an + 2n - 1.$$

С другой стороны $2\sum_{i=1}^{n} f(u_i) \geq n(n+1)$. Таким образом, должно выполняться двойное неравенство:

$$n(n+1) \leq 2\sum_{i=1}^{n} f(u_i) \leq 2an + 2n - 1.$$

Это, в свою очередь, означает, что $n(n+1) \leq 2an + 2n - 1$ или $n(n-2a-1) \leq -1$. Последнее неравенство может быть верным только при $n < 2a + 1$.

Случай, когда $a = 1$ не рассматриваем, так как граф может быть (1, 1)-дистанционным антимагическим только если каждая его компонента является изоморфным образом P_2 [1]. Пусть $a = 2$, тогда n может принимать значения 2, 3, 4.

Если $n = 2$ и $V(P_2 \circ P_1) = \{u_1, u_2, v_1, v_2\}$, тогда метку 2 можно присвоить только одной из вершин u_1 или u_2. Предположим, что $f(u_1) = 2$, получим уравнение $2f(u_2) + f(v_1) + f(v_2) = 6$, не имеющее решений на множестве $\{1, 3, 4\}$.

Если $n = 3$ и $V(P_3 \circ P_1) = \{u_1, u_2, u_3, v_1, v_2, v_3\}$, тогда метку 2 можно присвоить только одной из вершин u_1, u_2 или u_3. Без потери общности, предположим $f(u_1) = 2$, получим уравнение $3f(u_2) + 3f(u_3) + f(v_1) + f(v_2)f(v_3) = 17$, не имеющее решений на множестве $\{1, 3, 4, 5, 6\}$. Аналогично для $n = 4$, уравнение

$$3f(u_2) + 3f(u_3) + 2f(u_4) + f(v_1) + f(v_2)f(v_3) + f(v_4) = 32$$

не имеет решений на множестве $\{1, 3, 4, 5, 6, 7, 8\}$. Таким образом, корона $P_n \circ P_1$ не допускает $(a, 1)$-дистанционной антимагической разметки, если $a \leq 2$. Теорема доказана.

Список литературы

1. Gallian J. A. A dynamic survey of graph labeling // The electronic journal of combinatorics. — 2015. — 18. — P. 157–163.

2. Arumugam S., Kamatchi N. On $(a; d)$-distance antimagic graphs // Australasian journal of combinatorics. — 2012. — Vol. 54. — P. 279–287.

3. Nalliah M. Antimagic labelings of graphs and digraphs: Ph. D. thesis. — The National Centre for Advanced Research in Discrete Mathematics, University of Kalasalingam, 2014.

О НЕКОТОРЫХ КОНСТРУКЦИЯХ *SD*-ГРАФОВ

З. А. Шерман (Киев)

Данная работа посвящена квадратной разностной разметке графа, которая впервые была введена в 2012 году Аджифа, Принси, Локеш и Ранжини [1].

Под графом понимаем конечный неориентированный граф без петель и кратных ребер. Пусть $G = (V, E)$ — граф с множеством вершин $V(G)$ и множеством ребер $E(G)$. Будем считать, что $|V(G)| = p$, $|E(G)| = q$.

Функцию f называют квадратной разностной разметкой графа G с p вершинами, если f — биекция из $V(G)$ на множество $\{0, 1, 2, ..., p-1\}$ и индуцируемая ею реберная разметка $f^*(u, v) = |[f(u)]^2[f(v)]^2|$ является инъекцией из $E(G)$ в множество натуральных чисел. Граф, допускающий квадратную разностную разметку, называется квадратным разностным графом или *SD графом*.

Исследуются на наличие квадратной разностной разметки такие типы графов как цепное соединение циклов и дизъюнктивное объединение звезд. Так же доказано существование квадратной разностной разметки дизъюнктивного объединения любого SD графа с цепью.

Теорема 1. *Произвольное цепное соединение n копий цикла C_3 является квадратным разностным графом для любого натурального n.*

Теорема 2. *Дизъюнктивное объединение звезд K_{1,n_i} , где $i = 1, 2, ..., m$ допускает квадратную разностную разметку для любых натуральных m и n_i.*

Теорема 3. *Дизъюнктивное объединение любого SD графа G с цепью P_k, является квадратным разностным графом для любого k.*

Список литературы

1. Ajitha V., Princy K. L., Lokesha V. and Ranjini P. S. On square difference Graphs // Int. J. of Mathematical Combinatorics — 2012. — Vol. 1, i. 1. — P. 31–40.

Секция «Математическая теория интеллектуальных систем»

К ВОПРОСУ О ВОССТАНОВЛЕНИИ ТРЕХМЕРНОГО ТЕЛА ПО ЕГО ПЛОСКИМ ПРОЕКЦИЯМ

Д. В. Алексеев (Москва)

В данной работе рассматривается задача восстановления тела по двум плоским проекциям. В работах [3, 4] описан процесс восстановления тела по плоским проекциям с точностью до аффинной эквивалентности. В [1, 2] описаны оптимизированные алгоритмы решения этой задачи. В указанных работах не приводится критерия возможности восстановления тела, т.е. условия, позволяющие по двум наборам точек определить, являются ли они проекциями одного и того же трехмерного тела. В данной работе такой критерий приводится в теореме 1.

Также рассматривается более сложная задача восстановления трехмерного тела с точностью до метрической эквивалентности проекции. Задача состоит в том, что надо построить трехмерное тело и задать две плоскости и два направления проектирования так, чтобы проекции были равны данным (как геометрические фигуры). Эта задача решается в теореме 2.

Определение 1. Будем называть *изображением* (двумерным) произвольный занумерованный набор (непустое конечное множество) точек на плоскости.

Определение 2. Будем называть *телом* произвольный занумерованный набор (непустое конечное множество) точек в трехмерном пространстве (с указанием порядка).

Определение 3. Пусть дано двухмерное изображение, состоящее из n точек $\mathcal{A} = (A_1, \ldots, A_n)$. Кроме того, пусть задан вектор $\bar{p}$ и прямая l, не параллельная вектору $\bar{p}$. Будем называть такие прямые (не параллельные $\bar{p}$) *допустимыми*. Рассмотрим прямые a_i, проходящие через соответствующие точки A_i параллельно вектору $\bar{p}$ $(i = 1, \ldots, n)$. Проекцией изображения $\mathcal{A}$ по направлению $\bar{p}$ на прямую l называется изображение $\mathcal{A}' = A'_1, \ldots, A'_n$, в котором A'_i есть точка пересечения прямых a_i и l $(i = 1, \ldots, n)$. Пусть на

прямой l введена система координат, тогда вектор координат точек $X(A'_1), \ldots, X(A'_n)$ будем называть *отпечатком* множества $\mathcal{A}$ и обозначать $F_{l,p}(\mathcal{A})$.

Определение 4. Пусть дано 3-мерное изображение, состоящее из n точек $\mathcal{A} = (A_1, \ldots, A_n)$. Кроме того, пусть задан вектор $\bar{p}$ и плоскость Π, не параллельная вектору $\bar{p}$. Рассмотрим прямые a_i, проходящие через соответствующие точки A_i, $i = 1, \ldots, n$, параллельно вектору $\bar{p}$. *Проекцией* изображения $\mathcal{A}$ по направлению $\bar{p}$ на плоскость Π называется изображение $\mathcal{A}' = A'_1, \ldots, A'_n$, в котором A'_i есть точка пересечения прямой a_i с плоскостью Π $(i = 1, \ldots, n)$.

В работе рассматриваются следующие задачи:

Задача 1. Пусть даны два плоских изображения. Построить трехмерное тело и указать плоскости и направления проектирования, такие, что проекции указанного тела на эти плоскости аффинно эквивалентны данным плоским изображениям.

Задача 2. Пусть даны два плоских изображения. Построить трехмерное тело и указать плоскости и направления проектирования, такие, что проекции указанного тела на эти плоскости метрически эквивалентны данным плоским изображениям. Т.е. существуют изометрические преобразования, переводящие проекции в данные изображения.

Определение 5. *Условие коллинеарности двух проекций.* Пусть заданы изображения $\mathcal{A}' = (A'_1, \ldots, A'_n)$ и $\mathcal{A}'' = (A''_1, \ldots, A''_n)$. Пусть в изображениях $\mathcal{A}'$ и $\mathcal{A}''$ точки $A'_{i_1}, A'_{i_2}, A'_{i_3}$ не лежат на одной прямой и $A''_{i_1}, A''_{i_2}, A''_{i_3}$ не лежат на одной прямой. Рассмотрим аффинное отображение $\mathcal{T}$, которое переводит $\mathcal{T} : A'_{i_1} \mapsto A''_{i_1}$, $\mathcal{T} : A'_{i_2} \mapsto A''_{i_2}$, $\mathcal{T} : A'_{i_2} \mapsto A''_{i_2}$. Будем говорить, что изображения $\mathcal{A}'$ и $\mathcal{A}''$ *коллинеарны* относительно точек i_1, i_2, i_3, если все векторы $\mathcal{T}(A'_i)A''_i$ попарно взаимно коллинеарны (нулевой вектор коллинеарен любому). Будем это обозначать как $\mathcal{A}' \|_{i_1,i_2,i_3} \mathcal{A}''$.

Теорема 1. *Пусть заданы изображения* $\mathcal{A}' = (A'_1, \ldots, A'_n)$ *и* $\mathcal{A}'' = (A''_1, \ldots, A''_n)$. *Пусть в изображениях* $\mathcal{A}'$ *и* $\mathcal{A}''$ *выбраны по* 4 *соответствующие точки (не ограничивая общности можно считать, что их индексы* $1, 2, 3, 4$*), обладающие следующими свойствами: a) Первые три* A'_1, A'_2, A'_3 *не лежат на одной прямой и* A''_1, A''_2, A''_3 *не лежат на одной прямой. b) Изображения* $A'_1A'_2A'_3A'_4$ *и* $A''_1A''_2A''_3A''_4$ *не являются аффинно-эквивалентными. Тогда необходимым и достаточном условием существования решения Задачи* 1 *(восстановления с точностью до аффинной эквивалентности) является условие коллинеарности изображений* $\mathcal{A}'$ *и* $\mathcal{A}''$ *относитель-*

но тройки A_1, A_2, A_3.

Теорема 2. *Пусть заданы изображения* $\mathcal{A}' = (A'_1, \ldots, A'_n)$ *и* $\mathcal{A}'' = (A''_1, \ldots, A''_n)$. *Пусть в изображениях* $\mathcal{A}'$ *и* $\mathcal{A}''$ *выбраны по* 4 *соответствующие точки* (*не ограничивая общности, можно считать, что их индексы равны* $1, 2, 3, 4$)*, обладающие следующими свойствами: a*) *Первые три точки* A'_1, A'_2, A'_3 *не лежат на одной прямой и точки* A''_1, A''_2, A''_3 *не лежат на одной прямой. b*) *Изображения* $A'_1A'_2A'_3A'_4$ *и* $A''_1A''_2A''_3A''_4$ *не являются аффинно-эквивалентными. Тогда необходимым и достаточном условием существования решения Задачи* 2 (*восстановления с точностью до метрической эквивалентности*) *является условие коллинеарности изображений* $\mathcal{A}'$ *и* $\mathcal{A}''$ *относительно тройки* A_1, A_2, A_3.

Автор выражает благодарность проф. В. Н. Козлову за ценные замечания и внимание к работе.

Список литературы

1. Алексеев Д. В. Использование метода В. Н. Козлова в образовательном процессе на кафедре МаТИС // Интеллектуальные системы — 2013. — Т. 17, № 1–4. — С. 16–20.

2. Алексеев Д. В. К вопросу о восстановлении тела по плоским проекциям // Интеллектуальные системы. Теория и приложения — Т. 18, № 3. — С. 47–60.

3. Козлов В. Н. Элементы математической теории зрительного восприятия. — М.: Изд-во ЦПИ при мех.-мат. ф-те МГУ, 2001.

4. Kozlov V. Mathematical model of reconstructing a three-dimensional image from plane projections // Pattern Recognition and Image Analysis. — 2011. — Vol. 2. — P. 279–282.

5. Kozlov V. Conclusiveness and heuristics in visual recognition // Pattern Recognition and Image Analysis. — 2014. — Vol. 24, iss. 4. — P. 1–7.

ТОЧНАЯ ПАРАМЕТРО-ЭФФЕКТИВНАЯ РАСШИФРОВКА ЛИНЕЙНЫХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

А. В. Быстрыгова (Ташкент)

Точную расшифровку функции можно наглядно представлять как игру между учеником и учителем, когда учитель загадал функцию из некоторого класса, известного ученику, а ученик, задавая

запросы учителю, должен полностью восстановить вектор значений загаданной функции.

Под параметро-эффективной расшифровкой понимают расшифровку функций, существенно зависящих от малого числа переменных.

Пусть $\Psi(k)$ — некоторый класс функций k-значной логики ($k \geqslant 2$). Под *запросом на значение* к функции $f \in \Psi(k)$ будем понимать вектор (набор) $a \in E^n, E = \{0, 1, \ldots, k-1\}$. Под *ответом на запрос на значение* будем понимать значение $f(a)$.

Под *запросом на сравнение* к функции $f \in \Psi(k)$ будем понимать пару (a, b), $a, b \in E^n$, $E = \{0, 1, \ldots, k-1\}$. Под *ответом на запрос на сравнение* будем понимать значение

$$\operatorname{sign}(f(a) - f(b)) = \begin{cases} 1 & \text{если } f(a) > f(b) \\ 0 & \text{если } f(a) = f(b) \\ -1 & \text{если } f(a) < f(b) \end{cases}$$

В данной работе рассматривается точная параметро-эффективная расшифровка запросами на значение и запросами на сравнение функций вида $f(x_0, x_1, \ldots, x_{n-1}) = c_0x_0 + c_1x_1 + \ldots + c_{n-1}x_{n-1}$, $c_i, x_i \in \{0, 1, 2, \ldots, k-1\}$, $|\{i : c_i \neq 0\}| = p$, где «+» — операция сложения по модулю k.

При рассмотрении расшифровки запросами на значение будем в обозначениях дописывать индекс $_V$, запросами на сравнение — $_C$.

Под *алгоритмом расшифровки* будем понимать условный эксперимент, который последовательно генерирует запросы к функции в зависимости от ответов на предыдущие запросы. Будем говорить, что *алгоритм расшифровывает функцию* f, если значения функции на наборах, сгенерированных условным экспериментом, однозначно определяют таблицу значений функции f. Обозначим множество алгоритмов расшифровки класса $\Psi(k)$ через $\mathcal{A}(\Psi(k))$.

Пусть $A \in \mathcal{A}(\Psi(k))$, $f \in \Psi(k)$, тогда обозначим через $\varphi(A, f)$ число запросов на значение функции, требуемое алгоритму A для расшифровки функции f. Будем называть $\varphi(A, f)$ *сложностью алгоритма* A *на функции* f. Положим

$$\varphi(k, n, p) = \min_{A \in \mathcal{A}(\Psi(k))} \max_{f \in \Psi^{p,n}(k)} \varphi(A, f).$$

В работе [1] получены получены оценки сложности расшифровки запросами на значение линейных булевых функций для случаев $p = 2$ и $p = 3$, отличающиеся от точного значения не более чем на 2.

В работе [2] была рассмотрена задача точной расшифровки линейных булевых функций запросами на значение, получена верхняя оценка сложности $p \log n + p$.

В данной работе получены верхние и нижние оценки сложности параметро-эффективной расшифровки запросами на значение и запросами на сравнение линейных функций k-значной логики с нулевым свободным членом. При стремлении числа переменных к бесконечности получен порядок сложности расшифровки для обоих типов запросов.

Теорема 1. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k > 2)$ *имеет место следующее неравенство*

$$\varphi_V(k, n, p) \leqslant 1 + (p-1) \cdot (\rceil \log_2 (k-1) \lceil + \rceil \log_2 (n-1) \rceil) + p \rceil \log_2 n \lceil.$$

Теорема 2. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k \geqslant 2)$ *имеют место следующие неравенства:*

$$\begin{aligned} \varphi_C(k, n, p) \quad \leqslant \quad & 1 + (p-1) \cdot (\rceil \log_2 (k-1) \lceil + \rceil \log_2 (n-1) \rceil) + \\ & p \rceil \log_2 n \lceil + p \cdot \rceil \log_2 k \lceil, \text{ если } k > 2; \end{aligned}$$

$$\varphi_C(2, n, p) \leqslant 1 + (p-1) \cdot \rceil \log_2 (n-1) \lceil + p \rceil \log_2 n \lceil.$$

Теорема 3. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k \geqslant 2)$ *имеет место следующее неравенство*

$$\varphi_V(k, n, p) \geqslant p \log_2 (k-1) + p \cdot \log_2 (n-p+1) - \log_2 p.$$

Теорема 4. *Для любых натуральных* n, k, p $(n > 2,\ 1 \leqslant p < n/2,\ k \geqslant 2)$ *имеет место следующее неравенство*

$$\varphi_C(k, n, p) \geqslant p \log_2 (k-1) + p \cdot \log_2 (n-p+1) - \log_2 p.$$

Из теорем 1–4 получаем следующее

Следствие. $\varphi_V(k, n, p) = \varphi_C(k, n, p) = O(p \log n)$ *при* $n \longrightarrow \infty$.

Автор выражает благодарность научному руководителю, д.ф.-м.н. профессору Э. Э. Гасанову за постановку задачи и помощь в работе.

Список литературы

1. Быстрыгова А. В. Сложность расшифровки линейных булевых функций // Интеллектуальные системы. — 2015. — Т. 19, вып. 3. — С. 101–126.

2. Hofmeister T. An application of codes to attribute-efficient learning // EuroCOLT'99 Proceedings of the 4th European Conference on Computational Learning Theory, 1999.

О СТАБИЛИЗАЦИИ АВТОНОМНОЙ МОДЕЛИ МИГРАЦИОННЫХ ПРОЦЕССОВ

Д. И. Васильев (Москва)

В работе рассматривается модель, предсказывающая миграцию населения внутри страны в зависимости от уровня зарплат. В качестве сети городов рассматривается граф, вершинам которого приписано текущее число людей в нём, максимальное число людей, которое может в нем находиться и невозрастающая по количеству людей функция зарплаты. На каждом шаге выбирается пара городов, и, если это выгодно, один из работников переезжает из одного города в другой. Формализуем это следующим образом:

Если $m \in N$, то обозначим $N_m = \{0, 1, \ldots, m\}$.

Пусть $G = (V, E)$ — полный граф без петель с n вершинами, т. е. $V = \{1, 2, \ldots, n\}$, $E = \{\{v_1, v_2\} : v_1, v_2 \in V, v_1 \neq v_2\}$. Пусть каждой вершине графа приписана тройка: (m_i, q_i, f_i), где $m_i \in N$, $q_i \in N_{m_i}$, $f_i : N_{m_i} \to N$, причем f_i невозрастающая функция, т.е. для любых $a, b \in N_{m_i}$ если $a \geqslant b$, то $f_i(a) \leqslant f_i(b))$, $i \in \{1, 2, \ldots, n\}$.

Обозначим $Q(G) := \{q = (q_1, q_2, \ldots, q_n) : q_i \in N_{m_i}, i \in \{1, 2, \ldots, n\}\}$, $\mathcal{G}^n$ — множество всех таким образом нагруженных полных графов без петель с n вершинами.

В дальнейшем для удобства восприятия вершины графа будем интерпретировать как города, для каждого города $i \in \{1, 2, \ldots, n\}$ число m_i будет восприниматься как максимально возможное число людей в городе, q_i — текущее число людей в городе, f_i — функция зарплат в i-м городе в зависимости от числа проживающих в городе людей. Вектор $q = (q_1, q_2, \ldots, q_n)$ будем называть *состоянием* графа G.

Рассмотрим автомат без выходов $A^G = (E, Q(G), \varphi, q_0)$, где E — входной алфавит, $Q(G)$ — алфавит состояний, $\varphi : Q(G) \times E \to Q(G)$ — функция переходов, q_0 — начальное состояние. Автомат A^G задается канонической системой

$$\begin{cases} q(1) = q_0, \\ q(t+1) = \varphi(q(t), v(t)), \end{cases}$$

где для $q = (q_1, q_2, \ldots, q_n)$, $v = \{v_1, v_2\}$,

$$\varphi(q, v) = \begin{cases} q', \text{ если } f_{v_2}(q_{v_2} + 1) > f_{v_1}(q_{v_1}), q_{v_2} < m_{v_2}, q_{v_1} > 0, \\ q'', \text{ если } f_{v_1}(q_{v_1} + 1) > f_{v_2}(q_{v_2}), q_{v_1} < m_{v_1}, q_{v_2} > 0, \\ q \text{ в остальных случаях,} \end{cases} \quad (1)$$

$$q' = (q_1, \ldots, q_{v_1-1}, q_{v_1} - 1, q_{v_1+1}, \ldots, q_{v_2-1}, q_{v_2} + 1, q_{v_2+1}, \ldots, q_n),$$

$$q'' = (q_1, \ldots, q_{v_1-1}, q_{v_1} + 1, q_{v_1+1}, \ldots, q_{v_2-1}, q_{v_2} - 1, q_{v_2+1}, \ldots, q_n).$$

В нашей интерпретации функция переходов устроена таким образом, что для пары городов v_1, v_2, если зарплата в городе v_2 после увеличения числа жителей на единицу больше, чем зарплата в городе v_1, то из города v_1 один человек переезжает в город v_2.

Через E^* будем обозначать множество всех слов в алфавите E. Через E^∞ будем обозначать множество всех сверхслов в алфавите E.

Расширим функцию φ на $Q(G) \times E^*$, а именно, если $\alpha \in E^*$, $v \in E$, то индуктивно определим

$$\varphi(q, \alpha v) = \varphi(\varphi(q, \alpha), v).$$

Пусть $\alpha \in E^\infty$, α_t — первые t символов сверхслова α. Определим

$$A^G(\alpha) = \begin{cases} \lim\limits_{t \to \infty} \varphi(q_0, \alpha_t), \text{ если такой предел существует,} \\ * \text{ — в противном случае.} \end{cases}$$

Теорема. *Для любого графа G из $\mathcal{G}^n$, любого сверхслова α из E^∞ имеем $A^G(\alpha) \neq *$.*

Пусть граф G находится в состоянии q и пусть в этом состоянии в городах s различных значений зарплат f_1,f_2,...,f_s, причём $f_1 < f_2 < ... < f_s$. Пусть r_i это количество городов, зарплата в которых равна f_i, $i = 1, 2, ..., s$. Понятно, что $\sum\limits_{i=1}^{s} r_i = n$. Сопоставим состоянию q вектор пар $ord_G(q) = ((f_1, r_1), \ldots, (f_s, r_s))$.

Введём на парах (f_i, r_i) следующий линейный порядок:

- если $f^i > f^j$, то $(f^i, r^i) > (f^j, r^j)$ независимо от r^i и r^j;
- если $f^i = f^j$, то $(f^i, r^i) > (f^j, r^j)$ точно тогда, когда $r^i < r^j$.

Введём лексикографический порядок на множестве всех векторов, состоящих из таких пар.

Лемма. *Для любых $G \in \mathcal{G}^n$, $q \in Q$, $\{a, b\} \in E$ если $\varphi(q, \{a, b\}) \neq q$, то $ord_G(\varphi(q, \{a, b\})) > ord_G(q)$.*

Для определённости будем считать, что мигранты переезжают из города a в город b, то есть $f_a(q_a) < f_b(q_b + 1)$, $q_b < m_b$, $q_a > 0$. Пусть количество городов с зарплатой $f_a(q_a)$ равно r_a, а количество городов с зарплатой $f_b(q_b)$ равно r_b. Пусть $(f_a(q_a), r_a)$ является i-ым элементом вектора $ord_G(q)$, а $(f_b(q_b), r_b)$ является j-ым элементом этого вектора. Поскольку $f_b(q_b + 1) \leqslant f_b(q_b)$, то $f_a(q_a) < f_b(q_b)$ и значит $i < j$. Обозначим пару, являщуюся $i+1$-м элементом вектора $ord_G(q)$, через (f_c, r_c). Возможно $f_c = f_b$, тогда $r_c = r_b$ и $j = i + 1$.

Обозначим через r' число городов, зарплата в которых равна $f_b(q_b + 1)$, если таких городов нет, то $r' = 0$. Обозначим $q^+ = \varphi(q, \{a, b\})$.

Когда один мигрант переезжает в город b, зарплата там становится $f_b(q_b+1)$, то есть в $ord_G(q^+)$ появляется пара $(f_b(q_b+1), r'+1)$. Поскольку $f_b(q_b+1) > f_a(q_a)$, то позиция этой пары в $ord_G(q^+)$ будет не меньше чем i, причём эта пара окажется в i-ой позиции вектора только если $r_a = 1$ и $f_b(q_b + 1) \leq f_c$. Равенство $r_a = 1$ означает, что после отъезда одного мигранта из города a, не останется городов с зарплатой $f_a(q_a)$, и следовательно, на i-ю позицию переместится пара со значением зарплаты $\min(f_a(q_b + 1), f_c)$, которое больше, чем $f_a(q_a)$.

Если же $r_a > 1$, то после отъезда одного мигранта из города a число городов с зарплатой $f_a(q_a)$ уменьшится как минимум на 1, а зарплата в городе a останется прежней, либо возрастёт, то есть на i-ой позиции вектора $ord_G(q^+)$ окажется пара со значением зарплаты $\min(f_a(q_a - 1), f_c)$, которое больше чем $f_a(q_a)$.

Следовательно, $ord_G(q)$ и $ord_G(q^+)$ совпадают до $(i-1)$-й позиции включительно, а в i-й позиции в $ord_G(q^+)$ стоит большая пара, то есть $ord_G(q^+) > ord_G(q)$.

Докажем теорему. Предположим, что значение функции $q(t)$ изменяется бесконечное число раз с ростом t. . Тогда по доказанной лемме $ord_G(q(t))$ неограниченно возрастает, что невозможно, так как множество различных векторов $ord_G(q)$ конечно. Значит, значение $q(t)$ может меняться конечное число раз. Теорема доказана.

ЧАСТИЧНОЕ ПРОГНОЗИРОВАНИЕ ОБЩЕРЕГУЛЯРНЫХ СВЕРХСОБЫТИЙ В МНОГОЗНАЧНОМ АЛФАВИТЕ

И. К. Ведерников (Москва)

В статье А. Г. Вереникина и Э. Э. Гасанова [1] были введены прогнозирующие автоматы — конечные автоматы, предсказывающие сверхслово или множество сверхслов. Автомат прогнозирует сверхслово, если через некоторое конечное время после начала подачи сверхслова, он начинает угадывать каждый следующий символ, то есть на выходе в момент времени t выдавать элемент входной последовательности под номером $t+1$.

В работе [2] А. А. Мастихиной было введено понятие частичного прогнозирования, а в работе [3] для общерегулярных сверхсобытий в двоичном алфавите получен критерий прогнозируемости.

В данной работе исследуется частичная прогнозируемость в многозначных алфавитах, получен критерий.

Введем основные определения.

Определение. Пусть $E_k = \{0, 1, \ldots, k-1\}$ — конечный алфавит. Через E_k^* и E_k^∞ обозначим соответственно множество всех слов конечной длины и множество всех сверхслов в алфавите E_k. По определению будем считать, что пустое слово Λ принадлежит E_k^*. Подмножества E_k^* называются *событиями*, а подмножества E_k^∞ — *сверхсобытиями*.

Определение. Если R_1 — событие и R_2 — событие или сверхсобытие, то через R_1R_2 обозначим их *произведение*, то есть все слова (сверхслова) вида $\alpha\beta$, где $\alpha \in R_1, \beta \in R_2$.

Определение. Если R — событие, то R^* — *итерация* события R, то есть $R^* = R \cup R^2 \cup R^3 \cup \ldots \cup R^i \ldots$, а R^∞ — *сверхитерация* события R, $R^\infty = \{\alpha_1\alpha_2\alpha_3 \ldots | \ \alpha_i \in R, i = 1, 2, 3 \ldots\}$.

Если α — сверхслово в алфавите E_k, n — натуральное число, то n-ую букву сверхслова α будем обозначать $\alpha(n)$, а через $\alpha]_n$ обозначим префикс длины n сверхслова α, т.е. $\alpha]_n = \alpha(1)\alpha(2)\ldots\alpha(n)$.

В работе рассматриваются конечные инициальные автоматы $V = (E_k, Q, E_k, \varphi, \psi, q_0)$, где $E_k = \{0, 1, \ldots, k-1\}$ — входной и выходной алфавит, Q — множество состояний, которое является конечным подмножеством некоторого фиксированного счетного множества, $\varphi : Q \times E_k \to Q$ — функция переходов, $\psi : Q \times E_k \to E_k$ — функция выходов, q_0 — начальное состояние.

Функции φ и ψ естественно расширяются на $Q \times E_k^*$, а именно, если $\alpha \in E_k^*$, $a \in E_k$, то индуктивно определим $\varphi(q, \alpha a) =$

$\varphi(\varphi(q,\alpha),a)$, $\psi(q,\alpha a) = \psi(\varphi(q,\alpha),a)$. Введем также обозначения $\overline{\varphi}(q,\alpha) = \varphi(q,\alpha]_1)\varphi(q,\alpha]_2)\dots\varphi(q,\alpha)$, если α — слово, а если α — сверхслово, то $\overline{\varphi}(q,\alpha) = \varphi(q,\alpha]_1)\varphi(q,\alpha]_2)\dots\varphi(q,\alpha]_n)\dots$. Аналогичные обозначения вводятся для функции выходов.

Определение. Если α — сверхслово в алфавите A, то *пределом* сверхслова α назовем такое множество $A' \subseteq A$, что в сверхслове α бесконечное число раз встречаются символы из A' и только они. Этот факт будем обозначать через $A' = \lim\alpha$.

Определение. Сверхсобытие R *представимо* автоматом $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ с помощью семейства F, $F \subseteq 2^Q$, тогда и только тогда, когда для любого $\alpha \in R$, существует $Q' \in F$, такое, что $\lim\overline{\varphi}(q_0,\alpha) = Q'$.

Определение. Будем говорить, что символ $\alpha(t+1)$ сверхслова $\alpha = \alpha(1)\alpha(2)\dots\alpha(t+1)\dots$ *угадан* автоматом $V = (A, Q, B, \varphi, \psi, q_0)$, если $\psi(q,\alpha]_t) = \alpha(t+1)$.

Определение. Пусть $\alpha \in E_k^\infty$, обозначим $\sigma_\alpha = \underline{\lim}_{n\to\infty} N/n$, где N — количество угаданных автоматом V символов в слове $\alpha]_n$. Будем говорить, что σ_α – *степень прогнозирования* слова α автоматом V.

Считаем, что множество слов *частично прогнозируемо*, если существует такой автомат, что степень прогнозирования для каждого сверхслова множества строго больше нуля.

Определение. *Регулярное событие* над алфавитом E_k.

1. $\varnothing, \{a\}, a \in E_k$, — регулярные события.

2. Пусть R_1, R_2 являются регулярными событиями. Тогда события $R_1R_2, R_1 \cup R_2, R_1^*$ также регулярны.

Определение. *Общерегулярное сверхсобытие* над алфавитом E_k.

1. Если R — регулярное событие над алфавитом E_k, то R^* — общерегулярное сверхсобытие над алфавитом E_k.

2. Если R_1 — регулярное событие над алфавитом E_k, R_2 — общерегулярное сверхсобытие над алфавитом E_k, то R_1R_2 — общерегулярное сверхсобытие над алфавитом E_k.

3. Если R_1, R_2 — общерегулярные сверхсобытия над алфавитом E_k, то $R_1 \cup R_2$ — общерегулярное сверхсобытие над алфавитом E_k.

Определение. *Сильно связным множеством* назовем такое множество состояний C, $C \subseteq Q$, автомата $V = (E_k, Q, E_k, \varphi, \psi, q_0)$, что для любых $q', q'' \in C$ найдется такое слово α из E_k^*, что $\varphi(q',\alpha) = q''$ и $\overline{\varphi}(q',\alpha) \in C^*$, т.е. по слову α автомат переходит из состояний q' в состояние q'', проходя только состояния из C. Множество, состоящее из одного состояния, по определению считается сильно связным.

Определение. Любое сильно связное множество состояний мощности более одного назовем *автоматным циклом*. Одноэлементное множество состояний $C = \{q\}$ является *автоматным циклом* только если существует символ a из E_k, что $\varphi(q, a) = q$. *Длиной автоматного цикла* назовем число состояний в автоматном цикле.

Определение. *Состоянием выхода* для автоматного цикла C назовем такое состояние q, что существует единственное a, $a \in E_k$, такое, что $\varphi(q, a) \in C$.

Теорема. *Общерегулярное сверхсобытие, представимое конечным инициальным автоматом $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ с помощью некоторого семейства F, $F \subset 2^Q$, частично прогнозируемо, тогда и только тогда, когда для любого $Q' \in F$ и для любого автоматного цикла C, $C \subseteq Q'$, существует состояние выхода.*

Автор выражает благодарность профессору Э. Э. Гасанову и доценту А. А. Мастихиной за постановку задачи и помощь в работе.

Список литературы

1. Вереникин А. Г., Гасанов Э. Э. Об автоматной детерминизации множеств сверхслов // Дискретная математика. — 2006. — Т. 18, вып. 2. — С. 84–97.

2. Мастихина А. А. О частичном угадывании сверхслов // Интеллектуальные системы. — 2007. — Т. 11, вып. 1–4. — С. 561–572.

3. Мастихина А. А. Критерий частичного предвосхищения общерегулярных сверхсобытий // Дискретная математика. — 2011. — Т. 23, вып. 4 — С. 103–114.

РЕКОНФИГУРИРУЕМЫЙ НА ЛЕТУ АППАРАТНЫЙ БЧХ ДЕКОДЕР

Э. Э. Гасанов, П. А. Пантелеев (Москва)

Бинарные БЧХ коды представляют собой мощный класс помехоустойчивых кодов. Они имеют широкий диапазон применений в системах оптической и беспроводной связи, в магнитной записи и т.д.

Рассмотрим алгоритм декодирования БЧХ. Вход БЧХ декодера есть кодовое слово $(c_{n-1}, \ldots, c_0)$, где каждый символ $c_i \in \{0, 1\}$. Кодовое слово будем также задавать полиномом $c(x) = c_{n-1}x^{n-1} +$

$\ldots + c_1 x + c_0$. Этот полином используется модулем вычисления синдромов (Syndrome Calculation, SC), который вычисляет $2t$ синдромов $S_1, S_2, \ldots, S_{2t}$ следующим образом: $S_i = c(\alpha^i)$, $i = 1, 2, \ldots, 2t$, где t — максимальное число ошибок, которое БЧХ код может исправить, а α — примитивный элемент поля расширения $GF(2^m)$, связанного с этим кодом БЧХ. В этом случае длина кодового слова равна $n = 2^m - 1$. Затем эти синдромы приходят к модулю решения ключевых уравнений (Key Equation Solver, KES), который вычисляет полином локаторов ошибок $\Lambda(x)$, корнями которого являются позиции ошибок. Затем модуль коррекции ошибок (Error Correction, EC), используя $\Lambda(x)$, корректирует позиции ошибок в кодовом слове, сохраняемом в специальном модуле FIFO (очередь).

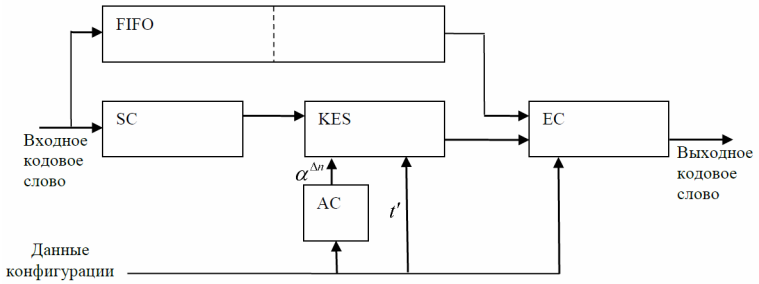


Рис. 4: Схема конфигурируемого БЧХ декодера

Большинство реализаций БЧХ декодеров не позволяют пользователю изменять параметры БЧХ кода, такие как максимальное число ошибок и длина кодового слова. Однако современные приложения кодов БЧХ в контроллерах твердотельных дисков (solid-state disk, SSD) делают необходимым изменение этих параметров во время функционирования. При этом, чтобы достичь быстрой скорости, время изменения конфигурации такого контроллера должно быть как можно меньше. Поэтому реконфигурируемые декодеры должны иметь специальный вход (см. рис.1) под названием "Данные конфигурации". Он состоит из пары (n', t'), где n' — текущая длина кодового слова, t' — текущее максимальное число исправляемых ошибок.

В данной работе мы предлагаем новую реконфигурируемую на лету аппаратную схему БЧХ декодера. Это означает, что изменение конфигурации в этой конструкции может быть сделано за константное число тактов, независящее от длины кодового слова и числа исправляемых ошибок.

Не трудно изменить схему 1 так, чтобы она могла обрабатывать БЧХ коды с числом ошибок $t' < t$. Единственное отличие состоит в том, что KES блок должен выполнять $2t'$ итераций вместо $2t$. Но если мы хотим использовать БЧХ код с другой длиной $n' < n$, то мы должны использовать усеченные коды БЧХ. Это означает, что вместо кодового слова полной длины $(c_{n-1}, \ldots, c_0)$ на вход БЧХ декодера будет поступать усеченное кодовое слово $(c_{n'-1}, \ldots, c_0)$, которое можно рассматривать как кодовое слово полной длины $(c_{n'-1}, \ldots, c_0, 0 \ldots, 0)$ или в полиномиальной форме $c(x) = x^{\Delta n} c'(x)$, где $c'(x) = c_{n'-1}x^{n'-1} + \ldots + c_1 x + c_0$ и $\Delta n = n - n' = 2^m - 1 - n'$. Следовательно, если мы будем использовать стандартную схему для вычисления синдромов, то она вместо синдромов $S_i = c(\alpha^i) = \alpha^{i\Delta n} c'(\alpha^i)$, $i = 1, 2, \ldots, 2t$ произведет значения $S'_i = c'(\alpha_i)$. Так что, если мы хотим получить правильные значения синдромов $S_1, S_2, \ldots, S_{2t}$, то мы должны сначала вычислить значения $S'_1, S'_2, \ldots, S'_{2t}$, а затем использовать формулу $S_i = \alpha^{i\Delta n} S'_i$, $i = 1, 2, \ldots, 2t$. Основная проблема состоит в том, что Δn зависит от параметра конфигурации n' — текущей длины кодового слова, и значение $\alpha^{\Delta n}$ не может быть вычислено за небольшое фиксированное число тактов, поскольку величина Δn может быть очень большой.

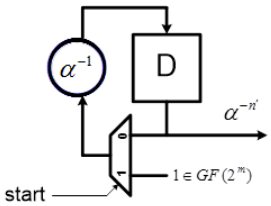


Рис. 5: Схема Альфа Калькулятора

Основная идея данной работы заключается в вычислении значения $\alpha^{\Delta n}$ одновременно с вычислением синдромов $S'_1, S'_2, \ldots, S'_{2t}$. Для того, чтобы упростить вычисление $\alpha^{\Delta n}$, заметим, что $\alpha^{\Delta n} = \alpha^{2^m - 1 - n'} = \alpha^{-n'}$ так как $\alpha^{2^m - 1} = 1$ в поле $GF(2^m)$. Так что для того, чтобы вычислить $\alpha^{-n'}$, мы можем использовать константный умножитель в поле $GF(2^m)$, который выполняет умножение на α^{-1}. Модуль, который выполняет эти вычисления, называется Альфа Калькулятором (Alpha Calculator, AC) и реализован, как показано на рис.2. Если сигнал start $= 1$, то вычисления запускаются. Модуль

AC работает одновременно с модулем SC (см. рис.1) и в конце вычислений он производит значение $\alpha^{-n'}$.

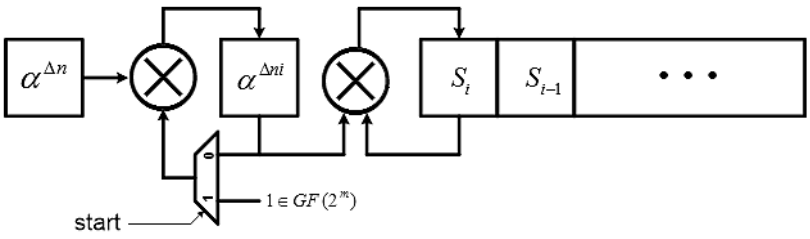


Рис. 6: Схема обновления синдромов

После того, как значение $\alpha^{-n'}$ получено, оно подается на KES блок (см. рис.1). В нашей реализации модуля KES значения синдромов $S_1, S_2, \ldots, S_{2t}$ используются последовательно. На первой итерации используется только S_1, на второй — только S_1, S_2, и т.д. Поэтому, мы имеем достаточно времени, чтобы вычислить все значения $S_1 = \alpha^{\Delta n} S'_1, S_2 = \alpha^{2\Delta n} S'_2, \ldots, S_{2t} = \alpha^{2t\Delta n} S'_{2t}$, используя только два умножителя в поле $GF(2^m)$, как показано на рис.3. На этом рисунке сигнал "start" выводится из блока SC и если start = 1, то это означает, что модули SC и AC закончили свои расчеты и модуль KES должен начать работать.

Список литературы

1. Panteleev P. A., Gasanov E. E., Neznanov I. V., Sokolov A. P., Shutkin Yu. A. Reconfigurable BCH decoder. United States Patent: 8,621,329, December 31, 2013.

СВОЙСТВА АФИННО ЭКВИВАЛЕНТНЫХ ПЛОСКИХ ИЗОБРАЖЕНИЙ

В. Н. Козлов (Москва)

Изображение — это конечное множество точек на плоскости. Кодом изображения A называем пару $\langle M_A, T_A \rangle$, в которой M_A — множество номеров точек изображения, T_A — множество всех чисел вида $\rho_{mnu,ksp} = S_{mnu}/S_{ksp}$, где S_{mnu} и S_{ksp} — площади треугольников с

вершинами в точках соответственно m, n, u и k, s, p. При $S_{ksp} = 0$ полагаем $\rho_{mnu,ksp}$ неопределенным. Изображения A и B с кодами $\langle M_A, T_A\rangle$ и $\langle M_B, T_B\rangle$ называем эквивалентными, если существует такая биекция $\psi : M_A \to M_B$, что $\rho_{mnu,ksp} = \rho_{\psi(m)\psi(n)\psi(u),\psi(k)\psi(s)\psi(p)}$. Если все точки изображения не лежат на одной прямой или двух параллельных прямых, то изображение называем плоским.

Теорема 1 [2]. *Два плоских изображения эквивалентны тогда и только тогда, когда они аффинно эквивалентны.*

Содержательно теорема 1 означает, в частности, что код изображения задает его с точностью до аффинных преобразований.

Пусть B есть часть изображения A. Если код для A есть $\langle M_A, T_A\rangle$, то, очевидно, код $\langle M_B, T_B\rangle$ можно получить, если собрать в M_B номера из M_A всех точек, вошедших в B, и собрав в T_B все те $\rho_{mnu,ksp}$ из T_A, для которых m, n, u, k, s, p вошли в M_B. Говорим в этом случае, что код $\langle M_B, T_B\rangle$ есть часть кода $\langle M_A, T_A\rangle$.

Известно, что для построения изображения A по коду $\langle M_A, T_A\rangle$ достаточно таких элементов $\rho_{mnu,ksp}$ из T_A, у которых тройки mnu и ksp разнятся только одним номером. Возникает вопрос: какова может быть роль других элементов $\rho_{mnu,ksp}$ в коде?

Назовем изображения A и B эквидистантными, если существует такая биекция $\psi : M_A \to M_B$, при которой для любых точек с номерами m, n, u из M_A (не лежащих на одной прямой), число $\rho_{mnu,\psi(m)\psi(n)\psi(u)}$ есть константа, не зависящая от выбора точек m, n, u.

Название «эквидистантные изображения» объясняется следующей аналогией с более простым случаем. Пусть A и B есть изображения, совместимые параллельным переносом. Тогда, очевидно, существует биекция $\psi : M_A \to M_B$ такая, что все расстояния $r(a, \psi(a))$ между соответствующими точками двух изображений одинаковы. Отрезки $r(a, \psi(a))$ для всех a из M_A в этом случае не только равны, но и параллельны. Очевидно, имеет место и обратное: если все эти отрезки равны и параллельны, то A и B совместимы параллельным переносом.

Теорема 2. *Два плоских изображения эквидистантны тогда и только тогда, когда они аффинно эквивалентны.*

Доказательство. Пусть A и B аффинно эквивалентны. Тогда существует такая биекция $\psi : M_A \to M_B$, что B переводится в B', совмещенное с A, т. е. при этом каждая точка a из A совмещена с точкой $\psi(a)$. Ясно, что при этом для каждой тройки m, n, u из A (не лежащих на одной прямой) и соответствующей тройки k', s', p' из B' (здесь $k' = \psi(m)$, $s' = \psi(n)$, $p' = \psi(u)$) имеем $\rho_{mnu,k's'p'} =$

$S_{mnu}/S_{k's'p'} = q$. Вернем теперь обратным преобразованием B' в B. При этом площадь каждого треугольника с вершинами $k's'p'$ из B' при переводе в треугольник ksp с вершинами из B умножится на одну и ту же для всех треугольников величину q. Следовательно $\rho_{mnu,ksp} = S_{mnu}/S_{ksp} = S_{mnu}/(qS_{k's'p'}) = 1/q$.

Пусть теперь A и B эквидистантны. Если B' получено из B аффинным преобразованием, то нетрудно видеть, A и B' тоже эквидистантны. Выберем некоторые три точки (не на одной прямой) m, n, u на A, и пусть преобразованное B' таково, что его точки k', s', p', соответствующие точкам m, n, u, совпали с ними, т. е. площади треугольников mnu и $k's'p'$ равны. Но тогда, с учетом эквидистантности, должны быть равны площади и всех остальных соответствующих друг другу треугольников из A и B'. Однако это значит, что коды $\langle M_A, T_A\rangle$ и $\langle M_{B'}, T_{B'}\rangle$ эквивалентны, и, значит, в силу теоремы 1, изображения A и B' аффинно эквивалентны. Но тогда аффинно эквивалентны и изображения A и B. Теорема доказана.

Таким образом, нами прояснена роль элементов $\rho_{mnu,ksp}$ кода с полностью различными тройками mnu и ksp. Роль элементов с двумя различиями в этих тройках пока не ясна.

Список литературы

1. Крушинский Л. В., Кудрявцев В. Б., Козлов В. Н. О некоторых результатах применения математики к моделированию в биологии // Математические вопросы кибернетики. Вып. 1. — 1988. — С. 52–88.

2. Козлов В. Н. Введение в математическую теорию зрительного восприятия. — М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2007.

ВЫДЕЛЕНИЕ ОБЩЕЙ ПОДФОРМУЛЫ ФОРМУЛ ИСЧИСЛЕНИЯ ПРЕДИКАТОВ ДЛЯ РЕШЕНИЯ РЯДА ЗАДАЧ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Т. М. Косовская (Санкт-Петербург)

Рассматриваются задачи искусственного интеллекта при логико-предметном подходе в следующей постановке. Исследуемый объект является конечным множеством $\omega = \{\omega_1, \ldots, \omega_t\}$. На элементах ω

задан набор предикатов $p_1, \ldots, p_n$, характеризующих свойства и отношения между элементами объекта ω. Задано разбиение множества Ω всех исследуемых объектов на K (возможно пересекающихся) классов $\Omega = \bigcup_{k=1}^{K} \Omega_k$. Логическим описанием класса Ω_k называется бескванторная формула в ДНФ $A_k(\overline{x})$, такая что если $A_k(\overline{\omega})$ (где $\overline{\omega}$ – некоторая перестановка элементов из ω), то $\omega \in \Omega_k$. Логическим описанием $S(\omega)$ объекта ω называется набор всех истинных постоянных атомарных формул вида $p_i(\overline{\tau})$ или $\neg p_i(\overline{\tau})$, выписанных для всех возможных частей τ объекта ω. В рамках логико-предметного подхода основными задачами являются следующие.

Задача идентификации. Проверить, принадлежит ли объект ω или его часть классу Ω_k.

$$S(\omega) \Rightarrow \exists \overline{x}_{\neq} A_k(\overline{x})$$

Задача классификации. Найти все такие номера классов k, что $\omega \in \Omega_k$.

$$S(\omega) \Rightarrow \vee_{k=1}^{K} A_k(\overline{\omega}).$$

Задача анализа сложного объекта.

$$S(\omega) \Rightarrow \vee_{k=1}^{K} \exists \overline{x_k}_{\neq} A_k(\overline{\omega}).$$

В [1, 2] доказаны экспоненциальные оценки числа шагов алгоритмов, решающих сформулированные задачи. В зависимости от алгоритма (алгоритм полного перебора и алгоритмы, основанные на доказательстве выводимости в исчислении предикатов) в показателе экспоненты стоит либо число аргументов в описании класса, либо количество атомарных формул в описании класса. Там же доказана NP-трудность рассматриваемых задач.

Для уменьшения числа шагов решения рассматриваемых задач в [3] предложено понятие многоуровневого описания классов, заключающееся в выделении достаточно «коротких» общих с точностью до имён переменных подформул у элементарных конъюнкций, составляющих описания классов. Такие подформулы являются обобщёнными признаками объектов, присущих многим объектам из одного класса. Там же доказаны оценки уменьшения числа шагов для рассматриваемых алгоритмов.

До последнего времени не было алгоритма, позволяющего выделять такие подформулы, но эвристически найденные подформулы показывали существенное уменьшение числа шагов.

Для задачи распознавания объектов с неполной информацией в [4] было предложено понятие неполной выводимости. Это понятие

оказалось удобным для выделения «коротких» общих с точностью до имён переменных подформул у элементарных конъюнкций, составляющих описания классов [5].

Автоматическое выделение требуемых подформул позволило разработать понятие самокорректирующейся предикатной сети, в которой имеется два блока: обучающий («долго» работающий) блок, в котором автоматически по обучающей выборке строятся многоуровневые описания классов, и распознающий («быстро» работающий) блок, в котором распознаются новые объекты. Если распознавание было ошибочным, то возможно дообучение сети с помощью обучающего блока. При этом структура (количество уровней и количество проверяемых формул в уровне) сети может измениться.

Выделение максимальных общих с точностью до имён аргументов подформул позволяет рассмотреть и решить следующую задачу мультиагентного описания объекта.

Имеется m агентов $a_1, \ldots, a_m$, которые могут измерить некоторые значения признаков на некоторых элементах объекта ω (то есть определить свойства некоторых элементов исследуемого объекта и некоторые отношения между этими элементами). Каждый из агентов $a_1, \ldots, a_m$ обладает информацией $I_1, \ldots, I_m$ соответственно. Информация, которой обладает каждый агент, абсолютно достоверна.

Требуется построить описание объекта ω в виде конъюнкции атомарных формул или их отрицаний, задающих свойства элементов заданного объекта и отношения между этими элементами при условии, что агент a_j может не знать реального количества элементов в объекте ω и предполагать, что он имеет дело с объектом $\omega^j = \{\omega_1^j, ...\omega_{t_j}^j\}$ (нумерация элементов у каждого агента своя, например, агенты рассматривают один и тот же объект с разных сторон).

Результатом применения алгоритма выделения максимальной общей подформула является не только сама подформула, но и унификаторы для этой подформулы и тех формул, из которых она выделена. Тем самым обеспечивается выделение общей (с точностью до имён элементов) информации, собранной разными агентами.

Оценка числа шагов работы алгоритма мультиагентного описания объекта составляет $O(t^t \cdot ||I|| \cdot m^2)$ «шагов» для алгоритма полного перебора, где t и $||I||$ — максимальные количества аргументов и атомарных формул в I_i $(i = 1, \ldots m)$ соответственно и $O(s^{||I||} \cdot ||I||^3 \cdot m^2)$ для алгоритма, основанного на поиске вывода исчислении предикатов, где s — максимальное количество атомарных формул с одним и тем же предикатом в каждой элементарной конъюнкции I_i.

Работа выполнена при финансовой поддержке РФФИ (проект № 14-08-01276).

Список литературы

1. Косовская Т. М. Доказательства оценок числа шагов решения некоторых задач распознавания образов, имеющих логические описания // Вестн. С.-Петербург. ун-та. Сер. 1. —2007. — Вып. 4. — С. 82–90.

2. Косовская Т. М. Некоторые задачи искусственного интеллекта, допускающие формализацию на языке исчисления предикатов, и оценки числа шагов их решения // Труды СПИИРАН. — 2010. — Вып. 14. — С. 58–75.

3. Косовская Т. М. Многоуровневые описания классов для уменьшения числа шагов решения задач распознавания образов, описываемых формулами исчисления предикатов // Вестн. С.-Петербург. ун-та. Сер. 10. — 2008. — Вып. 1. — С. 64–72.

4. Косовская Т. М. Частичная выводимость предикатных формул как средство распознавания объектов с неполной информацией // Вестн. С.-Петербург. ун-та. Сер. 10. — 2009. — Вып. 1. — С. 74–84.

5. Косовская Т. М. Подход к решению задачи построения многоуровневого описания классов на языке исчисления предикатов // Труды СПИИРАН. —2014. — Вып. 34. — С. 204–217.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА ДОРОГАХ

А. А. Лыков, В. А. Малышев, М. В. Меликян (Москва)

Проблеме описания и организации транспортных потоков посвящено множество работ, см. глобальный обзор [2]. Условно эти работы можно разделить на два класса: 1) макроподход, где основным является понятие потока, аналогичное потоку жидкости в трубах [1]; 2) микроподход, где основные объекты — отдельные машины и взаимодействия между ними. В микроподходе в основном это работы вероятностного характера, не касающиеся вопросов искусственного интеллекта, в которых исследуется случайность в разных ее проявлениях, даже для случайного движения машин. Детерминированному движению машин посвящено существенно меньше работ. Наша

работа лежит в рамках последнего подхода, однако отличается конкретностью модели, где можно получить явное описание областей устойчивости, как в смысле безопасности, так и эффективности.

Обозначения. Поток машин по однополосной дороге представляется точками прямой R

$$... < x_i(t) < ... < x_1(t) < x_0(t),$$

где $x_i(t)$ — координата переднего бампера машины с номером i, $v_i(t) > 0$ — скорость машины i. Машина с номером 0 (лидер) едет произвольным образом в зависимости от препятствий на дороге и от возможностей водителя. Машина с нолером i должна выдерживать расстояние до машины $i-1$.

Пусть $D(v)$ — минимально безопасное расстояние между соседними машинами. Предполагается, что оно известно и является обязательным для всех машин, то есть должно быть (для всех t и i)

$$x_{i-1}(t) - x_i(t) > D(v_i) + d_{i-1},$$

где d_i — длина машины i. Можно взять $d_i = 0$ (добавляя максимально возможное значение d_i к $D(v)$), то есть считать машины точечными частицами.

Если скорость $v_0(t) = v$ постоянна, дорога не имеет перекрестков и если все машины могут двигаться с той же скоростью, то плотность может быть $D^{-1}(v)$.Препятствия к такому движению может быть только изменение скорости впереди идущей машины. Мы разберем два случая причин такого изменения: наличие перекрестков и флуктуации движения лидера.

Перекрестки. Управление движением на перекрестках может быть двух видов: 1) светофоры, то есть циклическая остановка некоторых потоков — им посвящено максимальное число исследований, 2) без остановки движения путем уменьшения скорости и увеличения расстояния между машинами. Остановимся сначала на этом случае одного перекрестка n дорог. Пусть есть n дорог $k = 1, \ldots, n$, причем с одинаковыми расстояниями и скоростями $d_k = d, v_k = v$. Тогда существует безопасный режим движения с плотностью машин $\rho_{critical} = \frac{1}{nD(v)}$, но не существует безопасного режима с большей плотностью. Тот же результат имеет место для любого числа дорог и перекрестков при условии, что граф дорог не имеет циклов. В этом случае под n понимается максимальная из кратностей перекрестков.

Если же все n скоростей v_k и расстояний d_k допускаются различными, то определим поток машин на дороге k как

$$J_k = \rho_k v_k = \frac{v_k}{d_k}.$$

Возникает естественный вопрос: для каких v_k, d_k возможно движение такое что $d_k \geq D(v_k)$ для некоторого $D(v_k)$? А также, какими должны быть v_k, d_k, чтобы средний поток

$$J = \frac{1}{m}\sum_{k=1}^{m} J_k$$

был максимальным (здесь m общее количество дорог). Например, ответ на данный вопрос для случая двух дорог, когда $D(v_k) = D_0,\ k = 1, 2$ для некоторого D_0, имеет следующий вид.

1. Если $\frac{J_1}{J_2}$ иррационально, то такого движения не существует.

2. Пусть $\frac{J_1}{J_2} = \frac{n_1}{n_2}$, где n_1, n_2 целые такие, что $(n_1, n_2) = 1$. Тогда движение существует тогда и только тогда, когда

$$\frac{n_2}{d_1} + \frac{n_1}{d_2} < \frac{1}{D_0}. \tag{1}$$

Пусть теперь v_1, v_2 и D_0 фиксированы. Пусть $\Sigma(v_1, v_2, D_0)$ - множество всех пар (d_1, d_2), для которых существует движение. Тогда для максимального потока имеет место

$$\sup_{(d_1,d_2)\in\Sigma(v_1,v_2,d)} J(d_1, d_2) = \frac{\hat{v}}{2D_0},$$

где $\hat{v} = \frac{2}{\frac{1}{v_1}+\frac{1}{v_2}}$ — гармоническое среднее v_1 и v_2.

Если граф дорог имеет циклы, ситуация существенно более сложная, и требует более подробного описания.

Переменное движение в одном потоке. Рассматривается простейший локальный алгоритм управления, основанный на физическом принципе взаимодействия в цепочке молекул [7]. Однако, система ОДУ в нашей модели не является гамильтоновой. Каждая машина знает только свою скорость и расстояние до впереди идущей машины, однако с малым запаздыванием по времени (реакция измерительных приборов). Таким образом, выполнена система $N \leq \infty$

уравнений Ньютона с гармонической силой, удерживающей расстояние близким к d, а также (абсолютно необходимая) диссипативная сила

$$\frac{d^2x_k}{dt^2} = \omega^2(x_{k-1}(t-\epsilon_1) - x_k(t-\epsilon_1) - d) - \alpha v_k(t-\epsilon_2).$$

Обозначая расстояния между машинами $r_k(t) = z_{k-1}(t) - z_k(t)$, мы получаем для величин

$$I = \inf_{k\geqslant 1}\inf_{t\geqslant 0} r_k(t), \quad S = \sup_{k\geqslant 1}\sup_{t\geqslant 0} r_k(t)$$

большие нуля оценки снизу для I и конечные оценки сверху для S.

Выделены три области на плоскости параметров $\omega, \alpha > 0$, которые для случая $\epsilon_1 = \epsilon_2 = 0$ имеют вид: 1) $\alpha > 2\omega$, где имеет место устойчивость, 2) $\alpha < \sqrt{2}\omega$, где имеет место неустойчивость, 3) $\sqrt{2}\omega \leq \alpha \leq 2\omega$, где устойчивость имеет место только для более узкого класса начальных условий и движения лидера.

Список литературы

1. Prigogine I., Herman R. Kinetic theory of vehicular traffic. — N.Y.: Elsevier, 1971.

2. Helbing D. Traffic and related self-driven many particle systems // Rev. Mod. Phys. — 2001. — 73. — P. 1067–1141.

О НОВОЙ ВЕРСИИ АЛГОРИТМА ПОСТРОЕНИЯ БАЗИСНОГО КОНЕЧНОГО АВТОМАТА

А. А. Мельникова (Димитровград)

В статье приводится новая версия одного из возможных алгоритмов построения базисного конечного автомата, определённого и исследованного в [1] и др. Алгоритм является некоторым изменением алгоритма, приведённого в [2, 3].

Применяемые далее обозначения согласованы с [2, 4]. Дуги автоматов $\widetilde{L}$ и $\widetilde{L^R}$ будем обозначать заглавными греческими буквами,

не совпадающими по написанию с латинскими — до буквы Ξ для автомата $\widetilde{L}$ и начиная с буквы Π для автомата $\widetilde{L^R}$, а также для зеркального к последнему автомата $\left(\widetilde{L^R}\right)^R$. Для некоторой конкретной дуги Γ, идущей из вершины A в вершину B и имеющей пометку $a \in \Sigma$, будем писать $\alpha^a(\Gamma) = A$ и $\beta^a(\Gamma) = B$. Проделаем для каждой буквы a алфавита Σ следующую процедуру. Пусть δ_π^a — помеченные буквой a дуги автомата $\widetilde{L}$ (т.е. элементы множества δ_π), а δ_ρ^a — помеченные буквой a дуги автомата $\widetilde{L^R}$ (т.е. элементы множества δ_ρ). Аналогично сказанному выше, будем таким же образом обозначать соответствующее множество дуг автомата $\left(\widetilde{L^R}\right)^R$.

Рассмотрим бинарное отношение $\#^a \subseteq \delta_\pi^a \times \delta_\rho^a$, определённое следующим образом. Для некоторых $\Gamma \in \delta_\pi^a$ и $\Omega \in \delta_\rho^a$ полагаем $\Gamma \#^a \Omega$ тогда и только тогда, когда для некоторого слова $w \in L$ имеем представление $w = uav$, и при этом:

$$\begin{aligned} &u \in \mathcal{L}^{in}_{\widetilde{L}}(\alpha^a(\Gamma))\,,\ u \in \mathcal{L}^{in}_{\left(\widetilde{L^R}\right)^R}(\alpha^a(\Omega))\,,\\ &v \in \mathcal{L}^{out}_{\widetilde{L}}(\beta^a(\Gamma))\,,\ v \in \mathcal{L}^{out}_{\left(\widetilde{L^R}\right)^R}(\beta^a(\Omega))\,. \end{aligned} \tag{1}$$

Приведённое нами определение отношения $\#^a$ с помощью (1) можно рассматривать как *алгоритм* его построения.

Теорема. *Пусть $\Gamma \in \delta_\pi$ и $\Omega \in \delta_\rho$ — некоторые дуги канонических автоматов для языков L и L^R соответственно. Тогда в базисном автомате $\mathcal{BA}(L)$ имеется дуга*

$$\delta_T\Big(\big(\alpha^a(\Gamma), \alpha^a(\Omega)\big), a\Big) \ni \big(\beta^a(\Gamma), \beta^a(\Omega)\big) \tag{2}$$

тогда и только тогда, когда $\Gamma \#^a \Omega$.

Рассмотрим пример построения базисного автомата с помощью описанного здесь алгоритма. Для этого сначала приведём графы переходов автоматов $\widetilde{L}$ (исходного) и $<L>$ (соответствующего ему); они вместе с обозначениями дуг заглавными греческими буквами даны на рисунках 1 и 2 соответственно:

Теперь рассмотрим букву $a \in \Sigma$ и построим отношение $\#^a$. Наличие восьми элементов этого отношения можно показать с помощью таблицы 1.

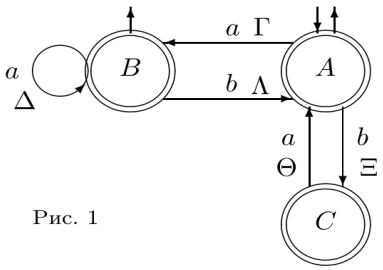


Рис. 1

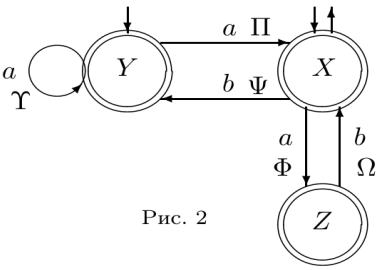


Рис. 2

$\#^a$	Π	Υ	Φ
Γ	a	$\underline{a}a$	ab
Δ	$a\underline{a}$	$a\underline{a}a$	$a\underline{a}b$
Θ	ba	$b\underline{a}a$	

Таб. 1

В таблице 1 парам дуг автоматов $\widetilde{L}$ и $<L>$ поставлены в соответствие слова рассматриваемого языка, и при этом — в случае, когда в слове более одной буквы a, — подчёркнута та буква a этого слова, читая которую автоматы (они оба — однозначные, "unambiguous automata") проходят по этим дугам. (В клетки таблицы можно вписать и другие слова рассматриваемого языка; нами выбраны минимальные по длине.)

Рассмотрим следующую таблицу 2, в которой в клетке, соответствующей паре дуг автоматов $\widetilde{L}$ и $<L>$, запишем дугу базисного автомата согласно (2):

$\#^a$	Π	Υ	Φ
Γ	$(A,Y)\to(B,X)$	$(A,Y)\to(B,Y)$	$(A,X)\to(B,Z)$
Δ	$(B,Y)\to(B,X)$	$(B,Y)\to(B,Y)$	$(B,X)\to(B,Z)$
Θ	$(C,Y)\to(A,X)$	$(C,Y)\to(A,Y)$	

Таб. 2

Для $b\in\Sigma$ построенная аналогичным образом таблица 2×2 отношения $\#^b$ содержит следующие 3 элемента:

$\#^b$	Ψ		Ω	
Λ	aab	$(B,X)\to(A,Y)$	ab	$(B,Z)\to(A,X)$
Ξ	b	$(A,X)\to(C,Y)$		

Таб. 3

Оставшиеся операции, необходимые для окончания построения базисного автомата, выполняются очевидным образом.

Список литературы

1. Vakhitova A. The basis automaton for the given regular language // The Korean Journal of Computational and Applied Mathematics. — 1999. — Vol. 6, No. 3. — P. 617–624.

2. Melnikov B., Melnikova A. A new algorithm of constructing the basis finite automaton // Informatica (Lithuania). — 2002. — Vol. 13, No. 3. — P. 299–310.

3. Мельников Б., Мельникова А. Новый алгоритм построения базисных конечных автоматов // Тезисы докладов XIII Межд. науч. конф. «Проблемы теоретической кибернетики». — 2002. — М.: Изд-во МГУ. — С. 124.

4. Мельникова А. Некоторые свойства базисного автомата // Вестник Воронежского государственного университета. Серия «Физика. Математика». — 2012. — № 2. — С. 184–189.

О СИНТАКСИЧЕСКОМ АНАЛИЗЕ НОРМАТИВНЫХ АКТОВ

Е. М. Перпер (Москва)

Под *синтаксическим анализом* текста будем понимать процесс, который по набору токенов, соответствующих словам предложения, создаёт набор синтаксических отношений между этими словами.

Токен представляет собой тройку, в которую входят: слово; *лемма* — каноническая форма слова (например, для существительного это будет то же слово, но в именительном падеже и единственном числе); набор *морфологических характеристик* (для существительного это род, падеж, число и т.д., для глагола это вид, время и т.д). Процесс построения токенов для всех слов текста называется *морфологическим анализом* текста.

Синтаксическое отношение — это отношение между парой слов предложения. Одно из слов считается в этом отношении главным, а другое — зависимым. У каждого синтаксического отношения есть название, определяемое по частям речи слов, участвующих в отношении, их морфологическим характеристикам и т.д. Например,

отношение между словами «высокое» и «дерево» называется *определительным*. Полный список синтаксических отношений приведён в [1]. Если каждому слову предложения сопоставить вершину графа, а каждому синтаксическому отношению между словами предложения — дугу, ведущую из вершины, которой соответствует главное слово отношения, в вершину, которой соответствует зависимое слово, то получившийся граф окажется ориентированным деревом. Это дерево называется *деревом зависимостей*.

Данная работа посвящена созданию программы, осуществляющей синтаксический анализ предложения, взятого из текста нормативного акта. Данный тип текстов был выбран из-за определённой бедности используемого в этих текстах языка, а также потому, что результаты работы такой программы можно применять на практике — например, для того, чтобы автоматически заполнять формы бухгалтерской отчётности, как это описано в [2].

В описываемой в работе программе синтаксический анализ осуществляется следующим образом. На вход программы поступают токены, полученные морфологическим анализатором, созданным на проекте АОТ [3]. В самой программе имеется список *правил*, которые позволяют находить синтаксические связи между словами. Для каждого токена и каждого правила проверяется, применимо ли это правило к данному токену; если применимо, то создаётся продиктованное этим правилом синтаксическое отношение.

Каждое правило состоит из трёх частей. Первая часть проверяет, подходит ли слово для этого правила: обладает ли оно нужным набором морфологических характеристик. В большинстве случаев значение леммы не проверяется, однако есть и правила, которые работают с конкретными леммами. В тех случаях, когда целью правила является построения синтаксического отношения, в котором рассматриваемое слово было бы зависимым, проверяется также, что слово ещё не является зависимым ни в каком построенном синтаксическом отношении. Объясняется эта проверка просто: каждое слово может входить в какое угодно число синтаксических отношений в качестве главного, но лишь в одно отношение — в качестве зависимого.

Вторая часть заключается в поиске слова, которое может входить в синтаксическое отношение с рассматриваемым словом. В некоторых правилах ищется не одно слово, а несколько, притом таких, что каждое из них могло бы образовывать синтаксические отношения либо с другим найденным словом, либо с рассматриваемым словом.

Наконец, третья часть строит синтаксические отношения между рассматриваемым словом и найденными словами.

Приведём пример правила. Рассмотрим правило, которое для существительного (обозначим его N_1) ищет ближайшее находящееся

после него в предложении слово, не являющееся прилагательным в родительном падеже (обозначим это слово N_2). Пусть такое слово найдено и является существительным в родительном падеже. Если между ним и N_1 в предложении нет запятых, точек с запятой и двоеточий, а закрывающих скобок не меньше, чем открывающих, то между N_1 и N_2 создаётся *квазиагентивное* синтаксическое отношение, в котором главным словом является N_1, а зависимым — N_2. Это правило, например, строит синтаксическое отношение между словами «объектам» и «средств», а также между словами «средств» и «организаций» в предложении «По объектам основных средств некоммерческих организаций амортизация не начисляется».

В настоящий момент в программе описано 31 правило, позволяющее проводить синтаксический анализ предложений нормативного акта о бухгалтерском учёте ПБУ 6/01. Продолжается тестирование программы на предложениях из нормативных актов и пополнение списка правил в тех случаях, когда имеющихся правил недостаточно для построения дерева зависимостей, однако такие случаи достаточно редки.

Автор выражает благодарность научному руководителю, профессору, д.ф.-м.н. Э. Э. Гасанову за постановку задачи и помощь в научной работе.

Список литературы

1. Синтаксически размеченный корпус русского языка: информация для пользователей. — Электронный ресурс: `www.ruscorpora.ru/instruction-syntax.html`.

2. Кудрявцев В. Б., Гасанов Э. Э., Перпер Е. М. Автоматическая генерация компьютерной программы, моделирующей нормативно-правовой акт // Интеллектуальные системы. Теория и приложения — 2014. —Т. 18, вып. 2. — С. 133–156.

3. Автоматическая обработка текста. — Электронный ресурс: `www.aot.ru`.

ЛИНЕЙНО РЕАЛИЗУЕМЫЕ АВТОМАТЫ

С. Б. Родин (Москва)

На практике часто необходимо решать задачу перехода от автоматного описания функционирования на язык схем. Например, при логическом синтезе чипов на первом этапе функционирование чипа описывается как конечный автомат. Переход к описанию на языке

схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $\{0,1\}$. При этом важно выбрать кодирование, при котором достигается возможно меньшая сложность схемы. Введем некоторые понятия.

Определение. Нумерованным автоматом назовем пятерку $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, где A-входной алфавит, $Q = \{0...n-1\}$, B-выходной алфавит, φ — функция переходов, ψ — функция выходов.

В работе изучаются автоматы с входным алфавитом $A = E_2$ и выходным алфавитом $B = E_2$

Определение. Кодированием множества $Q = \{0...n-1\}$ назовем взаимоднозначное отображение $F : \{0...n-1\} \to {E_2}^k$. Каждое кодирование F для автомата на множестве Q порождает булевский оператор [1] $\phi : {E_2}^{k+1} \to {E_2}^{k+1}$, где

$$\phi(a, \alpha_1, ..., \alpha_k) = (F(\varphi(a, F^{-1}(\alpha_1, ..., \alpha_k))), \psi(a, F^{-1}(\alpha_1, ..., \alpha_k))),$$

$$a \in A, \alpha_i \in E_2.$$

Данный оператор может быть рассмотрен как набор $k+1$ булевских функций, зависящих от $k+1$ переменной. Обозначим этот набор через $\mathcal{F}_{\mathfrak{A}}(F)$.

Определение. Если для заданного нумерованного автомата $\mathfrak{A}$ существует кодирование F, такое что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики, назовем такой автомат линейно реализуемым посредством кодирования F,или просто линейно реализуемым.

Обозначим через $X_{\mathfrak{A}} = \{s : Q \to Q \,|\, \exists a \in E_2, s(q) = \varphi(a, q)$ для любого $q \in Q\}$, а через $S_{\mathfrak{A}} =< X_{\mathfrak{A}} >$, замыкание множества $X_{\mathfrak{A}}$ относительно операции умножения подстановок [4]. Множество $S_{\mathfrak{A}}$ будем называть внутренней полугруппой переходной системы V, а $X_{\mathfrak{A}}$ — порождающим множеством внутренней полугруппы.

Поскольку входным алфавитом является E_2, то множество $X_{\mathfrak{A}}$ состоит из двух элементов. Обозначим через p_0 подстановку, соответствующую входному символу 0, через p_1 — подстановку, соответствующую входному символу 1 [4].

Определение Пусть задана подстановка $p : \{0, ..., n-1\} \to \{0, ..., n-1\}$. Положим $M_q = \{i \in \{0, ..., n-1\} | p(i) = q\}$. Через $\widetilde{p} : 2^{\{0,...,n-1\}} \to \{0, ..., n-1\}$ обозначим отображение такое, что

$$\widetilde{p}(M) = \begin{cases} q, \text{ если } M = M_q \\ \text{неопределено, в противном случае.} \end{cases}$$

Теорема 1. *Пусть задан нумерованный автомат* $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$, *где* $Q = \{0, \ldots, n-1\}$, *такой что* φ *не зависит существенным образом от входного символа.* $\mathfrak{A}$ *линейно реализуем, тогда и только тогда,когда функции, реализованные в состояниях автомата, имеют одинаковое число существенных переменных* (*то есть во всех состояниях реализуются либо* $\{x, \overline{x}\}$, *либо* $\{0, 1\}$).

Теорема 2. *Пусть задан нумерованный автомат* $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$, *где* $Q = \{0, \ldots, n-1\}$, *такой что* φ *зависит существенным образом от входного символа.* $\mathfrak{A}$ *линейно реализуем посредством кодирования* $F : Q \to E_2^k$, *тогда и только тогда,когда*

- $\widetilde{p_0}$ *и* $\widetilde{p_1}$ *— имеют одинаковую область определения;*
- $p = \widetilde{p_0}^{-1} \cdot \widetilde{p_1}$ *является перестановкой;*
- $p(q) \neq q$, $\forall q \in Q$*;*
- $p(q)$ *есть произведение независимых транспозиций;*
- *функции, реализованные в состояниях автомата, имеют одинаковое число существенных переменных* (*то есть во всех состояниях реализуются либо* $\{x, \overline{x}\}$, *либо* $\{0, 1\}$).

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

2. Лидл Р., Нидеррайтер Г. Конечные поля. — М.: Мир, 1988.

3. Карагаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1982.

4. Арбиб М. А. Декомпозиция автоматов и расширение полугрупп // Алгебраическая теория автоматов, языков и полугрупп — М.: «Статистика», 1975. — С. 46–64.

5. Родин С. Б. Линейно реализуемые переходные системы // Интеллектуальные системы. — Т. 14, вып. 1–4. — С. 491–502.

Секция «Дискретная геометрия»

О ТИПОВЫХ ЧИСЛАХ ГИПЕРПОВЕРХНОСТЕЙ КЕНМОЦУ И САСАКИ В СПЕЦИАЛЬНЫХ ЭРМИТОВЫХ МНОГООБРАЗИЯХ

М. Б. Банару (Смоленск)

Эрмитова геометрия (или геометрия почти эрмитовых многообразий) имеет теснейшие связи со многими другими областями математики. Например, относительно недавно в ней нашел приложения такой важнейший раздел дискретной математики как теория графов [1, 2]. Другое содержательное и интересное приложение дискретной математики в теории почти эрмитовых многообразий — характеризация гиперповерхностей этих многообразий в терминах типовых чисел (характеризация Такаджи—Курихары). В данной работе рассматривается именно такая характеризация гиперповерхностей Сасаки и Кенмоцу специальных эрмитовых (special Hermitian, SH-) многообразий.

Почти контактной метрической структурой на многообразии N называется [3] система тензорных полей $\{\Phi, \xi, \eta, g\}$ на этом многообразии, для которой выполняются условия:

$$\eta(\xi) = 1;\ \Phi(\xi) = 0;\ \eta \circ \Phi = 0;\ \Phi^2 = -id + \xi \otimes \eta;$$

$$\langle \Phi X, \Phi Y \rangle = \langle X, Y \rangle - \eta(X)\eta(Y),\ X, Y \in \aleph(N).$$

Здесь Φ — поле тензора типа $(1, 1)$, ξ — векторное поле, η — ковекторное поле, $g = \langle \cdot, \cdot \rangle$ — риманова метрика, $\aleph(N)$ — модуль гладких векторных полей на многообразии N. Также известно, что многообразие, допускающее почти контактную метрическую структуру, нечетномерно и ориентируемо [3].

К числу наиболее содержательных и интересных видов почти контактных метрических структур относятся структуры Кенмоцу и Сасаки, которые, как известно [4], характеризуются тождествами

$$\nabla_X(\Phi)Y = \langle \Phi X, Y \rangle \xi - \eta(Y)\Phi X,$$

$$\nabla_X(\Phi)Y = \langle X, Y\rangle\,\xi - \eta(Y)X,\ \ X, Y \in \aleph(N),$$

соответственно. Многообразия Кенмоцу и Сасаки и их различные обобщения — одна из самых популярных тематик современной контактной геометрии. Такие многообразия интенсивно исследуются как с точки зрения дифференциальной геометрии, так и теоретической физики [3]. В этой области работают известнейшие современные геометры, в частности Д. Блэр (США), В. Ф. Кириченко (Россия), Г. Питиш (Румыния) и М. М. Трипати (Индия), а также многие другие математики из разных стран.

В. Ф. Кириченко обратил внимание на то, что несмотря на внешнее сходство тождеств, определяющих структуры Сасаки и Кенмоцу, свойства многообразий Кенмоцу в определенном смысле противоположны свойствам сасакиевых многообразий [4].

Не оспаривая ни в коей мере это мотивированное утверждение, заметим только, что и сходство между свойствами многообразий Сасаки и Кенмоцу тоже немалое. Например, результаты из статей [5] и [6] о гиперповерхностях Кенмоцу и Сасаки 6-мерных эрмитовых подмногообразий алгебры октав выглядят абсолютно идентично.

Приведем еще два результата, которые с очевидностью говорят о сходстве некоторых свойств структур Кенмоцу и Сасаки.

Теорема 1. *Гиперповерхность Кенмоцу SH-многообразия является минимальной в том и только том случае, когда ее типовое число четно.*

Теорема 2. *Гиперповерхность Сасаки SH-многообразия является минимальной в том и только том случае, когда ее типовое число четно.*

Из этих теорем вытекает ряд геометрических следствий, связанных с существованием структур Кенмоцу и Сасаки на минимальных гиперповерхностях специальных эрмитовых многообразий.

Работа является продолжением исследований автора, рассматривавшего ранее характеризации Такаджи–Курихары почти контактных метрических гиперповерхностей почти эрмитовых многообразий (см., например [7–11]).

Список литературы

1. Carriazo A., Fernandez L.M. Submanifolds associated with graphs // Proc. Amer. Math. Soc. — 2004. — V. 132(11). — P. 3327–3336.

2. Carriazo A., Fernandez L.M., Rodriguez-Hidalgo A. Submanifolds weakly associated with graphs // Proc. Indian Acad. Sci. (Math. Sci.). — 2009. — V. 119, is. 3. — P. 297–318.

3. Кириченко В. Ф. Дифференциально-геометрические структуры на многообразиях. — М.: МПГУ, 2003.

4. Кириченко В. Ф. О геометрии многообразий Кенмоцу // ДАН. — 2001. — Т. 80, № 5. — С. 585–587.

5. Банару М. Б. Аксиома гиперповерхностей Кенмоцу для 6-мерных эрмитовых подмногообразий алгебры Кэли // Сибирский математический журнал. — 2014. — Т. 55, № 2. — С. 261–266.

6. Банару М. Б. Аксиома сасакиевых гиперповерхностей и 6-мерные эрмитовы подмногообразия алгебры октав // Математические заметки. — 2016. — Т. 99, № 1. — С. 140–144.

7. Банару М. Б. О типовом числе слабо косимплектических гиперповерхностей приближенно келеровых многообразий // Фундаментальная и прикладная математика. — 2002. — Т. 8, вып. 2. — С. 357–364.

8. Банару М. Б. О типовом числе косимплектических гиперповерхностей 6-мерных эрмитовых подмногообразий алгебры Кэли // Сибирский математический журнал. — 2003. — Т. 44, № 5. — С. 981–991.

9. Банару М. Б. О типовых числах почти контактных метрических гиперповерхностей почти эрмитовых многообразий // Материалы VIII Международного семинара «Дискретная математика и её приложения». — М: Изд-во механико-математического ф-та МГУ, 2004. — С. 379–381.

10. Банару М. Б. Почти контактные метрические гиперповерхности с типовым числом 1 или 0 в приближенно келеровых многообразиях // Вестник Московского университета. Сер. 1. Математика. Механика. — 2014. — № 3. — С. 60–62.

11. Банару М. Б. О почти контактных метрических гиперповерхностях с типовым числом 1 в 6-мерных келеровых подмногообразиях алгебры Кэли // Известия высших учебных заведений. Математика. — 2014. — № 10. — С. 13–18.

ГИПЕРБОЛИЧЕСКИЕ ЛИНЗОВЫЕ 3-МНОГООБРАЗИЯ НАД ПЛАТОНОВОЙ ПОВЕРХНОСТЬЮ $\{5, 5\}$ РОДА 4

Ф. Л. Дамиан (Кишинев),
В. С. Макаров, П. В. Макаров (Москва)

В сообщениях [4, 5] был обоснован метод построения гиперболических 3-многообразий исходя из предположения наличия в них вполне геодезического подмногообразия, геометрия которого известна.

Впервые такой пример был нами описан при изучении симметрических 3-подмногообразий 4-многообразия Дэвиса [2, 3]. Этот пример послужил толчком к исследованию некоторых икосаэдрических гиперболических многообразий с вполне геодезическим краем [6], для которых краем оказалась платонова поверхность [1] рода 4 и которая изящно описывается инциденциями граней большого звездного додекаэдра $\{5, 5/2\}$. Напомним, что в [6] многообразия с таким краем строились из ортогонально усеченных ромбического триаконтаэдра и икосаэдра. Если эти фундаментальные многогранники разрезать на равные многогранники призматического типа и собрать их над платоновай картой края, то мы получем 2 "многогранника", схема отождествления граней которых перенесена с указанных выше многогранников. Они аналогичны бесконечным эквидистантным многогранникам (в данном случае правильным [10]), которые будем называть конечными линзовыми многогранниками.

С другой стороны, построение этих же примеров можно начать с образования конечного "линзового" многогранника: берется прямое произведение поверхности на отрезок и полученный обьект ограняется в соответствии с одной из платоновых карт базы. При таком подходе многообразие из ортогонально усеченного ромбического триаконтаэдра получается как линзовый полиэдр с двугранными углами $2\pi/3$ над картой $\{4, 5\}$ и схемой отождествления 2-граней "тор из шестиугольника". Многообразие из ортогонально усеченного икосаэдра представленно линзой над картой $\{5, 5\}$ (в дуальном ее положении) и схемой отождествления, перенесенной с многообразия Зейферта—Вебера [7], посредством звездного $\{5, 5/2\}$. При этом образуются несущественные циклы ребер (по три). В обоих примерах плоскости граней, инцидентных вершине, принадлежат эллиптической связке. Если через многогранник $\{5, 5/2\}$ перенести на карту в базе схему отождествления сферического пространства додекаэдра Пуанкаре [8], то на $\{5, 5\}$ в циклах собирается по пять ребер и следовательно для значения двугранного угла в $2\pi/5$ вершины линзового многогранника должны выйти за абсолют и быть ортогонально усечены. В результате образуется новая компонента края, идентичная базе, а плоскости граней определявших вершину, принадлежат гиперболической связке [11].

На рассматриваемой поверхности рода 4 кроме платоновых карт $\{5, 5\}$ и $\{4, 5\}$, имеется еще $\{5, 4\}$. Для параболического случая, когда вершины линзового многогранника на абсолюте, мы будем использовать в базе карту $\{5, 4\}$ на той же поверхности. У такой линзы с параболическими вешинами все двугранные углы прямые. Его экви-

дистантную границу можно окрасить шахматно и тогда любое парное отождествление “белых” граней дает геодезическую границу из “черных” граней.

Мы остановились на самых симметричных схемах отождествления. Если воспользоваться, при опосредованном через многогранник $\{5, 5/2\}$, схемой отождествления “белых” граней, индуцированной с проективной плоскости, то “черные” грани образуют шесть идентичных компонент края, коими являются сферы с пятью каспами. Если применить схему отождествления, перенесенную с многообразия Пуанкаре, то граница из “черных” граней окажется однокомпонентной и будет представлена схемой инциденций граней звездного многогоранника $\{5, 5/2\}$ со всеми вершинами на абсолюте. При использовании схемы отождествления Зейферта—Вебера, через $\{5, 5/2\}$, граница получаемого многообразия так же однокомпонентна, но комбинаторно представлена многогранником $\{5, 3\}$ со всеми вершинами на абсолюте. Отметим что во всех случаях образующаяся граница является вполне геодезической.

Если в рассмотренных случаях взять по два идентичных экземпляра линзовых многообразий, то легко избавится от края. Однако возможностей комбинирования различных многообразий и способов устранения геодезических краев огромное множество, и следовательно можно построить счетное количество новых гиперболических многообразий конечного обьема.

Список литературы

1. Coxeter H. S M. Regular polytopes. — N.-Y.: 1963.

2. Davis M. W. A hyperbolic 4–manifold // Proceedings of the American Mathematical Society. — 1985. — Vol. 93, no. 2. — P. 325–328.

3. Дамиан Ф. Л. К построению гиперболических четырехмерных многообразий // Геометрия дискретных групп. Математические исследования. — 1990. — Вып. 119. — С. 79–84.

4. Damian F., Makarov V. S. On lens polytopes // International Seminar on Discrete Geometry. 2002. Moldova State University. — P. 32–35.

5. Makarov V. S., Damian F. L., Makarov P. V. Compact lens and hyperbolic manifolds // XIII Internat. Conf. ”Algebra, Number Theory and Discrete Geometry” dedicated to S.S.Ryshkov. 2015. Tula Pedagog. St. Univ. — P. 305–307.

6. Дамиан Ф. Л., Макаров В. С. О трехмерных гиперболических многообразиях с икосаэдрической симметрией // Buletunul Academiei de Ştiinţe a Republicii Moldova. Matematica. — 1995. — № 1. — P. 82–89.

7. Seifert H., Weber C. Die beiden Dodekaederräume // Math. Ztschr. — 1933. — Bd. 35. — S. 237–253.

8. Зейферт Г., Трельфалль В. Топология. — М.Л.: ГТТЛ, 1938.

9. Damian F. L., Makarov V. S. Star polytopes and hyperbolic three-manifolds // Buletunul Academiei de Ştiinţe a Republicii Moldova. Matematica. — 1998. — 2. — P. 102–108.

10. Makarov V. S. Geometric methods of construction of discrete groups of motions of a Lobachevskii space. Itogi Nauki i Tekhniki. Ser. Probl. Geom., VINITI, Moscow. Vol.15. — 1983. — P. 3–59.

11. Damian F., Makarov V. S., Makarov P. V. Star complexes over the regular maps Int. Conf. "Geometry, Topology, and Applications". Yaroslavl, Russia. 2013. — P. 27–32.

ЖЁСТКИЕ ФРАГМЕНТЫ НА ПРОСТЫХ ТРЁХМЕРНЫХ МНОГОГРАННИКАХ С НЕ БОЛЕЕ ЧЕМ ШЕСТИУГОЛЬНЫМИ ГРАНЯМИ

Н. Ю. Ероховец (Москва)

В работе исследуются фрагменты, ограниченные простыми рёберными циклами на поверхности простых трёхмерных многогранников с не более чем шестиугольными гранями. Обозначим множество таких многогранников через $\mathcal{P}_6$, а множество фрагментов на них через $\mathcal{D}_6$. Известно, что каждый такой фрагмент гомеоморфен кругу, поэтому является разбиением круга на многоугольники. Пусть p_k — число k-угольных граней простого многогранника P. Из формулы Эйлера получатся следующая известная формула

$$3p_3 + 2p_4 + p_5 = 12 + \sum_{k \geqslant 7}(k-6)p_k.$$

Назовём *дефектом* многогранника P или фрагмента D величину $\pi = 3p_3 + 2p_4 + p_5$. Если P имеет не более, чем шестиугольные грани, то $\pi(P) = 12$.

Фуллереном называется простой трёхмерный многогранник, у которого все грани являются пятиугольниками или шестиугольниками. Для любого фуллерена $\pi(P) = p_5(P) = 12$.

3-*поясом* простого трёхмерного многогранника называется набор граней (F_i, F_j, F_k), такой что $F_i \cap F_j, F_j \cap F_k, F_k \cap F_i \neq \varnothing$ и $F_i \cap F_j \cap F_k = \varnothing$. k-*поясом*, $k \geqslant 4$, называется циклическая последовательность двумерных граней $(F_{i_1}, \ldots, F_{i_k})$, в которой две грани пересекаются тогда и только тогда, когда они при обходе по циклу следуют друг за другом.

Рассмотрим замощение плоскости $\mathbb{R}^2$ правильными шестиугольниками. Для трёх шестиугольников с общей вершиной возьмём векторы $\mathbf{a}_1$ и $\mathbf{a}_2$, соединяющие центр одного шестиугольника с центрами остальных шестиугольников. Для неотрицательных целых чисел (p, q), $p \geqslant q$, рассмотрим вектор $\mathbf{c} = p\mathbf{a}_1 + q\mathbf{a}_2$. Факторизация плоскости по вектору $\mathbf{c}$ задаёт разбиение цилиндра на шестиугольники. Рассмотрим замкнутую цепочку граней на цилиндре, которая получается, если от заданного шестиугольника пройти p раз вдоль вектора $\mathbf{a}_1$ и q раз вдоль вектора $\mathbf{a}_2$ в произвольном порядке. Граница этой цепочки состоит из двух простых рёберных циклов, которые получаются друг из друга переносом на вектор $\mathbf{a}_1 - \mathbf{a}_2$. Если поверхность многогранника $P \in \mathcal{P}_6$ комбинаторно эквивалентна поверхности, получающейся разрезанием цилиндра вдоль двух таких параллельных циклов и заклеиванием циклов фрагментами из $\mathcal{D}_6$ с $\pi(D) = 6$, то P называется *нанотрубкой типа* (p, q).

Основной результат можно сформулировать следующим образом.

Теорема. *Для любого $k \geqslant 3$ существует конечный набор фрагментов $\mathcal{Q}_k \subset \mathcal{D}_6$ с $\pi(Q) = 6$ для всех $Q \in \mathcal{Q}_k$, такой что семейства многогранников $\mathcal{S}_k \subset \mathcal{P}_6$, $\mathcal{S}_3 \subset \mathcal{S}_4 \subset \cdots \subset \mathcal{S}_k$, где каждый многогранник в $\mathcal{S}_k \setminus \mathcal{S}_{k-1}$ состоит из последовательности $r \geqslant 0$ примыкающих друг к другу k-поясов шестиугольников и двух примыкающих к ним фрагментов из $\mathcal{Q}_k$, обладают следующими свойствами:*

1) *все многогранники в $\mathcal{S}_k$, кроме конечного числа, являются нанотрубками*;

2) *многогранник $P \in \mathcal{P}_6$ принадлежит $\mathcal{S}_k$ тогда и только тогда, когда он содержит фрагмент из $\mathcal{Q}_k$*;

3) *Многогранник $P \in \mathcal{P}_6$ принадлежит хотя бы одному семейству S_k тогда и только тогда, когда он содержит фрагмент с дефектом, равным шести.*

4) *Любой фуллерен P имеет фрагмент, состоящий из шести пятиугольников, и принадлежит хотя бы одному семейству $\mathcal{S}_k$, $k \geqslant 5$.*

Таким образом, фрагменты из $\mathcal{Q}_k$ являются *жёсткими*, то есть накладывают жёсткие условия на комбинаторику многогранника P, содержащего один из таких фрагментов.

Пример 1. Множество $\mathcal{Q}_3$ состоит из шести фрагментов. Первый фрагмент состоит из трёх сходящихся в одной вершине четырёхугольников. Второй и третий фрагмент получаются из первого последовательной срезкой одной и двух внутренних вершин. Эти фрагменты отвечают нанотрубкам типа $(3, 0)$. Четвёртый фрагмент состоит из сходящихся в одной вершине треугольника, четырёхугольника и пятиугольника. Пятый фрагмент получается из него срезкой внутренней вершины. Шестой фрагмент получается из пятого срезкой вершины, в которой сходятся треугольник, четырёхугольник и пятиугольник. Эти фрагменты отвечают нанотрубкам типа $(2, 1)$.

Пример 2. Фрагмент из пятиугольника, окружённого пятью пятиугольниками, является жёстким для фуллеренов: если фуллерен содержит такой фрагмент, то он является нанотрубкой типа $(5, 0)$ и получается из двух таких фрагментов вставкой любого числа 5-поясов шестиугольников между ними.

Доказательство пунктов 1), 2), 3) теоремы получается из описания структуры k-поясов и простых рёберных циклов в работе [1] (теорема 3 и теорема 4).

Для доказательства пункта 4) мы используем следующую лемму и её следствие.

Лемма. *Для каждого трёхмерного простого многогранника с m гипергранями существует последовательность фрагментов, отличающихся на одну двумерную грань, начиная с одной грани, заканчивая $(m-1)$ гранью.*

Этот результат следует из шеллинговости многогранников, а в случае многогранников из $\mathcal{P}_6$ может быть доказан непосредственно.

Следствие. *Для любого фуллерена существует фрагмент D с дефектом $\pi(D) = 6$.*

Отметим, что существуют многогранники в $\mathcal{P}_6$, не имеющие фрагментов с дефектом, равным шести. Примером является треугольная призма.

Работа выполнена при частичной финансовой поддержке гранта победителям конкурса "Молодая математика России".

Список литературы

1. Ероховец Н. Ю. k-пояса и простые рёберные циклы простых многогранников с не более, чем шестиугольными гранями // Дальневосточный математический журнал. — 2015. — Т. 15, № 2. —С. 197–213.

О ШАРНИРНИКАХ С ОДИНАКОВЫМ ВНУТРЕННИМ НАПРЯЖЕНИЕМ

М. Д. Ковалёв (Москва)

Рассматриваем закреплённые шарнирно рычажные конструкции в евклидовой плоскости. Структура такой конструкции определяется *шарнирной структурной схемой* (ШСС) — абстрактным связным графом $G(V, E)$ без петель и кратных рёбер, имеющим вершины двух видов $V = V_1 \cup V_2$ [1]. Вершинам из V_1 отвечают свободные шарниры (вращательные пары), вершинам из V_2 — шарниры конструкции, закреплённые в плоскости. Причём, вершины из V_2 смежны лишь вершинам из V_1. Рёбрам графа отвечают рычаги конструкции. Эти рычаги могут свободно вращаться вокруг соединяющих их шарниров. *Закрепленной шарнирной схемой* (ЗШС) в плоскости называют ШСС, каждой закрепленной вершине $v_i \in V_2$ которой сопоставлена точка $p_i \in R^2$. Задание ЗШС определяет так называемой *рычажное отображение*. Пусть $V_1 = \{v_1, \ldots, v_m\}$, $|E| = r$, тогда рычажное отображение $F : R^{2m} \to \mathcal{R}^r$, задаётся формулами $d_{ij} = (p_i - p_j)^2, v_i v_j \in E$, где в правой части стоят скалярные квадраты векторов. Оно играет ключевую роль в геометрии шарнирных механизмов. Пусть $p_i \in R^2$, $1 \leq i \leq m$. Точка $p = (p_1, p_2, \ldots, p_m) \in R^{2m}$ называется *шарнирником*. Ей отвечает либо шарнирная ферма, либо определённое положение шарнирного механизма. Шарнирник, у которого хотя бы один рычаг имеет нулевую длину (и совпадают смежные шарниры), мы называем *сократимым*, в противном случае — *несократимым*. Если $\dim F(R^{2m}) = r$, то рычажное отображение F и соответствующая ЗШС называются *правильными*. Правильная ЗШС в R^2 называется *изостатической*, если $2m = r$. Конструкции с такими ЗШС чаще всего применяются на практике.

Пусть $p_i p_j$ рычаг с концевыми шарнирами p_i, $p_j \in R^2$. Силу, с которой этот рычаг действует на шарнир p_i, принято записывать как $\omega_{ij}(p_i - p_j)$, где скаляр ω_{ij} называется *внутренним напряжением рычага* $p_i p_j$ [2]. Величины $\omega_{ij} = \omega_{ji}$ напряжений указывают меру напряженности рычагов: если $\omega_{ij} < 0$, то рычаг $p_i p_j$ растянут, если же $\omega_{ij} > 0$, то он сжат. Условие равновесия сил, приложенных к i-му свободному шарниру со стороны смежных шарниров шарнирника, имеет вид

$$\sum_j \omega_{ij}(p_i - p_j) = 0,$$

где суммирование проводится по всем шарнирам смежным в ШСС

i-му. *Внутренние напряжения* шарнирника $\omega=\{\omega_{ij}\}$ определяются как нетривиальные решения однородной системы линейных уравнений:

$$\sum_j \omega_{ij}(p_i - p_j) = 0, \qquad 1 \le i \le m,$$

при заданных положениях p_i шарниров. Механический смысл этой системы суть равновесие сил в каждом свободном шарнире конструкции. Если система имеет лишь тривиальное решение, то говорим, что шарнирник *не допускает внутренних напряжений*. Если система имеет такое решение $\omega=\{\omega_{ij}\}$, что $\omega_{ij} \neq 0$ для любого $(i,j) \in E$, то внутреннее напряжение ω называем *полным*.

Если в этой системе начать считать напряжения $\omega = \{\omega_{ij}\}$ известными, а положения свободных шарниров неизвестными, то для нахождения последних получим систему линейных уравнений:

$$(\sum_{j,(v_i,v_j)\in E} \omega_{ij})p_i - \sum_{j,(v_i,v_j)\in E_1} \omega_{ij}p_j = \sum_{j,(v_i,v_j)\in E_2} \omega_{ij}p_j^0, \qquad 1 \le i \le m.$$

здесь E_2 — множество рёбер, смежных закреплённым шарнирам, $E_1 = E \setminus E_2$. Матрицу $\Omega(\omega)$ этой системы называют матрицей *напряжений*. Пусть для заданного шарнирника $p^0 = \{p_1^0, ..., p_m^0\}$ с закреплением $p_{m+1}^0, ..., p_{m+n}^0$ имеем $p(\omega) = (p_1(\omega), ..., p_m(\omega))$ — множество всех решений последней системы уравнений. Оно представляет собой линейное многообразие размерности $2\,\mathrm{coRank}\,\Omega(\omega)$ в R^{2m}.

Рассмотрим две бесконечных последовательности ШСС: D_m и M_m [3]. Вообще говоря, им отвечают изостатические ЗШС. Схема D_m состоит из цепи $p_1p_2\dots p_m$, составленной из свободных шарниров, и присоединённых к ней закреплённых шарниров $q_0, q_1, \dots, q_m$, причём к шарниру p_1 присоединены закреплённые шарниры q_0 и q_1, а к шарниру $p_i,\ i > 1$ — шарнир q_i. Схема M_m состоит из замкнутого многоугольника $p_1p_2\dots p_m$, с вершинами в свободных шарнирах, и присоединённых к нему рычагами закреплённых шарниров $q_1, \dots, q_m$, причём к шарниру p_i присоединён закреплённый шарнир q_i. Назовём ЗШС *распрямлённой*, если все её закреплённые шарниры лежат на прямой, и *нераспрямлённой* в противном случае. Два шарнирника $p' \neq p$ с одной ЗШС назовём *изометричными*, если $F(p') = F(p)$.

Если ЗШС распрямлена и все её закреплённые шарниры лежат на прямой L, то для любого шарнирника p, не лежащего на L, имеется изометричный шарнирник $p' \neq p$ зеркально симметричный p отно-

сительно L. Такие изометричные шарнирники с одинаковыми полными внутренними напряжениями существуют уже для распрямлённой ЗШС D_2.

Теорема 1. *Для нераспрямлённых изостатических ЗШС типа D_m и M_m невозможны изометричные несократимые шарнирники $p' \neq p$, допускающие одно и то же полное напряжение ω.*

Полнота напряжения необходима. Действительно, возьмём шарнирник p со схемой D_2, шарнир p_1 которого лежит посередине между закреплёнными шарнирами q_0 и q_1, а шарнир p_2 не лежит на прямой q_2p_1. У этого шарнирника имеется неполное внутреннее напряжение ненулевое и одинаковое на рычагах q_0p_1 и q_1p_1, и нулевое на рычагах p_1p_2 и q_2p_2. Имеется изометричный ему шарнирник p', получаемый из p отражением шарнира p_2 от прямой q_2p_1, допускающий то же самое внутреннее напряжение.

Существуют плоские нераспрямлённые изостатические ЗШС, для которых имеются изометричные шарнирники, допускающие одно и то же полное напряжение. Для них справедливы следующие теоремы.

Теорема 2. *Если в многообразии $p(\omega)$ имеется два изометричных шарнирника, то число пар изометричных шарнирников в $p(\omega)$ бесконечно.*

Теорема 3. *В случае* $\operatorname{coRank}\Omega(\omega) = 1$, *если в двумерной плоскости $p(\omega)$ имеется два различных изометричных шарнирника, то множество шарнирников, не имеющих изометричного в $p(\omega)$, есть прямая.*

Список литературы

1. Ковалев М. Д. Геометрическая теория шарнирных устройств // Изв. РАН Сер. матем. — 1994. — 58 (1). — С. 45–70.

2. Ковалев М. Д. О восстановимости шарнирников по внутренним напряжениям // Изв. РАН Сер. матем. — 1997. — 61 (4). — С. 37–66.

3. Ковалев М. Д. Определитель матрицы напряжений и восстановимость шарнирных конструкций по внутренним напряжениям // Изв. РАН Сер. матем. — 2016. — 80 (3). — С. 43–66.

ГЕОМЕТРИЯ БИКРИСТАЛЛОВ И ТРЁХМЕРНЫЕ СФЕРИЧЕСКИЕ МНОГООБРАЗИЯ

Я. В. Кучериненко, В. С. Макаров (Москва)

Симметрия двойника характеризуется точечными трёхмерными группами сросшихся кристаллов и их взаиморасположениями [1]. Изучение взаимных ориентаций в бикристаллах (и в любых парах фигур, имеющих конечные группы симметрии) [2], привело нас к дискретным группам трёхмерной сферы [3], а в данной работе – к сферическим многообразиям.

Исследования, результаты которых изложены ниже, были стимулированы работой [4] и указанными в ней нерешёнными вопросами. Все дискретные группы, действующие на S^3 без неподвижных точек, классифицируютя в [4] по пяти счётным сериям: $C_n \times C_m$, $D_n^* \times C_m$, $T^* \times C_m$, $O^* \times C_m$, $I^* \times C_m$, (где n и m выбираются так, чтобы перемножаемые группы, помимо симметрии в центре S^3, не содержали поворотов с одинаковыми угловыми характеристиками). Для первых двух из них Постников дал описание областей Дирихле в виде линз и правильных призм, а для остальных трёх серий – только для случаев $T^* \times C_1$, $O^* \times C_1$ и $I^* \times C_1$ – в виде октаэдра, усечённого куба и додекаэдра, (последний случай соответствует известному многообразию Пуанкаре).

Для практических целей материаловедения бывает важно знать равноменность распределения ориентаций кристаллических зёрен в образце, для описания каждой из которых обычно выбирают поворот с минимальным углом [5]. Области таких минимальных поворотов имеющие форму выпуклых многогранников в пространстве Родригеса [5, 6], как оказалось, являются центральными (гномоническими) проекциями граней изоэдральных разбиений трёхмерной сферы [3, 7] на касательную трёхмерную гиперплоскость (разбиение является изоэдральным т.к. на ней действует группа, связывающая в одну орбиту все различные описания одной и той же разориентировки кристаллов [3]).

Изучение не одной клетки, а всего разбиения Дирихле с действующей на нём группой позволило обнаружить, что группа стабилизатора любой точки орбиты изоморфна точечной группе симметрии кристаллического двойника [3]. Кроме того на S^3 при рассмотрении двойников и сростков любых двух *одинаковых* кристаллов всегда появляется центр симметрии в точке $(0, 0, 0, 1)$ (следует из [2]), отвечающей тождественному повороту. Поэтому, для получения групп без неподвижных точек, нам понадобится пара *разных* кристаллов (фи-

гур), имеющих только поворотную симметрию и не имеющих одинаковых поворотных симметрий. Выбор разных исходных установок кристаллов относительно координатной системы не приводит к другой группе (или другой орбите), но лишь к их другой ориентации на S^3 [3]. Если при этом всякий раз будем брать $(0,0,0,1)$ в качестве начальной точки, то получим уже новые орбиты и таким способом сможем задать любую из них, что было использовано нами в качестве практического приёма для сравнения групп на S^3 и их факторпространств. Это позволило нам рассмотреть результаты работы [4] с разных сторон: найти примеры групп с разными многогранники Дирихле и, в то же время, для некоторых разных групп получить одинаковые орбиты и одинаковые разбиения Дирихле:

$C_6^* \times C_1$	$C_3^* \times C_2^*$, $2 \parallel 3$:	12 линз, толщиной $\pi/6$
$D_3^* \times C_1$	$C_3^* \times C_2^*$, $2 \perp 3$:	12 6-призм толщиной $\pi/3$
$D_6^* \times C_1$	$D_2^* \times C_3^*$, $2 \parallel 3$:	24 12-призм толщиной $\pi/6$
$T^* \times C_1$	$D_2^* \times C_3^*$, 3 как в кубе:	24 октаэдра { 3,4,3 }
$D_{12}^* \times C_1$	$D_4^* \times C_3^*$, $4 \parallel 3$:	48 24-призм толщиной $\pi/12$
$O^* \times C_1$	$D_4^* \times C_3^*$, 3 как в кубе:	48 24-призм толщиной $\pi/12$
$I^* \times C_1$	$T^* \times C_5^*$, $5 \parallel [01\tau]$:	120 додекаэдров { 5,3,3 },

где в третьем столбце указаны взамные ориентации поворотных осей в исходных установках фигур. В последней строчке таблицы, наряду с известным многообразием Пуанкаре, указан и пример, не описанный в [4] с геометрической точки зрения (самый простой из них).

Разбиения Дирихле для других примеров нам удалось описать для серий $T^* \times C_m^*$, $O^* \times C_m^*$ и $I^* \times C_m^*$, направив одинаково оси максимальных порядков перемножаемых групп. Полученные фигуры – «ломаные 3-, 4- и 5-угольные призмы» (основания которых, напоминающие правильные 3-, 4- и 5-угольники) скручены между собой соответственно на $\pi/3m$, $\pi/4m$, $\pi/5m$ (это – и расстояния между центрами оснований), а боковые грани – в основном ромбы. В следующей таблице приведены некоторые их геометрические характеристики.

Группа	$T^* \times C_m^*$	$O^* \times C_m^*$	$O^* \times C_m^*$	$I^* \times C_m^*$	$I^* \times C_m^*$
Серия	1	$2a$	$2b$	$3a$	$3b$
m	$2i+3$	$6i-1$	$6i+1$	$6i+1$	$6i-1$
$3n$	$9m$	$8m+8$	$8m+16$	$5m+10$	$5m+20$
3В	$18m$	$16m+40$	$16m+56$	$10m+50$	$10m+70$
Р	$9m+3$	$8m+20$	$8m+28$	$5m+25$	$5m+35$
3Г	$9m+15$	$8m+26$	$8m+34$	$5m+31$	$5m+35$
3р	$9m-9$	$8m-28$	$8m-20$	$5m-35$	$5m-25$

Для серий $3a$ и $3b$ пропукаем значения m, кратные 5; n – число вершин основания; В, Р и Г – числа вершин, рёбер и граней ячейки; р – число боковых граней, имеющих форму ромба; i – натуральное.

Список литературы

1. Мокиевский В. А. Морфология кристаллов. — Л.: Изд-во Недра, 1983. — 295 С.

2. Кучериненко Я. В. О взаимном расположении двух фигур в пространствах постоянной кривизны // Материалы VIII Международного семинара "Дискретная математика и ее приложения"(2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2005. — С. 398–401.

3. Кучериненко Я. В. Разбиения трёхмерной сферы и срастания кристаллических зёрен // Труды II Всероссийской научной школы "Математические исследования в кристаллографии, минералогии и петрографии"(Апатиты, 16–17 октября 2006 г.). — Апатиты: Изд-во K&M, 2006. — С. 63–72.

4. Постников М. М. Трехмерные сферические формы // сб. "Дискретная геометрия и топология"к 100-летию со дня рождения Б. Н. Делоне, Тр. МИАН СССР. — М.: Наука, 1991. — С. 114–146.

5. Sutton A. P., Balluffi R. W. Interfaces in crystalline materials. — Oxford: Clarendon press, 1996.

6. Frank. F. C. Orientation mapping // Metalurgical transactions A. — 1988. — V. 19A, — P. 403–408.

7. Handscomb. D. C. On the random disorientation of two cubes // Canadian journal of mathematics. — 1958. — V. 10 — P. 85–88.

К ТЕОРЕМЕ О ТИПАХ ВЫПУКЛЫХ МНОГОГРАННИКОВ С ПАРКЕТНЫМИ ГРАНЯМИ

Е. С. Окладникова, А. В. Тимофеенко (Красноярск)

Правильногранником называется многогранник, грани которого правильные или составлены из правильных многоугольников так,

что вершины этих многоугольников служат и вершинами многогранника. С точностью до подобия найдены все выпуклые правильногранники, [1, 2]. Кроме правильных ещё пять паркетных многоугольников служат гранями некоторых правильногранников, см. электронный атлас [3]. Напомним, [4], выпуклый многоугольник называется *паркетным*, если он может быть составлен из конечного числа равноугольных многоугольников. Кроме четырех бесконечных серий, существует конечное число типов выпуклых многогранников с паркетными гранями.

Теоремы настоящей работы нацелены на решение проблемы *"Каковы все типы выпуклых многогранников с паркетными гранями?"* В публикации [4] отмечается, что кроме четырёх бесконечных серий существует лишь конечное число типов выпуклых многогранников с паркетными гранями и найти их можно по схеме, которая привела в работе [5] к нахождению всех выпуклых тел с правильными гранями. Теоремы 1 и 2 дают представление насколько увеличивается объём вычислений при поиске тел с паркетными гранями в сравнении с правильногранными телами.

В работе [5] выпуклые правильногранные многогранники, нерассекаемые никакой плоскостью по рёбрам на правильногранные части, названы простыми. Если же таким свойством обладает выпуклый правильногранник, то его называют *несоставным*. Согласно публикациям [5–7] существуют только следующие несоставные тела:

$$\Pi_3, \Pi_4, \dots ; A_4, A_5, \dots ; M_1, M_2, \dots , M_{28}, Q_1, Q_2 \dots , Q_6. \qquad (1)$$

Первыми в этом списке расположены бесконечные серии призм и антипризм. За ними следуют правильногранные пирамиды M_1, M_2, M_3 с трёх-, четырёх- и пятиугольными основаниями соответственно и другие тела, которые называют сегодня многогранниками Залгаллера, Иванова и Пряхина.

Соединением одинаковыми гранями из несоставных тел можно получить каждый выпуклый правильногранник. В отличие от выпуклых правильногранников, каждому типу которых соответствует единственный с точностью до подобия многогранник, типу выпуклого тела с паркетными гранями соответствует, как правило, бесконечное множество попарно неподобных многогранников. Такие тела встречаются и в следующей, доказанной на вэбинаре "Группы и правильногранники" [9] теореме.

Теорема 1. *Выпуклый многогранник с рёбрами длины один или два составлен из не более четырнадцати правильногранных пира-*

мид с единичными рёбрами тогда и только тогда, когда он является одним из следующих тел:

1) M_1, M_2, M_3;

2) $M_1 + M_1$, $M_1 + M_2$, $M_2 + M_2$, $M_3 + M_3$;

3) $^\circ S_{2,2} + M_1$, $S_{2,2} + M_2$, $^\circ S_{2,2} + M_2'$;

4) $^\circ S_{3,1}+M_2$, $^\circ S_{3,1}+M_2'$, $S_{3,2}+M_1$, $S_{2,2}+S_{2,2}$, $S_{2,2}+S_{2,2}'$, $^\circ S_{2,2}+S_{2,2}''$;

5) $^\circ S_{4,1} + M_1$, $^\circ S_{4,4} + M_2$;

6) $^\circ S_{5,1} + M_1$, $^\circ S_{5,2} + M_1$, $^\circ S_{5,2} + M_2$, $^\circ S_{3,1} + S_{3,1}$, $^\circ S_{3,1} + S_{3,3}$;

7) $^\circ S_{6,2} + M_1$, $^\circ S_{6,5} + M_2$, $S_{4,6} + S_{3,1}$;

8) $^\circ S_{7,1} + M_1$, $^\circ S_{7,2} + M_1$, $S_{7,3} + M_2$, $^\circ S_{6,2} + S_{2,2}$, $^\circ S_{6,5} + S_{2,2}$, $^\circ S_{5,1} + S_{3,1}$;

9) $^\circ S_{8,3} + M_2$, $^\circ S_{6,5} + S_{3,1}$, $^\circ S_{6,5} + S_{3,3}$;

10) $^\circ S_{9,1} + M_1$, $^\circ S_{9,1} + M_2$, $^\circ S_{9,3} + M_2$, $^\circ S_{8,3} + S_{2,2}$, $^\circ S_{5,1} + S_{5,1}$;

11) $^\circ S_{10,1} + M_2$, $^\circ S_{10,4} + M_2$, $^\circ S_{10,5} + M_1$;

12) $^\circ S_{11,2} + M_1$, $^\circ S_{11,3} + M_1$, $S_{9,1} + S_{3,1}$, $^\circ S_{9,1} + S_{3,1}'$, $^\circ S_{9,3} + S_{3,1}$;

13)$^\circ S_{12,3} + M_2$, $^\circ S_{12,4} + M_1$, $^\circ S_{10,4} + S_{3,1}$;

14) $^\circ S_{13,1} + M_1$, $^\circ S_{13,1} + M_2$, $^\circ S_{13,3} + M_2$, $^\circ S_{12,3} + S_{2,2}$, $S_{7,3} + S_{7,3}$, $S_{7,3} + S_{7,3}'$;

15) $^\circ S_{14,1} + M_2$, $S_{14,5} + M_2$, $S_{14,6} + M_2$, $S_{12,4} + S_{3,3}$, $^\circ S_{12,5} + S_{3,3}$;

причём многогранник $S_{i,j}$ расположен в списке (i) на j-м месте, штрих указывает на различие многогранников, составленных из двух одинаковых тел, кружком помечены тела с фиктивными вершинами.

Как доказано в [8], семь многогранников списка разбиваются плоскостью на тела с паркетными гранями. Из них пять тел составлены из правильногранных пирамид с единичными рёбрами. Все выпуклые с рёбрами длины 1 или 2 соединения не более 15 таких пирамид расположены выше в теореме 1. Поэтому справедлива

Теорема 2. *Если выпуклый правильногранник никакой плоскостью не рассекается на правильногранники, но существует плоскость, делящая его на многогранники с правильными или составленными из правильных многоугольников гранями, то он составлен из правильногранных пирамид тогда и только тогда, когда является одним из пяти тел: трёхскатный купол M_4, усечённый тетраэдр M_{10}, усечённый октаэдр M_{16}, наклонная призма Q_1, двенадцатигранник Иванова Q_2.*

Работа выполнена при финансовой поддержке РФФИ (проект 15-01-04897).

Список литературы

1. Тимофеенко А. В. К перечню выпуклых правильногранников // Современные проблемы математики и механики. — 2011. — Т. VI., вып. 3 — С. 155–170.

2. Гурин А. М., Залгаллер В. А. К истории изучения выпуклых многогранников с правильными гранями и гранями составленными из правильных // Труды Математического Общества Санкт-Петербурга. —2008. — Т. 14. — С. 215–294.

3. Convex regular-faced polyhedra with conditional edges // Электронный ресурс: `http://tupelo-schneck.org/polyhedra`.

4. Пряхин Ю. А. Выпуклые многогранники, грани которых равноугольны или сложены из равноугольных // Зап. науч. семинаров ЛОМИ. —1974. — Т. 45. — С. 111–112.

5. Залгаллер В. А. Выпуклые многогранники с правильными гранями // Зап. науч. семинаров ЛОМИ. — 1967. — Т. 2. — С. 5–218.

6. Иванов Б.А. Многогранники с гранями, сложенными из правильных многоугольников // Украинский геометрический сборник. —1971. — Т. 10. —С. 20–34.

7. Пряхин Ю. А. О выпуклых многогранниках с правильными гранями // Украинский геометрический сборник. —1973. — Т. 14. — С. 83–88.

8. Тимофеенко А. В. О выпуклых многогранниках с равноугольными и паркетными гранями // Чебышевский сборник. —2011. — Т. 12, вып. 2. — С. 118–126.

9. Группы и правильногранники // Электронный ресурс: `http://icm.krasn.ru/seminar.php?id=reghedra`.

ГРАНИЧНЫЕ ЗНАЧЕНИЯ ДЛЯ ОТНОШЕНИЙ ТИПА ШТЕЙНЕРА

А. С. Пахомова (Москва)

Одной из известных задач геометрической оптмизации является задача нахождения кратчайшей сети, соединяющей данное конечное множество M точек метрического пространства X. При этом ответ зависит от рассматриваемого семейства допустимых сетей, среди которых выбирается кратчайшая. Рассмотрим несколько различных классов взвешенных деревьев, соединяющих множество M. Если рассматривать только графы, множество вершин которых совпадает

с множеством точек M, а в качестве веса ребра рассматривать расстояние по метрике пространства X между вершинами, мы получим конструкцию *минимального остовного дерева* для M. Суммарный вес ребер дерева можно уменьшить, если рассматривать графы, которые содержат еще какие-то дополнительные вершины из пространства X, не входящие в M. В этом случае мы говорим о *минимальном дереве Штейнера* для M. Если же не ограничиваться рассмотрением точек пространства X, а рассмотреть всевозможные изометрические вложения множества M в произвольные метрические пространства и искать деревья Штейнера в них, мы получим конструкцию *минимального заполнения* множества M. Для каждого описанного класса можно поставить задачу нахождения дерева минимального веса. Вес минимального остовного дерева для множества M будем обозначать $\mathrm{mst}(M)$, вес минимального дерева Штейнера — $\mathrm{smt}(M)$, а вес минимального заполнения — $\mathrm{mf}(M)$. Подробнее об этих понятиях можно узнать в работах [1] и [2].

Отношением Штейнера метрического пространства (X, ρ) называется величина

$$\mathrm{sr}(X,\rho) = \inf_{\{M \mid M \subset X\}} \left\{ \frac{\mathrm{smt}(M)}{\mathrm{mst}(M)} \mid 1 < \#M < \infty \right\},$$

где $\#M$ обозначает количество элементов в множестве M.

Отношение Штейнера появилось впервые в работах Джилберта и Поллака в 60-х годах двадцатого века. Интерес к нему связан в частности с гипотезой Джилберта—Поллака [3] об отношении Штейнера евклидовой плоскости. Однако стоит заметить, что многочисленные попытки доказать ее [4] так и не привели к успеху, оставив данный вопрос открытым для исследования [5]. Тем не менее, в ходе изучения отношения Штейнера были получены многие важные результаты, связанные как с общими свойствами этого отношения, так и с отношением Штейнера для конкретных пространств.

Если вместо указанного отношения рассмотреть отношение веса $\mathrm{mf}(M)$ к $\mathrm{mst}(M)$, мы получим определение *отношения Штейнера—Громова* $\mathrm{sgr}(X, \rho)$. А если вместо указанного отношения рассмотреть отношение $\mathrm{mf}(M)$ к $\mathrm{smt}(M)$, мы получим определение *суботношения Штейнера* $\mathrm{ssr}(X, \rho)$. Суботношение Штейнера и отношение Штейнера—Громова, как и конструкция минимального заполнения для конечного метрического пространства, впервые были предложены А.О. Ивановым и А.А. Тужилиным в работе [2]. Три описанных выше отношения мы будем называть *отношениями типа Штейнера*. В тех случаях, когда неважно, о каком из трех отношения идет

речь, мы будем использовать запись $r(X)$.

Помимо описанных выше отношений типа Штейнера можно рассмотреть *n-точечные отношения типа Штейнера* для фикисированного натурального $n \geq 2$. Для этого в определении соответствующего отношения точную нижнюю грань по всем конечным подмножествам нужно заменить на точную нижнюю грань по тем подмножествам, что содержат не более n точек.

Таким образом, отношения типа Штейнера являются важной характеристикой метрического пространства, показывающей, насколько хорошо минимальные деревья из разных классов приближают друг друга.

Следующая теорема была доказана в работе [6] для случая отношения Штейнера и в работе автора [7] для двух других отношений.

Теорема. *Для любого отношения типа Штейнера $r(X)$ справедливы оценки $\frac{1}{2} \leq r(X) \leq 1$. Для любого n-точечного отношения типа Штейнера $r_n(X)$ справедливы оценки $\frac{n}{2(n-1)} \leq r_n(X) \leq 1$.*

Отдельный интерес представляет рассмотрение метрических пространств, значение отношения типа Штейнера которых равно 1, т.е. является максимально возможным. Автором были описаны все метрические пространства, для которых отношение Штейнера—Громова равно единице.

Теорема. *Пусть (X, ρ) — метрическое пространство. Следующие условия эквивалентны:*

1) $sgr(X) = 1$;

2) *Для любого* $n \geq 2$ $sgr_n(X) = 1$;

3) *Для некоторого* $n > 3$ $sgr_n(X) = 1$;

4) *Все треугольники в пространстве X вырождены, т.е. для любых трех точек неравенство треугольника является равенством;*

5) *X изометрично некоторому подмножеству евклидовой прямой или четырехточечному пространству $\{x_1, x_2, x_3, x_4\}$, в котором все треугольники вырождены и $\rho(x_i, x_j) = \rho(x_k, x_l)$ для любой перестановки (i, j, k, l) индексов $(1, 2, 3, 4)$.*

Автор выражает благодарность своему научному руководителю д. ф.-м. н. А. О. Иванову, д. ф.-м. н. А. А. Тужилину и всем участникам семинара «Оптимальные сети» за помощь и проявленный интерес к работе. Работа выполнена при финансовой поддержке гранта РФФИ (проект 16–01–00378а) и гранта Президента РФ поддержки ведущих научных школ РФ (проект НШ–7962.2016.1).

Список литературы

1. Иванов А. О., Тужилин А. А. Одномерная проблема Громова

о минимальном заполнении // Матем. сб. — 2012. — 203 (5). — С. 65–118.

2. Ivanov A. O., Tuzhilin A. A. Minimal fillings of finite metric spaces: The state of the art //Discrete Geometry and Algebraic Combinatorics (Vol. 625 of Contemporary Mathematics, AMS, Providence, RI, 2014). — P. 9–35.

3. Gilbert E. N., Pollak H. O., Steiner minimal trees // SIAM J. Appl. Math. — 1968. — 16 (1). — P. 1–29.

4. Du D.-Z., Hwang F. K. A proof of the Gilbert—Pollak conjecture on the Steiner ratio // Algoritmica. — 1992. — Vol.7. — P. 121–135.

5. Ivanov A. O., Tuzhilin A. A. The Steiner Ratio Gilbert—Pollak Conjecture Is Still Open // Algorithmica. — Vol. 62, iss. 1–2. — P. 630–632.

6. Cieslik D. The Steiner Ratio. — Kluwer Academic Publishers, 2001

7. Пахомова А. С. Оценки для суботношения Штейнера и отношения Штейнера—Громова // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2014. — № 1 – С. 17–25.

МНОГОГРАННИКИ С СИММЕТРИЧНЫМИ РОМБИЧЕСКИМИ ВЕРШИНАМИ

В. И. Субботин (Новочеркасск)

Рассмотрены свойства замкнутых выпуклых многогранников в трёхмерном евклидовом пространстве, связанные с симметрией звёзд некоторых вершин многогранника.

Определение 1. Вершина многогранника называется *ромбической*, если её звезда состоит из равных одинаково расположенных ромбов.

Таким образом, все ромбы сходятся в вершине либо острыми, либо тупыми углами. Если таких ромбов n штук, то вершину будем называть *n-ромбической*, а совокупность этих n ромбов-ромбической шапочкой. Под звездой ромбической шапочки будем понимать объединение ромбической шапочки и всех граней, имеющих хотя бы одну общую вершину с ромбами шапочки.

Определение 2. Ромбическая вершина называется *симметричной*, если она расположена на оси вращения звезды её ромбической шапочки.

Определение 3. Ромбическая вершина называется *изолированной*, если её звезда не имеет общих элементов со звездой любой другой ромбической вершины многогранника.

Если рассматривать многогранники, каждая вершина которых является симметричной ромбической, но не изолированной, то, как известно, класс таких многогранников исчерпывается двумя многогранниками: ромбическим додекаэдром и ромботриаконтаэдром [1].

Далее будем рассматривать многогранники, каждая ромбическая вершина которых является симметричной и изолированной. При этом каждая грань F, не входящая в звезду ромбической вершины, имеет ось вращения, перпендикулярную F. Предполагается, что эта ось вращения является осью вращения звезды грани F. Такой класс многогранников будем обозначать RS.

Доказана следующая теорема:

Теорема 1. *Всякий многогранник класса RS может быть получен при помощи преобразования отсечения некоторых трёхгранных вершин одного из сильно симметричных относительно вращения граней многогранников и последующего симметричного продления полученных треугольных сечений до ромбов.*

Для доказательства теоремы достаточно из всех многогранников, сильно симметричных относительно вращения граней [1], выбрать те, к которым применимо указанное в формулировке теоремы преобразование.

На основании этой теоремы получаются следующие типы многогранников класса RS, исчерпывающие этот класс:

1) многогранник, полученный из усечённого ромбического триаконтаэдра [2];

2) многограннмк, полученный из 2-го полуусечённого ромбического триаконтаэдра [2];

3) многогранник, полученный из усечённого икосаэдра;

4) вытянутый ромбический додекаэдр;

5) вытянутые ромбоэдры.

Следующий класс, рассматриваемый в работе — класс многогранников с двумя изолированными симметричными ромбическими вершинами, которые разделены равными правильными многоугольниками одного типа. Причём все ромбы обеих звёзд вершин равны между собой. Этот класс будем обозначать RR.

Доказана следующая теорема:

Теорема 2. *Всякий многогранник класса RR принадлежит одному из следующих типов:*

1) *вытянутый ромбический додекаэдр;*

2) 20-*гранник с квадратными гранями, разделяющими 5-*

ромбические вершины;
3) *многогранники с правильными треугольными гранями, разделяющими n-ромбические вершины,* $3 < n < 12$.

Замечание. Отметим, что многогранники класса RS с двумя ромбическими вершинами можно использовать для построения каждого из пяти трёхмерных *параллелоэдров* с помощью соответствующего геометрического преобразованиия.

Список литературы

1. Субботин В. И. Перечисление многогранников, сильно симметричных относительно вращения // Труды участников международной школы-семинара по геометрии и анализу памяти Н. В. Ефимова (5–11 сент. 2002 г.). — С. 77–78.

2. Субботин В. И. О многогранниках, сильно симметричных относительно вращения // Чебышевский сборник. — 2006. — Т. 7, вып. 2(18). — С. 168–171.

Секция «Теория кодирования и математические вопросы теории защиты информации»

К ВОПРОСУ О ДЕДУКТИВНОЙ БЕЗОПАСНОСТИ ВЫЧИСЛЕНИЙ НАД ЗАШИФРОВАННЫМИ ДАННЫМИ

Н. П. Варновский, В. А. Захаров, А. В. Шокуров (Москва)

Открытие стойких систем вполне гомоморфного шифрования [1] создало теоретические предпосылки решения задачи обеспечения информационной безопасности систем удаленных вычислений, включая системы облачных вычислений. Однако, как показано в [2], даже в том случае, когда проводится лишь вычисление функций от хранящихся на облаке конфиденциальных значений аргументов, защита данных невозможна уже для системы с двумя пользователями. Для преодоления этой трудности в статье [3] была предложена специальная модель облачных вычислений, в состав которой помимо облачного сервера входят криптосерверы, на которых реализуется пороговая гомоморфная криптосистема с открытым ключом (TSHE). В статье [4] показано, что если TSHE является стойкой и доля криптосерверов, контролируемых противником, не превосходит заданного порога, то предложенная система облачных вычислений является стойкой для вычислений ограниченной глубины.

Доказанная в [4] стойкость облачных вычислений не отменяет, тем не менее, возможности противника компрометировать конфиденциальные данные пользователей: располагая вычисленными значениями функций $f_i(c_1, \ldots, c_n), i \in I$, зависящих от данных пользователя, противник может попытаться решить обратную задачу и вычислить значения аргументов этих функций. Для предотвращения этой возможности в системе облачных вычислений [3, 4] предусмотрен контроль доступа: облако передает запрос клиента в центр аутентификации, который проверяет полномочия клиента на вычисление запрашиваемой функции и, при наличии таковых, санкционирует выполнение запроса. Однако вопрос о том, как осуществлять проверку полномочий, оставался открытым. Данная статья инициирует исследование этого вопроса.

Рассмотрим упрощенную модель облачной базы данных. Каждый пользователь $u_i, 1 \leq i \leq n$, хранит в базе данных конфиденциальное истинностное значение σ_i базового предиката P_i, ассоциированного с этим пользователем. Клиент базы данных может обращаться к ней с запросами. Запросом является произвольная булева формула $\varphi(P_1, \ldots, P_n)$, зависящая от предикатов пользователей. Ответом на запрос является значение $\varphi(\sigma_1, \ldots, \sigma_n)$. Клиент базы данных имеет полномочие обращаться с запросами из некоторого множества $\mathcal{Q} = \{\varphi_1, \ldots, \varphi_N\}$. Сформулируем требование безопасности для множества запросов.

Для всякой формулы φ и $\delta, \delta \in \{0, 1\}$, обозначим записью φ^δ формулу $\neg\varphi$, если $\delta = 0$, и φ, если $\delta = 1$. Для набора формул $\mathcal{Q} = (\varphi_1, \ldots, \varphi_N)$ и двоичного набора $\Delta = (\delta_1, \ldots, \delta_N)$ запись $\mathcal{Q}^\Delta$ будет обозначать набор формул $(\varphi_1^{\delta_1}, \ldots, \varphi_N^{\delta_N})$. Для набора формул $\mathcal{Q} = (\varphi_1, \ldots, \varphi_N)$, зависящих от предикатов $P_1, \ldots, P_n$, и двоичного набора $\Sigma = (\sigma_1, \ldots, \sigma_n)$ обозначим записью $\mathcal{Q}(\Sigma)$ набор значений функций $(\varphi_1(\Sigma), \ldots, \varphi_N(\Sigma))$. Символами $\bar{0}$ и $\bar{1}$ обозначим двоичные наборы, состоящие из 0 и 1 соответственно. Символом $\models$ обозначается отношение логического следования в классической логике высказываний.

Определение. Набор запросов $\mathcal{Q} = \{\varphi_1, \ldots, \varphi_N\}$ к базе данных, состоящей из значений базовых предикатов $P_1, \ldots, P_n$, называется *дедуктивно безопасным*, если для любого двоичного набора $\Sigma = (\sigma_1, \ldots, \sigma_n)$ соотношение $\mathcal{Q}^{\mathcal{Q}(\Sigma)} \models P_i^{\sigma_i}$ не выполняется ни для одного предиката $P_i, 1 \leq i \leq n$.

Дедуктивная безопасность набора запросов подразумевает, что клиент базы данных, получив ответы на все доступные ему запросы, не может дедуктивно выведать значения предикатов пользователей базы данных. Таким образом, контроль полномочий клиента состоит в проверке дедуктивной безопасности множества запросов, с которыми клиент обращается к базе данных.

Теорема 1. *Набор запросов $\mathcal{Q}$ является дедуктивно безопасным тогда и только тогда, когда для любого предиката $P_i, 1 \leq i \leq n$, и для любого набора Σ_1 истинностных значений базовых предикатов существует такой набор Σ_2, для которого выполняются соотношения $P_i(\Sigma_1) \neq P_i(\Sigma_2)$ и $\mathcal{Q}(\Sigma_1) = \mathcal{Q}(\Sigma_2)$.*

Из теоремы 1 следует

Теорема 2. *Задача проверки дедуктивной безопасности наборов запросов к базе данных является со-NP^{NP}-полной.*

Поскольку задача проверки дедуктивной безопасности запросов является вычислительно трудной, целесообразно выделить некото-

рые практически значимые классы запросов, для которых эта задача может быть решена эффективно. Булева функция $f(y_1, \ldots, y_k)$ называется симметрической, если для любой перестаноки $\theta : [1, k] \to [1, k]$ верно равенство $f(y_1, \ldots, y_k) = f(y_{\theta(1)}, \ldots, y_{\theta(k)})$. В сущности, симметрические запросы призваны собирать статистические сведения о данных пользователей базой данных. Дедуктивная безопасность таких запросов означает, что статистические сведения, собранные клиентом базы данных, не позволяют ему получить сведения о данных какого-либо пользователя этой базы.

Теорема 3. *Пусть $\mathcal{Q}$ — некоторое множество симметрических запросов к базе данных. Тогда $\mathcal{Q}$ является дедуктивно безопасным тогда и только тогда, когда существует такая пара наборов Σ_0 и Σ_1 истинностных значений базовых предикатов, для которых выполняются соотношения $\Sigma_0 \neq \bar{0}$, $\Sigma_1 \neq \bar{1}$, $\mathcal{Q}(\Sigma_0) = \mathcal{Q}(\bar{0})$ и $\mathcal{Q}(\Sigma_1) = \mathcal{Q}(\bar{1})$.*

Предложенный критерий дедуктивной безопасности симметрических запросов можно проверить за полиномиальное время.

Следствие. *Если $\mathcal{Q}$ — некоторое множество симметрических запросов к базе данных, то для его дедуктивной безопасности достаточно, чтобы выполнялось равенство $\mathcal{Q}(\bar{0}) = \mathcal{Q}(\bar{1})$.*

Работа поддержана грантом РФФИ (проект 16-01-00714).

Список литературы

1. Gentry C. Fully homomorphic encryption using ideal lattices // Proceedings of the 41-st ACM Symposium on Theory of Computing. New York: ACM, 2009. — P. 169–178.

2. Van Dijk M., Juels A. On the impossibility of cryptography alone for privacy-preserving cloud computing // Proceedings of the 5-th USENIX Conference on Hot Topics in Security. — Berkeley: USENIX Association, 2010. — P. 1–8.

3. Варновский Н. П., Мартишин С. А. Храпченко М. В., Шокуров А. В. Пороговые системы гомоморфного шифрования и защита информации в облачных вычислениях // Программирование. — 2015. — № 4. — С. 47–51.

4. Варновский Н. П., Захаров В. А., Шокуров А. В. К вопросу о существовании доказуемо стойких систем облачных вычислений // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2015. — № 2. — С. 32–38.

ДЗЕТА-ФУНКЦИИ МНОГООБРАЗИЙ И СЕМЕЙСТВ МНОГООБРАЗИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

Н. М. Глазунов (Киев)

Дан краткий обзор дзета и L-функций многообразий и семейств многообразий над конечными полями вида $\mathbb{F}_q$, где $q = p^n$, число p простое, а n — натуральное. Обзор включает недавние результаты, которые получили C. Greither, N. Ramachandran, и другие. В терминах элементов колец Витта рассмотрен случай L-функций семейства накрытий Артина-Шрайера.

Дзета и L-функции семейств алгебраических кривых. Пусть X есть алгебраическое многообразие или схема конечного типа [1] над $\mathbb{F}_q$. Для X над $\mathbb{F}_q$ имеются два альтернативных определения дзета-функции: (i) пусть $x \in X$ есть замкнутая точка X и $d(x)$ степень её поля вычетов над $\mathbb{F}_q$. Тогда $Z(X,t)$ определяется как $\prod_{x\in X}(1-t^{d(x)})^{-1}$; (ii) пусть $\#X(\mathbb{F}_{q^r})$ есть число $\mathbb{F}_{q^r}$-рациональных точек на X. Тогда $Z(X,t) = \exp(\sum_{r\geq 1}\#X(\mathbb{F}_{q^r})\frac{t^r}{r})$. В работе [2] исследуется случай семейства суперэллиптических кривых. Рассматривается суперэллиптическая кривая над полем $K = \mathbb{F}_q(t)$ и её модель $\mathcal{E}$ над проективной прямой. В [2] предполагается, что все особенности $\mathcal{E}$ рациональны, и формулируются условия, когда это так. Автор [2] использует мотивную интерпретацию якобиана исследуемой кривой, разрабатывает и применяет новую технику для построения соответствующих L-функций, получает сравнения для степени L-функций и верхнюю оценку для аналитического ранга соответствующего якобиана.

В работе [3] автор исследует дзета-функции схем конечного типа [1] над $\mathbb{F}_q$. Среди представленных в [3] результатов — выражения для дзета-функций произведения схем X и Y, дзета-функция n-кратного произведения схемы X, а также выражения для дзета-функций гладких собственных геометрически связных многообразий над $\mathbb{F}_{q^m}$, представленные через произведения Витта дзета-функций соответствующих схем.

Большое кольцо Витта. Пусть A есть коммутативное кольцо с единицей. Большим кольцом Витта (выше и далее — кольцом Витта) $W(A)$ называют коммутативное кольцо с единицей, аддитивная группа $(W(A),+)$ которого изоморфна подгруппе $(1+tA[[t]],\times)$ группы единиц $A[[t]]^*$ кольца $A[[t]]$ относительно умножения формальных

степенных рядов, а умножение $*$ определяется единственным способом условием $(1-at)^{-1} * (1-bt)^{-1} = (1-abt)^{-1}, a, b \in A$ и функториально относительно $W(-)$: любой гомоморфизм колец $f\colon A \to B$ индуцирует гомоморфизм колец $W(f)\colon W(A) \to W(B)$. Единицей относительно сложения является элемент $1 = 1 + 0t + 0t^2 + \cdots$, а единицей относительно умножения - элемент $[1] = (1-t)^{-1}$.

L-функции накрытий Артина—Шрайера как элементы кольца Витта. Постоянным накрытием Артина—Шрайера называют накрытие вида $y^p - y = cx + \frac{d}{x}, c, d \in \mathbb{F}_q^*$. Можно рассмотреть и относительный случай, рассматривая накрытия Артина—Шрайера над проективной прямой над $\mathbb{F}_q$, то есть над полем функций $\mathbb{F}_q(t)$. В последнем случае непостоянные накрытия Артина—Шрайера имеют вид $y^p - y = c(t)x + \frac{d(t)}{x}, c(t), d(t) \in \mathbb{F}_q[t]$. Здесь мы рассматриваем случай постоянных накрытий Артина—Шрайера над простым конечным полем. Хорошо известно (см. например, [4]), что L-функция такого накрытия имеет вид $L(X,t) = 1 - T_p(c,d)t + pt^2$, где $T_p(c,d) = \sum_{x=1}^{p-1} \exp(2\pi i \frac{cx+\frac{d}{x}}{p})$ есть сумма Клостермана.

Теорема 1. *Пусть X и Y есть накрытия Артина—Шрайера. Тогда $L(X \times Y, t)$ функция произведения таких накрытий есть произведение Витта L-функций накрытий: $L(X \times Y, t) = L(X,t) * L(Y,t)$.*

Множество всех накрытий Артина—Шрайера параметризуется пространством модулей $\mathcal{M} = \mathbb{F}_p^* \times \mathbb{F}_p^*$.

Теорема 2. *L-функция произведения всех накрытий Артина-Шрайера над $\mathcal{M}$ имеет вид $L(X_1 \times \cdots \times X_{(p-1)^2}, t) = L(X_1, t) * \cdots * L(X_{(p-1)^2}, t)$.*

Список литературы

1. Шафаревич И. Р. Основы алгебраической геометрии. Тт. 1–2. — М.: Наука, 1988.

2. Greither C. Families of curves with Galois action and their L-functions // J. Number Theory. — 2015. — Vol. 154. — P. 292–323.

3. Ramachandran N. Zeta functions, Grothendieck groups, and the Witt ring // Bull. Sci. Math. — 2015. — V. 139, I. 6. — P. 599–627.

4. Глазунов Н. М. Разработка методов обоснования гипотез формальных теорий. — Saarbrucken.: LAP, 2014.

СЖИМАЕМОЕ ОПОЗНАВАНИЕ: МАТЕМАТИЧЕСКИЕ ОСНОВЫ И КОМПЬЮТЕРНАЯ РЕАЛИЗАЦИЯ

Н. М. Глазунов, О. В. Кузик (Киев)

Задача восстановления матрицы по выборке её элементов, которая может быть соотнесена с кодированием источника, формулируется как задача выпуклой оптимизации [1–3]. Изначально присущей особенностью рассматриваемой задачи восстановления матрицы по выборке её элементов является недифференцируемость этой задачи, что обуславливает проблематичность применения классических методов дифференцируемой оптимизации. В связи с этим обстоятельством для её решения предлагается применение r-алгоритмов [1, 4]. Представлена общая схема, компьютерная реализация которой выполняется на Java.

Постановки задачи и применения. В рамках кодирования источника сжатое опознавание интерпретируется как восстановление информации источника по неполным данным, кодирующим элементы этой информации. Хотя ниже речь идет о вещественных матрицах, фактически при вычислениях матрицы целочисленны, или имеют рациональные коэффициенты. Задача восстановления матрицы по выборке её элементов возникает во многих математических и прикладных исследованиях. Упомянем следующие прикладные задачи: базы данных; триангуляция по неполным данным; сжатое опознавание (Compressed Sensing); машинное обучение (Machine Learning).

Пусть X есть искомая матрица, $M_{i,j}$ известные значения. Одна из математических формулировок вышеперечисленных задач имеет следующее представление:

$$\begin{array}{l}\text{minimize } \operatorname{rank}(X)\\ \text{subject to } X_{i,j} = M_{i,j},\ (i,j) \in \Omega,\end{array}$$

где (i, j) есть множество индексов, $M_{i,j} \in \Omega$ наблюдаемые значения. К сожалению, как доказано в [3], в такой постановке задача суперэкспоненциальна по сложности.

Напомним [1], что задача полуопределенного программирования состоит в минимизации линейной функции от m вещественных переменных относительно матричного неравенства

$$\begin{array}{l}\text{minimize } c^T x\\ \text{subject to } F(x) \geq 0,\end{array}$$

где $F(x) = F_0 + \sum_{i=1}^{m} x_i F_i$ и $F_0, F_1, \ldots, F_m$ есть симметрические матрицы. Задача полуопределенного программирования является зада-

чей выпуклой оптимизации, так как целевая функция и ограничения выпуклы: если $F(x) \geq 0$ и $F(y) \geq 0$, то для всех $\lambda, 0 \leq \lambda \leq 1$ $F(\lambda x + (1-\lambda)y) = \lambda F(x) + (1-\lambda)F(y) \geq 0$.

Пусть X есть матрица размера $n \times m$, X^* есть матрица, сопряженная к X. Тогда собственные значения матриц XX^* и X^*X совпадают и являются положительными. Арифметические значения квадратных корней общих собственных значений матриц XX^* и X^*X называют сингулярными значениями матрицы X. Далее полагаем, что σ_k есть k-е сингулярное значение матрицы X, и что эти сингулярные значения занумерованы в порядке убывания $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_n > 0$ где σ_n есть наименьшее сингулярное значение. Сингулярные значения $\sigma_{n+1}, \ldots$ полагают нулевыми.

Математическая модель. Скалярное произведение (X, Y) матриц X и Y размера $n \times m$ определяют как след $\mathrm{tr}(X^*Y)$ произведения указанных матриц. Напомним, что субградиентом матричной выпуклой функции f называют матрицу $g_f(X_0)$, удовлетворяющую неравенству $f(X) - f(X_0) \geq (g_f(X_0), X - X_0)$ для всех вещественных матриц размера $n \times m$. Ядерной нормой матрицы X называют величину $\|X\|_* = \sum_{k=1}^{n} \sigma_k(X)$ где $\sigma_k(X)$ k-е сингулярное значение X. Исследуется задача оптимизации (с ядерной нормой):

$$\begin{array}{l} \text{minimize } \|(X)\|_* \\ \text{subject to } X_{i,j} = M_{i,j}, (i,j) \in \Omega. \end{array}$$

Метод решения. Метод решения вышеприведенной оптимизационной задачи основывается на матричном расширении r-алгоритма Н. З. Шора [1]. Для сингулярного разложения матрицы ранга s выражение для субградиента ядерной нормы этой матрицы известно. В процессе выполнения r-алгоритма преобразуется пространство поиска и выполняются ортогональные проектирования.

Реализация. В настоящее время реализация выполняется на Java. Главная процедура `ShorNonDifferentiableMethod` использует набор утилит, реализующих метод, а также служащих для целей тестирования.

Список литературы

1. Shor N. Z. Nondifferentiable optimization and polynomial problems. — Boston.: Kluwer Acad. Publ., 1998.

2. Candès E., Recht B. Exact Matrix Completion via Convex Optimization // Found. Comput. Math. — 2009. — 9. — P. 717–772.

3. Chistov A. L., Grigoriev D. Yu. Complexity of quantifier elimination in the theory of algebraically closed fields // Lecture Notes in Computer Science. — 1984. — Vol. 176. — P. 17–31.

4. Глазунов Н. М. Арифметическое моделирование случайных процессов и r-алгоритмы // Кибернетика и системный анализ. — 2012. — 1. — С. 23–32.

ОБ ИСПОЛЬЗОВАНИИ АТАКИ ЛИНЕЙНЫМ РАЗЛОЖЕНИЕМ ПРИ ПОСТРОЕНИИ ПРОТОКОЛА ГЕНЕРАЦИИ ОБЩЕГО КЛЮЧА

И. В. Зубков (Москва)

Введение. Недавно В. А. Романьков предложил в [1] принципиально новую атаку на протоколы, названную *атакой линейным разложением.* С помощью данной атаки при условии, что используемая в криптосистеме группа является линейной, за время, полиномиальное от исходных данных, во многих случаях удается получить секретный ключ, не находя секретные данные пользователей. Новизна предлагаемого ниже подхода к построению протокола заключается в том, что первый пользователь на одном из этапов применяет атаку линейным разложением для нахождения промежуточных данных.

Атака линейным разложением. Пусть дана линейная группа G. Пусть U, V — два конечных подмножества G, коммутирующие друг с другом. Пусть $A = \langle U\rangle$ и $B = \langle W\rangle$ являются подмоноидами G, порожденными множествами U и W соответственно. Для любых $a \in A, b \in B, g \in G$ положим $g^a = aga^{-1}$, $g^b = bgb^{-1}$.

Тогда по открытым данным U, W, g, g^a, g^b за полиномиальное число операций от исходных данных можно вычислить g^{ab}.

Протокол генерации общего ключа. Пусть $G = GL_k(\mathbf{F}_{3^m})$ и $Aut(G)$ — группа автоморфизмов группы G. Далее, пусть U и W — два подмножества $Aut(G)$, причем элементы U попарно коммутируют с элементами из W, а также элементы U коммутируют друг с другом. Обозначим через A и B подгруппы $Aut(G)$, порожденные U и W соответственно. Зафиксируем элемент $g \in G$. Открытые данные: U, W, g.

Алиса выбирает автоморфизм $b_1 \in B$, вычисляет $b_1(g)$, затем строит матрицу $f \in G$ такую, чтобы для любого $u \in U$ было выполнено $u(f) = f$, причем матрица $b_1(g) + f$ должна быть вырожденной, и отправляет Бобу $b_1(g) + f$.

Боб выбирает два автоморфизма $a_1, a_2 \in A$ и отправляет Алисе пару элементов $a_1(b_1(g)+f) = a_1(b_1(g))+f, a_2(b_1(g)+f) = a_2(b_1(g))+f$. Алиса вычитает из обоих элементов, полученных от Боба, матрицу f и применяет автоморфизм b_1^{-1} к полученной паре: $b_1^{-1}(a_1(b_1(g))) = a_1(g), b_1^{-1}(a_2(b_1(g))) = a_2(g)$.

После этого она применяет атаку линейным разложением и получает матрицу $a_1(a_2(g))$. Наконец, Алиса выбирает автоморфизм $b_2 \in B$ и отправляет Бобу $b_2(g)$.

Получение ключа. Алиса вычисляет $K_A = b_2(a_1(a_2(g)))$, Боб вычисляет $K_B = a_1(a_2(b_2(g)))$. Тогда общий ключ равен $K = K_A = K_B$, поскольку элементы A и B попарно коммутируют.

Выбор U, W, g. Для любого $g \in G$ определим $\chi \in Aut(G)$ так: положим $\chi(g) = \det(g) \cdot g$.

Рассмотрим три попарно коммутирующие матрицы $x, y, z \in GL_k(\mathbf{F}_{3^m})$. Тогда определим $U = \{\overline{x}; \overline{y}\}$, $W = \{\chi; \overline{z}\}$, где автоморфизмы типа $\overline{x}$ понимаются как действие сопряжением соответствующей матрицей x, то есть $\overline{x}(g) = xgx^{-1}$, где $g \in G$.

Для определения матриц x, y, z строится матрица $P \in GL_{20m}(\mathbf{F}_3)$, реализующая умножение на некоторый примитивный элемент r в мультипликативной группе поля $\mathbf{F}_{3^{20m}}$. Столбцы матрицы P^i, где $i \in \mathbb{N}$, представляют из себя столбцы матрицы P, умноженные на r^{i-1}, поэтому все матрицы P, P^2, …, $P^{3^{20m}-1}$ различны, поскольку порядок r равен $3^{20m} - 1$.

Матрицы x, y и z будут блочно-диагональными, причем верхние три блока будут размером $20m$, два из которых являются единичными матрицами, а третий — матрица P, стоящая на первом, втором и третьем местах в x, y и z соответственно. Последние блоки обозначим за x_1, y_1 и z_1, которые будут принадлежать классу C_{k-60m}, состоящему из коммутирующих матриц. Пусть C — фиксированная матрица, принадлежащая $GL_{k-60m}(\mathbf{F}_{3^m})$. Определим

$$C_{k-60m} = \{CDC^{-1} \mid D = diag\{d_1, \ldots, d_{k-60m}\}, d_1, \ldots, d_{k-60m} \in \mathbf{F}_{3^m}^*\}.$$

В качестве элемента $g \in G$ берем матрицу, состоящую из 16 блоков, причем размеры верхних левых девяти блоков равны $20m$, блоки, стоящие на диагоналях, являются невырожденными, а блоки, стоящие ниже диагональных, — нулевые.

В качестве используемой на втором этапе протокола матрицы f Алиса выбирает блочно-диагональную матрицу, два верхних блока которой равны P^{t_1} и P^{t_2} соответственно, где t_1, t_2 — случайные натуральные числа, не превосходящие $3^{20m} - 1$, третий — F' выбирается

из условия, что при приведении матрицы $b_1(g) + f$ методом Гаусса к ступенчатому виду мы должны получить вырожденную матрицу, четвертый — $F'' \in C_{k-60m}$.

Вычислительная сложность протокола. Сложность протокола оценена при фиксированных значениях параметров $k = 10001$, $m = 53$: на протокол требуется максимум 2^{105} операций в поле $\mathbf{F}_3$.

Оценка мощности множества генерируемых ключей. Количество различных ключей не менее 2^{1680}.

Стойкость протокола. Злоумышленник знает элементы g, $b_1(g) + f$, $a_1(b_1(g) + f), a_2(b_1(g) + f), b_2(g)$, следовательно, может получить $a_1(a_2(b_1(g) + f))$. Для поиска ключа можно попытаться найти автоморфизм $b' \in Aut(G)$ такой, что $b'(b_1(g) + f) = b_2(g)$, причем b' коммутирует со всеми элементами из U. Тогда при успешном поиске вычисляется $b' \circ a_1(a_2(b_1(g)+f)) = a_1(a_2(b'(b_1(g)+f))) = a_1(a_2(b_2(g))) = K$. Но тогда матрица $b_1(g) + f$ является прообразом $b_2(g)$ при действии автоморфизмом b', следовательно, является невырожденной. Полученное противоречие доказывает, что данный тип атаки к протоколу не применим.

Полный перебор всех автоморфизмов из подгрупп A и B также невозможен, поскольку они содержат не меньше, чем 2^{1680} различных элементов.

Благодарности. Автор выражает благодарность научному руководителю к.ф.-м.н. А. Е. Пакратьеву за постановку задачи и помощь в работе, а также к.ф.-м.н. А. В. Галатенко и к.ф.-м.н. В. А. Носову, которые ознакомились с результатами работы и сделали ряд полезных замечаний.

Список литературы

1. Романьков В. А. Алгебраическая криптография. — Омск: изд-во Ом. гос ун-та, 2013.

ПОДМНОЖЕСТВА МАЛОЙ МОЩНОСТИ В СИСТЕМАХ ШТЕЙНЕРА $S(2,4,4^h)$.

М. Э. Коваленко (Москва)

Системой Штейнера $S(t,k,v)$ называется пара $(V,\mathcal{B})$, где V — множество из v элементов, а $\mathcal{B}$ — семейство k-элементных подмножеств V, называемых *блоками*, таких, что любое t-элементное подмножество V лежит ровно в одном блоке. С основными результатами по системам Штейнера можно ознакомиться, например, в [1].

Наиболее изученными являются системы Штейнера с параметрами $t=2$ и $k=3$ называемые *системами троек Штейнера* $S(2,3,v)$. В России исследованием подобных систем Штейнера занимаются, в частности, В. А. и Д. В. Зиновьевы [2]. Системы Штейнера с $t=3, k=4$ также известны как *системы четверок Штейнера* $S(3,4,v)$ и тоже, в свою очередь, активно исследуются, в том числе и в России. Из последних работ можно отметить работу Д. И. Ковалевской и Ф. И. Соловьевой [3].

В последнее время уделяется больше внимания и системам Штейнера с $t=2, k=4$: так в 2010 году вышел первый обзор [4] о системах Штейнера $S(2,4,v)$. Но в то же время остается большое количество неисследованных вопросов и взаимосвязей с другими комбинаторными структурами.

Частным случаем $S(2,q,q^n)$ систем Штейнера являются системы прямых в аффинном пространстве $\mathbf{F}_q^n$ — $\mathbf{EG}_1(4,h)$.

А именно, аффинная геометрия $\mathbf{EG}(n,p^s)$ — аффинное пространство $\mathbf{F}_{p^s}^n$, где точки — это вектора из $\mathbf{F}_{p^s}^n$, прямые — это одномерные подпространства $\mathbf{F}_{p^s}^n$ и их смежные классы (по операции сложения векторов), d-мерные плоскости — d-мерные подпространства $\mathbf{F}_{p^s}^n$ и их смежные классы.

При этом, как известно, например, из [5], существует единственная система Штейнера $S(2,4,16)$, и она изоморфна аффинной плоскости. Заметим, что с ростом n появляются $S(2,q,q^n)$ системы Штейнера, не изоморфные системе, соответствующей набору прямых в аффинном пространстве.

Системы Штейнера, изоморфные аффинным геометриям, назовем *системами Штейнера особого вида.*

Здесь и далее подразумевается, что поле $\mathbf{F}_4$ реализовано в виде фактор-алгебры $\mathbf{F}_2[x]\Big/\{x^2+x+1\}$.

Теперь обратимся к строению $S(2,4,n)$. Введем для $S(2,4,n)$ следующие обозначения для различных множеств по 4 элемента, а имен-

но: $\mathbf{B}_0$ — блоки $S(2,4,n)$; $\mathbf{B}_1$ — 4-х элементные множества, пересекающиеся с каким-нибудь блоком ровно по трем элементам; $\mathbf{B}_2$ — остальные 4-х элементные множества, т. е. пересекающиеся со всеми блоками не более чем по двум элементам.

Заметим, что эти классы множеств не пересекаются. Рассмотрим множества $\mathbf{B}_2$. Они могут быть получены из трех пар блоков (так как разбиваются на три различные пары по два элемента), блоки внутри пар могут пересекаться или нет. Такие три пары блоков назовем *образующими*. Среди множеств, входящих в $\mathbf{B}_2$, за $\mathbf{S}_i$ обозначим множество четверок, для которых среди 3 пар образующих их блоков ровно в i парах есть пересечение. Выберем четверку из $\mathbf{S}_2$. Назовем две пары пересекающихся образующих блоков *проверочными*.

Рассмотрим совокупность всех подмножеств $\mathbf{F}_4^h$ как векторное пространство над $\mathbf{F}_2$ с операцией симметрической разности. Обозначим это векторное пространство за $\mathcal{A}(h)$, а за $x_i(a)$ — i-ю координату элемента $a \in A \in \mathcal{A}(h)$ или, что то же самое, $a \in \mathbf{F}_4^h$. Выбранное пространство эквивалентно булеву кубу размерности 4^h.

Итак, в $\mathbf{F}_4^h$ каждому двоичному вектору $c \in \mathbf{F}_2^{4^h}, \mathrm{wt}(c) = p$, соответствует p-множество точек из V, а им в свою очередь соответствуют p точек из $\mathbf{F}_4^h$, каждая из этих точек задается h координатами из $\mathbf{F}_4$. Тогда введем операцию сложения блоков или множеств точек из $\mathbf{F}_4^h$: при сложении рассматриваем двоичные векторы кода, соответствующие слагаемым, получаем двоичный вектор суммы и рассматриваем соответствующий ему блок или множество точек. Эта операция по своей сути эквивалентна операции симметрической разности для множеств. Блокам $S(2,4,4^h)$ соответствуют прямые $\mathbf{F}_4^h$.

Теорема 1. *Для любой системы Штейнера $S(2,4,4^h)$ особого вида сумма любых проверочных блоков принадлежит этой системе.*

Квазигруппой Штейна называют пару $(P;\circ)$, если P группоид, а $\circ$ удовлетворяет следующим свойствам:

$$x \circ x = x;\ (x \circ y) \circ y = y \circ x;\ (y \circ x) \circ y = x.$$

Тогда рассмотрим $B := \{\{x, y, x \circ y, y \circ x\} | x, y \in P, x \neq y\}$. Очевидно, что (P, B) является системой Штейнера $S(2,4,v)$, и по системе Штейнера $S(2,4,v)$ можно построить квазигруппу Штейна. Для этого определим на $\{0,1,2,3\}$ бинарную операцию «$\cdot$»:

$$\left(\begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 2 & 3 & 1 \\ 1 & 3 & 1 & 0 & 2 \\ 2 & 2 & 3 & 2 & 0 \\ 3 & 1 & 0 & 1 & 3 \end{array}\right).$$

Тогда для каждого блока $b \in B$ выберем биекцию $\phi_b : b \to \{0;1;2;3\}$ и определим на P операцию «$\circ$» так: $x \circ y := \phi_b^{-1}(\phi_b(x) \cdot \phi_b(y))$, для всех $x, y \in P$, для которых определены $\phi_b(x)$ и $\phi_b(y)$. Полученная пара $(P;\circ)$ будет квазигруппой Штейна.

Известно, что, если для квазигруппы Штейна выполняется дистрибутивность $(x \circ y) \circ (z \circ w) = (x \circ z) \circ (y \circ w)$, то соответствующая система Штейнера будет особого вида. Также можно отметить выполнение указанной дистрибутивности для блоков и проверочных четверок. То же верно и для проверочных блоков. Можно утверждать следующее:

Теорема 2. *В системах Штейнера особого вида отсутствуют четверки вида* $\mathbf{S}_1$ *и* $\mathbf{S}_3$.

Более того для четверок $\mathbf{S}_3$ верно и обратное:

Теорема 3. *Если для любых проверочных блоков их сумма принадлежит системе Штейнера, то в ней не могут лежать четверки, для которых среди трех пар образующих блоков во всех парах есть пересечение.*

Список литературы.

1. Colbourn C. J., Dinitz J. H. Handbook of combinatorial designs, second edition. — Chapman and Hall, CRC, 2006.

2. Zinoviev V.A., Zinoviev D.V. Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+1 over $\mathbf{F}_2$ // Problems of Information Transmission — 2012. — Vol. 48, no. 2 — P. 102–126.

3. Ковалевская Д. И., Соловьева Ф. И. О системах четвёрок Штейнера малого ранга, вложимых в расширенные совершенные двоичные коды // Дискретн. анализ и исслед. опер. — 2012. — Т. 19, № 5. — С. 47 – 62.

4. Reid C., Rosa A. Steiner systems $S(2,4,v)$ — a survey // The Electronic Journal of Combinatorics. — 2010. — DS18.

5. Таранников Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011.

ОБОБЩЁННЫЕ ТАБЛИЦЫ СООТВЕТСТВИЯ СОСТОЯНИЙ СПЕЦИАЛЬНЫХ КЛАССОВ РЕГУЛЯРНЫХ ЯЗЫКОВ И ОЦЕНКИ ЧИСЛА ЭТИХ ТАБЛИЦ

С. Ю. Корабельщикова (Архангельск),
Б. Ф. Мельников (Самара)

Согласно [1, 2] и др., каждому регулярному языку можно с помощью специального сюръективного отображения поставить в соответствие определённое для этого языка бинарное отношение # (или, по-другому, таблицу соответствия состояний). Это бинарное отношение определено для пар, состоящих из Q_π (состояние автомата $\widetilde{L}$ — канонического автомата для рассматриваемого регулярного языка L) и Q_ρ (состояние автомата $\widetilde{L^R}$ — канонического автомата для регулярного языка L^R). Более того, также согласно [1, 2] (см. также [3]), при некоторых ограничениях на отношение # любой вариант этого отношения соответствует некоторому регулярному языку L — языку полного конечного автомата.

При этом по таблице соответствия состояний определяются псевдоблоки — пара непустых подмножеств $P \subseteq Q_\pi$ и $R \subseteq Q_\rho$, таких что

$$(\forall p \in P)\ (\forall r \in R)\ (p \# r).$$

Среди псевдоблоков особое значение имеют блоки, для каждого из которых (пусть рассматриваемый псевдоблок — снова (P, R)) дополнительно выполняются следующие два условия:

$$\big(\forall p \in Q_\pi \backslash P\big)\ \big(\text{пара}\,(P \cup \{p\}, R)\,\text{не является псевдоблоком}\big);$$

$$\big(\forall r \in Q_\rho \backslash R\big)\ \big(\text{пара}\,(P, R \cup \{r\})\,\text{не является псевдоблоком}\big).$$

Несложно показывается, что в случае $|Q_\pi| = |Q_\rho| = n$ максимально возможным количеством блоков является $2^n - 2$.

При рассмотрении специальных классов регулярных языков [4; гл.7] (см. также [5, 6] и др.) возникают задачи, являющиеся обобщением вышеописанных на k-мерный случай. В этом случае состояния канонических конечных автоматов $\widetilde{L}$ и $\widetilde{L^R}$ строятся на основе различных вариантов двух непустых непересекающихся подмножеств k-элементных множеств. В общем вместо бинарных рассматриваются k-арные отношения, для которых аналогичным образом

определяются псевдоблоки и блоки. Например, для $k = 3$ псевдоблоком является тройка непустых подмножеств $P \subseteq Q_\pi$, $R \subseteq Q_\rho$ и $S \subseteq Q_\sigma$, таких что

$$(\forall p \in P)\ (\forall r \in R)\ (\forall s \in S)\ (\#(p, r, s)).$$

Полученные объекты мы называем обобщёнными таблицами соответствия состояний специальных классов регулярных языков.

После определения блока несложно показывается, что если тройка (P, R, S) образует блок (в 3-мерном случае), то пара (P, R) образует блок в 2-мерном случае. (Аналогично — для 2 оставшихся пар подмножеств, для многомерного случая, и т.д.)

Обозначив записью $\Omega_k(n)$ максимально возможное число k-арных блоков в случае, когда каждое из k подмножеств состоит из n элементов, мы при $k = 2$ несложно получаем достижимую нижнюю оценку значения $\Omega_2(n)$:

$$\Omega_2(n) = 2^n - 2.$$

(Здесь в наших обозначениях в 2-мерном случае выше рассматриваются 2 подмножества, P и R.) Поэтому на основе вышеизложенного очевидны такие нижние оценки значений $\Omega_k(n)$:

$$\Omega_k(n) \geq 2^n - 2.$$

Сформулируем сказанное выше, а также некоторые факты, в виде следующих утверждений.

Утверждение 1. $\Omega_2(n) = 2^n - 2$.

Утверждение 2. $(\forall k \geq 2)\,(\Omega_k(n) < \Omega_{k+1}(n))$.

Отметим, что из сказанного выше следовало только нестрогое неравенство. Строгое неравенство является следствием того факта, что при построении проекции k-арного отношения на меньшую размерность прообразы некоторых псевдоблоков, не являющихся блоками, могут являться блоками.

Утверждение 3.

$$\Omega_3(n) \geq 6 - n + \sum_{i=2}^{n-1} (2^i - 2) \cdot C_n^i\,.$$

Последняя оценка получена путём рассмотрения конкретного примера.

Список литературы

1. Долгов В. Н., Мельников Б. Ф. Построение универсального конечного автомата. I. От теории к практическим алгоритмам // Вестник Воронежского государственного университета. Серия «Физика. Математика». — 2013. — № 2. — С. 173–181.

2. Долгов В. Н., Мельников Б. Ф. Построение универсального конечного автомата. II. Примеры работы алгоритмов // Вестник Воронежского государственного университета. Серия «Физика. Математика». — 2014. — № 1. — С. 78–85.

3. Долгов В. Н., Мельников Б. Ф. Об алгоритмах автоматического построения Ватерлоо-подобных конечных автоматов на основе полных автоматов // Эвристические алгоритмы и распределенные вычисления. — 2014. — № 4. — С. 24–45.

4. Саломаа А. Жемчужины теории формальных языков. — М.: Мир, 1986.

5. Мельников Б. Ф. Описание специальных подмоноидов глобального надмоноида свободного моноида // Известия высших учебных заведений. Математика. — 2004. — № 3. — С. 46–56.

6. Корабельщикова С. Ю., Чесноков А. И., Тутыгин А. Г. О первообразных корнях из языков специального вида // Труды IX Международной конференции «Дискретные модели в теории управляющих систем». — 2015. — С. 116–118.

О РАССТОЯНИИ ХЭММИНГА МЕЖДУ САМОДУАЛЬНЫМИ БУЛЕВЫМИ БЕНТ-ФУНКЦИЯМИ

А. В. Куценко (Новосибирск)

В данной работе рассматриваются бент-функции — булевы функции от чётного числа переменных, обладающие максимально возможной нелинейностью — одним из важнейших криптографических свойств и в силу этого представляющие большой интерес.

Скалярным произведением векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_2^n$ называется число $\langle x, y\rangle = \bigoplus\limits_{i=1}^{n} x_i y_i$, где операция $\oplus$ есть *сложение* по модулю 2. *Преобразование Уолша—Адамара*

булевой функции f от n переменных — целочисленная функция $W_f : \mathbb{Z}_2^n \to \mathbb{Z}$: $W_f(y) = \sum\limits_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x,y \rangle}$. В 60-х годах XX века О. Ротхаусом было введено понятие *бент-функции*. Одними из первых отечественных учёных, исследовавших эти функции в то же время, были В. А. Елисеев и О. П. Степченков [1]. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{Z}_2^n$ [2]. Для каждой бент-функции f равенством $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$, $x \in \mathbb{Z}_2^n$ определяется *дуальная* к ней булева функция $\tilde{f}$. Бент-функция f называется *самодуальной (анти-самодуальной)*, если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается как $dist(f, g)$.

Сложной задачей является полная характеризация и описание класса самодуальных бент-функций. Этим и другим вопросам посвящены несколько работ за рубежом (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou и др.). В частности, в работе [3] перечислены все самодуальные бент-функции от 2, 4, 6 переменных и все квадратичные самодуальные бент-функции от 8 переменных. В статье [4] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных можно найти в работе [5].

Известна следующая конструкция бент-функций — *конструкция Мэйорана—МакФарланда*, 1973 г.: пусть h — любая перестановка на $\mathbb{Z}_2^n$, пусть g — произвольная булева функция от $n/2$ переменных. Тогда функция $f(x, y) = \langle x, h(y) \rangle \oplus g(y)$ является бент-функцией от n переменных [6]. Эта конструкция является достаточно богатой. В работе [3] были найдены необходимые и достаточные условия самодуальности бент-функции, построенной с помощью конструкции Мэйорана—МакФарланда, в случае $h \in GL(n/2, \mathbb{Z}_2)$.

В работе получен полный спектр расстояний Хэмминга между бент-функциями из класса Мэйорана—МакФарланда, совпадающими со своими дуальными, со следующим ограничением: перестановка, фигурирующая в данной конструкции, должна быть элементом полной линейной группы соответствующего порядка. На основании этого результата сделан вывод о минимальном расстоянии Хэмминга между рассмотренными функциями.

Теорема. *Пусть f_1, f_2 — различные бент-функции от чётного*

числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана—МакФарланда при условии, что перестановка является элементом $GL(n/2, \mathbb{Z}_2)$. Если f_1, f_2 — самодуальные бент-функции, то

$$dist(f_1, f_2) = \begin{cases} 2^{n-1} \\ 2^{n-1}\left(1 \pm \frac{1}{2}\right) \\ 2^{n-1}\left(1 \pm \frac{1}{2^2}\right) \\ \vdots \\ 2^{n-1}\left(1 \pm \frac{1}{2^{n/2-1}}\right) \\ 2^n \end{cases}.$$

Следствие. *Пусть f_1, f_2 — различные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана—МакФарланда при условии, что перестановка является элементом $GL(n/2, \mathbb{Z}_2)$. Если f_1, f_2 — самодуальные бент-функции, то*

$$dist(f_1, f_2) \geqslant 2^{n-2}.$$

Список литературы

1. Tokareva N. Bent functions: results and applications to cryptography. — Acad. Press. Elsevier, 2015.

2. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. — 1976. — V. 20, I. 3. — P. 300–305.

3. Carlet C., Danielson L. E., Parker M. G., Solé P. Self dual bent functions // Int. J. Inform. Coding Theory. — 1. — 2010. — P. 384–399.

4. Hou X. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. — 2012. — 63. — P. 183–198.

5. Feulner T., Sok L., Solé P., Wassermann A. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr — 2013. — 68. — P. 395–406.

6. McFarland R. L. A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. — 1973. — V. 15, I. 1. — P. 1–10.

О РАСПРЕДЕЛЕНИИ НЕТЕРМИНАЛОВ В ДЕРЕВЬЯХ ВЫВОДА СОГЛАСОВАННОЙ СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКИ

И. М. Мартынов (Нижний Новгород)

В работе исследуются деревья вывода высоты t, порождаемые согласованной стохастической КС-грамматикой, при $t \to \infty$.

Стохастической КС-грамматикой [1] называется четвёрка $G = \langle V_N, V_T, R, s\rangle$, где V_N и V_T — конечные алфавиты *нетерминальных* и *терминальных* символов, $s \in V_N$ — аксиома, $R = \cup_{i=1}^{n} R_i$, где $n = |V_N|$ и R_i — конечное множество *правил вывода* r_{ij} вида:

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij},$$

где $j = 1, 2, \ldots, |R_i|$, $A_i \in V_N$, $\beta_{ij} \in (V_N \cup V_T)^*$, и p_{ij} — вероятность применения правила r_{ij}, причём $0 < p_{ij} \leq 1$ и $\sum_{j=1}^{n_i} p_{ij} = 1$.

Применение правила r_{ij} грамматики к слову $\alpha \in (V_N \cup V_T)^*$ состоит в замене какого-либо вхождения нетерминала A_i в α на слово β_{ij}. Язык L_G, порождаемый грамматикой G, содержит все слова из алфавита V_T, которые можно получить из аксиомы s последовательным применением правил вывода.

Каждому слову α из L_G соответствует последовательность $\omega(\alpha) = (r_1, r_2, \ldots, r_k)$ правил вывода, с помощью последовательного применения которых слово α можно получить из аксиомы s. При этом $\omega(\alpha)$ называется *выводом* слова α. Выводу слова соответствует *дерево вывода* [2] d, вероятность $p(d)$ которого определяется как произведение вероятностей правил, образующих вывод: $p(d) = \prod_{i=1}^{k} p(r_i)$. Одному и тому же слову $\alpha \in L_G$ может соответствовать более одного дерева вывода. Вероятность слова $\alpha \in L_G$ определяется как сумма вероятностей всех порождающих его деревьев.

Грамматика называется *согласованной*, если сумма вероятностей всех конечных деревьев вывода равна 1. Согласованная стохастическая грамматика G задаёт распределение вероятностей на множестве слов порождаемого ею языка L_G. В работе рассматриваются согласованные грамматики.

По стохастической КС-грамматике строится матрица A первых моментов. Её элемент a_j^i определяется как $\sum_{k=1}^{n_i} p_{ik} s_{ik}^j$, где величина s_{ik}^j равна числу нетерминальных символов A_j в правой части правила вывода r_{ik}. *Перронов корень* [3] матрицы A обозначим через r. Известно, что для согласованной грамматики $r \leq 1$.

Будем обозначать $A_i \to A_j$, если в грамматике имеется правило вывода вида $A_i \xrightarrow{p_{ij}} \alpha_1 A_j \alpha_2$, где $\alpha_1, \alpha_2 \in (V_N \cup V_T)^*$. Рефлексивное транзитивное замыкание отношения $\to$ обозначим $\to_*$. Будем обозначать $A_i \leftrightarrow_* A_j$, если одновременно $A_i \to_* A_j$ и $A_j \to_* A_i$. Множество V_N нетерминалов разбивается на классы эквивалентности $K_1, K_2, \ldots, K_m$ по отношению $\leftrightarrow_*$. Будем обозначать $K_i \prec K_j$, если существуют $A_{k_i} \in K_i$ и $A_{k_j} \in K_j$, такие что $A_{k_i} \to A_{k_j}$. Рефлексивное транзитивное замыкание $\prec$ обозначим $\prec_*$.

Случай $r < 1$ (докритический случай) рассматривался Л. П. Жильцовой в [4] и других работах. А. Е. Борисов обобщил полученные результаты на случай $r \leq 1$ для разложимой грамматики, содержащей два класса нетерминалов.

Пусть классы нетерминалов пронумерованы таким образом, что $i \leq j$ для любых $K_i \prec_* K_j$. Матрица A первых моментов грамматики в этом случае имеет вид:

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1,m} \\ 0 & A_{22} & \cdots & A_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{m,m} \end{pmatrix}.$$

Для каждого класса K_i матрица A_{ij} неразложима. Обозначим через r_i перронов корень матрицы A_{ii}. Очевидно, $r = \max_i\{r_i\}$. Обозначим $J = \{i : r_i = r\}$.

Для пары классов K_i и K_j рассмотрим всевозможные цепочки $K_{i_1} \prec K_{i_2} \prec \ldots \prec K_{i_k}$, где $i_1 = i$ и $i_k = j$. Обозначим через s_{ij} максимальное число классов с номерами из J в такой цепочке. Будем также обозначать $s_i = \max_j\{s_{ij}\}$.

Рассмотрим случайное дерево вывода d высоты t, порождённое грамматикой. Обозначим число применений правила r_{ij} в таком дереве через $q_{ij}(t)$, и число нетерминалов A_i в дереве через $q_i(t)$.

Теорема 1. *Для деревьев вывода высоты t, порождённых согласованной стохастической КС-грамматикой, выполняются соотношения:*

$$M(q_{ij}(t)) \sim c_i \cdot p_{ij} \cdot t^{\left(\frac{1}{2}\right)^{s_1 - s_{1l} - 1}},$$

$$M_i(t) \sim d_i \cdot t^{\left(\frac{1}{2}\right)^{s_1 - s_{1l} - 1}}$$

где p_{ij} — вероятность правила r_{ij}, c_i и d_i — некоторые константы, и $A_i \in K_l$.

Теорема 2. *Для любой пары нетерминалов $A_i \in K_h$, $A_j \in K_l$, такой что $s_{1h} = s_{1l}$, при $t \to \infty$ выполняется условие:*

$$D\left(\frac{q_i(t)}{q_j(t)} - \frac{d_i}{d_j}\right) \to 0,$$

где $q_i(t)$, $q_j(t)$ — число нетерминалов A_i и A_j в случайном дереве вывода высоты t, d_i и d_j — некоторые константы.

Теоремы 1 и 2 обобщают результаты, опубликованные в [5] и [6].

Таким образом, соотношение числа нетерминалов в деревьях вывода высоты t становится всё ближе к фиксированному значению при $t \to \infty$.

Список литературы

1. Фу. К. Структурные методы в распознавании образов. — М.: Мир, 1977.

2. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. — М.: МИР, 1978.

3. Гантмахер Ф. Р. Теория матриц. — М.: ФИЗМАТЛИТ, 2010.

4. Жильцова Л. П. Закономерности применения правил грамматики в выводах слов стохастического контекстно-свободного языка // Математические вопросы кибернетики. — М.: Наука, 2000. Вып. 9. — С. 101–126

5. Мартынов И. М. О распределении нетерминалов в деревьях вывода стохастической КС-грамматики вида "цепочки"// Материалы XVII Международной конференции "Проблемы теоретической кибернетики"(Казань, 16–20 июня 2014 г.). — С. 195–197.

6. Мартынов И. М. О числе нетерминалов в деревьях вывода разложимой стохастической КС-грамматики // Труды IX Международной конференции "Дискретные модели в теории управляющих систем". (Москва и Подмосковье, 20–22 мая 2015 г.) — С. 159-161.

О ПРИМЕНЕНИИ БУЛЕВЫХ ФУНКЦИЙ ДЛЯ ПОСТРОЕНИЯ КВАЗИГРУПП И СИНТЕЗА БЛОЧНЫХ ШИФРОВ

В. А. Носов, А. Е. Панкратьев (Москва)

Для криптографических приложений большой интерес представляют способы построения широких классов квазигрупп. Различные

квазигрупповые операции, определенные на одном множестве элементов, используются для синтеза поточных шифров [1]; таблица Кэли квазигруппы, представляющая собой латинский квадрат, служит основой для шифра табличного гаммирования.

Один из способов построения больших параметрических семейств латинских квадратов основан на использовании семейств функций, обладающих свойством правильности [2]. А именно, семейство функций $F = \{f_1, \ldots, f_n\}$ от n переменных $x_1, \ldots, x_n$ называется правильным, если для любых различных наборов $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ найдется индекс α такой, что $x'_\alpha \neq x''_\alpha$, но при этом $f_\alpha(x') = f_\alpha(x'')$.

Теорема [2]. *Пусть L — матрица размера $2^n \times 2^n$, элементы которой суть n-мерные двоичные векторы, причем номера строк и столбцов матрицы L представлены также в виде двоичных векторов размерности n. Далее, пусть элемент $L(x, y) = (z_1, \ldots, z_n)$ на пересечении строки $x = (x_1, \ldots, x_n)$ и столбца $y = (y_1, \ldots, y_n)$ определяется формулами*

$$z_i = x_i + y_i + f_i(p_1(x_1, y_1), p_2(x_2, y_2), \ldots, p_n(x_n, y_n)), \qquad i = 1, \ldots, n,$$

где p_i и f_i, $i = \overline{1, n}$, являются булевыми функциями соответственно от 2 и от n переменных.

Тогда матрица L является латинским квадратом при любом выборе функций p_i, $i = \overline{1, n}$, в том и только том случае, когда семейство $F = \{f_1, f_2, \ldots, f_n\}$ является правильным.

Имеется ряд примеров правильных семейств функций в произвольных размерностях. Кроме того, установлены некоторые их свойства (в том числе в терминах графа существенной зависимости) и исследованы мощности образов соответствующих отображений. Однако вопрос о нахождении количества правильных семейств функций произвольной размерности и их полной классификации пока остается открытым.

Еще одно криптографическое применение правильных семейств функций связано с возможным обобщением схемы Фейстеля.

Схема Фейстеля [2] — криптографический примитив, широко используемый при синтезе блочных шифров. Входной блок текста подразбивется на правую и левую половины (L_0, R_0) и преобразуется по формулам

$$\begin{cases} L_1 = R_0, \\ R_1 = L_0 \oplus F(R_0, K_0), \end{cases}$$

где функция F осуществляет усложняющее преобразование, зависящее от ключа K_0. Как правило, в системах защиты информации используется несколько итераций схемы Фейстеля с подходящим выбором ключей.

Рассмотрим шифр, который преобразует блок $x = (x_1, \ldots, x_n)$ двоичного текста длины $n = 2^k$ в блок $y = (y_1, \ldots, y_n)$ шифртекста по правилу

$$y_j = x_j + f_j(p_1(x_1), p_2(x_2), \ldots, p_n(x_n)), \qquad j = \overline{1,n}, \qquad (0)$$

где p_i и f_i, $i = \overline{1,n}$, суть булевы функции от 1 и от n аргументов соответственно. Сформулируем условия, которым должно удовлетворять семейство функций $F_0 = \{f_1, \ldots, f_n\}$ для того, чтобы отображение (0) являлось биекцией при любом выборе функций $p_1, \ldots, p_n$.

Теорема. *Отображение* (0) *является биекцией при любом выборе функций* p_i, $i = \overline{1,n}$, *тогда и только тогда, когда семейство функций* F_0 *является правильным.*

Теперь представим входной блок в виде последовательности биграмм $(x_1, \ldots, x_n) \to (x'_1, \ldots, x'_{n/2})$, $x'_i = (x_{2i-1}, x_{2i})$, и определим преобразование $x' \to y'$ блока биграмм по следующим формулам:

$$y'_j = x'_j + f'_j(p'_1(x'_1), p'_2(x'_2), \ldots, p'_{n/2}(x'_{n/2})), \qquad j = \overline{1,n/2}. \qquad (1)$$

Здесь p'_i и f'_i, $i = \overline{1,n}$, — функции 4-значной логики.

Теорема. *Отображение* (1) *является биекцией при любом выборе функций* p_i, $i = \overline{1,n}$, *тогда и только тогда, когда семейство функций* $F_1 = \{f'_1, \ldots, f'_{n/2}\}$ *является правильным.*

Теперь объединим биграммы в пары, далее перейдем к фрагментам по 8 бит, и продолжим укрупнять разбиение входного блока, попарно объединяя фрагменты. На каждом шаге приведенное выше утверждение о биективности отображения остается справедливым.

Наконец, на $(k-1)$-м шаге укрупнения мы получаем два полублока $x_1^{(k-1)} = (x_1, x_2, \ldots, x_{2^{k-1}})$, $x_2^{(k-1)} = (x_{2^{k-1}+1}, x_{2^{k-1}+2}, \ldots, x_{2^k})$, которые преобразуются по формулам

$$y_j^{(k-1)} = x_j^{(k-1)} + f_j^{(k-1)}(p_1^{(k-1)}(x_1^{(k-1)}), p_2^{(k-1)}(x_2^{(k-1)})), \qquad (k-1)$$

где $j = 1, 2$.

Теорема. *Отображение* $(k-1)$ *является биекцией при любом выборе* $p_1^{(k-1)}, p_2^{(k-1)}$ *если и только если семейство* $\{f_1^{(k-1)}, f_2^{(k-1)}\}$

является правильным; в случае двух функций это означает, что одна из функций является константой, а другая не зависит существенным образом от одноименного аргумента.

Нетрудно видеть, что, с точностью до перестановки полублоков, полученное преобразование соответствует классической схеме Фейстеля.

Таким образом, в работе предлагается метод обобщения схемы Фейстеля посредством подразбиения входного блока на более чем два фрагмента, выбора правильного семейства функций $\{f_j\}$, и использования преобразований (0), (1), ..., $(k-1)$, где функции p_j играют роль сменных ключей. Вопрос об оптимальном выборе шага укрупнения остается открытым, поскольку его нахождение сопряжено с определением мощности ключевого пространства, что напрямую связано с подсчетом количества правильных семейств соответствующей размерности.

Список литературы

1. Markovski S., Gligoroski D., Bakeva V. Quasigroup string processing: Part 1 // Proc. of Maced. Acad. of Sci. and Arts for Math. and Tech. Sci. — 1999. — XX (1–2). — P. 13–28.

2. Feistel H. Cryptography and computer privacy // Scientific American. — 1973. — 228 (5). — P. 15–23.

3. Nosov V. A., Pankratiev A. E. Latin squares over Abelian groups // Journal of Mathematical Sciences. — 2008. — 149 (3). — P. 1230–1234.

О ВОЗМОЖНОСТИ ПОСТРОЕНИЯ m-УСТОЙЧИВЫХ ФУНКЦИЙ С ОПТИМАЛЬНОЙ НЕЛИНЕЙНОСТЬЮ В РАМКАХ ОДНОГО МЕТОДА

Ю. В. Таранников (Москва)

Вес $\mathrm{wt}(f)$ булевой функции f над $\mathbf{F}_2^n$ — это число наборов x из $\mathbf{F}_2^n$, для которых $f(x) = 1$. *Подфункцией* булевой функции f называется функция f', полученная подстановкой в f некоторых констант 0 или 1 вместо некоторых переменных.

Для двух булевых функций f_1 и f_2 на $\mathbf{F}_2^n$ расстояние между f_1 и f_2 определяется как $d(f_1, f_2) = |\{x \in \mathbf{F}_2^n | f_1(x) \neq f_2(x)\}|$. Для заданной функции f из $\mathbf{F}_2^n$ минимум расстояний $d(f, l)$, где l пробегает множество всех аффинных функций, называется *нелинейностью* функции f и обозначается через $\mathrm{nl}(f)$.

Булева функция f от n переменных называется m-устойчивой, если $\mathrm{wt}(f') = 2^{n-m-1}$ для любой ее подфункции f' от $n-m$ переменных.

Нелинейность и корреляционная иммунность (m-устойчивость) относятся к числу наиболее важных криптографических характеристик булевых функций, поэтому крайне желательно, чтобы функции, использующиеся в шифрах, обладали одновременно высокими нелинейностью и устойчивостью. Однако в 2000 была доказана [1–3] верхняя оценка нелинейности m-устойчивых функций на $\mathbf{F}_2^n$:

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^{m+1} \tag{1}$$

при $m \leq n-2$, в которой если и может достигаться равенство, то только при $\frac{n-3}{2} \leq m \leq n-2$. Одновременно в [2] были построены функции, для которых достигалось равенство в (1) при $\frac{2n-7}{3} \leq m \leq n-2$. Отсюда актуальной стала задача построения функций, достигающих равенства в оценке (1) (как говорили, построения функций с максимально возможной нелинейностью). С практической точки зрения важна не столько нелинейность, сколько *относительная нелинейность,* т. е. величина $\frac{\mathrm{nl}(f)}{2^n}$, точнее, отклонение относительной нелинейности от 0.5. Отклонение относительной нелинейности любой булевой функции на $\mathbf{F}_2^n$ от 0.5 не меньше $\frac{1}{2^{\frac{n}{2}+1}}$, в то же время, если построить m-устойчивую функцию на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ при m, близком к $0.5n$, то отклонение ее относительной нелинейности от 0.5 будет равно $\frac{1}{2^{n-m-1}}$, т. е. близко к нижней оценке наилучшего возможного отклонения. Поэтому прогресс в задаче построения m-устойчивых функций на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ при m, близких к $0.5n$, по прежнему является важным, потому что позволит соединить нелинейность, близкую к оптимальной, с очень высокой устойчивостью. Область значений параметров, для которых построены функции, на которых достигается равенство в (1), неоднократно расширялась. В 2014 году с помощью техники *обобщенных подходящих матриц* в [4] построены функции, достигающие равенства в (1), для $m \geq 0.5789...n(1+o(1))$. В [5] техни-

ка рекурсивного построения обобщенных подходящих матриц была сформулирована на языке несократимых разложений сумм продуктов.

Утверждение 1. [5] *Пусть* $n, C_k \in \mathbf{N}$, $C_k \le A_{n,k}$, $k = 0, 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$, *где* $A_{n,k}$ — *максимально возможное значение длины суммы* (n,k)*-продуктов с несократимым разложением. Положим* $C = \frac{1}{1+\log_2 X_{max}}$, *где* X_{max} — *старший корень многочлена* $x^n - \sum\limits_{k=0}^{\lfloor \frac{n}{2} \rfloor} C_k x^k$. *Тогда для любого* $\varepsilon > 0$, *начиная с некоторого* n_0, *для всех пар* (n,m), *таких что* $\frac{m}{n} > C + \varepsilon$, $n \ge n_0$, $m \le n-2$, *существует* m*-устойчивая функция от* n *переменных, на которой достигается равенство в* (1).

В связи с этим становится понятно, что для того, чтобы с помощью техники рекурсивного построения обобщенных подходящих матриц работ [4] и [5] была возможность построить m-устойчивые функции на $\mathbf{F}_2^n$ с оптимальной нелинейностью с отношением m/n, стремящимся к 0.5, нужно, чтобы старший корень X_{max} уравнения

$$x^n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} A_{n,k} x^k \tag{2}$$

с ростом n стремился к 2.

В настоящей работе показывается, что X_{max} не стремится к 2.

Пусть $k/n \to \lambda$; предположим, что k-е слагаемое — максимальное в правой части (2).

Из $A_{n,k} \le \frac{\binom{n}{k}}{2^k}$ следует, что $X_{max}^n \le X_{max}^k \cdot \frac{2^{nH(k/n)}}{2^k} \cdot Pol(n)$, т. е.

$$X_{max} \le 2^{(H(\lambda)-\lambda)/(1-\lambda)}.$$

Аналогично из $A_{n,k} \le \binom{n}{2k}$ следует, что $X_{max}^n \le X_{max}^k \cdot 2^{nH(2k/n)} \cdot Pol(n)$, т. е.

$$X_{max} \le 2^{H(2\lambda)/(1-\lambda)}.$$

Таким образом, $X_{max} \le \min\{2^{(H(\lambda)-\lambda)/(1-\lambda)}, 2^{H(2\lambda)/(1-\lambda)}\}$.

Равенство $H(\lambda) - \lambda = H(2\lambda)$ достигается при $\frac{H(\lambda)-\lambda}{1-\lambda} = 0.97896...$, что с учетом поведения графиков функций дает $X_{max} \le 1.971044...$

Отсюда следует, что ограничиваясь средствами, предложенными в [4, 5], нельзя построить m-устойчивые функции от n переменных с

оптимальной нелинейностью при $m/n \leq \frac{1}{1+\log_2(1.971044...)}(1+o(1)) = 0.505316...(1+o(1))$. Впрочем, сказанное не исключает дальнейшего совершенствования методов. Заметим, что отношение m/n, близкое к 0.505316..., для многих практических целей является хорошим, поэтому построения в рамках техники [5] тоже представляют интерес.

Работа выполнена при финансовой поддержке РФФИ, проект 16–01–00226.

Список литературы

1. Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions // Advanced in Cryptology: Crypto 2000, Proceedings. Lecture Notes in Computer Science. — Springer-Verlag, 2000. — V. 1880. — P. 515–532.

2. Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity // Proceedings of Indocrypt 2000. Lecture Notes in Computer Science. — Springer-Verlag, 2000. — V. 1977. — P. 19–30.

3. Zheng Y., Zhang X.-M. Improved upper bound on the nonlinearity of high order correlation immune functions // Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000. Lecture Notes in Computer Science. — Springer-Verlag, 2001. — V. 2012. — P. 264–274.

4. Tarannikov Y. V. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters // Сибирские электронные математические известия — 2014. — V. 11. — P. 229-245 (`http://semr.math.nsc.ru/v11/p229-245.pdf`).

5. Таранников Ю. В. Несократимые разложения однородных произведений двучленов для построения m-устойчивых функций с максимально возможной нелинейностью // Проблемы теоретической кибернетики. Материалы XII международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 271–272.

СОХРАНЯЮЩИЕ МЕРУ И ЭРГОДИЧЕСКИЕ АСИНХРОННО АВТОМАТНЫЕ ОТОБРАЖЕНИЯ

Л. Б. Тяпаев (Саратов)

Автоматные преобразования над алфавитом $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, 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 [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 [4–7]. 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 (преобразователь) это шестерка объектов $\mathfrak{A} = (\mathfrak{I}, \mathcal{S}, \mathcal{O}, S, O, s_0)$, где $\mathfrak{I}$ — входной алфавит, $\mathcal{S}$ — множесто состояний автомата, $\mathcal{O}$ — выходной алфавит, $S\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{S}$ — функция переходов, $O\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{O}$ — функция выхода, $s_0 \in \mathcal{S}$ — начальное состояние. *Асинхронный автомат* $\mathfrak{B}$ определяется похожим образом, за исключением функции выхода: $O\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{O}^*$. 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 $\mathfrak{I} = \mathcal{O} = \mathbb{F}_p$.

В случае с автоматом $\mathfrak{A}$ слова конечной длины над алфавитом $\mathbb{F}_p$ суть неотрицательные целые числа: слово $u = \alpha_{n-1} \ldots \alpha_1 \alpha_0$, где $\alpha_i \in \mathbb{F}_p$ $i = 0, 1, 2, \ldots, n-1$, мы рассматриваем как число $\alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{n-1} \cdot p^{n-1}$, записанное в системе счисления с основанием p. В свою очередь, это число есть элемент кольца вычетов $\mathbb{Z}/p^n\mathbb{Z}$ по модулю p^n. Т. о., каждому автомату $\mathfrak{A}$ соответсвует отображение $\mathbb{Z}/p^n\mathbb{Z}$ в $\mathbb{Z}/p^n\mathbb{Z}$, для всех $n = 1, 2, 3 \ldots$. Более того, каждый автомат $\mathfrak{A}$ *определяет отображение* $f_{\mathfrak{A}}$ *из кольца целых* p*-адических чисел* $\mathbb{Z}_p$ *в себя*: слово бесконечной длины $\alpha = \ldots \alpha_{n-1} \ldots \alpha_1 \alpha_0$ над алфавитом $\mathbb{F}_p$ рассматривается как целое p-адическое число x, $x = x(\alpha) = \alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{n-1} \cdot p^{n-1} + \ldots = \sum_{i=0}^{\infty} \delta_i(x) \cdot p^i$, где $\delta_i(x) \in \mathbb{F}_p$. Для

любого $x \in \mathbb{Z}_p$ положим $\delta_i(f_{\mathfrak{A}}(x)) = O(\delta_i(x), s_i)$, $i = 0, 1, 2, \ldots$, где $s_i = S(\delta_{i-1}(x), s_{i-1})$, $i = 1, 2, \ldots$. 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 [1]; класс асинхронно автоматных отображений — нет.

Рассмотрим асинхронно автоматные отображения специального типа. Отображение $f_{\mathfrak{B}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется *отображением с задержкой* n, $n \in \mathbb{N}$, если данный асинхронный автомат $\mathfrak{B}$ бесконечное слово $\alpha = \ldots \alpha_{n-1} \ldots \alpha_1 \alpha_0$ преобразует в слово $\beta = \ldots \beta_{n+1} \beta_n$ так что, $O(\delta_i(\alpha_{n-1} \ldots \alpha_1 \alpha_0), s_i) = e$, где e пустое слово, $i = 0, 1, 2 \ldots, n-1$, $s_i = S(\delta_i(\alpha_{n-1} \ldots \alpha_1 \alpha_0), s_{i-1})$, $i = 1, 2, \ldots, n-1$; $O(\delta_i(\alpha), s_i) = \delta_i(\beta)$, $i = n, n+1, \ldots$. Заметим что, как правило, термин «задержка» («задержка на n тактов») используется в более узком смысле (по сравнению, например, с [3]): 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* [2], определяется асинхронным автоматом с одиночной задержкой.

Динамическая система есть тройка $(\mathbb{S}, \mu, f)$, где S есть измеримое пространство с мерой μ, а $f \colon \mathbb{S} \to \mathbb{S}$ измеримая функция. Пространство $\mathbb{S}$ называют *фазовым пространством. Траекторией динамической системы* называется последовательность $x_0, x_1 = f(x_0), \ldots\ x_i = f(x_{i-1}) = f^i(x_0), \ldots$. Точка x_0 называется *начальной точкой* траектории. Отображение $F \colon \mathbb{S} \to \mathbb{S}$ 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 фазовом 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 $\mu_p(B_{p^{-k}}(a)) = p^{-k}$. Пусть F_k редукция f по модулю $p^{n \cdot (k-1)}$ на элементах кольца $\mathbb{Z}/p^{n \cdot k}\mathbb{Z}$ для $k = 2, 3, \ldots$.

Теорема. *Отображение $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ с задержкой n сохраняет меру тогда и только тогда, когда число $\#F_k^{-1}(x)$ F_k-прообразов*

точки $x \in \mathbb{Z}/p^{n\cdot(k-1)}\mathbb{Z}$ *равно* p^n, $k = 2, 3, \ldots$.

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 $\{x_0, x_1, \ldots, x_{r-1}\}$, где $x_j = f^j(x_0)$, $0 \le j \le r-1$. Такая орбита называется r-*циклом*. Пусть $\gamma(k)$ есть $r(k)$-цикл $\{x_0, x_1, \ldots, x_{r(k)-1}\}$, $k = 1, 2, 3, \ldots$, где $x_j = (f \mod p^{kn})^j(x_0)$, $0 \le j \le r(k)-1$.

Теорема. *Пусть отображение* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *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. Grigorchuk R. I, Nekrashevich V. V., Sushchanskii V. I. Automata, dynamical systems, and groups // Proc. Steklov Institute Math. — 2000. — 231. — P. 128–203.

3. Linz P.. An introduction to formal languages and automata. — Jones and Bartlett learning, 2011.

4. Тяпаев Л. Б. Геометрическая модель поведения автоматов и их неотличимость // Математика. Механика. — Изд-во Сар. ун-та, 1999. — С. 139–143.

5. 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. — 6 (1-2) — С. 121–133.

6. Тяпаев Л. Б. Геометрические образы автоматов и динамические системы// Материалы X Международного семинара "Дискретная математика и ее приложения". — М.: Изд-во мех.-мат. факультета МГУ, 2010. — С. 510–513.

7. Тяпаев Л. Б., Василенко Д. В. Дискретные динамические системы, определяемые геометрическими образами автоматов // Интеллектуальные системы. — 2013. — 17 (1-4). — С. 196–201.

О ДВУХ НОВЫХ РЕКУРСИВНЫХ КОНСТРУКЦИЯХ ПЛАТОВИДНЫХ УСТОЙЧИВЫХ БУЛЕВЫХ ФУНКЦИЙ

Е. В. Хинко (Москва)

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и регулярно поднимается в работах многих авторов. Например, в [1] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работе [2] построены соответствующие конструкции функций. В [3] Ю. В. Тарannиковым построены рекурсивные конструкции устойчивых булевых функций с высокой нелинейностью, где на каждом шаге рекурсии добавляется пара квазилинейных переменных. К относительно схожей теме в [4] также обращался К. В. Захаров, исследовавший рекурсивные конструкции бент-функций, которые можно считать подмножеством платовидных, с шагом числа переменных 2.

Задачу проделанной работы можно в общей формулировке поставить следующим образом: пусть имеются b, $b \in \mathbb{N}$, платовидных m-устойчивых булевых функций от n переменных $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, среди которых, возможно, есть совпадающие с точностью до взятия отрицания; добавим три переменные x_{n+1}, x_{n+2} и x_{n+3}. Новые функции от $n+3$ переменных обозначим $f_{n+3}^s(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, x_{n+3})$, $s = 1, \ldots, 8$.

Представляет интерес подбор соотношений индикаторов σ_{sj} и порождающих функций f_n^i, чтобы для полученных новых функций от $n+3$ переменных выполнялись следующие свойства:

а) сохранение свойства платовидности;

б) обеспечение роста устойчивости;

в) рекурсивное воспроизведение конструкции.

Связь между функциями от n и $n+3$ переменных можно схематично записать так:

$$f_{n+3}^s = \sigma_{s1} g_{s1} \ |\sigma_{s2} g_{s2} \ |\sigma_{s3} g_{s3} \ |\sigma_{s4} g_{s4} \ |\sigma_{s5} g_{s5} \ |\sigma_{s6} g_{s6} \ |\sigma_{s7} g_{s7} \ |\sigma_{s8} g_{s8},$$

где $g_{sj} = f_n^i$ или $g_{sj} = \overline{f_n^i}$; $s, j \in \{1, \ldots, 8\}$; $i \in \{1, \ldots, b\}$.

Введём обозначение

$$\sigma_{sj} g_{sj} = \begin{cases} f_n^i, \sigma_{sj} = 1, \\ \overline{f_n^i}, \sigma_{sj} = -1, \end{cases}$$

где $s = 1, \ldots, 8$. Здесь σ_{sj} выполняет роль индикатора: выбирается функция или её отрицание.

В [5] автором была построена конструкция с примерами начальных функций для случая $b = 4$, удовлетворяющая приведённым условиям, где порождающие функции $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, удовлетворяют следующим свойствам:
(К1) каждый двоичный набор $u \in V_n$ содержится в носителе спектра в точности нуля, двух или всех четырёх функций;
(К2) мощности всевозможных попарных пересечений носителей спектров порождающих функций f_n^i, $i = 1, \ldots, 4$, совпадают, а мощность пересечения носителей спектров всех четырёх функций равна четверти мощности носителя спектра каждой функции;
(К3) для каждого набора $u \in V_n$, содержащегося в носителе спектра всех четырёх функций f_n^i, $i = 1, \ldots, 4$, коэффициенты Уолша трёх функций одного знака, а четвёртой — другого знака.

Отличительной особенностью построенной в [5] конструкции, а также конструкций, построенных в данной работе, является то, что рассматривается случай порождающих функций с пересекающимися носителями спектра, в то время как в большинстве из построенных ранее конструкций порождающие функции обладали непересекающимися носителями спектра.

В настоящей работе представлены две новые конструкции, удовлетворяющие поставленной задаче.

Первая конструкция схожа с построенной в [5], в ней присутствуют такие же соотношения между функциями f_n^i, $i = 1, \ldots, 4$ и f_{n+3}^i, $i = 1, \ldots, 4$, что и в [5], однако (К2) выглядит иначе: "мощность пересечения носителей спектров всех четырёх функций f_n^i, $i = 1, \ldots, 4$, равна пяти восьмым мощности носителя спектра каждой функции". Таким образом показано, что вторая часть (К2) из [5] является достаточным, но не необходимым условием существования конструкции, удовлетворяющей поставленной задаче, для случая $b = 4$.

Вторая конструкция является примером выполнения поставленной задачи для случая $b = 2$.

В качестве индикаторов σ_{sj}, как и в конструкции для $b = 4$ из [5], берутся строки матрицы Адамара—Сильвестра порядка 8 (строки нумеруются с 1), только немного видоизменённые:
$f_{n+3}^1 : S^1 = (+-+-+--+)$ (то есть строка 2, с инвертированными символами 7-8 или строка 6 с инвертированными символами 5–6),
$f_{n+3}^2 : S^2 = (+--++-+-)$ (то есть строка 4, с инвертированными символами 7-8 или строка 8 с инвертированными символами 5–6).

Полученные функции также могут быть записаны следующим образом:
$f^1_{n+3}(\overrightarrow{x}, x_{n+1}, x_{n+2}, x_{n+3}) = f^1_n(\overrightarrow{x}) \cdot (x_{n+1}+1) + f^2_n(\overrightarrow{x}) \cdot x_{n+1} + x_{n+1} \cdot x_{n+2} + x_{n+3}$,
$f^2_{n+3}(\overrightarrow{x}, x_{n+1}, x_{n+2}, x_{n+3}) = f^1_n(\overrightarrow{x}) \cdot (x_{n+1}+1) + f^2_n(\overrightarrow{x}) \cdot x_{n+1} + x_{n+1} \cdot x_{n+2} + x_{n+2} + x_{n+3}$.

Список литературы

1. Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001. Proc. Lecture Notes in CS. — V. 2247. — P. 254–256.

2. Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics. — V. 6.

3. Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — 2002. — С. 91–148.

4. Захаров К. В. О порождении бент-функций рекурсивными конструкциями. — Дипломная работа, 2008.

5. Хинко Е. В. Об одной рекурсивной конструкции платовидных устойчивых булевых функций с шагом числа переменных 3 // ПДМ. — 2016. — № 1 (31). — С. 92–103.

ХЕШ-ФУНКЦИИ В БУЛЕВОМ КУБЕ

А. В. Чашкин (Москва)

Пусть $D \subseteq \{0,1\}^n$. Линейный оператор $f_a : \{0,1\}^n \to \{0,1\}^m$ назовем линейной a-хеш-функцией ранга m множества D, если у любого элемента из $f_a(D) = \{\boldsymbol{y} \in \{0,1\}^m \,|\, \boldsymbol{y} = f_a(\boldsymbol{x}),\ \boldsymbol{x} \in D\}$ в D существует не более a прообразов. Известно (см., например, [1]), что при $a = 1$ имеет место следующее утверждение.

Теорема 1. *Для любой области $D \subseteq \{0,1\}^n$, состоящей из не более чем $\sqrt{2^n}$ наборов, найдется линейная 1-хеш-функция, для числа компонент которой справедливо неравенство*

$$m \leq \lfloor 2 \log_2 |D| \rfloor - 1.$$

Покажем, что для бóльших значений параметра a справедлива аналогичная теорема.

Теорема 2. *Пусть D — M-элементное подмножество в $\{0,1\}^n$ и $a \leq M^{1/2} 2^{-5}$. Для D найдется линейная a-хеш-функция, для числа компонент которой справедливо неравенство*

$$m \leq \lfloor 2 \log_2 M - 2 \log_2 a \rfloor - 1.$$

Для доказательства теоремы 1 достаточно несколько раз подряд использовать тот простой факт, что линейный оператор $f : \{0,1\}^k \to \{0,1\}^{k-1}$ является линейной 1-хеш-функцией множества $D \subseteq \{0,1\}^k$ тогда и только тогда, когда его ядро не пересекается с множеством попарных сумм элементов из D. В основе доказательства теоремы 2 лежит аналогичный факт: *линейный оператор $f : \{0,1\}^k \to \{0,1\}^{k-2}$ является линейной 2-хеш-функцией множества $D \subseteq \{0,1\}^k$ тогда и только тогда, когда его ядро содержит не более одной из трех попарных сумм любых трех элементов из D.* Действительно, линейный оператор f отображает наборы $\boldsymbol{x}, \boldsymbol{y}$ и $\boldsymbol{z}$ в один и тот же набор только в том случае, когда попарные суммы этих наборов принадлежат ядру оператора, т. е. $f(\boldsymbol{x} \oplus \boldsymbol{y}) = f(\boldsymbol{x} \oplus \boldsymbol{z}) = f(\boldsymbol{y} \oplus \boldsymbol{z}) = 0$. При этом, если 2-мерное подпространство содержит две попарные суммы, например, $\boldsymbol{x} \oplus \boldsymbol{y}$ и $\boldsymbol{x} \oplus \boldsymbol{z}$, то это подпространство содержит и третью сумму, так как $\boldsymbol{y} \oplus \boldsymbol{z} = (\boldsymbol{x} \oplus \boldsymbol{y}) \oplus (\boldsymbol{x} \oplus \boldsymbol{z})$.

В доказываемой далее лемме используется простое обобщение указанного выше свойства линейного оператора быть 2-хеш-функцией множества.

Лемма 1. *Пусть D — M-элементное подмножество в $\{0,1\}^n$, f_a — a-хеш-функция ранга m множества D, и*

$$a^2 2^{2m-2} \geq 9M^3. \tag{1}$$

Тогда для D существует $2a$-хеш-функция ранга $m-2$.

Доказательство. Множество $f_a(D)$ разобъем на два подмножества A и B, первое из которых состоит из элементов, имеющих в D не менее $a/3$ прообразов, а второе из всех остальных. Очевидно, что $|A| \leq 3M/a$. Трехэлементное подмножество в $f_a(D)$ назовем

«плохим», если число прообразов его элементов больше $2a$. Легко видеть, что подмножество будет «плохим» только в том случае, когда не менее двух его элементов лежит в A. Поэтому число «плохих» подмножеств не больше чем

$$\binom{|A|}{2}|B| + \binom{|A|}{3} = \frac{|A|(|A|-1)}{2}|B| + \frac{|A|(|A|-1)(|A|-2)}{6} < \\ < \frac{|A|^2}{2}\Big(|B| + \frac{|A|}{3}\Big) < \frac{|A|^2 M}{2} \le \frac{9M^3}{2a^2}.$$

При $m \ge 5$ из предыдущего неравенства и неравенства (1) следует, что

$$\frac{(2^m-1)(2^m-2)}{6} > 2^{2m-3} \ge 9M^3/2a^2 > \binom{|A|}{2}|B| + \binom{|A|}{3},$$

т. е. число двумерных подпространств в $\{0,1\}^m$ больше числа «плохих» трехэлементных подмножеств в $f_a(D)$. Каждое трехэлементное подмножество $\{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}\}$ в $\{0,1\}^m$ однозначно определяет в $\{0,1\}^m$ единственное двумерное подпространство $\mathsf{H}_{\boldsymbol{xyz}} = \langle \boldsymbol{x}\oplus\boldsymbol{y}, \boldsymbol{x}\oplus\boldsymbol{z}\rangle$, которое содержит все три попарные суммы элементов этого множества. Поэтому в $\{0,1\}^m$ найдется 2-мерное подпространство H, которое не совпадает ни с одним из подпространств $\mathsf{H}_{\boldsymbol{xyz}}$, соответствующих «плохим» подмножествам. Следовательно, это подпространство H содержит не более одной из трех попарных сумм элементов из любого «плохого» подмножества в $f_a(D)$.

Пусть $f_{\mathsf{H}} : \{0,1\}^m \to \{0,1\}^{m-2}$ — линейный оператор с ядром H. Покажем, что композиция $f_{\mathsf{H}} \circ f_a$ будет $2a$-хеш-функцией множества D ранга $m-2$. Действительно, оператор f_{H} отображает в один и тот же набор не более четырех элементов множества $f_a(D)$. Если все эти элементы лежат в B, то число их прообразов в D не превосходит $4a/3$. Если один элемент лежит в A, а три — в B, то число их прообразов в D не превосходит $2a$. В остальных случаях среди этих элементов найдется не менее двух элементов из A, т. е. среди этих элементов можно выбрать три, которые будут образовывать «плохое» подмножество в $f_a(D)$, что, очевидно, невозможно, так как противоречит выбору оператора f_{H}. Таким образом, у рассматриваемых элементов общее число прообразов в D не больше $2a$. Лемма доказана.

Доказательство теоремы 2. Индукцией по k покажем, что если $k \le \lfloor \log_2 M^{1/2} \rfloor - 5$, то на множестве D существует 2^{k+1}-хеш-функция

$f_{2^{k+1}}$ ранга $m_k = \lfloor 2\log_2 M - 2(k+1)\rfloor - 1$. В основание индукции положим случай $k = 0$. В этом случае в силу теоремы 1 для множества D существует линейная 1-хеш-функция f_{2^0} с $m_0 = \lfloor 2\log_2 M\rfloor - 1$ компонентами. Допустим, что при $k \geq 0$ на D существует 2^k-хеш-функция f_{2^k} ранга $m_k = \lfloor 2\log_2 M - 2k\rfloor - 1$. Тогда из неравенства

$$2^{2k}2^{2m_k-2} = 2^{2k+2\lfloor 2\log_2 M-2k\rfloor-4} \geq 2^{4\log_2 M-2k-6} =$$
$$= M^4 2^{-2k-6} = M^4 2^{-2\lfloor \log_2 M^{1/2}\rfloor+4} > 16M^3$$

следует, что можно воспользоваться леммой 1. В силу этой леммы для множества D существует линейная 2^{k+1}-хеш-функция $f_{2^{k+1}}$ ранга $m_{k+1} = \lfloor 2\log_2 M - 2(k+1)\rfloor - 1$.

Пусть $2^k < a \leq 2^{k+1}$. Тогда линейный оператор $f_{2^{k+1}}$ будет на множестве D a-хеш-функцией ранга $m_{k+1} \leq \lfloor 2\log_2 M - 2\log_2 a\rfloor - 1$. Теорема доказана.

Работа выполнена при финансовой поддержке РФФИ, проект 14-01-00598.

Список литературы

1. Чашкин А. В. О линейных операторах, инъективных на произвольных подмножествах // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки, 156. — 2014. — Вып. 3. — С. 132–141.

РАСПРЕДЕЛЕНИЕ РАНГА КВАДРАТИЧНОЙ ФОРМЫ НАД ПОЛЕМ ИЗ ДВУХ ЭЛЕМЕНТОВ

А. В. Черемушкин (Москва)

Каждую квадратичную форму от n переменных ранга $2r$, $1 \leq r \leq \lfloor n/2\rfloor$, можно линейным преобразованием аргументов привести к виду $x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2r-1}x_{2r} \oplus l(x_1, \ldots, x_n)$, где l — некоторая линейная функция. Вероятность того, что квадратичная форма от n переменных имеет ранг $2r$, равна $p_{2r}(n) = Q_r(n)/2^{n(n-1)/2}$, где $Q_r(n)$ — число квадратичных форм от n переменных ранга $2r$. Из

описания групп автоморфизмов квадратичных форм [1 – 3] следует, что

$$Q_r(n) = \frac{(2^n-1)\dots(2^n-2^{2r-1})}{|\mathbf{Sp}(2r,2)|}, \tag{1}$$

где $|\mathbf{Sp}(2r,2)| = 2^{r^2}\prod\limits_{i=1}^{r}(2^{2i}-1)$. При $1 \le r \le n/2-1$ имеем

$$\frac{Q_r(n)}{Q_{r+1}(n)} = \frac{4}{(2^{n-2r}-1)(2^{n-2r-1}-1)}\left(1-\frac{1}{2^{2r+2}}\right). \tag{2}$$

Поэтому числа $Q_r(n)$, $1 \le r \le n/2-1$, образуют монотонно возрастающую последовательность.

Основным результатом является

Теорема. *Пусть $k = [n/2]$, $n = 2k+c$, $c = 0,1$, и последовательность ε_k выбрана так, что $\varepsilon_k\sqrt{\log_2 k} \to \infty$ при $k \to \infty$. Тогда при $n \to \infty$ доля квадратичных форм от n переменных ранга меньшего, чем $2k-2\left\lceil\sqrt{(\log_2 k)/2}+(\varepsilon_k+(-1)^c)/2\right\rceil$, стремится к нулю. Поэтому для ранга почти всех квадратичных форм q от n переменных при $n \to \infty$ справедлива оценка*

$$2k \ge r(q) \ge 2k-2\left\lceil\sqrt{\frac{1}{2}\log_2 k}+\frac{\varepsilon_k+(-1)^c}{2}\right\rceil+2.$$

Изучим теперь более подробно свойства распределения ранга. Сначала оценим вероятность максимальности ранга. Имеем

$$p_n(2k) = \begin{cases} \left(1-\frac{1}{2^{2k-1}}\right)\left(1-\frac{1}{2^{2k-3}}\right)\dots\left(1-\frac{1}{2}\right), & n=2k; \\ \left(1-\frac{1}{2^{2k+1}}\right)\left(1-\frac{1}{2^{2k-1}}\right)\dots\left(1-\frac{1}{2^3}\right), & n=2k+1. \end{cases}$$

В частности, $p_{2k-2}(2k-1) = 2p_{2k}(2k)$ при $k \ge 2$.

Верхнюю оценку вероятности $p_{2k}(2k)$ с наперед заданной точностью можно получить путём перемножения только части сомножителей, например, при $k > 14$

$$p_{2k}(2k) = \prod_{i=1}^{k}\left(1-\frac{1}{2^{2i-1}}\right) < \prod_{i=1}^{14}\left(1-\frac{1}{2^{2i-1}}\right) < 0{,}4194224428.$$

Нижнюю оценку вероятности $p_{2k}(2k)$ можно получить, используя подход из работы [4]:

$$\ln p_{2k}(2k) = \sum_{i=1}^{k} \ln\left(1 - \tfrac{1}{2^{2i-1}}\right) = -\sum_{i=1}^{k} \sum_{m=1} \tfrac{1}{m} \left(\tfrac{1}{2^{2i-1}}\right)^m =$$
$$= -\sum_{m=1} \tfrac{2^m}{m} \sum_{i=1}^{k} \left(\tfrac{1}{2^{2m}}\right)^i = -\sum_{m=1} \tfrac{2^{-m}}{m} \tfrac{1-1/(2^{2m})^k}{1-1/2^{2m}}.$$

При $k > s$ можно воспользоваться приближённой формулой

$$\ln p_{2k}(2k) > -\frac{2^{2m}}{2^{2m}-1} \ln 2 - \sum_{m=1}^{s-1} \tfrac{2^{-m}}{m} \left(\tfrac{1}{2^{2m}-1} - \tfrac{1}{2^{2r}-1}\right).$$

В частности, полагая $s = 8$, получаем, что при $k > 8$ имеет место нижняя оценка $p_{2k}(2k) > 0{,}41942244$. Поэтому при больших чётных $n = 2k > 28$

$$0{,}4194224428 > p_{2k}(2k) > 0{,}41942244.$$

При больших нечетных $n = 2k + 1 > 27$ получаем

$$0{,}8388448856 > p_{2k}(2k+1) = 2p_{2k+2}(2k+2) > 0{,}83884488.$$

Так как с уменьшением ранга вероятности $p_n(2r)$ быстро убывают, то для математического ожидания и дисперсии ранга случайной квадратичной формы от n переменных можно получить оценки с заданной точностью. Например, справедливо

Утверждение. *Пусть $k = \lfloor n/2 \rfloor$. При $n > 28$ для математического ожидания и дисперсии ранга $r(q)$ случайной квадратичной формы q от n переменных справедливы оценки:*

1) *при $n = 2k$ имеем*

$$\begin{aligned} 2k - 1{,}2014788 < {} & \mathrm{E}\, r(q) < 2k - 1{,}201478798\,(1 - 1/2^n), \\ 1{,}13053549\,(1 - 1/2^n) < {} & \mathrm{D}\, r(q) < 1{,}13053551; \end{aligned}$$

2) *при $n = 2k + 1$ имеем*

$$\begin{aligned} 2k - 0{,}324311085 < {} & \mathrm{E}\, r(q) < 2k - 0{,}324311084\,(1 - 1/2^n), \\ 0{,}554431153\,(1 - 1/2^n) < {} & \mathrm{D}\, r(q) < 0{,}554431159. \end{aligned}$$

Как следствие получаются оценки уровня аффинности двоичных функций степени нелинейности не выше двух. Уровень аффинности la(f) двоичной функции f определяется как минимальное число переменных, произвольная фиксация значений которых делает функцию аффинной. В терминах теории графов это соответствует вершинному покрытию графа, ассоциированного с квадратичной формой. Обобщенный уровень аффинности $\mathcal{L}a(f)$ двоичной функции f определяется как минимальное число линейных комбинаций переменных, некоторая фиксация значений которых делает функцию аффинной, $\mathcal{L}a(f) \leq$ la(f).

Поскольку обобщенный уровень аффинности квадратичной формы ранга $2r$ равен r, то из приведенных выше асимптотических оценок ранга непосредственно вытекают оценки обобщенного уровня аффинности для почти всех квадратичных функций, а также нижняя оценка вершинного покрытия для почти всех неориентированных графов. В частности, можно заметить, что оценки уровня аффинности почти всех квадратичных форм из [5] не являются точными.

Список литературы

1. Dixon L. E. Linear groups with an expositions to the Galois field theory. — Leipzig: Publ. by B. G. Teubner, 1901.

2. Дьедонне Ж. Геометрия классических групп. — М.: Мир, 1974.

3. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

4. Рязанов Б. В., Чечета С. И. О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. — 1995. — Т. 7, вып. 3. — С. 129–145.

5. Буряков М. Л. Асимптотические оценки уровня аффинности для почти всех булевых функций // Дискретная математика. — 2008. — Т. 20, вып. 3. — С. 73–79.

СПИСОК ПЛЕНАРНЫХ ДОКЛАДОВ, ПРОЧИТАННЫХ НА СЕМИНАРЕ

В. В. Кочергин (Москва) *Об одной задаче О. Б. Лупанова*

М. П. Минеев, В. Н. Чубариков (Москва) *Криптография и p-адический анализ*

А. М. Зубков, А. А. Серов (Москва) *Итерации случайных отображений конечных множеств*

Л. А. Шоломов (Москва) *Две постановки задачи кодирования недоопределенных данных*

С. А. Ложкин, В. А. Коноводов (Москва) *Синтез схем и формул из элементов с прямыми и итеративными входами*

Ф. М. Аблаев, М. Ф. Аблаев (Казань) *Квантовое криптографическое хеширование*

В. Б. Кудрявцев (Москва) *О кафедре МаТИС*

С. Н. Селезнёва (Москва) *Сложность полиномиальных представлений функций k-значной логики*

А. В. Тимофеенко (Красноярск) *К теории выпуклых многогранников с правильными и сложенными из правильных многоугольников гранями*

А. А. Часовских (Москва) *Условия выразимости и полноты в классах линейных автоматов*

И. П. Чухров (Москва) *Задача минимизации булевых функций: условия минимальности и вероятностный метод*

Ф. И. Соловьёва (Новосибирск) *О пропелинейных, транзитивных и гомогенных кодах*

Д. С. Кротов (Новосибирск) *Трейды в комбинаторных конфигурациях*

Д. Г. Мещанинов (Москва) *Семейства замкнутых классов в P_k, определяемых полиномиальными и аддитивными представлениями функций*

Р. М. Колпаков (Москва) *Об оценке числа и эффективном поиске повторов и палиндромов с разрывами в формальных словах*

С О Д Е Р Ж А Н И Е

Пленарные доклады

Секция «Синтез, сложность и надежность управляющих систем»

Секция «Функциональные системы»

Секция «Комбинаторный анализ»

Секция «Теория графов»

Секция «Математическая теория интеллектуальных систем»

Секция «Дискретная геометрия»

Секция «Теория кодирования и математические вопросы теории защиты информации»