ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ VIII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 24–29 октября 2011 г.)

Часть II

Москва 2011

МАТЕРИАЛЫ
VIII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 24–29 октября 2011 г.)

Часть II

Москва 2011

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 11–01–06838

М34 Материалы VIII молодежной научной школы по дискретной математике и ее приложениям (Москва, 24–29 октября 2011 г.). Часть II. Под редакцией А. В. Чашкина. 2011. — 56 с.

Сборник содержит материалы VIII молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 24 по 29 октября 2011 г. при поддержке Российского фонда фундаментальных исследований (проект 11–01–06838). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
VIII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ
И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 24–29 октября 2011 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *О. С. Дудакова*

СОДЕРЖАНИЕ

О МНОЖЕСТВЕ ВСЕХ ОПТИМАЛЬНЫХ АЛГОРИТМОВ ДЛЯ ОДНОГО КЛАССА БИЛИНЕЙНЫХ ОТОБРАЖЕНИЙ

В. В. Лысиков (Москва)

Введение

Пусть F — некоторое поле, а K — его квадратичное расширение. В данной работе рассматривается многообразие оптимальных билинейных алгоритмов для умножения элемента K на вектор из пространства K^n или, что то же самое, для матричного умножения формата $\langle 1,1,n\rangle_K$, рассматриваемого над базовым полем F.

1. Билинейные алгоритмы и тензоры

Пусть U, V, W — конечномерные линейные пространства над некоторым базовым полем F, $\varphi\colon U\times V\to W$ — билинейное отображение.

Определение 1. *Билинейным алгоритмом* сложности r, вычисляющим φ, называется набор r троек (f_k, g_k, w_k), $f_k\in U^*, g_k\in V^*, w_k\in W$ такой, что

$$\varphi(u,v)=\sum_{k=1}^{r} f_k(u)g_k(v)w_k \quad \text{для любых } u\in U, v\in V. \tag{1}$$

Билинейной сложностью или *рангом* отображения φ называется наименьшая возможная сложность вычисляющего его билинейного алгоритма, а те алгоритмы, на которых эта сложность достигается, называются *оптимальными*.

Если рассмотреть отображение φ как тензор из $U^*\otimes V^*\otimes W$, то билинейным алгоритмам соответствуют представления этого тензора в виде суммы разложимых тензоров $f_i\otimes g_i\otimes w_i$, а билинейная сложность оказывается равной рангу тензора, как он определяется в алгебре.

2. Эквивалентные алгоритмы

При действии невырожденных линейных преобразований на компоненты тензора его ранг остается неизменным. Особым является случай, когда при этом остается неизменным и сам тензор. Это позволяет получать из одного билинейного алгоритма другие алгоритмы вычисления того же отображения.

Определение 2. На тензорном произведении $\bigotimes_{i=1}^{n} V_i$ естественным образом действует группа $\Gamma^\circ=\prod_{i=1}^{n}\mathrm{GL}(V_i)$. Множество всех отображений $\Phi\in\Gamma^\circ$ таких, что $\Phi(t)=t$, образует подгруппу $\Gamma^\circ(t)$, которая называется *(малой) группой изотропии* тензора t.

Для билинейных преобразований стабилизирующие преобразования удобно искать в виде $\Phi = F^* \otimes G^* \otimes H^{-1}$.

$$\Phi \in \Gamma^\circ(\varphi) \Leftrightarrow \varphi(F(u), G(v)) = H(\varphi(u, v)) \quad \text{для любых } u \in U, v \in V. \tag{2}$$

Определение 3. Два билинейных алгоритма, вычисляющие отображение φ, называются эквивалентными, если они получаются друг из друга действием отображений из группы $\Gamma^\circ(\varphi)$ и перестановкой слагаемых.

3. Группа изотропии модуля

Векторное пространство K^n над расширением K базового поля F является частным случаем модуля над F-алгеброй. В этом разделе описывается структура группы изотропии умножения в некотором модуле M над ассоциативной F-алгеброй A с единицей (в дальнейшем рассматриваются только такие алгебры). В доказательстве используются некоторые определения и факты из алгебры, которые можно найти в [4].

Определение 4. Пусть ${}_AM$ — модуль, σ — автоморфизм алгебры A. Линейный оператор $G\colon M \to M$ будем называть σ-псевдоавтоморфизмом модуля M, если $G(am) = \sigma(a) \cdot Gm$ для любых элементов $a \in A, m \in M$. Множество всех σ-псевдоавтоморфизмов будем обозначать $\mathrm{Aut}_A^\sigma M$.

Теорема 1. *Пусть A — конечномерная алгебра, ${}_AM$ — конечно порожденный точный модуль. Группа изотропии $\Gamma^\circ(M)$ модуля M состоит в точности из отображений вида*

$$F^* \otimes G^* \otimes H^{-1}, \tag{3}$$

где $Fx = a\sigma(x)$, $G \in \mathrm{Aut}_A^\sigma M$ и $Hm = a \cdot Gm$ для некоторых $a \in A^\times$ и $\sigma \in \mathrm{Aut}\, A$ и произвольных $x \in A$, $m \in M$.

Доказательство. Легко видеть, что все такие преобразования действительно являются стабилизирующими. Докажем, что для любого стабилизирующего преобразования F, G и H имеют указанный вид.

Пусть $F^* \otimes G^* \otimes H^{-1} \in \Gamma^\circ(M)$. Тогда, согласно (2),

$$Fx \cdot Gm = H(xm) \text{ для всех } x \in A, m \in M \tag{4}$$

Обозначим $a = F(1)$. Тогда

$$Hm = a \cdot Gm \tag{5}$$

Так как G и H — невырожденные линейные операторы, то $M = aM$, т. е. оператор умножения на a невырожден, и, следовательно, a обратим (здесь используется предположение о точности модуля M и то, что M есть конечномерное пространство над F).

Рассмотрим теперь отображение $\sigma(x) = a^{-1} \cdot Gx$.

$$Fx \cdot Gm = H(xm) = a \cdot G(xm) \Rightarrow G(xm) = \sigma(x) \cdot Gm. \tag{6}$$

Отсюда следует, что

$$\sigma(xy) \cdot Gm = G(xym) = \sigma(x)\sigma(y) \cdot Gm. \tag{7}$$

Так как M — точный модуль, m произвольно, а G невырожден, это значит, что

$$\sigma(xy) = \sigma(x)\sigma(y). \tag{8}$$

В силу произвольности x и y получаем, что σ — автоморфизм A.

В итоге получили, что $Fx = a\sigma(x)$, где a — обратимый элемент, а σ — автоморфизм A. Равенство в правой части (6) означает, что G есть σ-псевдоавтоморфизм M.

Следствие 1. *Группа изотропии умножения* mult: $K \times K^n \to K$, *где* K — *квадратичное расширение базового поля* F, *порождается отображениями* $L_a^* \otimes \mathrm{id} \otimes T_a^{-1}$, $\mathrm{id} \otimes G^* \otimes G^{-1}$, $\sigma^* \otimes \Sigma^* \otimes \Sigma$, *где* id — *тождественный оператор,* $a \in K^\times$, $L_a x = ax$, $T_a m = am$, G — *произвольный* K-*линейный оператор на* K^n, σ — *единственный нетривиальный автоморфизм* K, Σ — *оператор применения* σ *ко всем координатам вектора из* K^n.

4. Структура оптимальных алгоритмов для $\langle 1, 1, n\rangle_K$

Известно [3], что ранг умножения mult: $K \times K^n \to K^n$, где K — расширение степени d, равен $(2d-1)n$, что для случая квадратичного расширения дает $3n$.

Введем на K и на K^n (рассматриваемых как линейные пространства над F) внутреннее произведение, которое зададим формулами $(x, y) = f(xy)$ и $(x, y) = f(\sum x_i y_i)$ соответственно, где f — произвольный ненулевой линейный функционал из K^*. Это внутреннее произведение индуцирует изоморфизм Z: $x \mapsto (x, -)$, при котором K-линейные операторы на K^n соответствуют операторам вида G^* на $(K^n)^*$, где G — K-линейный оператор. Действительно,

$$(G^*(Zx))y = (Zx)(Gy) = (x, Zy) = (G^T x, y) = (Z(G^T x))y. \tag{9}$$

Определим некоторые понятия, являющиеся «переводом» введенных де Гроотом в [2] инструментов на бескоординатный язык тензоров.

Определение 5. *Слоем* тензора $t \in X \otimes W$, соответствующим линейному функционалу $h \in W^*$ будем называть элемент $h \circ t \in X$, полученный из t с помощью линейного преобразования, переводящего $x \otimes w$ в $h(w)x$. Множество всех слоев тензора t образует линейное подпространство в X, которое мы будем обозначать $\mathcal{L}(t)$

Утверждение 1 [1]. *В оптимальном билинейном алгоритме*

$$\varphi = \sum_{i=1}^{r} f_i \otimes g_i \otimes w_i$$

билинейные формы (произведения алгоритма) $f_i \otimes g_i$ линейно независимы, а набор w_i однозначно определяется по набору произведений.

Определение 6. Будем говорить, что алгоритм $\varphi = \sum_{i=1}^{r} f_i \otimes g_i \otimes w_i$ *порождается* семейством билинейных форм $\{p_j\}, 1 \leqslant j \leqslant s$, если все произведения $f_i \otimes g_i$ принадлежат линейной оболочке $\langle p_1, p_2, \ldots, p_s \rangle + \mathcal{L}(\varphi)$.

Утверждение 2 [1]. *Пусть $\varphi\colon U \times V \to W$ — билинейное отображение, $\varphi(U,V) = W$, $\operatorname{rk}\varphi = r$, $\dim W = p$. Тогда оптимальный билинейный алгоритм*

$$\varphi = \sum_{i=1}^{r} f_i \otimes g_i \otimes w_i, \quad \varphi \in U^* \otimes V^* \otimes W$$

порождается некоторыми $r - p$ своими произведениями $f_i \otimes g_i$.

Докажем основную лемму, характеризующую наборы произведений, порождающие алгоритмы для $\langle 1, 1, n \rangle_K$.

Лемма 1. *Пусть K — квадратичное расширение базового поля F. Если произведения $f_i \otimes g_i$, $1 \leqslant i \leqslant n$, порождают билинейный алгоритм умножения элементов K на векторы из K^n, то $Z^{-1}g_i$ линейно независимы над K.*

Доказательство. От противного. Пусть g_i линейно зависимы и линейная оболочка $L = \sum KZ^{-1}g_i \subsetneq K^n$. Пусть $X = \{x | (x,y) = 0 \ \forall y \in L\}$. Если произведения $f_i \otimes g_i$ порождают алгоритм умножения в ${}_K K^n$, то ограничения $f_i \otimes g_i|_X$ порождают алгоритм умножения в пространстве ${}_K X$, так как

$$ax = \sum_{k=1}^{r} f_k(a) g_k(x) w_k = \sum_{k=1}^{r} f_k(a) g_k|_X(x) w'_k, \quad w'_k = P w_k, \tag{10}$$

где P — некоторая проекция с K^n на X.

Так как по построению $g_i(x) = (Z^{-1}g_i, x) = 0$ для $x \in X$, получаем, что все произведения этого алгоритма должны лежать в $\mathcal{L}(\operatorname{mult}|_{K \times X})$. Однако это пространство не содержит никаких форм ранга 1, кроме 0, так как если $f \otimes g = h \circ \operatorname{mult}|_{K \times X}$, $a \in \ker f$, $a \neq 0$ то $h(aX) = 0$, т. е. $aX \neq X$, что противоречит условию $a \neq 0$.

Следствие 2. *Если произведения $f_i \otimes g_i$ порождают билинейный алгоритм умножения* $\operatorname{mult}\colon K \times K^n \to K^n$, *то существует эквивалентный ему алгоритм, в котором эти произведения переходят в $Zc_i \otimes Z(c_i e_i)$, где $c_i \in K$, e_i — i-й базисный вектор K^n.*

Теорема 2. *Любой оптимальный алгоритм вычисления $\langle 1, 1, n \rangle$ эквивалентен алгоритму вида*

$$\operatorname{mult} = \sum_{i=1}^{3n} Zc_i \otimes Z(c_i s_i) \otimes w_i, \tag{11}$$

где $c_i \in K$, $s_i = \sum k_{ij} e_j$, $k_{ij} \in F$.

Доказательство. Оптимальный алгоритм для mult порождается некоторыми n своими произведениями. По предыдущей лемме, существует эквивалентный алгоритм, в котором эти произведения имеют вид $p_i = Zc_i \otimes Z(c_i e_i)$. Заметим, что эти произведения, так же, как и само отображение mult, обладают свойством $p_i(x, ys) = p_i(y, xs)$, где $x, y \in K$, $s \in \langle e_1, \ldots, e_n \rangle_F$. Следовательно, остальные произведения также обладают этим свойством, как лежащие в линейной оболочке $\langle p_1, \ldots, p_n \rangle + \mathcal{L}(\mathrm{mult})$, а из форм ранга 1 этим свойством обладают только формы вида $f \otimes g = Zc \otimes Z(cs)$, где $c \in K$, $s \in \langle e_1, \ldots, e_n \rangle_F$, то есть те, матрица которых состоит из n симметричных клеток размера 2×2.

Список литературы

1. H. F. de Groote. Lectures on the Complexity of Bilinear Problems. — Springer, 1987.
2. H. F. de Groote. On Varieties of Optimal Algorithms for the Computation of Bilinear Mappings I-III // Theor. Comp. Sci — 1978. — Vol. 7. — С. 1–24, 127–148, 239–249.
3. L. Auslander, S. Winograd. The multiplicative complexity of certain semilinear systems defined by polynomials // Advances in Applied Mathematics. — 1980. — Vol. 1, no. 3. — С. 257–299.
4. Дрозд Ю. А., Кириченко В. В. Конечномерные алгебры. — Киев: Вища школа, 1980.

О ВЛИЯНИИ НЕКОТОРЫХ ЧИСЛОВЫХ ХАРАКТЕРИСТИК ГРАФОВ НА СЛОЖНОСТЬ ОПРЕДЕЛЕНИЯ ЧИСЛА НЕЗАВИСИМОСТИ

Д. С. Малышев (Нижний Новгород)

Введение

Работа посвящена алгебраическому подходу к формированию границы полиномиальной разрешимости задачи о независимом множестве (далее, кратко, задачи НМ). Напомним, что *задача о независимом множестве* для заданного графа состоит в том, чтобы определить его *число независимости* — наибольшее количество попарно несмежных вершин. Суть подхода состоит в выборе какого-нибудь числового параметра графов и определении тех «максимальных» значений данного параметра, при которых задача еще остается эффективно решаемой. Известны многочисленные примеры успешного применения такого подхода — определения соответствующего порога. Например, задача НМ полиномиально разрешима для графов со степенями вершин не более чем 2, но остается NP-полной во множестве графов со степенями вершин не более чем 3. Вместе с тем, во всех известных автору результатах

«граница» оказывается не зависящей от количества вершин в графе (т. е. константой). Однако, хотелось бы выявить «пороги» и в тех случаях, когда они константами являться не будут. При этом, разумеется, речь будет идти уже о функциональной, а не числовой, постановке проблемы.

В этой публикации рассматриваются две характеристики графов — количество ребер и упаковочное число. Изучаются «предельные» ограничения на рост этих характеристик (как функций от количества вершин), при которых задача НМ для получаемого множества графов еще остается полиномиально разрешимой.

1. Влияние количества ребер в связных графах на трудоемкость решения задачи НМ

В работе [1] рассматривались специальные подмножества множества всех графов. Каждая такая совокупность (обозначаемая через $\mathcal{G}_{f(n)}$) задавалась монотонной функцией $f(n) : \mathbb{N} \to \mathbb{N}$ и определялась как множество графов из $\bigcup\limits_{n=1}^{\infty} \{G : G - \text{связный}, |V(G)| = n, |E(G)| \leq f(n)\}$. Таким образом, функция $f(n)$ ограничивает сверху рост количества ребер в графах. В той же работе [1] была поставлена задача об отыскании такой функции $f^{'}(n)$, что при любом $\epsilon > 0$ задача НМ полиномиально разрешима в классе $\mathcal{G}_{[(1-\epsilon)f^{'}(n)]}$ и NP-полна в классе $\mathcal{G}_{[(1+\epsilon)f^{'}(n)]}$. Иными словами, была поставлена задача об отыскании асимптотической границы на рост количества ребер в графах из рассматриваемого семейства классов, где задача НМ еще остается полиномиально разрешимой. Соответствующий разделитель был найден в [1] и было показано, что можно положить $f^{'}(n) = n$.

Следующим шагом исследований является «ничейная земля» результата из [1], т. е. изучение тех функций $f(n)$, которые при $n \to \infty$ эквивалентны n. Целью исследований является получение информации о росте второго члена разделителя полиномиальных и неполиномиальных случаев. По-видимому, здесь асимптотическая постановка неуместна, поскольку, вероятно, если задача НМ является полиномиально разрешимой в классе $\mathcal{G}_{n+g(n)}$ $(g(n) \in o(n))$, то для любого $k \in \mathbb{N}$ задача НМ остается таковой для графов из $\mathcal{G}_{n+kg(n)}$. Значит, когда $f(n) \sim n$ при $n \to \infty$, то имеет смысл рассматривать асимптотическую постановку для какой-нибудь функции (корня, двоичного логарифма и т. п.) от $f(n) - n$. Однако и здесь не удается получить сколь-нибудь значительного продвижения (не удается даже поставить соответствующую «разумную» задачу). Все же, некоторую информацию о втором члене можно почерпнуть из теорем 1 и 2.

Теорема 1 [2]. *При любом натуральном C задача НМ полиномиально разрешима для графов из $\mathcal{G}_{n+C[\log_2(n)]}$.*

Интерпретации следующих результатов подразумевают отсутствие субэкспоненциальных алгоритмов для решения задачи НМ (напомним, что алгоритм решения этой задачи называется *субэкпоненциальным*, если время его работы ограничено величиной $2^{o(n)}$, где n — количество вершин в графе). Вера

в отсутствие таких алгоритмов для задачи НМ является широко распространенной [3–5] и автор настоящей публикации разделяет ее. Формулировка теоремы 2 использует понятие *нелогарифмической функции* $g(n) : \mathbb{N} \to \mathbb{N}$, т. е. неограниченной неубывающей функции, экспонента которой растет быстрее, чем полином от n.

Теорема 2 [2]. *Если задача НМ не разрешима за субэкпоненциальное время, то для любой нелогарифмической функции $g(n)$ эта задача не решаема за полиномиальное время для графов класса $\mathcal{G}_{n+\frac{g^2(n)}{2}}$.*

Результаты теоремы 2 можно несколько усилить. Для получения этого усиления необходимо доказать справедливость следующего утверждения.

Лемма 1. *Если задача НМ не разрешима за субэкпоненциальное время, то для любой при $n \to \infty$ функции $\phi(n) \to \infty$ эта задача не решаема за субэкспоненциальное время для графов из класса $\mathcal{G}_{\frac{n^2-\frac{n^2}{\phi^2(n)}}{2}}$.*

Доказательство. Очевидно, что для графа с n вершинами факт существования независимого множества мощности k проверяется за время $O(n^{O(1)}C_n^k)$. Покажем, что если число независимости этого графа не превосходит $\frac{n}{\phi(n)}$, то оно вычисляется за субэкспоненциальное время. Действительно, ввиду энтропийной оценки для биномиальных коэффициентов ($C_n^k \le 2^{nH(\frac{k}{n})}$ при $k \le \frac{n}{2}$, где $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$), имеем, что при $\phi(n) \ge 2$ справедливо неравенство $C_n^{\frac{n}{\phi(n)}} \le 2^{nH(\frac{1}{\phi(n)})}$. Легко проверить, что $H(\frac{1}{\phi(n)}) \in O(\frac{\log(\phi(n))}{\phi(n)})$. Отсюда и из замечания из первого предложения доказательства следует, что для графов с обозначенным ростом числа независимости имеет место субэкспоненциальная разрешимость задачи НМ. Значит, такие алгоритмы могут отсутствовать только в множестве графов, число независимости каждого n-вершинного представителя которых не меньше, чем $\frac{n}{\phi(n)}$. Легко проверить, что количество ребер в любом таком графе не превосходит $\frac{n^2-\frac{n^2}{\phi^2(n)}}{2}$. Лемма 1 доказана.

Имея оценку из леммы 1 и применяя сведение из работы [2] можно довольно легко доказать справедливость теоремы 3.

Теорема 3. *Если задача НМ не разрешима за субэкпоненциальное время, то для любой нелогарифмической функции $g(n)$ эта задача не решаема за полиномиальное время для графов класса $\mathcal{G}_{n+\frac{g^2(n)(1-\frac{1}{\phi^2(g(n))})}{2}}$.*

2. Влияние упаковочного числа графов на трудоемкость решения задачи НМ

H-Упаковочное число графа G — наибольшее k, при котором G содержит k непересекающихся по вершинам подграфов, каждый из которых изоморфен H. Это число обозначается через $p_H(G)$. Например, если $H = K_1$, то

$p_H(G) = |V(G)|$, а если $H = K_2$, то $p_H(G)$ — размер наибольшего паросочетания графа G. В этом разделе работы изучается сложность задачи НМ для классов графов вида $\mathcal{G}^H_{f(n)} = \{G : p_H(G) \leq f(|V(G)|)\}$ в зависимости от выбора графа H и функции $f(n) : \mathbb{N} \to \mathbb{N}$. Отметим, что для многих графов H выбор функции $f(n)$ никак не влияет на сложность задачи НМ. Действительно, если H не принадлежит определенному классу графов, то, согласно теореме 1 из работы [6], задача НМ является NP-полной в классе $\{G : p_H(G) = 0\}$. Речь идет о классе $\mathcal{T}$, состоящем из всевозможных графов, каждая компонента связности которых является деревом с не более чем тремя листьями. С другой стороны, если H — пустой граф с s вершинами, то $p_H(G) = [\frac{|V(G)|}{s}]$. Легко проверить, что в этом случае $\mathcal{G}^H_{f(n)}$ состоит из всех графов, количество вершин которых принадлежит подмножеству $\tilde{\mathbb{N}}$ множества $\mathbb{N}$, определяемому монотонной функцией $f(n)$. Тем самым принадлежность $G \in \mathcal{G}^H_{f(n)}$ определяется только принадлежностью числа $|V(G)|$ множеству $\tilde{\mathbb{N}}$, а не структурой графа G (и распознавание этой принадлежности выполняется за единичное время). Поэтому далее случай пустого графа H не рассматривается. Таким образом, задачу поиска «границы» целесообразно рассматривать только для непустых графов H из класса $\mathcal{T}$. Полная классификация случаев полиномиальной разрешимости задачи НМ для рассматриваемой совокупности классов графов содержится в следующем утверждении.

Теорема 4 [7]. *Если задача НМ не разрешима за субэкпоненциальное время, то для любого непустого графа $H \in \mathcal{T}$ и любой функции $f(n) : \mathbb{N} \to \mathbb{N}$ задача о независимом множестве является полиномиально разрешимой в классе графов $\mathcal{G}^H_{f(n)}$ тогда и только тогда, когда $f(n) \in O(\log(n))$.*

По-видимому, попытки обобщения рассматриваемой проблемы на порожденные подграфы H (и поиска «разделяющей» функции) будут безрезультатными уже для $H = K_1$. Действительно, в этом случае соответствующим параметром графа G будет число независимости $\alpha(G)$. Для выявления «разделяющей» функции, видимо, возникнет необходимость разрабатывать алгоритмы с параметризованной оценкой трудоемкости $O(g(\alpha(G))n^C)$, где $g(n)$ — некоторая функция, а C — некоторая константа. Однако, существование таких алгоритмов маловероятно [8]. Именно поэтому все внимание сосредоточено на параметре $p_H(G)$.

Список литературы

1. Малышев Д. С. Совместное влияние количества ребер и компонент связности в графах на сложность вычисления числа независимости // Материалы Российской конференции «Дискретная оптимизация и исследование операций» (Республика Алтай, 2010 г.), С. 136.
2. Малышев Д. С. Анализ влияния числа ребер в связных графах на трудоемкость решения задачи о независимом множестве // Дискретный анализ и исследование операций. — 2011. — Т. 18, вып. 3. — С. 83–87.

3. Impagliazzo R., Paturi R. Which problems have strongly exponentional complexity? // Journal of Computer and System Sciences. — 2001. — V. 62. — P. 512–530.
4. Chen J., Huang X., Kanj I., Xia G. Strong computational lower bounds via parameterized complexity // Journal of Computer and System Sciences. — 2006. — V. 72. — C. 1346–1367.
5. Dantsin E., Wolpert A. On moderately exponential time for SAT // Lecture Notes in Computer Science. — 2010. — V. 6175. — P. 313–325.
6. Коробицын Д. В. О сложности задач на наследственных классах графов // Дискретная математика. — 1992. — Т. 4, вып. 4, — С. 34–40.
7. Малышев Д. С. Влияние роста упаковочного числа графов на сложность задачи о независимом множестве // Дискретная математика (направлено в журнал).
8. Downey R., Fellows M. Parameterized complexity. — New York: Springer-Verlag, 1999.

ОБ ОДНОМ КЛАССЕ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ С ЭКСПОНЕНЦИАЛЬНЫМ РОСТОМ РАНГОВОЙ ФУНКЦИИ

Е. В. Михайлец (Москва)

Рассмотрим произвольную систему A функций k-значной логики P_k. *Системой неявных уравнений* над системой функций A будем называть всякую систему уравнений вида:

$$\begin{cases} \varphi_1(x_1, \ldots, x_n, y) = \psi_1(x_1, \ldots, x_n, y), \\ \ldots \\ \varphi_m(x_1, \ldots, x_n, y) = \psi_m(x_1, \ldots, x_n, y), \end{cases} \tag{1}$$

где функции φ_i, ψ_i, $i = 1, \ldots, m$, представляют собой суперпозиции над системой функций A либо тождественные функции.

Будем говорить, что система неявных уравнений вида (1) *реализует* функцию $f(x_1, \ldots, x_n)$ k-значной логики, если при любых фиксированных значениях переменных $x_1, \ldots, x_n$ она имеет единственное решение $y = f(x_1, \ldots, x_n)$. Всякую систему неявных уравнений над системой функций A, реализующую функцию $f(x_1, \ldots, x_n)$, будем называть *неявным представлением* функции f над A. Функцию $f(x_1, \ldots, x_n)$ в P_k будем называть *неявно выразимой* над системой функций A, если существует хотя бы одно неявное представление f над A.

Множество всех функций из P_k, неявно выразимых над системой функций A, будем называть *неявным расширением* системы A и будем обозначать через $I(A)$. Непосредственно из определения неявного представления вытекает равенство $I(A) = I([A])$, благодаря которому при изучении поведения

ранговых функций можно ограничиться исследованием только замкнутых по суперпозиции классов функций k-значной логики.

Если функция $f(x_1, \ldots, x_n)$ принадлежит замыканию системы функций A, $f \in [A]$, для нее существует неявное представление над системой A, состоящее из единственного уравнения $y = f(x_1, \ldots, x_n)$. Следовательно, для любой системы функций A в P_k выполняется соотношение $[A] \subseteq I(A)$. Таким образом, понятие неявной выразимости можно считать одним из обобщений понятия выразимости функций суперпозициями и, соответственно, неявное расширение — обобщением операции замыкания по суперпозиции.

Если все функции k-значной логики неявно выразимы над системой функций A, т. е. $I(A) = P_k$, то систему функций A будем называть *неявно полной* в P_k.

Понятие неявной выразимости впервые было введено А. В. Кузнецовым [3]. Впоследствии исследования в этой области продолжил О. М. Касим-Заде. В работе [1] О. М. Касим-Заде полностью решил проблему неявной выразимости и неявной полноты в двузначной логике P_2. В частности, в работе [1] показано, что в двузначной логике P_2 существует один замкнутый по суперпозиции минимальный неявно полный класс — класс всех монотонных функций. Отсюда вытекает следующий критерий неявной полноты в P_2: произвольная система булевых функций неявно полна в P_2 тогда и только тогда, когда ее замыкание по суперпозиции содержит класс всех монотонных функций.

В трехзначной логике P_3 критерий неявной полноты в терминах минимальных неявно полных классов получен Е. А. Ореховой. Она доказала, что в P_3 существует двадцать семь различных минимальных неявно полных замкнутых классов функций и привела описание всех двадцати семи классов (см. [6]).

Решив проблему неявной выразимости в P_2, О. М. Касим-Заде поставил вопрос о сложности неявных представлений. В работе [2] он рассмотрел наиболее естественную меру сложности — число уравнений в неявном представлении, назвав эту величину *рангом представления*.

Пусть f — произвольная функция из неявного расширения заданной системы A функций k-значной логики, $f \in I(A)$. Следуя [2], назовем *рангом* функции f над системой функций A и будем обозначать через $m_A(f)$ наименьшее число уравнений, достаточное для построения неявного представления f над A.

Будем называть *ранговой функцией* системы функций A функцию Шеннона $m_A(n) = \max m_A(f)$, где максимум берется по всем функциям k-значной логики, принадлежащим неявному расширению системы A и существенно зависящим не более чем от n переменных.

О. М. Касим-Заде в работе [2] получил оценки роста ранговой функции для всех замкнутых классов булевых функций. В частности, для класса M всех монотонных функций, являющегося единственным замкнутым минимальным неявно полным классом в P_2, ранговая функция равна $m_M(n) = \lceil (n+2)/2 \rceil$.

Автором были получены оценки роста ранговой функции для всех минимальных неявно полных классов в P_3. Двадцать семь замкнутых мини-

мальных неявно полных классов трехзначной логики, описанных Е. А. Ореховой (см. [6]), по отношению двойственности делятся на шесть классов эквивалентности. Ранговые функции двойственных систем функций совпадают. Таким образом, ранговая функция любой минимальной неявно полной системы функций в P_3 совпадает с ранговой функцией одного из шести классов функций W_1, W_2, W_3, W_4, W_5, W_6, принадлежащих различным классам эквивалентности.

Классы функций W_i, $i = 1, \ldots, 6$, получены замыканием по суперпозиции от систем функций, приведенных в таблице 1. Для задания функций одной и двух переменных используются таблицы значений (см. [6]). Например, функцию $\max(x_1, x_2)$ в P_3 можно задать с помощью таблицы:

$x_1 \setminus x_2$	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

.

Таблица 1

Класс	Порождающая система
W_1	$\begin{array}{ccc\|ccc\|cc} 0&0&0&0&1&1&0&1\\ 0&1&1&1&1&1&0&1\\ 0&1&1&1&1&1&1&1 \end{array}$
W_2	$\begin{array}{ccc\|ccc\|cc} 0&0&0&0&2&2&0&2\\ 0&0&0&2&2&2&0&2\\ 0&0&2&2&2&2&0&2 \end{array}$
W_3	$\begin{array}{ccc\|ccc\|ccc\|c} 0&0&2&0&1&2&0&0&0&1\\ 0&1&2&1&1&2&0&0&2&1\\ 2&2&2&2&2&2&0&0&2&1 \end{array}$
W_4	$\begin{array}{ccc\|ccc\|c} 0&0&2&0&1&2&2\\ 0&1&2&1&1&2&2\\ 0&0&2&0&0&2&1 \end{array}$
W_5	$\begin{array}{ccc\|ccc\|cc} 0&0&2&0&1&2&0&1\\ 0&1&2&1&1&2&0&1\\ 2&2&2&2&2&2&1&1 \end{array}$
W_6	$\begin{array}{ccc\|ccc\|cc} 0&0&2&0&1&2&2&1\\ 0&1&2&1&1&2&2&1\\ 2&2&2&2&2&2&0&1 \end{array}$

Ранговые функции классов W_1, W_2, W_3, W_4 имеют линейный порядок роста (подробнее см. [5]). Для классов W_5 и W_6 порядок роста ранговой функции оказался экспоненциальным (см. [4]).

Основной результат настоящей работы заключается в существенном улучшении верхней оценки ранговой функции класса W_5 и формулируется следующей теоремой.

Теорема 1. *При всех натуральных n для ранговой функции класса W_5 справедливы соотношения:*

$$2^{(n+1)/2} - \frac{1}{2} \leq m_W(n) \leq 2^n(n+2).$$

Автор выражает благодарность своему научному руководителю Октаю Мурадовичу Касим-Заде за постановку задачи и всестороннее внимание к данной работе.

Работа выполнена при финансовой поддержке РФФИ (проект № 11–01–00508), и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Касим-Заде О. М. О неявной выразимости булевых функций // Вестник МГУ. Серия 1. Математика. Механика. — 1996. —№ 2. — С. 44–49.
2. Касим-Заде О. М. Об одной метрической характеристике неявных и параметрических представлений булевых функций // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 133–188.
3. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука, 1979. — С. 5–33.
4. Михайлец Е. В. О ранге неявных представлений над одним классом функций трехзначной логики // Материалы VII Молодежной научной школы по дискретной математике и ее приложениям (Москва, ИПМ, 2009). — М.: Изд-во мех.-мат. ф-та МГУ, 2009.
5. Михайлец Е. В. О ранге неявных представлений над некоторыми классами функций трехзначной логики // Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, МГУ, 2010). — М.: Изд-во мех.-мат. ф-та МГУ, 2010.
6. Орехова Е. А. Об одном критерии неявной полноты в трехзначной логике // Математические вопросы кибернетики. Вып. 12. — М.: Наука. Физматлит, 2003. — С. 27–74.

О СВОЙСТВАХ ЗАМКНУТЫХ КЛАССОВ В P_3, ПОРОЖДЕННЫХ МОНОТОННЫМИ СИММЕТРИЧЕСКИМИ ФУНКЦИЯМИ

А. В. Михайлович (Москва)

Рассматриваются замкнутые классы функций трехзначной логики, порожденные монотонными симметрическими функциями. Известно [1], что все замкнутые классы булевых функций имеют конечный базис. В [2] показано, что при всех $k \geq 3$ в P_k существуют как замкнутые классы со счетным базисом, так и классы, не имеющие базиса. В [3–5] рассмотрены некоторые семейства замкнутых классов, порожденных монотонными симметрическими функциями; для них приведены критерии базируемости и конечной порожденности. В данной работе рассматривается более широкое семейство классов, порожденных монотонными симметрическими функциями, для которого меняется критерий конечной порожденности. Все необходимые определения можно найти в [3–7].

Обозначим через $\widehat{\mathrm{MR}}$ множество всех монотонных относительно порядка $0 < 1 < 2$ функций из P_3, принимающих значения только из множества $\{0, 1\}$ и равных нулю на наборах, содержащих хотя бы одну нулевую компоненту. Обозначим через MR множество всех функций из $\widehat{\mathrm{MR}}$, принимающих нулевое значение на наборах, состоящих из одних единиц. Обозначим через $\widehat{\mathrm{MS}}$ (соответственно MS) множество всех симметрических функций из $\widehat{\mathrm{MR}}$ (соотв. MR). Множество функций A из $\widehat{\mathrm{MR}}$ называется k-ограниченным, если число единиц в наборах, на которых функции из множества A принимают значение 1, не превосходит k и существует функция $f(x_1, \ldots, x_n)$ из A и набор $\widetilde{\alpha}$ из $\{1, 2\}^n$, содержащий ровно k единиц, такой, что $f(\widetilde{\alpha}) = 1$. Обозначим через $i_n(x_1, \ldots, x_n)$, $n \geq 1$, функцию из $\widehat{\mathrm{MR}}$, принимающую значение 1 на всех наборах из $\{1, 2\}^n$. Положим $I = \cup\{i_n\}$, где объединение берется по всем $n \geq 1$. Очевидно, что для любого $n \geq 2$ выполняется равенство $I = [\{i_n\}]$. Пусть Φ — некоторая формула над $\widehat{\mathrm{MR}}$. Множество всех функций, символы которых содержатся в формуле Φ, обозначим через $\Theta(\Phi)$.

Пусть $f, g \in \mathrm{MS}$. Будем говорить, что функция f не превосходит функцию g относительно $\preceq$, (соответственно, $\preceq_I$) если $f \in [\{g\}]$ (соотв. $f \in [\{g\} \cup I]$). Нетрудно показать, что на множестве неконгруэнтных функций из MS отношения $\preceq$ и $\preceq_I$ являются отношениями частичного порядка. Множество попарно неконгруэнтных функций H из MS называется цепью относительно порядка $\preceq$ (соотв. $\preceq_I$), если любые два элемента множества H сравнимы относительно порядка $\preceq$ (соотв. $\preceq_I$). Пусть G — множество попарно неконгруэнтных функций из MS. Цепь $H \subset G$ называется ограниченной максимальной цепью относительно порядка $\preceq$ (соотв. $\preceq_I$) множества G, если для любой цепи $H_1 \subset \mathrm{MS}$, такой, что $H \subseteq H_1$, $H \neq H_1$, цепь H_1 не является подмножеством множества G, и существует функция f из H, такая, что для любой функции

$g \in H$ выполняется неравенство $g \preceq f$ (соотв. $g \preceq_I f$).

Для доказательства основных результатов нам потребуются следующие вспомогательные утверждения.

Утверждение 1. *Пусть* $\mathfrak{A} \subseteq \widehat{\mathrm{MS}}$, $f(x_1, \ldots, x_n) \in \mathrm{MS} \cap [\mathfrak{A}]$, Φ — *некоторая формула над* $\mathfrak{A}$, *реализующая функцию* f, Φ_1 — *подформула формулы* Φ, *имеющая вид* $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, *где* $g \in \mathrm{MS} \cap \mathfrak{A}$, *а* $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — *формулы над* $\mathfrak{A}$. *Тогда справедливы неравенства* $e_f \leq e_g$, $\frac{e_f}{d_f} \leq \frac{e_g}{d_g}$, $\left]\frac{d_g}{d_f}\right[\leq \frac{e_g}{e_f}$.

Утверждение 2. *Пусть* $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m) \in \mathrm{MS}$, $n \geq m \geq 1$, $e_f \leq e_g$. *Тогда* $f \preceq_I g$.

Утверждение 3. *Пусть* $\mathfrak{A} \subseteq \widehat{\mathrm{MS}}$, $f \in [\mathfrak{A}] \cap \mathrm{MS}$, Φ — *некоторая формула над* $\mathfrak{A}$, *реализующая функцию* f, $g \in \Theta(\Phi) \cap \mathrm{MS}$. *Тогда* $f \preceq_I g$.

Доказательство утверждений 1 – 3 проводится аналогично доказательству соответствующих утверждений из [3].

Утверждение 4. *Пусть* G — *множество попарно неконгруэнтных функций из* $\widehat{\mathrm{MS}}$, $G \not\subseteq \mathrm{MS}$, $F = [G]$, *а* $\mathfrak{B}$ — *множество всех верхних граней ограниченных максимальных цепей множества* $G \cap \mathrm{MS}$ *относительно порядка* $\preceq$. *Пусть класс* F *имеет базис* $\mathfrak{A}$. *Тогда для любой функции* $f \in \mathfrak{A}$ *существует функция* $g_f \in \mathfrak{B}$, *такая, что* $f \in [\{g_f\} \cup I]$ *и* $g_f \in [\{f\}]$.

Доказательство. Пусть класс F имеет базис $\mathfrak{A}$. Для каждой функции f из $\mathfrak{A}$ зафиксируем формулу Υ_f над G, реализующую функцию f. Преобразуем произвольную формулу Φ над $\mathfrak{A}$ в формулу $\pi(\Phi)$ над G следующим образом. Если формула Φ имеет вид x_i, то $\pi(\Phi) = x_i$. Пусть формула Φ имеет вид $f(\mathcal{B}_1, \ldots, \mathcal{B}_p)$, где $\mathcal{B}_1, \ldots, \mathcal{B}_p$ — формулы над $\mathfrak{A}$ или символы переменных. Пусть формулам $\mathcal{B}_1, \ldots, \mathcal{B}_p$ над $\mathfrak{A}$ уже сопоставлены формулы $\pi(\mathcal{B}_1), \ldots, \pi(\mathcal{B}_p)$ над G соответственно. Тогда $\pi(\Phi) = \Upsilon_f(\pi(\mathcal{B}_1), \ldots, \pi(\mathcal{B}_p))$.

Пусть $g(x_1, \ldots, x_m) \in \mathfrak{B}$. Рассматривая произвольную формулу Φ над $\mathfrak{A}$, реализующую функцию g, и соответствующую ей формулу $\pi(\Phi)$ над G, получаем, что $\Theta(\pi(\Phi)) \subseteq \{g\} \cup I$. Следовательно, существует функция $f \in \mathfrak{A}$, такая, что $f \in [\{g\} \cup I]$. Нетрудно показать, что $g \in [\{f\}]$.

Пусть $f \in F$, f не порождает верхнюю грань ограниченной максимальной цепи множества G относительно порядка $\preceq$. Предположим, что $f \in \mathfrak{A}$. Рассматривая произвольную формулу Υ_f над G, реализующую функцию f, получаем, что для любой подформулы $\Psi = g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$ формулы Υ_f выполняется включение $g \in \mathfrak{A} \backslash \{f\} \subseteq [\mathfrak{A} \backslash \{f\}]$. Но тогда $f \in [\mathfrak{A} \backslash \{f\}]$, что противоречит тому, что $f \in \mathfrak{A}$ и $\mathfrak{A}$ — базис класса F. Следовательно, каждая функция из $\mathfrak{A}$ порождает некоторую функцию из $\mathfrak{B}$.

Теорема 1. *Пусть* G — *множество попарно неконгруэнтных функций из* $\widehat{\mathrm{MS}}$, $G \not\subseteq \mathrm{MS}$, $F = [G]$. *Тогда класс* F *имеет базис в том и только том случае, когда каждая функция из* $G \cap \mathrm{MS}$ *содержится в некоторой ограниченной максимальной цепи множества* $G \cap \mathrm{MS}$ *относительно порядка* $\preceq_I$.

Доказательство теоремы может быть проведено с использованием утверждений 3 и 4 аналогично доказательству теоремы 1 из [3].

Утверждение 5. *Пусть* $G \subseteq \widehat{\mathrm{MS}}$, $G \not\subseteq \mathrm{MS}$. *Тогда каждая функция из* G *содержится в некоторой ограниченной максимальной цепи множества* G *относительно порядка* $\preceq_I$ *в том и только том случае, когда каждая функция из* $G \cap \mathrm{MS}$ *содержится в некоторой ограниченной максимальной цепи множества* $G \cap \mathrm{MS}$ *относительно порядка* $\preceq$.

Доказательство утверждения основано на том, что для любой функции из g множества G существует только конечное число функций f, таких, что $g \preceq_I f$ и $g \not\preceq f$.

Теорема 2. *Пусть* G *— множество попарно неконгруэнтных функций из* $\widehat{\mathrm{MS}}$, $F = [G]$. *Тогда класс* F *имеет базис в том и только том случае, когда каждая функция из* G *содержится в некоторой ограниченной максимальной цепи множества* $G \cap \mathrm{MS}$ *относительно порядка* $\preceq$.

Доказательство следует из теоремы 1 и утверждения 5.

Теорема 3. *Пусть* G *— множество попарно неконгруэнтных функций из* $\widehat{\mathrm{MS}}$, $G \not\subseteq \mathrm{MS}$, $F = [G]$. *Тогда класс* F *имеет конечный базис в том и только том случае, когда для некоторого* $k \geq 0$ *множество* G *является* k*-ограниченным.*

Доказательство. *Необходимость.* Пусть $\mathfrak{A}$ — некоторый базис класса F. В силу утверждения 4 для любой функции f из $\mathfrak{A}$ существует функция g из $\mathfrak{B}$, такая, что $f \in [\{g\} \cup I]$, $g \in [\{f\}]$. Следовательно, существует конечный базис $\mathfrak{A}'$ класса F, такой, что $\mathfrak{A}' \subseteq \mathfrak{B} \cup I$. Поскольку множество $\mathfrak{A}'$ конечно, существует число $k \in \mathbb{Z}^+$, такое, что множество $\mathfrak{A}'$ является k-ограниченным. Рассмотрим произвольную функцию $g(x_1, \ldots, x_n) \in G$. Пусть она реализуется некоторой формулой Φ над $\mathfrak{A}$, которая имеет вид $h(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, где $h \in \mathfrak{A}'$, $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — формулы над $\mathfrak{A}'$. По утверждению 1 выполняется неравенство $e_g \leq e_h$ Следовательно, множество G является k-ограниченным.

Достаточность. Пусть множество G является k-ограниченным. Пусть $f(x_1, \ldots, x_n) \in G$, $e_f = k$. Из утверждения 2 следует, что для любой функции $g(x_1, \ldots, x_m)$, такой, что $e_g \leq e_f$, $m \geq n$, выполняется соотношение $g \in [\{f\} \cup I]$. Обозначим через $\mathcal{B}$ множество всех функций $h(x_1, \ldots, x_m) \in G$, таких, что $e_h < e_f$, $m < n$. Очевидно, что множество $\mathcal{B}$ конечно. Поскольку для любой функции $g \in G$ выполняется неравенство $e_g \leq e_f$, то $g \in [\{f\} \cup I]$ или $g \in \mathcal{B}$. Следовательно, $F = [\mathcal{B} \cup \{f\}]$. Поскольку множество $\mathcal{B} \cup \{f\}$ конечно, то класс F имеет конечный базис.

Автор выражает благодарность профессору А. Б. Угольникову за постановку задачи и постоянное внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект № 11–01–00508) и программы фундаментальных исследований ОМН РАН “Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения”.

Список литературы

1. Post E. L. The two-valued iterative systems of mathematical logic // Annals of Math. Studies. — Princeton Univ. Press, 1941. — 122 p.
2. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — 127, № 1. — С. 44–46.
3. Михайлович А. В. О классах функций трехзначной логики, порожденных монотонными симметрическими функциями // Вестн. Моск. ун-та. Матем. Механ. — 2009. — № 1. — С. 33–37.
4. Михайлович А. В. О свойствах замкнутых классов трехзначной логики, порожденных монотонными симметрическими функциями // Труды VIII междунар. конференции "Дискретные модели в теории управляющих систем" (Москва, 6–9 апреля 2009 г.). — М.: МАКС Пресс, 2009. — С. 223–225.
5. Михайлович А. В. О классах функций трехзначной логики, порожденных симметрическими функциями // Материалы 3-й Российской школы-семинара "Синтаксис и семантика логических схем" (Иркутск, 10–14 августа 2010 г.). — Иркутск: Изд-во ГОУ ВПО "Восточно-Сибирская государственная академия образования", 2010. — С. 64–67.
6. Михайлович А. В. О замкнутых классах функций трехзначной логики, порожденных периодическими симметрическими функциями // Материалы XVI междунар. конференции "Проблемы теоретической кибернетики" (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. — С. 319–323.
7. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001. — 384 с.

УПАКОВКИ И ПОКРЫТИЯ ГРАФОВ ОТНОСИТЕЛЬНО 3-ПУТИ

Д. Б. Мокеев (Нижний Новгород)

Введение

Пусть $\mathbf{X}$ — множество графов. $\mathbf{X}$-*упаковкой* графа G называется множество его непересекающихся порожденных подграфов, каждый из которых изоморфен какому-нибудь графу из $\mathbf{X}$. Наибольшее число подграфов в $\mathbf{X}$-упаковке графа G будем обозначать через $pack(\mathbf{X}; G)$. $\mathbf{X}$-*покрытием* графа G называется множество вершин, после удаления которых получается граф, не содержащий порожденных подграфов, принадлежащих $\mathbf{X}$. Наименьшее число вершин в $\mathbf{X}$-покрытии графа G будем обозначать через $cover(\mathbf{X}; G)$. В случае, когда $\mathbf{X}$ состоит из единственного графа H, будем говорить просто об

H-покрытии и H-упаковке. В частности, K_2-упаковки — это паросочетания, а K_2-покрытия известны как вершинные покрытия.

Очевидно, всегда выполняется неравенство $pack(\mathbf{X}; G) \leq cover(\mathbf{X}; G)$. Теорема Кёнига утверждает, что для двудольных графов имеет место равенство $pack(P_2; G) = cover(P_2; G)$. Верно и в известном смысле обратное утверждение: если это равенство выполняется для графа G и любого его порожденного подграфа, то этот граф — двудольный.

Определение. Граф G будем называть *кёниговым* графом относительно множества $\mathbf{X}$, если для любого его порожденного подграфа H выполняется равенство $pack(\mathbf{X}; H) = cover(\mathbf{X}; H)$. Класс всех кёниговых графов относительно $\mathbf{X}$ обозначим через $\mathbf{K}(\mathbf{X})$.

Класс $\mathbf{K}(\mathbf{X})$ при любом $\mathbf{X}$ является наследственным и, следовательно, может быть описан множеством минимальных запрещенных (порожденных) подграфов. Для P_2 такую характеризацию дает теорема Кёнига вместе с известным критерием двудольности. Кроме этой классической теоремы известен еще только один результат такого рода для обыкновенных графов — в работе [1] описаны все запрещенные подграфы для класса $\mathbf{K}(\mathbf{C})$, где $\mathbf{C}$ — множество всех простых циклов.

Цель настоящей работы — охарактеризовать класс $\mathbf{K}(P_3)$. Применяется 2 подхода к описанию этого класса: множеством всех его минимальных запрещённых порождённых подграфов (найдены все такие подграфы), а так же путём построения с помощью операций подразбиения ребер и замены вершин кликами.

Далее вместо $pack(P_3; G)$ и $cover(P_3; G)$ пишем просто $pack(G)$ и $cover(G)$, под покрытием и упаковкой подразумеваем P_3-покрытие и P_3-упаковку, а под кёниговым графом — кёнигов граф относительно P_3.

Расширение графов

Заметим, что граф кёнигов тогда и только тогда, когда каждая его компонента связности — кёнигов граф. Поэтому мы будем рассматривать только связные графы.

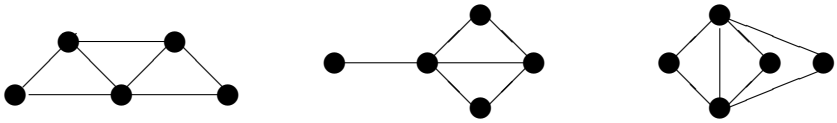
Определение. Операция замены вершины x t-кликой состоит в том, что эта вершина удаляется из графа, к нему добавляются t новых вершин, попарно смежных между собой. Каждая из них соединяется ребром с каждой вершиной, с которой была смежна x. Граф, получаемый из графа G заменой некоторых его вершин степени 1 и 2 кликами (возможно, разного размера), назовем расширением графа G, а клики, на которые были заменены вершины, будем называть секциями. Каждая вершина, не подвергавшаяся замене, считается отдельной секцией.

Лемма 1. *Каждое наименьшее покрытие любого расширения любого графа состоит из целых секций.*

Лемма 2. *Любое расширение любого дерева принадлежит классу* $\mathbf{K}(P_3)$.

Запрещенные подграфы

Непосредственной проверкой легко установить, что три графа, изображенные на рисунке 1, не являются кёниговыми. Для каждого из них $pack(G) = 1$, $cover(G) = 2$. При этом каждый порожденный подграф каждого из них принадлежит классу $\mathbf{K}(P_3)$. Таким образом, справедлива



D_1 D_2 D_3

Рис. 1

Лемма 3. *Графы D_1, D_2, D_3 являются минимальными запрещенными графами для $\mathbf{K}(P_3)$.*

Рассмотрим теперь несколько бесконечных серий минимальных запрещенных подграфов для $\mathbf{K}(P_3)$. Очевидно,

$$pack(C_{3k}) = pack(C_{3k+1}) = pack(C_{3k+2}) = k,$$
$$cover(C_{3k}) = cover(C_{3k-1}) = cover(C_{3k-2}) = k.$$

Поэтому и ввиду леммы 2 справедливо следующее утверждение.

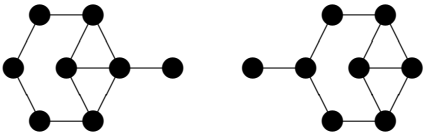
Лемма 4. *Цикл C_n принадлежит классу $\mathbf{K}(P_3)$, если n кратно 3, и является минимальным запрещенным графом для $\mathbf{K}(P_3)$, если n не кратно 3.*

Рассмотрим граф, получающийся из цикла C_n добавлением двух вершин, не смежных между собой, каждая из которых соединяется ребром с одной вершиной цикла. Этот граф обозначим через $A(n, k)$, где k — расстояние между вершинами цикла, смежными с добавленными вершинами.

Лемма 5. *Если n кратно 3, а k не кратно 3, то $A(n, k)$ является минимальным запрещенным графом для класса $\mathbf{K}(P_3)$.*

Рассмотрим граф, получающийся из цикла C_n добавлением двух вершин a и b, не смежных между собой, причем a соединяется ребром с одной вершиной цикла, а b — с тремя подряд идущими вершинами цикла. Этот граф обозначим через $B(n, k)$, где k — расстояние между вершиной, смежной с a, и средней из трех вершин, смежных с b. На рисунке 2 показаны графы $B(6, 0)$ и $B(6, 3)$. Отметим, что первый из них содержит запрещенный подграф D_2.

Лемма 6. *Если n и k кратны 3, $k \neq 0$, то $B(n, k)$ — минимальный запрещенный граф для класса $\mathbf{K}(P)$.*



$B(6,0)$ $B(6,3)$

Рис. 2

Через $C(k_1,k_2,k_3)$ обозначим граф, который получается из цикла длины $n=k_1+k_2+k_3$ заменой 2-кликами трех вершин, расстояния между которыми равны k_1,k_2,k_3.

Лемма 7. *Если* $k_1 \equiv k_2 \equiv k_3 \equiv 1 \pmod 3$ *и* $k_i \geq 4$, $i=1,2,3$, *то* $C(k_1,k_2,k_3)$ *— минимальный запрещенный подграф для класса* $\mathbf{K}(P_3)$.

Перечисленные запрещённые подграфы полностью описывают класс $\mathbf{K}(P_3)$. Иными словами, справедлива следующая теорема:

Теорема 1.

$$\mathbf{K}(P_3) = Free(\{D_1,D_2,D_3\} \cup \{C_n | n \text{ не кратно } 3\} \cup$$
$$\cup \{A(n,k) | n \text{ кратно } 3, k \text{ не кратно } 3\} \cup \{B(n,k) | n \text{ и } k \text{ кратны } 3\} \cup$$
$$\cup \{C(k_2,k_2,k_3) | k_1 \equiv k_2 \equiv k_3 \equiv 1 \pmod 3 \text{ и } k_i \geq 4,\ i=1,2,3\}).$$

"Конструктивный" подход к описанию класса $\mathbf{K}(P_3)$

Связные графы из класса $\mathbf{K}(P_3)$ удобно разделить на две категории: расширенные циклы и все остальные графы, их будем называть ординарными.

Для "конструктивного" описания ординарных графов введём операцию 2-расширения графа:

Определение. Пусть H — мультиграф без петель. Каждое цикловое ребро (ребро, принадлежащее какому-нибудь циклу) этого мультиграфа подразобьем двумя вершинами. Эти вершины будем называть новыми. Заменим каждую новую вершину и каждую вершину степени 1 или 2, не принадлежащую циклу, какой-нибудь кликой. Полученный таким образом граф будем называть 2-расширением исходного мультиграфа.

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

(1) G *— ординарный кёнигов граф*;

(2) G *является 2-расширением некоторого мультиграфа, отличного от простого цикла.*

Рассмотрим теперь расширенные циклы. Очевидно, что следует уделить внимание расширениям только тех циклов, число вершин в которых кратно 3. В частности, любое расширение циклов C_6 и C_9 является кёниговым графом. Для общего же случая справедлива следующая теорема:

Теорема 3. *Любое расширение любого цикла C_{3k} является кёниговым графом, тогда и только тогда, когда не содержит в качестве порождённого подграфа граф $C(k_1, k_2, k_3)$, где $k_1 \equiv k_2 \equiv k_3 \equiv 1 \pmod 3$ и $k_i \geq 4$, $i = 1, 2, 3$.*

Список литературы

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

О СВОЙСТВАХ ОДНОМЕСТНЫХ МОНОТОННЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Д. Ю. Панин (Москва)

Рассматривается некоторое множество одноместных функций многозначной логики, монотонных относительно частичного порядка специального вида. На этом множестве функций вводятся операции свертки и композиции [1–2]. Получен критерий полноты для рассматриваемой функциональной системы (см. также [3–4]). Подобные вопросы возникают при изучении свойств предполных классов монотонных функций, не имеющих конечных порождающих систем [5–8].

Пусть $n \geq 1$. Положим $Q_k = \{0, a_1, a'_1, \ldots, a_{k-1}, a'_{k-1}, 1\}$, где $1 \leq k \leq n$, $Q = Q_n$, $a_0 = a'_0 = 0$, $a_n = a'_n = 1$. Введем на элементах множества Q отношение частичного порядка $\leq$ следующим образом:

1) $\varepsilon_i \leq \varepsilon_j$ для всех $\varepsilon_i, \varepsilon_j$, таких, что $\varepsilon_i \in \{a_i, a'_i\}$, $\varepsilon_j \in \{a_j, a'_j\}$, $0 \leq i < j \leq n$;

2) $\varepsilon \leq \varepsilon$ для всех $\varepsilon \in Q$.

Пусть $\alpha, \beta \in Q$. Если для этих элементов выполняется по крайней мере одно из соотношений $\alpha \leq \beta$, $\beta \leq \alpha$, то эти элементы называются *сравнимыми*, в противном случае — *несравнимыми*.

Будем обозначать через F множество всех функций $f(x)$, определенных на множестве Q, принимающих значения из Q, монотонных относительно частичного порядка $\leq$ и таких, что $f(\delta) \leq \delta$ для всех $\delta \in Q$. Введем на множестве F операцию композиции. Пусть $f(x)$, $g(x) \in F$. *Композицией функций f и g* будем называть функцию $(f \circ g)(x)$, значение которой на любом элементе $\alpha \in Q$ определяется равенством $(f \circ g)(\alpha) = f(g(\alpha))$. *Сверткой функций f и g* будем называть функцию $(f * g)(x)$, значение которой на любом элементе $\alpha \in Q$ определяется следующим образом:

$$(f * g)(\alpha) = \begin{cases} \alpha, & \text{если } g(\alpha) \neq 0; \\ f(\alpha), & \text{если } g(\alpha) = 0. \end{cases}$$

Пусть $\mathfrak{A} \subseteq F$. Определим по индукции понятие *формулы над* $\mathfrak{A}$, а также понятие *функции, реализуемой формулой*.

1. Выражение вида $f(x)$, где $f(x) \in \mathfrak{A}$, является формулой над $\mathfrak{A}$. Такая формула называется *тривиальной* и реализует функцию $f(x)$.

2. Пусть Φ_1 — формула над $\mathfrak{A}$, реализующая функцию $f_1(x)$, а Φ_2 — формула над $\mathfrak{A}$, реализующая функцию $f_2(x)$. Тогда выражения $\Phi_1 \circ \Phi_2$ и $\Phi_1 * \Phi_2$ являются формулами над $\mathfrak{A}$ и реализуют функции $(f_1 \circ f_2)(x)$ и $(f_1 * f_2)(x)$ соответственно.

При этом предполагается, что других формул над $\mathfrak{A}$ нет.

Замыканием множества $\mathfrak{A} \subseteq F$ будем называть множество всех функций, которые могут быть реализованы формулами над $\mathfrak{A}$ (обозначение $< \mathfrak{A} >$). Очевидно, что $< \mathfrak{A} >$ содержится в F. Систему $\mathfrak{A}$ будем называть *полной*, если $< \mathfrak{A} > = F$.

Цепью длины m, $1 \leq m \leq n$, будем называть последовательность элементов $b_0, b_1, b_2, \ldots, b_{m-1} \in Q$, таких, что $b_0 = 0$, $b_i \in \{a_i, a'_i\}$ для всех $i = 1, \ldots, m-1$.

Пусть $\Omega \subseteq Q$. Положим

$$S_\Omega = \{f \in F \mid f(\delta) = \delta \text{ для всех } \delta \in \Omega\},$$

В частности, $S_{\{a_1\}}$ — множество всех функций из F, сохраняющих элемент a_1.

Будем обозначать через H_1 множество всех функций h из F, для которых выполнены следующие условия:

1) $h(1) \neq 1$;

2) найдутся номер k, $2 \leq k \leq n-1$, и цепь Ω длины $k-1$, такие, что $h \in S_\Omega$ и $\{h(a'_k), h(a_k)\} = \{a_{k-1}, a'_{k-1}\}$.

Будем обозначать через H_2 множество всех функций h из F, для которых $h(1) \neq 1$ и найдется цепь Ω длины n, такая, что $h \in S_\Omega$.

Имеет место следующий критерий полноты для систем функций из F.

Теорема 1. *Система $H \subseteq F$ является полной тогда и только тогда, когда $H_1 \subseteq H$ и $H_2 \subseteq H$.*

При доказательстве теоремы 1 используется следующая лемма.

Лемма 1. *Пусть $f_1, f_2 \in F$, $h \in H_1 \cup H_2$ и $h = f_2 \circ f_1$ или $h = f_2 * f_1$, тогда $f_2 = h$ или $f_1 = h$.*

Работа выполнена при финансовой поддержке РФФИ, проект 11–01–00508, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2008.
2. Яблонский С. В. Функциональные построения в k-значной логике // Труды математического института АН СССР. — 1958. — Т. 51. — С. 5–142.

3. Панин Д. Ю. О порождении одноместных монотонных функций многозначной логики // Вестник Московского университета. Математика. Механика. — 2010. № 6. — С. 52–55.
4. Панин Д. Ю. О некоторых свойствах одноместных монотонных функций многозначной логики // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.). Нижний Новгород: Изд-во Нижегородского гос. ун-та, 2011. — С. 349–352.
5. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — V. 3. — P. 211–218.
6. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. Springer Monographs in Mathematics. — Berlin: Springer, 2006. — 668 p.
7. Дудакова О. С. О конечной порожденности предполных классов монотонных функций многозначной логики // Математические вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 13–104.
8. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестник Московского университета. Математика. Механика. — 2008. №. 1. — С. 31–37.

ОБ ОДНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЕ ФУНКЦИОНИРОВАНИЯ ДИСКРЕТНОЙ МОДЕЛИ ГЕННОЙ СЕТИ

А. В. Приходько (Новосибирск)

Введение

Регуляторный контур генной сети представляется в виде связного ориентированного графа $G(V, D)$, где $V = \{v_0, \ldots, v_{n-1}\}$ — множество вершин, отождествляемое с продуктами генетических элементов (РНК, белки), а D — множество дуг, имеющих смысл регуляторных связей.

В качестве графов мы рассматриваем ориентированные циркулянтные графы $G_{n,k}$, где n — число вершин в этом графе, а $k-1$ — число входящих и выходящих дуг, $k \leq n$.

В вершинах графа в каждый момент времени подсчитываются значения функций $f_v(x_{i_1}, \ldots, x_{i_n})$, сопоставленных вершинам, а переменные x_{i_j}, $j \in \{1, \ldots, k\}$, приписаны дугам, входящим в вершину v. Значения функции $f_v : B^k \longrightarrow B$, где $B = \{0, 1\}$, содержательно соответствуют наличию конечного продукта, далее называемому весом вершины, синтезируемого с генетического элемента, соответствующего заданной вершине.

Функционирование генной сети характеризуется изменением концентрации ее веществ, т. е. n-наборов из B^n, соответствующих значениям функции

f_v в вершинах сети в каждый момент времени. Таким образом, для каждого начального состояния динамика изменения состояний определяется отображением $A : \Omega_p \longrightarrow \Omega_p$, где Ω_p — множество наборов весов вершин графа $G_{n,k}$. Будем называть r-состоянием то состояние сети, которое получается после r отображений начального состояния.

Считаем, что вес $p = 2$. Также будем считать, что все функции f_v в вершинах из V равны и определяются следующим образом: для любой вершины v функция $f_v(x_{i-k+1}, \ldots, x_{i-1}) = x'_i$, где x'_i выражается следующим образом:

$$x'_i = \bigoplus_{j=i-k+1}^{i-1} x_j = x_{i-k+1} \oplus \ldots \oplus x_{i-1}. \tag{1}$$

Отображение $A : \Omega_2 \longrightarrow \Omega_2$, определяемое таким образом, назовем действием аддитивного (автономного) автомата $A(f_\oplus, 2)$ на множестве Ω_2. Здесь и далее действие автомата задается на графе $G_{n,k}$.

Последовательность наборов $X^1, \ldots, X^r \in \Omega_2$ называется циклом длины r аддитивного автомата $A(f_\oplus, 2)$, если

$$A(X^i) = X^{i+1} \text{ для } i \in \overline{1, r} \text{ и } X^{r+1} = X.$$

Цикл называется простым, если он не содержит в себе других циклов. Неподвижная точка отображения $A : \Omega_2 \longrightarrow \Omega_2$ — это цикл длины 1. Анализ поведения генной сети включает исследование динамики изменения ее состояний: исследование циклов, нахождение неподвижных точек и т. д.

1. Циклы

Любое начальное состояние с течением времени порождает соответственно либо неподвижную точку, либо простой цикл. Сначала рассмотрим частный случай ориентированного циркулянтного графа с двумя входящими и выходящими дугами для каждой вершины: $G_{n,3}$. Для каждой вершины v функция f_v определяется следующим образом:

$$f_v(x_{i-1}, x_{i-2}) = x'_i, \quad x'_i = x_{i-1} \oplus x_{i-2}.$$

В силу цикличности полагаем, что $v_n = v_0$, следовательно, $x_n = x_0$. Сформулируем задачу о наибольшем цикле: Дан ориентированный циркулянтный граф $G_{n,3}$ с функциями $\oplus$ в вершинах. Какова длина наибольшего простого цикла в функциональном графе отображений?

Теорема 1. *Пусть $n = 2^r z$, где z — нечетное. Пусть k_1 — минимальное натуральное число такое, что $2^{k_1 - r} \equiv 1 \pmod{z}$ и $k_1 > r$. Тогда верны следующие утверждения*:

1) *Если $n = 2^t$, $t = 0, 1, \ldots$, то максимальная длина простого цикла равна* 1.

2) *Если $n \neq 2^t$, то максимальная длина простого цикла ограничена сверху величиной $2^{k_1 - r}$.*

Теорема 2. *Пусть $n = 2^r z$, где z — нечетное. Пусть k_2 — минимальное натуральное число такое, что $2^{k_2-r} \equiv z-1 \pmod{z}$ и $k_2 > r$ (если такого k_2 не существует, полагаем $k_2 = \infty$). Тогда верны следующие утверждения*:

1) *Если $n = 2^t$, $t = 0, 1, \ldots$, то максимальная длина простого цикла равна* 1.

2) *Если $n \neq 2^t$, то максимальная длина простого цикла ограничена сверху величиной $2^{k_2-r}\frac{n}{(3\cdot 2^r, n)}$.*

2. Неподвижные точки

Пусть теперь у нас имеется ориентированный циркулянтный граф $G_{n,k}$ с произвольным числом входящих-выходящих ребер $k-1$. Рассмотрим произвольное состояние — неподвижную точку: $(x_0 x_1 x_2 \ldots x_{n-1})$. Опишем зависимость переменных через формулы:

$$x_i = x_{i-k+1} \oplus \ldots \oplus x_{i-1} \tag{2}$$

Прежде всего, выделим особую неподвижную точку вида $(00\ldots00)$. Она называется нулевой неподвижной точкой. Приведем алгоритм нахождения неподвижных точек. Он заключается в том, что мы выбираем, исходя из величины k, такие n, при которых могут существовать неподвижные точки:

1) Будем составлять ряд L из нулей и единиц. Пусть первые $k-1$ элементов в ряду — единицы: $L = (11\ldots11xxx\ldots)$, x — неизвестные элементы. Будем считать, что первые $k-1$ элементов ряда — значения переменных $x_0, \ldots, x_{k-2}$.

2) Кроме того, образуем некоторое множество M, куда будем записывать подслова из L длины $k-1$. Добавим туда первый элемент из нашего ряда — $(11\ldots11)$.

3) Вычислим значение переменной x_{k-1}, используя формулы (2), и полученное значение (допустим, это 0) припишем к ряду L на месте неизвестного элемента: $L = (11\ldots110xx\ldots)$. Также добавим новое подслово $(11\ldots110)$ в M.

4) Далее вычисляем новые элементы ряда L аналогичным образом, каждый раз пополняя ряд на 1 элемент и добавляя 1 новое подслово во множество M. Заметим, что разность числа элементов в M и длина ряда L всегда постоянна и равна $k-2$.

5) В силу конечного числа возможных элементов из M рано или поздно некоторый новый добавленный элемент будет совпадать с уже ранее добавленным. Пусть такой элемент имеет номер j. Тогда текущая длина ряда будет равна $((k-2)+j)$. При этом в ряду самые "крайние" подслова будут совпадать.

6) Таким образом, если мы выбросим из ряда одно из "крайних" подслов, мы получим конечную последовательность длины $j-1$, цикличную относительно функции сложения по модулю 2 от $k-1$ подряд идущих элементов.

Мы получим конечную циклическую последовательность

$$L = (y_0, y_1 \ldots, x_{j-2})$$

длины $j-1$ из бинарных элементов 0 и 1, которая фактически описывает следующий класс N_1 возможных неподвижных точек для данного k:

$$n=(j-1)t,\ t\in\mathbb{N}\text{ и }i+C\equiv h\pmod{(j-1)}\Longrightarrow x_i=y_h,\ C=const \qquad (3)$$

Класс N_1 образуют все возможные значения n, удовлетворяющие условиям (3). Смысл константы заключен в том, что нумерация вершин может быть произвольной, и вершина v_0 — также произвольна. Иными словами, совершая в любой неподвижной точке сдвиг (изменение индексов на 1), мы получаем другую неподвижную точку.

Т. к. длина слов в множестве M равна $k-1$, то максимальное число различных подслов в M равно $2^{k-1}-1$ (вычитаем единицу, т. к. не учитываем нулевую неподвижную точку). Если на момент создания класса неподвижных точек число элементов из M не достигает $2^{k-1}-1$, то это означает, что найдены не все неподвижные точки.

В этом случае мы опять будем составлять новый ряд L, в котором самым первым словом будет некоторое слово длины $k-1$, которого еще нет в M. Тут же добавляем это новое слово в M, и дальше, по вышеописанному алгоритму, образуем конечный циклический ряд L_2, который определит еще один класс N_2 неподвижных точек.

Дальше действуем аналогично до тех пор, пока после получения очередного класса неподвижных точек мощность множества M не достигнет $2^{k-1}-1$. Это и будет означать, что мы нашли все возможные неподвижные точки для данного k.

Таким образом, если у нас дан граф $G_{n,k}$, мы можем воспользоваться алгоритмом нахождения неподвижных точек для данного k, и тогда возможны следующие варианты:

1) Если существует такое значение i, что $n\in N_i$, то для данной модели графа $G_{n,k}$ существует неподвижная точка (не обязательно одна), отличная от нулевой и описанная в классе N_i. Эта неподвижная точка находится в процессе применения алгоритма нахождения неподвижных точек.

2) Если такого i, что $n\in N_i$, не существует, то для данной модели существует только одна неподвижная точка — нулевая.

3. Некоторые свойства

Заметим, что выше мы рассматривали модель графа $G_{n,k}$ с функциями (1). Рассмотрим более общую модель (обозначим $G'_{n,k}$), отличающуюся от вышеописанной модели функцией в вершинах:

$$x'_i=f_v(x_{i-j_0},\ldots,x_{i-j_{k-2}})=x_{i-j_0}\oplus x_{i-j_1}\oplus\ldots\oplus x_{i-j_{k-2}}. \qquad (4)$$

Граф $G'_{n,k}$ с функциями в вершинах вида (4) будем обозначать через $G'_{n,k}(j_0,j_1,\ldots,j_{k-2})$. Видно, что система с графом $G_{n,k}$ — частный случай $G'_{n,k}(j_0,j_1,\ldots,j_{k-2})$.

Утверждение 1. *Любая неподвижная точка для модели $G_{n,k}$ является неподвижной точкой и для модели $G'_{n,k}(2,4,\ldots,2(k-1))$.*

Утверждение 2. *Если в модели* $G'_{n,k}(j_0, j_1, \ldots, j_{k-2})$ *имеется ровно* S *ненулевых неподвижных точек, то в модели* $G'_{pn,k}(pj_0, pj_1, \ldots, pj_{k-2})$ *будет ровно* S^p *ненулевых неподвижных точек, где* p *— натуральное.*

Основные результаты: найдена точная оценка сверху для максимальной длины простого цикла функционирования модели $G_{n,3}$. Перспектива дальнейшей работы состоит в усилении оценки длины и вывод точной формулы для любого n. Также установлены некоторые закономерности при анализе неподвижных точек, и дан алгоритм их нахождения.

Список литературы

1. Евдокимов А. А, Лиховидова Е. О. Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник ТГУ. — 2008. — Т. 2, вып. 3.
2. Григоренко Е. Д, Евдокимов А. А, Лихошвай В. А, Лобарева И. А. Неподвижные точки и циклы автоматных отображений, моделирующих функционирование генных сетей // Вестник ТГУ. — 2005. — Вып. 14.
3. Харари Ф. Теория графов. — М.: Едиториал УРСС, 2003.

О МИНИМИЗАЦИИ ОБЪЕМА ПАМЯТИ СХЕМ, ВЫЧИСЛЯЮЩИХ УСЕЧЕННОЕ ДПФ

И. С. Сергеев (Москва)

В работе строятся схемы для усеченного ДПФ и умножения многочленов, эффективные с точки зрения сложности и объема памяти. Основной результат заключается в том, что усеченное ДПФ порядка N (т. е. ДПФ порядка $2^{\lceil \log_2 N \rceil}$, приведенное к векторам длины N) реализуется схемой сложности $1,5N \log_2 N + O(N)$ и объема памяти $N + 1$.

Напомним, что *дискретное преобразование Фурье порядка* N определяется как $\left(\mathbf{K}[x] / \left(x^N - 1\right) \to \mathbf{K}^N\right)$-преобразование

$$\text{ДПФ}_{N,\zeta} : \Gamma(x) \to \left(\Gamma(\zeta^0), \Gamma(\zeta^1), \ldots, \Gamma(\zeta^{N-1})\right),$$

где $\mathbf{K}$ — коммутативное ассоциативное кольцо с единицей, ζ — *примитивный корень степени* N в этом кольце. (Элемент $\zeta \in \mathbf{K}$ называется примитивным корнем (из единицы) степени N, если $\zeta^N = 1$ и при любом простом $p \mid N$ элемент $\left(\zeta^{N/p} - 1\right)$ не является делителем нуля в $\mathbf{K}$.)

Если элемент $N = 1 + \ldots + 1 \in \mathbf{K}$ обратим, то существует обратное к ДПФ преобразование (называемое *обратным ДПФ*), удовлетворяющее соотношению $\text{ДПФ}^{-1}_{N,\zeta} = N^{-1}\text{Pol} \circ \text{ДПФ}_{N,\zeta^{-1}} \circ \text{Pol}$, где Pol — тривиальное преобразование, переводящее вектор коэффициентов в многочлен (точнее, в элемент

кольца $\mathbf{K}[x]/\left(x^N-1\right)$):

$$\mathrm{Pol}:(\gamma_0,\ldots,\gamma_{N-1})\to\sum_{i=0}^{N-1}\gamma_i x^i.$$

Более того, ДПФ задает изоморфизм колец, причем операции в кольце образов выполняются покомпонентно. В частности, просто выполняется умножение. Поэтому при помощи ДПФ удобно умножать многочлены (сводя умножение к умножению Фурье-образов), тем более, что обратное ДПФ практически совпадает с прямым. На этом приеме построены все известные асимптотически быстрые алгоритмы умножения многочленов и чисел.

В качестве средства вычислений будем рассматривать *схемы из функциональных элементов* [1] (далее, просто схемы) над арифметическим базисом $\{x\pm y,\,xy\}\cup\{ax|a\in\mathbf{K}\}$ или *неветвящиеся программы* над тем же базисом. Неветвящаяся программа (далее, просто программа) — это схема, для которой фиксирована последовательность выполнения операций (срабатывания элементов схемы). Одной схеме соответствуют, вообще говоря, несколько программ.

Стандартным образом определяются несколько мер сложности схем (программ). Собственно *сложность* — число функциональных элементов в схеме (программе). *Объем памяти* программы — максимальное по всем итерациям число промежуточных данных (включая все уже вычисленные выходы), используемых в последующих итерациях. Несколько искусственно объем памяти схемы можно определить как минимальный объем памяти по всем программам, соответствующим данной схеме.

Наиболее эффективно реализуется ДПФ порядка степени двойки. А именно, используя метод Кули–Тьюки (*быстрое преобразование Фурье*), ДПФ порядка 2^k можно реализовать схемой из $k2^k$ элементов сложения-вычитания, $(k-2)2^{k-1}+1$ элементов умножения на степени примитивного корня (степени 2^k), и имеющей объем памяти 2^k+1. Добавив в схему $k2^{k-1}$ элементов умножения на 2 или дополнив базис функцией $2x+y$ и перестроив схему без увеличения сложности, объем памяти можно сократить до 2^k.

ДПФ порядка 2^k идеально подходит для умножения многочленов суммарной степени 2^k-1. Для случаев, когда степень существенно меньше ближайшей сверху степени двойки, применяются разнообразные приемы рационализации вычислений, которые, как правило, сводятся к тому, что ДПФ порядка степеней двойки используются как можно более полно.

Один из таких приемов основан на концепции усеченного ДПФ [4]. *Усеченное ДПФ* (*УДПФ*) *порядка* N применяется к многочленам степени $<N$ и определяется как набор из некоторых N компонент вектора $\mathrm{ДПФ}_{2^{\Lambda(N)},\zeta}$, где $\Lambda(N)=\lceil\log_2 N\rceil$. Или, если более формально,

$$\mathrm{УДПФ}_{N,\zeta}:\mathbf{K}[x]/\prod_{i=0}^{N-1}(x-\zeta^{k_i})\to\mathbf{K}^N:\Gamma(x)\to\left(\Gamma(\zeta^{k_0}),\Gamma(\zeta^{k_1}),\ldots,\Gamma(\zeta^{k_{N-1}})\right)$$

при некоторых $k_i \in \mathbb{N}$, где ζ — примитивный корень степени $2^{\Lambda(N)}$.

В работе [4] был предложен специальный выбор параметров k_i и построены схемы для прямого и обратного УДПФ порядка N, имеющие сложность $1,5N\log_2 N + O(N)$. Объем памяти этих схем (точнее, надлежащим образом перестроенных схем), как отмечено в [3], равен $2^{\Lambda(N)}$. В [3] приведена конструкция схемы с объемом памяти $N+O(1)$, однако большей асимптотической сложности, хотя по порядку и той же самой, $O(N\log N)$.

В работе [5] предложено в качестве точек УДПФ порядка N выбирать корни многочленов $x^{2^i}+1$ суммарной степени N.

Для дальнейшего изложения введем понятие *нечетного ДПФ* (*НДПФ*) *порядка* N:

$$\text{НДПФ}_{N,\zeta} : \mathbf{K}[x]/(x^N+1) \to \mathbf{K}^N : \Gamma(x) \to \left(\Gamma(\zeta^1), \Gamma(\zeta^3), \ldots, \Gamma(\zeta^{2N-1})\right),$$

где ζ — примитивный корень степени $2N$. Другими словами, компонентами НДПФ порядка N являются компоненты ДПФ порядка $2N$, отличные от компонент ДПФ порядка N. Простой способ реализации $\text{НДПФ}_{N,\zeta}$ состоит в композиции замены переменной $x \to \zeta x$ и $\text{ДПФ}_{N,\zeta^2}$. Соответственно, обратное НДПФ можно реализовать как композицию $\text{ДПФ}^{-1}_{N,\zeta^2}$ и замены переменной $x \to x/\zeta$.

Пусть $N = 2^{n_1} + \ldots + 2^{n_s}$, где $n_1 > \ldots > n_s$. Тогда УДПФ порядка N в [5] задается набором отображений $\text{НДПФ}_{2^{n_i},\,\zeta^{2^{\Lambda(N)-n_i}}}$, $1 \le i \le s$.

Схемы УДПФ, построенные в [5], имеют несколько меньшую сложность (в члене $O(N)$), чем схемы из [4], но такой же объем памяти (сложность можно еще немного понизить, используя результаты [2]).

В действительности, УДПФ [5] можно реализовать схемой сложности $1,5N\log_2 N + O(N)$ и объема памяти $N+1$ (или N, см. выше). Это является улучшением результата [3] и вытекает из следующего утверждения.

Пусть в нашем распоряжении есть схемы для НДПФ порядка 2^k сложности $\Phi(k)$ и объема памяти $v_\Phi(k)$, а также схемы для обратных НДПФ порядка 2^k сложности $\Phi'(k)$ и объема памяти $v'_\Phi(k)$.

Теорема 1. *УДПФ порядка N можно реализовать схемой сложности $8N - 5\cdot 2^{n_1} + \sum_i \Phi(n_i)$ и объема памяти $N + \max_i\{v_\Phi(n_i) - 2^{n_i}\}$.*

Обратное УДПФ порядка N можно реализовать схемой сложности $6N - 2^{n_1+2} + \sum_i \Phi'(n_i)$ и объема памяти $N + \max_i\{v'_\Phi(n_i) - 2^{n_i}\}$.

В доказательстве используются эффективные с точки зрения сложности и объема памяти схемы, реализующее одновременное приведение по модулям многочленов $x^{2^{n_i}}+1$ и наоборот: восстановление многочлена, имеющего заданные остатки от деления на многочлены $x^{2^{n_i}}+1$. Вопрос о минимизации сложности и глубины таких схем рассматривался в [2].

Аналогичным образом получается следующий результат. Пусть имеются схемы для умножения многочленов по модулям $x^{2^k}+1$ с коэффициентами над кольцом, в котором обратим элемент 2. Сложность и объем памяти таких схем обозначим через $M(k)$ и $v_M(k)$ соответственно.

Теорема 2. *Умножение многочленов суммарной степени* $N-1$ *можно реализовать схемой сложности* $22N - 14 \cdot 2^{n_1} + \sum_i M(n_i)$ *и объема памяти* $2N + \max_i\{v_M(n_i) - 2^{n_i+1}\}$.

Автор благодарен научному руководителю С. Б. Гашкову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ, проекты 11–01–00508 и 11–01–00792–а, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд. МГУ, 1984.
2. Сергеев И. С. Регуляризация некоторых оценок сложности умножения многочленов // Материалы VII молодежной научной школы по дискретной математике и ее приложениям (Москва, 18–23 мая 2009 г.). — Часть II. — М.: Изд-во Института прикладной математики РАН. — 2009. — С. 26–32.
3. Harvey D., Roche D. S. An in-place truncated Fourier transform and application to polynomial multiplication // Proc. ISSAC 2010 (Munich, Germany). — NY: ACM Press, 2010. — P. 325–329.
4. Van der Hoeven J. The truncated Fourier transform and applications // Proc. ISSAC 2004 (Santander, Spain). — NY: ACM Press, 2004. — P. 290–296.
5. Mateer T. Fast Fourier algorithms with applications // Ph. D. Thesis. — Clemson University, 2008.

О РАЗМЕРЕ ЭЛЕМЕНТОВ ТРАНСФОРМИРУЮЩИХ МАТРИЦ ПРИ ПОДОБИИ МАТРИЦ НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

С. В. Сидоров (Нижний Новгород)

Введение

Пусть A и B — две целочисленные матрицы порядка n. Будем говорить, что матрица A подобна матрице B над кольцом целых чисел $\mathbf{Z}$, если существует такая матрица $X \in \mathbf{Z}^{n\times n}$, что $B = X^{-1}AX$ и $\det X \in \{1, -1\}$. Матрица X называется трансформирующей матрицей. Случай матриц второго порядка подробно разбирается в [1].

Основная цель доклада — показать, что элементы минимальной трансформирующей матрицы могут субэкспоненциально зависеть от элементов исходных матриц.

1. Вспомогательная лемма

Обозначим через $\Lambda_{A,B}$ множество целочисленных матриц X, удовлетворяющих условию $AX = XB$. Если матрицы A и B размера 2×2 имеют одинаковый характеристический многочлен, который неприводим над $\mathbf{Q}$, то $\Lambda_{A,B}$ является двумерным модулем. Пусть T_1 и T_2 — базис $\Lambda_{A,B}$. Тогда любая трансформирующая матрица имеет вид $xT_1 + yT_2$ для некоторых целых x и y. Определитель матрицы $xT_1 + yT_2$ является бинарной квадратичной формой относительно x и y, поэтому существование трансформирующей матрицы в этом случае эквивалентно разрешимости в целых числах уравнения $ax^2 + bxy + cy^2 = \pm 1$, частным случаем которого является уравнение Пелля $x^2 - Dy^2 = \pm 1$ (предполагаем, что D не является полным квадратом). Уравнение $x^2 - Dy^2 = 1$ для любого D имеет положительные решения. В свою очередь, уравнение $x^2 - Dy^2 = -1$ не для всех D имеет положительные решения. Если $D = p$ — простое число, то при условии $p \equiv 1 \pmod 4$ это уравнение имеет положительные решения, а при условии $p \equiv 3 \pmod 4$ не имеет положительных решений. Следующая лемма показывает некоторые свойства решений уравнения $x^2 - Dy^2 = \pm 1$, если D — нечетная степень простого числа.

Лемма. *Пусть p — простое число и (x_k, y_k) — минимальное положительное решение уравнения Пелля*

$$x^2 - p^{2k+1}y^2 = \pm 1, k \geq 0.$$

Если y_0 не делится на p, то

1) $x_k + p^k y_k \sqrt{p} = (x_0 + y_0\sqrt{p})^{p^k}, k \geq 0$;

2) $x_k \equiv x_0 \pmod p, k \geq 0$;

3) *если* $p \neq 3$, *то* $y_k \equiv y_0 \pmod p$; *если* $p = 3$, *то* $y_0 = 1$, $y_k \equiv 2 \pmod 3, k \geq 1$.

Доказательство. Индукция по k. При $k = 0$ очевидно. Если (x_k, y_k) — минимальное положительное решение уравнения $x^2 - p^{2k+1}y^2 = \pm 1$, то (x_k, py_k) — некоторое решение уравнения $x^2 - p^{2k-1}y^2 = \pm 1$. Но все положительные решения (u_n, v_n) уравнения Пелля $x^2 - p^{2k-1}y^2 = \pm 1$ удовлетворяют условию $u_n + p^{k-1}v_n\sqrt{p} = (x_{k-1} + p^{k-1}y_{k-1}\sqrt{p})^n, n \geq 0$. Следовательно, нужно найти такое минимальное n, что $v_n \equiv 0 \pmod p$. Тогда $(x_k, y_k) = (u_n, v_n/p)$ будет минимальным решением для уравнения $x^2 - p^{2k+1}y^2 = \pm 1$. По формуле бинома Ньютона получаем

$$u_n = x_{k-1}^n + \binom{n}{2} p^{2k-1} x_{k-1}^{n-2} y_{k-1}^2 + \binom{n}{4} p^{4k-2} x_{k-1}^{n-4} y_{k-1}^4 + \ldots + \binom{n}{n} p^{\frac{n}{2}(2k-1)} y_{k-1}^n,$$

$$p^{k-1}v_n = \binom{n}{1}p^{k-1}x_{k-1}^{n-1}y_{k-1} + \binom{n}{3}p^{3k-2}x_{k-1}^{n-3}y_{k-1}^3 + \ldots + \\ + \binom{n}{n-1}p^{(2k-1)\frac{n-2}{2}}x_{k-1}y_{k-1}^{n-1},$$

если n — четное и

$$u_n = x_{k-1}^n + \binom{n}{2}p^{2k-1}x_{k-1}^{n-2}y_{k-1}^2 + \binom{n}{4}p^{4k-2}x_{k-1}^{n-4}y_{k-1}^4 + \ldots + \\ + \binom{n}{n-1}p^{(2k-1)\frac{n-1}{2}}x_{k-1}y_{k-1}^{n-1},$$

$$p^{k-1}v_n = \binom{n}{1}p^{k-1}x_{k-1}^{n-1}y_{k-1} + \binom{n}{3}p^{3k-2}x_{k-1}^{n-3}y_{k-1}^3 + \ldots + \binom{n}{n}p^{(2k-1)\frac{n-1}{2}}y_{k-1}^n,$$

если n — нечетное.

Так как мы ищем минимальное n, для которого $v_n \equiv 0 \pmod p$, то $nx_{k-1}^{n-1}y_{k-1} \equiv 0 \pmod p$. Очевидно, что $x_{k-1} \not\equiv 0 \pmod p$. По предположению индукции $y_{k-1} \equiv y_0 \pmod p$, если $p \neq 3$. Значит, $y_{k-1} \not\equiv 0 \pmod p$. В случае $p = 3$ имеем $y_{k-1} \equiv 1 \pmod 3$ при $k = 1$ и $y_{k-1} \equiv 2 \pmod 3$ при $k > 1$. В любом случае $y_{k-1} \not\equiv 0 \pmod 3$. Значит, $n \equiv 0 \pmod p$ и минимальное n равно p. Тем самым, доказано, что $x_k + p^k y_k\sqrt{p} = (x_{k-1} + p^{k-1}y_{k-1}\sqrt{p})^p$. По предположению индукции имеем $x_{k-1} + p^{k-1}y_{k-1}\sqrt{p} = (x_0 + y_0\sqrt{p})^{p^{k-1}}$. Используя предыдущее равенство, немедленно получаем доказываемое в пункте 1).

Далее, $x_k = u_p \equiv x_{k-1}^p \equiv x_{k-1} \equiv x_0 \pmod p$. Последнее сравнение имеет место по предположению индукции. Этим доказан второй пункт леммы.

Теперь

$$y_k = v_p/p = x_{k-1}^{p-1}y_{k-1} + C_p^3 p^{2k-2}x_{k-1}^{p-3}y_{k-1}^3 + C_p^5 p^{4k-3}x_{k-1}^{p-5}y_{k-1}^5 \ldots \equiv \\ \equiv x_{k-1}^{p-1}y_{k-1} + C_p^3 p^{2k-2}x_{k-1}^{p-3}y_{k-1}^3 \pmod p.$$

Откуда $y_k \equiv y_{k-1} \pmod p$, если $p \neq 3$. Если же $p = 3$, то

$$y_1 \equiv y_0 + y_0^3 = 1 + 1^3 = 2 \pmod 3$$

и $y_k \equiv y_{k-1} \pmod 3, k \geq 2$. Используя предположение индукции, получаем $y_k \equiv y_0 \pmod p$, если $p \neq 3$ и $y_k \equiv 2 \pmod 3, k \geq 1$ если $p = 3$. Третий пункт леммы доказан.

Предположение о том, что y_0 не делится на p, известно как гипотеза Ankeny—Artin—Chowla (см. [2]). На данный момент не найдено контрпримеров к данной гипотезе.

2. Пример минимальной трансформирующей матрицы с субэкспоненциальной нормой

Пусть p — простое число, $p \equiv 1 \pmod 4$. Тогда уравнение $x^2 - py^2 = -1$ разрешимо в положительных x и y (см. [3]), причем x — четное число. Действительно, $y^2 \equiv x^2 + 1 \pmod 4$. Если бы x было нечетным, то $x^2 \equiv 1 \pmod 4$

и $y^2 \equiv 2 \pmod 4$. Но последнее сравнение не имеет решений. Таким образом, x — четное.

Рассмотрим матрицы

$$A = \begin{pmatrix} 0 & 4 \\ p^{2k+1} & 0 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 1 \\ 4p^{2k+1} & 0 \end{pmatrix}.$$

Базис модуля $\Lambda_{A,F}$ образуют матрицы

$$T_1 = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 & 1 \\ p^{2k+1} & 0 \end{pmatrix}.$$

Тогда любая трансформирующая матрица S будет иметь вид $S = xT_1 + yT_2$. Далее $\det S = \det(xT_1 + yT_2) = \det \begin{pmatrix} 4x & y \\ p^{2k+1}y & x \end{pmatrix} = 4x^2 - p^{2k+1}y^2$. Уравнение $4x^2 - p^{2k+1}y^2 = \pm 1$ для любого натурального k имеет целочисленные решения, если разрешимо уравнение $4x^2 - py^2 = \pm 1$. Обозначим через (x_k, y_k) минимальное решение уравнения $4x^2 - p^{2k+1}y^2 = \pm 1$, $k \geq 0$. Тогда $(2x_k, y_k)$ — минимальное положительное решение уравнения $x^2 - p^{2k+1}y^2 = \pm 1$. Следовательно, согласно лемме

$$2x_k + p^k y_k \sqrt{p} = (2x_0 + y_0\sqrt{p})^{p^k}.$$

Рассмотрим матричную норму $||A|| = \max\limits_{i,j}\{|a_{ij}|\}$. Тогда выполняются равенства $||A|| = p^{2k+1}$, $||F|| = 4p^{2k+1}$, $||S|| = \max\{p^{2k+1}y, 4x\}$. Поскольку $4x_k > 2(2x_0)^{p^k}$, $p^{2k+1}y_k > y_0^{p^k}\sqrt{p}^{p^k+2k+1}$, то для нормы минимальной трансформирующей матрицы S_k верно равенство $\log ||S_k|| = O(\sqrt{||A||})$. Тем самым доказана следующая теорема.

Теорема. *Существуют подобные над кольцом целых чисел матрицы A и B, для которых норма минимальной трансформирующей матрицы субэкспоненциально зависит от норм исходных матриц.*

Работа выполнена при поддержке РФФИ, проект № 09-01-00545-а.

Список литературы

1. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел // Известия ВУЗ. Математика. — 2006. — № 4. —С. 57–64.
2. Ankeny N. C. , Artin E. , Chowla S. The Class-Number of Real Quadratic Number Fields // The Annals of Mathematics, Second Series. — 1952. — Vol. 56. — No. 3. — Pp. 479–493
3. Lagarias J. C. On the Computational Complexity of Determining the Solvability or Unsolvability of the Equation $X^2 - DY^2 = -1$ // Transactions of the American Mathematical Society. — 1980. — Vol. 260. — No. 2. — Pp. 485–508

О ПРЕДСТАВЛЕНИИ ОГРАНИЧЕНИЙ, ЗАПИСАННЫХ С ПОМОЩЬЮ SQL, ДЛЯ ПОСТРОЕНИЯ ВОССТАНОВЛЕНИЙ БАЗ ДАННЫХ.

Е. Е. Трифонова (Москва)

Основные определения

Схемой базы данных будем называть некое конечное множество предикатов $\mathbb{P}$ и множество ограничений, записанных в виде формулы Φ. *Базой данных* D будем называть совокупность таблиц $\mathbb{T}$ и формулы $\Phi : D = \langle \mathbb{T}, \Phi \rangle$. При этом каждом предикату P из множества предикатов $\mathbb{P}$ ставится в соответствие таблица T из $\mathbb{T}$, которая определяет значение истинности предиката. Элементом таблицы является *кортеж*.

Будем обозначать множество кортежей, которые присутствуют в таблице T, как X_T, а множество кортежей, которые присутствуют в базе D, как $X = X(D)$, $X = \bigcup\limits_{T \in \mathbb{T}} X_T$. Определим множество функций $F : X \to \mathbb{N}$, где $\mathbb{N}$ — множество натуральных чисел. *Вспомогательным предикатом* от двух переменных $g(x_1, x_2)$ будем называть выражение вида $(f_i(x_1)\mathcal{R}f_j(x_2))$, где $f_i, f_j \in F$, а $\mathcal{R}$ — одно из отношений $<, >, \leqslant, \geqslant, \neq, =$. Пусть G — множество всевозможных вспомогательных предикатов.

Для сокращения записи будем называть *вспомогательным условием* и обозначать как $h(x_1, \ldots, x_n)$ формулу, построенную следующим образом:

$$h(x_1, \ldots, x_n) = g_1(x_{i_1}, x_{j_1}) \Diamond g_2(x_{i_2}, x_{j_2}) \Diamond \ldots \Diamond g_k(x_{i_k}, x_{j_k}),$$

где $i_1, \ldots, i_k, j_1, \ldots, j_k \in \{1, \ldots, n\}$, $g_1, g_2, \ldots, g_k \in G$, $\Diamond$ — место размещения логических операторов & и $\vee$.

В качестве формулы-ограничения Φ будем рассматривать замкнутые формулы на языке первого порядка, записанные с использованием связок $\vee$, &, $\neg$, $\to$, предикатов из $\mathbb{P}$ и вспомогательных предикатов из G. Переменные принимают значения из множества кортежей X. Если формула Φ истинна на множестве X, то базу данных D будем называть *непротиворечивой*. Если все таблицы базы данных пусты, то считаем, что любая формула Φ, удовлетворяющая вышеуказанным условиям, истинна.

Если формула Φ ложна на множестве X, то будем говорить, что в базе данных D содержатся противоречия. Устранять противоречия будем посредством удаления кортежей из базы данных. *Восстановлением* Q для базы данных D будем называть базу данных, для которой выполняется следующее: схемы баз данных Q и D совпадают; каждый кортеж из таблицы Q содержится в соответствующей таблице D; база данных Q не содержит противоречий; добавление к Q любого кортежа из D, который в Q не содержится, в соответствующую таблицу приводит к тому, что в Q возникают противоречия.

Будем обозначать как Z_Q множество кортежей, удалённых из D для получения восстановления Q: $Z_Q = X(D) \setminus X(Q)$. Для каждой базы, содержащей противоречия, существует некоторое множество восстановлений. Те из них, которые содержат наибольшее число кортежей, будем называть *наилучшими восстановлениями*. Множество наилучших восстановлений для базы D будем обозначать как $\mathbb{Q}_{max} = \mathbb{Q}_{max}(D)$.

Выражение ограничений SQL через формулы

Рассмотрим, как можно записать формулы-ограничения, задаваемые конструкциями в SQL, в виде формул с использованием предикатов из $\mathbb{P}$ и G. В SQL поддерживаются следующие конструкции для описания ограничений целостности: UNIQUE, NOT NULL, CHECK, PRIMARY KEY, FOREIGN KEY и REFERENCES. Будем считать, что функции $f_i(x)$ отображают соответствующую i-ю компоненту кортежа в число; C_j и C_{NULL} — будем использовать для обозначения констант из $\mathbb{N}$. Кроме того, будем считать, что рассматриваем первые четыре ограничения для первого элемента кортежа.

UNIQUE:

$$\forall x_1 \forall x_2 (P(x_1) \& P(x_2) \to h(x_1, x_2)),$$

где

$$h(x_1, x_2) = (f_1(x_1) = f_1(x_2)) \& (f_2(x_1) = f_2(x_2)) \& \ldots \& (f_k(x_1) = f_k(x_2)) \vee \\ \vee (f_1(x_1) \neq f_1(x_2)).$$

NOT NULL:

$$\forall x_1 (P(x_1) \to h(x_1)),$$

где $h(x_1) = (f_1(x_1) \neq C_{NULL})$.

CHECK:

$$\forall x_1 (P(x_1) \to h(x_1)),$$

где $h(x_1) = (f_1(x_1) \leqslant C_1), C_1$ — некая константа, обуславливающая правило, вместо $\leqslant$ может стоять любой из символов $<, >, \leqslant, \geqslant, \neq, =$.

PRIMARY KEY:

$$\forall x_1 (P(x_1) \to h_1(x_1)) \& \& \forall x_2 \forall x_3 (P(x_2) \& P(x_3) \to h_2(x_2, x_3)),$$

где $h_1(x_1) = (f_1(x_1) \neq C_{NULL})$,

$$h_2(x_2, x_3) = (f_1(x_1) = f_1(x_2)) \& (f_2(x_1) = f_2(x_2)) \& \ldots \& (f_k(x_1) = f_k(x_2)) \vee \\ \vee (f_1(x_1) \neq f_1(x_2)).$$

FOREIGN KEY и REFERENCES (T^1 — родительская таблица, T^2 — дочерняя таблица, используется инструкция CASCADE или NO ACTION):

$$\begin{gathered} \forall x_1 \exists x_2 (P_2(x_1) \to P_1(x_2) \& h_1(x_1, x_2)) \& \\ \& \forall x_3 (P_1(x_3) \to h_2(x_3)) \& \\ \& \forall x_4 \forall x_5 (P_1(x_4) \& P_1(x_5) \to h_3(x_4, x_5)) \& \\ \& \forall x_6 (P_2(x_6) \to h_4(x_6)) \& \\ \& \forall x_7 \forall x_8 (P_2(x_7) \& P_2(x_8) \to h_5(x_7, x_8)), \end{gathered}$$

где

$h_1(x_1, x_2) = (f_1(x_1) = f_1(x_2))$,
$h_2(x_3) = (f_1(x_3) \neq C_{NULL})$,
$h_3(x_4, x_5) = (f_1(x_4) = f_1(x_5))\&(f_2(x_4) = f_2(x_5))\& \ldots \&(f_k(x_4) = f_k(x_5)) \vee$
$\vee(f_1(x_4) \neq f_1(x_5))$,
$h_4(x_6) = (f_1(x_6) \neq C_{NULL})$,
$h_5(x_7, x_8) = (f_1(x_7) = f_1(x_8))\&(f_2(x_7) = f_2(x_8))\& \ldots \&(f_k(x_7) = f_k(x_8)) \vee$
$\vee(f_1(x_7) \neq f_1(x_8))$.

FOREIGN KEY и REFERENCES (инструкция SET DEFAULT):

$$(\forall x_1 \exists x_2 (P_2(x_1) \to P_1(x_2)\&h_1(x_1, x_2)) \vee (\forall x_1 P_2(x_1) \to h_2(x_1)))\& \\ \&\forall x_3 (P_1(x_3) \to h_3(x_3))\& \\ \&\forall x_4 \forall x_5 (P_1(x_4)\&P_1(x_5) \to h_4(x_4, x_5))\& \\ \&\forall x_6 (P_2(x_6) \to h_5(x_6))\& \\ \&\forall x_7 \forall x_8 (P_2(x_7)\&P_2(x_8) \to h_6(x_7, x_8)),$$

где

$h_1(x_1, x_2) = (f_1(x_1) = f_1(x_2))$,
$h_2(x_1) = (f_1(x_1) = C_2)$,
$h_3(x_3) = (f_1(x_3) \neq C_{NULL})$,
$h_4(x_4, x_5) = (f_1(x_4) = f_1(x_5))\&(f_2(x_4) = f_2(x_5))\& \ldots \&(f_k(x_4) = f_k(x_5)) \vee$
$\vee(f_1(x_4) \neq f_1(x_5))$,
$h_5(x_6) = (f_1(x_6) \neq C_{NULL})$,
$h_6(x_7, x_8) = (f_1(x_7) = f_1(x_8))\&(f_2(x_7) = f_2(x_8))\& \ldots \&(f_k(x_7) = f_k(x_8)) \vee$
$\vee(f_1(x_7) \neq f_1(x_8)) \vee (f_1(x_7) = C_2)\&(f_1(x_8) = C_2)$.

В случае инструкции SET NULL часть $\forall x_6(P_2(x_6) \to h_5(x_6))$ отсутствует, а C_2 везде в условиях заменяется на C_{NULL}.

Таким образом получаем, что данные формулы могут быть получены из базисных формул следующих трёх видов:

$$\forall x(P(x) \to h(x)) \tag{1}$$

$$\forall x_1 \forall x_2 (P(x_1)\&P(x_2) \to h(x_1, x_2)) \tag{2}$$

$$\forall x_1 \exists x_2 (P_1(x_1) \to P_2(x_2)\&h(x_1, x_2)) \tag{3}$$

Построение наилучшего восстановления для некоторых формул

Будем называть классом A множество конечных формул, построенных из формул вида (1), (2), (3), соединённых конъюнкцией и дизъюнкцией, где $P, P_1, P_2 \in \mathbb{P}$ и h, h_1 - вспомогательные условия, построенные по приведённым выше правилам с использованием вспомогательных предикатов из G.

Пусть задана формула Φ и требуется построить наилучшее восстановление $Q_{max} \in \mathbb{Q}_{max}$. Рассмотрим его построение для некоторых формул из класса A.

Утверждение 1. *Пусть* $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ *— соответствующие им таблицы,* $\Phi = \forall x_1(P_1(x_1) \to h_1(x_1))\& \ldots \&\forall x_n(P_n(x_n) \to h_n(x_n))$.

Тогда $X(Q_{max}) = \bigcup\limits_{i=1}^{n} \{x|(x \in T_i)\&(h_i(x) = 1)\}$.

Доказательство. Формула Φ представляет собой конъюнкцию элементарных формул вида (1) и фактически означает, что в таблице каждого из предикатов P_i должны содержаться данные, которые удовлетворяют записанному условию. Если какой-то кортеж ему не удовлетворяет, то его надо удалить.

Утверждение 2. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ *— соответствующие им таблицы,*

$$\Phi = \forall x_1(P_1(x_1) \to h_1(x_1)) \vee \forall x_1(P_2(x_2) \to h_2(x_2)) \vee \ldots \vee \forall x_n(P_n(x_n) \to h_n(x_n)).$$

Для каждого $i = 1, \ldots, n$ *положим* $D_i = \langle \mathbb{T}, \Phi_i \rangle$, *где* $\Phi_i = \forall x_i(P_i(x_i) \to h_i(x_i))$. *Тогда* $X(Q_{max}(D))$ *будет равно тому из множеств* $X(Q_{max}(D_i))$, $i = 1, \ldots, n$, *где содержится больше кортежей.*

Доказательство. Формула Φ представляет собой дизъюнкцию элементарных формул вида (1). Если эта формула ложна, то чтобы сделать её истинной, необходимо, чтобы хотя бы одно из слагаемых стало равным «истине». Поскольку нам нужно наилучшее восстановление, то надо сделать истинным то слагаемое, для которого это можно сделать с минимальным числом удалений.

Утверждение 3. *Пусть* $P_1, P_2 \in \mathbb{P}$, T_1, T_2 *— таблицы, соответствующие* P_1, P_2, $\Phi = \forall x_1 \exists x_2(P_1(x_1) \to P_2(x_2)\&h(x_1, x_2))$.

Тогда $Z_{Q_{max}} = \{x|(x \in T_1)$ *и для всех* $y \in T_2$ $h(x, y) = 0\}$, *если таблица* T_2 *— не пустая,* $Z_{Q_{max}} = X_{T_1}$, *если* T_2 *— пустая.*

Доказательство. Возникновение противоречий для данной формулы может быть из-за того, что для какого-либо кортежа из P_1 нет такого кортежа из P_2, чтобы условие выполнялось, соответственно, надо удалить все такие кортежи из P_1. Если же P_2 — пустая, то тогда необходимо удалить все кортежи из P_1.

Работа выполнена при финансовой поддержке РФФИ (грант 11-01-00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Трифонова Е. Е. О построении восстановлений баз данных для некоторых классов формул-ограничений // Материалы XVI Межд. конф. «Проблемы теоретической кибернетики» (Нижний Новгород, 20–25 июня 2011 г.). Нижний Новгород: Изд-во Нижегородского гос. ун-та, 2011. — С. 477–481.

2. Chomicki J., Marchinkowski J. Minimal-change integrity maintenance using tuple deletion // Inf. Comput. 197 (1–2), 90–121, 2005.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ СХЕМАМИ КОМПОЗИЦИИ СИСТЕМ ИЗ ДВУХ МОНОМОВ ОТ ДВУХ ПЕРЕМЕННЫХ

Е. Н. Трусевич (Москва)

В работе исследуется сложность вычисления мономов с помощью операции композиции при возможности многократного использования значений промежуточных вычислений.

Под мономом над множеством переменных $\mathcal{X} = \{x_1, x_2, \dots x_q\}$, $q \geq 1$, будем понимать выражение вида $x_1^{a_1} x_2^{a_2} \dots x_q^{a_q}$, где a_i — целые неотрицательные числа, $\sum_{i=1}^{q} a_i > 0$.

Следуя А. И. Ширшову [1], введем понятие композиции мономов. Пусть $U = x_1^{a_{11}} \dots x_q^{a_{1q}}$, $V = x_1^{a_{21}} \dots x_q^{a_{2q}}$ — произвольные мономы над множеством переменных $\mathcal{X}$ и задан моном $R = x_1^{r_1} \dots x_q^{r_q}$, где $0 \leq r_i \leq \min(a_{1i}, a_{2i})$, $1 \leq i \leq q$ (отметим, что в отличие от остальных мономов, для выражения R может быть выполнено условие $\sum_{i=1}^{q} r_i = 0$, однако будем в дальнейшем называть его мономом). *Композицией* мономов U и V относительно монома R называется моном $x_1^{a_{11}+a_{21}-r_1} \dots x_q^{a_{1q}+a_{2q}-r_q}$, который будем обозначать через $(U, V)_R$.

Последовательность S, состоящая из мономов

$$X_1, \dots, X_q, X_{q+1}, \dots, X_{q+n}, \tag{1}$$

называется *схемой композиции для монома* X_{q+n}, если эта последовательность удовлетворяет условиям:

1) для $i = 1, \dots, q$ выполняется равенство $X_i = x_i$;

2) для $i = q+1, \dots, q+n$ найдутся s и t, не превосходящие $i-1$, а также моном R_i, такие что $X_i = (X_s, X_t)_{R_i}$.

Под *сложностью* $L_{sh}(S)$ схемы композиции вида (1) понимается число n.

Схемой композиции для системы мономов

$$\mathcal{A} = \{x_1^{a_{11}} \dots x_q^{a_{1q}}, \dots, x_1^{a_{p1}} \dots x_q^{a_{pq}}\}$$

назовем схему композиции S для некоторого монома из системы $\mathcal{A}$, которая содержит в качестве элементов остальные мономы из множества $\mathcal{A}$.

Положим $L_{sh}(\mathcal{A}) = \min L_{sh}(S)$, где минимум берется по всем схемам композиции для системы $\mathcal{A}$. Величину $L_{sh}(\mathcal{A})$ назовем *сложностью системы мономов* $\mathcal{A}$. Система мономов $\mathcal{A}$ полностью определяется матрицей показателей степеней

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1q} \\ \vdots & & & \vdots \\ a_{p1} & a_{p2} & \dots & a_{pq} \end{pmatrix}.$$

Поэтому можно говорить не только о сложности $L_{sh}(\mathcal{A})$ вычисления системы $\mathcal{A}$, но и о *сложности* $L_{sh}(A)$ *матрицы* A, задающей эту систему. Далее не будем различать эти понятия и будем считать, что $L_{sh}(A) = L_{sh}(\mathcal{A})$.

Понятие схемы композиции можно проинтерпретировать на языке схем из функциональных элементов [2–3].

Ранее Ю. В. Мерекиным был исследован [4] случай вычисления системы мономов, состоящей из одного монома. Он установил, что

$$L_{sh}(x_1^{a_1} \dots x_q^{a_q}) = \lceil \log a \rceil + q - 1, \text{ где } a = \max(a_1 \dots a_q)$$

(здесь и далее под $\log x$ понимается $\log_2 x$). В данной работе изучается сложность реализации схемами композиции системы из двух мономов от двух переменных.

Теорема 1. *Пусть в целочисленной матрице*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

с неотрицательными элементами нет нулевых строк и столбцов, а минимальным элементом матрицы A *является элемент* c. *Тогда*

$$L_{sh}(A) = \lceil \log d \rceil + \left\lceil \log \max \left(\frac{a}{\max(c,1)}, \frac{b}{d} \right) \right\rceil + \operatorname{sgn} b + \gamma(A),$$

где $\gamma(A) \in \{0,1\}$, *причем* $\gamma(A) = 0$ *при* $b = 0$ *или* $b \geq d$.

Для доказательства теоремы сформулируем четыре вспомогательных утверждения — две леммы для доказательства верхней оценки и две леммы для доказательства нижней оценки. Отметим, что при доказательстве нижних оценок схем композиции будем использовать язык схем из функциональных элементов.

Лемма 1. *Пусть схема* S_0 *является схемой композиции для монома* $x^{a_0}y^{b_0}$, *где* $a_0 b_0 \neq 0$. *Тогда для вычисления монома* $x^a y^b$, *где* $\frac{a}{a_0} \geq \frac{b}{b_0} \geq 1$, *можно построить схему композиции* S, *добавив к последовательности* S_0 *не более* $\left\lceil \log \frac{a}{a_0} \right\rceil$ *членов, т. е.* $L_{sh}(S) - L_{sh}(S_0) \leq \left\lceil \log \frac{a}{a_0} \right\rceil$.

Лемма 2. *Пусть* $d \neq 0$. *Тогда справедливо неравенство*

$$L_{sh} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \leq \lceil \log d \rceil + \left\lceil \max \left(\log a, \log \frac{b}{d} \right) \right\rceil + 2.$$

Лемма 3. *Пусть в схеме композиции* S, *вычисляющей моном* $x^a y^b$, *где* $a \geq 1$, $b \geq 1$ *в некоторой вершине* v_0 *вычисляется моном* $x^{a_0}y^{b_0}$, *где* $a \geq a_0$. *Тогда для подсхемы* S_0, *которая содержит только те вершины, от которых есть ориентированный путь к вершине* v_0, *справедливо неравенство*

$$L_{sh}(S) - L_{sh}(S_0) \geq \left\lceil \log \frac{a}{\max(a_0, 1)} \right\rceil + 1 - \operatorname{sgn}(\min(a_0, b_0)).$$

Лемма 4. *Пусть* $ad \neq 0$. *Тогда справедливо неравенство*

$$L_{sh}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \geq \lceil \log d \rceil + \left\lceil \log \max\left(a, \frac{b}{d}\right) \right\rceil + \operatorname{sgn} b.$$

Доказательство теоремы. *Верхняя оценка.* Построим схему композиции, вычисляющую матрицу $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. При $c = 0$ утверждение теоремы напрямую следует из леммы 2. Далее считаем, что $c \geq 1$. Рассмотрим несколько случаев.

Случай 1. Пусть $b \geq d$. Тогда $L_{sh}(x^c y^d) = \lceil \log d \rceil + 1$ и применима лемма 1.

Случай 1.1. Пусть $\frac{a}{c} \geq \frac{b}{d}$. Тогда моном $x^a y^b$ можно получить из монома $x^c y^d$, используя не более чем $\left\lceil \log \frac{a}{c} \right\rceil$ операций композиции.

Случай 1.2. Пусть $\frac{a}{c} \leq \frac{b}{d}$. Аналогично получаем, что моном $x^a y^b$ можно вычислить за не более чем $\left\lceil \log \frac{b}{d} \right\rceil$ операций.

Следовательно, в случае 1 получаем оценку:

$$L_{sh}(A) \leq \lceil \log d \rceil + \left\lceil \max\left(\log \frac{a}{c}, \log \frac{b}{d}\right) \right\rceil + 1.$$

Случай 2. Пусть $b < d$. По теореме 2 из [4] получаем, что

$$L_{sh}(x^c y^b) = \lceil \log b \rceil + 1.$$

Используя лемму 1, получаем, что моном $x^a y^b$ можно получить из монома $x^c y^b$ за не более, чем $\left\lceil \log \frac{a}{c} \right\rceil$ операций, а моном $x^c y^d$ за не более, чем $\left\lceil \log \frac{d}{b} \right\rceil$ операций композиции. Следовательно,

$$L_{sh}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \leq \lceil \log b \rceil + \left\lceil \log \frac{a}{c} \right\rceil + \left\lceil \log \frac{d}{b} \right\rceil + 1 \leq \lceil \log d \rceil + \left\lceil \log \frac{a}{c} \right\rceil + 2.$$

Таким образом,

$$L_{sh}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \leq \lceil \log d \rceil + \max\left(\left\lceil \log \frac{a}{\max(c,1)} \right\rceil, \left\lceil \log \frac{b}{d} \right\rceil\right) + 2.$$

Верхняя оценка доказана.

Нижняя оценка. При $c = 0$ утверждение теоремы следует из леммы 4. Далее считаем, что $c \geq 1$. Пусть S — минимальная схема из элементов композиции, вычисляющая мономы $x^a y^b$ и $x^c y^d$. Выберем подсхему S_0 так, чтобы в нее входили все вершины, от которых есть ориентированный путь до вершины, в которой вычисляется моном $x^c y^d$. Тогда $L_{sh}(S_0) \geq L_{sh}(x^c y^d) = \lceil \log d \rceil + 1$, так как $d \geq c$. Поскольку $\frac{a}{c} \geq 1$, то применима лемма 3. Соответственно,

$$L_{sh}(S) - L_{sh}(S_0) \geq \left\lceil \log \max\left(\frac{b}{d}, \frac{a}{c}\right) \right\rceil.$$

Поэтому

$$L_{sh}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = L_{sh}(S) \geq \lceil \log d \rceil + \left\lceil \log \max\left(\frac{b}{d}, \frac{a}{c}\right)\right\rceil + 1.$$

Теорема 1 доказана.

Теперь приведем полученный в теореме 1 результат к стандартному симметричному относительно элементов матрицы виду. Обозначим через $D(A)$ максимальный по модулю минор матрицы A.

Лемма 5. *Пусть* $1 \leq c = \min(a, b, c, d)$. *Тогда выполнены неравенства*

$$0 \leq \log d + \max \log\left(\frac{a}{c}, \frac{b}{d}\right) - \left(\log c + \log D\begin{pmatrix} a/c & b/c \\ 1 & d/c \end{pmatrix}\right) \leq 1.$$

Доказательство. Очевидно, что утверждение леммы эквивалентно неравенствам

$$0 \leq \log \max\left(\frac{ad}{c}, b\right) - \log \max\left(a, b, c, d, \left|\frac{ad-bc}{c}\right|\right) \leq 1.$$

Обозначим $\log \max\left(\frac{ad}{c}, b\right)$ через α, а $\log \max\left(a, b, c, d, \left|\frac{ad-bc}{c}\right|\right)$ через β. Рассмотрим несколько случаев:

Случай 1. Пусть $bc \geq ad$. Поскольку $c \leq a$ и $c \leq d$, из $bc \geq ad$ следует, что $b \geq a$ и $b \geq d$. Покажем, что $b \geq \left|\frac{ad-bc}{c}\right|$. Действительно, выполняются соотношения $\frac{\left|\frac{ad-bc}{c}\right|}{b} = \frac{bc-ad}{bc} = 1 - \frac{ad}{bc} \leq 1$. Следовательно, $\beta = \log b = \alpha$.

Случай 2. Пусть $ad > bc$.

Случай 2.1. Пусть $\beta = \log a$. Тогда $a \geq b$, $a \geq c$, $a \geq d$ и $a \geq \left|\frac{ad-bc}{c}\right| = \frac{ad-bc}{c}$. Для того, чтобы доказать, что $0 \leq \alpha - \beta \leq 1$ покажем, что $\frac{\frac{ad}{c}}{a} \leq 2$. Действительно, $ac \geq ad - bc$. Следовательно, $bc \geq a(d-c)$. А из этого, учитывая что $a \geq b, a \geq c$, получаем неравенство $\frac{d}{c} \leq 2$.

Случай 2.2. Пусть $\beta = \log b$. Тогда $b \geq a$, $b \geq c$, $b \geq d$ и $b \geq \left|\frac{ad-bc}{c}\right| = \frac{ad-bc}{c}$. Для того, чтобы доказать, что $0 \leq \alpha - \beta \leq 1$ покажем, что $\frac{\frac{ad}{c}}{b} \leq 2$. Действительно, $bc \geq ad - bc$. Следовательно, $\frac{ad}{bc} \leq 2$.

Случай 2.3. Пусть $\beta = \log d$. Тогда $d \geq a$, $d \geq c$, $d \geq b$ и $d \geq \left|\frac{ad-bc}{c}\right| = \frac{ad-bc}{c}$. Для того, чтобы доказать, что $0 \leq \alpha - \beta \leq 1$ покажем, что $\frac{\frac{ad}{c}}{d} \leq 2$. Действительно, $dc \geq ad - bc$. Следовательно, $bc \geq d(a-c)$. А из этого, учитывая что $d \geq b, d \geq c$, получаем неравенство $\frac{a}{c} \leq 2$.

Случай 2.4. Пусть $\beta = \log\left(\frac{ad-bc}{c}\right)$. Тогда $\frac{ad-bc}{c} \geq b$. Для того, чтобы доказать неравенство $0 \leq \alpha - \beta \leq 1$, покажем, что $\frac{ad}{ad-bc} \leq 2$. Действительно, $ad - bc \geq bc$. Следовательно, $bc \leq \frac{1}{2}ad$. Далее получаем $\frac{ad}{ad-bc} \leq \frac{ad}{\frac{1}{2}ad} = 2$.

Таким образом, в случае 2 получаем, что

$$0 \leq \log \frac{ad}{c} - \log \max\left(a, b, c, d, \frac{ad-bc}{c}\right) \leq 1.$$

Лемма 5 доказана.

Теорему 1 в силу леммы 5 можно переформулировать следующим образом.

Теорема 2. *Пусть в целочисленной матрице*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

с неотрицательными элементами нет нулевых строк и столбцов, и пусть $m = \max(\min(a, b, c, d), 1)$. *Тогда*

$$L_{sh}(A) = \log m + \log D \begin{pmatrix} a/m & b/m \\ c/m & d/m \end{pmatrix} + O(1).$$

Список литературы

1. Ширшов А. И. Некоторые алгоритмические проблемы для алгебр Ли // Сиб. матем. журнал. — 1962. — Т. 3. — С. 292–296.
2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматлит, 1963. — С. 63–97.
3. Лупанов О. Б. Конспект лекций по курсу "Введение в математическую логику". — М.: Изд-во мех.-матем. ф-та МГУ, 2007.
4. Мерекин Ю. В. О порождении слов с использованием операции композиции // Дискретн. анализ и исслед. опер. Сер. 1. — 2003. — Т. 10, № 4. — С. 70–78.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ ФОРМУЛАМИ СПЕЦИАЛЬНОГО ВИДА.

Д. В. Трущин (Москва)

Рассматривается задача о реализации функций трехзначной логики α–формулами, т. е. такими формулами, в которых каждая подформула содержит не более одной нетривиальной главной подформулы. В качестве меры сложности формул рассматривается глубина. В работе приводится класс функций, для которого функция Шеннона по глубине над рассматриваемой полной системой с точностью до аддитивной константы равна 2^n. Кроме того получены верхние оценки глубины произвольной функции над указанной системой.

Пусть $k \geq 2$, $n \geq 1$. Через P_k обозначим множество всех функций k–значной логики, а через $H(n)$ — множество всех функций, принадлежащих множеству H, $H \subseteq P_k$, и зависящих только от переменных $x_1, \ldots, x_n$. Пусть $\mathfrak{A}$ — конечная система функций из P_k. Замыкание системы $\mathfrak{A}$ (относительно операций суперпозиции и введения фиктивной переменной) обозначим через $[\mathfrak{A}]$. Необходимые определения можно найти в [1].

Пусть Φ — некоторая формула над $\mathfrak{A}$. *Сложностью* $L(\Phi)$ этой формулы называется число символов переменных, входящих в нее. *Глубину* $D(\Phi)$ формулы Φ определим индуктивно. Если Φ состоит только из символа переменной, то $D(\Phi) = 0$. Если Φ имеет вид $f(\Phi_1, \ldots, \Phi_m)$, где $f \in \mathfrak{A}$, а $\Phi_1, \ldots, \Phi_m$ — некоторые формулы над $\mathfrak{A}$, то $D(\Phi) = 1 + \max D(\Phi_i)$, где максимум берется по всем $i = 1, \ldots, m$. Для любой функции $f \in [\mathfrak{A}]$ положим $L_{\mathfrak{A}}(f) = \min L(\Phi)$, $D_{\mathfrak{A}}(f) = \min D(\Phi)$, где минимум берется по всем формулам Φ над $\mathfrak{A}$, реализующим f.

Известно [2], что для любой полной конечной системы булевых функций $\mathfrak{A}$ и любой булевой функции $f(x_1, \ldots, x_n)$ выполнено соотношение

$$L_{\mathfrak{A}}(f) \lesssim \frac{2^n}{\log_2(n)}.$$

В работе [3] показано, что для произвольной конечной системы булевых функций $\mathfrak{A}$ и любой функции $f(x_1, \ldots, x_n) \in [\mathfrak{A}]$ справедливы неравенства

$$L_{\mathfrak{A}}(f) \leq c^n,\ D_{\mathfrak{A}}(f) \leq dn,$$

где c и d — некоторые константы, зависящие от $\mathfrak{A}$.

Следуя [4], определим индуктивно понятие *α–формулы* над конечной системой $\mathfrak{A}$ функций алгебры логики. Символ переменной является элементарной α–формулой. Символ нульместной функции из $\mathfrak{A}$ является α–формулой. Выражение вида $u(\Phi)$, где Φ — α–формула над $\mathfrak{A}$, а u — символ одноместной функции из $\mathfrak{A}$, является α–формулой. Наконец, выражение вида $g(\Phi, x_{i_2}, \ldots, x_{i_m})$, где Φ — α–формула над $\mathfrak{A}$, $m \geq 2$, g — символ m–местной функции из $\mathfrak{A}$, а $x_{i_2}, \ldots, x_{i_m}$ — символы переменных, также является α–формулой. Отметим, что каждая α–формула является формулой над $\mathfrak{A}$. Множество всех функций, реализуемых α–формулами над $\mathfrak{A}$, будем называть *α–пополнением* системы $\mathfrak{A}$ и обозначать через $[\mathfrak{A}]_\alpha$. Система $\mathfrak{A} \subseteq P_k$ называется *α–порождающей* для некоторого класса функций $H \subseteq P_k$, если $[\mathfrak{A}]_\alpha = H$. Система $\mathfrak{A} \subseteq P_k$ называется *α–полной*, если она является α–порождающей для P_k.

Пусть $\mathfrak{A}$ — конечная система функций из P_k и пусть $f \in [\mathfrak{A}]_\alpha$. Положим $D^\alpha_{\mathfrak{A}}(f) = \min D(\Phi)$, $L^\alpha_{\mathfrak{A}}(f) = \min L(\Phi)$, где минимум берется по всем α–формулам Φ над $\mathfrak{A}$, реализующим f.

Пусть $H \subseteq [\mathfrak{A}]_\alpha$ — некоторый класс функций, реализуемых α–формулами над системой $\mathfrak{A}$. Положим $D^\alpha_{\mathfrak{A}}(H(n)) = \max D^\alpha_{\mathfrak{A}}(F)$, где максимум берется по всем функциям $f \in H(n)$. Положим $D^\alpha_{\mathfrak{A}}(n) = D^\alpha_{\mathfrak{A}}(J(n))$, где $J = [\mathfrak{A}]_\alpha$. Отметим, что справедливы неравенства

$$r_1 D^\alpha_{\mathfrak{A}}(f) \leq L^\alpha_{\mathfrak{A}}(f) \leq r_2 D^\alpha_{\mathfrak{A}}(f),$$

где r_1 и r_2 — положительные константы, зависящие от $\mathfrak{A}$.

В работе [5] показано, что для любой конечной системы $\mathfrak{A}$ булевых функций существует многочлен $P(n)$ такой, что $D^\alpha_{\mathfrak{A}}(n) \leq P(n)$. Известно также

[6, 5], что в P_2 не существует конечных α–полных систем. При этом в P_k при $k \geq 3$ конечные α–полные системы существуют [4, 6, 7].

В данной работе рассматриваются функции трехзначной логики. Везде ниже сложение функций из P_3 осуществляется по модулю 3. Положим $E_3 = \{0, 1, 2\}$.

Двухместную функцию $f(x_1, x_2) \in P_3$ будем называть *бинарной операцией с правым сокращением*, если для любых $b, c \in E_3$ существует и притом ровно один элемент $a \in E_3$, такой, что $f(a, b) = c$. Множество всех бинарных операций с правым сокращением обозначим через $\mathfrak{B}$.

Одноместную функцию $s(x) \in P_3$ будем называть *подстановкой*, если для любых различных $a_1, a_2 \in E_3$ справедливо неравенство $s(a_1) \neq s(a_2)$. Множество всех подстановок обозначим через S. Пусть $s \in S$. Легко видеть, что существует бинарная операция с правым сокращением f, такая, что для любых $a, b \in E_3$ имеет место равенство $f(a, b) = s(a)$, т. е. $f(x, y) = s(x)$. Таким образом, $[\mathfrak{B}]_\alpha = [\mathfrak{B} \cup S]_\alpha$. В работе [7] показано, что система, состоящая из всех бинарных операций с правым сокращением и всех подстановок содержит α–полную подсистему. Поэтому система $\mathfrak{B}$ также α–полна.

Пусть $n \geq 1$, $\tilde{a} = (a_1, a_2, \ldots, a_n, c) \in E_3^{n+1}$. Следуя [4], положим

$$\psi_{\tilde{a}}(x_1, \ldots, x_n) = \begin{cases} c, \text{ если } x_i = a_i, i = 1, \ldots n, \\ 0, \text{ иначе.} \end{cases}$$

Теорема 1. *Пусть* $n \geq 1$, $(a_1, \ldots, a_n, c) \in E_3^{n+1}$, *причем* $c \neq 0$. *Тогда справедливо неравенство*

$$D_{\mathfrak{A}}^{\alpha}(\psi_{\tilde{\alpha}}) \geq 2^n - 2.$$

Пусть $n \geq 1$ и $w(x_1, \ldots, x_n) \in P_3$. Функцию w будем называть *двоично–представимой*, если существуют такие элементы $a_1, \ldots, a_n \in E_3$ и такая функция $f(x_1, \ldots, x_n) \in P_3$, что $w(x_1, \ldots, x_n) = f(\gamma_1(x_1), \ldots, \gamma_n(x_n))$, где

$$\gamma_i(x_i) = \begin{cases} 1, \text{ если } x_i = a_i, \\ 2, \text{ иначе,} \end{cases}$$

$1 \leq i \leq n$. Множество всех двоично–представимых функций обозначим через W.

Теорема 2. *Пусть* $n \geq 1, m \geq 1$, $w_1, \ldots, w_m \in W(n)$, $f = w_1 + \ldots + w_n$. *Тогда справедливо неравенство*

$$D_{\mathfrak{A}}^{\alpha}(f) \leq m2^n - 1.$$

Следствие 1. *Пусть* $n \geq 1$, $w \in W(n)$. *Тогда справедливо неравенство*

$$D_{\mathfrak{A}}^{\alpha}(w) \leq 2^n - 1.$$

Для каждого $b \in E_3$ положим

$$\xi_b(x) = \begin{cases} 1, \text{ если } x = b, \\ 2, \text{ иначе.} \end{cases}$$

Кроме того положим

$$f_b(x_1,\dots,x_n)=\begin{cases} b, \text{ если } x_i=1, i=1,\dots n,\\ 0, \text{ иначе.}\end{cases}$$

Легко видеть, что для любого набора $\tilde{a}=(a_1,\dots,a_n,c)\in E_3^{n+1}$ имеет место равенство $\psi_{\tilde{a}}(x_1,\dots,x_n)=f_c(\xi_{a_1}(x_1),\dots,\xi_{a_n}(x_n))$, т. е. функция $\psi_{\tilde{a}}$ принадлежит классу W. Тогда из сформулированных выше утверждений вытекает

Следствие 2. *Пусть $n\geq 1$. Тогда имеет место неравенство*

$$2^n-2\leq D^{\alpha}_{\mathfrak{A}}(W(n))\leq 2^n-1.$$

Следствие 3. *При $n\to\infty$ имеет место асимптотическое равенство*

$$D^{\alpha}_{\mathfrak{A}}(W(n))=2^n+\underline{O}(1).$$

Любую функцию $f\in P_3(n)$ можно представить в виде

$$\sum_{(a_1,\dots,a_n)\in E_3^n}\psi_{(a_1,\dots,a_n,f(a_1,\dots,a_n))}.$$

Тогда справедливо

Следствие 4. *Пусть $n\geq 1$, $f\in P_3(n)$. Тогда имеет место неравенство*

$$D^{\alpha}_{\mathfrak{A}}(f)\leq 6^n-1.$$

В заключение автор выражает искреннюю признательность А. Б. Угольникову за постановку задачи и обсуждение результатов работы.

Работа выполнена при финансовой поддержке РФФИ (проект 11-01-00508) и программы фундаментальных исследований Отделения математических наук РАН “Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения”, проект “Задачи оптимального синтеза управляющих систем”.

Список литературы

1. Угольников А. Б. Классы Поста. — М.: Изд–во ЦПИ при мех.-матем. ф-те МГУ им. М. В. Ломоносова, 2008.
2. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики — 1960. — Вып. 3. — С. 61–80.
3. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики — 1988. — Вып. 1. — С. 242–245.
4. Глухов М. М. Об α-замкнутых классах и α-полных системах функций k-значной логики // Дискретная математика. — 1989. — **1**, вып. 1. — С. 16–21.

5. Трущин Д. В. О глубине α-пополнений систем булевых функций // Вестн. Моск. ун-та. — 2009. — Сер. 1. Математика. Механика. Вып. 2. — С. 72–75.
6. Чернышов А. Л. Условия α-полноты систем функций многозначной логики // Дискретная математика. — 1992. — **4**, вып. 4. — С. 117–130.
7. Шабунин А. Л. Примеры α-полных систем k-значной логики при $k = 3, 4$ // Дискретная математика. — 2006. — **18**, вып. 4. — С. 45–55.

ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ ДЕВЯТИ РАУНДОВ БЛОЧНОГО ШИФРА SMS4

Г. И. Шушуев (Новосибирск)

Введение

SMS4 — стандарт блочного шифра KHP для защиты беспроводных сетей LAN WAPI (Wired Authentical and Privacy Infrastructure). Алгоритм шифрования, написанный на китайском языке, был опубликован правительством KHP в январе 2006 г., английский перевод опубликован в 2008 г. [2].

Существует не так много работ по криптоанализу SMS4. Интегральный криптоанализ 13-раундовой версии был впервые представлен в 2007 году группой авторов во главе с F. Liu. Алгебраический криптоанализ представлен W. Ji и L. Hu в том же году. Дифференциальный криптоанализ на невозможных разностях 16-раундового шифра был описан в [5] и результаты были улучшены в [7]. Прямоугольный криптоанализ 14-раундовой версии рассматривался в [5,7], 16-раундовой версии — в [8] и 18-раундовой версии — в [4]. Бумеранг-атака 18-раундов шифра представлена в [4]. Дифференциальный криптоанализ 21-раундовой версии приводится в [8] и 22-раундов — в [4,9]. Линейный криптоанализ 22-раундовой версии можно найти в [4,3]. Многомерный линейный криптоанализ 23-раундов шифра приводится в [1].

раунды	статистика	время	память	метод
22	$2^{118,8}$	2^{117}	2^{112}	Линейный [3]
22	2^{117}	$2^{112,3}$	2^{110}	Дифференциальный [9]
23	$2^{126,6}$	$2^{127,4}$	$2^{120,7}$	Многомерный линейный [1]

В таблице приведено сравнение сложностей наиболее успешных методов криптоанализа укороченного SMS4. Заметим, что все существующие методы до сих пор остаются непрактическими, в связи с чем задача криптоанализа SMS4 остаётся актуальной.

В основу данной работы был положен метод линейного криптоанализа, описанный в [4]. Но в [4] используется не самое лучшее линейное приближение раунда. В работе описан линейный криптоанализ 9-ти раундов блочно-

го шифра SMS4, для этого были исследованы всевозможные линейные приближения S-блока, линейные приближения раунда, проверена оптимальность схемы согласования раундов, исследована связь между объёмом статистики и трудоёмкостью вычислений.

1. Описание алгоритма

SMS4 – 32-раундовая модифицированная сеть Фейстеля. Открытый текст P, шифртекст C и ключ K имеют размер 128 бит. Открытый текст представляется как четыре 32-битовых слова $P = (P_0, P_1, P_2, P_3)$, X^i промежуточный шифртекст после i-го раундов, где $i = 1, 2, \ldots, 32$.

Пусть S — это 8×8 S-блок шифра SMS4. Тогда нелинейное преобразование τ 32-битного слова $A = (a_0, a_1, a_2, a_3)$ определяется как

$$\tau(A) = S(a_0)||S(a_1)||S(a_2)||S(a_3),$$

где $||$ стандартная конкатенация. Линейное перемешивающее преобразование L определяется как

$$L(X) = X \oplus (X <<< 2) \oplus (X <<< 10) \oplus (X <<< 18) \oplus (X <<< 24),$$

где $X <<< n$ означает циклический сдвиг X влево на n бит.

Процесс шифрования SMS4 осуществляется следующим образом:

1. Входной открытый текст $X^0 = P = (P_0, P_1, P_2, P_3)$,
2. Для i от 1 до 32
   $P_{i+3} = P_{i-1} \oplus F(P_i \oplus P_{i+1} \oplus P_{i+2} \oplus RK_i) = P_{i-1} \oplus L(\tau(P_i \oplus P_{i+1} \oplus P_{i+2} \oplus RK_i))$,
   $X^i = (P_i, P_{i+1}, P_{i+2}, P_{i+3})$,
3. Выходной шифртекст $C = (P_{35}, P_{34}, P_{33}, P_{32})$.

Для нахождения раундовых подключей ключ

$$K = (MK_0, MK_1, MK_2, MK_3),$$

состоящий из 128 бит, складывается с системным параметром T. Раундовый ключ RK_j вычисляется следующим образом:

1. Вход $(K_0, K_1, K_2, K_3) = (MK_0 \oplus T_0, MK_1 \oplus T_1, MK_2 \oplus T_2, MK_3 \oplus T_3)$, где $\mathtt{T_0} = \mathtt{0xa3b1bac6}, \mathtt{T_1} = \mathtt{0x56aa3350}, \mathtt{T_2} = \mathtt{0x677d9197}, \mathtt{T_3} = \mathtt{0xb27022dc}$.
2. Выход $RK_j = K_{j+3} = K_{j-1} \oplus L'(\tau(K_j \oplus K_{j+1} \oplus K_{j+2} \oplus CK_j))$, где $CK_j = (28j, 28j + 7, 28j + 14, 28j + 21)$, каждая из четырех компонент CK_j есть двоичная запись числа по модулю 256.

$$L'(X) = X \oplus (X <<< 2) \oplus (X <<< 10) \oplus (X <<< 18) \oplus (X <<< 24).$$

2. Общие сведения

Линейный криптоанализ [6], изобретённый Мацуи в 1993 году, — один из основных статистических методов криптоанализа в симметричной криптографии. Этот метод использует линейное соотношение битов входных, выходных блоков и ключа, которое выполняется с вероятностью отличной от $\frac{1}{2}$. Это соотношение исследуется на парах открытый текст — шифртекст для получения зависимости на битах ключа. Или, в случае второго алгоритма Мацуи, — для получения части ключа.

3. Поиск линейного соотношения

Поиск соотношения осуществляется путем анализа каждого из раундов шифрования. В свою очередь анализ раунда, в случае SMS4, требует анализа такого нелинейного преобразования, как S-блок.

Определение. Маска Γ_α — это вектор, соответствующий двоичной записи числа α.

S-блок — нелинейное преобразование, от которого напрямую зависит криптостойкость шифра. Для анализа S-блока строится таблица линейного преобладания размером 256×256. Порядковый номер столбца соответствует входной маске, порядковый номер строки — выходной, значение на пересечении i-ой строки и j-ого столбца равное d означает, что величина $\Gamma_i \cdot a$ (скалярное произведение) совпадает с величиной $\Gamma_j \cdot b$, где a и b всевозможные входы и выходы S-блока, в $128 + d$ случаях из 256. Всего различных входов S-блока 8×8 может быть $2^8 = 256$. Т.е. можно утверждать, что соотношение построенное с помощью входной маски Γ_i и выходной Γ_j, выполняется с вероятностью $\frac{128+d}{256} = \frac{1}{2} + \frac{d}{256}$. Очевидно чем $|d|$ больше, тем больше отклонение вероятности от $\frac{1}{2}$.

Вход функции F — это 32-битное слово a, которое делится на 4 части по 8 бит (8-битные слова a_1, a_2, a_3, a_4) и каждые 8 бит проходят через соответствующий S-блок. Выход после S-блоков — 32-битное слово b. Рассмотрим 32-битные маски Γ_α и Γ_β. Цель — найти вероятность того, что выполняется равенство $\Gamma_\alpha \cdot a = \Gamma_\beta \cdot b$ (или, что то же самое,

$$\Gamma_{\alpha_1} \cdot a_1 \oplus \Gamma_{\alpha_2} \cdot a_2 \oplus \Gamma_{\alpha_3} \cdot a_3 \oplus \Gamma_{\alpha_4} \cdot a_4 = \Gamma_{\beta_1} \cdot b_1 \oplus \Gamma_{\beta_2} \cdot b_2 \oplus \Gamma_{\beta_3} \cdot b_3 \oplus \Gamma_{\beta_4} \cdot b_4,$$

где Γ_{α_i} и Γ_{β_j} 8-битные маски). Для этого воспользуемся леммой:

Лемма о "набегании знаков"(pilling-up) [6]. *Пусть* X_i $(1 \le i \le n)$ — *независимые случайные величины, каждая из которых принимает значение* 0 *с вероятностью* $1/2 + \varepsilon_i$ *и значение* 1 *с вероятностью* $1/2 - \varepsilon_i$ $(-1/2 \le \varepsilon \le 1/2)$. *Тогда случайная величина* $X_1 \oplus X_2 \oplus \ldots \oplus X_n$ *принимает значение* 0 *с вероятностью* $1/2 + \varepsilon$ *и значение* 1 *с вероятностью* $1/2 - \varepsilon$, *где*

$$\varepsilon = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i.$$

В данном случае n принимает значение от 1 до 4 в зависимости от количества задействованных S-блоков. S-блок задействован, если соответствующая маска $\Gamma_{\alpha_i} \neq (0,0,0,0,0,0,0,0)$. Вероятность того, что выполняется соотношение $\Gamma_{\alpha_i} \cdot a_i = \Gamma_{\beta_i} \cdot b_i$ для соответствующего S-блока — $1/2 + \varepsilon_i$. Очевидно, что чем меньше S-блоков задействовано, тем больше ε. Затем слово b проходит через перемешивающее преобразование L. Оно линейно, поэтому на вероятность сохранения соотношения не влияет, но само соотношение преобразует. Выход функции F — 32-битное слово c. Соотношение $\Gamma_\beta \cdot b = \Gamma_\gamma \cdot c$ выполняется с вероятностью 1.

Была написана программа вычисляющая преобладание — ε (отклонение вероятности от $\frac{1}{2}$) перехода одной 32-битной маски в другую. В данной работе взято соотношение из [1] вида $\Gamma_\alpha \cdot a = \Gamma_\alpha \cdot c$, которое использует три S-блока и выполняется с $\varepsilon = 2^2(\frac{14}{256} \cdot \frac{16}{256} \cdot \frac{16}{256}) \approx 2^{-10.19}$. Нами было проверено отсутствие более вероятных соотношений с двумя и менее активными S-блоками, а также с тремя S-блоками с преобладанием $\frac{16}{256}$. Одой из таких масок, для выбранного соотношения, будет Γ_α= `0x0011fba`. Причем τ(`0x0011fba`) = `0x0084be2f`, L(`0x0084be2f`) = `0x0011fba`=Γ_α.

4. Согласование раундов

Обычно несложно найти линейные соотношения на раунд выполняющиеся с вероятностью $\frac{1}{2} + \varepsilon$. Но их надо ещё согласовать между собой, что-бы получить линейное соотношение на весь шифр. Способ это сделать и есть схема согласования раундов. В данной работе используется схема из [1], но применённая к девяти раундам SMS4. Из неё получается следующее 9-раундовое приближение:

$$\Gamma_\alpha \cdot P_4 \oplus \Gamma_\alpha \cdot P_9 = \Gamma_\alpha \cdot RK_5 \oplus \Gamma_\alpha \cdot RK_6 \qquad (1)$$

В этой схеме раундовое приближение используется два раза, значит по piling-up лемме итоговое преобладание примет значение $2(2^{-10.19})^2 = 2^{-19,38}$ или без округлений, получим $2 \cdot (2^2 \cdot (\frac{14}{256} \cdot \frac{16}{256} \cdot \frac{16}{256}))^2 = 1,46031 \cdot 10^{-6}$. Это и есть теоретическое преобладание ε_t.

5. Второй алгоритм Мацуи

Алгоритм описан в [6]. Применим его в данном случае, для этого нужна статистика — пары открытый текст, шифртекст (P, C), которая набирается на *одном*, неизменном ключе. Количество пар статистики — $|S|$. Поскольку ключ неизменен, то $\Gamma_\alpha \cdot RK_5 \oplus \Gamma_\alpha \cdot RK_6 = const$. Вообще говоря, константа неизвестна, но для неизменного ключа она равна либо 0, либо 1. Равенство (1) теоретически выполняется с известной вероятностью равной $1/2 + \varepsilon_t$, где ε_t—теоретическое преобладание.

Теперь осуществляется перебор по всем RK_{1i} (2^{32} вариантов). Для каждого RK_{1i} можно вычислить P_4, т.к. C известно, то известно и P_9. Значит можно вычислить N_0 и N_1 (количество пар статистики, для которых левая часть (1) принимает значение 0 и 1 соответственно). Эксперименталь-

ное преобладание, соответствующее RK_{1i}, вычисляется следующим образом: $|\varepsilon_{ei}| = |\frac{N_0}{N_0+N_1} - 0,5| = |\frac{N_1}{N_0+N_1} - 0,5|$. Теперь надо запомнить определенное множество наиболее правдоподобных первых раундовых подключей $\Omega(\zeta)$.

$$\Omega(\zeta) := \{RK_{1i} : |\varepsilon_t - |\varepsilon_{ei}|| < \zeta\},$$

где ζ — доверительная граница. Ключи, экспериментальное преобладание которых, отличается от теоретического, больше чем на ζ, в доверительный интервал не включаются. Мощность Ω обратно пропорциональна объёму статистики. Осталось найти правильный ключ, для этого надо восстанавливать часть ключа K по известному RK_1. По каждому $RK_{1i} \in \Omega$ можно восстановить r битов ключа K, поэтому нужно перебрать $128-r = k$ оставшихся битов K. Всего кандидатов в ключи будет $m \cdot 2^k$. Для каждого кандидата в ключи K_i, надо зашифровать первый из открытых текстов статистики, и если получается соответствующий шифртекст, то ключ верен.

Псевдокод:

цикл по $RK_{1i} \in \{$`0x00000000`$, ..., $`0xffffffff`$\}$.....$[2^{32}]$
{
....цикл по (P, C) статистике.....$|S|$
....{
.....1 раунд зашифрования
.....если $\Gamma_\alpha \cdot P_4 \oplus \Gamma_\alpha \cdot P_9 = 0$, то $N_0 + +$;
.....если $\Gamma_\alpha \cdot P_4 \oplus \Gamma_\alpha \cdot P_9 = 1$, то $N_1 + +$;
....}
....$|\varepsilon_e| = |\frac{N_0}{N_0+N_1} - 0,5| = |\frac{N_1}{N_0+N_1} - 0,5|$ для RK_{1i};
....если $|\varepsilon_t - |\varepsilon_{ei}|| < \zeta$, то $RK_{1i} \in \Omega$;
}
цикл по $K_i : RK_{1i} \in \Omega$.....$[|\Omega| \cdot 2^k]$
{
....9 раундов зашифрования
....если encrypt$(P) = C$ для пары (P, C),
.....то K_i - истинный ключ
}

Трудоёмкость алгоритма $(2^{32} \cdot |S|/9 + |\Omega| \cdot 2^k) \cdot T$, где T — время выполнения 9 раундов шифрования. Оценим трудоёмкость.

Вычислим примерные значения $|S|$, $|\Omega|$, k. Т.к. RK_1 — 32-битный подключ, то $r \approx 32$, значит $k < 100$. Для нахождения зависимости между числом кандидатов в ключи — m и объёмом статистики — $|S|$ построим таблицу:

Статистика	$\lvert\varepsilon_t - \lvert\varepsilon_{ei}\rvert\rvert$	Время	m/N	m/N	m/N	m/N
10^6	$6,855 \cdot 10^{-4}$	0,23	9/10	78/90	161/186	199/250
10^7	$2,226 \cdot 10^{-4}$	2,32	9/10	77/90	156/186	210/250
10^8	$1,236 \cdot 10^{-5}$	23,17	6/10	64/90	148/186	172/250
10^9	$4,227 \cdot 10^{-7}$	231,12	6/10	59/90	139/186	166/250
10^{10}	$2,689 \cdot 10^{-6}$	2362	5/10	?/90	?/186	?/250

Приведено время вычисления значения $|\varepsilon_t - |\varepsilon_{ei}||$ для одного RK_{1i} в секундах. Пусть N — число рассматриваемых RK_{1i}, m — число тех из них, что попали в Ω. Увеличение количества рассматриваемых пар статистики уменьшает количество кандидатов в ключи, но существенно замедляет время выполнения алгоритма.

Из таблицы видно, что при $|S| = 10^{10} \approx 2^{33,22}$ величина m составляет примерно 60% от N. Значит при $N = 2^{32}$, т. е. полном переборе по подключу, $m = |\Omega| \approx 2^{31,26}$. При $|S| = 2^{128}$, т. е. полном переборе по всей статистике $|\Omega| = 2^0$, т. к. будет один RK_1 с $\varepsilon_e = \varepsilon_t$. Значит при $|S| = 2^{81}$ $|\Omega| < 2^{16}$, т. к. $81 \approx (35 + 128)/2$ и $16 \approx (0 + 31)/2$. Из этих соображений строится таблица:

$\lvert S\rvert$	$\lvert\Omega\rvert$	$2^{32} * \lvert S\rvert/9 + \lvert\Omega\rvert \cdot 2^k$
2^{35}	2^{31}	$2^{64} + 2^{131} \approx 2^{131}$
..	..	..
2^{81}	2^{16}	$2^{110} + 2^{116} \approx 2^{116}$
2^{84}	2^{15}	$2^{113} + 2^{115} \approx 2^{115}$
2^{87}	2^{14}	$2^{116} + 2^{114} \approx 2^{116}$
..	..	..
2^{128}	2^0	$2^{157} + 2^{100} \approx 2^{157}$

Видно, что при $|S| = 2^{84}$ получаем минимальную трудоёмкость линейного криптоанализа девяти раундов блочного шифра SMS4, равную 2^{115}.

Работа выполнена при финансовой поддержке РФФИ (проект 11-01-00997).

Список литературы

1. J. Cho, K. Nyberg. Improved linear cryptoanalysis of SMS4 block cipher // Symmetric Key Encryption Workshop 2011 (Lyngby, Denmark. February 16–17, 2011). — Proc. — Pp. 1–14.
2. W. Diffie, G. Ledin (translators). SMS4 encryption algorithm for. wireless networks // Cryptology ePrint Archive, Report 2008/329, 2008. http://eprint.iacr.org/2008/329
3. J. Etrog and M. Robshaw. The cryptanalysis of reduced-round SMS4 // Selected Areas in Cryptography, 15th International Workshop, SAC 2008. Sackville, New Brunswick, Canada, August 14–15. — Revised Selected Papers, vol 5381, 2008. — Pp. 51–65.
4. T. Kim, J. Kim, S. Hong, J. Sung. Linear and differential cryptanalysis of reduced SMS4 block cipher // Cryptology ePrint Archive, Report 2008/281, 2008. http://eprint.iacr.org/2008/281.
5. J. Lu. Attacking reduced-round versions of the SMS4 block cipher in the Chinese WAPI standard // Information and Communication Security, 9th International Conference, ICICS 2007. Zhengzhou, China, December 12–15, 2007. — Proceeding, Lecture Notes in Computer Science. — Vol. 4861. — Springer, 2007. — Pp. 306–318.

6. M. Matsui. Linear Cryptoanalysis Method for DES Cipher // Advances in Cryptology — Proceedings of EUROCRYPT 1993, LNCS 765. — Pp. 386–397. — Spiringer-Verlag, 1994.
7. D. Toz and O. Dunkelman. Analysis of two attacks on reduced-round versions of SMS4 // Information and Communication Security, 10th International Conference, ICICS 2008. Birmingham, UK, October 20–22, 2008. — Processings, Lecture Notes in Computer Science. — Vol. 5308. — Spring, 2008. — Pp. 141–156.
8. L. Zhang, W. Zhang and W. Wu. Cryptanalysis of reduced-round SMS4 block cipher // Informatio Security and Privacy, 13th Australasian Conference, ACISP 2008. Wollongong, Australia, July 7–9, 2008. — Proceedings, Lecture Notes in Computer Science. — Vol. 5107. — Springer, 2008. — Pp. 216–229.
9. W. Zhang, W. Wu, D. Feng, B. Su. Some new observations on the SMS4 block cipher in the Chinese WAPI Standard // Information Security Practice and Experience, 5th International Conference, ISPEC 2009. Xi'an, China, April 13–15, 2009. — Proceeding, Lecture Notes in Computer Science. — Vol. 5451. — Springer, 2009. — Pp. 324–335.

О КВАЗИГРУППОВЫХ СВЁРТКАХ РАСПРЕДЕЛЕНИЙ ВЕРОЯТНОСТЕЙ

А. Д. Яшунский (Москва)

Рассматривалась задача о свёртках распределений вероятностей на конечных бинарных квазигруппах. Подобная задача может рассматриваться как обобщение цепей Маркова, порождаемых ассоциативными алгебраическими системами, на случай неассоциативных систем. Примером исследования ассоциативных систем могут служить работы о случайных блужданиях в группах (см. обзор [3]). Интерес к квазигруппам в подобных задачах обусловлен, в частности, возможностями их применения в криптологии [4]. Например, построение потоковых фильтров с использованием квазигрупп рассматривалось в работе [2], где, впрочем использовалась лишь ассоциативная конструкция, основанная на квазигруппах.

В данной работе мы рассмотрим поведение свёрток распределений вероятностей, порождаемых квазигруппами в общем случае, не используя непосредственное сведение к цепям Маркова.

Пусть $Q = \{1, 2, \ldots, q\}$ — конечная бинарная квазигруппа с заданными операциями умножения, а также правого и левого деления (подробнее см. [1]). Пусть $u = (u_1, \ldots, u_q)$ и $v = (v_1, \ldots, v_q)$ — распределения вероятностей, заданные на Q. *Свёрткой* $u * v$ будем называть распределение с компонентами

$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j\backslash i},$$

где $j\backslash i$ — операция левого деления в Q. *Носителем* распределения вероятностей u называется множество $N(u) = \{i \in Q : u_i > 0\}$.

Свёртка выражает распределение значения результата при квазигрупповом умножении двух случайных независимых элементов из Q, имеющих распределения u и v, соответственно.

Будем рассматривать распределения, получающиеся в результате многократного применения операции свёртки к некоторому начальному распределению π. Определим множество D_n выражений свёртки *глубины* n:

$$D_0(\pi) = \{\pi\}, \quad D_{n+1}(\pi) = \{(u * v) : u \in D_k(\pi), v \in D_m(\pi), \max\{k, m\} = n\}.$$

Аналогично определяются множества L_m выражений *сложности* m:

$$L_0(\pi) = \{\pi\}, \quad L_{m+1}(\pi) = \{(u * v) : u \in L_r(\pi), v \in L_s(\pi), r + s = m\}.$$

При достаточно общих предположениях можно показать, что с ростом глубины (и сложности) выражения свёртки приближаются к равномерному распределению вероятностей. Это формулируется в следующих теоремах.

Теорема 1. *Пусть w получается свёрткой глубины n с начальным распределением π, $|N(\pi)| > \frac{|Q|}{2}$. Тогда найдётся $d \in [0, 1) : \max\limits_i \left| w_i - \frac{1}{|Q|} \right| \leqslant d^n$.*

Теорема 2. *Пусть w получается свёрткой сложности m с начальным распределением π, $|N(\pi)| > \frac{|Q|}{2}$. Тогда найдётся $\alpha > 0 : \max\limits_i \left| w_i - \frac{1}{|Q|} \right| \leqslant \frac{1}{m^\alpha}$.*

В случае, если носитель $N(\pi)$ имеет размер менее $|Q|/2$, можно построить примеры отсутствия сходимости распределений по глубине или сложности. Действительно, рассмотрим квазигруппу со следующей таблицей умножения:

$\cdot$	1	2	3	4	5	6
1	1	3	2	4	6	5
2	3	2	5	1	4	6
3	2	4	6	5	1	3
4	4	1	3	6	5	2
5	5	6	1	2	3	4
6	6	5	4	3	2	1

Для начального распределения π с носителем $N(\pi) = \{1, 2\}$, носителем распределения $(\pi * \pi) * (\pi * \pi)$ является вся квазигруппа Q. Следовательно, любые распределения, получающиеся из $(\pi * \pi) * (\pi * \pi)$, будут иметь носитель, совпадающий с Q.

С другой стороны, можно построить последовательность распределений $(\pi * \pi), ((\pi * \pi) * \pi), (((\pi * \pi) * \pi) * \pi), \ldots$ растущей глубины (и сложности), носитель которых в точности равен $\{1, 2, 3, 4\}$. Таким образом, для данной квазигруппы и указанного начального распределения π, при любых достаточно больших значениях глубины (сложности) найдутся как распределения, носитель которых совпадает с Q, так и распределения, носитель которых строго

меньше Q. То есть, в общем случае распределение большой глубины (сложности) не обязательно приближается к равномерному.

Однако, даже при произвольном носителе $N(\pi)$ для распределений имеет место «сходимость в среднем». Определим $d^{(n)}(\pi)$ — среднее распределение по выражениям из $D_n(\pi)$:

$$d^{(n)}(\pi) = \frac{1}{|D_n(\pi)|} \sum_{u \in D_n(\pi)} u.$$

Теорема 3. *Для квазигруппы Q и начального распределения π существуют подквазигруппа $Q' \subseteq Q$, число $d \in [0;1)$ и номер n' такие, что для любого $n \geqslant n'$:*

$$\max_{i \in Q'} \left| (d^{(n)}(\pi))_i - \frac{1}{|Q'|} \right| \leqslant d^{n-n'}.$$

Аналогично определяется $\ell^{(m)}(\pi)$ — среднее распределение по выражениям из $L_m(\pi)$:

$$\ell^{(m)}(\pi) = \frac{1}{|L_m(\pi)|} \sum_{u \in L_m(\pi)} u.$$

Однако для $\ell^{(m)}(\pi)$ сходимость носит более сложный характер:

Теорема 4. *Для квазигруппы Q и начального распределения π существуют номер m', множества $Q_b \subseteq Q$, $(b = 0, \ldots, r-1)$ и числа $\alpha, \beta > 0$ такие, что для $rk + b \geqslant m'$:*

$$\max_{i \in Q_b} \left| (\ell^{(rk+b)}(\pi))_i - \frac{1}{|Q_b|} \right| \leqslant \frac{\beta}{k^\alpha}.$$

Автор выражает благодарность О. М. Касим-Заде за полезные обсуждения и внимание к работе. Работа выполнена при финансовой поддержке программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» и РФФИ (проект №11–01–00508).

Список литературы

1. Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967. — 225 с.
2. Markovski S., Gligoroski D., Bakeva V. Quasigroup String Processing: Part 1 // Maced. Acad. of Sci. and Arts, Sc. Math. Tech. Scien. XX 1–2 (1999). — P. 13–28.
3. Saloff-Coste L. Random walks on finite groups. // Probability on discrete structures. Encyclopaedia Math. Sci., 110, ed. Kesten H. — Springer, Berlin, 2004. — P. 263–346.
4. Şcerbacov V. Quasigroups in cryptology // Computer Science Journal of Moldova. — 2009. — V. 17, № 2 (50). — P. 193–228.