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

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

МАТЕРИАЛЫ VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ II

Москва 2007

МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ II

Москва 2007

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 07–01–06018

М34 Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.). Часть II. Под редакцией А. В. Чашкина. 2007. — 52 с.

Сборник содержит материалы VI молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 16 по 21 апреля 2007 г. при поддержке Российского фонда фундаментальных исследований (проект 07–01–06018). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание
МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 16–21 апреля 2007 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *Ф. М. Ковалев*

СОДЕРЖАНИЕ

НЕКОТОРЫЕ СВОЙСТВА АЛГЕБР, СОДЕРЖАЩИХ ПОДАЛГЕБРУ, ИЗОМОРФНУЮ АЛГЕБРЕ МАТРИЦ

В. Б. Ларионов (Москва)

Одной из интересных и тяжёлых задач является задача умножения матриц. Её история начинается с замечательного результата Штрассена. Он показал в [5], что две квадратные матрицы размера 2 можно умножить, используя только 7 умножений линейных комбинаций элементов матриц, что повлекло за собой асимптотическую оценку $n^{\log_2 7}$ на количество умножений. Этот результат неоднократно улучшался (историю этого можно посмотреть в [7] и остановился на $O(n^{2.38})$ в работе [4] более пятнадцати лет назад.

В [2] показано, что для задачи умножения матриц может быть использована идея "расширения модели". Для этого нам понадобится несколько определений.

Определение. *Алгеброй называется линейное пространство с заданной на нём операцией умножения, линейной по обоим сомножителям.*

Определение. *Алгебра P называется алгеброй с простым умножением, если существует базис $e_1, e_2, \ldots, e_k$ в P и подстановка σ порядка k такие, что $e_i e_j = 0$ при $j \neq \sigma(i)$.*

В данном случае метод "расширения модели"приводит нас к задаче поиска алгебры с простым умножением, содержащей подалгебру матриц ([2]) и удовлетворяющей тому, что линейная оболочка строк её таблицы умножения ([1]) есть в точности подалгебра матриц (это следует из утверждения, доказанного в [6]). В данной работе будут построены все 7-мерные алгебры с простым умножением, содержащие подалгебру матриц размера 2 на 2 при условии наличия на всей алгебре антиавтоморфизма.

Пусть P — 7-мерная алгебра, $M \subset P$ – подалгебра, изоморфная алгебре квадратных матриц размера 2 на 2.

Определение. *Пусть вектору $f \in M$ при отображении из алгебры в матрицы соответствует матрица M_f размера 2 на 2. Тогда весом матрицы M_f будем называть количество ненулевых координат вектора f.*

Итак, предположим, что на P есть антиавтоморфизм Ψ, удовлетворяющий свойству линейности и соотношению

$$\Psi^2 = e, \tag{1}$$

где e — тождественное отображение.

Следующие технические леммы приведём без доказательства, поскольку они очень громоздкие (все они опираются на свойства алгебры матриц и антиавтоморфизмов, которые можно найти в [3]).

Лемма 1. *Все собственные значения описанного выше антиавтоморфизма Ψ равны ± 1, и Ψ имеет полный набор собственных векторов. Кроме того, n линейно независимых собственных векторов лежат в M.*

Лемма 2. *Не существует линейного антиавтоморфизма Ψ, на алгебре квадратных матриц размера 2 на 2 M такого, что выполнено (1) и собственное значение данного антиавтоморфизма λ_0 ($\lambda_0 = \pm 1$) имеет кратность 3, а $(-\lambda_0)$ — кратность 1, и собственное подпространство, отвечающее $(-\lambda_0)$ имеет базисом матрицу M_0 ранга 1.*

Линейную оболочку векторов $v_1, \ldots, v_n$ будем обозначать $\ell(v_1, \ldots, v_n)$, а подпространство матриц размера 2 на 2, у которых оба собственных значения нулевые, обозначим L_0. Несложно проверить, что размерность L_0 равна 3.

Лемма 3. 1) *Не существует антиавтоморфизма Ψ на алгебре квадратных матриц размера 2 на 2 такого, что выполнено (1), у Ψ есть двухмерное собственное подпространство L с собственным значением α, натянутое на две матрицы H_1, H_2 ранга 1.*

2) *Если расширять L, добавляя матрицу H_3 ранга 1 (линейно независимую с H_1, H_2), чтобы существовал антиавтоморфизм Ψ с собственным подпространством $L \oplus \ell(H_3)$ (где "$\oplus$" означает прямую сумму подпространств) с собственным значением α, то в случае $\alpha = -1$ $L \oplus \ell(H_3) = L_0$, а в случае $\alpha = 1$ $L \oplus \ell(H_3) = L_1 = \ell\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}\right)$ (с точностью до изоморфизма).*

3) *В предыдущем пункте в случае подпространства L_0 в некотором базисе*

$$\Psi = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}, \tag{2}$$

а в случае L_1 :

$$\Psi = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & -c \\ -b & d \end{bmatrix}. \tag{3}$$

Будем обозначать эти антиавтоморфизмы соответственно Ψ_0 и Ψ_1.

Пусть $\{e_i\}_{i=0}^{6}$ — базис P из определения алгебры с простым умножением. Будем предполагать, что такой базис единственный. Тогда

$$\Psi(e_i) = e_{\beta(i)} c_i,$$

где β — перестановка на множестве $\{0,\dots,6\}$, c_i — некоторые константы.

Из (1) следует, что перестановка β состоит только из неподвижных элементов и циклов длины 2.

Определим теперь класс антиавтоморфизмов, который мы будем исследовать. Вначале рассмотрим случай, когда 3 собственные значения автоморфизма, не относящиеся к подалгебре M (лемма 1) равны между собой и равны α. Соответствующее 3-мерное собственное подпространство обозначим M'.

Лемма 4. 1) *В β есть хотя бы один цикл длины 2.*

2) *При сделанном выше предположении у β есть как минимум 2 цикла длины 2.*

Итак, по лемме 4 у перестановки β будет как минимум 2 цикла длины 2. Пусть это (12)(34), тогда:

$$e_1 = g_1 + m_1, \quad e_2 = g_1 + \alpha\Psi(m_1), \quad e_3 = g_2 + m_2, \quad e_4 = g_2 + \alpha\Psi(m_2),$$

где $g_i \in M'$, $m_i \in M$. Обозначим

$$h_i = m_i - \alpha\Psi(m_i).$$

Будем обозначать H_i матрицу, соответствующую вектору h_i при вложении в алгебру. Предположим, что у перестановки β 3 неподвижных элемента. Тогда антиавтоморфизм Ψ обладает двухмерным собственным подпространством, с собственным значением $(-\alpha)$ натянутым на матрицы H_1 и H_2 (очевидно, они линейно независимы). Это следует из того факта, что у Ψ собственное подпространство с собственным значением α $\ell(e_0, e_5, e_6, e_1 + e_2, e_3 + e_4)$ размерности 5. Но матрицы H_i веса 2, ранга 1. Получаем противоречие с леммой 3.

Следовательно, $\beta = (0)(12)(34)(56)$ и

$$e_5 = g_3 + m_3, \quad e_6 = g_3 + \alpha\Psi(m_3), \quad h_3 = m_3 - \alpha\Psi(m_3).$$

Перенумеруем базисные вектора так, чтобы

$$h_1 = [0,1,0,0,0,0,-1],\ h_2 = [0,0,1,0,0,-1,0],\ h_3 = [0,0,0,1,-1,0,0]. \quad (4)$$

Рассмотрим вначале случай $\alpha = 1$.

В этом случае по лемме 3 $H_1 \sim H_2 \sim H_3 \sim \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Лемма 5. *В этом случае с точностью до изоморфизма возможна только одна алгебра, задаваемая таблицей умножения:*

$$\begin{array}{ll} e_0e_0 & f_e \\ e_1e_2 & h_1h_2 \\ e_2e_3 & h_2h_3 \\ e_3e_1 & h_3h_1 \\ e_4e_5 & h_3h_2 \\ e_5e_6 & h_2h_1 \\ e_6e_4 & h_1h_3. \end{array} .$$

Доказательство. Заметим, что $H_i^2 = 0$ $(i = 1, 2, 3)$.

Поскольку P — алгебра с простым умножением, а H_i — матрицы веса 2, то для каждого i найдутся j, k такие, что $H_iH_j = 0$ и $H_kH_i = 0$ $(i, j, k = 1, 2, 3)$. Причём, так как мы предположили, что базис $\{e_i\}_{i=1}^7$ — единственный, то такие номера j, k для каждого i будут тоже единственными. В данном случае $i = j = k$. Следовательно,

$$H_iH_j \neq 0 \text{ при } i \neq j, \tag{5}$$

поэтому произведения базисных векторов вида e_0e_i, e_ie_0, e_ie_i $(i > 0)$ обязаны равняться нулю, иначе легко понять, что условие выше нарушиться. Заметим, что (5) верно для любых матриц из L_0 ранга 1.

Простыми рассуждениями легко понять, что для обеспечения условия (5), перестановка σ обязана иметь два цикла длины 3, то есть можно занумеровать вектора базиса так, что $\sigma = (0)(123)(456)$ (при этом можно сохранить условие (4)). Также очевидно, чему будут равняться произведения $e_ie_{\sigma(i)}$ $(i > 0)$.

Докажем, что при некотором масштабировании вектора e_0 произведение e_0e_0 будет равно единичной матрице. Пусть вектор из алгебры, соответствующий единичной матрице

$$f_e = [a, b, c, d, d, c, b].$$

Это общий случай для вектора, для которого выполнено $\Psi_0(f_e) = f_e$.

$$f_e^2 = a^2e_0e_0 + bch_1h_2 + cdh_2h_3 + dbh_3h_1 + dch_3h_2 + cbh_2h_1 + bdh_1h_3 =$$

$$= a^2e_0e_0 + bc(h_1h_2 + h_2h_1) + cd(h_2h_3 + h_3h_2) + bd(h_1h_3 + h_3h_1).$$

Из первого пункта леммы 3 следует, что $h_ih_j + h_jh_i = const\ E$ для $i \neq j$. Пусть

$$H_1H_2 + H_2H_1 = \alpha E,$$

$$H_1H_3 + H_3H_1 = \beta E,$$

$$H_2H_3 + H_3H_2 = \gamma E.$$

Домножим h_i (то есть, соответствующие базисные вектора e_i и e_{7-i}) $i = 1, 2, 3$ на соответственно

$$-\sqrt{\frac{\alpha\beta}{\gamma}},\ -\sqrt{\frac{\alpha\gamma}{\beta}},\ -\sqrt{\frac{\beta\gamma}{\alpha}}.$$

Очевидно, после этой операции будет справедливо

$$H_iH_j + H_jH_i = -E \ \ i \neq j.$$

С учётом этого

$$f_e^2 = a^2 e_0 e_0 - f_e(bc + cd + bd) = f_e,$$

$$e_0 e_0 = f_e \frac{1 + bc + cd + bd}{a^2}.$$

Понятно, что $a \neq 0$ (иначе M построено на $e_1, \ldots, e_6$). Осталось масштабировать e_0 так, чтобы

$$a^2 = 1 + bc + cd + bd.$$

Пользуясь доказанными леммами 3 и 6, легко получить следующую таблицу для алгебры:

$$\begin{array}{lccccccc}
e_0e_0 & 2 & -1 & -1 & -1 & -1 & -1 & -1 \\
e_1e_2 & -1 & 0 & 0 & 1 & 0 & 1 & 1 \\
e_2e_3 & -1 & 1 & 0 & 0 & 1 & 1 & 0 \\
e_3e_1 & -1 & 0 & 1 & 0 & 1 & 0 & 1 \\
e_4e_5 & -1 & 0 & 1 & 1 & 0 & 0 & 1 \\
e_5e_6 & -1 & 1 & 1 & 0 & 1 & 0 & 0 \\
e_6e_4 & -1 & 1 & 0 & 1 & 0 & 1 & 0.
\end{array} \tag{6}$$

Случай $\alpha = -1$ аналогичным образом даёт алгебру:

$$\begin{array}{lccccccc}
e_0e_0 & 0 & 1 & 0 & -1 & 1 & 0 & -1 \\
e_1e_5 & -1 & 0 & 0 & 1 & 0 & 1 & 1 \\
e_2e_6 & 1 & -1 & -1 & 0 & -1 & 0 & 0 \\
e_3e_4 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
e_4e_2 & -1 & 0 & 1 & 1 & 0 & 0 & 1 \\
e_5e_3 & 1 & -1 & 0 & 0 & -1 & -1 & 0 \\
e_6e_1 & 0 & -1 & 0 & 0 & 0 & 0 & 1.
\end{array} \tag{7}$$

А случай, когда антиавтоморфизм имеет собственные значения разных знаков на M':

$$\begin{array}{lccccccc} e_0e_0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ e_1e_1 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ e_2e_2 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ e_3e_3 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ e_4e_5 & -1 & -1 & 0 & 0 & -1 & -1 & 0 \\ e_5e_6 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\ e_6e_4 & -1 & 0 & 0 & -1 & 0 & -1 & -1. \end{array} \qquad (8)$$

Итак, доказана следующая

Теорема 1. *При условии наличия антиавтоморфизма существует ровно три неизоморфные 7-мерные алгебры, содержащие подалгебры матриц размера 2 на 2, задаваемые таблицами* (6), (7), (8).

Список литературы

1. Алексеев В. Б., Ларионов В. Б. О расширениях с простым умножением для алгебры матриц. // Труды VII международной конференции "Дискретные модели в теории управляющих систем", М. 2006 С. 17–22.

2. Алексеев В. Б. Минимальные расширения с простым умножением для алгебры матриц второго порядка. // Дискретная математика, 1997, т.9, № 1. С. 71–82.

3. Маркус М., Минк Х. Обзор по теории матриц и матричных неравенст. //М. Едиториал УРСС. 1994. 232 с.

4. Coppersmith D., Winograd S. Matrix multiplication via arithmetic progression. //J. Symb. Comp., 1990, 9, 251–280.

5. Strassen V. Gaussian elimination is not optimal. //Numer. Math., 1969, v.13, 454–456.

6. Плукас М. О некоторых свойствах алгебр с простым умножением, содержащих ассоциативные подалгебры. //Дискретная математика, 1997, № 2, С. 79–90.

7. Алексеев В.Б. Сложность умножения матриц. Обзор. //кибернетический сборник М.: Мир, 1988, № 25, С. 189–236.

ОЦЕНКА НЕЛИНЕЙНОСТИ ВЫСОКИХ ПОРЯДКОВ БУЛЕВОЙ ФУНКЦИИ ЧЕРЕЗ ЗНАЧЕНИЕ ЕЕ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ

М. С. Лобанов (Москва)

С появлением "алгебраических" атак (см. например [2,5]) на потоковые шифры от булевых функций, используемых в этих криптографических схемах в качестве нелинейных фильтров, наряду с другими стало требоваться и условие обладания высокой алгебраической иммунностью. В связи с этим возник вопрос, как связана алгебраическая иммунность с другими важными криптографическими свойствами булевых функций.

В работе [3] был доказан результат, эквивалентный следующей оценке на нелинейность r-ого порядка:

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}.$$

Позже в [4] нами была доказана нижняя оценка нелинейности (r=1) функции через значенниее ее алгебраической иммунности:

$$nl(f) \geq 2\sum_{i=0}^{k-2} \binom{n-1}{i}.$$

И там же для всех допустимых значений алгебраической иммунности были построены функции, на которых достигается равенство в приведенной оценке.

Еще позднее C.Carlet в [1] обобщил доказанную нами оценку на случай других r:

$$nl_r(f) \geq 2\sum_{i=0}^{k-r-1} \binom{n-r}{i}.$$

Отметим, что ни одна из двух приведенных выше оценок для нелинейности r-ого порядка не влечет другую.

В данной работе мы покажем, что задача получения оценки нелинейность r-ого порядка через значение алгеброической иммунности полностью сводиться к оценки размерности определенного линейного пространства. И как следствие из этого получим новую оценку, перекрывающую обе существовавшие ранее.

Известно, что булева функция единственным образом представляется полиномом.

Определение. *Степенью булевой функции называется длина самого длинного слагаемого в ее полиноме (количество переменных в этом слагаемом).*

Определение. *Булева функция g над F_2^n называется аннигилятором булевой функции f над F_2^n, если $fg = 0$.*

Очевидно, что аннигиляторы f образуют линейное подпространство в пространстве всех булевых функций от n переменных.

Определение. *Алгебраической иммунностью $AI(F)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n, где g не равная тождественно нулю функция с минимальной степенью, такая что $fg = 0$ или $(f+1)g = 0$.*

Известно [2, 5], что для любой f над F_2^n выполнено $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Определение. *Весом $wt(x)$ набора x из F_2^n называется число единиц в x.*

Определение. *Расстояние между булевыми функциями f_1 и f_2 определяется как $d(f_1, f_2) = \mid \{x \in F_2^n \mid f_1(x) \neq f_2(x)\} \mid$.*

Определение. *Нелинейностью r-того порядка $nl_r(f)$ булевой функции f над F_2^n называется* $\min\limits_{l,\ deg(l) \leq r} d(f, l)$.

Определение. *Пусть h булева функция от n переменны. Обозначим через $An_k(h)$ линейное пространство аннигиляторов степени не выше k и через $d_{k,h}$ его размерность.*

Определение. *Пусть $C = \{\overline{x}_1, \ldots, \overline{x}_n\}$ множество двоичных наборов длины n. При любого $k \leq n$, произвольному набору $x = (x_1, \ldots, x_n)$ можно сопоставить однородное линейное уравнение, получаемое подстановкой компонент набора в*

$$a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \cdots + \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}$$

и приравниванием полученного выражения к 0. Тогда назовем k-рангом множества C ранг системы линейных уравнений, полученных таким образом из наборов множества C. Обозначим его через $r_k(C)$.

Ищем для функции f аннигиляторы степени не выше k методом неопределенных коэффициентов:

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \cdots + \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}.$$

Функция g является аннигилятором f тогда и только тогда, когда $f(x) = 1$ влечет $g(x) = 0$. Получаем систему линейных уравнений.

Несложно заметить, что $d_{k,f} = dim(An_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - r_k(supp(f))$.

Утверждение 1. *Пусть f и f_0 функции от n переменных, $AI(f_0) \geq k$. Тогда $d(f, f_0) \geq dim(An_{k-1}(f)) + dim(An_{k-1}(f+1))$.*

Доказательство. Так как $AI(f_0) \geq k$, то $r_{k-1}(supp(f_0)) = \sum_{i=0}^{k-1} \binom{n}{i}$.

В тоже время $r_{k-1}(supp(f)) = \sum_{i=0}^{k-1} \binom{n}{i} - d_{k-1,f}$. Следовательно, существует не меньше чем $d_{k-1,f}$ наборов, где f_0 равна единице, а f нулю.

Аналогично рассматриваем $f + 1$ и $f_0 + 1$, получаем оценку на число наборов, где f единица, а f_0 ноль.

Определение. *Пусть h булева функция от n переменных. Обозначим через $B_k(h)$ линейное пространство функций от n переменных степени не выше k, которые при умножении на h снова дают функции степени не выше k.*

Утверждение 2. *Сумма $dim(An_k(f))$ и $dim(An_k(f+1))$ равна $dim(B_k(f))$.*

Доказательство. Рассмотрим пару (g_1, g_2), где $g_1 \in An_k(f)$, $g_2 \in An_k(f+1)$, тогда имеем $fg_1 + (f+1)g_2 = 0$, отсюда $f(g_1 + g_2) = g_2$. Получаем соответствие между парами функций, первая из которых из $An_k(f)$, вторая из $An_k(f+1)$, и функциями из $B_k(f)$. Несложно проверить, что соответствие взаимооднозначное.

Лемма 1. *Пусть $r_k(supp(f)) = wt(f)$, где $k < \lceil \frac{n}{2} \rceil$, тогда $dim(An_k(f+1)) = 0$.*

Доказательство. Из условия следует, что для любого набора x, такого что $f(x) = 1$, существует функция g степени не выше k, что произведение fg равно 1 только на одном наборе x. В противном случае существовала бы функция отличная от f лишь на наборе x с k-рангом $r_k(supp(f)) = wt(f)$ и весом равным $wt(f) - 1$, что невозможно.

Пусть существует функция f', $deg(f') \leq k$ и $f \neq 0$, что $(f+1)f' = 0$. Возьмем набор x, такой что $f'(x) = 1$. Из того что $supp(f') \subseteq supp(f)$, следует, что существует g' степени не выше k, что произведение $f'g'$ равно 1 только на одном наборе x. Но степень произведения двух булевых функций не превосходит суммы степеней этих функций, тогда $deg(f'g') < n$, что противоречит, тому что $f'g'$ равно 1 ровно на одном наборе.

Следствие 1. *Пусть $dim(An_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - wt(f)$, где $k \leq \lceil \frac{n}{2} \rceil$, тогда $dim(An_{\lceil \frac{n}{2} \rceil - 1}(f+1)) = 0$.*

Следствие 2. *Пусть* $n = 2k + 1$ *и* $An_k(f) = 0$, *тогда* $AI(f) = k + 1$.

Утверждение 3. *Пусть* $deg(f) \leq \lceil \frac{n}{2} \rceil$, $k \leq \lceil \frac{n}{2} \rceil$, *тогда существует функция* g, *такая что* $AI(g) = k$ *и* $d(f, g) = dim(B_{k-1}(f))$.

Доказательство. Среди наборов, на которых f равна 1 найдется $r_{k-1}(supp(f))$ таких, что их $(k-1)$-ранг тоже будет равен $r_{k-1}(supp(f))$, обозначим это множество наборов через C_1. Аналогично, рассмотрев $f+1$ получим множество C_0 из $r_{k-1}(supp(f+1))$ наборов. Из леммы 1 следует, что мы можем дополнить C_1 за счет $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f))$ наборов, которые не входят в C_0 и на которых f равна 0, так чтобы k-ранг нового множества был в точности $\sum_{i=0}^{k-1} \binom{n}{i}$. Аналогично мы можем дополнить и множество C_0 за счет $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f+1))$ наборов, которые не входят в C_1 и на которых f равна 1, так чтобы k-ранг нового множества был в точности $\sum_{i=0}^{k-1} \binom{n}{i}$.

Из выше сказанного следует, что можно изменить значение f на $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f)) + \sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f+1)) = dim(An_{k-1}(f)) + dim(An_{k-1}(f+1)) = dim(B_{k-1}(f))$ наборах и получить функцию g, такую что $dim(An_{k-1}(g)) = dim(An_{k-1}(g+1)) = 0$, следовательно $AI(g) = k$.

Таким образом, с учетом утверждений 1-3 мы доказали, что задача нахождения наиболее сильной оценки нелинейности r-ого порядка функции через значение ее алгебраической иммунности k полностью сводиться к нахождению $min_{deg(g) \leq r} dim(B_{k-1}(g))$. Сформулируем это в качестве теоремы:

Теорема 1. *Пусть* $f(x_1, \ldots, x_n)$ *имеет* $AI(f) = k$, *тогда*

$$nl_r(f) \geq min_{deg(g) \leq r} dim(B_{k-1}(g)).$$

И существует функция f_0, $AI(f_0) = k$, *для которой*

$$nl_r(f_0) = min_{deg(g) \leq r} dim(B_{k-1}(g)).$$

Теперь посмотрим какие конкретные оценки можно получить из этой теоремы.

Утверждение 4. *Пусть* $deg(f) = r$, *тогда* $dim(B_{k-1}(f))$ *не меньше чем* $\sum_{i=0}^{k-r-1} \binom{n}{i}$.

Доказательство. Просто берем все функции степени не больше $(k-r-1)$.

Следствие 3. *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}.$$

Мы получили оценку из работы [3].

Утверждение 5. *Пусть* $deg(f) = r$, *тогда* $dim(B_{k-1}(f))$ *не меньше чем* $2\sum_{i=0}^{k-r-1}\binom{n-r}{i}$.

Доказательство. Можно считать, что полином f содержит слагаемое $x_1x_2\dots x_r$. Рассмотрим функции вида $fg_1 + (f+1)g_2$, где g_1 и g_2 любые функции от $x_{m+1},\dots,x_n$ степени не более $(k-r-1)$. Несложно проверить, что все такие функции различны и принадлежат $B_{k-1}(f)$.

Следствие 4. *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq 2\sum_{i=0}^{k-r-1}\binom{n-r}{i}.$$

Мы получили оценку из работы [1].

Утверждение 6. *Пусть* $deg(f) = r$, *тогда* $dim(B_{k-1}(f))$ *не меньше чем*

$$\sum_{i=0}^{k-r-1}\binom{n}{i} + \sum_{i=k-2r}^{k-r-1}\binom{n-r}{i}.$$

Доказательство. Можно считать, что полином f содержит слагаемое $x_1x_2\dots x_r$. Рассмотрим функции вида $g_1 + fg_2$, где g_1 любая функции степени не более $(k-r-1)$, а g_2 любая функция от $x_{r+1},\dots,x_n$ степени не более $(k-r-1)$, содержащая лишь мономы длины не менее $k-2r$.

Несложно проверить, что все такие функции принадлежат $B_{k-1}(f)$. Проверка того, что все функции различны, сводиться к проверке того, что из $g_1 + fg_2 = 0$ следует $g_1 = 0$ и $g_2 = 0$. Равенство $g_2 = 0$ следует из того, что в противном случае функция fg_2 содержала бы моном длины не менее $(k-r)$, который был бы и в полиноме f (т.к. $\deg(f_1) \leq (k-r-1)$). Равенство $g_1 = 0$ следует непосредственно из $g_1 + fg_2 = 0$ и $g_2 = 0$.

Следствие 5. *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq \sum_{i=0}^{k-r-1}\binom{n}{i} + \sum_{i=k-2r}^{k-r-1}\binom{n-r}{i}.$$

Мы получили оценку, которая улучшает обе существовавших ранее оценки.

Список литературы

1. Carlet C. On the higher order nonlinearities of algebraic immune functions. CRYPTO 2006, LNCS 4117, pp. 584–601.

2. Courtois N and Meier W. Algebraic attacks on stream ciphers with linear feedback. In Anvances in Cryptology — EUROCRYPT 2003, LNCS 2656, pp. 345–359. Springer Verlag, 2003.

3. Dalai D. K., Gupta K. C. and Maitra S. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. Indocrypt 2004, Chennai, India, December 20-22, pages 92–106, LNCS 3348, Springer Verlag, 2004.

4 Lobanov M. Tight bound between nonlinearity and algebraic immunity. Cryptology ePrint archive(http://eprint.iacr.org/), Report 2005/437.

5. Meier W., Pasalic E. and Carlet C. Algebraic attacks and decomposition of Boolean functions. In Advances in Cryptology — EUROCRYPT 2004, LNCS 3027, pp. 474–491. Springer Verlag, 2004.

ГРАНИЧНЫЕ КЛАССЫ ОТНОСИТЕЛЬНО КЛАССА ПЛАНАРНЫХ ГРАФОВ ДЛЯ ЗАДАЧИ О НЕЗАВИСИМОМ МНОЖНСТВЕ

Д. С. Малышев (Нижний Новгород)

Введение

Независимым множеством в обыкновенном графе называется множество попарно несмежных вершин. Задача о независимом множестве для данного графа состоит в нахождении независимого множества наибольшей мощности. Для краткости задачу о независимом множестве будем называть *задачей НМ.*

Класс графов $\mathbf{K}$ называется *НМ-простым*, если существует алгоритм, решающий эту задачу для любого графа $G \in \mathbf{K}$ за полиномиальное время и *НМ-сложным*, если для графов этого класса задача НМ остается NP-полной [1].

Класс графов $\mathbf{X}$ называется *наследственным*, если он замкнут относительно изоморфизма, переименования ребер, удаления вершин и *сильно наследственным*, если он замкнут еще и относительно удаления ребер. Любой наследственный класс (и только наследственный класс) графов $\mathbf{X}$ может быть задан множеством запрещенных порожденных подграфов $\mathbf{S}$, это означает, что $\mathbf{X}$ состоит из тех и только тех графов, которые не имеют порожденных подграфов из $\mathbf{S}$. В этом случае принята запись $\mathbf{X}=Free(S)$. Если $\mathbf{S}$ является конечным, то такой наследственный класс называется *конечно определенным.*

В [1] дано определение граничного класса и доказано, что конечно определенный класс графов является НМ-сложным тогда и только тогда, когда в нем содержится какой-нибудь граничный класс. В этой работе вводится

более широкое понятие относительного граничного класса. Наследственный класс графов $\mathbf{X}$ назовем *предельным классом относительно наследственного класса* $\mathbf{Y}$ (*или предельным относительно* $\mathbf{Y}$), если существует такая последовательность $\mathbf{X}_1 \supseteq \mathbf{X}_2 \supseteq \ldots$ НМ-сложных классов, содержащихся в классе $\mathbf{Y}$, что $\cap_n \mathbf{X}_n = \mathbf{X}$. Минимальный по включению предельный относительно $\mathbf{Y}$ класс назовем *граничным относительно* $\mathbf{Y}$ *классом*. Из последнего определения следует, что $\mathbf{X} \subseteq \mathbf{Y}$. Класс $\mathbf{X}$ назовем *конечно определенным относительно наследственного класса* $\mathbf{Y}$, если существует такое конечное множество графов $\mathbf{M}$, что $\mathbf{X} = \mathbf{Y} \cap Free(\mathbf{M})$. Для относительных граничных классов легко доказывается обобщение теоремы 3 из работы [1], а именно, относительный конечно определенный класс графов является НМ-сложным тогда и только тогда, когда в нем содержится какой-нибудь относительный граничный класс.

Триодом $T_{i,j,k}$ называется дерево, имеющее ровно одну вершину степени три и ровно три листа, отстоящих от вершины степени три на расстояниях i, j, k соответственно. Пусть $\mathbf{T}$ — класс всех графов, у которых каждая из компонент связности является деревом не более чем с тремя листьями. Иными словами, класс $\mathbf{T}$ состоит только из тех графов, у которых каждая из компонент является либо триодом, либо простым путем. В работе [1] доказано, что $\mathbf{T}$ является граничным классом, а если $P \neq NP$, то $\mathbf{T}$— единственный сильно наследственный граничный класс. Возможно, $\mathbf{T}$— единственный граничный класс не только среди сильно наследственных. Доказательство этого предположения равносильно доказательству того, что для любого графа $G \in \mathbf{T}$ класс $Free(G)$ является НМ-простым. К настоящему времени это доказано для графов с не более 5 вершинами из $\mathbf{T}$ (за исключением P_5 и графов вида $pK_2 + qK_1$). Таким образом, вопрос о единственности $\mathbf{T}$ как граничного класса оказался сложным.

В настоящей работе рассматривается класс планарных графов. Класс $\mathbf{T}$ является граничным относительно **Planar**. Доказательство этого легко получить по аналогии с доказательством теоремы 4 из [1]. Возможно, что $\mathbf{T}$ — единственный граничный класс относительно **Planar**. Это утверждение пока не доказано, но в его исследовании удалось продвинуться значительно дальше, чем в исследовании аналогичного предположения для класса всех графов. В настоящей публикации доказывается НМ-простота класса $\mathbf{Planar} \cap Free(T_{1,1,i})$ для любого натурального i.

Определения и результаты

Предположим, что имеется планарный граф G и что он задан в виде своей плоской укладки. Определим понятие *глубины* графа G. Из плоской укладки графа G удалим вершины с инцидентными им ребрами, принадлежащие внешней грани. Множество этих вершин обозначим через V_1. С оставшейся укладкой будем проделывать аналогичную операцию до тех

пор, пока множество вершин не станет пустым. В результате мы получим разбиение множества вершин графа на подмножества $V_1, V_2, \ldots, V_k$, которые будем называть *уровнями* графа. Величину k назовем глубиной графа G и будем обозначать $\gamma(G)$.

Разделяющая клика графа — это множество вершин, порождающее полный подграф, удаление которого приводит к увеличению числа компонент связности. Назовем *C-блоком* максимальный по включению порожденный подграф данного графа, не имеющий разделяющей клики. Пусть $\mathbf{K}$— некоторый класс графов, тогда обозначим через $[\mathbf{K}]_c$ множество всех графов, у которых каждый C-блок принадлежит $\mathbf{K}$. В дальнейшем, нам понадобятся две операции над классами графов, которые сохраняют свойство HM-простоты.

Лемма 1 [1]. *Если* $\mathbf{X}$ *— HM-простой наследственный класс графов, то* $[\mathbf{X}]_c$ *также является HM-простым.*

Следствие. *Класс планарных графов единичной глубины является HM-простым.*

Лемма 2 [2]. *Если* $\mathbf{K}$ *— HM-простой наследственный класс, то для любого фиксированного* r *класс* $[\mathbf{K}]_r$ *является HM-простым.*

Лемма 3. *Если* G *- связный граф и* G *не принадлежит классу* $Free(T_{1,1,i})$ $(i \geq 3)$, *то либо* $G \in Free(T_{1,1,1})$, *либо* $diam(G) < 2i + 3$.

Следствие. *Если* G *— связный граф* и $G \in \mathbf{Planar} \cap Free(T_{1,1,i})$ $(i \geq 3)$, *то* $\gamma(G) < 2i + 3$.

Если G не содержит разделяющих клик, а V_1 — первый уровень графа G, то граф, порожденный множеством V_1, является простым циклом. Для каждой вершины $x \in V(G) \setminus V_1$ определим множество $N(x, V_1)$ всех вершин из V_1, смежных с x. Пусть $deg(x, V_1)$ - мощность множества $N(x, V_1)$. Для каждой вершины $x \in V(G) \setminus V_1$ определим величину $m(x)$ как максимальное количество последовательных вершин из V_1, не смежных с x.

Лемма 4. *Пусть* $\gamma(G) > 1$ *и* G *— C-блок, не содержащий порожденного* $T_{1,1,i}$, V_1 *— первый уровень графа* G. *Тогда, если для некоторой вершины* $x \in V(G) \setminus V_1$ *выполнено неравенство* $deg(x, V_1) > 5$, *то* $m(x) < i + 1$.

Теорема. *Для любого натурального* i *класс* $\mathbf{Planar} \cap Free(T_{1,1,i})$ *является HM-простым*

Доказательство. Обозначим через $\mathbf{Q}_{i,r}$ подмножество класса $\mathbf{Planar} \cap Free(T_{1,1,i})$, состоящее из графов глубины не более чем r. Покажем, что для любых натуральных i и r класс $\mathbf{Q}_{i,r}$ является НМ-простым.

Известно [3,4], что классы $Free(T_{1,1,i})$ при $i = 1, 2$ являются НМ-простыми. Отсюда следует НМ-простота рассматриваемых классов $\mathbf{Q}_{i,r}$ при $i = 1, 2$ и любых r. Пусть теперь $i \geq 3$. Дальнейшее доказательство проведем индукцией по r. Класс $\mathbf{Q}_{i,1}$ является НМ-простым ввиду следствия леммы 1.

Пусть G — связный граф из $\mathbf{Q}_{i,r+1}$. Если $G \in Free(T_{1,1,1})$, то задача НМ для графа G полиномиально разрешима. Поэтому будем считать, что $G \in \mathbf{Q}_{i,r+1} \setminus Free(T_{1,1,1})$. Ввиду леммы 1 можно считать, что G не содержит разделяющих клик. Из леммы 3 следует, что $diam(G) < 2i + 3$. Пусть V_1 — первый уровень графа G. Если $|V_1| \leq 2i + 3$, то $G \in [\mathbf{Q}_{i,r}]_{2i+3}$. Из леммы 2 следует, что класс $[\mathbf{Q}_{i,r}]_{2i+3}$ НМ-простой. Далее будем считать, что $|V_1| > 2i + 3$.

Пусть $v_1, v_2, \ldots, v_t$ — все вершины из V_1 и пусть они покрашены в черный цвет. Рассмотрим вершины v_1 и $v_{[t/2]}$. Пусть P — путь из v_1 в $v_{[t/2]}$ длины, меньшей чем $2i+3$. Рассмотрим всевозможные независимые множества подграфа, порожденного множеством вершин этого пути. Для каждого такого множества S рассмотрим граф $G^*(S)$, порожденный множеством вершин $V(G) \setminus (N(S) \cup V(P))$, где $V(P)$ — множество вершин подграфа, порожденного вершинами из P, $N(S)$ — множество тех вершин графа G, которые смежны хотя бы с одной вершиной из множества S. Ясно, что зная решение задачи НМ для графов $G^*(S)$ для всех S, можно за время $O(1)$ найти решение задачи НМ для графа G. Пусть $G_1(S), \ldots, G_p(S)$ — те компоненты связности графа $G^*(S)$, которые содержат черные вершины и имеют глубину, равную $r + 1$. (Остальные компоненты принадлежат классу $\mathbf{Q}_{i,r}$) Если множество S содержит такую вершину x, что $deg(x, V_1) > 5$, то ввиду леммы 4 каждый из этих графов содержит не более чем $i + 1$ черную вершину, а следовательно, каждый из них принадлежит НМ-простому классу $[\mathbf{Q}_{i,k}]_{i+1}$. Если такой вершины не найдется, то ясно, что $p \leq 5|S| < 10i + 15$. Каждый из графов $G_1(S), \ldots, G_p(S)$ содержит не более $[t/2]+1$ черных вершин, причем в каждом из них на первом уровне все черные вершины стоят последовательно. К каждому из этих графов применимы те же действия, что и к графу G. (т.е. если рассматриваемый граф $G_i(S)$ $(i = 1, \ldots, p)$ не принадлежит ни классу $Free(T_{1,1,1})$, ни классу $[\mathbf{Q}_{i,k}]_{2i+3}$, то концы пути P_i следует выбирать по следующему правилу — на первом уровне графа $G_i(S)$ такие две вершины, что одна из них является черной, делящей последовательно стоящие черные вершины на две "дуги", отличающиеся не более чем на одну вершину.)

Таким образом, всю процедуру решения задачи НМ для графа G можно изобразить в виде дерева решений. Листья этого дерева соотвествуют

графам из классов $[\mathbf{Q}_{i,k}]_{2i+3} \setminus Free(T_{1,1,1})$, $Free(T_{1,1,1})$, а внутренние узлы соответствуют графам, содержащим не менее $2i+3$ черных вершин и имеющих глубину, равную $k+1$ и не принадлежащих классу $Free(T_{1,1,1})$. Т.к. множество черных вершин каждый раз делится на две почти равные части, то высота данного дерева ограничена сверху величиной $\lceil \log_2(n) \rceil$.

Оценим в дереве решений общее количество внутренних узлов. Каждый внутренний узел имеет не более чем $c = (10i+15)2^{2i+3}$ непосредственных потомков, являющихся внутренними узлами, следовательно, общее количество внутренних узлов в дереве решений не превосходит $c^{\lceil \log_2(n) \rceil + 1}$, т.е. ограничено полиномом от n. Общее число потомков каждого внутреннего узла, являющихся листьями, не превосходит n, следовательно, число узлов в дереве решений ограничено сверху полиномом от n.

Утверждение теоремы следует из следствия леммы 3 и НМ-простоты класса $Q_{i,r}$ для любых натуральных i и r.

Список литературы

1 Alekseev V.E. On easy and hard hereditary classes of graphs with respect to the independent set problem. Discrete Applied Mathematics 132(2004

2 Алексеев В.Е., Коробицын Д.В. О сложности некоторых задач на наследственных классах графов. Дискретная математика, 1992г. Т. 4, вып. 4.

3 Minty.G.J. On maximal independent sets in claw-free graphs. J.Combin Theory Ser.B 28(3) (1980).

4 Алексеев. В.Е. Полиномиальный алгоритм для нахождения наибольшего независимого множества в графах без вилок. Дискретный анализ и исследование операций. Серия 1. Том 6, номер 4. Новосибирск: Из-во института математики, 1999г.

СЛОЖНОСТЬ ПРИМЕНЕНИЯ СИМВОЛЬНЫХ МЕТОДОВ В КРИПТОАНАЛИЗЕ АЛГОРИТМА ГОСТ 28147-89

А. С. Мелузов (Москва)

Введение. В статье описан способ применения символьных методов криптографического анализа к алгоритму ГОСТ 28147-89. Для этого приведены способы построения системы полиномиальных уравнений, описывающих работу алгоритма ГОСТ 28147-89, проведена оценка сложности и

структуры получаемой системы полиномиальных уравнений, а также проведена оценка эффективности алгоритмов решения систем полиномиальных уравнений над конечными полями с использованием стандартных базисов (базисов Гребнера).

1. Постановка задачи. В настоящее время в целях криптоанализа широко используется следующий подход, целиком и полностью основанный на методах символьных вычислений в кольцах многочленов над различными алгебраическими структурами. А именно: с использованием различных методик функционирование криптосхемы описывается с помощью системы полиномиальных уравнений над какой-либо алгебраической структурой (как правило, над конечным полем) с тем, чтобы иметь возможность свести задачу криптоанализа к решению построенной системы полиномиальных уравнений в символьном виде. Как правило, этот шаг выполняется путем построения базиса Грёбнера соответствующего полиномиального идеала с использованием одного из широко известных алгоритмов, таких, как алгоритм Бухбергера, XL-метод, алгоритмы F_4 и F_5, принадлежащие Ж.-К. Фажере.

Необходимо применить данный подход к алгоритму блочного шифрования ГОСТ 28147-89 в режиме простой замены.

2. Алгоритм ГОСТ 28147-89. В режиме простой замены алгоритм ГОСТ 28147-89 работает следующим образом: открытые данные, подлежащие зашифрованию, разбивают на блоки по 64 бит в каждом. Блок открытого текста представляется в виде конкатенации двух блоков по 32 бита каждый:

$$T_0 = (a_1(0), \ldots, a_{32}(0), b_1(0), \ldots, b_{32}(0)) = a(0)||b(0), \tag{1}$$

где в последующем a_1 считается младшим, а a_{32} — старшим битом двоичной записи некоторого целого числа.

Объем ключа составляет 256 бит $(W_{256}, \ldots, W_1)$, которые разбиваются на восемь 32-х разрядных вектора

$$\begin{gathered} X_0 = (W_{32}, \ldots, W_1), \\ X_1 = (W_{64}, \ldots, W_{33}) \\ \ldots\ldots \\ X_7 = (W_{256}, \ldots, W_{225}). \end{gathered} \tag{2}$$

Уравнения зашифрования в режиме простой замены имеют вид:

$$\begin{cases} a(j) = \left(a(j-1) + X_{(j-1) \bmod 8}\right) KR \oplus b(j-1), \\ b(j) = a(j-1), j = \overline{1,24}, \\ a(j) = \left(a(j-1) + X_{(32-j)}\right) KR \oplus b(j-1), \\ b(j) = a(j-1), j = \overline{25,31}, \\ a(32) = a(31), \\ b(32) = (a(31) + X_0) KR \oplus b(31). \end{cases} \tag{3}$$

Здесь + — операция сложения по модулю 2^{32} двух чисел, двоичным представлением которых являются операнды, причем результатом операции является двоичный вектор длины 32, являющийся двоичным представлением получившегося 32-х разрядного числа.

Преобразование K выглядит следующим образом: поступающтй на его вход 32-х разрядный вектор разбивается на 8 подвекторов длины 4, каждый из которых, в свою очередь, поступает на вход соответствующего *узла замены* $K_1, \ldots, K_8$, осуществляющего перестановку на множестве двоичных векторов длины 4. Восемь результатов перестановок путем конкатенации составляют результирующий вектор:

$$XK = (X_8 || \ldots || X_1)\, K = (K_8(X_8) || \ldots || K_1(X_1))\,. \tag{4}$$

R — операция циклического сдвига на одиннадцать шагов в сторону старших разрядов:

$$(y_{32}, \ldots, y_1)R = (y_{21}, y_{20}, \ldots, y_2, y_1, y_{32}, y_{31}, \ldots, y_{23}, y_{22}). \tag{5}$$

Операция $\oplus$ есть покоординатное суммирование 32-разрядных векторов по модулю 2.

3. Построение системы полиномиальных уравнений. Обратимся теперь к вопросу о построении системы полиномиальных уравнений, аппроксимирующей зашифрование в режиме простой замены согласно алгоритму ГОСТ 28147-89.

Очевидно, что для того, чтобы построить полиномиальную аппроксимацию полного алгоритма зашифрования, достаточно построить полиномиальную аппроксимацию для одного раунда. Полиномиальная аппроксимация для 32 раундов получается путем введения дополнительных переменных и дупликации системы.

3.1. Модульное сложение. Первый этап при построении системы полиномиальных уравнений, аппроксимирующей один раунд алгоритма ГОСТ 28147-89, состоит в том, чтобы выразить координаты двоичного представления суммы двух чисел по модулю 2^{32} как булевы функции от координат двоичных представлений складываемых чисел.

Это можно сделать, итеративно вычисляя функции переноса в старший разряд и, на их основе, координатные функции, согласно формулам [4,(1)]: для $\bar{r} = (r_0, \ldots, r_{n-1}), \bar{x} = (x_0, \ldots, x_{n-1}), \bar{a} = (a_0, \ldots, a_{n-1})$ при

$$\begin{aligned} &r_0 + r_1 \cdot 2 + \cdots + r_{n-1} \cdot 2^{n-1} = \\ &\quad = (x_0 + \cdots + x_{n-1} \cdot 2^{n-1}) + (a_0 + \cdots + a_{n-1} \cdot 2^{n-1}) \pmod{2^n} \end{aligned} \tag{6}$$

имеют место равенства:

$$\begin{aligned} &r_0 = x_0 \oplus a_0 \oplus c_0, \quad c_0 = 0, \\ &r_i = x_i \oplus a_i \oplus c_i, \quad c_i = x_{i-1}a_{i-1} \oplus x_{i-1}c_{i-1} \oplus a_{i-1}, \\ &i = \overline{1, n-1}. \end{aligned} \tag{7}$$

Как видно из соотношений (6) и (7), i-я координатная функция суммы $\bar{x} + \bar{a}$ имеет степень $i + 1$, и содержит $2^i + 1$ термов. Поэтому нахождение координатных функций суммы $\bar{x} + \bar{a}$ при значениях i, близких к 32, является трудоемкой вычислительной задачей, невыполнимой на обычном персональном компьютере.

3.2. Блоки замены. Второй этап построения системы полиномиальных уравнений, аппроксимирующей один раунд криптоалгоритма ГОСТ 28147-89, состоит в том, чтобы построить покоординатную аппроксимацию булевыми функциями узлов замены с последующим вычислением композиции полученной аппроксимации и найденных на первом этапе координатных функций модульного сложения. Можно сделать двумя способами.

Во-первых, естественный способ состоит в представлении каждого узла замены $K_i, i = \overline{1,8}$ как вектора $(f_{i,1}, \ldots, f_{i,4})$ из четырех булевых функций от четырех переменных.

Во-вторых, можно обратиться к методике, предложенной в статье [2, Раздел 3.2].

Каждая методика имеет свои плюсы и свои минусы. Первый способ предпочтителен по той причине, что в этом случае не приходится вводить новые служебные переменные, и, таким образом, число переменных, входящих в уравнения системы, значительно ниже. Однако сами уравнения, как правило, имеют более высокую степень и состоят из большего числа термов. Второй способ имеет своим преимуществом то, что этот путь позволяет получить значительно большее число уравнений, причем фиксированной степени (а именно по 21 уравнению степени не выше 2 от входных переменных для каждого узла замены).

При использовании второго способа, структура итоговой системы полиномиальных уравнений представляется более ясной, поэтому будем использовать именно его.

3.3. Сдвиг и побитовое сложение. Последний этап построения системы полиномиальных уравнений, аппроксимирующей один раунд криптоалгоритма ГОСТ 28147-89, состоит в подстановке в полученные уравнения переменных, соответствующих результату работы данного раунда, просуммированных с переменными, описывающими результат работы раунда за два до текущего в соответствии с (3) (или с битами левой части открытого текста, если описываемый раунд — первый и правой части открытого текста, если второй) с учетом операции побитового сдвига, в соответствии с (3). Для этого выходы узлов замены были выражены через левую (правую) часть открытого текста (или результат работы раунда за два до текущего), а выходы — через результат работы описываемого раунда работы алгоритма (или зашифрованный текст, если описываемый раунд — последний или предпоследний). Если y_i — i-й бит выхода узлов замены, z_i — i-й бит результата работы текущего раунда текста, а l_i — i-й бит результата работы

предыдущего раунда, то верно следующее соотношение:

$$y_i = z_{(i+11) \bmod 32} + l_{(i+11) \bmod 32}.$$

3.3. Построение итоговой системы. Таким образом, мы получим системы полиномиальных уравнений, описывающие каждый раунд алгоритма шифрования ГОСТ 28147-89. С помощью отождествления переменных, соответствующим одним и тем же значениям (например, результаты работы первого раунда будут складываться со значениями, полученными после побитового сдвига в третьем раунде, а также подаваться на вход регистра модульного сложения с ключом во втором раунде), получим систему полиномиальных уравнений, описывающую алгоритм шифрования ГОСТ 28147-89 целиком.

Итак, при анализе криптографического алгоритма ГОСТ 28147-89 было показано, что система полиномиальных уравнений, аппроксимирующая его работу в режиме простой замены зависит от 1248 переменных (из которых 256 — биты ключа, а 992 — вспомогательные переменные (промежуточные результаты работы на каждом раунде)), и состоит из 5376 уравнений, по 672 уравнения 7,15,23,31,39,47,55 и 63 степени.

4. Оценка сложности решения построенной системы. После построения системы полиномиальных уравнений, аппроксимирующей работу алгоритма ГОСТ 28147-89, необходимо её решить. Решение СПУ будем осуществлять методом построения базиса Грёбнера.

Существует довольно много алгоритмов, строящих базис Грёбнера заданной системы уравнений, однако, самым быстрым на данный момент является алгоритм F_5, принадлежащий Ж.-К. Фажере.

В статье [1] подробно рассматриваются особенности применения этого алгоритма к полиномам над полем $GF(2)$.

Суть алгоритма состоит в построении последовательности матриц $\mathcal{M}_{d,m}$, столбцы которых соответствуют всевозможным мономам степени d, выстроенным в лексикографичеком порядке, а строки соответствуют всевозможным произведениям $t \times f_j$, где t — моном, такой что $deg(t \times f_j) = d$, а $1 \leq j \leq m$, $f_1, \ldots, f_m$ – полиномы, входящие в исходную систему.

Далее, над каждой такой матрицей производятся преобразования, приводящие её к треугольному виду. Поскольку матрица сильно разряжена, можно считать, что сложность таких преобразований будет равна $\mathcal{O}(k^2)$, где k — ранг матрицы $\mathcal{M}_{d,m}$.

Общая сложность алгоритма определяется сложностью вычислений линейной алгебры для наибольшей матрицы. В соответствии с [1] такой матрицей будет та, которая соответствует полиномам степени D_{reg}. А D_{reg} — степень полурегулярности исходной системы. Степень полурегулярности вычисляется как номер первого неположительного члена порождающего ряда

последовательности полиномов (исходной системы). Сумма порождающего ряда равна $S_{m,n}(z) = (1+z)^n / \prod_{k=1}^{m}(1+z^{d_k})$, где n — число неизвестных в исходной системе, d_k — степень k-того полинома, $f_1, \ldots, f_m$ — полиномы, входящие в исходную систему.

В соответствии с описанной в [1] методикой, был построен порождающий ряд последовательности полиномов, описывающей работу алгоритма ГОСТ 28147-89 в режиме простой замены:

$$\frac{(1+z)^{1248}}{((1+z^7)(1+z^{15})(1+z^{23})(1+z^{31})(1+z^{39})(1+z^{47})(1+z^{55})(1+z^{63}))^{672}}$$

и найден его первый неположительный член, номер которого соответствует степени регулярности системы полиномиальных уравнений (последовательности полиномов). Степень полурегулярности для системы полиномиальных уравнений, описывающей работу криптоалгоритма ГОСТ 28147-89 в режиме простой замены $D_{reg} = 402$.

Следовательно, максимальный размер матрицы в алгоритме F_5 будет равен рангу матрицы $\mathcal{M}_{d,m}$ на шаге D_{reg} и равен числу столбцов этой матрицы, то есть

$$\binom{n}{D_{reg}} = \binom{1248}{402} \approx 2^{1126},$$

а сложность вычисления базиса Гребнера построенной системы будет равна $\mathcal{M} \cdot 2^{2252}$, при допущении, что коэффициент сложности вычислений линейной алгебры $\omega = 2$, по причине сильной разреженности матриц. Здесь $\mathcal{M}$ – константа, зависящая от вычислительной техники, на которой будет выполняться алгоритм.

Однако, можно добиться ускорения алгоритма с помощью применения параллельных вычислений. Векторные команды и одновременное вычисление независимых по данным частей алгоритма могут значительно ускорить вычисления.

Необходимо заметить, что основную роль в сложности играет длина блока и количество раундов. Например, если применить аналогичные рассуждения к алгоритму, в котором по сравнению с ГОСТ 28147-89 длина блока 16 бит, длина ключа 16 бит, а число раундов равно 2, то получим систему уравнений, его аппроксимирующую, которая состоит из 84 уравнений, по 42 уравнения 7 и 15 степеней. Дополнительных переменных не будет (результат работы первого раунда является левой частью шифрованного текста), то есть всего будет 16 неизвестных – биты ключа. В разложении в ряд следующего выражения:

$$\frac{(1+z)^{16}}{((1+z^7)(1+z^{15}))^{42}}$$

первым неположительным членом будет член с номером 10. То есть степень полурегулярности такой системы равна 10, размер матрицы в алгоритме F_5 будет равен 8008, а сложность вычислений $\approx 2^{26}$. Отметим, что это верхняя оценка. На практике, уравнения могут иметь меньшие степени, и сложность вычислений будет меньше.

Список литературы

1. Magali Bardet, Jean-Charles Faugère, Bruno Salvy. Complexity of Gröebner basis computation for Semi-regular Overdetemined sequences over F_2 with solutions in F_2.

2. Courtois N. T., PieprzykJ . Crytoanalysis of block ciphers with overdefined systems of equations. // ASIACRYPT 2002, LNCS 2501, pp.267–287, 2002.

3. Jean-Charles Faugère. A new efficient algorithm for computation Gröebner bases without reduction to zero (F_5).

4. Braeken A., Semaev I. The ANF of the Composition of Addition and Multiplication mod2^n with a Boolean Function // Fast Software Encryption 2005, Proceedings, pp. 115–127.

О РАНГЕ НЕЯВНЫХ ПРЕДСТАВЛЕНИЙ НАД КЛАССАМИ МОНОТОННЫХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

Е. В. Михайлец (Москва)

Понятие неявной выразимости функций k-значной логики введено А. В. Кузнецовым как одно из обобщений понятия выразимости функций суперпозициями [3].

Пусть A — произвольная система функций k-значной логики, $A \subseteq P_k$. *Системой неявных уравнений* над системой функций A будем называть всякую систему уравнений вида

$$\begin{cases} \Phi_1(x_1, \ldots, x_n, y) = \Psi_1(x_1, \ldots, x_n, y), \\ \ldots \\ \Phi_q(x_1, \ldots, x_n, y) = \Psi_q(x_1, \ldots, x_n, y), \end{cases} \tag{1}$$

где $\Phi_1, \ldots, \Phi_q$, $\Psi_1, \ldots, \Psi_q$ — некоторые формулы над системой функций A.

Говорят, что функция $f(x_1, \ldots, x_n)$ k-значной логики *неявно выразима* над системой функций A, если существует система неявных уравнений над

A вида (1), имеющая при любых фиксированных значениях $x_1, \ldots, x_n$ единственное решение $y = f(x_1, \ldots, x_n)$. При этом соответствующую систему уравнений называют *неявным представлением* функции $f(x_1, \ldots, x_n)$ над A.

Множество всех функций f, $f \in P_k$, неявно выразимых над системой функций A, называется *неявным расширением* системы A и обозначается через $I(A)$ [2]. Благодаря очевидному соотношению $I(A) = I([A])$, при исследовании неявных расширений можно ограничиться рассмотрением только замкнутых относительно суперпозиции классов функций k-значной логики.

Если любая функция k-значной логики неявно выразима над A, т. е. $I(A) = P_k$, то систему функций A называют *неявно полной* в P_k.

Рассмотрим произвольную функцию f из неявного расширения некоторой системы A функций k-значной логики, $f \in I(A)$. Назовем *рангом* функции f над системой A и будем обозначать через $m_A^k(f)$ наименьшее число уравнений, достаточное для построения неявного представления f над A.

Как обычно, вводится функция Шеннона $m_A^k(n) = \max m_A^k(f)$, называемая *ранговой функцией* системы A (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 [1] исследовал поведение ранговой функции $m_A^2(n)$ для всех замкнутых классов булевых функций. Для классов D_2 и F_i^μ, где $i = 2, 3, 6, 7$ и $\mu = 2, 3, \ldots, \infty$, в работе [1] получены порядки роста величины $m_A^2(n)$, а для всех остальных замкнутых классов найден точный вид ранговой функции. В частности, для класса монотонных функций О. М. Касим-Заде [1] доказал следующую теорему.

Теорема 1. *При всех натуральных n для ранговой функции $m_A^2(n)$, где A — класс монотонных функций в P_2, имеет место равенство*

$$m_A^2(n) = \left\lceil \frac{n+2}{2} \right\rceil .$$

В k-значной логике можно рассмотреть обобщения понятия монотонности, отвечающие различным частичным порядкам на множестве E_k, где $E_k = \{0, 1, \ldots, k-1\}$. В частности, можно ввести определение монотонной функции следующим образом.

Пусть $\mathfrak{M}$ — произвольный частичный порядок, заданный на множестве E_k. Отношение порядка $\mathfrak{M}$ будем обозначать символом "$\leq_{\mathfrak{M}}$".

Цепью в частично упорядоченном множестве $< E_k; \mathfrak{M} >$ будем называть всякую последовательность различных попарно сравнимых элементов $\alpha^0 \leq_{\mathfrak{M}} \alpha^1 \leq_{\mathfrak{M}} \cdots \leq_{\mathfrak{M}} \alpha^r$ из этого множества. *Длиной цепи* называется

величина, на единицу меньшая, чем число элементов цепи. То есть длина цепи из $r+1$ элементов равна r. Каждому частичному порядку $\mathfrak{M}$ можно поставить в соответствие максимальную длину цепи в частично упорядоченном множестве $< E_k; \mathfrak{M} >$, обозначаемую через $s(\mathfrak{M})$. Легко видеть, что $0 \leq s(\mathfrak{M}) \leq k-1$.

Пусть помимо частичного порядка $\mathfrak{M}$ на множестве E_k задан еще один частичный порядок $\mathfrak{M}'$. Если для любых $\alpha, \beta \in E_k$ таких, что $\alpha \leq_{\mathfrak{M}'} \beta$, выполняется отношение $\alpha \leq_{\mathfrak{M}} \beta$, то будем говорить, что порядок $\mathfrak{M}'$ *подчинен* порядку $\mathfrak{M}$ и факт подчиненности обозначать через $\mathfrak{M}' \subseteq \mathfrak{M}$. Легко видеть, что для порядков, удовлетворяющих условию $\mathfrak{M}' \subseteq \mathfrak{M}$, справедливо $s(\mathfrak{M}') \leq s(\mathfrak{M})$.

Совокупность всех наборов $(\alpha_1, \ldots, \alpha_n)$ с компонентами из E_k: $\alpha_i \in E_k, 1 \leq i \leq n$, будем обозначать через E_k^n ($E_k^n = \underbrace{E_k \times \cdots \times E_k}_{n \text{ раз}}$) [4].

Отношение частичного порядка $\mathfrak{M}$, заданное на множестве E_k, можно естественным образом распространить на множество E_k^n. Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ — наборы с компонентами из $< E_k; \mathfrak{M} >$. Положим $\tilde{\alpha} \leq_{\mathfrak{M}} \tilde{\beta}$, если $\alpha_i \leq_{\mathfrak{M}} \beta_i$ для любого $i, 1 \leq i \leq n$.

Рассмотрим произвольную функцию k-значной логики $f(x_1, \ldots, x_n)$, $f : E_k^n \to E_k$. Зададим на области определения функции f частичный порядок $\mathfrak{M}$, на области значений — порядок $\mathfrak{M}'$, причем $\mathfrak{M}' \subseteq \mathfrak{M}$. Назовем функцию f *монотонной относительно пары порядков* $(\mathfrak{M}, \mathfrak{M}')$, если для любых наборов значений аргумента $\tilde{\alpha}$ и $\tilde{\beta}$ таких, что $\tilde{\alpha} \leq_{\mathfrak{M}} \tilde{\beta}$, имеет место соотношение $f(\tilde{\alpha}) \leq_{\mathfrak{M}'} f(\tilde{\beta})$.

В настоящей работе утверждается, что все классы функций k-значной логики, монотонных относительно любой пары порядков $(\mathfrak{M}, \mathfrak{M}')$, удовлетворяющей условиям $\mathfrak{M}' \subseteq \mathfrak{M}$ и $s(\mathfrak{M}') \geq 1$, являются неявно полными. Ограничение $s(\mathfrak{M}') \geq 1$ означает наличие в частично упорядоченном множестве $< E_k; \mathfrak{M}' >$ хотя бы одной пары сравнимых элементов, отличных друг от друга. Также получено точное выражение для ранговой функции указанных классов функций, зависящее явно только от n и от максимальных длин цепей $s(\mathfrak{M})$ и $s(\mathfrak{M}')$. В случае совпадения максимальных длин цепей, отвечающих порядкам $\mathfrak{M}$ и $\mathfrak{M}'$, выражение для ранговой функции совпадает с выражением из теоремы 1. Сформулируем основную теорему.

Теорема 2. *Пусть $k \geq 2$ и на множестве E_k заданы частичные порядки $\mathfrak{M}$ и $\mathfrak{M}'$ такие, что $\mathfrak{M}' \subseteq \mathfrak{M}$ и $s(\mathfrak{M}') \geq 1$. Пусть A — класс всех функций в P_k, монотонных относительно пары порядков $(\mathfrak{M}, \mathfrak{M}')$. Тогда система функций A неявно полна в P_k и ранговая функция системы A имеет вид*

$$m_A^k(n) = \left\lceil \frac{(n+1)s(\mathfrak{M}) + 1}{2s(\mathfrak{M}')} \right\rceil .$$

Следствие 1. *В условиях теоремы* 2 *при выполнении равенства* $s(\mathfrak{M}) = s(\mathfrak{M}')$ *выражение для ранговой функции системы* A *приобретает вид*

$$m_A^k(n) = \left\lceil \frac{n+2}{2} \right\rceil .$$

В частности, следствие имеет место, если частичный порядок $\mathfrak{M}'$ совпадает с порядком $\mathfrak{M}$.

Автор выражает благодарность своему научному руководителю О. М. Касим-Заде за всестороннее внимание к данной работе. Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00994), Программы поддержки ведущих научных школ РФ и Программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

1. 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.

2. Касим–Заде О. М. О неявной выразимости булевых функций // Вестник МГУ. Математика. Механика. — 1995. — № 2. — С. 44–49.

3. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука, 1979. — С. 5–33.

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

ПЕРИОДИЧНОСТЬ СОВЕРШЕННЫХ РАСКРАСОК РАДИУСА r > 1 БЕСКОНЕЧНОЙ ПРЯМОУГОЛЬНОЙ РЕШЕТКИ

С. А. Пузынина (Новосибирск)

Раскраска вершин графа G в n цветов называется совершенной радиуса r, если количество вершин цвета j в шаре радиуса r с центром в вершине цвета i не зависит от выбора вершины. Параметры совершенной раскраски задаются квадратной матрицей порядка n. Совершенные раскраски радиуса 1 ранее изучались и имели различные названия, в частности,

equitable partitions, partition designes, делитель графа. Понятие совершенной раскраски является обобщением понятия совершенного кода, фактически совершенный код является частным случаем совершенной раскраски в два цвета.

Изучаются совершенные раскраски графа бесконечной прямоугольной решетки. Раскраски этого графа можно рассматривать как двумерные слова над конечным алфавитом цветов.

Доказано, что каждая совершенная раскраска радиуса $r > 1$ графа бесконечной прямоугольной решетки является периодической.

1. Введение

Пусть G — граф, $A = (a_{ij})$ — квадратная матрица порядка n, $r \geq 1$. Рассмотрим раскраску графа G в n цветов и произвольную вершину x цвета i. Если количество вершин цвета j (отличных от x) на расстоянии не более r от вершины x не зависит от выбора вершины x и равно a_{ij}, то раскраска называется *совершенной радиуса* r с матрицей A. Ранее совершенные раскраски радиуса 1 изучались в различных контекстах и имели различные названия, в частности, их называли equitable partitions (равномерными разбиениями) [3].

В настоящей работе рассматриваются совершенные раскраски графа $G(\mathbb{Z}^2)$ бесконечной прямоугольной решетки. Назовем матрицу A *допустимой*, если существует совершенная раскраска графа $G(\mathbb{Z}^2)$ с матрицей A для соответствующего r. Основной результат заключается в том, что любая совершенная раскраска радиуса $r > 1$ бесконечной прямоугольной решетки является периодической. Совершенные раскраски бесконечной прямоугольной решетки могут рассматриваться как двумерные слова над конечным алфавитом цветов. Для доказательства этого факта используется метод R-продолжаемых слов, который был предложен в [4] и использован для изучения двумерных слов другого типа, называемых центрированными функциями.

Заметим, что случай $r \geq 2$ принципиально отличается от случая $r = 1$. Существуют непериодические совершенные раскраски радиуса 1. В [5] доказано, что для любой допустимой матрицы радиуса 1 существует периодическая совершенная раскраска, причем она может быть получена из непериодической методом свитчинга бинарных диагоналей. Бинарная диагональ — это диагональ, состоящая из двух чередующихся цветов, под свитчингом бинарной диагонали подразумевается перестановка цветов внутри диагонали.

В [1] М. Аксенович классифицировала все допустимые матрицы совершенных раскрасок радиуса 1 в 2 цвета бесконечной прямоугольной решетки и нашла некоторые необходимые условия для того, чтобы матрица была допустимой радиуса $r \geq 2$.

Понятие совершенной раскраски — это обобщение понятия совершенного кода. Действительно, совершенная раскраска n-регулярного графа с матрицей $\begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$ является совершенным кодом с расстоянием 3 (кодовые вершины — это вершины цвета 1).

2. Определения и обозначения

Пусть $G = (V, E)$ — граф. Расстояние между двумя вершинами $\mathbf{x}$ и $\mathbf{y}$, обозначаемое $d(\mathbf{x}, \mathbf{y})$, — это обычная графская метрика. *Шар* $B_r(\mathbf{x})$ радиуса r с центром в вершине $\mathbf{x}$ определяется следующим образом:

$$B_r(\mathbf{x}) = \{\mathbf{y} \in V |\ d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Аналогично *сфера* $S_r(\mathbf{x})$ задается следующим условием:

$$S_r(\mathbf{x}) = \{\mathbf{y} \in V |\ d(\mathbf{x}, \mathbf{y}) = r\}.$$

Пусть $A = (a_{ij})_{i,j=1}^{n}$ — целочисленная неотрицательная матрица, r — целое число, $r \geq 1$. Рассмотрим раскраску вершин графа G в n цветов:

$$\varphi : V \to \{1, ..., n\}.$$

Пусть x — произвольная вершина цвета i: $\varphi(x) = i$. Если число вершин цвета j (отличных от вершины x) в шаре $B_r(x)$ не зависит от выбора вершины x и равно a_{ij}, то раскраски называется *совершенной радиуса* r с матрицей A. Другими словами, раскраска совершенная, если число вершин каждого цвета в шаре радиуса r зависит только от цвета центра этого шара.

Нас интересуют совершенные раскраски графа $G(\mathbb{Z}^2)$ бесконечной прямоугольной решетки. Этот граф 4-регулярный, его вершинами являются всевозможные упорядоченные пары целых чисел-координат. Две вершины $\mathbf{x} = (x_1, x_2)$ и $\mathbf{y} = (y_1, y_2)$ смежны, если $|x_1 - y_1| + |x_2 - y_2| = 1$. Обозначим $\|\mathbf{x}\| = d(\mathbf{x}, \mathbf{0})$, где $\mathbf{0} = (0, 0)$.

Примеры совершенных раскрасок в 2 цвета см. на Рис. 1. На рисунках для наглядности мы окрашиваем клетки вместо вершин, то есть фактически рассматриваем граф, двойственный к $G(\mathbb{Z}^2)$ и изоморфный ему.

3. Конструкции и примеры

Конструкция А. Одним из методов получения совершенных раскрасок является так называемый орбитный метод. Рассмотрим граф G с группой автоморфизмов H, пусть H' — подгруппы группы H. Если мы раскрасим каждую орбиту множества вершин V под действием H' в свой цвет, мы получим совершенную раскраску радиуса $r \in \mathbb{N}$ графа G (см. [2]).

Конструкция В. Другой метод получения совершенных раскрасок основывается на объединении цветов.

Лемма 1. *Пусть φ — совершенная раскраска радиуса r в n цветов с матрицей A, раскраска ψ получается из φ объединением цветов в m групп L_1, ..., L_m. Раскраска ψ является совершенной радиуса r в m цветов тогда и только тогда, когда матрица A удовлетворяет следующему условию: для любых $i, j \in \{1, ..., m\}$, $i \neq j$, для любых $p, s \in L_i$,*

$$\sum_{q \in L_j} a_{pq} = \sum_{q \in L_j} a_{sq}.$$

Матрицей совершенной раскраски ψ является $B = (b_{ij})_{i,j=1}^{m}$, где $b_{ij} = \sum_{q \in L_j} a_{pq}$, для $p \in L_i$.

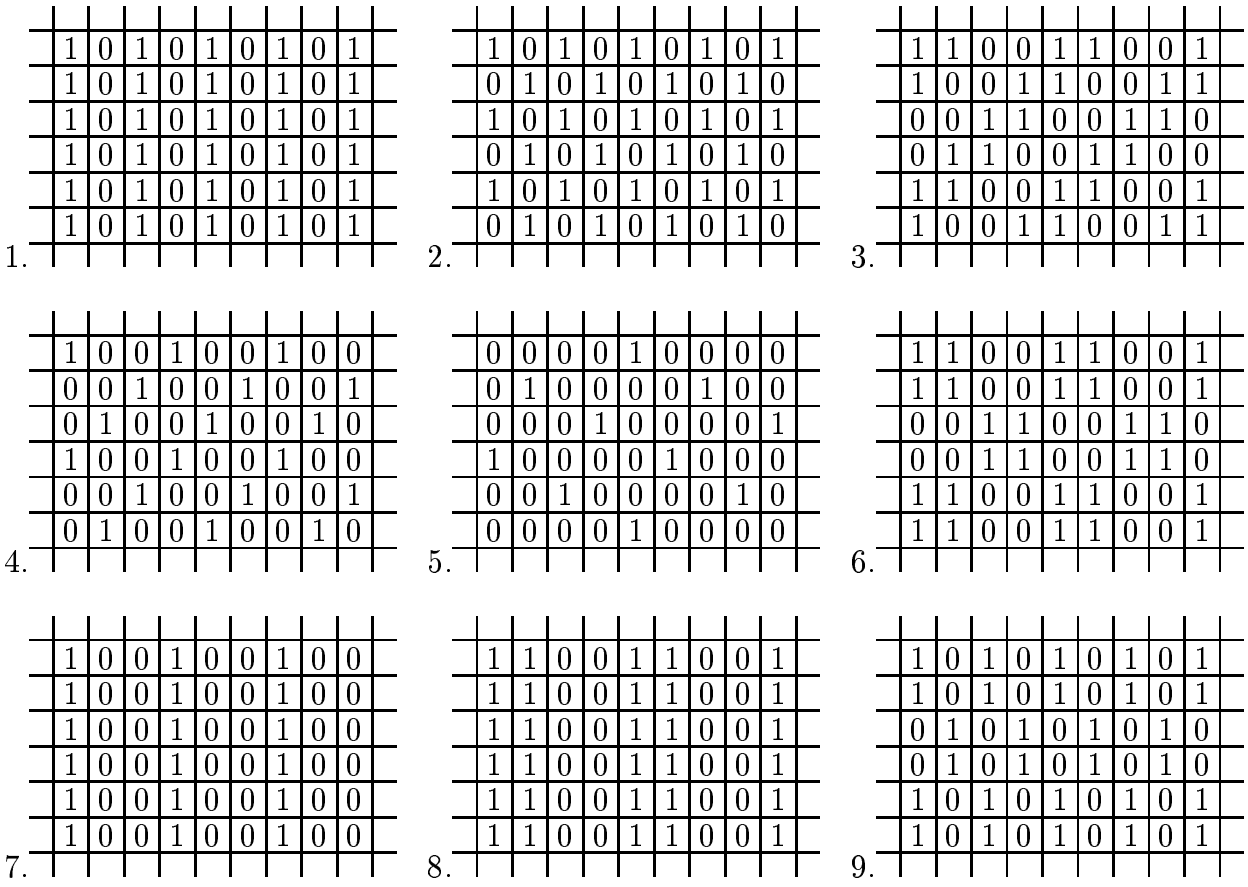

Рис. 1.

Примеры.

1. Орбитные раскраски в два цвета. Существует 9 орбитных раскрасок в два цвета (см. Рис. 1). Эти раскраски содержатся в множестве совершенных раскрасок радиуса 1, которые были описаны Аксенович [1].

2. Трансляционные раскраски. Пусть H' — группа трансляций, порожденная двумя неколлинеарными векторами $\mathbf{u} = (u_1, u_2)$ и $\mathbf{v} = (v_1, v_2)$. Раскрасив каждую орбиту $\mathbb{Z}^2$ под действием группы H' в свой цвет, мы

получим трансляционную раскраску. Эта раскраска совершенная любого радиуса в $|u_1v_2 - u_2v_1|$ цветов. Число цветов равно числу вершин в параллелограмме, натянутом на векторы $\mathbf{u}$ и $\mathbf{v}$.

3. Совершенный код и раскраски, получаемые из него объединением цветов. Рассмотрим трансляционную раскраску, порожденную векторами $(r+1, r)$ и $(r, -r-1)$. Эта раскраска совершенная радиуса r в $n = 2r^2+2r+1$ цветов с соответствующей матрицей

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

По Лемме 1 мы можем объединить цвета и получить совершенную раскраску с матрицей

$$\begin{pmatrix} k & n-k \\ k+1 & n-k-1 \end{pmatrix}.$$

При $k = 0$ эта раскраска является совершенным кодом с минимальным расстоянием $2r + 1$.

4. Периодичность

В этом разделе мы рассматриваем периодичность совершенных раскрасок радиуса $r > 1$ на графе $G(\mathbb{Z}^2)$.

Раскраска φ называется $\mathbf{v}$-*периодической* (или $\mathbf{v}$ – это вектор периодичности раскраски φ) если $\varphi(\mathbf{x} + \mathbf{v}) = \varphi(\mathbf{x})$ для всех $\mathbf{x} \in \mathbb{Z}^2$. Совершенная раскраска, которая является $\mathbf{v}$- и $\mathbf{u}$-периодической для некоторых неколлинеарных $\mathbf{v}$ и $\mathbf{u}$, называется *периодической. Фундаментальным параллелограммом* называется множество вершин в параллелограмме, порожденном векторами $\mathbf{u}$ и $\mathbf{v}$. В случае $\mathbf{u} = (a, 0)$, $\mathbf{v} = (0, b)$ мы используем слово "прямоугольник" вместо слова "параллелограмм".

Раскраски бесконечной прямоугольной решетки могут интерпретироваться как двумерные слова над конечным алфавитом цветов $\{1, ..., n\}$. Будем говорить, что двумерное слово ω *R-продолжаемое*, если для любых $\mathbf{x}, \mathbf{z} \in \mathbb{Z}^2$ равенство $\omega|_{B_R(\mathbf{x})} = \omega|_{B_R(\mathbf{z})}$ влечет $\omega|_{B_{R+1}(\mathbf{x})} = \omega|_{B_{R+1}(\mathbf{z})}$. Обозначение $\omega|_{B_R(\mathbf{x})} = \omega|_{B_R(\mathbf{z})}$ означает, что $\omega(\mathbf{x} + \mathbf{y}) = \omega(\mathbf{z} + \mathbf{y})$ для любых $\mathbf{y}$, таких что $\|\mathbf{y}\| \leq R$.

Лемма 2. *Пусть ω — двумерное слово над конечным алфавитом. Если ω является R-продолжаемым для некоторого $R \geq 0$, то ω периодическое.*

Доказательство леммы можно найти в [4].

Замечание. В качестве следствия из доказательства этой леммы мы можем получить, что векторы периодичности могут быть выбраны следующим образом: $\mathbf{u} = (a, 0)$ и $\mathbf{v} = (0, b)$, где $a, b \leq n^{2R^2+2R+1}$ (n — это число

элементов алфавита, $2R^2 + 2R + 1$ — число вершин в шаре радиуса R). Поэтому число вершин в фундаментальном прямоугольнике $a \times b$ не более $n^{2(2R^2+2R+1)}$.

Доказана следующая теорема.

Теорема 1. *Пусть $\varphi : \mathbb{Z}^2 \to \{1, ..., n\}$ — совершенная раскраска радиуса $r \geq 2$ бесконечной прямоугольной решетки. Тогда φ периодическая.*

Из доказательства теоремы 1 и замечания к лемме 2 можно получить верхнюю границу на число вершин в фундаментальном прямоугольнике:

Следствие 1. *Пусть φ — совершенная раскраска радиуса $r \geq 2$ бесконечной прямоугольной решетки в n цветов. Тогда число вершин в фундаментальном прямоугольнике для φ не более чем*

$$n^{2(2(2r^2+5r+1)^2+2(2r^2+5r+1)+1)}.$$

Заметим, что если $\mathbf{v}$ и $\mathbf{u}$ — векторы периодичности совершенной раскраски φ, то φ может быть получена объединением цветов (Конструкция B) из трансляционной раскраски, порожденной векторами $\mathbf{v}$ и $\mathbf{u}$ (Конструкция A, пример 2). Следствие 1 дает верхнюю оценку на число цветов в соответствующей трансляционной раскраске: это число не более чем

$$n^{2(2(2r^2+5r+1)^2+2(2r^2+5r+1)+1)}.$$

Таким образом, мы нашли общий способ получения всех совершенных раскрасок радиуса $r \geq 2$ в n цветов, но он требует проверки большого числа случаев, поэтому у нас до сих пор нет даже описания всех совершенных раскрасок радиуса 2 в 2 цвета.

Автор выражает благодарность С. В. Августиновичу за внимание к работе и ценные замечания.

Работа выполнена при поддержке РФФИ (грант 07-01-00248) и Фонда содействия отечественной науке.

Список литературы

1. Axenovich M. On multiple coverings of the infinite rectangular grid with balls of constant radius. Discrete Mathematics, vol. 268, pp. 31–49, 2003.

2. Cvetkovic D. M., Doob M., Zahs H. Spectra of graphs. VEB Deutcher Verlag der Wissenschaften, Berlin, 1980.

3. Godsil C. D., Martin W. J. Quotients of association schemes. J. Combin. Theory, ser. A, vol. 69, no. 2, pp. 185–199, 1995.

4. Puzynina S. A., Avgustinovich S. V. On periodicity of two-dimensional words. сдано в печать в спец. выпуск Theoretical Computer Science.

5. Пузынина С. А. Периодичность совершенных раскрасок бесконечной прямоугольной решетки. Дискрет. анализ и исслед. операций, 1:11, №. 1, с. 79–92, 2004.

ОЦЕНКА ТРУДОЕМКОСТИ АЛГОРИТМА КОППЕРСМИТА-ТОМЕ ВЫЧИСЛЕНИЯ ЛИНЕЙНЫХ ГЕНЕРАТОРОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАТРИЦ НАД КОНЕЧНЫМИ ПОЛЯМИ ДЛЯ СЛУЧАЯ ПОЛЯ GF(2)

В. И. Рудской (Москва)

Одним из наиболее эффективных методов решения больших разреженных систем линейных уравнений над конечными полями является блочный алгоритм Видемана, предложенный Д. Копперсмитом в работе [1]. Он находит решение системы путем построения последовательности матриц специального вида и вычисления линейного генератора этой последовательности.

Введем несколько определений. Пусть $A(X)$ — матрица размера $m \times n$, элементами которой являются формальные степенные ряды над K. Степенью вектора-столбца из многочленов будем называть максимум степеней его элементов. Будем говорить, что $A(X)$ *линейно генерируется* вектором $u(X) \in K[X]^n$ до степени L, если существует такой вектор $v(X) \in K[X]^m$, что

$$A(X)u(X) = v(X) + \Omega(X^L),$$

где $\Omega(X^L) \in K[[X]]^m$ — некоторый вектор из степенных рядов над K, в которых отсутствуют члены степени меньше L. В случае когда $L = +\infty$, то будем говорить, что $A(X)$ линейно генерируется до любой степени. Копперсмит в работе [1] предложил использовать для вычисления линейного генератора наименьшей возможной степени следующий алгоритм.

Алгоритм Копперсмита. Алгоритм вычисляет линейный генератор до степени $L = \frac{N}{m} + \frac{N}{n}$ матрицы $A(X) \in K[X]^{m \times n}, m \geq n$, максимальная степень элементов которой равна $L - 1$. Здесь N намного больше, чем m и n (в блочном алгоритме Видемана N — размерность матрицы системы, m и n — размеры блоков). Алгоритм работает не с векторами $u(X)$ и $v(X)$, а с матрицами, составленными из нескольких таких векторов. Пусть потенциальные генераторы собраны в матрицу $f(X) \in K[X]^{n \times (n+m)}$, а соответствующие им $v(X)$ собраны в матрицу $g(X) \in K[X]^{m \times (n+m)}$. Для $1 \leq j \leq n+m$

введем число δ_j. Это число было названо Копперсмитом «номинальной степенью» и фактически является верхней границей степеней элементов j-го столбца матрицы $A(X)f(X)$. Алгоритм является итерационным и на шаге, соответствующем значению счетчика t, выполняется следующее равенство:

$$A(X)f(X) = g(X) + X^t e(X),$$

где матрица $e(X) \in K[X]^{m\times(m+n)}$ — текущая «невязка», которую мы стремимся обнулить, и каждый столбец этого матричного уравнения удовлетворяет условиям:

$$A(X)f_j(X) = g_j(X) + X^t e_j(X), \tag{1}$$

$$\deg f_j \le \delta_j, \quad \deg g_j < \delta_j, \quad \deg e_j \le L + \delta_j - t \tag{2}$$

(здесь и далее нижний индекс $_j$ обозначает столбец). Кроме того, потребуем выполнения еще одного условия:

$$rank([X^0]e_j) = m, \tag{3}$$

где $[X^k]P$ обозначает коэффициент при X^k в многочлене P.

Инициализация алгоритма. Положим $t_0 = \lceil \frac{m}{n} \rceil$. Все δ_j положим равными t_0. Первые m столбцов матрицы f заполняются таким образом, что столбцы $[X^{t_0}](Af_j)$ для всех $1 \le j \le m$ линейно независимы (это почти всегда можно сделать). Оставшаяся $n \times n$ подматрица инициализируется тождественной матрицей порядка n. Легко проверить, что условия (1)–(3) выполнены.

Итерация алгоритма. На каждом шаге итерации мы стремимся обнулить $[X^0]e$. Это достигается модификацией алгоритма Гаусса. Справедлива следующая

Теорема 1. [2, Theorem 2.2] *Если условия* (1)–(3) *выполняются на шаге* t, *тогда существует алгоритм* `ALGO1`, *который по известным* $[X^0]e^{(t)}$ *и* $\delta_1^{(t)}, \ldots, \delta_{m+n}^{(t)}$ *вычисляет матрицу* $P^{(t)}$ *размерности* $(m+n)\times(m+n)$ *и числа* $\delta_1^{(t+1)}, \ldots, \delta_{m+n}^{(t+1)}$, *такие, что*

$$f^{(t+1)} = f^{(t)}P^{(t)},$$

$$g^{(t+1)} = g^{(t)}P^{(t)},$$

$$e^{(t+1)} = e^{(t)}P^{(t)}\frac{1}{X},$$

и числа $\delta_1^{(t+1)}, \ldots, \delta_{m+n}^{(t+1)}$ *удовлетворяют условиям* (1)–(3) *на шаге* $t+1$. *Кроме того, выполнено равенство*

$$\sum_j \delta_j^{(t+1)} - \sum_j \delta_j^{(t)} = m.$$

Доказательство теоремы проводится конструктивно с явным описанием алгоритма из работы [1]. Сложность алгоритма `ALGO1` в количестве **процессорных** операций в предположении, что вычисления происходят в поле $GF(2)$, а размеры матриц m, n меньше длины регистра, можно оценить как

$$C_{\texttt{ALGO1}} = \frac{1}{2}(m+n)^2 + 14m(m+n) + 3(m+n) + m.$$

Алгоритм Копперсмита выполняет на каждой итерации алгоритм `ALGO1` до наступления условия $t > \frac{N}{m} + \frac{N}{n} + t_0$. Алгоритм Копперсмита имеет квадратичную (от L) сложность из-за необходимости вычисления $[X^t](Af)$ на каждом шаге. Французский математик Э. Томе в [3] предложил модификацию алгоритма Копперсмита, имеющую субквадратичную сложность.

Алгоритм Копперсмита–Томе. Заметим, что если матрица $e^{(t)}(X)$ известна до степени k, то можно вычислить матрицы $P^{(t)} \dots P^{(t+k-1)}$ не вычисляя $f(X)$. Будем называть *k-контекстом* пару вида $E = (e(X), \Delta)$, где $\Delta = (\delta_j^{(t)})$ и $e(X)$ известна до степени $k-1$ включительно. Пусть E — контекст, соответствующий шагу алгоритма с номером t. Обозначим через $\pi_E^{(a,b)}$ матрицу $P^{(t+a)} \cdots P^{(t+b-1)}$. Тогда исходная задача вычисления линейного генератора эквивалентна задаче нахождения $\pi_{E^{(t_0)}}^{(0,L-t_0)}$, где $E^{(t_0)} = (e^{(t_0)}, \Delta^{(t_0)})$ — начальный контекст. Для решения этой задачи Томе предложил рекурсивный алгоритм, действующий по принципу «разделяй и властвуй».

Алгоритм `MSLGDC` (matrix sequences linear generator by divide and conquer).
Вход: b-контекст $E = (e(X), \Delta)$
Выход: матрица $\pi_E^{(0,b)}$
{
$if(b == 0) \quad return\ I_{m+n}$
$if(b == 1) \quad return\ \texttt{ALGO1}(e, \Delta)$
$(e_L, \Delta_L) = ((e\ mod\ X^{\lfloor \frac{b}{2} \rfloor}), \Delta)$
$\pi_L = \texttt{MSLGDC}(e_L, \Delta_L)$
$(e_R, \Delta_R) = (((e\pi_L\ mod\ X^b)\ div\ X^{\lfloor \frac{b}{2} \rfloor}), \Delta\pi_L)$
$\pi_R = \texttt{MSLGDC}(e_R, \Delta_R)$
$\pi = \pi_L \times \pi_R$
$return\ \pi$
}

Теорема 2. [2, Theorem 3.4] *Если поле K поддерживает быстрое преобразование Фурье (FFT)[4], то сложность алгоритма `MSGDC` можно оценить как*

$$M_1 m(m+n) b \log^2 b + 3M_1 m(m+n)^2 b \log b + O((m+n)^2 b \log b),$$

где M_1 — сложность умножения в поле K.

К сожалению, в интересующем нас случае $K = GF(2)$ (возникающему, например, в алгоритмах факторизации больших целых чисел) утверждение теоремы непосредственно применить нельзя, потому что поле $GF(2)$ не поддерживает FFT. Однако можно модифицировать алгоритм Томе для этого случая.

Модификация алгоритма Томе для случая поля $GF(2)$. Рассмотрим алгоритм умножения многочленов из $GF(2)[x]$:

1. Рассматриваем многочлены из $GF(2)[x]$ как многочлены из $\mathbb{Z}[x]$
2. Используем эффективный алгоритм умножения в $\mathbb{Z}[x]$
3. В получившемся многочлене приводим коэффициенты по модулю 2
4. Рассматриваем приведенный многочлен как многочлен над $GF(2)$

Легко проверить корректность описанного алгоритма. Его сложность можно оценить как $M_{\mathbb{Z}}(n) + O(n)$, где $M_{\mathbb{Z}}(n)$ обозначает сложность умножения двух многочленов из $\mathbb{Z}[x]$ степени меньше n.

Будем рассматривать многочлен из $\mathbb{Z}[x]$ как многочлен над полем комплексных чисел $\mathbb{C}[x]$. Как известно, поле комплексных $\mathbb{C}$ чисел поддерживает FFT, то есть для умножения многочленов в $\mathbb{C}[x]$ можно использовать быстрое преобразование Фурье. С теоретической точки зрения это означает, что оценки, указанные в теореме 2, справедливы, при условии, что M_1 обозначает сложность умножения в поле $\mathbb{C}$. Расширение модели приведет к появлению членов порядка

$$O((m+n)^2 b) \lessapprox O((m+n)^2 b \log b),$$

которыми можно пренебречь при асимптотической оценке. Отметим, что указанные оценки линейны по числу умножений в поле и субквадратичны по степени рассматриваемых многочленов.

При реализации на ЭВМ операции над комплексными числами реализуются как операции над парами вещественных чисел, при этом операции над вещественными числами выполняются приближенно. При использовании высокой точности сложность операций будут зависеть от битовой длины чисел и, как будет показано далее, от степени перемножаемых многочленов. При реализации надо обеспечить точность вычисления, достаточную для однозначного определения коэффициентов при обратном переходе из $\mathbb{C}[x]$ в $GF(2)[x]$. Можно показать, что для умножения двух многочленов степени не выше b достаточно обеспечить точность

$$\varepsilon < \left(b^3(3\log_2 b + 4)\right)^{-1}.$$

При этом длина целой части чисел, над которыми производятся операции не превысит $3\log_2 b$ и следовательно общее число двоичных знаков должно быть не меньше

$$l(b) = 3\log_2 b + \log_2 \varepsilon = 6\log_2 b + \log_2(3\log_2 b + 4).$$

Вернемся к оценке величины M_1 для многочленов степени не выше b. Если использовать стандартный алгоритм умножения чисел, квадратичный по длине входа, то сложность операции умножения в $\mathbb{C}$ можно оценить как $M_1(b) = 4l(b)^2 + 2l(b)$, а сложность сложения как $M_2(b) = 2l(b)$ бинарных операций. Количество процессорных операций будет совпадать с указанными оценками с точностью до постоянного множителя, определенного разрядностью процессора.

Оценим сложность алгоритма Копперсмита–Томе вычисления $\pi_E^{(0,L)}$. Будем использовать арифметику с фиксированной длиной: для любой глубины рекурсии арифметические операции будут проводится над числами длины $l(L)$. Наибольшую сложность имеют операции $\pi = \pi_L \times \pi_R$ и

$$e_R = \left(\left(e\pi_L \bmod X^b \right) \operatorname{div} X^{\lfloor \frac{b}{2} \rfloor} \right).$$

Для их реализации воспользуемся быстрым преобразование Фурье. Обозначим через $C(b)$ сложность алгоритма Копперсмита-Томе. Легко проверить, что она удовлетворяет рекурсивному равенству:

$$\begin{aligned} C(b) = {} & 2C\left(\frac{b}{2}\right) + 2m(m+n)(M_1\frac{b}{2}\log b + M_2 b\log b) \\ & + 3(m+n)^2\left(M_1\frac{b}{2}\log b + M_2 b\log b\right) + (m+n)^2(M_1+M_2)b \\ & + m(m+n)^2(M_1+M_2)b + (m+n)^3(M_1+M_2)b + 3m(m+n), \end{aligned}$$

$$C(1) = C_{\texttt{ALGO1}}(m,n).$$

Если предположить, что интересующее нас значение $L = 2^t$, то $C(L)$ оценивается величиной:

$$\frac{1}{2}F_1 L\log^2 L + \left(F_2 - \frac{1}{2}F_1\right) L\log L + \left(C_{\texttt{ALGO1}}(m,n) + 3(m+n)m\right) L,$$

где

$$F_1 = \left(\frac{1}{2}M_1(L) + M_2(L)\right)(m+n)(4m+3n),$$

$$F_2 = (M_1(L) + M_2(L))(m+n)^2(2m+n+1).$$

Или асимптотически более грубо, с учетом всех обозначений:

$$C(L) \approx O\left((m+n)^2 L \log^4 L + (m+n)^3 L \log^3 L\right).$$

Таким образом, нами показана возможность использования алгоритма Копперсмита–Томе вычисления линейного генератора последовательности матриц над конечным полем для случая поля $GF(2)$ с сохранением асимптотической субквадратичной оценки сложности.

Полученная оценка довольно точная, что позволяет сравнить алгоритмы `MSLGDC` с FFT и `MSLGDC` с обычным алгоритмом умножения многочленов, имеющим сложность $O(b^2)$, но с маленькой константой в $O(\cdot)$. Сравнение показывает, что для 128-разрядного (например, векторного) процессора и размеров блоков $m = n = 128$ асимптотическое преимущество проявляется при размерах системы порядка $6 \cdot 10^5$. На практике, например, в алгоритмах факторизации больших целых чисел, размеры систем могут достигать порядка $10^6 \sim 10^8$. В этом случае применение алгоритма `MSLGDC` с FFT оправдано и будет давать выигрыш по времени в несколько порядков.

Список литературы

1. Coppersmith D. Solving linear equations over $GF(2)$ via block Wiedemann algorithm. Math. Comp. 62, 205 (Jan. 1994), 333-350.

2. Thomé E. Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm. In B. Mourrain, editor, ISSAC '2001, pages 323-331. ACM Press, 2001a. Proceedings

3. Thomé E. Fast Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm // J. Symbolic Computation. — 2002.

4. von zur Gathen J. and Gerhard J. Modern Computer Algebra. Cambridge University Press, Cambridge, England, 1999.

О ГЛУБИНЕ СХЕМ ДЛЯ МНОГОКРАТНОГО СЛОЖЕНИЯ И УМНОЖЕНИЯ ЧИСЕЛ

И. С. Сергеев (Москва)

В настоящей работе рассматривается подход к построению схем из функциональных элементов, реализующих многократное сложение и умножение чисел с небольшой глубиной. Обзорная лекция, посвященная минимизации

глубины таких схем, была прочитана А. В. Чашкиным на одной из предыдущих школ этой серии [6]. Схемы строятся над базисом из всех двухвходовых элементов. Понятия сложности и глубины схем изложены в [3].

В начале 60-х гг. Ю. П. Офман [2] и ряд зарубежных авторов (см. [8]) предложили способ реализации умножения n-разрядных чисел схемой глубины $O(\log n)$. В этом способе умножение сводится к n-кратному сложению (как в школьном методе), которое, в свою очередь, сводится к обычному сложению при помощи схемы компрессоров.

Под (p,q)-компрессором, где $q < p$, понимается схема, по набору из p чисел вычисляющая q новых чисел с сохранением суммы, и имеющая глубину, не зависящую от разрядности слагаемых. Самым простым и наиболее популярным является (3,2)-компрессор. Он преобразует набор из трех чисел $X = [x_{k-1}, \ldots, x_0]$, $Y = [y_{k-1}, \ldots, y_0]$, $Z = [z_{k-1}, \ldots, z_0]$ в пару чисел $U = [u_k, \ldots, u_1, 0]$ и $V = [v_{k-1}, \ldots, v_0]$, таких, что $U + V = X + Y + Z$. Пара разрядов (u_{i+1}, v_i) вычисляется подсхемой, изображенной на рис. 1. Таким образом, k-разрядный (3,2)-компрессор имеет сложность $5k$ и глубину 3.

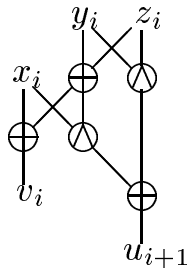

Рис. 1

При оптимизации глубины схем из (3,2)-компрессоров существенно используется несимметричность глубин выходов компрессора относительно глубин входов. В стандартном способе из двух (3,2)-компрессоров строится (4,2)-компрессор, используя который несложно построить схему сведения n-кратного сложения к обычному с глубиной $4\lceil \log_2 n \rceil - 3$ (эта конструкция описана в [6] для другой интерпретации входов и с менее аккуратной оценкой глубины).

Обозначим через $D(n)$ глубину минимальной реализации сведения n-кратного сложения к обычному схемой из (3,2)-компрессоров. В дальнейшем для упрощения изложения, под входами и выходами компрессора будут пониматься числа-слагаемые, глубину числа определяет разряд с наибольшей глубиной. Асимптотически точная оценка величины $D(n)$ была получена в [8]. Пусть $\lambda = 1,205\ldots$ — единственный вещественный корень уравнения $\lambda^3 + \lambda^2 - \lambda - 2 = 0$. Справедлива

Теорема 1. [8] $\log_\lambda n - 3,3 < D(n) < \log_\lambda n + O(1)$.

Отметим, что $\log_\lambda n \approx 3,71 \log_2 n$. Нижняя оценка следует из соотношения $\lambda^{D(n)} + \lambda^{D(n)-1} \geq n$, которое вытекает из следующей простой леммы.

Лемма 1. *Пусть a, b, c — глубины входов $(3,2)$-компрессора; d и $d-1$ — глубины выходов, тогда $\lambda^d + \lambda^{d-1} \geq \lambda^a + \lambda^b + \lambda^c$.*

Верхняя оценка доказывается в [8] общим, но практически не эффективным методом. Константа, которая скрывается за обозначением $O(1)$,

достаточно велика; кроме того, построенная методом [8] схема содержит примерно в шесть раз больше компрессоров, чем необходимо. На самом деле, верна

Теорема 2. *Для любого $n > 3$ выполнено: $D(n) > \log_\lambda n - 2,7$. Кроме того, существует схема Λ сведения n-кратного сложения к обычному, состоящая из $n-2$ компрессоров, глубина которой не превосходит $\log_\lambda n - 0,8$, а сложность — $5(nk + 4n - 2k)$, где k — разрядность суммируемых чисел.*

Перед тем, как дать пояснения к доказательству, введем некоторые понятия. Будем считать компрессор расположенным на глубине d, если его выходы имеют глубины $d + 2$ и $d + 3$. Пусть $T \subset \mathbf{N} \cup \{0\}$. Положим $\sigma(T) = \sum_{t \in T} \lambda^t$. Через S_r обозначим схему, образованную компрессорами схемы S, расположенными на глубинах, меньших r. Через $T(S_r)$ обозначим множество глубин выходов схемы S_r, в котором числа, меньшие r, заменены на r. Положим $\sigma(S_r) = \sigma(T(S_r))$. Из леммы 1 очевидно, что

$$n = \sigma(S_0) \le \sigma(S_1) \le \ldots \le \sigma(S_{d-2}) = \lambda^d + \lambda^{d-1}, \qquad (1)$$

где n — число входов, а d — глубина схемы S.

Нижняя оценка теоремы 2 следует из (1) и неравенств

$$\sigma(S_1) - \sigma(S_0) \ge n(\lambda - 1)/3, \quad \sigma(S_{d-2}) - \sigma(S_{d-6}) \ge \lambda^{d-5}(\lambda - 1),$$

справедливых для произвольной схемы S.

Для доказательства верхней оценки используется очевидный метод последовательного добавления компрессоров в схему, в котором каждый очередной компрессор располагается на возможно меньшей глубине. При оценке глубины построенной схемы Λ ключевой является следующая лемма, которая доказывается по индукции.

Лемма 2. *Пусть $r > 0$, а m_0, m_1 и m_2 — соответственно количество чисел r, $r + 1$ и $r + 2$ во множестве $T(\Lambda_r)$. Тогда выполнено:*

$$m_0 \le 2m_1 + 2, \quad m_1 \le 1,5m_0 + 2m_2, \quad m_2 \le m_1.$$

Обозначим $\Delta_r = \sigma(\Lambda_{r+1}) - \sigma(\Lambda_r)$. По построению, $\Delta_r = a_r(\lambda - 1)\lambda^r$, $a_r \in \mathbf{Z}$. Из первого неравенства леммы следует, что $a_r \le 2$. При этом, если $a_r = 2$, то, как легко убедиться, $a_{r+1} = 0$. Принимая во внимание $a_{d-4} \le 1$ и $a_{d-3} = 0$ (где d — глубина Λ), получаем

$$\sigma(\Lambda_{d-2}) - \sigma(\Lambda_1) \le (\lambda - 1) \sum_{i=1}^{d-4} \lambda^i,$$

что, с учетом $\Delta_0 \le (\lambda-1)(2+n/3)$, приводит к окончательной оценке $d < \log_\lambda n - 0,8$.

Оценка сложности схемы Λ складывается из величины $5k(n-2)$, отвечающей числу компрессоров, и добавочного члена, отвечающего удлинению чисел-слагаемых с увеличением глубины. Последний оценивается величиной $20n$, что выводится из следующих легко проверяемых фактов: (1) количество компрессоров, расположенных на глубине r не превосходит $(\lambda+1)\lambda^{d-r-1}/(\lambda+2)$ и (2) выход некоторого компрессора, имеющий глубину r, является не более чем $(k+\lfloor r/3\rfloor)$-разрядным числом.

Нижняя оценка теоремы 2 показывает, что глубина постренной схемы не более чем на единицу отличается от оптимальной. Схема, построенная стандартным способом, имеет худшую глубину для всех n, кроме 4, 8, 16, 32, для которых оба метода дают одинаковый результат.

Для окончательного вычисления суммы выходы схемы компрессоров подаются на входы сумматора. Сумматор n-разрядных чисел, построенный методом В. М. Храпченко [4], имеет асимптотически оптимальную глубину $(1+o(1))\log_2 n$. Для n в пределах нескольких тысяч выгоднее использовать другие методы, например, метод М. И. Гринчука с верхней оценкой глубины $2\log_3(16\lfloor n/2\rfloor)$ (см. [1]). Так, для умножения справедливо

Следствие 1. *Существует схема умножения двух n-разрядных чисел сложности $O(n^2)$ и глубины не более $5(\log_2 n+1)$.*

Для сравнения, вариантом метода А. А. Карацубы [2] можно построить схему с асимптотически меньшим порядком сложности $n^{\log_2 3}$, но с глубиной $(11+o(1))\log_2 n$ (см. [6], но там приводится менее аккуратная оценка глубины). Метод Карацубы обычно не применяется при $n < 300$. Вариант метода Шёнхаге—Штрассена [10] имеет сложность $O(n\log n\log\log n)$ и глубину $(9+o(1))\log_2 n$, однако почти не используется на практике.

Отметим, что компрессоры удобно использовать для вычислений по модулю 2^k-1 (перенося k-е разряды промежуточных слагаемых на место младших). В целях минимизации глубины для реализации заключительного модулярного сложения двух чисел можно использовать $2k$-разрядный сумматор.

В заключение — несколько замечаний о применении более сложных компрессоров. Примеры компрессоров, асимптотически более эффективных, чем (3,2)-компрессор, приводились в работах [5] (для базиса $\{\wedge,\vee,{}^-\}$) и [8]. Известны, например, (5,3)-компрессор и (6,3)-компрессор, из которых методом [8] строятся схемы сведения n-кратного сложения к обычному с глубиной асимптотически $3,65\log_2 n$ и $3,57\log_2 n$ соответственно. Можно также построить (11,5)-компрессор с показателем эффективности $3,55\log_2 n$. Для получения наилучшей известной асимптотической оценки $3,44\log_2 n$ [7] используются схемы из т. н. полукомпрессоров [9].

Методы [7–9] сугубо теоретические, однако предложенные компрессоры можно использовать для построения практических схем небольшой глубины. Используя (5,3) и (6,3)-компрессоры наряду с (3,2)-компрессорами, можно строить схемы меньшей глубины, чем описано выше, уже при малых n, в частности, при $n = 32$. Специальный (7,3)-компрессор позволяет реализовать умножение по методу Карацубы с глубиной $(10 + o(1)) \log_2 n$. Уменьшение глубины во всех случаях достигается ценой некоторого увеличения сложности: кажется, неизвестны (p, q)-компрессоры, у которых отношение сложности к $p - q$ меньше, чем $5k$, где k —разрядность слагаемых.

Автор признателен научному руководителю С. Б. Гашкову за постановку задачи и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы «Ведущие научные школы» (проект НШ–5400.2006.1) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Гашков С. Б., Гринчук М. И., Сергеев И. С. О построении схем сумматоров малой глубины. // Дискретный анализ и исследование операций. Серия 1. — 2007. — Т. 14, №1. — С. 27–44.

2. Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. // Докл. АН СССР. — 1962. — Т. 145(2). — С. 293–294.

3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд. МГУ, 1984.

4. Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора. // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 107–120.

5. Храпченко В. М. Некоторые оценки для времени умножения. // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 221–227.

6. Чашкин А. В. Быстрое умножение и сложение целых чисел. // В сб. «Дискретная математика и ее приложения». II. — М.: изд-во ЦПИ при мех.-мат. ф-те МГУ, 2001. — С. 91–110.

7. Grove E. Proofs with potential. — Ph.D. thesis, U.C. Berkeley, 1993.

8. Paterson M., Pippenger N., Zwick U. Optimal carry save networks. // LMS Lecture Notes Series. — V. 169. Boolean function Complexity. — Cambridge University Press, 1992. — P. 174–201.

9. Paterson M., Zwick U. Shallow circuits and concise formulae for multiple addition and multiplication. // Comput. Complexity. — 1993. — V. 3. — P. 262–291.

10. Schönhage A., Strassen V., Schnelle multiplikation groser zahlen. // Computing. — 1971. — V. 7. — P. 271–282. [Русский перевод: Шёнхаге А., Штрассен В. Быстрое умножение больших чисел. // Кибернетический сборник. Вып. 10. — М.: Мир, 1973. — С. 87–98].

О СТРОЕНИИ КЛАССОВ ПОДОБИЯ МАТРИЦ ВТОРОГО И ТРЕТЬЕГО ПОРЯДКОВ НАД Z

С. В. Сидоров (Нижний Новгород)

1. Введение

Классическая задача о подобии матриц над полем рациональных чисел $\mathbf{Q}$ (см., например, [1]) естественным образом обобщается на кольцо целых чисел $\mathbf{Z}$. Квадратные матрицы A и B с коэффициентами из поля $\mathbf{Q}$ называются подобными над $\mathbf{Q}$, если существует такая невырожденная матрица S с рациональными коэффициентами, что $AS = SB$ (подобие над $\mathbf{Q}$ будем обозначать $A \approx B$).

Определение. *Будем говорить, что матрица $B \in \mathbf{Z}^{n\times n}$ подобна матрице $A \in \mathbf{Z}^{n\times n}$ над кольцом $\mathbf{Z}$, если существует $S \in \mathbf{Z}^{n\times n}$ такая, что $AS = SB$ и $\det S \in \{1, -1\}$ и обозначать это $A \sim B$. Матрица S называется трансформирующей B в A матрицей.*

Задача о подобии матриц над $\mathbf{Z}$ рассматривалась многими авторами (см., например, [3,4,5]). Хотя в [3] получен алгоритм определения подобия матриц над $\mathbf{Z}$ в общем случае, строение классов подобия изучено мало. Отношение подобия есть отношение эквивалентности. Следовательно, множество $\mathbf{Z}^{n\times n}$ разбивается на классы подобных матриц. При этом это разбиение различно для отношения подобия над полем $\mathbf{Q}$ и над кольцом $\mathbf{Z}$. Ясно, что подобие матриц над $\mathbf{Q}$ является необходимым условием для подобия над $\mathbf{Z}$, но не является достаточным даже для матриц второго порядка (см. контрпримеры в [2]). Отсюда следует, что класс $K_Q(A)$ матриц, подобных A над $\mathbf{Q}$, разбивается на подклассы матриц, подобных над $\mathbf{Z}$. Обозначим $K_Z(A) = \{B \in \mathbf{Z}^{n\times n} | B \sim A\}$. Тогда $K_Q(A) = \bigcup\limits_{i\in I} K_Z(A_i)$. Если матрицы подобны (над $\mathbf{Z}$ или над $\mathbf{Q}$), то они имеют один и тот же характеристический многочлен $d(\lambda)$. Цель работы — показать разбиение классов подобия для матриц второго и третьего порядков, характеристические многочлены которых раскладываются на линейные множители над $\mathbf{Q}$. В каждом из таких классов найдена каноническая матрица, характеризующая класс.

2. Случай матриц 2×2

Для характеристического многочлена $d(\lambda)$ матрицы $A \in \mathbf{Z}^{2\times 2}$ возможны следующие варианты:
1) $d(\lambda) = (\lambda-\alpha)^2$; 2) $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)$; 3) $d(\lambda) = \lambda^2 + u\lambda + v$ неприводим над $\mathbf{Z}$.

В первом случае A подобна над $\mathbf{Q}$ одной из жордановых матриц:
$J_1(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$, $J_2(\alpha) = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$.

Во втором случае A подобна над $\mathbf{Q}$ матрице
$J_3(\alpha, \beta) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$.

В третьем случае A подобна над $\mathbf{Q}$ матрице Фробениуса
$F_1 = \begin{pmatrix} -u & -v \\ 1 & 0 \end{pmatrix}$

Теорема 1. *Если $d(\lambda) = (\lambda-\alpha)^2$, где $\alpha \in \boldsymbol{Z}$, то*
1. $K_Q(J_1(\alpha)) = K_Z(J_1(\alpha)) = \{J_1(\alpha)\}$,
2. $K_Q(J_2(\alpha)) = \bigcup\limits_{s\geq 1} K_Z(R_s(\alpha))$, *где*

$R_s(\alpha) = \begin{pmatrix} \alpha & s \\ 0 & \alpha \end{pmatrix}$, $s \geq 1$ — *каноническая матрица.*

Теорема 2. *Если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)$, $\alpha, \beta \in \boldsymbol{Z}$, $\beta > \alpha$, то $K_Q(J_3(\alpha,\beta)) = \bigcup\limits_{s=0}^{\lfloor\frac{\beta-\alpha}{2}\rfloor} K_Z(R_s(\alpha,\beta))$, где*

$R_s(\alpha,\beta) = \begin{pmatrix} \alpha & s \\ 0 & \beta \end{pmatrix}$, $0 \leq s \leq \lfloor\frac{\beta-\alpha}{2}\rfloor$ — *каноническая матрица.*

Теорема 3. *Класс $K_Q(F_1)$ разбивается на конечное число классов целочисленно подобных матриц.*

3. Случай матриц 3×3

Пусть матрица $A \in \mathbf{Z}^{3\times 3}$ имеет приводимый над $\mathbf{Z}$ характеристический многочлен $d(\lambda)$. Возможны следующие варианты: 1) все корни $d(\lambda)$ лежат в $\mathbf{Z}$; 2) $d(\lambda) = (\lambda-\alpha)(\lambda^2+u\lambda+v)$, причем $\lambda^2+u\lambda+v$ неприводим над $\mathbf{Z}$.

В первом случае A подобна над $\mathbf{Q}$ одной из жордановых матриц:
a) если $d(\lambda) = (\lambda-\alpha)^3$, то A подобна над $\mathbf{Q}$ одной из матриц $J_4(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$, $J_5(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$, $J_6(\alpha) = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$.
b) если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)^2$, то A подобна над $\mathbf{Q}$ либо $J_7(\alpha,\beta) =$

$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}$, либо $J_8(\alpha,\beta) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 1 \\ 0 & 0 & \beta \end{pmatrix}$.

c) если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)(\lambda-\gamma)$, то A подобна над $\mathbf{Q}$ матрице $J(\alpha,\beta,\gamma) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$.

Во втором случае A подобна над $\mathbf{Q}$ матрице Фробениуса

$$F_2 = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & -u & -v \\ 0 & 1 & 0 \end{pmatrix}.$$

Теорема 4. *Пусть* $d(\lambda) = (\lambda-\alpha)^3, \alpha \in \mathbf{Z}$. *Тогда*

1. $K_Q(J_4(\alpha)) = K_Z(J_4(\alpha)) = \{J_4(\alpha)\}$,

2. $K_Q(J_5(\alpha)) = \bigcup K_Z(S_d(\alpha))$, $S_d(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & d \\ 0 & 0 & \alpha \end{pmatrix}$, $d \geq 1$

3. $K_Q(J_6(\alpha)) = \bigcup K_Z(S_{a,b,r}(\alpha))$,

$S_{a,b,r}(\alpha) = \begin{pmatrix} \alpha & a & r \\ 0 & \alpha & b \\ 0 & 0 & \alpha \end{pmatrix}$, $a, b \geq 1$, $0 \leq r < \text{НОД}(a,b)$.

Теорема 5. *Пусть* $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)^2, \alpha, \beta \in \mathbf{Z}$. *Тогда*

1. $K_Q(J_7(\alpha,\beta)) = \bigcup K_Z(S_d(\alpha,\beta))$,

$S_d(\alpha,\beta) = \begin{pmatrix} \alpha & d & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}$, $d = 0$ *или* d *— положительный делитель* $|\beta-\alpha|$ (*не равный* $|\beta-\alpha|$)

2. $K_Q(J_8(\alpha,\beta)) = \bigcup K_Z(S_{a_1,a_2,a_3}(\alpha,\beta))$,

$$S_{a_1,a_2,a_3}(\alpha,\beta) = \begin{pmatrix} \alpha & a_1 & a_2 \\ 0 & \beta & a_3 \\ 0 & 0 & \beta \end{pmatrix},$$

где a_1, a_2, a_3 *удовлетворяют условиям*

I) $a_3 \geq 1$, $0 \leq a_2 \leq \lfloor \frac{|\beta-\alpha|}{2} \rfloor$, $a_1 = 0$

IIa) если $|\beta-\alpha|$ *– нечетное, то*

$a_3 \geq 1$, $1 \leq a_1 \leq \lfloor \frac{|\beta-\alpha|}{2} \rfloor$, $0 \leq a_2 < d$, *где* $d = \text{НОД}(|\beta-\alpha|, a_1)$

IIb) если $|\beta-\alpha|$ *— четное, то*

1) $1 \leq a_1 \leq \frac{|\beta-\alpha|}{2} - 1$, $a_3 \geq 1$, $0 \leq a_2 < d$

2) $a_1 = \frac{|\beta-\alpha|}{2}$, $a_3 \geq 1$,

если $\beta - \alpha > 0$, *то* $-\lfloor \frac{a_1 - r}{2} \rfloor \leq a_2 \leq \lfloor \frac{r}{2} \rfloor$,

если $\beta - \alpha < 0$, *то* $-\lfloor \frac{r}{2} \rfloor \le a_2 \le \lfloor \frac{a_1 - r}{2} \rfloor$,
где r — *остаток от деления* a_3 *на* a_1.

Теорема 6. *Пусть* $d(\lambda) = (\lambda - \alpha)(\lambda - \beta)(\lambda - \gamma), \alpha, \beta, \gamma \in \mathbf{Z}, \alpha < \beta < \gamma$. *Тогда* $K_Q(J(\alpha, \beta, \gamma)) = \bigcup K_Z(S_{a_1, a_2, a_3}(\alpha, \beta, \gamma))$,

$$S_{a_1,a_2,a_3}(\alpha,\beta,\gamma) = \begin{pmatrix} \alpha & a_1 & a_2 \\ 0 & \beta & a_3 \\ 0 & 0 & \gamma \end{pmatrix},$$

где a_1, a_2, a_3 *удовлетворяют условиям*
I) $a_1 = 0$, $0 \le a_2 \le \lfloor \frac{\gamma - \alpha}{2} \rfloor$, $0 \le a_3 \le \lfloor \frac{\gamma - \beta}{2} \rfloor$
IIa) *если* $\gamma - \beta$ – *нечетное, то*
$1 \le a_1 \le \lfloor \frac{\beta - \alpha}{2} \rfloor$, $0 \le a_2 < \gamma - \alpha$, $0 \le a_3 \le \lfloor \frac{\gamma - \beta}{2} \rfloor$
IIb) *если* $\gamma - \beta$ – *четное, то*
1) $1 \le a_1 \le \lfloor \frac{\beta - \alpha}{2} \rfloor$, $0 \le a_2 < \gamma - \alpha$, $0 \le a_3 \le \frac{\gamma - \beta}{2} - 1$
2) $1 \le a_1 \le \lfloor \frac{\beta - \alpha}{2} \rfloor$, $-\lfloor \frac{a_1}{2} \rfloor \le a_2 \le \lfloor \frac{\gamma - \alpha - a_1}{2} \rfloor$, $a_3 = \frac{\gamma - \beta}{2}$.

Теорема 7. *Класс* $K_Q(F_2)$ *разбивается на конечное число классов целочисленно подобных матриц.*

Работа выполнена при частичной финансовой поддержке РФФИ. Код проекта 05-01-00552-а.

Список литературы

1. Гантмахер Ф. Р. Теория матриц. — 4-е изд. — М.: Наука, 1988. — 552с.

2. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел// Известия ВУЗ. Математика — 2006. — N4. — С. 57–64.

3. Grunewald F. Solution of the conjugacy problem in certain arithmetic groups. in Word Problems II, (ed Adian, Boone, Higman). North-Holland, Amsterdam 1980, pp 101–139.

4. Newman M. Integral matrices. New York and London: Academic Press, 1972. 224p.

5. Latimer C.G. and MacDuffee C.C. A correspondence between classes of ideals and classes of matrices. Annals Math. 34, (1933), 313–316.

О СРЕДНЕЙ МОЩНОСТИ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

П. С. Степанов (Москва)

Постановка задачи

Пусть дана схема A из функциональных элементов с n входами и одним выходом в базисе B, реализующая функцию F. Пусть булевы наборы $\tilde{\alpha}_i$ подаются на входы схемы с некоторыми вероятностями $p_{\tilde{\alpha}_i}$. Допускается любое распределение $\{p_{\tilde{\alpha}}\}_{\tilde{\alpha}\in B_n}$, где $p_{\tilde{\alpha}} \geqslant 0$ и $\sum\limits_{\tilde{\alpha}\in B_n} p_{\tilde{\alpha}} = 1$.

Определение 1. Пусть f_e — функция, реализуемая на элементе e схемы A. Величину $S(e) = \sum p_{\tilde{\alpha}} f_e(\tilde{\alpha})$, где сумма берется по всем наборам $\tilde{\alpha}$, будем называть *средней мощностью элемента* e.

Определение 2. Пусть $L(A)$ — сложность (число элементов) схемы A, $(e_1, \ldots, e_{L(A)})$ - элементы схемы A. Величина $S(A)$, определяемая соотношением $S(A) = \sum\limits_{i=1}^{L(A)} S(e_i)$, называется *средней мощностью* схемы A.

Определение 3. Схемы, реализующие одинаковые функции, называются *эквивалентными*.

Определение 4. Схема, имеющая наименьшую среднюю мощность среди всех эквивалентных ей схем, называется *оптимальной*.

Очевидно, что для любой схемы существует эквивалентная ей оптимальная схема.

С содержательной точки зрения, если предположить, что при появлении на выходе элемента схемы единицы, этот элемент имеет единичную тепловую мощность, т.е. выделяет единицу тепла в единицу времени, то средняя мощность схемы характеризует среднее тепловыделение схемы. Таким образом, возникает задача построения схемы с наименьшим тепловыделением по произвольному распределению вероятностей входных наборов, реализующей заданную функцию.

В данной статье рассматривается простейший случай этой задачи, когда $B = \{\&\}$, а реализуемая функция F есть конъюнкция n переменных, $F = x_1 \& \ldots \& x_n$.

Структура оптимальной схемы

Определение 5. Схема A называется *бесповторной*, если каждый вход схемы и выход каждого элемента схемы соединен не более, чем с одним входом не более, чем одного элемента схемы или выходом схемы.

Лемма 1. Для любого распределения $\{p_{\tilde{\alpha}}\}$ найдется бесповторная оптимальная схема.

Определение 6. Будем говорить, что схема имеет вид *цепи*, если ее входы и элементы можно занумеровать таким образом, что входы первого элемента будут соединены с двумя первыми входами схемы, а входы i-го элемента будут соединены с выходом $(i-1)$-го элемента и $(i+1)$-м входом схемы для всех $i = 2, \ldots, n-1$.

Теорема 1. Для любого распределения вероятностей $\{p_{\tilde{\alpha}}\}$ входных наборов длины n, среди схем, реализующих конъюнкцию n переменных в базисе $\{\&\}$, найдется оптимальная схема, имеющая вид цепи.

Таким образом, поиск оптимальной схемы достаточно производить только среди схем, имеющих вид цепи. Для исследования этой задачи воспользуемся геометрической интерпретацией.

Геометрическая интерпретация

Распределение вероятностей появления наборов длины n на входах схемы можно рассматривать, как точку в 2^n-мерном евклидовом пространстве. Обратное соответствие, очевидно, имеет место не для всех точек пространства, а только для тех, координаты которых неотрицательны и в сумме дают единицу. Таким образом, множество точек, которым можно поставить в соответствие некоторое распределение вероятностей входных наборов, представляет собой симплекс, натянутый на точки с координатами $(0, \ldots, 1, \ldots, 0)$, где единица занимеает i-ю позицию, $i = 1, \ldots, 2^n$. Обозначим его через T_0. Размерность симплекса T_0 равна $2^n - 1$.

Определение 7. Будем говорить, что схема A *оптимальна в точке* P симплекса T_0, если она оптимальна при распределении вероятностей входных наборов, соответствующем точке P.

Определение 8. Множество всех точек симплекса T_0, в которых схема A оптимальна назовем *областью оптимальности* схемы A.

Модифицируем задачу: вместо того, чтобы искать оптимальную схему по известному распределению вероятностей входных наборов, будем искать для каждой схемы ее область оптимальности.

Оси координат, соответствующие наборам, упорядочим по возрастанию количества единиц в наборах, причем порядок осей, соответствующих наборам с одинаковым числом единиц, выберем произвольный. Другими словами, первая координата соответствует набору из одних нулей, следующие n координат соответствуют наборам с одной единицей и так далее. Последняя координата соответствует набору из одних единиц.

Заметим, что вероятности некоторых наборов не влияют на оптимальность схемы. К таким наборам относятся:

1. Наборы, содержащие менее двух единиц. Мощность схемы на таких наборах будет равна нулю. Таких наборов $n+1$.

2. Набор из одних единиц. Мощность схемы на таком наборе равна сложности схемы, но так как все рассматриваемые схемы имеют одинаковую сложность, то вклад такого набора в среднюю мощность схемы будет одинаковым для всех схем.

Следовательно, при определении оптимальной схемы, вероятности появления указанных наборов можно не учитывать. Таким образом, без ограничения общности можно считать сумму вероятностей наборов, указанных в пунктах 1 и 2 равной нулю, т. е. вместо всего пространства рассматривать его сечение гиперплоскостью. Ограничение симплекса T_0 на полученное сечение обозначим через T_1. Легко показать, что T_1 тоже симплекс. Далее, можно отбросить оси координат, соответствующие несущественным наборам, уменьшив тем самым размерность пространства до $(2^n - n - 2)$. Обозначим полученное пространство через E_n. Такое сужение пространства избавляет нас от необходимости учитывать вероятности несущественных наборов, а также дает возможность наглядно представить пространство распределений при $n = 3$, т. к. его размерность уменьшится с 8 до 3. Проекцию симплекса T_1 на E_n обозначим через T_2.

Очевидно, что, если мы будем знать, как устроены области оптимальности схем в симплексе T_2, то мы будем знать, как устроены области оптимальности схем не только в симплексе T_1, но и в симплексе T_0, т. е. во всем пространстве распределений входных наборов.

Итак, пусть область Z есть пересечение областей оптимальности всех схем в симплексе T_2.

Рассмотрим следующие $n-2$ точки пространства E_n:

$P_k = (\underbrace{0,\ldots,0}_{N_k},\underbrace{p^{(k)},\ldots p^{(k)}}_{C_n^k},0,\ldots,0)$, где $p^{(k)} = \frac{1}{C_n^k}$, $N_k = \sum\limits_{i=2}^{k-1} C_n^i$, $k = 2,\ldots,n-1$. Другими словами, все координаты, соответствующие наборам, содержащим ровно k единиц, равны $p^{(k)}$, а остальные координаты равны нулю.

Теорема 2. Область Z имеет размерность $n-3$ и представляет собой выпуклую линейную оболочку точек P_k, где $k = 2,\ldots,n-1$. А именно, любую точку M области Z можно представить в виде $M = \sum\limits_{i=2}^{n-1} \lambda_i P_i$, где $\sum\limits_{i=2}^{n-1} \lambda_i = 1$, $\lambda_i \geq 0$ при $i = 2,\ldots,n-1$.

Пример

Для $n = 3$ пространство E_3 имеет размерность 3, а оси координат со-

ответствуют наборам $(0,1,1)$, $(1,0,1)$ и $(1,1,0)$. Симплекс T_2 представляет собой треугольник, вершины которого имеют координаты $(1,0,0)$, $(0,1,0)$ и $(0,0,1)$, а область Z состоит из одной точки с координатами $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$.

Для $n = 4$ пространство E_4 имеет размерность 10, а оси координат соответствуют наборам с двумя и тремя единицами. Область Z в этом случае имеет размерность 2 и представляет собой отрезок с концами в точках $P_2 = (\frac{1}{6},\frac{1}{6},\frac{1}{6},\frac{1}{6},\frac{1}{6},\frac{1}{6},0,0,0,0)$ и $P_3 = (0,0,0,0,0,0,\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4})$. Средняя мощность любой оптимальной схемы A на этом отрезке в точке $M = tP_2 + (1-t)P_3, t \in [0,1]$, будет равна $S(A) = \frac{9-7t}{12}$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00994), Программы поддержки ведущих научных школ РФ и Программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики"(проект "Синтез и сложность управляющих систем").

Список литературы

1. Касим-Заде О.М. Об одной мере сложности схем из функциональных элементов //Проблемы кибернетики. Вып. 38. М.: Наука, 1981.

2. Касим-Заде О.М. О мощности индивидуальных функций //Сборник трудов семинара по дискретной математике и ее приложениям (Москва, МГУ, 2-4 февраля 1993г.). М.: Изд-во механико-математического факультета МГУ, 1998. С. 63–65.

3. Лейхтвейс К. Выпуклые множества. М.: Наука, 1985.

4. Люстерник Л.А. Выпуклые фигуры и многогранники. М.: Гостехиздат, 1956.

5. Яблонский С.В. Введение в дискретную математику. Издание 4-е, стереотипное. М.: Высшая школа, 2003.