Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.62

О РЕШЕНИИ КВАДРАТНЫХ УРАВНЕНИЙ В БИНАРНЫХ ПОЛЯХ

К. Л. Глуско, С. С. Титов

Передача информации в современных каналах связи основана на использовании многобитовых последовательностей, которые можно интерпретировать как элементы конечных полей. Поэтому решение задач в бинарных полях больших степеней и представление этих решений в виде битовых строк является важной проблемой. Решение квадратных уравнений в конечных полях используется в разных областях математики и защиты информации. В эллиптической криптографии, к примеру, это позволяет в два раза уменьшить количество бит для хранения точек эллиптической кривой при реализации криптографических примитивов [1, 2].

След — линейная операция $\mathrm{Tr}_{F/K}$, отображающая элементы поля F в элементы поля K, обладающая свойствами идемпотентности, коммутативности, ассоциативности и дистрибутивности [3].

Различают понятия абсолютного и относительного следа элемента поля. В поле $\mathrm{GF}(q)$, где $q = p^n$, $\mathrm{Tr}(z) \in \mathrm{GF}(q)$ и может принимать значения 0, 1, ..., $p-1$, формула абсолютного следа элемента поля имеет вид

$$\mathrm{Tr}(z) = z + z^p + z^{p^2} + \ldots + z^{p^{n-1}}.$$

Значение следа элемента часто является определяющим для выполнения тех или иных условий. Любое квадратное уравнение в поле характеристики два приводится к стандартному виду $x^2 + x = z$, где z — элемент данного поля, x — искомый корень [1]. Для решения такого квадратного уравнения при $\mathrm{Tr}(z) = 0$ в конечных полях $\mathrm{GF}(2^n)$ при нечётном n используется так называемая формула полуследа:

$$\mathrm{Sr}(z) = x = z + z^4 + z^{16} + \ldots + z^{2^{n-1}}.$$

Утверждение 1. Формула полуследа дает решение квадратного уравнения с нулевым следом в поле $\mathrm{GF}(2^n)$, где n нечётное.

Утверждение 2 [1, 4]. При чётном n не существует линеаризированного многочлена вида $z = \sum\limits_{s \in S} a^{2^s}$ (S — подмножество в $\{0, 1, \ldots, n-1\}$), дающего решение квадратного уравнения $z^2 + z = a$.

Решение квадратного уравнения может быть представлено в стандартном базисе, т. е. в базисе вида $\{1, \lambda, \lambda^2, \lambda^3, \ldots, \lambda^{n-1}\}$, но мы воспользуемся разложением в нормальном базисе, т. е. в базисе вида $\{\beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{n-1}}\}$, где λ и β — корни неприводимых многочленов степени n [2]. Отметим, что построение нормальных базисов является задачей нетривиальной.

Для построения базиса $\{\beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{n-1}}\}$ используем операцию симметричного квадратичного расширения $\alpha = \beta + \beta^{-1}$, где α является элементом поля F, β — элементом поля K, а поле K — расширением поля F [5].

Теорема 1. Если множество $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ является нормальным базисом в поле $\mathrm{GF}(2^n)$, след α^{-1} равен единице и $\alpha = \beta + \beta^{-1}$ в поле $\mathrm{GF}(2^{2^n})$, то множество $\{\beta, \beta^2, \ldots, \beta^{2^{2n-1}}\}$ также является нормальным базисом в поле $\mathrm{GF}(2^{2^n})$ [4].

Разложим квадратное уравнение $x^2 + x = a$ в нормальном базисе $\{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}}\}$:

$$\begin{cases} x = \alpha x_0 + \alpha^2 x_1 + \alpha^4 x_2 + \ldots + \alpha^{2^{k-1}} x_{k-1}, \\ a = \alpha a_0 + \alpha^2 a_1 + \alpha^4 a_2 + \ldots + \alpha^{2^{k-1}} a_{k-1}, \\ x^2 = \alpha^2 x_0 + \alpha^4 x_1 + \alpha^8 x_2 + \ldots + \alpha^{2^k} x_{k-1}. \end{cases}$$

Просуммируем эти уравнения и с учётом необходимого условия равенства нулю множителей при степенях α получим

$$\begin{cases} x_0 + a_0 + x_{k-1}^2 = 0, \\ x_1 + a_1 + x_0^2 = 0, \\ x_2 + a_2 + x_1^2 = 0, \\ \ldots \quad \ldots \quad \ldots \\ x_{k-1} + a_{k-1} + x_{k-2}^2 = 0. \end{cases}$$

Решив систему, получим формулу для x_0:

$$x_0 = (\mathrm{Sr}(\mathrm{Sr}(\mathrm{Sr}(\ldots(\mathrm{Sr}(b_0)))))),$$

где $b_0 = x_0^{2^k} + x_0$ и число операций Sr равно k.

Аналогично находим остальные элементы корней.

Описанный метод дает возможность быстро найти корни квадратных уравнений $x^2 + x = a$ в полях $\mathrm{GF}(2^m)$ при любых m и представить эти решения в виде битовых строк.

ЛИТЕРАТУРА

1. *Болотов А. А., Гашков С. В., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. С. 76–81.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. С. 41–63.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. С. 74–75.
4. *Глуско К. Л.* След и полуслед в конечных полях // Материалы науч.-техн. конф., посв. 55-летию УрГУПС. Екатеринбург: Уральский государственный университет путей сообщения, 2011. Т. 1. Вып. 97(180) С. 356–364.
5. *Демкина О. Е., Титов С. С., Торгашева А. В.* Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования // Молодые учёные — транспорту: Труды IV науч.-техн. конф. Екатеринбург: Уральский государственный университет путей сообщения, 2003. С. 391–404.

УДК 519.7

ЛИНЕЙНАЯ СЛОЖНОСТЬ ОБОБЩЁННЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ $2^m p^n$

В. А. Едемский, О. В. Антонова

Пусть $X = \{x_i\}, x_i \in \{0,1\}$ — последовательность с периодом $N = 2^m p^n$, где p — нечётное простое число, а m, n — натуральные числа. Её минимальный многочлен $m(t)$ и линейную сложность L над полем $\mathrm{GF}(2)$ можно определить по следующим формулам:

$$m(t) = (t^N - 1)/\left((t^{p^n} - 1)^{2^m}, S(t)\right), \qquad L = N - \deg\left((t^{p^n} - 1)^{2^m}, S(t)\right),$$

где $S(t)$ — производящая функция цикла последовательности. Следовательно, если α — примитивный корень степени p^n из единицы в расширении поля $\mathrm{GF}(2)$, то для вычисления минимального многочлена и линейной сложности последовательности X достаточно найти корни многочлена $S(t)$ в множестве $\{\alpha^v : v = 0, 1, \ldots, p^n - 1\}$ и определить их кратность. Метод вычисления значений $S(\alpha^v)$ для обобщённых циклотомических последовательностей с периодом p^n предложен в [1, 2], здесь обобщим его на последовательности с периодом $2^m p^n$.

Пусть $H_k = \{\theta^{k+td} \pmod{p^n} : t = 1, \ldots, p^{n-1}(p-1)/d\}$, $k = 0, 1, \ldots, d-1$ — циклотомические классы порядка d по модулю p^n, где θ — первообразный корень по модулю p^n, а d — делитель $p - 1$, $d \geqslant 2$. Справедливо разбиение

$$\mathbb{Z}_{p^n} = \bigcup_{j=0}^{n-1} \bigcup_{k=0}^{d-1} p^j H_k \cup \{0\}.$$

Кольцо классов вычетов $\mathbb{Z}_N$ изоморфно прямому произведению $\mathbb{Z}_{2^m} \otimes \mathbb{Z}_{p^n}$ относительно изоморфизма $\varphi(a) = (a \bmod 2^m, a \bmod p^n)$. Пусть $H_{l,k} = \varphi^{-1}\left(\{l\} \otimes \bigcup_{j=0}^{n-1} p^j H_k\right)$ для $l = 0, 1, \ldots, 2^m - 1; k = 0, 1, \ldots, d-1$, тогда $H_{l,k}$ и множество $\{0, p^n, \ldots, (2^m - 1)p^n\}$ образуют разбиение $\mathbb{Z}_N$.

Рассмотрим последовательность X, определяемую следующим образом:

$$x_i = \begin{cases} 1, & \text{если } i \bmod N \in C, \\ 0 & \text{иначе.} \end{cases} \tag{1}$$

Здесь $C = \bigcup_{l=0}^{2^m-1} \bigcup_{k \in I_l} H_{l,k} \cup \{0, 2p^n, \ldots, 2^{m-1}p^n\}$; I_l, $l = 0, 1, \ldots, 2^m - 1$ — подмножества индексов, элементы которых могут принимать значения от 0 до $d - 1$.

Пусть $\mathbf{S}_d(x) = \left(S_d(x), S_d(x^\theta), \ldots, S_d(x^{\theta^{d-1}})\right)$, $\mathbf{R}(x) = \sum_{k \in I} \mathbf{S}_d(x^{\theta^k})$ и $\mathbf{Q}(x) = \sum_{k \in J} \mathbf{S}_d(x^{\theta^k})$, где $S_d(t) = \sum_{u \in H_0} t^{u \bmod p}$, а I, J — множества, состоящие из номеров k, входящих нечётное число раз в подмножества I_l, $l = 0, 1, \ldots, 2^m - 1$, с чётными и нечётными номерами соответственно. Обозначим координаты вектор-функций $\mathbf{R}(x)$ и $\mathbf{Q}(x)$ при $x = \alpha^{p^{n-1}}$ через r_i, q_i для $i = 0, 1, \ldots, d-1$. Пусть $\delta = 1$ для $m = 1$ и $\delta = 0$ при $m > 1$.

Теорема 1. Если $v \in p^f H_j$, $f = 0, 1, \ldots, n-1$, $j = 0, 1, \ldots, d-1$, то α^v — корень многочлена $S(t)$ тогда и только тогда, когда $r_j + q_j = (|I| + |J|)f(p-1)/d + \delta$, и корень α^v многочлена $S(t)$ кратный тогда и только тогда, когда $r_j = |I| f(p-1)/d + \delta$.

Теорема 1 показывает, что известные значения $\mathbf{R}(x), \mathbf{Q}(x)$, а фактически $\mathbf{S}_d(x)$, позволяют оценить линейную сложность последовательности X. Метод вычисления значений $\mathbf{S}_d(x)$ предложен в [1], следовательно, теорема 1 определяет метод анализа линейной сложности последовательностей с периодом $2^m p^n$, сформированных по правилу (1).

Воспользовавшись теоремой 1, несложно получить следующие утверждения.

Лемма 1. Если $d = 2$ и $I_0 = I_1 = \{0\}$, то для последовательности X, сформированной по правилу (1) при $N = 2p^n$, линейная сложность $L = 2p^n$, а её минимальный многочлен $m(t) = t^{2p^n} - 1$.

Лемма 2. Если $d = 4$ и $I_0 = \{0, 1\}$, то для линейной сложности последовательности X, сформированной по правилу (1) при $N = 2p^n$, справедливо:

1) $L = 2p^n$, если $I_1 = \{0, 1\}$, или $I_1 = \{0, 2\}$ и $\left(\frac{2}{p}\right)_4 \neq 1$, или $I_1 = \{0, 3\}$ и $\left(\frac{2}{p}\right) \neq 1$, где $\left(\frac{2}{p}\right)$ — символ Лежандра, а $\left(\frac{2}{p}\right)_4$ — символ 4-степенного вычета;
2) $L = (3p^n + 1)/2$, если $I_1 = \{0, 3\}$ и $\left(\frac{2}{p}\right) = 1$, $\left(\frac{2}{p}\right)_4 \neq 1$;
3) $L = (5p^n + 1)/4$, если $\left(\frac{2}{p}\right)_4 = 1$ и $I_1 = \{0, 2\}$ или $I_1 = \{0, 3\}$.

Аналогично можно получить следующие оценки линейной сложности последовательностей.

Лемма 3. Если $d = 2$ и последовательность X с периодом $4p^n$ определена правилом (1) при $I_0 = I_1 = I_2 = \{0\}, I_3 = \{1\}$, то $L \geqslant 4p^n - 4$.

Лемма 4. Если $d = 4$ и последовательность X с периодом $8p^n$ определена правилом (1) при $I_0 = I_1 = I_2 = I_5 = \{0\}$, $I_3 = \{1\}$, $I_4 = I_6 = \{2\}$ и $I_7 = \{3\}$, то $L \geqslant 8p^n - 8$, если $\left(\frac{2}{p}\right) \neq 1$, и $L \geqslant 4p^n - 8$, если $\left(\frac{2}{p}\right) = 1$.

Таким образом, предложен метод анализа линейной сложности последовательностей с периодом $2^m p^n$, построенных на основе обобщённых циклотомических классов. Метод позволяет как явно рассчитать линейную сложность и минимальный многочлен рассматриваемых последовательностей, так и оценить её, а также определить характеристики последовательностей, обладающих заведомо высокой линейной сложностью.

Подробное изложение представленных результатов можно найти в [3].

ЛИТЕРАТУРА

1. *Едемский В. А.* О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010. Т. 22. № 1. С. 74–82.
2. *Edemskiy V. A.* About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1} // Designs, Codes and Cryptography. 2011. V. 61. No. 3. P. 251–260.
3. *Едемский В. А., Антонова О. В.* Линейная сложность обобщённых циклотомических последовательностей с периодом $2^m p^n$ // Прикладная дискретная математика. 2012. № 3 (в печати).

УДК 519.212.2

О РАСПРЕДЕЛЕНИЯХ ВЕСОВЫХ СПЕКТРОВ СЛУЧАЙНЫХ ЛИНЕЙНЫХ ДВОИЧНЫХ КОДОВ

А. М. Зубков, В. И. Круглов

Рассмотрим N-мерное линейное пространство $B_N = \mathrm{GF}(2)^N = \{X = (x_1, \ldots, x_N) : x_1, \ldots, x_N \in \mathrm{GF}(2)\}$. Под линейным кодом размерности k понимается k-мерное подпространство $L \subset B_N$ (см. [1, 2]).

Весом $\mathrm{w}(X)$ двоичного вектора $X = (x_1, \ldots, x_N) \in B_N$ называется количество ненулевых координат в векторе X. Через B_N^s и $B_N^{\leqslant s}$ будем обозначать соответственно множества векторов фиксированного веса s и веса, не превосходящего s, в B_N :

$$B_N^s = \{X \in B_N : \mathrm{w}(X) = s\}, \quad B_N^{\leqslant s} = \{X \in B_N : \mathrm{w}(X) \leqslant s\},$$

тогда $B_N = \bigsqcup_{s=0}^{N} B_N^s$.

Пусть $v_s(L) = |L \cap B_N^s|$ и $v_{\leqslant s}(L) = |L \cap B_N^{\leqslant s}|$ — количество векторов веса s и количество векторов веса не больше s в линейном коде L; набор $\{v_s(L)\}_{s=0}^N$ называют весовым спектром кода L.

Теорема 1. Если L — случайный k-мерный код в B_N, имеющий равновероятное распределение на множестве всех таких кодов, то при $s = 1, \ldots, N$

$$\mathbf{E}v_s(L) = C_N^s \frac{2^k - 1}{2^N - 1}, \ \mathbf{D}v_s(L) = C_N^s \frac{\left(2^k - 1\right)}{(2^N - 1)} \frac{\left(2^N - 2^k\right)}{(2^N - 2)} \left(1 - \frac{C_N^s}{2^N - 1}\right)$$

и при $s, t \in \{1, \ldots, N\}$, $s \neq t$,

$$\mathrm{cov}(v_s(L), v_t(L)) = -C_N^s C_N^t \frac{(2^k - 1)(2^N - 2^k)}{(2^N - 1)^2 (2^N - 2)}.$$

Теорема 2. При $s = 1, \ldots, N$

$$\mathbf{E}v_{\leqslant s}(L) = \frac{2^k - 1}{2^N - 1} \sum_{r=1}^{s} C_N^r, \ \mathbf{D}v_{\leqslant s}(L) = \frac{\left(2^k - 1\right)}{(2^N - 1)} \frac{\left(2^N - 2^k\right)}{(2^N - 2)} \left(1 - \frac{1}{2^N - 1} \sum_{r=1}^{s} C_N^r\right) \sum_{r=1}^{s} C_N^r.$$

Следствие 1. Если $L \subset B_N$ — случайное равновероятное k-мерное подпространство и $\mu(L) = \min\{\mathrm{w}(x) : x \in L \backslash \{0\}\}$, то

$$\frac{1}{1 + \dfrac{2^N - 2^k}{2^N - 2} \left(\mathbf{E}v_{\leqslant s}(L)\right)^{-1}} \leqslant \mathbf{P}\{\mu(L) \leqslant s\} \leqslant \mathbf{E}v_{\leqslant s}(L).$$

Теорема 3. Если X и Y — независимые случайные векторы из B_N, причем X имеет равномерное распределение на B_N^s, а Y — равномерное распределение на B_N^t, то при $|s - t| \leqslant m \leqslant \min\{s + t, N\}$

$$\mathbf{P}\{\mathrm{w}(X \oplus Y) = m\} = p^{(N)}(t, s, m) \stackrel{\mathrm{def}}{=} \frac{C_s^{\frac{t+s-m}{2}} C_{N-s}^{\frac{t-s+m}{2}}}{C_N^t} I\{m \equiv t + s \,(\mathrm{mod}\, 2)\},$$

$$\mathbf{E}\mathrm{w}(X \oplus Y) = s + t - \frac{2st}{N}, \ \mathbf{D}\mathrm{w}(X \oplus Y) = 4 \frac{s(N - s)t(N - t)}{N^2(N - 1)}.$$

Теорему 3 можно использовать для вычисления моментов сумм

$$v_s^*(X_1,\dots,X_n) \stackrel{\text{def}}{=} \sum_{a_1,\dots,a_n=0}^{1} I\left\{\mathrm{w}\left(\sum_{j=1}^{n} a_j X_j\right) = s\right\}, s \in \{0,1,\dots,N\},$$

где $X_1, X_2, \dots, X_n \in B_N$ — независимые случайные векторы, распределения которых инвариантны относительно перестановок координат.

Теорема 4. Пусть $X_1,\dots,X_n$ — независимые случайные векторы, имеющие равномерное распределение на B_N^s, тогда

$$\mathbf{P}\{X_1,\dots,X_n \text{ линейно зависимы}\} \leqslant \frac{1}{2^N}\sum_{t=0}^{N} C_N^t \left[\left(1+\frac{c_{N,s,t}}{C_N^s}\right)^n - n\frac{c_{N,s,t}}{C_N^s} - 1\right],$$

где $c_{N,s,t} = \sum\limits_{j\geqslant 0}(-1)^j C_t^j C_{N-t}^{s-j}$.

ЛИТЕРАТУРА

1. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

УДК 519.7

ОЦЕНКИ ЧИСЛА БУЛЕВЫХ ФУНКЦИЙ, ИМЕЮЩИХ АФФИННЫЕ И КВАДРАТИЧНЫЕ ПРИБЛИЖЕНИЯ ЗАДАННОЙ ТОЧНОСТИ[1]

А. М. Зубков, А. А. Серов[1]

Пусть $V_n = (\mathrm{GF}(2))^n$. Обозначим через $\mathbb{F}_2^{V_n}$ множество всех булевых функций и через $\mathbb{L}_n$, $\mathbb{A}_n$ и $\mathbb{Q}_n$ — множества всех линейных, аффинных и квадратичных функций от n булевых аргументов соответственно; тогда $\mathbb{L}_n \subset \mathbb{A}_n \subset \mathbb{Q}_n$, $|\mathbb{L}_n| = 2^n$, $|\mathbb{A}_n| = 2^{n+1}$, $|\mathbb{Q}_n| = 2^{\binom{n}{2}+n+1}$.

Пусть $\rho(f,g) = |\{x \in V_n : f(x) \neq g(x)\}|$ — расстояние Хэмминга между булевыми функциями $f, g \in \mathbb{F}_2^{V_n}$ и $\rho(f,A) = \min\limits_{g\in A}\rho(f,g)$ для произвольных $f \in \mathbb{F}_2^{V_n}$ и $A \subset \mathbb{F}_2^{V_n}$. В [1–3] показано, что если $f \in \mathbb{F}_2^{V_n}$ — случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^{V_n}$, то для каждого фиксированного $x \in \mathbb{R}$

$$\lim_{n\to\infty}\mathbf{P}\left\{\frac{\rho(f,\mathbb{L}_n)-a_n}{b_n} < x\right\} = 1-e^{-e^x}, \quad \lim_{n\to\infty}\mathbf{P}\left\{\frac{\rho(f,\mathbb{A}_n)-a_n}{b_n} < x-\ln 2\right\} = 1-e^{-e^x},$$
$$\lim_{n\to\infty}\mathbf{P}\left\{\frac{\rho(f,\mathbb{Q}_n)-c_n}{d_n} < x\right\} = 1-e^{-e^x},$$

где

$$a_n = 2^{n-1} - 2^{\frac{n-1}{2}}\sqrt{n\ln 2}\left(1-\frac{\ln\ln 2^n + \ln 4\pi}{4n\ln 2}\right), \quad b_n = \frac{2^{\frac{n-1}{2}}}{2\sqrt{n\ln 2}},$$
$$c_n = 2^{n-1} - 2^{\frac{n-2}{2}}n\sqrt{\ln 2}\left\{1+\frac{1}{2n}-\frac{4\ln(\pi n^2\ln 2)-\ln 2}{8n^2\ln 2}\right\}, \quad d_n = \frac{2^{\frac{n-2}{2}}}{n\sqrt{\ln 2}}.$$

[1]Работа поддержана грантом РФФИ, проект № 11-01-00139.

Из результатов [2, 3] следует, что если $\mathbb{F}_2^{V_n,\,\mathbb{A}_n}(r) = \{f \in \mathbb{F}_2^{V_n} : \rho(f,\mathbb{A}_n) \leqslant r\}$ и $\mathbb{F}_2^{V_n,\,\mathbb{Q}_n}(r) = \left\{f \in \mathbb{F}_2^{V_n} : \rho(f,\mathbb{Q}_n) \leqslant r\right\}$ — множества булевых функций, расстояния Хэмминга от которых до множеств $\mathbb{A}_n$ и $\mathbb{Q}_n$ соответственно не превосходят r, то для любого $\varepsilon > 0$

$$\lim_{n\to\infty} 2^{-2^n}\left|\mathbb{F}_2^{V_n,\,\mathbb{A}_n}\left(r_{n,1}^{+\varepsilon}\right)\right| = \lim_{n\to\infty} 2^{-2^n}\left|\mathbb{F}_2^{V_n,\,\mathbb{Q}_n}\left(r_{n,2}^{+\varepsilon}\right)\right| = 0,$$
$$\lim_{n\to\infty} 2^{-2^n}\left|\mathbb{F}_2^{V_n,\,\mathbb{A}_n}\left(r_{n,1}^{-\varepsilon}\right)\right| = \lim_{n\to\infty} 2^{-2^n}\left|\mathbb{F}_2^{V_n,\,\mathbb{Q}_n}\left(r_{n,2}^{-\varepsilon}\right)\right| = 1,$$

где $r_{n,1}^{\pm\varepsilon} = 2^{n-1} - (1\pm\varepsilon)\sqrt{2^{n-1}n\ln 2}$; $\quad r_{n,2}^{\pm\varepsilon} = 2^{n-1} - (1\pm\varepsilon)n\sqrt{2^{n-2}\ln 2}$.

Теорема 1 [4]. Если $n \geqslant 2$, то

$$(1 - Q_1(n,r))2^{n+1}\sum_{m=0}^{r} C_{2^n}^m \leqslant |\,\mathbb{F}_2^{V_n,\,\mathbb{A}_n}(r)| \leqslant 2^{n+1}\sum_{m=0}^{r} C_{2^n}^m, \tag{1}$$

где $Q_1(n,r) = 0$ при $0 \leqslant r < 2^{n-2}$,

$$Q_1(n,r) < \frac{1}{15}\,2^{-\left(c^2-\frac{3}{2}\right)n}\exp\left\{\frac{2(c^2n)^{3/2}}{2^{n/2}}\right\}$$

при $n \geqslant 8$, $r = 2^{n-1} - c\sqrt{2^{n-1}n\ln 2} \geqslant 0$ и $c > 1$.

Следствие 1. Если $r_n = 2^{n-1} - c(n)\sqrt{2^{n-1}n\ln 2} \geqslant 0$, $c(n) > \sqrt{3/2}$ и $n \to \infty$, то

$$Q_1\left(n, r_n\right) \to 0\,.$$

Теорема 2. Если $n \geqslant 3$, то

$$(1 - Q_2(n,r))2^{\binom{n}{2}+n+1}\sum_{m=0}^{r} C_{2^n}^m \leqslant |\,\mathbb{F}_2^{V_n,\,\mathbb{Q}_n}(r)| \leqslant 2^{\binom{n}{2}+n+1}\sum_{m=0}^{r} C_{2^n}^m, \tag{2}$$

где $Q_2(n,r) = 0$ при $0 \leqslant r < 2^{n-3}$,

$$Q_2(n,r) < \frac{2^{-n^2\left(c^2-3\right)/6+n+1}}{n^2}\exp\left\{\frac{(cn)^3}{7\cdot 2^{n/2}}\right\}$$

при $n \geqslant 15$, $r = 2^{n-1} - cn\sqrt{2^{n-2}\ln 2} \geqslant 0$ и $c > 1$.

Следствие 2. Если $r_n = 2^{n-1} - c(n)n\sqrt{2^{n-2}\ln 2} \geqslant 0$, $c(n) > \sqrt{3}$ и $n \to \infty$, то

$$Q_2\left(n, r_n\right) \to 0\,.$$

Таким образом, если выполнены условия следствия 1 (следствия 2), то левые и правые части оценок (1) (оценок (2)) асимптотически эквивалентны.

ЛИТЕРАТУРА

1. *Ryasanov B. V.* Probabilistic methods in the theory of approximation of discrete functions // 3rd International Petrozavodsk Conference. 1993. P. 403–412.
2. *Рязанов Б. В., Чечёта С. И.* О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. 1995. № 3. С. 129–145.
3. *Серов А. А.* Предельное распределение расстояния между случайной булевой функцией и множеством аффинных функций // Теория вероятн. и ее примен. 2010. № 4. С. 791–795.

4. *Зубков А. М., Серов А. А.* Оценки числа булевых функций, имеющих аффинные приближения заданной точности // Дискретная математика. 2010. № 4. С. 3–19.

УДК 519.7

О НЕЛИНЕЙНОСТИ НЕКОТОРЫХ БУЛЕВЫХ ФУНКЦИЙ С МАКСИМАЛЬНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ

Н. А. Коломеец

После публикации работ [1, 2] большое внимание уделяется алгебраической иммунности булевых функций. Алгебраическая иммунность булевой функции f (обозначается через $\mathrm{AI}(f)$) — это минимальная положительная алгебраическая степень булевой функции, аннулирующей f или $f \oplus 1$, т. е.

$$\mathrm{AI}(f) = \min_{g \neq 0} \{\deg(g) : \forall x\, f(x)g(x) = 0 \text{ или } \forall x\, (f(x) \oplus 1)g(x) = 0\}.$$

Известно, что для функции f от n переменных $AI(f) \leqslant \lceil n/2 \rceil$. Для криптографических приложений наибольший интерес представляют функции с максимально возможной алгебраической иммунностью, т. е. с $\mathrm{AI}(f) = \lceil n/2 \rceil$ (такое значение алгебраической иммунности достижимо для любого n).

В данной работе исследуется нелинейность функций, обладающих максимально возможной алгебраической иммунностью, а именно: рассматриваются функции, построенные с помощью одной из самых простых конструкций для чётного числа переменных, которая предложена D. K. Dalai и др. в работе [3]:

$$f(x) = \begin{cases} 0, & \mathrm{wt}(x) < n/2, \\ b \in \{0, 1\}, & \mathrm{wt}(x) = n/2, \\ 1, & \mathrm{wt}(x) > n/2, \end{cases} \tag{1}$$

где n — количество переменных (n чётно); $\mathrm{wt}(x)$ — вес Хэмминга вектора x. Все такие функции обладают алгебраической иммунностью $n/2$.

Нелинейностью булевой функции f (обозначается через $\mathrm{nl}(f)$) называется расстояние Хэмминга от функции f до класса аффинных функций (функций вида $a_1x_1 \oplus \ldots \oplus a_nx_n \oplus a_0$). Это также одно из важнейших криптографических свойств булевых функций.

Получена следующая верхняя оценка нелинейности функций вида (1).

Теорема 1. Для функций f вида (1) выполняется

$$\mathrm{nl}(f) \leqslant 2^{n-1} - \binom{n-1}{n/2}.$$

В той же работе [3] рассматривается нелинейность функций, полученных с помощью данной конструкции, а именно доказано

Утверждение 1 (Dalai и др. [3]). Для функции

$$f(x) = \begin{cases} 0, & \mathrm{wt}(x) \leqslant n/2, \\ 1, & \mathrm{wt}(x) > n/2 \end{cases}$$

от n переменных (n чётно) верно

$$\mathrm{nl}(f) = 2^{n-1} - \binom{n-1}{n/2}.$$

Таким образом, оценка из теоремы 1 достижима.

Поскольку максимальная нелинейность для функций от чётного числа переменных равна $2^{n-1}-2^{n/2-1}$, нелинейность функций вида (1) заметно отличается от максимально возможной.

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic Attacks on Stream Ciphers with Linear Feedback // LNCS. 2003. V. 2656. P. 345–359.
2. *Meier W., Pasalic E., and Carlet C.* Algebraic Attacks and Decomposition of Boolean Functions // LNCS. 2004. V. 3027. P. 474–491.
3. *Dalai D.K., Maitra S., and Sarkar S.* Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity // Designs, Codes and Cryptography. 2006. V. 40. Iss. 1. P. 41–58.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ. II

О. Л. Колчева, И. А. Панкратова

Следуя [1], будем говорить, что булева функция f *статистически не зависит от подмножества U своих аргументов*, если для любой её подфункции f', полученной фиксированием значений всех переменных в U, имеет место $\mathrm{w}(f') = \mathrm{w}(f)/2^{|U|}$, где $\mathrm{w}(f)$ — вес функции f.

В [2] доказано следующее утверждение.

Утверждение 1. Пусть x, y, z — переменные со значениями в $(\mathbb{Z}_2)^n$, $(\mathbb{Z}_2)^m$ и $(\mathbb{Z}_2)^l$ соответственно и функция $f(x, y)$ статистически не зависит от переменных в x. Тогда и функция $h(x, y, z) = g\,(f(x, y), z)$, где g — любая функция от $l + 1$ переменных, статистически не зависит от переменных в x.

В общем случае это утверждение не допускает обобщения на случай нескольких внутренних функций f. Получено следующее достаточное условие статистической независимости от аргументов суперпозиции произвольной функции с двумя внутренними функциями.

Утверждение 2. Пусть x, y, z — переменные со значениями в $(\mathbb{Z}_2)^n$, $(\mathbb{Z}_2)^m$ и $(\mathbb{Z}_2)^l$ соответственно, функции $f_1(x, y)$, $f_2(x, y)$, $u(x, y) = f_1(x, y) \oplus f_2(x, y)$ статистически не зависят от переменных в x. Тогда и функция $h(x, y, z) = g\,(f_1(x, y), f_2(x, y), z)$, где g — любая функция от $l + 2$ переменных, статистически не зависит от переменных в x.

Доказательство. Для любых $a \in \{0, 1\}^n$, $i, j \in \{0, 1\}$ обозначим $c^a_{ij} = |\{y \in \in \{0, 1\}^m : f_1(a, y) = i, f_2(a, y) = j\}|$. В силу статистической независимости функций f_1, f_2, u от переменных в x для любого $a \in \{0, 1\}^n$ выполняется

$$c^a_{10} + c^a_{11} = \mathrm{w}(f_1)/2^n, \quad c^a_{01} + c^a_{11} = \mathrm{w}(f_2)/2^n, \quad c^a_{01} + c^a_{10} = \mathrm{w}(u)/2^n.$$

Отсюда получаем $c^a_{01} = (\mathrm{w}(u) - \mathrm{w}(f_1) + \mathrm{w}(f_2))/2^{n+1}$, $c^a_{10} = (\mathrm{w}(u) + \mathrm{w}(f_1) - \mathrm{w}(f_2))/2^{n+1}$, $c^a_{11} = (\mathrm{w}(f_1) + \mathrm{w}(f_2) - \mathrm{w}(u))/2^{n+1}$, $c^a_{00} = 2^m - (\mathrm{w}(u) + \mathrm{w}(f_1) + \mathrm{w}(f_2))/2^{n+1}$, т. е. c^a_{ij} не зависит от a для всех $i, j \in \{0, 1\}$. Тогда и вес подфункции функции h, полученной фиксацией переменных в x набором значений a, не зависит от a, так как $\mathrm{w}(h(a, y, z)) =$

$= \sum\limits_{i,j\in\{0,1\}} c_{ij}^a \cdot \mathrm{w}(g(i,j,z))$. Следовательно, функция h статистически не зависит от переменных в x. ■

Следующее утверждение характеризует условия статистической независимости от переменных в x суммы двух функций в частном случае — когда одна из функций зависит только от x.

Утверждение 3. Пусть x, y — переменные со значениями в $(\mathbb{Z}_2)^n$ и $(\mathbb{Z}_2)^m$ соответственно и функция $f(x,y)$ статистически не зависит от переменных в x. Тогда функция $f(x,y) \oplus g(x)$, где g — любая функция от n переменных, статистически не зависит от переменных в x, если и только если f уравновешена или $g = \mathrm{const}$.

Доказательство. По условию $\mathrm{w}(f(a,y)) = \mathrm{w}(f)/2^n$ для всех $a \in \{0,1\}^n$; следовательно, $\mathrm{w}(f(a,y) \oplus g(a))$ не зависит от a, если и только если $g = \mathrm{const}$ или $\mathrm{w}(f)/2^n = 2^m - \mathrm{w}(f)/2^n$; последнее равенство равносильно уравновешенности f. ■

ЛИТЕРАТУРА

1. *Агибалов Г. П., Панкратова И. А.* Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров // Прикладная дискретная математика. 2010. № 3(9). С. 51–68.
2. *Колчева О. Л., Панкратова И. А.* О статистической независимости суперпозиции булевых функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 11–12.

УДК 519.712.2

ОБ ОДНОЙ ЗАДАЧЕ КОМБИНАТОРНОЙ ОПТИМИЗАЦИИ[1]

А. С. Кузнецова, К. В. Сафонов

Пусть есть n стульев, каждый из которых имеет уникальный порядковый номер $i = 1, 2, \ldots, n$. Стулья расставлены по окружности. На стулья произвольным образом садятся n человек так, что на каждом стуле оказывается по одному человеку. Каждый человек имеет уникальный порядковый номер $j = 1, 2, \ldots, n$. Посадка называется правильной, если у всех стульев порядковые номера совпадают с номерами сидящих на них людей, в противном случае посадка называется неправильной. Будем называть перестановкой перемену мест двух сидящих рядом людей. Требуется вычислить наименьшее число перестановок d, которые позволят получить правильную посадку из произвольной начальной посадки.

Перестановки (p, q), указанные в условии задачи, порождают симметрическую группу S_n степени n. Запишем данную группу через порождающие элементы и определяющие соотношения. Пусть $x_1 = (1,2)$, $x_2 = (2,3)$, …, $x_{n-1} = (n-1, n)$, $x_n = (1, n)$ — порождающие элементы группы S_n. Теперь запишем определяющие соотношения R для S_n:

$$R = \begin{cases} x_i^2 = e, \ i = 1, 2, \ldots, n, \\ (x_i x_j)^2 = e, \text{ если } 1 < |j - i| < n - 1, \\ (x_i x_j)^3 = e, \text{ если } |j - i| = 1 \text{ или } |j - i| = n - 1, \\ x_1 x_2 \ldots x_{n-2} x_{n-1} x_{n-2} \ldots x_2 x_1 = x_n. \end{cases}$$

Таким образом,

$$S_n = \langle x_1, x_2, \ldots, x_n \mid R \rangle.$$

[1]Работа поддержана грантом РФФИ, проект № 10-01-00509-а.

Построим группу S_n в формате минимальных слов по алгоритму из [1]. В итоге максимальная длина минимальных слов группы S_n является решением задачи.

Ниже в таблице приведены решения для $n = 2, 3, \ldots, 12$, полученные при помощи компьютерных вычислений.

n	2	3	4	5	6	7	8	9	10	11	12
d	1	2	4	6	9	12	16	20	25	30	36

Аналогичные задачи встречаются на практике, например при проектировании компьютерных вычислительных сетей [2]. Сеть процессоров может быть представлена как неориентированный граф, в котором процессоры являются вершинами, а две вершины графа соединены ребром, если имеется прямое соединение между соответствующими процессорами. С одной стороны, желательно, чтобы между процессорами было как можно меньше соединений, а с другой — обмен данными между процессорами предпочтительно производить с наименьшим числом посредников. Очевидно, эти два критерия противоречат друг другу. На теоретико-групповом языке диаметр графа вычислительной сети равен максимальной длине минимальных слов соответствующей графу группы.

ЛИТЕРАТУРА

1. *Кузнецов А. А., Антамошкин А. Н., Шлёпкин А. К.* Моделирование периодических групп // Системы управления и информационные технологии. 2008. № 2. С. 4–8.
2. *Halt D., Eick B., and O'Brien E.* Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005.

УДК 519.6

СТРУКТУРНЫЕ СВОЙСТВА ПРИМИТИВНЫХ НАБОРОВ НАТУРАЛЬНЫХ ЧИСЕЛ

С. Н. Кяжин, В. М. Фомичев

При исследовании перемешивающих свойств композиции преобразований конечного множества возникает задача распознавания примитивности квадратной неотрицательной матрицы M и определения её экспонента [1, 2], то есть наименьшего натурального числа γ, при котором $M^\gamma > 0$.

При изучении указанных свойств матрица $M = (m_{ij})$ обладает ровно теми же свойствами, что и её носитель, то есть матрица $\nu(M) = (\nu m_{ij})$, где

$$\nu m_{ij} = \begin{cases} 1, \text{ если } m_{ij} > 0, \\ 0, \text{ если } m_{ij} = 0. \end{cases}$$

Вместо матрицы M можно равносильным образом исследовать примитивность и экспонент орграфа Γ, матрица смежности вершин которого совпадает с $\nu(M)$. Заметим, что множество 0,1-матриц порядка n образует полугруппу G_n относительно операции $*$, где $A * B = \nu(AB)$.

Критерий примитивности орграфа определяется длинами его простых контуров [1]. Если $C_1, \ldots, C_k$ — все простые контуры орграфа Γ длин $l_1, \ldots, l_k$ соответственно, то орграф Γ примитивный, если и только если наибольший общий делитель $\gcd(l_1, \ldots, l_k) = 1$. Таким образом, один из способов распознавания примитивности

орграфа Γ состоит в определении длин $l_1, \ldots, l_k$ всех его простых циклов и в проверке примитивности набора чисел $(l_1, \ldots, l_k)$, где набор натуральных чисел примитивен, если и только если эти числа взаимно просты.

Распознавание примитивности набора чисел $(l_1, \ldots, l_k)$ можно выполнить, применив $k-1$ раз алгоритм Евклида к элементам набора. Альтернативный подход состоит в использовании заранее составленной таблицы примитивных наборов при ограничении на числа $l_1, \ldots, l_k$.

Работа посвящена исследованию свойств примитивных наборов чисел и задаче построения таблицы примитивных наборов при ограничении на числа $l_1, \ldots, l_k$.

Утверждение 1. Если A — примитивный набор чисел, то примитивен любой набор, полученный из A добавлением любого натурального числа или (при $|A| > 1$) удалением числа a, кратного одному из остальных чисел набора.

Определение 1. Примитивный набор A размера $k \geqslant 1$ называется тупиковым, если $A = (1)$ или при $k > 1$ удаление из набора любого элемента нарушает его примитивность.

Определение 2. Примитивный набор A размера $k > 1$ называется r-примитивным, где $0 \leqslant r \leqslant k-1$, если после удаления из A любого подмножества порядка r примитивность получившегося набора сохраняется.

Рассмотрим набор натуральных чисел $A = (a_1, \ldots, a_k)$, где каждое из чисел набора не превышает m. Пусть 2^A — булеан множества $\{a_1, \ldots, a_k\}$, $P(A, r)$ — множество всех примитивных наборов порядка r из 2^A, $P(A) = \bigcup\limits_{r \leqslant k} P(A, r)$. На множестве $P(A)$ определим отношение частичного порядка: $(b_1, \ldots, b_l) \leqslant (a_1, \ldots, a_r)$, если и только если $l \leqslant r$ и найдется бесповторная упорядоченная выборка $(i_1, \ldots, i_l)$ из $(1, \ldots, r)$, такая, что $i_1 < \ldots < i_l$ и b_j делит a_{i_j} для всех $j = 1, \ldots, l$.

Определение 3. Тупиковый набор $B \in P(A)$ называется минимальным в $P(A)$, если не существует другого набора $B' \in P(A)$, такого, что $B' \leqslant B$, и r-минимальным в $P(A)$, если не существует другого набора $B' \in P(A)$ длины r, такого, что $B' \leqslant B$.

Утверждение 2. Если A — примитивный набор, то $\langle P(A), \leqslant \rangle$ — верхняя полурешётка, в которой максимальный элемент есть A и любой минимальный элемент есть тупиковый минимальный набор.

Для набора A рассмотрим наибольший общий делитель как функцию, определённую на 2^A. При $B = \{a_{i_1}, \ldots, a_{i_l}\} \in 2^A$ обозначим $\gcd(B) = \gcd(a_{i_1}, \ldots, a_{i_l})$, если $B \neq \varnothing$, и $\gcd(\varnothing) = \operatorname{lcm}(a_1, \ldots, a_k)$, где $\gcd(a_{i_1}, \ldots, a_{i_l})$ и $\operatorname{lcm}(a_{i_1}, \ldots, a_{i_l})$ — наибольший общий делитель и наименьшее общее кратное чисел $a_{i_1}, \ldots, a_{i_l}$ соответственно; $D(A) = \{\gcd(B) : B \in 2^A\}$. Множество $D(A)$ частично упорядочено по отношению делимости: $\gcd(B) \leqslant \gcd(B')$ для $B, B' \in 2^A$, если и только если $\gcd(B)$ делит $\gcd(B')$.

Утверждение 3. Если A — примитивный тупиковый набор, то $D(A)$ — решётка, антиизоморфная решётке 2^A.

Обозначим через A_i коатомы решётки 2^A и через μ_i — атомы решётки $D(A)$: $A_i = \{a_1, \ldots, a_k\} \setminus \{a_i\}$, $\mu_i = \gcd(A_i)$, $i = 1, \ldots, k$.

Теорема 1. Набор A — примитивный тупиковый, если и только если $(\mu_1, \ldots, \mu_k)$ — набор попарно взаимно простых чисел, отличных от 1. При этом $a_i = (c_i \mu_1 \cdot \ldots \cdot \mu_k)/\mu_i$, где $(c_1, \ldots, c_k)$ есть 1-примитивный набор натуральных чисел и $\gcd(c_i, \mu_i) = 1$ для $i = 1, \ldots, k$.

Следствие 1. Примитивный тупиковый набор A является k-минимальным, если и только если $(\mu_1, \ldots, \mu_k)$ — набор простых чисел и $c_i = 1$ для $i = 1, \ldots, k$.

По утверждению 1 любой примитивный набор A можно получить из соответствующего тупикового набора A' добавлением любого числа. По следствию 1 любой тупиковый набор A' можно получить из соответствующего k-минимального набора A'' умножением элемента набора a_i на число, взаимно простое с $\mu_i, i \in \{1, \ldots, k\}$.

Алгоритм перечисления множества всех k-минимальных примитивных наборов, состоящих из чисел, не превышающих m, состоит в следующем. В соответствии с теоремой 1 и следствием 1 k-минимальный тупиковый примитивный набор $A = (a_1, \ldots, a_k)$ состоит из чисел $a_i = (\mu_1 \cdot \ldots \cdot \mu_k)/\mu_i$, где $(\mu_1, \ldots, \mu_k)$ — набор различных простых чисел. Тогда если $\mu_1 < \ldots < \mu_k$, то достаточно перечислить все наборы $(\mu_1, \ldots, \mu_k)$ со свойством $\mu_2 \cdot \ldots \cdot \mu_k \leqslant m$.

В качестве μ_k перебираем все простые числа в пределах, указанных неравенством

$$p_s \leqslant \mu_s \leqslant \left(\frac{m}{3\Psi_{s-1}}\right)^{\frac{1}{k-s+1}}, \tag{1}$$

где $\Psi_i = p_3 \cdot \ldots \cdot p_i$; p_n — n-е простое число. При $3 \leqslant s < k$ и каждом фиксированном наборе чисел $(\mu_{s+1}, \ldots, \mu_k)$ в качестве μ_s перебираем все простые числа в пределах, указанных в (1). При каждом фиксированном наборе чисел $(\mu_3, \ldots, \mu_k)$ перебираем все простые числа μ_1 и μ_2, где $2 \leqslant \mu_1 < \mu_2 < m^{\frac{1}{k-1}}$.

Оценена вычислительная сложность алгоритма, измеренная числом построенных наборов различных простых чисел $(\mu_1, \ldots, \mu_k)$. Количество таковых не превышает $\mathrm{O}\left(m^{\ln k}\left(\ln^2 m \cdot \prod\limits_{j=2}^{k-1} \Psi_j\right)^{-1}\right)$. При $k > 2$ для оценки величин Ψ_k можно использовать оценку [3]: $p_k > k \ln k$. Тогда $\Psi_k > \dfrac{k!}{2} \prod\limits_{j=3}^{k} \ln j$.

Значения Ψ_k для $k = 3, \ldots, 8$ приведены в таблице.

k	3	4	5	6	7	8
Ψ_k	5	35	385	5005	85085	1616615

Данная таблица показывает, что при ограничении $a_1, \ldots, a_k \leqslant m$ число k-минимальных примитивных наборов быстро убывает с ростом k.

Рассмотренные свойства и алгоритм составления таблицы примитивных наборов могут быть использованы для изучения перемешивающих свойств преобразований, в частности для вычисления экспонентов перемешивающих матриц и соответствующих графов. Алгоритмические вопросы построения простых циклов в графе и вычисления экспонента орграфа рассмотрены более детально в [4].

ЛИТЕРАТУРА

1. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
2. *Фомичёв В. М.* Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010.
3. *Rosser B.* The n-th prime is greater than $n \log n$ // Proc. London Math. Soc. 1939. V. 45. P. 21–44.
4. *Кяжин С. Н., Фомичев В. М.* О примитивных наборах натуральных чисел // Прикладная дискретная математика. 2012. № 2. С. 5–14.

УДК 519.61+519.7

О ПОРЯДКЕ РОСТА ЧИСЛА ИНЪЕКТИВНЫХ И СВЕРХРАСТУЩИХ ВЕКТОРОВ И НЕКОТОРЫХ ОСОБЕННОСТЯХ СИЛЬНОГО МОДУЛЬНОГО УМНОЖЕНИЯ

Д. М. Мурин

В 1978 г. Р. Меркль и М. Хеллман [1] предложили знаменитую ранцевую криптосистему. В ее основе лежит преобразование сверхрастущего вектора $A = (a_1, a_2, \ldots, a_n)$ $(a_i \in \mathbb{N}, i = 1, \ldots, n)$ с помощью сильного модульного умножения относительно натурального модуля $m \in \left(\sum\limits_{i=1}^{n} a_i, 2\sum\limits_{i=1}^{n} a_i\right]$ и натурального множителя $t \in (1, m)$ в инъективный вектор $B = (b_1, b_2, \ldots, b_n)$ $(b_i \in \mathbb{N}, i = 1, \ldots, n)$, который служит открытым ключом.

В настоящей работе рассматриваются вопросы о том, какую часть от множества всех возможных векторов размерности n составляют инъективные и сверхрастущие векторы, и о равномерности покрытия множества упорядоченных инъективных векторов размерности n векторами, полученными из сверхрастущих векторов с помощью операции сильного модульного умножения и процедуры сортировки элементов вектора по возрастанию. Определения понятий упорядоченного (возрастающего), инъективного и сверхрастущего вектора, сильного модульного умножения можно найти в монографии [2].

О порядке роста числа инъективных и сверхрастущих векторов

Обозначим через $F_1(n, M)$ число упорядоченных инъективных векторов размерности n, максимальный элемент которых равен M, а через $F_2(n, M)$ — число сверхрастущих векторов размерности n, максимальный элемент которых равен M.

Число векторов с максимальным элементом M, имеющих размерность n, равно $\sum\limits_{k=1}^{n} C_n^k (M-1)^{n-k}$, из чего можно заключить, что $F_1(n, M) \leqslant \dfrac{n(M-1)^{n-1}}{n!}$, т. е. $F_1(n, M)$ при фиксированном n ограничено сверху некоторым полиномом степени $n-1$ от M. Оказывается, что справедлива следующая

Теорема. При фиксированном $n \geqslant 2$ и $M \geqslant 2^{n-1}$ выполняется неравенство $F_1(n, M) \geqslant F_2(n, M) \geqslant P(M)$, где $P(M)$ — некоторый полином $(n-1)$-й степени от M.

Например, $F_2(n, M) \geqslant \left(\dfrac{M - 2^{n-1} + 1}{2^{n-2}} - 1\right)\left(\dfrac{M - 2^{n-1} + 1}{2^{n-1}}\right)^{n-2}$ при $n \geqslant 2$ и $M \geqslant 2^{n-1}$. Это позволяет заключить, что функции $F_1(n, M)$ и $F_2(n, M)$ ведут себя подобно полиномам степени $n-1$ от M, а пределы $\lim\limits_{M\to\infty} \dfrac{F_1(n, M)}{\sum\limits_{k=1}^{n} C_n^k (M-1)^{n-k}}$, $\lim\limits_{M\to\infty} \dfrac{F_2(n, M)}{\sum\limits_{k=1}^{n} C_n^k (M-1)^{n-k}}$ при фиксированном n существуют, конечны и не равны 0.

Отметим, что $F_2(n, M) = 0$ при фиксированном $n \geqslant 2$ и $M < 2^{n-1}$.

О некоторых особенностях сильного модульного умножения

Рассмотрим множество сверхрастущих векторов размерности n, максимальный элемент которых строго меньше M. Операция сильного модульного умножения с модулем $m \leqslant M$ с последующим применением процедуры сортировки элементов вектора по возрастанию отображает указанное множество во множество упорядоченных инъективных векторов размерности n, максимальный элемент которых строго меньше M.

Обозначим через $F_3(n, < M)$ число упорядоченных инъективных векторов размерности n, максимальный элемент которых строго меньше M (т. е. мощность множества упорядоченных потенциальных векторов шифрования).

Обозначим через $F_4(n, < M)$ число различных упорядоченных инъективных векторов размерности n, полученных с помощью сильного модульного умножения относительно модуля m и всех возможных множителей $1 < t < m$ из сверхрастущих векторов размерности n, максимальный элемент которых строго меньше M, при условии, что для каждого сверхрастущего вектора $A = (a_1, \ldots, a_n)$ модуль m пробегает интервал $(\sum\limits_{i=1}^{n} a_i, \min(2\sum\limits_{i=1}^{n} a_i, M)]$. Таким образом, $F_4(n, < M)$ — мощность множества упорядоченных действительных векторов шифрования.

Различные тройки (сверхрастущий вектор, модуль, множитель) могут определять один упорядоченный инъективный вектор. Число троек, определяющих один упорядоченный инъективный вектор, назовем *числом представлений* данного вектора.

Обозначим через $F(n, < M)$ отношение $F_4(n, < M)/F_3(n, < M)$.

Проведенные вычислительные эксперименты позволяют выдвинуть следующую гипотезу.

Гипотеза. При фиксированном $n \in \mathbb{N}$ значение $F(n, < M)$ достигает 0,9 при значениях M, близких к 2^{2n}.

Так, при $n = 3$ и 4 значение $F(n, < M)$ достигает 0,9 при $M = 2^{2n-2} + 2^n - 1$.

В ходе проведения компьютерных экспериментов установлено, что в результате применения к сверхрастущим векторам операции сильного модульного умножения (при выборе модуля и множителя описанным выше способом) с последующим применением процедуры сортировки элементов вектора по возрастанию чаще получаются векторы, имеющие малую евклидову длину. На рис. 1 приведены результаты одного из экспериментов для $n = 3$ и $M = 34$. Каждому натуральному числу на оси Ln соответствует упорядоченный инъективный вектор. Меньшим натуральным числам соответствуют векторы с меньшей евклидовой длиной. По оси Representation number отложено число представлений упорядоченного инъективного вектора.

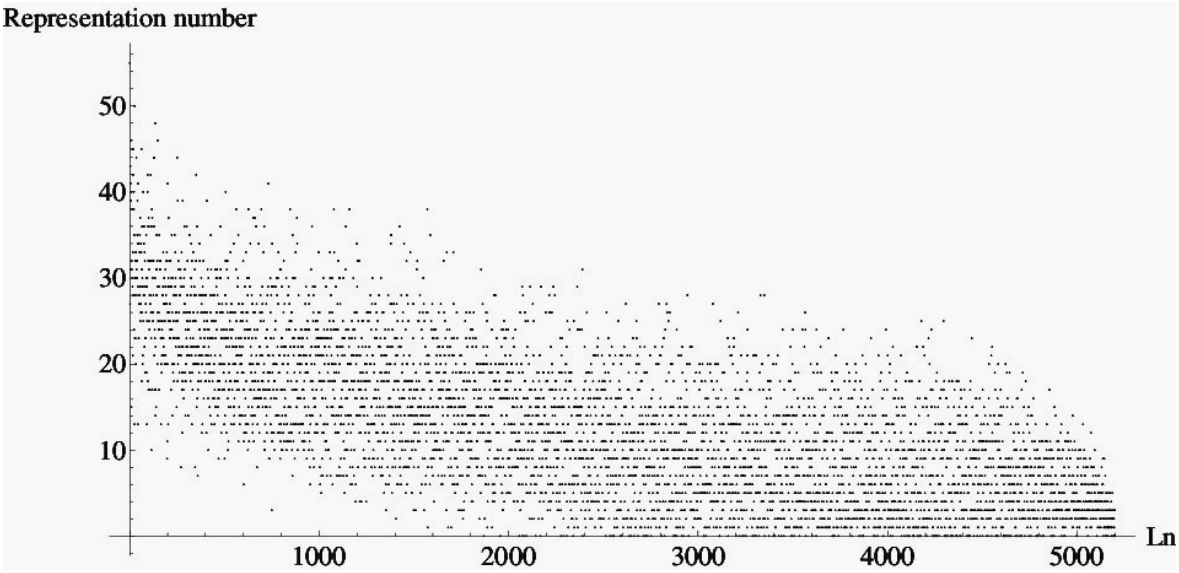

Рис. 1. Число представлений упорядоченных инъективных векторов при $n = 3$, $M = 34$

ЛИТЕРАТУРА

1. *Merkle R. C. and Hellman M. E.* Hiding information and signatures in trap-door knapsacks // IEEE Trans. Inform. Theory. 1978. V. IT-24. P. 525–530.
2. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995. 318 с.

УДК 512.542.74

ОПИСАНИЕ КЛАССА ПОДСТАНОВОК, ПРЕДСТАВИМЫХ В ВИДЕ ПРОИЗВЕДЕНИЯ ДВУХ ПОДСТАНОВОК С ФИКСИРОВАННЫМ ЧИСЛОМ МОБИЛЬНЫХ ТОЧЕК. II

А. Б. Пичкур

Пусть подстановка $G \in S_N$, $\Gamma(G) \subseteq \{1, \ldots, N\}$ — множество мобильных точек подстановки G, $2 \leqslant q \leqslant N$, $\Gamma_N(q) = \{G \in S_N : |\Gamma(G)| = q\}$ — множество всех подстановок степени N, имеющих ровно q мобильных точек.

В предшествующей работе (см. [1]) полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q)$ при $4 \leqslant q \leqslant N/2$ и $N \geqslant 8$.

В данной работе описано множество всех подстановок из $\Gamma_N(q) \cdot \Gamma_N(q+t)$ при $t \geqslant 1$. Этот результат имеет практические приложения в криптографии.

Сначала приведём результаты о строении множества $\Gamma_N(q) \cdot \Gamma_N(q+1)$.

Утверждение 1. Если $N \geqslant 6$, $2 \leqslant q_1 < q_2 < N$, то имеет место включение $\Gamma_N(q_1) \cdot \Gamma_N(q_2) \subseteq \Gamma_N(q_1+1) \cdot \Gamma_N(q_2+1)$.

Теорема 1. Пусть $N \geqslant 8$, $3 \leqslant q \leqslant N/2$, $G \in S_N$. Если $1 < |\Gamma(G)| \leqslant 2q-1$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+1)$, для которых выполняется равенство $G = H_1 \cdot H_2$.

Далее рассмотрим, какие подстановки из множеств $\Gamma_N(2q+1)$, $\Gamma_N(2q)$ принадлежат произведению $\Gamma_N(q) \cdot \Gamma_N(q+1)$.

Утверждение 2. Пусть $N \geqslant 4$, $2 \leqslant q < N/2$, подстановка $G \in \Gamma_N(2q+1)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \ldots, m_r$, $\sum\limits_{i=1}^{r} m_i = 2q+1$. Подстановка G принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$ в том и только в том случае, когда существует такое подмножество $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$, что $m_{i_1} + \cdots + m_{i_k} = q$.

Утверждение 3. Пусть $N \geqslant 4$, $2 \leqslant q \leqslant N/2$, подстановка $G \in \Gamma_N(2q)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \ldots, m_r$, $\sum\limits_{i=1}^{r} m_i = 2q$. Подстановка G принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$ в том и только в том случае, когда выполнено условие: существует $i_0 \in \{1, \ldots, r\}$ и существует такое подмножество $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\} \setminus \{i_0\}$, что $m_{i_0} > 2$ и $q - m_{i_1} + m_{i_2} + \cdots + m_{i_k} \in \in \{2, \ldots, m_{i_0} - 1\}$.

Итак, в теореме 1 и утверждениях 2 и 3 полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q+1)$ при $3 \leqslant q \leqslant N/2$.

Наконец, приведем результаты о строении множества $\Gamma_N(q) \cdot \Gamma_N(q+t)$, $t \geqslant 2$.

Теорема 2. Пусть $N > 10$, $2 \leqslant t < N-2$, $2 \leqslant q < (N-t)/2+1$, $G \in S_N$. Если $t \leqslant |\Gamma(G)| \leqslant 2q+t-2$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+t)$, для которых выполняется равенство $G = H_1 \cdot H_2$.

Можно доказать утверждения, аналогичные утверждениям 2 и 3, которые показывают, какие подстановки из множеств $\Gamma_N(2q+t-1)$, $\Gamma_N(2q+t)$ принадлежат произведению $\Gamma_N(q)\cdot\Gamma_N(q+t)$.

ЛИТЕРАТУРА

1. *Пичкур А. Б.* Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек // Прикладная дискретная математика. Приложение. 2011. №4. С. 16–17.

УДК 519.7

О КОМБИНАТОРНЫХ СВОЙСТВАХ ГРУППЫ, ПОРОЖДЁННОЙ XL-СЛОЯМИ[1]

Б. А. Погорелов, М. А. Пудовкина

Алгоритмы блочного шифрования реализуются итеративным применением более простых преобразований, которые должны обеспечивать свойства перемешивания, рассеивания и усложнения. Для получения данных свойств обычно используются слои преобразований трёх типов: наложение ключа (X-слой), преобразования над отдельными частями блока текста (слой s-боксов) и линейное преобразование (линейный слой, или L-слой). Блочные шифрсистемы с таким построением раундовых преобразований и побитным подмешиванием раундового ключа в каждом раунде называют XSL-сетями. Ряд линейных преобразований, используемых в линейном слое в алгоритмах шифрования и обеспечивающих хорошее рассеивание, являются приводимыми. Естественно, приводимыми являются и характеристические многочлены подстановочных матриц, используемых в SP-сетях. Это приводит к импримитивности подгруппы $C(g)$ аффинной группы $AGL_n(2)$, порождённой слоем наложения раундового ключа (т. е. всеми сдвигами) и приводимой невырожденной матрицей $g\in GL_n(2)$. В данной работе рассматриваются свойства графов орбиталов группы $C(g)$.

Пусть $\mathbb{N}$ — множество всех натуральных чисел; V_n — векторное пространство размерности n над GF(2); $X^\times = X\backslash\{0\}$; $\tilde{g}$ — матрица линейного преобразования g в стандартном базисе $\varepsilon_0,\dots,\varepsilon_{n-1}$, где $\varepsilon_i = (0,...,0,1,\underbrace{0,...,0}_{i})\in V_n$, $i\in\{0,\dots,n-1\}$; GL_n — полная линейная группа; $\chi_g(x)$ — характеристический многочлен линейного преобразования $g\in GL_n(2)$; $m_{\gamma,g}(x)$ — минимальный многочлен вектора $\gamma\in V_n^\times$ относительно преобразования g.

Напомним, что орбиталами группы G, действующей на множестве X, называются орбиты группы G при её действии на множестве X^2. Действие группы G на множестве X^2 задано как $(\alpha,\beta)^f=(\alpha^f,\beta^f)$ для всех $(\alpha,\beta)\in X^2$ и $f\in G$.

Лемма 1. Для произвольного преобразования $g\in GL_n$ и векторов $\alpha,\beta,\alpha',\beta'\in V_n$, $\alpha\neq\beta$, $\alpha'\neq\beta'$, тогда и только тогда $(\alpha',\beta')\in(\alpha,\beta)^{C(g)}$, когда $\alpha'\oplus\beta'\in(\alpha\oplus\beta)^{\langle g\rangle}$.

Таким образом, различными нетривиальными графами орбиталов группы $C(g)$ являются $\bar{\Gamma}_{(\mathbf{0},\gamma_1)}(g),\dots,\bar{\Gamma}_{(\mathbf{0},\gamma_{d-1})}(g)$, где $\gamma_1^{\langle g\rangle},\dots,\gamma_{d-1}^{\langle g\rangle}$ — попарно различные орбиты группы $\langle g\rangle$ на $V_n^\times$. Среди графов орбиталов группы $C(g)$ могут встречаться изоморфные.

Существует тесная связь между строением характеристического многочлена $\chi_g(x)$ преобразования g, примитивностью (2-транзитивностью) и связностью графов орбиталов группы $C(g)$. Так, группа $C(g)$ примитивна тогда и только тогда, когда много-

[1]Работа выполнена при поддержке гранта Президента РФ НШ №6260.2012.10е

член $\chi_g(x)$ неприводим. Кроме того, группа $C(g)$ 2-транзитивна тогда и только тогда, когда многочлен $\chi_g(x)$ примитивен.

Утверждение 1. Для произвольных вектора $\gamma \in V_n^{\times}$, преобразования $g \in GL_n$ с характеристическим многочленом $\chi_g(x)$ граф $\bar{\Gamma}_{(\mathbf{0},\gamma)}(g)$ связен для всех векторов $\gamma \in V_n^{\times}$ тогда и только тогда, когда характеристический многочлен $\chi_g(x)$ неприводим.

Утверждение 2. Для вектора $\gamma \in V_n^{\times}$ граф $\bar{\Gamma}_{(\mathbf{0},\gamma)}(g)$ связен тогда и только тогда, когда $m_{\gamma,g}(x) = \chi_g(x)$. Если группа $C(g)$ примитивна, то все её графы орбиталов изоморфны.

В алгебраической теории графов наибольший интерес представляют следующие классы графов: вершинно-транзитивные, рёберно-транзитивные, дистанционно-регулярные, дистанционно-транзитивные [1].

Утверждение 3. Пусть $n \geqslant 2$, $i \in \{1, \ldots, d-1\}$, $\bar{\Gamma}_{(\mathbf{0},\gamma_i)}(g)$ — нетривиальный связный граф диаметра $b \geqslant 2$. Тогда: а) $\bar{\Gamma}_{(\mathbf{0},\gamma_i)}(g)$ — рёберно-транзитивный граф; б) если $\gamma_i^{\langle g \rangle}$ является базисом V_n, то граф $\bar{\Gamma}_{(\mathbf{0},\gamma_i)}(g)$ является дистанционно-транзитивным и $\mathrm{Aut}\bar{\Gamma}_{(\mathbf{0},\gamma_i)}(g) \approx S_2 \uparrow S_n$.

Графом Хемминга на V_n будем называть граф с множеством вершин V_n и множеством рёбер $\{(\alpha,\beta) \in V_n^2 : \chi_n(\alpha,\beta) = 1\}$. Очевидно, что если граф изоморфен графу Хемминга, то его метрика изоморфна метрике Хемминга. Отметим, если множество $\gamma_i^{\langle g \rangle}$ является базисом V_n, то граф $\bar{\Gamma}_{(\mathbf{0},\gamma_i)}(g)$ изоморфен графу Хемминга и является дистанционно-регулярным.

Теорема 1. Пусть $n \geqslant 2$, преобразование $g \in GL_n$ и вектор $\gamma \in V_n$ такие, что

$$m_{\gamma,g}(x) = x^{r(q-1)} \oplus x^{r(q-2)} \oplus \ldots \oplus x^r \oplus 1 = \frac{(x^r)^q - 1}{x^r - 1},$$

где $rq = m = \left|\gamma^{\langle g \rangle}\right|$. Граф $\bar{\Gamma}_{(\mathbf{0},\gamma)}(g)$ дистанционно-регулярный тогда и только тогда, когда выполняется одно из условий: а) $r = 1$; б) $r \geqslant 2$ и $q = 3$.

ЛИТЕРАТУРА

1. *Godsil C. and Royle G.* Algebraic Graph Theory. Springer Verlag, 2001.

УДК 519.14

О БУЛЕВЫХ ФУНКЦИЯХ, ПОЧТИ УРАВНОВЕШЕННЫХ В ГРАНЯХ[1]

В. Н. Потапов

Обозначим через E^n множество упорядоченных двоичных наборов (вершин) длины n. Введём операцию $[x,y] = (x_1y_1, \ldots, x_ny_n)$ для наборов $x, y \in E^n$. Количество единиц в наборе $y \in E^n$ называется *весом набора* и обозначается через $\mathrm{wt}(y)$. Множество вершин чётного веса будем обозначать через E_0^n (нечётного — через E_1^n) . *Гранью размерности* $(n - \mathrm{wt}(y))$ называется множество $E_y^n(z) = \{x \in E^n : [x,y] = [z,y]\}$.

Пусть $S \subset E^n$; через χ^S будем обозначать характеристическую функцию множества S. Функция χ^S называется *корреляционно-иммунной порядка* $(n-m)$, если для любой грани $E_y^n(z)$ размерности m пересечения $E_y^n(z) \cap S$ имеют одинаковую мощность.

[1]Работа выполнена при поддержке РФФИ (проекты 11-01-997, 10-01-00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0362).

Через $\mathrm{cor}(S)$ будем обозначать максимальный порядок корреляционной иммунности, $\mathrm{cor}(S) = \max\{n-m\}$. Корреляционно-иммунная функция χ^S называется *уравновешенной*, если $|S| = 2^{n-1}$. Тогда множество S пересекается с гранями размерности m ровно по половине вершин, т. е. $|E_y^n(z) \cap S| = |E_y^n(z)|/2$. В [1] установлено, что неуравновешенная непостоянная булева функция χ^S удовлетворяет неравенству $\mathrm{cor}(S) \leqslant 2n/3-1$. Ясно, что непостоянная корреляционно-иммунная функция порядка $n-1$ является счётчиком чётности или нечётности ($\chi^{E_0^n}$ или $\chi^{E_1^n} = \chi^{E_0^n} \oplus 1$). Корреляционно-иммунные функции порядка $n-\mathrm{const}$ немногочисленны и описаны в [2]. Некоторые оценки числа корреляционно-иммунных функций меньших порядков имеются в [2–4].

Ниже рассматривается класс почти уравновешенных функций, содержащий значительное количество не эквивалентных булевых функций, максимально подобных корреляционно-иммунным функциям высокого порядка. Функцию χ^S будем называть *почти уравновешенной*, если для любой грани $E_y^n(z)$ любой размерности пересечение $E_y^n(z) \cap S$ отличается от половины мощности грани не более чем на 1, т. е. $-1 \leqslant |E_y^n(z) \cap S| - |E_y^n(z)|/2 \leqslant 1$.

В соответствии с определением класс почти уравновешенных функций является *наследственным*, т. е. все ретракты почти уравновешенных функций, полученные произвольной фиксацией произвольного набора переменных, являются почти уравновешенными. Одним из способов задания наследственного класса булевых функций является перечисление минимальных запретов. Булева функция g размерности k называется *минимальным запретом* для наследственного класса P, если $g \notin P$, но все её ретракты содержатся в P. Поскольку P — наследственный класс, функции из класса P не имеют ретрактов, совпадающих с запретом g.

Теорема 1. Множество почти уравновешенных булевых функций является наследственным классом с бесконечным набором минимальных запретов.

Будем обозначать через $P(n)$ множество функций от n аргументов из класса P. Пусть $f \in P(n)$, вершину $x \in E^n$ будем называть *свободной* относительно f, если найдётся функция $f' \in P(n)$, отличающаяся от f только на аргументе x.

Утверждение 1. Пусть P — наследственный класс и для некоторого m любая функция $f \in P(m)$ не имеет свободных вершин. Тогда $|P(n)| \leqslant 2^{\sum_{k=0}^{m-1} \binom{n}{k}}$.

Далее рассмотрим множество трёхзначных функций $f : E^n \to \{-1, 0, 1\}$, определённых на булевом кубе. Приведённые выше определения наследственного класса, минимального запрета и свободной вершины естественным образом распространяются на такие функции. Определим класс B трёхзначных уравновешенных функций следующим образом: $f \in B$, если для любой грани $\gamma = E_y^n(z)$ любой размерности сумма значений функции в ней не превышает по модулю единицы, т. е. $\sum\limits_{x \in \gamma} f(x) \in \{-1, 0, 1\}$. Через B_0 будем обозначать подкласс класса B, удовлетворяющий дополнительным условиям $f^{-1}(1) \subset E_0^n$ и $f^{-1}(-1) \subset E_1^n$. Ясно, что классы B и B_0 являются наследственными.

Утверждение 2. Булева функция f является почти уравновешенной тогда и только тогда, когда $f - \chi^{E_1^n} \in B_0$.

Преобразованием Мёбиуса функции $h : E^n \to \mathbb{R}$ называется функция

$$M[h] : E^n \to \mathbb{R}, \quad \text{где} \quad M[h](y) = (-1)^{\mathrm{wt}(y)} \sum_{\substack{x \in E^n, \\ [x,y]=x}} h(x).$$

Из формулы включения-исключения и определения классов B и B_0 получаем

Утверждение 3.

а) $M[M[h]] = h$ для любой функции $h : E^n \to \mathbb{R}$.

б) $M[B] = B$.

в) $M[f] \in B_0 \cup (-B_0)$, если и только если $f \in B$ и $\overline{0}$ — свободная вершина функции f.

Справедливость п. *в* следует из того, что вершина является свободной, только если во всех гранях, содержащих вершину, сумма значений функции имеет одинаковый знак.

В следующих утверждениях приведены несколько способов построения функций из классов B и B_0.

Утверждение 4.

а) Пусть $f \in B$ (или $f \in B_0$), тогда $f \cdot \chi^\gamma \in B$ (или $f \cdot \chi^\gamma \in B_0$) для любой грани γ.

б) Пусть $f \in B_0(n)$, тогда $(-1)^{\chi E_1^n} - f \in B_0(n)$.

в) Пусть γ_1, γ_2 — грани в E^n и $\gamma_1 \cap \gamma_2 \neq \varnothing$. Определим функцию f равенством $f(x_1, \ldots, x_n, x_{n+1}) = x_{n+1}\chi^{\gamma_1}(-1)^{\chi E_1^n} + (x_{n+1} \oplus 1)\chi^{\gamma_2}(-1)^{\chi E_0^n}$. Тогда $f \in B_0(n+1)$.

Утверждение 5.

а) Пусть $f \in B(n)$, $g \in B(m)$ и $F(x, y) = f(x)g(y)$. Тогда $F \in B(n+m)$.

б) Пусть $f \in B_0(n)$, $g \in B_0(m)$ и $F(x, y) = f(x)g(y)$. Тогда $F \in B_0(n+m)$.

Доказательства утверждений 4 и 5 легко получить непосредственной проверкой.

Булев n-мерный куб E^n естественным образом наделяется структурой векторного пространства над полем GF(2). Будем называть *носителем* вектора $x \in E^n$ множество позиций, на которых в векторе x находятся единицы. Рассмотрим набор векторов $z^1, \ldots, z^k$ с попарно не пересекающимися носителями. Пусть $V \subset E^n$ — подпространство, натянутое на векторы $z^1, \ldots, z^k$, $V = \{\bigoplus \alpha_i z^i : \alpha \in E^k\}$. Пусть $f : E^k \to \{-1, 0, 1\}$. Определим функцию $G_V[f] : E^n \to \{-1, 0, 1\}$ равенствами $G_V[f](x) = f(\alpha)$, если $x = \bigoplus \alpha_i z^i$, и $G_V[f](x) = 0$, если $x \notin V$.

Теорема 2.

а) Если $f \in B(k)$, то $G_V[f] \in B(n)$.

б) Класс $B(n)$ содержит не менее $e^{c\sqrt{n}}$, $c > 0$, неэквивалентных функций.

ЛИТЕРАТУРА

1. *Fon-Der-Flaass D. G.* A bound of correlation immunity // Siberian Electronic Mathematical Reports. 2007. V. 4. P. 133–135.
2. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 91–148.
3. *Воробьёв К. В., Фон-Дер-Флаасс Д. Г.* О совершенных 2-раскрасках гиперкуба // Сибирские электронные математические известия. 2010. Т. 7. С. 65–75.
4. *Потапов В. Н.* О совершенных раскрасках булева n-куба и корреляционно-иммунных функциях малой плотности // Сибирские электронные математические известия. 2010. Т. 7. С. 372–382.

УДК 519.7

СТРУКТУРНЫЕ СВОЙСТВА X, S-СЛОЁВ

М. А. Пудовкина

Блочные шифрсистемы, у которых раундовая функция является композицией трёх типов преобразований: наложения ключа (X-слой), преобразования над отдельными частями блока текста (S-слой) и линейного преобразования (L-слой), — называются XSL-сетями. В работе [1] для блочных шифрсистем XSL рассмотрены комбинаторные свойства группы, порождённой X, L-слоями. В данной работе рассматриваются свойства группы, порождённой X, S-слоями.

Пусть $\mathbb{R}$ — множество всех действительных чисел; $\mathbb{N}$ — множество всех натуральных чисел; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $S(X)$ — множество всех подстановок на множестве X; $X^\times = X \backslash \{0\}$; V_m — векторное пространство размерности m над GF(2); $\mathbb{R}^+ = \{a \in \mathbb{R} : a \geqslant 0\}$; $n, m, d \in \mathbb{N}$, $n = md$; $\mathrm{ord}(g)$ — порядок подстановки $g \in S(X)$; $s = (s_{d-1}, \ldots, s_0)$, $s_i \in S(X)$; $IG_W = (S_b \wr S_r, W)$ — группа сплетения в её импримитивном действии, где $W = \{W_1, \ldots, W_r\}$ — фиксированная система импримитивности с r блоками мощности b; $\mathbf{p}(g) = (p_{\varepsilon\delta}(g))$ — матрица разностей переходов подстановки $g \in S(X)$ на группе $(X, +)$. Для произвольного вектора $\alpha \in X$ зададим преобразование $h_\alpha : X \to X$ как $h_\alpha : \beta \to \beta + \alpha$, $H_n = \{h_\alpha : X \to X \,|\, \alpha \in X\}$. С матрицей $\mathbf{a} = (a_{ij})$ над $\mathbb{R}^+$ свяжем матрицу $\overline{\overline{\mathbf{a}}} = (\overline{\overline{a}}_{ij})$, у которой

$$\overline{\overline{a}}_{ij} = \begin{cases} 1, a_{ij} > 0, \\ 0, a_{ij} = 0. \end{cases}$$

Пусть X — регулярная абелева группа. Рассмотрим группы $C(s) = \langle s, h_\alpha : \alpha \in X^n \rangle$, $C(s_i) = \langle s_i, h_\alpha : \alpha \in X \rangle$, $i = 1, \ldots, d$. Очевидно, что $C(s) = C(s_1) \times \ldots \times C(s_d)$.

Зафиксируем произвольное число $i \in \{1, \ldots, d\}$.

Если $X = V_m$ и группа $C(s_i)$ импримитивна, то для произвольного вектора $\alpha \in V_m$ выполняется равенство $(W + \alpha)^s = W + \beta_\alpha$ для некоторых подпространства $W < V_m$ и вектора $\beta_\alpha \in V_m$. Из работы [2] следует, что в этом случае $C(s_i) = IG_W$ и подстановка s_i обладает фактор-структурой. Отсюда получаем, что если $s_i \notin IG_W$ для любого подпространства $W < V_m$, то группа $C(s_i)$ примитивна. Для числа $t \geqslant 2$ и множества X положим

$$X^{[t]} = \left\{(\alpha_{t-1}, \ldots, \alpha_0) \in X^t : \alpha_i \neq \alpha_j,\ i, j \in \{0, \ldots, t-1\},\ i \neq j\right\},$$
$$X^{\times[t]} = \left\{(\alpha_{t-1}, \ldots, \alpha_0) \in \left(X^\times\right)^t : \alpha_i \neq \alpha_j,\ i, j \in \{0, \ldots, t-1\},\ i \neq j\right\}.$$

Рассмотрим матрицу $\mathbf{p}^{(t)}(g) = \left(p^{(t)}_{\varepsilon\delta}(g)\right)$ разностей t-грамм переходов подстановки $g \in S(X)$ на группе $(X, +)$, где

$$p^{(t)}_{\varepsilon\delta}(g) = |X|^{-1} \left|\{\alpha \in X : (\alpha + \varepsilon_i)^g = \alpha^g + \delta_i,\ i = 0, \ldots, t-1\}\right|,$$

$\varepsilon = (\varepsilon_{t-1}, \ldots, \varepsilon_0) \in X^{\times[t]}$, $\delta = (\delta_{t-1}, \ldots, \delta_0) \in X^{\times[t]}$. Положим $\mathbf{p}(g) = \mathbf{p}^{(1)}(g)$.

Лемма 1. Для произвольных подстановки $g \in S(X)$ и числа $t \in \mathbb{N}$ справедливы следующие равенства:

1) $\overline{\overline{\mathbf{p}^{(t)}(g^i)}} = \overline{\overline{(\mathbf{p}^{(t)}(g))^i}}$ для $i \in \mathbb{N}$;
2) для произвольных фиксированных чисел $j_1, \ldots, j_c \in \mathbb{N}_0$ и наборов $(\theta_{t-1}, \ldots, \theta_0) \in \in X^{[t]}$, $(\gamma_{t-1}, \ldots, \gamma_0) \in X^{[t]}$ существуют элементы $\beta_1, \ldots, \beta_c \in X$, одновременно

удовлетворяющие равенствам

$$(\dots((\theta_i+\beta_1)^{g^{j_1}}+\beta_2-\beta_1^{g^{j_1}})^{g^{j_2}}+\beta_3-\beta_2^{g^{j_2}})^{g^{j_3}}\dots+\beta_{c-1}-\beta_c^{g^{j_{c-1}}})^{g^{j_c}}-(\beta_c)^{g^{j_c}}=\gamma_i,$$

$i=0,\dots,t-1$, тогда и только тогда, когда $\overline{\overline{p^{(t)}_{\theta,\gamma}(g^{j_1+\dots+j_c})}}>0$.

Назовём матрицу $\mathbf{p}$ положительной, если все её элементы больше нуля. В этом случае будем использовать запись $\mathbf{p}>0$. (Матрица $\mathbf{p}$ называется эргодической, если $\mathbf{p}^q>0$ для некоторого числа $q\in\mathbb{N}$.)

Утверждение 1.

1) Пусть g — произвольная подстановка из $S(X)$, $l=\mathrm{ord}(g)$, $t\in\mathbb{N}$, $t\geqslant 2$. Группа $C(g)$ является t-транзитивной тогда и только тогда, когда $\sum\limits_{i=1}^{l}\left(\mathbf{p}^{(t-1)}(g)\right)^i>0$.
2) Пусть $\left(\mathbf{p}^{(t-1)}(g)\right)^b>0$ для некоторого числа $b\in\mathbb{N}$. Тогда для любых векторов $\delta,\delta'\in X^{[t]}$ существует элемент $h_{\beta_1}g\dots h_{\beta_b}gh_{\beta_{b+1}}\in C(g)$, $\beta_1,\dots,\beta_{b+1}\in X$, удовлетворяющий равенству $(\delta)h_{\beta_1}g\dots h_{\beta_b}gh_{\beta_{b+1}}=\delta'$.

Следствие 1. Если $t\in\mathbb{N}$, $t\geqslant 2$ и матрица $\mathbf{p}^{(t-1)}(g)$ эргодическая, то группа $C(g)$ t-транзитивна.

Приведём пример того, что группа $C(g)$ может быть 2-транзитивной, но матрица $\mathbf{p}(g)$ не являться эргодической. Пусть g — линейное преобразование с примитивным характеристическим многочленом. Тогда $\mathbf{p}(g)$ — подстановочная матрица порядка 2^m-1. Очевидно, что матрица $\mathbf{p}(g)$ не является эргодической, но матрица $\sum\limits_{j=1}^{2^m-1}\overline{\overline{\mathbf{p}(g^j)}}$ положительная.

Рассмотрим классы подстановок с одинаковыми матрицами $\mathbf{p}^{(t)}(g)$. Для подстановки $g\in S(X)$ и $t\in\mathbb{N}$ положим $\mathrm{P}^{(t)}(g)=\left\{s\in S(X):\mathbf{p}^{(t)}(g)=\mathbf{p}^{(t)}(s)\right\}$. Ясно, что для любых подстановок $g_1,g_2\in S(X)$ справедливо соотношение

$$\mathrm{P}^{(t)}(g_1)\cap\mathrm{P}^{(t)}(g_2)\in\left\{\varnothing,\mathrm{P}^{(t)}(g_1)\right\}.$$

Подстановке $g\in S(X)$ и векторам $\delta,\lambda\in X$ поставим в соответствие такое преобразование $g_{(\delta,\lambda)}:X\to X$, что $(\alpha)g_{(\delta,\lambda)}=(\alpha+\delta)^g+\lambda$. Очевидно, что $g_{(\delta,\lambda)}$ — подстановка на множестве X. Множество всех таких подстановок обозначим как $AP(g)$.

Для $t\in\mathbb{N}$, $\delta\in X^{\times[t]}$, $i\in\{0,\dots,t\}$ положим

$$B_{t,i}(\delta)=\left\{(\theta_t,\dots,\theta_0)\in X^{\times[t+1]}:(\theta_t,\dots,\theta_{i+1},\theta_{i-1},\dots,\theta_0)=\delta\right\},$$
$$U_t(\delta)=\left\{\left(\delta_{(t-1)^b},\dots,\delta_{0^b}\right):b\in S_t\right\}.$$

Лемма 2. Для любых $g\in S(X)$, $t\in\mathbb{N}$ справедливы такие соотношения:

1) $p^{(t)}_{\varepsilon\delta}(g)=p^{(t)}_{\lambda\theta}(g)$ для элементов $\varepsilon,\delta\in X^{\times[t]}$, $\lambda\in U_t(\varepsilon)$, $\theta\in U_t(\delta)$;
2) $p^{(t)}_{\varepsilon\delta}(g)=\sum\limits_{i=0}^{t}\sum\limits_{\lambda\in B_{t,i}(\varepsilon)}\sum\limits_{\theta\in B_{t,i}(\delta)}p^{(t+1)}_{\lambda\theta}(g)$ для элементов $\varepsilon,\delta\in X^{\times[t]}$;
3) $AP(g)\subseteq\mathrm{P}^{(t)}(g)$;
4) $\mathrm{P}^{(1)}(g)\supseteq\mathrm{P}^{(2)}(g)\supseteq\dots\supseteq\mathrm{P}^{(t)}(g)$;
5) $p^{(t)}_{\varepsilon\delta}(g)=0$, если $p^{(t+1)}_{\lambda\theta}(g)=0$ для всех $\lambda\in B_{t,i}(\varepsilon)$, $\theta\in B_{t,i}(\delta)$, $i=0,\dots,t$.

Утверждение 2. Для $a_1,a_2\in GL(X)$, $g\in S(X)$, $t\in\mathbb{N}$ тогда и только тогда $a_1ga_2^{-1}\in\mathrm{P}^{(t)}(g)$, когда $p^{(t)}_{\varepsilon\delta}(a_1ga_2^{-1})=p^{(t)}_{\varepsilon^{a_1}\delta^{a_2}}(g)$ для любых $\varepsilon,\delta\in X^{\times[t+1]}$.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О комбинаторных свойствах группы, порождённой X, L-слоями // Прикладная дискретная математика. Приложение. 2012. № 5. С. 22–23.
2. *Пудовкина М. А.* Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. 2008. № 1. С. 25–28.

УДК 519.7

СОВЕРШЕННАЯ УРАВНОВЕШЕННОСТЬ ДИСКРЕТНЫХ ФУНКЦИЙ И УСЛОВИЕ ГОЛИЧА

С. В. Смышляев

Для всяких $n \geqslant 1$, $k \geqslant 2$ через E_k будем обозначать множество $\{0, 1, \ldots, k-1\}$, через $\mathrm{P}_k^{(n)}$ — множество k-значных функций n переменных $f\colon \mathrm{E}_k^n \to \mathrm{E}_k$; $\mathrm{P}_k = \bigcup\limits_{n=0}^{\infty} \mathrm{P}_k^{(n)}$. Для всякого натурального l и всякой функции $f \in \mathrm{P}_k^{(n)}$ будем рассматривать отображение $f_l\colon \mathrm{E}_k^{l+n-1} \to \mathrm{E}_k^l$, $f_l(x_1, x_2, \ldots, x_{l+n-1}) = (f(x_1, \ldots, x_n), \ldots, f(x_l, \ldots, x_{l+n-1}))$.

Определение 1. Функция $f \in \mathrm{P}_k^{(n)}$ называется совершенно уравновешенной (обозначение $f \in \mathcal{PB}_k^{(n)}$), если для всякого натурального l и всякого $y \in \mathrm{E}_k^l$ верно равенство $\left|f_l^{-1}(y)\right| = k^{n-1}$.

Определение 2. Функция $f \in \mathrm{P}_k^{(n)}$ имеет правый барьер длины $b \geqslant 1$, если из равенства $f_b(x_1, x_2, \ldots, x_{n-1}, x'_n, \ldots, x'_{b+n-1}) = f_b(x_1, x_2, \ldots, x_{n-1}, x''_n, \ldots, x''_{b+n-1})$ следует $x'_n = x''_n$.

Абсолютно аналогично случаю $k = 2$ (см. [1]) для произвольного $k \geqslant 2$ доказывается, что наличие барьера влечет совершенную уравновешенность в P_k.

Й. Голичем в работе [2] в 1996 г. рассмотрен (при $k = 2$) вопрос о важном для используемых в фильтрующих генераторах функций свойстве, являющемся естественным усилением свойства совершенной уравновешенности.

Определение 3. Функция $f \in \mathcal{PB}_k^{(n)}$ называется сильно совершенно уравновешенной, если при добавлении любого числа фиктивных переменных между существенными она сохраняет совершенную уравновешенность.

Нетрудно показать, что перестановочность дискретной функции по первой или последней существенной переменной влечет за собой сильную совершенную уравновешенность. Голич в работе [2] предположил, что верно и обратное; данная гипотеза позже, начиная с работы М. Дихтла [3], стала называться гипотезой Голича.

Гипотеза 1 [2]. При $k = 2$ из сильной совершенной уравновешенности некоторой k-значной функции следует её перестановочность (т. е. линейность) по первой или последней существенной переменной.

Косвенное подтверждение справедливости гипотезы Голича было впервые получено в [1] (2008 г.). В работе [4] (2012 г.) гипотеза Голича полностью доказана. Таким образом, известно, что невозможно построить кодирующее устройство на основе регистра сдвига и фильтрующей функции (над алфавитом $\{0, 1\}$), обеспечивающее сохранение истинной случайности битовой последовательности при любом выборе точек входа (см. [2]). Интересен вопрос о возможности построения таких кодирующих

устройств над алфавитом большей мощности — в особенности в случае алфавита мощности $k = 2^m$, $m \geqslant 2$, т. е. в случае рассмотрения кодирующих устройств, преобразующих входную битовую последовательность блоками длины m.

Условие Голича. Сильная совершенная уравновешенность в P_k эквивалентна перестановочности по первой или последней существенной переменной.

Из результатов работ [2, 4] следует, что условие Голича выполнено в P_2. Настоящая работа посвящена рассмотрению следующего обобщения гипотезы Голича, связывающего справедливость условия Голича в P_k с простотой числа k.

Гипотеза 2. Условие Голича выполнено в P_k тогда и только тогда, когда k — простое.

Теорема 1. Для всякого составного k существует функция $f \in \mathcal{PB}_k^{(2)}$, существенно зависящая от обеих переменных и не перестановочная ни по одной из них.

Следствие 1. Если k — составное, то условие Голича не выполнено в P_k.

Теорема 2. Для всякого составного k существует функция $f \in \mathrm{P}_k$ с правым барьером длины 2, существенно зависящая от последней переменной и не перестановочная по ней.

Теорема 3. Для всякого составного k и всякого $n \geqslant 2$ существует сильно совершенно уравновешенная функция $f \in \mathrm{P}_k^{(n)}$, существенно зависящая от всех n переменных, которая не является перестановочной ни по первой, ни по последней переменной, но является сильно совершенно уравновешенной.

Теорема 4. Пусть k — простое и функция $f \in \mathrm{P}_k^{(n)}$ имеет правый барьер длины 2. Тогда f не зависит существенно от последней переменной и перестановочна по предпоследней.

Следствие 2. При простом k условие Голича не нарушается на функциях с барьером длины 2.

Следствие 3. Условие Голича не нарушается на функциях с барьером длины 2 в P_k тогда и только тогда, когда k — простое.

Теорема 5. При $k \in \{2, 3, 5, 7\}$ все совершенно уравновешенные функции из $\mathrm{P}_k^{(2)}$ перестановочны по первой или последней переменной.

Следствие 4. При $k \in \{2, 3, 5, 7\}$ условие Голича не нарушается на функциях из $\mathrm{P}_k^{(2)}$.

Таким образом, гипотеза 2 полностью доказана в части необходимости k быть простым для выполнения условия Голича в P_k. Кроме того, доказан ряд утверждений, косвенно подтверждающих справедливость гипотезы 2 в части достаточности.

ЛИТЕРАТУРА

1. *Logachev O. A., Salnikov A. A., Smyshlyaev S. V., and Yashchenko V. V.* Perfectly Balanced Functions in Symbolic Dynamics // Proc. NATO ARW, Veliko Tarnovo, Bulgaria, 6–9 October 2008. P. 222–233.
2. *Golić J. Dj.* On the Security of Nonlinear Filter Generators // LNCS. 1996. V. 1039. P. 173–188.
3. *Dichtl M.* On nonlinear filter generators // LNCS. 1997. V. 1267. P. 103–106.

4. *Smyshlyaev S. V.* Perfectly Balanced Boolean Functions and Golić Conjecture // J. Cryptology. 2012. No. 25(3). P. 464–483.

УДК 519.7

О РАЗЛОЖЕНИИ БУЛЕВОЙ ФУНКЦИИ В СУММУ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Булева функция от чётного числа переменных, максимально удалённая от класса всех аффинных функций, называется *бент-функцией*. В работах [1, 2] исследована связь между вопросом о числе бент-функций и проблемой разложения произвольной булевой функции в сумму двух бент-функций. Была представлена серия гипотез, одна из которых заключается в том, что каждую булеву функцию от n переменных степени не больше $n/2$ можно представить в виде суммы двух бент-функций от n переменных. В [2] с помощью компьютера гипотеза проверена для малых значений $n \leqslant 6$.

В 2011 г. Л. Ку и С. Ли [3] разобрали случай малых n аналитически. В общем случае они доказали, что в виде суммы двух бент-функций может быть представлена любая квадратичная булева функция, любая бент-функция Мак-Фарланда, любая функция частичного расщепления (*partial spread function*).

В данной работе доказан ослабленный вариант гипотезы.

Теорема 1. Любая булева функция от n переменных степени d, где $d \leqslant n/2$, n чётно, может быть представлена в виде суммы не более чем $2\binom{2b}{b}$ бент-функций от n переменных, где b — наименьшее число, $b \geqslant d$, такое, что n делится на $2b$.

Заметим, что разложение, указанное в теореме, можно провести с помощью только бент-функций Мак-Фарланда.

ЛИТЕРАТУРА

1. *Токарева Н. Н.* Гипотезы о числе бент-функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 21–23.
2. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. in Mathematics of Communications (AMC). 2011. V. 5. No. 4. P. 609–621.
3. *Qu L. and Li C.* Representing a Boolean function as the sum of two Bent functions // Discrete Applied Mathematics. 2012 (to appear).

УДК 681.03

ЛАТИНСКИЕ КВАДРАТЫ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

М. Э. Тужилин

Подсчёт числа латинских квадратов порядка n — сложная комбинаторная задача, их точное число известно только для n от 1 до 11 [1].

Латинские квадраты находят применение в комбинаторике, алгебре (изучение латинских квадратов тесно связано с изучением квазигрупп), теории кодов, статистике и многих других областях [2].

[1]Исследование выполнено при поддержке РФФИ (проекты 10-01-00424, 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 г. (гос. контракт 02.740.11.0429).

Впервые в криптографии латинский квадрат был применён в шифре И. Тритемия [3]. Значение латинских квадратов для криптографии иллюстрирует теорема Шеннона, в соответствии с которой единственными совершенными шифрами являются шифры гаммирования, наложение гаммы в которых определяется латинским квадратом [4]. Попытка обобщить подход Шеннона и ввести понятие «сильно совершенный шифр» предпринята в [5].

Краткий обзор результатов по применению латинских квадратов для построения схем аутентификации, шифрования и однонаправленных функций содержится в [6].

В ряду примеров применения латинских квадратов для построения поточных шифров необходимо выделить предложенный в 2005 г. шифр Edon80 [7], который дошёл до третьего тура конкурса ESTREAM. Разработчики шифра из 576 существующих латинских квадратов 4-го порядка тщательно выбрали 4, на основе которых в криптосхеме строится конвейер из 80 латинских квадратов, он используется для выработки гаммы.

При разработке блочного шифра IDEA [8] авторы использовали три квазигруппы, соответствующие операциям сложения по модулю 2, сложения по модулю 2^{16} и умножения по модулю $2^{16}+1$. При этом высокие криптографические свойства шифра они обосновали существованием единственной изотопии между двумя из используемых квазигрупп.

Латинские квадраты являются привлекательным средством для построения схем разделения секрета. Секретом является латинский квадрат, а все участники схемы получают его частично заполненным (он называется частичным). Задача распознавания того, может ли частичный квадрат быть однозначно дополнен до латинского, NP-полна. Наряду с большим количеством латинских квадратов это обстоятельство и определяет стойкость схемы [9]. Предложенная схема может быть усовершенствована [10]. В свою очередь, на основе таких схем разделения секрета можно строить и криптографические хеш-функции [11]. Другой пример построения криптографической хеш-функции на основе случайного латинского квадрата приведён в [12].

Разработанное в 2008 г. для участия в конкурсе SHA-3 на новый американский стандарт хеш-функции семейство Edon-R [13] не прошло во второй тур, но интересно тем, что в основе конструкции лежит построение и использование некоммутативной неассоциативной нелинейной квазигруппы.

В [14] предложен протокол с нулевым разглашением. Каждый участник имеет открытый ключ, которым являются два эквивалентных латинских квадрата. Секретным ключом является изотопия между ними.

В заключение отметим, что о растущем внимании к теме свидетельствует появление обзоров [6, 15].

ЛИТЕРАТУРА

1. *McKay B. D. and Wanless I. M.* On the number of Latin Squares // Ann. Combin. 2005. No. 9. P. 335–344.
2. *Laywine C. F. and Mullen G. L.* Discrete mathematics using Latin squares. New York: Wiley, 1998.
3. *Trithemius J.* Polygraphiae. 1518.
4. *Shannon C.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. No. 15(2). P. 125–156.
5. *Massey J. L., Maurer U., and Wang M.* Non-Expanding, Key-Minimal, Robustly-Perfect, Linear and Bilinear Ciphers // Adv. Cryptology — EUROCRYPT'87. Berlin, Heidelberg: Springer Verlag, 1988. P. 237–247.

6. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.
7. *Gligoroski D., Markovski S., Kocarev L., and Gusev M.* Edon80 // `http://www.ecrypt.eu.org/stream/edon80p3.html`
8. *Lai X. and Massey J.* A Proposal for a New Block Encryption Standard // Adv. Cryptology — EUROCRYPT'90. New York: Springer Verlag, 1991. P. 55–70.
9. *Cooper J., Donovan D., and Seberry J.* Secret Sharing Schemes Arising From Latin Squares // Bulletin of the ICA. 1994. V. 12. P. 33–43.
10. *Chum C. S. and Zhang X.* The Latin squares and the secret sharing schemes // Groups Complex. Cryptol. 2010. V. 2. P. 175–202.
11. *Chum C. S.* Hash functions, Latin squares and secret sharing schemes. New York: ProQuest, 2010.
12. *Pal S. K., Bhardwaj D., Kumar R., and Bhatia V.* A New Cryptographic Hash Function based on Latin Squares and Non-linear Transformations // Adv. Comput. Conf. IACC, 2009. P. 862–867.
13. *Gligoroski D., Ødegård R. S., Mihova M., et al.* Cryptographic Hash Function Edon-R // Proc. IWSCN, 2009. P. 1–9.
14. *Dènes J. and Dènes T.* Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack // Quasigroups and Related Systems. 2001. No. 8. P. 7–14.
15. *Shcherbacov V. A.* Quasigroups in cryptology // Comput. Sci. J. Moldova. 2009. V. 17. No. 2(50). P. 193–228.

УДК 519.7

СВОЙСТВО КРАТНЫХ ПРОИЗВОДНЫХ БЕНТ-ФУНКЦИЙ КАСАМИ[1]

А. А. Фролова

Одно из криптографических свойств булевой функции — это высокая нелинейность. Булевы функции, обладающие экстремальной нелинейностью, при чётном числе переменных называются *бент-функциями*. Описание класса всех бент-функций от произвольного числа переменных остается открытой проблемой, однако известны некоторые конструкции бент-функций [1]. Одна из них — алгебраическая конструкция Касами. Булева функция от n переменных рассматривается как функция над конечным полем $\mathrm{GF}(2^n)$. Любая булева функция f от n переменных может быть представлена с помощью функции *следа* $\mathrm{tr}(\beta) : \mathrm{GF}(2^n) \to \mathrm{GF}(2)$ следующим образом (см. подробнее [2]):

$$f(\beta) = \mathrm{tr}(\sum_{j=0}^{2^n-1} a_j \beta^j), \text{ где } a_j \in \mathrm{GF}(2^n), \text{ а } \mathrm{tr}(\beta) = \sum_{i=0}^{n-1} \beta^{2^i} \text{ для любого } \beta \in \mathrm{GF}(2^n).$$

Определение 1. Булева функция от n переменных (n чётное) вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ называется *булевой функцией Касами*, если выполнено условие

1) $k = 2^{2d} - 2^d + 1$, где $(n, d) = 1,\ 0 < d < n$.

Если к тому же выполнено условие

2) λ не принадлежит множеству $\{\gamma^3 : \gamma \in \mathrm{GF}(2^n)\}$,

то f является бент-функцией и называется *бент-функцией Касами*.

[1]Исследование выполнено при поддержке гранта РФФИ, проект № 11-01-00997.

В работе [3] показано, что при выполнении условия 2 функция Касами является бент, однако впервые (при ограничении, что число переменных n не делится на три) это доказано в работе Дж. Диллона и Х. Доббертина в 2004 г. [4]. Бент-функции Касами являются наиболее сложными из мономиальных конструкций (т. е. конструкций вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$). Степень функции Касами от n переменных может принимать все возможные чётные значения вплоть до $n/2$ (заметим, что максимальная степень бент-функции от n переменных равна $n/2$). Известно, что они не аффинно эквивалентны своим дуальным функциям и бент-функциям из классов PS и Майорана — МакФарланда. Кроме того, известно, что в классе бент-функций Касами существуют функции, не являющиеся нормальными, т. е. тождественно равными константе на некотором аффинном подпространстве размерности $n/2$.

Однако до сих пор не известна связь между алгебраическим и комбинаторным представлениями бент-функций. В данной работе исследуются комбинаторные свойства бент-функций Касами. Получен результат о кратных производных функций Касами, следствием которого является свойство зависимости алгебраической нормальной формы (АНФ) функции от произведений переменных.

Будем рассматривать конечное поле $\mathrm{GF}(2^n)$ как векторное пространство размерности n.

Определение 2. *Производная по направлению* $a \in \mathrm{GF}(2^n)$ булевой функции f определяется как $D_a f(\beta) = f(\beta) + f(\beta + a)$ для любого $\beta \in \mathrm{GF}(2^n)$.

Авторами [5] исследована вторая производная бент-функций Касами и доказана теорема о том, что для любых ненулевых различных направлений $a, b \in \mathrm{GF}(2^n)$ производная $D_a D_b f$ бент-функции Касами не равна тождественно нулю при степени функции $\deg(f) \geqslant 4$ и числе переменных $n \geqslant 8$.

В данной работе доказана следующая

Теорема 1. Пусть $f(\beta)$ — булева функция Касами от n переменных вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $k = 2^{2d} - 2^d + 1$, $0 < d < n$, n чётное. Тогда для любого $n \geqslant 8$ справедливы следующие утверждения:

(i) при $\deg(f) = t$, где $4 \leqslant t \leqslant n/2$, производная $D_{a_1} \dots D_{a_{t-3}} f(\beta)$ не равна тождественно нулю для любых линейно независимых векторов $a_1, \dots, a_{t-3} \in \mathrm{GF}(2^n)$;

(ii) при $\deg(f) = t$, где $4 \leqslant t \leqslant (n+3)/3$, производная $D_{a_1} \dots D_{a_{t-2}} f(\beta)$ не равна тождественно нулю для любых линейно независимых векторов $a_1, \dots, a_{t-2} \in \mathrm{GF}(2^n)$.

Вводится следующее понятие.

Определение 3. Булева функция называется *k-существенно зависимой*, если для любого произведения из k различных переменных существует моном в АНФ функции, содержащий это произведение.

Заметим, что булева функция f является k-существенно зависимой, если для любых различных векторов $a_1, \dots, a_k \in \mathrm{GF}(2^n)$ вида $a_i = (0, \dots, 0, 1, 0, \dots, 0)$, содержащих 1 в координате s_i, где $0 \leqslant s_i \leqslant (n-1)$, $1 \leqslant i \leqslant k$, кратная производная $D_{a_1} \dots D_{a_k} f(\beta)$ не равна тождественно нулю.

Следствием результата в [5] и теоремы 1 является следующая

Теорема 2. Пусть $f(\beta)$ — булева функция Касами от n переменных вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $k = 2^{2d} - 2^d + 1$, $0 < d < n$, n чётное. Тогда для любого $n \geqslant 8$ справедливы следующие утверждения:

(i) при $\deg(f) \geqslant 4$ функция f является 2-существенно зависимой;

(ii) при $\deg(f) = t$, где $4 \leqslant t \leqslant n/2$, функция f является $(t-3)$-существенно зависимой;

(iii) при $\deg(f) = t$, где $4 \leqslant t \leqslant (n+3)/3$, функция f является $(t-2)$-существенно зависимой.

Заметим, что если функция обладает свойством k-существенной зависимости, то она также является l-существенной зависимой для всех $l < k$. В силу этого интересен вопрос о максимально возможном k, для которого функция является k-существенно зависимой. По результатам непосредственного исследования функций Касами от малого числа переменных (до 14) и теоремы 2 сформулирована следующая

Гипотеза 1. Функция Касами степени t при числе переменных $n \geqslant 8$, где $t \leqslant n/2$, обладает свойством $(t-2)$-существенной зависимости, но не обладает свойством $(t-1)$-существенной зависимости.

Нетрудно заметить, что для доказательства гипотезы остаётся рассмотреть один случай, т. е. доказать, что при $(n+3)/3 \leqslant t \leqslant n/2$ функция является $(t-2)$-существенно зависимой.

ЛИТЕРАТУРА

1. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения // Saarbrucken, Germany: LAP LAMBERT Academic Publishing, 2011.
2. *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // Chapter of the monograph "Boolean Methods and Models", Cambridge Univ. Press / eds. P. Hammer and Y. Crama, to appear. `www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`.
3. *Langevin P. and Leander G.* Monomial Bent Function and Stickelberger's Theorem // Finite Fields and Their Applications. 2008. V. 14. P. 727–742.
4. *Dillon J. F. and Dobbertin H.* New cyclic difference sets with Singer parameters // Finite Fields and Their Applications. 2004. V. 10. P. 342–389.
5. *Sharma D. and Gangopadhyay S.* On Kasami Bent Function // Cryptology ePrint Archive, Report 2008/426. `http://eprint.iacr.org`

УДК 519.816

ДЕКОМПОЗИЦИЯ И АППРОКСИМАЦИЯ НЕДООПРЕДЕЛЁННЫХ ДАННЫХ[1]

Л. А. Шоломов

Задан алфавит $A_0=\{a_0, a_1, \ldots, a_{m-1}\}$ *основных символов*. Пусть $M=\{0, 1, \ldots, m-1\}$ и каждому непустому $T \subseteq M$ сопоставлен символ a_T. Символы алфавита $A = \{a_T : T \subseteq M\}$ называются *недоопределёнными*, и *доопределением* символа $a_T \in A$ считается всякий основной символ a_i, $i \in T$. Символ a_M, доопределимый любым основным символом, называется *неопределённым* и обозначается $*$.

Источник X, порождающий символы $a_T \in A$ независимо с вероятностями p_T, называется *недоопределённым источником*, а величина

$$\mathcal{H}(X) = \min_Q \Big\{ - \sum_{T \subseteq M} p_T \log \sum_{i \in T} q_i \Big\},$$

[1]Работа выполнена при поддержке ОНИТ РАН по проекту 1.1 программы «Интеллектуальные информационные технологии, системный анализ и автоматизация».

где $\log x = \log_2 x$, минимум берется по наборам $Q = (q_i,\ i \in M)$, $q_i \geqslant 0$, $\sum\limits_{i \in M} q_i = 1$, называется его *энтропией*. Для недоопределённых данных эта величина играет роль энтропии Шеннона [1].

Источники X и Y будем называть *равносильными* и записывать $X \approx Y$, если для любого источника Z выполнено $\mathcal{H}(XZ) = \mathcal{H}(YZ)$. Будем говорить, что источник X *не слабее* Y (Y *не сильнее* X), и записывать $X \succsim Y$, если $XY \approx X$. Можно показать, что $X \approx Y$ тогда и только тогда, когда $X \succsim Y$ и $X \precsim Y$. Существуют эффективные (т. е. полиномиальные) алгоритмы проверки соотношений $X \approx Y$ и $X \succsim Y$. Преобразования и отношения на множестве недоопределённых источников рассмотрены в [2].

Под алфавитом A источника X будем понимать множество символов a_T, для которых $p_T > 0$. Зададимся натуральным числом s и заменим в источнике X каждый символ $a_T \in A$ некоторым набором $\tilde{a}_T \in \{0, 1, *\}^s$. Полученный источник $\tilde{X}$ будем рассматривать как произведение $X_1 \cdot \ldots \cdot X_s$ источников, порождающих символы 0, 1 и $*$, и будем называть *разложением* (соответствующим источнику X).

Разложение $\tilde{X}$ назовем *декомпозицией* источника X, если $\tilde{X} \approx X$. Разложение $\tilde{X}$ назовем *аппроксимацией* (нижней) источника X, если $\tilde{X} \precsim X$ и для всякого разложения $\tilde{X}'$, такого, что $\tilde{X}' \precsim X$, выполнено $\tilde{X} \succsim \tilde{X}'$. Очевидно, что если аппроксимация существует, она единственна с точностью до равносильности, и если декомпозиция существует, аппроксимация является декомпозицией.

Теорема 1. Для всякого недоопределённого источника аппроксимация существует и может быть эффективно построена.

Источник X_i, $i = 1, \ldots, s$, назовем *устранимым* из разложения $X_1 \cdot \ldots \cdot X_s$, если

$$X_1 \cdot \ldots \cdot X_s \approx X_1 \cdot \ldots \cdot X_{i-1} X_{i+1} \cdot \ldots \cdot X_s.$$

Теорема 2. Существует эффективный алгоритм проверки устранимости источника из разложения.

Используя его, можно путём последовательного удаления устранимых источников эффективно построить *неизбыточную* аппроксимацию (в частности, декомпозицию), из которой нельзя удалить ни одного источника без потери свойства быть аппроксимацией. Обобщением теоремы 2 является следующий факт.

Теорема 3. Существует эффективный алгоритм проверки равносильности двух различных разложений.

Эта теорема позволяет сравнивать заданные разложения, но не даёт возможности их порождать. Для порождения может быть использована система преобразований, гарантируемая следующей теоремой.

Теорема 4. Существует (явно описана) полная система равносильных преобразований, позволяющая по всякому разложению построить любое равносильное ему разложение.

Введём еще один вид декомпозиции. Рассмотрим разложение $\tilde{X} = X_1 \cdot \ldots \cdot X_s$, построенное по источнику X. Пусть, как и раньше, $\tilde{a}_T \in \{0, 1, *\}^s$ означает набор, соответствующий символу $a_T \in A$, и пусть каждому символу $a_i \in A_0$ приписан набор $\tilde{a}_i \in \{0, 1\}^s$. *Наборы* множества $\tilde{A}_0 = \{\tilde{a}_i : i \in M\}$ будем называть *основными*. Обозначим через $\{\tilde{a}_T\}$ множество доопределений набора $\tilde{a}_T$ и будем считать, что разложение $\tilde{X}$ порождает (с вероятностями $p_T > 0$) множества $\{\tilde{a}_T\}$. *Ограничением разложения* $\tilde{X}$ *на множество основных наборов* назовем источник $\tilde{X}_{\tilde{A}_0}$, который порождает

(с вероятностями p_T) множества $\{\tilde{a}_T\} \cap \tilde{A}_0$. Скажем, что разложение $\tilde{X}$ образует *декомпозицию источника X на множестве основных наборов*, если $\tilde{X}_{\tilde{A}_0}$ изоморфно X. Это означает, что $\{\tilde{a}_T\} \cap \tilde{A}_0 = \{\tilde{a}_i : i \in T\}$.

Теорема 5. Для всякого недоопределённого источника существует и может быть эффективно построена декомпозиция на множестве основных наборов.

Число s источников в этой декомпозиции не превосходит $\min(|A|, |A_0|)$, где $|\cdot|$ означает мощность множества, и эта оценка по порядку неулучшаема.

ЛИТЕРАТУРА

1. *Шоломов Л. А.* Элементы теории недоопределённой информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.
2. *Шоломов Л. А.* Преобразование нечетких данных с сохранением информационных свойств // Дискрет. анализ и исслед. опер. Сер. 1. 2005. Т. 12. № 3. С. 85–104.