$g : \text{GF}(2^k) \rightarrow \text{GF}(2)$ — уравновешенная функция от k переменных и $g(0) = 0$. Тогда функция $f(x, y) = g(x \cdot y^{2^k-2})$ является бент-функцией от $2k$ переменных.

В данной работе исследуется алгебраическая иммунность некоторых бент-функций Диллона. В качестве уравновешенных рассматриваются линейные функции, как самые простые. Доказана

Теорема 1. Пусть функция $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$ линейна, $g \neq \text{const}$ и f построена с помощью конструкции Диллона по функции g , а именно $f(x, y) = g(x \cdot y^{2^k-2})$. Тогда $\text{AI}(f) \leq \lceil k/2 \rceil + 1$. При $k = 2, \dots, 8$ оценка достигается.

Из теоремы заключаем, что алгебраическая иммунность бент-функций Диллона, построенных с помощью линейных булевых функций, отличается от максимально возможной почти в 2 раза.

В конструкции Диллона свойства бент-функции f зависят от выбора g . Возникает ряд вопросов — существуют ли такие g , чтобы $\text{AI}(f)$ была максимальной, а если существуют, то какими свойствами обладают.

В работе [2] предлагается способ построения таких g . Пусть $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$, $\text{supp}(g) = \{\alpha^s, \dots, \alpha^{s+2^{k-1}-1}\}$, где α — примитивный элемент поля $\text{GF}(2^k)$ и $s \in \mathbb{N}$. Тогда бент-функция f , построенная с помощью конструкции Диллона, обладает максимальной алгебраической иммунностью. Доказано

Утверждение 1. Пусть $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$, $\text{supp}(g) = \{\alpha^s, \dots, \alpha^{s+2^{k-1}-1}\}$, где α — примитивный элемент $\text{GF}(2^k)$ и $s \in \mathbb{N}$. Тогда для $k = 2, 3, \dots, 8$ верно $\deg(g) = k - 1$.

ЛИТЕРАТУРА

1. *Dillon J. F.* Elementary Hadamard difference sets. Ph. D. Thesis. Univ. of Maryland, 1974.
2. *Tu Z. and Deng Y.* A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity // *Designs, Codes and Cryptography*. 2011. V. 60. Iss. 1. P. 1–14.

УДК 519.6

ЭКВИВАЛЕНТНОСТЬ ПРИМИТИВНЫХ МНОЖЕСТВ

В. М. Фомичев

Исследована эквивалентность примитивных множеств натуральных чисел в связи с диофантовой проблемой Фробениуса. Эквивалентность используется для упрощения определения числа Фробениуса $g(a_1, \dots, a_k)$, а также всех чисел, не содержащихся в аддитивной полугруппе, порождённой множеством $\{a_1, \dots, a_k\}$.

Ключевые слова: функция Фробениуса, примитивное множество, аддитивная полугруппа чисел.

Основные обозначения:

$\mathbb{N}$ — множество натуральных чисел, $k, n \in \mathbb{N}$, $A = \{a_1, \dots, a_k\} \subset \mathbb{N}$;

$(a_1, \dots, a_k)$ — наибольший общий делитель чисел $a_1, \dots, a_k$;

$\langle a_1, \dots, a_k \rangle$ — аддитивная полугруппа, порождённая множеством $\{a_1, \dots, a_k\}$;

$n\{a_1, \dots, a_k\} = \{na_1, \dots, na_k\}$;

$A^{(i)} = \{a_1, \dots, a_i\}$, $C(A^{(i)}) = d_i \mathbb{N}_0 \setminus \langle A^{(i)} \rangle$, $d_i = (a_1, \dots, a_i)$, $i = 2, \dots, k$.

Множество $A = \{a_1, \dots, a_k\}$ натуральных чисел, $k > 1$, называется примитивным, если $(a_1, \dots, a_k) = 1$.

Функция Фробениуса $g(a_1, \dots, a_k)$ определена на всех примитивных множествах $\{a_1, \dots, a_k\}$ как наибольшее натуральное число $t \notin \langle a_1, \dots, a_k \rangle$ — число, не представимое в виде линейной комбинации чисел $a_1, \dots, a_k$ (рассматриваются линейные комбинации только с целыми неотрицательными коэффициентами):

$$g(a_1, \dots, a_k) = \max\{t \in \mathbb{N} : t \neq n_1 a_1 + \dots + n_k a_k\}.$$

Число Фробениуса $g(A) = \max C(A)$, где $C(A) = C(A^{(k)})$ — множество всех натуральных чисел, не представимых линейными комбинациями чисел $a_1, \dots, a_k$. Задача определения $g(a_1, \dots, a_k)$ известна как диофантова проблема Фробениуса (ПФ). Задача определения множества $C(A)$ называется расширенной проблемой Фробениуса (РПФ).

При $k = 2$ описание множества $C(A)$ и формула числа Фробениуса даны Дж. Сильвестром [1] ещё в 1884 г., формула числа Фробениуса имеет вид $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

При $k > 2$ алгоритмы РПФ до недавнего времени не исследовались, в то же время активно изучался порядок множества $C(A)$ и некоторые его свойства [2, гл. 5]. В [3] представлен алгоритм РПФ и дана оценка его сложности.

Намного активнее исследовалась ПФ. Вместе с тем прогресс в получении формул следует признать умеренным, получены формулы только для множеств частного вида при $k = 3, 4$. Эти трудности в определённой мере объяснимы; показано [4], что уже при $k = 3$ не существует конечного числа полиномов, позволяющих выразить через них число Фробениуса $g(a_1, a_2, a_3)$ с помощью разбиения области определения.

Более продуктивным стал алгоритмический подход к определению $g(a_1, \dots, a_k)$. Построен ряд алгоритмов как при $k = 3$ (O. Rodseth, J. Davison и др. [2]), так и при произвольном k . В работах [5, 6] разработан алгоритм вычисления функции Фробениуса при любом k с помощью экспоненцирования неотрицательной матрицы M порядка a_k и определения её экспонента с использованием соотношения $g(a_1, \dots, a_k) = \exp M - a_k$. Вычислительная сложность алгоритма в битовых операциях равна $O(a_k^3)$, требуемая память — $O(a_k^2 \log a_k)$ битов. В [7] предложено (без обоснования корректности) улучшение этого алгоритма со сложностью $O(a_k^2)$.

В [8] построен теоретико-графовый алгоритм определения $g(a_1, \dots, a_k)$ со сложностью $O(a_1(k + \log a_1))$ арифметических операций. В [9] эта оценка снижена до величины порядка $O(ka_1)$ операций.

В [3] на основе исследования отношений эквивалентности предложена редукция РПФ и ПФ для множества A к РПФ и ПФ соответственно для собственного подмножества порядка h , где $2 \leq h \leq \min(k, a_1)$. Редукция позволила снизить оценку $O(ka_1)$ до величины $O(l(A) + ha_1)$ арифметических операций, $l(A) \leq k$ — характеристика множества A .

Исследования отношений эквивалентности в данной работе получили дальнейшее развитие.

1. Эквивалентность множеств, $k > 2$

Примитивное множество $A = \{a_1, \dots, a_k\}$ рассмотрим как возрастающую последовательность, где $1 < a_1 < \dots < a_k$. Числа a_i и a_j множества A назовём a_1 -эквивалентными, если $a_i = a_j \pmod{a_1}$. Примитивное множество $A = \{a_1, \dots, a_k\}$ разбивается на h классов a_1 -эквивалентности, где $2 \leq h \leq \min\{k, a_1\}$. Трансверсал множества A по отношению a_1 -эквивалентности, состоящий из наименьших чисел классов, назовём a_1 -трансверсалом множества A и обозначим A/a_1 . Обозначим $W(A/a_1)$ последовательность порядковых номеров $i \geq 2$ чисел a_1 -трансверсала.

Множество A называется приведённым, если $a_i \notin \langle A^{(i-1)} \rangle$, $i = 2, \dots, k$. Неприведённое примитивное множество A содержит приведённые примитивные подмножества. Построим приведённое подмножество $B_A \subseteq A$, называемое A -базисом: $a_1 \in B_A$; $a_2 \in B_A$, если и только если a_2 не кратно a_1 ; пусть из $\{a_1, \dots, a_{i-1}\}$ в подмножество B_A включены числа $b_1, \dots, b_j$, тогда $a_i \in B_A$, если и только если $d_{i-1} > d_i$ или $(d_{i-1} = d_i$ и $a_i \in C(b_1, \dots, b_j))$, $i = 3, \dots, k$. Обозначим $W(B_A)$ последовательность порядковых номеров i чисел A -базиса.

Наименьшее натуральное $p(A)$, такое, что $d_{p(A)} = 1$, называется индексом примитивности множества A . Положим $p(A) = p$, тогда $p \leq k$, $d_p = \dots = d_k = 1$. Последовательность порядковых номеров $i \in \{2, \dots, p\}$, таких, что $d_{i-1} > d_i$, обозначим $L(A)$.

Подмножества D и D' множества A эквивалентны (g -эквивалентны), если $\langle D \rangle = \langle D' \rangle$ (если $g(D) = g(D')$); будем это отношение обозначать $D \cong D'$ (соответственно $D \cong^g D'$). Тогда $D \cong D'$, если и только если $C(D) = C(D')$, и если $D \cong D'$, то $g(D) = g(D')$.

Утверждение 1. $B_A \subseteq A/a_1 \subseteq A$, $B_A \cong A/a_1 \cong A$, где $|B_A| \leq |A/a_1| \leq \min\{k, a_1\}$; оценка достижима.

Следствие 1. Множество $A = \{a_1, \dots, a_k\}$ содержит эквивалентное подмножество порядка не больше $\min\{k, a_1\}$.

Пример 1 (построение A/a_1). Для $A = \{5, 13, 18, 20, 38\}$ считаем по mod 5: $5 \equiv 20$, $13 \equiv 18 \equiv 38$, тогда $A/5 = \{5, 13\}$.

Пусть $a_1 \geq 3$ и $A = A/a_1$, т.е. $k \leq a_1$ и числа $a_1, \dots, a_k$ несравнимы по модулю a_1 ; $L(A) = \{n_2, \dots, n_r\}$, $1 < r < k$, т.е. $d_{n_j-1} > d_{n_j}$, $j = 2, \dots, r$. Тогда A разбивается на r отрезков $A_1, \dots, A_r$, где $A_j = (a_{n_j}, \dots, a_{n_{j+1}-1})$, $j = 1, \dots, r$, $n_1 = 1$, $n_r = p$, $n_{r+1} = k + 1$.

Обозначим $J_1 = A_1 \setminus \{a_1\}$, $J(A)$ — множество чисел $a_i \in A$, таких, что $d_{i-1} = d_i$ и a_i не делит ни одно число из $C(A^{(i-1)})$ (т.е. $J(A) \subseteq \{n_2 + 1, \dots, k\} \setminus \{n_2, \dots, n_r\}$), $W(J)$ — последовательность порядковых номеров чисел из $J(A)$.

Далее без ущерба для общности считаем, что $n_2 = 2$. Приведём некоторые известные свойства.

Утверждение 2.

- 1) Если $B \subset A$ и $A \setminus B \subset \langle B \rangle$, то $A \cong B$.
- 2) Множество $A^{(i)}/d_i = \{a_1/d_i, \dots, a_i/d_i\}$ примитивное, $\langle A^{(i)} \rangle = d_i \langle A^{(i)}/d_i \rangle$, $i = 2, \dots, k$.
- 3) $g(a_1, \dots, a_k) \leq (a_1 - 1)(a_k - 1) - 1$ [2, теорема 3.1.1].

Теорема 1. $A \cong A \setminus J(A)$; если $n_2 > 2$, то $A \cong A \setminus (J_1 \cup J(A))$.

Обозначим $\gamma_j = d_{n_j}((a_1/d_{n_j} - 1)(a_{n_j}/d_{n_j} - 1) - 1)$, $l_1 = 1$, l_j — наибольший номер, такой, что $n_j \leq l_j < n_{j+1}$ и $a_{l_j} \leq \gamma_j$ (при $a_1 \geq 3$ условия корректны в силу утверждения 2; $S_1 = (a_1)$, $S_j = (a_{n_j}, \dots, a_{l_j})$, т.е. отрезок S_j составлен из первых (наименьших) $l_j - n_j + 1$ чисел отрезка A_j , $j = 2, \dots, r$; $S(A)$ есть конкатенация отрезков $S_1, S_2, \dots, S_r$, $l(A) = |S(A)|$.

Следствие 2. $A \cong S(A)$, $l(A) \leq \min\{k, a_1 a_p - a_1 - 2a_p + p\}$, где $p = p(A)$.

Алгоритмы построения A/a_1 и $A \setminus S(A)$ являются полиномиальными. Алгоритм построения $A \setminus J(A)$ экспоненциальный, по сложности он равносильен решению расширенной проблемы Фробениуса [3].

Пример 2. Пусть $A = \{5, 13, 18, 20, 57\}$. Вычисляем $A/5 = \{5, 13, 57\}$, $J(A/5) : L(A/5) = \{13\}$, $r = 2$, $A_1 = \{5\}$, $A_2 = \{13, 52\}$, $\gamma_2 = 47 < 57$. Тогда $J(A/5) = \{57\}$, $(A/5) \setminus J(A/5) = \{5, 13\}$. Окончательно $A \cong \{5, 13\}$.

2. Эквивалентность примитивных пар чисел

Обозначим через $[A]$ класс g -эквивалентности, содержащий примитивное множество A ; $[A]_m$ — класс всех примитивных множеств порядка m , g -эквивалентных A , $m = 2, 3, \dots$

Теорема 2. Пусть (a, b) — примитивная пара чисел. Тогда

$$[(a, b)]_2 = (a + \delta, b + \varepsilon) : a - b + 1 < \varepsilon < 0, \delta = (1 - a)\varepsilon / (b + \varepsilon - 1) \in \mathbb{N}; \\ 1 - a < \delta < 0, \varepsilon = (1 - b)\delta / (a + \delta - 1) \in \mathbb{N}.$$

Следствие 3.

Если $a > 2$, то $(2, g(a, b) + 2) \in [(a, b)]_2$; если $a > 3$, то $(3, (g(a, b) + 3)/2) \in [(a, b)]_2$.

Пример 3. Построим множество $[(13, 22)]_2$, $g(13, 22) = 251$. При $\delta > 0$ имеем $-8 < \varepsilon < 0$, при $\varepsilon > 0$ имеем $-12 < \delta < 0$.

ε	-7	-6	-5	-4	-3	-2	-1
δ	6	72/15	60/16	48/17	2	24/19	12/20

ε	21/11	42/10	7	84/8	15	21	147/5	42	63	105	231
δ	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11

Согласно таблице, $(\delta, \varepsilon) \in \{(2, -3), (6, -7)\}$. Пары $(13, 22)$ g -эквивалентна примитивная приведённая упорядоченная пара $(15, 19)$. Пара $(19, 15)$ исключена из класса $[(13, 22)]_2$, так как не упорядочена. Тогда $(\delta, \varepsilon) \in \{(-3, 7), (-5, 15), (-6, 21), (-8, 42), (-9, 63), (-10, 105), (-11, 231)\}$ и $(13, 22)$ g -эквивалентна парам $(10, 29)$, $(8, 37)$, $(7, 43)$, $(5, 64)$, $(4, 85)$, $(3, 127)$ и $(2, 253)$. Класс g -эквивалентности $[(13, 22)]_2$ содержит (вместе с $(13, 22)$) 9 пар.

Вывод: Отношения эквивалентности примитивных множеств позволяют сократить сложность решения РПФ и ПФ с помощью полиномиального алгоритма редукции примитивного множества A к подмножеству $B = (A/a_1) \setminus S(A/a_1)$. Сложность экспоненцирования неотрицательной матрицы [5, 6] имеет в сочетании с редукцией оценку $O(a^3)$, где $a = \max B$. Оценка Боккера — Липтак [9] понижается до величины порядка $O(l(A) + ha_1)$, где $h = |B|$.

ЛИТЕРАТУРА

1. *Sylvester J. J.* Problem 7382 // *Mathematical Questions from the Educational Times*. 1884. V. 37. P. 26.
2. *Alfonso J. R.* *The Diophantine Frobenius problem*. Oxford University Press, 2005.
3. *Фомичев В. М.* Решение диофантовой проблемы Фробениуса // *Дискретная математика*. 2013. № 2.
4. *Curtis F.* On formulas for the Frobenius number of a numerical semigroup // *Math. Scand.* 1990. V. 67. P. 190–192.
5. *Heap B. R. and Lynn M. S.* A graph-theoretic algorithm for the solution of a linear diophantine problem of Frobenius // *Numerische Math.* 1964. No. 6. P. 346–354.
6. *Heap B. R. and Lynn M. S.* On a linear diophantine problem of Frobenius: an improved algorithm. // *Numerische Math.* 1965. No. 7. P. 226–231.

7. Bogart C. Calculating Frobenius numbers with Boolean Toeplitz matrix multiplication // For Dr. Cull, CS 523, March 17, 2009. Oregon State University.
8. Nijenhuis M. A minimal-path algorithm for the “money changing problem” // The American Mathematical Monthly. 1979. V. 86. P. 832–835.
9. Bocker S. and Liptak Z. The “money changing problem” revisited: computing the Frobenius number in time $O(ka_1)$. Technical Report No. 2004-2, Univ. of Bielefeld, Technical Faculty, 2004.

УДК 519.7

ИТЕРАТИВНАЯ КОНСТРУКЦИЯ APN-ФУНКЦИЙ¹

А. А. Фролова

Векторные булевы функции F и G назовём γ -эквивалентными, если для каждой пары векторов $a \neq 0$, b уравнения $F(x) \oplus F(x \oplus a) = b$ и $G(x) \oplus G(x \oplus a) = b$ одновременно имеют или не имеют решений. Установлено, что все классы γ -эквивалентности APN-функций от n переменных имеют мощность 2^{2^n} . Предложена итеративная конструкция APN-функций.

Ключевые слова: векторная булева функция, APN-функция, γ -эквивалентность, итеративная конструкция.

Булевой функцией от n переменных называется любое отображение $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$. Весом Хэмминга $\text{wt}(f)$ булевой функции f называется количество единиц в векторе её значений. Векторной булевой функцией F называется любое отображение $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$. Векторную функцию можно рассматривать как набор из m координатных булевых функций от n переменных, т. е. $F = (f_1, \dots, f_m)$.

Булевы функции, используемые в криптографических приложениях, должны обладать рядом специальных свойств для обеспечения стойкости к некоторым видам криптоанализа. В работе [1] определено следующее требование к функции. Векторная функция F называется δ -дифференциально равномерной, если для любых векторов $a \neq 0$, b уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений. Для обеспечения стойкости шифра к дифференциальному криптоанализу необходимо использовать δ -дифференциально равномерные векторные булевы функции с малым значением δ .

Далее рассматриваем только случай $n = m$. В этом случае минимальное возможное δ равно двум. APN-функцией (Almost Perfect Nonlinear) называется 2-дифференциально равномерная векторная функция. В работе [2] приведён обзор по известным APN-функциям. Открытыми вопросами остаются оценки количества и новые способы построения APN-функций.

Пусть $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$. Для F и любого вектора $a \neq 0$ определяется множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{Z}_2^n\}.$$

Для F строится булева функция γ_F от $2n$ переменных следующим образом:

$$\gamma_F(a, b) = \begin{cases} 1, & \text{если } a \neq 0 \text{ и } b \in B_a(F), \\ 0 & \text{иначе.} \end{cases}$$

Известно, что F — APN-функция тогда и только тогда, когда $\text{wt}(\gamma_F) = 2^{2^n-1} - 2^{n-1}$. Пусть $F, F' : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$.

¹Работа поддержана грантом РФФИ, проект № 12-01-31097.