Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 511

АЛГОРИТМ ВЫЧИСЛЕНИЯ D-ПРОБЕЛЬНЫХ ЧИСЕЛ И D-ВЕЙЕРШТРАССОВЫХ ТОЧЕК

Е. С. Алексеенко

Множество вейерштрассовых точек является важным инвариантом алгебраической кривой, который можно использовать для изучения автоморфизмов. Исследуя вейерштрассовы точки, можно, например, показать, что группа автоморфизмов кривой конечна. Рассмотрим функциональные поля кривых; будем использовать определения и обозначения из [1, 2].

Будем полагать, что F/k — алгебраическое функциональное поле степени трансцендентности один над полем констант k. Предполагаем, что F/k имеет сепарирующий элемент и род g поля F/k инвариантен относительно расширения поля констант. Считаем также известными процедуры вычисления точек, дивизоров и пространств, ассоциированных с дивизором D (пространства Римана — Роха): $\mathscr{L}(D) = \{a \in F^{\times} : (a) + D \geqslant 0\} \bigcup \{0\}$.

Определение 1. Пусть D — дивизор, P — точка степени один поля F/k. Целое число $\mu \geqslant 1$ называется D-пробельным числом точки P, если $\mathscr{L}(D + (\mu - 1)P) = \mathscr{L}(D + \mu P)$.

Теорема 1. Все точки степени один поля Fk/k, быть может кроме конечного их числа, имеют одинаковые $\mathrm{con}_{Fk/F}(D)$-пробельные числа.

Определение 2. D-пробельные числа поля F/k определены почти для всех точек по предыдущей теореме. Точка степени один поля F/k называется D-вейерштрассовой точкой, если ее D-пробельные числа отличны от D-пробельных чисел поля F/k.

Теорема 2. Существует, по крайней мере, одна вейерштрассова точка поля $F\bar{k}/\bar{k}$ для $g \geqslant 2$, где $\bar{k}$ — алгебраическое замыкание поля k.

Пусть L — линейная система поля F/k. Отметим, что L можно рассматривать как множество эффективных дивизоров $\{(a) + E : a \in V - \{0\}\}$ для дивизора E и некоторого k-линейного пространства $\mathscr{L}(E)$. Полной линейной системой является линейная система, определенная с помощью E и $\mathscr{L}(E)$. Отметим также, что для любого дивизора $E \in L$ полная линейная система определена с помощью E и k-линейного пространства V, порожденного $\{a \in F^{\times} : (a) = D - E, D \in L\}$. Таким образом, можно рассматривать L как класс эквивалентности пары (E, V), где $(E, V) \approx (E - (a), aV)$. Следует также отметить, что $\deg(L) = \deg(E)$, $\dim(L) = \dim(V)$. Будем полагать, что $L(\mu P) = \{D \in L : v_P(D) \geqslant \mu\}$ для целого $\mu \geqslant 0$.

Определение 3. Пусть L — полная линейная система и P — точка степени один. Целое число $\mu \geqslant 0$ называется порядком (вронскианом) L в точке P, если $L(\mu P) \neq \neq L((\mu + 1)P)$.

Теорема 3. Пусть L — полная линейная система, определенная с помощью $W-D$. Тогда μ является D-пробельным числом тогда и только тогда, когда $\mu-1$ — порядок L в точке P.

В соответствии с теоремой 3, для того, чтобы вычислить пробельные числа и вейерштрассовы точки, достаточно исследовать порядки L в различных точках.

Теорема 4. Каждый порядок μ линейной системы L в точке P удовлетворяет условию $0 \leqslant \mu \leqslant \deg(L)$. Существует $\dim(L)$ порядков L в точке P.

Определение 4. Пусть L — полная линейная система, определенная с помощью E и V. Пусть $v_1, \ldots, v_n$ — базис V, x — сепарирующий элемент F/k и $\varepsilon_1, \ldots, \varepsilon_n$ — порядки L. Дивизор $R(L) = (\det(D_x^{(\varepsilon_i)}(v_j))_{i,j}) + \left(\sum_{i=1}^{n} \varepsilon\right)(dx) + nE$ называется дивизором ветвления в L.

Опишем алгоритм вычисления вейерштрассовых точек алгебраического функционального поля, ассоциированного с алгебраической кривой, произвольной характеристики.

Алгоритм 1

Вход: Функциональное поле F/k, сепарирующий элемент x, дивизор D.
Выход: D-пробельные числа и D-пробельные вейерштрассовы точки.

Шаг 1. Вычисляем канонический дивизор $W := (dx)$.

Шаг 2. Если $\dim(W - D) = 0$, то дивизор ветвления полной линейной системы, определенной с помощью $W - D$, является нулевым и не существует D-пробельных чисел и D-пробельных вейерштрассовых точек. Алгоритм завершен.

Шаг 3. Вычисляем базис $v_1, \ldots, v_n$ в $\mathscr{L}(W - D)$.

Шаг 4. Полагаем $\varepsilon_1 := 0$; $M := (v_1, ..., v_n)$; $i := 1$; $\varepsilon := 0$; $G := \varnothing$.

Шаг 5. $i := i + 1$. Если $i > n$, то переходим к шагу 8.

Шаг 6. $\varepsilon := \varepsilon + 1$. Если $\binom{\varepsilon}{g} \neq 0$ в k для некоторого $g \in G$, то $G := G \bigcup \{\varepsilon\}$ и повторяем шаг 6.

Шаг 7. Обозначим $\acute{M} \in F^{i \times n}$ — матрица, полученная добавлением $D_x^{(\varepsilon)}(v_1), \ldots, D_x^{(\varepsilon)}(v_n))$ к M. Если $\operatorname{rank} \acute{M} > \operatorname{rank} M$, то $M := \acute{M}$; $\varepsilon_i := \varepsilon$ и переходим к шагу 5. Иначе $G := G \bigcup \{\varepsilon\}$ и переходим к шагу 6.

Шаг 8. Вычисляем дивизор ветвления $R := (\det(M)) + \left(\sum_{i=1}^{n} \varepsilon\right)(dx) + n(W - D)$ полной системы, определенной с помощью $W - D$.

Шаг 9. Возвращаем $\varepsilon_1 + 1, \ldots, \varepsilon_n + 1$ и точки степени один, лежащие в носителе R.

Пример 1. Рассмотрим функциональное поле F/k, определенное уравнением $y^7 + y = x^4$ над полем $\mathbb{F}_{49}$. Род поля $g = 9$, число точек степени один $N = 176$. Используя алгоритм, получаем, что 1, 2, 3, 4, 5, 8, 9, 10, 15 — пробельные числа поля F/k. Все 176 точек степени один являются вейерштрассовыми точками. Существуют 8 вейерштрассовых точек веса 9 с пробельными числами 1, 2, 3, 5, 6, 9, 10, 13, 17 и 168 вейерштрассовых точек веса 5 с пробельными числами 1, 2, 3, 4, 5, 9, 10, 11, 17. Дивизор ветвления имеет степень 912. Все вычисления были проведены в системе компьютерной алгебры MAGMA.

ЛИТЕРАТУРА

1. *Kuribayashi A. and Komiya K.* On Weierstrass Points of non-hyperelliptic compact Riemann surfaces of genus three // Hiroshima Math J. 1977. No. 7. P. 743–768.
2. *Stichtenoth H.* Algebraic Function Fields and Codes. Berlin; Heidelberg; New York: Springer Verlag, 1993.

УДК 519.174

КОДИРОВАНИЕ КОНЕЧНОЙ ЦЕЛОЧИСЛЕННОЙ РЕШЕТКИ В КЛАССЕ ОТОБРАЖЕНИЙ ОГРАНИЧЕННОГО ИСКАЖЕНИЯ[1]

А. А. Евдокимов

Пусть ε и δ — натуральные числа из области определения метрик ρ_G и ρ_H, заданных на множествах вершин $V(G)$ и $V(H)$ графов G и H, а $S_k(v)$ — шар с центром в точке $v \in V(G)$ и радиусом k. Скажем, что отображение $f : G \to H$, действующее из $V(G)$ в $V(H)$, обладает свойством $\langle \varepsilon, \delta \rangle$-ограниченного искажения, если

$$f(S_\delta(v)) \subseteq (S_\varepsilon(f(v))$$

для любой вершины $v \in V(G)$.

Скажем, что отображение $f : G \to H$ сохраняет $\langle \varepsilon, \delta \rangle$-отделимость, если

$$\operatorname{Im} f \cap S_\varepsilon(f(v)) \subseteq f(S_\delta(v)).$$

Вложение $f : G \to H$ графа G в H называем $\langle \varepsilon, \delta \rangle$-вложением, если f обладает свойством $\langle \varepsilon, \delta \rangle$-ограниченного искажения и сохраняет $\langle \varepsilon, \delta \rangle$-отделимость.

В отличие от аналогичных определений в [1 – 3], здесь выбраны $\langle \varepsilon, \delta \rangle$-язык и окрестности (шары), чтобы подчеркнуть общность с определениями классической математики. При «малых» значениях параметров $\langle \varepsilon, \delta \rangle$-вложение означает, что оно связные части не разрывает, а «далёкие» не становятся «близкими». Первое является дискретным аналогом непрерывного отображения, а вместе со вторым свойством — аналогом гомеоморфного вложения.

Пусть $N_m = \{0, 1, \ldots, m-1\}$ и $N_m^2 = N_m \times N_m$ — двумерная целочисленная решетка размера $m \times m$ с расстоянием

$$\rho_{N^2}(u, v) = |x_1 - x_2| + |y_1 - y_2|$$

между ее вершинами (узлами решетки) $u = (x_1, y_1)$ и $v = (x_2, y_2)$.

В [3] описана конструкция $\langle 3, 2 \rangle$-вложения целочисленной решетки N_{14}^2 (плоского решётчатого табло) в булев гиперкуб I^{10} и показано, что наибольший размер решетки N_m^2 для любого $\langle 3, 2 \rangle$-вложения $f : N_m^2 \to I^{10}$ равен 14×14; $\langle 3, 2 \rangle$-вложение сохраняет все расстояния, не превосходящие 3, а вершины, находящиеся на расстоянии больше 1, не могут оказаться на расстоянии 0 или 1. Таким образом, изометричное 3×3 окно в классе обратимых кодирований двоичными словами длины 10 возможно для квадратного табло из 196 ячеек размера 1×1.

Теорема 1. Существует и эффективно строится конструкция $\langle 4, 3 \rangle$-вложения $f : N_m^2 \to I^n$ целочисленной решётки размера $m \times m$ в булев куб I^n, избыточность

[1]Работа поддержана проектами РФФИ № 09-01-00070 и 11-01-00997 и программой фундаментальных исследований Отделения математических наук РАН.

которого асимптотически минимальна, а мощность решётки удовлетворяет неравенству

$$| \mathbb{N}_m^2 | > 2^{n-2\log_2 n(1+\varepsilon_n)},$$

где $\varepsilon_n \to 0$ при $n \to \infty$.

Рассмотренные свойства вложений обобщаются на произвольные метрические пространства, хотя выше для простоты сформулированы для графов с обычной метрикой.

Найдены также оптимальные кодирования решёток, определяемые их 2-интервальными вложениями, специальный случай которых для малых значений параметров рассмотрен в [3].

ЛИТЕРАТУРА

1. *Евдокимов А. А.* Метрические свойства вложений и коды, сохраняющие расстояния // Труды Института математики СО РАН. Новосибирск: Наука, 1988. Т. 10. С. 116–132.
2. *Евдокимов А. А.* Локально изометрические вложения графов и свойство продолжения метрики // Сиб. журн. исслед. операций. 1994. Т. 1. № 1. С. 5–12.
3. *Евдокимов А. А.* Вложения графов в n-мерный булев куб и интервальное кодирование табло // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 15–19.

УДК 519.7

КОЛИЧЕСТВО БЕНТ-ФУНКЦИЙ НА МИНИМАЛЬНОМ РАССТОЯНИИ ОТ КВАДРАТИЧНОЙ БЕНТ-ФУНКЦИИ[1]

Н. А. Коломеец

Бент-функции — это булевы функции, максимально удаленные от класса аффинных функций. Впервые бент-функции были рассмотрены О. Ротхаусом [1]. Бент-функции имеют огромное число приложений: в криптографии, теории кодирования, теории информации. Тем не менее для них до сих пор существует много нерешенных проблем. Одна из наиболее важных проблем — описание всех бент-функций, в частности нахождение конструкций для бент-функций.

В работе рассматривается получение бент-функций на минимальном расстоянии от квадратичной бент-функции. В [2] показано, что две бент-функции от $2k$ переменных находятся на минимальном расстоянии тогда и только тогда, когда они отличаются на аффинном подпространстве размерности k и обе функции на нем аффинны. В данной работе описываются все бент-функции на минимальном расстоянии от квадратичной бент-функции $(x_1x_{k+1} \oplus x_2x_{k+2} \oplus \ldots \oplus x_kx_{2k})$, а также подсчитывается число бент-функций на минимальном расстоянии от произвольной квадратичной бент-функции.

Пусть A — произвольная матрица; через $a_{(i)}$ будем обозначать её i-й столбец. Будем описывать линейные подпространства с помощью базисов Гаусса — Жордана. Отметим, что в наших обозначениях базисные векторы являются *столбцами* базисной матрицы.

Определение 1. Пусть G — матрица с k столбцами, образованная векторами $u_{(1)}, \ldots, u_{(k)}$ длины n. Через $l(u_{(i)})$ обозначим $\min\{j : {u_{(i)}}_j \neq 0\}$. Матрица G является *базисом Гаусса — Жордана* подпространства размерности k в пространстве размерности n, если выполняются следующие условия:

[1]Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0362).

1) если $i_1 < i_2$, то $l(u_{(i_1)}) < l(u_{(i_2)})$;
2) если $i_1 \neq i_2$, то $u_{(i_1)_{l(u_{(i_2)})}} = 0$.

В этом случае через $l(G)$ обозначим множество $\{l(u_{(1)}), \ldots, l(u_{(k)})\}$. Все строки матрицы G с номерами из множества $l(G)$ будем называть *ведущими строками*. Все остальные строки будем называть *неведущими*. Через L_G обозначим подпространство с базисом $u_{(1)}, \ldots, u_{(k)}$. Заметим, что столбцы матрицы G действительно являются базисными векторами пространства L_G, а матрицу G^{T} называют также *редуцированной ступенчатой матрицей*.

Известно, что любое линейное подпространство имеет ровно один базис Гаусса — Жордана.

Введем определение *допустимого* базиса Гаусса — Жордана. Пусть базис Гаусса — Жордана G для подпространства размерности k в пространстве размерности $2k$ имеет следующий вид:

$$\left(\begin{array}{c|c} \mathrm{A} & 0 \\ \hline \mathrm{Z} & \mathrm{Y} \end{array}\right),$$

где матрица A размера $k \times t$ не содержит нулевых столбцов, а матрица Y имеет размер $k \times (k-t)$. Заметим, что матрицы A и Y являются базисами Гаусса — Жордана. Пусть $L_Y = L_A^{\perp}$. Удалим из матрицы A все строки с номерами из $l(Y)$. Пусть все оставшиеся строки образуют матрицу A'. Аналогичные действия проделаем и с матрицей Z: удалим все строки с номерами из $l(Y)$ и образуем из оставшихся строк матрицу Z'. Заметим, что все удаленные из матрицы Z строки являются нулевыми, так как G является базисом Гаусса — Жордана. Таким образом, получили матрицы A' и Z' размера $t \times t$. Базис Гаусса — Жордана G назовем *допустимым*, если $t \leqslant 1$ или элементы матрицы Z' при $t \geqslant 2$ являются решениями следующей системы уравнений с матрицей размера $(t(t-1)/2) \times t^2$:

$$\begin{pmatrix} {a'_{(2)}}^{\mathrm{T}} & {a'_{(1)}}^{\mathrm{T}} & 0 & 0 & \ldots & 0 \\ \ldots & & & & & \\ {a'_{(t)}}^{\mathrm{T}} & 0 & 0 & \ldots & 0 & {a'_{(1)}}^{\mathrm{T}} \\ \ldots & & & & & \\ 0 & {a'_{(3)}}^{\mathrm{T}} & {a'_{(2)}}^{\mathrm{T}} & 0 & \ldots & 0 \\ \ldots & & & & & \\ 0 & {a'_{(t)}}^{\mathrm{T}} & 0 & \ldots & 0 & {a'_{(2)}}^{\mathrm{T}} \\ \ldots & & & & & \\ 0 & 0 & 0 & \ldots & {a'_{(t)}}^{\mathrm{T}} & {a'_{(t-1)}}^{\mathrm{T}} \end{pmatrix} \cdot \begin{pmatrix} {z'}_{(1)} \\ {z'}_{(2)} \\ \\ \\ \cdot \\ \cdot \\ \cdot \\ \\ \\ {z'}_{(t)} \end{pmatrix} = 0.$$

Следующая теорема описывает все бент-функции на минимальном расстоянии от квадратичной бент-функции.

Теорема 1. Для бент-функции $f(x) = x_1x_{k+1} \oplus x_2x_{k+2} \oplus \ldots \oplus x_kx_{2k}$ функция $f(x) \oplus \mathrm{Ind}_L(x)$ является бент-функцией на минимальном расстоянии от $f(x)$ тогда и только тогда, когда множество L является линейным подпространством с допустимым базисом Гаусса — Жордана или сдвигом такого подпространства.

Теорема 2. Любая квадратичная бент-функция от $2k$ переменных имеет ровно $2^k(2^1+1) \cdot \ldots \cdot (2^k+1)$ бент-функций на минимальном расстоянии 2^k.

Заметим, что число бент-функций от $2k$ переменных на минимальном расстоянии от заданной бент-функции можно оценить сверху числом 2^{k^2+2k} (это оценка сверху числа всевозможных аффинных подпространств размерности k), а число бент-функций на минимальном расстоянии от квадратичной бент-функции асимптотически равно $C \cdot 2^{k(k+3)/2}$. Таким образом, число бент-функций на минимальном расстоянии от квадратичной бент-функции больше, чем корень из этой тривиальной верхней оценки.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. No. 20. P. 300–305.
2. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–21.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ[1]

О. Л. Колчева, И. А. Панкратова

Интерес к статистической независимости булевой функции от подмножества аргументов возникает в связи с построением статистических аналогов функции [1], которые, в свою очередь, используются в линейном криптоанализе [2, 3].

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 $\Pr[f' = 1] = \Pr[f = 1]$; или, что то же самое, $\mathrm{w}(f') = \mathrm{w}(f)/2^{|U|}$, где $\mathrm{w}(f)$ — вес функции f. В частности, для статистического аналога $\varphi(x, y, k) = 0$ функции шифрования $F(x, k)$, где x, k, y — переменные со значениями в множествах открытых текстов, ключей и шифртекстов соответственно, условие статистической независимости функции $\varphi_F(x, k) = \varphi(x, F(x, k), k)$ от переменных в x является необходимым для того, чтобы вероятность выполнения уравнения $\varphi_F = 0$ сохранялась при подстановке в это уравнение любого значения x при равновероятном выборе k [1].

Требование статистической независимости функции от *конкретного* подмножества аргументов более слабое, чем условие корреляционной иммунности [4]: функция является корреляционно-иммунной порядка m, если и только если она статистически не зависит от *любого* m-элементного подмножества своих аргументов.

В [1] сформулирован тест статистической независимости: функция $f(x, y)$, где x, y — переменные со значениями в $(\mathbb{Z}_2)^n$ и $(\mathbb{Z}_2)^m$ соответственно, статистически не зависит от булевых переменных в x, если и только если $\hat{f}(u, 0^m) = 0$ для любого ненулевого вектора $u \in (\mathbb{Z}_2)^n$. Здесь $\hat{f}$ — преобразование Уолша — Адамара функции f; 0^m — m-компонентный нулевой вектор.

Сформулируем некоторые простейшие свойства статистической независимости.

1) Если функция имеет s линейных переменных, то она статистически не зависит от любого $(s-1)$-элементного подмножества своих аргументов.
2) Если функция статистически не зависит от U, то она статистически не зависит от любого подмножества U.

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

3) Если функция f статистически не зависит от подмножества U своих аргументов, то $2^{|U|}|\mathrm{w}(f)$.
4) Пусть f_1, f_2, …, f_{2^m} — компоненты разложения функции f по некоторым m переменным, и все они статистически не зависят от подмножества U. Тогда и f статистически не зависит от U.

Основным результатом является следующее

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 $h(x,y,z) = g\left(f(x,y),z\right)$, где g — любая функция от $l+1$ переменных, статистически не зависит от переменных в x.

Доказательство. Воспользуемся тестом статистической независимости. Пусть u — любой ненулевой вектор из $\mathbb{Z}_2^n$; тогда по условию $\hat{f}(u,0^m)=0$. Вычислим коэффициент Уолша — Адамара функции h:

$$\hat{h}(u,0^m,0^l) = \sum_{x,y,z} (-1)^{g(f(x,y),z)\oplus(u,x)} = \sum_z \underbrace{\left(\sum_{\substack{x,y,\\ f(x,y)=0}} (-1)^{g(0,z)\oplus(u,x)} + \sum_{\substack{x,y,\\ f(x,y)=1}} (-1)^{g(1,z)\oplus(u,x)} \right)}_{A}.$$

Для каждого $z \in \mathbb{Z}_2^l$ имеет место один из следующих двух случаев:

1) $g(0,z) = g(1,z) = c \in \{0,1\}$, тогда $A = (-1)^c \sum\limits_{x,y} (-1)^{(u,x)} = 0$;

2) $g(0,z) = \overline{g(1,z)} = c \in \{0,1\}$, тогда $A = (-1)^c \left(\sum\limits_{\substack{x,y,\\ f(x,y)=0}} (-1)^{(u,x)} - \sum\limits_{\substack{x,y,\\ f(x,y)=1}} (-1)^{(u,x)} \right) =$
$= (-1)^c \sum\limits_{x,y} (-1)^{f(x,y)\oplus(u,x)} = (-1)^c \hat{f}(u,0^m) = 0.$

Таким образом, $\hat{h}(u,0^m,0^l)=0$, и утверждение доказано. ■

К сожалению, это утверждение не допускает обобщения на случай нескольких функций f; так, если функции $f_1(x,y)$, $f_2(x,y)$, …, $f_s(x,y)$ статистически не зависят от переменных в x, то функция $g(f_1(x,y), f_2(x,y), \ldots, f_s(x,y), z)$ не обязательно обладает этим свойством.

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. *Matsui M.* Linear Cryptanalysis Method for DES Cipher // LNCS. 1993. V. 765. P. 386–397.
3. *Matsui M.* The First Experimental Cryptanalysis of the Data Encryption Standard // LNCS. 1994. V. 839. P. 1–11.
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

УДК 519.7

КЛАССИФИКАЦИЯ ГРАФОВ АНФ КВАДРАТИЧНЫХ БЕНТ-ФУНКЦИЙ ОТ ШЕСТИ ПЕРЕМЕННЫХ

Е. П. Корсакова

В математике часто возникает задача построения булевых функций, обладающих свойством нелинейности. Особенный интерес представляют функции, для которых эти свойства экстремальны. Такие булевы функции от четного числа переменных называются бент-функциями. Определим понятие бент-функции более строго. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция W_f, заданная на множестве $\mathbb{Z}_2^n$ равенством $W_f(v) = \sum\limits_{u \in \mathbb{Z}_2^n} (-1)^{<u,v> \oplus f(u)}$. *Бент-функцией* называется булева функция от n переменных (n четно), такая, что модуль каждого коэффициента Уолша — Адамара этой функции равен $2^{n/2}$.

Несмотря на то, что масштабы исследования бент-функций велики, в настоящее время они изучены довольно плохо. Например, задача описания всех бент-функций от n переменных решена лишь при малых значениях n. При $n \geqslant 10$ класс бент-функций не описан, его мощность неизвестна.

Обратимся к вопросу классификации бент-функций степени 2 от 6 переменных. Известно [1], что все квадратичные бент-функции аффинно эквивалентны между собой. Введем для таких функций понятие более сильной эквивалентности, а именно графовой эквивалентности. Каждой функции сопоставим граф на шести вершинах. Вершины графа отождествим с переменными булевой функции, ребрами соединим те вершины, которые образуют слагаемое в квадратичной части алгебраической нормальной формы (АНФ) функции. Для каждого графа определим его тип — упорядоченный по убыванию набор степеней его вершин. Две функции назовем *графово эквивалентными*, если соответствующие им графы изоморфны. В данной работе решена задача графовой классификации всех квадратичных бент-функций от 6 переменных.

Все квадратичные бент-функции аффинно эквивалентны функции $x_1x_2 \oplus x_3x_4 \oplus \oplus x_5x_6$. Поэтому для нахождения графов использовались аффинные преобразования этой функции, заданные верхнетреугольными матрицами с 1 на диагонали, 0 или 1 над диагональю, а именно вида

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

где на местах * стоят 0 или 1. Написана программа на C, которая, перебирая все возможные матрицы данного вида, определяет типы графов. В результате получено 37 типов и 50 графово неэквивалентных бент-функций. В таблице приведены все типы в левой колонке и соответствующие им бент-функции — в правой. Функция задана вектором лексикографически упорядоченных коэффициентов в квадратичной части АНФ (в скобках указан возможный способ её построения из бент-функции от четырёх переменных).

№ п/п	Тип	Функция
1	1 1 1 1 1 1	100000000100001 (iter1)
2	2 2 1 1 1 1	100001000100001 (iter1)
3	2 2 2 2 1 1	100001000100101 (iter2)
4	3 2 2 1 1 1	100001001001100 (iter1) 100001001100001 (iter3)
5	3 2 2 2 2 1	100001001100101 100001000010111
6	3 3 2 2 1 1	100001001110001 (iter1) 100001000110101 (iter2)
7	3 3 2 2 2 2	011001011100001 101101001100001
8	3 3 3 1 1 1	100001010110001 (iter2)
9	3 3 3 2 2 1	100001001100111 (iter2) 100001001110101 100001001100111
10	3 3 3 3 1 1	100001010110110 (iter2) 111001100100001 (iter1) 111000000110101 (iter1)
11	3 3 3 3 2 2	110011100100101 110101001100101 111001001100101 101101001100101
12	4 2 2 2 1 1	100001101100001 (iter3)
13	4 3 2 2 2 1	100001101100101 100001100100111
14	4 3 3 2 1 1	100001101100011
15	4 3 3 2 2 2	111011000100101
16	4 3 3 3 2 1	111100001110100 (iter3)
17	4 3 3 3 3 2	110011000110111
18	4 4 3 2 2 1	100001101100111
19	4 4 3 3 1 1	100001101101110 (iter2)
20	4 4 3 3 2 2	110001011110011
21	4 4 3 3 3 1	100001100111111
22	4 4 3 3 3 3	111011001110101
23	4 4 4 3 3 2	011101001110111
24	4 4 4 4 3 1	100001101111111
25	4 4 4 4 3 3	111001100010111 110101101100111
26	5 2 2 2 2 1	100001111100001
27	5 3 3 2 2 1	100001111100101
28	5 3 3 3 2 2	110001000111111
29	5 3 3 3 3 3	110101001111110
30	5 4 3 3 2 1	100001111111100
31	5 4 4 3 2 2	110111000111101
32	5 4 4 4 3 2	111101000111111
33	5 4 4 4 4 1	100001111111111
34	5 5 3 3 3 3	111001100111111
35	5 5 4 4 3 3	111001111111011
36	5 5 5 4 4 3	111101111111110
37	5 5 5 5 5 5	111111111111111

Поясним обозначения. Конструкция iter1 означает, что к бент-функции от четырёх переменных добавляется слагаемое x_5x_6; iter2 — слагаемое $x_ix_5 \oplus x_jx_6$, где $i, j \in \in \{1, 2, 3, 4\}$; iter3 — слагаемое $x_ix_5 \oplus x_5x_6$, где $i \in \{1, 2, 3, 4\}$. Пример: АНФ функции, заданной вектором 100001101100011, имеет вид $x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_4x_6 \oplus \oplus x_5x_6$. Данное исследование помогает выявить общие закономерности построения бент-функций от $(n + 2)$ переменных с помощью бент-функций от n переменных.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.

УДК 519.7

СЛАБОЦЕНТРАЛЬНЫЕ КЛОНЫ И ПРОБЛЕМА ПОЛНОТЫ В НИХ[1]

Н. Г. Парватов

Проблема полноты и критериальные системы. Пусть E — конечное множество. Через P_E обозначается множество функций $f : E^n \to E$ при всевозможных целых положительных n. Классы таких функций, замкнутые операциями суперпозции и

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

содержащие селекторные функции, называются *клонами*, а клоны, включающие множество $A \subseteq P_E$, — *A-клонами*.

Будем интересоваться *проблемой полноты в A-клоне* (иначе — проблемой A-полноты в клоне) B, состоящей в описании всех его *A-порождающих подмножеств*, порождающих его с использованием операций суперпозиции, селекторов и функций из множества A. Инструментом решения этой проблемы является *A-критериальная* система. Так называется система $\mathcal{S}$ A-клонов, собственным образом содержащихся в клоне B, если всякий A-клон, собственным образом содержащийся в клоне B, можно расширить до некоторого клона из $\mathcal{S}$. A-критериальная система $\mathcal{S}$ называется *безызбыточной*, если она не содержит пары сравнимых по включению клонов и совпадает тогда с системой $\mathcal{S}(A, B)$ всех максимальных A-клонов среди строго содержащихся в B, в остальных случаях лишь включённой в $\mathcal{S}$.

Обозначим через Π_E множество предикатов $p : E^n \to \{\text{И,Л}\}$ при всевозможных натуральных n. Неинвариантный для клона B предикат p из Π_E называется *B-предельным* [1], если всякий отличный от p предикат, полученный из него проектированием, отождествлением переменных, B-сужением (пересечением с инвариантным для B предикатом) или симметризацией (пересечением с перестановочно эквивалентным предикатом), ужé инвариантен для клона B. Обозначим через $\Lambda(A, B)$ множество инвариантных для A B-предельных предикатов и через $\tilde{\Lambda}(A, B)$ — множество клонов $B \cap \mathrm{pol}_E(p)$, где $p \in \Lambda(A, B)$. В [1] доказана

Теорема 1. Система $\tilde{\Lambda}(A, B)$ является A-критериальной для клона B. Эта система конечная, если клон B обладает конечным A-порождающим подмножеством.

Заметим, что теорема 1 не исключает возможной избыточности системы $\tilde{\Lambda}(A, B)$.

Слабоцентральные клоны. Пусть c — некоторый элемент из множества E. Предикат p из Π_E назовём *c-слабоцентральным*, если в любом удовлетворяющем ему наборе замена любой компоненты значением c приводит к набору, также удовлетворяющему p. Для любого множества Y *c-слабоцентральных* предикатов из Π_E клон $\mathrm{pol}_E(Y)$ также называется *c-слабоцентральным*. Иными словами, произвольный клон является *c-слабоцентральным*, если он включает (наименьший по включению) клон $\mathrm{pol}_E(W_E^c)$, описываемый множеством W_E^c всех *c-слабоцентральных* предикатов. (Интересно, что это множество замкнуто операциями проектирования, подстановки переменных, конъюнкции и даже дизъюнкции, но не содержит диагоналей, кроме тривиальных.) В двоичном случае такими наименьшими клонами $\mathrm{pol}_E(W_E^c)$ при различных c из множества $E = \{0, 1\}$ являются клоны неразделённых либо разделённых булевых функций. Слабоцентральные клоны обладают рядом интересных свойств и допускают ряд равносильных определений.

Частным случаем слабоцентральных клонов являются определяемые ниже клоны сохранения c-системы множеств. Назовём c-системой систему $\tilde{\varepsilon}$ подмножеств множества E, обладающую следующими свойствами:

1) наследственностью: если некоторое множество принадлежит системе $\tilde{\varepsilon}$, то и всякая его часть принадлежит $\tilde{\varepsilon}$;
2) слабой центральностью по c: если множество H принадлежит системе $\tilde{\varepsilon}$, то множество $H \cup \{c\}$ также принадлежит ей.

Обозначим через $Q_E(\varepsilon)$ клон функций из P_E, сохраняющих систему ε, и через $\Phi_E(\varepsilon)$ — клон функций, сохраняющих её по некоторой переменной. Несложно понять, что клоны $Q_E(\varepsilon)$ и $\Phi_E(\varepsilon)$ являются c-слабоцентральными.

Введённые клоны имеют важные приложения, отметим следующие два.

Пример 1. Пусть E — конечная верхняя полурешётка и ε — система её подмножеств с нижней гранью. Тогда клон $Q_E(\tilde{\varepsilon})$ совпадает с клоном квазимонотонных функций на полурешётке E, введённых Г. П. Агибаловым [2], а клон $\Phi_E(\tilde{\varepsilon})$ совпадает с клоном слабосущественных квазимонотонных функций из [3].

Пример 2. Как клон сохранения некоторой c-системы можно определить любой (предполный по теореме Розенберга) клон функций из P_E, сохраняющих произвольный отличный от диагонали центральный вполне рефлексивный симметричный предикат.

Проблема полноты в слабоцентральном клоне. Из-за указанных приложений слабоцентральных клонов представляется важной проблема полноты в них.

Теорема 2. Пусть A и B — *c-слабоцентральные* клоны, такие, что $A \subseteq B$. Тогда множество $\tilde{\Lambda}(A, B)$ является безызбыточной A-критериальной системой для клона B; в частности, для произвольных предикатов p и q из $\Lambda(A, B)$ строгое включение $B \cap \mathrm{pol}_E(p) \subset B \cap \mathrm{pol}_E(q)$ невозможно. Более того, для произвольных предикатов p и q из $\Lambda(A, B)$ равенство клонов $B \cap \mathrm{pol}_E(p) = B \cap \mathrm{pol}_E(q)$ равносильно перестановочной эквивалентности этих предикатов.

Сформулированная теорема сводит задачу построения безызбыточной A-критериальной системы в клоне B для слабоцентральных клонов A и B к нахождению B-предельных предикатов из $\Lambda(A, B)$. Помимо этого, имеет место

Следствие 1. Слабоцентральный клон обладает безызбыточной критериальной системой.

Отметим также, что доказанная в [3] теорема легко обобщается как теорема о $\Phi_E(\varepsilon)$-полноте в клоне $Q_E(\varepsilon)$ для произвольной c-системы $\tilde{\varepsilon}$.

ЛИТЕРАТУРА

1. *Парватов Н. Г.* О выделении максимальных подклонов // Прикладная дискретная математика. 2011. № 1. С. 14–25.
2. *Агибалов Г. П.* Дискретные автоматы на полурешётках. Томск: Изд-во Том. ун-та, 1993. 227 с.
3. *Парватов Н. Г.* Теорема о функциональной полноте в классе квазимонотонных функций на конечной полурешётке // Дискр. анализ и исслед. опер. Сер. 1. 2006. Т. 13. № 3. С. 62–82.

УДК 519.7

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

А. Б. Пичкур

Пусть S_N — группа подстановок степени N; $G \in S_N$; $\Gamma(G) \subseteq \{1, \ldots, N\}$ — 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 данной работе описано множество всех подстановок из $\Gamma_N(q) \cdot \Gamma_N(q)$. Данный результат имеет практические приложения в криптографии.

В научной литературе рассматривается схожая задача описания множества подстановок, принадлежащих произведению двух или более классов сопряженных элементов из S_N (или из A_N — знакопеременной группы подстановок) [1 – 6].

Доказаны следующие результаты.

Утверждение 1. Если $N \geqslant 6$, $2 \leqslant q_1 < q_2 \leqslant N/2$, то $\Gamma_N(q_1) \cdot \Gamma_N(q_1) \subseteq \Gamma_N(q_2) \times \times \Gamma_N(q_2)$.

Теорема 1. Пусть $N \geqslant 8$, $4 \leqslant q \leqslant N/2$, $G \in S_N$. Если $|\Gamma(G)| \leqslant 2q-2$, то существуют подстановки $H_1, H_2 \in \Gamma_N(q)$, 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 $\Gamma_N(q) \cdot \Gamma_N(q)$.

Утверждение 2. 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 лежит в $\Gamma_N(q) \cdot \Gamma_N(q)$ в том и только в том случае, когда существует такое подмножество $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$, что $m_{i_1} + \ldots + m_{i_k} = q$.

Утверждение 3. Пусть $N \geqslant 4$, $2 \leqslant q \leqslant N/2$, 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 лежит в $\Gamma_N(q) \cdot \Gamma_N(q)$ 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 $q - m_{i_1} + m_{i_2} + \ldots + m_{i_k} \in \{2, \ldots, m_{i_0} - 1\}$.

Итак, в теореме 1, утверждениях 2 и 3 полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q)$ при $4 \leqslant q \leqslant N/2$.

ЛИТЕРАТУРА

1. *Bertram E.* Even permutations as a product of two conjugate cycles // J. Combin. Theory (A). 1972. V. 12. No. 3. P. 368–380.
2. *Bertram E. and Wei V. K.* Decomposing a permutation into two large cycles; an enumeration // SIAM J. Algebraic Discrete methods. 1980. V. 1. No. 4. P. 450–461.
3. *Moran G.* Reflection classes whose cubes cover the alternating group // J. Combin. Theory (A). 1976. V. 21. No. 1. P. 1–19.
4. *Moran G.* Permutations as products of k conjugate involutions // J. Combin. Theory (A). 1975. V. 19. No. 2. P. 240–242.
5. Product of conjugacy classes in groups / eds. Z. Arad, M. Herzog. Lecture Notes in Mathematics. V. 1112. Berlin: Springer Verlag, 1985. 244 p.
6. *Тужилин М. Э.* О порождении знакопеременной группы полурегулярными инволюциями // Обозрение прикладной и промышленной математики. 2004. Т. 11. Вып. 4. С. 938–939.

УДК 519.7

О ПРИБЛИЖЕНИИ ПОДСТАНОВОК ИМПРИМИТИВНЫМИ ГРУППАМИ

Б. А. Погорелов, М. А. Пудовкина

С 70-х годов прошлого века изучаются и строятся классы функций, максимально далёких от множества всех аффинных функций. Однако вместо множества всех таких функций можно также рассматривать симметрическую группу на конечном множестве X, а вместо множества всех аффинных функций — множество всех подстановок, сохраняющих некоторую систему импримитивности W с r блоками мощности w,

которая берётся из множества $W_{w,r}$ всех таких нетривиальных систем и фиксирована. Максимальная группа подстановок, сохраняющая данную систему импримитивности $W \in W_{w,r}$, есть группа сплетения $IG_W = (S_w \wr S_r, W)$ в её импримитивном действии. Близость межу подстановками $g, h \in S_n$ измеряется расстоянием Хемминга $\chi(g, h)$.

В работе рассматриваются два параметра:

— порядок W-примитивности, то есть число

$$\chi_W(g) = \min\{\chi(g, h) : h \in IG_W\};$$

— порядок (w, r)-примитивности, то есть число

$$\chi_{(w,r)}(g) = \min\{\chi(g, h) : h \in IG_W,\ W \in W_{w,r}\}.$$

Если соответствующие параметры больше нуля, то подстановку g будем называть W-примитивной, (w, r)-примитивной; в противном случае — W-импримитивной, (w, r)-импримитивной. При рассмотрении W-примитивности каждой подстановке ставится в соответствие матрица, характеризующая удалённость данной подстановки от группы IG_W. Через коэффициенты данной матрицы получено выражение для $\chi_W(g)$. Описаны классы максимально W-примитивных подстановок, являющихся «бент-подстановками» относительно системы импримитивности. Приведены оценки числа таких подстановок.

Порядок (w, r)-примитивности подстановки $g \in S(X)$ определяется только её цикловой структурой, то есть является функцией на классах сопряжённых элементов в группе $S(X)$. Перечислены цикловые структуры подстановок из множества $IG_{(w,r)} = \bigcup\limits_{W \in W_{(w,r)}} IG_W$. Поскольку множество $IG_{(w,r)}$ является объединением классов сопряжённых элементов группы $S(X)$, то цикловая структура элемента g однозначно характеризует его принадлежность множеству $IG_{(w,r)}$. В целом задача нахождения порядка (w, r)-примитивности оказалась сложнее. Получены порядки (w, r)-примитивности при чётном n в крайних случаях $w = 2$ и $r = 2$.

Исходя из общего подхода, получены порядки (w, r)-примитивности для s-боксов криптосистем AES, ARIA, Whirlpool, MISTY1, Camellia, FOX .

УДК 519.14

О СОВЕРШЕННЫХ 2-РАСКРАСКАХ q-ЗНАЧНОГО ГИПЕРКУБА[1]

В. Н. Потапов

Обозначим через Z_q множество $\{0, \ldots, q-1\}$. Декартово произведение Z_q^n называется q-значным n-мерным кубом (гиперкубом). Функция $f : Z_q^n \to Z_q$ называется *корреляционно-иммунной порядка* $n - m$, если мощность пересечения грани размерности m с множеством $f^{-1}(a)$ зависит только от $a \in Z_q$. Через $\mathrm{cor}(f)$ будем обозначать максимальный порядок корреляционной иммунности. *Плотностью* булевозначной функции χ^S будем называть отношение $\rho(S) = |S|/q^n$. Если $\rho(S) = 1/2$, то булевозначную корреляционно-иммунную функцию χ^S называют *уравновешенной*.

[1]Работа выполнена при поддержке РФФИ (проекты №10-01-00424, 10-01-00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0429).

Расстоянием Хэмминга $d(x,y)$ между вершинами $x=(x_1,x_2,\ldots,x_n)$ и $y=(y_1, y_2,\ldots,y_n)$ называется число позиций, в которых наборы x и y различаются. Определим величину $A(S)$ как среднее число вершин из $S\subseteq Z_q^n$, которые находятся на расстоянии 1 от вершины из дополнения $Z_q^n\setminus S$, т. е. $A(S)=\dfrac{1}{q^n-|S|}\sum\limits_{x\notin S}|\{y\in S: d(x,y)=1\}|$.

Отображение $\mathrm{col}: Z_q^n\to\{0,\ldots,k\}$ называется *совершенной раскраской* с матрицей параметров $M=\{m_{ij}\}$, если для любых i и j, для каждой вершины цвета i число соседей цвета j равняется m_{ij}. В дальнейшем рассматриваются только раскраски в два цвета (2-раскраски). Будем считать, что $\{0,1\}$ — множество цветов. В этом случае булевозначная функция col является характеристической функцией множества вершин цвета 1.

Совершенный код (исправляющий одну ошибку) $C\subset Z_q^n$ можно рассматривать как множество единиц совершенной 2-раскраски с матрицей параметров $M=\begin{pmatrix} n(q-1)-1 & 1\\ n(q-1) & 0\end{pmatrix}$. Если число q является степенью простого числа, то раскраска с такими параметрами существует только при $n=(q^j-1)/(q-1)$. При $q=2$ список известных параметров совершенных 2-раскрасок имеется в [1, 2].

Известно (см., например, [3, 4]), что совершенная раскраска булева n-куба с матрицей параметров $\begin{pmatrix} n-b & b\\ c & n-c\end{pmatrix}$ является корреляционно-иммунной функцией порядка $(b+c)/2-1$, т. е. из регулярной распределённости вершин некоторого множества по шарам радиуса 1 следует равномерное распределение вершин этого множества по граням. Весьма интересным представляется выяснение возможности обратного следствия.

В [5] доказано, что если для некоторого множества $S\subset Z_2^n$ величины $\mathrm{cor}(\chi^S)$ и $\rho(S)$ совпадают с соответствующими параметрами для совершенного кода, то множество S является совершенным кодом. В [3] установлено, что неуравновешенная булева функция $f=\chi^S$ $(S\subset Z_2^n)$ удовлетворяет неравенству $\mathrm{cor}(f)\leqslant 2n/3-1$. Кроме того, в случае равенства $\mathrm{cor}(f)=2n/3-1$ функция f является совершенной раскраской. Подобным образом, если для множества $S\subset Z_2^n$ неравенство Биербрауэра — Фридмана (см. [6, 7]) превращается в равенство $\rho(S)=1-\dfrac{n}{2(\mathrm{cor}(f)+1)}$, то функция χ^S является совершенной 2-раскраской [8].

Оказывается, имеет место следующий критерий.

Теорема 1.

а) Для каждой булевозначной функции $f=\chi^S$, где $S\subset Z_q^n$, справедливо неравенство $\rho(S)q(\mathrm{cor}(f)+1)\leqslant A(S)$.

б) Булевозначная функция $f=\chi^S$ является совершенной 2-раскраской тогда и только тогда, когда $\rho(S)q(\mathrm{cor}(f)+1)=A(S)$.

Таким образом, равномерное распределение вершин множества по граням гиперкуба при экстремальных условиях на плотность множества влечёт регулярное распределение вершин множества по шарам. Более того, любая совершенная 2-раскраска получается как максимально равномерно распределённая по граням булевозначная функция при некоторых дополнительных односторонних ограничениях на размещение её единиц. При доказательстве теоремы использовались методы, развитые в [7].

ЛИТЕРАТУРА

1. *Fon-Der-Flaass D. G.* Perfect 2-colorings of a hypercube // Siber. Math. J. 2007. V. 48. No. 4. P. 740–745.
2. *Фон-Дер-Флаасс Д. Г.* Совершенные 2-раскраски 12-мерного куба, достигающие границы корреляционной иммунности // Сибирские электронные математические известия. 2007. Т. 4. С. 292–295.
3. *Fon-Der-Flaass D. G.* A bound of correlation immunity // Siber. Electron. Math. Rep. 2007. V. 4. P. 133–135.
4. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 91–148.
5. *Ostergard P. R. J., Pottonen O., and Phelps K. T.* The perfect binary one-error-correcting codes of length 15: Part II-Properties // IEEE Trans. Inform. Theory. 2010. V. 56. P. 2571–2582.
6. *Friedman J.* On the bit extraction problem // Proc. 33rd IEEE Symposium on Foundations of Computer Science. 1992. P. 314–319.
7. *Bierbrauer J.* Bounds on orthogonal arrays and resilient functions // J. Combinat. Designs. 1995. V. 3. P. 179–183.
8. *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 519.6

АЛГЕБРЫ ЯЗЫКОВ, АССОЦИИРОВАННЫЕ С ОТМЕЧЕННЫМИ ГРАФАМИ

Е. А. Пряничникова

В теории конечных автоматов одним из важнейших результатов является теорема Клини, в которой утверждается, что класс языков, распознаваемых конечными автоматами, совпадает с классом рациональных языков, представимых регулярными выражениями алгебры Клини [1].

В данной работе определяется понятие языка, допустимого в отмеченном графе, вводится система операций на формальных языках, которая, в частности, может использоваться в биологии, генетике, а также ДНК-вычислениях [2], и понятие регулярных выражений для этой системы операций.

Исследованы основные свойства семейства алгебр языков, допустимых в отмеченных графах; доказано, что язык допустим в отмеченном графе тогда и только тогда, когда он описывается регулярным выражением во введенной системе операций; разработаны методы анализа и синтеза языков, ассоциированных с отмеченными графами.

Пусть X — конечный алфавит; X^* — множество всех слов конечной длины в алфавите X; X^n — множество всех слов длины n в алфавите X; $X^{\geqslant n}$ — множество всех слов конечной длины в алфавите X, длина которых больше или равна n.

Определим на множестве X^* частичную бинарную операцию $\overset{n}{\circ}$ склеивания двух слов с параметром n следующим образом: для всех $w_1, w_2 \in X^*$

$$w_1 \overset{n}{\circ} w_2 = \begin{cases} xyz, & \text{если } w_1 = xy,\ w_2 = yz,\ y \in X^n; \\ \text{не определено} & \text{в противном случае.} \end{cases}$$

Введем на языках $L, R \subseteq X^*$ следующие операции:

1) $L \cup R = \{w : w \in L \text{ или } w \in R\}$;

2) $L \overset{n}{\circ} R = \{w_1 \overset{n}{\circ} w_2 : w_1 \in L \text{ и } w_2 \in R\}$;

3) $L^{\overset{n}{+}} = \bigcup\limits_{i=1}^{\infty} L^i$, где $L^1 = L$; $L^{i+1} = L^i \overset{n}{\circ} L$ для всех $i \geqslant 1$.

Рассмотрим семейство алгебр $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$. В случае, когда $n = 0$, операция $\overset{n}{\circ}$ совпадает с операцией конкатенации, а рассматриваемая алгебра является алгеброй регулярных языков.

Регулярные выражения в алгебре $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$ определим следующим образом:

1) $\varnothing$ является регулярным выражением и представляет язык $L(\varnothing) = \varnothing$;
2) x является регулярным выражением и представляет язык $L(x) = \{x\}$ для всех $x \in \bigcup\limits_{0 \leqslant i \leqslant n+1} X^i$;
3) если R и Q — регулярные выражения, представляющие языки $L(R)$ и $L(Q)$ соответственно, то выражения $(R \overset{n}{\circ} Q)$, $(R \cup Q)$, $(R^{\overset{n}{+}})$ также являются регулярными, причем $L(R \overset{n}{\circ} Q) = L(R) \overset{n}{\circ} L(Q)$, $L(R \cup Q) = L(R) \cup L(Q)$, $L(R^{\overset{n}{+}}) = (L(R))^{\overset{n}{+}}$.

Графом с отмеченными дугами (вершинами) назовем четверку $G = (Q, E, X, \mu)$, где Q — конечное множество вершин; $E \subseteq Q \times Q$ — множество дуг; X — конечное множество отметок дуг; $\mu : E \to X$ ($\mu : Q \to X$) — функция отметок дуг (вершин). Отметкой пути будем называть последовательность отметок входящих в этот путь дуг (вершин).

Пусть $I \subseteq Q$ — множество начальных вершин графа G с отмеченными дугами или с отмеченными вершинами, $F \subseteq Q$ — множество финальных вершин. Отметки всех путей в графе G, начальные вершины которых принадлежат множеству I, а конечные — множеству F, назовем языком, допускаемым графом G, и обозначим $L(G)$.

Теорема 1. Язык $L \subseteq X^*$ допустим в графе с отмеченными дугами (вершинами) тогда и только тогда, когда он описывается регулярным выражением любой алгебры из семейства $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$.

Эта теорема в некотором смысле аналогична широко известной теореме Клини для конечных автоматов. В случае, когда $n = 0$ и рассматриваются только графы с отмеченными дугами, теорема 1 совпадает с теоремой Клини. На основе доказательства теоремы разработаны методы анализа и синтеза языков, представимых в отмеченных графах.

ЛИТЕРАТУРА

1. *Капитонова Ю. В., Летичевский А. А.* Математическая теория проектирования вычислительных систем. М.: Наука, 1988.
2. *Anderson J.* Automata Theory with Modern Applications. Cambridge: Cambridge University Press, 2006.

УДК 519.7

ГИПОТЕЗЫ О ЧИСЛЕ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Проблема определения числа всех *бент-функций* — булевых функций от четного числа переменных, максимально удаленных от множества аффинных функций, — яв-

[1]Исследование выполнено при поддержке РФФИ (проекты № 09-01-00528, 10-01-00424, 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429).

ляется одной из фундаментальных в этой области. Известно, что разрыв между существующими нижней и верхней оценками этого числа огромен. В работе исследуется роль класса итеративных бент-функций в решении этой задачи и формулируется серия гипотез о числе бент-функций.

Бент-функция g от n переменных называется *итеративной бент-функцией*, если она получена из четырех бент-функций $f_0,\ f_1,\ f_2,\ f_3$ от $n-2$ переменных с помощью конструкции

$$g(00,x)=f_0(x),\ g(01,x)=f_1(x),\ g(10,x)=f_2(x),\ g(11,x)=f_3(x).$$

При этом необходимым и достаточным условием того, чтобы определенная таким образом булева функция g была бент-функцией, является выполнение равенства $\widetilde{f_0}+\widetilde{f_1}+\widetilde{f_2}+\widetilde{f_3}=1$, где $\widetilde{f}$ обозначает дуальную бент-функцию. Этот способ был предложен А. Канто и П. Шарпин в работе [1], см. также [2].

Пусть $\mathcal{B}_n$ и $\mathcal{BI}_n$ обозначают соответственно множество всех бент-функций и множество всех итеративных бент-функций от n переменных. В [2, 3] показано, что $|\mathcal{B}_{n+2}| \geqslant |\mathcal{BI}_{n+2}| \geqslant \sum\limits_{f'\in\mathcal{B}_n}\sum\limits_{f''\in\mathcal{B}_n} |\ (\mathcal{B}_n+f')\cap(\mathcal{B}_n+f'')\ |$. Продолжим начатое исследование.

Пусть X_n — множество всех булевых функций от n переменных, которые можно представить в виде суммы двух бент-функций, т. е.

$$X_n=\bigcup_{f\in\mathcal{B}_n}(\mathcal{B}_n+f).$$

Кратностью покрытия булевой функции h назовем число бент-функций f от n переменных, таких, что h принадлежит множеству $\mathcal{B}_n+f$. Обозначим кратность функции через $m(f)$. Несложно заметить, что $\sum\limits_{f\in X_n} m(f)=|\mathcal{B}_n|^2$.

Доказаны следующие утверждения.

Теорема 1. Справедливо $|\mathcal{BI}_{n+2}|=\sum\limits_{f\in X_n} m(f)^2$.

Теорема 2. Выполняется $|\mathcal{BI}_{n+2}|\geqslant|\mathcal{B}_n|^4/|X_n|$.

Таким образом, из задачи нахождения числа всех итеративных бент-функций от n переменных возникают следующие вопросы.

Открытые вопросы. Какие булевы функции от n переменных могут быть представлены в виде суммы двух бент-функций? Сколько различных таких представлений имеет булева функция? Как распределены числа $m(f)$?

Заметим, что поскольку степень каждой бент-функции от n переменных не выше $n/2$, то множество X_n также содержит только функции степени не выше $n/2$, т. е. $|X_n|\leqslant 2^{1+n+\binom{n}{2}+\ldots+\binom{n}{n/2}}=2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$. Проверено, что при $n=2,4,6$ множество X_n содержит *все* булевы функции степени не выше $n/2$. Сформулируем следующую сильную гипотезу.

Гипотеза 1. Каждая булева функция от n переменных степени не больше $n/2$ представима в виде суммы двух бент-функций от n переменных.

Если гипотеза 1 верна, то из нее практически сразу следует справедливость следующей гипотезы об асимптотике числа всех бент-функций.

Гипотеза 2. Число всех бент-функций от n переменных асимптотически равно $2^{2^{n-c}+d\binom{n}{n/2}}$, где c, d — некоторые константы, причем $1 \leqslant c \leqslant 2$.

Гипотеза 2 означает, что число всех бент-функций скорее ближе к тривиальной верхней оценке их числа (в грубом приближении 2^{2^n}), чем к нижней (около $2^{2^{(n/2)+\log(n-2)-1}}$).

С другой стороны, возникают гипотезы, отражающие роль множества итеративных бент-функций в классе всех бент-функций. Проверено, что при малых n, равных $2, 4, 6$, оценка теоремы 2 становится всё более точной.

Например, для последнего случая ($n = 6$) с привлечением методов Монте-Карло вычислено с малой погрешностью значение $|\mathcal{BI}_8|$, а именно показано, что с вероятностью 0,999 выполняется $2^{87{,}36} < |\mathcal{BI}_8| < 2^{87{,}38}$, тогда как по оценке теоремы 2 имеем $|\mathcal{BI}_8| > 197\,004\,891\,331\,091\,000\,000\,000\,000 \approx 2^{87{,}35}$.

Гипотеза 3. Оценка теоремы 2 асимптотически точна, т. е. справедливо

$$\lim_{n\to\infty} \frac{\log\log|\mathcal{BI}_{n+2}|}{\log\log(|\mathcal{B}_n|^4/|X_n|)} = 1.$$

Сформулируем также следующую гипотезу, смысл которой неформально сводится к тому, что «поведение» класса всех бент-функций определяется лишь итеративными бент-функциями.

Гипотеза 4. Класс $\mathcal{BI}_n$ является *базовым классом* в множестве $\mathcal{B}_n$, т. е. выполняется

$$\lim_{n\to\infty} \frac{\log\log|\mathcal{BI}_n|}{\log\log|\mathcal{B}_n|} = 1.$$

ЛИТЕРАТУРА

1. *Canteaut A. and Charpin P.* Decomposing Bent Functions // IEEE Trans. Inform. Theory. 2003. V. 49. P. 2004–2019.
2. *Токарева Н. Н.* Новая комбинаторная конструкция бент-функций // Прикладная дискретная математика. Приложение. 2010. № 3. С. 13–14.
3. *Tokareva N.* On the number of bent functions: lower bounds and hypotheses // Crypto Archive 2011, Report 083. `http://eprint.iacr.org/2011/083.pdf`.