фиксированного оптимального алгоритма, порождающей какое-либо доопределение слова $\mathbf{x}$. Эта величина задана с точностью до аддитивной константы: сложности $K(\mathbf{x})$ и $K'(\mathbf{x})$ по различным оптимальным алгоритмам удовлетворяют соотношению $K(\mathbf{x}) \approx K'(\mathbf{x})$, где $f \approx g$ означает, что разность $f - g$ ограничена [1]. Будем говорить, что алфавит A *алгоритмически сильнее* алфавита B, и записывать $A \succsim_a B$, если для любых соответственных последовательностей $\mathbf{a}$ и $\mathbf{b}$ выполнено $K(\mathbf{ab}) \approx K(\mathbf{a})$.

Теорема 1. Введенные соотношения недоопределенных алфавитов по силе эквивалентны, т. е.

$$A \succsim_f B \Leftrightarrow A \succsim_c B \Leftrightarrow A \succsim_s B \Leftrightarrow A \succsim_a B.$$

С учётом теоремы будем применять запись $A \succsim B$ без уточнения смысла, в каком она понимается. Будем алфавиты A и B называть *равносильными* и записывать $A \eqsim B$, если $A \succsim B$ и $B \succsim A$.

Теорема 2. Для соответственных алфавитов A и B существуют полиномиальные алгоритмы проверки соотношений $A \succsim B$ и $A \eqsim B$.

Задача сжатия недоопределённых последовательностей ставится как задача такого их кодирования, которое обеспечивает для каждой из них возможность восстановления какого-либо доопределения [2]. Если $\mathbf{a}$ и $\mathbf{b}$ — соответственные последовательности в равносильных алфавитах A и B, то кодирование для $\mathbf{a}$ может рассматриваться и как кодирование для $\mathbf{b}$, поскольку доопределение $\mathbf{a}^0$, найденное по коду для $\mathbf{a}$, позволяет получить доопределение для $\mathbf{b}$ в виде $F(\mathbf{a}^0)$ (см. функциональный подход). Если кодирование для $\mathbf{a}$ оптимально, оно оптимально и для $\mathbf{b}$. За счёт перехода к равносильному алфавиту иногда удаётся упростить процедуру оптимального кодирования.

ЛИТЕРАТУРА

1. *Колмогоров А. Н.* Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 1965. Т. 1. № 1. С. 3–11.
2. *Шоломов Л. А.* Элементы теории недоопределенной информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.

УДК 519.7

ВЕКТОРНЫЕ БУЛЕВЫ ФУНКЦИИ НА РАССТОЯНИИ ОДИН ОТ APN-ФУНКЦИЙ

Г. И. Шушуев

Доказано, что на расстоянии один от произвольной APN-функции все функции являются дифференциально 4-равномерными.

Ключевые слова: *векторная булева функция, дифференциально δ-равномерная функция, APN-функция.*

В работе исследуются метрические свойства класса векторных булевых функций, а именно APN-функций. Знание метрических свойств позволяет получать конструкции таких функций, а также сокращать перебор при поиске функций, обладающих определённым свойством. Например, метрические свойства класса бент-функций исследовались в работах [1, 2].

В 1994 г. K. Nyberg [3] было введено понятие дифференциально δ-равномерных векторных булевых функций (differentially δ-uniform). Векторная булева функция

$F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ называется *дифференциально δ-равномерной*, если при любом ненулевом векторе $a \in \mathbb{Z}_2^n$ и произвольном векторе b уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений, где δ — целое число.

Для векторной функции F и любого ненулевого вектора a определим множество

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

Максимальная достижимая мощность множества $B_a(F)$ равна 2^{n-1}. В частности, если при любом ненулевом векторе a выполнено $|B_a(F)| = 2^{n-1}$, то функция F является APN, а если выполнено $|B_a(F)| \geqslant 2^{n-1} - 1$, то дифференциально 4-равномерной. Минимальное δ, при котором функция является дифференциально δ-равномерной, назовём *порядком* дифференциальной равномерности. *Расстоянием* между векторными булевыми функциями F и G называется мощность множества $\{x \in \mathbb{Z}_2^n : F(x) \neq G(x)\}$.

Утверждение 1. Пусть F — APN-функция от n переменных. Тогда все функции на расстоянии один от F являются дифференциально 4-равномерными.

Доказательство. Пусть F — APN-функция. Тогда при любом ненулевом векторе $a \in \mathbb{Z}_2^n$ выполнено равенство $|B_a(F)| = 2^{n-1}$. Рассмотрим функцию G, совпадающую с F во всех точках, кроме некоторого $x_1 \in \mathbb{Z}_2^n$. Пусть

$$\overline{B_a}(G) = \{G(x) \oplus G(x \oplus a) : x \in \mathbb{Z}_2^n \backslash \{x_1, x_1 \oplus a\}\}.$$

При любом ненулевом векторе $a \in \mathbb{Z}_2^n$ множество $\overline{B_a}(F)$ совпадает с $\overline{B_a}(G)$ и выполнено равенство $|\overline{B_a}(G)| = 2^{n-1} - 1$.

Заметим, что $B_a(G) = \overline{B_a}(G) \cup \{G(x_1) \oplus G(x_1 \oplus a)\}$. Тогда для любого значения $G(x_1)$, в том числе отличного от $F(x_1)$, и при любом ненулевом $a \in \mathbb{Z}_2^n$ выполнено $|B_a(G)| \geqslant$ $\geqslant |\overline{B_a}(G)| = 2^{n-1} - 1$, т. е. функция G является дифференциально 4-равномерной. ■

Гипотеза. Пусть F — APN-функция от n переменных. Тогда все функции на расстоянии один от F являются дифференциально равномерными порядка 4.

Другими словами, на расстоянии один от APN-функций не может быть других APN-функций, т. е. минимальное расстояние между APN-функциями не меньше двух. На расстоянии два APN-функции могут быть; например, функции $F =$ $= (0, 0, 1, 2, 1, 4, 2, 4)$ и $G = (0, 0, 1, 2, 1, 4, 4, 2)$ отличаются двумя последними значениями и обе являются APN-функциями.

Заметим, что гипотеза верна, если и только если существует $a \in \mathbb{Z}_2^n$, для которого выполнено равенство $|B_a(G)| = |\overline{B_a}(G)|$. Для этого требуется, чтобы сумма $G(x_1) \oplus$ $\oplus\, G(x_1 \oplus a)$ принадлежала множеству $\overline{B_a}(G)$.

ЛИТЕРАТУРА

1. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
2. *Коломеец Н. А.* Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. операций. 2012. Т. 19. № 1. С. 41–58.
3. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.