

Имеет место следующее утверждение, которое представляет в некотором роде обратный результат.

**Утверждение 2.** Пусть  $\varepsilon \in \{-1, 1\}$  и весовая структура функции  $F$  для некоторого  $c \in P$  описывается значениями

$$\begin{aligned}\forall a \in P \setminus \{c\} \quad (N_a(F) = q^{n-1} + \varepsilon q^{n/2-1}), \\ N_c(F) = q^{n-1} - \varepsilon(q-1)q^{n/2-1}.\end{aligned}$$

Тогда значение периода функции  $F$  делится на величину  $q^{n/2} - \varepsilon$ .

Представленные утверждения позволяют в ряде случаев указать точные значения весовой структуры  $q$ -ичных бент-функций. Однако, как показывает следующее утверждение, область действия данных результатов существенно ограничена.

**Утверждение 3.** Пусть  $H$  — множество всех гомоморфизмов из группы  $(Q, +)$  в группу  $(P, +)$ . Множество функций  $\{F + h : h \in H\}$  содержит не более одной функции, период которой строго меньше  $q^n - 1$ .

Таким образом, среди бент-функций вида  $F + h$  (где  $h$  — гомоморфизм соответствующих групп) не более одной функции может иметь период, значение которого удовлетворяет условиям теоремы 2.

## ЛИТЕРАТУРА

1. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишкин В. А., Шишков А. Б. Бент-функции и гипербент-функции над полем из  $2^l$  элементов // Проблемы передачи информации. 2008. Т. 44. Вып. 1. С. 15–37.
2. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. операций. 2010. Т. 17. Вып. 1. С. 34–64.
3. Солодовников В. И. Бент-функции из конечной абелевой группы // Дискретная математика. 2002. Т. 14. Вып. 1. С. 99–113.
4. Кузьмин А. С., Нечаев А. А., Шишкин В. А. Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. С. 86–111.

УДК 621.391: 519.728

## О СРАВНЕНИИ НЕДООПРЕДЕЛЕННЫХ АЛФАВИТОВ<sup>1</sup>

Л. А. Шоломов

Представлены несколько подходов к сравнению недоопределённых алфавитов по силе и доказана их эквивалентность. Установлено, что введённые соотношения по силе полиномиально проверяемы.

**Ключевые слова:** недоопределённый алфавит, равносильные алфавиты, энтропия недоопределённых данных, сложность по Колмогорову.

Задан конечный алфавит  $A_0 = \{a_i : i \in M\}$  основных символов. Каждому непустому  $T \subseteq M$  соответствует недоопределённый символ  $a_T$ , доопределением которого считается всякий основной символ  $a_i$ ,  $i \in T$ . Выделена система  $\mathcal{T} \subseteq 2^M$  некоторых подмножеств  $T \subseteq M$  и с ней связан недоопределённый алфавит  $A = \{a_T : T \in \mathcal{T}\}$ .

Пусть помимо  $A_0$  и  $A$  заданы основной алфавит  $B_0 = \{b_j : j \in L\}$ , недоопределённый алфавит  $B = \{b_U : U \in \mathcal{U} \subseteq 2^L\}$  и соответствие  $R_{AB} \subseteq A \times B$ , указывающее,

<sup>1</sup>Работа поддержана ОНИТ РАН по программе фундаментальных исследований.

каким образом символы алфавитов  $A$  и  $B$  взаимно сопоставлены друг другу (символам одного алфавита могут соответствовать несколько символов другого). Назовём алфавиты  $A$  и  $B$  с заданным для них соответствием  $R_{AB}$  *соответственными алфавитами*; последовательности  $\mathbf{a} = a_{T_1} \dots a_{T_n}$  и  $\mathbf{b} = b_{U_1} \dots b_{U_n}$ , для которых  $(a_{T_i}, b_{U_i}) \in R_{AB}$ ,  $i = 1, \dots, n$ , *соответственными последовательностями*.

В работе представлено несколько подходов к сравнению соответственных недоопределённых алфавитов по силе. Первый из них — функциональный — основан на функциональной выразимости символов одного алфавита через символы другого. Следующие три подхода терминологически связаны с подходами к введению меры информации, представленными в работе А. Н. Колмогорова [1]. Это комбинаторный, вероятностный (статистический) и алгоритмический подходы. Доказано, что все подходы приводят к одному и тому же соотношению алфавитов по силе.

**Функциональный подход.** Скажем, что алфавит  $B$  функционально выразим через  $A$ , если существует функция  $F : A_0 \rightarrow B_0$ , такая, что для всех пар  $(a_T, b_U) \in R_{AB}$  выполнено  $F(a_T) \subseteq b_U$ , где  $F(a_T) = \{F(a_i) : i \in T\}$ ,  $b_U = \{b_j : j \in U\}$ . Будем говорить, что алфавит  $A$  функционально сильнее  $B$ , и записывать  $A \succsim_f B$ , если  $B$  функционально выразим через  $A$ . Соотношение  $A \succsim_f B$  может быть эквивалентно представлено в терминах соответственных последовательностей, а именно:  $A \succsim_f B$  тогда и только тогда, когда существует такая функция  $F : A_0 \rightarrow B_0$ , что для всякой пары  $\mathbf{a} = a_{T_1} \dots a_{T_n}$ ,  $\mathbf{b} = b_{U_1} \dots b_{U_n}$  соответственных последовательностей и любого доопределения  $\mathbf{a}^0 = a_{i_1} \dots a_{i_n}$  последовательности  $\mathbf{a}$  последовательность  $F(\mathbf{a}^0) = F(a_{i_1}) \dots F(a_{i_n})$  доопределяет  $\mathbf{b}$ . В терминах соответственных последовательностей будут даны и последующие определения.

**Комбинаторный подход.** Для последовательности  $\mathbf{a}$  в алфавите  $A$  введём класс  $\mathcal{K}(\mathbf{a})$  всех последовательностей в алфавите  $A$ , в которых каждый символ  $a_T \in A$  встречается такое же, как в  $\mathbf{a}$  число раз. Обозначим через  $N(\mathbf{a})$  минимальную мощность множества последовательностей в основном алфавите  $A_0$ , среди которых имеются доопределения всех последовательностей из  $\mathcal{K}(\mathbf{a})$ . Аналогично, паре последовательностей  $\mathbf{a} = a_{T_1} \dots a_{T_n}$  и  $\mathbf{b} = b_{U_1} \dots b_{U_n}$  сопоставим класс  $\mathcal{K}(\mathbf{a}, \mathbf{b})$  всех пар последовательностей с теми же кратностями появления пар  $(a_T, b_U) \in A \times B$ , что и в  $(\mathbf{a}, \mathbf{b})$ , и минимальную мощность  $N(\mathbf{a}, \mathbf{b})$  доопределяющего  $\mathcal{K}(\mathbf{a}, \mathbf{b})$  множества пар. Будем считать, что алфавит  $A$  комбинаторно сильнее алфавита  $B$ , и записывать  $A \succsim_c B$ , если для любых соответственных последовательностей  $\mathbf{a}$  и  $\mathbf{b}$  выполнено  $N(\mathbf{a}, \mathbf{b}) = N(\mathbf{a})$ .

**Статистический подход.** Будем рассматривать недоопределённые источники  $X$  в алфавите  $A$ , порождающие независимо символы  $a_T \in A$  с некоторыми вероятностями  $p_T$ . Определим энтропию  $\mathcal{H}(X)$  источника  $X$ , положив

$$\mathcal{H}(X) = \min_Q \left\{ - \sum_{T \in \mathcal{T}} p_T \log_2 \sum_{i \in T} q_i \right\},$$

где минимум берётся по наборам  $Q = (q_i, i \in M)$  вероятностей символов  $a_i$  основного алфавита  $A_0$ . О свойствах и роли этой энтропии см. в [2]. Источники  $X$  и  $Y$  в алфавитах  $A$  и  $B$ , заданные совместным распределением  $p(a_T, b_U)$ ,  $a_T \in A$ ,  $b_U \in B$ , назовём *соответственными*, если  $p(a_T, b_U) > 0$  лишь в случае  $(a_T, b_U) \in R_{AB}$ . Будем говорить, что алфавит  $A$  статистически сильнее алфавита  $B$ , и записывать  $A \succsim_s B$ , если для любых пар соответственных источников  $X$  и  $Y$  выполнено  $\mathcal{H}(XY) = \mathcal{H}(X)$ .

**Алгоритмический подход.** Модифицируя применительно к недоопределённым данным систему понятий из [1], назовём *колмогоровской сложностью*  $K(\mathbf{x})$  недоопределённого слова  $\mathbf{x}$  минимальную длину двоичной программы для произвольно

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  $A \approx B$ , 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  $A \approx B$ .

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  $\delta$ -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. К. Nyberg [3] было введено понятие дифференциально  $\delta$ -равномерных векторных булевых функций (differentially  $\delta$ -uniform). Векторная булева функция