

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

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

Заметим, что если функция обладает свойством k -существенной зависимости, то она также является l -существенно 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 $n \geq 8$, где $t \leq n/2$, 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 $(n+3)/3 \leq t \leq n/2$ функция является $(t-2)$ -существенно зависимой.

ЛИТЕРАТУРА

1. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения // Saarbrücken, 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 ДАННЫХ¹

Л. А. Шоломов

Задан алфавит $A_0 = \{a_0, a_1, \dots, a_{m-1}\}$ основных символов. Пусть $M = \{0, 1, \dots, m-1\}$ 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

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

¹Работа 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 $Q = (q_i, i \in M)$, $q_i \geq 0$, $\sum_{i \in M} q_i = 1$, 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 $X \succeq Y$, если $XY \approx X$. Можно показать, что $X \approx Y$ тогда и только тогда, когда $X \succeq Y$ и $X \preceq Y$. Существуют эффективные (т. е. полиномиальные) алгоритмы проверки соотношений $X \approx Y$ и $X \succeq Y$. 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 $X_1 \cdot \dots \cdot X_s$ 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 $\tilde{X} \preceq X$ и для всякого разложения $\tilde{X}'$, такого, что $\tilde{X}' \preceq X$, выполнено $\tilde{X} \succeq \tilde{X}'$. 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 , $i = 1, \dots, s$, назовем *устранимым* из разложения $X_1 \cdot \dots \cdot X_s$, если

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

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 $\tilde{X} = X_1 \cdot \dots \cdot X_s$, 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 неуллучшаема.

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.