ПДМ. Приложение. 2009. № 2.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

5–17

Токарева Н. Н. Бент-функции и их обобщения // ПДМ. Приложение. 2009. № 2. С. 5–17.

18–42

Шоломов Л. А. Элементы теории недоопределенной информации // ПДМ. Приложение. 2009. № 2. С. 18–42.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

43–73

Агибалов Г. П. Конечные автоматы в криптографии // ПДМ. Приложение. 2009. № 2. С. 43–73.

74–114

Скобелев В. Г. Комбинаторно-алгебраические модели в криптографии // ПДМ. Приложение. 2009. № 2. С. 74–114.

115–150

Черемушкин А. В. Криптографические протоколы: основные свойства и уязвимости // ПДМ. Приложение. 2009. № 2. С. 115–150.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

151–190

Девянин П. Н. Обзорные лекции по моделям безопасности компьютерных систем // ПДМ. Приложение. 2009. № 2. С. 151–190.

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

№2 ПРИЛОЖЕНИЕ Ноябрь 2009

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

БЕНТ-ФУНКЦИИ И ИХ ОБОБЩЕНИЯ[1]

Н. Н. Токарева

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

E-mail: tokareva@math.nsc.ru

Лекция посвящена бент-функциям — булевым функциям, максимально удаленным в метрике Хэмминга от множества всех аффинных функций. Это экстремальное свойство определяет большое число приложений бент-функций в самых разных областях. Рассматриваются также обобщения бент-функций.

Ключевые слова: *бент-функция, обобщения бент-функций.*

Введение

Бент-функции впервые были введены О. Ротхаусом в 60-х годах XX века. Выпускник Принстонского университета Оскар Ротхаус (1927–2003) после службы во время Корейской войны в войсках связи поступил на работу математиком в Агентство Национальной Безопасности США. С 1960 по 1966 г. он работал в Институте оборонного анализа (IDA). Его криптографические работы того времени оценивались руководством IDA достаточно высоко. Как и его преподавательская деятельность: «he was one of the most important teachers of cryptology to mathematicians and mathematics to cryptologists» [8]. На это же время приходится и его первая работа о бент-функциях [36]. В открытой печати она появилась только в 1976 г. [37]. В ней были установлены базовые свойства бент-функций, предложены их простейшие конструкции и намечена классификация бент-функций от шести переменных.

В настоящее время бент-функции и их приложения изучаются очень активно.

Семейства бент-последовательностей из элементов $+1$ и -1, построенные на основе бент-функций, имеют предельно низкие значения как взаимной корреляции, так и автокорреляции (достигают нижней границы Велча). Такие семейства успешно применяются в коммуникационных системах коллективного доступа, а также в работе со стандартом CDMA. Технология цифровой сотовой связи CDMA (Code Division Multiple Access — множественный доступ с кодовым разделением каналов) была стандартизована в 1993 г. американской телекоммуникационной промышленной ассоциацией (US TIA) в виде стандарта IS–95. В настоящее время технология используется большинством поставщиков беспроводного оборудования во всем мире согласно стандартам IMT–2000 мобильной связи третьего поколения (в России — стандарты IMT–MC 450 или CDMA–450). В системах CDMA для предельного снижения отношения пиковой и

[1]Работа выполнена при финансовой поддержке гранта Президента РФ для молодых российских ученых (МК-1250.2009.1), Российского фонда фундаментальных исследований (проекты 07-01-00248, 08-01-00671, 09-01-00528), Фонда содействия отечественной науке, ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (гос. контракт 02.740.11.0429).

средней мощностей сигнала (peak-to-average power ratio) используются коды постоянной амплитуды. Их построение напрямую связано с выбором специального подмножества бент-функций.

В блочных и поточных шифрах бент-функции и их векторные аналоги способствуют предельному повышению стойкости этих шифров к линейному и дифференциальному методам криптоанализа. Стойкость достигается за счет использования сильно нелинейных булевых функций в S-блоках (см., например, шифр CAST). Бент-функции и их обобщения находят свое применение также в схемах аутентификации, хэш-функциях (см. HAVAL) и псевдослучайных генераторах. См. также пример использования бент-функций в поточном шифре Grain.

Несмотря на высокий интерес к бент-функциям, прогресс в их изучении самый минимальный. Для мощности класса бент-функций не найдена асимптотика, не установлено приемлемых нижних и верхних оценок. Мало изучены и их обобщения, возникающие из новых постановок прикладных задач.

Данная лекция построена на основе двух обзоров автора [5, 6] и по сути является их кратким конспектом. Приводятся основные свойства, конструкции, эквивалентные представления бент-функций. Значительное внимание уделяется обобщениям бент-функций. В конце статьи приводятся открытые вопросы в этой области.

Нам потребуются следующие определения и обозначения:

q, n — натуральные числа;

$+$ — сложение по модулю q;

$x = (x_1, \ldots, x_n)$ — q-значный вектор;

$\mathbb{Z}_q^n$ — множество всех q-значных векторов длины n;

$\mathbb{F}_{q^n}$ — поле Галуа порядка q^n;

$\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n$ — скалярное произведение векторов;

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — булева функция от n переменных;

$\boldsymbol{f}$ — вектор значений длины 2^n функции f. Будем считать, что аргументы функции (т. е. векторы длины n) перебираются в лексикографическом порядке;

$\mathrm{dist}(f, g)$ — *расстояние Хэмминга* между функциями f и g, т. е. число позиций, в которых различаются векторы $\boldsymbol{f}$ и $\boldsymbol{g}$;

АНФ — *алгебраическая нормальная форма* функции;

$\deg(f)$ — *степень нелинейности* булевой функции f, т. е. число переменных в самом длинном слагаемом ее АНФ;

$W_f(y) = \sum\limits_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle + f(x)}$ — преобразование Уолша—Адамара булевой функции f;

N_f — *нелинейность* булевой функции f, т. е. расстояние Хэмминга от данной функции до множества всех аффинных функций;

максимально нелинейная функция — булева функция с максимально возможным значением N_f;

бент-функция (n чётное) — булева функция, такая, что все её коэффициенты Уолша—Адамара равны $\pm 2^{n/2}$;

$\mathfrak{B}_n$ — класс бент-функций от n переменных;

аффинно эквивалентные функции f и g от n переменных: существуют невырожденная $n \times n$-матрица A, векторы b, c длины n и константа $\lambda \in \mathbb{Z}_2$, такие, что $g(x) = f(Ax + b) + \langle c, x\rangle + \lambda$.