6. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.
7. *Gligoroski D., Markovski S., Kocarev L., and Gusev M.* Edon80 // `http://www.ecrypt.eu.org/stream/edon80p3.html`
8. *Lai X. and Massey J.* A Proposal for a New Block Encryption Standard // Adv. Cryptology — EUROCRYPT'90. New York: Springer Verlag, 1991. P. 55–70.
9. *Cooper J., Donovan D., and Seberry J.* Secret Sharing Schemes Arising From Latin Squares // Bulletin of the ICA. 1994. V. 12. P. 33–43.
10. *Chum C. S. and Zhang X.* The Latin squares and the secret sharing schemes // Groups Complex. Cryptol. 2010. V. 2. P. 175–202.
11. *Chum C. S.* Hash functions, Latin squares and secret sharing schemes. New York: ProQuest, 2010.
12. *Pal S. K., Bhardwaj D., Kumar R., and Bhatia V.* A New Cryptographic Hash Function based on Latin Squares and Non-linear Transformations // Adv. Comput. Conf. IACC, 2009. P. 862–867.
13. *Gligoroski D., Ødegård R. S., Mihova M., et al.* Cryptographic Hash Function Edon-R // Proc. IWSCN, 2009. P. 1–9.
14. *Dènes J. and Dènes T.* Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack // Quasigroups and Related Systems. 2001. No. 8. P. 7–14.
15. *Shcherbacov V. A.* Quasigroups in cryptology // Comput. Sci. J. Moldova. 2009. V. 17. No. 2(50). P. 193–228.

УДК 519.7

СВОЙСТВО КРАТНЫХ ПРОИЗВОДНЫХ БЕНТ-ФУНКЦИЙ КАСАМИ[1]

А. А. Фролова

Одно из криптографических свойств булевой функции — это высокая нелинейность. Булевы функции, обладающие экстремальной нелинейностью, при чётном числе переменных называются *бент-функциями*. Описание класса всех бент-функций от произвольного числа переменных остается открытой проблемой, однако известны некоторые конструкции бент-функций [1]. Одна из них — алгебраическая конструкция Касами. Булева функция от n переменных рассматривается как функция над конечным полем $\mathrm{GF}(2^n)$. Любая булева функция f от n переменных может быть представлена с помощью функции *следа* $\mathrm{tr}(\beta) : \mathrm{GF}(2^n) \to \mathrm{GF}(2)$ следующим образом (см. подробнее [2]):

$$f(\beta) = \mathrm{tr}(\sum_{j=0}^{2^n-1} a_j \beta^j), \text{ где } a_j \in \mathrm{GF}(2^n), \text{ а } \mathrm{tr}(\beta) = \sum_{i=0}^{n-1} \beta^{2^i} \text{ для любого } \beta \in \mathrm{GF}(2^n).$$

Определение 1. Булева функция от n переменных (n чётное) вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ называется *булевой функцией Касами*, если выполнено условие

1) $k = 2^{2d} - 2^d + 1$, где $(n, d) = 1,\ 0 < d < n$.

Если к тому же выполнено условие

2) λ не принадлежит множеству $\{\gamma^3 : \gamma \in \mathrm{GF}(2^n)\}$,

то f является бент-функцией и называется *бент-функцией Касами*.

[1]Исследование выполнено при поддержке гранта РФФИ, проект № 11-01-00997.

В работе [3] показано, что при выполнении условия 2 функция Касами является бент, однако впервые (при ограничении, что число переменных n не делится на три) это доказано в работе Дж. Диллона и Х. Доббертина в 2004 г. [4]. Бент-функции Касами являются наиболее сложными из мономиальных конструкций (т. е. конструкций вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$). Степень функции Касами от n переменных может принимать все возможные чётные значения вплоть до $n/2$ (заметим, что максимальная степень бент-функции от n переменных равна $n/2$). Известно, что они не аффинно эквивалентны своим дуальным функциям и бент-функциям из классов PS и Майорана — МакФарланда. Кроме того, известно, что в классе бент-функций Касами существуют функции, не являющиеся нормальными, т. е. тождественно равными константе на некотором аффинном подпространстве размерности $n/2$.

Однако до сих пор не известна связь между алгебраическим и комбинаторным представлениями бент-функций. В данной работе исследуются комбинаторные свойства бент-функций Касами. Получен результат о кратных производных функций Касами, следствием которого является свойство зависимости алгебраической нормальной формы (АНФ) функции от произведений переменных.

Будем рассматривать конечное поле $\mathrm{GF}(2^n)$ как векторное пространство размерности n.

Определение 2. *Производная по направлению* $a \in \mathrm{GF}(2^n)$ булевой функции f определяется как $D_a f(\beta) = f(\beta) + f(\beta + a)$ для любого $\beta \in \mathrm{GF}(2^n)$.

Авторами [5] исследована вторая производная бент-функций Касами и доказана теорема о том, что для любых ненулевых различных направлений $a, b \in \mathrm{GF}(2^n)$ производная $D_a D_b f$ бент-функции Касами не равна тождественно нулю при степени функции $\deg(f) \geqslant 4$ и числе переменных $n \geqslant 8$.

В данной работе доказана следующая

Теорема 1. Пусть $f(\beta)$ — булева функция Касами от n переменных вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $k = 2^{2d} - 2^d + 1$, $0 < d < n$, n чётное. Тогда для любого $n \geqslant 8$ справедливы следующие утверждения:

(i) при $\deg(f) = t$, где $4 \leqslant t \leqslant n/2$, производная $D_{a_1} \dots D_{a_{t-3}} f(\beta)$ не равна тождественно нулю для любых линейно независимых векторов $a_1, \dots, a_{t-3} \in \mathrm{GF}(2^n)$;

(ii) при $\deg(f) = t$, где $4 \leqslant t \leqslant (n+3)/3$, производная $D_{a_1} \dots D_{a_{t-2}} f(\beta)$ не равна тождественно нулю для любых линейно независимых векторов $a_1, \dots, a_{t-2} \in \mathrm{GF}(2^n)$.

Вводится следующее понятие.

Определение 3. Булева функция называется *k-существенно зависимой*, если для любого произведения из k различных переменных существует моном в АНФ функции, содержащий это произведение.

Заметим, что булева функция f является k-существенно зависимой, если для любых различных векторов $a_1, \dots, a_k \in \mathrm{GF}(2^n)$ вида $a_i = (0, \dots, 0, 1, 0, \dots, 0)$, содержащих 1 в координате s_i, где $0 \leqslant s_i \leqslant (n-1)$, $1 \leqslant i \leqslant k$, кратная производная $D_{a_1} \dots D_{a_k} f(\beta)$ не равна тождественно нулю.

Следствием результата в [5] и теоремы 1 является следующая

Теорема 2. Пусть $f(\beta)$ — булева функция Касами от n переменных вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $k = 2^{2d} - 2^d + 1$, $0 < d < n$, n чётное. Тогда для любого $n \geqslant 8$ справедливы следующие утверждения:

(i) при $\deg(f) \geqslant 4$ функция f является 2-существенно зависимой;

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

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

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

ЛИТЕРАТУРА

1. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения // Saarbrucken, 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 ДАННЫХ[1]

Л. А. Шоломов

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

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

[1]Работа выполнена при поддержке ОНИТ РАН по проекту 1.1 программы «Интеллектуальные информационные технологии, системный анализ и автоматизация».