Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/10/12

О НЕКОТОРЫХ СВЯЗЯХ РАСЩЕПЛЯЕМОСТИ БУЛЕВЫХ ФУНКЦИЙ С ИХ АЛГЕБРАИЧЕСКИМИ, КОМБИНАТОРНЫМИ И КРИПТОГРАФИЧЕСКИМИ СВОЙСТВАМИ

А. А. Бабуева

Получены верхняя оценка алгебраической степени аффинно-расщепляемой функции, достаточные условия аффинной расщепляемости дуальной бент-функции. Для функций, обладающих нетривиальным пространством линейных структур, получена верхняя оценка нелинейности.

Ключевые слова: *булевы функции, бент-функции, аффинная расщепляемость.*

Понятие сужения булевой функции активно используется как в синтезе, так и в анализе криптографических функций. В качестве основных причин исследований этого понятия можно назвать следующие:

— анализ свойств булева отображения удобно проводить, используя семейство сужений этого отображения на специальным образом подобранное множество областей;
— существует тесная связь свойств сужений и исходного булева отображения (в том числе и наследование свойств).

В работе исследованы свойства сужений бент-функций и аффинно-расщепляемых функций. Бент-функцию можно определить как функцию, которая плохо аппроксимируется аффинными функциями. В блочных и поточных шифрах бент-функции и их векторные аналоги используются для синтеза криптографических отображений, устойчивых к ряду методов криптографического анализа. Свойство аффинной расщепляемости по некоторому подпространству [1] говорит о том, что сужение булевой функции на любой сдвиг этого подпространства совпадает с некоторой аффинной функцией. Если криптографическая функция является аффинно-расщепляемой, то задача её исследования заметно упрощается. Поэтому исследование сужений именно бент-функций и аффинно-расщепляемых функций, а также вопрос о том, может ли бент-функция быть аффинно-расщепляемой, представляет особый интерес. В работе рассматриваются такие параметры булевых функций, как нелинейность, алгебраическая степень, спектр Уолша — Адамара, нормальность, слабая нормальность.

Получены следующие результаты.

1) Доказано соотношение, связывающее величины квадратов коэффициентов неполного преобразования Уолша — Адамара функции на смежных классах по подпространству с квадратами коэффициентов Уолша — Адамара исходной функции (сформулировано в [2]).

Теорема 1. Пусть f — булева функция от n переменных, L — подпространство V_n размерности d, $u \in V_n$. Тогда

$$\sum_{i=1}^{2^{n-d}} \Big(\sum_{x \in v_i \oplus L} (-1)^{f(x) \oplus \langle u,x \rangle} \Big)^2 = \frac{1}{2^{n-d}} \sum_{y \in u \oplus L^\perp} W_f^2(y),$$

где $v_1, \ldots, v_{2^{n-d}}$ — представители смежных классов $\{L \oplus v : \ v \in V_n\}$.

2) Доказано равенство значений коэффициентов неполного преобразования Уолша — Адамара бент-функции и дуальной к ней функции на нулевом наборе.

Теорема 2. Пусть f — бент-функция, L — самодуальное подпространство. Тогда

$$\sum_{x \in L} (-1)^{f(x)} = \sum_{x \in L} (-1)^{\widetilde{f}(x)}.$$

3) Доказано, что если бент-функция нормальна (слабо нормальна), то и дуальная ей функция нормальна (слабо нормальна). Булеву функцию f от n переменных будем называть нормальной (слабо нормальной), если существует плоскость $\pi = L \oplus u$ размерности $n/2$, такая, что f является константой (аффинной) на этой плоскости.

4) Получена верхняя оценка алгебраической степени аффинно-расщепляемой функции.

Теорема 3. Пусть f — аффинно-расщепляемая по подпространству L функция от n переменных, $\dim L = r$. Тогда $\deg(f) \leqslant n - r + 1$.

5) Доказано, что свойство аффинной расщепляемости инвариантно относительно полной аффинной группы.

6) Получены достаточные условия аффинной расщепляемости дуальной бент-функции.

Теорема 4. Пусть f — бент–функция от $n = 2k$ переменных и f — аффинно-расщепляемая по подпространству $L \subset V_n$, $\dim L = k$. Если для полных систем представителей смежных классов $\{u^1 \oplus L, \ldots, u^{2^k} \oplus L\}$ и $\{v^1 \oplus L^\perp, \ldots, v^{2^k} \oplus L^\perp\}$ выполнены условия

$$f_{u^i \oplus L}(x) = \langle c^i, x \rangle \oplus \varepsilon^i, \quad c^i \in v^i \oplus L^\perp, \quad \varepsilon^i \in \{0,1\}, \quad i = 1, \ldots, 2^k,$$

то дуальная бент-функция $\widetilde{f}$ аффинно-расщепляема по подпространству $L^\perp$.

7) Получена верхняя оценка нелинейности булевой функции, обладающей нетривиальным пространством L_f линейных трансляторов (структур).

Теорема 5. Пусть булева функция f от n переменных имеет линейную структуру и $\dim L_f = r$. Тогда

$$\mathrm{nl}(f) \leqslant 2^{n-1} - 2^{(n-r)/2-1}.$$

ЛИТЕРАТУРА

1. *Коломеец Н. А.* Бент-функции, аффинные на подпространствах, и их метрические свойства: дис. ... канд. физ.-мат. наук. Новосибирск, 2014. 68 с.
2. *Logachev O. A., Yashchenko V. V., and Denisenko M. P.* Local affinity of Boolean mappings // NATO Science for Peace and Security Series — D: Information and Communication Security. V. 18. Boolean Functions in Cryptology and Information Security. IOS Press, 2008. P. 148–172.