А. В. Иванов (Москва, ТВП). **Зависимость свойств приведенного представления булевой функции от выбора базиса, в котором оно задано.**

Пусть $\mathrm{F}_2 = \mathrm{GF}(2)$ — поле из двух элементов, e — единица F_2, $\mathrm{F}_{2^n} = \mathrm{GF}(2^n)$ — расширение F_2 натуральной степени n, $\mathrm{tr}_t^n(\alpha) = \sum_{k=0}^{n/t-1} \alpha^{2^{tk}}$ — функция след из F_{2^n} в его подполе $\mathrm{F}_{2^t} = \mathrm{GF}(2^t)$, для такого натурального t, что $t|n$.

Результаты получены с использованием представления булевых функций от n переменных в виде многочленов над F_{2^n}, принимающих значения в F_2. Опишем механизм получения подобного представления. Пусть $\varphi(x_0, x_1, \ldots, x_{n-1})$ — булева функция, $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$, $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ — двойственные базисы F_{2^n} как векторного пространства над F_2. Для любого набора $(x_0, x_1, \ldots, x_{n-1}) \in (\mathrm{F}_2)^n$ однозначно определен элемент $x = \sum_{j=0}^{n-1} x_j \varepsilon_j$ поля F_{2^n}. В [1] показано, что существует такой многочлен $\Phi(x) \in \mathrm{F}_{2^n}[x]$, что

$$\varphi(x_0, x_1, \ldots, x_{n-1}) = \mathrm{tr}_1^n\left(\Phi\left(\sum_{j=0}^{n-1} x_j \varepsilon_j\right)\right). \tag{1}$$

При этом $\Phi(x)$ определен однозначно, если он имеет вид

$$\Phi(x) = \sum_{t \in M_n} c_t \xi_t x^t, \tag{2}$$

где M_n — набор минимальных представителей всех различных циклотомических классов множества $1, 2, \ldots, 2^n - 1$ и для каждого t: $r(t) = \min\{k \in \mathbf{N}\colon\ t2^k \equiv t (\mathrm{mod}\, 2^n - 1)\}$, $c_t \in \mathrm{F}_{2^{r(t)}}$, ξ_t — такой фиксированный элемент F_{2^n}, что $\mathrm{tr}_{r(t)}^n(\xi_t) = e$. В этом случае $\Phi(x)$ вида (2) называют *редуцированным многочленом*, а представление (1), где $\Phi(x)$ имеет вид (2), — *приведенным представлением* (далее — tr-*представлением*) для φ в базисе $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$.

Нас будет интересовать свойство удаленности (в смысле расстояния Хемминга между векторами значений) функции от некоторого множества функций — класса приближений. Известно ([2]), что существуют функции от четного числа переменных, равноудаленные от всех линейных — так называемые *бент-функции*.

В [1], [3] исследовались функции, заданные tr-представлением, имеющие равные расстояния до всех собственных мономиальных (редуцированный многочлен tr-представления которых есть моном, задающий подстановку на соответствующем поле). За такими функциями закрепился термин «гипер-бент-функции» или «ГБФ».

Класс бент-функций инвариантен относительно невырожденной линейной замены переменных (см., например, [2]). Основной результат данного доклада демонстрирует отличие свойств ГБФ и бент-функций:

Теорема. 1) *Для любой бент-функции от* 4 *переменных существуют два таких базиса пространства* $(\mathrm{F}_{2^4})_{\mathrm{F}_2}$, *что* tr-*представление данной функции в первом базисе является, а во втором не является ГБФ.*

2) *Для любого* $\lambda > 2$ *существуют функции от* 2λ *переменных, для каждой из которых можно найти два таких базиса пространства* $(\mathrm{F}_{2^{2\lambda}})_{\mathrm{F}_2}$, *что* tr-*представление функции в первом базисе является, а во втором не является ГБФ.*

Работа выполнена при поддержке гранта Президента РФ НШ № 8564.2006.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Кузьмин А. С.*, *Марков В. Т.*, *Нечаев А. А.*, *Шишков А. Б.* Приближение булевых функций мономиальными. — Дискретн. матем., 2006, т. 18 (1), с. 9–29.
2. *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МНЦМО, 2004.

3. *Youssef A. M.*, *Gong G.* Hyper-bent functions. — Proceedings of Advances in Cryptology: EUROCRYPT'2001. Lect. Notes in Comp. Sci. New York: Springer-Verlag, 2001, v. 2045, p. 406–419.