2008 Теоретические основы прикладной дискретной математики № 1(1)

DOI 10.17223/20710410/1/2

УДК 519.651

МОНОМИАЛЬНЫЕ ПРИБЛИЖЕНИЯ ПЛАТОВИДНЫХ ФУНКЦИЙ*

А.В. Иванов

Московский государственный институт радиотехники, электроники и автоматики

E-mail: alexiva@pochta.ru

Рассматриваются вопросы приближения платовидных булевых функций мономиальными. При исследовании свойств платовидных функций используется их представление в виде многочленов над конечным полем. Получены условия, необходимые для того, чтобы расстояние Хэмминга между векторами значений платовидной функции и любой собственной мономиальной принимало не более трех возможных значений.

Ключевые слова: *булевы функции*, *мономиальные приближения булевых функций*, *приведенное представление*, *платовидные функции.*

При решении широкого класса криптографических задач часто возникает необходимость найти приближение двоичной функции из некоторого заданного множества функций. Вероятность совпадения значений аппроксимации со значениями исходной функции при случайном равновероятном выборе аргументов является мерой качества приближения. Как правило, в роли класса приближений рассматривают множество линейных функций. Это связано с тем, что для данного множества удается решить наибольшее количество сопутствующих методу задач – найти наилучшее приближение для заданной функции, получить содержательные оценки качества приближения, описать функции, наихудшим образом приближаемые классом.

Однако в ряде случаев использование нелинейных аппроксимаций позволяет повысить эффективность решения той или иной криптоаналитической задачи. В связи с этим в последнее время предпринимаются попытки расширить класс линейных приближений с целью улучшения точности аппроксимации булевых функций при сохранении других важных характеристик класса.

В работе рассматриваются вопросы приближения платовидных булевых функций мономиальными функциями.

Используются следующие обозначения:

$\mathbb{F}_2 = \mathrm{GF}(2)$ – поле из двух элементов;

e – единица поля $\mathbb{F}_2$;

$\mathbb{F}_{2^n} = \mathrm{GF}(2^n)$ – расширение поля $\mathbb{F}_2$ натуральной степени n;

$\mathrm{tr}_t^n(\alpha) = \sum_{k=0}^{\frac{n}{t}-1} \alpha^{2^{t\cdot k}}$ – функция след из поля $\mathbb{F}_{2^n}$ в его подполе $\mathbb{F}_{2^t} = \mathrm{GF}(2^t)$ для натурального t такого, что $t|n$;

$\overline{t_1, t_2}$, где $t_1, t_2 \in Z$, – множество целых чисел, больших t_1-1 и меньших t_2+1;

$||t||$ – количество единиц в двоичной записи числа t;

$\rho_n(t)$, где $t \in Z$, – число из множества $\overline{1, 2^n-1}$, определяемое условием $\rho_n(t) \equiv t \pmod{2^n-1}$.

Далее, где это необходимо, будем отождествлять ноль и единицу поля $\mathbb{F}_2$ с целыми числами 0 и 1 соответственно. При получении основных результатов использовано представление булевых функций от n переменных в виде многочленов над полем $\mathbb{F}_{2^n}$, принимающих значения в поле $\mathbb{F}_2$. Опишем механизм получения подобного представления.

Пусть $\varphi(x_0, x_1, \ldots, x_{n-1})$ – булева функция от n переменных; $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$, $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ – пара двойственных базисов поля $\mathbb{F}_{2^n}$ как векторного пространства над полем $\mathbb{F}_2$. Для любого набора булевых величин $x_0, x_1, \ldots, x_{n-1}$ однозначно определен элемент $x = \sum_{j=0}^{n-1} x_j \cdot \varepsilon_j$ поля $\mathbb{F}_{2^n}$. В [1] показано, что существует многочлен $\Phi(x)$ над полем $\mathbb{F}_{2^n}$, такой, что

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

* Работа выполнена при поддержке гранта Президента РФ НШ №8564.2006.10.

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

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

где M_n – набор минимальных представителей всех различных циклотомических классов множества чисел $\overline{1, 2^n - 1}$, и для каждого t:

$r(t) = \min\{k \in \mathbb{N} : t \cdot 2^k \equiv t \pmod{2^n - 1}\}$;

c_t – выбирается из поля $\mathbb{F}_{2^{r(t)}}$;

ξ_t – фиксированный элемент поля $\mathbb{F}_{2^n}$, такой, что справедливо соотношение $\mathrm{tr}^n_{r(t)}(\xi_t) = e$.

В этом случае многочлен $\Phi(x)$ вида (2) называют редуцированным многочленом, а представление (1), где многочлен $\Phi(x)$ имеет вид (2), – приведенным представлением для $\varphi(x_0, x_1, \ldots, x_{n-1})$ в базисе $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$.

Индекс нелинейности редуцированного многочлена $\Phi(x)$ вида (2) задается равенством

$$\mathrm{ind}\,\Phi(x) = \max\{||t||: t \in M_n,\ c_t \neq 0\}$$

и совпадает со степенью нелинейности функции $\varphi(x_0, x_1, \ldots, x_{n-1})$.

Использование подобного представления булевых функций в ряде случаев существенно упрощает решение комплекса задач по исследованию классов приближающих функций.

В качестве показателя близости приближающей функции $G(x)$ к исходной функции $F(x)$ будем использовать величину

$$\Delta(F, G) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)+G(x)}. \tag{3}$$

Если $G(x)$ – линейная функция, то $\Delta(F, G)$ есть коэффициент Уолша – Адамара функции $F(x)$. Коэффициенты Уолша – Адамара произвольной функции $F(x) : \mathbb{F}_{2^n} \to \mathbb{F}_2$ удовлетворяют равенству Парсеваля

$$\sum_{\alpha \in \mathbb{F}_{2^n}} \left(\Delta(F, \mathrm{tr}^n_1(\alpha x))\right)^2 = 2^{2n},$$

из которого следует оценка

$$\max\{|\Delta(F, \mathrm{tr}^n_1(\alpha x))| : \alpha \in \mathbb{F}_{2^n}\} \geq 2^{n/2}. \tag{4}$$

Функции, для которых неравенство (4) обращается в равенство, существуют только для четных значений n и носят название *бент-функций*.

В случае, когда число переменных нечетно, задача описания функций, плохо приближаемых линейными, значительно труднее. На пути ее решения, в частности, интерес вызывают функции, у которых число различных коэффициентов Уолша – Адамара сравнительно невелико. Из равенства Парсеваля вытекает, что если все ненулевые квадраты коэффициентов Уолша – Адамара одинаковы, то они равны 2^{2n-2s} при некотором $s \leq n/2$. Такие функции называются *платовидными порядка* $2s$ или, в случае $s = (n-1)/2$, *полубент-функциями*.

Одно из направлений задачи изучения нелинейных приближений связано с рассмотрением в качестве приближающего множества класса так называемых мономиальных функций, то есть таких, у которых редуцированный многочлен приведенного представления состоит из одного монома (см. [1]). В работе [5] приведены примеры функций от четного числа переменных, наихудшим образом приближаемых собственными мономиальными (редуцированный многочлен которых задает подстановку на $\mathbb{F}_{2^n}$). От авторов они получили название «гипербент-функций». Позднее в работе [6] была предпринята попытка использовать аппарат построения гипербент-функций для случая нечетного n.

В рамках данной работы мы рассмотрим вопрос о существовании функций, для которых при некотором s выполнено:

$$(\Delta(F, \mathrm{tr}^n_1(\alpha x^\delta)))^2 \in \{0, 2^{2n-2s}\} \text{ для любых } \alpha \in \mathbb{F}_{2^n} \text{ и } \delta \in \overline{1, 2^n - 1},\ (\delta, 2^n - 1) = 1. \tag{5}$$

Замечание 1. Известно (см., например, [3]), что если для всех $\alpha \in \mathbb{F}_{2^n}$

$$|\Delta(F, \mathrm{tr}^n_1(\alpha x))| \equiv 0 \pmod{2^w},$$

то $\deg F \leq n - w + 1$. Следовательно, степень платовидной функции порядка $2s$ не превосходит $s + 1$.

Теорема. Необходимыми условиями существования платовидных функций порядка $2s$ от нечетного числа переменных n, для которых выполняется условие (5), являются:

1) $s = (n-1)/2$;

2) существуют натуральные σ, делящие $2^n - 1$, такие, что для любого δ, взаимно простого с $2^n - 1$,

$$||\rho_n(\sigma\delta)|| \in \{(n-1)/2, (n+1)/2\}.$$

Доказательство. В доказательстве теоремы применим рассуждения, аналогичные использованным в [1].

Пусть $F(x):\mathbb{F}_{2^n}\to\mathbb{F}_2$ – платовидная порядка $2s$ функция от n переменных. Выберем натуральное δ взаимно простым с 2^n-1. Тогда существует натуральное $\eta=\eta(\delta)$, такое, что $\delta\eta\equiv 1 \pmod{2^n-1}$.

Рассмотрим функцию $F_\eta(x):\mathbb{F}_{2^n}\to\mathbb{F}_2$, определяемую равенством $F_\eta(x) = F(x^\eta)$ для любого x из поля $\mathbb{F}_{2^n}$. Так как

$$\Delta\left(F,\mathrm{tr}_1^n\left(\alpha x^\delta\right)\right)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{F(x)+\mathrm{tr}_1^n\left(\alpha x^\delta\right)}=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{F\left(x^\eta\right)+\mathrm{tr}_1^n\left(\alpha x^{\delta\eta}\right)}=\Delta\left(F_\eta,\mathrm{tr}_1^n\left(\alpha x\right)\right),$$

то выполнение для всех $\alpha\in\mathbb{F}_{2^n}$ условия

$$(\Delta(F,\mathrm{tr}_1^n(\alpha x^\delta)))^2\in\{0,2^{2n-2s}\}$$

равносильно тому, что функция $F_\eta(x)$ также является платовидной порядка $2s$.

Пусть теперь

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

и

$$\Phi_\eta(x)=\sum_{t\in M_n}c'_t\cdot\xi_t\cdot x^t$$

– редуцированные многочлены приведенных представлений функций $F(x)$ и $F_\eta(x)$ соответственно. Согласно [1],

$$\mathrm{ind}\,\Phi_\eta(x)=\max\{||\rho_n(t\eta)||:t\in M_n,c_t\neq 0\}. \tag{6}$$

В соответствии с замечанием 1 для выполнения условия (5) необходимо

$$\mathrm{ind}\,\Phi(x)\le s+1 \quad\text{и}\quad \mathrm{ind}\,\Phi_\eta(x)\le s+1. \tag{7}$$

Перебирая все $\delta\in\overline{1,2^n-1}$, такие, что $(\delta,2^n-1)=1$, и строя для них натуральные $\eta=\eta(\delta)$ со свойством

$$\delta\eta\equiv 1 \pmod{2^n-1},$$

получим опять все множество натуральных чисел, меньших числа 2^n-1 и взаимно простых с ним. Тогда из выражений (6) и (7) следует, что (5) имеет место, только если

$||\rho_n(t\eta)||\le s+1$ для всех $t\in M_n$ и всех $\eta\in\overline{1,2^n-1}$, таких, что $c_t\neq 0$ и $(\eta,2^n-1)=1$.

Зафиксируем элемент η с указанными свойствами и рассмотрим $\eta'=2^n-1-\eta$. Очевидно, что $(\eta',2^n-1)=1$. Тогда выполнение (5) требует

$$||\rho_n(t\eta)||\le s+1 \text{ и } ||\rho_n(t\eta')||\le s+1 \text{ для всех } t\in M_n, \text{ таких, что } c_t\neq 0. \tag{8}$$

При этом

$$\rho_n(t\eta')=2^n-1-\rho_n(t\eta)$$

и

$$||\rho_n(t\eta')||=n-||\rho_n(t\eta)||. \tag{9}$$

Из (9) следует, что условие (8) влечет

$$||\rho_n(t\eta)||\le s+1,\ n-||\rho_n(t\eta)||\le s+1 \text{ для всех } t\in M_n, \text{ таких, что } c_t\neq 0,$$

или, что то же,

$$n-s-1\le||\rho_n(t\eta)||\le s+1 \text{ для всех } t\in M_n, \text{ таких, что } c_t\neq 0.$$

Последнее выполнено только тогда, когда

$$s\ge(n-2)/2. \tag{10}$$

Так как порядок платовидной функции от нечетного числа переменных n не может превышать $(n-1)/2$, то из (10) следует

$$s=(n-1)/2. \tag{11}$$

Таким образом, необходимым условием выполнения (5) является

$||\rho_n(t\eta)||\in\{(n-1)/2,(n+1)/2\}$ для всех $t\in M_n,\eta\in\overline{1,2^n-1}$, таких, что $c_t\neq 0$, $(\eta,2^n-1)=1$. (12)

Очевидно, что для любого $t\in M_n$ существует σ_t такой, что

$$(\sigma_t,2^n-1)=1$$

и

$$\rho_n(t\sigma_t)=(t,2^n-1).$$

Следовательно, (12) равносильно

$||\rho_n(\sigma_t\eta)||\in\{(n-1)/2,(n+1)/2\}$ для всех $t\in M_n,\eta\in\overline{1,2^n-1}$, таких, что $c_t\neq 0$, $(\eta,2^n-1)=1$. (13)

(11) и (13) в совокупности доказывают утверждение теоремы.

Следствие. Если число $2^n - 1$ простое, то функций от n переменных, удовлетворяющих условию (5), не существует.

Утверждение 1. Пусть n нечетно, $G(y) : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $t|(2^n - 1)$ и функция $F(x) : \mathbb{F}_{2^n} \to \mathbb{F}_2$ определена условием $F(x) = G(x^t)$ для каждого $x \in \mathbb{F}_{2^n}$. Тогда если $t > 1$, то $F(x)$ не может являться платовидной порядка n–1.

Доказательство. Очевидно, что вес платовидной функции порядка n–1 может принимать одно из трех значений:

$$2^{n-1},\ 2^{n-1} - 2^{(n-1)/2},\ 2^{n-1} + 2^{(n-1)/2}.$$

С другой стороны, если θ – примитивный элемент поля $\mathbb{F}_{2^n}$, то период последовательности

$$(F(\theta^{ti}) : i \in \mathbb{N})$$

делит $(2^n - 1)/t$. Следовательно, вес функции $F(x)$ кратен t.

Рассмотрим три возможных случая.

1) Так как $(2^{n-1}, 2^n - 1) = 1$, то $F(x)$ имеет вес 2^{n-1}, только если $t = 1$.

2) Так как $2^n - 1$ нечетно, то

$$(2^{n-1} - 2^{(n-1)/2}, 2^n - 1) = (2^{(n-1)/2}(2^{(n-1)/2} - 1), 2^n - 1) = (2^{(n-1)/2} - 1, 2^n - 1).$$

Согласно [2],

$$(2^{(n-1)/2} - 1, 2^n - 1) = 2^{((n-1)/2,\ n)} - 1,$$

но $(n-1)/2$ и n, очевидно, взаимно просты. Значит,

$$(2^{n-1} - 2^{(n-1)/2}, 2^n - 1) = 2^{((n-1)/2,\ n)} - 1 = 1$$

и $F(x)$ имеет вес $2^{n-1} - 2^{(n-1)/2}$, только если $t = 1$.

3) Так как $2^n - 1$ нечетно и $(2^{(n-1)/2} - 1, 2^{(n-1)/2} + 1) = 1$, то

$$(2^{n-1} + 2^{(n-1)/2}, 2^n - 1) = (2^{(n-1)/2}(2^{(n-1)/2} + 1), 2^n - 1) = (2^{(n-1)/2} + 1, 2^n - 1) = ((2^{n-1} - 1, 2^n - 1)/(2^{(n-1)/2} - 1, 2^n - 1)).$$

Из п. 2 следует, что

$$((2^{n-1} - 1, 2^n - 1)/(2^{(n-1)/2} - 1, 2^n - 1)) = (2^{(n-1,\ n)} - 1).$$

Так как $(n-1, n) = 1$, то

$$(2^{n-1} + 2^{(n-1)/2}, 2^n - 1) = 1$$

и $F(x)$ имеет вес $2^{n-1} + 2^{(n-1)/2}$, только если $t = 1$.

Таким образом, из пп. 1, 2 и 3 следует, что при $t > 1$ не существует платовидных функций порядка n–1, представимых в указанном виде.

Утверждение 2. Если для некоторого нечетного n, большего пяти, мощность множества

$$W_n = \{\sigma \in \overline{1, 2^n - 1} : \sigma | (2^n - 1),\ ||\rho_n(\sigma\delta) \pmod{2^n - 1}|| \in \{(n-1)/2, (n+1)/2\}$$

$$\text{для всех } \delta \in \overline{1, 2^n - 1},\ \text{таких, что } (\delta, 2^n - 1) = 1\},$$

не превосходит двух, то функций от n переменных, удовлетворяющих условию (5) для какого-либо значения s, не существует.

Доказательство. Если множество W_n пусто, то результат утверждения следует непосредственно из теоремы.

Если W_n состоит из единственного элемента σ, то редуцированный многочлен приведенного представления функции $F(x)$, удовлетворяющей условию (5), должен (см. доказательство теоремы) иметь вид

$$\Phi(x) = \sum_{\substack{\eta \in \overline{1, 2^n - 1}: \\ (\eta, 2^n - 1) = 1}} c_\eta \left(x^\sigma\right)^\eta.$$

Следовательно, функция $F(x)$ представима в форме $F(x) = G(x^\sigma)$ и, согласно утверждению 1, не может являться платовидной порядка n–1.

Пусть $W_n = \{\sigma', \sigma''\}$. В этом случае редуцированный многочлен приведенного представления функции $F(x)$, удовлетворяющей условию (5), должен иметь вид

$$\Phi(x) = \sum_{\substack{\eta \in \overline{1, 2^n - 1}: \\ (\eta, 2^n - 1) = 1}} \left(c'_\eta \left(x^{\sigma'}\right)^\eta + c''_\eta \left(x^{\sigma''}\right)^\eta\right).$$

Следовательно, $F(x)$ представима в форме

$$F(x) = G(x^{(\sigma', \sigma'')}). \tag{14}$$

Покажем, что $(\sigma', \sigma'') > 1$. Пусть это не так. Тогда σ' и σ'' – взаимно простые делители числа $2^n - 1$. Получим

$$\sigma' \cdot \sigma'' \mid 2^n - 1. \tag{15}$$

С другой стороны, так как двоичный вес этих чисел не меньше $(n-1)/2$ и $(2^{(n-1)/2} - 1, 2^n - 1) = 1$, то, не ограничивая общности,

$$\sigma' \geq 3 \cdot 2^{(n-3)/2} - 1$$

и

$$\sigma'' \geq 7 \cdot 2^{(n-5)/2} - 1.$$

В условиях утверждения это влечет

$$\sigma' \cdot \sigma'' \geq (3 \cdot 2^{(n-3)/2} - 1)(7 \cdot 2^{(n-5)/2} - 1) = 42 \cdot 2^{(n-5)} - 13 \cdot 2^{(n-5)/2} + 1 = 2^n - 1 + (10 \cdot 2^{(n-5)} - 13 \cdot 2^{(n-5)/2} + 2) > 2^n - 1.$$

Но последнее противоречит (15). Таким образом, $(\sigma', \sigma'') > 1$. Тогда из (14) и результата утверждения 1 следует, что $F(x)$ не может являться платовидной порядка $n-1$.

Утверждение доказано.

Замечание 2. Из теоремы следует, что для существования платовидных функций порядка $n-1$ от n переменных, удовлетворяющих условию (5), необходимо наличие делителей σ числа $2^n - 1$, таких, что для любого δ, взаимно простого с $2^n - 1$,

$$||\rho_n(\sigma\delta)|| \in \{(n-1)/2, (n+1)/2\}.$$

По результатам эксперимента для $5 \leq n \leq 33$ числа с указанным свойством обнаружены только при

$$n = 21 \ (\sigma = 42799)$$

и

$$n = 29 \ (\sigma = 256999).$$

Таким образом, опираясь на данные эксперимента и утверждение 2, можно заключить, что для $n \leq 33$ не существует функций, удовлетворяющих условию (5).

ЛИТЕРАТУРА

1. *Кузьмин А.С.*, *Марков В.Т.*, *Нечаев А.А.*, *Шишков А.Б.* Приближение булевых функций мономиальными // Дискр. мат. 2006. Т. 18. № 1. С. 9 – 29.
2. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
3. *Логачев О.А.*, *Сальников А.А.*, *Ященко В.В.* Булевы функции в теории кодирования и криптологии. М.: МНЦМО, 2004.
4. *Мак-Вильямс Ф. Дж.*, *Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. *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.
6. *Youssef A.M.*, *Gong G.* Boolean functions with large distance to all bijective monomials: N odd case // Proceedings of the Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, August 16 – 18, 2001.