А. Н. Велигура, Об аппроксимации булевых функций линейными разветвлениями, *Матем. вопр. криптогр.*, 2023, том 14, выпуск 1, 15–25

DOI: 10.4213/mvk428

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2023 Т. 14 № 1 С. 15–25

УДК 519.716.322+519.719.2 DOI https://doi.org/10.4213/mvk428

Об аппроксимации булевых функций линейными разветвлениями

А. Н. Велигура

Национальный исследовательский ядерный университет «МИФИ»,
Финансовый университет
при Правительстве Российской Федерации, Москва

Получено 05.X.2022

Аннотация. Рассматриваются приближения булевых функций линейными разветвлениями — кусочно-линейными булевыми функциями, области линейности которых являются линейными многообразиями. Найдено представление расстояния от линейного разветвления до булевой функции через ее спектральные коэффициенты, предложен алгоритм построения ближайшего к данной функции линейного разветвления для заданного разветвляющего отображения.

Ключевые слова: булевы функции, линейные функции, линейные разветвления

On approximations of Boolean functions by linear spreads

A. N. Veligura

National Research Nuclear University MEPhI,
Financial University under the Government of the Russian Federation, Moscow

Abstract. We study approximations of Boolean functions by linear spreads, i. e. piecewise linear Boolean functions such that the domain of each piece is a linear manifold. The representation of the distance from the given Boolean function to the nearest linear spread is given in terms of spectral coefficients of the function. An algorithm for constructing the linear spread which is nearest to the given Boolean function for given spreading transform is suggested.

Keywords: Boolean functions, linear functions, linear spreads

Citation: Matematicheskie Voprosy Kriptografii, 2023, v. 14, № 1, pp. 15–25 (Russian)

1. Введение

Задача приближения булевых функций линейными функциями возникает в различных приложениях дискретной математики; этой задаче посвящено большое число работ. Обзоры результатов о булевых функциях, в том числе о приближениях их линейными, можно найти, например, в [1, 2]. Наряду с линейными приближениями «в чистом виде» рассматривались и конструкции на их основе, к которым относятся линейные разветвления. В настоящее время есть ряд методов использования линейных разветвлений для решения практических задач, например метод локальных многообразий [3, 4]. Целью данной работы является решение задачи выбора ближайшего к данной булевой функции f линейного разветвления.

2. Обозначения и вспомогательные результаты

Будем использовать стандартные обозначения и определения, в основном следуя работам [1, 8]. Пусть V_n – n-мерное векторное пространство над полем из двух элементов, Ψ_n – множество булевых функций от n переменных, псевдобулева функция от n переменных есть отображение V_n в множество действительных чисел $\mathbb{R}$. Если псевдобулева функция принимает только значения 0 и 1, то при необходимости ее можно рассматривать как булеву функцию, и наоборот. Векторы по умолчанию будем считать столбцами, верхний индекс T обозначает транспонирование. Там, где это не приводит к недоразумениям, будем для векторов и их компонент использовать одну и ту же букву с соответствующим индексом, например для $\rho \in V_k$ считаем, что $\rho = (\rho_1, \ldots, \rho_k)$.

Преобразованием Уолша – Адамара (псевдо)булевой функции $f \in \Psi_n$ будем называть псевдобулеву функцию

$$\hat{f}(\alpha) = \sum_{x \in V_n} (-1)^{f(x)+\alpha^T x} = \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha^T x}, \alpha \in V_n.$$

Здесь, как обычно, знак $\oplus$ обозначает покоординатное сложение векторов по модулю 2. Дельта-функцией (Дирака) будем называть (псевдо)булеву функцию

$$\delta(x) = \begin{cases} 1, & x = 0, \\ 0, & x \neq 0, \end{cases} \quad x \in V_n,$$

определенную для всех $n \geqslant 1$. Нетрудно видеть, что

$$\delta(x_1, \ldots, x_n) = \delta(x_1) \cdot \ldots \cdot \delta(x_n) = 2^{-n} \sum_{\rho \in V_n} (-1)^{\rho^T x}. \qquad (2.1)$$

Расстоянием $dist(f, g)$ между булевыми функциями f и g от одинакового числа переменных будем считать число аргументов, на которых они не совпадают.

3. Кусочно-линейные функции и линейные разветвления

Пусть есть разбиение пространства V_n на t не пересекающихся множеств $U_1, \ldots, U_t : V_n = U_1 \cup \ldots \cup U_t, U_i \cap U_j = \varnothing$ при $i \neq j$, и пусть есть t аффинных булевых функций $L_1, \ldots, L_t$. Обозначим через $I_1, \ldots, I_t$ булевы функции — индикаторы множеств $U_1, \ldots, U_t$:

$$I_i(x) = \begin{cases} 1 & \text{при } x \in U_i, \\ 0 & \text{в противном случае,} \end{cases} \qquad x \in V_n, i = 1, \ldots, t.$$

Тогда функцию

$$\Phi(x) = \sum_{i=1}^{t} I_i(x) L_i(x)$$

назовем кусочно-линейной с областями линейности $U_1, \ldots, U_t$. К кусочно-линейным функциям относятся, очевидно, линейные разветвления [1, 5–7] — кусочно-линейные функции, области линейности которых имеют вид линейных многообразий: $U_\rho = \{x \in V_n \colon h(x) = \rho\}, \rho \in V_k$, где $h \colon V_n \to V_k$ — линейное отображение, называемое разветвляющим: $h(x) = (h_1(x), \ldots, h_k(x)), h_i(x)$ — его координатные функции, которые далее будем записывать в виде $h_i(x) = h_i^T(x), i = 1, \ldots, k, V_k$ — разветвляющее пространство. Здесь и далее считаем векторы $h_1, \ldots, h_k$ линейно независимыми. В этом случае индикаторы областей линейности представляют собой функции

$$I_\rho(x) = \delta(h_1^T x \oplus \rho_1, \ldots, h_k^T x \oplus \rho_k), \quad \rho = (\rho_1, \ldots, \rho_k) \in V_k,$$

и, соответственно,

$$\Phi(x) = \sum_{\rho \in V_k} \delta(h_1^T x \oplus \rho_1, \ldots, h_k^T x \oplus \rho_k)(a_\rho^T x \oplus b_\rho), \qquad (3.1)$$

где $(a_\rho \in V_n, b_\rho \in V_1)$ — коэффициенты аффинной функции, действующей в области линейности $U_\rho, \rho \in V_k$.

4. Расстояние от булевой функции до заданного линейного разветвления

Теорема. *Пусть* $f \in \Psi_n$ *— булева функция,* $h_1, \ldots, h_k \in V_n$, $a_\rho \in V_n$, $b_\rho \in V_1$ *заданы для всех* $\rho \in V_k$,

$$\Phi(x) = \sum_{\rho \in V_k} \delta(h_1^T x \oplus \rho_1, \ldots, h_k^T x \oplus \rho_k)(a_\rho^T x \oplus b_\rho)$$

— линейное разветвление. Тогда

$$dist(\Phi, f) = 2^{n-1} - 2^{-k-1} \sum_{\rho \in V_k} (-1)^{b_\rho} \sum_{\lambda \in V_k} (-1)^{\lambda^T \rho} \hat{f}\left(a_\rho \oplus \sum\nolimits_{i=1}^{k} \lambda_i h_i\right).$$

Доказательство. Представим число векторов, на которых функции f и Φ совпадают, используя (2.1) и (3.1):

$$\begin{aligned}
2^n - dist(\Phi, f) &= \sum_{x \in V_n} \delta(\Phi(x) \oplus f(x)) \\
&= \sum_{x \in V_n, \rho \in V_k} \delta(f(x) \oplus a_\rho^T \oplus b_\rho) \delta(h_1^T x \oplus \rho_1, \ldots, h_k^T x \oplus \rho_k) \\
&= 2^{-k-1} \sum_{x \in V_n, \rho \in V_k} (1 + (-1)^{f(x) \oplus a_\rho^T x \oplus b_\rho}) \sum_{\lambda \in V_k} (-1)^{\sum_{i=1}^k \lambda_i (h_i^T \oplus \rho_i)} \\
&= 2^{-k-1} \sum_{x \in V_n, \rho \in V_k} (1 + (-1)^{f(x) \oplus a_\rho^T x \oplus b_\rho}) \sum_{\lambda \in V_k} (-1)^{(\sum_{i=1}^k \lambda_i h_i)^T x} (-1)^{\lambda^T \rho} \\
&= 2^{-k-1} \sum_{\lambda \in V_k} \sum_{\rho \in V_k} (-1)^{\lambda^T \rho} \sum_{x \in V_n} (-1)^{(\sum_{i=1}^k \lambda_i h_i)^T x} \\
&\quad + 2^{-k-1} \sum_{\rho \in V_k, \lambda \in V_k} \sum_{x \in V_n} (-1)^{f(x) + a_\rho^T x + b_\rho + (\sum_{i=1}^k \lambda_i h_i)^T x} (-1)^{\lambda^T \rho} \\
&= 2^{n-1} + 2^{-k-1} \sum_{\rho \in V_k} (-1)^{b_\rho} \sum_{\lambda \in V_k} (-1)^{\lambda^T \rho} \hat{f}\left(a_\rho \oplus \sum\nolimits_{i=1}^{k} \lambda_i h_i\right).
\end{aligned}$$

Тогда

$$dist(\Phi, f) = 2^{n-1} - 2^{-k-1} \sum_{\rho \in V_k} (-1)^{b_\rho} \sum_{\lambda \in V_k} (-1)^{\lambda^T \rho} \hat{f}\left(a_\rho \oplus \sum_{i=1}^{k} \lambda_i h_i\right). \quad (4.1)$$

Теорема доказана. □

Таким образом, расстояние от функции до фиксированного линейного разветвления есть аффинная функция от коэффициентов Уолша – Адамара данной булевой функции. Подобные задачи часто рассматриваются в вероятностной постановке. Вероятность того, что $\Phi(x) = f(x)$ при случайном и равновероятном выборе $x \in V_n$, равна

$$\mathbf{P}(\Phi(x) = f(x)) = \frac{2^n - dist(\Phi, f)}{2^n}$$
$$= \frac{1}{2} + \frac{1}{2^{n+k+1}} \sum_{\rho \in V_k} (-1)^{b_\rho} \sum_{\lambda \in V_k} (-1)^{\lambda_\rho^T} \hat{f} \left(a_\rho \oplus \sum_{i=1}^{k} \lambda_i h_i \right).$$

5. Аппроксимация булевой функции линейным разветвлением

Рассмотрим задачу поиска для данной булевой функции f ближайшего (в смысле рассматриваемой метрики) линейного разветвления при фиксированной размерности k разветвляющего пространства. Поставленная задача может рассматриваться как поиск векторов $\{a_\rho \in V_n, b_\rho \in V_1 \mid \rho \in V_k\}, h_1, \ldots, h_k \in V_n$, доставляющих максимум величине (см. (4.1))

$$D(\{a_\rho \in V_n, b_\rho \in V_1 \mid \rho \in V_k\}; h_1, \ldots, h_k)$$
$$= \sum_{\rho \in V_k} (-1)^{b_\rho} \sum_{\lambda \in V_k} (-1)^{\lambda^T \rho} \hat{f} \left(a_\rho \oplus \sum_{i=1}^{k} \lambda_i h_i \right). \tag{5.1}$$

5.1. Случай фиксированного разветвляющего отображения

Из равенства (5.1) следует, что поиск ближайшего линейного разветвления при заданных $h_1, \ldots, h_k$ сводится к выбору нужных аффинных функций независимо для каждой области линейности, что эквивалентно нахождению для каждого $\rho \in V_k$ величины

$$M(\rho; h_1, \ldots, h_k) = \operatorname*{argmax}_{y \in V_n} \left| \sum\nolimits_{\lambda \in V_k} (-1)^{\lambda^T \rho} \hat{f} \left(y \oplus \sum\nolimits_{i=1}^{k} \lambda_i h_i \right) \right|. \tag{5.2}$$

Максимум может достигаться не при единственном значении $y \in V_n$; в этом случае в качестве $M(\rho; h_1, \ldots, h_k)$ будем использовать любое из этих значений.

Приведем два алгоритма нахождения величин $M(\rho; h_1, \ldots, h_k)$ для всех $\rho \in V_k$, первый из них состоит в прямом вычислении этих величин с использованием формулы (5.2) и может использоваться в качестве отправной точки для сравнения с другими алгоритмами. Оценим число битовых операций для выполнения алгоритмов как функцию от n, k. Заметим, что коэффициенты Уолша – Адамара представляют собой целые числа, имеющие не более n двоичных разрядов, поэтому трудоемкость их сложения в битовых операциях пропорциональна n, как и трудоемкость сложения n-мерных двоичных векторов. Входными данными алгоритмов являются функция f, заданная в табличном виде (таблицей истинности), и векторы $h_1, \ldots, h_k$. На выходе алгоритмов получаем для всех $\rho \in V_k$ значения $M(\rho; h_1, \ldots, h_k)$ и соответствующие им значения величин

$$\left| \sum_{\lambda \in V_k} (-1)^{\lambda^T \rho} \hat{f}\left(y \oplus \sum\nolimits_{i=1}^{k} \lambda_i h_i \right) \right|.$$

Алгоритм 1.
Шаг 1. Найдем и сохраним все коэффициенты Уолша – Адамара функции f.
Шаг 2. Построим и сохраним все векторы подпространства, порожденного векторами $h_1, \ldots, h_k$.
Шаг 3. Найдем и сохраним значения $\hat{f}\left(y \oplus \sum_{i=1}^{k} \rho_i h_i \right)$ для всех $y \in V_n, \rho \in V_k$.
Шаг 4. Найдем $M(\rho; h_1, \ldots, h_k)$ для каждого $\rho \in V_k$.
Выполнение алгоритма 1 завершено.

Число битовых операций для выполнения шага 1 с использованием быстрого преобразования Фурье пропорционально $n2^n$.

Число битовых операций для выполнения шага 2 пропорционально $n2^n$.

Число битовых операций для выполнения шага 3 пропорционально $n2^{n+k}$.

Оценим число битовых операций для выполнения шага 4.

Сумма в (5.2) содержит 2^k слагаемых, число битовых операций для ее непосредственного вычисления при фиксированных $y \in V_n, \rho \in V_k$ пропорционально $n2^k$. Для нахождения $M(\rho; h_1, \ldots, h_k)$ для одного $\rho \in V_k$ эту сумму нужно вычислить для всех $y \in V_n$, на что потребуется число битовых операций, пропорциональное $n2^{n+k}$. Выполнив

это для всех $\rho \in V_k$, получим значения всех величин $M(\rho; h_1, \ldots, h_k)$. Число битовых операций для этого пропорционально $n2^{n+2k}$.

Число битовых операций для нахождения с помощью алгоритма 1 величин $M(\rho; h_1, \ldots, h_k)$ при всех $\rho \in V_k$ есть сумма трудоемкостей выполнения шагов 1–4 и оценивается сверху величиной, пропорциональной $n2^{2k+n} + n2^{n+k} + n2^{n+1}$.

Для описания алгоритма 2 введем обозначение:

$$c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m) = \sum_{\lambda \in V_m} (-1)^{\lambda^T \rho} \hat{f}\left(y \oplus \sum\nolimits_{i=1}^{m} \lambda_i h_i\right), m = 1, \ldots, k. \tag{5.3}$$

Тогда

$$M(\rho; h_1, \ldots, h_k) = \operatorname*{argmax}_{y \in V_n} \left| c_k(y; \rho_1, \ldots, \rho_k; h_1, \ldots, h_k) \right|.$$

Утверждение. *Для $m = 1, \ldots, k$ имеют место равенства*

$$\begin{gathered} c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m) = c_{m-1}(y; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1}) \\ +(-1)^{\rho_m} c_{m-1}(y \oplus h_m; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1}), \\ y \in V_n, (\rho_1, \ldots, \rho_m) \in V_m, \end{gathered} \tag{5.4}$$

где $c_0 = \hat{f}(y)$.

Доказательство. Согласно (5.3)

$$\begin{aligned} c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m) &= \sum_{\lambda \in V_m} (-1)^{\lambda^T \rho} \hat{f}\left(y \oplus \sum\nolimits_{i=1}^{m} \lambda_i h_i\right) \\ &= \sum_{(\lambda_1, \ldots, \lambda_{m-1}) \in V_{m-1}} (-1)^{\sum_{i=1}^{m-1} \lambda_i \rho_i} \hat{f}\left(y \oplus \sum\nolimits_{i=1}^{m-1} \lambda_i h_i\right) \\ &+ \sum_{(\lambda_1, \ldots, \lambda_{m-1}) \in V_{m-1}} (-1)^{\sum_{i=1}^{m-1} \lambda_i \rho_i + \rho_m} \hat{f}\left(y \oplus h_m \oplus \sum\nolimits_{i=1}^{m-1} \lambda_i h_i\right) \\ &= c_{m-1}(y; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1}) \\ &+(-1)^{\rho_m} c_{m-1}(y \oplus h_m; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1}). \end{aligned}$$

При $m = 1$ согласно (5.3) $c_1(y; \rho_1; h_1) = \hat{f}(y) + (-1)^{\rho_1} \hat{f}(y \oplus h_1)$, тогда естественно считать $c_0(y) = \hat{f}(y)$.

Утверждение доказано. □

Заметим, что из (5.4) следуют равенства

$$c_k(y \oplus h_k; \rho_1, \ldots, \rho_{k-1}, 0; h_1, \ldots, h_k) = c_k(y; \rho_1, \ldots, \rho_{k-1}, 0; h_1, \ldots, h_k), \tag{5.5}$$

$$c_k(y \oplus h_k; \rho_1, \ldots, \rho_{k-1}, 1; h_1, \ldots, h_k) = -c_k(y; \rho_1, \ldots, \rho_{k-1}, 1; h_1, \ldots, h_k). \tag{5.6}$$

Алгоритм 2.

Шаг 1.

Найдем и сохраним коэффициенты $\hat{f}(y)$ Уолша – Адамара функции f для всех $y \in V_n$. Положим $c_0(y) = \hat{f}(y), y \in V_n$.

Шаг 2.

Для $m = 1, \ldots, k$ найдем

$$c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m)$$
$$= c_{m-1}(y; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1}) + (-1)^{\rho_m} c_{m-1}(y \oplus h_m; \rho_1, \ldots, \rho_{m-1})$$

для всех $y \in V_n$, $(\rho_1, \ldots, \rho_m) \in V_m$ и сохраним найденные значения. После нахождения $c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m)$ для всех $y \in V_n, (\rho_1, \ldots, \rho_m) \in V_m$ нет необходимости хранить значения $c_{m-1}(y; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1})$.

Шаг 3.

Найдем 2^k максимумов $\max\limits_{y \in V_n} c_k \, |c_k(y; \rho_1, \ldots, \rho_k; h_1, \ldots, h_k)|$ для всех $(\rho_1, \ldots, \rho_k) \in V_k$ и соответствующие им значения $M((\rho_1, \ldots, \rho_k); h_1, \ldots, h_k))$.

Выполнение алгоритма 2 завершено.

Число битовых операций для выполнения шага 1 с использованием быстрого преобразования Фурье пропорционально $n2^n$. Шаг 2 состоит из k стадий, пронумеруем их числами $m = 1, \ldots, k$. Стадия m состоит в получении $c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m)$, уже располагая значениями $c_{m-1}(y; \rho_1, \ldots, \rho_{m-1}; h_1, \ldots, h_{m-1})$ для всех $y \in V_n, (\rho_1, \ldots, \rho_{m-1}) \in V_{m-1}$. Для выполнения стадии m шага 2, согласно (5.4) с учетом (5.5), (5.6), нужно будет выполнить 2^{n+m-1} операций сложения не более чем n-разрядных целых чисел и столько же операций сложения n-мерных булевых векторов $y \oplus h_m$. Отсюда следует, что если $T(n, m)$ – число битовых операций для получения $c_m(y; \rho_1, \ldots, \rho_m; h_1, \ldots, h_m)$ для всех $y \in V_n, (\rho_1, \ldots, \rho_m) \in V_m$, то

$$T(n, m) = T(n, m-1) + n2^{n+m} = T(n, 0) + n2^n \sum_{j=1}^{m} 2^j,$$

значит, $T(n,k) = 2^{n+k+1} - n2^{n+1} + T(n,0)$, где $T(n,0)$ — число битовых операций для получения коэффициентов $\hat{f}(y)$ для всех $y \in V_n$. Число $T(n,0)$ есть число битовых операций для выполнения шага 1 и нами уже учтено. Выполнение шага 3 потребует для каждого вектора $(\rho_1,\dots,\rho_k) \in V_k$ выбора максимума из 2^n величин $\{c_k(y;\rho_1,\dots,\rho_k;h_1,\dots,h_k)|y \in V_n\}$, на что потребуется в общей сложности 2^{n+k} операций сравнения.

Примечание. Выбор указанных максимумов можно выполнять в ходе нахождения величин $c_k(y;\rho_1,\dots,\rho_k;h_1,\dots,h_k)$, т. е. на стадии k шага 2, что имеет ту же трудоемкость. Число битовых операций для нахождения с помощью алгоритма 2 для всех $\rho \in V_k$ величин $M(\rho,h_1,\dots,h_k)$ есть сумма трудоемкостей выполнения шагов 1–3 и оценивается сверху величиной, пропорциональной $n2^{n+k+1} - n2^{n+1} + 2^{n+k} + n2^n$ битовых операций. Это по порядку величины в 2^k раз меньше затрат на решение этой задачи вычислением по формуле (5.2) с применением алгоритма 1.

5.2. Случай нефиксированного разветвляющего отображения

Если разветвляющее отображение не фиксировано, то с учетом введенных обозначений поиск ближайшего к данной функции линейного разветвления сводится к максимизации величины

$$\sum_{\rho\in V_k} |c_k(a_\rho;\rho_1,\dots,\rho_k;h_1,\dots,h_k)|$$

по всем $\{a_\rho \in V_n \,|\, \rho \in V_k\}, h_1,\dots,h_k \in V_n$, где $h_1,\dots,h_k$ линейно независимы.

Поиск решения этой оптимизационной задачи, которое бы не сводилось к полному перебору неэквивалентных базисов $h_1,\dots,h_k$ и применению результатов п. 5.1, выходит за рамки данной работы. Здесь рассмотрим только случай $k = 1$. Тогда в наших обозначениях

$$\begin{gathered}
c_1(y;\rho_1;h_1) = \hat{f}(y) + (-1)^{\rho_1}\hat{f}(y\oplus h_1),\\
M(0;h_1) = \operatorname*{argmax}_y \left|\hat{f}(y) + \hat{f}(y\oplus h_1)\right|,\\
M(1;h_1) = \operatorname*{argmax}_y \left|\hat{f}(y) - \hat{f}(y\oplus h_1)\right|,\\
\max_{a_0,a_1,h_1\in V_n,b_0,b_1\in\{0,1\}} D(\{a_0,a_1,b_0,b_1\};h_1)
\end{gathered}$$

$$= \max_{h_1}(\max_{x}(\hat{f}(x) + \hat{f}(x \oplus h_1)) + \max_{x}(\hat{f}(x) - \hat{f}(x \oplus h_1)))$$

$$= \max_{h_1}(\hat{f}(M(0;h_1)) + \hat{f}(M(0;h_1) \oplus h_1) + \hat{f}(M(1;h_1)) - \hat{f}(M(1;h_1) \oplus h_1)).$$

В некоторых случаях задача максимизации величины $D(a_0, a_1 \in V_n; b_0, b_1 \in \{0,1\}; h_1)$ упрощается. Например, если n четно и функция f является бент-функцией, то $\left|\hat{f}(a)\right| = 2^{\frac{n}{2}}$ для любого a. Тогда для любых a_0, a_1, h_1

$$\left|\hat{f}(y) + \hat{f}(y \oplus h_1)\right| \leqslant 2^{\frac{n}{2}+1}, \left|\hat{f}(y) - \hat{f}(y \oplus h_1)\right| \leqslant 2^{\frac{n}{2}+1}.$$

Выбрав a_0, a_1, h_1 так, чтобы $\hat{f}(a_0) = \hat{f}(a_1) = \hat{f}(a_0 + h_1) = 2^{\frac{n}{2}}$, $\hat{f}(a_1 + h_1) = -2^{\frac{n}{2}}$, получим

$$\max_{a_0,a_1,h_1 \in V_n, b_0,b_1 \in \{0,1\}} D(\{a_0, a_1, b_0, b_1\}; h_1) = 2^{\frac{n}{2}+2},$$

минимальное расстояние до разветвления

$$dist(\Phi, f) = 2^n - 2^{-2} \max_{a_0,a_1,h_1 \in V_n, b_0,b_1 \in \{0,1\}} D(\{a_0, a_1, b_0, b_1\}; h_1) = 2^{\frac{n}{2}},$$

при этом $\mathbf{P}(\Phi(x) = f(x)) = \dfrac{1}{2} + 2^{-n-2}2^{\frac{n}{2}+2} = \dfrac{1}{2} + 2^{-\frac{n}{2}}$. Соответственно все ближайшие к данной функции f линейные разветвления при одномерном разветвляющем пространстве имеют вид

$$\Phi(x) = \sum_{\rho=0}^{1} \delta(h_1^T x \oplus \rho) a_\rho^T x = (h_1^T x \oplus 1)(a_0^T x) \oplus (h_1^T x)(a_1^T x)$$

$$= (h_1^T x)\left((a_0 \oplus a_1)^T x\right) \oplus a_0^T x,$$

где a_0, a_1, h_1 выбраны, как указано выше. Этот выбор не составляет труда, так как, например, при $f(0) = 0$ половина коэффициентов Уолша – Адамара равны $2^{\frac{n}{2}}$, а остальные равны $-2^{\frac{n}{2}}$.

Список литературы

[1] Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В., *Булевы функции в теории кодирования и криптологии*, 2-е изд., М.: МЦНМО, 2012.

[2] Глухов М.М., "О приближении дискретных функций линейными функциями", *Математические вопросы криптографии*, **7**:4 (2016), 29–50.

[3] Логачев О.А., Сукаев А.А., Федоров С.Н., "Об одном методе решения систем квадратичных булевых уравнений, использующем локальные аффинности", *Информ. и её примен.*, **13**:2 (2019), 37–46.

[4] Бабуева А.А., Логачев О.А., Ященко В.В., “О связи локальных аффинностей булевой функции с некоторыми видами ее вырожденности”, *Дискретная математика*, **34**:2 (2022), 7–25.

[5] Токарева Н.Н., *Нелинейные булевы функции: бент-функции и их обобщения*, Saarbrucken: LAP LAMBERT Academic Publishing, 2011.

[6] Tokareva N., *Bent Functions: Results and Applications to Cryptography*, Acad. Press, Elsevier, 2015.

[7] Ященко В.В., “О критерии распространения для булевых функций и о бент-функциях”, *Проблемы передачи информации*, **33**:1 (1997), 75–86.

[8] Ивченко Г.И., Медведев Ю.И., Миронова В.А., “Структура спектров булевых функций”, *Математические вопросы криптографии*, **7**:1 (2016), 57–70.