ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 1998. Серия 1. Том 5, № 2, 90–96

УДК 519.71

О ДВУХ ХАРАКТЕРИСТИКАХ НЕЛИНЕЙНОСТИ БУЛЕВЫХ ОТОБРАЖЕНИЙ

В. В. Ященко

Рассмотрены две характеристики нелинейности булевого отображения F: $\mu l(F)$ — максимальный элемент таблицы разностей, применяемой в разностном криптоанализе; $il(F)$ — максимальный размер области кусочной аффинности отображения. Показано, что $\mu l(F) \geqslant il(F)$. В случае кусочно аффинных отображений получены выражения для элементов таблицы разностей. Эти выражения позволяют строить кусочно аффинные отображения с минимальным значением $\mu l(F)$.

1. Определения, обозначения и результаты

Пусть V_n обозначает векторное пространство размерности n над полем из двух элементов $\{0,1\}$, а $B(n,m)$ — множество отображений $F : V_n \to V_m$; в частности, $B(n,1)$ есть множество булевых функций от n переменных. Через $GA(n)$ будем обозначать полную аффинную группу преобразований пространства V_n, т. е. преобразований вида

$$x \to Ax + b,$$

где A — невырожденная матрица порядка n, а b — некоторый вектор из V_n. Любое отображение $F \in B(n,m)$ задает разбиение V_n на непересекающиеся множества $F^{-1}(\beta)$, $\beta \in V_m$, которые называют *блоками разбиения.* Набор мощностей блоков $\{|F^{-1}(\beta)|, \beta \in V_m\}$ назовем *весом отображения* F, а числа $|F^{-1}(\beta)|$ — *элементами веса.* Так как $V_n = \bigcup\limits_{\beta \in V_m} F^{-1}(\beta)$, то $\sum\limits_{\beta \in V_m} |F^{-1}(\beta)| = 2^n$. Для булевых функций весом принято называть не пару чисел $\{|F^{-1}(0)|, |F^{-1}(1)|\}$, а одно число $|F^{-1}(1)|$. Производной $D^\alpha F$ отображения $F \in B(n,m)$ по направлению $\alpha \in V_n$ называют отображение

$$(D^\alpha F)(x) = F(x+\alpha) + F(x),$$

здесь один знак «+» применен в двух смыслах — как сложение в пространствах V_n и V_m. При этом производная по направлению $0 \in V_n$

является нулевым отображением. Веса всех производных по ненулевым направлениям можно расположить в виде таблицы R^F из $2^n - 1$ строк и 2^m столбцов: строку с номером $\alpha \in V_n \setminus \{0\}$ таблицы R^F составляют элементы веса отображения $D^\alpha F$, т. е. для любых $\alpha \in V_n \setminus \{0\}$ и $\beta \in V_m$

$$R^F_{\alpha,\beta} = |(D^\alpha F)^{-1}(\beta)|.$$

Таблица R^F имеет многочисленные применения в разностном криптоанализе (см., например, [2, 3]) под разными названиями, но чаще всего ее называют *таблицей разностей.* В этих же приложениях рассматривается следующая характеристика отображения F — максимальный элемент его таблицы разностей:

$$\mu l(F) = \max_{\substack{\alpha \in V_n \setminus \{0\} \\ \beta \in V_m}} R^F_{\alpha,\beta}.$$

Величина $\mu l(F)$ определенным образом характеризует отклонение отображения F от аффинных отображений (для которых $\mu l(F) = 2^n$). В этом смысле максимально удаленными от аффинных отображений являются отображения F, минимизирующие величину $\mu l(F)$. Оценкам этого минимума, а также выделению некоторых классов отображений F с заданным (минимальным или близким к нему) значением $\mu l(F)$ посвящено много работ, примыкающих к задачам разностного криптоанализа. Для случая $m = 1$

$$\min_{F \in B(n,1)} \mu l(F) = 2^{n-1},$$

и это равенство достигается на множестве так называемых бент-функций, которые активно изучаются в теории кодирования уже более 20 лет (см. [1, 4]). Впрочем, ни полного описания класса бент-функций, ни даже асимптотики их числа пока не получено.

В работе [3] вводится также следующее понятие: отображение $F \in B(n, m)$ называется *разностно s-равномерным,* если $\mu l(F) \leqslant s$. (Формально данное в [3] определение несколько отличается от этого, но для целей данной работы это отличие несущественно.)

Отметим следующий достаточно очевидный факт: для любого отображения $F \in B(n, m)$ и любых отображений $C \in GA(n) : V_n \to V_n$ и $P \in GA(m) : V_m \to V_m$ справедливо равенство

$$\mu l(PFC) = \mu l(F).$$

При изучении характеристики $\mu l(F)$ это позволяет рассматривать отображения $F \in B(n, m)$ «с точностью до аффинных замен переменных», т. е. при необходимости выбирать подходящие базисы в V_n и V_m.

Введем теперь понятие кусочно аффинного отображения. Пусть N — некоторое натуральное число, $\rho : V_n \to \{1, \dots, N\}$ — некоторое отображение, $A_i : V_n \to V_m$, $i = 1, \dots, N$, — некоторое семейство аффинных отображений. Отображение $F \in B(n, m)$ определим следующим равенством: для любого $x \in V_n$

$$F(x) = A_{\rho(x)}(x).$$

Будем говорить, что F — кусочно аффинное отображение с областями кусочной аффинности $\rho^{-1}(i)$, $i = 1, \dots, N$, разветвляющим отображением ρ и разветвляемыми отображениями A_i, $i = 1, \dots, N$. Важной числовой характеристикой кусочно аффинного отображения является максимальный размер областей его кусочной аффинности:

$$il(F) = \max_{i=1,\dots,N} |\rho^{-1}(i)|.$$

Величина $il(F)$ определенным образом характеризует отклонение F от аффинных отображений и в этом смысле максимально удаленными от аффинных являются отображения F с минимальным значением $il(F)$.

Ясно, что фиксированное отображение F можно представить различными способами в виде кусочно аффинного отображения (за счет большой свободы в выборе N, ρ, A_i). Например, разбиение $\{\rho^{-1}(i)\}$ можно «измельчить», оставив отображения A_i теми же самыми (возможно, на подобластях). Ясно, что при этом отображение F не изменится, а изменится только его представление в форме кусочно аффинного. Очевидно также, что для любого отображения существует представление в кусочно аффинной форме. Поэтому можно рассмотреть все представления данного отображения F в кусочно аффинной форме и выбирать из них каким-нибудь нужным образом «самые крупные». Принцип выбора определяется удобством применения к конкретной задаче. Для настоящей работы достаточно ввести два варианта «самых крупных» кусочно аффинных представлений данного отображения F.

Под величиной $il(F)$ для произвольного отображения F будем понимать $\max il(\Phi)$, где максимум берется по всем кусочно аффинным отображениям Φ, равным F, с дополнительным условием на допустимые разветвляющие отображения ρ:

для каждого из них найдется $\alpha_0 \in V_n$, $\alpha_0 \neq 0$, такое, что $\rho(x + \alpha_0) = \rho(x)$ для всех $x \in V_n$.

Среди так определенных допустимых разветвляющих отображений наибольший интерес представляют линейные разветвляющие отображения. В этом случае имеем

$\rho : V_n \to V_k$— линейное, k— некоторое натуральное,
$N = 2^k$,
$|\rho^{-1}(z)| = 2^{n-k}$ для любого $z \in V_k$,
$\rho(x + \alpha_0) = \rho(x)$ для любого α_0 такого, что $\rho(\alpha_0) = 0$.

Если ограничиться только линейными разветвляющими отображениями, то вместо характеристики $il(F)$ естественно рассматривать величину $ill(F)$ — значение параметра k для «самого крупного» кусочно аффинного представления F с линейными разветвляющими отображениями. Из определений следует, что для любого отображения $F \in B(n, m)$ выполнено неравенство

$$il(F) \geqslant 2^{n-ill(F)}.$$

Следующий факт является очевидным: для любого отображения $F \in B(n, m)$ и любых отображений $C \in GA(n) : V_n \to V_n$ и $P \in GA(n) : V_m \to V_m$ выполнены равенства

$$il(PFC) = il(F),$$
$$ill(PFC) = ill(F).$$

В частности, при изучении характеристики $ill(F)$ это позволяет ограничиться рассмотрением линейных разветвляющих отображений специального вида, например «проектирований»:

$$\rho(x_1, \ldots, x_n) = (x_1, \ldots, x_k).$$

Рассмотрим теперь один частный случай кусочно аффинных отображений — кусочно постоянные отображения. Для них все A_i в некотором кусочно аффинном представлении являются постоянными отображениями. Ясно, что все кусочно постоянные представления данного отображения F являются некоторыми «измельчениями» единственного «максимального» кусочно постоянного представления, для которого области кусочного постоянства совпадают с блоками разбиения $F^{-1}(\beta)$. Полезно описать вес кусочно постоянного отображения $F(x) = A_{\rho(x)}(x)$, где $A_i(x) = \beta_i$ и $i = 1, \ldots, N$, — постоянные отображения:

$$|F^{-1}(\beta)| = \begin{cases} \sum\limits_{i:\beta_i=\beta} |\rho^{-1}(i)|, & \text{если } \beta \in \{\beta_1, \ldots, \beta_N\}, \\ 0, & \text{если } \beta \notin \{\beta_1, \ldots, \beta_N\}. \end{cases}$$

2. Соотношение между $\mu l(F)$ и $il(F)$

Лемма. *Пусть $F \in B(n, m)$ — кусочно аффинное отображение и для разветвляющего отображения ρ имеется $\alpha_0 \in V_n$, $\alpha_0 \neq 0$, такое, что при любом $x \in V_n$*

$$\rho(x + \alpha_0) = \rho(x).$$

Тогда $D^{\alpha_0}F$ является кусочно постоянным отображением с тем же разветвляющим отображением ρ.

Доказательство. Пользуясь определением $D^{\alpha_0}F$, кусочной аффинностью F, аффинностью разветвляемых отображений A_i и условием $\rho(x+\alpha_0) \equiv \rho(x)$, получаем

$$(D^{\alpha_0}F)(x) = F(x+\alpha_0) + F(x) = A_{\rho(x+\alpha_0)}(x+\alpha_0) + A_{\rho(x)}(x)$$
$$= A_{\rho(x)}(x) + A_{\rho(x)}(\alpha_0) + A_{\rho(x)}(x) = A_{\rho(x)}(\alpha_0).$$

Тем самым отображение $D^{\alpha_0}F$ представлено в виде кусочно постоянного отображения с разветвляющим отображением ρ. Лемма доказана.

Теорема. *Для любого отображения $F \in B(n,m)$ выполнено неравенство*

$$\mu l(F) \geqslant il(F).$$

Доказательство. Пусть F представлено в виде «самого крупного» кусочно аффинного отображения, так что

$$il(F) = \max_{i=1,\dots,N} |\rho^{-1}(i)|,$$

и для разветвляющего отображения ρ найдется $\alpha_0 \in V_n$, $\alpha_0 \neq 0$, такое, что

$$\rho(x+\alpha_0) = \rho(x) \text{ для всех } x \in V_n.$$

Для оценки $\mu l(F)$ рассмотрим таблицу разностей R^F. Из определения ясно, что

$$\mu l(F) \geqslant \max_{\beta \in V_m} R^F_{\alpha_0,\beta}.$$

Строка $\{R^F_{\alpha_0,\beta}, \beta \in V_m\}$ — это вес отображения $D^{\alpha_0}F$, которое по лемме является кусочно постоянным отображением с разветвляющим отображением ρ. Выше отмечалось, что максимальный элемент веса у такого отображения не меньше $\max\limits_{i=1,\dots,N} |\rho^{-1}(i)|$ — максимального размера области кусочного постоянства. Последняя величина по выбору кусочно аффинного отображения равна $il(F)$. Объединяя все неравенства, получаем

$$\mu l(F) \geqslant il(F).$$

Теорема доказана.

Из сказанного получаем

Следствие. *Для любого отображения $F \in B(n,m)$ выполнено неравенство*

$$\mu l(F) \geqslant 2^{n-ill(F)}.$$

Отметим, что при доказательстве теоремы фактически описывались значения элементов $R^F_{\alpha_0,\beta}$ таблицы R^F. В случае линейных разветвляющих отображений можно продвинуться дальше и описать все элементы таблицы R^F, выразив их через ранги некоторых матриц.

Введем несколько дополнительных обозначений. Пусть $F(x) = A_{\rho(x)}(x)$ — кусочно аффинное отображение с линейным разветвляющим отображением $\rho : V_n \to V_k$. Производную $D^\alpha F$ представим в следующем виде:

$$(D^\alpha F)(x) = F(x+\alpha) + F(x) = A_{\rho(x+\alpha)}(x+\alpha) + A_{\rho(x)}(x)$$
$$= (A_{\rho(x)+\rho(\alpha)} + A_{\rho(x)})(x) + A_{\rho(x)+\rho(\alpha)}(\alpha).$$

По определению величина $R^F_{\alpha,\beta} = |(D^\alpha F)^{-1}(\beta)|$ равна числу решений системы уравнений

$$(A_{\rho(x)+\rho(\alpha)} + A_{\rho(x)})(x) + A_{\rho(x)+\rho(\alpha)}(\alpha) = \beta \tag{1}$$

относительно неизвестных $x \in V_n$ с параметрами $\alpha \in V_n$ и $\beta \in V_m$. Положим $\rho(\alpha) = \delta \in V_k$. Эту систему можно «линеаризовать» в следующем смысле. Введем новый параметр $\varepsilon \in V_k$ и положим $\rho(x) = \varepsilon$. Тогда рассматриваемая система уравнений эквивалентна объединению (в смысле объединения множеств решений) 2^k следующих линейных систем уравнений:

$$\begin{cases} (A_{\varepsilon+\delta} + A_\varepsilon)(x) = \beta + A_{\varepsilon+\delta}(\alpha), \\ \rho(x) = \varepsilon. \end{cases} \tag{2}$$

Множество решений системы (1) является объединением 2^k множеств решений систем (2) для различных $\varepsilon \in V_k$, причем при разных ε множества решений системы (2) не пересекаются. Обозначим ранг матрицы системы (2) через $r(\varepsilon, \delta)$:

$$r(\varepsilon,\delta) = \operatorname{rang} \left\| \begin{matrix} A_{\varepsilon+\delta} + A_\varepsilon \\ \rho \end{matrix} \right\|.$$

Для фиксированных $\alpha \in V_n$, $\beta \in V_m$ через $S(\alpha,\beta)$ обозначим множество совместных систем (2), т. е.

$$S(\alpha,\beta) = \left\{ \varepsilon \in V_k : r(\varepsilon,\delta) = \operatorname{rang} \left\| \begin{matrix} A_{\varepsilon+\delta} + A_\varepsilon & \beta + A_{\varepsilon+\delta}(\alpha) \\ \rho & \varepsilon \end{matrix} \right\| \right\}.$$

(Ранг матрицы системы (2) равен рангу расширенной матрицы.) Теперь уже очевидна следующая

Теорема. *Пусть $F(x) = A_{\rho(x)}(x)$ — кусочно аффинное отображение с линейным разветвляющим отображением $\rho : V_n \to V_k$. Тогда*

$$R^F_{\alpha,\beta} = \sum_{\varepsilon \in S(\alpha,\beta)} 2^{n - r(\varepsilon,\rho(\alpha))}.$$

Полученное для $R^F_{\alpha,\beta}$ выражение показывает, что необходимо подробнее изучать введенные новые характеристики кусочно аффинных отображений $r(\varepsilon,\delta)$ и $S(\alpha,\beta)$.

С другой стороны, доказанные соотношения позволяют подойти к задаче выделения классов отображений F с заданным (минимальным или близким к нему) значением $\mu l(F)$. Можно зафиксировать значение $il(F)$ (или $ill(F)$) и в этом классе минимизировать значение $\mu l(F)$. Классы отображений с заданным значением $ill(F)$ выглядят наиболее прозрачно с алгебраической точки зрения. Поэтому большой интерес представляет задача описания таких отображений F, что

$$\mu l(F) = 2^{n-ill(F)}.$$

ЛИТЕРАТУРА

1. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. **Chabaud F., Vaudenay S.** Links between differential and linear cryptoanalysis // Advances in cryptology-EUROCRYPT'94. Berlin: Springer-Verl., 1995. P. 363–374. (Lecture Notes in Comput. Sci.; V. 950).
3. **Nyberg K.** Differentially uniform mappings for cryptography // Advances in cryptology-EUROCRYPT'93. Berlin: Springer-Verl., 1994. P. 54–64. (Lecture Notes in Comput. Sci.; V. 765).
4. **Rothaus O. S.** On «bent» functions // J. Combin. Theory. Ser. A. 1976. V. 20, N 3. P. 300-305.

Адрес автора:

МГУ, лаборатория по мат.
проблемам криптографии,
Воробьевы горы,
119899 Москва,
Россия

Статья поступила
19 ноября 1996 г.