М. Л. Буряков
Московский государственный университет им. М. В. Ломоносова

О НЕКОТОРЫХ СВОЙСТВАХ КОЭФФИЦИЕНТОВ ЧИСЛОВОЙ НОРМАЛЬНОЙ ФОРМЫ БУЛЕВЫХ ФУНКЦИЙ

1. Введение

Булевы функции играют значительную роль в криптографических приложениях, являясь основными примитивами многих криптосистем, в особенности потоковых шифров. Булевы функции имеют приложение также в теории кодирования. Рассмотрению свойств булевых функций, влияющих на стойкость криптосистем, посвящено огромное количество работ, и новые способы исследования булевых функций могут расширить представления об их свойствах.

Существуют различные способы задания булевых функций: через таблицу истинности, с помощью алгебраической нормальной формы (в русскоязычной литературе часто используется понятие полиномов Жегалкина), с помощью спектральных характеристик функции, с помощью понятия следа. Каждый из этих способов имеет свои преимущества и недостатки для исследования различных свойств булевых функций, в том числе криптографических (см., например, [1]). Также в [1] представлен еще один способ задания любых комплексозначных функций над n-мерном линейным пространством (в том числе булевых) — так называемая числовая нормальная форма функции. Этот способ описания булевых функций используется реже (чем алгебраическая нормальная форма, спектральное и др.), хотя потенциально несет в себе не меньше информации о них.

В данной работе рассматриваются некоторые свойства коэффициентов числовой нормальной формы булевых функций, в частности, некоторые связи между этими коэффициентами и криптографическими параметрами.

2. Обозначения и определения

Будем обозначать F_2 — конечное поле из двух элементов, $V_n = \mathrm{F}_2^{\,n}$ — линейное пространство вектор-столбцов размерности n над полем F_2, BF_n — множество булевых функций от n переменных, то есть множество всех возможных отображений из V_n в F_2. Для $\mathrm{x} \in V_n$ и $f \in \mathrm{F}_n$ через $\mathrm{wt}(\mathbf{x})$ и $\mathrm{wt}(f)$ соответственно обозначим их веса Хэмминга. Скалярное произведение векторов $\mathbf{x}$ и $\mathbf{y}$ из V_n будем обозначать $\langle \mathbf{x}, \mathbf{y} \rangle = \bigoplus_{i=1}^{n} \boldsymbol{x}^{(i)} \boldsymbol{y}^{(i)}$. Представление булевой функции f из BF_n в виде многочлена из кольца $\mathrm{F}_2[x^{(1)}, \ldots, x^{(n)}]/((x^{(1)})^2 \oplus x^{(1)}, \ldots, (x^{(n)})^2 \oplus x^{(n)})$ называют алгебраической нормальной формой (АНФ) данной функции, $\deg f$ — алгебраическая степень этого многочлена ([2]).

Числовой нормальной формой (ЧНФ) булевой функции называют ее представление в виде многочлена с целыми коэффициентами:

$$f(\mathbf{x}) = \sum_{\mathbf{u} \in V_n} \lambda_f(\mathbf{u}) \left(\prod_{i=1} (x^{(i)})^{u^{(i)}} \right) = \sum_{\mathbf{u} \in V_n} \lambda_f(\mathbf{u}) \mathbf{x}^{\mathrm{u}}.$$

В [1] показано, что такое представление существует и единственно для любой комплекснозначной функции на V_n.

Пусть $f \in BF_n$. Для наборов $1 \le i_1 < \ldots < i_k \le n$ и $\mathbf{b} = (b^{(1)}, \ldots, b^{(k)})^T \in V_k$ при $k \le n$ обозначим через $f_{i_1, \ldots, i_k}^{b^{(1)}, \ldots, b^{(k)}}$ булеву функцию из F_{n-k}, полученную из f фиксацией переменных $x^{(i_1)} = b^{(1)}, \ldots, x^{(i_1)} = b^{(k)}$ и называемую подфункцией функции f (см. [2]).

Для произвольной функции $f \in BF_n$ и произвольного вектора $\boldsymbol{u} \in V_n$ определим коэффициенты Фурье

$$\overline{W}_f(\mathbf{u}) = \sum_{\mathbf{u} \in V_n} f(\mathbf{x})(-1)^{\langle \boldsymbol{u}, \boldsymbol{x} \rangle}$$

и коэффициенты Уолша-Адамара

$$W_f(\mathbf{u}) = \sum_{\mathbf{x}\in V_n} (-1)^{f(\mathbf{x})\oplus\langle \mathbf{u}.\mathbf{x}\rangle}$$

этой функции.

Нелинейностью булевой функции называют ее удаленность от функций со степенью не больше 1:

$$N_f = \max_{\substack{g\in F_n,\\ \deg g\le 1}} \operatorname{dist}(f,g) = 2^{n-1} - \frac{1}{2}\max_{\mathbf{u}\in V_n}\left|W_f(\mathbf{u})\right|.$$

Булева функция $f \in BF_n$ называется корреляционно-иммунной порядка, m, $1 \le m \le n$ если для любой подфункции этой функции выполняется соотношение

$$\mathrm{wt}\left(f_{i_1,\ldots,i_m}^{a^{(1)},\ldots,a^{(m)}}\right) = \frac{\mathrm{wt}(f)}{2^m}.$$

Частичным уровнем аффинности (см. [3]) $\mathrm{la}^0 f$ булевой функции $f \in BF_n$ называется наименьшее число k, при котором существует подфункция функции f такая, что $\deg f_{i_1,\ldots,i_k}^{0,\ldots,0} \le 1$.

3. Свойства коэффициентов ЧНФ

В [1] показано, что коэффициенты ЧНФ функции $f \in BF_n$ выражаются через значения этой функции по формуле:

$$\lambda_f(\mathbf{u}) = (-1)^{\mathrm{wt}(\mathbf{u})} \sum_{\mathbf{x}\in V_n,\mathbf{x}\le\mathbf{u}} (-1)^{\mathrm{wt}(\mathbf{x})} f(\mathbf{x}). \qquad (1)$$

Непосредственно из формулы (1) видно, что для любой функции $f \in BF_n$ и любого вектора $\boldsymbol{x} \in V_n$ выполняется неравенство $\left|\lambda_f(\mathbf{u})\right| \le 2^{\mathrm{wt}(\mathbf{u})}$. Также можно показать более точную оценку.

Предложение 1. *Для коэффициентов числовой нормальной формы булевой функции $f(\boldsymbol{x})$ для векторов $\boldsymbol{u} \neq \boldsymbol{0}$ выполняется неравенство:*

$$\left|\lambda_f(\mathbf{u})\right| \le 2^{\mathrm{wt}(\mathbf{u})-1}.$$

Доказательство. Воспользуемся формулой (1):

$$\lambda_f(\mathbf{u}) = (-1)^{\mathrm{wt}(\mathbf{u})} \sum_{\mathbf{x}\in V_n,\mathbf{x}\le\mathbf{u}} (-1)^{\mathrm{wt}(\mathbf{x})} f(\mathbf{x}) = (-1)^{\mathrm{wt}(\mathbf{u})}\left[\sum_{\substack{\mathbf{x}\in V_n,\mathbf{x}\le\mathbf{u}\\ \mathrm{wt}(\mathbf{x})=0 \bmod 2}} f(\mathbf{x}) - \sum_{\substack{\mathbf{x}\in V_n,\mathbf{x}\le\mathbf{u}\\ \mathrm{wt}(\mathbf{x})=1 \bmod 2}} f(\mathbf{x})\right].$$

Заметим, что количество векторов, по которым ведется суммирование в первой сумме, равно количеству векторов, по которым ведется суммирование во второй сумме, и равно $2^{\mathrm{wt}(u)-1}$. Отсюда непосредственно следует справедливость доказываемого утверждения.

Также известно ([1]), что для коэффициентов ЧНФ булевой функции справедливо их представление через коэффициенты Фурье и Уолша-Адамара этой функции:

$$\lambda_f(\mathbf{u}) = 2^{-n}(-2)^{\mathrm{wt}(\mathbf{u})} \sum_{\mathbf{x}\in V_n,\mathbf{x}\ge\mathbf{u}} \overline{W}_f(\mathbf{x}), \qquad (2)$$

$$\lambda_f(\mathbf{u}) = (-1)^{\mathrm{wt}(\mathbf{u})} \frac{2^{\mathrm{wt}(\mathbf{u})}}{2^{n+1}}\left[\frac{\delta(\mathbf{u})}{2} - \sum_{\mathbf{x}\in V_n,\mathbf{x}\ge\mathbf{u}} W_f(\mathbf{x})\right]. \qquad (3)$$

Поскольку для корреляционно-иммунных функций порядка все коэффициенты Уолша равны нулю $\bmod 2^{m+1}$ (см. [2]), то непосредственно из формулы (2) следует, что для таких функций все коэффициенты числовой нормальной формы равны нулю $\bmod 2^{\mathrm{wt}(\mathbf{u})+m+1-n}$ (при $\mathrm{wt}(\mathbf{u}) + m + 1 \ge n$) и не превосходят по модулю 4^{m+1}.

Предложение 2. *Для коэффициентов числовой нормальной формы булевой функции* $f(\mathbf{x})$ *при* $\mathbf{u} \neq \mathbf{0}$ *выполняется неравенство:*

$$\left|\lambda_f(\mathbf{u})\right| \le \frac{1}{2}\max_{\mathbf{v}\in V_n}\left|W_f(\mathbf{v})\right|.$$

Доказательство. Доказательство утверждения следует из формулы (3):

$$\left|\lambda_f(\mathbf{u})\right| \le \frac{2^{\mathrm{wt}(\mathbf{u})}}{2^{n+1}}\sum_{\mathbf{x}\in V_n,\mathbf{x}\ge\mathbf{u}}\left|W_f(\mathbf{x})\right| \le \frac{2^{\mathrm{wt}(\mathbf{u})}}{2^{n+1}}\cdot 2^{n-\mathrm{wt}(\mathbf{u})}\max_{\mathbf{v}\in V_n}\left|W_f(\mathbf{v})\right| \le \frac{1}{2}\max_{\mathbf{v}\in V_n}\left|W_f(\mathbf{v})\right|.$$

Из предложения 2, в частности, следует оценка нелинейности N_f функции $f(\mathbf{x})$ через коэффициенты числовой нормальной формы:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\mathbf{x}\in V_n}\left|W_f(\mathbf{x})\right| \le 2^{n-1} - \max_{\mathbf{v}\in V_n,\mathbf{v}\neq\mathbf{0}}\left|\lambda_f(\mathbf{v})\right|.$$

Предложение 3. *Пусть* $f \in BF_n$, $\mathbf{u} \in V_n$, $\mathrm{wt}(\mathbf{u}) = k > 0$, $\{i_1, \ldots, i_k\} = \{1, \ldots, n\} \setminus \mathrm{supp}(\mathbf{u})$. *Тогда*

$$\lambda_f(\mathbf{u}) = (-1)^k\left[\mathrm{wt}\left(f'^{0,\ldots,0}_{i_1,\ldots,i_{n-k}}\right) - 2^{k-1}\right],$$

где $f'(\mathbf{x}) = f(\mathbf{x}) \oplus \langle \mathbf{x}, \mathbf{1}\rangle$.

Доказательство. Известно ([2]), что для любой булевой функции $f \in BF_n$ и вектора $\mathbf{v} \in V_n$ веса m выполняется равенство:

$$\sum_{\mathbf{x}\in V_n,\mathbf{x}\le\mathbf{v}} W_f(\mathbf{x}) = 2^n - 2^{m+1}\,\mathrm{wt}\left(f^{0,\ldots,0}_{i_1,\ldots,i_m}\right), \qquad (4)$$

где $i_1, \ldots, i_n$ — координаты вектора $\mathbf{v}$, равные 1.

Воспользуемся для нашего случая формулой (3):

$$\lambda_f(\mathbf{u}) = (-1)^{k+1}\frac{2^k}{2^{n+1}}\sum_{\mathbf{x}\in V_n,\mathbf{x}\ge\mathbf{u}} W_f(\mathbf{x}) = (-1)^{k+1}\frac{2^k}{2^{n+1}}\sum_{\substack{\mathbf{x}\in V_n,\\ \mathbf{x}\oplus 1\le\mathbf{u}\oplus 1}} W_f(\mathbf{x}) = (-1)^{k+1}\frac{2^k}{2^{n+1}}\sum_{\substack{\mathbf{x}\in V_n,\\ \mathbf{x}\le\mathbf{u}\oplus 1}} W_{f'}(\mathbf{x}).$$

Далее применяем формулу (4) и получаем:

$$\lambda_f(\mathbf{u}) = (-1)^{k+1}\frac{2^k}{2^{n+1}}\sum_{\substack{\mathbf{x}\in V_n,\\ \mathbf{x}\le\mathbf{u}\oplus 1}} W_{f'}(\mathbf{x}) = (-1)^{k+1}\frac{2^k}{2^{n+1}}\left[2^n - 2^{n-k+1}\,\mathrm{wt}\left(f'^{0,\ldots,0}_{i_1,\ldots,i_{n-k}}\right)\right] = (-1)^k\left[\mathrm{wt}\left(f'^{0,\ldots,0}_{i_1,\ldots,i_{n-k}}\right) - 2^{k-1}\right].$$

Из предложения 3 следует, что если

$$\max_{\substack{\mathbf{u}\in V_n,\\ |\lambda_f(\mathbf{u})| = 2^{\mathrm{wt}(\mathbf{u})-1}}} \mathrm{wt}(\mathbf{u}) = k,$$

то $\mathrm{la}^0 f \le n - k$.

Предложение 4. *Пусть* $f \in BF_n$ *и* $\deg f \le r$ *(степень АНФ). Тогда для коэффициентов числовой нормальной формы этой функции выполняется неравенство:*

$$\left|\lambda_f(\mathbf{u})\right| < 4^{\left\lceil \frac{n}{r}\right\rceil - 1}.$$

Доказательство. Согласно теореме Мак-Эллис ([2]) коэффициенты Фурье $\overline{W}_f(\mathbf{u})$ делятся на $2^{\lceil n/r\rceil - 1}$ для любого $\mathbf{u} \in V_n$. Отсюда с учетом формулы (2) следует, что

$$\left|\lambda_f(\mathbf{u})\right| \le \frac{2^{\mathrm{wt}(\mathbf{u})}}{2^n}\sum_{\mathbf{x}\in V_n,\mathbf{x}\ge\mathbf{u}} q_{\mathbf{x}}\,2^{\left\lceil \frac{n}{r}\right\rceil - 1} = \frac{2^{\mathrm{wt}(\mathbf{u}) + \left\lceil \frac{n}{r}\right\rceil - 1}}{2^n}\sum_{\mathbf{x}\in V_n,\mathbf{x}\ge\mathbf{u}} q_{\mathbf{x}},$$

где $q_{\mathbf{x}}$ — некоторые целые числа, $0 \le q_{\mathbf{x}} < 2^{\lceil n/r\rceil - 1}$.

Получаем, что

$$\left|\lambda_f(\mathbf{u})\right| < \frac{2^{\mathrm{wt}(\mathbf{u}) + \left\lceil \frac{n}{r}\right\rceil - 1}}{2^n}\cdot 2^{n-\mathrm{wt}(\mathbf{u})}\cdot 2^{\left\lceil \frac{n}{r}\right\rceil - 1} = 4^{\left\lceil \frac{n}{r}\right\rceil - 1}.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Carlet C., Guillot P.* A new representation of Boolean functions // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 13th International Symposium, AAECC-13, Lecture Notes in Computer Science. Vol. 1719. Springer-Verlag, 1999. P. 94–103.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптографии. М.: МЦНМО, 2004.
3. *Логачев О. А., Сальников А. А., Ященко В. В.* Комбинирующие k-аффинные функции // Математика и безопасность информационных технологий. Материалы конференции в МГУ, 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 176–178.

В. Г. Криволапов
Московский инженерно-физический институт (государственный университет)

РЕАЛИЗАЦИЯ МОДЕЛИ СИСТЕМЫ РЕАГИРОВАНИЯ НА DOS-АТАКИ СЕТЯМИ ПЕТРИ

Понятие системы довольно многогранно. Так, С. Кельтон и Дж. Лоу в своей книге «Имитационное моделирование» дают следующее определение: система — это совокупность объектов, например, людей или механизмов, функционирующих и взаимодействующих друг с другом для достижения определенной цели [1. С. 20–23]. Для анализа системы используют проведение опытов с реальной системой либо эксперименты с моделью этой системы. Когда модель достаточно проста, можно вычислить ее соотношения и параметры и по-лучить точное аналитическое решение. Однако некоторые аналитические решения могут быть чрезвычайно сложными и требовать при этом огромных компьютерных ресурсов. В этом случае модель следует изучать с помощью имитационного моделирования, то есть многократного испытания модели с нужными входными данными, чтобы определить их влияние на выходные критерии оценки работы системы. Применительно к модели процесса защиты, исходя из того, что процесс защиты довольно трудно представить аналитически, предпочтительнее имитационные методы как наиболее универсальные, поэтому в качестве подхода к моделированию системы информационной безопасности предлагается использовать аппарат сетей Петри [7].

Сети Петри — это инструмент для математического моделирования и исследования сложных систем. Цель представления системы в виде сети Петри и последующего анализа этой сети состоит в получении важной информации о структуре и динамическом поведении моделируемой системы. На данный момент теория сетей Петри довольно хорошо изучена и используется в различных предметных областях, к примеру [2, 3, 4, 5, 6]. Что особенно важно, так это существование для сетей Петри алгоритмически эффективных способов решения задач достижимости, безопасности и конечности сетей, представляющих основной интерес при моделировании задач информационной безопасности.

В сети Петри условия моделируются позициями, события — переходами. При этом входы перехода являются предусловиями соответствующего события; выходы — постусловиями. Возникновение события моделируется запуском соответствующего перехода. Выполнение условия представляется фишкой в позиции, соответствующей этому условию. Запуск перехода удаляет фишки, представляющие выполнение предусловий, и образует новые фишки, которые представляют выполнение постусловий.

Важная особенность сетей Петри — это их асинхронная природа. В сетях Петри отсутствует измерение времени. В них учитывается лишь важнейшее свойство времени — частичное упорядочение событий.