ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и кибернетики
Кафедра защиты информации и криптографии

И.А. Панкратова

БУЛЕВЫ ФУНКЦИИ В КРИПТОГРАФИИ

Учебное пособие

Томск
2014

УДК 519.7
П164

Панкратова И.А.
П164 Булевы функции в криптографии : учеб. пособие. – Томск : Издательский Дом Томского государственного университета, 2014. – 88 с.

Пособие представляет собой конспект курса лекций с тем же названием, читаемого автором в течение ряда лет студентам кафедры защиты информации и криптографии по специальности «Компьютерная безопасность». Знакомство с курсом предполагает знание студентами основ дискретной математики (раздел «Булевы функции») и начальных понятий алгебры и теории вероятностей.

Предисловие автора

Булевы функции играют большую роль в криптографии, в частности, при построении поточных шифров — в качестве комбинирующих и фильтрующих функций в генераторах ключевого потока; блочных шифров — в качестве функций блоков замены, и др. Для обеспечения стойкости этих шифров к различным видам атак (статистическим, алгебраическим, дифференциальному и линейному криптоанализу, ...) функции должны удовлетворять целому ряду требований, часто противоречащих друг другу:

— уравновешенность;
— высокая степень нелинейности;
— отсутствие корреляции со своими переменными;
— существенная и нелинейная зависимость от всех переменных;
— отсутствие запрета
— и т. д.

В данном пособии изучаются все эти свойства булевых функций (которые, ввиду их важности для приложений, можно назвать «криптографическими») и рассматриваются некоторые вопросы построения булевых функций с «хорошими» криптографическими свойствами. Несмотря на наличие многочисленных публикаций на эти темы, в том числе и ряда учебников (отметим, прежде всего, книги [1, 4, 8, 11]), многие вопросы пока ещё остаются открытыми; некоторые из них упоминаются и в данном пособии. Более того, видимо, многие вопросы даже ещё и не поставлены перед наукой, и полнота здесь едва ли возможна в силу того, что постоянно появляются новые атаки на шифры и, как следствие, необходимость вводить и исследовать новые требования к шифрам и к используемым в них функциям.

В конце разделов 1–4 приведены задачи, которые рекомендуется решить для лучшего усвоения теоретического материала. Решения некоторых наиболее интересных задач (их номера отмечены звёздочками) можно найти в разделе 7.

Автор выражает признательность Г. П. Агибалову за ценные рекомендации по улучшению пособия, а также студентам кафедры защиты информации и криптографии, чьи вопросы и замечания во время лекций помогли устранить ряд неточностей в изложении. Информация о всех замеченных ошибках и опечатках будет с благодарностью принята по адресу pank@isc.tsu.ru.

Основные обозначения

$\mathbb{Z}_2$	поле из двух элементов 0 и 1;
$P_2(n)$	множество всех булевых функций от n переменных;
$\mathrm{w}(a)$	вес булева вектора a;
$\Pr[A]$	вероятность случайного события A;
$\mu(f)$	преобразование Мёбиуса функции f;
$\deg f$	(алгебраическая) степень функции f;
$\mathcal{A}(n)$	множество всех аффинных функций в $P_2(n)$;
$\mathcal{L}(n)$	множество всех линейных функций в $P_2(n)$;
$\mathcal{B}(n)$	множество всех бент-функций в $P_2(n)$;
$\mathcal{LS}(n)$	множество всех функций в $P_2(n)$, имеющих линейную структуру;
(a, x)	(булево) скалярное произведение булевых векторов a и x;
$\langle a, x\rangle$	арифметическое скалярное произведение булевых векторов a и x;
$\mathrm{cor}(f)$	максимальный порядок корреляционной иммунности функции f;
$\mathrm{sut}(f)$	максимальный порядок устойчивости функции f;
$\mathrm{d}(f, g)$	расстояние между функциями f и g;
$\hat{f}$	преобразование Уолша — Адамара функции f;
$\delta(a, b)$	символ Кронекера: $\delta(a,b) = \begin{cases} 1, & \text{если } a = b, \\ 0 & \text{иначе;} \end{cases}$
F	характеристическая последовательность функции f: $F = \left((-1)^{f(0^n)} \dots (-1)^{f(1^n)}\right)$;
$\widehat{F}$	вектор коэффициентов преобразования Уолша — Адамара функции f: $\widehat{F} = \left(\hat{f}(0^n) \dots \hat{f}(1^n)\right)$;
N_f	нелинейность функции f;
$N(n)$	функция Шеннона для нелинейности;
CN_f	совершенная нелинейность функции f;
$CN(n)$	функция Шеннона для совершенной нелинейности;
$\begin{pmatrix} n \\ m \end{pmatrix}$	число сочетаний из n по m;
$f'_a(x)$	производная функции f по направлению a: $f'_a(x) = f(x) \oplus f(x \oplus a)$;

$\Delta_{f,g}(x)$	функция взаимной корреляции f и g;
$\Delta_f(x)$	функция автокорреляции f;
SAC	строгий лавинный критерий;
SAC(m)	строгий лавинный критерий порядка m;
PC(k)	критерий распространения степени k;
PC(k, m)	критерий распространения степени k порядка m;
M_{Δ_f}	количество ненулевых значений функции автокорреляции f;
$M_{\hat{f}}$	количество ненулевых коэффициентов Уолша — Адамара функции f;
σ_f	лавинная характеристика f — сумма квадратов;
Δ_f	лавинная характеристика f — абсолютный показатель;
AN(f)	множество аннигиляторов функции f;
AI(f)	алгебраическая иммунность функции f.

1. Корреляционная иммунность булевых функций

1.1. Вес функции

Булевой функцией от n переменных называется функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. Будем обозначать множество всех булевых функций от n переменных через $P_2(n)$; ясно, что $|P_2(n)| = 2^{2^n}$.

Весом булева вектора $a = a_1 \dots a_n$ называется количество единичных компонент в нём; будем обозначать вес через $\mathrm{w}(a)$: $\mathrm{w}(a) = \sum\limits_{i=1}^{n} a_i$. Так же будем обозначать и *вес булевой функции* $f \in P_2(n)$: $\mathrm{w}(f) = \sum\limits_{x \in \mathbb{Z}_2^n} f(x) = |\{x \in \mathbb{Z}_2^n : f(x) = 1\}|$. Если $\mathrm{w}(f) = 2^{n-1}$, то функция f называется *уравновешенной* или *равновероятной*, так как она при случайном выборе аргумента x принимает оба значения с одинаковой вероятностью: $\Pr[f(x)=1] = \Pr[f(x)=0]$, где по определению $\Pr[f(x)=1] = \mathrm{w}(f)/2^n$ и $\Pr[f(x)=0] = 1 - \Pr[f(x)=1]$. В криптографических приложениях очень часто рассматриваются именно уравновешенные функции.

Утверждение 1.1 (о весе булевой функции).

1. Пусть функция g зависит от аргумента y фиктивно, т. е. $g(x_1, \dots, x_n, y) = f(x_1, \dots, x_n)$. Тогда $\mathrm{w}(g) = 2\mathrm{w}(f)$.
2. Пусть $f(x_1, \dots, x_n)$ и $g(y_1, \dots, y_m)$ зависят от непересекающихся множеств переменных. Тогда:
   а) функция $f \cdot g$ не уравновешена, если f и g — не константы 1;
   б) функция $f \oplus g$ уравновешена, если и только если f или g уравновешена.

Доказательство.

1. Утверждение следует из того, что $g(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n, 1) = f(x_1, \dots, x_n)$ для всех $x_1 \dots x_n \in \mathbb{Z}_2^n$.
2. Обозначим $x = x_1 \dots x_n$, $y = y_1 \dots y_m$.
   а) Пусть $\mathrm{w}(f)=r < 2^n$, $\mathrm{w}(g)=s < 2^m$. Поскольку $f(x)g(y)=1$, если и только если $f(x) = 1$ и $g(y) = 1$, то $\mathrm{w}(f \cdot g) = rs$. Предположим, что функция $f \cdot g$ уравновешена, т. е. $2^{n+m-1} = \mathrm{w}(f \cdot g) = rs$. Тогда $r = 2^k$ и $s = 2^l$ для некоторых $k \leqslant n-1$, $l \leqslant m-1$. Значит, $\mathrm{w}(f \cdot g) \leqslant 2^{n+m-2}$, что противоречит предположению.
   б) Заметим, что $f(x) \oplus g(y)=1$, если и только если $f(x) \neq g(y)$. Следовательно, $\mathrm{w}(f \oplus g) = \mathrm{w}(f)\mathrm{w}(\bar{g}) + \mathrm{w}(g)\mathrm{w}(\bar{f})$.

Достаточность. Пусть функция f уравновешена, т. е. $\mathrm{w}(f) = \mathrm{w}(\bar{f}) = 2^{n-1}$. Тогда $\mathrm{w}(f \oplus g) = 2^{n-1}(\mathrm{w}(g) + \mathrm{w}(\bar{g})) = 2^{n+m-1}$.

Необходимость. Предположим, что $\mathrm{w}(f) = r \neq 2^{n-1}$ и $\mathrm{w}(g) = s$. Тогда $\mathrm{w}(f \oplus g) = r(2^m - s) + s(2^n - r) = (2^n - 2r)s + 2^m r = 2^{n+m-1}$; последнее равенство имеет место в силу уравновешенности $f \oplus g$. Отсюда запишем: $s = (2^{n+m-1} - 2^m r)/(2^n - 2r) = 2^{m-1}$, что означает уравновешенность функции g.

Утверждение доказано. ■

Заметим, что п. 1 утверждения 1.1 означает, что добавление или удаление фиктивной переменной не влияет на уравновешенность функции.

1.2. Алгебраическая нормальная форма булевой функции

Вспомним известные из курса дискретной математики свойства булевых функций.

1. Разложение Шеннона:
   $f(x_1, \ldots, x_n) = \overline{x}_1 f(0, x_2, \ldots, x_n) \vee x_1 f(1, x_2, \ldots, x_n)$;
2. $\overline{x} = x \oplus 1$;
3. $x \vee y = x \oplus y \oplus xy$.

С учётом свойств 2 и 3 разложение Шеннона можно переписать следующим образом:
$f(x_1, \ldots, x_n) = (x_1 \oplus 0 \oplus 1) f(0, x_2, \ldots, x_n) \oplus (x_1 \oplus 1 \oplus 1) f(1, x_2, \ldots, x_n)$.

Разложение можно проводить по любому количеству переменных.

Утверждение 1.2 (о разложении по переменным).
Пусть $f \in P_2(n)$, $m \leqslant n$. Тогда

$$f(x_1, \ldots, x_n) = \bigoplus_{a_1 \ldots a_m \in \mathbb{Z}_2^m} (x_1 \oplus a_1 \oplus 1) \cdot \ldots \times \times (x_m \oplus a_m \oplus 1) f(a_1, \ldots, a_m, x_{m+1}, \ldots, x_n). \tag{1.1}$$

Доказательство. Выберем произвольный набор $b_1 \ldots b_m \in \mathbb{Z}_2^m$ и подставим его в формулу (1.1) вместо переменных $x_1 \ldots x_m$. Слева получим $f(b_1, \ldots, b_m, x_{m+1}, \ldots, x_n)$; в сумме справа в силу условия $b_i \oplus a_i \oplus 1 = 1 \Leftrightarrow b_i = a_i$ останется одно слагаемое, также равное $f(b_1, \ldots, b_m, x_{m+1}, \ldots, x_n)$. ■

Функции $f(a_1, \ldots, a_m, x_{m+1}, \ldots, x_n)$ из формулы (1.1) называются *коэффициентами разложения функции f по переменным* $x_1, \ldots, x_m$.

Утверждение 1.3. Пусть $f_1, \ldots, f_{2^m}$ — все коэффициенты разложения функции f по некоторым m переменным. Тогда

$$\mathrm{w}(f) = \sum_{i=1}^{2^m} \mathrm{w}(f_i).$$

Доказательство. Следует из того, что области определения функций f_i образуют разбиение области определения функции f, и в своей области определения f_i совпадает с f. ■

Запишем разложение функции $f \in P_2(n)$ по всем переменным:

$$\begin{aligned} f(x_1, \ldots, x_n) &= \bigoplus_{a_1 \ldots a_n \in \mathbb{Z}_2^n} (x_1 \oplus a_1 \oplus 1) \cdot \ldots \times \\ &\times (x_n \oplus a_n \oplus 1) f(a_1, \ldots, a_n) = \\ &= \bigoplus_{\substack{a_1 \ldots a_n \in \mathbb{Z}_2^n: \\ f(a_1, \ldots, a_n) = 1}} (x_1 \oplus a_1 \oplus 1) \cdot \ldots \cdot (x_n \oplus a_n \oplus 1). \end{aligned} \tag{1.2}$$

Представление (1.2) называется *совершенной алгебраической нормальной формой* функции f. Раскроем в нём скобки и приведём подобные слагаемые ($u \oplus u = 0$); получим *алгебраическую нормальную форму* (*АНФ*) функции f — сумму различных слагаемых (*мономов*) вида $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$, где, как обычно, $x^0 = 1$, $x^1 = x$. В русской литературе АНФ обычно называют *полиномом Жегалкина*.

Представление булевой функции в виде АНФ единственно, что доказывается из мощностных соображений: всего различных мономов 2^n, поэтому из них можно составить 2^{2^n} различных сумм — столько же, сколько существует функций в $P_2(n)$, и каждая сумма (формула) задаёт единственную функцию.

Сопоставим функции $f(x_1, \ldots, x_n)$ булеву функцию $g(x_1, \ldots, x_n)$, положив $g(a_1, \ldots, a_n) = 1$ в том и только в том случае, когда моном $x_1^{a_1} \ldots x_n^{a_n}$ входит в АНФ функции f в качестве слагаемого. Тогда можно записать:

$$f(x_1, \ldots, x_n) = \bigoplus_{a_1 \ldots a_n \in \mathbb{Z}_2^n} g(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}. \tag{1.3}$$

Значения функции g называются *коэффициентами АНФ* функции f; отображение μ на множестве булевых функций, при котором $\mu(f) = g$ — *преобразованием Мёбиуса*.

Пример 1.1. Пусть функция $f(x_1, x_2, x_3)$ задана следующей таблицей:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

По формуле (1.2) построим совершенную алгебраическую нормальную форму функции f, а затем преобразуем её в АНФ:

$$f(x_1, x_2, x_3) = (x_1 \oplus 1)(x_2 \oplus 1)x_3 \oplus (x_1 \oplus 1)x_2x_3 \oplus x_1x_2(x_3 \oplus 1) \oplus$$
$$\oplus x_1x_2x_3 = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 \oplus x_1x_2x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus$$
$$\oplus x_1x_2 \oplus x_1x_2x_3 = x_1x_3 \oplus x_3 \oplus x_1x_2.$$

Таким образом, получили следующее преобразование Мёбиуса функции f:

a_1	a_2	a_3	$\mu(f)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Описанный способ вычисления преобразования Мёбиуса является трудоёмким и малопригодным для программной реализации. Выведем более простую формулу получения $\mu(f)$.

Заметим, что $x_i^{a_i} = 1$, если и только если $a_i \leqslant x_i$. Обозначим $x = x_1 \dots x_n$, $a = a_1 \dots a_n$, $x^a = x_1^{a_1} \dots x_n^{a_n}$. Тогда $x^a = 1$, если и

только если $a \leqslant x$, т. е. $a_i \leqslant x_i$ для всех $i = 1, \ldots, n$. С учётом этого формулу (1.3) можно переписать следующим образом:

$$f(x) = \bigoplus_{a \in \mathbb{Z}_2^n} g(a) x^a = \bigoplus_{a \leqslant x} g(a). \tag{1.4}$$

Это позволяет вычислять значения функции f по её коэффициентам АНФ. Например, для функции f из примера 1.1:
$f(0,0,1) = g(0,0,0) \oplus g(0,0,1) = 1$;
$f(0,1,0) = g(0,0,0) \oplus g(0,1,0) = 0$;
$f(0,1,1) = g(0,0,0) \oplus g(0,0,1) \oplus g(0,1,0) \oplus g(0,1,1) = 1$;
и т. д.

Верно обращение формулы (1.4).

Утверждение 1.4 (о преобразовании Мёбиуса). Пусть $f \in P_2(n)$, $g = \mu(f)$. Тогда для любого $a \in \mathbb{Z}_2^n$ имеет место

$$g(a) = \bigoplus_{x \leqslant a} f(x). \tag{1.5}$$

Доказательство. Индукция по весу вектора a.

Б а з а и н д у к ц и и. $g(0^n) = f(0^n)$ (0^n — это вектор длины n веса 0).

П р е д п о л о ж е н и е и н д у к ц и и. Пусть утверждение верно для всех векторов a веса меньше, чем p.

Ш а г и н д у к ц и и. Докажем утверждение для вектора a веса p. По формуле (1.4) и по предположению индукции запишем

$$f(a) = \bigoplus_{x \leqslant a} g(x) = \bigoplus_{x < a} g(x) \oplus g(a) = \bigoplus_{x < a} \bigoplus_{y \leqslant x} f(y) \oplus g(a).$$

Обозначим двойную сумму в последней части равенства через S и присмотримся к ней внимательнее:

$$S = \bigoplus_{x < a} \bigoplus_{y \leqslant x} f(y) = \bigoplus_{y < a} f(y) \bigoplus_{y \leqslant x < a} 1 = \bigoplus_{y < a} f(y).$$

Здесь последнее равенство имеет место в силу того, что существует $(2^{\mathrm{w}(a) - \mathrm{w}(y)} - 1)$ — нечётное число — таких x, для которых выполнено условие $y \leqslant x < a$. Следовательно, $g(a) = S \oplus f(a) = \bigoplus_{y \leqslant a} f(y)$. ■

Следствие 1. $\mu(\mu(f)) = f$.

Определение 1.1. *Степенью монома* называется количество сомножителей в нём. Наибольшая степень монома в АНФ функции f называется *степенью* (*алгебраической степенью*) функции f; обозначается $\deg f$.

Так, функция из примера 1.1 имеет степень 2.

Следствие 2. Пусть $f \in P_2(n)$. Тогда $\deg f = n$, если и только если $\mathrm{w}(f)$ нечётен.

Утверждение следует из равенства $g(1^n) = \bigoplus\limits_{x \in \mathbb{Z}_2^n} f(x)$, где 1^n — это вектор длины n, состоящий из единиц.

Таким образом, половина всех булевых функций имеет максимально возможную степень.

Определение 1.2. *Скалярным произведением* векторов $a, x \in \mathbb{Z}_2^n$ называется выражение $(a, x) = a_1 x_1 \oplus \ldots \oplus a_n x_n$. Функция (a, x) называется *линейной*; множество всех линейных функций от n переменных обозначается $\mathcal{L}(n)$:

$$\mathcal{L}(n) = \{(a, x) : a \in \mathbb{Z}_2^n\}.$$

Функция степени 0 или 1 называется *аффинной*; множество всех аффинных функций от n переменных обозначается $\mathcal{A}(n)$:

$$\mathcal{A}(n) = \{a_0 \oplus (a, x) : a_0 \in \mathbb{Z}_2, a \in \mathbb{Z}_2^n\}.$$

Докажем ещё одно полезное утверждение.

Утверждение 1.5 (о связи веса и степени функции). Если $f \in P_2(n)$ и $\deg f = d \geqslant 1$, то $2^{n-d} \leqslant \mathrm{w}(f) \leqslant 2^n - 2^{n-d}$.

Доказательство. Пусть $x_{i_1} x_{i_2} \ldots x_{i_d}$ — моном наибольшей степени, входящий в АНФ функции f. Разложим f по остальным (не входящим в данный моном) $n - d$ переменным; пусть $f_1, \ldots, f_{2^{n-d}}$ — коэффициенты этого разложения. В АНФ каждого из коэффициентов входит слагаемое $x_{i_1} x_{i_2} \ldots x_{i_d}$, поэтому все эти коэффициенты не являются константами. Значит, $1 \leqslant \mathrm{w}(f_i) \leqslant 2^d - 1$ для $i = 1, \ldots, 2^{n-d}$, и $\mathrm{w}(f) = \sum\limits_{i=1}^{2^{n-d}} \mathrm{w}(f_i)$ по утверждению 1.3. Отсюда получаем нужные неравенства. ■

В частности, если $\deg f = 1$, то функция f уравновешена.

1.3. Линейные и квазилинейные переменные

Определение 1.3. Говорят, что *функция* $f(x_1, \ldots, x_n)$ *линейно зависит от переменной* x_i, если f представима в виде

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus x_i,$$

где $g \in P_2(n-1)$.

Из утверждения 1.1 (свойство $2б$) следует: если функция зависит линейно от некоторой своей переменной, то она уравновешена.

Определение линейной зависимости от переменной можно переформулировать так: $f(x_1, \ldots, x_n)$ зависит от переменной x_i линейно, если $f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$ для всех $a_1 \ldots a_{i-1} a_{i+1} \ldots a_n \in \mathbb{Z}_2^{n-1}$. По аналогии вводится понятие квазилинейных переменных.

Определение 1.4. Говорят, что *функция* $f(x_1, \ldots, x_n)$ *зависит от пары своих переменных* x_i, x_j *квазилинейно*, если $f(a) \neq f(b)$ для любых двух наборов $a, b \in \mathbb{Z}_2^n$, различающихся только в i-й и j-й компонентах; в этом случае переменные x_i, x_j называются *квазилинейной парой переменных.*

Утверждение 1.6. Функция $f(x_1, \ldots, x_n, y, z)$ зависит от y, z квазилинейно, если и только если f может быть представлена в следующем виде:

$$f(x_1, \ldots, x_n, y, z) = g(x_1, \ldots, x_n, y \oplus z) \oplus y.$$

Доказательство. Пусть x — произвольный набор из $\mathbb{Z}_2^n$.
Достаточность.

$$f(x,0,0) = g(x,0); \quad f(x,1,1) = g(x,0) \oplus 1 = \bar{f}(x,0,0);$$
$$f(x,0,1) = g(x,1); \quad f(x,1,0) = g(x,1) \oplus 1 = \bar{f}(x,0,1).$$

Необходимость. Требуемое представление получается после разложения f по y, z, замены $f(x,1,1)$ на $f(x,0,0) \oplus 1$, $f(x,1,0)$ на $f(x,0,1) \oplus 1$, раскрытия скобок и приведения подобных. ■

Утверждение 1.7. Если функция зависит от пары своих переменных квазилинейно, то она уравновешена.

Доказательство. Пусть $x \in \mathbb{Z}_2^n$, $f(x,y,z) \in P_2(n+2)$ и f зависит от переменных y, z квазилинейно. Тогда по утверждению 1.6 функцию f можно представить в виде

$$f(x_1,\ldots,x_n,y,z) = g(x_1,\ldots,x_n,y\oplus z)\oplus y.$$

Разложим её по переменным y, z:

$$f(x,y,z) = yz(g(x,0)\oplus 1) \ \oplus \ y(z\oplus 1)(g(x,1)\oplus 1)\oplus$$
$$\oplus\,(y\oplus 1)zg(x,1) \ \oplus \ (y\oplus 1)(z\oplus 1)g(x,0).$$

По утверждению 1.3 запишем
$\mathrm{w}(f) = \mathrm{w}(\bar{g}(x,0)) + \mathrm{w}(\bar{g}(x,1)) + \mathrm{w}(g(x,1)) + \mathrm{w}(g(x,0)) = 2^{n+1}$. ■

Пример 1.2. Пусть функция $f(x,y,z)$ задана следующей таблицей (в последнем столбце приведено преобразование Мёбиуса):

x	y	z	f	$\mu(f)$
0	0	0	0	0
0	0	1	0	0
0	1	0	1	1
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	0	1
1	1	1	1	0

Проверим по определению:

$$f(0,0,0) = \bar{f}(0,1,1); \quad f(0,0,1) = \bar{f}(0,1,0);$$
$$f(1,0,0) = \bar{f}(1,1,1); \quad f(1,0,1) = \bar{f}(1,1,0).$$

Следовательно, f зависит от y,z квазилинейно.

Запишем АНФ функции f:

$$f(x,y,z) = y\oplus xz\oplus xy = \underbrace{x(y\oplus z)}_{g(x,y\oplus z)}\oplus y.$$

1.4. Понятие корреляционной иммунности

Пусть X — случайная величина со значениями в U, Z — случайная величина со значениями в V. Говорят, что величины X, Z *статистически независимы*, если

$$\forall u\in U\ \forall v\in V\ \ (\Pr[X=u, Z=v] = \Pr[X=u]\cdot\Pr[Z=v])\,.$$

Пусть $f \in P_2(n)$; $X^{(1)}, \ldots, X^{(n)}$ — независимые равномерно распределённые случайные величины со значениями в $\mathbb{Z}_2$ (т. е. $\Pr[X^{(i)} = 0] = \Pr[X^{(i)} = 1] = 1/2$ для всех $i = 1, \ldots, n$); $Z = f\left(X^{(1)}, \ldots, X^{(n)}\right)$ — случайная величина с распределением $\Pr[Z = 1] = \mathrm{w}(f)/2^n$, $\Pr[Z = 0] = 1 - \mathrm{w}(f)/2^n$.

Определение 1.5. Функция $f \in P_2(n)$ *статистически не зависит от подмножества своих переменных* $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$, $0 < m \leqslant n$, если случайные величины $X^{(i_1,\ldots,i_m)} = \left(X^{(i_1)}, \ldots, X^{(i_m)}\right)$ и $Z = f\left(X^{(1)}, \ldots, X^{(n)}\right)$ статистически независимы.

Определение 1.6 (статистическое). Функция $f \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leqslant n$, если она статистически не зависит от любого m-элементного подмножества своих аргументов, т. е. если для любого набора индексов $(i_1, i_2, \ldots, i_m)$, $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$, случайные величины $X^{(i_1,\ldots,i_m)}$ и $Z = f\left(X^{(1)}, \ldots, X^{(n)}\right)$ статистически независимы.

Дадим теоретико-информационную интерпретацию статистической независимости. *Взаимной информацией* X и Z называется величина

$$I(X, Z) = H(X) - H(X|Z),$$

где $H(X)$ — энтропия случайной величины X; $H(X|Z)$ — условная энтропия случайной величины X относительно случайной величины Z.

Взаимная информация X и Z равна 0, если условная и безусловная энтропии равны, т. е. знание Z ничего не добавляет к знаниям об X.

Определение 1.7 (теоретико-информационное). Функция $f \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leqslant n$, если для любого набора индексов $(i_1, i_2, \ldots, i_m)$, $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$, $I\left(X^{(i_1,\ldots,i_m)}, f\left(X^{(1)}, \ldots, X^{(n)}\right)\right) = 0$.

Функцию $g \in P_2(m)$ будем называть *подфункцией* функции $f \in P_2(n)$, $n \geqslant m$, если g получена из f подстановкой констант вместо некоторых $n - m$ переменных.

Определение 1.8 (комбинаторное). Функция $f \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leqslant n$, если для любой её подфункции g от $n - m$ переменных выпол-

няется равенство $\Pr[g = 1] = \Pr[f = 1]$ (или, что то же самое, $\mathrm{w}(g) = \mathrm{w}(f)/2^m$).

Эквивалентность определений 1.6 и 1.7 известна из курса теории информации. Докажем равносильность определений 1.6 и 1.8. В самом деле,

$$\Pr[X^{(i_1,\ldots,i_m)} = a_1 \ldots a_m] = \frac{1}{2^m};$$

$$\Pr[f = 1] = \frac{\mathrm{w}(f)}{2^n};$$

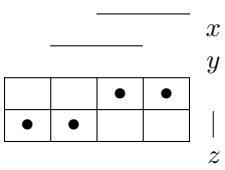
$$\Pr[X^{(i_1,\ldots,i_m)} = a_1 \ldots a_m, f = 1] = \frac{\mathrm{w}(g)}{2^n},$$

где подфункция g получена из f подстановкой констант $a_1, \ldots, a_m$ вместо переменных $x_{i_1}, \ldots, x_{i_m}$ соответственно. Ясно, что последняя (совместная) вероятность равна произведению первых двух, если и только если $\mathrm{w}(g) = \mathrm{w}(f)/2^m$.

Уравновешенная функция из $P_2(n)$ является корреляционно-иммунной порядка m, если все её подфункции от $n - m$ переменных уравновешены.

Определение 1.9. Уравновешенная корреляционно-иммунная порядка m функция называется *m-устойчивой*.

Пример 1.3. Пусть функция $f(x, y, z)$ задана следующей матрицей в коде Грея:



Любая подфункция функции f от двух переменных уравновешена (любой интервал ранга 2 на матрице в коде Грея имеет две единицы). Некоторые подфункции от одной переменной не уравновешены (например, $f(0, y, 0) \equiv 0$; $f(1, y, 0) \equiv 1$). Следовательно, функция f является 1-устойчивой, но не является 2-устойчивой.

Требование корреляционной иммунности функции связано с противостоянием корреляционной атаке, основная идея кото-

рой состоит в следующем. Рассмотрим комбинируюший генератор ключевого потока (рис. 1). Здесь РСЛОС$_1$–РСЛОС$_n$ — двоичные регистры сдвига с линейной обратной связью; $f(x_1, \ldots, x_n)$ — комбинирующая функция; $\gamma_1\gamma_2\ldots$ — вырабатываемый генератором ключевой поток. Ключом генератора являются начальные состояния всех регистров; объём ключа равен $2^{l_1+\ldots+l_n}$, где l_i — длина РСЛОС$_i$ для $i = 1, \ldots, n$.

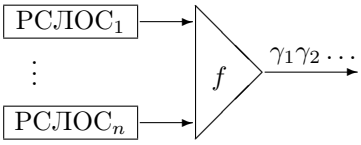


Рис. 1. Комбинируюший генератор

Вспомним, что РСЛОС, полином обратной связи которого является примитивным, вырабатывает последовательность $z = z_1 z_2 \ldots$, близкую по своим свойствам к случайной; в частности, при достаточно большой длине последовательности для случайно выбранного её бита z_i имеет место $\Pr[z_i = 0] \approx 1/2$. Следовательно, если $y = y_1 y_2 \ldots$ — произвольная не зависящая от z последовательность, то

$$\Pr[z_i = y_i] = \Pr[z_i = 0] \cdot \Pr[y_i = 0] + \Pr[z_i = 1] \cdot \Pr[y_i = 1] \approx$$
$$\approx \frac{1}{2}\left(\Pr[y_i = 0] + \Pr[y_i = 1]\right) = \frac{1}{2}.$$

Предположим, что $\Pr[f = x_1] \neq 1/2$ (в этом случае говорят, что *функция f коррелирует с переменной x_1*); с помощью корреляционной атаки найдём начальное состояние s_1 РСЛОС$_1$. Для этого будем перебирать все возможные 2^{l_1} состояний РСЛОС$_1$, для каждого из них строить порождаемую регистром последовательность $z = z_1 z_2 \ldots$ и считать количество совпадений с ключевой последовательностью $z_i = \gamma_i$. Для всех последовательностей, кроме одной (порождаемой из s_1), доля совпадений будет $\approx 1/2$. Тем самым определим часть ключа — состояние s_1. Если функция f имеет корреляцию со всеми своими переменными (или со всеми, кроме одной — тогда состояние регистра, соответствующего этой переменной, найдём последним, зная состояния всех остальных регистров), то найдём ключ гене-

ратора за $2^{l_1}+\ldots+2^{l_n}$ опробований, что много меньше сложности атаки грубой силы.

Утверждение 1.8. Если функция $f(x_1,\ldots,x_n)$ не корреляционно-иммунная порядка 1, то существует переменная x_i, для которой $\Pr[f = x_i] \neq 1/2$.

Доказательство. По определению 1.8 существует подфункция g, полученная из f фиксацией одной переменной (скажем, x_i), для которой $\mathrm{w}(g) \neq \mathrm{w}(f)/2$. Разложим функцию f по переменной x_i: $f = x_i f_1 \oplus (x_i \oplus 1) f_2$. Одна из функций f_1 или f_2 — это g, и поскольку по утверждению 1.3 $\mathrm{w}(f) = \mathrm{w}(f_1) + \mathrm{w}(f_2)$, то $\mathrm{w}(f_1) \neq \mathrm{w}(f_2)$. Получим:

$$\Pr[f \neq x_i] = \frac{\mathrm{w}(f \oplus x_i)}{2^n};$$

$$f \oplus x_i = x_i(f_1 \oplus 1) \oplus (x_i \oplus 1) f_2;$$

$$\mathrm{w}(f \oplus x_i) = \mathrm{w}(f_1 \oplus 1) + \mathrm{w}(f_2) = 2^{n-1} - \mathrm{w}(f_1) + \mathrm{w}(f_2) \neq 2^{n-1}.$$

Значит, $\Pr[f = x_i] \neq 1/2$. ■

Утверждение 1.9. Корреляционно-иммунная порядка m функция является корреляционно-иммунной любого меньшего порядка.

Доказательство. Достаточно доказать, что корреляционно-иммунная порядка m функция $f \in P_2(n)$ является корреляционно-иммунной порядка $m-1$.

Пусть g — произвольная подфункция функции f от $n-m+1$ переменных. Разложим g по любой её переменной: $g = x_i g_1 \oplus \oplus (x_i \oplus 1) g_2$; здесь g_1 и g_2 — подфункции функции f от $n-m$ переменных. Так как f корреляционно-иммунная порядка m, $\mathrm{w}(g_1) = \mathrm{w}(g_2) = \mathrm{w}(f)/2^m$. Тогда $\mathrm{w}(g) = \mathrm{w}(g_1) + \mathrm{w}(g_2) = \mathrm{w}(f)/2^{m-1}$, что означает, что f — корреляционно-иммунная порядка $m-1$. ■

С учётом доказанного естественно ввести обозначение для максимального порядка корреляционной иммунности:

$$\mathrm{cor}(f) = \max\{m \in \mathbb{N} : f \text{— корреляционно-иммунная порядка } m\}.$$

Из утверждения 1.9 следует, что m-устойчивая функция является k-устойчивой для любого $k < m$. По аналогии с $\mathrm{cor}(f)$

вводится обозначение для максимального порядка устойчивости:

$$\operatorname{sut}(f) = \begin{cases} -1, & \text{если } f \text{ не уравновешена,} \\ \operatorname{cor}(f), & \text{если } f \text{ уравновешена.} \end{cases}$$

Перечислим некоторые простейшие свойства введённых величин.

1. $\operatorname{cor}(f) = \operatorname{cor}(\bar{f})$.
2. Пусть $\mathrm{w}(f) = 2^t r$, где r нечётное. Тогда $\operatorname{cor}(f) \leqslant t$.
3. Если f линейно зависит от s переменных, то $\operatorname{sut}(f) \geqslant s - 1$.
4. Все корреляционно-иммунные порядка n функции в $P_2(n)$ — это константа 0 и константа 1.

Утверждение 1.10 (об устойчивых подфункциях). Если $f = x_1 f_1 \oplus (x_1 \oplus 1) f_2$ и f_1, f_2 — m-устойчивы, то f также m-устойчива.

Доказательство. Пусть $f \in P_2(n)$. Заметим, что f уравновешена, так как $\mathrm{w}(f) = \mathrm{w}(f_1) + \mathrm{w}(f_2) = 2^{n-1}$.

Зафиксируем у функции f любые m переменных из $x_2, \ldots, x_n$. Получим подфункцию $g = x_1 g_1 \oplus (x_1 \oplus 1) g_2$, где g_1, g_2 получены фиксацией m переменных у подфункций f_1 и f_2 соответственно. В силу m-устойчивости последних $\mathrm{w}(g_1) = \mathrm{w}(g_2) = 2^{n-m-2}$, откуда $\mathrm{w}(g) = 2^{n-m-1}$.

Зафиксируем $x_1 = 0$ и ещё $m - 1$ переменных из $x_2, \ldots, x_n$. При такой фиксации подфункция функции f совпадает с подфункцией g_2 от $n - m$ переменных функции f_2, которая по условию и ввиду утверждения 1.9 является $(m-1)$-устойчивой. Следовательно, $\mathrm{w}(g_2) = 2^{n-m-1}$.

Для фиксации $x_1 = 1$ рассуждения аналогичны. ■

Из доказанного следует более общее

Утверждение 1.11. Пусть все 2^l компонент разложения функции f по некоторым l переменным m-устойчивы. Тогда f также m-устойчива.

1.5. Неравенство Зигенталера

Теорема 1.1 (Зигенталер, 1984 г.). Пусть $f \in P_2(n)$.

1. Если $\operatorname{cor}(f) = m$, то $\deg f \leqslant n - m$.
2. Если f уравновешена и $\operatorname{sut}(f) = m \leqslant n-2$, то $\deg f \leqslant n-m-1$.

Доказательство. Пусть $\deg f = d$. Выберем в АНФ функции f любое слагаемое степени d и зафиксируем $n - d$ переменных, не входящих в это слагаемое. Получим подфункцию g степени d от d переменных; по следствию 2 из утверждения 1.4 вес g нечётен.

1. Зафиксируем в g ещё одну переменную двумя возможными значениями; получим подфункции g_1 и g_2 от $d-1$ переменных, и в силу того, что $\mathrm{w}(g_1)+\mathrm{w}(g_2) = \mathrm{w}(g)$ — нечётное число, выполняется неравенство $\mathrm{w}(g_1) \neq \mathrm{w}(g_2)$. Поскольку $\mathrm{cor}(f) = m$, все подфункции функции f от фиксированного числа k переменных при $k \geqslant n - m$ имеют одинаковый вес. Следовательно, $d - 1 < n - m$, или $d \leqslant n - m$.

2. Из условия $\mathrm{sut}(f) = m$ следует, что $\mathrm{w}(h) = 2^{k-1}$ для любой подфункции h от $k \geqslant n - m$ переменных, и $\mathrm{w}(h)$ чётен в силу условия $m \leqslant n - 2$. Значит, $d < n - m$, или $d \leqslant n - m - 1$. ■

Неравенство Зигенталера представляет собой первый из многочисленных (как мы увидим далее) примеров противоречивости криптографических свойств функции друг другу: высокий порядок корреляционной иммунности функции влечёт её невысокую степень и наоборот.

Опишем все функции f в $P_2(n)$, для которых $\mathrm{cor}(f) = n - 1$.

Утверждение 1.12. Все функции в $P_2(n)$ с условием $\mathrm{cor}(f) = n - 1$ — это функции вида $f(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \oplus \ldots \oplus x_n \oplus c$, $c \in \mathbb{Z}_2$.

Доказательство. Пусть $f \in P_2(n)$, $\mathrm{cor}(f) = n - 1$. По неравенству Зигенталера $\deg f \leqslant 1$, но если $\deg f = 0$, то $\mathrm{cor}(f) = n$. Следовательно, $\deg f = 1$ и f уравновешена.

Если f зависит от некоторой переменной фиктивно, то при фиксации остальных $n - 1$ переменных получим константу — неуравновешенную подфункцию, что противоречит условию $\mathrm{cor}(f) = n - 1$. Следовательно, f существенно зависит от всех своих переменных; таких функций степени 1 всего две, их вид указан в формулировке теоремы. ■

Таким образом, функции в $P_2(n)$, у которых $\mathrm{cor}(f) > n - 2$, не интересны для криптографии в силу своей аффинности; m-устойчивые функции максимально возможной степени для $m \leqslant n - 2$ имеют специальное название.

Определение 1.10. Если функция f из $P_2(n)$ уравновешена, $\mathrm{sut}(f) = m \leqslant n-2$ и $\deg f = n-m-1$, то f называется *m-оптимальной*.

1.6. Преобразование Уолша — Адамара

Определение 1.11. *Расстоянием Хэмминга* $\mathrm{d}(f,g)$ между функциями $f, g \in P_2(n)$ называется количество наборов, на которых значения этих функций различаются:

$$\mathrm{d}(f,g) = |\{x \in \mathbb{Z}_2^n : f(x) \neq g(x)\}| = \mathrm{w}(f \oplus g).$$

Определение 1.12. *Преобразованием Уолша — Адамара (ПУА) функции* $f \in P_2(n)$ называется функция $\hat{f} : \mathbb{Z}_2^n \to \mathbb{Z}$, где для каждого $a \in \mathbb{Z}_2^n$

$$\hat{f}(a) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus (a,x)}.$$

Значения $\hat{f}(a)$ называются *коэффициентами ПУА*.

Заметим, что

$$(-1)^{f(x)\oplus(a,x)} = \begin{cases} 1, & \text{если } f(x) = (a,x), \\ -1, & \text{если } f(x) \neq (a,x). \end{cases}$$

Таким образом, $\hat{f}(a) = \sigma - \delta$, где σ — количество совпадений функций $f(x)$ и (a,x); δ — количество их несовпадений. С учётом равенств $\delta = \mathrm{d}(f,(a,x))$, $\sigma = 2^n - \delta$ можно записать

$$\hat{f}(a) = 2^n - 2\mathrm{d}(f,(a,x)).$$

Определение 1.13. Неупорядоченный набор абсолютных значений коэффициентов ПУА булевой функции называется её *спектром*.

Пример 1.4.

x	$f(x)$	$\hat{f}(x)$
00	0	-2
01	1	2
10	1	2
11	1	2

Простейшие свойства ПУА

1. $\hat{f}(0^n) = 2^n - 2\mathrm{w}(f)$, и $\hat{f}(0^n) = 0$, если и только если f уравновешена.
2. Если $g = \bar{f}$, то $\hat{g}(a) = -\hat{f}(a)$ для всех $a \in \mathbb{Z}_2^n$.
3. Если $g(x) = f(x \oplus b)$, т. е. функция g получена из f отрицанием некоторых переменных, то

$$\hat{g}(a) = \sum_x (-1)^{f(x\oplus b)\oplus(a,x)} = \sum_x (-1)^{f(x)\oplus(a,x\oplus b)} = (-1)^{(a,b)}\hat{f}(a).$$

4. Пусть $f \in P_2(n)$, $b \in \mathbb{Z}_2^n$, $g(x) = f(x) \oplus (b, x)$. Тогда

$$\hat{g}(a) = \sum_x (-1)^{f(x)\oplus(b,x)\oplus(a,x)} = \sum_x (-1)^{f(x)\oplus(b\oplus a,x)} = \hat{f}(b \oplus a).$$

5. Пусть $f(x) = c$ — константа. Функция $c \oplus (a, x)$ уравновешена для всех $a \neq 0^n$, следовательно, $\hat{f}(a) = 0$ для всех ненулевых a. Кроме того,

$$\hat{f}(0^n) = 2^n - 2\mathrm{w}(f) = \begin{cases} -2^n, & \text{если } c = 1, \\ 2^n, & \text{если } c = 0. \end{cases}$$

6. Пусть $f(x) = (b, x) \oplus c$ — аффинная функция. По свойствам 4, 5 получим: $\hat{f}(a) = 0$ для всех $a \neq b$; $\hat{f}(b) = (-1)^c \cdot 2^n$.
7. Пусть $f(x, y) = g(x) \oplus h(y)$, где $g \in P_2(n)$; $h \in P_2(m)$; множества переменных x и y не пересекаются. Тогда для любых $a \in \mathbb{Z}_2^n$, $b \in \mathbb{Z}_2^m$

$$\hat{f}(ab) = \sum_{x,y} (-1)^{g(x)\oplus h(y)\oplus(a,x)\oplus(b,y)} =$$

$$= \sum_x (-1)^{g(x)\oplus(a,x)} \sum_y (-1)^{h(y)\oplus(b,y)} = \hat{g}(a)\hat{h}(b).$$

8. Пусть $f(x_1, \ldots, x_n)$ зависит от переменной x_i фиктивно. Тогда $\hat{f}(a) = 0$ для всех a, таких, что $a_i = 1$.

В самом деле, обозначим $x' = x_1 \ldots x_{i-1}x_{i+1} \ldots x_n$, $a' = a_1 \ldots a_{i-1}a_{i+1} \ldots a_n$ и заметим, что $(a, x) = (a', x') \oplus a_i x_i$. Тогда если $a_i = 1$, то

$$\hat{f}(a) = \sum_x (-1)^{f(x)\oplus(a,x)} = \sum_{\substack{x, \\ x_i=0}} (-1)^{f(x)\oplus(a',x')} +$$

$$+ \sum_{\substack{x, \\ x_i=1}} (-1)^{f(x)\oplus(a',x')\oplus 1} = 0.$$

Из свойств 2, 4 следует, что аффинная добавка не изменяет спектра функции.

Определение 1.14. Говорят, что *функция* $g \in P_2(n)$ *получена из функции* $f \in P_2(n)$ *с помощью аффинного преобразования переменных*, если существуют такие невырожденная булева матрица $A_{n\times n}$ и вектор $b \in \mathbb{Z}_2^n$, что $g(x) = f(Ax \oplus b)$ для любого $x \in \mathbb{Z}_2^n$. (Здесь и всюду далее в произведении Ax под x подразумевается вектор-столбец переменных $x_1, \ldots, x_n$.)

Пример 1.5. Пусть $f(x,y) = x \oplus y \oplus xy$, $A = \begin{Vmatrix} 1 & 1 \\ 0 & 1 \end{Vmatrix}$, $b = 01$. Тогда $g(x,y) = f(A(x,y) \oplus b) = f(x \oplus y, y \oplus 1) = xy \oplus 1$.

Утверждение 1.13. Пусть функция $g(x)$ получена из $f(x)$ с помощью аффинного преобразования переменных. Тогда спектры функций f и g совпадают.

Доказательство. Пусть $g(x) = f(Ax \oplus b)$. С помощью замены $y = Ax \oplus b$ (т. е. $x = A^{-1}(y \oplus b)$) получим:

$$\hat{g}(a) = \sum_x (-1)^{f(Ax\oplus b)\oplus(a,x)} =$$

$$= \sum_y (-1)^{f(y)\oplus(a,A^{-1}y)}(-1)^{(a,A^{-1}b)} = \pm\sum_y (-1)^{f(y)\oplus(a,A^{-1}y)} =$$

$$= \pm\sum_y (-1)^{f(y)\oplus(aA^{-1},y)} = \pm\hat{f}(aA^{-1}).$$

Осталось заметить, что aA^{-1} пробегает всё множество $\mathbb{Z}_2^n$, если это делает a. ■

Для $f \in P_2(n)$, $b = b_1 \ldots b_n \in \mathbb{Z}_2^n$ обозначим через f^b подфункцию функции f, которая получается из неё фиксацией $x_i = 0$ для всех i, таких, что $b_i = 1$.

Наряду с булевым скалярным произведением введём в рассмотрение *арифметическое скалярное произведение векторов* a *и* x: $\langle a, x\rangle = \sum\limits_{i=1}^{n} a_i x_i = \mathrm{w}(a \cdot x)$. В показателе (-1) операции $\oplus$ и $+$ взаимозаменяемы, поэтому

$$\hat{f}(a) = \sum_x (-1)^{f(x)\oplus(a,x)} = \sum_x (-1)^{f(x)\oplus\langle a,x\rangle} =$$

$$= \sum_x (-1)^{f(x)+(a,x)} = \sum_x (-1)^{f(x)+\langle a,x\rangle}.$$

Теорема 1.2 (тождество Саркара).

$$\sum_{a \leqslant b} \hat{f}(a) = 2^n - 2^{\mathrm{w}(b)+1} \cdot \mathrm{w}(f^b).$$

Доказательство.

$$\sum_{a \leqslant b} \hat{f}(a) = \sum_{a \leqslant b} \sum_{x} (-1)^{f(x)+\langle a,x \rangle} = \sum_{x} (-1)^{f(x)} \sum_{a \leqslant b} (-1)^{\langle a,x \rangle} =$$

$$= \underbrace{\sum_{\substack{x, \\ \langle b,x \rangle = 0}} (-1)^{f(x)} \sum_{a \leqslant b} (-1)^{\langle a,x \rangle}}_{S_1} + \underbrace{\sum_{\substack{x, \\ \langle b,x \rangle \neq 0}} (-1)^{f(x)} \sum_{a \leqslant b} (-1)^{\langle a,x \rangle}}_{S_2}.$$

Рассмотрим суммы S_1 и S_2. Если $\langle b, x \rangle \neq 0$, то существует i, для которого $b_i = x_i = 1$. Тогда если $a' \leqslant b$ и векторы a' и a'' различаются только в i-й компоненте, то $a'' \leqslant b$ и значения $\langle a', x \rangle$ и $\langle a'', x \rangle$ отличаются на 1, т. е. имеют разную чётность. Таким образом, в этом случае $\sum\limits_{a \leqslant b} (-1)^{\langle a,x \rangle} = 0$, а значит, $S_2 = 0$.

Из условий $\langle b, x \rangle = 0$ и $a \leqslant b$ следует $\langle a, x \rangle = 0$, поэтому в первой сумме $\sum\limits_{a \leqslant b} (-1)^{\langle a,x \rangle} = 2^{\mathrm{w}(b)}$. Кроме того, равенство $\langle b, x \rangle = 0$ означает, что $x_i = 0$ при $b_i = 1$; функция $f(x)$ при таких x пробегает все значения подфункции f^b. Обозначим область определения последней X_b; окончательно получаем:

$$\sum_{a \leqslant b} \hat{f}(a) = S_1 = 2^{\mathrm{w}(b)} \sum_{\substack{x, \\ \langle b,x \rangle = 0}} (-1)^{f(x)} = 2^{\mathrm{w}(b)} \sum_{x \in X_b} (-1)^{f^b(x)} =$$

$$= 2^{\mathrm{w}(b)} \sum_{x \in X_b} (-1)^{f^b(x) \oplus (0^{n-\mathrm{w}(b)}, x)} = 2^{\mathrm{w}(b)} \cdot \hat{f^b}(0^{n-\mathrm{w}(b)}) =$$

$$= 2^{\mathrm{w}(b)} \left(2^{n-\mathrm{w}(b)} - 2\mathrm{w}(f^b) \right) = 2^n - 2^{\mathrm{w}(b)+1} \cdot \mathrm{w}(f^b).$$

Теорема доказана. ■

Следствие.

$$\sum_{a \in \mathbb{Z}_2^n} \hat{f}(a) = (-1)^{f(0^n)} \cdot 2^n.$$

В дальнейшем очень полезна будет следующая формула:

$$\sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle a,x \rangle} = 2^n \delta(a, 0^n), \tag{1.6}$$

где $\delta(a, 0^n)$ — символ Кронекера, $a \in \mathbb{Z}_2^n$. Её справедливость следует из уравновешенности функции (a, x) при любом $a \neq 0^n$.

Теорема 1.3 (соотношение ортогональности).
Пусть $f \in P_2(n)$. Тогда

$$\sum_a \hat{f}(a)\hat{f}(x \oplus a) = 2^{2n}\delta(x, 0^n).$$

Доказательство.

$$\sum_a \hat{f}(a)\hat{f}(x \oplus a) = \sum_a \left(\sum_y (-1)^{f(y)\oplus(a,y)}\right)\left(\sum_z (-1)^{f(z)\oplus(x\oplus a,z)}\right) =$$

$$= \sum_{a,y,z} (-1)^{f(y)\oplus f(z)\oplus(a,y)\oplus(x\oplus a,z)} =$$

$$= \sum_{y,z} (-1)^{f(y)\oplus f(z)\oplus(x,z)} \underbrace{\sum_a (-1)^{(a,y\oplus z)}}_{2^n\delta(y,z)} =$$

$$= 2^n \sum_z (-1)^{(x,z)} \sum_y (-1)^{f(y)\oplus f(z)}\delta(y, z) = 2^n \underbrace{\sum_z (-1)^{(x,z)}}_{2^n\delta(x,0^n)} = 2^{2n}\delta(x, 0^n).$$

Теорема доказана. ■

Следствие (равенство Парсеваля). Для $f \in P_2(n)$

$$\sum_a \hat{f}^2(a) = 2^{2n}. \tag{1.7}$$

Следующая теорема даёт способ построения функции f, если известно её ПУА.

Теорема 1.4 (формула обращения). Для $f \in P_2(n)$

$$(-1)^{f(x)} = 2^{-n}\sum_a \hat{f}(a)(-1)^{(a,x)}.$$

Доказательство.

$$2^{-n}\sum_a \hat{f}(a)(-1)^{(a,x)} = 2^{-n}\sum_a (-1)^{(a,x)}\sum_y (-1)^{f(y)\oplus(a,y)} =$$

$$= 2^{-n}\sum_y (-1)^{f(y)} \underbrace{\sum_a (-1)^{(a,x\oplus y)}}_{2^n\delta(x,y)} = \sum_y (-1)^{f(y)}\delta(x, y) = (-1)^{f(x)}.$$

Теорема доказана. ■

Пример 1.6. Пусть $(2\ \ 2\ \ 2\ \ -2)$ — вектор значений ПУА функции $f \in P_2(2)$. Найдём $f(x)$.

$$\begin{aligned}
(-1)^{f(00)} &= 2^{-2}(2+2+2-2) = 1, && f(00) = 0;\\
(-1)^{f(01)} &= 2^{-2}(2-2+2+2) = 1, && f(01) = 0;\\
(-1)^{f(10)} &= 2^{-2}(2+2-2+2) = 1, && f(10) = 0;\\
(-1)^{f(11)} &= 2^{-2}(2-2-2-2) = -1, && f(11) = 1.
\end{aligned}$$

Таким образом, ПУА однозначно определяет функцию. Однако понятно, что не всякий целочисленный вектор длины 2^n является вектором значений ПУА для некоторой булевой функции; следующее утверждение проясняет эту ситуацию.

Утверждение 1.14. Пусть $g : \mathbb{Z}_2^n \to \mathbb{Z}$ — некоторая целочисленная функция. Булева функция f, такая, что $\hat{f}(a) = g(a)$ для любого $a \in \mathbb{Z}_2^n$, существует, если и только если выполнено соотношение ортогональности $\sum\limits_a g(a)g(x \oplus a) = 2^{2n}\delta(x, 0^n)$.

Доказательство. Необходимость следует из теоремы 1.3.

Для доказательства достаточности надо показать, что $\sum\limits_y g(y)(-1)^{(x,y)} = \pm 2^n$ для любого $x \in \mathbb{Z}_2^n$. Тогда по теореме 1.4 будет построена требуемая функция f. Используем тот факт, что если z пробегает множество $\mathbb{Z}_2^n$, то и $y \oplus z$ пробегает то же множество при любом фиксированном $y \in \mathbb{Z}_2^n$:

$$\begin{aligned}
\left(\sum_y g(y)(-1)^{(x,y)}\right)^2 &= \sum_y g(y)(-1)^{(x,y)} \sum_z g(z)(-1)^{(x,z)} =\\
&= \sum_y g(y)(-1)^{(x,y)} \sum_z g(y \oplus z)(-1)^{(x,y\oplus z)} =\\
= \sum_z (-1)^{(x,z)} \sum_y g(y)g(y \oplus z) &= \sum_z (-1)^{(x,z)} \cdot 2^{2n}\delta(z, 0^n) = 2^{2n}.
\end{aligned}$$

Таким образом, $\sum\limits_y g(y)(-1)^{(x,y)} = \pm 2^n$. ■

Формулу обращения, как и формулу вычисления ПУА, удобно задавать в матричной форме. Введём для этого необходимые понятия.

Определение 1.15. *Матрицей Адамара порядка* k называется такая $k \times k$-матрица H с элементами ± 1, что $HH^{\mathrm{T}} = kE$, где E — единичная матрица.

Определение 1.16. *Матрицей Сильвестра — Адамара* H_{2^n} называется квадратная матрица порядка 2^n, определяемая следующими рекуррентными соотношениями:

$$H_1 = \|1\|, \quad H_{2^n} = \left\| \begin{array}{cc} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & -H_{2^{n-1}} \end{array} \right\|. \tag{1.8}$$

Введём в рассмотрение матрицу $||h_{ij} : i, j \in \mathbb{Z}_2^n||$, где $h_{ij} = (-1)^{(i,j)}$. Нетрудно убедиться, что введённая так матрица является матрицей Сильвестра — Адамара, которая, в свою очередь, является матрицей Адамара.

Наконец, введём векторы $F = \left((-1)^{f(0^n)} \dots (-1)^{f(1^n)}\right)$ (который часто называют *характеристической последовательностью функции* f) и $\widehat{F} = \left(\hat{f}(0^n) \dots \hat{f}(1^n)\right)$ — вектор коэффициентов ПУА функции f. Из определения ПУА следует, что

$$\widehat{F} = F \cdot H_{2^n}, \tag{1.9}$$

а из свойств матрицы Адамара получаем формулу обращения

$$F = 2^{-n} \widehat{F} \cdot H_{2^n}. \tag{1.10}$$

Теорема 1.5 (о свёртке). Пусть $h(x) = f(x) \oplus g(x)$. Тогда $\hat{h}(u) = 2^{-n} \sum\limits_v \hat{g}(v) \hat{f}(v \oplus u)$ для всех $u \in \mathbb{Z}_2^n$.

Доказательство. Воспользуемся формулой обращения:

$$\hat{h}(u) = \sum_x (-1)^{f(x) \oplus g(x) \oplus (u,x)} = 2^{-n} \sum_x (-1)^{f(x) \oplus (u,x)} \sum_v \hat{g}(v) (-1)^{(v,x)} =$$
$$= 2^{-n} \sum_v \hat{g}(v) \sum_x (-1)^{f(x) \oplus (u \oplus v, x)} = 2^{-n} \sum_v \hat{g}(v) \hat{f}(v \oplus u).$$

Теорема доказана. ■

1.7. Тесты статистической независимости и корреляционной иммунности

Утверждение 1.15. Функция $f(x, y)$, где x, y — переменные со значениями в $\mathbb{Z}_2^n$ и $\mathbb{Z}_2^m$ соответственно, статистически

не зависит от переменных в x, если и только если функция $f(x,y) \oplus (u,x)$ уравновешена для любого ненулевого вектора $u \in \mathbb{Z}_2^n$.

Доказательство. Заметим, что условие статистической независимости f от переменных в x равносильно выполнению равенства $\mathrm{w}(f(a,y)) = \mathrm{w}(f)/2^n$ для любого вектора $a \in \mathbb{Z}_2^n$.

Необходимость. Разложим функцию $f(x,y) \oplus (u,x)$ по всем переменным в x; коэффициенты этого разложения имеют вид $f_a(y) = f(a,y) \oplus (u,a)$ для всевозможных $a \in \mathbb{Z}_2^n$. Если $(u,a) = 0$ (а это условие при фиксированном ненулевом u выполняется ровно для половины всех a), то $\mathrm{w}(f_a) = \mathrm{w}(f(a,y)) = \mathrm{w}(f)/2^n$. Если же $(u,a) = 1$, то $\mathrm{w}(f_a) = 2^m - \mathrm{w}(f(a,y)) = 2^m - \mathrm{w}(f)/2^n$. По утверждению 1.3 запишем

$$\mathrm{w}(f(x,y) \oplus (u,x)) = 2^{n-1}\mathrm{w}(f)/2^n + 2^{n-1}(2^m - \mathrm{w}(f)/2^n) = 2^{n+m-1},$$

что и доказывает уравновешенность функции $f(x,y) \oplus (u,x)$.

Достаточность. Докажем сначала, что $\mathrm{w}(f(a,y)) = \mathrm{w}(f)/2^n$ для нулевого вектора a. Запишем вес функции $f(x,y) \oplus (u,x)$ как сумму весов коэффициентов разложения и учтём уравновешенность этой функции:

$$\mathrm{w}(f(x,y) \oplus (u,x)) = 2^{n+m-1} = \sum_{a \in \mathbb{Z}_2^n} \mathrm{w}(f(a,y) \oplus (u,a)) =$$

$$= \sum_{a,(u,a)=0} \mathrm{w}(f(a,y)) + \sum_{a,(u,a)=1} (2^m - \mathrm{w}(f(a,y))),$$

откуда $\sum\limits_{a,(u,a)=0} \mathrm{w}(f(a,y)) = \sum\limits_{a,(u,a)=1} \mathrm{w}(f(a,y))$. Просуммируем обе части последнего равенства по всем $u \neq 0^n$:

$$\sum_{u \neq 0^n} \sum_{\substack{a, \\ (u,a)=0}} \mathrm{w}(f(a,y)) = \sum_{u \neq 0^n} \sum_{\substack{a, \\ (u,a)=1}} \mathrm{w}(f(a,y)).$$

Заметим, что при любом фиксированном $a \neq 0^n$ и всевозможных $u \neq 0^n$ равенство $(u,a) = 1$ выполняется 2^{n-1} раз, а равенство $(u,a) = 0$ верно в остальных $(2^{n-1} - 1)$ случаях. При $a = 0^n$ всегда $(u,a) = 0$. Поэтому получим

$$(2^n - 1)\mathrm{w}(f(0^n,y)) + (2^{n-1} - 1) \sum_{a \neq 0^n} \mathrm{w}(f(a,y)) = 2^{n-1} \sum_{a \neq 0^n} \mathrm{w}(f(a,y)),$$

откуда

$$\sum_{a\in\mathbb{Z}_2^n} \mathrm{w}(f(a,y)) = 2^n \mathrm{w}(f(0^n,y))$$

и $\mathrm{w}(f(0^n,y)) = \mathrm{w}(f)/2^n$.

Для случая $a \neq 0^n$ рассмотрим функцию $g(x,y) = f(x\oplus a, y)$. Ясно, что $\mathrm{w}(f) = \mathrm{w}(g)$ и $f(a,y) = g(0^n,y)$; кроме того, функция $g(x,y)\oplus(u,x)$ уравновешена в случае уравновешенности $f(x,y)\oplus$ $\oplus(u,x)$, так как

$$\mathrm{w}(g(x,y)\oplus(u,x)) = \sum_{x,y}(f(x\oplus a,y)\oplus(u,x)) =$$
$$= \sum_{x,y}(f(x,y)\oplus(u,x\oplus a)) = \sum_{x,y}(f(x,y)\oplus(u,x)\oplus(u,a)).$$

Последняя сумма здесь (в зависимости от значения (u,a)) есть вес функции $f(x,y)\oplus(u,x)$ или её отрицания, что для уравновешенной функции одно и то же. По доказанному выше $\mathrm{w}(g(0^n,y)) = \mathrm{w}(g)/2^n$, т. е. $\mathrm{w}(f(a,y)) = \mathrm{w}(f)/2^n$. ■

Очевидно, что функция $f(x,y)\oplus(u,x)$ уравновешена, если и только если $\hat{f}(u,0^m) = 0$. С учётом этого тест статистической независимости может быть переформулирован следующим (более конструктивным) образом.

Утверждение 1.16. Функция $f(x,y)$, где x,y — переменные со значениями в $\mathbb{Z}_2^n$ и $\mathbb{Z}_2^m$ соответственно, статистически не зависит от переменных в x, если и только если для любого ненулевого вектора $u\in\mathbb{Z}_2^n$ имеет место равенство $\hat{f}(u,0^m) = 0$.

Пример 1.7.

x	$f(x)$	$\hat{f}(x)$
000	1	0
001	1	0
010	0	−4
011	0	4
100	0	0
101	1	0
110	1	−4
111	0	−4

Функция f статистически не зависит от $\{x_1, x_3\}$, поскольку $\hat{f}(001) = \hat{f}(100) = \hat{f}(101) = 0$. В том же самом несложно убедиться по таблице значений функции.

Важным следствием утверждения 1.16 является следующая теорема (характеризационная для корреляционно-иммунных булевых функций).

Теорема 1.6. Функция $f \in P_2(n)$ является корреляционно-иммунной порядка m, если и только если $\hat{f}(a) = 0$ для всех векторов $a \in \mathbb{Z}_2^n$, таких, что $1 \leqslant \mathrm{w}(a) \leqslant m$.

Функция $f \in P_2(n)$ является m-устойчивой, если и только если $\hat{f}(a) = 0$ для всех $a \in \mathbb{Z}_2^n$, таких, что $0 \leqslant \mathrm{w}(a) \leqslant m$.

Рассмотрим вопрос о статистической независимости суперпозиции функций.

Утверждение 1.17. Пусть x, y, z — переменные со значениями в $\mathbb{Z}_2^n$, $\mathbb{Z}_2^m$ и $\mathbb{Z}_2^l$ соответственно и функция $f(x, y)$ статистически не зависит от переменных в x. Тогда и функция $h(x, y, z) = g\,(f(x, y), z)$, где g — любая функция от $l + 1$ переменных, статистически не зависит от переменных в x.

Доказательство. Пусть u — любой ненулевой вектор из $\mathbb{Z}_2^n$; тогда $\hat{f}(u, 0^m) = 0$ по утверждению 1.16. Вычислим коэффициент Уолша — Адамара функции h:

$$\hat{h}(u, 0^m, 0^l) = \sum_{x,y,z} (-1)^{g(f(x,y),z)\oplus(u,x)} =$$

$$= \sum_z \underbrace{\left(\sum_{\substack{x,y,\\ f(x,y)=0}} (-1)^{g(0,z)\oplus(u,x)} + \sum_{\substack{x,y,\\ f(x,y)=1}} (-1)^{g(1,z)\oplus(u,x)} \right)}_{A}.$$

Для каждого $z \in \mathbb{Z}_2^l$ имеет место один из следующих двух случаев:

1. $g(0, z) = g(1, z) = c \in \mathbb{Z}_2$, тогда $A = (-1)^c \sum\limits_{x,y} (-1)^{(u,x)} = 0$;
2. $g(0, z) = \overline{g(1, z)} = c \in \mathbb{Z}_2$, тогда

$$A = (-1)^c \left(\sum_{\substack{x,y,\\ f(x,y)=0}} (-1)^{(u,x)} - \sum_{\substack{x,y,\\ f(x,y)=1}} (-1)^{(u,x)} \right) =$$
$$= (-1)^c \sum_{x,y} (-1)^{f(x,y)\oplus(u,x)} = (-1)^c \hat{f}(u, 0^m) = 0.$$

Таким образом, $\hat{h}(u, 0^m, 0^l) = 0$, и утверждение доказано. ■

К сожалению, это утверждение не допускает обобщения на случай нескольких функций f; так, если функции $f_1(x, y)$, $f_2(x, y)$, …, $f_s(x, y)$ статистически не зависят от переменных в x, то функция $g(f_1(x, y), f_2(x, y), \ldots, f_s(x, y), z)$ не обязательно обладает этим свойством.

Пример 1.8. Функции $f_1(x_1, x_2) = x_1 \oplus x_2$ и $f_2(x_1, x_2) = x_2$ статистически не зависят от переменной x_1, но суперпозиция $g(x_1, x_2) = f_1 \cdot f_2 = x_1 x_2 \oplus x_2$ этим свойством не обладает.

Утверждение 1.18. Пусть x, y, z — переменные со значениями в $\mathbb{Z}_2^n$, $\mathbb{Z}_2^m$ и $\mathbb{Z}_2^l$ соответственно, функции $f_1(x, y)$, $f_2(x, y)$, $u(x, y) = f_1(x, y) \oplus f_2(x, y)$ статистически не зависят от переменных в x. Тогда и функция

$$h(x, y, z) = g\left(f_1(x, y), f_2(x, y), z\right),$$

где g — любая функция от $l + 2$ переменных, статистически не зависит от переменных в x.

Доказательство. Для любых $a \in \mathbb{Z}_2^n$, $i, j \in \mathbb{Z}_2$ обозначим $c_{ij}^a = |\{y \in \mathbb{Z}_2^m : f_1(a, y) = i, f_2(a, y) = j\}|$. В силу статистической независимости функций f_1, f_2, u от переменных в x для любого $a \in \mathbb{Z}_2^n$ выполняется

$$c_{10}^a + c_{11}^a = \mathrm{w}(f_1)/2^n, \quad c_{01}^a + c_{11}^a = \mathrm{w}(f_2)/2^n, \quad c_{01}^a + c_{10}^a = \mathrm{w}(u)/2^n.$$

Отсюда получаем $c_{01}^a = (\mathrm{w}(u) - \mathrm{w}(f_1) + \mathrm{w}(f_2))/2^{n+1}$, $c_{10}^a = (\mathrm{w}(u) + \mathrm{w}(f_1) - \mathrm{w}(f_2))/2^{n+1}$, $c_{11}^a = (\mathrm{w}(f_1) + \mathrm{w}(f_2) - \mathrm{w}(u))/2^{n+1}$, $c_{00}^a = 2^m - (\mathrm{w}(u) + \mathrm{w}(f_1) + \mathrm{w}(f_2))/2^{n+1}$, т. е. c_{ij}^a не зависит от a для всех $i, j \in \mathbb{Z}_2$. Тогда и вес подфункции функции h, полученной фиксацией переменных в x набором значений a, не зависит

от a, так как $\mathrm{w}(h(a,y,z)) = \sum\limits_{i,j\in\mathbb{Z}_2} c_{ij}^a \cdot \mathrm{w}(g(i,j,z))$. Следовательно, функция h статистически не зависит от переменных в x. ■

Следующее утверждение характеризует условия статистической независимости от переменных в x суммы двух функций в частном случае — когда одна из функций зависит только от x.

Утверждение 1.19. Пусть x, y — переменные со значениями в $\mathbb{Z}_2^n$ и $\mathbb{Z}_2^m$ соответственно и функция $f(x,y)$ статистически не зависит от переменных в x. Тогда функция $f(x,y) \oplus g(x)$, где g — любая функция от n переменных, статистически не зависит от переменных в x, если и только если f уравновешена или $g = \mathrm{const}$.

Доказательство. По условию $\mathrm{w}(f(a,y)) = \mathrm{w}(f)/2^n$ для всех $a \in \mathbb{Z}_2^n$; следовательно, $\mathrm{w}(f(a,y) \oplus g(a))$ не зависит от a, если и только если $g = \mathrm{const}$ или $\mathrm{w}(f)/2^n = 2^m - \mathrm{w}(f)/2^n$; последнее равенство равносильно уравновешенности f. ■

Следующая теорема описывает некоторые необходимые условия корреляционной иммунности функции.

Теорема 1.7.

1. Если $f \in P_2(n)$ — корреляционно-иммунна порядка $m \leqslant n-1$, то $2^{m+1} | \hat{f}(a)$ для всех $a \in \mathbb{Z}_2^n$.
2. Если $f \in P_2(n)$ — уравновешена и корреляционно-иммунна порядка $m \leqslant n-2$, то $2^{m+2} | \hat{f}(a)$ для всех $a \in \mathbb{Z}_2^n$.

Доказательство. Индукция по весу a.

1. Б а з а и н д у к ц и и.

Имеем $\hat{f}(0^n) = 2^n - 2\mathrm{w}(f)$; $2^{m+1} | 2^n$ в силу $m+1 \leqslant n$; $2^m | \mathrm{w}(f)$ в силу корреляционной иммунности функции f. Таким образом, $2^{m+1} | \hat{f}(0^n)$. Очевидно также, что $2^{m+1} | \hat{f}(a)$ для всех ненулевых векторов a, вес которых не превосходит m, так как для этих a выполнено равенство $\hat{f}(a) = 0$.

П р е д п о л о ж е н и е и н д у к ц и и. Пусть $2^{m+1} | \hat{f}(b)$ для всех b, $\mathrm{w}(b) \leqslant k$, где $k \geqslant m$.

Ш а г и н д у к ц и и. Пусть $\mathrm{w}(a) = k+1$. По тождеству Саркара $\sum\limits_{b \leqslant a} \hat{f}(b) = 2^n - 2^{k+2}\mathrm{w}(f^a)$; здесь в правой части $2^{m+1} | 2^n$ и $2^{m+1} | 2^{k+2}$; в левой части по предположению индук-

ции все слагаемые, кроме $\hat{f}(a)$, делятся на 2^{m+1}. Значит, и $\hat{f}(a)$ делится на 2^{m+1}.

2. Для уравновешенной функции $\hat{f}(0^n) = 0$, поэтому $2^{m+2}|\hat{f}(0^n)$. Шаг индукции доказывается аналогично п. 1. ■

Вопросы и задачи

1. Сколько существует уравновешенных функций в $P_2(n)$?
2. Какова мощность класса $\mathcal{A}(n)$? $\mathcal{L}(n)$?
3. (*) Доказать, что булева функция f линейна, если и только если $f(x \oplus y) = f(x) \oplus f(y)$ для всех x, y.
4. Найти АНФ следующих функций:
   а) $x_1 \vee x_2 \vee x_3$;
   б) $x_1 \sim x_2$;
   в) $x_1x_2x_3$;
   г) $(x_1 \sim x_2) \sim x_3$;
   д) $(x_1 \vee x_2)x_3 \to x_2$.
5. Указать условия, которым должны удовлетворять коэффициенты АНФ линейной самодвойственной функции.
6. Сколько существует уравновешенных линейных функций в $P_2(5)$, зависящих фиктивно от первой переменной?
7. Сколько существует функций в $P_2(n)$, степень которых не превосходит k, $k \leqslant n$? равна n?
8. Сколько существует функций в $P_2(n)$, $n \geqslant 2$, линейных по x_1? квазилинейных по x_1, x_2?
9. Изобразить на матрице в коде Грея функцию от трёх переменных, линейную по x_3 и квазилинейную по x_1, x_2. Выписать АНФ всех таких функций.
10. Найти линейное доопределение частичных булевых функций:
    а) $f = (011 - -1 - -)$;
    б) $g = (0 - -11 - 0-)$.
11. Подсчитать число булевых функций от $n \geqslant 2$ переменных, не изменяющихся при перестановке x_1 и x_2.
12. Сколько существует монотонных булевых функций от четырёх переменных, принимающих значение 0 на всех векторах веса 2?
13. Найти вес монотонной функции от пяти переменных, которая равна 0 на всех векторах веса 1 и равна 1 на всех векторах веса 2.

14. Изобразить на матрице в коде Грея функцию от трёх переменных, веса 2, 1-го порядка корреляционной иммунности.
15. (*) Пусть f и g — функции от непересекающихся множеств переменных. Найти $\mathrm{sut}(f \oplus g)$.
16. (*) Пусть $f(x) \in P_2(n)$, $g(y) = (a, y) \oplus b \in \mathcal{A}(m)$, $\mathrm{w}(a) = k > 0$, множества переменных функций f и g не пересекаются. Доказать:

$$\mathrm{cor}(f \oplus g) = \begin{cases} k - 1, & \text{если } f \text{ не уравновешена,} \\ k + \mathrm{cor}(f), & \text{если } f \text{ уравновешена.} \end{cases}$$

17. (*) Пусть для $f \in P_2(n)$ выполнено условие $2^k | \hat{f}(a)$ для всех $a \in \mathbb{Z}_2^n$. Доказать: $\deg f \leqslant n - k + 1$.

2. Нелинейность булевых функций

2.1. Определение и свойства нелинейности

Пусть $f \in P_2(n)$, $G \subseteq P_2(n)$ — некоторое подмножество функций. *Расстоянием* $\mathrm{d}(f, G)$ *от функции* f *до класса функций* G называется расстояние от f до ближайшей к ней функции из G: $\mathrm{d}(f, G) = \min\limits_{g \in G} \mathrm{d}(f, g)$.

Определение 2.1. *Нелинейностью функции* f называется расстояние от f до класса аффинных функций.

Будем обозначать нелинейность функции f через N_f:

$$N_f = \mathrm{d}(f, \mathcal{A}(n)) = \min_{g \in \mathcal{A}(n)} \mathrm{d}(f, g).$$

Выведем формулу вычисления N_f через преобразование Уолша — Адамара. По определению $\hat{f}(a) = 2^n - 2\mathrm{d}(f, (a, x))$, откуда

$$\mathrm{d}(f, (a, x)) = 2^{n-1} - \frac{1}{2}\hat{f}(a).$$

Тогда $\mathrm{d}(f, (a, x) \oplus 1) = 2^n - \mathrm{d}(f, (a, x)) = 2^{n-1} + \dfrac{1}{2}\hat{f}(a)$

и $$\min\left(\mathrm{d}(f, (a, x)), \mathrm{d}(f, (a, x) \oplus 1)\right) = 2^{n-1} - \frac{1}{2}|\hat{f}(a)|.$$

Если теперь возьмём минимум по всем a, то получим формулу для вычисления N_f:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^n} |\hat{f}(a)|. \tag{2.1}$$

Отсюда, ввиду $\max |\hat{f}(a)| > 0$, получаем тривиальную оценку $N_f < 2^{n-1}$.

Определение 2.2. *Наилучшим аффинным приближением функции* f называется ближайшая к f аффинная функция.

Формула (2.1) даёт возможность найти не только N_f, но и наилучшее аффинное приближение функции: пусть $\max\limits_a |\hat{f}(a)| = |\hat{f}(b)|$; тогда если $\hat{f}(b) > 0$, то наилучшим аффинным приближением f является функция (b, x), а если $\hat{f}(b) < 0$ — функция $(b, x) \oplus 1$.

Пример 2.1. Пусть $f(x,y,z) = (01111010)$. Вычислим преобразование Уолша — Адамара: $\hat{f} = (-2\ -2\ 2\ 2\ -2\ 6\ 2\ 2)$. Поскольку $\max|\hat{f}(a)| = 6 = \hat{f}(101)$, то наилучшее аффинное приближение функции f — это $x \oplus z = (01011010)$, и $\mathrm{d}(f,(x \oplus z)) = 1 = 2^2 - 6/2$.

Простейшие свойства нелинейности

1. Пусть $f(x) \in P_2(n)$, $h(x) \in \mathcal{A}(n)$. Тогда $N_f = N_{f \oplus h}$.
   Это следует из того, что аффинная добавка не меняет спектра функции (свойства 2 и 4 ПУА, с. 21).
2. Пусть $f(x_1,\ldots,x_n,y) = g(x_1,\ldots,x_n) \oplus cy$, $c \in \mathbb{Z}_2$ (т. е. f зависит от y фиктивно или линейно). Тогда $N_f = 2\,N_g$.

   Доказательство. Пусть $x = (x_1 \ldots x_n)$, $a \in \mathbb{Z}_2^n$, $b, e \in \mathbb{Z}_2$. Тогда $N_f = \min\limits_{a,b,e} \mathrm{d}(f,(ab,xy) \oplus e) = \min\limits_{a,b,e} \mathrm{w}(h(x,y))$, где $h(x,y) = g(x) \oplus cy \oplus (a,x) \oplus by \oplus e$. Если $c \oplus b = 1$, то h зависит от y линейно и, следовательно, уравновешена: $\mathrm{w}(h) = 2^n$. Если $c \oplus b = 0$, то h зависит от y фиктивно. Тогда $\mathrm{w}(h) = 2\,\mathrm{w}(g(x) \oplus \oplus (a,x) \oplus e) = 2\mathrm{d}(g,(a,x) \oplus e) \geqslant 2\,N_g$; здесь первое равенство верно по утверждению 1.1, последнее неравенство — по определению нелинейности, причём для некоторых a, e в нём достигается равенство. Таким образом, $N_f = \min(2^n, 2\,N_g)$, и ввиду $N_g < 2^{n-1}$ получаем $N_f = 2\,N_g$. ■

3. Пусть $f(x_1,\ldots,x_n,y,z) = g(x_1,\ldots,x_n,y \oplus z) \oplus y$ (т. е. f зависит от переменных y, z квазилинейно — утверждение 1.6). Тогда $N_f = 2\,N_g$.

   Доказательство. Пусть $x = (x_1 \ldots x_n)$, $a \in \mathbb{Z}_2^n$, $b, c, d \in \mathbb{Z}_2$. Тогда $N_f = \min\limits_{a,b,c,d} \mathrm{w}(h(x,y,z))$, где

$$h(x,y,z) = f(x,y,z) \oplus (a,x) \oplus by \oplus cz \oplus d =$$

$$= g(x, y \oplus z) \oplus (a,x) \oplus (b \oplus 1)y \oplus cz \oplus d.$$

   Возможные случаи:

   а) $b = c$. Тогда

$$h(x,y,z) = g(x, y \oplus z) \oplus (a,x) \oplus b(y \oplus z) \oplus y \oplus d = h'(x, y \oplus z) \oplus y,$$

   т. е. функция h имеет квазилинейные переменные и $\mathrm{w}(h) = 2^{n+1}$ по утверждению 1.7.

б) $b \oplus 1 = c$. Тогда

$$h(x, y, z) = g(x, y \oplus z) \oplus (a, x) \oplus c(y \oplus z) \oplus d = h'(x, y \oplus z).$$

В этом случае $\mathrm{w}(h) = 2\,\mathrm{w}(h') \geqslant 2\,N_g$, и для некоторых a, c, d равенство достигается.

Таким образом, $N_f = \min(2^{n+1}, 2\,N_g) = 2\,N_g$. ■

2.2. Бент-функции

Определение 2.3. Функция $f \in P_2(n)$ называется *бент-функцией*, если $\hat{f}(a) = \pm 2^{n/2}$ для любого $a \in \mathbb{Z}_2^n$.

Класс всех бент-функций от n переменных обозначается $\mathcal{B}(n)$.

Простейшие свойства бент-функций

1. Бент-функции существуют только для чётных n.
2. Бент-функции не уравновешены.
3. Если $f \in \mathcal{B}(n)$, то $\mathrm{w}(f) = 2^{n-1} \pm 2^{n/2-1}$.
4. Бент-функции статистически зависят от всех своих аргументов.
5. Пусть $f \in \mathcal{B}(n), h \in \mathcal{A}(n)$. Тогда $f \oplus h \in \mathcal{B}(n)$.
   Это следует из свойств 2 и 4 ПУА.
6. $f(x_1, x_2) = x_1 x_2$ — бент-функция.
   Проверяется непосредственно: $\widehat{F} = (2\ 2\ 2\ -2)$.
7. Пусть $f \in P_2(n)$, $g \in P_2(m)$ — функции от непересекающихся множеств переменных. Тогда $f \oplus g$ — бент-функция, если и только если f и g — бент-функции.

   Доказательство. Достаточность. Пусть $\hat{f}(a) = \pm 2^{n/2}$, $\hat{g}(b) = \pm 2^{m/2}$. Тогда $\widehat{f \oplus g}(ab) = \hat{f}(a)\hat{g}(b) = \pm 2^{(n+m)/2}$. Следовательно, $f \oplus g$ — бент-функция.

   Необходимость. Пусть $\widehat{f \oplus g}(ab) = \pm 2^{(n+m)/2}$ для всех a, b. Предположим, $\hat{f}(a) = k$ для некоторого a. Тогда $\hat{g}(b) = \pm 2^{(n+m)/2}/k$ для всех $b \in \mathbb{Z}_2^m$. По равенству Парсеваля запишем

$$2^{2m} = \sum_b \hat{g}^2(b) = 2^m \frac{2^{n+m}}{k^2},$$

   откуда $k^2 = 2^n$, $k = \pm 2^{n/2}$, $\hat{g}(b) = \pm 2^{m/2}$. Значит, f и g — бент-функции. ■

8. Бент-функции существуют для любого чётного n.
   Следует из свойств 6 и 7.

9. Класс бент-функций замкнут относительно любого аффинного преобразования переменных.
   Следует из утверждения 1.13.

Введём в рассмотрение *функцию Шеннона для нелинейности* $N(n)$ как расстояние от класса аффинных функций до самых далёких функций из $P_2(n)$:

$$N(n) = \max_{f \in P_2(n)} N_f = \max_{f \in P_2(n)} \min_{g \in \mathcal{A}(n)} \mathrm{d}(f, g).$$

Теорема 2.1 (о функции Шеннона для нелинейности).
1) $N(n) \leqslant 2^{n-1} - 2^{n/2-1}$, и
2) $N(n) = 2^{n-1} - 2^{n/2-1}$, если и только если n чётно.

Доказательство. Пусть $f \in P_2(n)$; запишем для неё равенство Парсеваля: $\sum\limits_{a \in \mathbb{Z}_2^n} \hat{f}^2(a) = 2^{2n}$. Имеем 2^n неотрицательных слагаемых, сумма которых равна 2^{2n}. Следовательно, $\max\limits_{a \in \mathbb{Z}_2^n} \hat{f}^2(a) \geqslant 2^n$, откуда $\max\limits_{a \in \mathbb{Z}_2^n} |\hat{f}(a)| \geqslant 2^{n/2}$. Значит,

$$N_f = 2^{n-1} - \frac{1}{2} \max |\hat{f}(a)| \leqslant 2^{n-1} - 2^{n/2-1},$$

откуда следует утверждение 1 теоремы.

Если $N(n) = 2^{n-1} - 2^{n/2-1}$, то n чётно, так как $N(n)$ целое. С другой стороны, если n чётно, то существует бент-функция f от n переменных, для которой $N_f = 2^{n-1} - 2^{n/2-1}$. Утверждение 2 теоремы доказано. ■

Функция $f \in P_2(n)$ называется *максимально нелинейной*, если $N_f = N(n)$. Для чётного n классы максимально нелинейных функций и бент-функций совпадают; для нечётного n значение $N(n)$ в настоящее время не известно.

Теорема 2.2 (о степени бент-функции). Пусть $f \in \mathcal{B}(n)$, $n \geqslant 4$. Тогда $\deg f \leqslant n/2$.

Доказательство. Вспомним тождество Саркара (теорема 1.2):

$$\sum_{a \leqslant b} \hat{f}(a) = 2^n - 2^{\mathrm{w}(b)+1} \cdot \mathrm{w}(f^b) \tag{2.2}$$

и присмотримся к подфункции f^b в нём. Если в векторе b компонента b_i равна 1, то переменная x_i фиксируется в 0, а если $b_i = 0$, то $x_i \in \mathbb{Z}_2$. Другими словами, подфункция f^b определена на тех и только тех наборах x, где $x \leqslant \bar{b}$. Тогда

$$\mathrm{w}(f^b) = \sum_{x \leqslant \bar{b}} f(x) = g(\bar{b}) \pmod 2, \text{ где } g = \mu(f). \tag{2.3}$$

Из равенств (2.2) и (2.3) получим

$$g(\bar{b}) = 2^{n-\mathrm{w}(b)-1} - \frac{\sum\limits_{a \leqslant b} \hat{f}(a)}{2^{\mathrm{w}(b)+1}} = 2^{\mathrm{w}(\bar{b})-1} - \frac{\sum\limits_{a \leqslant b} \hat{f}(a)}{2^{\mathrm{w}(b)+1}} \pmod 2.$$

Рассмотрим произвольный вектор b, такой, что $\mathrm{w}(\bar{b}) > n/2$, т. е. $\mathrm{w}(b) < n/2$. Так как $n/2 \geqslant 2$, имеем $2^{\mathrm{w}(\bar{b})-1} = 0 \pmod 2$. Рассмотрим сумму $S = \sum\limits_{a \leqslant b} \hat{f}(a)$. Если $\mathrm{w}(b) = 0$, то $S = \hat{f}(0^n) = \pm 2^{n/2}$ и $S/2 = 0 \pmod 2$. Если $\mathrm{w}(b) \neq 0$, то S — сумма чётного числа слагаемых вида $\pm 2^{n/2}$, т. е. $S = (k_1 - k_2)2^{n/2}$, где k_1 и k_2 — количество положительных и отрицательных слагаемых соответственно. В силу $k_1 - k_2 = 0 \pmod 2$ получаем $S = 0 \pmod{2^{n/2+1}}$, откуда $S/2^{\mathrm{w}(b)+1} = 0 \pmod 2$ ввиду $\mathrm{w}(b) < n/2$. Таким образом, $g(\bar{b}) = 0$ для всех векторов, для которых $\mathrm{w}(\bar{b}) > n/2$. Следовательно, $\deg f \leqslant n/2$. ■

Из этой теоремы получается тривиальная верхняя оценка количества бент-функций:

$$|\mathcal{B}(n)| \leqslant 2^{1+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{n/2}} = 2^{2^{n-1}+\binom{n}{n/2}/2}.$$

Все квадратичные бент-функции от n переменных аффинно эквивалентны функции $f(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n$, т. е. могут быть получены из неё с помощью аффинного преобразования переменных и аффинной добавки. При $d \geqslant 3$ вопрос аффинной классификации бент-функций степени d открыт.

Следующая теорема характеризует бент-функции с помощью матриц Адамара (определение 1.15 на с. 26).

Теорема 2.3. Функция $f \in P_2(n)$, где n чётное, является бент-функцией, если и только если матрица

$$H = 2^{-n/2} || \hat{f}(a \oplus b) : a, b \in \mathbb{Z}_2^n ||$$

есть матрица Адамара.

Доказательство. Достаточность. Элементы матрицы Адамара принимают значения ± 1, поэтому $\hat{f}(a \oplus b) = \pm 2^{n/2}$ для всех a, b, т. е. f — бент-функция.

Необходимость.

1. Элементы матрицы H принимают значения ± 1.
2. Рассмотрим произвольный элемент h_{ab} произведения матриц HH^{T}.

$$h_{ab} = 2^{-n} \sum_{x \in \mathbb{Z}_2^n} \hat{f}(a \oplus x)\hat{f}(x \oplus b) =$$

$$= 2^{-n} \sum_{x} \hat{f}(x)\hat{f}(x \oplus a \oplus b) = 2^{-n} \cdot 2^{2n}\delta(a \oplus b, 0^n) = 2^n \delta(a, b);$$

здесь предпоследнее равенство имеет место в силу соотношения ортогональности (теорема 1.3).

Из предложений 1, 2 и определения 1.15 следует, что H — матрица Адамара. ■

Пример 2.2. Рассмотрим бент-функцию $f(x_1, x_2) = x_1 x_2$.

$$2^{-1} \left\| \hat{f}(a \oplus b) \right\| = \begin{Vmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{Vmatrix} \text{— матрица Адамара,}$$

отличная от матрицы Сильвестра — Адамара (определение 1.16).

Пусть $f \in \mathcal{B}(n)$. Введём в рассмотрение *дуальную к f функцию* $\tilde{f}$ как $(-1)^{\tilde{f}(x)} = 2^{-n/2}\hat{f}(x)$. Очевидно, что $\tilde{f}(x) \in \mathbb{Z}_2$, т. е. $\tilde{f}$ — булева функция.

Пример 2.3.

x	$f(x)$	$\hat{f}$	$\tilde{f}$
00	1	2	0
01	0	−2	1
10	0	−2	1
11	0	−2	1

Свойства дуальных функций:

1. $\tilde{f}$ — бент-функция, так как

$$\hat{\tilde{f}}(a) = \sum_x (-1)^{\tilde{f}(x)\oplus(a,x)} = 2^{-n/2} \underbrace{\sum_x \hat{f}(x)(-1)^{(a,x)}}_{2^n(-1)^{f(a)}} =$$

$$= 2^{n/2}(-1)^{f(a)} = \pm 2^{n/2}.$$

2. $\hat{\tilde{\tilde{f}}} = f$, так как $(-1)^{\hat{\tilde{f}}} = 2^{-n/2}\hat{\tilde{f}}(x) = (-1)^{f(x)}$.

Утверждение 2.1. Если $f \in \mathcal{B}(n)$, то $\left\|(-1)^{f(a\oplus b)} : a, b \in \mathbb{Z}_2^n\right\|$ — матрица Адамара.

Доказательство. $\left\|(-1)^{f(a\oplus b)}\right\| = 2^{-n/2}\left\|\hat{\tilde{f}}(a\oplus b)\right\|$; $\tilde{f}$ — бент-функция. Утверждение следует теперь из теоремы 2.3. ■

Теорема 2.4 (конструкция Мэйорана — МакФарланда). Пусть $x, y \in \mathbb{Z}_2^n$, π — взаимно-однозначное отображение на $\mathbb{Z}_2^n$, $g \in P_2(n)$ — произвольная функция. Тогда функция $f(x,y) = (\pi(x), y) \oplus g(x)$ — бент-функция от $2n$ переменных.

Доказательство. Найдём коэффициент Уолша — Адамара функции f для $a, b \in \mathbb{Z}_2^n$:

$$\hat{f}(ab) = \sum_{x,y\in\mathbb{Z}_2^n} (-1)^{(\pi(x),y)\oplus g(x)\oplus(a,x)\oplus(b,y)} =$$

$$= \sum_{x\in\mathbb{Z}_2^n} (-1)^{g(x)\oplus(a,x)} \sum_{y\in\mathbb{Z}_2^n} (-1)^{(\pi(x)\oplus b,y)} =$$

$$= 2^n \sum_{x\in\mathbb{Z}_2^n} (-1)^{g(x)\oplus(a,x)}\delta(\pi(x), b) = 2^n(-1)^{g(\pi^{-1}(b))\oplus(a,\pi^{-1}(b))} = \pm 2^n.$$

Теорема доказана. ■

Функции вида $f(x,y) = (\pi(x), y) \oplus g(x)$ образуют класс Мэйорана — МакФарланда; обозначим его $\mathcal{M}(2n)$ для $x, y \in \mathbb{Z}_2^n$. При фиксированном $x = a$ подфункция $f(a, y)$ аффинная; таким образом, вектор значений функции $f(x,y)$ представляет собой конкатенацию векторов значений аффинных функций.

Из теоремы 2.2 следует, что при чётном $n > 2$ существуют бент-функции степени d для любого $d = 2, 3, \ldots, n/2$ (достаточно взять функцию g степени d).

Утверждение 2.2. $|\mathcal{M}(2n)| = 2^n! \cdot 2^{2^n}$.

Доказательство. Поскольку количество подстановок π на $\mathbb{Z}_2^n$ равно $2^n!$, а количество функций g — 2^{2^n}, то достаточно показать, что разным парам (π, g) соответствуют разные функции из класса $\mathcal{M}$. В самом деле, из $(\pi_1(x), y) \oplus g_1(x) = (\pi_2(x), y) \oplus g_2(x)$ следует $(\pi_1(x) \oplus \pi_2(x), y) = g_1(x) \oplus g_2(x)$, откуда ввиду независимости левой части от y получаем $\pi_1(x) \oplus \pi_2(x) \equiv 0$, т. е. $\pi_1 = \pi_2$ и $g_1 = g_2$. ■

Из утверждения 2.2 следует нижняя оценка количества бент-функций: $|\mathcal{B}(n)| \geqslant 2^{n/2}! \cdot 2^{2^{n/2}}$.

2.3. Совершенная нелинейность

Определение 2.4. *Производной функции f по направлению a* называется функция $f'_a = f(x) \oplus f(x \oplus a)$.

Пример 2.4.

x	$f(x)$	f'_{00}	f'_{01}	f'_{10}	f'_{11}
00	0	0	0	0	1
01	0	0	0	1	0
10	0	0	1	0	0
11	1	0	1	1	1

Свойства производной

1. Производная любой функции по нулевому направлению — функция-константа 0.
2. $f'_a(x) = f'_a(x \oplus a)$.
3. $(f \oplus g)'_a = f'_a \oplus g'_a$.
4. $f'_a \equiv 0$ для всех $a \Leftrightarrow f = \text{const}$.
5. Производные функции f по всем направлениям являются константами, если и только если $f \in \mathcal{A}(n)$.
   Достаточность очевидна. Для доказательства необходимости рассмотрим производные по направлениям $\mathbf{e}_i = 0^{i-1}10^{n-i}$:

$$f'_{\mathbf{e}_i}(x_1, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \oplus \\ \oplus f(x_1, \ldots, x_{i-1}, \bar{x_i}, x_{i+1}, \ldots, x_n),$$

   и если эта производная для всех $x \in \mathbb{Z}_2^n$ равна 0, то функция f зависит от переменной x_i фиктивно, а если 1 — то линейно. Следовательно, $f \in \mathcal{A}(n)$.

6. $f'_{a\oplus b}(x) = f(x) \oplus f(x \oplus a \oplus b) = f(x) \oplus f(x \oplus a) \oplus f(x \oplus a) \oplus \oplus f(x \oplus a \oplus b) = f'_a(x) \oplus f'_b(x \oplus a)$.
7. Если $f \neq \text{const}$, то $\deg f' \leqslant \deg f - 1$ (достаточно рассмотреть производную монома $x_{i_1} \dots x_{i_k}$).

Определение 2.5. Говорят, что *функция* $f \in P_2(n)$ *имеет линейную структуру*, если существует ненулевое направление $a \in \mathbb{Z}_2^n$, такое, что $f'_a = \text{const}$.

Из свойства 6 производной следует, что направления, по которым производные функции f равны константам, образуют линейное пространство.

Класс функций с линейной структурой от n переменных обозначается $\mathcal{LS}(n)$.

Простейшие свойства класса $\mathcal{LS}(n)$

1. $\mathcal{A}(n) \subseteq \mathcal{LS}(n)$ (следует из свойства 5 производной).
2. Если f имеет линейную или фиктивную переменную, то $f \in \mathcal{LS}(n)$.
   Пусть $f(x_1, \dots, x_{n-1}, y) = g(x_1, \dots, x_{n-1}) \oplus cy$, где $c \in \mathbb{Z}_2$. Нетрудно убедиться, что $f'_{0\dots01} = c$.
3. Если f зависит квазилинейно от некоторых переменных, то $f \in \mathcal{LS}(n)$.
   По утверждению 1.6 функция f может быть представлена в виде $f(x, y, z) = g(x, y \oplus z) \oplus y$, $x \in \mathbb{Z}_2^{n-2}$. Тогда $f'_{0\dots011} = g(x, y \oplus z) \oplus y \oplus g(x, y \oplus 1 \oplus z \oplus 1) \oplus y \oplus 1 = 1$.
4. Если $f \in \mathcal{LS}(n)$, $g \in \mathcal{A}(n)$, то $f \oplus g \in \mathcal{LS}(n)$.
   Следует из определения класса $\mathcal{LS}(n)$ и свойств 3, 5 производной.

Следующее утверждение объясняет интерес к классу функций с линейной структурой, точнее (как мы увидим далее), к удалённости от этого класса функций, используемых при построении криптосистем.

Утверждение 2.3 (о слабости функций класса $\mathcal{LS}(n)$).

Пусть $f \in \mathcal{LS}(n)$. Тогда существует невырожденная булева матрица $A_{n\times n}$, такая, что функция $g(x) = f(Ax)$ имеет линейную или фиктивную переменную.

Доказательство. Пусть $f'_a = \text{const} = c \in \mathbb{Z}_2$. Тогда $f(x \oplus ua) = f(x) \oplus uc$ для всех $x \in \mathbb{Z}_2^n$, $u \in \mathbb{Z}_2$. Пусть $\mathbf{e}_i$ — булев вектор длины n с единственной единицей в i-й компоненте, $i = 1, \dots, n$. Построим невырожденную матрицу A, первый

столбец которой равен a, а остальные произвольны; заметим, что $A\mathbf{e}_1 = a$. Для $x = (x_1 \dots x_n)$ запишем:

$$f(Ax) = f(A(x_1\mathbf{e}_1 \oplus \dots \oplus x_n\mathbf{e}_n)) =$$
$$= f(x_1(A\mathbf{e}_1) \oplus A(x_2\mathbf{e}_2 \oplus \dots \oplus x_n\mathbf{e}_n)) =$$
$$= f(x_1 a \oplus A(x_2\mathbf{e}_2 \oplus \dots \oplus x_n\mathbf{e}_n)) = f(A(x_2\mathbf{e}_2 \oplus \dots \oplus x_n\mathbf{e}_n)) \oplus x_1 c,$$

что означает, что x_1 — линейная или фиктивная (в зависимости от значения c) переменная. ■

Пример 2.5. Пусть $f(x_1, x_2, x_3) = 1 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3$. Линейных и фиктивных переменных у этой функции нет. Найдём производную по направлению 110:

$$f'_{110} = 1 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus 1 \oplus (x_1 \oplus 1) \oplus (x_2 \oplus 1)x_3 \oplus (x_1 \oplus 1)x_3 = 1.$$

Построим матрицу A:

$$A = \begin{Vmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix}.$$

Тогда $g(x) = f(Ax) = 1 \oplus x_1 \oplus (x_1 \oplus x_2)x_3 \oplus x_1x_3 = 1 \oplus x_1 \oplus x_2x_3$ — линейна по переменной x_1.

Определение 2.6. *Совершенной нелинейностью функции f* называется расстояние от f до класса функций с линейной структурой.

Совершенная нелинейность функции f обозначается CN_f (от *Complete Nonlinearity*):

$$CN_f = \mathrm{d}(f, \mathcal{LS}(n)) = \min_{g \in \mathcal{LS}(n)} \mathrm{d}(f, g).$$

В силу включения $\mathcal{A}(n) \subseteq \mathcal{LS}(n)$ имеет место неравенство $N_f \geqslant CN_f$.

Утверждение 2.4. Пусть $f \in P_2(n)$. Тогда

1. $CN_f \leqslant 2^{n-2}$;
2. $CN_f = 2^{n-2}$, если и только если производные функции f по всем ненулевым направлениям уравновешены.

Доказательство. Выберем произвольный ненулевой набор $a \in \mathbb{Z}_2^n$ и разобьём множество $\mathbb{Z}_2^n$ на неупорядоченные пары $\{x, x \oplus a\}$; всего таких пар будет 2^{n-1}. Множество пар разобьём на два подмножества:

$$Q(a,f) = \{\{x, x \oplus a\} : f(x) = f(x \oplus a)\} = \{\{x, x \oplus a\} : f'_a(x) = 0\};$$
$$R(a,f) = \{\{x, x \oplus a\} : f(x) \neq f(x \oplus a)\} = \{\{x, x \oplus a\} : f'_a(x) = 1\};$$

заметим, что $|Q(a,f)| + |R(a,f)| = 2^{n-1}$, откуда

$$\min\{|Q(a,f)|, |R(a,f)|\} \leqslant 2^{n-2}; \tag{2.4}$$

равенство здесь имеет место, если и только если производная f'_a уравновешена.

Построим функцию g_1 так: для каждой пары $\{x, x \oplus a\} \in Q(a,f)$ положим $g_1(y) = f(y)$ ровно на одном наборе y из этой пары. Тогда $g_1(x) = g_1(x \oplus a)$ для всех x, т. е. $g_1 \in \mathcal{LS}(n)$ и g_1 — ближайшая к f функция, производная которой по направлению a равна $\mathrm{const}\,1$. Аналогично построим функцию g_2: для каждой пары $\{x, x \oplus a\} \in R(a,f)$ положим $g_2(y) = f(y)$ ровно на одном наборе $y \in \{x, x \oplus a\}$; тогда $g_2(x) = g_2(x \oplus a)$ для всех x и g_2 — ближайшая к f функция, производная которой по направлению a равна $\mathrm{const}\,0$. С учётом этих рассуждений и того, что $\mathrm{d}(f, g_1) = |Q(a,f)|$, $\mathrm{d}(f, g_2) = |R(a,f)|$, получаем

$$CN_f = \mathrm{d}(f, \mathcal{LS}(n)) = \min_{a \neq 0^n} \min\{|Q(a,f)|, |R(a,f)|\}, \tag{2.5}$$

откуда ввиду неравенства (2.4) следует $CN_f \leqslant 2^{n-2}$. Равенство здесь достигается, если и только если $|Q(a,f| = |R(a,f)| = 2^{n-2}$ для всех $a \neq 0^n$, т. е. в случае уравновешенности производных по всем ненулевым направлениям. ■

С учётом того, что $|R(a,f)| = \mathrm{w}(f'_a)/2$, $|Q(a,f)| = (2^n - \mathrm{w}(f'_a))/2$, формулу (2.5) можно записать как

$$CN_f = \min_{a \neq 0^n} \min\{\mathrm{w}(f'_a), 2^n - \mathrm{w}(f'_a)\}/2. \tag{2.6}$$

Определение 2.7. Функция $f \in P_2(n)$ называется *совершенно нелинейной*, если $CN_f = 2^{n-2}$.

В соответствии с утверждением 2.4, совершенно нелинейные функции максимально удалены от класса функций с линейной структурой и их производные уравновешены по всем ненулевым направлениям.

Утверждение 2.5. Функция $f \in P_2(n)$ совершенно нелинейна, если и только если f — бент-функция.

Доказательство. Необходимость.

$$\hat{f}^2(a) = \sum_{x\in\mathbb{Z}_2^n} (-1)^{f(x)\oplus(a,x)} \sum_{y\in\mathbb{Z}_2^n} (-1)^{f(y)\oplus(a,y)} =$$
$$= \sum_{x,y} (-1)^{f(x)\oplus f(y)\oplus(a,x\oplus y)} =$$
$$= \sum_{x=y} (-1)^{f(x)\oplus f(y)\oplus(a,x\oplus y)} + \sum_{x\neq y} (-1)^{f(x)\oplus f(y)\oplus(a,x\oplus y)}.$$

Заметим, что первая сумма в последнем выражении равна 2^n, а во второй произведём замену $b = x \oplus y$; получим

$$\hat{f}^2(a) = 2^n + \sum_{b\neq 0^n} (-1)^{(a,b)} \sum_x (-1)^{f(x)\oplus f(x\oplus b)} = 2^n.$$

Последнее равенство имеет место в силу уравновешенности функции $f(x) \oplus f(x \oplus b)$ при любом ненулевом b. Следовательно, $\hat{f}(a) = \pm 2^{n/2}$, и f — бент-функция.

Достаточность. Если $f \in \mathcal{B}(n)$, то по утверждению 2.1 матрица $H = \left\|(-1)^{f(a\oplus b)}\right\|$ является матрицей Адамара. Рассмотрим элемент матрицы $HH^{\mathrm{T}} = 2^n E = \|h_{ab}\|$:

$$2^n \delta(a,b) = h_{ab} = \sum_x (-1)^{f(a\oplus x)\oplus f(x\oplus b)}.$$

Для $b = 0^n$ и любого $a \neq 0^n$ получим, что $0 = \sum_x (-1)^{f(a\oplus x)\oplus f(x)} =$ $= \sum_x (-1)^{f'_a(x)}$, откуда следует, что $f'_a(x)$ уравновешена, и по утверждению 2.4 и определению 2.7 f совершенно нелинейна. ■

Из утверждений 2.4 и 2.5 следует

Теорема 2.5 (критерий Ротхауза). Функция f является бент-функцией, если и только если её производные по всем ненулевым направлениям уравновешены.

Следствие. Функция f является бент-функцией, если $\left\|(-1)^{f(a\oplus b)} : a, b \in \mathbb{Z}_2^n\right\|$ — матрица Адамара.

Доказательство. Из того, что $\left\|(-1)^{f(a\oplus b)}\right\|$ — матрица Адамара, для всех $a \neq b$ следует равенство

$$0 = \sum_x (-1)^{f(a\oplus x)\oplus f(x\oplus b)} = \sum_y (-1)^{f(a\oplus b\oplus y)\oplus f(y)} = \sum_y (-1)^{f'_{a\oplus b}(y)},$$

что, в свою очередь, означает уравновешенность производных функции f по всем ненулевым направлениям. ■

Объединяя утверждение 2.1 и это следствие, получим ещё одну характеризацию бент-функций матрицами Адамара.

Утверждение 2.6. Функция f является бент-функцией, если и только если $\left\|(-1)^{f(a\oplus b)} : a, b \in \mathbb{Z}_2^n\right\|$ — матрица Адамара.

По аналогии с $N(n)$ введём *функцию Шеннона для совершенной нелинейности*:

$$CN(n) = \max_{f\in P_2(n)} \mathrm{d}(f, \mathcal{LS}(n)) = \max_{f\in P_2(n)} \min_{g\in\mathcal{LS}(n)} \mathrm{d}(f, g).$$

Теорема 2.6.

1. $CN(n) \leqslant 2^{n-2}$;
2. $CN(n) = 2^{n-2}$, если и только если n чётно.

Доказательство. Следует из утверждения 2.4, критерия Ротхауза (теорема 2.5) и существования бент-функций от n переменных для любого чётного n. ■

Таким образом, для чётного n классы бент-функций, совершенно нелинейных и максимально нелинейных функций совпадают; для нечётного n совершенно нелинейных функций, как и бент-функций, не существует.

2.4. Нелинейность корреляционно-иммунных функций

Следующие теоремы показывают, что чем выше порядок корреляционной иммунности функции, тем ниже верхняя граница её нелинейности.

Теорема 2.7. Пусть $f \in P_2(n)$, $\mathrm{cor}(f) = m \leqslant n-1$, f не уравновешена. Тогда $N_f \leqslant 2^{n-1} - 2^m$.

Доказательство. Воспользуемся тем, что $\mathrm{cor}(f) = \mathrm{cor}(\bar{f})$ и $N_f = N_{\bar{f}}$; выберем из f и $\bar{f}$ ту функцию, вес которой меньше,

чем 2^{n-1}. Пусть для определённости это будет f. Тогда для g — подфункции функции f от $n-m$ переменных — выполняется условие $\mathrm{w}(g) = \mathrm{w}(f)/2^m \leqslant 2^{n-m-1}-1$. Отсюда $\mathrm{w}(f) = 2^m \mathrm{w}(g) \leqslant$ $\leqslant 2^{n-1} - 2^m$, и ввиду $N_f \leqslant \mathrm{w}(f)$ получаем нужное неравенство. Теорема доказана. ■

Теорема 2.8. Пусть $f \in P_2(n)$, $\mathrm{cor}(f) = m \leqslant n-2$. Тогда если $N_f \neq 2^{n-1} - 2^m$, то $N_f \leqslant 2^{n-1} - 2^{m+1}$.

Доказательство. По утверждению 1 теоремы 1.7 о необходимых условиях корреляционной иммунности (с. 31) для всех a имеет место $2^{m+1} | \hat{f}(a)$. Из того, что $N_f = 2^{n-1} - \dfrac{1}{2} \max\limits_{a \in \mathbb{Z}_2^n} |\hat{f}(a)| \neq$ $\neq 2^{n-1} - 2^m$, следует, что $\max\limits_{a \in \mathbb{Z}_2^n} |\hat{f}(a)| \neq 2^{m+1}$. Значит, существует a, для которого $|\hat{f}(a)| \geqslant 2^{m+2}$. Отсюда получаем утверждение теоремы. ■

Теорема 2.9. Пусть $f \in P_2(n)$, f уравновешена и m-устойчива, $m \leqslant n-2$. Тогда $N_f \leqslant 2^{n-1} - 2^{m+1}$.

Доказательство. По утверждению 2 теоремы 1.7 для всех a имеет место делимость $2^{m+2} | \hat{f}(a)$. Значит, существует набор a, для которого $|\hat{f}(a)| \geqslant 2^{m+2}$. Следовательно, $\max\limits_{a} |\hat{f}(a)| \geqslant 2^{m+2}$ и $N_f \leqslant 2^{n-1} - 2^{m+1}$. ■

По аналогии с понятием m-оптимальной функции (определение 1.10) вводится специальное название для m-устойчивых функций максимально возможной нелинейности.

Определение 2.8. Если функция f из $P_2(n)$ уравновешена, $\mathrm{sut}(f) = m \leqslant n-2$ и $N_f = 2^{n-1} - 2^{m+1}$, то f называется *m-насыщенной*.

Теорема 2.10 (о нелинейности неоптимальных функций). Если функция f из $P_2(n)$ уравновешена, $\mathrm{sut}(f) = m \leqslant n-3$ и $\deg f \leqslant n-m-2$, то $N_f \leqslant 2^{n-1} - 2^{m+2}$.

Доказательство. Для функции f из теоремы существует подфункция f_1 от $n-m-1$ переменных, такая, что $\mathrm{w}(f_1) \neq$ $\neq 2^{n-m-2}$. Заметим, что $\mathrm{w}(f_1)$ чётный, так как $f_1 \in P_2(n-m-1)$ и $\deg f_1 \leqslant \deg f < n-m-1$ (следствие 2 на с. 11). Тогда $\mathrm{w}(f_1) \leqslant 2^{n-m-2} - 2$ или $\mathrm{w}(f_1) \geqslant 2^{n-m-2} + 2$; последнее равносильно $\mathrm{w}(\bar{f}_1) \leqslant 2^{n-m-2} - 2$. Из свойств 2 и 3 преобразования Уолша —

Адамара (с. 21) следует, что отрицание функции и её переменных влияет только на знаки коэффициентов Уолша — Адамара (т. е. не изменяет значение нелинейности и порядок устойчивости функции), поэтому без ограничения общности рассмотрим случай $\mathrm{w}(f_1) \leqslant 2^{n-m-2} - 2$ и будем считать, что подфункция f_1 получена фиксацией $m+1$ переменных нулями.

Пусть $b = b_1 \dots b_n \in \mathbb{Z}_2^n$, $\mathrm{w}(b) = m+1$ и $b_i = 1$, если и только если переменная x_i фиксирована; тогда $f_1 = f^b$ из тождества Саркара (теорема 1.2). С учётом условия $\mathrm{sut}(f) = m$ и теоремы 1.6 запишем

$$\hat{f}(b) = \sum_{a \leqslant b} \hat{f}(a) = 2^n - 2^{m+2} \cdot \mathrm{w}(f_1) \geqslant 2^n - 2^n + 2^{m+3} = 2^{m+3},$$

откуда $N_f \leqslant 2^{n-1} - 2^{m+2}$. ■

Утверждение 2.7. Если функция m-насыщенна, то она m-оптимальна.

Доказательство. Для $m \leqslant n-3$ утверждение непосредственно следует из теоремы 2.10. Если $\mathrm{sut}(f) = m = n-2$, то по неравенству Зигенталера (теорема 1.1) и в силу уравновешенности функции $\deg f = 1 = n - m - 1$. ■

Определение 2.9. Если для функции $f \in P_2(n)$ квадрат каждого коэффициента Уолша — Адамара равен либо 0, либо 2^{2n-2r}, то f называется *платовидной функцией порядка* $2r$ (или просто *платовидной*).

В частности, бент-функции платовидны порядка n; аффинные — платовидны порядка 0. Для платовидной порядка $2r$ функции $\hat{f}(a) \in \{0, \pm 2^{n-r}\}$, и величина 2^{n-r} называется *амплитудой платовидной функции*.

Теорема 2.11. m-Насыщенная функция из $P_2(n)$ является платовидной порядка $2(n-m-2)$.

Доказательство. Для функции f из теоремы $N_f = 2^{n-1} - 2^{m+1}$, откуда с учётом формулы (2.1) на с. 34 получаем $\max\limits_a |\hat{f}(a)| = 2^{m+2}$. По необходимому условию корреляционной иммунности (теорема 1.7) $2^{m+2} | \hat{f}(a)$ для всех $a \in \mathbb{Z}_2^n$. Значит, $\hat{f}(a) \in \{0, \pm 2^{m+2}\}$. ■

Из теоремы 2.1 о функции Шеннона для нелинейности следует, что $N_f \leqslant 2^{n-1} - 2^{n/2-1}$ для любой функции $f \in P_2(n)$, и эта граница ниже, чем устанавливаемая теоремами 2.7, 2.9, при $m \leqslant n/2 - 1$ и $m \leqslant n/2 - 2$ соответственно. Следующая теорема уточняет границу нелинейности для функций малого порядка корреляционной иммунности.

Теорема 2.12. Пусть $f \in P_2(n)$, n чётное. Тогда:

1. Если $0 < \mathrm{cor}(f) = m \leqslant n/2 - 1$, то $N_f \leqslant 2^{n-1} - 2^{n/2-1} - 2^m$.
2. Если f уравновешена, $\mathrm{sut}(f) = m \leqslant n/2 - 2$, то $N_f \leqslant 2^{n-1} - 2^{n/2-1} - 2^{m+1}$.

Доказательство. Докажем п. 2 (п. 1 доказывается аналогично). Функция f уравновешена, поэтому f — не бент-функция. Следовательно, $\max\limits_a |\hat{f}(a)| > 2^{n/2}$. Из теоремы 1.7 о необходимом условии корреляционной иммунности следует, что $2^{m+2} \big| \max\limits_a |\hat{f}(a)|$; кроме того, $2^{m+2} \big| 2^{n/2}$, так как по условию $m \leqslant n/2 - 2$. Значит, $\max\limits_a |\hat{f}(a)| \geqslant 2^{n/2} + 2^{m+2}$, откуда с учётом формулы (2.1) следует утверждение 2 теоремы. ■

Вопросы и задачи

1. (*) Пусть $f(x) \in P_2(n)$, $g(y) \in \mathcal{L}(m)$, множества переменных x и y не пересекаются. Доказать: наилучшим аффинным приближением функции $f \oplus g$ является $h \oplus g$, где h — наилучшее аффинное приближение функции f.
2. (*) Пусть $f(x) \in P_2(n)$, $g(y) \in P_2(m)$, множества переменных x и y не пересекаются. Выразить $N_{f \oplus g}$ через N_f и N_g.
3. Доказать, что $f(x)$ не является бент-функцией, если она зависит фиктивно, линейно или квазилинейно от некоторых переменных.
4. (*) Пусть $f \in P_2(n)$, n нечётно, $x \in \mathbb{Z}_2^{n-1}$, $y \in \mathbb{Z}_2$ и $f(x, y) = y \cdot f_1(x) \oplus (y \oplus 1) f_2(x)$, где $f_1, f_2 \in \mathcal{B}(n-1)$. Найти N_f.
5. (*) Пусть $f \in P_2(n)$, $n > 1$, $h \in \mathcal{A}(n)$ и $\mathrm{d}(f, h) \leqslant 2^{n-2}$. Доказать: h — наилучшее аффинное приближение функции f.
6. Пусть $f \in \mathcal{B}(2n)$, $n > 2$, $\deg f = n$. Доказать, что f нельзя представить в виде суммы двух функций от непересекающихся множеств переменных.
7. (*) Доказать: если $f \in \mathcal{M}(2n)$, то и $\tilde{f} \in \mathcal{M}(2n)$.

8. (*) Доказать: если $f \in \mathcal{LS}(n)$, $n > 1$, то $\mathrm{w}(f) = 0 (\mathrm{mod}\, 2)$.
9. (*) Пусть $f \in P_2(n)$, $h \in \mathcal{A}(n)$. Доказать: $CN_f = CN_{f \oplus h}$.
10. (*) Доказать: $f'_a \in \mathcal{LS}(n)$ для всех $f \in P_2(n)$, $a \in \mathbb{Z}_2^n$.
11. (*) Доказать: всякая квадратичная функция является бент-функцией или имеет линейную структуру.
12. (*) Описать все функции класса $\mathcal{LS}(2)$; $\mathcal{LS}(3)$.
13. (*) Доказать: $f'_a = \mathrm{const}\, c$, если и только если $\hat{f}(z) = 0$ для всех z, таких, что $(z, a) = c \oplus 1$.
14. (*) Доказать, что если $f \in P_2(n)$ — платовидная функция порядка $2r$, то $|\{a \in \mathbb{Z}_2^n : \hat{f}(a) \neq 0\}| = 2^{2r}$.
15. (*) Доказать, что для любой платовидной функции $f \in P_2(n)$ меньшего, чем n, порядка найдётся такая линейная функция g, что сумма $f \oplus g$ уравновешена.
16. (*) Пусть $S = \{a \in \mathbb{Z}_2^n : \hat{f}(a) \neq 0\}$. Доказать: $\max\limits_a |\hat{f}(a)| = 2^n / \sqrt{|S|}$, если и только если f платовидна.
17. (*) Доказать: если функция f платовидна порядка $2r$, то $\deg f \leqslant r + 1$.

3. Лавинные характеристики булевых функций

3.1. Автокорреляция и взаимная корреляция

Определение 3.1. Пусть $f, g \in P_2(n)$. *Функцией взаимной корреляции* f и g называется функция $\Delta_{f,g} : \mathbb{Z}_2^n \to \mathbb{Z}$, где для любого $u \in \mathbb{Z}_2^n$

$$\Delta_{f,g}(u) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus g(x \oplus u)}.$$

Заметим, что $\Delta_{f,g}(u)$ равно разности между числом совпадений и числом несовпадений значений $f(x)$ и $g(x \oplus u)$. С учётом того, что вероятность совпадения случайных булевых значений равна $1/2$, естественно ввести следующее определение.

Определение 3.2. Функции f и g называются *совершенно некоррелированными*, если $\Delta_{f,g}(u) = 0$ для любого u.

Определение 3.3. *Функцией автокорреляции для* $f \in P_2(n)$ называется функция, определяемая как

$$\Delta_f(u) = \Delta_{f,f}(u) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus f(x \oplus u)} = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f'_u(x)}.$$

Свойства функции автокорреляции

1. $\Delta_f(0^n) = 2^n$.
2. $\Delta_f(u) = 0$, если и только если производная f'_u уравновешена.
3. $\Delta_f(u) = \Delta_{\bar{f}}(u)$ для любого u.
4. $\Delta_f(u) = \widehat{f'_u}(0^n)$.
5. Пусть $f \in P_2(n)$, $g \in \mathcal{A}(n)$. Тогда $\Delta_{f \oplus g}(u) = \pm \Delta_f(u)$ для любого $u \in \mathbb{Z}_2^n$ (следует из того, что $g'_u = \text{const}$ для любого u).
6. Пусть $h(x, y) = f(x) \oplus g(y)$ и множества переменных x и y не пересекаются. Тогда $\Delta_h(ab) = \Delta_f(a) \cdot \Delta_g(b)$.
7. С помощью функции автокорреляции можно вычислить совершенную нелинейность функции $f \in P_2(n)$:

$$CN_f = 2^{n-2} - \frac{1}{4} \max_{a \neq 0^n} |\Delta_f(a)|$$

(следует из определения функции автокорреляции и формулы (2.6)).

Теорема 3.1 (о взаимной корреляции). Пусть $f, g \in P_2(n)$. Тогда

$$(\Delta_{f,g}(0^n), \ldots, \Delta_{f,g}(1^n))\, H_{2^n} = \left(\hat{f}(0^n)\hat{g}(0^n), \ldots, \hat{f}(1^n)\hat{g}(1^n)\right),$$

где H_{2^n} — матрица Сильвестра — Адамара (определение 1.16).

Доказательство. Вычислим v-ю компоненту вектора слева.

$$\sum_u \Delta_{f,g}(u)(-1)^{(u,v)} = \sum_u \sum_x (-1)^{f(x)\oplus g(x\oplus u)\oplus (u,v)} =$$
$$= \sum_x (-1)^{f(x)} \sum_u (-1)^{g(x\oplus u)\oplus (u,v)} = \sum_x (-1)^{f(x)} \sum_z (-1)^{g(z)\oplus (z\oplus x,v)} =$$
$$= \sum_x (-1)^{f(x)\oplus (x,v)} \sum_z (-1)^{g(z)\oplus (z,v)} = \hat{f}(v)\hat{g}(v).$$

Теорема доказана. ■

Следствие 1. При $g = f$ получим

$$(\Delta_f(0^n), \ldots, \Delta_f(1^n))\, H_{2^n} = \left(\hat{f}^2(0^n), \ldots, \hat{f}^2(1^n)\right).$$

Следствие 2.

$$(\Delta_{f,g}(0^n), \ldots, \Delta_{f,g}(1^n)) = 2^{-n} \left(\hat{f}(0^n)\hat{g}(0^n), \ldots, \hat{f}(1^n)\hat{g}(1^n)\right) H_{2^n}$$

(следует из свойств матрицы Сильвестра — Адамара).

Следствие 3.

$$(\Delta_f(0^n), \ldots, \Delta_f(1^n)) = 2^{-n} \left(\hat{f}^2(0^n), \ldots, \hat{f}^2(1^n)\right) H_{2^n}.$$

Свойства 2 и 3 показывают, что функцию взаимной корреляции (автокорреляции) можно вычислить из векторов (вектора) коэффициентов Уолша — Адамара по схеме Грина (см. раздел 6.3).

Следствие 4. Функции f и g из $P_2(n)$ совершенно не коррелированы, если и только если $\hat{f}(u)\hat{g}(u) = 0$ для всех $u \in \mathbb{Z}_2^n$ (или, что то же самое, $\{u \in \mathbb{Z}_2^n : \hat{f}(u) \neq 0\} \cap \{u \in \mathbb{Z}_2^n : \hat{g}(u) \neq 0\} = \varnothing$).

3.2. Строгий лавинный критерий

Определение 3.4. Говорят, что *функция f удовлетворяет строгому лавинному критерию* (SAC — *Strict Avalanche Criterion*), если $\Delta_f(u) = 0$ для всех u, таких, что $\mathrm{w}(u) = 1$.

Или: функция f удовлетворяет строгому лавинному критерию, если её производные по всем направлениям веса 1 уравновешены (по свойству 2 функции автокорреляции).

Или: функция $f \in P_2(n)$ удовлетворяет строгому лавинному критерию, если для любого $i = 1, \ldots, n$ при случайном выборе $x \in \mathbb{Z}_2^n$ и замене i-й компоненты в нём на противоположную значение $f(x)$ изменится с вероятностью $1/2$.

Пример 3.1.

x	$f(x)$	$\Delta_f(x)$
00	0	4
01	1	0
10	1	0
11	1	0

При изменении 1-го бита в x значение $f(x)$ изменится для $x = 00$ и $x = 10$; 2-го бита — для $x = 00$ и $x = 01$. Таким образом, функция удовлетворяет SAC.

Утверждение 3.1. Пусть $f \in P_2(n)$ удовлетворяет SAC. Тогда:

1. Функция f не имеет линейных и фиктивных переменных.
2. Если $n \geqslant 3$, то $\mathrm{w}(f) = 0 \pmod 2$ и, следовательно, $\deg f < n$.

Доказательство.

1. Предположим, что $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{n-1}) \oplus cx_n$ для $c \in \mathbb{Z}_2$. Тогда $f'_{0^{n-1}1} = c$ — не уравновешенная функция, что противоречит определению SAC.
2. Рассмотрим вектор a веса 1. Производная f'_a уравновешена, поэтому $|R(f,a)| = |Q(f,a)| = 2^{n-2}$, где $R(f,a) = \{x \in \mathbb{Z}_2^n : f(x) \neq f(x \oplus a)\}$; $Q(f,a) = \{x \in \mathbb{Z}_2^n : f(x) = f(x \oplus a)\}$. Таким образом, f принимает значение 1 ровно на одном наборе в каждой паре из $R(f,a)$ и на каких-то парах из $Q(f,a)$, т. е. $\mathrm{w}(f) = 0 \pmod 2$.

Утверждение доказано. ■

Определение 3.5. Говорят, что *функция f удовлетворяет строгому лавинному критерию порядка m* (SAC(m)), если любая её подфункция от $n-m$ переменных удовлетворяет SAC.

Из п. 1 утверждения 3.1 следует, что не существует функций в $P_2(n)$, удовлетворяющих SAC($n-1$).

Утверждение 3.2. Если функция f удовлетворяет SAC(m), то она удовлетворяет SAC($m-1$).

Доказательство. Пусть $f \in P_2(n)$; заметим, что $m \leqslant n-2$ и $n-m+1 \geqslant 3$. Выберем произвольную подфункцию $g(y) \in \in P_2(n-m+1)$ функции f и произвольный булев вектор a длины $n-m+1$ веса 1. Разложим g по переменной y_i, соответствующей $a_i = 0$:

$$g(y) = y_i h(z) \oplus (y_i \oplus 1) q(z);$$

здесь $z = (y_1 \dots y_{i-1} y_{i+1} \dots y_{n-m+1})$. Пусть $b = (a_1 \dots a_{i-1} a_{i+1} \dots a_{n-m+1})$ (очевидно, что $\mathrm{w}(b) = 1$). Вычислим производную функции g по направлению a:

$$g'_a(y) = y_i h(z) \oplus (y_i \oplus 1) q(z) \oplus y_i h(z \oplus b) \oplus (y_i \oplus 1) q(z \oplus b) = \\ = y_i h'_b(z) \oplus (y_i \oplus 1) q'_b(z).$$

Но h и q — подфункции функции f от $n-m$ переменных, производные которых по направлению веса 1 уравновешены, так как f удовлетворяет SAC(m). По утверждению 1.3 $\mathrm{w}(g'_a) = \mathrm{w}(h'_b) + \mathrm{w}(q'_b)$, поэтому g'_a — тоже уравновешенная функция, что в силу произвольности выбора g и a доказывает утверждение. ■

Следующая теорема описывает функции, удовлетворяющие строгому лавинному критерию максимального порядка.

Теорема 3.2. В $P_2(n)$ критерию SAC($n-2$) удовлетворяют функции вида

$$f(x_1, \dots, x_n) = \bigoplus_{1 \leqslant i < j \leqslant n} x_i x_j \oplus (a, x) \oplus b, \tag{3.1}$$

где $a \in \mathbb{Z}_2^n$, $b \in \mathbb{Z}_2$, и только они.

Доказательство.

1. Докажем, что функция (3.1) удовлетворяет SAC($n-2$). При любой фиксации $(n-2)$ переменных получим подфункцию

$h(x_i, x_j) = x_i x_j \oplus c_i x_i \oplus c_j x_j \oplus c$ для некоторых $c_i, c_j, c \in \mathbb{Z}_2$. Нетрудно убедиться, что её производные по направлениям 01 и 10 уравновешены.

2. Докажем, что если f удовлетворяет SAC$(n-2)$, то она имеет вид (3.1). Выберем произвольные переменные x_i, x_j, $i \neq j$, и зафиксируем все остальные переменные нулями. Тогда в АНФ подфункции останутся только те слагаемые из АНФ исходной функции, степени которых не больше 2. Полученная подфункция удовлетворяет SAC, поэтому она не имеет линейных и фиктивных переменных, а это значит, что в её АНФ входит слагаемое $x_i x_j$. Следовательно, АНФ функции f содержит слагаемые вида $x_i x_j$ для всех $i \neq j$.

Докажем теперь, что $\deg f = 2$. Предположим противное; выберем некоторый моном наибольшей степени и две переменные x_i, x_j, входящие в этот моном. Пусть $y = \{x_1, \ldots, x_n\} \setminus \{x_i, x_j\}$. Представим функцию f в виде

$$f(x_1, \ldots, x_n) = x_i x_j f_1(y) \oplus x_i f_2(y) \oplus x_j f_3(y) \oplus f_4(y),$$

где, в соответствии с предположением, $f_1 \neq \text{const}$. Тогда существует значение y, при котором $f_1(y) = 0$, и при соответствующей фиксации переменных получим аффинную подфункцию, т. е. подфункцию, не удовлетворяющую SAC, что противоречит требованию SAC$(n-2)$ для f. ■

Теорема 3.3 (о степени функции, удовлетворяющей SAC). Пусть $f \in P_2(n)$, $n \geqslant 3$, f удовлетворяет SAC(m) для $m < n-2$. Тогда $\deg f \leqslant n - m - 1$.

Доказательство. Предположим, что $\deg f = d > n - m - 1$. Выберем в АНФ функции f произвольный моном длины d и зафиксируем все переменные, не входящие в него. Получим подфункцию от $d \geqslant n - m \geqslant 3$ переменных степени d, которая по п. 2 утверждения 3.1 не удовлетворяет SAC. Значит, функция f не удовлетворяет SAC$(n-d)$, что ввиду $n - d \leqslant m$ невозможно по условию и утверждению 3.2. ■

Заметим, что оценка в этой теореме достижима (см. задачу 2).

3.3. Критерий распространения

Определение 3.6. Говорят, что *функция* $f \in P_2(n)$ *удовлетворяет критерию распространения* (PC — *Propagation Criterion*) *по направлению* $a \in \mathbb{Z}_2^n$, если $\Delta_f(a) = 0$, т. е. если f'_a уравновешена. Говорят, что *функция* $f \in P_2(n)$ *удовлетворяет критерию распространения степени* k (обозначается $\mathrm{PC}(k)$), если $\Delta_f(a) = 0$ для всех векторов a, таких, что $1 \leqslant \mathrm{w}(a) \leqslant k$.

Содержательный смысл критерия распространения следующий. Если функция $f \in P_2(n)$ удовлетворяет $\mathrm{PC}(k)$, то для любого набора индексов $1 \leqslant i_1 < i_2 < \ldots < i_l \leqslant n$, $l \leqslant k$, изменение компонент с номерами $i_1, \ldots, i_l$ в случайно выбранном x с вероятностью $1/2$ приводит к изменению значения $f(x)$.

Определение 3.7. Говорят, что *функция* $f \in P_2(n)$ *удовлетворяет критерию распространения степени* k *порядка* m ($\mathrm{PC}(k, m)$), если любая её подфункция от $n - m$ переменных удовлетворяет $\mathrm{PC}(k)$.

Из определения видно, что $\mathrm{PC}(1) = \mathrm{SAC}$, $\mathrm{PC}(1, m) = \mathrm{SAC}(m)$. Функция из примера 3.1 удовлетворяет $\mathrm{PC}(2)$.

Свойства критерия распространения

1. Если $f \in P_2(n)$ удовлетворяет $\mathrm{PC}(k)$, $g \in \mathcal{A}(n)$, то $f \oplus g$ удовлетворяет $\mathrm{PC}(k)$.
2. Если функции $f(x)$ и $g(y)$ удовлетворяют $\mathrm{PC}(k)$ и множества переменных x и y не пересекаются, то и функция $h(x, y) = f(x) \oplus g(y)$ удовлетворяет $\mathrm{PC}(k)$ (следует из свойства 6 функции автокорреляции).
3. Критерию $\mathrm{PC}(n)$ в $P_2(n)$ удовлетворяют бент-функции, и только они.
4. Если $f \in P_2(n)$ удовлетворяет $\mathrm{PC}(n-1)$, то $\mathrm{cor}(f) \leqslant 1$.
   В самом деле, по следствию 1 из теоремы 3.1 запишем

$$\hat{f}^2(u) = \sum_x \Delta_f(x)(-1)^{(u,x)} = \Delta_f(0^n) + \Delta_f(1^n)(-1)^{\mathrm{w}(u)} =$$
$$= 2^n + \Delta_f(1^n)(-1)^{\mathrm{w}(u)}.$$

   Предположим, что $\mathrm{cor}(f) > 1$. Тогда при $\mathrm{w}(u) = 1$ получим $0 = 2^n - \Delta_f(1^n)$, откуда $\Delta_f(1^n) = 2^n$. Но при $\mathrm{w}(u) = 2$ будем иметь $\hat{f}^2(u) = 2^{n+1} \neq 0$, что противоречит предположению и теореме 1.6.

Теорема 3.4 (о функции, удовлетворяющей SAC$(n-2)$).
Пусть $f \in P_2(n)$ удовлетворяет SAC$(n-2)$. Тогда f удовлетворяет PC(k,m), если $k+m \leqslant n-1$, либо $k+m=n$ и k чётное.

Доказательство. Согласно теореме 3.2, достаточно рассмотреть только функцию вида $f(x_1,\ldots,x_n) = \bigoplus\limits_{1\leqslant i<j\leqslant n} x_i x_j \oplus (a,x) \oplus b$, $a \in \mathbb{Z}_2^n$, $b \in \mathbb{Z}_2$. Найдём производную этой функции по направлению $c \in \mathbb{Z}_2^n$:

$$f'_c(x) = \bigoplus_{1\leqslant i<j\leqslant n} x_i x_j \oplus \bigoplus_{1\leqslant i<j\leqslant n} (x_i \oplus c_i)(x_j \oplus c_j) \oplus d = \\ = \bigoplus_{i\neq j} c_j x_i \oplus e = \bigoplus_{c_j=1} \bigoplus_{i\neq j} x_i \oplus e,$$

где d, e — некоторые константы из $\mathbb{Z}_2$. Пусть $\mathrm{w}(c) = k > 0$. Тогда для любого j переменная x_j входит в сумму k или $k-1$ раз, если соответственно $c_j = 0$ или $c_j = 1$. Зафиксируем любые m переменных. Если $k < n-m$, то среди компонент в c, соответствующих незафиксированным переменным, есть и нулевые, и единичные компоненты. В этом случае хотя бы одна переменная входит в сумму нечётное число раз, откуда следует уравновешенность производной подфункции. Это означает, что f удовлетворяет PC(k,m).

Если $k = n-m$, то при фиксации m переменных, соответствующих нулевым компонентам в c, для оставшихся переменных выполняется условие $c_j = 1$, т. е. все они входят в сумму $k-1$ раз. В этом случае производная будет уравновешена только в том случае, когда $k-1$ нечётное, т. е. k чётное. ■

3.4. Глобальные лавинные характеристики

Заметим, что критерий распространения PC(k) характеризует лишь локальные свойства функции — к её функции автокорреляции предъявляется жёсткое требование $(\Delta_f(a) = 0)$, но только на подмножестве векторов $(1 \leqslant \mathrm{w}(a) \leqslant k)$. Другой подход состоит во введении глобальных лавинных характеристик, характеризующих функцию автокорреляции в целом. Рассматриваются две таких характеристики:

$\sigma_f = \sum\limits_u \Delta_f^2(u)$ — сумма квадратов и

$\Delta_f = \max\limits_{u\neq 0^n} |\Delta_f(u)|$ — абсолютный показатель.

Чем меньше значения σ_f, Δ_f, тем лучше лавинные характеристики функции f.

Утверждение 3.3 (свойства σ_f). Пусть $f \in P_2(n)$. Тогда:

1) $2^{2n} \leqslant \sigma_f \leqslant 2^{3n}$;
2) $\sigma_f = 2^{2n}$, если и только если $f \in \mathcal{B}(n)$;
3) $\sigma_f = 2^{3n}$, если и только если $f \in \mathcal{A}(n)$.

Доказательство. Поскольку $\Delta_f(0^n) = 2^n$ и $\sigma_f \geqslant \Delta_f^2(0^n)$, верно $\sigma_f \geqslant 2^{2n}$. Здесь будем иметь равенство, если и только если $\Delta_f(u) = 0$ для всех $u \neq 0^n$, что выполняется для бент-функций и только для них.

Обозначим $a = (\Delta_f(0^n), \ldots, \Delta_f(1^n)); b = \left(\hat{f}^2(0^n), \ldots, \hat{f}^2(1^n)\right)$. Тогда $\sigma_f = (a, a)$ и по следствию 3 из теоремы 3.1 (с. 52) $a = 2^{-n} b H_{2^n}$. Рассмотрим скалярное произведение

$$(bH_{2^n}, bH_{2^n}) = \sum_i \left(\sum_j b_j (-1)^{(i,j)} \sum_k b_k (-1)^{(i,k)} \right) =$$
$$= \sum_j b_j \sum_k b_k \sum_i (-1)^{(i, k \oplus j)} = 2^n \sum_j b_j \sum_k b_k \delta(k, j) = 2^n \sum_j b_j^2.$$

Тогда

$$\sigma_f = (a, a) = 2^{-2n} (bH_{2^n}, bH_{2^n}) = 2^{-n} \sum_j \hat{f}^4(j) \leqslant$$
$$\leqslant 2^{-n} \left(\sum_j \hat{f}^2(j) \right)^2 = 2^{-n} \left(2^{2n}\right)^2 = 2^{3n}; \tag{3.2}$$

предпоследнее равенство здесь верно в силу равенства Парсеваля (1.7). В цепочке соотношений (3.2) неравенство превращается в равенство, если и только если $\hat{f}^2(u)\hat{f}^2(v) = 0$ для всех $u \neq v$, что означает $\hat{f}(u) \neq 0$ для единственного $u \in \mathbb{Z}_2^n$. Из равенства Парсеваля получим $\hat{f}(u) = \pm 2^n$; следовательно, $f(x)$ совпадает с функцией (u, x) или её отрицанием. ■

Утверждение 3.4 (свойства Δ_f). Пусть $f \in P_2(n)$. Тогда:

1) $0 \leqslant \Delta_f \leqslant 2^n$;
2) $\Delta_f = 0$, если и только если $f \in \mathcal{B}(n)$;
3) $\Delta_f = 2^n$, если и только если $f \in \mathcal{LS}(n)$.

Доказательство. Свойство 1 следует из определения: $\Delta_f = \max\limits_{u\neq 0^n} |\Delta_f(u)| = \max\limits_{u\neq 0^n} \left|\sum\limits_x (-1)^{f'_u(x)}\right|$; $\Delta_f = 0$, если и только если производные функции f по всем ненулевым направлениям уравновешены, что равносильно условию $f \in \mathcal{B}(n)$; $\Delta_f = 2^n$, если и только если производная функции f по некоторому ненулевому направлению равна константе, что означает $f \in \mathcal{LS}(n)$. ■

3.5. Частично бент-функции

Пусть $f \in P_2(n)$. Обозначим

$$M_{\Delta_f} = |\{x \in \mathbb{Z}_2^n : \Delta_f(x) \neq 0\}|; \quad M_{\hat{f}} = \left|\{x \in \mathbb{Z}_2^n : \hat{f}(x) \neq 0\}\right|.$$

Утверждение 3.5. Для любой функции $f \in P_2(n)$

$$M_{\Delta_f} \cdot M_{\hat{f}} \geqslant 2^n.$$

Доказательство. Пусть $\max\limits_x \left|\hat{f}(x)\right| = \left|\hat{f}(a)\right|$. Рассмотрим функцию $g(x) = f(x) \oplus (a, x)$; по свойству 4 преобразования Уолша — Адамара (с. 21) и свойству 5 функции автокорреляции (с. 51) $M_{\hat{f}} = M_{\hat{g}}$ и $M_{\Delta_f} = M_{\Delta_g}$; кроме того, $|\hat{g}(0^n)| = |\hat{f}(a)| = \max\limits_x |\hat{g}(x)|$, так как спектры функций f и g совпадают. Для функции g запишем:

$$\sum_x \Delta_g(x) \leqslant M_{\Delta_g} \cdot \max_x \Delta_g(x) = M_{\Delta_g} \cdot 2^n; \tag{3.3}$$

$$\sum_x \hat{g}^2(x) = 2^{2n} \leqslant M_{\hat{g}} \cdot \hat{g}^2(0^n) = \tag{3.4}$$

$$= M_{\hat{g}} \sum_x \Delta_g(x) \leqslant M_{\hat{g}} \cdot M_{\Delta_g} \cdot 2^n; \tag{3.5}$$

здесь последнее равенство верно в силу следствия 1 из теоремы 3.1. Получили, что утверждение выполнено для функции g, а значит, и для функции f. ■

Определение 3.8. Функция $f \in P_2(n)$ называется *частично бент-функцией*, если $M_{\Delta_f} \cdot M_{\hat{f}} = 2^n$.

Вспомним, что количество и распределение нулевых значений коэффициентов Уолша — Адамара характеризуют корреляционную иммунность функции, а нулевые значения функции автокорреляции означают выполнение критерия распространения по

соответствующим направлениям. Таким образом, частично бент-функции в некотором смысле оптимальны по совокупности этих характеристик (произведение количеств ненулевых значений коэффициентов Уолша — Адамара и функции автокорреляции для них минимально). Заметим, что частично бент-функциями являются все бент-функции (для них $M_{\hat{f}} = 2^n$, $M_{\Delta_f} = 1$) и все аффинные функции (для них $M_{\hat{f}} = 1$, $M_{\Delta_f} = 2^n$).

Утверждение 3.6. Частично бент-функции платовидны.

Доказательство. Пусть f — частично бент-функция, $\max\limits_x \left|\hat{f}(x)\right| = \left|\hat{f}(a)\right|$ и $g(x) = f(x) \oplus (a, x)$. Поскольку g — также частично бент-функция, в формуле (3.4) имеем равенство $\sum\limits_x \hat{g}^2(x) = M_{\hat{g}} \cdot \hat{g}^2(0^n)$. Следовательно, $\sum\limits_x \hat{f}^2(x) = M_{\hat{f}} \cdot \max\limits_x \hat{f}^2(x)$; это возможно, если все ненулевые значения $\hat{f}^2(x)$ одинаковы и равны $\max\limits_x \hat{f}^2(x)$. ■

Утверждение 3.7. Пусть $f \in P_2(n)$ — частично бент-функция. Тогда существует такой вектор $a \in \mathbb{Z}_2^n$, что для каждого $x \in \mathbb{Z}_2^n$ выполнено одно из равенств $\Delta_f(x) = 0$ или $\Delta_f(x) = = (-1)^{(a,x)} \cdot 2^n$.

Доказательство. В формуле (3.3) имеем равенство $\sum\limits_x \Delta_g(x) = = M_{\Delta_g} \cdot 2^n$, если все ненулевые значения $\Delta_g(x)$ равны 2^n. Для функции $f(x) = g(x) \oplus (a, x)$ получим

$$\Delta_f(x) = \sum_u (-1)^{g(u) \oplus (a,u) \oplus g(u \oplus x) \oplus (a, u \oplus x)} = (-1)^{(a,x)} \cdot \Delta_g(x).$$

Утверждение доказано. ■

Другими словами, производные частично бент-функции уравновешены или константы. В качестве вектора a в утверждении 3.7 может выступать любой вектор со свойством $\hat{f}(a) \neq 0$.

Утверждение 3.8. Пусть $f \in P_2(n)$ — частично бент-функция и $E_f = \{a \in \mathbb{Z}_2^n : f'_a = \text{const}\}$ — пространство её линейных структур. Тогда f удовлетворяет $\text{PC}(k)$, если и только если вес любого ненулевого вектора в E_f больше k.

Доказательство. Из утверждения 3.7 следует, что $\Delta_f(a) = 0$ для всех $a \notin E_f$, в частности, для всех a веса от 1 до k. ■

Утверждение 3.9. Частично бент-функция уравновешена, если и только если её производная по некоторому направлению равна константе 1.

Доказательство. Необходимость. Пусть $f \in P_2(n)$ — уравновешенная частично бент-функция. Тогда $\hat{f}(0^n) = 0$. По следствию 1 из теоремы 3.1 (с. 52) $\hat{f}^2(0^n) = \sum\limits_a \Delta_f(a)$, а по утверждению 3.7 $\Delta_f(a) \in \{0, \pm 2^n\}$. Тогда

$$\hat{f}^2(0^n) = \sum_a \Delta_f(a) = 2^n(c_1 - c_2) = 0,$$

где c_1 — количество положительных значений $\Delta_f(a)$ (соответствующих случаю $f'_a = \mathrm{const}\,0$); c_2 — количество отрицательных значений (для $f'_a = \mathrm{const}\,1$). Но $c_1 > 0$ силу условия $\Delta_f(0^n) = 2^n$; следовательно, и $c_2 > 0$.

Достаточность. Если $f'_a = \mathrm{const}\,1$, то $f(x) = \overline{f(x \oplus a)}$ для всех $x \in \mathbb{Z}_2^n$, что означает уравновешенность f. ■

Вопросы и задачи

1. (*) Пусть $f \in P_2(n)$, $n > 2$, $\deg f = 2$. Доказать: f удовлетворяет $\mathrm{SAC}(t)$, если и только если каждая переменная встречается в мономах длины 2 не менее $t + 1$ раза.
2. (*) Докажите, что следующая функция удовлетворяет $\mathrm{SAC}(m)$, $m \leqslant n - 2$:
$$f(x_1, \ldots, x_n) = x_1 \ldots x_{n-m-1} \oplus \bigoplus_{1 \leqslant i < j \leqslant n} x_i x_j.$$
3. (*) Пусть $f \in P_2(n)$ — квадратичная функция, не бент. Доказать: $\Delta_f = 2^n$.
4. (*) Пусть $f \in P_2(n)$, $f \notin \mathcal{LS}(n)$, $\deg f = d \geqslant 3$. Доказать: $\Delta_f \leqslant 2^n - 2^{n-d+2}$.
5. (*) Пусть $f \in \mathcal{B}(2k)$. Для следующих функций ответить на вопросы: является ли функция уравновешенной? платовидной? частично бент-функцией? Найти порядок корреляционной иммунности; нелинейность; степень критерия распространения; направления, по которым функция удовлетворяет критерию распространения:
   а) $g(x_1, x_2, \ldots, x_{2k+1}) = x_1 \oplus f(x_2, \ldots, x_{2k+1})$;
   б) $g(x_1, x_2, \ldots, x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, \ldots, x_1 \oplus x_{2k+1})$.

4. Алгебраическая иммунность

4.1. Алгебраическая атака

В 2003 г. появилась новая атака на фильтрующие генераторы (в частности, на LILI-128, Toyocrypt), которая получила название алгебраической и была позднее применена к комбинирующим генераторам и блочным шифрам [12, 14]. Для описания возможностей противостояния этой атаке и появилось понятие алгебраической иммунности булевых функций. Обсудим сначала основные идеи алгебраической атаки.

Рассмотрим фильтрующий генератор (рис. 2).

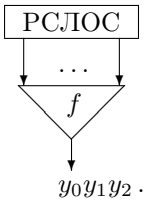


Рис. 2. Фильтрующий генератор

Ключом генератора является начальное состояние регистра $S_0 = (s_0 \ldots s_{k-1})$. Пусть L — известное линейное преобразование состояния генератора, выполняющееся за один такт его работы. Тогда если криптоаналитику станет известен фрагмент ключевого потока $y_0y_1 \ldots y_l$, то он получит систему уравнений

$$\begin{cases} y_0 = f(S_0), \\ y_1 = f(L(S_0)), \\ \ldots \\ y_l = f(L^l(S_0)). \end{cases} \tag{4.1}$$

Предположим, что выполнено одно или оба из следующих условий:

1) существует функция $g(x)$, такая, что $f(x)g(x) = h(x) \not\equiv 0$ и $\deg h$ мала;
2) существует функция $g(x) \not\equiv 0$ малой степени, такая, что $f(x)g(x) \equiv 0$.

Тогда в случае $\gamma_i = 0$ и условия 1

$$h(L^i(S_0)) = f(L^i(S_0))g(L^i(S_0)) = 0.$$

Если же $\gamma_i = 1$, то ввиду условия 2

$$g(L^i(S_0)) = f(L^i(S_0))g(L^i(S_0)) = 0.$$

Если $\deg h < \deg f$ и $\deg g < \deg f$, то получим систему уравнений меньшей, чем у (4.1), степени.

Присмотримся к условию 1 подробнее. Домножив на $f(x)$ равенство $f(x)g(x) = h(x)$, получим $fg = hf$, и значит, $h = fg = hf$, откуда $(f \oplus 1)h = 0$.

Таким образом, для противостояния алгебраической атаке требуется, чтобы у всех не равных тождественно 0 функций g, таких, что $fg \equiv 0$ или $(f \oplus 1)g \equiv 0$, была достаточно высокая степень. Это требование отражено в понятии алгебраической иммунности.

4.2. Понятие алгебраической иммунности и его свойства

Определение 4.1. Функция g называется *аннигилятором* функции f, если $g \neq \mathrm{const}\,0$ и $f(x)g(x) \equiv 0$.

Аннигиляторы существуют у всех функций, кроме $\mathrm{const}\,1$; в частности, $f \oplus 1$ — аннигилятор f. Множество всех аннигиляторов функции f будем обозначать $\mathrm{AN}(f)$; нетрудно убедиться, что $|\mathrm{AN}(f)| = 2^{2^n - \mathrm{w}(f)} - 1$.

Определение 4.2. *Алгебраической иммунностью функции* f называется минимальная из степеней аннигиляторов f и $f \oplus 1$; обозначается $\mathrm{AI}(f)$:

$$\mathrm{AI}(f) = \min_{g \in \mathrm{AN}(f) \cup \mathrm{AN}(f \oplus 1)} \deg g.$$

Теорема 4.1. Пусть $f \in P_2(n)$. Тогда $\mathrm{AI}(f) \leqslant \left\lceil \dfrac{n}{2} \right\rceil$.

Доказательство. Из функций f и $f \oplus 1$ выберем ту, вес которой не превышает 2^{n-1}; пусть это f. Построим таблицу, строки которой сопоставим значениям x, на которых $f(x) = 1$ (их количество — $\mathrm{w}(f)$), а столбцы — мономам степеней $0, 1, \ldots, \lceil n/2 \rceil$ (их будет $\sum\limits_{i=0}^{\lceil n/2 \rceil} \left(\begin{array}{c} n \\ i \end{array} \right) > 2^{n-1} \geqslant \mathrm{w}(f)$); на пересечении строки и

столбца запишем значение монома на наборе x. Поскольку столбцов больше, чем строк, то существует их ненулевая линейная комбинация, равная 0 на всех значениях x; эта комбинация задаёт АНФ некоторой функции g, причём $\deg g \leqslant \lceil n/2 \rceil$ и $g(x) = 0$ для всех x, для которых $f(x) = 1$, т. е. $g \in \mathrm{AN}(f)$.

Если $\mathrm{w}(f) > 2^{n-1}$, то аналогичным способом найдём аннигилятор функции $f \oplus 1$ степени не больше, чем $\lceil n/2 \rceil$. ■

Пример 4.1. Пусть $f(x_1, x_2, x_3) = (01010011)$. Построим таблицу:

x, $f(x) = 1$	1	x_1	x_2	x_3	x_1x_2	x_1x_3	x_2x_3
001	1	0	0	1	0	0	0
011	1	0	1	1	0	0	1
110	1	1	1	0	1	0	0
111	1	1	1	1	1	1	1

Из таблицы видно, что аннигиляторами функции f являются функции $x_1 \oplus x_2 \oplus x_1x_3 \oplus x_2x_3$, $x_1 \oplus x_1x_2$, $1 \oplus x_1 \oplus x_3 \oplus x_1x_3$ и любая их ненулевая линейная комбинация.

Утверждение 4.1.
Пусть $f(x) \in P_2(n)$, $h(x) \in \mathcal{A}(n)$, $\mathrm{AI}(f) = d$. Тогда

$$d - 1 \leqslant \mathrm{AI}(f \oplus h) \leqslant d + 1.$$

Доказательство. Пусть $g \in \mathrm{AN}(f) \cup \mathrm{AN}(f \oplus 1)$ и $\deg g = d$.

1. Пусть $fg \equiv 0$. Тогда если $(h \oplus 1)g \equiv 0$, то $(f \oplus h \oplus 1)g \equiv 0$ и $g \in \mathrm{AN}(f \oplus h \oplus 1)$. Если $(h \oplus 1)g \not\equiv 0$, то $(h \oplus 1)g \in \mathrm{AN}(f \oplus h)$ ввиду равенства $(f \oplus h)(h \oplus 1)g = f(h \oplus 1)g \equiv 0$.
2. Пусть $(f \oplus 1)g \equiv 0$. Тогда если $(h \oplus 1)g \equiv 0$, то $(f \oplus h)g = (f \oplus 1 \oplus h \oplus 1)g \equiv 0$ и $g \in \mathrm{AN}(f \oplus h)$. Если $(h \oplus 1)g \not\equiv 0$, то $(h \oplus 1)g \in \mathrm{AN}(f \oplus h \oplus 1)$, поскольку $(f \oplus h \oplus 1)(h \oplus 1)g = (f \oplus 1)(h \oplus 1)g \equiv 0$.

Получили: функция g или $(h \oplus 1)g$ является аннигилятором функции $f \oplus h$ или $f \oplus h \oplus 1$; в любом случае $\mathrm{AI}(f \oplus h) \leqslant d + 1$.

Предположим теперь, что $\mathrm{AI}(f \oplus h) < d - 1$. Тогда по только что доказанному $\mathrm{AI}(f \oplus h \oplus h) < d$, но $\mathrm{AI}(f \oplus h \oplus h) = \mathrm{AI}(f) = d$. Полученное противоречие завершает доказательство. ■

Утверждение 4.2. Пусть $f_1, f_2 \in P_2(n)$, $\mathrm{AI}(f_1)=d_1$, $\mathrm{AI}(f_2)=d_2$, $f(x_1,\ldots,x_n,x_{n+1}) = (x_{n+1}\oplus 1)f_1 \oplus x_{n+1}f_2$. Тогда

$$\mathrm{AI}(f) \leqslant \min(d_1,d_2)+1.$$

Доказательство. Пусть $g \in \mathrm{AN}(f_1)\cup\mathrm{AN}(f_1\oplus 1)$ и $\deg g = d_1$. Тогда если $g\cdot f_1 \equiv 0$, то $(x_{n+1}\oplus 1)gf \equiv 0$, а если $g(f_1\oplus 1)\equiv 0$, то $(x_{n+1}\oplus 1)g(f\oplus 1)\equiv 0$. Значит, $\mathrm{AI}(f)\leqslant d_1+1$. Аналогично, $\mathrm{AI}(f)\leqslant d_2+1$. Следовательно, $\mathrm{AI}(f)\leqslant \min(d_1,d_2)+1$. ■

Отсюда вывод: из подфункций с низкой алгебраической иммунностью не построить функцию с высокой алгебраической иммунностью.

Следствие 1. Пусть $f_1, f_2 \in P_2(n)$, $f(x_1,\ldots,x_n,x_{n+1}) = (x_{n+1}\oplus 1)f_1 \oplus x_{n+1}f_2$, n чётное, $\mathrm{AI}(f) = n/2+1$ (максимально возможная). Тогда $\mathrm{AI}(f_1) = \mathrm{AI}(f_2) = n/2$ (тоже максимально возможная).

Утверждение 4.3. Пусть $f\in P_2(n)$, f_1 — подфункция f от $n-m$ переменных, $\deg f_1 = d$. Тогда $\mathrm{AI}(f)\leqslant m+d$.

Доказательство. По формуле (1.1)

$$f(x_1,\ldots,x_n) = \bigoplus_{a_1\ldots a_m\in\mathbb{Z}_2^m} (x_1\oplus a_1\oplus 1)\cdot\ldots\times$$
$$\times(x_m\oplus a_m\oplus 1)f(a_1,\ldots,a_m,x_{m+1},\ldots,x_n);$$

заметим, что все слагаемые в этом разложении попарно ортогональны. Выберем вектор $(a_1\ldots a_m)$, при котором $f(a_1,\ldots,a_m, x_{m+1},\ldots,x_n) = f_1$, и рассмотрим функцию $g = (x_1\oplus a_1\oplus 1)\times \times\ldots\cdot(x_m\oplus a_m\oplus 1)(f_1\oplus 1)$. Очевидно, что $fg\equiv 0$ и, поскольку $\deg g = m+d$, утверждение доказано. ■

Утверждение 4.4. Пусть $f\in P_2(n)$ и $\mathrm{AI}(f) = d$. Тогда $\sum\limits_{i=0}^{d-1}\left(\begin{array}{c} n \\ i \end{array}\right) \leqslant \mathrm{w}(f) \leqslant \sum\limits_{i=0}^{n-d}\left(\begin{array}{c} n \\ i \end{array}\right)$.

Доказательство. Будем действовать по схеме доказательства теоремы (4.1) и попробуем построить аннигилятор функции f степени, не превосходящей $d-1$. Количество строк в таблице будет равно $\mathrm{w}(f)$; количество столбцов (мономов) — $\sum\limits_{i=0}^{d-1}\left(\begin{array}{c} n \\ i \end{array}\right)$, и если столбцов больше, чем строк, то существует

их линейная зависимость, т. е. найдётся аннигилятор степени, не превосходящей $d-1$, чего быть не должно. Нижняя оценка доказана.

С другой стороны, у функции $f \oplus 1$ тоже не должно быть аннигилятора степени меньше d. Поэтому

$$2^n - \mathrm{w}(f) = \mathrm{w}(f \oplus 1) \geqslant \sum_{i=0}^{d-1} \binom{n}{i},$$

откуда $\mathrm{w}(f) \leqslant 2^n - \sum\limits_{i=0}^{d-1} \binom{n}{i} = \sum\limits_{i=d}^{n} \binom{n}{i} = \sum\limits_{i=0}^{n-d} \binom{n}{i}$. ■

Следствие 2. Если $f \in P_2(n)$, n нечётное и $\mathrm{AI}(f)=(n+1)/2$ (максимально возможное), то f уравновешена.

Утверждение 4.5. Пусть $f \in P_2(n)$, $\mathrm{AI}(f) = d$. Тогда $N_f \geqslant \sum\limits_{i=0}^{d-2} \binom{n}{i}$.

Доказательство. Пусть $\max\limits_x |\hat{f}(x)| = |\hat{f}(a)|$. Тогда

$$N_f = \min(\mathrm{w}(f(x) \oplus (a,x)), \mathrm{w}(f(x) \oplus (a,x) \oplus 1)). \tag{4.2}$$

Пусть $\mathrm{AI}(f(x) \oplus (a,x)) = d_1$; тогда и $\mathrm{AI}(f(x) \oplus (a,x) \oplus 1) = d_1$. По утверждению 4.1 $d_1 \geqslant d-1$; по утверждению 4.4 с учётом (4.2) получим $N_f \geqslant \sum\limits_{i=0}^{d_1-1} \binom{n}{i} \geqslant \sum\limits_{i=0}^{d-2} \binom{n}{i}$. ■

В [3] доказана точная (достижимая) оценка нелинейности:

$$N_f \geqslant 2 \sum_{i=0}^{d-2} \binom{n-1}{i}.$$

Вопросы и задачи

1. (*) Проведите алгебраическую атаку на генератор с регистром длины 3, функция обратной связи которого равна $x_{i+3} = x_i \oplus x_{i+2}$, и фильтрующей функцией $f(x_0, x_1, x_2) = x_0x_1x_2 \oplus x_0x_1 \oplus x_0 \oplus x_1$, если известен начальный отрезок гаммы $\gamma = 010$.
2. Докажите, что $\mathrm{AI}(f) \leqslant \deg f$; $\mathrm{AI}(f) = \mathrm{AI}(g)$, если g получена из f аффинным преобразованием переменных.
3. (*) Докажите, что $\mathrm{AI}(f \oplus h) \leqslant \mathrm{AI}(f) + \mathrm{AI}(h)$.
4. (*) Пусть $f \in \mathcal{B}(n)$, $n \geqslant 4$. Докажите, что $\mathrm{AI}(f) \geqslant 2$.

5. Запреты булевых функций

При анализе последовательности, вырабатываемой фильтрующим генератором (рис. 2 на с. 62), возникает ещё одно понятие — запрет булевой функции. Если $x_1x_2\dots x_n$, $x_2x_3\dots x_{n+1}$, $\dots$, $x_mx_{m+1}\dots x_{n+m-1}$ — последовательные состояния РСЛОС генератора, а $y_1y_2\dots y_m$ — соответствующая этим состояниям выходная последовательность, т. е. $y_i = f(x_i,\dots,x_{n+i-1})$, $i = 1,\dots,m$, то будем говорить, что выходная последовательность $y_1y_2\dots y_m$ порождается входной последовательностью $x_1x_2\dots x_{n+m-1}$.

Определение 5.1. Говорят, что булева функция $f\in P_2(n)$ *имеет запрет* $y_1\dots y_m \in \mathbb{Z}_2^m$, если система уравнений

$$f(x_i,\dots,x_{n+i-1}) = y_i, \quad i = 1,\dots,m, \tag{5.1}$$

несовместна. Если для любых $m \in \mathbb{N}$ и $y_1\dots y_m \in \mathbb{Z}_2^m$ система (5.1) совместна, то функция f называется *функцией без запрета*.

Понятно, что наличие запрета у функции фильтрующего генератора является его слабостью: этот запрет никогда не появится в выходной последовательности генератора, что ухудшает её статистические свойства.

Пример 5.1. Функция $f(x_1,x_2) = x_1x_2$ имеет запрет 101, так как система уравнений

$$\begin{cases} x_1x_2 = 1, \\ x_2x_3 = 0, \\ x_3x_4 = 1 \end{cases}$$

несовместна (из первого и третьего уравнений следует, что $x_1 = x_2 = x_3 = x_4 = 1$, откуда $x_2x_3 = 1$).

Утверждение 5.1. Функция, линейная по первой или по последней своей существенной переменной, является функцией без запрета.

Доказательство. Пусть $f \in P_2(n)$ и x_k, $1 \leqslant k \leqslant n$, — её последняя существенная переменная, т. е. $f(x_1,\dots,x_n) = x_k \oplus \oplus g(x_1,\dots,x_{k-1})$ для некоторой функции $g \in P_2(k-1)$. Предположим, что $y_1\dots y_m \in \mathbb{Z}_2^m$ — запрет минимальной длины функции f. Тогда вектор $y_1\dots y_{m-1}$ не является запретом для f, т. е.

система уравнений

$$f(x_i, \ldots, x_{n+i-1}) = y_i, \quad i = 1, \ldots, m-1, \tag{5.2}$$

совместна. Заметим, что система (5.2) не зависит от переменных x_i с номерами $i > k+m-2$; пусть $b_1 b_2 \ldots b_{k+m-2}$ — её решение. Добавим к (5.2) ещё одно уравнение

$$f(x_m, \ldots, x_{n+m-1}) = x_{m+k-1} \oplus g(x_m, \ldots, x_{m+k-2}) = y_m.$$

Тогда вектор $b_1 b_2 \ldots b_{k+m-2} b_{k+m-1}$, где $b_{m+k-1} = y_m \oplus g(b_m, \ldots, b_{m+k-2})$, является решением этой расширенной системы с вектором правых частей $y_1 \ldots y_m$, что невозможно, так как $y_1 \ldots y_m$ — запрет.

Случай, когда функция f линейна по первой своей существенной переменной, рассматривается аналогично: находим решение системы

$$f(x_i, \ldots, x_{n+i-1}) = y_i, \quad i = 2, \ldots, m,$$

а затем добавляем к ней уравнение $f(x_1, \ldots, x_n) = y_1$. ■

Заметим, что линейность функции по промежуточной (не первой и не последней) переменной не является достаточной для отсутствия запрета; например, функция $x_1 \oplus x_2 \oplus x_3 \oplus x_1 x_3$ имеет запрет 10101.

Утверждение 5.2. Если функция f не уравновешена, то она имеет запрет.

Доказательство. Пусть $f \in P_2(n)$ — неуравновешенная функция, a — то из значений 0, 1, которое функция f принимает меньшее число раз, и $w = |\{x \in \mathbb{Z}_2^n : f(x) = a\}| < 2^{n-1}$. Рассмотрим выходную последовательность длины $kn+1$

$$a y_2 y_3 \ldots y_n a y_{n+2} \ldots y_{2n} a \ldots y_{(k-1)n+2} \ldots y_{kn} a, \tag{5.3}$$

в которой на первом, $(n+1)$-м, …, $(kn+1)$-м местах стоят значения a, а остальные элементы произвольны. Ясно, что входная последовательность $x_1 x_2 \ldots x_{(k+1)n}$, порождающая (5.3), должна удовлетворять системе уравнений

$$\begin{cases} f(x_1, x_2, \ldots, x_n) = a, \\ f(x_{n+1}, x_{n+2}, \ldots, x_{2n}) = a, \\ \ldots \\ f(x_{kn+1}, x_{kn+2}, \ldots, x_{(k+1)n}) = a. \end{cases} \tag{5.4}$$

Система (5.4) имеет w^{k+1} решений, так как у любых двух уравнений в ней нет общих переменных и каждое уравнение имеет w решений; количество различных последовательностей вида (5.3) равно $2^{(n-1)k}$. Так как $w < 2^{n-1}$, для некоторого достаточно большого k выполнится неравенство $2^{(n-1)k} > w^{k+1}$; другими словами, при этом k найдётся последовательность (5.3), не порождаемая ни одной входной последовательностью, т. е. запрет. ■

Определение 5.2. Функция $f \in P_2(n)$ называется *сильно равновероятной*, если для любых $m \in \mathbb{N}$ и $y_1 \dots y_m \in \mathbb{Z}_2^m$ система (5.1) имеет ровно 2^{n-1} решений.

Теорема 5.1. Булева функция не имеет запрета тогда и только тогда, когда она сильно равновероятна.

Доказательство. Достаточность очевидна. Необходимость доказывается аналогично утверждению 5.2. ■

Заметим, что утверждение 5.2 можно получить как следствие данной теоремы.

Легко убедиться в справедливости следующего утверждения.

Утверждение 5.3. Пусть функции $f \in P_2(n)$ и $g \in P_2(m)$ не имеют запретов. Тогда:

1. функция $f(x_1, \dots, x_n) \oplus 1$ не имеет запрета;
2. функция $h(x_1, \dots, x_n) = f(x_1 \oplus 1, \dots, x_n \oplus 1)$ не имеет запрета;
3. функция $q(x_1, \dots, x_{n+m-1}) = g(f(x_1, \dots, x_n), f(x_2, \dots, x_{n+1}), \dots, f(x_m, \dots, x_{n+m-1}))$ не имеет запрета.

Задача эффективного описания функций без запрета пока не решена.

6. Алгоритмические аспекты

6.1. Вычисление веса функции

Пусть булева функция задана вектором своих значений. Тогда задача вычисления её веса — это задача взвешивания булева вектора. Приведём знакомый всем с первого курса алгоритм.

Алгоритм 1. Вычисление веса булева вектора

Вход: булев вектор x.
Выход: $\mathrm{w}(x)$.
1: $n = 0$.
2: **Пока** $x \neq 0$
3: $\quad x := x \wedge (x-1)$; $\; n := n+1$.
4: Ответ: n.

Всякий раз на шаге 3 в векторе x обнуляется одна единица (самая правая), при этом увеличивается счётчик единиц. Поскольку количество повторений цикла равно весу вектора, то алгоритм 1 эффективен для взвешивания маловесных векторов.

Заметим, что с помощью обнуления в векторе x одной единицы можно проверить, является ли x степенью двойки; эта проверка полезна при вводе строки значений функции. Если условие выполнено, т. е. $x = 2^n$, то n находится как количество младших нулей в x с помощью дихотомического **Алгоритма 2** (знак $\gg$ обозначает операцию сдвига вектора вправо, $\ll$ — сдвига влево с потерей исчезающих и заполнением нулями освободившихся разрядов).

Можно предложить следующий способ взвешивания 32-битного вектора. Пусть заранее вычислены веса байтов — векторов длины 8 и записаны в таблицу: $\mathrm{TAB}[i] = \mathrm{w}(i)$, $i = 0, 1, \ldots, 255$. Тогда

$$\mathrm{w}(x) = \mathrm{TAB}[x \wedge \mathrm{0xFF}] + \mathrm{TAB}[(x \gg 8) \wedge \mathrm{0xFF}] + \\ + \mathrm{TAB}[(x \gg 16) \wedge \mathrm{0xFF}] + \mathrm{TAB}[x \gg 24].$$

Здесь префикс 0x обозначает представление следующей за ним константы в шестнадцатеричной системе счисления.

Ещё один способ взвешивания вектора основан на стратегии «*разделяй и властвуй*». Вектор делится на 2-разрядные поля

Алгоритм 2. Подсчёт количества младших нулей в 32-разрядном ненулевом булевом векторе

Вход: 32-разрядный ненулевой булев вектор x.
Выход: количество младших нулей в x.

```
1: n := 1
2: Если (x ≪ 16) = 0 то
3:     n := n + 16;  x := x ≫ 16;
4: Если (x ≪ 24) = 0 то
5:     n := n + 8;  x := x ≫ 8;
6: Если (x ≪ 28) = 0 то
7:     n := n + 4;  x := x ≫ 4;
8: Если (x ≪ 30) = 0 то
9:     n := n + 2;  x := x ≫ 2;
10: Ответ: n − x&1.
```

и в каждое поле помещается количество единиц в нём. Затем складываются значения в соседних полях, результат помещается в 4-разрядное поле, и т. д.

Пример 6.1. Для $x = 01110100$ последовательно получим:

01|11|10|00;
01|10|01|00 (взвесили по 2 разряда);
0011|0001 (сложили соседние пары);
00000100 — ответ (сложили четвёрки).

Суммирование значений в соседних полях можно выполнить параллельно. Если x — 32-разрядный вектор, то весь процесс описывается следующей последовательностью команд:

1. $x := (x \wedge 0x55555555) + ((x \gg 1) \wedge 0x55555555)$;
2. $x := (x \wedge 0x33333333) + ((x \gg 2) \wedge 0x33333333)$;
3. $x := (x \wedge 0x0F0F0F0F) + ((x \gg 4) \wedge 0x0F0F0F0F)$;
4. $x := (x \wedge 0x00FF00FF) + ((x \gg 8) \wedge 0x00FF00FF)$;
5. $x := (x \wedge 0x0000FFFF) + ((x \gg 16) \wedge 0x0000FFFF)$.

Общее число операций, включая присваивание, равно 25.

Попробуем упростить представленную последовательность команд. Заметим, что результат взвешивания не превосходит 32 и потому займёт не более шести младших битов результата. Добавим шестой шаг — выделение из полученного значения нужных

битов — и не будем заботиться об остальных битах. Тогда в команде 5 конъюнкции можно не выполнять; приходим к варианту: 5. $x := x + (x \gg 16)$.

В команде 3 суммируются значения 4-битных полей, и сумма не превосходит 8, т. е. также помещается в 4-битное поле. Поэтому выделение полей можно выполнить один раз после суммирования: 3. $x := (x + (x \gg 4)) \wedge 0\text{x}0\text{F}0\text{F}0\text{F}0\text{F}$. Аналогично для команды 4; более того, операцию конъюнкции в ней можно вообще опустить, так как мы договорились заботиться лишь о младших шести битах.

Наконец, команду 1 можно преобразовать с помощью следующей изящной формулы. Пусть x — булев вектор длины n, который можно рассматривать также как n-разрядное двоичное число. Тогда

$$\mathrm{w}(x) = x - \left[\frac{x}{2}\right] - \left[\frac{x}{4}\right] - \ldots - \left[\frac{x}{2^{n-1}}\right].$$

В самом деле, если $x = \sum\limits_{i=0}^{n-1} x_i 2^i$, то $\left[\frac{x}{2^j}\right] = \sum\limits_{i=j}^{n-1} x_i 2^{i-j}$, и

$$x - \sum_{j=1}^{n-1} \left[\frac{x}{2^j}\right] = \sum_{i=0}^{n-1} x_i \left(2^i - \sum_{t=0}^{i-1} 2^t\right) = \sum_{i=0}^{n-1} x_i = \mathrm{w}(x).$$

При $n = 2$, как в команде 1, получаем $\mathrm{w}(x) = x - \left[\frac{x}{2}\right]$. Окончательно приходим к следующему варианту.

Алгоритм 3. Вычисление веса 32-разрядного булева вектора

Вход: 32-разрядный булев вектор x.
Выход: $\mathrm{w}(x)$.

1: $x := x - ((x \gg 1) \wedge 0\text{x}55555555)$;
2: $x := (x \wedge 0\text{x}33333333) + ((x \gg 2) \wedge 0\text{x}33333333)$;
3: $x := (x + (x \gg 4)) \wedge 0\text{x}0\text{F}0\text{F}0\text{F}0\text{F}$;
4: $x := x + (x \gg 8)$;
5: $x := x + (x \gg 16)$.
6: Ответ: $x \wedge 0\text{x}3\text{F}$.

Общее число операций в алгоритме 3 равно 20. Поскольку на каждой итерации цикла в алгоритме 1 выполняется 6 операций

и количество итераций равно весу вектора, то применение алгоритма 3 предпочтительнее уже для векторов веса 4.

Заметим, что с помощью той же идеи можно определить чётность веса булева вектора, или сумму по модулю 2 всех его компонент. Эта операция может оказаться полезной при вычислении скалярного произведения.

Алгоритм 4. Сумма по модулю 2 компонент булева вектора

Вход: 32-разрядный булев вектор x.
Выход: $\mathrm{w}(x) \mod 2$.
1: $x := x \oplus (x \gg 1)$;
2: $x := x \oplus (x \gg 2)$;
3: $x := x \oplus (x \gg 4)$;
4: $x := x \oplus (x \gg 8)$;
5: $x := x \oplus (x \gg 16)$.
6: Ответ: $x \wedge 0\mathrm{x}1$.

Если булева функция зависит более чем от 5 переменных, то её вектор значений занимает несколько 32-разрядных слов, т. е. представляет собой массив таких слов. Для вычисления веса функции нужно просуммировать веса элементов массива. Этот процесс можно распараллелить следующим образом. С помощью команд 1–3 алгоритма 3 будем взвешивать 8-битные поля в каждом элементе массива, а полученные значения суммировать (также в 8-битных полях). Чтобы избежать угрозы переполнения, будем обрабатывать так по $[255/8] = 31$ элементов, после чего прибавлять к текущему весу массива значения полученных 8-битных сумм. Получим алгоритм 5; эксперимент, проделанный студентом Александром Курносенко, показывает, что по быстродействию этот алгоритм превосходит последовательное суммирование весов элементов массива примерно на 30–50 %.

Алгоритм 5. Вычисление веса массива

Вход: Массив $a = (a_0, \ldots, a_{n-1})$ 32-разрядных булевых векторов.

Выход: $\mathrm{w}(a) = \sum_{i=0}^{n-1} \mathrm{w}(a_i)$.

```
1:  w(a) := 0; i := 0.
2:  Пока i < n
3:      gr := min(i + 31, n); s := 0; j := i.
4:      Пока j < gr
5:          x := a_j;
6:          x := x − ((x ≫ 1) ∧ 0x55555555);
7:          x := (x ∧ 0x33333333) + ((x ≫ 2) ∧ 0x33333333);
8:          x := (x + (x ≫ 4)) ∧ 0x0F0F0F0F;
9:          s := s + x; j := j + 1.
10:     s := (s ∧ 0x00FF00FF) + ((s ≫ 8) ∧ 0x00FF00FF);
11:     s := (s ∧ 0x0000FFFF) + (s ≫ 16);
12:     w(a) := w(a) + s; i := i + 31.
13: Ответ: w(a).
```

6.2. Преобразование Мёбиуса

С помощью преобразования Мёбиуса решается задача построения АНФ булевой функции, и вычислить его значения для функции $f(x)$ можно по формуле 1.5 $g(a) = \bigoplus_{x \leqslant a} f(x)$. Обсудим возможные способы выполнения этого вычисления.

Способ 1. Будем перебирать все x и проверять условие $x \leqslant a$ по формуле $x \leqslant a \Leftrightarrow a \wedge x = x$, или $x \leqslant a \Leftrightarrow a \vee x = a$. Заметим, что достаточно проверить условия только для тех x, которые не больше a при сравнении их как двоичных чисел.

Способ 2. Без перебора и проверок перечислим все значения $x \leqslant a$; изящный способ такого перечисления предложен студентом Максимом Куликовым: начинаем со значения $x = a$ и получаем следующее значение x из предыдущего по формуле $x := (x - 1) \wedge a$, пока не получим $x = 0$.

Пример 6.2. Пусть $a = 1001$. Тогда x последовательно принимает значения 1001; 1000; 0001; 0000.

Второй способ заметно выигрывает у первого по быстродействию, однако недостаток обоих состоит в отсутствии параллелизма — на каждом шаге прибавляется только одно значение (один бит) $f(x)$.

Способ 3. Построим матрицу отношения предшествования булевых векторов $M_{2^n} = ||m_{ax}||$, строкам и столбцам которой сопоставлены булевы векторы длины n и $m_{ax} = 1 \Leftrightarrow x \leqslant a$. Например,

$$M_2 = \begin{array}{c|cc} a\backslash x & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 1 & 1 \end{array}; \quad M_4 = \begin{array}{c|cccc} a\backslash x & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 1 & 1 & 0 & 0 \\ 10 & 1 & 0 & 1 & 0 \\ 11 & 1 & 1 & 1 & 1 \end{array}.$$

Нетрудно убедиться, что

$$M_{2^n} = \left\| \begin{array}{cc} M_{2^{n-1}} & 0 \\ M_{2^{n-1}} & M_{2^{n-1}} \end{array} \right\| \tag{6.1}$$

и $\mu(f) = M_{2^n} \cdot \mathbf{f}$, где $\mathbf{f}$ — вектор-столбец значений функции f. Если $\mathbf{f}_0$ и $\mathbf{f}_1$ — соответственно младшая и старшая половины вектора значений f, то по формуле (6.1) получим следующую рекурсивную формулу:

$$M_{2^n} \cdot \mathbf{f} = \left\| \begin{array}{cc} M_{2^{n-1}} & 0 \\ M_{2^{n-1}} & M_{2^{n-1}} \end{array} \right\| \cdot \left\| \begin{array}{c} \mathbf{f}_0 \\ \mathbf{f}_1 \end{array} \right\| = \left\| \begin{array}{c} M_{2^{n-1}} \cdot \mathbf{f}_0 \\ M_{2^{n-1}} \cdot (\mathbf{f}_0 \oplus \mathbf{f}_1) \end{array} \right\|.$$

На «дне» рекурсии для функции от одной переменной

$$\mu(f) = \left\| \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right\| \cdot \left\| \begin{array}{c} f(0) \\ f(1) \end{array} \right\| = \left\| \begin{array}{c} f(0) \\ f(0) \oplus f(1) \end{array} \right\|.$$

Для функции от трёх переменных с вектором значений $\mathbf{f}$ преобразование Мёбиуса g вычисляется с помощью следующей последовательности команд:

1. $g := \mathbf{f}$;
2. $g := g \oplus ((g \gg 1) \wedge 0\text{x}55)$;
3. $g := g \oplus ((g \gg 2) \wedge 0\text{x}33)$;
4. $g := g \oplus ((g \gg 4) \wedge 0\text{x}0\text{F})$.

Таблица иллюстрирует этот процесс:

x	$f(x)$	Значение g			
		Шаг 1	Шаг 2	Шаг 3	Шаг 4
000	a	a	a	a	a
001	b	b	$a \oplus b$	$a \oplus b$	$a \oplus b$
010	c	c	c	$a \oplus c$	$a \oplus c$
011	d	d	$c \oplus d$	$a \oplus b \oplus c \oplus d$	$a \oplus b \oplus c \oplus d$
100	e	e	e	e	$a \oplus e$
101	h	h	$e \oplus h$	$e \oplus h$	$a \oplus b \oplus e \oplus h$
110	i	i	i	$e \oplus i$	$a \oplus c \oplus e \oplus i$
111	j	j	$i \oplus j$	$e \oplus h \oplus i \oplus j$	$a \oplus b \oplus c \oplus d \oplus$ $\oplus e \oplus h \oplus i \oplus j$

Заметим, что в реализации на ЭВМ естественнее размещать значения функции для $x = 0\ldots00,\ 0\ldots01,\ \ldots,\ 1\ldots11$ от младших разрядов к старшим; в этом случае надо изменить направление сдвига и константы в командах 2–4 на 0xAA, 0xCC и 0xF0 соответственно.

6.3. Преобразование Уолша — Адамара

Вспомним формулу (1.9): $\widehat{F} = F \cdot H_{2^n}$, где H_{2^n} — матрица Сильвестра — Адамара. Это умножение выполняется за 2^{2n} операций сложения/вычитания, так как элементами H_{2^n} являются ± 1. Существует способ вычисления ПУА за $n \cdot 2^n$ операций; он называется *быстрым преобразованием Уолша — Адамара*, или *схемой Грина*, и основан на интересном свойстве матрицы Сильвестра — Адамара.

Определение 6.1. *Кронекеровским произведением матриц* $A_{n\times n}$ и $B_{m\times m}$ называется матрица порядка nm следующего вида:

$$A \otimes B = \left\| \begin{array}{ccc} a_{11}B & \ldots & a_{1n}B \\ \ldots & \ldots & \ldots \\ a_{n1}B & \ldots & a_{nn}B \end{array} \right\|.$$

Заметим, что

1) кронекеровское произведение ассоциативно;
2) $H_{2^n} = H_2 \otimes H_{2^{n-1}}$ (следует из соотношений (1.8));
3) $(E_2 \otimes A)(E_2 \otimes B) = E_2 \otimes AB$. Здесь и далее E_k — единичная матрица порядка $k \geqslant 1$; A и B — произвольные $(n \times n)$-матрицы.

Утверждение 6.1.

(6.2) $H_{2^n} = A^{(1)}_{2^n} \cdot A^{(2)}_{2^n} \cdot \ldots \cdot A^{(n)}_{2^n}$, где $A^{(i)}_{2^n} = E_{2^{n-i}} \otimes H_2 \otimes E_{2^{i-1}}$.

Доказательство. Индукция по n.

Б а з а и н д у к ц и и. При $n = 1$ имеем $H_2 = A^{(1)}_2$.

П р е д п о л о ж е н и е и н д у к ц и и. Пусть формула (6.2) верна для некоторого $n \geqslant 1$.

Ш а г и н д у к ц и и. Имеют место равенства: $A^{(i)}_{2^{n+1}} = E_2 \otimes A^{(i)}_{2^n}$ при $i = 1, \ldots, n$, так как $E_{2^{n+1-i}} = E_2 \otimes E_{2^{n-i}}$; $A^{(n+1)}_{2^{n+1}} = H_2 \otimes E_{2^n}$. Тогда

$$A^{(1)}_{2^{n+1}} \cdot \ldots \cdot A^{(n+1)}_{2^{n+1}} = \left(E_2 \otimes A^{(1)}_{2^n}\right) \cdot \ldots \cdot \left(E_2 \otimes A^{(n)}_{2^n}\right)\left(H_2 \otimes E_{2^n}\right) =$$
$$= \left(E_2 \otimes H_{2^n}\right)\left(H_2 \otimes E_{2^n}\right) = H_2 \otimes H_{2^n} = H_{2^{n+1}}.$$

Утверждение доказано. ■

Пример 6.3. Вычислим H_4.

$$A^{(1)}_4 = E_2 \otimes H_2 = \begin{Vmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{Vmatrix};$$

$$A^{(2)}_4 = H_2 \otimes E_2 = \begin{Vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{Vmatrix};$$

$$H_4 = A^{(1)}_4 \cdot A^{(2)}_4 = \begin{Vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{Vmatrix}.$$

В чём же смысл замены по формуле (6.2) одной матрицы произведением n матриц? Нетрудно убедиться, что матрицы $A^{(i)}_{2^n}$ в каждом столбце содержат только по два ненулевых элемента, следовательно, умножение вектора на столбец выполняется за одну операцию сложения/вычитания, на матрицу — за 2^n операций. Таким образом, с использованием формулы 6.2 ПУА вычисляется за $n \cdot 2^n$ операций. Рис. 3 иллюстрирует процесс для

функции от двух переменных с характеристической последовательностью $(a\ b\ c\ d)$. Читатель, знакомый с быстрым преобразованием Фурье, несомненно, увидит аналогию.

$$(a\ b\ c\ d)\cdot A_4^{(1)} = (a+b \quad a-b \quad c+d \quad c-d) = (e\ h\ i\ j);$$
$$(e\ h\ i\ j)\cdot A_4^{(2)} = (e+i \quad h+j \quad e-i \quad h-j).$$

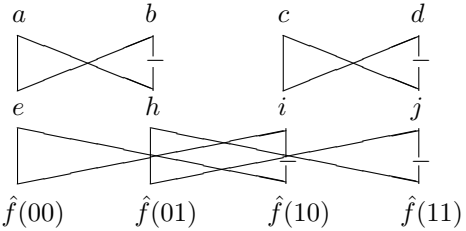


Рис. 3. Схема Грина вычисления ПУА

В заключение приведём алгоритм А. Д. Закревского перебора сочетаний из n по k единиц, который полезен при вычислении степени функции, порядка её корреляционной иммунности и др. Начальный вектор, равный $\underbrace{1\ldots1}_{k}0\ldots0$, вычисляется как

$$a = ((1 \ll k) - 1) \ll (n - k).$$

Переход к следующему сочетанию:

$$b := (a+1) \wedge a;$$
$$c := \mathrm{w}((b-1) \oplus a) - 2;$$
$$a := (((((a+1) \oplus a) \ll 1) + 1) \ll c) \oplus b.$$

7. Решения некоторых задач

Глава 1

3. Необходимость очевидна. Достаточность докажем от противного. Предположим, что $f \in P_2(n)$ зависит от некоторой переменной (без ограничения общности, пусть это будет x_1) нелинейно и нефиктивно; обозначим $x' = x_2 \dots x_n$. Тогда можно записать $f(x) = x_1 g_1(x') \oplus g_2(x')$, где $g_1 \neq \text{const}$. Для произвольного набора x' получим

$$g_2(x') = f(0x') = f(1x' \oplus 10^{n-1}) = f(1x') \oplus f(10^{n-1}) = \\ = g_1(x') \oplus q_2(x') \oplus g_1(0^{n-1}) \oplus g_2(0^{n-1}),$$

откуда $g_1(x') = g_1(0^{n-1}) \oplus g_2(0^{n-1})$, что противоречит условию $g_1 \neq \text{const}$.

15. Рассмотрим случай уравновешенных функций f и g. По свойству 7 ПУА $\widehat{f \oplus g}(ab) = \hat{f}(a)\hat{g}(b)$. По теореме 1.6 $\hat{f}(a) = 0$ для всех a, $\mathrm{w}(a) \leqslant \mathrm{sut}(f)$, и $\hat{g}(b) = 0$ для всех b, $\mathrm{w}(b) \leqslant \mathrm{sut}(g)$. Если $\mathrm{w}(ab) \leqslant \mathrm{sut}(f) + \mathrm{sut}(g) + 1$, то обязательно $\mathrm{w}(a) \leqslant \mathrm{sut}(f)$ или $\mathrm{w}(b) \leqslant \mathrm{sut}(g)$. Следовательно, $\widehat{f \oplus g}(ab) = 0$ для всех таких ab. С другой стороны, существуют векторы c и d веса $\mathrm{sut}(f) + 1$ и $\mathrm{sut}(g) + 1$ соответственно, для которых $\hat{f}(c) \neq 0$ и $\hat{g}(d) \neq 0$. Значит, $\widehat{f \oplus g}(cd) \neq 0$; окончательно получаем $\mathrm{sut}(f \oplus g) = \mathrm{sut}(f) + \mathrm{sut}(g) + 1$.

Случай, когда хотя бы одна из f, g не уравновешена, рассматривается аналогично.

16. По свойству 7 ПУА $\widehat{f \oplus g}(cd) = \hat{f}(c)\hat{g}(d)$; по свойству 6 $\hat{g}(d) = 0$ для всех $d \neq a$. Таким образом, $\widehat{f \oplus g}(cd) \neq 0$ только при $d = a$, т. е. при $\mathrm{w}(cd) \geqslant k$. Следовательно, $\mathrm{cor}(f \oplus g) \geqslant k-1$. Если f не уравновешена, то $\hat{f}(0^n) \neq 0$, откуда $\widehat{f \oplus g}(0^n a) \neq 0$ и $\mathrm{cor}(f \oplus g) = k - 1$.

Если f уравновешена, то $\widehat{f \oplus g}(ca) = 0$ для всех таких c, что $0 \leqslant \mathrm{w}(c) \leqslant \mathrm{cor}(f)$ (соответственно $k \leqslant \mathrm{w}(ca) \leqslant k + \mathrm{cor}(f)$), и существует вектор c веса $\mathrm{cor}(f) + 1$, такой, что $\widehat{f \oplus g}(ca) \neq 0$.

17. Вспомним определение подфункции f^b из тождества Саркара: для $b \in \mathbb{Z}_2^n$ переменная x_i функции f фиксируется и принимает значение 0, если и только если $b_i = 1$; другими словами, f^b определена на тех и только тех x, для которых $x \leqslant \bar{b}$.

Тогда $\mathrm{w}(f^b) = \sum\limits_{x \leqslant \bar{b}} f(x) = g(\bar{b}) (\mathrm{mod}\, 2)$, где $g = \mu(f)$; здесь последнее равенство имеет место по формуле 1.5 для преобразования Мёбиуса. Выберем произвольный вектор b, такой, что $\mathrm{w}(\bar{b}) > n - k + 1$, т. е. $\mathrm{w}(b) < k - 1$. Из условия задачи следует, что $\sum\limits_{a \leqslant b} \hat{f}(a) = 2^k t$ для некоторого целого t, а по тождеству Саркара $\sum\limits_{a \leqslant b} \hat{f}(a) = 2^n - 2^{\mathrm{w}(b)+1} \cdot g(\bar{b}) (\mathrm{mod}\, 2)$. Отсюда получаем

$$g(\bar{b}) = \frac{2^n - 2^k t}{2^{\mathrm{w}(b)+1}} = 0 (\mathrm{mod}\, 2),$$

и $\deg f \leqslant n - k + 1$.

Глава 2

1. Пусть $g(y) = (c, y)$ и $h(x) = (a, x) \oplus b$ — наилучшее аффинное приближение функции f. Тогда из формулы (2.1) следует $\max |\hat{f}(x)| = |\hat{f}(a)|$; по свойству 6 ПУА (с. 21) $\max |\hat{g}(y)| = \hat{g}(c)$; по свойству 7 ПУА $\max |\widehat{f \oplus g}(xy)| = |\hat{f}(a)\hat{g}(c)|$. Осталось заметить, что $\hat{g}(c) > 0$, поэтому знаки $\hat{f}(a)$ и $\hat{f}(a)\hat{g}(c)$ совпадают.
2. Ответ: $N_{f \oplus g} = 2^m N_f + 2^n N_g - 2 N_f N_g$.
4. Пусть $a \in \mathbb{Z}_2^{n-1}$, $b \in \mathbb{Z}_2$.

$$\hat{f}(ab) = \sum_{x,y} (-1)^{f(x,y) \oplus (a,x) \oplus by} =$$

$$= \sum_{\substack{x, \\ y=0}} (-1)^{f_2(x) \oplus (a,x)} + \sum_{\substack{x, \\ y=1}} (-1)^{f_1(x) \oplus (a,x) \oplus b} = \hat{f}_2(a) \pm \hat{f}_1(a).$$

   Из того, что f_1, f_2 — бент-функции, следует $\hat{f}_1(a), \hat{f}_2(a) = \pm 2^{(n-1)/2}$, откуда $\hat{f}(ab) \in \{\pm 2^{(n+1)/2}, 0\}$, $\max |\hat{f}(ab)| = 2^{(n+1)/2}$ и по формуле (2.1) $N_f = 2^{n-1} - 2^{(n-1)/2}$.
5. Предположим, что существует $g \in \mathcal{A}(n)$, $g \neq h$, для которой $\mathrm{d}(f, g) < \mathrm{d}(f, h) \leqslant 2^{n-2}$. Поскольку $g \oplus h \in \mathcal{A}(n)$, то $\mathrm{w}(g \oplus h) \in \{2^{n-1}, 2^n\}$. Но $\mathrm{w}(g \oplus h) = \mathrm{d}(g, h) \leqslant \mathrm{d}(f, h) + \mathrm{d}(f, g) < 2\mathrm{d}(f, h) \leqslant 2^{n-1}$. Полученное противоречие доказывает утверждение.

7. Пусть $x, y \in \mathbb{Z}_2^n$, $f(x,y) = (\pi(x), y) \oplus g(x)$. Тогда

$$2^n \cdot (-1)^{\tilde{f}(x,y)} = \hat{f}(x,y) = \sum_{a,b \in \mathbb{Z}_2^n} (-1)^{f(a,b) \oplus (a,x) \oplus (b,y)} =$$
$$= \sum_{a,b \in \mathbb{Z}_2^n} (-1)^{(\pi(a),b) \oplus g(a) \oplus (a,x) \oplus (b,y)} =$$
$$= \sum_{a \in \mathbb{Z}_2^n} (-1)^{g(a) \oplus (a,x)} \underbrace{\sum_{b \in \mathbb{Z}_2^n} (-1)^{(\pi(a),b) \oplus (b,y)}}_{2^n \delta(\pi(a),y)} =$$
$$= 2^n (-1)^{g(\pi^{-1}(y)) \oplus (\pi^{-1}(y),x)}.$$

Значит, $\tilde{f}(x,y) = g(\pi^{-1}(y)) \oplus (\pi^{-1}(y), x)$, т. е. $\tilde{f} \in \mathcal{M}(2n)$.

8. Пусть $f'_a = \text{const}$. Тогда или $f(x) = f(x \oplus a)$ для всех x (т. е. единичных значений — чётное число), или $f(x) = \overline{f(x \oplus a)}$ для всех x (и тогда $\mathrm{w}(f) = 2^{n-1}$).
9. Пусть g_1 — ближайшая к f, а g_2 — ближайшая к $f \oplus h$ функции из класса $\mathcal{LS}(n)$. Тогда

$$CN_f = \mathrm{d}(f, g_1) = \mathrm{w}(f \oplus g_1) = \mathrm{w}(f \oplus h \oplus h \oplus g_1) =$$
$$= \mathrm{d}(f \oplus h, h \oplus g_1) \geqslant CN_{f \oplus h};$$

здесь последнее неравенство имеет место в силу условия $h \oplus g_1 \in \mathcal{LS}(n)$ по свойству 4 класса $\mathcal{LS}(n)$ (с. 42). Аналогично получаем:

$$CN_{f \oplus h} = \mathrm{d}(f \oplus h, g_2) = \mathrm{w}(f \oplus h \oplus g_2) = \mathrm{d}(f, h \oplus g_2) \geqslant CN_f.$$

Следовательно, $CN_f = CN_{f \oplus h}$.

10. Обозначим $g(x) = f'_a(x) = f(x) \oplus f(x \oplus a)$ и рассмотрим её производную: $g'_a(x) = f(x) \oplus f(x \oplus a) \oplus f(x \oplus a) \oplus f(x) \equiv 0$.
11. Достаточно воспользоваться свойством 7 производных (с. 42).
12. $\mathcal{LS}(2) = \mathcal{A}(2)$; $\mathcal{LS}(3) = \{f \in P_2(3) : \mathrm{w}(f) = 0 \pmod 2\}$ (следует из задач 8, 11, следствия 2 утверждения о преобразовании Мёбиуса (с. 11) и из несуществования бент-функций для нечётного числа переменных).

13. Необходимость. Рассмотрим произвольный вектор z со свойством $(z,a) = c \oplus 1$.

$$\hat{f}(z) = \sum_x (-1)^{f(x)\oplus(z,x)} = \sum_x (-1)^{f(x\oplus a)\oplus(z,x)\oplus(z,a)} =$$
$$= \sum_x (-1)^{f(x)\oplus c\oplus(z,x)\oplus c\oplus 1} = -\hat{f}(z).$$

Следовательно, $\hat{f}(z) = 0$.
Достаточность. Воспользуемся формулой обращения (теорема 1.4 на с. 24).

$$(-1)^{f'_a(x)} = (-1)^{f(x)}(-1)^{f(x\oplus a)} =$$
$$= 2^{-2n}\sum_y \hat{f}(y)(-1)^{(x,y)}\sum_z \hat{f}(z)(-1)^{(x\oplus a,z)} =$$
$$= 2^{-2n}\sum_y \hat{f}(y)(-1)^{(x,y)}\sum_z \hat{f}(z\oplus y)(-1)^{(x\oplus a,z\oplus y)} =$$
$$= 2^{-2n}\sum_z (-1)^{(z,x\oplus a)}\sum_y \hat{f}(y)\hat{f}(z\oplus y)(-1)^{(y,a)}.$$

По условию $\hat{f}(y) = 0$ при всех y, для которых $(y,a) \neq c$. Поэтому можем вынести константу $(-1)^{(y,a)} = (-1)^c$ за знак суммы и с учётом соотношения ортогональности (теорема 1.3, с. 24) продолжить цепочку равенств:

$$(-1)^{f'_a(x)} = 2^{-2n}(-1)^c\sum_z (-1)^{(z,x\oplus a)}2^{2n}\delta(z,0^n) = (-1)^c.$$

Следовательно, $f'_a(x) = c$ для любого x.

14. Утверждение следует из определения платовидной функции и из равенства Парсеваля (1.7).
15. Из задачи 14 следует, что найдётся вектор $a \in \mathbb{Z}_2^n$, такой, что $\hat{f}(a) = 0$. Тогда для функции $g(x) = (a,x) \in \mathcal{L}(n)$ по свойству 4 ПУА (с. 21) получим: $\widehat{f\oplus g}(0^n) = \hat{f}(a) = 0$, что означает уравновешенность функции $f \oplus g$.
16. Из равенства Парсеваля следует, что $2^{2n} \leqslant \max\limits_a \hat{f}^2(a)|S|$, откуда $\max\limits_a |\hat{f}(a)| \geqslant 2^n/\sqrt{|S|}$, и равенство достигается, если и только если все ненулевые значения $|\hat{f}(a)|$ одинаковы.
17. Утверждение следует из задачи 17 главы 1 при $k = n - r$.

1. Пусть $x \in \mathbb{Z}_2^{n-1}$, $y \in \mathbb{Z}_2$ и $f(x,y) = y(a,x) \oplus g(x) \oplus by$ для некоторых $a \in \mathbb{Z}_2^{n-1}$, $g \in P_2(n-1)$, $b \in \mathbb{Z}_2$.
   Необходимость. Предположим, что $\mathrm{w}(a) \leqslant t$. Зафиксируем переменные x_i для всех i, где $a_i = 1$; получим функцию, линейно или фиктивно зависящую от y и, следовательно, не удовлетворяющую SAC. Это противоречит условию.
   Достаточность. Пусть $\mathrm{w}(a) \geqslant t+1$. Тогда $f'_{0^{n-1}1}(x,y) = (a,x) \oplus b$ — уравновешенная функция при любой фиксации любых t переменных. Следовательно, f удовлетворяет $\mathrm{SAC}(t)$.
2. У к а з а н и е. Найдите производные функции f по направлениям $\mathbf{e}_1$ и $\mathbf{e}_{n-m}$.
3. Из того, что $\deg f'_a \leqslant 1$ для любого $a \in \mathbb{Z}_2^n$ и f — не бент-функция, следует, что существует $a \neq 0^n$, для которого $f'_a = \mathrm{const}$. Следовательно, $\Delta_f = 2^n$.
4. Рассмотрим произвольный ненулевой вектор $x \in \mathbb{Z}_2^n$; пусть $k = \deg f'_x$. Тогда $k \leqslant d-1$; $k \geqslant 1$ в силу условия $f \notin \mathcal{LS}(n)$. По утверждению 1.5 получим:

$$2^{n-d+1} \leqslant 2^{n-k} \leqslant \mathrm{w}(f'_x) \leqslant 2^n - 2^{n-k} \leqslant 2^n - 2^{n-d+1}.$$

   Для завершения доказательства осталось воспользоваться равенством $\Delta_f(x) = 2^n - 2\mathrm{w}(f'_x)$.
5. а) Функция g уравновешена, так как имеет линейную переменную. Для $a \in \mathbb{Z}_2$ и $b \in \mathbb{Z}_2^{2k}$:
   $g'_{ab}(x_1, x_2, \ldots, x_{2k+1}) = a \oplus f'_b(x_2, \ldots, x_{2k+1})$ — уравновешена для всех $b \neq 0^{2k}$. Следовательно, g удовлетворяет критерию распространения по всем направлениям, кроме 0^{2k+1} и 10^{2k}; степень РС равна 0; $M_{\Delta_g} = 2$;
   $\hat{g}^2(ab) = \Delta_g(0^{2k+1}) + (-1)^a \Delta_g(10^{2k}) = 2^{2k+1}(1-(-1)^a)$; следовательно, $\mathrm{cor}(g) = 0$; g платовидна; $M_{\hat{g}} = 2^{2k}$; g является частично бент-функцией.
   По свойству 2.1 нелинейности (с. 35)

$$N_g = 2N_f = 2(2^{2k-1} - 2^{k-1}) = 2^{2k} - 2^k.$$

   б) Для $a = (a_1 \ldots a_{2k+1})$:

$g'_a(x_1, x_2, \ldots, x_{2k+1}) = a_1 \oplus f'_b(x_1 \oplus x_2, \ldots, x_1 \oplus x_{2k+1})$, где $b = (a_1 \oplus a_2, \ldots, a_1 \oplus a_{2k+1})$, — уравновешена для всех $b \neq 0^{2k}$. Следовательно, g удовлетворяет PC($2k$); $M_{\Delta_g} = 2$;

$$\hat{g}^2(a) = \Delta_g(0^{2k+1}) + (-1)^{\mathrm{w}(a)}\Delta_g(1^{2k+1}) = \\ = 2^{2k+1}(1 - (-1)^{\mathrm{w}(a)});$$

следовательно, g уравновешена, платовидна, частично бент, $\mathrm{cor}(g) = 0$, $N_g = 2^{2k} - 2^k$.

Глава 4

1. Пусть (s_0, s_1, s_2) — начальное состояние генератора. Тогда его состояния в следующие два такта работы равны $(s_1, s_2, s_0 \oplus s_2)$ и $(s_2, s_0 \oplus s_2, s_0 \oplus s_1 \oplus s_2)$. Запишем систему уравнений для перехваченного отрезка гаммы:

$$\begin{cases} s_0 s_1 s_2 \oplus s_0 s_1 \oplus s_0 \oplus s_1 = 0, \\ s_0 s_1 s_2 \oplus s_1 \oplus s_2 = 1, \\ s_0 s_1 s_2 \oplus s_1 s_2 \oplus s_0 = 0. \end{cases}$$

Найдём аннигиляторы минимальной степени для функций f и $f \oplus 1$ — это $g_1 = x_0 x_1 \oplus x_0 \oplus x_1 \oplus 1$ и $g_2 = x_0 \oplus x_1$ соответственно. Заменим, в соответствии со схемой алгебраической атаки, первое и третье уравнения системы на $g_2(L^i(s_0, s_1, s_2)) = 0$, $i = 0, 2$; второе — на $g_1(L(s_0, s_1, s_2)) = 0$. Получим:

$$\begin{cases} s_0 \oplus s_1 = 0, \\ s_1 s_2 \oplus s_1 \oplus s_2 \oplus 1 = 0, \\ s_0 = 0. \end{cases}$$

Решением системы является начальное состояние генератора $(s_0, s_1, s_2) = 001$.

3. Пусть $\deg g_1 = \mathrm{AI}(f)$, $\deg g_2 = \mathrm{AI}(h)$. Тогда $g_1 g_2$ — аннигилятор функции $f \oplus h$, если $f g_1 = 0$ и $h g_2 = 0$ или $(f \oplus 1) g_1 = 0$ и $(h \oplus 1) g_2 = 0$, и аннигилятор функции $f \oplus g \oplus 1$ в остальных случаях ($f g_1 = 0$ и $(h \oplus 1) g_2 = 0$ или $(f \oplus 1) g_1 = 0$ и $h g_2 = 0$).

4. От противного: предположим, что $h \in \mathcal{A}(n)$ — аннигилятор функции f (для аннигилятора функции $f \oplus 1$ рассуждения аналогичны, так как $f \oplus 1$ — тоже бент-функция). Очевидно, что $h \neq \text{const}$, поэтому $\mathrm{w}(h) = 2^{n-1}$. Для $a, b \in \{0,1\}$ обозначим $M_{ab} = \{x \in \mathbb{Z}_2^n : f(x) = a, h(x) = b\}$. Тогда $M_{11} = \varnothing$; $|M_{01}| = \mathrm{w}(h) = 2^{n-1}$; $|M_{10}| = \mathrm{w}(f) = 2^{n-1} \pm 2^{n/2-1}$ (по свойству 3 бент-функций, с. 36). Из определения бент-функции следует, что $\mathrm{d}(f,h) = 2^{n-1} \pm 2^{n/2-1}$, т. е. $|M_{01}| + |M_{10}| = 2^{n-1} \pm 2^{n/2-1}$, и при $n \geqslant 4$ это не равно $2^n \pm 2^{n/2-1}$. Получили противоречие.

Литература

1. *Агибалов Г. П.* Избранные теоремы начального курса криптографии. Томск: Изд-во НТЛ, 2005.
2. *Бабаш А. В., Шанкин Г. П.* Криптография. М.: СОЛОН-Р, 2002.
3. *Лобанов М. С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Т. 18. Вып. 3. С. 152–159.
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
5. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М: МНЦМО, 2004.
6. *Тарannиков Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Мат. вопросы кибернетики. Вып. 11. 2002. С. 91–148.
7. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrücken: LAP LAMBERT Academic Publishing, 2011.
8. *Токарева Н. Н.* Симметричная криптография. Краткий курс. Новосибирск: Изд-во НГУ, 2012.
9. *Уоррен Г.* Алгоритмические трюки для программистов. М.: Вильямс, 2003.
10. *Фомичёв В. М.* Дискретная математика и криптология. М.: Диалог-МИФИ, 2003.
11. *Фомичёв В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
12. *Courtois N. and Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
13. *Dalai D. K.* On some necessary conditions of Boolean functions to resist algebraic attack. Ph. D. Thesis. Kolkata, India, 2006.
14. *Meier W., Pasalic E., and Carlet C.* Algebraic attack and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474–491.

Содержание

Издание подготовлено в авторской редакции

Отпечатано на участке оперативной полиграфии
Издательского Дома Томского государственного университета

Заказ № 138 от «4» февраля 2014 г. Тираж 40 экз.