КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ*

И. В. Агафонова

ivagafonova@home.eltel.net

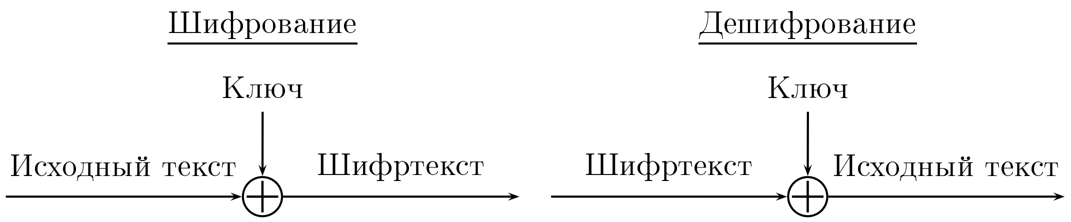
18 декабря 2007 г.

1. О булевых функциях в криптографии

В традиционных системах шифрования, переводящих открытое сообщение в зашифрованное с помощью секретного ключа, решающую роль играет аппарат булевых функций. К этим функциям предъявляется ряд требований, имеющих целью предельно осложнить расшифровку сообщения лицом, не являющимся его адресатом.

Для иллюстрации применения булевых функций приведём схему поточного шифрования, когда каждый поступающий символ тут же преобразуется в символ шифртекста.

Поточные шифры основаны на так называемом *шифре Вернама*, имеющем следующую схему:



Исходный текст, ключ, шифртекст — бинарные строки одинаковой длины. Операция $\oplus$ означает побитовое сложение по модулю 2. При дешифровании схема та же, что и при шифровании, только исходный текст и шифртекст меняются местами. Другое название шифра Вернама — одноразовый шифрблокнот (one time pad). Действительно, дважды такой шифр не используют:

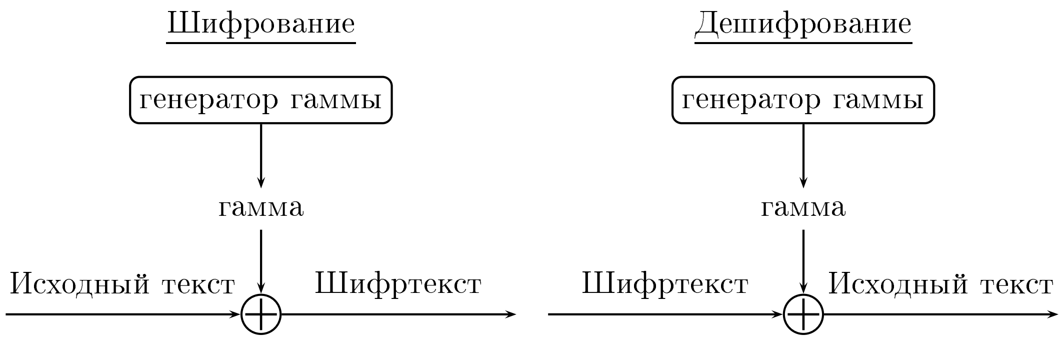
*Семинар по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD»: `http://www.dha.spb.ru/`

при сложении двух шифртекстов, соответствующих одному ключу, получается сумма исходных текстов, что даёт много информации об исходных текстах и даже часто позволяет их прочесть.

Шеннон доказал, что при совершенно случайном ключе, используемом один раз, шифр Вернама является абсолютно стойкой криптосистемой, то есть перехват шифртекста не даёт никакой информации о переданном сообщении. Это единственный в настоящее время шифр с таким свойством.

На практике чаще всего отправитель и получатель сообщений выбирают вместо ключа в шифре Вернама псевдослучайную последовательность, которая по оговорённому (не секретному) алгоритму генерируется из короткого секретного ключа. Такая последовательность носит название *ключевой поток* или *гамма* (key stream, gamma).

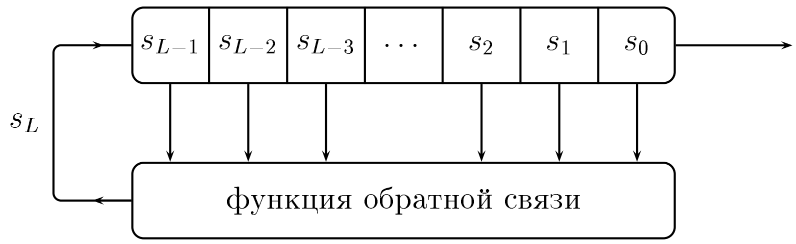
Теперь процесс шифрования выглядит так:



Стандартно секретный ключ размножается до гаммы с помощью устройств, называемых *регистрами сдвига с линейной обратной связью* (Linear Feedback Shift Register, сокращённо LFSR).

Регистр сдвига образован множеством ячеек памяти, в каждой из которых записан один бит информации. В начале работы ячейки содержат секретный ключ. На каждом шаге содержимое ячеек пропускается через функцию, называемую функцией обратной связи.

Значение, вырабатываемое этой функцией, записывается в крайнюю левую ячейку регистра, при этом все биты сдвигаются на одну позицию вправо, а крайний правый бит покидает регистр, и именно он является выходным значением регистра на данном шаге. Вот первый шаг:



Обозначим $s^{(i)} = (s_i, s_{i+1}, \dots, s_{i+L-1})$, $i = 0, 1, \dots$ — текущее состояние регистра. Состояние $s^{(0)}$ — начальное.

Тогда выходной символ s_i есть функция от $s^{(i)}$.

Линейность функции обратной связи означает, что $s_i = \langle c, s^{(i)} \rangle$, где $c = (c_1, c_2, \dots, c_L)$ — заданная последовательность битов длины L, а скалярное произведение определяется формулой

$$\langle x, u \rangle = \bigoplus_i x_i\, u_i\,,$$

как это принято в пространстве двоичных векторов[1].

2. Принципы Шеннона

По К. Шеннону, шифрование должно использовать следующие принципы:

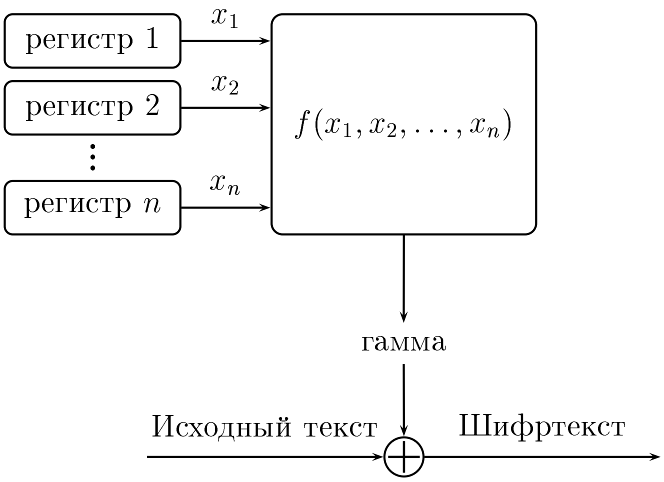
- Рассеивание (Diffusion) — распространение влияния одного знака открытого текста на много знаков шифртекста, а также распространение влияния одного элемента ключа на много знаков шифртекста.
- Перемешивание, усложнение, запутывание (Confusion) — свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифртекстом

Устройство LFSR реализует принцип рассеивания, но не запутывания. Текст, шифруемый посредством только одного LFSR, защищён плохо[2]. Общепринято для запутывания использовать несколько регистров LFSR. Пусть, например, длина секретного ключа равна L. Этот ключ можно разделить между несколькими регистрами длин L_i так, чтобы $L_1 + L_2 + \dots + L_n = L$, и комбинировать выходы всех n регистров посредством булевой функции f:

---

[1] На выбор вектора коэффициентов $c = (c_1, c_2, \dots, c_L)$ накладывается ограничение, а именно: двоичный многочлен $1 + c_1\, x + c_2\, x_2 + \dots + c_L\, x_L$ (он называется ассоциированным многочленом) должен быть примитивным. Если ассоциированный многочлен примитивен, то при любом начальном состоянии регистра выходная последовательность будет иметь максимально возможный период $2L-1$. Это важно, так как чем больше период, тем больше скрыта детерминированность процесса, тем ближе последовательность к случайной.

[2] Существует алгоритм Берлекэмпа-Мэсси (Berlekamp-Massey), который на основании перехваченной шифровки восстановит и длину регистра L, и коэффициенты ассоциированного многочлена, если только длина перехваченного текста не менее $2L$.



Такая картина уже соответствует реальному механизму шифрования.

Более полувека, минувшие с момента формулирования принципов Шеннона, подтвердили их значимость. За эти годы предпринимались различного вида атаки на криптосистемы, в связи с которыми появились основные криптографические характеристики булевых функций, некоторые из которых больше относятся к рассеиванию, другие больше к запутыванию. Все эти характеристики надо учитывать при конструировании булевых функций. Требуется компромисс между ними, ибо булева функция не может быть оптимальна сразу по всем криптографическим показателям, как это показывают, в частности, теоремы 1 и 2. Этим теоремам в первую очередь и посвящается предлагаемый доклад.

3. Алгебраическая нормальная форма булевых функций

Условимся относительно обозначений.

F_2 — конечное поле из двух элементов, 0 и 1. Операции в F_2 — умножение и сложение по модулю 2.

V_n — n-мерное векторное пространство над полем F_2, $V_n = (F_2)^n$. Сложение в пространстве V_n побитовое по модулю 2. Через $\mathbb{O}$ обозначен нулевой вектор пространства V_n.

Единичные векторы $e^{(i)}$ с единицей в i-й позиции и нулями в остальных образуют базис пространства V_n.

Булева функция от n переменных есть отображение из V_n в F_2. Мы будем ниже иметь дело также с *расширенными булевыми функциями* — отображениями из V_n в $\mathbb{Z}$ (множество целых чисел). Рассматривают и ещё более общие *псевдо-булевы функции* — отображения из V_n в $\mathbb{R}$ (множество действительных чисел).

Множество всех булевых функций от n переменных обозначим $\mathcal{F}_n$.

Число векторов пространства V_n равно 2^n как число всевозможных комбинаций n базисных векторов с коэффициентами 0 и 1. По той же причине число элементов любого линейного подпространства $E \subset V_n$ при $\dim E = m$ равно 2^m.

Булева или расширенная булева функция $f(x)$ задана, если имеется список её значений при всех $x \in V_n$. Например, при $n = 3$, $x = (x_1, x_2, x_3)$, одну из булевых функций можно задать таблицей:

№	x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0	1
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	0
6	1	1	0	1
7	1	1	1	1

В строках этой таблицы (называемой таблицей истинности) векторы пространства V_n записаны в лексикографическом порядке по возрастанию. Векторам соответствуют двоичные числа от 0 до $2n-1$, также упорядоченные по возрастанию. Такое упорядочение называется естественным.

При соблюдении естественного упорядочения для задания булевой функции достаточно задать набор её значений f_i, $i \in 0 : n-1$, так что $f = 10010011$.

Каждая функция из $\mathcal{F}_n$ имеет единственное представление в виде *алгебраической нормальной формы* или АНФ (в отечественной литературе распространён также термин «полином Жегалкина»). АНФ есть выражение булевой функции в виде

$$f(x) = \bigoplus_{N \in P\{1,2,\ldots,n\}} a_N \prod_{i \in N} x_i \,,$$

где $P\{1, 2, \ldots, n\}$ — множество всех подмножеств $\{1, 2, \ldots, n\}$ (булеан), $a_N \in F_2$.

Так, функция с приведённой выше таблицей истинности имеет представление $f(x) = 1 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3$. Для вычисления АНФ заданной функции имеются несложные алгоритмы (см., например, [1, 2]), на которых мы не будем здесь останавливаться.

Степень монома (булева одночлена) $x^N = \prod_{i \in N} x_i$ определяется как $|N|$ (число элементов подмножества N).

Алгебраическая степень булевой функции f есть степень АНФ этой функции (как многочлена от нескольких переменных).

Булева функция степени 1 называется *аффинной*. Её АНФ имеет вид

$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n \oplus b = \langle a, x \rangle \oplus b\,,$$

где $b \in F_2$, $a \in V_n$.

Мы видели, что для криптографических целей булева функция не должна быть линейной (точнее, аффинной). Вообще чем меньше функция «похожа на аффинную», тем лучше. В это неформальное пожелание можно вложить различные смысловые оттенки. Вот некоторые из них:

1) «Функция с хорошей нелинейностью» далека от множества аффинных функций в смысле какой-либо метрики.

2) «Функция с хорошей нелинейностью» должна выражаться полиномом как можно более высокой степени.

3) «Функция с хорошей нелинейностью» не должна линейно зависеть ни от одной из своих переменных и не должна приобретать такую зависимость после какой-либо линейной замены переменной. Это свойство формулируют так: функция не должна иметь ненулевых линейных структур.

Собственно термин «нелинейность» принят для показателя нелинейности, использующего понятия веса Хэмминга и расстояния Хэмминга.

Весом Хэмминга или просто *весом* двоичного вектора называется число единиц среди его компонент. *Вес Хэмминга булевой функции* есть вес вектора её значений. Обозначать вес вектора или функции будем $\mathrm{wt}(x)$ и $\mathrm{wt}(f)$.

Расстояние Хэмминга между двумя функциями f и g есть вес функции $f \oplus g$. Другими словами, это число тех $x \in V_n$, на которых $f(x) \neq g(x)$.

Нелинейностью $N(f)$ булевой функции f называется расстояние Хэмминга между f и множеством аффинных функций $\mathcal{A}_n$.

4. Преобразования Уолша-Адамара

Знаковые функции и функции Уолша

Для количественной оценки нелинейности и других криптографических показателей вычисляют ряд характеристик булевых функций. В первую очередь это спектры Уолша-Адамара.

Определим для булевой или расширенной булевой функции f её *знаковую функцию* или *экспоненту*

$$\exp f(x) = (-1)^{f(x)}.$$

Знаковая функция является расширенной булевой функцией на V_n.

Очевидное преобразование, переводящее 0 в 1 и 1 в -1, задаёт взаимно однозначное соответствие $\exp f(x) = 1-2f(x)$. Таблицу истинности для $\exp f(x)$ часто называют полярной или хара́ктерной таблицей истинности для f. Она полностью определяет функцию f.

Рассмотрим линейную булеву функцию $L_a(x) = \langle a, x\rangle$ на V_n. Можем записать её знаковую функцию

$$v(a,x) = \exp\big(L_a(x)\big) = (-1)^{\langle a,x\rangle}.$$

Функция $v(a,x)$ — это *дискретная функция Уолша*[3]. На a и x мы смотрим одновременно и как на двоичные векторы из V_n, и как на целые числа, двоичная запись которых, дополненная при необходимости слева нулями, совпадает с этими векторами.

Нам понадобится ряд утверждений, касающихся знаковых функций и, в частности, дискретных функций Уолша. Все их мы будем доказывать здесь, чтобы не отсылать читателя к дополнительным источникам. Сразу отметим очевидные свойства

$$\begin{aligned}
&v(a,x) = v(x,a) && \forall x \in V_n\,, \quad \forall a \in V_n\,,\\
&\big|v(a,x)\big| = 1 && \forall x \in V_n\,, \quad \forall a \in V_n\,,\\
&v(\mathbb{O},x) = v(x,\mathbb{O}) = 1 && \forall x \in V_n\,.
\end{aligned}$$

Пусть E — некоторое подпространство пространства V_n. Обозначим через $E^\perp$ множество $E^\perp = \{u \in V_n : \langle u,x\rangle = 0\,\forall x \in E\}$ (*ортогональное* или *сопряжённое* подпространство к пространству E). Легко убедиться, что множество $E^\perp$ является линейным пространством, причём $\dim E^\perp = n - \dim E$ [4].

УТВЕРЖДЕНИЕ 1. *Пусть $a \notin E^\perp$ (то есть на линейном подпространстве E линейная функция $\langle a,x\rangle$ принимает не только нулевые значения). Тогда $\sum_{x\in E} v(a,x) = 0$.*

---

[3] О функциях Уолша см., например, [3].

[4] Действительно, любой вектор $u \in E^\perp$ удовлетворяет системе однородных линейных уравнений $\langle u, b^{(i)}\rangle = 0$, где $\{b^{(i)}, i \in 1 : \dim E\}$ — базис подпространства E. Тогда базис пространства решений имеет размерность $n - \dim E$.

Доказательство. Разобьём пространство E на два подмножества:

$$E_0 = \{x \in E : \langle a, x\rangle = 0\}, \quad E_1 = \{x \in E : \langle a, x\rangle = 1\}.$$

По условию, множество E_1 не пусто. Возьмём какой-либо вектор $x^* \in E_1$. Складывая x^* с каждым элементом из E_1 (включая сам x^*), будем получать элементы множества E_0, так что $|E_0| \geqslant |E_1|$. Складывая x^* с каждым элементом из E_0, будем получать элементы множества E_1, так что $|E_1| \geqslant |E_0|$. Тогда $|E_0| = |E_1|$, так что среди слагаемых будет столько же значений 1, сколько и значений (-1). Сумма равна 0. □

Из утверждения 1 выведем две полезные формулы.
Так как $V_n^{\perp} = \{\mathbb{O}\}$, то

$$\sum_{x \in V_n} v(a, x) = \delta_0(a)\, 2^n, \tag{1}$$

где обозначено $\delta_0(a) = \begin{cases} 1 & \text{при } a = \mathbb{O}, \\ 0 & \text{при } a \neq \mathbb{O}. \end{cases}$

Так как при $a \in E^{\perp}$ выполняется $\sum_{x \in E} v(a, x) = \sum_{x \in E} (-1)^0 = |E|$, то

$$\sum_{x \in E} v(a, x) = |E|\, I_{E^{\perp}}(a), \tag{2}$$

где $I_{E^{\perp}}$ — индикатор (характеристическое множество) пространства $E^{\perp}$.

F- и *W*-преобразования

Преобразованием Уолша-Адамара 1-го рода (или F-преобразованием) булевой или расширенной булевой функции f назовём расширенную булеву функцию на V_n, задаваемую формулой

$$F_f(u) = \sum_{x \in V_n} f(x)\, v(x, u), \quad u \in V_n\,.$$

Знак $\sum$ соответствует обычному целочисленному суммированию.

> Сокращённое наименование «F-преобразование» принято здесь в связи с тем, что в литературе по булевым функциям в криптографии его чаще всего называют преобразованием Фурье. (См., например, [2], [4]). Наименованию, связанному с именами Уолша и Адамара, отдано предпочтение в книге [5].

УТВЕРЖДЕНИЕ 2. *Для любой расширенной булевой функции f на V_n и любого $a \in V_n$ выполняется равенство $F_{f(x \oplus a)}(u) = v(a, u)\, F_{f(x)}(u)$.*

Доказательство. По определению, $F_{f(x\oplus a)}(u) = \sum_{x\in V_n} f(x\oplus a)\, v(x,u)$. Прибегнем к замене переменной $x := x \oplus a$. Если x пробегает всё пространство V_n, то и $x \oplus a$ тоже пробегает всё пространство V_n. Поэтому

$$F_{f(x\oplus a)}(u) = \sum_{x\in V_n} f(x)\, v(x\oplus a, u) = \sum_{x\in V_n} f(x)\, v(x,u)\, v(a,u) =$$
$$= v(a,u) \sum_{x\in V_n} f(x)\, v(x,u) = v(a,u)\, F_{f(x)}(u).$$

Получена требуемая формула. □

УТВЕРЖДЕНИЕ 3. *Для любой расширенной булевой функции f на V_n выполняется $F_{F_f} = 2^n f$.*

Доказательство. Нам требуется показать, что для любого $a \in V_n$ имеет место равенство $\sum_{u\in V_n} F_f(u) v(a,u) = 2^n f(a)$. Согласно утверждению 2,

$$\sum_{u\in V_n} F_f(u)\, v(a,u) = \sum_{u\in V_n} F_{f(x\oplus a)}(u).$$

Для любой функции $g(x)$ имеем

$$\sum_{u\in V_n} F_g(u) = \sum_{u\in V_n} \sum_{x\in V_n} g(x)\, v(x,u)(u) = \sum_{x\in V_n} g(x) \sum_{u\in V_n} v(x,u) \overset{(1)}{=}$$
$$= \sum_{x\in V_n} g(x)\, \delta_0(x)\, 2^n = 2^n g(\mathbb{O}).$$

Применяя этот результат к функции $g(x) = f(x \oplus a)$, получаем

$$\sum_{u\in V_n} F_{f(x\oplus a)}(u) = 2^n f(a),$$

что и требовалось. □

Из утверждения 3 следует *формула обращения* преобразования Уолша-Адамара 1-го рода:

$$f(x) = 2^{-n} \sum_{u\in V_n} F_f(u)\, v(u,x).$$

Преобразованием Уолша-Адамара 2-го рода (или W-преобразованием) булевой или расширенной булевой функции f назовём F-преобразование её знаковой функции $W_f(u) = F_f\big(\exp f(u)\big)$, то есть расширенную булеву функцию на V_n, задаваемую формулой

$$W_f(u) = \sum_{x\in V_n} \exp\big(\langle x,u\rangle \oplus f(x)\big), \quad u \in V_n\,.$$

Соответствующая формула обращения имеет вид

$$\exp f(x) = 2^{-n} \sum_{u \in V_n} W_f(u)\, v(u, x).$$

Набор коэффициентов $\{F_f(u)\}$ или $\{W_f(u)\}$ некоторой булевой или расширенной булевой функции при всех $u \in V_n$ называется её *спектром Уолша-Адамара* 1-го или 2-го рода соответственно.

Связь между коэффициентами Уолша-Адамара 1-го и 2-го рода даётся формулой

$$W_f(u) = \delta_0(u)\, 2^n - 2F_f(u). \tag{3}$$

Убедимся, что эта формула верна. По определению,

$$W_f(u) = \sum_{x \in V_n} \exp\big(\langle x, u\rangle \oplus f(x)\big).$$

Разобьём эту сумму на две:

$$W_f(u) = \sum_{x \in \operatorname{supp} f} \exp\big(\langle x, u\rangle \oplus f(x)\big) + \sum_{x \in V_n \setminus \operatorname{supp} f} \exp\big(\langle x, u\rangle \oplus f(x)\big) =$$

$$= -\sum_{x \in \operatorname{supp} f} \exp\langle x, u\rangle + \sum_{x \in V_n \setminus \operatorname{supp} f} \exp\langle x, u\rangle = -\sum_{x \in \operatorname{supp} f} v(u, x) + \sum_{x \in V_n \setminus \operatorname{supp} f} v(u, x).$$

Из (1) следует, что

$$\sum_{x \in V_n \setminus \operatorname{supp} f} v(u, x) = \delta_0(u)\, 2^n - \sum_{x \in \operatorname{supp} f} v(u, x).$$

В то же время

$$F_f(u) = \sum_{x \in V_n} f(x)\, v(u, x) = \sum_{x \in \operatorname{supp} f} v(u, x).$$

Формула (3) доказана.

Оценка нелинейности. Бент-функции

Значение нелинейности функции $f \in \mathcal{F}_n$ вычисляется по формуле

$$N(f) = 2^{n-1} - \tfrac{1}{2} \max_{a \in V_n} |W_f(a)|\,. \tag{4}$$

Докажем формулу (4). Вес Хэмминга функции f есть

$$\operatorname{wt}(f) = \sum_{x \in V_n} f(x) = \sum_{x \in V_n} \frac{1 - \exp f(x)}{2}\,.$$

Так как $\sum_{x\in V_n} \exp f(x) = W_f(\mathbb{O})$, то получаем $\mathrm{wt}(f) = 2^{n-1} - \frac{W_f(\mathbb{O})}{2}$. Тогда

$$\mathrm{wt}\,\big(f(x)\oplus\langle a,x\rangle\big) = 2^{n-1} - \frac{W_{f(x)\oplus\langle a,x\rangle}(\mathbb{O})}{2} = 2^{n-1} - \frac{W_f(a)}{2}\,.$$

Аффинная функция задаётся либо формулой $g(x) = \langle a,x\rangle$, либо формулой $g(x) = \langle a,x\rangle \oplus 1$. В первом случае расстояние между функциями f и g есть

$$\mathrm{dist}(f,g) = \mathrm{wt}\,\big(f\oplus\langle a,x\rangle\big) = 2^{n-1} - \frac{W_f(a)}{2}\,,$$

во втором

$$\mathrm{dist}(f,g) = \mathrm{wt}\,\big(f\oplus\langle a,x\rangle\oplus 1\big) = 2^{n} - \mathrm{wt}\,\big(f\oplus\langle a,x\rangle\big) = 2^{n-1} + \frac{W_f(a)}{2}\,.$$

Таким образом, минимальное расстояние от f до множества аффинных функций — это величина

$$2^{n-1} - \tfrac{1}{2}\max_{a\in V_n}|W_f(a)|\,,$$

то есть выполняется (4).

Пример. По полученной формуле подсчитаем нелинейность функции 3-х переменных $f = 10010011$. Она равна 2 и является максимально возможной для функции из $\mathcal{F}_3$, как будет видно ниже из неравенства, дающего границу нелинейности.

Найдём сумму квадратов коэффициентов Уолша-Адамара 1-го рода:

$$\begin{aligned}\sum_{u\in V_n} F_f^2(u) &= \sum_{u\in V_n}\sum_{x\in V_n} f(x)\,v(x,u)\sum_{y\in V_n} f(y)\,v(y,u) =\\ &= \sum_{u\in V_n}\sum_{x,y\in V_n} f(x)\,f(y)\,v(x,u)\,v(y,u) =\\ &= \sum_{u\in V_n}\sum_{x,y\in V_n} f(x)\,f(y)\,v(x\oplus y,u) \overset{(1)}{=}\\ &= \sum_{u\in V_n}\sum_{x,y\in V_n} f(x)\,f(y)\cdot 2^n\delta_0(x\oplus y) = 2^n\sum_{x\in V_n} f^2(x).\end{aligned}$$

Мы доказали *равенство Парсеваля*

$$\sum_{u\in V_n} F_f^2(u) = 2^n\sum_{x\in V_n} f^2(x).$$

Из этого соотношения находим

$$\sum_{u\in V_n} W_f^2(u) = 2^n\sum_{x\in V_n}\big(\exp f(x)\big)^2 = 2^n\cdot 2^n = 2^{2n}.$$

Полученное равенство

$$\sum_{u\in V_n} W_f^2(u) = 2^{2n} \tag{5}$$

тоже называется *равенством Парсеваля.*

В силу равенства (5) получаем $\max_{u\in V_n} W_f^2(u) \geqslant 2^n$, следовательно,

$$\max_{u\in V_n} |W_f(u)| \geqslant 2^{\frac{n}{2}}.$$

Отсюда и из (4) сразу вытекает неравенство

$$N(f) \leqslant 2^{n-1} - 2^{\frac{n}{2}-1},$$

так что $2^{n-1} - 2^{\frac{n}{2}-1}$ есть верхняя граница нелинейности.

Функция $f \in \mathcal{F}_n$ называется *бент-функцией*, если при любом $u \in V_n$ выполнено $|W_f(u)| = 2^{\frac{n}{2}}$ (при нечётных n понятие не определяется). Как мы видим, бент-функции при чётном n являются максимально нелинейными.

Спектры аффинно эквивалентных функций

Рассмотрим, как изменится спектр Уолша-Адамара при (невырожденном) аффинном преобразовании входных координат.

Функции g и h из $\mathcal{F}_n$ называются *аффинно эквивалентными*, если существуют невырожденное линейное преобразование L на V_n и вектор $a \in V_n$ такие, что $h(x) = g(L\,x \oplus a)$.

Преобразование $L\,x$ равносильно умножению на неособенную матрицу L порядка $n \times n$ над полем F_2.

В этом определении, очевидно, g и h можно поменять местами.

Пусть функции g и h аффинно эквивалентны. Найдём

$$W_h(u) = \sum_{x\in V_n} \exp\,\langle x, u\rangle \oplus h(x) = \sum_{x\in V_n} \exp\,\langle x, u\rangle \oplus g(L\,x \oplus a) =$$

(замена $y = L\,x \oplus a$, то есть $x = L^{-1}a \oplus L^{-1}y$)

$$= \sum_{y\in V_n} \exp\big(\langle L^{-1}a \oplus L^{-1}y, u\rangle \oplus g(y)\big) =$$

$$= \exp\langle L^{-1}a, u\rangle \sum_{y\in V_n} \exp\big(\langle L^{-1}y, u\rangle \oplus g(y)\big) =$$

(обозначение $L' = (L^{-1})^T$)

$$= \exp\langle a, L'u\rangle \sum_{y\in V_n} \exp\big(\langle y, L'u\rangle \oplus g(y)\big) = v(a, L'u)\,W_g(L'u).$$

Если $a = \mathbb{O}$, то есть преобразование чисто линейное, то $v(a,x) = 1$ для всех x. Это означает, что **спектр функции h есть просто перемешанный спектр функции g**. При $a \neq \mathbb{O}$ часть коэффициентов может ещё поменять знак. Для спектра 1-го рода дело обстоит точно так же, доказательство полностью аналогично приведённому.

В частности, отсюда следует, что бентность является аффинным инвариантом. Но и при таком достоинстве бент-функций их прямое использование в криптосистемах не практикуется, поскольку они не являются уравновешенными.

> Функция f из $\mathcal{F}_n$ называется уравновешенной или сбалансированной (balanced), если её вес Хэмминга равен $2n - 1$, то есть она принимает значения 0 и 1 одинаковое число раз.
>
> На функции, используемые в криптографии, накладывается требование уравновешенности, чтобы избежать статистических зависимостей между входом и выходом. Эти зависимости могут использоваться в атаках на шифр.
>
> Уравновешенность функции, как легко видеть, характеризуется условием $W_f(0) = 0$. Для бент-функций это условие не выполняется.

5. Производные булевых функций по направлению. Подпространство линейных структур

Производной по направлению $u \in V_n$ функции $f \in \mathcal{F}_n$ называется булева функция $D_u f(x) = f(x) \oplus f(x \oplus u)$.

Свойства производных

1°. Для любых $u, v, x \in V_n$ верно равенство $D_{u\oplus v} f(x) = D_u f(x) \oplus D_v f(x \oplus u)$.

Для доказательства достаточно воспользоваться определением:

$$D_{u\oplus v} f(x) = f(x) \oplus f(x \oplus u \oplus v) = \big[f(x) \oplus f(x \oplus u)\big] \oplus \\ \oplus \big[f(x \oplus u) \oplus f(x \oplus u \oplus v)\big] = D_u f(x) \oplus D_v f(x \oplus u).$$

2°. Производная функции $f \in \mathcal{F}_n$ по направлению i-го базисного вектора $e^{(i)}$ является константой в том и только в том случае, когда эта функция может быть представлена в виде

$$f(x_1, x_2, \ldots, x_n) = \varepsilon\, x_1 \oplus g(x_2, \ldots, x_n), \qquad (*)$$

где $\varepsilon \in F_2$ — эта константа.

Доказательство. Не ограничивая общности можно провести рассуждения для $e^{(1)}$.

Пусть $D_{e^{(1)}}f(x) = \varepsilon$ при всех $x \in V_n$. Тогда по определению производной по направлению $(1, 0, \ldots, 0)$ выполняется равенство

$$f(x_1 \oplus 1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) \oplus \varepsilon.$$

В частности, при $x_1 = 0$ имеем

$$f(1, x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n) \oplus \varepsilon.$$

Подставляя это равенство в тождество[5)]

$$f(x_1, x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n) \oplus x_1 \big[f(0, x_2, \ldots, x_n) \oplus f(1, x_2, \ldots, x_n)\big],$$

получаем

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= f(0, x_2, \ldots, x_n) \oplus x_1 \big[f(0, x_2, \ldots, x_n) \oplus f(0, x_2, \ldots, x_n) \oplus \varepsilon\big] = \\ &= f(0, x_2, \ldots, x_n) \oplus x_1\, \varepsilon. \end{aligned}$$

Последнее равенство даёт представление $(*)$, если в качестве функции g взять

$$g(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n).$$

Обратное утверждение получается сразу из $(*)$ применением определения производной:

$$D_{e^{(1)}}f(x) = \varepsilon\, x_1 \oplus g(x_2, \ldots, x_n) \oplus \varepsilon\, (x_1 \oplus 1) \oplus g(x_2, \ldots, x_n) = \varepsilon.$$

Производная равна ε. □

3°. Производная функции $f \in \mathcal{F}_n$ постоянна по каждому направлению в том и только в том случае, когда эта функция аффинна.

Доказательство. Для аффинной функции то, что производная постоянна, проверяется сразу по определению. Проведём обратное рассуждение.

Производная функции f по базисному вектору $e^{(1)}$ постоянна, и по свойству 2°

$$f(x_1, x_2, \ldots, x_n) = \varepsilon_1\, x_1 \oplus g_1(x_2, \ldots, x_n).$$

Так как производная функции g_1 по $e^{(2)}$, как нетрудно убедиться, равна производной f по $e^{(2)}$ и тоже постоянна, получаем

$$g_1(x_2, \ldots, x_n) = \varepsilon_2\, x_2 \oplus g_2(x_3, \ldots, x_n),$$

[5)] Тождество легко проверяется, оно верно и при $x_1 = 0$, и при $x_1 = 1$.

и так далее. На последнем шаге придём к равенству

$$g_{n-2}(x_{n-1}, x_n) = \varepsilon_{n-1}\, x_{n-1} \oplus g_{n-1}(x_n).$$

Функции одной координаты все аффинны, так что

$$g_{n-1}(x_n) = \varepsilon_n\, x_n \oplus b, \quad b \in F_2.$$

Функция f получила аффинное представление. □

Вектор $u \in V_n$, по направлению которого производная $D_u f$ постоянна, называют *линейной структурой* функции f.

УТВЕРЖДЕНИЕ 4. *Функция $f \in \mathcal{F}_n$ имеет какую-либо ненулевую линейную структуру тогда и только тогда, когда эта функция аффинно эквивалентна функции, для которой вектор $e^{(1)}$ является линейной структурой.*

Доказательство. Пусть u — ненулевая линейная структура функции f. Рассмотрим функцию $h(x) = f(L\,x)$, где преобразование L обладает свойством $L\,e^{(1)} = u$ [6].

Функции f и h аффинно эквивалентны. Найдём производную

$$\begin{aligned} D_{e^{(1)}} h(x) &= h(x) \oplus h(x \oplus e^{(1)}) = f(L\,x) \oplus f\big(L(x \oplus e^{(1)})\big) = \\ &= f(L\,x) \oplus f(L\,x \oplus u) = D_u f(x). \end{aligned}$$

Так как $D_u f(x)$ — константа, то и $D_{e^{(1)}} h(x)$ — константа.

Докажем обратное. Пусть $f(x) = h(L\,x \oplus a)$, причём $D_{e^{(1)}} h(x) = \text{const}$. Возьмём $u = L^{-1} e^{(1)}$, так что $L\,u = e^{(1)}$. Тогда

$$\begin{aligned} D_u f(x) &= f(x) \oplus f(x \oplus u) = h(L\,x \oplus a) \oplus h\big(L(x \oplus u) \oplus a\big) = \\ &= h(L\,x \oplus a) \oplus h(L\,x \oplus Lu \oplus a) = h(L\,x \oplus a) \oplus h(L\,x \oplus e^{(1)} \oplus a) = \\ &= D_{e^{(1)}} h(L\,x \oplus a) = \text{const}\,. \end{aligned}$$

Значит, u — линейная структура функции f. Очевидно, $u \neq \mathbb{O}$. □

Нетрудно видеть, что множество всех линейных структур функции f является линейным подпространством пространства V_n. Чтобы проверить это, достаточно убедиться, что нулевой вектор $\mathbb{O}$ является линейной структурой[7] и что $D_{u \oplus v} f = \text{const}$ при $D_u f = \text{const}$ и $D_v f = \text{const}$. Последнее следует из свойства 1° производных.

[6] Матрица такого преобразования имеет первый столбец, совпадающий с u, а остальные столбцы подбираются из V_n так, чтобы обеспечить невырожденность. При $u_1 = 1$ это могут быть столбцы единичной матрицы, то есть векторы $e^{(i)}$, $i = 2, 3, \ldots, n$. При $u_1 = 0$ это могут быть $e^{(i)}$, $i \in 1 : n$, $i \neq k$, где индекс k выбран так, чтобы $u_k = 1$.

[7] Это тривиально, $D_{\mathbb{O}} f(x) = f(x) \oplus f(x \oplus \mathbb{O}) = 0$.

6. Автокорреляция и теорема Винера-Хинчина

Автокорреляционной функцией или, кратко, *автокорреляцией* функции $f \in \mathcal{F}_n$ называется расширенная булева функция $\Delta_f(u)$, имеющая вид

$$\Delta_f(u) = \sum_{x\in V_n} \exp\big(f(x) \oplus f(x \oplus u)\big) = W_{D_u f}(\mathbb{O}).$$

УТВЕРЖДЕНИЕ 5. *Для любой функции $f \in \mathcal{F}_n$ выполняется*

$$\sum_{u\in V_n} \Delta_f(u) = W_f^2(\mathbb{O}).$$

Доказательство. Имеем:

$$\sum_{u\in V_n} \Delta_f(u) = \sum_{u\in V_n}\sum_{x\in V_n} \exp\big(f(x) \oplus f(x\oplus u)\big) = \sum_{x\in V_n}\sum_{u\in V_n} \exp\big(f(x) \oplus f(x\oplus u)\big) =$$

$$\text{(замена } u := x \oplus u\text{)}$$

$$= \sum_{x\in V_n} \exp f(x) \sum_{u\in V_n} \exp f(u) = W_f(\mathbb{O}) \cdot W_f(\mathbb{O}).$$ □

Свёртку расширенных булевых функций f и g введём как функцию $c = f * g$, вычисляемую по формуле[8)]

$$c(x) = \sum_{y\in V_n} f(x\oplus y)\, g(y) = \qquad \text{(замена переменной } y := x \oplus y\text{)}$$

$$= \sum_{y\in V_n} f(y)\, g(x \oplus y).$$

УТВЕРЖДЕНИЕ 6. *Для расширенных булевых функций f и g выполнено равенство $F_{f*g} = F_f \cdot F_g$, где под умножением функций в правой части равенства понимается покомпонентное умножение.*

Доказательство. Для любого $u \in V_n$ имеем

$$F_{f*g}(u) = \sum_{x\in V_n} (f*g)(x)\, v(x,u) = \sum_{x\in V_n}\sum_{y\in V_n} f(y)\, g(x\oplus y)\, v(x,u) =$$

$$= \sum_{x\in V_n}\sum_{y\in V_n} f(y)\, g(x\oplus y)\, v(x\oplus y, u)\, v(y,u) =$$

---

8) Иногда, как в [3], для чисто булевых функций f и g свёртка определяется чуть иначе: внешняя сумма есть $\bigoplus_{y\in V_n}$. Но при таком определении не выполнена, например, приводимая далее важная теорема Винера-Хинчина.

$$
\begin{aligned}
&= \sum_{y\in V_n}\sum_{x\in V_n} f(y)\, g(x\oplus y)\, v(x\oplus y, u)\, v(y,u) = \\
&= \sum_{y\in V_n} f(y)\, v(y,u) \sum_{x\in V_n} g(x\oplus y)\, v(x\oplus y, u) = \\
&\quad \text{(замена переменной } x := x\oplus y\text{)} \\
&= F_f(u)\cdot F_g(u).
\end{aligned}
$$

Утверждение доказано. □

Следующее утверждение мы приведём в двух равносильных формулировках.

УТВЕРЖДЕНИЕ 7 (Теорема Винера-Хинчина). *Для любой функции* $f \in \in \mathcal{F}_n$ *при всех* $u \in V_n$ *справедливо равенство*

$$F_{\exp f \,*\, \exp f}(u) = W_f^2(u),$$

записываемое также в виде

$$F_{\Delta_f}(u) = W_f^2(u).$$

Доказательство. Первое равенство есть результат применения утверждения 6 к паре одинаковых функций, а именно функций $\exp f$. Второе получается из первого. Действительно,

$$
\begin{aligned}
\big(\exp f * \exp f\big)(u) &= \sum_{x\in V_n} \exp f(x) \exp f(u\oplus x) = \\
&= \sum_{x\in V_n} \exp\big(f(x)\oplus f(u\oplus x)\big) = \Delta_f(u).
\end{aligned}
$$

□

7. Две числовые характеристики и их совместное ограничение

Нас будет интересовать число ненулевых значений расширенных булевых функций $\Delta_f(u)$ и $W_f(u)$. Обозначим

$$N_\Delta = \left|u\in V_n : \Delta_f(u)\neq 0\right|,$$

$$N_W = \left|u\in V_n : W_f(u)\neq 0\right|.$$

Каждая из этих величин определяется булевой функцией f, и с каждой из них связаны свои криптографические показатели, причём одни показатели будут наилучшими при как можно меньшем значении N_Δ, другие — при как можно меньшем значении N_W. Ниже будут сформулированы и доказаны две фундаментальные теоремы, касающиеся этих величин.

ТЕОРЕМА 1. *Для любой функции $f \in \mathcal{F}_n$ выполнено неравенство*

$$N_\Delta \cdot N_W \geqslant 2^n. \tag{6}$$

Д о к а з а т е л ь с т в о. Равенство Парсеваля можно записать в виде

$$\sum_{u \in V_n,\, W_f(u) \neq 0} W_f^2(u) = 2^{2n}.$$

В этой сумме число слагаемых равно N_W, так что получаем, обозначив $u_0 = \arg\max W_f^2(u)$, следующую цепочку неравенств:

$$\begin{aligned} \frac{2^{2n}}{N_W} &\leqslant W_f^2(u_0) = \qquad \text{(по утверждению 7)} \\ &= \sum_{u \in V_n} \Delta_f(u) v(u, u_0) \leqslant \sum_{u \in V_n} |\Delta_f(u)| = \sum_{u \in V_n,\, \Delta_f(u) \neq 0} |\Delta_f(u)| \leqslant N_\Delta \cdot 2^n. \end{aligned}$$

Последнее неравенство имеет место потому, что величина $\big|\Delta_f(u)\big|$, являясь суммой единиц с различными знаками в количестве 2^n, при любом u не превосходит 2^n.

Итоговое неравенство равносильно доказываемому. $\square$

Далее нам понадобятся обобщения утверждений 6 и 7 на линейное подпространство E пространства V_n. Введём обозначения для функций на E:

$\big(f \overset{E}{*} g\big)(x) = \sum\limits_{y \in E} f(x \oplus y)\, g(y)$, $x \in E$ — свёртка на подпространстве,

$\Delta_f^E(u) = \sum\limits_{x \in E} \exp\big(f(x) \oplus f(x \oplus u)\big)$, $u \in E$ — автокорреляция на подпространстве,

$F_f^E(u) = \sum\limits_{x \in E} f(x)\, v(x, u)$, $u \in E$ — F-преобразование на подпространстве,

$W_f^E(u) = \sum\limits_{x \in E} f(x)\, v(x, u)$, $u \in E$ — W-преобразование на подпространстве.

УТВЕРЖДЕНИЕ 8. *Для любого $u \in V_n$ выполнено*

$$F^E_{f \overset{E}{*} g}(u) = F_f^E \cdot F_g^E.$$

Д о к а з а т е л ь с т в о полностью повторяет доказательство утверждения 6 с заменой при суммировании пространства V_n на подпространство E.

УТВЕРЖДЕНИЕ 9 (Теорема Винера-Хинчина для подпространства). *Для любого $u \in V_n$ выполнено*

$$F^E_{\Delta^E_f}(u) = \big(W^E_f(u)\big)^2.$$

Доказательство. Имеем

$$\Delta^E_f(x) = \sum_{x\in E} \exp\big(f(x) \oplus f(x\oplus u)\big) = \sum_{x\in E} \exp f(x) \cdot \exp f(x\oplus u) = \exp f \overset{E}{*} \exp f.$$

Применяется утверждение 8, роль g и f играет знаковая функция $\exp f$. $\square$

Функция f называется *бент-функцией на подпространстве* E, если для всех $u \in E$ выполнено равенство

$$\big|W^E_f(u)\big| = 2^{\frac{\dim E}{2}}.$$

УТВЕРЖДЕНИЕ 10. *Функция f является бент-функцией на подпространстве E тогда и только тогда, когда для любого ненулевого $z \in E$ выполняется равенство $\Delta^E_f(z) = 0$.*

Доказательство. Заметим,что

$$\Delta^E_f(\mathbb{O}) = \sum_{x\in E} \exp\big(f(x) \oplus f(x)\big) = |E| = 2^{\dim E}.$$

Поэтому $\Delta^E_f(z) = \delta_0(z)\, 2^{\dim E}$.

Пусть $\Delta^E_f(z) = 0$ при всех $z \in E$, $z \neq \mathbb{O}$. Используя утверждение 9, находим

$$\big(W^E_f(u)\big)^2 = F^E_{\Delta^E_f}(u) = \sum_{z\in E} \Delta^E_f(z)\, v(z,u) = \sum_{z\in E} \delta_0(z)\, 2^{\dim E}\, v(z,u).$$

По смыслу $\delta_0(z)$, в этой сумме только одно ненулевое слагаемое, соответствующее $z = \mathbb{O}$. Поэтому $\big(W^E_f(u)\big)^2 = 2^{\dim E}$, так что f — бент-функция на E. Обратно, пусть $\big(W^E_f(u)\big)^2 = 2^{\dim E}$, то есть, по утверждению 9, $\sum_{z\in E} \Delta^E_f(z)\, v(z,u) = 2^{\dim E}$. В то же время при $z = \mathbb{O}$ имеем

$$\Delta^E_f(\mathbb{O})\, v(\mathbb{O},u) = \Delta^E_f(\mathbb{O}) = 2^{\dim E}.$$

Тогда остальные слагаемые этой суммы равны 0. $\square$

Характеризация частично-бент функций

Частично бент-функцией (partially-bent function) называется булева функция, для которой в неравенстве (6) достигается равенство:

$$N_\Delta \cdot N_W = 2^n. \tag{7}$$

ЛЕММА. *Равенство $\Delta_f(u) = 2^n \exp \varepsilon$ справедливо тогда и только тогда, когда при всех $x \in V_n$ выполнено $D_u f(x) = \varepsilon$.*

Доказательство. Пусть $D_u f(x) = \varepsilon$ при всех x. По определению,

$$\Delta_f(u) = \sum_{x \in V_n} \exp D_u f(x).$$

Значит, $\Delta_f(u) = \sum_{x \in V_n} \exp \varepsilon = 2^n \exp \varepsilon$.

Обратно, пусть $\Delta_f(u) = 2^n \exp \varepsilon$. Так как $\Delta_f(u)$ есть сумма 2^n чисел, равных по модулю единице, то это равенство выполняется лишь в случае, когда все слагаемые этой суммы равны $\exp \varepsilon$, то есть при $D_u f(x) = \varepsilon$. □

ТЕОРЕМА 2 (впервые доказана в [6]). *Равенство* (7) *равносильно каждому из двух эквивалентных условий:*

1) *При любом и либо $\Delta_f(u) = 0$, либо существует $t \in V_n$ такое, что $\Delta_f(u) = 2^n\, v(t, u)$.*

2) *Пространство V_n разлагается в прямую сумму двух подпространств E и E' (причём E' имеет чётную размерность) таких, что для всех $x \in E$, $y \in E'$ имеет место разложение*

$$f(x \oplus y) = g(x) \oplus h(y),$$

где функция $g(x)$ является линейной на E, а функция $h(y)$ является бент-функцией на E'.

Доказательство проведём по схеме (7) $\longrightarrow$ 1) $\longrightarrow$ 2) $\longrightarrow$ (7).

$\boxed{(7) \longrightarrow 1)}$

Возьмём $u_0 = \arg\max W_f^2(u)$. Рассмотрим функцию $\varphi(u) = f(u) \oplus \langle u_0, u\rangle$. Для неё

$$\text{(a)} \qquad W_\varphi(\mathbb{O}) = \sum_{x \in V_n} \exp\big(\langle x, \mathbb{O}\rangle \oplus \varphi(x)\big) = \\ = \sum_{x \in V_n} \exp \varphi(x) = \sum_{x \in V_n} \exp\big(f(x) \oplus \langle u_0, x\rangle\big) = W_f(u_0)$$

(по определению W-преобразования),

$$\text{(b)} \qquad \Delta_\varphi(u) = \sum_{x\in V_n} \exp\big(\varphi(x)\oplus\varphi(x\oplus u)\big) =$$
$$= \sum_{x\in V_n} \exp\big(f(x)\oplus\langle u_0,x\rangle\oplus f(x\oplus u)\oplus\langle u_0, x\oplus u\rangle\big) =$$
$$= \sum_{x\in V_n} \exp\big(f(x)\oplus\langle u_0,u\rangle\oplus f(x\oplus u)\big) =$$
$$= v(u_0,u)\sum_{x\in V_n} \exp\big(f(x)\oplus f(x\oplus u)\big) = v(u_0,u)\,\Delta_f(u).$$

Таким образом, значения $\Delta_\varphi(u)$ и $\Delta_f(u)$ на одном и том же u либо оба нулевые, либо оба ненулевые.

Вся цепочка неравенств из доказательства теоремы 1 в случае (7) перейдёт в цепочку равенств. В частности, $W_f^2(u_0) = N_\Delta\cdot 2^n$.

Согласно утверждению 5,

$$\sum_{u\in V_n}\Delta_\varphi(u) = W_f^2(\mathbb{O}) \overset{\text{(a)}}{=} W_f^2(u_0) = N_\Delta\cdot 2^n.$$

Тогда при каждом $u\in V_n$ либо $\Delta_\varphi(u)=0$, либо $\Delta_\varphi(u)=2^n$, откуда в силу (b) либо $\Delta_\varphi(u)=0$, либо $\Delta_f(u) = v(u_0,u)\cdot 2^n$.

$\boxed{1)\longrightarrow 2)}$

В качестве подпространства E возьмём $E = \big\{u\in V_n : \Delta_f(u) = v(t,u)\cdot 2^n\big\}$, то есть носитель функции $\Delta_f(u)$. По лемме, $u\in E$ означает, что u — линейная структура функции f.

Более того, E есть множество всех линейных структур функции f. Действительно, возьмём $z\notin E$. Тогда $\sum_{x\in V_n}\exp D_z f(x) = \Delta_f(z) = 0$. В этом случае половина производных $D_z f(x)$, $x\in V_n$, равна 0, а половина 1, так что z не является линейной структурой.

Итак, E — множество линейных структур, и оно, как мы уже видели, является линейным подпространством.

В качестве E' возьмём прямое дополнение подпространства E до V_n, $V_n = E + E'$. Для любого $z\in E'$ выполняется

$$\Delta_f(z) = \sum_{u\in V_n}\exp D_z f(u) = 0.$$

Представив $u = x\oplus y$, распишем эту сумму:

$$\Delta_f(z) = \sum_{x\in E}\sum_{y\in E'}\exp\big(f(x\oplus y)\oplus f(x\oplus y\oplus z)\big).$$

По лемме, условие $x \in E$ равносильно тому, что при всех $s \in V_n$ имеет место равенство $D_x f(s) = \langle t, x \rangle$. Это равенство разбивает при любом s функцию $f(x \oplus s)$ на 2 слагаемых: $f(x \oplus s) = f(s) \oplus \langle t, x \rangle$. В том числе:

$$\begin{array}{lll} \text{при } s = y & \text{имеем} & f(x \oplus y) = f(y) \oplus \langle t, x \rangle, \\ \text{при } s = y \oplus z & \text{имеем} & f(x \oplus y \oplus z) = f(y \oplus z) \oplus \langle t, x \rangle. \end{array} \qquad (*)$$

Складывая два эти равенства, получаем

$$f(x \oplus y) \oplus f(x \oplus y \oplus z) = f(y) \oplus f(y \oplus z).$$

Таким образом,

$$\Delta_f(z) = \sum_{x \in E} \sum_{y \in E'} \exp\big(f(y) \oplus f(y \oplus z)\big).$$

Во внешней сумме все слагаемые одинаковы, их число равно $2^{\dim E}$, поэтому

$$\Delta_f(z) = 2^{\dim E} \sum_{y \in E'} \exp\big(f(y) \oplus f(y \oplus z)\big) = \Delta_f^{E'}(z).$$

Так как $\Delta_f(z) = 0$, то и $\Delta_f^{E'}(z) = 0$ при $z \in E'$, $z \neq \mathbb{O}$.

Последнее равенство означает, по утверждению 10, бентность функции f на подпространстве E'. Значит, $h(y)$ есть просто сужение f на E' (функция, определённая на E', значения которой совпадают со значениями функции f на E').

Равенство $(*)$ даёт требуемое представление. Функция $g(x) = \langle t, x \rangle$ линейна.

$\boxed{2) \longrightarrow (7)}$

Пусть любое $u \in V_n$ представляется в виде $u = x \oplus y$, $x \in E$, $y \in E'$, при этом $f(x \oplus y) = \langle t, x \rangle \oplus h(y)$, $h(y)$ является бент-функцией на E'. Скалярное произведение изображает линейную функцию.

По определению,

$$\Delta_f(z) = \sum_{u \in V_n} \exp\big(f(x) \oplus f(u \oplus z)\big).$$

Представив $u = x \oplus y$, $x \in E$, $y \in E'$, $z = x_1 \oplus y_1$, $x_1 \in E$, $y_1 \in E'$, придём к равенству

$$\Delta_f(z) = \sum_{x \in E} \sum_{y \in E'} \exp\big(f(x \oplus y) \oplus f(x \oplus y \oplus x_1 \oplus y_1)\big).$$

Подставим $f(x \oplus y) = \langle x, t\rangle \oplus h(y)$. Получим

$$\begin{aligned}\Delta_f(z) &= \sum_{x\in E}\sum_{y\in E'} \exp\big(\langle x, t\rangle \oplus h(y) \oplus \langle x \oplus x_1, t\rangle \oplus h(y \oplus y_1)\big) = \\ &= \sum_{x\in E}\sum_{y\in E'} \exp\big(\langle x_1, t\rangle \oplus h(y) \oplus h(y \oplus y_1)\big) = \\ &= \exp\langle x_1, t\rangle \sum_{x\in E}\sum_{y\in E'} \exp\big(h(y) \oplus h(y \oplus y_1)\big) = v(x_1, t) \sum_{x\in E} \Delta_h^{E'}(y_1).\end{aligned}$$

Так как h — бент-функция на E', то по утверждению 10 при $y_1 \neq \mathbb{O}$ (то есть для $z \notin E$) будет выполнено $\Delta_h^{E'}(y_1) = 0$ и, следовательно, $\Delta_f(z) = 0$, а при $y_1 = \mathbb{O}$ (то есть для $z = x_1 \in E$), как нетрудно посчитать, $\Delta_f(z) = v(x_1, t) \cdot 2^n \neq 0$. Таким образом, $N_\Delta = |E| = 2^{\dim E}$.

Такое же исследование проведём для N_W.

По утверждению 7, $F_{\Delta_f}(u) = W_f^2(u)\ \forall\ u \in V_n$. Как было показано в конце раздела 4, аффинное преобразование координат не меняет набор значений W_f^2. Поэтому мы будем искать не $W_f^2(u)$, а $W_f^2(u \oplus t)$, что более удобно.

$$\begin{aligned}W_f^2(u \oplus t) &= \sum_{z\in V_n} \Delta_f(z)\, v(z, u \oplus t) = \sum_{z\in E} \Delta_f(z)\, v(z, u \oplus t) = \\ &= \sum_{z\in E} 2^n v(z, t)\, v(z, u \oplus t) = 2^n \sum_{z\in E} v(z, u) \overset{(2)}{=} \\ &= 2^n |E|\, I_{E^\perp}(u) = \begin{cases} 0, & \text{если } u \notin E^\perp, \\ 2^n|E|, & \text{если } u \in E^\perp. \end{cases}\end{aligned}$$

Отсюда сразу следует, что $N_W = |E^\perp|$. Так как $\dim E^\perp = n - \dim E$, то $N_W = 2^{n-\dim E}$. Перемножая, получаем то, что требовалось: $N_\Delta \cdot N_W = 2^n$.

Теорема 2 доказана. □

ЛИТЕРАТУРА

1. Марченков С. С. *Булевы функции.* М.: Физматлит, 2002.

2. Carlet C. *Boolean functions for cryptography and error correcting codes* // In: Crama Y., Hammer P. L. (Eds.), *Boolean Methods and Models*, Cambridge University Press, готовится к выходу. С текстом можно ознакомиться на `http://www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`

3. Залманзон Л. А. *Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях.* М.: Наука, 1989. 496 с.

4. Логачёв О. А., Сальников А. А., Ященко В. В. *Булевы функции в теории кодирования и криптологии.* М.: МЦНМО, 2004. 470 с.

5. Сачков В. Н. *Введение в комбинаторные методы дискретной математики.* (2-е изд.). М.: МЦНМО, 2004. 424 с.

6. Carlet C. *Partially-bent functions* // Designs, Codes and Cryptography. 1993. V. 3. No. 2. P. 135–145.