УДК 519.719.325

К ВОПРОСУ О ЛИНЕЙНОЙ ДЕКОМПОЗИЦИИ ДВОИЧНЫХ ФУНКЦИЙ

А. В. Черемушкин

Учебно-методическое объединение по образованию в области информационной безопасности, г. Москва, Россия

Изучены условия однозначности разложения булевой функции в простую бесповторную декомпозицию при линейной замене переменных. Вводится понятие подпространства существенных переменных. Найдены условия, при выполнении которых каждое из двух подпространств существенных переменных функций-компонент в простой декомпозиции функции с тривиальной группой инерции в группе сдвигов однозначно определяет другое. Рассмотрен также случай итеративной декомпозиции.

Ключевые слова: *булевы функции, сопряжённое пространство, простая декомпозиция, итеративная декомпозиция.*

DOI 10.17223/20710410/31/4

ON LINEAR DECOMPOSITION OF BOOLEAN FUNCTIONS

A. V. Cheremushkin

EMA IS, Moscow, Russia

E-mail: avc238@mail.ru

Disjunctive decompositions of Boolean functions taken after a linear substitution on the set of arguments are considered. For any component of such a decomposition, a notion of a substantial variables subspace is introduced. The main topic of the article is to give some sufficient condition under which the both these subspaces unequally determine each other in a simple disjunctive decomposition of a function having the trivial stabiliser group of shifts. The case of iterative disjunctive decomposition is considered too.

Keywords: *Boolean function, vector space, dual space, simple disjunctive decomposition, iterative disjunctive decomposition.*

Введение

В данной работе предлагается подход к изучению свойств разложения булевой функции в простую бесповторную декомпозицию при линейной замене переменных. При рассмотрении таких декомпозиций удобнее рассматривать функции-компоненты, участвующие в этой декомпозиции, не как функции, заданные на соответствующих подпространствах, а как функции, заданные также на всём пространстве, но определяемые своими подпространствами существенных переменных. Ранее автором были рассмотрены некоторые частные случаи бесповторных декомпозиций [1], включая выделение линейных сомножителей и некоторые виды сумм функций от независимых

переменных, а также полностью рассмотрен случай разложимости функции в произведение от независимых переменных [2]. Основной задачей данной работы является нахождение условий, при выполнении которых каждое из двух подпространств существенных переменных функций-компонент в простой декомпозиции функции с тривиальной группой инерции в группе сдвигов однозначно определяет другое. Рассматривается также случай итеративной декомпозиции, в котором можно явно установить связь между двумя различными простыми декомпозициями.

1. Основные определения

Введём обозначения, которые, несмотря на свою громоздкость, в дальнейшем помогут яснее понять особенности действия линейной группы на множестве функций.

Пусть V — векторное пространство размерности n, $n \geqslant 1$, над полем $\mathrm{GF}(2)$, т. е. $V = (\mathrm{GF}(2))^n$, и $\mathcal{F}_n$ есть множество всех функций $f : V \to \mathrm{GF}(2)$. Если зафиксировать некоторый базис $e = (e^1, e^2, \ldots, e^n)$ пространства V, то для произвольного вектора $x \in V$ двоичные коэффициенты $x_1, x_2, \ldots, x_n$ в его разложении $x = \sum\limits_{i=1}^{n} x_i e^i$ будем называть его *координатами в базисе* e, а их набор обозначать символом x_e, т. е. $x_e = (x_1, x_2, \ldots, x_n)$. Кроме того, любой функции $f \in \mathcal{F}_n$ будем ставить в соответствие функцию $f_e \in \mathcal{F}_n$, называемую *представлением* f *в базисе* e и определяемую как $f_e(x_e) = f(x)$ для всех $x \in V$.

Пусть далее V^* — векторное пространство, состоящее из всех линейных функций в $\mathcal{F}_n$. Если $x \in V$ и $a^* \in V^*$, то значение линейной функции a^* на векторе x удобно обозначать в виде (x, a^*). Базис $e = (e^1, e^2, \ldots, e^n)$ пространства V и базис $e^* = (e^{*1}, e^{*2}, \ldots, e^{*n})$ пространства V^* называются *сопряжёнными* (один другому), если для всех i, j, $1 \leqslant i, j \leqslant n$,

$$(e^i, e^{*j}) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Говорим, что функция $g \in \mathcal{F}_n$ получена из функции $f \in \mathcal{F}_n$ *линейной заменой переменных* вида $x \mapsto xA$, где A — некоторая квадратная матрица размера $n \times n$ над $\mathrm{GF}(2)$, если $g(x) = f(xA)$ для всех $x \in V$.

Сделаем несколько поясняющих замечаний.

Замечание 1. Для любых сопряжённых базисов e и $e^* = (e^{*1}, e^{*2}, \ldots, e^{*n})$ пространств V и V^* соответственно, для любого вектора $x \in V$ и любой его координаты x_i в базисе e справедливо $x_i = (x, e^{*i})$.

Замечание 2. При выборе другого базиса $e' = (e'^1, e'^2, \ldots, e'^n)$ пространства V получаем

$$f(x) = f_e(x_e) = f_{e'}(x_{e'}) = f_{e'}(x_e C),$$

где C — матрица перехода от базиса e' к базису e: $e = e'C$.

Замечание 3. Для любой функции $f \in \mathcal{F}_n$ и любого базиса e пространства V множество всех функций, полученных из функции f_e путем линейной замены переменных, совпадает с множеством функций $f_{e'}$ для всевозможных базисов e' пространства V.

Действительно, каждой линейной замене переменных функции f_e вида $x_e \mapsto x_e A$ соответствует представление $f_{e'}$ функции f в новом базисе e', матрица перехода от которого к базису e имеет вид $C = A^{-1}$:

$$f_e(x_e A) = f_{e'}(x_e).$$

Замечание 4. Если $C = (c_{ij})$ — матрица перехода в пространстве V от базиса $e' = (e'^1, e'^2, \ldots, e'^n)$ к базису $e = (e^1, e^2, \ldots, e^n)$ и $e^* = (e^{*1}, e^{*2}, \ldots, e^{*n})$ и $e'^* = (e'^{*1}, e'^{*2}, \ldots, e'^{*n})$ суть базисы пространства V^*, сопряжённые к e и e' соответственно, то имеют место соотношения

$$e^i = \sum_{j=1}^{n} c_{ij} e'^j, \qquad e'^{*i} = \sum_{j=1}^{n} c_{ji} e^{*j}, \qquad i = 1, \ldots, n,$$

и матрицей перехода от e'^* к e^* является $(A^{-1})^T$.

Доказательство вытекает из следующих цепочек равенств:

$$x = \sum_{i=1}^{n} x_i e^i = \sum_{j=1}^{n} x'_j e'^j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x_i c_{ij} \right) e'^j = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} c_{ij} e'^j,$$

$$x'_i = \sum_{j=1}^{n} x_j c_{ji} = \sum_{j=1}^{n} (x, e^{*j}) c_{ji} = \left(x, \sum_{j=1}^{n} c_{ji} e^{*j} \right) = (x, e'^{*i}),$$

где $x_{e'} = (x'_1, x'_2, \ldots, x'_n) = x_e C$.

Для каждого целого $t \geqslant 0$ определим подпространства $\mathcal{U}_t$ пространства функций $\mathcal{F}_n$:

$$\mathcal{U}_t = \{f \ : \deg f \leqslant t\}.$$

Заметим, что $\mathcal{U}_0 = \{0, 1\}$. При $t < 0$ положим $\mathcal{U}_t = \{0\}$ — *нулевое подпространство*. Для функций f и h в $\mathcal{F}_n$ будем говорить, что они сравнимы по модулю $\mathcal{U}_t$, и писать $f \equiv h \pmod{\mathcal{U}_t}$, если $f \oplus h \in \mathcal{U}_t$. В данной работе рассматриваются сравнения только при $t = 0$ и -1 (обычное равенство функций).

Для любого вектора $a \in V$ подстановка $\sigma_a : V \to V$, определяемая как $\sigma_a(x) = a \oplus x$ для каждого $x \in V$, называется *сдвигом V на a*. Сдвиги пространства V на всевозможные векторы в V образуют группу подстановок на V. Далее эта группа обозначается H_n. Таким образом, $H_n = \{\sigma_a : a \in V\}$. Для любой функции $f \in \mathcal{F}_n$ подгруппа в H_n, состоящая из сдвигов пространства V, сохраняющих f, т. е. из тех сдвигов $\sigma_a \in H_n$, для которых $f(x) = f(\sigma_a(x))$, называется *группой инерции* функции f в группе H_n и обозначается $(H_n)_f$. Иначе, $(H_n)_f = \{\sigma_a \in H_n : f(x) = f(a \oplus x)\}$. Наконец, для любого целого t через $(\mathbf{H}_n)_f^{(t)}$ обозначим *стабилизатор* множества функций $f \oplus \mathcal{U}_t$, а именно: $(\mathbf{H}_n)_f^{(t)} = \{\sigma_a \in H_n : f(x \oplus a) \oplus f(x) \in \mathcal{U}_t\}$.

Пусть $0 \leqslant t \leqslant n-1$, $1 \leqslant k \leqslant n$. Будем говорить, что переменные $x_{k+1}, \ldots, x_n$ функции $f_e(x_1, \ldots, x_n)$ являются *несущественными по модулю $\mathcal{U}_t$*, если найдётся функция $h_e(x_1, \ldots, x_k)$, такая, что $f \oplus h \in \mathcal{U}_t$. Нетрудно видеть, что переменная x_n является несущественной для функции f_e по модулю $\mathcal{U}_t$, если и только если $\Delta_b f \in \mathcal{U}_{t-1}$, где $\Delta_b f(x) = f(x) \oplus f(x \oplus b)$ и $b_e = (0, \ldots, 0, 1)$, или, что то же самое, если $\sigma_b \in (\mathbf{H}_n)_f^{(t-1)}$.

Пусть теперь функция f *зависит по модулю $\mathcal{U}_t$ существенно* лишь от k, $1 \leqslant k < n$, переменных, т. е.

$$f(x) = f_e(x_e) \equiv h_e(x_1, \ldots, x_k) \pmod{\mathcal{U}_t},$$

причём k — минимальное с этим свойством по всем базисам (или, что то же самое, по всем линейным заменам переменных). Тогда с этой функцией однозначно связаны два подпространства: подпространство $V_2 = \langle e^{k+1}, \ldots, e^n \rangle \subseteq V$ векторов, сдвиги по которым лежат в группе $(\mathbf{H}_n)_f^{(t-1)}$, и двойственное ему подпространство

$$V_1^* = (V_2)^\perp = \{e^* : (x, e^*) = 0, x \in V_2\} = \langle e^{*1}, \ldots, e^{*k} \rangle \subseteq V^*,$$

которое назовём *подпространством существенных переменных по модулю* $\mathcal{U}_t$. В данном случае будем использовать запись

$$f \equiv f(V_1^*) \pmod{\mathcal{U}_t},$$

которая подчеркивает, что функция f, заданная на пространстве V, обладает пространством существенных переменных по модулю $\mathcal{U}_t$, совпадающим с подпространством $V_1^* \subseteq V^*$. Функция h может быть однозначно задана по своему ограничению на подпространство V_1 — дополнение к V_2 в пространстве V. Но, в отличие от пространства существенных переменных ${V_1}^*$, подпространство V_1 неоднозначно определяется по функции h.

Термин «подпространство существенных переменных» оправдан в связи с тем, что для каждого ненулевого вектора $e^* \in V_1^*$ при всяком дополнении его до базиса всего пространства V^* у соответствующей двоичной функции будет существенная переменная, записываемая как линейная функция $y_1 = (x, e^*)$. Вместе с тем не всякой существенной переменной двоичной функции соответствует вектор из подпространства существенных переменных. Например, у двоичной функции $x_1(x_2 \oplus x_3)$ три существенных переменных, но подпространство существенных переменных порождается двумя векторами e_1^* и $e_2^* \oplus e_3^*$.

В частности, функция f имеет тривиальную группу инерции $(\mathbf{H}_n)_f^{(t-1)}$ в том и только в том случае, когда пространство существенных переменных функции f по модулю $\mathcal{U}_t$ совпадает со всем пространством V^*.

Заметим, что у функции f с тривиальной группой инерции $(\mathbf{H}_n)_f$ несущественной переменной $x_1 = (x, e^*)$ по модулю $\mathcal{U}_0$ функции f_e соответствует линейное слагаемое $f_e(x_1, \ldots, x_n) = x_1 \oplus h_e(x_2, \ldots, x_n)$. В частности, группа инерции $(\mathbf{H}_n)_f^{(0)}$ функции f нетривиальна в том и только в том случае, если она имеет тривиальную группу инерции $(\mathbf{H}_n)_f$ и не имеет инверторов, т. е. таких векторов, сдвиг на которые переводит функцию f в функцию $\bar{f}$.

Пусть $-1 \leqslant s \leqslant n-1$. Будем говорить, что функция $f \in \mathcal{F}_n$ *имеет аффинные сомножители по модулю* $\mathcal{U}_s$, если найдутся такие аффинная функция $l(x) = (x, a^*) \oplus b$, векторы $x \in V$, $0 \neq a^* \in V^*$, $b \in \{0, 1\}$ и функция h, что $f \equiv l \cdot h \pmod{\mathcal{U}_s}$. Заметим, что функция имеет аффинный сомножитель $(x, e^*) \oplus b$ в том и только в том случае, когда множество $M_f = \{a \in V : f(a) = 1\}$ содержится в линейном многообразии

$$W = W_0 \oplus a, \quad W_0 = \{x : (x, e^*) = 0\}, \quad (a, e^*) = b.$$

В частности, при $n \geqslant 2$ функция f не имеет линейных (аффинных) сомножителей в том и только в том случае, когда $\dim\langle M_f \rangle = n$ ($\dim\langle M_f \oplus a \rangle = n$ при всех $a \in V$).

Наконец, под линейной декомпозицией функции $f \in \mathcal{F}_n$ будем понимать бесповторную декомпозицию функции, получаемой из f некоторой линейной заменой её переменных и ввиду замечания 3 являющейся представлением f в некотором базисе пространства V, т. е. некоторой функцией f_e. Ниже рассматриваются простая и итеративная декомпозиции.

2. Простая декомпозиция

Пусть функция f с тривиальной группой инерции в группе сдвигов в некотором базисе допускает нетривиальную простую декомпозицию

$$f_e(x_1, \ldots x_n) = g_e(h_e(x_1, \ldots x_k), x_{k+1}, \ldots x_n), \quad 2 \leqslant k < n, \tag{1}$$

или иначе

$$f_e(x_1, \dots x_n) = h_e(x_1, \dots x_k) g_e^{(1)}(x_{k+1}, \dots x_n) \oplus g_e^{(0)}(x_{k+1}, \dots x_n).$$

Это равенство можно рассматривать как координатную запись равенства функций на пространстве V вида

$$f(V^*) = h({V_1}^*) g^{(1)}({V_2}^{*(1)}) \oplus g^{(0)}({V_2}^{*(0)}),$$

где $V^* = V_1^* \oplus V_2^*$ — разложение в прямую сумму; $V_1^* = \langle e_1^*, \dots e_k^* \rangle$; $V_2^{*(0)}$ и $V_2^{*(1)}$ — пространства существенных переменных функций $g^{(0)}$ и $g^{(1)}$;

$$V_2^* = V_2^{*(0)} + V_2^{*(1)} = \left\langle e_{k+1}^*, \dots e_n^* \right\rangle;$$

$e_1^*, \dots e_n^*$ — базис пространства V^*, сопряжённый с единичным базисом $e^1 = (1, 0, \dots, 0)$, $\dots$, $e^n = (0, \dots, 0, 1)$.

Если определим функцию $g(z, {V_2}^*) = z g^{(1)}({V_2}^{*(1)}) \oplus g^{(0)}({V_2}^{*(0)})$, $z \in \{0, 1\}$, то можно записать

$$f(V^*) = g(h({V_1}^*), {V_2}^*). \tag{2}$$

Функция g имеет одну дополнительную переменную, не участвующую в линейной замене переменных. Поэтому, чтобы не переходить к расширенному пространству, удобно рассматривать переменную z как параметр и изучать пространства существенных переменных функций $g^{(0)}$ и $g^{(1)}$, заданные на пространстве V. Связь пространства существенных переменных с тривиальностью группы инерции здесь уже будет выглядеть несколько сложнее.

Лемма 1. Если функция f в некотором базисе допускает нетривиальную простую декомпозицию вида (1), то она имеет тривиальную группу инерции в группе сдвигов в том и только в том случае, когда выполнено хотя бы одно из двух условий:

1) функции g_e и h_e имеют тривиальную группу инерции в группе сдвигов;

2) функция g_e содержит в группе сдвигов сдвиг на вектор с ненулевой первой координатой, а функция h_e имеет тривиальную группу инерции в группе сдвигов по модулю $\mathcal{U}_0$.

Действительно, группа инерции в группе сдвигов функции f будет нетривиальной, если выполнено одно из условий:

— группа инерции в группе сдвигов функции h_e нетривиальна;
— в группе инерции в группе сдвигов функции g_e есть нетривиальный вектор с нулевой первой координатой;
— в группе сдвигов функции g_e есть нетривиальный вектор с единичной первой координатой, причём группа инерции функции h_e содержит инвертор, то есть вектор, при сдвиге на который функция h_e переходит в функцию $\bar{h}_e$.

Последний случай иллюстрирует следующий пример. Функция

$$f_e(x_1, x_2, \dots, x_7) = (x_1 \oplus x_2 x_3) x_4 (x_6 \oplus x_7) \oplus x_6 x_7 \oplus x_4 x_5 (x_6 \oplus x_7)$$

при $h_e(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$ имеет инвертор (1,0,0), а функция

$$g_e(z, x_4, x_5, x_6, x_7) = z x_4 (x_6 \oplus x_7) \oplus x_6 x_7 \oplus x_4 x_5 (x_6 \oplus x_7)$$

может быть преобразована к виду

$$(z \oplus x_5) x_4 (x_6 \oplus x_7) \oplus x_6 x_7$$

и содержит в группе инерции сдвиг на вектор (1,0,1,0,0). Поэтому в группе инерции исходной функции будет сдвиг на вектор (1,0,0,0,1,0,0).

В дальнейшем будем полагать, что функция f имеет тривиальную группу инерции в группе сдвигов. В силу леммы 1 это означает, что для каждого базиса, удовлетворяющего условию (1),

— либо группы инерции в группе сдвигов функций h_e и g_e тривиальны;
— либо в группе инерции функции g_e есть один нетривиальный вектор с единичной первой координатой, но группа инерции функции h_e по модулю $\mathcal{U}_0$ тривиальна.

Заметим, что условие тривиальности группы инерции функции h_e по модулю $\mathcal{U}_0$ равносильно совпадению пространства существенных переменных функции h по модулю $\mathcal{U}_0$ с подпространством V_1^*.

Наша дальнейшая задача — выяснение того, в каких случаях каждое из подпространств V_1^* и V_2^* в равенстве (2) однозначно определяет другое. То, что в общем случае неоднозначность возможна, показывают следующие примеры.

Пример 1. Если h имеет аффинный сомножитель по модулю $\mathcal{U}_0$, то второе пространство может неоднозначно определяться по первому. Например, при $h_e(x_1, x_2, x_3, x_4) = \bar{x}_1 h'(x_2, x_3, x_4) \oplus 1$, $g_e(y, x_5x_6, x_7, x_8) = y(x_5x_6 \oplus x_7) \oplus (x_7x_8 \oplus x_7x_8)$ получаем

$$\begin{aligned} f_e(x_1, \ldots, x_8) &= (\bar{x}_1 h'(x_2, x_3, x_4) \oplus 1)(x_5x_6 \oplus x_7) \oplus (x_5x_6 \oplus x_7x_8) = \\ &= \bar{x}_1 h'(x_2, x_3, x_4)(x_5x_6 \oplus x_7) \oplus (x_7x_8 \oplus x_7) = \\ &= \bar{x}_1 h'(x_2, x_3, x_4)((x_5 \oplus x_1)x_6 \oplus x_7) \oplus (x_7x_8 \oplus x_7). \end{aligned}$$

Поэтому функция f допускает другую простую декомпозицию, у которой вместо подпространства $V_2^* = \langle e_5^*, \ldots e_8^* \rangle$ выступает подпространство $U_2^* = \langle e_1^* \oplus e_5^*, e_6^*, e_7^*, e_8^* \rangle$.

Пример 2. Если в разложении функции g_e по первой переменной $g_e = yg_e^1 \oplus g_e^0$ функция g_e^1 имеет аффинные сомножители, то первое пространство может неоднозначно определяться по второму. Например, при $g_e^1(x_5, x_6, x_7, x_8) = \bar{x}_5 g'(x_6, x_7, x_8)$

$$\begin{aligned} f_e(x_1, \ldots, x_8) &= h_e(x_1, x_2, x_3, x_4) g_e^1(x_5, x_6, x_7, x_8) \oplus g_e^0(x_5, x_6, x_7, x_8) = \\ &= h_e(x_1, x_2, x_3, x_4) \bar{x}_5 g'(x_6, x_7, x_8) \oplus g_e^1(x_5, x_6, x_7, x_8) = \\ &= h_e(x_1 \oplus x_5, x_2, x_3, x_4) \bar{x}_5 g'(x_6, x_7, x_8) \oplus g_e^0(x_5, x_6, x_7, x_8). \end{aligned}$$

Поэтому функция f допускает ещё одну простую декомпозицию, у которой вместо подпространства $V_1^* = \langle e_1^*, \ldots e_4^* \rangle$ надо взять подпространство $U_1^* = \langle e_1^* \oplus e_5^*, e_2^*, e_3^*, e_4^* \rangle$.

Пример 3. Если в группе инерции функции g_e есть вектор $(1, b_{k+1}, \ldots, b_n)$ с единичной первой координатой, т. е.

$$g_e(z, x_{k+1}, \ldots, x_n) = g_e(z \oplus 1, x_{k+1} \oplus b_{k+1}, \ldots, x_n \oplus b_n),$$

то для любой функции h_e выполнено тождество

$$g_e(h_e(x_1, \ldots, x_k), x_{k+1}, \ldots, x_n) = g_e(h_e(x_1, \ldots, x_k) \oplus x_1, x_{k+1} \oplus x_1 b_{k+1}, \ldots, x_n \oplus x_1 b_n).$$

Полагая $h'_e = h_e \oplus x_1$ и $g'_e(z, x_{k+1}, \ldots, x_n) = g_e(z, x_{k+1} \oplus x_1 b_{k+1}, \ldots, x_n \oplus x_1 b_n)$, получаем две простые декомпозиции вида (2), у которых подпространства $V_2^* = \left\langle e_{k+1}^*, \ldots e_n^* \right\rangle$ и $U_2^* = \left\langle e_1^* \oplus b_{k+1} e_{k+1}^*, \ldots, e_1^* \oplus b_n e_n^* \right\rangle$ различны.

Следующая теорема даёт условия, при которых каждое из пространств в простой декомпозиции однозначно определяет другое.

Теорема 1. Пусть функция f с тривиальной группой инерции в группе сдвигов допускает для некоторого базиса нетривиальную простую декомпозицию вида (2), удовлетворяющую следующим условиям:

а) функция h имеет тривиальную группу инерции в группе сдвигов по модулю $\mathcal{U}_0$;

б) функция g имеет тривиальную группу инерции в группе сдвигов;

в) функция h не имеет аффинных сомножителей по модулю $\mathcal{U}_0$;

г) функция $g^{(1)}$ не имеет аффинных сомножителей.

Тогда каждое из подпространств в разложении $V^* = V_1^* \oplus V_2^*$ однозначно определяет другое.

Доказательство. Составим базис пространства V^* из базисов подпространств V_1^* и V_2^*. Обозначим через X_1 и X_2 соответствующие наборы переменных, $x_e = (X_1, X_2)$. Тогда равенство (2) принимает вид

$$f_e(X_1, X_2) = g_e(h_e(X_1), X_2).$$

Докажем сначала, что подпространство V_1^* однозначно определяется по V_2^*.

Предположим противное. Тогда найдётся другая простая декомпозиция $f(V^*) = g'(h'(U_1^*), V_2^*)$, где подпространство U_1^* удовлетворяет условию $V^* = V_1^* \oplus V_2^* = U_1^* \oplus V_2^*$. Каждый вектор подпространства U_1^* представим в виде суммы векторов из подпространств V_1^* и V_2^*. Так как размерности подпространств U_1^* и V_1^* совпадают, можно выбрать базис подпространства U_1^* следующего вида:

$$u^1 = e^1 + w^1, \ldots, u^k = e^k + w^k,$$

где $e^1, \ldots, e^k$ — базис пространства V_1^*; $w^1, \ldots, w^k$ — некоторые векторы из подпространства V_2^*. Переходя в равенстве (2) к базисам $e^1, \ldots, e^n$ и $u^1, \ldots, u^k, e^{k+1}, \ldots, e^n$ пространства V^*, получаем $g_e(h_e(X_1), X_2) = g'_e(h'_u(X_1 \oplus X_2 L), X_2)$, где L — некоторая матрица, зависящая от вида векторов $w^1, \ldots, w^k$.

Пусть M_0 и M_1 — множества векторов из подпространства $V_2 = (V_1^*)^\perp$, на которых функция $g_e^{(1)}$ принимает значения 0 и 1 соответственно, $V_2 = M_0 \cup M_1$. Заметим, что множество M_1 содержит линейно независимые векторы, составляющие базис пространства V_2. Если бы размерность пространства, натянутого на M_1, была меньше размерности пространства V_2, то функция $g_e^{(1)}$ имела бы аффинный сомножитель, что противоречит условию п. г.

Для каждой фиксации $\tilde{X}_2$ значений переменных из множества X_2, соответствующих векторам из M_1, выполняется равенство

$$h_e(X_1) \cdot 1 \oplus g_e^{(0)}(\tilde{X}_2) = h'_u(X_1 \oplus \tilde{X}_2 L) g_e'^{(1)}(\tilde{X}_2) \oplus g_e'^{(0)}(\tilde{X}_2) = h'_u(X_1 \oplus \tilde{X}_2 L)1 \oplus g_e'^{(0)}(\tilde{X}_2).$$

Таким образом, получаем набор равенств вида $h_e(X_1) = h'_u(X_1 \oplus a_i) \oplus b_i$, где a_i — некоторый двоичный вектор; $b_i \in \{0, 1\}$. Так как по условию п. а группа инерции функции h_e тривиальна, каждому значению $b_i = b$ соответствует единственное значение $a_i = a_b$. Поэтому возможны только два вида равенств:

$$h_e(X_1) = h'_u(X_1 \oplus a_0) \oplus 0, \quad h_e(X_1) = h'_u(X_1 \oplus a_1) \oplus 1.$$

Если имеют место оба равенства, то $h_e(X_1 \oplus a_0 \oplus a_1) = h_e(X_1) \oplus 1$. Поэтому сдвиг на вектор $a_0 \oplus a_1 \neq 0$ лежит в группе инерции функции h_e в группе сдвигов по модулю $\mathcal{U}_0$, что противоречит условию п. а. Значит, возможно только одно из этих равенств. Пусть, например, выполнено равенство $h_e(X_1) = h'_u(X_1 \oplus a) \oplus b$.

Если $a \neq 0$, то область истинности M_1 функции $g_e^{(1)}$ должна содержаться в линейном многообразии, задаваемом системой уравнений $X_1 L = a$, что также противоречит условию п. г. Значит, линейное отображение L принимает на множестве M_1 только нулевое значение, причём множество M_1 содержит базис пространства V_2. Поэтому $L = 0$. Это означает, что $U_1^* = V_1^*$.

Докажем теперь, что подпространство V_2^* однозначно определяется по V_1^*. Рассуждаем аналогично. Предположим, что найдётся другая простая декомпозиция $f(V^*) = = g'_e(h'_e(V_1^*), U_2^*)$, где подпространство U_2^* удовлетворяет условию $V^* = V_1^* \oplus V_2^* = = V_1^* \oplus U_2^*$. Как и выше, зафиксируем произвольные базисы подпространств V_1^* и V_2^* и обозначим через X_1 и X_2 соответствующие наборы переменных. Тогда после аналогичного перехода к новому базису пространства U_2^* получаем равенство функций

$$g_e(h_e(X_1), X_2) = g'_u(h'_e(X_1), X_2 \oplus X_1 L)$$

при некоторой матрице L. Пусть M_0 и M_1 (M'_0 и M'_1) — множества векторов из подпространства $V_1 = (V_2^*)^\perp$, на которых функция h (h') принимает соответственно значение 0 и 1, $V_1 = M_0 \cup M_1 = M'_0 \cup M'_1$. Так как по условию п. в функция h не имеет аффинных сомножителей по модулю $\mathcal{U}_0$, то ни одно из множеств M_0 и M_1 не может содержаться в собственном аффинном многообразии подпространства V_1, и поэтому они должны иметь максимальный ранг, равный размерности пространства V_1.

При произвольной фиксации $\tilde{X}_1$ всех переменных из X_1, такой, что $h'_e(\tilde{X}_1) = 1$, получаем в результате равенство функций

$$g_e(h_e(\tilde{X}_1), X_2) = g'_u(1, X_2 \oplus \tilde{X}_1 L),$$

которые можно считать заданными на подпространстве $V_2 = (V_1^*)^\perp$. Если найдутся две фиксации $\tilde{X}_1 = a_0$ и $\tilde{X}_1 = a_1$, такие, что функция h_e принимает различные значения

$$g_e(1, X_2) = g'_u(1, X_2 \oplus a_1 L), \quad g_e(0, X_2) = g'_u(1, X_2 \oplus a_0 L),$$

то $a_0 L \neq a_1 L$, так как иначе $g_e^{(1)}(X_2) = g_e(1, X_2) \oplus g_e(0, X_2) \equiv 0$ и функция f_e не зависит от переменных из X_1. С помощью замены переменных получаем равенство

$$g_e(0, X_2 \oplus a_0 L) = g'_u(1, X_2) = g_e(1, X_2 \oplus a_1 L),$$

откуда следует тождество $g_e(z \oplus 1, X_2 \oplus a_0 L \oplus a_1 L) = g_e(z, X_2)$, что противоречит условию п. б. Поэтому при каждой такой фиксации функция h_e принимает одно и то же значение.

Рассмотрим сначала случай $h_e(\tilde{X}_1) = 1$. Здесь должно выполняться равенство функций $g_e(1, X_2) = g'_u(1, X_2 \oplus a_1 L)$.

Аналогично, при произвольной фиксации $\tilde{\tilde{X}}_1$ всех переменных из X_1, такой, что $h'_e(\tilde{\tilde{X}}_1) = 0$, получаем в результате равенство функций

$$g_e(h_e(\tilde{\tilde{X}}_1), X_2) = g'_u(0, X_2 \oplus \tilde{\tilde{X}}_1 L),$$

причём при каждой такой фиксации функция h_e должна принимать одно и то же значение. Если $h_e(\tilde{\tilde{X}}_1) = 1$, то $M'_0 \subseteq M_1$ и $V_1 = M'_0 \cup M'_1 \subseteq M_1$, что возможно, только если функция h_e является константой. Значит, $h_e(\tilde{\tilde{X}}_1) = 0$ и $M'_0 \subseteq M_0$, и при b_0 из M'_0 выполнено равенство функций $g_e(0, X_2) = g'_u(0, X_2 \oplus b_0 L)$. Значит, $M'_0 = M_0$ и $M'_1 = M_1$, откуда $h_e = h'_e$.

Предположим, что $L \neq 0$. Тогда, так как каждое из множеств M_0 и M_1 содержит базис пространства V_1, найдутся ненулевые векторы $u \in M_0$ и $v \in M_1$ пространства V_1, такие, что выполнены равенства $u_e L \neq 0$ и $v_e L \neq 0$. Для всех таких векторов должны выполняться равенства

$$g_e(1, X_2) = g'_u(1, X_2 \oplus v_e L), \quad g_e(0, X_2) = g'_u(0, X_2 \oplus u_e L).$$

Если $v, v' \in M_1$, то $g'_u(1, X_2 \oplus v_e L) = g_e(1, X_2 \oplus v'_e L)$, откуда

$$g_e(1, X_2 \oplus v_e L \oplus v'_e L) = g_e(1, X_2).$$

Значит, сдвиг на вектор $(v_e \oplus v'_e)L$ лежит в группе инерции функции $g_e(1, X_2)$. Так как множество M_1 содержит базис пространства V_1, множество векторов вида $v \oplus v'$, $v, v' \in M_1$, порождает подпространство H_1 размерности $\dim H_1 \geqslant \dim V_1 - 1$. Если $\dim H_1 = \dim V_1 - 1$, то $M_1 \subseteq v \oplus H_1$, что противоречит отсутствию аффинных сомножителей у функции h. Значит, $\dim H_1 = \dim V_1$.

Так как по предположению $L \neq 0$, а размерность M_0 совпадает с размерностью пространства V_1, найдётся вектор $u \in M_0$, такой, что $u_e L \neq 0$. Выразим u через базис, составленный из векторов w_t вида $v \oplus v'$, $v, v' \in M_1$:

$$u = \sum_i c_i w_i, \quad c_i \in \{0, 1\}.$$

Так как векторы $(w_i)_e L$ лежат в группе инерции функции $g_e(1, X_2)$, то и их сумма также лежит в группе инерции функции $g_e(1, X_2)$:

$$g_e(1, X_2) = g'_u(1, X_2 \oplus \sum_i c_i (w_i)_e L) = g'_e(1, X_2 \oplus u_e L).$$

Отсюда получаем тождество

$$g_e(z, X_2) = g'_u(z, X_2 \oplus u_e L), \quad u_e L \neq 0,$$

что противоречит тривиальности группы инерции в группе сдвигов функции f. Поэтому $L = 0$. Это означает, что $U_2^* = V_2^*$.

Случай $h_e(\tilde{X}_1) = 0$ рассматривается полностью аналогично. Имеем включение $M'_1 \subseteq M_0$ и равенство функций

$$g_e(0, X_2) = g'_u(1, X_2 \oplus a_1 L).$$

Если $h_e(\tilde{\tilde{X}}_1) = 0$, то $M'_0 \subseteq M_0$, что невозможно, так как функция h_e не является константой. Значит, $h_e(\tilde{\tilde{X}}_1) = 1$, $M'_0 \subseteq M_1$ и при некотором b_0 выполнено равенство функций

$$g_e(1, X_2) = g'_u(0, X_2 \oplus b_0 L).$$

Отсюда $M'_0 = M_1$ и $M'_1 = M_0$, т. е. $h_e = h'_e \oplus 1$. Далее надо повторить все рассуждения, поменяв местами функции $g'_u(0, X_2)$ и $g'_u(1, X_2)$. ■

3. Итеративная декомпозиция

В заключение рассмотрим случай итеративной декомпозиции, в котором можно явно установить связь между двумя различными простыми декомпозициями.

Теорема 2. Пусть функция f с тривиальной группой инерции в группе сдвигов допускает две нетривиальные простые декомпозиции

$$f(V^*) = g(h(V_1{}^*), V_2{}^*) = g'(h'(U_1{}^*), U_2{}^*), \tag{3}$$

где $V^* = V_1^* \oplus V_2^* = U_1^* \oplus U_2^*$ — разложения в прямую сумму, причём $V_1^* \subseteq U_1^*$. Тогда

1) для подпространства $W^* = V_2^* \bigcap U_1^*$ выполнены равенства $U_1^* = V_1^* \oplus W^*$, $V_2^* = W^* \oplus U_2^*$;
2) если обе простые декомпозиции удовлетворяют условиям теоремы 1, то найдётся функция m, удовлетворяющая равенству

$$f(V^*) = g'(m(h(V_1{}^*), W^*), U_2^*),$$

причём

$$g(y, V_2^*) = g'(m(y, W^*), U_2^*), \quad h'(U_1^*) = m(h(V_1{}^*), W^*).$$

Доказательство. Если $V_1^* = U_1^*$, то справедливость утверждения вытекает из теоремы 1. Пусть $V_1^* \subset U_1^*$ и $W^* = V_2^* \bigcap U_1^*$. С учётом размерностей

$$\begin{gathered}\dim W^* = \dim V_2^* + \dim U_1^* - \dim(V_2^* \cup U_1^*) = \\ = (n - \dim V_1^*) + \dim U_1^* - n = \dim U_1^* - \dim V_1^*\end{gathered}$$

получаем, что W^* — дополнение подпространства V_1^* в U_1^*, т. е. $U_1^* = V_1^* \oplus W^*$. Докажем, что $V_2^* = W^* \oplus U_2^*$.

Составим один базис $e_1^*, \ldots, e_n^*$ пространства V^* из базисов подпространств V_1^*, W^* и U_2^*, а второй базис $u_1^*, \ldots, u_n^*$ — из того же самого базиса подпространства V_1^* и базиса пространства $V_2{}^*$, который можно составить из базиса пространства W^*, дополнив его векторами вида $u^* = e^* + v^*$, где e^* — векторы из базиса подпространства U_2^*, а v^* — некоторые векторы из $V_1^* \oplus W^*$. Тогда равенство (3) в этих базисах можно записать в виде

$$g_u(h_e(X_1), X_2, X_3 \oplus X_1L_1 \oplus X_2L_2) = g'_e(h'_e(X_1, X_2), X_3), \tag{4}$$

где X_1, X_2, X_3 — соответствующие наборы переменных; L_1 и L_2 — некоторые матрицы.

Зафиксируем произвольным образом значения переменных из X_2 так, чтобы функция $h'_e(X_1, b)$ не была константой:

$$g_u(h_e(X_1), b, X_3 \oplus X_1L_1 \oplus bL_2) = g'_e(h'_e(X_1, b), X_3). \tag{5}$$

Изучим многочлены Жегалкина двоичных функций в левой и правой частях этого равенства. Функции h_e и g'_e удовлетворяют условиям теоремы 1. В правой части все переменные из X_3 являются существенными, поэтому в левой части они также все входят в многочлен Жегалкина. В левой части найдётся произведение переменных из X_3, умноженное на все конъюнкции многочлена Жегалкина функции $h_e(X_1)$, быть может, без свободного члена. Поэтому $h_e(X_1) \equiv h'_e(X_1, b) \pmod{\mathcal{U}_0}$ и обе части равенства (5) также существенно зависят от всех переменных их множества X_1. По теореме 1 получаем, что второе подпространство однозначно определяется по первому подпространству V_1^*, и поэтому в равенствах (4) и (5) должно быть $L_1 = 0$. А это означает, что $V_2^* = W^* \oplus U_2^*$.

Рассмотрим разложение функции g по первой переменной:

$$g(z, V_2^*) = \bar{z}g(0, V_2^{0*}) \vee zg(1, V_2^{1*}).$$

Здесь V_2^{0*} и V_2^{1*} — подпространства существенных переменных подфункций $g(0,*)$ и $g(1,*)$, причём должно выполняться равенство $V_2{}^* = V_2^{0*} + V_2^{1*}$. С другой стороны, в силу вида простой декомпозиции после фиксации значений всех переменных функции h может получиться только одна из двух подфункций функции g:

$$g(0, V_2^{0*}) = g'(h'^0(U_1^{0*}), U_2{}^*), \quad g(1, V_2^{1*}) = g'(h'^1(U_1^{1*}), U_2{}^*). \tag{6}$$

Здесь подпространство U_2^* однозначно определяется по U_1^*, а $U_1^{0*} \subseteq W^*$ и $U_1^{1*} \subseteq W^*$ — подпространства существенных переменных функций h'^0 и h'^1, полученных соответствующими фиксациями переменных из V_1^* у функции $h'(U_1{}^*) = h'(V_1^*, W^*)$. Заметим, что пространства U_1^{0*} и U_1^{1*} зависят не от способа фиксации переменных функции h, а только от получившегося значения функции h. Сравнивая пространства существенных переменных у функций, стоящих в левой и правой частях в равенствах (6), получаем разложения в прямую сумму $V_2^{0*} = U_1^{0*} \oplus U_2{}^*$ и $V_2^{1*} = U_1^{1*} \oplus U_2{}^*$. Из этих равенств вытекает $V_2{}^* = W^* \oplus U_2{}^*$, а значит, и $U_1^{0*} + U_1^{1*} = W^*$.

Если в равенствах (6) зафиксировать переменные, соответствующие некоторому базису пространства U_2^*, так, чтобы функция g' зависела существенно от оставшейся переменной, то получится, что функции $h'^0(U_1^{0*})$ и $h'^1(U_1^{1*})$ также определены однозначно и зависят не от способа фиксации переменных функции h, а только от получившегося значения функции h. Обозначим

$$m(z, W^*) = \bar{z}h'^0(U_1^{0*}) \vee zh'^1(U_1^{1*}).$$

Из равенств (6) получаем тождество

$$g(z, V_2{}^*) = g'(m(z, W^*), U_2{}^*).$$

Подставляя теперь вместо переменной z функцию $h(V_1^*)$, получаем равенство

$$f(V^*) = g'(m(h_1(V_1{}^*), W^*), U_2^*),$$

откуда, аналогичным образом фиксируя переменные, соответствующие некоторому базису пространства U_2^*, так, чтобы функция g' зависела существенно от оставшейся переменной, получаем $h'(U_1^*) = m(h(V_1{}^*), W^*)$. ■

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. Т. 4. М.: Физматлит, 2001. С. 273–314.
2. *Черемушкин А. В.* Однозначность разложения двоичной функции в бесповторное произведение нелинейных неприводимых сомножителей // Вестник Московского государственного университета леса «Лесной вестник». 2004. № 4(35). С. 86–90.

REFERENCES

1. *Cheremushkin A. V.* Metody affinnoy i lineynoy klassifikatsii dvoichnykh funkiy [Methods of affine and linear classification of binary functions]. Tr. Diskr. Mat., 2001, vol. 4, pp. 273–314. (in Russian)
2. *Cheremushkin A. V.* Odnoznachnost' razlozheniya dvoichnoy funktsii v bespovtornoe proizvedenie nelineynykh neprivodimykh somnozhiteley [The uniqueness of the binary function decomposition in a unrepeated product of non-linear irreducible factors]. Lesnoy vestnik, 2004, no. 4(35), pp. 86–90. (in Russian)