УДК 519.719.325

О ЛИНЕЙНОЙ РАЗЛОЖИМОСТИ ДВОИЧНЫХ ФУНКЦИЙ

А. В. Черемушкин

ФГУП «НИИ «Квант», г. Москва, Россия

Рассматривается множество возможных разложений двоичной функции в сумму (произведение) функций от непересекающихся множеств переменных при различных линейных преобразованиях аргументов, полученных отбрасыванием одночленов малой степени в их многочленах Жегалкина. Каждому такому разложению соответствует разложение векторного пространства в прямую сумму подпространств. Приведены условия, при которых такое разложение определяется однозначно с точностью до перестановки слагаемых (сомножителей) и связанных с ними подпространств между собой.

Ключевые слова: *двоичные функции, бесповторная декомпозиция, разложение в прямую сумму, линейное преобразование.*

DOI 10.17223/20710410/40/2

LINEAR DECOMPOSITION OF BOOLEAN FUNCTIONS INTO A SUM OR A PRODUCT OF COMPONENTS

A. V. Cheremushkin

Technology Federal State Unitary Enterprise "Research Institute Kvant", Moscow, Russia

E-mail: avc238@mail.ru

Let $f : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$ be a Boolean function, $n \geqslant 2$, and $\mathcal{U}_s$ be a set of Boolean functions f of degree $\deg f \leqslant s$. Here is a consideration of the disjunctive decomposition of f into sum and products modulo $\mathcal{U}_s$ of Boolean functions after a linear substitution on arguments. The main result is the following: if all arguments of the functions $f(xA)$ under linear substitutions A of the vector space $\mathrm{GF}(2)^n$ are essential modulo $\mathcal{U}_s$ and f may be represented as disjunctive sum $f \equiv f_1 \oplus \ldots \oplus f_m \pmod{\mathcal{U}_s}$, where m is maximal, then subsequent direct sum of subspaces $\mathrm{GF}(2)^n = V^{(1)} + \ldots + V^{(m)}$ is unique and invariant under stabilizer group of the function f in general linear group. The article contains analogous result describing sufficient uniqueness condition for disjunctive products $f \equiv f_1 \ldots f_m \pmod{\mathcal{U}_s}$, namely, every function f_i has no affine multipliers and the set $\{a \in V_i : f_i(x \oplus a) \oplus f_i(x)$ has affine multipliers$\}$ generates the whole subspace V_i, $i = 1, \ldots, m$. For instance, this class of functions contains a nondegenerated quadratic forms.

Keywords: *Boolean functions, disjunctive decomposition, disjunctive sum, disjunctive products, linear transformation.*

Пусть $\mathcal{F}_n = \{f : \mathrm{GF}(2)^n \to \mathrm{GF}(2)\}$ — множество двоичных функций от n переменных, $n \geqslant 1$, $\mathbf{H}_n$ — группа сдвигов. Для каждого целого $s \geqslant 0$ определим подпространство $\mathcal{U}_s = \{f : \deg f \leqslant s\}$ пространства функций $\mathcal{F}_n$, имеющих ограниченную

степень нелинейности. Заметим, что $\mathcal{U}_0 = \{0, 1\}$. При $s < 0$ положим $\mathcal{U}_s = \{0\}$ — нулевое подпространство. Обозначим $(\mathbf{H}_n)_f^{(s)}$ множество таких сдвигов $\begin{pmatrix} x \\ x \oplus a \end{pmatrix} \in \mathbf{H}_n$, что выполнено сравнение

$$f(x \oplus a) \equiv f(x) \,(\mathrm{mod}\, \mathcal{U}_s), \quad x \in \mathrm{GF}(2)^n.$$

При $s < 0$ группа $(\mathbf{H}_n)_f^{(s)}$ является обычной группой инерции $(\mathbf{H}_n)_f$ функции f.

Пусть $0 \leqslant t \leqslant n-1$, $1 \leqslant k \leqslant n$. Будем говорить, что переменные $x_{k+1}, \ldots, x_n$ функции $f(x_1, \ldots, x_n)$ являются несущественными по модулю $\mathcal{U}_s$, если найдётся функция $h(x_1, \ldots, x_k)$, такая, что $f \oplus h \in \mathcal{U}_s$. Нетрудно видеть, что переменная x_n является несущественной для функции f по модулю $\mathcal{U}_s$, если и только если

$$\begin{pmatrix} x \\ x \oplus e_n \end{pmatrix} \in (\mathbf{H}_n)_f^{(s-1)}$$

при $e^n = (0, \ldots, 0, 1)$.

Определение 1. Пусть $*$ — бинарная ассоциативная операция. Будем говорить, что функция $f \in \mathcal{F}_n$ *линейно разложима относительно* $*$ *по модулю* $\mathcal{U}_s$, если при некотором линейном преобразовании A пространства $\mathrm{GF}(2)^n$ и $1 \leqslant k < n$ найдутся функции f_1 и f_2, для которых выполнено сравнение

$$f(xA) \equiv f_1(x_1, \ldots, x_k) * f_2(x_{k+1}, \ldots, x_n) \,(\mathrm{mod}\, \mathcal{U}_s).$$

Заметим, что всего имеется четыре бинарных ассоциативных операции: $x \oplus y$, $x \cdot y$, $x \oplus y \oplus 1$ и $x \vee y$, однако при $s \geqslant 0$ достаточно ограничиться рассмотрением только двух операций: сложения и умножения.

1. Бесповторная сумма функций

Сначала исключим случай наличия слагаемых первой степени. Каждая функция, представимая в виде суммы функций с непересекающимися наборами аргументов, среди которых есть слагаемые, имеющие вид переменных в первой степени, линейно эквивалентна функции, у которой такое слагаемое только одно. Пусть, например, это x_n. Тогда вектор $e^n = (0, \ldots, 0, 1)$ порождает инвариантное подпространство, а описание групп инерции таких функций имеет следующий вид.

Теорема 1. Если имеет место равенство

$$f(x_1, \ldots, x_n) = h(x_1, \ldots, x_{n-1}) \oplus x_n$$

и $(\mathbf{H}_n)_f = 1$, то справедливы следующие изоморфизмы:

$$\mathbf{GL}\,(n, 2)_f \cong \mathbf{GL}\,(n-1, 2)_h^{(1)};$$
$$\mathbf{AGL}\,(n, 2)_f \cong \mathbf{AGL}\,(n-1, 2)_h^{(1)};$$
$$\mathbf{AGL}\,(n, 2)_f^{(0)} \cong \mathbf{AGL}\,(n-1, 2)_h^{(1)} \times \mathbf{H}_1.$$

Действительно, в этом случае $|(\mathbf{H}_n)_f^{(1)}| = 2$, причём $\begin{pmatrix} x \\ x \oplus e^n \end{pmatrix} \in (\mathbf{H}_n)_f^{(1)}$. Поэтому матрицы из группы $\mathrm{Pr}_{\mathbf{GL}\,(n,2)}\mathbf{AGL}\,(n, 2)_f^{(0)}$ имеют вид

$$Q = \begin{pmatrix} A & b \\ 0 \ldots 0 & 1 \end{pmatrix}.$$

Искомый изоморфизм задаётся соответствием $(Q,h)\mapsto((A,h^1),h_n)$, где $h=(h_1,\ldots,h_{n-1},h_n)=(h^1,h_n)$.

Заметим, что для сумм слагаемых второй степени и $s\leqslant 1$ ни об однозначности разложения, ни о сведении вычисления группы инерции всей функции к вычислению групп инерции слагаемых в принципе не может быть и речи, так как полученные функции имеют неприводимые группы инерции, в качестве которых выступают классические линейные симплектическая и ортогональная группы, являющиеся неприводимыми линейными группами.

В то же время для слагаемых степени три и выше, как правило, такое сведение уже может иметь место. Найдём достаточно общие условия, при которых можно показать однозначность разложения функции степени k в бесповторную сумму по модулю $\mathcal{U}_s$ при $-1\leqslant s\leqslant k-1$. Естественно, что для этого разложение должно иметь максимально возможное число слагаемых.

Сначала рассмотрим частный случай, когда разложение имеет вид, аналогичный каноническому представлению квадратичной формы.

Пусть $[G]\mathbf{S}_p$ обозначает экспоненцирование линейной группы $G\leqslant\mathbf{GL}(m,2)$ и симметрической группы $\mathbf{S}_p$ степени p, $[G]\mathbf{S}_p\leqslant\mathbf{GL}(mp,2)$. Эта группа состоит из матриц, полученных путем замещения ненулевых элементов подстановочных матриц произвольными матрицами из группы G. Воспользуемся следующей удобной конструкцией, введённой М. В. Лариным. Обозначим $\langle M_f\rangle$ подпространство, порождённое множеством $M_f\subset\mathrm{GF}(2)^n$.

Утверждение 1. Пусть множество $M_f=\{a\in\mathrm{GF}(2)^n : f(a)=1\}$ удовлетворяет условию$\langle M_f\rangle=\mathrm{GF}(2)^n$, причём его можно представить в виде такого нетривиального разбиения $M_f=M_1\cup\ldots\cup M_m$, что $\mathrm{GF}(2)^n=\langle M_1\rangle+\ldots+\langle M_m\rangle$ — разложение в прямую сумму и m — максимальное число с этим свойством. Тогда:

1) группа $\mathbf{GL}\,(n,2)_f$ сохраняет это разбиение и разложение;
2) если множество функций $\{f_i : M_{f_i}=M_i,\ i=1,\ldots,m\}$ разбивается на классы эквивалентности относительно $\mathbf{GL}\,(n,2)$ вида $\{f_{\mu_1},\ldots,f_{\mu_p}\},\ldots,\{f_{\nu_1},\ldots,f_{\nu_q}\}$, то

$$\mathbf{GL}\,(n,2)_f\cong[\mathbf{GL}\,(n_{\mu_1},2)_{f_{\mu_1}}]\mathbf{S}_p\times\cdots\times[\mathbf{GL}\,(n_{\nu_1},2)_{f_{\nu_1}}]\mathbf{S}_q.$$

Доказательство. Утверждение следует из того, что если два разбиения $M_f=$ $=M_1\cup\ldots\cup M_m$ и $M_f=L_1\cup\ldots\cup L_r$ порождают разложение пространства в прямую сумму, то их пересечение $M_f=\bigcup\limits_{i,j}M_i\cap L_j$ также порождает разложение пространства в прямую сумму подпространств. ■

Теорема 2 [1]. Если $n=mk$, $k\geqslant 3$, $m\geqslant 2$ и функция f имеет вид

$$f(x_1,\ldots,x_n)=\sum_{i=0}^{m-1}x_{ik+1}x_{ik+2}\cdots x_{ik+k},$$

то группа $\mathrm{Pr}_{\mathbf{GL}\,(n,2)}\mathbf{AGL}\,(n,2)_f^{(k-1)}$ изоморфно вложима в группу $[\mathbf{GL}\,(k,2)]\mathbf{S}_m$.

Доказательство. В данном случае множество векторов, для которых производные имеют линейные сомножители по модулю $\mathcal{U}_{k-2}$, совпадает с объединением подпространств $\langle e_{ik+1},e_{ik+2},\ldots,e_{ik+k}\rangle$, $i=1,\ldots,m$, где e_j — векторы стандартного базиса, $j=1,\ldots,n$. Это множество удовлетворяет условиям утверждения 1 и является инвариантным относительно группы $\mathrm{Pr}_{\mathbf{GL}\,(n,2)}\mathbf{AGL}\,(n,2)_f^{(k-1)}$. ■

Заметим, что в неявной форме в терминах полилинейных форм этот результат сформулирован в работе [2].

Перейдём теперь к рассмотрению общего случая (данный результат анонсирован в [3]). В дальнейшем будем использовать понятие подпространства существенных переменных (подробнее см. в [4]). Вместо двоичных функций на пространстве $\mathrm{GF}(2)^n$, являющемся множеством двоичных векторов, удобно рассматривать функции, заданные на произвольном пространстве V размерности n над полем $\mathrm{GF}(2)$. При фиксации базиса $e = (e^1, \ldots, e^n)$ этого пространства функция $f : V \to \mathrm{GF}(2)$ может быть записана в виде двоичной функции $f_e(x_1, \ldots, x_n)$, где $f_e : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$, а каждой переменной $x_i = (x, e^{*i})$ соответствует вектор сопряжённого базиса e^{*i} из сопряжённого пространства V^*.

Если 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), то с этой функцией однозначно связаны два подпространства: подпространство $W = \langle e^{k+1}, \ldots, e^n \rangle \subseteq V$ векторов, сдвиги по которым лежат в группе $(\mathbf{H}_n)_f^{(t-1)}$, и двойственное ему подпространство

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

называемое *подпространством существенных переменных по модулю* $\mathcal{U}_t$. В этом случае будем использовать обозначение $f = f(W^*)$.

Нетрудно видеть, что функция $f = f(V^*)$ линейно разложима в бесповторную сумму по модулю $\mathcal{U}_s$, если при некотором нетривиальном разложении пространства V^* в прямую сумму $V^* = V_1^* + V_2^*$ функция имеет вид $f \equiv f_1(V_1^*) \oplus f_2(V_2^*) \pmod{\mathcal{U}_s}$.

Лемма 1. Пусть имеется два разложения пространства V^* в прямую сумму ненулевых подпространств $V^* = V_1^* + V_2^* = U_1^* + U_2^*$. Если при $s \geqslant 2$ функция $f = f(x_1, \ldots, x_n) = f(V^*)$ имеет тривиальную группу инерции $(\mathbf{H}_n)_f^{(s-1)}$ и выполняется сравнение

$$f \equiv f_1(V_1^*) \oplus f_2(V_2^*) \equiv h_1(U_1^*) \oplus h_2(U_2^*) \pmod{\mathcal{U}_s}, \tag{1}$$

то функция f допускает разложение

$$f \equiv d_1(W_{11}^*) \oplus d_2(W_{12}^*) \oplus d_3(W_{21}^*) \oplus d_4(W_{22}^*) \pmod{\mathcal{U}_s},$$

где $W_{ij}^* = V_i^* \bigcap U_j^*$, $i, j = 1, 2$, удовлетворяют условиям

$$\begin{cases} V_1^* = W_{11}^* + W_{12}^*, \\ V_2^* = W_{21}^* + W_{22}^*, \\ U_1^* = W_{11}^* + W_{21}^*, \\ U_1^* = W_{12}^* + W_{22}^*, \end{cases}$$

d_i, $i = 1, \ldots, 4$, — некоторые функции, удовлетворяющие следующим сравнениям:

$$\begin{cases} f_1 \equiv d_1 \oplus d_2 \pmod{\mathcal{U}_s}, \\ f_2 \equiv d_3 \oplus d_4 \pmod{\mathcal{U}_s}, \\ h_1 \equiv d_1 \oplus d_3 \pmod{\mathcal{U}_s}, \\ h_2 \equiv d_2 \oplus d_4 \pmod{\mathcal{U}_s}. \end{cases}$$

Доказательство. При $n \leqslant 5$ таких разложений у функции f не существует. При $n = 6$ однозначность разложения (1) вытекает из теоремы 2. Пусть теорема верна для всех функций от $n-1 \geqslant 6$ переменных, докажем её для функции f от n переменных. Из условия $(\mathbf{H}_n)_f^{(s-1)} = 1$ следует, то все производные $\Delta_a f$, $0 \neq a \in V$, функции f имеют степень нелинейности не меньше s. Выберем вектор $0 \neq a \in V$ так, чтобы у производной $\Delta_a f$ было минимальное число существенных переменных по модулю $\mathcal{U}_s$. Так как производная суммы функций равна сумме соответствующих производных, то число существенных переменных по модулю $\mathcal{U}_s$ у производной $\Delta_a f$ суммы $f = f_1(V_1^*) \oplus f_2(V_2^*)$ может быть минимальным только в том случае, когда $a \in V_1$ или $a \in V_2$, где $V = V_1 + V_2$ — соответствующее разложение пространства V. Аналогично получаем, что $a \in U_1$ или $a \in U_2$. Пусть для определённости $a \in V_1 \cap U_1$.

Дополним вектор a до базиса пространства V так, что $e^1 = a$, $\langle e^1, \ldots, e^k\rangle = V_1$, $\langle e^{k+1}, \ldots, e^n\rangle = V_2$. Пусть $\langle e^{*1}, \ldots, e^{*n}\rangle$ — сопряжённый базис пространства V^*, такой, что $\langle e^{*1}, \ldots, e^{*k}\rangle = V_1^*$, $\langle e^{*k+1}, \ldots, e^{*n}\rangle = V_2^*$. Обозначим $U^* = (\langle a\rangle)^\perp = \langle e^{*2}, \ldots, e^{*n}\rangle \subset V^*$.

Выберем еще один базис $\langle u^1, \ldots, u^n\rangle$ пространства V так, чтобы $u^1 = a$ и $\langle u^1 \ldots, u^k\rangle = U_1$, $\langle u^{t+1}, \ldots, u^n\rangle = U_2$. Обозначим сопряжённый базис через $u^{*1}, \ldots, u^{*n}$, $\langle u^{*1}, \ldots, u^{*t}\rangle = U_1^*$, $\langle u^{*t+1}, \ldots, u^{*n}\rangle = U_2^*$. Имеем $(a, e^{*1}) = (a, u^{*1}) = 1$, $(a, e^{*i}) = (a, u^{*i}) = 0$ при $2 \leqslant i \leqslant n$.

Нетрудно видеть, что $U^* = \langle e^{*2}, \ldots, e^{*n}\rangle = \langle u^{*2}, \ldots, u^{*n}\rangle$.

Рассмотрим два случая:

1) $u^{*1} \in V_1^*$;

2) $u^{*1} \notin V_1^*$.

В п е р в о м с л у ч а е можно предполагать, что $u^{*1} = e^{*1}$. Тогда сравнение (1) принимает вид

$$f = f_1(x_1, \widetilde{V_1^*}) \oplus f_2(V_2^*) \equiv h_1(x_1, \widetilde{U_1^*}) \oplus h_2(U_2^*) \pmod{\mathcal{U}_s}, \tag{2}$$

где $x_1 = (x, e^{*1}) = (x, u^{*1})$, $\widetilde{V_1^*} = \langle e^{*2}, \ldots, e^{*k}\rangle$, $\widetilde{U_1^*} = \langle u^{*2}, \ldots, u^{*t}\rangle$, причём выполнены равенства $U^* = \widetilde{V_1^*} + V_2^* = \widetilde{U_1^*} + U_2^*$. Разложим функции f_1 и h_1 по первой переменной:

$$\begin{aligned} f_{1e}(x_1, \widetilde{V_1^*}) &\equiv x_1 f'_{1e}(\widetilde{V_1^*}') \oplus f_{1e}^{(0)}(\widetilde{V_1^*}^{(0)}) \pmod{\mathcal{U}_s}, \\ h_{1u}(x_1, \widetilde{U_1^*}) &\equiv x_1 h'_{1u}(\widetilde{U_1^*}') \oplus h_{1u}^{(0)}(\widetilde{U_1^*}^{(0)}) \pmod{\mathcal{U}_s}, \end{aligned}$$

где

$$\begin{aligned} &f'_{1e}(\widetilde{V_1^*}') = f_{1u}(1, \widetilde{U_1^*}) \oplus f_{1u}(0, \widetilde{U_1^*}), \\ &f_{1e}^{(0)}(\widetilde{V_1^*}^{(0)}) = f_{1u}(0, \widetilde{U_1^*}), \\ &h'_{1u}(\widetilde{U_1^*}') = h_{1u}(1, \widetilde{U_1^*}) \oplus h_{1u}(0, \widetilde{U_1^*}), \\ &h_{1u}^{(0)}(\widetilde{U_1^*}^{(0)}) = h_{1u}(0, \widetilde{U_1^*}), \end{aligned}$$

$\widetilde{V_1^*}'$, $\widetilde{V_1^*}^{(0)} \subseteq V_1^*$ и $\widetilde{U_1^*}'$, $\widetilde{U_1^*}^{(0)} \subseteq U_1^*$ — соответствующие пространства существенных переменных по модулю $\mathcal{U}_s$. Подставляя в сравнение (2) значения $x_1 = 0$ и $x_1 = 1$, получаем, что оно равносильно системе

$$\begin{cases} f_{1e}^{(0)}(\widetilde{V_1^*}^{(0)}) \oplus f_{2e}(V_2^*) \equiv h_{1u}^{(0)}(\widetilde{U_1^*}^{(0)}) \oplus h_{2u}(U_2^*) \pmod{\mathcal{U}_s}, \\ f'_{1e}(\widetilde{V_1^*}') \equiv h'_{1u}(\widetilde{U_1^*}') \pmod{\mathcal{U}_{s-1}}. \end{cases}$$

Так как в этих сравнениях стоят функции, у которых все переменные существенны по модулю $\mathcal{U}_s$, то, в частности, получаем $\widetilde{V_1^*} + V_2^* = \widetilde{U_1^*} + U_2^*$ и $\widetilde{V_1^*}' = \widetilde{U_1^*}'$.

Введём обозначения для подпространств пространства U^*:

$$\begin{cases} \widetilde{W}_{11}^{*(0)} &= \widetilde{V_1^*}^{(0)} \bigcap \widetilde{U_1^*}^{(0)}, \\ W_{12}^{*(0)} &= \widetilde{V_1^*}^{(0)} \bigcap U_2^* = V_1^* \bigcap U_2^*, \\ W_{21}^{*(0)} &= V_2^* \bigcap \widetilde{U_1^*}^{(0)} = V_2^* \bigcap U_1^*, \\ W_{22}^* &= V_2^* \bigcap U_2^*. \end{cases}$$

По предположению индукции для пространства U^*, размерность которого меньше размерности пространства V^*, найдутся функции $d_i^{(0)}$, такие, что функция $f^{(0)}$ допускает разложение

$$f^{(0)} \equiv d_1^{(0)}(\widetilde{W}_{11}^{*(0)}) \oplus d_2^{(0)}(W_{12}^{*(0)}) \oplus d_3^{(0)}(W_{21}^{*(0)}) \oplus d_4^{(0)}(W_{22}^*) \pmod{\mathcal{U}_s}.$$

При этом должны выполняться следующие сравнения:

$$\begin{cases} f_1^{(0)} &\equiv d_1^{(0)} \oplus d_2^{(0)} \pmod{\mathcal{U}_s}, \\ f_2 &\equiv d_3^{(0)} \oplus d_4^{(0)} \pmod{\mathcal{U}_s}, \\ h_1^{(0)} &\equiv d_1^{(0)} \oplus d_3^{(0)} \pmod{\mathcal{U}_s}, \\ h_2 &\equiv d_2^{(0)} \oplus d_4^{(0)} \pmod{\mathcal{U}_s}. \end{cases}$$

Полагая $d'_{1e} \equiv f'_{1e} \equiv h'_{1e} \pmod{\mathcal{U}_{s-1}}$, $d_1 = x_1 d'_1 \oplus d_1^{(0)}$, $W_{11}^* = \langle e^{*1} \rangle + \widetilde{V_1^*}' + \widetilde{W}_{11}^{*(0)}$ и $d_i = d_i^{(0)}$, $i = 1, 2, 3$, получаем требуемое утверждение.

В о в т о р о м с л у ч а е, не уменьшая общности, можно предполагать, что вектор u^{*1} имеет вид $u^{*1} = e^{*1} + e^{*k+1}$. Поэтому сравнение (1) принимает вид

$$f \equiv f_1(x_1, \widetilde{V}_1^*) \oplus f_2(V_2^*) \equiv h_1(x_1 \oplus x_{t+1}, \widetilde{U}_1^*) \oplus h_2(U_2^*) \pmod{\mathcal{U}_s}, \tag{3}$$

где $U_1^* = \langle e^{*1} + e^{*t+1} \rangle + \widetilde{U_1^*}$ и $U^* = \widetilde{V_1^*} + V_2^* = \widetilde{U_1^*} + U_2^*$.

Рассуждая аналогично, получаем, что (3) равносильно системе

$$\begin{cases} f_{1e}^{(0)}(\widetilde{V_1^*}^{(0)}) \oplus f_{2e}(V_2^*) \equiv x_{t+1} h'_{1u}(\widetilde{U_1^*}') \oplus h_{1u}^{(0)}(\widetilde{U_1^*}^{(0)}) \oplus h_{2u}(U_2^*) \pmod{\mathcal{U}_s}, \\ f'_{1e}(\widetilde{V_1^*}') \equiv h'_{1u}(\widetilde{U_1^*}') \pmod{\mathcal{U}_{s-1}}, \end{cases}$$

где $h_{1u}(y, \widetilde{U_1^*}) = y h'_{1u}(\widetilde{U_1^*}') \oplus h_{1u}^{(0)}(\widetilde{U_1^*}^{(0)})$, $h_{1u}^{(0)}(\widetilde{U_1^*}^{(0)}) = h_{1u}(0, \widetilde{U_1^*})$.

Теперь из второго сравнения получаем равенство подпространств $\widetilde{V_1^*}' = \widetilde{U_1^*}'$. С другой стороны, в первом равенстве в правой части содержится произведение переменной x_{t+1} на функцию h'_{1u}, зависящую от переменных из множества $\widetilde{U_1^*}'$, а в левой части переменная x_{t+1} может входить только во второе слагаемое, зависящее от переменных $x_{t+1}, \ldots, x_n$. Но это может быть только в том случае, когда $\widetilde{U_1^*}'$ — пустое множество, а переменная x_1 является линейным слагаемым. Получаем противоречие с тем, что по условию x_1 является существенной переменной по модулю $\mathcal{U}_s$ при $s \geqslant 2$. ■

Теорема 3. Если при $s \geqslant 2$ функция $f = f(x_1, \ldots, x_n)$ имеет тривиальную группу инерции $(\mathbf{H}_n)_f^{(s-1)}$ и линейно разложима в бесповторную сумму по модулю $\mathcal{U}_s$, то для этой функции найдётся однозначно определённое линейное разложение по модулю $\mathcal{U}_s$ в бесповторную сумму линейно неразложимых (в бесповторную сумму) слагаемых в том смысле, что любое другое такое разложение соответствует тому же самому разложению пространства в сумму подпространств, а соответствующие функции сравнимы по модулю $\mathcal{U}_s$.

Доказательство. Предположим, что имеется два разложения

$$f(V^*) \equiv f_1(V_1^*) \oplus f_2(V_2^*) \oplus \ldots \oplus f_m(V_m^*) \pmod{\mathcal{U}_s}, \quad m \geqslant 2,$$
$$f(V^*) \equiv h_1(U_1^*) \oplus h_2(U_2^*) \oplus \ldots \oplus h_l(U_l^*) \pmod{\mathcal{U}_s}, \quad l \geqslant 2,$$

в которых функции f_i и h_j линейно неразложимы в бесповторную сумму по модулю $\mathcal{U}_s$, $i = 1, \ldots, m$, $j = 1, \ldots, l$. Если разложения пространства

$$V^* = V_1^* + V_2^* + \ldots + V_m^* = U_1^* + U_2^* + \ldots + U_l^*$$

различны и не получаются одно из другого перенумерацией подпространств, то найдётся нетривиальное пересечение $V_i^* \cap U_j^*$ при некоторых i, j, и с помощью леммы 1 получаем противоречие с линейной неразложимостью функций f_i и h_j в бесповторную сумму по модулю $\mathcal{U}_s$, $i = 1, \ldots, m$, $j = 1, \ldots, l$. Поэтому разбиения пространства совпадают, а соответствующие функции сравнимы по модулю $\mathcal{U}_s$. ■

В качестве следствия получаем описание группы инерции таких функций в полной аффинной группе.

Следствие 1. Если в условиях теоремы 3 функция f представлена в виде суммы линейно неразложимых в бесповторную сумму по модулю $\mathcal{U}_s$ функций

$$f \equiv f_1 \oplus \ldots \oplus f_m \pmod{\mathcal{U}_s},$$

причём множество функций $\{f_1, \ldots, f_m\}$ разбивается на t классов аффинной эквивалентности по модулю $\mathcal{U}_s$: $\{f_{\mu_1}, \ldots, f_{\mu_p}\} \in \mathcal{F}_{n_1}, \ldots, \{f_{\nu_1}, \ldots, f_{\nu_q}\} \in \mathcal{F}_{n_t}$, то для группы инерции бесповторной суммы этих функций справедлив изоморфизм

$$\mathbf{AGL}\,(n,2)^{(s)}_{f_1 \oplus \ldots \oplus f_m} \cong [\mathbf{AGL}\,(n_1,2)^{(s)}_{f_{\mu_1}}]\mathbf{S}_p \times \ldots \times [\mathbf{AGL}\,(n_t,2)^{(s)}_{f_{\nu_1}}]\mathbf{S}_q.$$

Аналогичное описание справедливо для группы $\mathbf{GL}\,(n,2)$.

2. Бесповторное произведение функций

Как и в случае слагаемых первой степени, у функции необходимо сначала выделить аффинные сомножители. Говорят, что *функция f имеет аффинный сомножитель по модулю $\mathcal{U}_s$*, $-1 \leqslant s \leqslant n-1$, если найдутся такие функция $l(x) = (x, a^*) \oplus b$, $0 \neq a^* \in V^*$, $b \in V$, и функция h, что $f \equiv lh \pmod{\mathcal{U}_s}$. Приведём простейшие свойства таких функций.

Лемма 2. Пусть аффинная функция $l(x) = (x, a^*) \oplus b$ отлична от константы. Следующие условия равносильны:

(а) f имеет аффинный сомножитель l по модулю $\mathcal{U}_s$;
(б) $lf \equiv f \pmod{\mathcal{U}_{s+1}}$;
(в) $\overline{l}f \equiv 0 \pmod{\mathcal{U}_{s+1}}$.

Доказательство. Импликации (а) $\Rightarrow$ (б) и (б) $\Leftrightarrow$ (в) очевидны. Докажем (б) $\Rightarrow$ (а). Пусть $l(x) = (x, e^*) \oplus b$, $b \in \{0, 1\}$. Вектор e^* должен принадлежать пространству существенных переменных функции f, иначе $\deg lf = \deg f + 1$. Поэтому достаточно рассмотреть случай $l(x_1, \ldots, x_n) = x_1 \oplus b = x_1^{1-b}$. Разложим функцию f по первой переменной:

$$f(x_1, x_2, \ldots, x_n) = \overline{x}_1 f^{(0)}(x_2, \ldots, x_n) \oplus x_1 f^{(1)}(x_2, \ldots, x_n).$$

Условие $lf \overset{s+1}{\equiv} f$ имеет вид $x_1^{1-b} f^{(1-b)} \overset{s+1}{\equiv} \overline{x}_1 f^{(0)} \oplus x_1 f^{(1)}$, что эквивалентно $f^{(b)} \in \mathcal{U}_s$, откуда

$$f = \overline{x}_1 f^{(0)} \oplus x_1 f^{(1)} = x_1^{1-b} f^{(1-b)} \oplus x_1^b f^{(b)} =$$
$$= x_1^{1-b}(f^{(0)} \oplus f^{(1)}) \oplus f^{(b)} \equiv x_1^{1-b}(f^{(0)} \oplus f^{(1)}) \pmod{\mathcal{U}_s}.$$

Следствие доказано. ■

Следствие 2. Если $\deg f = k$, то f не имеет аффинных сомножителей по модулю $\mathcal{U}_{k-1}$ в том и только в том случае, когда $(x, e^*)f \not\equiv 0 (\bmod \mathcal{U}_k)$ при всех $0 \neq e^* \in V^*$, или, что то же самое, $\deg (x, e^*)f = k + 1$.

Доказательство. Если $(x, e^*) \oplus b$ — аффинный сомножитель по модулю $\mathcal{U}_{k-1}$, то $[(x, e^*) \oplus b]f \equiv f \pmod{\mathcal{U}_k}$, откуда $(x, e^*)f \equiv 0 \pmod{\mathcal{U}_k}$. С другой стороны, если $(x, e^*)f \equiv 0 \pmod{\mathcal{U}_k}$ при некотором $0 \neq e^* \in V^*$, то $[(x, e^*) \oplus 1]f \equiv f \pmod{\mathcal{U}_k}$ и поэтому $(x, e^*) \oplus 1$ — аффинный сомножитель по модулю $\mathcal{U}_{k-1}$. ■

Лемма 3. Пусть разложение функции f по первой переменной имеет вид

$$f(x_1, x_2, \ldots, x_n) = \overline{x}_1 f^{(0)}(x_2, \ldots, x_n) \oplus x_1 f^{(1)}(x_2, \ldots, x_n)$$

и $-1 \leqslant s \leqslant \deg f - 2$. Тогда f не имеет аффинных сомножителей по модулю $\mathcal{U}_s$ в том и только в том случае, когда функции $f^{(0)}, f^{(1)}$ не принадлежат $\mathcal{U}_{s-1}$ и не имеют аффинных сомножителей по модулю $\mathcal{U}_{s-1}$ с одинаковой линейной частью.

Доказательство. Пусть $e^1, \ldots, e^n$ — базис пространства V и $e^{*1}, \ldots, e^{*n}$ — сопряжённый базис. Рассмотрим разложение функции f по первой переменной $f = \overline{x}_1 f^{(0)} \oplus$ $\oplus\, x_1 f^{(1)}$, где $f_e^{(0)}(x_2, \ldots, x_n) = f_e(0, x_2, \ldots, x_n)$, $f_e^{(1)}(x_2, \ldots, x_n) = f_e(1, x_2, \ldots, x_n)$. Можно считать, что функции $f^{(0)}$ и $f^{(1)}$ заданы на пространстве $U = \langle e^2, \ldots, e^n \rangle = \langle e^{*1} \rangle^{\perp}$, поэтому

$$f = \overline{x}_1 f^{(0)}(U^*) \oplus x_1 f^{(1)}(U^*),$$

где $U^* = \langle e^{*2}, \ldots, e^{*n} \rangle$.

Пусть $(x, e^*) \oplus b \neq 0$ — аффинный сомножитель функции f по модулю $\mathcal{U}_s$, $e^* \in V^*$, $b \in \{0, 1\}$. Если векторы e^{*1} и e^* совпадают, то $((x, e^*) \oplus b) = x_1^{1-b}$ и

$$((x, e^*) \oplus b)f = x_1^{1-b}(\overline{x}_1 f^{(0)} \oplus x_1 f^{(1)}) = x_1^{1-b} f^{(1-b)} \equiv f \pmod{\mathcal{U}_{s+1}},$$

откуда $f^{(b)} \in \mathcal{U}_s$. Если же векторы e^{*1} и e^* линейно независимы, то либо $e^* = e^{*1} + u^*$, $u^* \in U^*$, либо $e^* = u^* \in U^*$. Можно полагать, что $u^* = e^{*2}$. В первом случае имеем $(x, e^*) = x_1 \oplus x_2$ и $(x_1 \oplus x_2 \oplus b)f = \overline{x}_1 x_2^{1-b} f^{(0)}(U^*) \oplus x_1 x_2^b f^{(1)}(U^*) \equiv f \pmod{\mathcal{U}_{s+1}}$, откуда $x_2^{1-b} f^{(0)} = f^{(0)} \pmod{\mathcal{U}_s}$ и $x^b f^{(1)} = f^{(1)} \pmod{\mathcal{U}_s}$.

Во втором случае $((x, e^*) \oplus b) = x_2^{1-b}$ и

$$((x, e^*) \oplus b)f = x_2^{1-b}(\overline{x}_1 f^{(0)} \oplus x_1 f^{(1)}) = \overline{x}_1 x_2^{1-b} f^{(0)} \oplus x_1 x_2^{1-b} f^{(1)} \equiv f \pmod{\mathcal{U}_{s+1}}.$$

Отсюда $x_2^{1-b} f^{(i)} \equiv f^{(i)} \pmod{\mathcal{U}_s}$, $i = 1, 2$. Поэтому $(x, e^*) \oplus b$ — аффинный сомножитель обеих функций $f^{(0)}$ и $f^{(1)}$ по модулю $\mathcal{U}_{s-1}$.

Обратное утверждение очевидно. ■

Пусть $\mathcal{N}L_s \subset \mathcal{F}_n$ — подмножество функций, не имеющих аффинных сомножителей по модулю $\mathcal{U}_s$, $s \geqslant -1$. Легко видеть, что справедливы включения

$$\mathcal{N}L_{-1} \supset \mathcal{N}L_0 \supset \mathcal{N}L_1 \supset \cdots \supset \mathcal{N}L_{n-2} = \varnothing.$$

Следствие 3. Если в условиях леммы 3 $f^{(0)}, f^{(1)} \notin \mathcal{U}_{s-1}$ и $f^{(0)}, f^{(1)} \in \mathcal{N}L_{s-1}^{(n-1)}$, то $f \in \mathcal{N}L_s^{(n)}$.

Если функция f имеет k аффинных сомножителей по модулю $\mathcal{U}_s$

$$l_i(x) = (x, a^{*i}) \oplus b_i,$$

где $a^{*i} \in V_n^*$ линейно независимы, $b_i \in \{0,1\}$, $i = 1, \ldots, k$, $k \geqslant 1$, но не имеет $k+1$ таких сомножителей, то будем говорить, что она *имеет ровно k аффинных сомножителей по модулю $\mathcal{U}_s$*. Доказательство следующей леммы очевидно.

Лемма 4. Пусть $k \geqslant 1$ и $s \leqslant \deg f - 1$. Тогда следующие условия эквивалентны:

а) f имеет ровно k аффинных сомножителей по модулю $\mathcal{U}_s$;

б) при некоторой линейной замене переменных с матрицей A функция f удовлетворяет условию $f(xA) \equiv x_1^{b_1} \ldots x_k^{b_k} h(x_{k+1}, \ldots, x_n) (\mathrm{mod}\ \mathcal{U}_s)$, где $b_i \in \{0,1\}$, $i = 1, \ldots, k$, и h не имеет аффинных сомножителей по модулю $\mathcal{U}_{s-k}$.

В условиях леммы 4 с функцией f однозначно связаны также два подпространства: *подпространство аффинных сомножителей* $L_1^* = \langle e^{*1}, \ldots, e^{*k} \rangle \leqslant V^*$ и двойственное к нему подпространство $(L_1^*)^\perp \subseteq V$, первое из которых является инвариантным относительно линейных преобразований из группы $G = \mathrm{Pr}_{\mathbf{GL}(n,2)} \mathbf{AGL}(n,2)_f^{(s)}$, а второе — относительно группы $G^* = \{A : (A^t)^{-1} \in G\}$. Описание групп инерции таких функций в полной линейной и аффинной группах приведено в [1]. Поэтому далее будем предполагать, что функция раскладывается в произведение нелинейных сомножителей.

Заметим, что для случая точного равенства функций (случай $s = -1$) разложение двоичной функции в бесповторное произведение нелинейных неразложимых сомножителей изучалось в работе [5], где показана однозначность такого разложения с точностью до перестановки эквивалентных сомножителей.

Приведём результаты, позволяющие в некоторых случаях описывать группы инерции функций для случая сравнения функций по модулю $\mathcal{U}_s$ при $s \geqslant 0$ для произведения функций без аффинных сомножителей. С их помощью можно, в частности, описывать группы инерции в обобщённых группах для бесповторных произведений квадратичных форм. В основе применяемого подхода лежит изучение структуры множества векторов, производные по направлению по которым имеют аффинные сомножители.

Лемма 5. Пусть $f(x) \equiv f_1(x^1) f_2(x^2) \ (\mathrm{mod}\, \mathcal{U}_{k-1})$, $\deg f = k$, $\deg f_i = k_i > 1$, $x^i = (x_{i_1}, \ldots, x_{i_{n_i}})$, $x = (x^1, x^2)$, $i = 1, 2$. Обозначим через V_i пространство $V_i = \{e^{i_1}, \ldots, e^{i_{n_i}}\}$, $i = 1, 2$, $V = V_1 \oplus V_2$, $V_1 \cup V_2 = \{0\}$. Тогда

1) для всех $a = (a^1, a^2)$, $a^i \in V_i$, $i = 1, 2$, выполняется сравнение

$$\Delta_a f \equiv (\Delta_{a^1} f_1) f_2 \oplus (\Delta_{a^2} f_2) f_1 \ (\mathrm{mod}\, \mathcal{U}_{k-2});$$

2) f имеет линейные сомножители по модулю $\mathcal{U}_{k-1}$ в том и только в том случае, когда при некотором i, $i \in \{1, 2\}$, функция f_i имеет линейные сомножители по модулю $\mathcal{U}_{k_i - 1}$.

Доказательство. Первое утверждение леммы вытекает из равенства

$$\Delta_a f(x) = (\Delta_{a^1} f_1)(x^1) f_2(x^2) \oplus (\Delta_{a^2} f_2)(x^2) f_1(x^1 \oplus a^1).$$

Докажем второе утверждение. Пусть функция f имеет линейный сомножитель по модулю $\mathcal{U}_{k-1}$: $(x, l^{*1} \oplus l^{*2}) f(x) \in \mathcal{U}_k$, где $l^{*i} \in V_i^*$, $i = 1, 2$. Тогда

$$(x, l^{*1}) f_1(x^1) f_2(x^2) \oplus f_1(x^1)(x, l^{*2}) f_2(x^2) \in \mathcal{U}_k.$$

Отсюда $(x, l^{*i}) f_i(x^i) \in \mathcal{U}_{k_i}$, $i = 1, 2$. ■

Пусть $L_s(f)$ — множество векторов $a \in V$, таких, что $\Delta_a f$ имеет аффинные сомножители по модулю $\mathcal{U}_s$, $-1 \leqslant s \leqslant \deg f - 1$. Очевидны включения

$$V = L_{\deg f-1} \supset L_{\deg f-2} \supset \cdots \supset L_0 \supset L_{-1}.$$

Лемма 6. Пусть выполняется условие леммы 5. Если, кроме того, при $i = 1, 2$ $f_i \in \mathcal{N}L_{k_i-1}$ и $|(\mathbf{H}_n)_{f_i}^{(k_i-2)}| = 1$, то $L_{k-2}(f) = L_{k_1-2}(f_1) \cup L_{k_2-2}(f_2)$.

Доказательство. Достаточно проверить только включение

$$L_{k-2}(f) \subseteq L_{k_1-2}(f_1) \cup L_{k_2-2}(f_2).$$

Предположим, что при некотором $a \in V$ функция $\Delta_a f$ имеет аффинный сомножитель по модулю $\mathcal{U}_{k-2}$. Тогда по следствию 2 при некотором $0 \neq e^* \in V^*$

$$(x, e^*)\Delta_a f(x) \equiv 0 \pmod{\mathcal{U}_{k-1}}.$$

Пусть $a = a^1 \oplus a^2$, $a^i \in V_{n_i}$, $a^1 \neq 0$, $i = 1, 2$. Если $e^* = e^{*1} \oplus e^{*2}$, $e^{*i} \in V_{n_i}$, $i = 1, 2$, то предыдущее сравнение принимает вид

$$(x, e^{*1} \oplus e^{*2})(\Delta_{a^1} f_1 \cdot f_2 \oplus \Delta_{a_2} f_2 \cdot f_1) \equiv 0 \pmod{\mathcal{U}_{k-1}}.$$

Раскрывая скобки, получаем

$$(x, e^{*1})\Delta_{a^1} f_1 \cdot f_2 \oplus (x, e^{*1}) f_1 \cdot \Delta_{a^2} f_2 \oplus \Delta_{a^1} f_1 \cdot (x, e^{*2}) f_2 \oplus f_1 \cdot (x, e^{*2})\Delta_{a^2} f_2 \equiv 0 \pmod{\mathcal{U}_{k-1}}.$$

Одночлены степени $k = k_1 + k_2$, в которых имеется $k_1 - 1$ переменных из первого множества и $k_2 + 1$ переменных из второго множества, могут появиться только из слагаемого $\Delta_{a^1} f_1 \cdot (x, e^{*2}) f_2$. Так как $|(\mathbf{H}_{n_1})_{f_1}^{(k_1-2)}| = 1$, то $\deg \Delta_{a^1} f_1 = k_1 - 1$, откуда $(x, e^{*2}) f_2 \in \mathcal{U}_{k_2}$. С другой стороны, функция f_2 не имеет линейных сомножителей по модулю $\mathcal{U}_{k_2-1}$. Поэтому в силу следствия 2 должно быть $e^{*2} = 0$ и $e^* = e^{*1} \neq 0$. Аналогично из второго слагаемого получаем $a^2 = 0$ и $a = a^1 \in L_{k_1-2}(f_1)$. ■

Теорема 4. Пусть выполнено сравнение

$$f(x) \equiv f_1(x^1) \cdots f_m(x^m) \pmod{\mathcal{U}_{k-1}},$$

где $\deg f = k$, $\deg f_i = k_i > 1$, $x^i = (x_{i_1}, \ldots, x_{i_{n_i}})$, $x = (x^1, \ldots, x^m)$, $|(\mathbf{H}_n)_{f_i}^{(k_i-2)}| = 1$, $i = 1, \ldots, m$, причём m — максимальное число с таким свойством среди всех функций, получающихся из f линейной заменой переменных. Обозначим через V_i подпространство $V_i = \{e^{i_1}, \ldots, e^{i_{n_i}}\}$, $i = 1, \ldots, m$, $V = V_1 \oplus \ldots \oplus V_m$. Тогда если $f_i \in \mathcal{N}L_{k_i-1}$ и $\langle L_{k_i-2}(f_i)\rangle = V_i$, $i = 1, \ldots, m$, то группа $\mathrm{Pr}_{\mathbf{GL}(n,2)}(\mathbf{AGL}(n, 2))_f^{(k-1)}$ сохраняет разложение $V = V_1 \oplus \ldots \oplus V_m$ в прямую сумму подпространств.

Доказательство. Из леммы 6 следует, что справедливо разложение

$$L_{k-2}(f) = L_{k_1-2}(f_1) \cup \ldots \cup L_{k_m-2}(f_m).$$

Пусть $L_{k_i-2}(f_i) = M_{i,1} \cup \ldots \cup M_{i,t_i}$ — максимальное разбиение, удовлетворяющее условию $\langle L_{k_i-2}(f_i)\rangle = \langle M_{i,1}\rangle \oplus \ldots \oplus \langle M_{i,t_i}\rangle$, $t_i \geqslant 1$, $i = 1, \ldots, m$. Тогда разбиение

$$L_{k-2}(f) = \bigcup_{i=1}^{m} \bigcup_{j=1}^{t_i} M_{i,j}$$

также удовлетворяет условию утверждения 1. Поэтому группа $\mathrm{Pr}_{\mathbf{GL}\,(n,2)}(\mathbf{AGL}\,(n,2))_f^{(k-1)}$ должна сохранять разложение $V = \bigcup\limits_{i=1}^{m}\bigcup\limits_{j=1}^{t_i} V_{i,j}$, где $V_{i,j} = \langle M_{i,j}\rangle$, $i = 1,\ldots,m$, $j = 1,\ldots,t_i$.

Составим базис пространства V из базисов подпространств $V_{i,j}$, $i = 1,\ldots,m$, $j = 1,\ldots,t_i$. Тогда, сравнивая старшие члены в многочленах Жегалкина у функций $h(x) = f(xC)$, где C — матрица линейного преобразования, соответствующего переходу к этому базису, и $h(xQ)$ при $Q \in \mathbf{AGL}\,(n,2)_h^{(k-1)}$, получим, что $\mathrm{Pr}_{\mathbf{GL}\,(n,2)}\mathbf{AGL}\,(n,2)_h^{(k-1)}$, а следовательно, и группа $\mathrm{Pr}_{\mathbf{GL}(n,2)}\mathbf{AGL}\,(n,2)_f^{(k-1)}$ должны сохранять разложение в прямую сумму подпространств $V = V_1 \oplus \ldots \oplus V_m$, что и доказывает теорему. ■

Следствие 4. Если в условиях теоремы 4 множество функций $\{f_1,\ldots,f_m\}$ при некотором $s \geqslant 1$ разбивается на классы $\mathbf{AGL}\,(n,2)\mathcal{U}_{k_i-s}$-эквивалентности $\{f_{\mu_1},\ldots,f_{\mu_p}\}$, …, $\{f_{\nu_1},\ldots,f_{\nu_q}\}$, то

$$\mathbf{AGL}\,(n,2)_f^{(k-s)} \cong \left[\mathbf{AGL}\,(n_{\mu_1},2)_{f_{\mu_1}}^{(k_{\mu_1}-s)}\right]\mathbf{S}_p \times \cdots \times \left[\mathbf{AGL}\,(n_{\nu_1},2)_{f_{\nu_1}}^{(k_{\nu_1}-s)}\right]\mathbf{S}_q.$$

При $s = 1$ утверждение теоремы вытекает из теоремы 4. При $s > 1$ оно вытекает из того факта, что группа $\mathbf{AGL}\,(n,2)_f^{(k-s)}$ является подгруппой группы $\mathbf{AGL}\,(n,2)_f^{(k-1)}$.

Следствие 5. Если в условиях теоремы 4 функции f_i являются невырожденными квадратичными формами ранга $2r_i \geqslant 4$, $i = 1,\ldots,m$, причём при некотором s, $1 \leqslant s \leqslant 3$, множество функций $\{f_1,\ldots,f_m\}$ разбивается на классы $\mathbf{AGL}\,(n,2)\mathcal{U}_{2-s}$-эквивалентности $\{f_{\mu_1},\ldots,f_{\mu_p}\},\ldots,\{f_{\nu_1},\ldots,f_{\nu_q}\}$, то

$$\mathbf{AGL}\,(n,2)_f^{(2m-s)} \cong \left[\mathbf{AGL}\,(n_{\mu_1},2)_{f_{\mu_1}}^{(2-s)}\right]\mathbf{S}_p \times \cdots \times \left[\mathbf{AGL}\,(n_{\nu_1},2)_{f_{\nu_1}}^{(2-s)}\right]\mathbf{S}_q.$$

Доказательство. Квадратичные формы невырождены, если число переменных совпадает со значением ранга. Поскольку невырожденные квадратичные формы f_i ранга $2r_i \geqslant 4$, $i = 1,\ldots,m$, удовлетворяют условию теоремы 4, то для доказательства достаточно показать, что m — максимальное число сомножителей среди всех разложений функции f, полученных при различных линейных заменах переменных.

Предположим, что это не так. Тогда у функции f есть линейные сомножители по модулю $\mathcal{U}_{2m-1}$. Но в силу леммы 5 из условия $f_i \in \mathcal{N}L_1$, $i = 1,\ldots,m$, вытекает $f \in \mathcal{N}L_{2m-1}$. ■

Следствие 6. Пусть выполняются условия теоремы 4 и функции f_i являются квадратичными формами ранга $2r_i \geqslant 4$, $i = 1,\ldots,m$, причём все они имеют тривиальные группы инерции в группе $\mathbf{H}_{n_i}$, где n_i — число переменных формы f_i, $i = 1,\ldots,m$. Тогда если при некотором s, $2 \leqslant s \leqslant 3$, множество форм $\{f_1,\ldots,f_m\}$ разбивается на классы $\mathbf{AGL}\,(n,2)\mathcal{U}_{2-s}$-эквивалентности $\{f_{\mu_1},\ldots,f_{\mu_p}\},\ldots,\{f_{\nu_1},\ldots,f_{\nu_q}\}$, то

$$\mathbf{AGL}\,(n,2)_f^{(2m-s)} \cong \left[\mathbf{AGL}\,(n_{\mu_1},2)_{f_{\mu_1}}^{(2-s)}\right]\mathbf{S}_p \times \cdots \times \left[\mathbf{AGL}\,(n_{\nu_1},2)_{f_{\nu_1}}^{(2-s)}\right]\mathbf{S}_q.$$

Доказательство. Если все квадратичные формы невырождены, то утверждение вытекает из предыдущего следствия.

Рассмотрим теперь случай, когда некоторые квадратичные формы могут быть вырожденными. Пусть это $f_{t+1},\ldots,f_m$. С учётом классификации квадратичных форм

достаточно рассмотреть случай, когда ранг квадратичной формы на единицу меньше числа переменных, т. е. можно полагать, что

$$f_i(x_{i,1},\dots,x_{i,n_i}) = x_{i,1}x_{i,2} \oplus \dots \oplus x_{i,n_i-2}x_{i,n_i-1} \oplus x_{i,n_i},$$

$n_i = 2r_i + 1 = m_i + 1$, $i = t+1,\dots,m$. Если ввести обозначение

$$f_i(x_{i,1},\dots,x_{i,n_i}) = h_i(x_{i,1},\dots,x_{i,n_i-1}) \oplus x_{i,n_i},$$

то функции h_i — невырожденные квадратичные формы, $i = t+1,\dots,m$. Пусть

$$f(x) = f_1(x^1)\dots f_m(x^m), \qquad f'(x) = f_1\dots f_t h_t\dots h_m.$$

Так как $f \equiv f' \pmod{\mathcal{U}_{2m-1}}$, переменные $x_{i,n_{t+1}},\dots,x_{i,n_m}$ являются несущественными по модулю $\mathcal{U}_{2m-1}$. Поэтому у всякого аффинного преобразования (Q,b), такого, что

$$(Q,b) \in \mathbf{AGL}\,(n,2)_f^{(2m-s)} \subseteq \mathbf{AGL}\,(n,2)_f^{(2m-1)},$$

матрица Q после перенумерации переменных может быть приведена к виду

$$Q = \begin{pmatrix} \mathrm{A} & \mathrm{B} \\ 0 & \mathrm{C} \end{pmatrix},$$

где C — $n\times n$-матрица, $(A,b^1) \in \mathbf{AGL}\,(n-(m-t),2)_{f'}^{(2m-1)}$, $b = (b^1,b^2)$. В силу теоремы 4 получаем, что преобразование (A,b^1) должно переставлять между собой функции $f_1,\dots,f_t,h_{t+1},\dots,h_m$.

Далее, не уменьшая общности, можно полагать, что преобразование (A,b^1) не изменяет порядка следования функций $f_1,\dots,f_t$, $h_{t+1},\dots,h_m$. Покажем, что преобразование (Q,b) также оставляет на месте функции $f_1,\dots,f_m$. Имеем

$$f(x) \equiv f_1\dots f_t h_{t+1}\dots h_m \oplus \sum_{i=t+1}^{n} x_{i,n_i} f_1\dots f_t h_{t+1}\dots h_{i-1}h_{i+1}\dots h_m \pmod{\mathcal{U}_{2m-2}}.$$

Тогда из сравнения $f(x) \equiv f(xQ\oplus b)) \pmod{\mathcal{U}_s}$ вытекает, что

$$\sum_{i=t+1}^{n} (l_{i,n_i}(x) \oplus x_{i,n_i}) f_1\dots f_t h_{t+1}\dots h_{i-1}h_{i+1}\dots h_m \equiv 0 \pmod{\mathcal{U}_{2m-2}}, \tag{4}$$

где $l_{i,n_i}(x)$ — линейная функция, описывающая координату с номером n_i вектора $xQ\oplus b$, $i = t+1,\dots,m$.

Пусть $l_{i,n_i}(x) = l'_{i,n_i}(x)\oplus l''_{i,n_i}(x)$, где $l'_{i,n_i}(x)$ — часть слагаемых функции $l_{i,n_i}(x)$, которая зависит от переменных $x_{i,j}$, $1 \leqslant j \leqslant n_i$, относящихся к функции h_i, $i = t+1,\dots,m$, а $l''_{i,n_i}(x)$ — от оставшихся переменных. Из вида слагаемых в правой части сравнения (4) следует, что при каждом $i = t+1,\dots,m$ после умножения $l''_{i,n_i}(x)$ на произведение $f_1\dots f_t h_{t+1}\dots h_{i-1}h_{i+1}\dots h_m$ в качестве ненулевых слагаемых в сравнении получаются только одночлены, не содержащие ни одной переменной $x_{i,j}$, $1 \leqslant j \leqslant n_i$, но содержащие произведения более трёх переменных других функций. Такие одночлены могут встретиться только в i-м слагаемом суммы из сравнения (4) и, следовательно, не могут ни с чем сократиться. Поэтому при каждом $i = t+1,\dots,m$ должно выполняться сравнение

$$l''_{i,n_i}(x) f_1\dots f_t h_{t+1}\dots h_{i-1}h_{i+1}\dots h_m \equiv 0 \pmod{\mathcal{U}_{2m-2}}.$$

Поскольку функции $f_1,\dots,f_t,h_{t+1},\dots,h_m$ по условию не имеют линейных сомножителей, должны выполняться равенства $l''_{i,n_i}(x) = 0$, $i = t+1,\dots,m$, что означает равенство нулю элементов подматрицы B матрицы Q. ■

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
2. *Dixon L. E.* Linear Groups with Exposition Galois Field Theory. Leipzig, 1901; 2nd ed.: N.Y.: Dover Publications, 1958.
3. *Черемушкин А. В.* Условие однозначности разложения двоичной функции в бесповторную сумму функций при линейной замене переменных // Прикладная дискретная математика. Приложение. 2017. № 10. С. 55–56.
4. *Черемушкин А. В.* К вопросу о линейной декомпозиции двоичных функций // Прикладная дискретная математика. 2016. № 1(31). С. 46–56.
5. *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. *Dixon L. E.* Linear Groups with Exposition Galois Field Theory. Leipzig, 1901; 2nd ed.: N.Y., Dover Publications, 1958.
3. *Cheremushkin A. V.* Uslovie odnoznachnosti razlozheniya dvoichnoy funktsii v bespovtornuyu summu funktsiy pri lineynoy zamene peremennykh [A condition for uniqueness of linear decomposition of a Boolean function into disjunctive sum of indecomposable functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2017, no. 10, pp. 55–56. (in Russian)
4. *Cheremushkin A. V.* K voprosu o lineynoy dekompozitsii dvoichnykh funktsiy [On linear decomposition of Boolean functions]. Prikladnaya Diskretnaya Matematika, 2016, no. 1(31), pp. 46–56. (in Russian)
5. *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)