Math-Net.Ru

Общероссийский математический портал

М. И. Анохин, О расщепляемости p -ичных функций, *Матем. сб.*, 2007, том 198, номер 7, 31–44

DOI: <https://doi.org/10.4213/sm1529>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.147.182.235

26 апреля 2023 г., 16:28:16

УДК 512.642+519.712.43

М. И. Анохин

О расщепляемости p -ичных функций

Функция φ из n -мерного векторного пространства V над полем F из p элементов (где p – простое число) в поле F называется расщепляемой, если $\varphi(u+w) = \psi(u) + \chi(w)$, $u \in U$, $w \in W$, для некоторых ненулевых подпространств U и W таких, что $U \oplus W = V$, и некоторых функций $\psi: U \rightarrow F$ и $\chi: W \rightarrow F$. В работе показано, как за полиномиальное от $\log p^{p^n}$ время проверить, является ли такая функция расщепляемой, и если да, то найти некоторое ее представление указанного вида. Изучаются также некоторые другие вопросы, связанные с расщепляемостью функций.

Библиография: 3 названия.

§ 1. Введение

Пусть V – n -мерное векторное пространство над полем F из p элементов, где p – простое число. Функция $\varphi: V \rightarrow F$ называется *расщепляемой*, если существует разложение пространства V в прямую сумму ненулевых подпространств U и W такое, что $\varphi(u+w) = \psi(u) + \chi(w)$, $u \in U$, $w \in W$, для некоторых функций $\psi: U \rightarrow F$ и $\chi: W \rightarrow F$. Основная цель настоящей работы – найти необходимые и достаточные условия расщепляемости функций, проверяемые за полиномиальное от $\log p^{p^n}$ время. Это дает решение задачи 2.17 из [1] (поставленной в случае, когда $p = 2$). В случае расщепляемости заданной функции $\varphi: V \rightarrow F$ наши методы позволяют также найти вышеуказанное представление этой функции (т.е. соответствующие подпространства U и W и функции ψ и χ) за полиномиальное (от $\log p^{p^n}$) время. Кроме того, изучаются некоторые другие вопросы, связанные с расщепляемостью функций. Некоторые результаты настоящей работы были анонсированы в [2].

Материал распределен в работе следующим образом. Параграф 2 содержит основные определения, обозначения и факты, используемые в работе. В §3 вводится общее понятие ортогональности на вышеуказанном пространстве V и изучаются нужные нам свойства этого понятия, которое, возможно, представляет и самостоятельный интерес. В §4 с произвольной функцией $\varphi: V \rightarrow F$ связываются ортогональности ∇ и $\diamond$ на пространстве V , играющие важную роль в дальнейшем. Основным результатом этого параграфа является теорема 1, согласно которой для произвольного разложения пространства V в прямую сумму непустого множества $\mathfrak{S}$ его ненулевых подпространств функция $\varphi: V \rightarrow F$ представима в виде

$$\varphi\left(\sum_{U \in \mathfrak{S}} x_U\right) = \sum_{U \in \mathfrak{S}} \varphi_U(x_U) \quad (x_U \in U, \quad U \in \mathfrak{S}) \quad (1)$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (гранты №№ 05-01-01018, 07-01-00154).

(где φ_U – функция из U в F при всех $U \in \mathfrak{S}$), если и только если $U \nabla W$ для любых различных подпространств $U, W \in \mathfrak{S}$. В частности, φ расщепляема тогда и только тогда, когда V разлагается в прямую сумму двух ненулевых ∇ -ортогональных подпространств (следствие 1). Кроме того, теорема 1 утверждает, что в произвольном представлении вида (1) для любого $U \in \mathfrak{S}$, где $\mathfrak{S} \neq \emptyset$, функция φ_U с точностью до аддитивной константы совпадает с $\varphi|_U$. Таким образом, нахождение представления вида (1) для данной функции $\varphi: V \rightarrow F$ сводится к нахождению разложения пространства V в прямую сумму некоторого непустого множества его ненулевых подпространств, в котором любые два различных подпространства ∇ -ортогональны.

В § 5 дается критерий расщепляемости произвольной функции $\varphi: V \rightarrow F$, а также способ нахождения разложения пространства V в прямую сумму двух ненулевых ∇ -ортогональных подпространств, если эта расщепляемость имеет место. Проверка этого критерия и нахождение такого разложения по указанному способу могут быть выполнены за полиномиальное от $\log p^{p^n}$ время. Отметим, что в § 5 общий случай разбит на четыре взаимоисключающих подслучая, каждый из которых рассматривается отдельно. Наконец, в § 6 обсуждается вопрос о том, при каких условиях разложение пространства V в прямую сумму множества его ненулевых подпространств, в котором любые два различных подпространства ∇ -ортогональны и никакое из них не является прямой суммой двух ненулевых ∇ -ортогональных подпространств, единственно. Очевидно, что к таким условиям относится нерасщепляемость рассматриваемой функции φ . Кроме того, если $V^\diamond = \{0\}$, то теорема 3 утверждает единственность вышеуказанного разложения и дает простой полиномиальный (от $\log p^{p^n}$) алгоритм его нахождения по произвольной функции $\varphi: V \rightarrow F$. Отметим, что какие-либо удобные необходимые и достаточные условия единственности такого разложения автору неизвестны. Наконец, показано, что среди функций $\varphi: V \rightarrow F$ доля как нерасщепляемых функций, так и функций, для которых $V^\diamond = \{0\}$, экспоненциально стремится к 1 при $n \rightarrow \infty$ и фиксированном p (см. предложения 1 и 2). В частности, любое из приведенных выше достаточных условий единственности указанного разложения выполняется для почти всех функций $\varphi: V \rightarrow F$.

Автор благодарит О. А. Логачёва, А. А. Сальникова и В. В. Яценко за постановку задачи и полезные обсуждения.

§ 2. Определения, обозначения и необходимые факты

На протяжении всей работы через p обозначается некоторое простое число, через F – поле из p элементов, а через V – n -мерное векторное пространство над полем F , где n – целое неотрицательное число. Все объекты и понятия линейной алгебры рассматриваются над основным полем F . Если X – подмножество V , то $\langle X \rangle$ обозначает подпространство, порожденное множеством X . Как обычно, через V^* мы обозначаем сопряженное пространство для V (т.е. векторное пространство всех линейных отображений из V в F).

Под словами “разложение векторного пространства” понимается его разложение в сумму некоторого множества подпространств. Такие разложения

отождествляются с соответствующими множествами подпространств. Внутренняя прямая сумма подпространств будет обозначаться символом $\oplus$. Избегая введения лишних индексов, мы пишем $\bigcup \mathfrak{S}$, $\sum \mathfrak{S}$ и $\bigoplus \mathfrak{S}$ вместо $\bigcup_{S \in \mathfrak{S}} S$, $\sum_{S \in \mathfrak{S}} S$ и $\bigoplus_{S \in \mathfrak{S}} S$ соответственно.

Пусть S – некоторое множество. Если R – симметричное бинарное отношение на S , то $\Gamma(S, R)$ обозначает неориентированный граф (без петель и кратных ребер) с множеством вершин S , в котором две различные вершины s_1 и s_2 смежны тогда и только тогда, когда $s_1 R s_2$. Через F^S будет обозначаться множество всех функций из S в F . Это множество является векторным пространством относительно поточечных операций сложения и умножения на элементы из F . Элементы F будут иногда отождествляться с функциями-константами из F^S , если это не приводит к двусмысленности. Отметим, что символы $\subset$ и $\supset$ в настоящей работе обозначают строгие включения.

Говоря об алгоритмах, на вход которым подается произвольная функция $\varphi \in F^V$, мы подразумеваем, что поле F есть множество $\{0, \dots, p-1\}$ с арифметическими операциями по модулю p , пространство V задано для алгоритма p^n символами элементов и таблицей их сложения (умножение на элементы поля F сводится к сложению), а функция φ – таблицей своих значений. Полиномиальность такого алгоритма означает, что время его работы на произвольном входе $\varphi \in F^V$ не превосходит $O(\log^d p^{p^n}) = O((p^n \log p)^d)$ для некоторой положительной константы d , где $\log$ – логарифм по некоторому фиксированному основанию, большему 1. Кроме того, все алгоритмы, рассматриваемые в работе, детерминированы.

Для произвольного $a \in V$ определим отображение $D_a: F^V \rightarrow F^V$ следующим образом:

$$(D_a \varphi)(x) = \varphi(x + a) - \varphi(x), \quad \varphi \in F^V, \quad x \in V.$$

Функция $D_a \varphi$ называется *производной функции φ по направлению a* ; это понятие хорошо известно (см., например, [1; определение 2.68], [3; определение 3]). Следующая лемма доказывается непосредственно.

ЛЕММА 1. Пусть $a, b \in V$ и $\varphi \in F^V$. Тогда

- 1) D_a является линейным отображением пространства F^V в себя;
- 2) $D_a D_b = D_b D_a$;
- 3) $D_{a+b} = D_a + D_b + D_a D_b$;
- 4) $D_v \varphi = 0$ для всех $v \in V$, если и только если φ – константа.

§ 3. Ортогональности и их свойства

Назовем *ортогональностью* на V любое симметричное бинарное отношение $\perp$ на этом пространстве такое, что для любого $v \in V$ множество $\{a \in V \mid a \perp v\}$ является подпространством пространства V . Пусть $\perp$ – произвольная ортогональность. Тогда отношение $\perp$ естественно переносится с элементов на подмножества V :

$$A \perp B \iff a \perp b \text{ для всех } a \in A, b \in B,$$

где $A, B \subseteq V$. Для множества $A \subseteq V$ его $\perp$ -ортогональное дополнение $A^\perp$ определяется следующим равенством:

$$A^\perp = \{v \in V \mid v \perp a \text{ для всех } a \in A\}.$$

Очевидно, что $A^\perp$ является подпространством пространства V для произвольного множества $A \subseteq V$. Вместо $\{a\}^\perp \supseteq B$, $A \perp \{b\}$ и $\{a\}^\perp$, где $a, b \in V$, $A, B \subseteq V$, мы будем писать $a \perp B$, $A \perp b$ и $a^\perp$ соответственно. Сформулируем нужные нам свойства отношения $\perp$ в следующей лемме, проверяемой непосредственно.

ЛЕММА 2. Пусть $a, b \in V$, $A, B \subseteq V$ и $\mathfrak{S}$ – некоторое множество подмножеств V . Тогда

- 1) $a^\perp \cap b^\perp \subseteq (a + b)^\perp$;
- 2) если $A \subseteq B$, то $A^\perp \supseteq B^\perp$;
- 3) если $A \perp B$, то $\langle A \rangle^\perp \supseteq \langle B \rangle^\perp$;
- 4) $\bigcap_{S \in \mathfrak{S}} S^\perp = (\bigcup \mathfrak{S})^\perp = \langle \bigcup \mathfrak{S} \rangle^\perp = (\sum_{S \in \mathfrak{S}} \langle S \rangle)^\perp$.

ЛЕММА 3. Пусть V является суммой $\perp$ -ортогональных подпространств U и W . Тогда если $V^\perp = \{0\}$, то $U^\perp = W$, $W^\perp = U$ и $U \cap W = \{0\}$ (и, следовательно, $V = U \oplus W$).

ДОКАЗАТЕЛЬСТВО. Очевидно, что $W \subseteq U^\perp$. Пусть теперь v – произвольный элемент $U^\perp$. Представим v в виде $u + w$, где $u \in U$ и $w \in W$. Тогда $u \in U^\perp$ (так как $w \in U^\perp$) и $u \in W^\perp$. Поэтому $u \in U^\perp \cap W^\perp = V^\perp = \{0\}$ (ввиду леммы 2, 4)) и $v = w \in W$. Таким образом, $U^\perp = W$. Меняя местами U и W , получаем равенство $W^\perp = U$. Наконец, из двух последних равенств и леммы 2, 4) вытекает, что $U \cap W = W^\perp \cap U^\perp = V^\perp = \{0\}$. Лемма доказана.

Пусть $v \mapsto \bar{v}$, $v \in V$, – естественный гомоморфизм V на $V/V^\perp$. Тогда на $V/V^\perp = \bar{V}$ корректно определено бинарное отношение $\bar{\perp}$:

$$\bar{a} \bar{\perp} \bar{b} \iff a \perp b.$$

Легко видеть, что это отношение является ортогональностью на $\bar{V}$. Следующая лемма очевидна.

ЛЕММА 4. Для любого множества $A \subseteq V$ справедливо равенство $\overline{A^\perp} = \bar{A}^\perp$. В частности, $\bar{V}^\perp = \{0\}$.

Назовем элемент $v \in V$ $\perp$ -разложимым, если $v = v_1 + v_2$ для некоторых $v_1, v_2 \in V$ таких, что $v_i^\perp \supset v^\perp$ при $i = 1, 2$. В противном случае элемент пространства V будет называться $\perp$ -неразложимым. Обозначим множество всех ненулевых $\perp$ -неразложимых элементов пространства V через $I_\perp$.

ЛЕММА 5. Множество $I_\perp$ порождает пространство V .

ДОКАЗАТЕЛЬСТВО. Предположим, что множество $V \setminus \langle I_\perp \rangle$ непусто. Выберем некоторый элемент $v \in V \setminus \langle I_\perp \rangle$, для которого подпространство $v^\perp$ максимально в множестве $\{u^\perp \mid u \in V \setminus \langle I_\perp \rangle\}$. Очевидно, что v $\perp$ -разложим, т.е. $v = v_1 + v_2$ для некоторых $v_1, v_2 \in V$, удовлетворяющих условиям $v_i^\perp \supset v^\perp$ при $i = 1, 2$. Но тогда $v_1, v_2 \in \langle I_\perp \rangle$ (ввиду максимальной $v^\perp$ в вышеуказанном множестве) и $v \in \langle I_\perp \rangle$, что противоречит выбору v . Лемма доказана.

Разложение $V = \sum \mathfrak{S}$ пространства V в сумму подпространств из некоторого их множества $\mathfrak{S}$ мы называем *нетривиальным*, если $U \neq \{0\}$ для всех $U \in \mathfrak{S}$. Вышеуказанное разложение пространства V называется *$\perp$ -ортогональным*, если $U \perp W$ для любых различных $U, W \in \mathfrak{S}$. Нетривиальное $\perp$ -ортогональное разложение $V = \bigoplus \mathfrak{S}$ пространства V будет называться *полным $\perp$ -ортогональным* разложением, если для каждого $U \in \mathfrak{S}$ не существует нетривиального $\perp$ -ортогонального разложения подпространства U в прямую сумму двух подпространств.

В дальнейшем нам понадобится следующее условие на отношение $\perp$:

$$a^\perp + b^\perp = V \implies (a + b)^\perp = a^\perp \cap b^\perp, \quad (2)$$

где $a, b \in V$.

ЛЕММА 6. Пусть $V = \sum \mathfrak{S}$ есть $\perp$ -ортогональное разложение пространства V . Предположим, что отношение $\perp$ удовлетворяет условию (2). Тогда

$$V^\perp = \sum_{U \in \mathfrak{S}} (U \cap V^\perp).$$

ДОКАЗАТЕЛЬСТВО. Включение $\sum_{U \in \mathfrak{S}} (U \cap V^\perp) \subseteq V^\perp$ тривиально. Пусть теперь $v \in V^\perp$. Представим v в виде $\sum_{U \in \mathfrak{S}} z_U$, где $z_U \in U$ при всех $U \in \mathfrak{S}$. Выберем произвольное подпространство $U \in \mathfrak{S}$ и положим $b = \sum_{W \in \mathfrak{S} \setminus \{U\}} z_W$. Тогда $v = z_U + b$, где $z_U^\perp + b^\perp = V$. Поэтому $V = v^\perp = z_U^\perp \cap b^\perp \subseteq z_U^\perp$ (ввиду условия (2)) и $z_U^\perp = V$. Таким образом, $z_U \in U \cap V^\perp$ для любого $U \in \mathfrak{S}$ и, следовательно, $v \in \sum_{U \in \mathfrak{S}} (U \cap V^\perp)$. Лемма доказана.

ЛЕММА 7. Пусть $V = \sum \mathfrak{S}$ есть $\perp$ -ортогональное разложение пространства V . Предположим, что отношение $\perp$ удовлетворяет равенству $V^\perp = \{0\}$ и условию (2). Тогда $I_\perp \subseteq \bigcup \mathfrak{S}$.

ДОКАЗАТЕЛЬСТВО. Пусть v – произвольный элемент $I_\perp$. Представим v в виде $\sum_{U \in \mathfrak{T}} z_U$ для некоторого множества $\mathfrak{T} \subseteq \mathfrak{S}$, где $z_U \in U$ при всех $U \in \mathfrak{T}$. Не ограничивая общности, мы считаем, что $\sum_{U \in \mathfrak{T}_0} z_U \neq v$ для любого множества $\mathfrak{T}_0 \subset \mathfrak{T}$.

Предположим, что $|\mathfrak{T}| \geq 2$. Представим $\mathfrak{T}$ в виде объединения двух непустых непересекающихся подмножеств $\mathfrak{T}_1$ и $\mathfrak{T}_2$ и положим $v_i = \sum_{U \in \mathfrak{T}_i} z_U$ для $i = 1, 2$. Тогда $v = v_1 + v_2$, $v_1^\perp + v_2^\perp = V$ и $v^\perp = v_1^\perp \cap v_2^\perp \subseteq v_i^\perp$ при $i = 1, 2$. Поэтому ввиду $\perp$ -неразложимости v существует $j \in \{1, 2\}$, для которого $v_j^\perp = v^\perp$ и, следовательно, $v_{3-j}^\perp = V$. Последнее равенство означает, что $v_{3-j} \in V^\perp = \{0\}$. Но тогда $v = v_j = \sum_{U \in \mathfrak{T}_j} z_U$, что противоречит предположению, сделанному выше (так как $\mathfrak{T}_j \subset \mathfrak{T}$). Таким образом, $|\mathfrak{T}| \leq 1$. С другой стороны, $|\mathfrak{T}| \geq 1$, так как $v \neq 0$. Это показывает, что $\mathfrak{T} = \{W\}$ для некоторого $W \in \mathfrak{S}$ и $v = z_W \in W \subseteq \bigcup \mathfrak{S}$. Лемма доказана.

В следующей лемме через Δ обозначается некоторая ортогональность на V такая, что если $a \Delta b$, то $a \perp b$ для произвольных $a, b \in V$.

ЛЕММА 8. Пусть $V = \bigoplus \mathfrak{S}$ – полное Δ -ортогональное разложение пространства V . Предположим, что отношение $\perp$ удовлетворяет условию (2)

и $V^\perp = \{0\}$. Пусть также $\mathfrak{C}$ – множество всех связных компонент графа $\Gamma(I_\perp, \emptyset)$. Тогда отображение

$$C \mapsto \langle C \rangle, \quad C \in \mathfrak{C}, \quad (3)$$

является биекцией $\mathfrak{C}$ на $\mathfrak{S}$. В частности, такое разложение (т.е. соответствующее множество $\mathfrak{S}$) единственно.

ДОКАЗАТЕЛЬСТВО. Из леммы 7 вытекает, что $I_\perp = \bigcup_{U \in \mathfrak{S}} (I_\perp \cap U)$. Поэтому $V = \langle I_\perp \rangle = \bigoplus_{U \in \mathfrak{S}} \langle I_\perp \cap U \rangle$ (см. лемму 5) и, следовательно,

$$\langle I_\perp \cap U \rangle = U \quad \forall U \in \mathfrak{S}. \quad (4)$$

В частности, $I_\perp \cap U \neq \emptyset$ при всех $U \in \mathfrak{S}$. Очевидно также, что

$$(I_\perp \cap U) \cap (I_\perp \cap W) = \emptyset \quad \text{и} \quad I_\perp \cap U \triangle I_\perp \cap W$$

для любых различных $U, W \in \mathfrak{S}$. Предположим, что для некоторого $U \in \mathfrak{S}$ множество $I_\perp \cap U$ является объединением непустых непересекающихся Δ -ортогональных подмножеств A и B . Тогда $U = \langle I_\perp \cap U \rangle = \langle A \rangle + \langle B \rangle$ (см. (4)), где $\langle A \rangle \neq \{0\}$, $\langle B \rangle \neq \{0\}$ (так как A и B непусты и содержатся в $I_\perp$) и $\langle A \rangle \triangle \langle B \rangle$ (лемма 2, 3)). Кроме того,

$$\langle A \rangle \cap \langle B \rangle \subseteq \langle B \rangle^\perp \cap \langle A \rangle^\perp \cap \bigcap_{W \in \mathfrak{S} \setminus \{U\}} W^\perp = V^\perp = \{0\}$$

в силу леммы 2, 4). Таким образом, $U = \langle A \rangle \oplus \langle B \rangle$ – нетривиальное Δ -ортогональное разложение подпространства $U \in \mathfrak{S}$, что противоречит условию леммы.

Итак, мы показали, что отображение

$$U \mapsto I_\perp \cap U, \quad U \in \mathfrak{S}, \quad (5)$$

является биекцией $\mathfrak{S}$ на $\mathfrak{C}$. Кроме того, композиция отображений (5) и (3) (в этом порядке) является тождественным отображением множества $\mathfrak{S}$ (ввиду (4)). Поэтому отображение (3) является биекцией $\mathfrak{C}$ на $\mathfrak{S}$, а именно, обратным отображением к биекции (5). Лемма доказана.

§ 4. Связь расщепляемости функций с некоторой ортогональностью

Фиксируем произвольную функцию $\varphi \in F^V$. Определим следующие бинарные отношения на пространстве V :

$$\begin{aligned} a \nabla b &\iff D_a D_b \varphi = 0, \\ a \diamond b &\iff D_a D_b \varphi \text{ – константа.} \end{aligned}$$

Из леммы 1 вытекает, что эти отношения являются ортогональностями на V . Разумеется, данные ортогональности зависят от функции φ , но мы не будем явно указывать их связь с этой функцией, так как последняя всегда предполагается фиксированной. Отметим, что в терминологии книги [1] (при $p = 2$) пространство $V^\diamond$ называется пространством 1-нелинейности функции φ , а V^∇ –

подпространством линейности, пространством линейных трансляторов (линейных структур) или пространством 0-нелинейности функции φ .

Для произвольных $\diamond$ -ортогональных элементов $u, v \in V$ положим $[u, v] = (D_u D_v \varphi)(x)$ при произвольном $x \in V$ (очевидно, что правая часть последнего равенства не зависит от x). Тогда из леммы 1 следует, что отображение

$$(u, v) \mapsto [u, v], \quad u, v \in V, \quad u \diamond v,$$

симметрично и билинейно по каждому аргументу (при фиксированном другом аргументе). Кроме того, имеет место эквивалентность

$$u \nabla v \iff [u, v] = 0 \quad (6)$$

при $u, v \in V, u \diamond v$.

ЛЕММА 9. Пусть $V = U \oplus W$ – ∇ -ортогональное разложение пространства V . Предположим, что $V^\nabla = \{0\}$. Тогда если U_0 – подпространство $U \cap V^\diamond$, то

$$\dim U_0 + \dim U_0^\nabla \cap U = \dim U.$$

ДОКАЗАТЕЛЬСТВО. Из эквивалентности (6) вытекает, что ядро линейного отображения, ставящего в соответствие произвольному $a \in U_0$ линейную функцию $x \mapsto [a, x]$, $x \in U$, принадлежащую U^* , равно $U^\nabla \cap U_0$. В то же время $U^\nabla \cap U_0 \subseteq U^\nabla \cap W^\nabla = V^\nabla = \{0\}$ ввиду леммы 2, 4). Поэтому образом пространства U_0 при указанном отображении является подпространство Ξ пространства U^* такое, что $\dim \Xi = \dim U_0$. Кроме того,

$$U_0^\nabla \cap U = \{x \in U \mid \xi(x) = 0 \text{ для всех } \xi \in \Xi\}$$

ввиду эквивалентности (6). Следовательно, $\dim U_0^\nabla \cap U = \dim U - \dim \Xi = \dim U - \dim U_0$. Лемма доказана.

ЛЕММА 10. Ортогональности $\diamond$ и $\bar{\diamond}$ удовлетворяют условию (2).

ДОКАЗАТЕЛЬСТВО. Пусть $a, b \in V$ удовлетворяют равенству $a^\diamond + b^\diamond = V$. Докажем включение

$$(a + b)^\diamond \subseteq a^\diamond \cap b^\diamond. \quad (7)$$

Предположим, что $v \in (a + b)^\diamond$, т.е. $D_v D_{a+b} \varphi$ – константа. Выберем произвольные элементы $u \in a^\diamond$ и $w \in b^\diamond$. Тогда из леммы 1 вытекает, что

$$\begin{aligned} D_u D_v D_a \varphi &= 0, & D_w D_v D_b \varphi &= 0, \\ D_u D_v D_b \varphi &= D_u D_v D_{a+b} \varphi - D_u D_v D_a \varphi - D_u D_v D_a D_b \varphi = 0, \\ D_w D_v D_a \varphi &= D_w D_v D_{a+b} \varphi - D_w D_v D_b \varphi - D_w D_v D_a D_b \varphi = 0. \end{aligned}$$

Поэтому

$$\begin{aligned} D_{u+w} D_v D_a \varphi &= D_u D_v D_a \varphi + D_w D_v D_a \varphi + D_u D_w D_v D_a \varphi = 0, \\ D_{u+w} D_v D_b \varphi &= D_u D_v D_b \varphi + D_w D_v D_b \varphi + D_u D_w D_v D_b \varphi = 0 \end{aligned}$$

согласно лемме 1, 3), 4). Но ввиду условия $a^\diamond + b^\diamond = V$ это означает, что $D_z D_v D_a \varphi = D_z D_v D_b \varphi = 0$ для любого $z \in V$. Следовательно, $D_v D_a \varphi$ и

$D_v D_b \varphi$ – константы (по лемме 1, 4)), т.е. $v \in a^\diamond \cap b^\diamond$. Таким образом, включение (7) доказано. Из включения (7) и леммы 2, 1) вытекает требуемое равенство

$$(a + b)^\diamond = a^\diamond \cap b^\diamond. \quad (8)$$

Пусть $v \mapsto \bar{v}$ ($v \in V$) – естественный гомоморфизм V на $V/V^\diamond$. Предположим, что $x, y \in V/V^\diamond = \bar{V}$ удовлетворяют равенству $x^\diamond + y^\diamond = \bar{V}$. Выберем некоторые $a, b \in V$ такие, что $\bar{a} = x$ и $\bar{b} = y$. Тогда ввиду леммы 4 $\overline{a^\diamond + b^\diamond} = x^\diamond + y^\diamond = \bar{V}$ и, следовательно, $a^\diamond + b^\diamond = V$, так как

$$V^\diamond \subseteq a^\diamond, \quad V^\diamond \subseteq b^\diamond \quad (9)$$

по лемме 2, 2). Поэтому для этих элементов a и b справедливо равенство (8) и

$$(x + y)^\diamond = \overline{(a + b)^\diamond} = \overline{a^\diamond \cap b^\diamond} = \overline{a^\diamond} \cap \overline{b^\diamond} = x^\diamond \cap y^\diamond$$

ввиду леммы 4 и включений (9). Лемма доказана.

Рассмотрим всевозможные представления функции φ в виде

$$\varphi\left(\sum_{U \in \mathfrak{S}} x_U\right) = \sum_{U \in \mathfrak{S}} \varphi_U(x_U), \quad x_U \in U, \quad U \in \mathfrak{S}, \quad (10)$$

соответствующем некоторому нетривиальному разложению $V = \bigoplus \mathfrak{S}$ пространства V , где $\mathfrak{S} \neq \emptyset$, $\varphi_U \in F^U$ для произвольного $U \in \mathfrak{S}$. Если $V \neq \{0\}$, то такие представления всегда существуют (достаточно в качестве $\mathfrak{S}$ взять $\{V\}$, а в качестве $\varphi_V - \varphi$). Следующая теорема показывает, для каких нетривиальных прямых разложений указанного вида функция φ обладает представлением вида (10), и дает описание всех этих представлений, соответствующих произвольному такому разложению.

ТЕОРЕМА 1. Пусть $V = \bigoplus \mathfrak{S}$ есть нетривиальное разложение пространства V , причем $\mathfrak{S} \neq \emptyset$. Тогда функция φ обладает представлением вида (10), соответствующим данному разложению, если и только если это разложение ∇ -ортогонально. Кроме того, если рассматриваемое разложение ∇ -ортогонально, то функции $\varphi_U \in F^U$, $U \in \mathfrak{S}$, удовлетворяют равенству (10) (при данном разложении) тогда и только тогда, когда

$$\varphi_U = \varphi|_U + c_U \quad \forall U \in \mathfrak{S}, \quad \text{где } c_U \in F \text{ и } \sum_{U \in \mathfrak{S}} c_U = (1 - |\mathfrak{S}|)\varphi(0). \quad (11)$$

ДОКАЗАТЕЛЬСТВО. Если функция φ представлена в виде (10), то ∇ -ортогональность соответствующего разложения проверяется непосредственно. Предположим теперь, что это разложение ∇ -ортогонально. Для каждого $U \in \mathfrak{S}$ выберем произвольный элемент $x_U \in U$. Докажем, что

$$\sum_{U \in \mathfrak{I}} \varphi(x_U) = \varphi\left(\sum_{U \in \mathfrak{I}} x_U\right) + (|\mathfrak{I}| - 1)\varphi(0) \quad (12)$$

для любого множества $\mathfrak{I} \subseteq \mathfrak{S}$. Предположим противное и выберем минимальное (относительно включения) множество $\mathfrak{M} \subseteq \mathfrak{S}$ такое, что равенство (12) при

$\mathfrak{T} = \mathfrak{M}$ не выполняется. Очевидно, что $|\mathfrak{M}| \geq 2$. Представим $\mathfrak{M}$ в виде объединения двух непустых непересекающихся подмножеств $\mathfrak{M}_1$ и $\mathfrak{M}_2$ и положим $a_i = \sum_{U \in \mathfrak{M}_i} x_U$ для $i = 1, 2$. Тогда

$$\begin{aligned} \sum_{U \in \mathfrak{M}} \varphi(x_U) &= \sum_{U \in \mathfrak{M}_1} \varphi(x_U) + \sum_{U \in \mathfrak{M}_2} \varphi(x_U) \\ &= \varphi(a_1) + (|\mathfrak{M}_1| - 1)\varphi(0) + \varphi(a_2) + (|\mathfrak{M}_2| - 1)\varphi(0), \end{aligned} \quad (13)$$

так как $\mathfrak{M}_i \subset \mathfrak{M}$ при $i = 1, 2$. Кроме того, из ∇ -ортогональности рассматриваемого разложения следует, что $a_1 \nabla a_2$. В частности,

$$(D_{a_1} D_{a_2} \varphi)(0) = \varphi(a_1 + a_2) - \varphi(a_1) - \varphi(a_2) + \varphi(0) = 0. \quad (14)$$

Из (13), (14) и очевидного равенства $|\mathfrak{M}_1| + |\mathfrak{M}_2| = |\mathfrak{M}|$ непосредственно вытекает, что (12) верно при $\mathfrak{T} = \mathfrak{M}$. Полученное противоречие с выбором $\mathfrak{M}$ доказывает справедливость равенства (12) при всех $\mathfrak{T} \subseteq \mathfrak{S}$.

Пусть $\varphi_U \in F^U$ для всех $U \in \mathfrak{S}$. Предположим, что эти функции удовлетворяют условиям (11). Тогда

$$\sum_{U \in \mathfrak{S}} \varphi_U(x_U) = \sum_{U \in \mathfrak{S}} \varphi(x_U) + \sum_{U \in \mathfrak{S}} c_U = \varphi\left(\sum_{U \in \mathfrak{S}} x_U\right)$$

в силу (12) при $\mathfrak{T} = \mathfrak{S}$. Это показывает, что функции φ_U удовлетворяют равенству (10). В частности, функция φ обладает представлением вида (10) с данным множеством $\mathfrak{S}$. Обратно, пусть функции φ_U удовлетворяют равенству (10). Для произвольного $U \in \mathfrak{S}$ положим $c_U = -\sum_{W \in \mathfrak{S} \setminus \{U\}} \varphi_W(0)$. Тогда из (10) следует, что $\varphi_U(x_U) = \varphi(x_U) + c_U$ для всех $U \in \mathfrak{S}$ и

$$\sum_{U \in \mathfrak{S}} c_U = (1 - |\mathfrak{S}|) \sum_{W \in \mathfrak{S}} \varphi_W(0) = (1 - |\mathfrak{S}|)\varphi(0).$$

Таким образом, функции φ_U удовлетворяют условиям (11). Теорема доказана.

Функция φ называется *расщепляемой*, если для нее существует представление вида (10), в котором $|\mathfrak{S}| = 2$ (см. также введение). Очевидно, что если последнее равенство заменить на неравенство $|\mathfrak{S}| \geq 2$, то полученное определение расщепляемости будет эквивалентно исходному. Из теоремы 1 вытекает

СЛЕДСТВИЕ 1. *Функция φ расщепляема тогда и только тогда, когда существует нетривиальное ∇ -ортогональное разложение пространства V в прямую сумму двух подпространств.*

§ 5. Необходимые и достаточные условия расщепляемости функций

Следующая лемма непосредственно вытекает из следствия 1.

ЛЕММА 11. *Предположим, что $V^\nabla \neq \{0\}$. Тогда функция φ расщепляема, если и только если $n \geq 2$. Кроме того, если $n \geq 2$, $u \in V^\nabla \setminus \{0\}$ и W – какое-либо прямое дополнение к $\langle u \rangle$ в V , то $V = \langle u \rangle \oplus W$ является нетривиальным ∇ -ортогональным разложением пространства V .*

ЛЕММА 12. *Предположим, что $V^\nabla = \{0\}$ и существует элемент u , удовлетворяющий условиям*

$$u \in V^\diamond, \quad u \not\in u. \quad (15)$$

Тогда функция φ расщепляема, если и только если $n \geq 2$. Кроме того, если $n \geq 2$ и элемент u удовлетворяет условиям (15), то $V = \langle u \rangle \oplus \langle u \rangle^\nabla$ является нетривиальным ∇ -ортогональным разложением пространства V .

ДОКАЗАТЕЛЬСТВО. Пусть элемент u (очевидно, отличный от 0) удовлетворяет условиям (15). Тогда если $\lambda u \in \langle u \rangle^\nabla$ при некотором $\lambda \in F$, то из эквивалентности (6) вытекает, что $\lambda = 0$. Следовательно, $\langle u \rangle \cap \langle u \rangle^\nabla = \{0\}$. Из леммы 9 вытекает, что $\dim \langle u \rangle + \dim \langle u \rangle^\nabla = n$. Поэтому $V = \langle u \rangle \oplus \langle u \rangle^\nabla$. Очевидно, что это разложение ∇ -ортогонально, а при $n \geq 2$ и нетривиально. Это показывает, что функция φ расщепляема, если и только если $n \geq 2$ (ввиду следствия 1). Лемма доказана.

Очевидно, что при $p = 2$ условия леммы 12 не могут выполняться, так как $u \nabla u$ для всех $u \in V$.

ЛЕММА 13. *Предположим, что $V^\nabla = \{0\}$, $u \nabla u$ для всех $u \in V^\diamond$ и $V^\diamond \not\subset V^\diamond$. Тогда функция φ расщепляема, если и только если $n \geq 3$. Кроме того, если $n \geq 3$ и $u_1 \not\in u_2$, где $u_1, u_2 \in V^\diamond$, то $V = \langle u_1, u_2 \rangle \oplus \langle u_1, u_2 \rangle^\nabla$ является нетривиальным ∇ -ортогональным разложением пространства V .*

ДОКАЗАТЕЛЬСТВО. Пусть элементы $u_1, u_2 \in V^\diamond$ удовлетворяют условию $u_1 \not\in u_2$ (существование таких элементов вытекает из условия $V^\diamond \not\subset V^\diamond$). Тогда если $\lambda_1 u_1 + \lambda_2 u_2 \in \langle u_1, u_2 \rangle^\nabla$ при некоторых $\lambda_1, \lambda_2 \in F$, то из эквивалентности (6) вытекает, что $\lambda_1 = \lambda_2 = 0$. Следовательно, u_1 и u_2 линейно независимы и $\langle u_1, u_2 \rangle \cap \langle u_1, u_2 \rangle^\nabla = \{0\}$. Из леммы 9 вытекает, что $\dim \langle u_1, u_2 \rangle + \dim \langle u_1, u_2 \rangle^\nabla = n$. Поэтому $V = \langle u_1, u_2 \rangle \oplus \langle u_1, u_2 \rangle^\nabla$. Очевидно, что это разложение ∇ -ортогонально, а при $n \geq 3$ и нетривиально. Если существует нетривиальное ∇ -ортогональное разложение $\langle u_1, u_2 \rangle$ в прямую сумму двух подпространств, то $\langle u_1, u_2 \rangle \nabla \langle u_1, u_2 \rangle$ (ввиду леммы 2, 3), что неверно. Поэтому при $n \leq 2$ пространство $V = \langle u_1, u_2 \rangle$ не имеет нетривиального ∇ -ортогонального разложения в прямую сумму двух подпространств. Это показывает, что функция φ расщепляема, если и только если $n \geq 3$ (ввиду следствия 1). Лемма доказана.

Предположим теперь, что $V^\nabla = \{0\}$ и $V^\diamond \nabla V^\diamond$. В дальнейшем через $v \mapsto \bar{v}$, $v \in V$, будет обозначаться естественный гомоморфизм V на $V/V^\diamond$. Пусть $\bar{V} = \bigoplus \mathfrak{M}$ – полное $\bar{\diamond}$ -ортогональное разложение пространства $\bar{V} = V/V^\diamond$. По лемме 8 (которая применима в данной ситуации ввиду лемм 10 и 4) такое разложение единственно, причем в качестве множества $\mathfrak{M}$ в нем можно взять $\{\langle H \rangle \mid H \in \mathfrak{H}\}$, где $\mathfrak{H}$ – множество всех связанных компонент графа $\Gamma(I_{\bar{\diamond}}, \bar{\rho})$. Очевидно также, что $|\mathfrak{M}| \leq \dim \bar{V} \leq n$.

Пусть $X \in \mathfrak{M}$. Обозначим через V_X полный прообраз подпространства X при естественном гомоморфизме V на $V/V^\diamond = \bar{V}$. Кроме того, выберем и зафиксируем некоторое линейно независимое подмножество $E_X \subseteq V_X$ такое, что $\langle E_X \rangle \oplus V^\diamond = V_X$. Если $\mathfrak{N} \subseteq \mathfrak{M}$, то для краткости мы полагаем $V_{\mathfrak{N}} = V^\diamond + \sum_{X \in \mathfrak{N}} V_X$ (очевидно, что $V_{\mathfrak{N}} = \sum_{X \in \mathfrak{N}} V_X$ при $\mathfrak{N} \neq \emptyset$) и $E_{\mathfrak{N}} = \bigcup_{X \in \mathfrak{N}} E_X$. Тогда легко видеть, что $V_{\mathfrak{N}}$ является полным прообразом подпространства $\bigoplus \mathfrak{N}$

при естественном гомоморфизме V на $V/V^\diamond$ и $V_{\mathfrak{N}} = \langle E_{\mathfrak{N}} \rangle \oplus V^\diamond$, где множество $E_{\mathfrak{N}}$ линейно независимо ($\mathfrak{N} \subseteq \mathfrak{M}$). Каждому элементу $e \in E_{\mathfrak{M}}$ мы поставим в соответствие переменную z_e , принимающую значения в $V^\diamond$. При этом, естественно, предполагается, что различным элементам $E_{\mathfrak{M}}$ соответствуют различные переменные.

ЛЕММА 14. *Предположим, что $V^\nabla = \{0\}$ и $V^\diamond \nabla V^\diamond$. Тогда функция φ расщепляема, если и только если для некоторого непустого подмножества $\mathfrak{N} \subset \mathfrak{M}$ выполняются следующие условия:*

- 1) $V^\diamond = (V_{\mathfrak{N}}^\nabla \cap V^\diamond) + (V_{\mathfrak{M} \setminus \mathfrak{N}}^\nabla \cap V^\diamond)$;
- 2) система уравнений

$$[a, z_b] + [b, z_a] = -[a, b], \quad a \in E_{\mathfrak{N}}, \quad b \in E_{\mathfrak{M} \setminus \mathfrak{N}}, \quad (16)$$

разрешима относительно переменных z_e , принимающих значения в $V^\diamond$, где $e \in E_{\mathfrak{M}}$.

Кроме того, если для непустого подмножества $\mathfrak{N} \subset \mathfrak{M}$ эти условия выполнены и $(r_e \mid e \in E_{\mathfrak{M}})$ – решение системы (16), где $r_e \in V^\diamond$, то

$$V = (\langle a + r_a \mid a \in E_{\mathfrak{N}} \rangle + (V_{\mathfrak{M} \setminus \mathfrak{N}}^\nabla \cap V^\diamond)) \oplus (\langle b + r_b \mid b \in E_{\mathfrak{M} \setminus \mathfrak{N}} \rangle + (V_{\mathfrak{N}}^\nabla \cap V^\diamond))$$

является нетривиальным ∇ -ортогональным разложением пространства V .

ДОКАЗАТЕЛЬСТВО. Предположим сначала, что функция φ расщепляема. Тогда ввиду следствия 1 существует нетривиальное ∇ -ортогональное разложение $V = U \oplus W$ пространства V . Из лемм 10 и 6 вытекает, что

$$V^\diamond = (U \cap V^\diamond) \oplus (W \cap V^\diamond). \quad (17)$$

Используя равенство (17), легко показать, что $\overline{U} \cap \overline{W} = \{0\}$. Поэтому $\overline{V} = \overline{U} \oplus \overline{W}$, где, очевидно, $\overline{U} \diamond \overline{W}$. Кроме того, по лемме 9

$$\dim U \cap V^\diamond + \dim (U \cap V^\diamond)^\nabla \cap U = \dim U.$$

С другой стороны, $\dim U \cap V^\diamond \leq \dim (U \cap V^\diamond)^\nabla \cap U$, так как $U \cap V^\diamond \subseteq (U \cap V^\diamond)^\nabla \cap U$. Следовательно,

$$\dim \overline{U} = \dim U - \dim U \cap V^\diamond = \dim (U \cap V^\diamond)^\nabla \cap U \geq \frac{\dim U}{2} > 0$$

и $\overline{U} \neq \{0\}$. Меняя местами U и W , получаем, что $\overline{W} \neq \{0\}$. Из доказанного выше вытекает существование непустого подмножества $\mathfrak{N} \subset \mathfrak{M}$ такого, что $\bigoplus \mathfrak{N} = \overline{U}$ и $\bigoplus (\mathfrak{M} \setminus \mathfrak{N}) = \overline{W}$ (напомним, что полное $\diamond$ -ортогональное разложение пространства $\overline{V}$ единственно). Взяв полные прообразы левых и правых частей двух последних равенств при естественном гомоморфизме V на $V/V^\diamond$, мы получим равенства

$$V_{\mathfrak{N}} = U + V^\diamond, \quad V_{\mathfrak{M} \setminus \mathfrak{N}} = W + V^\diamond. \quad (18)$$

Из равенств (18) ввиду лемм 2, 4) и 3 следует, что

$$\begin{aligned} V_{\mathfrak{N}}^\nabla \cap V^\diamond &= U^\nabla \cap V^{\diamond^\nabla} \cap V^\diamond = W \cap V^\diamond, \\ V_{\mathfrak{M} \setminus \mathfrak{N}}^\nabla \cap V^\diamond &= W^\nabla \cap V^{\diamond^\nabla} \cap V^\diamond = U \cap V^\diamond, \end{aligned} \quad (19)$$

так как $V^\diamond \subseteq V^{\diamond\vee}$. Справедливость условия 1) вытекает теперь из (17) и (19).

Пусть $a \in E_{\mathfrak{N}}$ и $b \in E_{\mathfrak{M} \setminus \mathfrak{N}}$. Выберем элементы $u_a \in U$, $w_b \in W$ и $r_a, r_b \in V^\diamond$ такие, что $a = u_a - r_a$ и $b = w_b - r_b$. Существование таких элементов следует из равенств (18). Ввиду эквивалентности (6) имеет место равенство

$$0 = [u_a, w_b] = [a + r_a, b + r_b] = [a, b] + [a, r_b] + [b, r_a],$$

так как $u_a \nabla w_b$, $a \diamond b$ и $r_a \nabla r_b$. Поэтому $(r_e \mid e \in E_{\mathfrak{M}})$ – решение системы (16).

Предположим теперь, что для непустого подмножества $\mathfrak{N} \subset \mathfrak{M}$ выполнены условия 1) и 2). Пусть также $(r_e \mid e \in E_{\mathfrak{M}})$ – решение системы (16), где $r_e \in V^\diamond$. Положим для краткости $U_0 = \langle a + r_a \mid a \in E_{\mathfrak{N}} \rangle$ и $W_0 = \langle b + r_b \mid b \in E_{\mathfrak{M} \setminus \mathfrak{N}} \rangle$. Очевидно, что $U_0 \nabla V_{\mathfrak{N}}^\vee \cap V^\diamond$ (так как $U_0 \subseteq V_{\mathfrak{N}}$), $W_0 \nabla V_{\mathfrak{M} \setminus \mathfrak{N}}^\vee \cap V^\diamond$ (так как $W_0 \subseteq V_{\mathfrak{M} \setminus \mathfrak{N}}$) и $V_{\mathfrak{N}}^\vee \cap V^\diamond \nabla V_{\mathfrak{M} \setminus \mathfrak{N}}^\vee \cap V^\diamond$ (так как $V^\diamond \nabla V^\diamond$). Пусть $a \in E_{\mathfrak{N}}$ и $b \in E_{\mathfrak{M} \setminus \mathfrak{N}}$. Тогда из условия 2) вытекает равенство

$$[a + r_a, b + r_b] = [a, b] + [a, r_b] + [b, r_a] = 0,$$

так как $a \diamond b$ и $[r_a, r_b] = 0$ (последнее равенство следует из условия $V^\diamond \nabla V^\diamond$ и эквивалентности (6)). Поэтому $(a + r_a) \nabla (b + r_b)$ ввиду эквивалентности (6). Таким образом, $U_0 \nabla W_0$ и

$$U_0 + (V_{\mathfrak{M} \setminus \mathfrak{N}}^\vee \cap V^\diamond) \nabla W_0 + (V_{\mathfrak{N}}^\vee \cap V^\diamond) \quad (20)$$

по лемме 2, 3).

Легко видеть, что

$$U_0 + V^\diamond = \langle E_{\mathfrak{N}} \rangle + V^\diamond = V_{\mathfrak{N}}, \quad W_0 + V^\diamond = \langle E_{\mathfrak{M} \setminus \mathfrak{N}} \rangle + V^\diamond = V_{\mathfrak{M} \setminus \mathfrak{N}}. \quad (21)$$

Поэтому

$$\begin{aligned} & (U_0 + (V_{\mathfrak{M} \setminus \mathfrak{N}}^\vee \cap V^\diamond)) + (W_0 + (V_{\mathfrak{N}}^\vee \cap V^\diamond)) \\ & = U_0 + W_0 + V^\diamond = V_{\mathfrak{N}} + V_{\mathfrak{M} \setminus \mathfrak{N}} = V \end{aligned} \quad (22)$$

ввиду условия 1) и равенств (21). Кроме того, $V^\diamond \subset V_{\mathfrak{N}}$ и $V^\diamond \subset V_{\mathfrak{M} \setminus \mathfrak{N}}$, так как $\bigoplus \mathfrak{N} \neq \{0\}$ и $\bigoplus (\mathfrak{M} \setminus \mathfrak{N}) \neq \{0\}$ ввиду непустоты множеств $\mathfrak{N}$ и $\mathfrak{M} \setminus \mathfrak{N}$. Поэтому $U_0 \neq \{0\}$ и $W_0 \neq \{0\}$ ввиду равенств (21). Из двух последних неравенств, равенства (22), условия (20) и леммы 3 вытекает, что

$$V = (U_0 + (V_{\mathfrak{M} \setminus \mathfrak{N}}^\vee \cap V^\diamond)) \oplus (W_0 + (V_{\mathfrak{N}}^\vee \cap V^\diamond))$$

является нетривиальным ∇ -ортогональным разложением пространства V , как и требовалось доказать. Расщепляемость функции φ теперь имеет место ввиду следствия 1. Лемма доказана.

Выберем какой-либо базис C пространства $V^\diamond$. Тогда очевидно, что

$$\left(\sum_{c \in C} r_{e,c} c \mid e \in E_{\mathfrak{M}} \right)$$

– решение системы (16), если и только если $(r_{e,c} \mid e \in E_{\mathfrak{M}}, c \in C)$ – решение системы

$$\sum_{c \in C} ([a, c] z_{b,c} + [b, c] z_{a,c}) = -[a, b], \quad a \in E_{\mathfrak{N}}, \quad b \in E_{\mathfrak{M} \setminus \mathfrak{N}},$$

от переменных $z_{e,c}$, $e \in E_{\mathfrak{M}}$, $c \in C$, принимающих значения в поле F . Это показывает, что нахождение решений системы (16) эквивалентно нахождению решений указанной системы из $|E_{\mathfrak{N}}| |E_{\mathfrak{M} \setminus \mathfrak{N}}|$ линейных уравнений от $|E_{\mathfrak{M}}| \dim V^{\diamond}$ переменных над полем F .

Таким образом, мы разбили общий случай на четыре взаимоисключающих подслучая и в каждом из этих подслучаев (см. леммы 11–14) дали необходимое и достаточное условие расщепляемости функции φ и способ нахождения нетривиального ∇ -ортогонального разложения пространства V в прямую сумму двух подпространств, если φ расщепляема. Легко видеть, что по данной произвольной функции $\varphi \in F^V$ за полиномиальное время можно определить, какой из этих четырех случаев имеет место для φ , проверить необходимое и достаточное условие расщепляемости и найти указанным способом нетривиальное ∇ -ортогональное разложение V в прямую сумму двух подпространств, если φ расщепляема. Поэтому имеет место

ТЕОРЕМА 2. *Существует полиномиальный алгоритм, который по произвольной функции $\varphi \in F^V$ проверяет, является ли она расщепляемой, и в случае расщепляемости φ находит нетривиальное ∇ -ортогональное разложение пространства V в прямую сумму двух подпространств.*

§ 6. О единственности полного ∇ -ортогонального разложения

Легко видеть, что в общем случае полное ∇ -ортогональное разложение пространства V не единственно. Поэтому представляет интерес нахождение условий, при которых такое разложение единственно. Очевидно, что к таким условиям относится нерасщепляемость функции φ (ввиду следствия 1). Следующая теорема (непосредственно вытекающая из лемм 10 и 8) утверждает, что при $V^{\diamond} = \{0\}$ также имеет место единственность полного ∇ -ортогонального разложения, и дает простой полиномиальный алгоритм нахождения такого разложения по произвольной функции $\varphi \in F^V$.

ТЕОРЕМА 3. *Предположим, что $V^{\diamond} = \{0\}$. Пусть также $\mathfrak{G}$ – множество всех связных компонент графа $\Gamma(I_{\diamond}, \emptyset)$. Тогда если $V = \bigoplus \mathfrak{X}$ есть полное ∇ -ортогональное разложение пространства V , то отображение $G \mapsto \langle G \rangle$, $G \in \mathfrak{G}$, является биекцией $\mathfrak{G}$ на $\mathfrak{X}$. В частности, такое разложение единственно.*

Покажем теперь, что среди функций из F^V доля как расщепляемых функций, так и функций, для которых $V^{\diamond} \neq \{0\}$, экспоненциально стремится к 0 при $n \rightarrow \infty$ и фиксированном p . Следующее предложение доказывается аналогично теореме 2.16 из [1].

ПРЕДЛОЖЕНИЕ 1. *Пусть константа c удовлетворяет неравенствам $0 < c < 1 - 1/p$. Тогда доля расщепляемых функций из F^V есть $o(p^{-cp^n})$ при $n \rightarrow \infty$ и фиксированном p .*

ДОКАЗАТЕЛЬСТВО. Функция φ расщепляема тогда и только тогда, когда она представима в виде $\varphi(u + w) = \psi(u) + \chi(w)$, $u \in U$, $w \in W$, для некоторого нетривиального разложения $V = U \oplus W$ и некоторых функций $\psi \in F^U$ и $\chi \in F^W$. Очевидно, что число разложений вида $V = U \oplus W$ при фиксированной размерности пространства U не превосходит числа базисов пространства V

(рассматриваемых как последовательности, а не множества). Этих базисов имеется не более p^{n^2} . Поэтому

$$|\{\varphi \in F^V \mid \varphi \text{ расщепляема}\}| \leq \sum_{k=1}^{n-1} p^{n^2} p^{p^k} p^{p^{n-k}} \leq np^{n^2+p+p^{n-1}},$$

так как $p^k + p^{n-k} \leq p + p^{n-1}$ при всех k , удовлетворяющих неравенствам $1 \leq k \leq n-1$. Следовательно,

$$0 \leq \frac{|\{\varphi \in F^V \mid \varphi \text{ расщепляема}\}|}{|F^V|p^{-cp^n}} \leq p^{\log_p n + n^2 + p + (c - (1-1/p))p^n} \rightarrow 0$$

при $n \rightarrow \infty$ и фиксированном p , так как $c - (1 - 1/p) < 0$. Предложение доказано.

ПРЕДЛОЖЕНИЕ 2. Пусть константа c удовлетворяет неравенствам $0 < c < 1 - 1/p$. Тогда доля функций из F^V , для которых $V^\diamond \neq \{0\}$, есть $o(p^{-cp^n})$ при $n \rightarrow \infty$ и фиксированном p .

ДОКАЗАТЕЛЬСТВО. Легко видеть, что $v \in V^\diamond$ (где $v \in V$), если и только если $D_v\varphi$ аффинна, т.е. имеет вид $\eta + d$ при некоторых $\eta \in V^*$ и $d \in F$. Очевидно, что число аффинных функций равно p^{n+1} . Кроме того, при произвольном $v \in V$ ядром линейного (см. лемму 1, 1)) отображения D_v является множество всех функций из F^V , постоянных на каждом смежном классе V по $\langle v \rangle$. Следовательно, если $v \in V \setminus \{0\}$, то полный прообраз произвольной функции из F^V при отображении D_v либо пуст, либо состоит из $p^{p^{n-1}}$ элементов. Поэтому

$$\begin{aligned} |\{\varphi \in F^V \mid V^\diamond \neq \{0\}\}| &\leq \sum_{v \in V \setminus \{0\}} |\{\varphi \in F^V \mid D_v\varphi \text{ аффинна}\}| \\ &\leq p^n p^{n+1} p^{p^{n-1}} \end{aligned}$$

и

$$0 \leq \frac{|\{\varphi \in F^V \mid V^\diamond \neq \{0\}\}|}{|F^V|p^{-cp^n}} \leq p^{2n+1+(c-(1-1/p))p^n} \rightarrow 0$$

при $n \rightarrow \infty$ и фиксированном p , так как $c - (1 - 1/p) < 0$. Предложение доказано.

Список литературы

- [1] О. А. Логачёв, А. А. Сальников, В. В. Яценко, *Булевы функции в теории кодирования и криптологии*, МЦНМО, М., 2004.
- [2] М. И. Анохин, “О расщепляемости r -ичных функций”, *Тезисы докладов XIV Международной конференции “Проблемы теоретической кибернетики”* (Пенза, 2005), Изд-во механико-математического факультета МГУ, М., 2005, 12.
- [3] О. А. Логачёв, А. А. Сальников, В. В. Яценко, “Некоторые характеристики “нелинейности” групповых отображений”, *Дискрет. анализ и исследование операций*, 8:1 (2001), 40–54.

М. И. Анохин (M. I. Anokhin)
 Московский государственный университет
 им. М. В. Ломоносова
E-mail: anokhin@mccme.ru

Поступила в редакцию
 14.02.2006 и 30.10.2006