УДК 510. 5+512. 64

В. Г. Скобелев, канд. физ.-мат. наук,
Д. В. Сперанский, д-р техн. наук
(Ин-т прикл. математики и механики НАН Украины, Донецк)

ИДЕНТИФИКАЦИЯ БУЛЕВЫХ ФУНКЦИЙ МЕТОДАМИ ЛИНЕЙНОЙ АЛГЕБРЫ

We prove that the problem of identification of a Boolean function by using methods of the theory of linear spaces over finite fields is solvable.

Доведена розв'язуваність задачі ідентифікації булевої функції методами теорії лінійних просторів над скінченними полями.

1. Введение. Задача идентификации булевой функции является одной из центральных задач дискретной математики, имеющей многочисленные приложения. Стандартный подход к ее решению основан на методе полного перебора и имеет экспоненциальную сложность (как, временную, так и емкостную). Известно, что одним из способов понижения сложности решения является замена (там, где это возможно) перебора алгебраическими операциями. В настоящей работе показано, что такой подход применим к рассматриваемой задаче. Предлагаемое решение основано на представлении булевой функции в виде подмножества линейного пространства и идентификации этого подмножества с помощью специально подобранных линейных операторов.

Понятия и обозначения, принятые в работе, такие же, как и в [1, 2].

2. Основные понятия и постановка задачи. Обозначим через $P_{m,n}$ m, $n\in N$, множество всех функций f: $\{0, 1\}^m \to \{0, 1\}^n$. Каждая функция $f\in P_{m,n}$ может быть представлена в виде $f = (f_1, \dots, f_n)$, где $f_j = \mathrm{pr}_j f\in P_{m,1}$, $j = 1, \dots, n$. Следовательно, $P_{m,n} = P_{m,1}^n$ для всех $m, n \in N$. Множество всех функций $f\in P_{m,1}$, сохраняющих константу 0, обозначим через $T_0(m)$, а множество всех линейных функций $f\in P_{m,1}$ — через $L(m)$. График функции $f\in P_{m,n}$ определим как множество

$$\mathrm{гр}f = \{(\alpha_1, \dots, \alpha_{m+n})\in \{0, 1\}^{m+n} | f(\alpha_1, \dots, \alpha_m) = (\alpha_{m+1}, \dots, \alpha_{m+n})\}.$$

Это множество, как и любое функциональное отношение, имеет следующее свойство: если $\overline{a} = (\alpha_1, \dots, \alpha_{m+n})\in \mathrm{гр}f$, $\overline{b} = (\beta_1, \dots, \beta_{m+n})\in \mathrm{гр}f$ и $\overline{a} \neq \overline{b}$, то существует, по крайней мере, одно такое значение $j\in \{1, \dots, m\}$, что $\alpha_j \neq \beta_j$. Рассмотрим следующую задачу.

Задача 1. Заданы функция $f\in P_{m,n}$ и множество $\Omega \subseteq \{0, 1\}^{m+n}$. Проверить, верно ли включение

$$\Omega \subseteq \mathrm{гр}f. \tag{1}$$

Замечание. Как правило, задача идентификации булевой функции формулируется в следующем виде: при заданных $f\in P_{m,n}$, $F\,(\varnothing \neq F \subseteq P_{m,n}\setminus\{f\})$ и $g \in \in \{f\} \cup F$ проверить, верно ли равенство $g = f$. Нетрудно показать, что эту задачу легко свести к задаче 1.

Так как $\{0, 1\}^{m+n}$ — конечное множество, то задача 1, в принципе, может быть решена методом полного перебора. Его основным недостатком является большая сложность (как временная, так и емкостная). Она обусловлена тем, что при таком подходе любой способ построения множества $\mathrm{гр}f$ фактически сводится к перечислению всех его элементов, а основными операциями, выполняемыми при проверке включения (1), являются попарные сравнения элементов множеств Ω и $\mathrm{гр}f$. Для понижения сложности решения задачи 1 необходимо выбрать в множестве $\{0, 1\}^{m+n}$ легко выполнимые операции, позволяющие, во-первых, эффективно проверять включение (1), а во-вторых, не строить множество $\operatorname{гр} f$ в явном виде, а задавать его легко вычислимой характеристической функцией. Известно, что при всех $k \in N$ система $GF^k(2) = (\{0, 1\}^k, +, \cdot)$ является k-мерным линейным пространством над полем $GF(2)$. Поэтому естественно исследовать возможность решения задачи 1 методами теории линейных пространств над полями Галуа. При таком подходе в качестве указанных выше операций могут быть выбраны стандартные операции пространства $GF^{m+n}(2)$. Этот выбор, в свою очередь, определяет легко вычислимые характеристические функции как такие, которые могут быть представлены в виде множества линейных операторов. Исходя из изложенного, выделим следующий класс характеристических функций.

Определение 1. *Линейной характеристической функцией для множества* $\operatorname{гр} f$, $f \in P_{m,n}$, *назовем такое множество* $\chi_f = \{M_i \mid j = 1, \ldots, l\}$ *матриц над полем* $GF(2)$, *что для любого вектора* $\overline{a} \in \{0, 1\}^{m+n}$ *равенство* $\overline{a} M_i = \overline{0}$ *верно хотя бы при одном значении* $i \in \{1, \ldots, l\}$ *тогда и только тогда, когда* $\overline{a} \in \operatorname{гр} f$.

Будем считать, что для любого вектора $\overline{a} \in \{0, 1\}^{m+n}$

$$\chi_f(\overline{a}) = \{\overline{a} M_i \mid i = 1, \ldots, l\}.$$

Из определения 1 вытекает, что линейная характеристическая функция множества $\operatorname{гр} f$, $f \in P_{m,n}$, удовлетворяет следующему условию: для любого вектора $\overline{a} \in \{0, 1\}^{m+n}$ верна эквивалентность

$$\overline{a} \in \operatorname{гр} f \Leftrightarrow \overline{0} \in \chi_f(\overline{a}).$$

Покажем, что решение задачи 1 всегда может быть сведено к построению соответствующей линейной характеристической функции и вычислению ее значений на заданном множестве векторов.

3. Вспомогательные результаты. Исследуем строение множества $\operatorname{гр} f$, $f \in P_{m,n}$.

Утверждение 1. *Для любой функции* $f \in P_{m,n}$ *число линейно независимых векторов, принадлежащих множеству* $\operatorname{гр} f$, *не меньше чем* m.

Доказательство. Для любой функции $f \in P_{m,n}$ множество $\operatorname{гр} f$ содержит элементы

$$\overline{e}_i = \Big(\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{m-i}, \beta_1, \ldots, \beta_n\Big), \quad i = 1, \ldots, m, \tag{2}$$

где

$$\beta_j = \operatorname{pr}_j f\Big(\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0\Big), \quad i = 1, \ldots, n.$$

Векторы $\overline{e}_i, \ldots, \overline{e}_m$ линейно независимы и их число равно m.

Утверждение доказано.

Теорема 1. *Множество* $\operatorname{гр} f$, $f \in P_{m,n}$, *является подпространством пространства* $GF^{m+n}(2)$ *тогда и только тогда, когда* $f \in (T_0(m) \cap L(m))^n$.

Доказательство. Известно, что множество $\operatorname{гр} f$, $f \in P_{m,n}$, является подпространством пространства $GF^{m+n}(2)$ тогда и только тогда, когда выполнены условия

$$\overline{0} \in \operatorname{гр} f \tag{3}$$

и

$$(\alpha_1, \ldots, \alpha_{m+n}), (\beta_1, \ldots, \beta_{m+n}) \in \operatorname{гр} f \Rightarrow (\alpha_1 + \beta_1, \ldots, \alpha_{m+n} + \beta_{m+n}) \in \operatorname{гр} f. \tag{4}$$

Соотношение (3) эквивалентно равенству $f(\overline{0}) = \overline{0}$. Последнее справедливо тогда и только тогда, когда $\mathrm{pr}_j f \in T_0(m)$ для всех $j = 1, \ldots, n$. Условие (4) эквивалентно условию

$$\mathrm{pr}_j f(\alpha_1, \ldots, \alpha_m) + \mathrm{pr}_j f(\beta_1, \ldots, \beta_m) =$$
$$= \mathrm{pr}_j f(\alpha_1 + \beta_1, \ldots, \alpha_m + \beta_m), \quad j = 1, \ldots, n,$$

для всех $(\alpha_1, \ldots, \alpha_m), (\beta_1, \ldots, \beta_m) \in \{0, 1\}^m$. Это условие, в свою очередь, эквивалентно условию $\mathrm{pr}_j f \in L(m)$ для всех $j = 1, \ldots, n$. Итак, показано, что $\operatorname{гр} f$, $f \in P_{m,n}$, является подпространством пространства $GF^{m+n}(2)$ тогда и только тогда, когда $\mathrm{pr}_j f \in T_0(m) \cap L(m)$ для всех $j = 1, \ldots, n$. Последнее условие эквивалентно условию $f \in (T_0(m) \cap L(m))^n$.

Теорема доказана.

***Следствие* 1.** *Множество* $\operatorname{гр} f$, $f \in P_{m,n}$, *является подпространством пространства* $GF^{m+n}(2)$ *тогда и только тогда, когда* $\mathrm{pr}_j f = x_{j1} + \ldots + x_{jr_j}$ *для всех* $j = 1, \ldots, n$.

Доказательство. По определению линейной функции

$$L^n(m) = \{ f \in P_{m,n} | \mathrm{pr}_j f = \alpha_j + x_{j1} + \ldots + x_{jr_j} \text{ для всех } j = 1, \ldots, n \},$$

где $\alpha_j (j = 1, \ldots, n)$ — элемент поля $GF(2)$. Следовательно,

$$(T_0(m) \cap L(m))^n = T_0^n(m) \cap L^n(m) =$$
$$= \{ f \in P_{m,n} | \mathrm{pr}_j f = x_{j1} + \ldots + x_{jr_j} \text{ для всех } j = 1, \ldots, n \}.$$

Следствие доказано.

Обозначим размерность подпространства V через $\mathrm{Dim}\, V$, а ортогональное дополнение подпространства V — через $V^{\perp}$.

Утверждение 2. *Если множество* $\operatorname{гр} f$, $f \in P_{m,n}$, *является подпространством пространства* $GF^{m+n}(2)$, *то* $\mathrm{Dim} \operatorname{гр} f = m$ *и* $\mathrm{Dim} (\operatorname{гр} f)^{\perp} = n$.

Доказательство. Предположим, что $\operatorname{гр} f$, $f \in P_{m,n}$, является подпространством пространства $GF^{m+n}(2)$. Из утверждения 1 вытекает, что $\mathrm{Dim} \operatorname{гр} f \geq m$. Покажем, что линейно независимые векторы $\overline{e}_1, \ldots, \overline{e}_m$, определяемые соотношением (2), образуют базис пространства $\operatorname{гр} f$. Выберем произвольный вектор $\overline{a} = (\alpha_1, \ldots, \alpha_m, \gamma_1, \ldots, \gamma_n) \in \operatorname{гр} f$. Пусть среди первых его m компонент ненулевыми будут те и только те, которые имеют номера $j_1, \ldots, j_r$, $1 \leq j_1 < \ldots < j_r \leq m$. Рассмотрим вектор $\overline{b} = \overline{e}_{j_1} + \ldots + \overline{e}_{j_r} = (\alpha_1, \ldots, \alpha_m, \delta_1, \ldots, \delta_n)$. Так как $\overline{a}, \overline{b} \in \operatorname{гр} f$ и $\operatorname{гр} f$ является линейным пространством, то $\overline{a} + \overline{b} = (0, \ldots, 0, \gamma_1 + \delta_1, \ldots, \gamma_n + \delta_n) \in \operatorname{гр} f$. В силу теоремы 1 $f \in T_0^n(m)$. Следовательно, $\gamma_j + \delta_j = 0$, т. е. $\gamma_j = \delta_j$, $j = 1, \ldots, n$. Это означает, что $\overline{a} = \overline{b} = \overline{e}_{j_1} + \ldots + \overline{e}_{j_r}$. Итак, показано, что любой вектор $\overline{a} \in \operatorname{гр} f$ является линейной комбинацией линейно независимых векторов $\overline{e}_1, \ldots, \overline{e}_m$. Следовательно, векторы $\overline{e}_1, \ldots, \overline{e}_m$ образуют базис пространства $\operatorname{гр} f$. Отсюда непосредственно вытекает, что $\mathrm{Dim} \operatorname{гр} f = m$, что и требовалось доказать.

Известно, что для любого подпространства V линейного пространства U справедливо равенство $\mathrm{Dim}\, V + \mathrm{Dim}\, V^{\perp} = \mathrm{Dim}\, U$. Воспользовавшись этим равенством, получим

$$\mathrm{Dim}\,(\mathrm{гр} f)^{\perp} = \mathrm{Dim}\, GF^{m+n}(2) - \mathrm{Dim}\,\mathrm{гр} f = m + n - m =$$

что и требовалось доказать.

Утверждение доказано.

Обозначим через $\mathrm{lin}\,\mathrm{гр} f$, $f \in P_{m,n}$, множество всех максимальных по включению подпространств пространства $GF^{m+n}(2)$, содержащихся во множестве $\mathrm{гр} f$.

Теорема 2. *Множество* $\mathrm{lin}\,\mathrm{гр} f$, $f \in P_{m,n}$, *непусто тогда и только тогда, когда* $f \in T_0^n(m)$.

Доказательство. Будем использовать необходимые и достаточные условия для подпространства пространства $GF^{m+n}(2)$, устанавливаемые соотношения (3) и (4).

Пусть $f \in P_{m,n} \setminus T_0^n(m)$. Тогда $\overline{0} \notin \mathrm{гр} f$. Это означает, что для любого подмножества множества $\mathrm{гр} f$ условие (3) не выполнено. Таким образом, ни одно подмножество множества $\mathrm{гр} f$ не является подпространством пространства $GF^{m+n}(2)$. Следовательно, $\mathrm{lin}\,\mathrm{гр} f = \varnothing$, что и требовалось доказать.

Для дальнейшего доказательства нам понадобится следующая лемма.

Лемма 1. *Для любого вектора* $\overline{a} \in \{0, 1\}^{m+n} \setminus \{\overline{0}\}$ *множество* $V = \{\overline{0}, \overline{a})$ *является подпространством пространства* $GF^{m+n}(2)$.

Доказательство. Так как $\overline{0} \in V$, то условие (3) выполнено. А так как $\overline{0} + \overline{0} = \overline{0}$, $\overline{0} + \overline{a} = \overline{a} + \overline{0} = \overline{a}$, $\overline{a} + \overline{a} = \overline{0}$, то выполнено и условие (4). Следовательно, V — подпространство пространства $GF^{m+n}(2)$.

Лемма доказана.

Предположим теперь, что $f \in T_0^n(m)$. Тогда $\overline{0} \in \mathrm{гр} f$. Так как $|\mathrm{гр} f| = 2^{m+n} > 1$, то существует ненулевой вектор $\overline{a} \in \mathrm{гр} f$. В силу леммы 1 множество $\{\overline{0}, \overline{a}\}$ является подпространством пространства $GF^{m+n}(2)$. Из соотношения $\{\overline{0}, \overline{a}\} \subseteq \mathrm{гр} f$ вытекает, что существует максимальное по включению подпространство V пространства $GF^{m+n}(2)$, удовлетворяющее условию $\{\overline{0}, \overline{a}\} \subseteq V \subseteq \mathrm{гр} f$. Итак, показано, что существует подпространство V, принадлежащее множеству $\mathrm{lin}\,\mathrm{гр} f$. Следовательно, $\mathrm{lin}\,\mathrm{гр} f \neq \varnothing$, что и требовалось доказать.

Теорема доказана.

Из теоремы 2 вытекает, что множество $\mathrm{lin}\,\mathrm{гр} f$, $f \in P_{m,n}$, может быть использовано для исследования свойств множества $\mathrm{гр} f$ тогда и только тогда, когда $f \in T_0^n(m)$. Следующее утверждение показывает, что исследование множества $\mathrm{гр} f$, $f \in P_{m,n}$, всегда можно свести к исследованию такого множества $\mathrm{гр}\, g$, что $g \in T_0^n(m)$.

Утверждение 3. *Для любой функции* $f \in P_{m,n}$ *существует единственная константа* $\overline{a} \in \{0, 1\}^n$ *такая, что* $g = f + \overline{a} \in T_0^n(m)$.

Доказательство. Пусть $f \in P_{m,n}$. Рассмотрим функцию $g = f + \overline{a}$, где $\overline{a} \in \{0, 1\}^n$. Выберем константу $\overline{a}$ так, чтобы было справедливо равенство $g(\overline{0}) = \overline{0}$. Имеем

$$g(\overline{0}) = \overline{0} \Leftrightarrow f(\overline{0}) + \overline{a} = \overline{0} \Leftrightarrow \overline{a} = f(\overline{0}),$$

откуда вытекает, что для любой функции $f \in P_{m,n}$ требуемая константа $\overline{a}$ существует и единственна.

Утверждение доказано.

Значение утверждения 3 состоит в следующем. Если $f \in P_{m,n} \setminus T_0^n(m)$, то заменив множество $\operatorname{гр} f$ множеством $\operatorname{гр} g$, где $g = f + f(\overline{0}) \in T_0^n(m)$, мы можем исследовать последнее в терминах множества $\operatorname{lin}\operatorname{гр} g$. Из способа построения функции g вытекает, что множество $\operatorname{гр} g$ получается из множества $\operatorname{гр} f$ в результате сдвига на вектор $f(\overline{0})$. Это означает, что и множество $\operatorname{гр} f$ получается из множества $\operatorname{гр} g$ в результате сдвига на тот же самый вектор $f(\overline{0})$. Указанное взаимно-однозначное соответствие между множествами $\operatorname{гр} f$ и $\operatorname{гр} g$ позволяет переформулировать любое утверждение относительно множества $\operatorname{гр} g$ в соответствующее утверждение относительно множества $\operatorname{гр} f$. Исходя из этого, в дальнейшем будем рассматривать только те функции, которые принадлежат множеству $T_0^n(m)$.

Теорема 3. *Для любой функции $f \in T_0^n(m)$ справедливо равенство*

$$\operatorname{гр} f = \bigcup_{V \in \operatorname{lin}\operatorname{гр} f} V. \tag{5}$$

Доказательство. Рассмотрим произвольную функцию $f \in T_0^n(m)$. Из определения множества $\operatorname{lin}\operatorname{гр} f$ вытекает, что для любого $V \in \operatorname{lin}\operatorname{гр} f$ справедливо включение $V \subseteq \operatorname{гр} f$. В силу утверждения 3 $\operatorname{lin}\operatorname{гр} f \neq \varnothing$. Следовательно, справедливо включение

$$\bigcup_{V \in \operatorname{lin}\operatorname{гр} f} V \subseteq \operatorname{гр} f. \tag{6}$$

Покажем, что для любого вектора $\overline{a} \in \operatorname{гр} f$

$$\overline{a} \in \bigcup_{V \in \operatorname{lin}\operatorname{гр} f} V. \tag{7}$$

Возможны два случая. Предположим, что $\overline{a} = \overline{0}$. Так как вектор $\overline{0}$ является элементом любого подпространства пространства $GF^{m+n}(2)$ и $\operatorname{lin}\operatorname{гр} f \neq \varnothing$, то при $\overline{a} = \overline{0}$ соотношение (7) справедливо.

Предположим теперь, что $\overline{a} \in \operatorname{гр} f \setminus \{\overline{0}\}$. В силу леммы 1 множество $\{\overline{0}, \overline{a}\}$ является подпространством пространства $GF^{m+n}(2)$. Из включения $\{\overline{0}, \overline{a}\} \subseteq \operatorname{гр} f$ вытекает, что существует такое максимальное по включению подпространство V пространства $GF^{m+n}(2)$, что $\{\overline{0}, \overline{a}\} \subseteq V \subseteq \operatorname{гр} f$. А так как $\overline{a} \in V$ и $V \in \operatorname{lin}\operatorname{гр} f$, то и при $\overline{a} \in \operatorname{гр} f \setminus \{\overline{0}\}$ соотношение (7) справедливо.

Итак, показано, что для любого вектора $\overline{a} \in \operatorname{гр} f$ справедливо соотношение (7). Это означает, что справедливо включение

$$\operatorname{гр} f \subseteq \bigcup_{V \in \operatorname{lin}\operatorname{гр} f} V. \tag{8}$$

Из (6) и (8) непосредственно вытекает справедливость равенства (5).

Теорема доказана.

Из теоремы (3) вытекает, что для любой функции $f \in T_0^n(m)$ множество $\operatorname{гр} f$ может быть "расщеплено" на подпространства, принадлежащие множеству

$\operatorname{lin}\operatorname{гр}f$. В силу теоремы 1 это "расщепление" тривиально, если $f\in (T_0(m)\cap \cap L(m))^n$.

Следующие две теоремы показывают, что в общем случае "расщепление" может, во-первых, содержать достаточно большое число подпространств, а во-вторых, состоять из различных по своей структуре подпространств.

Теорема 4. *Для любого $m\in N$ при всех $n\in N$ существует такая функция $f\in T_0^n(m)$, что*

$$|\operatorname{lin}\operatorname{гр}f| = 2^m - 1. \tag{9}$$

Доказательство. Рассмотрим функцию $f\in P_{m,n}$, $m, n\in N$, определенную следующим образом:

$$f(\overline{a}) = \begin{cases} \overline{0}, & \text{если } \overline{a}=\overline{0}; \\ (1,\dots,1), & \text{если } \overline{a}\neq\overline{0}. \end{cases} \tag{10}$$

Так как $f(\overline{0})=\overline{0}$, то $f\in T_0^n(m)$. В силу леммы 1 для любого вектора $\overline{a}\in \in \operatorname{гр}f\setminus\{\overline{0}\}$ множество $\{\overline{0}, \overline{a}\}$ является подпространством пространства $GF^{m+n}(2)$. Покажем, что $\{\overline{0}, \overline{a}\}\in \operatorname{lin}\operatorname{гр}f$ $(\overline{a}\in \operatorname{гр}f\setminus\{\overline{0}\})$.

Предположим противное, т. е. что $\{\overline{0}, \overline{a}\}\notin \operatorname{lin}\operatorname{гр}f$. Так как $\{\overline{0}, \overline{a}\}\subseteq \operatorname{гр}f$, то существует такое максимальное по включению подпространство V пространства $GF^{m+n}(2)$, что $\{\overline{0}, \overline{a}\}\subset V\subseteq \operatorname{гр}f$. Из включения $\{\overline{0}, \overline{a}\}\subset V$ вытекает, что $V\setminus\{\overline{0}, \overline{a}\}\neq\emptyset$. Следовательно, существует, по крайней мере, один вектор $\overline{b}\in V\setminus\{\overline{0}, \overline{a}\}$. Так как $\overline{a}, \overline{b}\in V$ и V — линейное подпространство, то $\overline{a}+\overline{b}\in V$. В силу (10)

$$\overline{a}+\overline{b} = (\alpha_1,\dots,\alpha_m,\underbrace{0,\dots,0}_{n \text{ раз}}).$$

А поскольку $\overline{a}\neq\overline{b}$, то $\overline{a}+\overline{b}\neq\overline{0}$. В силу (10) это означает, что $\overline{a}+\overline{b}\notin \notin \operatorname{гр}f$, что противоречит включению $V\subseteq\operatorname{гр}f$. Полученное противоречие показывает, что предположение неверно. Следовательно, $\{\overline{0}, \overline{a}\}\in \operatorname{lin}\operatorname{гр}f$ для всех $\overline{a}\in \operatorname{гр}f\setminus\{\overline{0}\}$. Отсюда вытекает, что

$$\operatorname{lin}\operatorname{гр}f = \{\{\overline{0}, \overline{a}\}\mid \overline{a}\in \operatorname{гр}f\setminus\{\overline{0}\}\}.$$

А так как $|\operatorname{гр}f\setminus\{\overline{0}\}| = 2^m-1$, то $|\operatorname{lin}\operatorname{гр}f| = 2^m-1$, что и требовалось доказать.

Теорема доказана.

Теорема 5. *Для любых $m, n\in N$ и*

$$l = \lfloor \sqrt{2m+0,25}-0,5 \rfloor \tag{11}$$

существует функция $f\in T_0^n(m)$ такая, что множество $\operatorname{lin}\operatorname{гр}f$ содержит последовательность подпространств $V_1,\dots,V_l$, удовлетворяющую следующим условиям:

1) $\operatorname{Dim} V_k = k \quad \forall\, k\in\{1,\dots,l\}$;

2) $V_i\cap V_j=\{\overline{0}\} \quad \forall\, i,j\in\{1,\dots,l\},\ i\neq j$.

Доказательство. Положим

$$B_k = \prod_{i=1}^{k(k-1)/2}(1+x_i),$$

$$C_k = \sum_{i=k(k-1)/2+1}^{k(k+1)/2} x_i, \tag{12}$$

$$D_k = \prod_{i=k(k+1)/2+1}^{m} (1 + x_i).$$

При фиксированном $m \in N$ наибольшим целым решением неравенства $k(k+1)/2 \le m$ является число l, определяемое равенством (11). Это означает, что при каждом фиксированном значении $m \in N$ формулы (12) имеют смысл только для $k \in \{1, \ldots, l\}$. При этом из (12) вытекает, что для всех $k \in \in \{1, \ldots, l\}$ верны эквивалентности

$$B_k = 1 \Leftrightarrow x_1 = \ldots = x_{k(k-1)/2} = 0, \tag{13}$$

$$C_k = 0 \Leftrightarrow x_{k(k-1)/2+1} = \ldots = x_{k(k+1)/2} = 0, \tag{14}$$

$$D_k = 1 \Leftrightarrow x_{k(k+1)/2+1} = \ldots = x_m = 0. \tag{15}$$

Рассмотрим функцию $f \in P_{m,n}$, определенную следующим образом:

$$\mathrm{pr}_j f = \sum_{k=1}^{l} B_k C_k D_k, \quad j = 1, \ldots, n. \tag{16}$$

В силу (14) и (16) $f(\overline{0}) = \overline{0}$ и, следовательно, $f \in T_0^n(m)$. Сопоставим с каждым значением $k \in \{1, \ldots, l\}$ множество векторов

$$V_k = \left\{ \underbrace{0, \ldots, 0}_{k(k-1)/2}, \alpha_1, \ldots, \alpha_k, \underbrace{0, \ldots, 0}_{m-k(k+1)/2}, \underbrace{\beta, \ldots, \beta}_{n} \,\middle|\, \alpha_i \in \{0,1\}\ (i = 1, \ldots, k), \beta = \sum_{i=1}^{k} \alpha_i \right\}. \tag{17}$$

Из (12) – (16) вытекает, что $V_k \subseteq \mathrm{gr} f$ для всех $k \in \{1, \ldots, l\}$. В каждом векторе, принадлежащем множеству V_k, компоненты с номерами $1, \ldots, k(k-1)/2$, $k(k+1)/2+1, \ldots, m$ являются нулевыми. Удаляя эти компоненты, получаем множество векторов

$$V_k' = \left\{ \alpha_1, \ldots, \alpha_k, \underbrace{\beta, \ldots, \beta}_{n} \,\middle|\, \alpha_i \in \{0,1\}\ (i = 1, \ldots, k), \beta = \sum_{i=1}^{k} \alpha_i \right\}.$$

В силу следствия 1 множество V_k' является подпространством пространства $GF^{k+n}(2)$. Это означает, что V_k является подпространством пространства $GF^{m+n}(2)$, причем в силу утверждения 2 $\mathrm{Dim}\, V_k = \mathrm{Dim}\, V_k' = k$.

Покажем, что $V_k \in \mathrm{lin\,gr} f$, $k \in \{1, \ldots, l\}$. Предположим противное, т. е. что $V_k \notin \mathrm{lin\,gr} f$. Тогда существует такое подпространство V пространства $GF^{m+n}(2)$, что $V_k \subset V \subseteq \mathrm{gr} f$. Выберем произвольные векторы

$$\overline{a} = \left(\underbrace{0, \ldots, 0}_{k(k-1)/2}, \alpha_1, \ldots, \alpha_k, \underbrace{0, \ldots, 0}_{m-k(k+1)/2}, \underbrace{\beta, \ldots, \beta}_{n} \right) \in V_k \setminus \{\overline{0}\}$$

и

$$\overline{b} = (\beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_n) \in V \setminus V_k.$$

Рассмотрим вектор

$$\overline{a} + \overline{b} = \left(\beta_1, \ldots, \beta_{k(k-1)/2}, \alpha_1, \ldots, \alpha_k, \beta_{k(k+1)/2+1}, \ldots, \beta_m, \beta + \gamma_1, \ldots, \beta + \gamma_n\right).$$

Так как $\overline{a}, \overline{b} \in V$, то $\overline{a} + \overline{b} \in V$. Из условий $\overline{b} \in V \setminus V_k$ и $V \subseteq \mathrm{gr} f$ вытекает, что, по крайней мере, одна из компонент β_j, где $j \in \{1, \ldots, k(k-1)/2, k(k+1)/2+1, \ldots, m\}$, отлична от нуля. Следовательно, в силу (13) – (16) каждая из компонент $\gamma_1, \ldots, \gamma_n$ не зависит от значений переменных $\alpha_1, \ldots, \alpha_k$. А так как $\beta = \sum_{i=1}^{k} \alpha_i$, то каждая из компонент $\beta + \gamma_1, \ldots, \beta + \gamma_n$ вектора $\overline{a} + \overline{b}$ зависит от значений $\alpha_1, \ldots, \alpha_k$. В силу (13) – (16) это означает, что $\overline{a} + \overline{b} \notin \mathrm{gr} f$. Полученное противоречие показывает, что предположение неверно. Следовательно, $V_k \in \mathrm{lin}\,\mathrm{gr} f$ для всех $k \in \{1, \ldots, l\}$. Итак, показано, что множество $\mathrm{lin}\,\mathrm{gr} f$ содержит такую последовательность подпространств $V_1, \ldots, V_l$, что $\mathrm{Dim}\, V_k = k$ для всех $k \in \{1, \ldots, l\}$. При этом из (17) вытекает, что $V_i \cap V_j = \overline{0}$ при $i \neq j$, $i, j \in \{1, \ldots, l\}$.

Теорема доказана.

4. Основные результаты. Пусть V — подпространство пространства $GF^{m+n}(2)$. Выберем в ортогональном дополнении $V^{\perp}$ произвольный базис $\overline{e}_1, \ldots, \overline{e}_{m+n-\mathrm{Dim}V}$. Обозначим через E_V матрицу порядка $(m+n) \times (m+n-\mathrm{Dim}\, V)$, столбцами которой являются векторы $\overline{e}_1, \ldots, \overline{e}_{m+n-\mathrm{Dim}V}$.

Теорема 6. *Для любой функции* $f \in T_0^n(m)$ *функция*

$$\chi_f = \{ E_V | V \in \mathrm{lin}\,\mathrm{gr} f \} \tag{18}$$

является линейной характеристической функцией множества $\mathrm{gr} f$.

Доказательство. Пусть $f \in T_0^n(m)$. В силу (18) для любого вектора $\overline{a} \in \{0, 1\}^{m+n}$ верна эквивалентность

$$\overline{0} \in \chi_f(\overline{a}) \Leftrightarrow \overline{a} E_V = \overline{0} \quad \text{для некоторого } V \in \mathrm{lin}\,\mathrm{gr} f. \tag{19}$$

По построению столбцы матрицы E_V образуют базис подпространства $V^{\perp}$. Следовательно, для любого вектора $\overline{a} \in \{0, 1\}^{m+n}$ верна эквивалентность

$$\overline{a} E_V = \overline{0} \Leftrightarrow \overline{a} \in V. \tag{20}$$

Из (19) и (20) вытекает, что для любого вектора $\overline{a} \in \{0, 1\}^{m+n}$ верна эквивалентность

$$\overline{0} \in \chi_f(\overline{a}) \Leftrightarrow \overline{a} \in V \quad \text{для некоторого } V \in \mathrm{lin}\,\mathrm{gr} f. \tag{21}$$

По условию $f \in T_0^n(m)$. Следовательно, в силу (5) и (21) для любого вектора $\overline{a} \in \{0, 1\}^{m+n}$ верна эквивалентность

$$\overline{0} \in \chi_f(\overline{a}) \Leftrightarrow \overline{a} \in \mathrm{gr} f.$$

Из последней эквивалентности и вытекает, что χ_f — линейная характеристическая функция множества $\mathrm{gr} f$.

Теорема доказана.

Из утверждения 3 и теоремы 6 вытекает, что решение задачи 1 может быть получено с помощью следующего алгоритма.

Алгоритм.

Шаг 1. Если $f \notin T_0^n(m)$, то $f = f + f(\overline{0})$, $\Omega = \Omega + f(\overline{0})$.

Шаг 2. Построить функцию χ_f, определяемую равенством (18).

Шаг 3. Вычислить $\chi_f(\overline{a})$ для всех $\overline{a} \in \Omega$.

Шаг 4. Если $\overline{0} \in \chi_f(\overline{a})$ для всех $\overline{a} \in \Omega$, то включение (1) верно, иначе включение (1) неверно.

Из теоремы 6 вытекает, что временная и емкостная сложности предложенного алгоритма соответственно равны

$$T = O\left(|\Omega|(m+n)((m+n)|\mathrm{lin\,rp}\, f| - \sum_{V \in \mathrm{lin\,rp}\, f} \mathrm{Dim}\, V) \right), \quad m, n \to \infty,$$

$$V = O\left((m+n)((m+n)|\mathrm{lin\,rp}\, f| + |\Omega| - \sum_{V \in \mathrm{lin\,rp}\, f} \mathrm{Dim}\, V) \right), \quad m, n \to \infty.$$

Из этих оценок вытекает, что решение задачи 1 с помощью предложенного алгоритма имеет полиномиальную сложность (как временную, так и емкостную) тогда и только тогда, когда выполнены условия

$$|\Omega| = O((m+n)^{k_1}), \quad m, n \to \infty,$$

$$|\mathrm{lin\,rp} f| = O((m+n)^{k_2}), \quad m, n \to \infty,$$

для некоторых $k_1, k_2 \in N$.

5. Специальный случай. Пусть V — циклическое подпространство пространства $GF^{m+n}(2)$. Это означает, что

$$(\alpha_1, \ldots, \alpha_{m+n}) \in V \Rightarrow (\alpha_2, \ldots, \alpha_{m+n}, \alpha_1) \in V.$$

Известно, что элементы циклического подпространства могут быть представлены в виде полиномов с коэффициентами из поля $GF(2)$. Такой подход позволяет строить k-мерное циклическое подпространство пространства $GF^{m+n}(2)$ с помощью умножения всех полиномов степени не выше $k-1$ на один и то же полином $p(x)$ степени $m+n-k$. Этот полином $p(x)$ называется порождающим полиномом циклического подпространства V. Полином $h(x)$, определяемый равенством $x^{m+n-1} - 1 = p(x)h(x)$, называется проверочным полиномом для циклического подпространства V. Известно, что полином $h(x)$ удовлетворяет следующему условию: для любого многочлена $c(x)$ степени не выше, чем $m+n-1$, верна эквивалентность

$$c(x) \in V \Leftrightarrow R_{x^{m+n-1}-1}(h(x)c(x)) = 0,$$

где $R_{a(x)}(b(x))$ означает остаток от деления $b(x)$ на $a(x)$. Следовательно, если $V \in \mathrm{lin\,rp} f$ — циклическое подпространство, то умножение вектора $\overline{a} \in \Omega$ на матрицу E_V можно заменить умножением полинома $a(x)$ на проверочный полином $h(x)$. Из изложенного вытекает, что с помощью линейных сдвиговых регистров с линейной обратной связью может быть реализована та и только та часть линейной характеристической функции χ_f, которая соответствует циклическим подпространствам, принадлежащим множеству $\mathrm{lin\,rp} f$.

1. *Дискретная* математика и математические вопросы кибернетики / Под общ. ред. С. В. Яблонского, О. Б. Лупанова. – М.: Наука, 1974. – Т. 1. – 215 с.
2. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.

Получено 26.04.93