А. В. Т а р а с о в (Москва, МИРЭА). **Системы образующих множеств выполняющих векторов булевых биюнктивных функций.**

Обозначения: V_n — множество двоичных векторов длины n; Bi — класс биюнктивных функций, т. е. функций, представимых в виде 2-КНФ:

$$f(x_1, \ldots, x_k) = \bigwedge_{i=1}^{t} (x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}}) \tag{1}$$

$Bi(n)$ — множество биюнктивных функций, зависящих от n переменных; v — тернарное преобразование пространства V_n, задаваемое равенством $v(\alpha, \beta, \gamma) = \alpha\beta \vee \alpha\gamma \vee \beta\gamma, \alpha, \beta, \gamma \in V_n$; E_f — множество выполняющих векторов булевой функции $f(x_1, \ldots, x_n)$; f_M — для заданного такая $M \subset V_n$ — булева функция, что $E_{f_M} = M$; $M_{ij}^{ab} = \{\alpha = (c_1, \ldots, c_n) \in M : c_i = a, c_j = b\}$; $\Lambda = \{(i, j, a, b : 1 \leqq i < j \leqq n, a, b \in \{0, 1\}\}$.

Теорема (см. [1]). *Булева функция $f(x_1, \ldots, x_k)$ биюнктивна тогда и только тогда, когда для любых трех векторов $\alpha, \beta, \gamma \in E_f$ вектор $\delta = v(\alpha, \beta, \gamma)$ является выполняющим вектором функции f.*

Рассмотрим универсальную алгебру $\Omega_n = (V_n, v)$. Пусть $M \subset V_n$. Через $\langle M \rangle$ обозначим подалгебру, порожденную множеством M. Множество M будем называть *v-замкнутым*, если $\langle M \rangle = M$ и *v-полным*, если $\langle M \rangle = V_n$. Множество M, следуя П. В. Ролдугину, назовем *комбинаторно полным порядка* 2, если $M_{ij}^{ab} \neq \varnothing$ для любых i, j, a, b таких, что $1 \leqq i < j \leqq n, a, b \in \{0, 1\}$.

Теорема 1. *Множество M является v-замкнутым тогда и только тогда, когда f_M — биюнктивна, и v-полным тогда и только тогда, когда M комбинаторно полно порядка* 2.

Теорема 2. *Пусть f — булева функция от n переменных. Наилучший верхний биюнктивный аналог g функции f определяется равенством $E_g = \langle E_f \rangle$.*

Пусть $M \subset V_n$. Упорядоченный набор $\lambda = (i, j, a, b) \in \Lambda$ будем называть 2-*запретом* множества M, если $M_{ij}^{ab} = \varnothing$. Множество 2-запретов множества M обозначим $Z_2(M)$. Для булевой функции f положим $Z(f) = Z(E_f)$. Число 2-запретов для каждого вектора $\alpha \in V_n$ как одноэлементного множества равно C_n^2. Положим $Z(\alpha) = Z(\{\alpha\})$.

Теорема 3. *Для всякой биюнктивной функции f вида* (1) *условие $\langle M \rangle = E_f$ выполняется тогда и только тогда, когда*

$$Z(f) = \bigcup_{\alpha \in M} Z(\alpha). \tag{2}$$

При этом задача построения такого множества M имеет полиномиальную от n сложность при задании f произвольной 2-КНФ вида (1).

В силу данной теоремы задача построения базиса (минимальной по включению системы образующих) эквивалентна задаче построения минимального покрытия множества $Z(f)$ в соответствии с (2) и сводится к следующей задаче дискретного программирования.

Пусть построено некоторое множество M, удовлетворяющее теореме. Положим $|Z(f)| = k, |M| = m$, и пусть множество $N \subset M$ образует базис. Пусть, далее, $Z(f) = \{\lambda_1, \ldots, \lambda_k\}$, $N = \{\alpha_1, \ldots, \alpha_m\}$. Составим 0-1-матрицу $A = (a_{ij})_{k \times m}$, в которой $a_{ij} = 1 \Leftrightarrow \lambda_i \in Z(\alpha_j)$. Если положить $y_j = 0$ при $Z(\alpha_j) \notin N$, $y_j = 1$ при $Z(\alpha_j) \in N$, $j = 1, 2, \ldots, m$, то задача построения базиса превращается в задачу минимизации функции $y_1 + y_2 + \cdots + y_m$ при условиях $a_{i1}y_1 + a_{i2}y_2 + \cdots + a_{ik}y_k > 0$, $i = 1, 2, \ldots, m$.

СПИСОК ЛИТЕРАТУРЫ

1. *Горшков С. П.* Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений. — Обозрение прикл. и промышл. матем. Сер. дискретн. матем., 1995, т. 2, в. 3, с. 325–398.