ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 5
2012

Ф. К. Алиев, А. В. Зайцева, И. В. Костенюк, А. Г. Сенцов (Москва, ТВП, МГТУ, Институт нанотехнологий микроэлектроники РАН). **Допустимые пары систем подмножеств множества двоичных векторов.**

Пусть V_2^n — множество двоичных векторов с n координатами $(n \in \mathbf{N})$. Обозначим A и B два непустых подмножества множества V_2^n, объединение которых совпадает с множеством V_2^n, т. е. $\varnothing \neq A \subset V_2^n$, $\varnothing \neq B \subset V_2^n$, $A \cap B = \varnothing$, $A \cup B = V_2^n$. Для этих множеств A и B можно указать такие системы подмножеств $\{A_1, A_2, \ldots, A_n\}$ и $\{B_1, B_2, \ldots, B_n\}$, что:

1) при $i \neq j$ справедливы равенства $A_i \cap A_j = \varnothing$ и $B_i \cap B_j = \varnothing$;

2) $A_1 \cup A_2 \cup \cdots \cup A_n = A$, $B_1 \cup B_2 \cup \cdots \cup B_n = B$;

3) для любого $k \in \{1, 2, \ldots, n\}$ множество векторов A_k таково, что если $A_k \neq \varnothing$, то каждый вектор $a^{(k)} \in A_k$ обладает тем свойством, что при инвертировании любых его координат в количестве меньшем, чем k, и неизменности остальных координат получается вектор, принадлежащий множеству A; но существует набор ровно из k координат вектора $a^{(k)}$, при инвертировании которых и неизменности остальных координат получается вектор, принадлежащий множеству B;

4) для любого $k \in \{1, 2, \ldots, n\}$ множество векторов B_k таково, что если $B_k \neq \varnothing$, то каждый вектор $b^{(k)} \in B_k$ обладает тем свойством, что при инвертировании любых его координат в количестве меньшем, чем k, и неизменности остальных координат получается вектор, принадлежащий множеству B; но существует набор ровно из k координат вектора $b(k)$, при инвертировании которых и неизменности остальных координат получается вектор, принадлежащий множеству A.

При выполнении вышеуказанных требований относительно систем подмножеств $\{A_1, A_2, \ldots, A_n\}$ и $\{B_1, B_2, \ldots, B_n\}$ множества V_2^n будем говорить, что представление множества V_2^n в виде $V_2^n = A_1 \cup A_2 \cup \cdots \cup A_n \cup B_1 \cup B_2 \cup \cdots \cup B_n$ является *допустимым разбиением* (ДР) множества V_2^n, а пару систем подмножеств $(\{A_1, A_2, \ldots, A_n\}, \{B_1, B_2, \ldots, B_n\})$ множества V_2^n назовем *допустимой парой систем подмножеств* (ДПСП) множества V_2^n.

Заметим, что ДР не является разбиением в смысле математического понятия «разбиение» [1], так как среди множеств $A_1, A_2, \ldots, A_n, B_1, B_2, \ldots, B_n$ допускаются и пустые множества.

Для ДПСП $(\{A_1, A_2, \ldots, A_n\}, \{B_1, B_2, \ldots, B_n\})$ множества V_2^n будем использовать также и более компактное обозначение (A_1^n, B_1^n).

Для мощностей $y_i = |A_i|$, $z_i = |B_i|$, где $i = 1, 2, \ldots, n$, очевидно, справедливы следующие соотношения: $y_i \geqslant 0$, $z_i \geqslant 0$, $Y = \sum_{i=1}^n y_i \geqslant 1$, $Z = \sum_{i=1}^n z_i \geqslant 1$, $Y + Z = |V_2^n| = 2^n$.

Множество всех ДПСП множества V_2^n обозначим $S(V_2^n)$. С каждой ДПСП $(A_1^n, B_1^n) \in S(V_2^n)$ и действительным числом q, удовлетворяющим двойному неравенству $0 < q \leqslant 1/2$, свяжем величину

$$F^{(q)}_{(A_1^n,B_1^n)}(y_1,y_2,\dots,y_n;z_1,z_2,\dots,z_n)=\frac{1-q}{2^n}\sum_{i=1}^{n} iy_i+\frac{q}{2^n}\sum_{i=1}^{n} iz_i.$$

Положим

$$F_{\min}(V_2^n;q)=\min_{(A_1^n,B_1^n)\in S(V_2^n)} F^{(q)}_{(A_1^n,B_1^n)}(y_1,y2,\dots,y_n;z_1,z_2,\dots,z_n).$$

ДПСП $(A_1^n,B_1^n)\in S(V_2^n)$ назовем *q-оптимальной парой систем подмножеств* (q ОПСП) множества V_2^n, если справедливо равенство $F^{(q)}_{(A_1^n,B_1^n)}(y_1,y_2,\dots y_n; z_1,z_2,\dots,z_n)=F_{\min}(V_2^n;q)$.

Некоторые результаты общего характера о ДПСП приведем в виде следующего утверждения.

Утверждение. А. *Для любой* ДПСП $(A_1^n,B_1^n)\in S(V_2^n)$ *выполняются следующие условия* :

a1) *если при некотором числе* $k\in\{2,3,\dots,n\}$ *справедливо неравенство* $A_k\neq\varnothing$, *то подмножества* $A_1,A_2,\dots,A_{k-1}$ *являются непустыми подмножествами*;

a2) *если при некотором числе* $k\in\{2,3,\dots,n\}$ *справедливо неравенство* $B_k\neq\varnothing$, *то подмножества* $B_1,B_2,\dots,B_{k-1}$ *являются непустыми подмножествами.*

B. *Пусть* ДПСП $(A_1^n,B_1^n)\in S(V_2^n)$. *Положим* $\widetilde{A}_1=A_1$, *подмножества* $\widetilde{A}_2,\dots,\widetilde{A}_n$ *— пустые множества,* $\widetilde{B}_k=B_k\cup A_{k+1}$, *где* $k\in\{1,2,\dots,n-1\}$, $\widetilde{B}_n=B_n$. *Тогда*:

b1) $(\widetilde{A}_1^n,\widetilde{B}_1^n)\in S(V_2^n)$;

b2) *для любого действительного числа* q, *удовлетворяющего двойному неравенству* $0<q\leqslant 1/2$, *справедливо неравенство*

$$F^{(q)}_{(\widetilde{A}_1^n,\widetilde{B}_1^n)}(y_1,y_2,\dots,y_n;z_1,z_2,\dots,z_n)\leqslant F^{(q)}_{(A_1^n,B_1^n)}(y_1,y_2,\dots,y_n;z_1,z_2,\dots,z_n),$$

при этом нестрогое неравенство обращается в строгое тогда и только тогда, когда выполняется условие $\cup_{k=2}^n A_k=\varnothing$.

C. *Если при некотором действительном числе* q, *удовлетворяющем двойному неравенству* $0<q\leqslant 1/2$, ДПСП $(A_1^n,B_1^n)\in S(V_2^n)$ *является* q ОПСП, *то подмножества* $A_2,A_3,\dots,A_n$ *являются пустыми подмножествами.*

Необходимость исследования множества ДПСП $S(V_2^n)$ и выделения в нем q ОПСП для различных действительных чисел q, удовлетворяющих двойному неравенству $0<q\leqslant 1/2$, возникает в связи с решением ряда задач в научно-практической области защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982, 256 с.