

**А. В. Шаповалов** (Москва, ТВП). **Об определении несовместности реализаций случайной системы псевдобоулевых уравнений с модифицируемыми переменными.**

Пусть  $\Phi_i = \{f_{i,1}, \dots, f_{i,|\Phi_i|}\}$  — упорядоченное множество псевдобоулевых функций, существенно зависящих ровно от  $i$  переменных (переменные принимают значения в множестве  $B = \{0, 1\}$ ), а функции принимают значения в конечном множестве  $A$ ,  $A \subset R$ ,  $|A| > 1$ ,  $i = 0, 1, \dots, m$ .

Случайная система уравнений  $S$  относительно неизвестных  $x_1, \dots, x_n$  состоит из  $M$  выбираемых последовательно, случайно и независимо друг от друга уравнений вида

$$f_{i,j}(x_{s_1} \oplus \delta_{s_1}, \dots, x_{s_i} \oplus \delta_{s_i}) = a. \quad (1)$$

Вероятность появления уравнения с функцией  $f_{i,j}$  в левой части и элементом  $a$  в правой части равна  $c_{i,j,a}$  для каждого набора  $(i, j, a)$ , где  $i = 0, 1, \dots, m$ ,  $j = 1, \dots, |\Phi_i|$ ,  $a$  принадлежит области значений функции  $f_{i,j}$ , сумма  $c_{i,j,a}$  по указанным наборам  $i, j, a$  равна 1. Выбор упорядоченного множества неизвестных  $\{x_{s_1}, \dots, x_{s_i}\}$  для каждого уравнения с функцией из  $\Phi_i$  осуществляется независимо, случайно и равновероятно по схеме без возвращения из всех  $n(n-1) \cdots (n-i+1)$  возможных упорядоченных наборов неизвестных по  $i$  штук. Все неизвестные  $x_{s_1}, \dots, x_{s_i}$  в каждом уравнении вида (1) модифицируются случайно, независимо от других уравнений и других переменных в этом уравнении с помощью прибавления к ним аддитивных добавок  $\delta_{s_1}, \dots, \delta_{s_i}$  соответственно, являющихся независимыми, одинаково распределенными случайными величинами, принимающими значения 1 и 0 с вероятностями  $p$  и  $q = 1 - p$ ,  $0 < p < 1$ .

Вероятность совместности  $\mathbf{P}_c(S)$  системы  $S$  равна сумме вероятностей ее совместных реализаций. Если существует такая функция  $Q(n)$ , что при  $n \rightarrow \infty$ :  $\mathbf{P}_c(S) \rightarrow 1$ , если  $M(n) = o(Q(n))$ , и  $\mathbf{P}_c(S) \rightarrow 0$ , если  $Q(n) = o(M(n))$ , то она называется *пороговой функцией совместности системы  $S$* . Пусть  $t_{i,j,a}^{(b)}$  — число однозначно определяющихся из уравнения (1) при  $\delta_{s_1} = \dots = \delta_{s_i} = 0$  переменных, равных  $b$ ,  $c^{(b)} = \sum_{(i,j,a)} c_{i,j,a} t_{i,j,a}^{(b)}$ ,  $b \in B$ .

Алгоритм **А** определения несовместности реализаций  $S$  заключается в определении значений неизвестных из уравнений с однозначно определяющимися переменными. При появлении противоречия между определенным значением неизвестного из очередного уравнения с полученным ранее значением этого неизвестного делается вывод о несовместности системы уравнений. Если уравнения закончились и противоречие не выявлено, то не делается никакого вывода о совместности системы.

Обозначим  $\pi_n$  сумму вероятностей реализации системы  $S$ , несовместность которых определит алгоритм **А**.

**Теорема.** Система  $S$  имеет пороговую функцию совместности  $\sqrt{n}$  тогда и только тогда, когда  $c^{(0)} + c^{(1)} > 0$ . В этом случае  $\pi_n \sim 1 - \mathbf{P}_c(S)$ ,  $\mathbf{P}_c(S) \sim e^{-c^2(pq(c^{(0)} - c^{(1)})^2 + c^{(0)}c^{(1)})}$  при  $M \sim c\sqrt{n}$ ,  $c > 0$ ,  $n \rightarrow \infty$ .

В условиях теоремы алгоритм **А** имеет трудоемкость  $O(\sqrt{n})$  и такую же предельную надежность, как и алгоритм полного перебора решений. Данная задача для нескольких случайных систем уравнений с одной функцией в левой части уравнений ранее решалась В. А. Копытцевым.