Секция «Дискретная математика и математическая кибернетика»

О точной расшифровке линейных булевых функций

Быстрыгова Анастасия Викторовна

Студент (бакалавр)

Филиал Московского государственного университета имени М.В.Ломоносова в г.Ташкенте, Ташкент, Узбекистан

E-mail: anastasiya.bistrigova@gmail.com

Рассматривается задача точной расшифровки функций вида $a_0x_0 \oplus a_1x_1 \oplus ... \oplus a_{n-1}x_{n-1}$, $a_i \in \{0,1\}$, $\sum_{i=0}^{n-1} a_i = k$, где $\oplus$ — означает сложение по модулю 2. Обозначим через $\varphi(n,k)$ сложность расшифровки запросами на значение вышеупомянутых функций. Через $]a[$ обозначим наименьшее целое число не меньшее a, через $[a]$ обозначим наибольшее целое число не большее a. Под $\log n$ будем понимать двоичный логарифм от n.

Теорема 1. *Для любого натурального n, $n > 2$, справедливы неравенства* $2]\log n[-2 \leqslant \varphi(n,2) \leqslant 2]\log n[-1$, *причем если* $\log n - [\log n] \in \{0\} \cup (1/2, 1)$, *то* $\varphi(n,2) = 2]\log n[-1$.

Теорема 2. *Для любого натурального n, $n > 5$, справедливы соотношения*

1) $3]\log n[-4 \leqslant \varphi(n,3) \leqslant 3]\log n[-2$, *если* $\log n - [\log n] \in (0, 1/3]$

2) $3]\log n[-3 \leqslant \varphi(n,3) \leqslant 3]\log n[-2$, *если* $\log n - [\log n] \in (1/3, 2/3]$

3) $\varphi(n,3) = 3]\log n[-2$, *если* $\log n - [\log n] \in \{0\} \cup (2/3, 1)$.

Теорема 3. *Для любого натурального n, $n > 5$, $4 \leqslant k < n/2$ имеет место неравенство:*

$$\varphi(n,k) \leqslant (k - 2^{[\log k]} + 2)k^{[\log k]/2 \cdot}]\log n[^{[\log k]} + \\ + k^{([\log k]+1)/2 \cdot}]\log n[^{[\log k]-1} + k]\log n[/2.$$

Слова благодарности

Автор выражает благодарность д.ф.-м.н. профессору Э.Э.Гасанову за постановку задачи и помощь в работе.