С. П. Горшков, **А. В. Двинянинов** (Москва, ТВП). **Нижняя и верхняя оценки порядка аффинности отображений** $V_n \to V_n$**.**

Введем обозначения: N — множество натуральных чисел, $N_0 = N \cup \{0\}$; V_n — n-мерное пространство булевых векторов, $n \in N_0$; Φ_n — множество всех отображений $V_n \to V_n$. Если действительные функции $g(n)$, $h(n)$ определены для всех натуральных $n \in N$ и существует такое $n_0 \in N$, что для всех $n \geqslant n_0$ выполняется $g(n) < h(n)$, то будем записывать $g(n) \widetilde{<} h(n)$.

Всякое отображение $F \in \Phi_n$ записывается системой координатных булевых функций $F = \{f_1(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n)\}$.

Отображение F называется *линейным* (*аффинным*), если все его координатные функции линейны (аффинны).

Введем еще некоторые определения, которые нами заимствованы из учебного пособия [1, с. 163–164].

Отображение $F \in \Phi_n$ *аффинно* на множестве M, где $M \subseteq V_n$, если найдется такое аффинное отображение $A \in \Phi_n$, что $F(\alpha) = A(\alpha)$ при любом $\alpha \in M$. Тогда отображение A назовем *линеаризующим* F *на множестве* M.

Пусть $M_1, M_2, \ldots, M_r$ — разбиение множества V_n, $A_1, A_2, \ldots, A_r$ — отображения, линеаризующие F, соответственно, на множествах $M_1, M_2, \ldots, M_r$. При этом r назовем *порядком разбиения множества* V_n, линеаризующего F. *Порядком аффинности отображения* F (обозначим его $\mathrm{ard}_a F$) назовем наименьший из порядков разбиений множества V_n, линеаризующих F.

Дальнейшие определения введены авторами данного доклада. Пусть $\mathrm{ard}_a \Phi_n = \max_{F \in \Phi_n} \mathrm{ard}_a F$. Величину $\mathrm{ard}_a \Phi_n$ назовем *порядком аффинности* Φ_n (или коротко: *порядком аффинности*).

Теорема 1. *При* $n \geqslant 2$ *для порядка аффинности справедлива нижняя оценка* $2^n/n^2 < \mathrm{ard}_a \Phi_n$.

Теорема 2. *Для порядка аффинности* Φ_n *справедлива верхняя асимптотическая оценка* $\mathrm{ard}_a \Phi_n \widetilde{<} 1,01 \cdot 2^n/n$.

СПИСОК ЛИТЕРАТУРЫ

1. *Фомичев В.М.* Дискретная математика и криптология. М.: Диалог–МИФИ, 2003, 397 с.