Секция «Математика и механика»

Нижняя граница скорости дизъюнктивных кодов.

Полянский Никита Андреевич
Студент
Московский государственный университет имени М.В. Ломоносова, Механико-математический факультет, Москва, Россия
E-mail: nikitapolyansky@gmail.com

Пусть N, t, s, и ℓ - целые числа, $1 \leq s < t$, $1 \leq \ell \leq t - s$. Двоичную $(N \times t)$-матрицу с N строками и t столбцами будем называть кодом X длины N и объема t.

Определение 1. [1]. Код X называется дизъюнктивным свободным от перекрытий (s, ℓ)-кодом (кратко, СП (s, ℓ)-кодом), если для любых двух непересекающихся множеств $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| =$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, существует строка $i \in [N]$, для которой

$$x_i(j) = 0 \quad \text{для любого}\, j \in \mathcal{S}, \quad \text{а} \quad x_i(k) = 1 \quad \text{для любого} \quad k \in \mathcal{L}.$$

Учитывая очевидную симметрию по s и ℓ, обозначим через $t_{cf}(N, s, \ell) = t_{cf}(N, \ell, s)$ - максимальный объем СП (s, ℓ)-кодов длины N, а через $N_{cf}(t, s, \ell) = N_{cf}(t, \ell, s)$ обозначим минимальное число строк СП (s, ℓ)-кодов объема t и определим скорость СП (s, ℓ)-кодов:

$$R(s, \ell) = R(\ell, s) \varlimsup_{N \to \infty} \frac{\log_2 t_{cf}(N, s, \ell)}{N} = \varlimsup_{t \to \infty} \frac{\log_2 t}{N_{cf}(t, , \ell)}.$$

Центральным результатом настоящей работы является теорема 1, в которой с помощью метода случайного кодирования на ансамбле равновесных двоичных кодов найдена нижняя граница $\underline{R}(s, \ell)$ для скорости $R(s, \ell)$, $2 \leq \ell \leq s$, и исследована асимптотика функции $\underline{R}(s, \ell)$, когда $s \to \infty$ и $\ell \geq 2$ фиксировано.

Теорема 1. (Граница случайного кодирования $\underline{R}(s, \ell)$.) Пусть $2 \leq l \leq s$. Тогда скорость СП (s, ℓ)-кодов

$$R(s, \ell) \geq \underline{R}(s, \ell) \ \frac{1}{s + \ell - 1} \max_{0 < z < 1} T(z, s, \ell),$$

где

$$T(z, s, \ell) \frac{\ell z^s (1 - z)^\ell}{1 - z^s (1 - z)^\ell} \log_2 \left[\frac{z}{1 - z} \right] + (s + \ell - 1) \times$$

$$\times \log_2 \left[1 - z^s (1 - z)^\ell \right] - (s + \ell) \frac{z - z^s (1 - z)^\ell}{1 - z^s (1 - z)^\ell} \log_2 \left[1 - z^{s-1} (1 - z)^\ell \right].$$

Если $s \to \infty$ и $\ell \geq 2$ фиксировано, то для нижней границы $\underline{R}(s, \ell)$ справедливо асимптотическое равенство

$$\underline{R}(s, \ell) = \frac{e^{-\ell} \ell^{\ell + 1} \log_2 s}{s^{\ell + 1}} (1 + o(1)), \quad s \to \infty, \quad \ell = 2, 3, \ldots.$$

Следующая теорема для скорости $R(s, l)$, СП (s, l)-кодов, $1 \leq \ell \leq s$, устанавливает более точную нижнюю асимптотическую границу.

Теорема 2. Для любого фиксированного $l = 1, 2, \ldots$ и $s \to \infty$ скорость $R(s, \ell)$ удовлетворяет асимптотическому неравенству

$$R(s,\ell) \geq \left(\frac{l+1}{e}\right)^{l+1} \frac{\log_2 s}{s^{l+1}}(1+o(1)), \qquad \ell = 1, 2, \ldots, \quad s \to \infty.$$

Литература

1. *Mitchell C.J, Piper F.C.* Key storage in Secure Networks // Discrete Applied Mathematics. 1988. V. 21. P. 215-228.

2. D'yachkov A.G., Rykov V.V., Rashad A.M. Superimposed Distance Codes // Problems of Control and Inform. Theory. 1989. V. 18. № 4. P. 237-250.

3. Чисар И., Кернер Я. Теория информации. Теоремы кодирования для дискретных систем без памяти. М.: Мир, 1985.

4. Лебедев В.С. Асимптотическая верхняя граница скорости кодов, свободных от (w, r)-перекрытий // Пробл. передачи информ. 2003. Т. 39. № 4. С. 3-9.

5. Дьячков А.Г., Воробьев И.В., Полянский Н.А., Щукин В.Ю. Границы скорости дизъюнктных кодов // 2014 Проблемы передачи информации, т.50, вып. 1, С.47-78.

Слова благодарности

Автор благодарен за идеи, замечания и предложения своему научному руководителю Дьячкову Аркадию Георгиевичу.