ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 2**

УДК 621.391 : 519.724

© 2021 г. **В.С. Лебедев**[1], **Н.А. Полянский**[2]

КОДИРОВАНИЕ В Z-КАНАЛЕ ПРИ БОЛЬШОМ ЧИСЛЕ ОШИБОК

Доказано, что максимальное число слов в коде, исправляющем долю $1/4+\varepsilon$ асимметричных ошибок в Z-канале, равно $\Theta(\varepsilon^{-3/2})$ при $\varepsilon \to 0$.

Ключевые слова: Z-канал, минимальное расстояние, равновесный код.

DOI: 10.31857/S0555292321020029

§ 1. Введение

В теории кодирования для моделирования некоторых асимметричных систем передачи и хранения информации используется Z-канал. В этом двоичном канале символ 0 передается всегда безошибочно. При передаче символа 1 может возникнуть ошибка, поэтому на приеме может быть получен как символ 1, так и 0. Мы рассмотрим модель передачи информации, когда число ошибок при передаче n символов ограничено числом τn для некоторого действительного числа τ, $0 \leqslant \tau \leqslant 1$.

Для данного двоичного слова $\boldsymbol{x} \in \{0,1\}^n$ определим Z-шар с центром в $\boldsymbol{x}$ и относительным радиусом τ, куда включим всевозможные слова, которые могут быть получены при передаче $\boldsymbol{x}$ по Z-каналу с не более чем τn ошибками. Для фиксированных параметров τ и n задача кодирования состоит в том, чтобы найти код $\mathcal{C} \subseteq \{0,1\}^n$, такой что для любых различных $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ соответствующие Z-шары с центрами в $\boldsymbol{x}$ и $\boldsymbol{y}$ и относительными радиусами τ не пересекались. При выполнении этого условия будем говорить, что код может исправить долю τ (асимметричных) ошибок в Z-канале. Отметим, что параметры кодов, исправляющих ошибки в Z-канале, исследовались в большом количестве работ. В частности, известно [1, 2], что асимптотическая скорость кодов, исправляющих долю τ асимметричных ошибок, равна асимптотической скорости кодов, исправляющих ту же самую долю τ ошибок в двоичном симметричном канале. Под двоичным симметричным каналом мы будем понимать канал, в котором при передаче как символа 0, так и символа 1 может произойти ошибка.

Из границы Плоткина [3] следует, что мощность кода, исправляющего долю $1/4+\varepsilon$ симметричных ошибок, ограничена сверху величиной $1+1/(4\varepsilon)$. Таким образом, можно сделать вывод, что асимптотическая скорость кодов, исправляющих долю $1/4+\varepsilon$ ошибок в Z-канале, равна нулю. Однако остаются и другие вопросы, касающиеся границ существования таких кодов. В частности, можно ли утверждать, что мощность кода $\mathcal{C} \subseteq \{0,1\}^n$, исправляющего долю $1/4+\varepsilon$ ошибок в Z-канале, ограничена некоторой функцией от ε, т.е. оценка $|C| \leqslant f(\varepsilon)$ не зависит от длины кода n.

[1] Исследование выполнено в ИППИ РАН при частичной финансовой поддержке Российского фонда фундаментальных исследований (номера проектов 19-01-00364 и 20-51-50007).

[2] Исследование выполнено в Техническом университете Мюнхена и Сколковском институте науки и технологий при частичной поддержке гранта немецкого научно-исследовательского сообщества (номер проекта WA3907/1-1).

В работе [2] утверждалось, что подобная граница выполнена лишь при $\varepsilon > 1/12$. При доказательстве этого утверждения автор [2] допустил ошибку при упрощении задачи линейного программирования, решение которой дает максимальное количество слов в коде, исправляющем долю $1/4 + \varepsilon$ ошибок в Z-канале. В данной статье мы покажем, что максимальное число слов в коде, исправляющем долю $1/4 + \varepsilon$ асимметричных ошибок, равно $\Theta(\varepsilon^{-3/2})$ при $\varepsilon \to 0$. Таким образом, в теореме 1 мы докажем верхнюю границу $|\mathcal{C}| \leqslant \varepsilon^{-3/2}(1 + o(1))$, а в теореме 2 построим код длины $\exp(O(\varepsilon^{-3/2}))$ и объема $|\mathcal{C}| \geqslant \dfrac{3\sqrt{3}}{128}\varepsilon^{-3/2}(1+o(1))$. Отметим, что подобный вопрос для двоичного симметричного канала был ранее разрешен в более строгой форме. Из результатов работ [3–5] следует, что максимальное число слов в коде, исправляющем долю $1/4 + \varepsilon$ симметричных ошибок, равно $(4\varepsilon)^{-1}(1 + o(1))$ при $\varepsilon \to 0$.

§ 2. Обозначения, определения и вспомогательные результаты

Множество целых чисел $\{i, i + 1, \ldots, j\}$ для некоторых целых чисел i и j, для которых выполнено $i \leqslant j$, будем обозначать через $[i, j]$. Если $i = 1$, то будем использовать сокращение $[j]$. Для обозначения векторов будем использовать полужирные символы, например, $\boldsymbol{x}$, а i-ю координату вектора $\boldsymbol{x}$ будем записывать как x_i. Вектор, состоящий из всех нулей, будем обозначать через $\mathbf{0}$. Пусть асимметричная функция $\Delta(\boldsymbol{x}, \boldsymbol{y})$, зависящая от двух векторов $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$, равна числу координат $i \in [n]$, таких что $x_i = 1$ и $y_i = 0$. Расстояние Хэмминга между двумя векторами $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ равно $d_H(\boldsymbol{x}, \boldsymbol{y}) = \Delta(\boldsymbol{x}, \boldsymbol{y}) + \Delta(\boldsymbol{y}, \boldsymbol{x})$. Весом вектора $\boldsymbol{x} \in \{0,1\}^n$ будем называть величину $\mathrm{wt}(\boldsymbol{x}) = d_H(\boldsymbol{x}, \mathbf{0})$, а относительным весом $\boldsymbol{x}$ – величину $\mathrm{wt}(\boldsymbol{x})/n$. Определим *Z-шар* и *S-шар* с центром в $\boldsymbol{x} \in \{0,1\}^n$ и радиусом t следующим образом:

$$B_t^{\mathrm{Z}}(\boldsymbol{x}) = \{\boldsymbol{y} \in \{0,1\}^n : \ y_i \leqslant x_i \ \forall i \in [n],\ \Delta(\boldsymbol{x}, \boldsymbol{y}) \leqslant t\},$$
$$B_t^{\mathrm{S}}(\boldsymbol{x}) = \{\boldsymbol{y} \in \{0,1\}^n : \ d_H(\boldsymbol{x}, \boldsymbol{y}) \leqslant t\}.$$

Кодом $\mathcal{C} \subseteq \{0,1\}^n$ будем называть произвольное подмножество двоичных векторов одной длины. *Мощность* (число слов) кода $\mathcal{C}$ будем обозначать через $|\mathcal{C}|$. Код $\mathcal{C} \subseteq \{0,1\}^n$ назовем *w-равновесным*, если вес всякого слова $\boldsymbol{x} \in \mathcal{C}$ равен $\mathrm{wt}(\boldsymbol{x}) = w$. Будем говорить, что код $\mathcal{C}$ *исправляет* t асимметричных (симметричных) ошибок, если для любых различных $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ соответствующие Z-шары (S-шары) с центрами в $\boldsymbol{x}$ и $\boldsymbol{y}$ и радиусами t не пересекаются, т.е. $B_t^{\mathrm{Z}}(\boldsymbol{x}) \cap B_t^{\mathrm{Z}}(\boldsymbol{y}) = \varnothing$ ($B_t^{\mathrm{S}}(\boldsymbol{x}) \cap B_t^{\mathrm{S}}(\boldsymbol{y}) = \varnothing$). Заметим, что код $\mathcal{C}$ исправляет t асимметричных ошибок тогда и только тогда, когда для любых различных $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ выполнено неравенство $\max(\Delta(\boldsymbol{x}, \boldsymbol{y}), \Delta(\boldsymbol{y}, \boldsymbol{x})) > t$. Код $\mathcal{C} \subseteq \{0,1\}^n$ исправляет *долю* τ асимметричных (симметричных) ошибок, если он исправляет t асимметричных (симметричных) ошибок для $t = \lceil \tau n \rceil$. В следующей лемме отметим очевидный, но важный результат [6].

Лемма 1. *Пусть код $\mathcal{C} \subseteq \{0,1\}^n$ является w-равновесным. Код $\mathcal{C}$ исправляет t асимметричных ошибок тогда и только тогда, когда он исправляет t симметричных ошибок.*

Далее напомним два известных результата, доказанных в работах [3] и [1] соответственно.

Лемма 2. *Пусть код $\mathcal{C} \subseteq \{0,1\}^n$ исправляет t, $t > n/4$, симметричных ошибок. Тогда мощность кода $\mathcal{C}$ ограничена следующим образом*:

$$|\mathcal{C}| \leqslant 2\left\lfloor \frac{2t+2}{4t+3-n} \right\rfloor.$$

Лемма 3. *Пусть код $\mathcal{C} \subseteq \{0,1\}^n$ является w-равновесным и исправляет t симметричных ошибок. Если выполнено соотношение $t + 1 \leqslant w \leqslant (n - \sqrt{n^2 - 4tn})/2$,*

то мощность кода $\mathcal{C}$ ограничена следующим образом:

$$|\mathcal{C}| \leqslant \left\lfloor \frac{tn}{w^2-(w-t)n} \right\rfloor .$$

§ 3. Верхняя граница

В следующем утверждении мы получим верхнюю границу на мощность кода, исправляющего долю $1/4+\varepsilon$ асимметричных ошибок. Идея доказательства этой верхней границы состоит в том, чтобы специальным образом разбить код на $O(\varepsilon^{-1/2})$ подкодов (слоев). Каждый слой будет содержать слова близкого веса. Тогда, удлиняя кодовые слова внутри одного слоя так, чтобы все они стали одинакового веса, мы сводим задачу к оценке мощности равновесного кода, решение которой известно (см. леммы 1–3).

Т е о р е м а 1. *Пусть $n > 36$ и код $\mathcal{C} \subseteq \{0,1\}^n$ исправляет долю асимметричных ошибок, равную $1/4+\varepsilon$ для некоторого $0 < \varepsilon < 1/12 - 3/n$. Тогда мощность кода ограничена следующим образом*: $|\mathcal{C}| \leqslant \dfrac{1+7/n+2\sqrt{\varepsilon}+4\varepsilon+16\sqrt{\varepsilon}/n}{\varepsilon^{3/2}} + 10$.

Д о к а з а т е л ь с т в о. Без ограничения общности можно считать, что число кодовых слов веса, меньшего $n/2$, не меньше, чем число кодовых слов веса, превосходящего $n/2$ (иначе можно рассмотреть код той же мощности, в котором кодовые слова получаются заменой нулей на единицы и наоборот). Для целого неотрицательного числа i обозначим $\rho_i := \dfrac{i}{2i+1}$. Определим подкод

$$\mathcal{A}_i := \{\boldsymbol{x} \in \mathcal{C} : \lfloor \rho_i n \rfloor < \mathrm{wt}(\boldsymbol{x}) \leqslant \lfloor \rho_{i+1} n \rfloor\}.$$

Удлиним все кодовые слова кода $\mathcal{A}_i$ путем добавления $\lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1$ координат так, чтобы все полученные слова имели вес $\lfloor \rho_{i+1} n \rfloor$. Заметим, что это можно сделать несколькими способами. Из леммы 1 следует, что получившийся код $\mathcal{A}'_i \subseteq \{0,1\}^{n+\lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1}$ содержит слова веса $\lfloor \rho_{i+1} n \rfloor$ и исправляет $\lceil (1/4+\varepsilon)n \rceil$ симметричных ошибок. Из леммы 3 (при $\varepsilon < 1/12 - 3/n$ условия леммы выполнены) получаем, что

$$|\mathcal{A}_i| = |\mathcal{A}'_i| \leqslant \frac{\lceil (1/4+\varepsilon)n \rceil (n + \lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1)}{\lfloor \rho_{i+1} n \rfloor^2 - (\lfloor \rho_{i+1} n \rfloor - \lceil (1/4+\varepsilon)n \rceil)(n + \lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1)} \leqslant$$
$$\leqslant \frac{(1/4+\varepsilon+1/n)(1+\rho_{i+1}-\rho_i)}{\rho_{i+1}^2 - (\rho_{i+1} - 1/4 - \varepsilon)(1+\rho_{i+1}-\rho_i)}.$$

В последнем неравенстве воспользовались тем, что $w^2-(w-t)n$ является монотонно убывающей функцией по w при $w \leqslant (n - \sqrt{n^2-4tn})/2$. Заметим, что

$$\rho_{i+1}^2 - (\rho_{i+1} - 1/4)(1+\rho_{i+1}-\rho_i) = 0,$$

поскольку $\rho_i = \dfrac{i}{2i+1}$. Значит, $|\mathcal{A}'_i| \leqslant 1 + (1/4+1/n)\varepsilon^{-1}$.

Пусть $i_0 := \lfloor 1/(2\sqrt{\varepsilon}) \rfloor$, и следовательно, $\rho_{i_0} \geqslant \dfrac{1-2\sqrt{\varepsilon}}{2+2\sqrt{\varepsilon}}$. Для неотрицательного целого числа j рассмотрим подкод

$$\mathcal{B}_j := \{\boldsymbol{x} \in \mathcal{C} : \lfloor \rho_{i_0} n \rfloor + j\lceil 2\varepsilon n \rceil < \mathrm{wt}(\boldsymbol{x}) \leqslant \lfloor \rho_{i_0} n \rfloor + (j+1)\lceil 2\varepsilon n \rceil\}.$$

Как и ранее, удлиним все слова кода $\mathcal{B}_j$ путем добавления $\lceil 2\varepsilon n \rceil$ координат так, чтобы полученные слова имели одинаковый вес. Получившийся код $\mathcal{B}'_j \subseteq \{0,1\}^{n+\lceil 2\varepsilon n \rceil}$ содержит слова веса $\lfloor \rho_{i_0} n \rfloor + (j+1)\lceil 2\varepsilon n \rceil$ и исправляет $\lceil (1/4+\varepsilon)n \rceil$ симметричных

ошибок. Используя лемму 2, можем оценить

$$|\mathcal{B}_j| = |\mathcal{B}'_j| \leqslant \frac{n + 4\varepsilon n + 8}{n + 4\varepsilon n + 3 - n - 2\varepsilon n - 1} \leqslant (1/2 + 4/n + 2\varepsilon)\varepsilon^{-1}.$$

Для того чтобы каждое слово кода $\mathcal{C}$, имеющее вес в интервале $[1, n/2]$, вошло в $\mathcal{A}_i$ для $i \in [0, i_0 - 1]$ или в $\mathcal{B}_j$ для $j \in [0, j_0 - 1]$, достаточно взять $j_0 := \lfloor 3/(4\sqrt{\varepsilon}) + 2 \rfloor$, так как

$$\frac{n/2 - \lfloor \rho_{i_0} n \rfloor}{\lceil 2\varepsilon n \rceil} \leqslant \frac{n/2 - \dfrac{1 - 2\sqrt{\varepsilon}}{2 + 2\sqrt{\varepsilon}} n}{2\varepsilon n} + 1 \leqslant \left\lfloor \frac{3}{4\sqrt{\varepsilon}} + 2 \right\rfloor.$$

Поскольку число кодовых слов с весом из интервала $[1, n/2]$ не меньше числа кодовых слов с весом из интервала $[n/2, n - 1]$, получаем

$$\begin{aligned}
|\mathcal{C}| &\leqslant 2\left(\sum_{i=0}^{i_0 - 1} |\mathcal{A}_i| + \sum_{j=0}^{j_0 - 1} |\mathcal{B}_j| \right) + 2 \leqslant \\
&\leqslant \frac{1}{\varepsilon^{3/2}}(\varepsilon + 1/4 + 1/n + 3/4 + 6/n + 3\varepsilon + 2\sqrt{\varepsilon} + 16\sqrt{\varepsilon}/n + 8\varepsilon^{3/2}) + 2 = \\
&= \frac{1 + 7/n + 4\varepsilon + 2\sqrt{\varepsilon} + 16\sqrt{\varepsilon}/n}{\varepsilon^{3/2}} + 10. \quad \blacktriangle
\end{aligned}$$

§ 4. Нижняя граница

В следующем утверждении мы докажем, что существует код длины $\exp(\Theta(\varepsilon^{-3/2}))$ и мощности $\Omega(\varepsilon^{-3/2})$, исправляющий долю $1/4 + \varepsilon$ асимметричных ошибок при $\varepsilon \to 0$. Мы воспользуемся соображениями, которые использовали при доказательстве теоремы 1, а именно: для построения кода большой мощности мы сначала найдем $\Omega(\varepsilon^{-1/2})$ равновесных кодов, таких что j-й код $\mathcal{C}_j$ содержит слова с относительным весом $1/2 - j\varepsilon$ и исправляет долю $1/4 + \Omega(\varepsilon)$ симметричных ошибок. Отметим, что конструкция такого кода при $j = 0$ была впервые предложена в работе [4], в которой авторы исследовали коды для списочного декодирования. Затем мы рассмотрим код $\widetilde{\mathcal{C}}_j$, являющийся многократным повторением кода $\mathcal{C}_j$, и случайно переставим координаты в этом коде. Эта операция не изменяет корректирующую способность кода. Итоговый код является объединением кодов $\widetilde{\mathcal{C}}_j$. Случайная перестановка координат внутри каждого из равновесных кодов гарантирует, что значение функции $\Delta(\boldsymbol{x}, \boldsymbol{y})$ для $\boldsymbol{x} \in \widetilde{\mathcal{C}}_j$ и $\boldsymbol{y} \in \widetilde{\mathcal{C}}_i$ при $j < i$ достаточно велико с большой вероятностью.

Теорема 2. *Существует код длины* $\exp(O(\varepsilon^{-3/2}))$, *исправляющий долю* $\dfrac{1}{4} + \varepsilon$ *асимметричных ошибок и содержащий не менее чем* $\dfrac{3\sqrt{3}}{128}\varepsilon^{-3/2}(1 + o(1))$ *кодовых слов при* $\varepsilon \to 0$.

Доказательство. Рассмотрим целое положительное $m := \lfloor 3/(32\varepsilon) \rfloor$ и определим константу $c := 2^{-3/2}$. Для всякого $j \in \{-\lfloor c\sqrt{m} \rfloor, \ldots, \lfloor c\sqrt{m} \rfloor\}$ обозначим $f_j := \binom{2m}{m - j}$. Рассмотрим двоичную матрицу A_j размера $2m \times f_j$, столбцы которой составляют множество всевозможных двоичных векторов длины $2m$ и веса $m - j$. Для двух произвольных различных строк $\boldsymbol{x}$ и $\boldsymbol{y}$ матрицы A_j подсчитаем число координат, в которых они различаются:

$$\Delta(\boldsymbol{x}, \boldsymbol{y}) = \Delta(\boldsymbol{y}, \boldsymbol{x}) = \binom{2m - 2}{m - j - 1}.$$

Значит, код, кодовыми словами которого являются строки матрицы A_j, исправляет долю ρ_j асимметричных ошибок, где

$$\rho_j := \frac{\binom{2m-2}{m-j-1}-1}{\binom{2m}{m-j}} = \frac{(m-j)(m+j)}{2m(2m-1)} - \frac{1}{\binom{2m}{m-j}} = \frac{1}{4} + \frac{m/2-j^2}{4m^2-2m} - \frac{1}{\binom{2m}{m-j}}.$$

Проверим, что для достаточно малого ε это выражение не меньше $\frac{1}{4}+\varepsilon$:

$$\frac{m/2-j^2}{4m^2-2m} - \frac{1}{\binom{2m}{m-j}} \geqslant \frac{m/2-c^2m}{4m^2-2m} - \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}} =$$
$$= \frac{3}{32m-16} - \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}} = \frac{3}{32m} + \frac{3}{2m(32m-16)} - \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}} \geqslant \varepsilon.$$

В последнем неравенстве были использованы соотношения $m = \lfloor 3/(32\varepsilon)\rfloor$, $c = 2^{-3/2}$, а также тот факт, что для достаточно большого m (малого ε) верно неравенство

$$\frac{3}{64m^2} > \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}}.$$

Действительно, правая часть последнего неравенства равна $2^{-2m(1+o(1))}$ при $m\to\infty$.

Для всякого целого положительного числа z определим матрицу $A_j^{(z)}$ размера $2m \times zf_j$, составленную из z копий матрицы A_j. Копии матрицы A_j записываются справа, т.е. удлиняются строки $A_j^{(z)} = (A_j, A_j, \ldots, A_j)$. Через $\widetilde{A}_j^{(z)}$ обозначим матрицу, полученную из $A_j^{(z)}$ случайной перестановкой ее столбцов. Подразумевается, что из всех возможных перестановок случайным образом выбирается одна, причем выбор равновероятен для всех перестановок. Заметим, что код, кодовыми словами которого являются строки матрицы $\widetilde{A}_j^{(z)}$, исправляет ту же долю асимметричных ошибок, что и код, полученный из A_j. Определим целые числа

$$z_j := \prod_{\substack{i=-\lfloor c\sqrt{m}\rfloor,\\ i\neq j}}^{\lfloor c\sqrt{m}\rfloor} \binom{2m}{m-i}, \quad N := \prod_{i=-\lfloor c\sqrt{m}\rfloor}^{\lfloor c\sqrt{m}\rfloor} \binom{2m}{m-i}, \quad M := 2m(2\lfloor c\sqrt{m}\rfloor+1).$$

Рассмотрим матрицу A размера $M\times N$, содержащую в качестве подматриц матрицы $\widetilde{A}_j^{(z_j)}$ для всех $j\in\{-\lfloor c\sqrt{m}\rfloor,\ldots,\lfloor c\sqrt{m}\rfloor\}$. Для определенности будем считать, что матрицы $\widetilde{A}_j^{(z_j)}$ записаны друг под другом в естественном порядке увеличения параметра j, начиная с $j=-\lfloor c\sqrt{m}\rfloor$. Используя параметр ε, стремящийся к нулю, число строк M и число столбцов N в матрице A оцениваются как

$$M = \frac{3\sqrt{3}}{128\varepsilon\sqrt{\varepsilon}}(1+o(1)), \quad N = \exp(\Theta(\varepsilon^{-3/2})).$$

Покажем, что для произвольных различных строк $\widetilde{\boldsymbol{x}}$ и $\widetilde{\boldsymbol{y}}$ матрицы A значение функции $\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}),\Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}}))$ достаточно велико с большой вероятностью при $\varepsilon\to 0$. Последнее условие гарантирует, что код исправит нужную долю асимметричных ошибок. Более формально, пусть $\widetilde{\boldsymbol{x}}$ и $\widetilde{\boldsymbol{y}}$ являются строками из $\widetilde{A}_j^{(z_j)}$ и $\widetilde{A}_i^{(z_i)}$, где $j<i$. Ясно, что $\mathrm{wt}(\widetilde{\boldsymbol{x}}) = \frac{m-j}{2m}N > \frac{m-i}{2m}N = \mathrm{wt}(\widetilde{\boldsymbol{y}})$ и $\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}),\Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}})) = \Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}})$.

Пусть $T = \{\mathrm{wt}(\widetilde{\boldsymbol{x}}) - \mathrm{wt}(\widetilde{\boldsymbol{y}}), \ldots, \min(\mathrm{wt}(\widetilde{\boldsymbol{x}}), N - \mathrm{wt}(\widetilde{\boldsymbol{y}}))\}$. Распределение вероятностей для случайной величины $\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}})$ выглядит следующим образом:

$$\Pr\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) = t\} = \begin{cases} \dfrac{\binom{\mathrm{wt}(\widetilde{\boldsymbol{x}})}{t}\binom{N - \mathrm{wt}(\widetilde{\boldsymbol{x}})}{\mathrm{wt}(\widetilde{\boldsymbol{y}}) - \mathrm{wt}(\widetilde{\boldsymbol{x}}) + t}}{\binom{N}{\mathrm{wt}(\widetilde{\boldsymbol{y}})}} & \text{для } t \in T, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Оценим вероятность того события, что $\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}})$ недостаточно велико:

$$\Pr\left\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) \leqslant N\left(\frac{1}{4} + \varepsilon\right)\right\} \leqslant N \max_{t \in [0, \lfloor N(\frac{1}{4}+\varepsilon)\rfloor]} \Pr\left\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) = t\right\}. \tag{1}$$

Пусть целое число t равно αN для некоторого действительного числа $\alpha \in \left[\frac{i-j}{2m}, \min\left(\frac{m-j}{2m}, \frac{m+i}{2m}\right)\right]$. Заметим, что N и m являются функциями от ε. Определим функцию

$$g_{i,j}(\alpha, \varepsilon) := \frac{1}{N}\log\left(\Pr\left\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) = t\right\}\right).$$

Для произвольных целых чисел $u > v \geqslant 1$ биномиальный коэффициент $\binom{u}{v}$ удовлетворяет неравенству

$$\sqrt{\frac{u}{8v(u-v)}}\,2^{uh(v/u)} \leqslant \binom{u}{v} \leqslant 2^{uh(v/u)},$$

где $h(x) := -x\log x - (1-x)\log(1-x)$. Значит, для $\alpha \in \left(\frac{i-j}{2m}, \min\left(\frac{m-j}{2m}, \frac{m+i}{2m}\right)\right)$ выполнена оценка

$$g_{i,j}(\alpha, \varepsilon) \leqslant \frac{m-j}{2m}h\left(\frac{2\alpha m}{m-j}\right) + \frac{m+j}{2m}h\left(\frac{j-i+2\alpha m}{m+j}\right) - h\left(\frac{m-i}{2m}\right) -$$
$$- \frac{\log\left(\frac{m^2}{2(m-i)(m+i)N}\right)}{2N} \leqslant r_{i,j}(\alpha, \varepsilon) + \delta(\varepsilon),$$

где функции $r_{i,j}(\alpha, \varepsilon)$ и $\delta_{i,j}(\varepsilon)$ определены следующим образом:

$$r_{i,j}(\alpha, \varepsilon) := \frac{m-j}{2m}h\left(\frac{2\alpha m}{m-j}\right) + \frac{m+j}{2m}h\left(\frac{j-i+2\alpha m}{m+j}\right) - h\left(\frac{m-i}{2m}\right),$$
$$\delta(\varepsilon) := \frac{\log(2N)}{2N}.$$

Используя соотношение $\dfrac{\partial h(x)}{\partial x} = \log\left(\dfrac{1-x}{x}\right)$, посчитаем производную функции $r_{i,j}(\alpha, \varepsilon)$:

$$q_{i,j}(\alpha, \varepsilon) := \frac{\partial r_{i,j}(\alpha, \varepsilon)}{\partial \alpha} = \log\left(\frac{m-j-2\alpha m}{2\alpha m}\right) + \log\left(\frac{m+i-2\alpha m}{j-i+2\alpha m}\right).$$

Пусть $\alpha_{i,j} = \alpha_{i,j}(\varepsilon) := \dfrac{(m-j)(m+i)}{4m^2}$. Несложно видеть, что функция $q_{i,j}(\alpha, \varepsilon)$ строго положительна при $\alpha < \alpha_{i,j}$, и функция $r_{i,j}(\alpha, \varepsilon) \leqslant 0$ для всех допустимых α, причем $r_{i,j}(\alpha_{i,j}, \varepsilon) = 0$. В силу выбора $m = \lfloor 3/(32\varepsilon)\rfloor$ и ограничений на i и j, т.е.

$-\lfloor c\sqrt{m}\rfloor \leqslant j < i \leqslant \lfloor c\sqrt{m}\rfloor$, получаем, что $\alpha_{i,j}(\varepsilon) - (1/4+\varepsilon) > 0$, а также

$$\alpha_{i,j}(\varepsilon) - \left(\frac{1}{4}+\varepsilon\right) = \frac{(m-j)(m+i)}{4m^2} - \left(\frac{1}{4}+\varepsilon\right) = \frac{(i-j)m - ij - 4\varepsilon m^2}{4m^2}.$$

Поскольку производная функции $r_{i,j}(\alpha,\varepsilon)$ положительна при $\alpha \leqslant 1/4+\varepsilon$, можем заключить, что

$$\sup_{\frac{i-j}{2m}<\alpha\leqslant\frac{1}{4}+\varepsilon} g_{i,j}(\alpha,\varepsilon) \leqslant r_{i,j}(1/4+\varepsilon,\varepsilon) + \delta(\varepsilon). \tag{2}$$

Заметим, что выполнено частичное разложение Тейлора с остаточным членом в форме Лагранжа:

$$\begin{aligned} &r_{i,j}(\alpha_{i,j},\varepsilon) = r_{i,j}(1/4+\varepsilon,\varepsilon) + (\alpha_{i,j} - 1/4 - \varepsilon) q_{i,j}(1/4+\varepsilon,\varepsilon) + \\ &+ (\alpha_{i,j} - 1/4 - \varepsilon)^2 \frac{\sigma_{i,j}(\theta,\varepsilon)}{2}, \end{aligned} \tag{3}$$

где $\sigma_{i,j}(\alpha,\varepsilon) := \dfrac{\partial q_{i,j}(\alpha,\varepsilon)}{\partial\alpha}$, а θ – некоторая точка между $1/4+\varepsilon$ и $\alpha_{i,j}$. Далее найдем вид функции $\sigma_{i,j}(\alpha,\varepsilon)$ и покажем ее ограниченность снизу на интервале $(1/4+\varepsilon, \alpha_{i,j})$:

$$\frac{\sigma_{i,j}(\alpha,\varepsilon)}{\log e} = \frac{j-m}{\alpha(m-j-2\alpha m)} - \frac{2m(m+j)}{(j-i+2\alpha m)(m+i-2\alpha m)}.$$

При $\varepsilon \to 0$ имеем $m = \Theta(\varepsilon^{-1})$. Следовательно, $\sigma_{i,j}(\theta,\varepsilon) = -16\log e(1+o(1))$ при $\varepsilon\to 0$, поскольку

$$\lim_{\varepsilon\to 0} \sup_{1/4+\varepsilon<\alpha<\alpha_{i,j}} \sigma_{i,j}(\alpha,\varepsilon) = -16\log e, \quad \lim_{\varepsilon\to 0} \inf_{1/4+\varepsilon<\alpha<\alpha_{i,j}} \sigma_{i,j}(\alpha,\varepsilon) = -16\log e.$$

Теперь оценим $q_{i,j}(1/4+\varepsilon,\varepsilon)$ при $\varepsilon\to 0$:

$$\begin{aligned} &q_{i,j}(1/4+\varepsilon,\varepsilon) = \log\left(1 + \frac{mi - 4\varepsilon m^2 - jm - ji}{(m/2+2\varepsilon m)(m/2+j-i+2\varepsilon m)}\right) = \\ &= 4\log e \frac{m(i-j) - 4\varepsilon m^2 - ji}{m^2}(1+o(1)). \end{aligned}$$

Также напомним, что $r_{i,j}(\alpha_{i,j},\varepsilon) = 0$. Подставляя вышеуказанные оценки в (3), имеем

$$\begin{aligned} &r_{i,j}(1/4+\varepsilon,\varepsilon) = -\left(\alpha_{i,j} - \frac{1}{4} - \varepsilon\right)\left(\frac{m(i-j) - 4\varepsilon m^2 - ji}{m^2}(4\log e - 2\log e)\right) \times \\ &\times (1+o(1)) \leqslant -\lambda\varepsilon^2 + o(\varepsilon^2) \end{aligned}$$

для некоторой константы $\lambda > 0$ и $\varepsilon\to 0$. Используя это неравенство, оценку $\delta(\varepsilon) = o(\varepsilon^2)$ и неравенство (2), оценим левую часть (1) следующим образом:

$$\Pr\left\{\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}) \leqslant N\left(\frac{1}{4}+\varepsilon\right)\right\} \leqslant N 2^{-\lambda\varepsilon^2 N + o(\varepsilon^2 N)} = o(1),$$

поскольку $\varepsilon^2 N = \exp(\Omega(\varepsilon^{-3/2}))$. Вероятность того, что $\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}), \Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}})) \leqslant N(1/4+\varepsilon)$ хотя бы для какой-то пары строк $\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}$ из матрицы A, оценим сверху величиной

$$\binom{M}{2} \max_{\substack{\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}\in A \\ \widetilde{\boldsymbol{x}}\neq\widetilde{\boldsymbol{y}}}} \Pr\left\{\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}), \Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}})) \leqslant N\left(\frac{1}{4}+\varepsilon\right)\right\} = o(1).$$

Это означает, что при $\varepsilon \to 0$ с большой вероятностью строки случайной матрицы A могут служить кодом, исправляющим долю $1/4 + \varepsilon$ асимметричных ошибок. ▲

§ 5. Заключение

Из теорем 1 и 2 вытекает следующее утверждение.

Следствие. *Максимальное число слов в коде, исправляющем долю* $1/4 + \varepsilon$ *асимметричных ошибок, равно* $\Theta(\varepsilon^{-3/2})$ *при* $\varepsilon \to 0$.

Отметим, что длина предъявленной случайной конструкции в теореме 2 достаточно велика. Было бы интересно найти существенно более короткий код, имеющий ту же по порядку мощность.

СПИСОК ЛИТЕРАТУРЫ

1. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. http://mi.mathnet.ru/ppi762
2. *Borden J.M.* A Low-Rate Bound for Asymmetric Error-Correcting Codes // IEEE Trans. Inform. Theory. 1983. V. 29. № 4. P. 600–602. https://doi.org/10.1109/TIT.1983.1056708
3. *Plotkin M.* Binary Codes with Specified Minimum Distance // IRE Trans. Inform. Theory. 1960. V. 6. № 4. P. 445–450. https://doi.org/10.1109/TIT.1960.1057584
4. *Alon N., Bukh B., Polyanskiy Y.* List-Decodable Zero-Rate Codes // IEEE Trans. Inform. Theory. 2018. V. 65. № 3. P. 1657–1667. https://doi.org/10.1109/TIT.2018.2868957
5. *Левенштейн В.И.* Применение матриц Адамара к одной задаче кодирования // Проблемы кибернетики. Вып. 5. М.: Физматгиз, 1961. С. 123–136.
6. *Варшамов Р.Р.* К теории несимметрических кодов // Докл. АН СССР. 1965. Т. 164. № 4. С. 757–760. http://mi.mathnet.ru/dan31642

Лебедев Владимир Сергеевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
lebedev37@mail.ru
Полянский Никита Андреевич
Сколковский институт науки и технологий (Сколтех)
Технический университет Мюнхена, Германия
nikitapolyansky@gmail.com

Поступила в редакцию
14.12.2020
После доработки
25.03.2021
Принята к публикации
26.03.2021