

УДК 621.391 : 519.725

© 2024 г. И.В. Воробьев¹, А.В. Лебедев, В.С. Лебедев

ИСПРАВЛЕНИЕ ОДНОЙ ОШИБКИ В АСИММЕТРИЧНОМ КАНАЛЕ С ОБРАТНОЙ СВЯЗЬЮ

Доказывается новая нижняя оценка мощности кода с полной обратной связью, исправляющего одну ошибку в двоичном асимметричном канале. Также представлена верхняя граница мощности кода, близкая к новой нижней границе.

Ключевые слова: асимметричный канал, обратная связь, кодовая конструкция.

DOI: 10.31857/S0555292324010042, EDN: EUSSZN

§ 1. Введение

В данной статье изучается двоичный асимметричный канал с мгновенной бесшумной обратной связью. Нами рассматривается комбинаторная модель асимметричного канала, в котором при передаче кодового слова длины n происходит не более одной ошибки.

В рассматриваемом нами асимметричном канале, также известном как Z-канал, при передаче символа 1 может произойти ошибка и на выходе канала будет получен символ 0, при этом символ 0 всегда передается безошибочно. Наличие полной обратной связи означает, что после передачи каждого символа кодер получает информацию о том, какой символ был принят декодером. Изучению двоичного асимметричного канала посвящено значительное количество работ. В работе [1] были предложены коды Варшамова – Тененгольца, позволяющие исправлять одну ошибку в асимметричном канале без обратной связи. В работах [2, 3] Варшамов показал, что для исправления t ошибок без обратной связи необходимо и достаточно, чтобы кодовые слова находились друг от друга на асимметричном расстоянии не менее $2t + 1$, где асимметричное расстояние между словами $\mathbf{x}, \mathbf{y}$ определяется как

$$p(\mathbf{x}, \mathbf{y}) = |\mathbf{x} - \mathbf{y}| + ||\mathbf{x}| - |\mathbf{y}||$$

(где $|\mathbf{x}|$ – число единиц в слове $\mathbf{x}$, часто называемое весом слова). Бассалыго в работе [4] вывел из этого, что мощность кода M для длины сообщения n в асимметричном канале не может превышать мощность кода в симметричном канале более чем в $t + 1$ раз. Таким образом, асимптотическая скорость кода без обратной связи ($R = \lim_{n \rightarrow \infty} \frac{\log M}{n}$), исправляющего t ошибок в асимметричном канале, ровно такая же, как и скорость кода, исправляющего t ошибок в симметричном канале. При наличии обратной связи и линейном числе ошибок асимптотическая скорость для симметричного и асимметричного каналов уже будет различаться [5, 6].

¹ Работа выполнена при частичной финансовой поддержке Российского научного фонда (номер проекта 22-41-02028).

При фиксированном числе ошибок t максимальное число передаваемых сообщений M с полной обратной связью асимптотически эквивалентно $2^{n+t} t! n^{-t}$. Это утверждение было доказано для $t = 1$ в [7] и для произвольного t в [8,9]. Позднее было показано, что такого же асимптотического результата можно добиться, используя обратную связь лишь один раз. Это было доказано для двоичного симметричного канала в [10] и для произвольного дискретного канала в [11].

Для оптимальной мощности кода любой длины, исправляющего одну ошибку в двоичном симметричном канале при наличии полной обратной связи, известен точный ответ [12]. Более того, в [13] показано, что можно построить код такой же мощности, использующий обратную связь только два раза. В случае же асимметричного канала точный ответ для одной ошибки до сих пор не получен. Известны только асимптотические результаты и таблицы оптимальных кодов для небольших длин (см. [7,13]).

В работе [7] доказано, что для передачи с полной обратной связью $M = 2^\ell$ сообщений достаточно длины кода

$$n = \ell - 1 + \lceil \log(\ell + 3) \rceil.$$

Выражая число сообщений через длину, получаем, что возможна передача

$$M = \frac{2^{n+1}}{n - \log n(1 + o(1))} = \frac{2^{n+1}}{n} \left(1 + \frac{\log n}{n} + o\left(\frac{\log n}{n}\right) \right) \quad (1)$$

сообщений.

В работе [14] нами был построен рекурсивный алгоритм, позволяющий получать оптимальные коды с полной обратной связью, исправляющие одну ошибку. Также была предложена модификация этого рекурсивного алгоритма, позволяющая относительно легко получать оценки мощностей кодов большой длины. В данной статье мы применяем упомянутый алгоритм для получения новой нижней оценки мощности кода, превосходящей результат (1). Также мы доказываем верхнюю границу мощности кода, близкую к новой нижней границе.

§ 2. Определения и обозначения

Рассмотрим канал с двоичным алфавитом $\{0,1\}$ на входе и на выходе. Кодер передает сообщение $\mathbf{x} \in \{0,1\}^n$, декодер получает сообщение $\mathbf{y} \in \{0,1\}^n$. Ошибкой будем называть замену символа 1 из последовательности $\mathbf{x}$ на символ 0 (а нулевой символ всегда передается безошибочно). Символом $[M]$ будем обозначать множество $\{1, 2, \dots, M\}$.

В данной статье рассматривается передача данных по каналу с полной обратной связью. Кодер передает сообщение $m \in [M]$. Первый передаваемый символ x_1 зависит только от сообщения m . После передачи каждого символа x_i кодер получает обратную связь о принятом символе y_i . Перед отправкой следующего символа кодер учитывает в своей стратегии информацию о полученных символах. Таким образом, второй передаваемый символ x_2 зависит не только от сообщения m , но и от принятого символа y_1 , и так далее.

Определим облако $B(m)$ для сообщения m как множество последовательностей $\mathbf{y}$, которые могут быть получены на выходе канала с не более чем одной ошибкой при передаче этого сообщения. Каждое облако $B(m)$ содержит последовательность, которая будет передана в том случае, если в канале не происходит ошибок. Назовем эту последовательность корневой. Отметим, что размер облака всегда превосходит вес корневой последовательности на 1.

Будем называть набор непересекающихся облаков $B(m)$, $m \in [M]$, кодом $\mathcal{C}$ мощности M , исправляющим одну ошибку. Точки пространства, не принадлежащие ни

одному облаку, будем называть свободными; количество таких точек будет обозначаться через F .

§ 3. Основной результат

Всюду далее под кодом будем понимать код с полной обратной связью, исправляющий одну ошибку в асимметричном канале.

При доказательстве основного результата мы будем опираться на следующее утверждение, доказанное в [14].

Предложение 1. *Если существует код длины n и мощности M , имеющий F свободных точек, $F \geq M$, то тогда существует код длины $n + 1$ и мощности $2M$, имеющий $2F - M$ свободных точек.*

Последовательное применение предложения 1 дает следующий результат.

Предложение 2. *Пусть существует код длины k и мощности M_0 , имеющий F свободных точек. Тогда для любого $N \leq 2F/M_0 - 1$ существует код длины $n = k + N$ и мощности $M = M_0 \cdot 2^N$.*

В зависимости от того, какой начальный код длины k используется в предложении 2, будут получаться коды с разными параметрами. В теореме 2 работы [14] показано, что применяя предложение 2 к тривиальному коду, состоящему из одного нулевого слова, мы повторяем результат (1).

В следующей теореме мы улучшаем этот результат, применяя предложение 2 к более сложному коду.

Теорема 1. *Существует код длины n и мощности*

$$M = \frac{2^{n+1}}{n - \alpha\sqrt{n}(1 + o(1))} = \frac{2^{n+1}}{n} \left(1 + \frac{\alpha}{\sqrt{n}} + o\left(\frac{1}{\sqrt{n}}\right) \right) \quad \text{при } n \rightarrow \infty,$$

где $\alpha > 0,4499$.

Доказательство. Построим код длины k и мощности

$$M_0 = \sum_{w=0}^s \binom{k - \lfloor \log k \rfloor}{w}$$

с одной обратной связью, исправляющий одну ошибку. Код строится следующим образом. Каждому сообщению поставим в соответствие двоичную последовательность длины $r = k - \lfloor \log k \rfloor$, имеющую вес не более s . При передаче сообщения на первых r символах передается соответствующая двоичная последовательность, последующие $\lfloor \log k \rfloor$ символов используются для исправления возможной ошибки. В случае, если ошибки не было, передается нулевое слово, в противном случае передается номер позиции, в которой произошла ошибка. Так как возможных позиций строго меньше чем k , то нам хватает длины кода для передачи нужной информации.

Пусть $s = \lfloor r/2 - C\sqrt{r} \rfloor$, где C – некая константа, которая будет оптимизирована в дальнейшем. Подсчитаем количество свободных точек в коде. Каждому сообщению соответствует корневое слово веса $w \leq s$, состоящее из последовательности веса w на первых $r = k - \lfloor \log k \rfloor$ символах, дополненной последовательностью из $\lfloor \log k \rfloor$ нулей. Поэтому соответствующее облако состоит из $w + 1$ точек. Таким образом, количество свободных точек вычисляется по формуле

$$F = 2^k - \sum_{w=0}^s \binom{r}{w} (w + 1).$$

Преобразуем выражение для мощности кода:

$$M_0 = \sum_{w=0}^s \binom{r}{w} = 1 + \sum_{w=1}^s \left(\binom{r-1}{w} + \binom{r-1}{w-1} \right) = \quad (2)$$

$$= \sum_{w=1}^{s+1} \binom{r-1}{w-1} + \sum_{w=1}^s \binom{r-1}{w-1} = 2 \sum_{w=1}^s \binom{r-1}{w-1} + \binom{r-1}{s} = \quad (3)$$

Теперь преобразуем выражение для количества свободных точек:

$$\begin{aligned} F &= 2^k - \sum_{w=0}^s \binom{r}{w} (w+1) = 2^k - \sum_{w=0}^s \binom{r}{w} w - \sum_{w=0}^s \binom{r}{w} = \\ &= 2^k - r \sum_{w=1}^s \binom{r-1}{w-1} - M_0 = \\ &= 2^k - M_0 - r \left(M_0 - \binom{r-1}{s} \right) \cdot \frac{1}{2} = \\ &= 2^k - M_0 - r M_0 / 2 + \frac{r}{2} \binom{r-1}{s} = \\ &= 2^k - M_0 - r M_0 / 2 + \frac{r-s}{2} \binom{r}{s}. \end{aligned} \quad (4)$$

Применяя N раз предложение 2, где

$$N = 2F/M_0 - 1, \quad (5)$$

получаем новый код. Длина нового кода $n = k + N$, а его мощность

$$M = M_0 \cdot 2^N = M_0 \frac{2^{n+1}}{2^{k+1}}. \quad (6)$$

Дальнейшие вычисления направлены на установление зависимости мощности M кода от его длины n .

Воспользуемся следующей асимптотической формулой для M_0 :

$$M_0 = \sum_{w=0}^s \binom{r}{w} = 2^r (\Phi(-2C) + o(1)) \quad \text{при } r \rightarrow \infty, \quad (7)$$

где

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{x^2}{2}} dx$$

– функция распределения стандартного нормального распределения $\mathcal{N}(0, 1)$. Эта формула легко выводится из центральной предельной теоремы, примененной к биномиальной случайной величине ξ с параметрами r и $1/2$.

Действительно, если поделить M_0 на 2^r , то мы получим вероятность того, что биномиальная случайная величина ξ с параметрами r и $1/2$ принимает значение не более s . Из центральной предельной теоремы следует, что

$$\frac{\xi - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}} \xrightarrow{d} \mathcal{N}(0, 1).$$

Имеем

$$M_0 = 2^r \mathbf{P}(\xi \leq s) = 2^r \mathbf{P}\left(\frac{\xi - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}} \leq \frac{s - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}}\right). \quad (8)$$

Заметим, что

$$\mathbf{E}\xi = \frac{r}{2}, \quad \mathbf{D}\xi = \frac{r}{4}, \quad s = \lfloor r/2 - C\sqrt{r} \rfloor,$$

и поэтому

$$M_0 = 2^r \mathbf{P}\left(\frac{\xi - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}} \leq \frac{-2C\sqrt{r}}{\sqrt{r}}(1 + o(1))\right) = 2^r(\Phi(-2C) + o(1)). \quad (9)$$

Для биномиального коэффициента воспользуемся известной формулой, которую можно найти, например, в [15]:

$$\binom{r}{s} = 2^r \frac{e^{-2C^2}}{\sqrt{\pi r/2}}(1 + o(1)). \quad (10)$$

Подставляя в формулу (5) выражения (7), (10) и (4), получаем следующее:

$$N = 2^{k+1}/M_0 - 3 - r + \frac{r-s}{\sqrt{r}} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{\pi/2}}(1 + o(1)) = \quad (11)$$

$$= 2^{k+1}/M_0 - k + \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1)). \quad (12)$$

Отсюда

$$\frac{2^{k+1}}{M_0} = N + k - \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1)), \quad (13)$$

а значит, с учетом формулы (6) верно следующее равенство:

$$M = \frac{2^{n+1}}{n - \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1))}. \quad (14)$$

Подставим в формулу (13) выражение (9) для M_0 :

$$\frac{2^{k+1}}{2^r \Phi(-2C)}(1 + o(1)) = n - \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1)), \quad (15)$$

т.е.

$$\begin{aligned} \frac{2k}{\Phi(-2C)}(1 + o(1)) &= n, \\ k &= \frac{n\Phi(-2C)}{2}(1 + o(1)). \end{aligned}$$

Подставляя это выражение в формулу (14) для M , получаем

$$M = \frac{2^{n+1}}{n - \sqrt{n} \frac{\sqrt{\Phi(-2C)}}{\sqrt{2}} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1))} = \frac{2^{n+1}}{n - \alpha\sqrt{n}(1 + o(1))},$$

где

$$\alpha = \frac{e^{-2C^2}}{2\sqrt{\Phi(-2C)\pi}}.$$

Максимальное значение α достигается при $C \approx 0,306$ и превышает 0,4499. ▲

§ 4. Верхняя граница

Докажем верхнюю границу мощности кода.

Теорема 2. *Мощность кода длины n не превосходит*

$$\frac{2^{n+1}}{n - 2\sqrt{n \ln n}(1 + o(1))} = \frac{2^{n+1}}{n} \left(1 + \frac{2\sqrt{\ln n}}{\sqrt{n}} + o\left(\frac{\sqrt{\ln n}}{\sqrt{n}}\right) \right).$$

Доказательство. Пусть передается M сообщений, каждому из которых соответствует корневое сообщение веса w_i , $1 \leq i \leq M$. Размер облака с корневым сообщением веса w равен $w + 1$, поэтому

$$\sum_{i=1}^M (w_i + 1) \leq 2^n.$$

Рассмотрим отдельно слова веса меньше $T = \frac{n}{2} - \sqrt{n \ln n}$ и слова веса не менее T . Пусть в первой группе M_0 слов, а во второй – M_1 . Количество слов M_0 в первой группе можно оценить с помощью неравенства Хёфдинга [16], примененного к случайной величине ξ , имеющей распределение $\text{Bin}(n, 1/2)$:

$$\mathbf{P}(\xi \leq T) \leq e^{-2 \ln n} = n^{-2}.$$

Отсюда следует, что $M_0 \leq 2^n \cdot n^{-2}$.

Для оценки M_1 заметим, что $M_1(T + 1) \leq 2^n$, а значит,

$$M_1 \leq \frac{2^{n+1}}{n - 2\sqrt{n \ln n}}.$$

Таким образом, общее количество сообщений не превосходит

$$M \leq \frac{2^{n+1}}{n - 2\sqrt{n \ln n}(1 + o(1))}. \quad \blacktriangle$$

Таким образом, мы видим, что нижняя и верхняя границы достаточно близки, а именно второй член известен с точностью до умножения на $O(\sqrt{\ln n})$. Однако в отличие от симметричного канала точную формулу для мощности кода получить не удастся.

СПИСОК ЛИТЕРАТУРЫ

1. Варшамов Р.Р., Тененгольц Г.М. Код, исправляющий одиночные несимметрические ошибки // АиТ. 1965. Т. 26. № 2. С. 288–292. <http://www.mathnet.ru/at11293>
2. Варшамов Р.Р. К теории несимметрических кодов // Докл. АН СССР. 1965. Т. 164. № 4. С. 757–760. <http://www.mathnet.ru/dan31642>
3. Варшамов Р.Р. О некоторых особенностях линейных кодов, корректирующих несимметрические ошибки // Докл. АН СССР. 1964. Т. 157. № 3. С. 546–548. <https://www.mathnet.ru/dan29877>

4. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. <http://www.mathnet.ru/ppi762>
5. *Deppe C., Lebedev V., Maringer G., Polyanskii N.* Coding with Noiseless Feedback over the Z-Channel // IEEE Trans. Inform. Theory. 2022. V. 68. № 6. P. 3731–3739. <https://doi.org/10.1109/TIT.2022.3148446>
6. *Lebedev A., Lebedev V., Polyanskii N.* Two-Stage Coding over the Z-Channel // IEEE Trans. Inform. Theory. 2022. V. 68. № 4. P. 2290–2299. <https://doi.org/10.1109/TIT.2022.3141082>
7. *Cicalese F., Mundici D.* Optimal Coding with One Asymmetric Error: Below the Sphere Packing Bound // Computing and Combinatorics (Proc. 6th Annu. Int. Conf. COCOON 2000. Sydney, Australia. July 26–28, 2000). Lect. Notes Comput. Sci. V. 1858. Berlin: Springer, 2000. P. 159–169. https://doi.org/10.1007/3-540-44968-X_16
8. *Dumitriu I., Spencer J.* A Halfliar's Game // Theoret. Comput Sci. 2004. V. 313. № 3. P. 353–369. <https://doi.org/10.1016/j.tcs.2002.09.001>
9. *Spencer J., Yan C.H.* The Halfie Problem // J. Combin. Theory Ser. A. 2003. V. 103. № 1. P. 69–89. [https://doi.org/10.1016/S0097-3165\(03\)00068-2](https://doi.org/10.1016/S0097-3165(03)00068-2)
10. *Бассалыго Л.А.* Недвоичные коды, исправляющие ошибки при наличии одnorазовой безошибочной обратной связи // Пробл. передачи информ. 2005. Т. 41. № 2. С. 63–67. <http://www.mathnet.ru/ppi96>
11. *Dumitriu I., Spencer J.* The Two-Batch Liar Game over an Arbitrary Channel // SIAM J. Discrete Math. 2005. V. 19. № 4. P. 1056–1064. <https://doi.org/10.1137/040617510>
12. *Pelc A.* Solution of Ulam's Problem on Searching with a Lie // J. Combin. Theory Ser. A. 1987. V. 44. № 1. P. 129–140. [https://doi.org/10.1016/0097-3165\(87\)90065-3](https://doi.org/10.1016/0097-3165(87)90065-3)
13. *Воробьев И.В., Денне К., Лебедев А.В., Лебедев В.С.* Исправление одной ошибки в каналах с обратной связью // Пробл. передачи информ. 2022. Т. 58. № 4. С. 38–49. <https://doi.org/10.31857/S0555292322040040>
14. *Vorobyev I., Lebedev A., Lebedev V.* Correcting Errors in Asymmetric and Generalized Asymmetric Channels with Feedback // Proc. XVIII Int. Symp. "Problems of Redundancy in Information and Control Systems" (REDUNDANCY'2023). Moscow, Russia. Oct. 24–27, 2023. P. 163–167. <https://doi.org/10.1109/Redundancy59964.2023.10330199>
15. *Spencer J., Florescu L.* Asymptopia. Providence, RI: Amer. Math. Soc., 2014.
16. *Hoeffding W.* Probability Inequalities for Sums of Bounded Random Variables // J. Amer. Statist. Assoc. 1963. V. 58. № 301. P. 13–30. <https://doi.org/10.2307/2282952>. Reprinted in: The Collected Works of Wassily Hoeffding. New York: Springer, 1994. P. 409–426.

Воробьев Илья Викторович
 Технический университет Мюнхена, Германия
vorobyev.i.v@yandex.ru
Лебедев Алексей Владимирович
Лебедев Владимир Сергеевич
 Институт проблем передачи информации
 им. А.А. Харкевича РАН, Москва
al_lebed95@mail.ru
lebedev37@mail.ru

Поступила в редакцию
 28.12.2023
 После доработки
 03.04.2024
 Принята к публикации
 03.04.2024