ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.72

© 2022 г. **И.В. Воробьев**[1], **К. Деппе**[2], **А.В. Лебедев**[3], **В.С. Лебедев**[3]

ИСПРАВЛЕНИЕ ОДНОЙ ОШИБКИ В КАНАЛАХ С ОБРАТНОЙ СВЯЗЬЮ

Исследуется задача исправления одной ошибки в произвольном дискретном канале без памяти с бесшумной мгновенной обратной связью. Для случая однократной обратной связи предложен способ построения оптимальных стратегий передачи данных. Полученный результат позволяет доказать, что для двоичного канала двух обратных связей достаточно для передачи такого же числа сообщений, как и при полной обратной связи. Также разработанная техника применяется к двоичному асимметричному каналу, для которого строятся стратегии передачи для малых длин.

Ключевые слова: кодирование с обратной связью, симметричный канал, асимметричный канал, граница Хэмминга, задача линейного программирования.

DOI: 10.31857/S0555292322040040, **EDN:** EBRKNL

§ 1. Введение

В данной статье исследуется исправление одной ошибки в произвольном дискретном канале без памяти с бесшумной мгновенной обратной связью. Далее мы будем по умолчанию предполагать все эти условия выполненными – канал без памяти, а обратная связь бесшумная и мгновенная. Наибольшее внимание уделяется двоичным симметричному и асимметричному каналам. В двоичном симметричном канале каждый символ может быть передан неправильно, например, 0 вместо 1 или наоборот. Обычно слово симметричный опускается, и такой канал называется просто двоичным каналом. В двоичном асимметричном канале вместо переданного символа 1 может быть получен 0, но символ 0 всегда передается безошибочно. Рассматривается комбинаторная модель канала с обратной связью и одной ошибкой при передаче символов.

Известно, что задача исправления t ошибок в двоичном канале с полной обратной связью эквивалентна следующей задаче комбинаторного поиска. Требуется найти элемент $x \in \mathcal{M}$ с помощью n вопросов вида: "Лежит ли элемент x в подмножестве A множества $\mathcal{M}$?" Вопросы задаются последовательно, т.е. каждый следующий вопрос может зависеть от ответов на предыдущие. Отвечающий на вопросы оппонент знает x и может солгать не более t раз. Впервые эта задача была сформулирована Реньи [1]. Для линейного числа ошибок в двоичном канале с полной обратной

[1] Работа выполнена при поддержке совместного гранта Российского фонда фундаментальных исследований и Национального научного фонда Болгарии (номер проекта 20-51-18002), Российского фонда фундаментальных исследований (номер проекта 20-01-00559), а также BMBF-NEWCOM (номер гранта 16KIS1005).

[2] Работа выполнена при поддержке грантов BMBF-NEWCOM (номер гранта 16KIS1005) и BMBF-6G-life (номер гранта 16KISK002).

[3] Работа выполнена при поддержке совместного гранта Российского фонда фундаментальных исследований и Национального научного фонда Болгарии (номер проекта 20-51-18002).

связью оптимальная скорость была вычислена Берлекампом [2] и Зигангировым [3]. Эта задача приобрела популярность после того, как в своей автобиографии [4] Улам задал подобный вопрос для $M = 10^6$. Оптимальные стратегии для всех M были найдены в [5] для $t = 1$, в [6] для $t = 2$ и в [7] для $t = 3$. Таблицы оптимальных стратегий были составлены в работе [8] для различных t и $M \leqslant 2^{20}$.

Исправление ошибок в двоичном асимметричном канале с полной обратной связью эквивалентно варианту задачи Улама с полуложью, впервые описанной в [9]. Отличие от оригинальной задачи состоит в том, что лгать можно только в случае, если правильный ответ положительный. Хороший обзор результатов по этой задаче можно найти в книге [10]. Для фиксированного числа ошибок t максимальная мощность множества $\mathcal{M}$ асимптотически эквивалентна $2^{n+t}/\binom{n}{t}$. Это было доказано для $t = 1$ в [11] и для произвольного t в [12, 13].

Отметим, что при фиксированном количестве ошибок даже однократной обратной связи достаточно для передачи асимптотически такого же количества сообщений, как и при полной обратной связи. Это было доказано для недвоичного симметричного канала в работе [14] и для произвольного дискретного канала в [15].

Ключевым результатом настоящей статьи является описание оптимальных стратегий с однократной обратной связью и одной ошибкой для произвольного дискретного канала. Разработанная техника применяется для построения стратегий передачи, исправляющих одну ошибку в двоичном канале с одной или двумя обратными связями, а также для построения стратегий, исправляющих одну ошибку в двоичном асимметричном канале с однократной обратной связью. Наиболее интересным из полученных результатов является, на наш взгляд, построение стратегии с двумя обратными связями, исправляющей одну ошибку в двоичном канале и передающей столько же сообщений, как и полностью адаптивная стратегия.

Оставшаяся часть статьи построена следующим образом. В § 2 приводятся основные определения. В § 3 сформулирована и доказана основная теорема, описывающая структуру оптимальных стратегий с одной ошибкой и однократной обратной связью. В § 4 основная теорема применяется для построения стратегии передачи данных по двоичному каналу с двумя обратными связями, исправляющей одну ошибку и позволяющей передать в точности столько же сообщений, сколько передается при полной обратной связи. В последнем параграфе разработанная техника применяется для поиска хороших стратегий для двоичного асимметричного канала с одной ошибкой и однократной обратной связью.

§ 2. Основные определения

Рассмотрим канал с q-ичным входным алфавитом $\mathcal{X} = \{0, \ldots, q-1\}$ и выходным алфавитом $\mathcal{Y} = \mathcal{X}$. Кодер передает сообщение $\boldsymbol{x} \in \mathcal{X}^n$, декодер получает сообщение $\boldsymbol{y} \in \mathcal{Y}^n$. Префикс длины p вектора $\boldsymbol{y}$ будем обозначать $\boldsymbol{y}_{\overline{p}}$. Ошибкой будем называть замену символа q_1 последовательности $\boldsymbol{x}$ на символ q_2, $q_1 \neq q_2$. Определим двудольный граф ошибок G, левая доля которого соответствует элементам из $\mathcal{X}$, а правая – элементам из $\mathcal{Y}$. Соединим $q_1 \in \mathcal{X}$ и $q_2 \in \mathcal{Y}$, $q_1 \neq q_2$, ребром, если при ошибке символ q_1 может перейти в q_2. Пример такого графа для троичного однонаправленного канала изображен на рис. 1.

В данной статье рассматривается передача данных по каналу с k обратными связями. Пусть длина кодового слова n разбита на $k+1$ частей:

$$n = n_1 + n_2 + \ldots + n_{k+1}.$$

Кодер передает сообщение $m \in [M]$. Первые n_1 передаваемых символов $x_1, \ldots, x_{n_1}$ зависят только от сообщения m. После передачи $N_{i-1} := n_1 + \ldots + n_{i-1}$ символов, $i \geqslant 2$, кодер имеет из канала обратной связи значения принятых символов $\boldsymbol{y}_{\overline{N_{i-1}}}$.

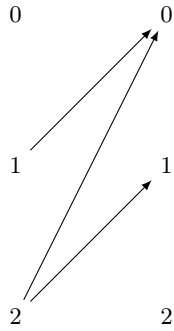

Рис. 1. Граф ошибок для троичного однонаправленного канала

Кодер посылает i-й блок из n_i символов, являющийся функцией от сообщения m и принятых им символов $\boldsymbol{y}_{\overline{N_{i-1}}}$. Случай $k = 0$ соответствует каналу без обратной связи, а случай $k = n - 1$ – каналу с полной обратной связью.

Определим облако $B_t(m)$ ($B(m)$ для $t = 1$) для сообщения m как множество последовательностей $\boldsymbol{y}$, которые могут быть получены на выходе канала с не более чем t ошибками при передаче этого сообщения. Будем называть набор непересекающихся облаков $B_t(m)$, $m \in [M]$, кодом $\mathcal{C}$, исправляющим t ошибок. Точки пространства, не принадлежащие ни одному облаку, будем называть свободными и обозначать через $\mathcal{F}(\mathcal{C})$. Коды, не использующие обратной связи, будем называть неадаптивными.

Отметим, что для симметричного канала без обратной связи облаками являются шары радиуса t в метрике Хэмминга. Для симметричного канала размеры всех облаков одинаковы, однако для произвольного графа ошибок это не так. Для предлагаемых в статье конструкций имеет смысл находить коды с максимальным количеством свободных точек для каждой длины и каждой мощности. Такие коды будем называть F-оптимальными.

В качестве примера опишем структуру облаков для двоичного канала с одной ошибкой и полной обратной связью. Каждое облако $B(m)$ содержит последовательность $\boldsymbol{y}$, которая будет передана в том случае, если в канале нет ошибок. Назовем эту последовательность корневой. Для любой координаты i в облаке присутствует последовательность $\boldsymbol{y}(i)$, которая совпадает с $\boldsymbol{y}$ в первых $i-1$ позициях, отличается в i-й позиции, а в остальных позициях имеет произвольные символы. Отсюда видно, что каждое облако состоит как минимум из $n + 1$ последовательностей. В частности, отсюда следуют граница Хэмминга на максимальное количество передаваемых сообщений.

§ 3. Однократная обратная связь

В этом параграфе предложена стратегия передачи сообщений с одной ошибкой и однократной обратной связью. Разобьем кодовую длину n на две части n_1 и n_2, где $n = n_1 + n_2$. Определим двудольный граф $H = (U \sqcup V, E)$ следующим образом. Левая и правая доли состоят из q^{n_1} вершин, соответствующих множествам входящих и выходящих последовательностей. Вершины u и v соединяются ребром, если последовательность, соответствующая v, может получиться из последовательности, соответствующей u, в результате одной ошибки. Отметим, что мы не соединяем ребрами вершины, соответствующие совпадающим последовательностям (это соответствует случаю, когда ошибки не происходит).

Теорема 1. *Пусть задан граф* $H = (U \sqcup V, E)$. *Стратегия, передающая*

$$M = \sum_{u \in U} M(u) \tag{1}$$

сообщений, существует тогда и только тогда, когда имеются коды $\mathcal{C}(u)$, *описанные выше, удовлетворяющие условию*

$$\sum_{u:\,(u,v)\in E} M(u) \leqslant F(v) \tag{2}$$

для любого $v \in V$.

Доказательство. Опишем произвольную стратегию кодирования. Сначала передается последовательность $\boldsymbol{u}$ длины n_1, которой соответствует вершина u из левой доли U графа H. Пусть количество сообщений, передача которых начинается с последовательности $\boldsymbol{u}$, равно $M(u)$. Рассмотрим случай, когда в первых n_1 символах ошибки не произошло. На оставшихся n_2 символах нам необходимо передать $M(u)$ различных сообщений, причем может произойти одна ошибка. Поэтому необходимо использовать код $\mathcal{C}(u)$ длины n_2 и мощности $M(u)$, исправляющий одну ошибку. Обозначим через $F(u)$ число свободных точек кода $C(u)$.

В том случае, если в первых n_1 символах произошла ошибка и вместо последовательности $\boldsymbol{u}$ была получена $\boldsymbol{v}$, для передачи $M(u)$ сообщений с началом $\boldsymbol{u}$ нужно $M(u)$ точек, причем это должны быть свободные точки кода $\mathcal{C}(v)$.

Таким образом, для каждого сообщения $\boldsymbol{v}$ должен существовать код $\mathcal{C}(v)$, свободные точки которого распределены между последовательностями $\boldsymbol{u}$, из которых можно попасть в последовательность $\boldsymbol{v}$, причем каждой такой последовательности $\boldsymbol{u}$ должно достаться не менее $M(u)$ свободных точек, что возможно тогда и только тогда, когда выполняется условие (2).

Теперь опишем алгоритм декодирования. Пусть последовательность из первых n_1 полученных символов соответствует вершине $v \in V$, последовательность из n_2 последних символов обозначим через $\boldsymbol{a}$. Если $\boldsymbol{a}$ не является свободной точкой кода $\mathcal{C}(v)$, то это значит, что ошибка произошла во второй части сообщения. В этом случае вторая часть сообщения соответствует центру шара, которому принадлежит точка $\boldsymbol{a}$.

Если же последовательность $\boldsymbol{a}$ оказалась свободной точкой кода $\mathcal{C}(v)$, то она относится к какой-то последовательности $\boldsymbol{u}$, из которой может быть получена $\boldsymbol{v}$. Именно эта последовательность $\boldsymbol{u}$ и передавалась на первой стадии кодирования. Вторая часть сообщения восстанавливается исходя из того, какая именно точка $\boldsymbol{a}$ была использована из не менее $M(u)$ точек, относящихся к $\boldsymbol{u}$. ▲

Нам не известен эффективный (полиномиальный от длины кода) способ нахождения оптимального набора кодов, удовлетворяющих (2). Однако даже выбор одинаковых кодов для всех последовательностей $\boldsymbol{u} \in \mathcal{X}^{n_1}$ может дать неплохой результат, как показано в следствии 1.

В качестве примера неоптимальности выбора одинаковых кодов для двоичного канала рассмотрим случай $n_1 = 2, n_2 = 1$. При выборе одинаковых кодов максимальное количество сообщений всегда делится на 2^{n_1}, и в данном случае оно равно 0, так как даже адаптивно на длине 3 нельзя передать больше двух сообщений. При выборе разных кодов можно передать два сообщения.

Следующее утверждение для двоичного симметричного канала будет использовано в дальнейшем для построения оптимальной стратегии с двумя обратными связями.

Следствие 1. *Пусть* $n_2 = 2^k - 1$, $n_1 = n - n_2$, $k \geqslant 1$. *Тогда в симметричном канале с одной ошибкой и однократной обратной связью можно передать*

$$M_1(n) = 2^{n_1} \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor$$

сообщений.

Доказательство. Назначим каждой точке $\boldsymbol{u}$ в качестве кода $\mathcal{C}(u)$ код Хэмминга длины n_2, из которого удалено x слов. Выберем x так, чтобы выполнялись ограничения (2), что эквивалентно неравенству

$$x2^k \geqslant n_1(2^{n_2-k} - x),$$

откуда получаем

$$x \geqslant \frac{n_1 2^{n_2-k}}{n_1 + 2^k}.$$

Тогда можно взять $x = \left\lceil \frac{n_1 2^{n_2-k}}{n_1 + 2^k} \right\rceil$. Количество оставшихся слов в выбранных кодах равно

$$2^{n_2-k} - \left\lceil \frac{n_1 2^{n_2-k}}{n_1 + 2^k} \right\rceil = \left\lfloor \frac{2^{n_2}}{n_1 + 2^k} \right\rfloor = \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor.$$

Суммарное количество передаваемых сообщений равно

$$M_1(n) = 2^{n_1} \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor. \quad \blacktriangle$$

§ 4. Двоичный симметричный канал с обратной связью

Обозначим через $\mathrm{Alg}_k(n)$ стратегию передачи сообщений по каналу длины n с одной ошибкой и k обратными связями. Опишем алгоритм построения стратегии $\mathrm{Alg}_k(n)$ из $\mathrm{Alg}_{k-1}(n-1)$, который будет использоваться в дальнейшем.

Алгоритм DADA (Double and Delete Algorithm) построения стратегии $\mathrm{Alg}_k(n)$ из $\mathrm{Alg}_{k-1}(n-1)$. Напомним, что каждое облако в двоичном симметричном канале длины $n-1$ содержит корневое сообщение и $n-1$ дополнительных, которые совпадают с корневым в первых $i-1$ символах и отличаются в i-м, $i = 1, 2, \ldots, n-1$. Из каждого облака сообщений длины $n-1$ построим два множества сообщений длины n, дописав слева ко всем сообщениям 0 для первого множества и 1 для второго. Для того чтобы из первого (второго) множества сделать облако на длине n, достаточно добавить любое сообщение, начинающееся на 1 (0). Будем называть такие множества неполными облаками. Далее, из каждой свободной точки сделаем две свободных точки, дописав слева 0 или 1. Потратим все имеющиеся свободные последовательности на то, чтобы какое-то количество неполных облаков превратить в облака. Если число неполных облаков не больше, чем свободных последовательностей длины n, то в конце этой процедуры у нас будет $2M(n-1)$ облаков и какое-то количество свободных точек, где $M(n-1)$ – количество сообщений, передаваемых алгоритмом $\mathrm{Alg}_{k-1}(n-1)$. В этом случае алгоритм DADA завершается.

В противном случае в конце этой процедуры получится какое-то количество облаков и какое-то количество неполных облаков, полностью покрывающих пространство.

В дальнейшем будем брать одно неполное облако, последовательности в котором начинаются на 1, и одно неполное облако, последовательности в котором начинаются на 0, и уничтожать их, превращая все их элементы в свободные точки. Такая

операция дает $2n$ свободных точек. Далее, свободные точки используются на то, чтобы из неполных облаков сделать облака. Операция повторяется до тех пор, пока неполные облака не закончатся.

В конце процедуры останется четное количество облаков и не более $2n$ свободных точек. Если количество свободных точек равно $2n$, то это значит, что только что два неполных облака были преобразованы в эти $2n$ свободных точек. Восстановим одно из этих неполных облаков обратно и превратим в облако, дополнив одной свободной точкой. В результате получится дополнительное облако.

Таким образом, доказана следующая

Теорема 2. *Предположим, что на длине $n-1$ построено $M(n-1)$ облаков для передачи сообщений с одной ошибкой и $k-1$ обратными связями, $k = 1, \dots, n-1$. Пусть*

$$U(n) = 2\left\lfloor \frac{2^n}{2(n+1)} \right\rfloor, \quad r(n) = 2^n - (n+1)U(n).$$

Тогда алгоритм DADA строит стратегию $\mathrm{Alg}_k(n)$, передающую $M(n)$ сообщений, где

$$M(n) = \begin{cases} 2M(n-1), & \text{если } 2M(n-1) \leqslant \dfrac{2^n}{n+1}, \\ U(n), & \text{если } 2M(n-1) > \dfrac{2^n}{n+1} \text{ и } r(n) < 2n, \\ U(n)+1, & \text{если } 2M(n-1) > \dfrac{2^n}{n+1} \text{ и } r(n) \geqslant 2n. \end{cases}$$

В случае полной обратной связи оптимальное количество сообщений, которое можно передать с одной ошибкой, было вычислено в работе [5]. В теореме 3 мы приводим новое более простое доказательство этого результата.

Теорема 3. *Пусть*

$$U(n) = 2\left\lfloor \frac{2^n}{2(n+1)} \right\rfloor, \quad r(n) = 2^n - (n+1)U(n).$$

Тогда по каналу с одной ошибкой возможно передать $M_{\mathrm{ad}}(n)$ сообщений, где

$$M_{\mathrm{ad}}(n) = \begin{cases} U(n), & \text{если } r(n) < 2n, \\ U(n)+1, & \text{если } r(n) \geqslant 2n. \end{cases} \tag{3}$$

Более того, это количество сообщений является оптимальным.

Замечание 1. На самом деле, r всегда четно и меньше $2n+2$, поэтому в последней строке условие $r \geqslant 2n$ можно заменить на $r = 2n$. Отметим, что второй случай реализуется очень редко. А именно, мощность кода равна $U(n)+1$ при $n = 1, 2$, а следующая длина кода, при которой это происходит, равна 49736. Таким образом, оптимальным количеством сообщений чаще всего является максимальное четное число, не превосходящее границы Хэмминга.

Доказательство. Будем строить стратегию передачи сообщений индуктивно. Для $n \leqslant 8$ формула проверяется вручную.

Теперь предположим, что для длины $n-1$, $n \geqslant 9$, у нас построено $M_{\mathrm{ad}}(n-1)$ облаков. Заметим, что количество неполных облаков не меньше

$$2M_{\mathrm{ad}}(n-1) \geqslant \frac{2^n}{n} - 4 > \frac{2^n}{n+1}$$

Таблица 1

Максимальные количества передаваемых сообщений в двоичном симметричном канале с одной ошибкой с однократной обратной связью и с полной обратной связью

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16
M_1	2	2	4	8	16	28	50	90	168	312	580	1088	2048	3854
M_{ad}	2	2	4	8	16	28	50	92	170	314	584	1092	2048	3854

при $n \geqslant 9$. Используем алгоритм DADA для построения адаптивной стратегии на длине n из стратегии на длине $n-1$. Так как $2M_{\text{ad}}(n-1) > \dfrac{2^n}{n+1}$, то $M_{\text{ad}}(n)$ равно $U(n)$ или $U(n)+1$ в зависимости от $r(n)$, что и требовалось доказать. ▲

Теорема 4. *В двоичном канале с двумя обратными связями и одной ошибкой можно передать $M_{\text{ad}}(n)$ сообщений, т.е. столько же, сколько и при полной обратной связи.*

Отметим, что однократной обратной связи для этого недостаточно, что можно увидеть из табл. 1.

Доказательство. Воспользуемся алгоритмом DADA для построения $\text{Alg}_2(n)$ из $\text{Alg}_1(n-1)$. В качестве $\text{Alg}_1(n-1)$ возьмем стратегию, построенную в следствии 1 с $M_1(n-1) = \left\lfloor \dfrac{2^{n_2}}{n_1+n_2+1} \right\rfloor 2^{n_1}$, где $n_2 = 2^k - 1$, $n_1 = n-1-n_2$.

Заметим (см. табл. 1), что для $n \leqslant 9$ даже однократной обратной связи достаточно для передачи такого же количества сообщений, как и при кодировании с полной обратной связью. Поэтому достаточно доказать утверждение для $n \geqslant 10$. Покажем, что $2M_1(n-1) > \dfrac{2^n}{n+1}$ при $n \geqslant 10$.

Это эквивалентно неравенству

$$2^{n_1+1} \left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor > \frac{2^{n_1+n_2+1}}{n_1+n_2+2}.$$

Сократив на 2^{n_1+1} и применив неравенство $\lfloor x \rfloor > x-1$, получаем

$$\left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor > \frac{2^{n_2}}{n_1+n_2+1} - 1 \geqslant \frac{2^{n_2}}{n_1+n_2+2}.$$

Последнее неравенство эквивалентно

$$2^{n_2} \geqslant (n_1+n_2+1)(n_1+n_2+2).$$

Вспоминая, что $n_2 \geqslant n_1$ и $n_2 = 2^k - 1$, получаем, что неравенство выполнено при $n_2 \geqslant 15$.

Таким образом, мы доказали неравенство $2M_1(n-1) > \dfrac{2^n}{n+1}$ для $n \geqslant 16$. Для $n \in [10, 15]$ неравенство можно проверить вручную по табл. 1. Воспользовавшись теоремами 2 и 3, получаем требуемое утверждение. ▲

§ 5. Двоичный асимметричный канал

В данном параграфе мы применяем полученные ранее теоремы к двоичному асимметричному каналу. Для этого нам нужно составить таблицы кодов с большим числом свободных точек. Для нахождения таких кодов будет использован метод линейного программирования.

В работах [16–18] линейное программирование использовалось для доказательства верхних оценок мощности неадаптивных кодов, исправляющих асимметричные

ошибки. Мы модифицируем методы этих работ для получения верхних оценок количества свободных точек в коде фиксированной длины и мощности.

Обозначим через $M_Z(n,t)$ максимальную мощность асимметричного кода длины n, исправляющего t ошибок. Кроме того, обозначим через $L(n,d,w)$ и $U(n,d,w)$ нижнюю и верхнюю границы мощности равновесного кода веса w и длины n с расстоянием d.

Теорема 5. *Пусть $n \geqslant 2t \geqslant 2$, $1 \leqslant M \leqslant M_Z(n,t)$. Определим*

$$\overline{F}(n,M,t) = \max\left(2^n - \sum_{i=0}^{n}\left(z_i \sum_{j=0}^{t}\binom{i}{i-j}\right)\right),$$

где максимум берется по всем z_i, удовлетворяющим следующим условиям:

1) z_i – *неотрицательные целые*;

2) $z_0 = 1$, $z_1 = z_2 = \ldots = z_t = 0$;

3) $\displaystyle\sum_{i=1}^{s}\binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s}\binom{w+j}{j} z_{w+j} \leqslant \binom{n}{w}$ *для* $0 \leqslant s \leqslant t < w < n-t$;

4) $\displaystyle\sum_{j=s}^{r} z_j L(r-s, 2t+2, r-j) \leqslant U(n+r-s, 2t+2, r)$ *для* $0 \leqslant s \leqslant r$;

5) $\displaystyle\sum_{j=s}^{r} z_{n-j} L(r-s, 2t+2, r-j) \leqslant U(n+r-s, 2t+2, r)$ *для* $0 \leqslant s \leqslant r$;

6) $\displaystyle\sum_{i=1}^{s}\binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s}\binom{w+j}{j} z_{w+j} + \left(\binom{w+t-s+1}{w} - \binom{t+1}{t-s+1} \times \right.$
$\displaystyle\left. \times \left\lfloor \frac{w+t-s+1}{t+1} \right\rfloor\right) z_{w+t-s+1} \leqslant \binom{n}{w}$ *для* $0 \leqslant s \leqslant t < w < n-t$,

$\displaystyle\sum_{i=1}^{s}\binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s}\binom{w+j}{j} z_{w+j} + \left(\binom{n-w+s+1}{s+1} - \binom{t+1}{t-s} \times \right.$
$\displaystyle\left. \times \left\lfloor \frac{n-w+s+1}{t+1} \right\rfloor\right) z_{w-s-1} \leqslant \binom{n}{w}$ *для* $0 \leqslant s \leqslant t < w < n-t$;

7) $\displaystyle\sum_{i=0}^{n} z_i = M$.

Тогда количество свободных точек F в коде длины n и мощности M, исправляющем t асимметричных ошибок, не превосходит $\overline{F}(n,M,t)$.

Доказательство. Обозначим через z_i, $0 \leqslant i \leqslant n$, количество кодовых слов веса i в коде длины n, исправляющем t асимметричных ошибок. В работах [16–18] было доказано, что числа z_i должны удовлетворять ограничениям 1), 3)–6). Легко видеть, что код с максимальным количеством свободных точек должен удовлетворять условию 2). Последнее условие фиксирует мощность рассматриваемого кода. Оптимизируемое выражение $\overline{F}(n,M,t)$ соответствует количеству свободных точек в коде с весовым распределением $\{z_i\}$. ▲

Используем также метод линейного программирования для поиска кодов с максимальным количеством свободных точек. Зафиксируем длину кода n, мощность кода M и количество исправляемых асимметричных ошибок t. Введем 2^n двоичных переменных x_i, соответствующих всем возможным кодовым словам. Для каждой точки p определим множество $D_t(p)$ кодовых слов, из которых в эту точку мож-

Таблица 2

Оптимальное количество свободных точек $(n, M, 1)$-кодов

$n = 6$	Мощность M	12	11	10	9	8
	Свободные точки F	16	23	28	33	38
$n = 7$	Мощность M	18	17	16	15	14
	Свободные точки F	48	56	62	68	73
$n = 8$	Мощность M	36	35	34	33	32
	Свободные точки F	76	85	92	99	106
$n = 9$	Мощность M	62	61	60	59	58
	Свободные точки F	177	186	193	200	207

но попасть, совершив t асимметричных ошибок. Введем ограничение $\sum\limits_{i \in D_t(p)} x_i \leqslant 1$. Максимизируем количество свободных точек $2^n - \sum\limits_{i=0}^{n} z_i(i+1)$, где z_i – количество кодовых слов веса i. Отметим, что количество свободных точек выражается через переменные x_i. Добавим ограничение $\sum x_i = M$, чтобы зафиксировать мощность кода. Отметим, что любое решение данной задачи линейного программирования (если оно существует) выдает оптимальное количество свободных точек для фиксированных длины и мощности кода. Для ускорения вычислений мы добавили ограничения из теоремы 5.

Несмотря на эти оптимизации, программа работает с 2^n переменными, а значит, решение может быть найдено только для достаточно малых значений n. В табл. 2 приводятся параметры некоторых F-оптимальных кодов для $t = 1$ и $n = 6, 7, 8$ и 9. Оптимальные весовые распределения приведены в табл. 3.

Параметры кодов длины $n = 6, 8$ и 9 совпадают с верхними границами, которые дает теорема 5. Для $n = 7$ и $M = 18$ мы получили 48 свободных точек вместо 49, которые дает верхняя граница из теоремы 5, т.е. верхняя граница из теоремы 5 не достигается. Все остальные значения совпадают с верхними границами.

Коды с оптимальным весовым распределением для длины $n = 7, 8$ были построены в [16]. Код для длины $n = 6$ тоже был известен ранее. Для длин $n = 6, 8$ и всех мощностей $M \leqslant M_Z(n, 1)$ оптимальные коды могут быть получены из кода максимальной мощности с весовым распределением, указанным в табл. 3, путем удаления $M_Z(n, d) - M$ кодовых слов максимального веса. Для длины $n = 7$ и мощности $M = 17$ нам известны два кода с разными весовыми распределениями с оптимальным количеством свободных точек: 1+0+3+5+5+3+0+0 и 1+0+3+5+6+1+1+0. Удаляя кодовые слова максимального веса из кода со вторым весовым распределением, получаем F-оптимальные коды для всех $M < 17$. Однако только код с первым весовым распределением можно дополнить до кода мощности 18.

Программа работает для всех длин $n < 9$. Для больших длин сложность слишком велика. Так как F-оптимальные конструкции для длин $n = 6, 8$ являются вложенными кодами, то мы ограничиваемся поиском среди таких семейств и для длины $n = 9$. Этот подход позволил найти такое семейство вложенных кодов, что максимальный код мощности 62 имеет весовое распределение, приведенное в табл. 3. Количество свободных точек в кодах семейства совпадает с верхними границами из теоремы 5 для всех мощностей M. Это означает, что коды из построенного семейства являются F-оптимальными. Отметим, что код максимальной мощности длины $n = 9$, построенный в [16], имеет 171 свободную точку, в то время как в нашем коде 177 свободных точек.

Имея в своем распоряжении таблицы кодов со свободными точками, мы можем воспользоваться теоремой 1 для построения стратегий передачи данных по асиммет-

Таблица 3

Оптимальные весовые распределения

Длина и мощность	Весовое распределение
$n = 6,\ M = 12$	$1+0+3+4+3+0+1$
$n = 7,\ M = 18$	$1+0+3+5+5+3+1+0$
$n = 7,\ M = 17$	$1+0+3+5+6+1+1+0$
$n = 8,\ M = 36$	$1+0+4+8+10+8+4+0+1$
$n = 9,\ M = 62$	$1+0+4+9+17+17+11+2+1+0$

Таблица 4

Количество передаваемых сообщений по асимметричному каналу с однократной обратной связью и одной ошибкой

n	5	6	7	8	9	10	11	12	13
M (следствие 2)	9	16	29	52	96	177	327	607	1120
M (теорема 1)	9	16	29	53	97	$\geqslant 177$	$\geqslant 329$	$\geqslant 607$	$\geqslant 1120$

ричному каналу с обратной связью. В случае, когда параметры $M(v)$ и $F(v)$ зависят только от веса слова, получаем следующее утверждение.

Следствие 2. *Пусть $M(v) = M_w$ и $F(v) = F_w$ для всех $v \in V$, таких что количество единиц в v равно w, т.е. $M(v)$ и $F(v)$ зависят только от веса слова v. Если условия*

$$(n_1 - w)M_{w+1} \leqslant F_w \tag{4}$$

выполняются для всех $w \in [0, n_1 - 1]$, то количество передаваемых сообщений равно

$$M = \sum_{w=0}^{n_1} \binom{n_1}{w} M_w. \tag{5}$$

Количества сообщений, передаваемых алгоритмами, построенными с помощью следствия 2 и теоремы 1, приведены в табл. 4. Для вычисления значений M_w и F_w, дающих оптимальный ответ, была использована техника динамического программирования. В приведенных ниже примерах мы даем подробное описание кодов, полученных с помощью следствия 2 и теоремы 1 для длин $n = 9$ и $n = 8$ соответственно.

Будем обозначать через $(n, M, F, t)_Z$ неадаптивный код длины n, исправляющий t асимметричных ошибок, имеющий M кодовых слов и F свободных точек. В первом примере продемонстрируем применение следствия 2, где используемый после обратной связи код зависит только от веса слова, передаваемого до обратной связи. На длине $n = 8$ применение следствия 2 позволяет передать только 52 сообщения. Во втором примере мы показываем, как с помощью теоремы 1 можно передать 53 сообщения. Это означает, что следствие 2 не всегда дает оптимальный ответ.

Пример 1. $n = 9,\ M = 96$.

Пусть $n_1 = 5$, $n_2 = 4$. Вершинам, соответствующим двоичным словам веса 0 и 1, мы сопоставляем $(4, 2, 12, 1)_Z$-код из двух слов $\{0000, 0011\}$. Вершинам веса 2 и 3 сопоставляем $(4, 3, 9, 1)_Z$-код из трех слов $\{0000, 0011, 1100\}$. Весам 4 и 5 сопоставляем $(4, 4, 4, 1)_Z$-код из четырех слов $\{0000, 0011, 1100, 1111\}$.

Проверим ограничения $(n_1 - w)M_{w+1} \leqslant F_w$ для $w \in [0, 4]$:

$w = 0:\ 5 \cdot 2 \leqslant 12,$

$w = 1:\ 4 \cdot 3 \leqslant 12,$

$w = 2:\ 3 \cdot 3 \leqslant 9,$

Таблица 5

Мощности кодов для асимметричного канала с полной обратной связью и одной ошибкой

n	5	6	7	8	9	10	11	12	13
M [11]	8	16	32	32	64	128	256	512	1024
M_{ad}	11	20	36	66	121	223	415	774	1452

$w = 3: \ 2 \cdot 4 \leqslant 9,$

$w = 4: \ 1 \cdot 4 \leqslant 4.$

С помощью формулы (5) вычисляем количество передаваемых сообщений:

$$1 \cdot 2 + 5 \cdot 2 + 10 \cdot 3 + 10 \cdot 3 + 5 \cdot 4 + 1 \cdot 4 = 96.$$

Пример 2. $n = 8$, $M = 53$.

Пусть $n_1 = 6$, $n_2 = 2$. Вершине 111111 сопоставим $(2, 2, 0, 1)_Z$-код $\{00, 11\}$. Вершинам 111000, 001110, 010101, 100011, 100100, 010010, 001001, 110000, 010100, 001000, 000010, 000001 сопоставим $(2, 0, 4, 1)_Z$-код из 0 слов. Остальным вершинам сопоставим $(2, 1, 3, 1)_Z$-код из одного слова $\{00\}$. Легко проверить, что условия (2) из теоремы 1 выполняются. Например, проверим условия для вершины $v = 101000$: есть всего 4 вершины $\{111000, 101100, 101010, 101001\}$, из которых можно попасть в v. Мощности соответствующих кодов

$$M(111000) = 0, \quad M(101100) = 1,$$
$$M(101010) = 1, \quad M(101001) = 1.$$

Сумма этих мощностей не превосходит $F(101000) = 3$, т.е. ограничение для вершины $v = 101000$ выполнено. Таким же образом можно проверить и ограничения для остальных вершин.

Суммарное количество передаваемых сообщений равно $2 + 0 + 51 = 53$.

Приведем таблицу с количеством сообщений, которое можно передать по каналу с одной асимметричной ошибкой и полной обратной связью. Наилучшие результаты получены в работе [11], где для передачи $M = 2^m$ сообщений требуется длина $n = m - 1 + \lceil \log_2(m + 3) \rceil$. Несмотря на то, что мы используем только однократную обратную связь, нам удается передать больше сообщений, чем в [11], при $n \leqslant 13$, кроме случая $n = 7$. Для асимметричного канала с полной обратной связью и одной ошибкой можно использовать алгоритм, аналогичный DADA, позволяющий строить коды с оптимальным количеством передаваемых сообщений M_{ad}. Мощности этих кодов приведены в табл. 5. Подробное описание построения таких кодов будет приведено в одной из последующих работ.

СПИСОК ЛИТЕРАТУРЫ

1. *Rényi A.* On a Problem of Information Theory // Magyar Tud. Akad. Mat. Kutató Int. Közl. 1961. V. 6. P. 505–516.
2. *Berlekamp E.R.* Block Coding for the Binary Symmetric Channel with Noiseless, Delayless Feedback // Error-Correcting Codes (Proc. Conf. Conducted by the Mathematics Research Center, United States Army, at the University of Wisconsin, Madison, May 6–8, 1968). New York: Wiley, 1969. P. 61–85.
3. *Зигангиров К.Ш.* О числе исправляемых ошибок при передаче по ДСК с обратной связью // Пробл. передачи информ. 1976. Т. 12. № 2. С. 3–19. `http://mi.mathnet.ru/ppi1683`
4. *Ulam S.M.* Adventures of a Mathematician. New York: Scribner, 1976.

5. *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
6. *Guzicki W.* Ulam's Searching Game with Two Lies // J. Combin. Theory Ser. A. 1990. V. 54. № 1. P. 1–19. https://doi.org/10.1016/0097-3165(90)90002-E
7. *Deppe C.* Solution of Ulam's Searching Game with Three Lies or an Optimal Adaptive Strategy for Binary Three-Error-Correcting Codes // Discrete Math. 2000. V. 224. № 1–3. P. 79–98. https://doi.org/10.1016/S0012-365X(00)00109-6
8. *desJardins D.L.* Precise Coding with Noiseless Feedback. Ph.D. Thesis. Dept. of Mathematics, Univ. of California, Berkeley, 2002. Available at http://www.desjardins.org/david/thesis/thesis.pdf
9. *Rivest R.L., Meyer A.R., Kleitman D.J., Winklmann K., Spencer J.* Coping with Errors in Binary Search Procedures // J. Comput. System Sci. 1980. V. 20. № 3. P. 396–404. https://doi.org/10.1016/0022-0000(80)90014-8
10. *Cicalese F.* Fault-Tolerant Search Algorithms: Reliable Computation with Unreliable Information. Berlin: Springer, 2013.
11. *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
12. *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
13. *Spencer J., Yan C.H.* The Halflie Problem // J. Combin. Theory Ser. A. 2003. V. 103. № 1. P. 69–89. https://doi.org/10.1016/S0097-3165(03)00068-2
14. *Бассалыго Л.А.* Недвоичные коды, исправляющие ошибки при наличии одноразовой безошибочной обратной связи // Пробл. передачи информ. 2005. Т. 41. № 2. С. 63–67. http://mi.mathnet.ru/ppi96
15. *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
16. *Delsarte P., Piret P.* Bounds and Constructions for Binary Asymmetric Error-Correcting Codes // IEEE Trans. Inform. Theory. 1981. V. 27. № 1. P. 125–128. https://doi.org/10.1109/TIT.1981.1056290
17. *Kløve T.* Upper Bounds on Codes Correcting Asymmetric Errors // IEEE Trans. Inform. Theory. 1981. V. 27. № 1. P. 128–131. https://doi.org/10.1109/TIT.1981.1056291
18. *Weber J., de Vroedt C., Boekee D.* New Upper Bounds on the Size of Codes Correcting Asymmetric Errors // IEEE Trans. Inform. Theory. 1987. V. 33. № 3. P. 434–437. https://doi.org/10.1109/TIT.1987.1057301

Воробьев Илья Викторович
Деппе Кристиан (Deppe, Christian)
Технический университет Мюнхена, Германия
vorobyev.i.v@yandex.ru
christian.deppe@tum.de
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
20.09.2022
После доработки
28.11.2022
Принята к публикации
28.11.2022