ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 3**

УДК 621.391 : 519.725

 Г. Маринге́р[1], Н.А. Полянский[2], И.В. Воробьев[3], Л. Вельтер[4]

КОДЫ С ОБРАТНОЙ СВЯЗЬЮ, ИСПРАВЛЯЮЩИЕ ВСТАВКИ И ВЫПАДЕНИЯ

Рассматривается задача передачи информации по комбинаторному каналу со вставками и выпадениями и обратной связью. Предположим, что отправитель передает n двоичных символов один за другим по каналу, в котором могут происходить вставки и выпадения. После передачи каждого символа отправитель узнает, какие вставки и выпадения произошли в канале, и адаптирует алгоритм кодирования. Целью статьи является разработка стратегии кодирования, позволяющей безошибочно передавать максимальное количество информации в предположении, что общее количество вставок и выпадений не превосходит τn для некоторой константы τ, $0 < \tau < 1$. Мы покажем, как эта задача может быть сведена к задаче передачи информации по каналу с замещениями. Таким образом, максимальная асимптотическая скорость кодов для комбинаторного канала со вставками и выпадениями с обратной связью полностью установлена. Вычисление максимальной асимптотической скорости кодов для комбинаторного канала с замещениями и обратной связью было частично выполнено Берлекэмпом и окончено позже Зигангировым. Однако доказательство Зигангирова нижней оценки скорости достаточно сложное. Мы возвращаемся к результату Зигангирова и представляем более подробное доказательство нижней границы.

Ключевые слова: кодирование с обратной связью, вставки и выпадения, асимптотическая скорость.

DOI: 10.31857/S0555292321030025

§ 1. Введение

Задача построения кодов, исправляющих вставки и выпадения, стала рассматриваться начиная с 1965 г., когда Левенштейн опубликовал свою работу [1], в которой показал, что всякий код исправляет t выпадений тогда и только тогда, когда он исправляет любую комбинацию из t выпадений и вставок. Более того, он показал, что коды Варшамова – Тененгольца [2] могут быть использованы для исправления одной вставки или выпадения. Примечательно, что большинство классических методов построения кодов, исправляющих замещения, не могут быть использованы для построения кодов для вставок и выпадений, поскольку данные виды ошибок приводят

[1] Работа выполнена при поддержке гранта немецкого научно-исследовательского сообщества (номер проекта WA3907/4-1).

[2] Работа выполнена при частичной поддержке гранта немецкого научно-исследовательского сообщества (номер проекта WA3907/1-1).

[3] Работа выполнена при частичной поддержке совместного гранта Российского фонда фундаментальных исследований (РФФИ) и Японского общества содействия науке (номер проекта 20-51-50007), а также гранта РФФИ (номер проекта 20-01-00559).

[4] Работа выполнена при поддержке гранта Европейского исследовательского совета из программы Horizon 2020 (номер проекта 801434).

к потери синхронизации между отправителем и получателем. Именно поэтому в последние годы были предложены новые подходы и развиты многочисленные методы построения кодов для комбинаторных и вероятностных каналов с выпадениями [3].

Сначала напомним некоторые известные результаты для комбинаторного канала с выпадениями без обратной связи. Пусть $\mathcal{C} \subseteq \{0,1\}^n$ является кодом, состоящим из 2^{Rn} двоичных кодовых слов длины n. Основная задача – построить код с максимально достижимой *скоростью* R, который может исправить долю τ комбинаторных ошибок типа выпадений, т.е. всевозможные комбинации τn выпадений.

Напомним, что корректирующую способность кода $\mathcal{C}$ можно определить через понятие наидлиннейшей общей подпоследовательности двух кодовых слов. Для того чтобы код исправлял долю τ ошибок, наидлиннейшая общая подпоследовательность между двумя различными кодовыми словами из $\mathcal{C}$ должна иметь длину менее $(1-\tau)n$. Очевидно, что при передаче произвольного слова через канал с долей $\tau \geqslant 1/2$ выпадений на выходе может получиться либо слово из всех единиц, либо слово из всех нулей. Таким образом, произвольный код $\mathcal{C}$ может содержать не более двух слов, и асимптотическая скорость для такого τ равна нулю. Первая конструкция кодов, исправляющих ненулевую долю ошибок типа выпадений и предполагающих эффективное кодирование и декодирование, была предложена в работе [4], авторы которой построили каскадный код, состоящий из недвоичного внешнего кода и хорошего двоичного кода, который может быть найден полным перебором. Последнее улучшение в данном направлении было получено в работах [5, 6], где было приведено семейство кодов с положительной скоростью для доли выпадений $\tau < \sqrt{2}-1 \approx 0{,}41$. Напомним, что для комбинаторного канала с ошибками типа замещений [7] нельзя построить коды с экспоненциально большим числом слов для доли ошибок $\tau \geqslant 0{,}25$. Насколько нам известно, не существует каких-либо других улучшений фундаментальных пределов для кодов, исправляющих выпадения. Таким образом, задача определения максимальной доли выпадений для кодов с положительной скоростью остается открытой в данной области.

Безошибочная обратная связь между отправителем и получателем может потенциально увеличить скорость кода, исправляющего долю выпадений τ. Модель с обратной связью для комбинаторных ошибок типа замещений была рассмотрена в работе Берлекэмпа [8]. В этой модели при передаче по каналу доля символов τ внутри передаваемого блока может поменяться на противоположные. Вдобавок после посылки очередного символа отправитель получает информацию о том, какой символ был получен на выходе канала с помощью безошибочной обратной связи. Таким образом, перед посылкой следующего символа отправитель может изменить свою стратегию на основании ранее полученных символов из канала. Максимальная асимптотическая скорость таких кодов была полностью охарактеризована Берлекэмпом [8] и Зигангировым [9]. Из их результатов следует, что скорость положительна при $\tau < 1/3$.

1.1. Обозначения. В этом пункте мы формально введем обозначения, которые будут использоваться на протяжении всей статьи. Множество целых чисел $\{1,\dots,n\}$ обозначим через $[n]$. Множество целых чисел $\{i+1, i+2, \dots, j\}$ будем кратко записывать через $(i,j]$. Под двоичным алфавитом будем подразумевать множество $\{0,1\}$. Двоичную строку длины n будем обозначать через $\boldsymbol{x} \in \{0,1\}^n$, где $\boldsymbol{x} = (x_1,\dots,x_n)$. Таким образом, символ $x_i \in \{0,1\}$ обозначает i-й элемент строки $\boldsymbol{x}$, где $i \in [n]$. Множество $\{0,1\}^*$ содержит все двоичные строки всевозможных длин и включает в себя пустую строку, которую мы обозначим через $(\ )$. Длина строки $\boldsymbol{x}$ обозначается символом $|\boldsymbol{x}|$. Для произвольных строк $\boldsymbol{x} \in \{0,1\}^{n_1}$ и $\boldsymbol{y} \in \{0,1\}^{n_2}$ обозначим конкатенацию строк $\boldsymbol{z} = (\boldsymbol{x} \,\|\, \boldsymbol{y})$, где $\boldsymbol{z} \in \{0,1\}^{n_1+n_2}$. Заметим, что двоичную строку $\boldsymbol{x} = (x_1,\dots,x_n) \in \{0,1\}^n$ можно также записать в виде $\boldsymbol{x} = (x_1 \,\|\, \dots \,\|\, x_n)$. Однако для n строк $\boldsymbol{y}_1,\dots,\boldsymbol{y}_n \in \{0,1\}^*$ мы разделяем конкатенацию строк, за-

писываемую в виде $\boldsymbol{y} = (\boldsymbol{y}_1 \,\|\, \ldots \,\|\, \boldsymbol{y}_n) \in \{0,1\}^*$, и упорядоченный набор строк $\widehat{\boldsymbol{y}} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \in (\{0,1\}^*)^n$. Набор строк $\widehat{\boldsymbol{y}}$ может быть единственным образом разложен на компоненты $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$, в то время как для строки $\boldsymbol{y}$, полученной в качестве конкатенации строк, это сделать невозможно.

Мы будем использовать две функции расстояния. Для двух произвольных строк $\boldsymbol{x} \in \{0,1\}^*$ и $\boldsymbol{y} \in \{0,1\}^*$ обозначим через $\Delta(\boldsymbol{x}, \boldsymbol{y})$ минимальное число выпадений и вставок, необходимых для получения $\boldsymbol{x}$ из $\boldsymbol{y}$. Мы также будем писать $d_H(\boldsymbol{x}, \boldsymbol{y})$ для обозначения расстояния Хэмминга между строками $\boldsymbol{x}$ и $\boldsymbol{y}$, имеющими одну длину. Все записываемые логарифмы берутся по основанию 2. Двоичная энтропия определяется как $h(x) := -x \log x - (1-x) \log(1-x)$.

1.2. Постановка задачи. В данной статье рассматривается задача передачи данных по комбинаторному каналу со вставками и выпадениями и обратной связью. Практический интерес к задаче обусловлен возможным применением к хранению данных с помощью ДНК последовательностей, где ошибки типа выпадений и вставок более распространены, чем замещения.

Для произвольного сообщения $m \in [M]$ отправитель кодирует m в двоичную строку $\boldsymbol{c} \in \{0,1\}^n$ таким образом, что после передачи строки по комбинаторному каналу со вставками и выпадениями получатель сможет декодировать исходное сообщение m по полученной строке $\boldsymbol{y}$. При передаче по каналу строки $\boldsymbol{c}$ могут происходить вставки и выпадения. Процесс кодирования и передачи сообщения состоит из n шагов, т.е. $\boldsymbol{c} = (c_1, \ldots, c_n)$. В момент времени i отправитель посылает новый двоичный символ $c_i \in \{0,1\}$ в канал. Внутри канала могут произойти вставки и выпадения. Полученную после внесения ошибок строку (возможно, пустую) обозначим через $\boldsymbol{y}_i \in \{0,1\}^*$. Отметим, что символы в процессе передачи по каналу могут быть вставлены в том числе и перед символом c_i. Получатель наблюдает только целую сконкатенированную строку $\boldsymbol{y} = (\boldsymbol{y}_1 \,\|\, \ldots \,\|\, \boldsymbol{y}_n)$, но не видит разбиения на строки $\boldsymbol{y}_i$. Иначе говоря, декодирующая функция $\mathrm{dec}(\boldsymbol{y})$ имеет следующий вид: $\mathrm{dec}\colon \{0,1\}^* \to [M]$. В момент времени $(i+1)$ отправитель корректирует свою стратегию отправки сообщения m, основываясь на упорядоченном наборе строк $\widehat{\boldsymbol{y}}^{(i)} := (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i) \in (\{0,1\}^*)^i$. Таким образом, символ $c_{i+1}\colon [M] \times (\{0,1\}^*)^i \to \{0,1\}$ является функцией исходного сообщения m и набора строк $\widehat{\boldsymbol{y}}^{(i)}$, т.е. $c_{i+1} = c_{i+1}(m, \widehat{\boldsymbol{y}}^{(i)})$. Общее количество ошибок, которое может произойти в процессе передачи по каналу, ограничено величиной t, т.е.

$$\sum_{i=1}^{n} \Delta\big(c_i(m, \widehat{\boldsymbol{y}}^{(i-1)}), \boldsymbol{y}_i\big) \leqslant t. \tag{1}$$

Целью статьи является нахождение максимального количества сообщений, которое может быть передано отправителем таким образом, что получатель всегда может восстановить переданное сообщение на основе строки $\boldsymbol{y}$, которая получается из передаваемой строки с помощью не более чем t вставок и выпадений. Формально, пусть $M_{\mathrm{id}}(n,t)$ обозначает максимальное количество сообщений, которое отправитель может передать получателю в данной модели. Мы рассматриваем случай линейной зависимости числа ошибок t от длины передаваемого сообщения n, т.е. $t = \lfloor \tau n \rfloor$, $0 \leqslant \tau \leqslant 1$. Определим *максимальную асимптотическую скорость* кодов с обратной связью, исправляющих долю τ вставок и выпадений, как

$$R_{\mathrm{id}}(\tau) := \limsup_{n \to \infty} \frac{\log M_{\mathrm{id}}(n, \lfloor \tau n \rfloor)}{n}.$$

Отметим, что длина полученной строки может достигать длины вплоть до $n + \lfloor \tau n \rfloor$, в то время как число отправленных символов равно n. Однако асимптотическая

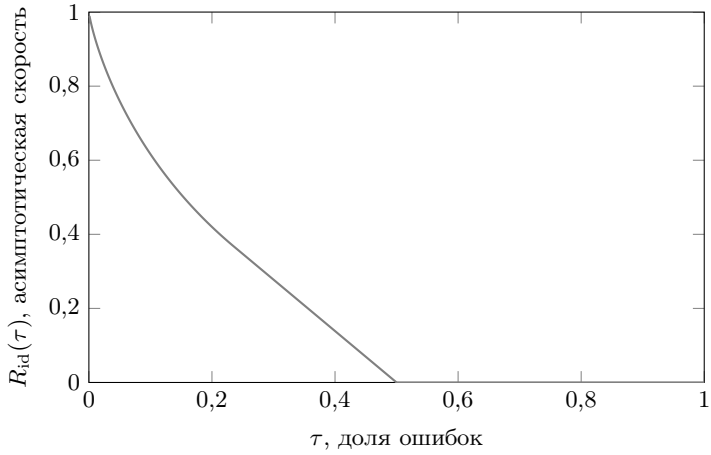

Рис. 1. Максимальная асимптотическая скорость двоичных кодов с обратной связью, исправляющих вставки и выпадения

скорость измеряется в количестве бит, нормированном на число переданных бит по каналу. В данной статье будет исследоваться величина $R_{\mathrm{id}}(\tau)$ для произвольного $\tau \in [0, 1]$.

1.3. Результаты статьи. В статье будет показано, что задача передачи информации по комбинаторному каналу со вставками и выпадениями может быть сведена к задаче передачи информации по комбинаторному каналу с замещениями. А именно, сначала мы доказываем, что любой алгоритм кодирования с n передачами по каналу с обратной связью, позволяющий исправить t вставок, может быть использован как алгоритм кодирования, исправляющий t замещений на длине $n + t$. Из этого результата будет выведена верхняя граница для $R_{\mathrm{id}}(\tau)$. Далее мы адаптируем алгоритм кодирования, изначально предложенный для канала с замещениями и обратной связью, для получения нижней границы на $R_{\mathrm{id}}(\tau)$. Эта нижняя граница совпадает с доказанной ранее верхней. Таким образом, будет получено точное значение $R_{\mathrm{id}}(\tau)$ для любой доли ошибок τ, $0 \leqslant \tau \leqslant 1$. Полученная асимптотическая скорость изображена на графике на рис. 1.

Теорема 1. *Максимальная асимптотическая скорость передачи информации по комбинаторному каналу со вставками и выпадениями и обратной связью описывается формулой*

$$R_{\mathrm{id}}(\tau) = \begin{cases} (1+\tau)\left(1 - h\left(\dfrac{\tau}{1+\tau}\right)\right) & \text{для } 0 \leqslant \tau \leqslant \sqrt{5} - 2, \\ (1-2\tau)\log\left(\dfrac{1+\sqrt{5}}{2}\right) & \text{для } \sqrt{5} - 2 < \tau \leqslant \dfrac{1}{2}, \\ 0 & \text{в противном случае.} \end{cases} \tag{2}$$

Вдобавок мы представим более подробную версию технического анализа Зигангирова [9] алгоритма Хорштейна [10] для комбинаторного канала с замещениями. Мы надеемся, что это сделает интуитивно понятный, но сложный для анализа алгоритм более доступным для широкой аудитории.

1.4. Структура статьи. Оставшаяся часть статьи организована следующим образом. В § 2 доказывается верхняя граница скорости $R_{\mathrm{id}}(\tau)$. В § 3 обсуждаются коды с обратной связью, исправляющие вставки и выпадения, и их сведение к кодам

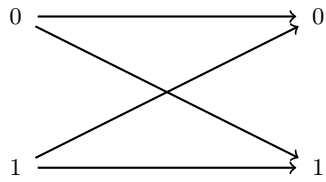

Рис. 2. Двоичный симметричный канал

с обратной связью, исправляющим замещения. Анализ кодов с обратной связью, исправляющих замещения, представлен в § 4. Статья завершается заключением в § 5.

§ 2. Верхняя граница на $R_{\mathrm{id}}(\tau)$

В этом параграфе мы вводим понятие комбинаторного канала с замещениями и доказываем, что коды с обратной связью, исправляющие долю τ вставок и выпадений, могут быть использованы как коды с обратной связью, исправляющие долю $\tau/(1+\tau)$ замещений. Это позволяет нам доказать верхнюю границу на максимальную достижимую скорость передачи по каналу со вставками и выпадениями, которая равна величине $R_{\mathrm{id}}(\tau)$, определенной в (2).

2.1. Комбинаторный канал с замещениями и обратной связью. В данной статье рассматривается только двоичный случай, поэтому и входной, и выходной алфавиты канала будут двоичными. Канал синхронизирован, и ошибкой мы называем событие, когда символ на выходе не равен соответствующему символу на входе (например, входной символ "0" заменяется на символ "1"). Передача одного бита изображена на рис. 2. Этот канал известен в теории кодирования как *двоичный симметричный канал.*

Пусть $[M] := \{1, \ldots, M\}$ обозначает множество сообщений. Задача отправителя состоит в безошибочной передаче получателю сообщения $m \in [M]$ вне зависимости от происходящих ошибок. Мы рассматриваем блочные коды с длиной блока n. Обозначим i-й символ, посылаемый отправителем в канал, через $c_i \in \{0,1\}$. Символ на выходе из канала обозначим через $y_i \in \{0,1\}$, причем $y_i \neq c_i$ в случае, если произошла ошибка. Перед посылкой i-го символа c_i в канал отправитель может скорректировать свою стратегию, основываясь на ранее принятых символах $\widehat{\boldsymbol{y}}^{(i-1)} := (y_1, \ldots, y_{i-1})$. Другими словами, $c_i \colon [M] \times \{0,1\}^{i-1} \to \{0,1\}$ является функцией от m и $\widehat{\boldsymbol{y}}^{(i-1)}$, т.е. $c_i = c_i(m, \widehat{\boldsymbol{y}}^{(i-1)})$. Отметим, что здесь $\widehat{\boldsymbol{y}}^{(i-1)}$ ничем не отличается от $\boldsymbol{y}^{(i-1)} := (y_1 \parallel \ldots \parallel y_{i-1}) \in \{0,1\}^{i-1}$, так как канал с замещениями синхронизирован. Основываясь на принятой из канала строке $\boldsymbol{y} := (y_1 \parallel \ldots \parallel y_n)$, получатель должен восстановить исходное передаваемое сообщение m. Другими словами, декодирующая функция $\mathrm{dec}(\boldsymbol{y})$ имеет вид $\mathrm{dec} \colon \{0,1\}^n \to [M]$. Мы ограничиваем величиной t общее количество ошибок, которое может произойти в канале, т.е. $d_H(\boldsymbol{c}, \boldsymbol{y}) \leqslant t$, где $\boldsymbol{c} := (c_1, \ldots, c_n)$. Пусть $M_s(n,t)$ равно максимальному количеству сообщений, которое отправитель может передать получателю безошибочно. Определим максимальную асимптотическую скорость кодов с обратной связью, исправляющих долю τ замещений, как

$$R_s(\tau) := \limsup_{n\to\infty} \frac{\log M_s(n, \lfloor \tau n \rfloor)}{n}.$$

2.2. Построение кодов, исправляющих замещения, из кодов, исправляющих вставки и выпадения. Для доказательства верхней оценки (2) максимальной скорости кодов с обратной связью, исправляющих вставки и выпадения, мы используем две

идеи. Сначала мы показываем, что код с обратной связью для вставок и выпадений может быть использован для исправления замещений.

Лемма 1. *Предположим, что нам дан код длины n и мощности M с обратной связью, способный исправлять t вставок и выпадений. Тогда существует код с обратной связью длины $n+t$ и мощности M, исправляющий t замещений.*

Далее воспользуемся верхней границей скорости $R_s(\tau)$, доказанной Берлекэмпом [8].

Теорема 2 (следствие из [8, гл. IV] и [9]). *Максимальная асимптотическая скорость для комбинаторного канала с замещениями удовлетворяет соотношению*

$$R_s(\tau) = \begin{cases} 1 - h(\tau) & \text{для } 0 \leqslant \tau \leqslant \dfrac{3-\sqrt{5}}{4}, \\ (1-3\tau)\log\left(\dfrac{1+\sqrt{5}}{2}\right) & \text{для } \dfrac{3-\sqrt{5}}{4} < \tau \leqslant \dfrac{1}{3}, \\ 0 & \text{в противном случае.} \end{cases}$$

Пользуясь леммой 1, мы получаем $M_s(n+t,t) \geqslant M_{\mathrm{id}}(n,t)$, и следовательно, $(1+\tau)R_s(\tau/(1+\tau)) \geqslant R_{\mathrm{id}}(\tau)$. Эта оценка и теорема 2 показывают, что асимптотическая скорость из теоремы 1 действительно является верхней границей на максимальную достижимую скорость комбинаторного канала со вставками и выпадениями. Таким образом, нам остается проверить справедливость леммы 1.

Доказательство леммы 1. Стратегии кодирования и декодирования данного кода с обратной связью, исправляющего вставки и выпадения, могут быть описаны функциями $c_i\colon [M] \times (\{0,1\}^*)^{i-1} \to \{0,1\}$ для $i \in [n]$ и $\mathrm{dec}\colon \{0,1\}^* \to [M]$. Мы определим кодирующую функцию $e_j\colon [M] \times \{0,1\}^{j-1} \to \{0,1\}$ для всех $j \in [n+t]$ для канала с замещениями, используя функции c_i в качестве вспомогательного инструмента. С помощью функций e_j отправитель сможет передать M сообщений по каналу с обратной связью и не более чем t замещениями на длине $n+t$.

Обозначим количество безошибочно полученных символов через i, количество переданных символов через j, индекс последнего правильно полученного символа через k, полученную на выходе канала строку через $\boldsymbol{z}$, упорядоченный набор полученных строк согласно выходу канала со вставками и выпадениями через $\widehat{\boldsymbol{y}}$.

Предлагаемая нами схема кодирования состоит из трех частей. Сначала инициализируются все счетчики и переменные, описывающие состояние схемы. Шаг 1 описывает процесс повторной передачи символа c_i, происходящей до тех пор, пока он не будет принят правильно. Шаг 2 используется лишь для того, чтобы передать нули в случае, если нами не была использована вся длина кода. Описывающие состояние алгоритма переменные i и k изменяются только на шаге 1.

Инициализация: Задаем $i \leftarrow 0$, $j \leftarrow 0$, $k \leftarrow 0$, $\boldsymbol{z} \leftarrow (\,)$ и $\widehat{\boldsymbol{y}} \leftarrow (\,)$.

Шаг 1: Определяем $e_{j+1}(m, \boldsymbol{z}) = c_{i+1}(m, \widehat{\boldsymbol{y}})$ и передаем этот символ. Обновляем $j \leftarrow j+1$. Пусть z_j – полученный символ. Обновляем $\boldsymbol{z} \leftarrow (\boldsymbol{z} \,\|\, z_j)$. Если $z_j \neq e_j(m, \boldsymbol{z})$, тогда повторяем шаг 1. Иначе, обновляем $i \leftarrow i+1$, определяем $\boldsymbol{y}_i \leftarrow \boldsymbol{z}_{[k+1,j]}$, обновляем $\widehat{\boldsymbol{y}} \leftarrow (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i)$ и $k \leftarrow j$. Если $i = n$, то переходим к шагу 2. Иначе, повторяем шаг 1.

Шаг 2: Если $j = n+t$, обновляем $\boldsymbol{y}_n \leftarrow (\boldsymbol{y}_n \,\|\, \boldsymbol{z}_{[k+1,n+t]})$, $\widehat{\boldsymbol{y}} \leftarrow (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)$ и завершаем алгоритм. Иначе, определяем $e_{j+1}(m, \boldsymbol{z}) = 0$ и передаем его. Обновляем $j \leftarrow j+1$. Пусть полученный символ равен z_j. Обновляем $\boldsymbol{z} \leftarrow (\boldsymbol{z} \,\|\, z_j)$. Повторяем шаг 2.

Алгоритм кодирования успешно завершает свою работу после $n+t$ шагов, так как у нас будет не меньше n правильно принятых символов в блоке длины $n+t$.

В качестве алгоритма декодирования можно переиспользовать алгоритм для кода со вставками и выпадениями, так как полученная на выходе из канала строка $\boldsymbol{z}$ является возможным выходом и для канала со вставками и выпадениями с не более чем t ошибками при кодировании функциями c_i, $i \in [n]$. В самом деле, если ввести обозначение $\widehat{\boldsymbol{y}}^{(i)} := (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i)$, то получится следующая цепочка равенств:

$$\sum_{i=1}^{n} \Delta\big(c_i(m, \widehat{\boldsymbol{y}}^{(i)}), \boldsymbol{y}_i\big) = \sum_{i=1}^{n} (|\boldsymbol{y}_i| - 1) = \sum_{i=1}^{n} |\boldsymbol{y}_i| - n = (n + t) - n = t.$$

Таким образом, декодирующая функция для кода со вставками и выпадениями выдаст правильное сообщение, т.е. $\operatorname{dec}(\boldsymbol{z}) = m$. ▲

§ 3. Нижняя оценка на $R_{\mathrm{id}}(\tau)$

В этом параграфе мы строим код с обратной связью, исправляющий вставки и выпадения и имеющий асимптотическую скорость, сколь угодно близкую к (2). Мы адаптируем алгоритм, изначально предложенный Хорштейном [10] и впоследствии доработанный Шалквейком [11] и Зигангировым [9]. Отметим, что этот же алгоритм уже использовался для комбинаторного канала с обратной связью и замещениями. Подчеркнем, что не любая кодирующая стратегия для комбинаторного канала с замещениями может быть так легко адаптирована для канала со вставками и выпадениями. Ключевым свойством алгоритма Хорштейна является то, что в случае ошибки отправитель перепосылает символ, посланный на прошлом шаге, до тех пор, пока он не будет принят безошибочно. Продемонстрируем важность этого свойства, рассмотрев общий вид кодирующего алгоритма для канала с обратной связью. Предположим, что в соответствии с ранее полученными символами, кодирующая стратегия предлагает послать по каналу символ $c_i = 0$, а в канале происходит вставка символа "1" перед c_i, т.е. $\boldsymbol{y}_i = 10$. Символ "1" в начале последовательности $\boldsymbol{y}_i$ можно интерпретировать как вставленный в конец строки $\boldsymbol{y}_{i-1}$. Для произвольного алгоритма кодирования возможна ситуация, при которой алгоритм кодирования предложит передавать символ $c_i = 1$ после наблюдения $\boldsymbol{y}_{i-1}$, что приводит к возможности создания двух ошибок ценой одной вставки. В алгоритме Хорштейна такое невозможно, что позволяет использовать этот алгоритм в модели со вставками и выпадениями.

3.1. Код с обратной связью, исправляющий вставки и выпадения. Предположим, что в канале может произойти не больше доли τ ошибок, и отправитель хочет передать $M = 2^{Rn}$ сообщений, где $R = R_{\mathrm{id}}(\tau) - \varepsilon$ и $\varepsilon > 0$. В зависимости от значений τ, ε и n отправитель и получатель выбирают два трансцендентных числа α и β, удовлетворяющих соотношению $\alpha + \beta = 2$. Для $\tau < \sqrt{5} - 2$ они выбирают α достаточно близким к $2\tau/(1 + \tau)$, а для $\sqrt{5} - 2 \leqslant \tau < 1/2$ параметр α выбирается в окрестности точки $(3 - \sqrt{5})/2$. Насколько близким должно быть α к указанным значениям, мы разъясняем в § 4. Далее отправитель делит отрезок $[0, 1]$ на M подотрезков длины $1/M$ и нумерует их элементами из $[M]$ слева направо. Длины этих M отрезков будут меняться в течение процесса передачи сообщения. Если отправитель планирует послать сообщение $m \in [M]$, тогда отрезок с номером m будем называть *истинным отрезком*. Пусть $T(i)$ обозначает истинный отрезок длины $t(i)$ после i-го шага. Обозначим объединение отрезков, находящихся слева и справа от отрезка $T(i)$ через $L(i)$ и $R(i)$. Теперь мы готовы к описанию процедур кодирования и декодирования предлагаемого алгоритма, который будем обозначать $\mathfrak{A}_{\mathrm{id}}(M, n, \alpha)$.

Замечание 1. Отметим, что так как трансцендентные числа всюду плотны в множестве действительных чисел, то мы можем приблизить ими любое действительное число с произвольной точностью.

Кодирование: В момент времени i отправитель проверяет, лежит ли центр истинного отрезка в полуинтервале $[0, 1/2)$. Если лежит, то по каналу передается символ $c_i = 0$. В противном случае посылается символ $c_i = 1$. Далее отправитель смотрит на принятую из канала строку $\boldsymbol{y}_i$ длины n_i и модифицирует длины всех M отрезков по следующему правилу. Отправитель перебирает все символы строки $\boldsymbol{y}_i = (y_{i,1}, \ldots, y_{i,n_i}) \in \{0,1\}^{n_i}$ слева направо. Если строка $\boldsymbol{y}_i$ пустая, то он переходит к передаче следующего символа. В противном случае, если $y_{i,j} = 0$, то длины всех отрезков, полностью лежащих внутри $[0, 1/2)$, умножаются на число β. Длины отрезков, полностью лежащих внутри $[1/2, 1]$, умножаются на α. Может существовать отрезок, содержащий точку $1/2$ как внутреннюю. Обозначим через x длину такого отрезка. Величина x может быть представлена в виде суммы $x = x_0 + x_1$, где x_0 – длина левой части отрезка, лежащей в $[0, 1/2)$. Тогда длина x этого отрезка заменяется длиной $\beta x_0 + \alpha x_1$. Если же полученный из канала символ $y_{i,j}$ равен 1, то отправитель умножает длины отрезков слева от точки $1/2$ на α, а отрезки с правой стороны увеличивает в β раз. По сравнению со случаем $y_{i,j} = 0$ роли чисел α и β меняются местами. В процессе передачи сообщения длины отрезков изменяются согласно алгоритму, однако порядок отрезков остается неизменным. В итоге отправитель делает n_i таких обновлений длин после передачи i-го символа. Легко заметить, что сумма длин отрезков всегда равна 1. Идея алгоритма состоит в том, что длина истинного отрезка постепенно увеличится, так что в конце процедуры он будет содержать точку $1/2$.

Сложность описанного алгоритма кодирования равна $\Theta(Mn)$. Однако из описания алгоритма ясно, что достаточно следить только за длинами отрезков $L(i)$, $T(i)$ и $R(i)$. Поэтому сложность может быть уменьшена до $\Theta(n)$.

Декодирование: После приема строки $\boldsymbol{y} = (y_1 \parallel \ldots \parallel y_{n'})$ длины $n' \in [n-t, n+t]$ получатель может восстановить точку зрения отправителя, обновляя длины отрезков тем же самым способом. После n' шагов отправитель находит сообщение, соответствующее отрезку, содержащему точку $1/2$. Сложность этого алгоритма декодирования равна $\Theta(Mn)$. Для уменьшения сложности получатель может обратить процедуру декодирования следующим образом. Перебирая символы строки $\boldsymbol{y}$ справа налево, можно отследить прообраз точки $1/2$. Более формально, пусть $P(n') := 1/2$. Для $j \in \{0, 1, \ldots, n'-1\}$ и $y_j = 0$ определим

$$P(j-1) := \begin{cases} \dfrac{P(j)}{\beta}, & \text{если } P(j) \leqslant \dfrac{\beta}{2}, \\ \dfrac{1}{2} + \dfrac{2P(j) - \beta}{2\alpha}, & \text{если } P(j) > \dfrac{\beta}{2}. \end{cases}$$

Для $y_j = 1$ пусть

$$P(j-1) := \begin{cases} \dfrac{P(j)}{\alpha}, & \text{если } P(j) \leqslant \dfrac{\alpha}{2}, \\ \dfrac{1}{2} + \dfrac{2P(j) - \alpha}{2\beta}, & \text{если } P(j) > \dfrac{\alpha}{2}. \end{cases}$$

В конце процесса декодирования получатель выберет сообщение $\widehat{m} := \lceil M \cdot P(0) \rceil$. Очевидно, что сложность такого упрощенного алгоритма декодирования также линейна, т.е. равна $\Theta(n)$.

3.2. Простое, но неправильное объяснение работы алгоритма. Приведем интуитивное объяснение, почему эта стратегия имеет смысл. В данном пункте мы рассматриваем только $\tau < \sqrt{5} - 2$, так как в этом случае

$$R_{\mathrm{id}}(\tau) = (1+\tau)\left(1 - h\left(\frac{\tau}{1+\tau}\right)\right).$$

Пусть $\alpha = 2\tau/(1+\tau)$. Предположим, что в процессе передачи количество раз, когда истинный отрезок содержит точку $1/2$, равно $o(n)$, а число вставок и выпадений равно $\tau_{\text{ins}}n + o(n)$ и $\tau_{\text{del}}n + o(n)$ соответственно, причем $\tau_{\text{ins}} + \tau_{\text{del}} \leqslant \tau$. Тогда после n шагов длина истинного отрезка $T(n)$ может быть ограничена снизу следующим образом:

$$
\begin{aligned}
&t(n) \geqslant M^{-1}\alpha^{\tau_{\text{ins}}n+o(n)}\beta^{(1-\tau_{\text{del}})n+o(n)} = \\
&= 2^{-(R_{\text{id}}(\tau)-\varepsilon)n+\tau_{\text{ins}}n\log(2\tau/(1+\tau))+(1-\tau_{\text{del}})n\log(2/(1+\tau))+o(n)} \geqslant \\
&\geqslant 2^{-(R_{\text{id}}(\tau)-\varepsilon)n+\tau n\log(2\tau/(1+\tau))+n\log(2/(1+\tau))+o(n)} = \\
&= 2^{\varepsilon n+o(n)}.
\end{aligned}
$$

В этой цепочке преобразований мы использовали тот факт, что $\tau_{\text{ins}}\log(2\tau/(1+\tau)) + (1-\tau_{\text{del}})\log(2/(1+\tau))$ при ограничении $\tau_{\text{ins}} + \tau_{\text{del}} \leqslant \tau$ достигает минимума при $\tau_{\text{ins}} = \tau$ и $\tau_{\text{del}} = 0$. Таким образом, в конце процедуры длина истинного отрезка будет очень велика, а сам отрезок будет содержать точку $1/2$. Однако на самом деле наше изначальное предположение неверно, и точка $1/2$ попадает в истинный отрезок гораздо чаще, чем $o(n)$ раз. Поэтому для доказательства корректности работы стратегии необходимы более сложные рассуждения.

3.3. Построение кодов, исправляющих вставки и выпадения, из кодов, исправляющих замещения. Алгоритм $\mathfrak{A}_{\text{id}}(M, n, \alpha)$, описанный в п. 3.1, был изначально предложен в очень похожем виде для канала с замещениями. Подчеркнем, что такой канал гарантирует синхронизацию между отправителем и получателем, т.е. после передачи символа c_i канал выдает ровно один символ y_i. Обозначим алгоритм кодирования для канала с замещениями, использующий коды длины n, как это описано в п. 3.1, через $\mathfrak{A}_s(M, n, \alpha)$. Формальное определение этого алгоритма для канала с замещениями будет дано в п. 4.1. В дальнейшем мы покажем, что используя алгоритм $\mathfrak{A}_{\text{id}}(M, n, \alpha)$, можно достичь скорости (2) при передаче данных по комбинаторному каналу со вставками и выпадениями. Для начала докажем следующую лемму.

Лемма 2. *Если для всех $n' \in [n-t, n+t]$ алгоритм $\mathfrak{A}_s(M, n', \alpha)$ может быть использован для безошибочной передачи произвольного сообщения $m \in [M]$ по комбинаторному каналу с обратной связью и не более чем $t' := \lfloor (n'-n+t)/2 \rfloor$ замещениями, то алгоритм $\mathfrak{A}_{\text{id}}(M, n, \alpha)$ может быть использован для корректной передачи любого сообщения $m \in [M]$ по каналу с обратной связью и не более чем t вставками и выпадениями.*

Доказательство. Пусть $\boldsymbol{y} = (\boldsymbol{y}_1 \,\|\, \ldots \,\|\, \boldsymbol{y}_n) = (y_1, \ldots, y_{n'})$ – возможная выходная строка длины $n' \in [n-t, n+t]$ при применении алгоритма $\mathfrak{A}_{\text{id}}(M, n, \alpha)$ для передачи сообщения $m \in [M]$ по комбинаторному каналу с не более чем t вставками и выпадениями. Мы покажем, что эта строка $\boldsymbol{y}$ также является возможным выходом канала при применении алгоритма $\mathfrak{A}_s(M, n', \alpha)$ для передачи того же сообщения $m \in [M]$ по комбинаторному каналу с не более чем $t' := \lfloor (n'-n+t)/2 \rfloor$ замещениями. Определим $\widehat{\boldsymbol{y}}^{(i-1)} := (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{i-1}) \in (\{0,1\}^*)^{i-1}$ и $\boldsymbol{y}^{(i-1)} := (y_1, \ldots, y_{i-1}) \in \{0,1\}^{i-1}$. Пусть $c_i = c_i(m, \widehat{\boldsymbol{y}}^{(i-1)})$ и $e_i = e_i(m, \boldsymbol{y}^{(i-1)})$ обозначают i-е биты, выданные алгоритмами кодирования кода для каналов с обратной связью и ошибками вида вставок и выпадений и ошибками-замещениями. Введем обозначение $\boldsymbol{e} := (e_1, \ldots, e_{n'})$. Теперь нам достаточно показать, что $d_H(\boldsymbol{e}, \boldsymbol{y}) \leqslant t'$. Пусть длина строки $\boldsymbol{y}_i$ равна n_i. Представим $\boldsymbol{e}$ в виде конкатенации $(\boldsymbol{e}_1 \,\|\, \ldots \,\|\, \boldsymbol{e}_n)$, так чтобы строка $\boldsymbol{e}_i$ имела длину n_i. Очевидно, что для "синхронизированных" моментов i и $N_i := n_1 + \ldots + n_{i-1} + 1$ оба алгоритма отправляют в канал одинаковые символы, т.е.

$$c_i(m, \widehat{\boldsymbol{y}}^{(i-1)}) = e_{N_i}(m, \boldsymbol{y}^{(N_i-1)}).$$

Из определения алгоритма следует, что если $y_j \neq e_j$, то $e_{j+1} = e_j$, т.е. в случае ошибки происходит переотправка символа. Таким образом,

$$d_H(\boldsymbol{e}_i, \boldsymbol{y}_i) \leqslant \begin{cases} n_i - 1, & \text{если } \Delta(c_i, \boldsymbol{y}_i) = n_i - 1, \\ n_i, & \text{если } \Delta(c_i, \boldsymbol{y}_i) = n_i + 1. \end{cases}$$

Отметим, что второй случай может произойти только в случае выпадения. Пусть общие количества вставок и выпадений равны t_{ins} и t_{del}. Напомним, что у нас имеются ограничения $t_{\text{ins}} + t_{\text{del}} \leqslant t$ и $n - t_{\text{del}} + t_{\text{ins}} = n'$. Отсюда следует, что $n' - n + 2t_{\text{del}} \leqslant t$ и $t_{\text{del}} \leqslant \lfloor (n - n' + t)/2 \rfloor$. В итоге получаем

$$d_H(\boldsymbol{e}, \boldsymbol{y}) = \sum_{i=1}^{n} d_H(\boldsymbol{e}_i, \boldsymbol{y}_i) \leqslant \sum_{i=1}^{n} n_i - \sum_{i=1}^{n} \mathbb{1}\{\Delta(c_i, \boldsymbol{y}_i) = n_i - 1\} \leqslant$$
$$\leqslant n' - (n - t_{\text{del}}) \leqslant t',$$

где $\mathbb{1}\{x = a\}$ обозначает индикатор события $x = a$. ▲

Теперь рассмотрим комбинаторный канал с замещениями. Для достижения максимальной асимптотической скорости комбинаторного канала с замещениями при доле ошибок $\tau \leqslant (3 - \sqrt{5})/4$ в качестве значения параметра α из алгоритма $\mathfrak{A}_s(M, n, \alpha)$ выбирается трансцендентное число, близкое к 2τ.

Лемма 3 (следует из [9]). *Пусть $\tau^* \leqslant (3 - \sqrt{5})/4$ является трансцендентным числом. Положим $\alpha^* = 2\tau^*$. Пусть $\mathfrak{A}_s(M, n, \alpha^*)$ используется для передачи данных по комбинаторному каналу с замещениями для различных τ. Тогда достижимая скорость как функция от различных τ выглядит как касательная к функции $R_s(\tau)$ в точке $(\tau^*, R_s(\tau^*))$.*

С помощью леммы 3 можно доказать следующее свойство монотонности.

Предложение 1. *Пусть $M_s(n, \tau, \alpha)$ обозначает максимальное количество сообщений M, которое может быть успешно передано алгоритмом $\mathfrak{A}_s(M, n, \alpha)$ по комбинаторному каналу с длиной блока n и не более чем τn замещениями. Пусть α и τ – трансцендентные числа, такие что $\alpha = 2\tau/(1+\tau)$ и $\alpha \leqslant (3 - \sqrt{5})/2$. Тогда выполняется следующее*:

$$\min_{k \in \{0,1,\ldots,\tau n\}} \log M_s\big(\lfloor n(1+\tau) \rfloor - 2k, \lfloor \tau n \rfloor - k, \alpha\big) =$$
$$= (1 + o(1)) \log M_s\big(\lfloor (1+\tau) n \rfloor, \lfloor \tau n \rfloor, \alpha\big) =$$
$$= n(1+\tau) R_s\Big(\frac{\tau}{1+\tau}\Big) + o(n).$$

Доказательство. Выбор $\alpha = 2\tau/(1+\tau)$ позволяет передавать с помощью алгоритма $\mathfrak{A}_s(M, \lfloor n(1+\tau) \rfloor, \alpha)$ количество сообщений, асимптотически эквивалентное максимальному возможному при условии, что число ошибок ограничено $\lfloor \tau n \rfloor$. Мы покажем, что несмотря на то что выбранное α, вероятно, не является оптимальным с точки зрения достижимой скорости для длины блока $\lfloor n(1+\tau) \rfloor - 2k$ и не более чем $\lfloor \tau n \rfloor - k$ ошибок, величина $\log M_s(\lfloor n(1+\tau) \rfloor - 2k, \lfloor \tau n \rfloor - k, \alpha)$ все равно асимптотически минимизируется при $k = 0$.

Согласно лемме 3, зафиксировав $\alpha = 2\tau/(1+\tau)$ и используя алгоритм $\mathfrak{A}_s(M, n', \alpha)$ для $n' = \lfloor n(1+\tau) \rfloor - 2k$ и не более чем $\lfloor \tau n \rfloor - k$ ошибок, возможно достичь скоростей, лежащих на касательной прямой к функции $R_s(x) = 1 - h(x)$ в точке $(\tau/(1+\tau), R_s(\tau/(1+\tau)))$.

Для доказательства утверждения о минимизации определим функцию

$$f(x) := \frac{\log M_s(n(1+\tau-2x),(\tau-x)n,\alpha)}{n} =$$
$$= (1+\tau-2x)\left(a\frac{\tau-x}{1+\tau-2x}+b\right)(1+o(1)),$$

где действительные числа a, b таковы, что достижимые скорости лежат на касательной в точке $(\tau/(1+\tau), R_s(\tau/(1+\tau)))$. Из этих соображений находим $a = \log\tau$ и $b = 1-\log(1+\tau)$.

Производная $f(x)$ при $n\to\infty$ равна

$$\frac{\partial f}{\partial x} = -a-2b+o(1) = \log\left(\frac{(1+\tau)^2}{\tau}\right)-2+o(1) > 0,$$

где неравенство следует из того, что выражение под логарифмом строго больше 4 при $\tau < 1/2$. Отсюда следует, что функция f асимптотически достигает минимума при $x = 0$. ▲

Мы уже показали, что выходная последовательность алгоритма $\mathfrak{A}_{\mathrm{id}}(M,n,\alpha)$ для комбинаторного канала со вставками и выпадениями также принадлежит множеству возможных выходных последовательностей для комбинаторного канала с замещениями при использовании алгоритма $\mathfrak{A}_s(M,n',\alpha)$ для длины $n'\in[n-t,n+t]$ и не более чем $t' = \lfloor(n'-n+t)/2\rfloor$ ошибок. Таким образом, из предложения 1 следует, что $R_{\mathrm{id}}(\tau)\geqslant(1+\tau)R_s(\tau/(1+\tau))$. Применяя теорему 2, получаем, что скорость $R_{\mathrm{id}}(\tau)$, определенная в (2), действительно достижима, и верхняя и нижняя границы скорости для комбинаторного канала со вставками и выпадениями совпадают.

§ 4. Анализ кода с обратной связью, исправляющего замещения

В этом параграфе мы напомним алгоритм передачи и его анализ, предложенный Зигангировым в [9]. Чтобы сделать этот параграф более самодостаточным, сначала будет описан процесс кодирования. Далее будут введены некоторые полезные понятия, и мы проанализируем алгоритм, не вдаваясь в технические подробности. Наконец, мы приведем доказательства вспомогательных технических утверждений, из которых будет следовать основной результат.

4.1. Код с обратной связью, исправляющий замещения. Предположим, что не более чем τn замещений может произойти при передаче n символов, и отправитель хочет передать одно из M сообщений. Если $0\leqslant\tau<(3-\sqrt{5})/4$, то сначала нужно определить действительные числа α и β, такие что $\alpha+\beta=2$, причем α достаточно близко к 2τ. Если $(3-\sqrt{5})/4\leqslant\tau\leqslant 1/3$, то α и β берутся таким образом, что $\alpha+\beta=2$, причем α достаточно близко к числу $(3-\sqrt{5})/2$, но при этом меньше этого числа. Таким образом, $\alpha<1$ и $\beta>1$. Также очевидно, что для такого выбора будет выполнено неравенство

$$\alpha\beta^2\leqslant 1. \tag{3}$$

Кодирование: Изначально отправитель берет отрезок $[0,1]$ и делит его на M подотрезков одной и той же длины. Занумеруем все эти отрезки слева направо. Таким образом, сообщение j, $j\in[M]$, связано естественным образом с j-м отрезком. Предположим, что отправитель хочет послать сообщение $m\in[M]$. Тогда отрезок с номером m будем называть *истинным отрезком*, и символом $T(i)$ мы будем обозначать истинный отрезок после отправки i символов. Определим объединение отрезков слева и справа от $T(i)$ через $L(i)$ и $R(i)$. Обозначим длины отрезков $L(i)$, $T(i)$ и $R(i)$

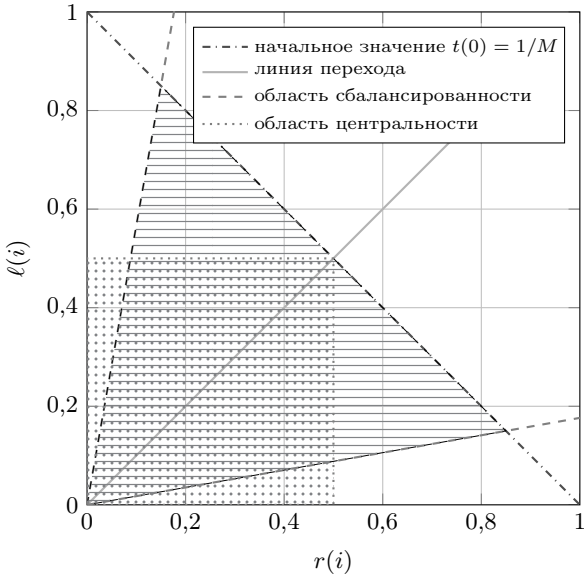

Рис. 3. Иллюстрация понятий перехода, сбалансированного и центрального истинного отрезка и соответствующих областей при $\tau = 0{,}15$, $\alpha = 2\tau$ и $\beta = 2 - \alpha$

через $\ell(i)$, $t(i)$ и $r(i)$. Очевидно, что $t(0) = 1/M$ и $\ell(i) + t(i) + r(i) = 1$. В i-й момент времени отправитель проверяет, находится ли центр отрезка $T(i-1)$ левее точки $1/2$, и отправляет "0" в канал при выполнении этого условия. В противном случае отправитель посылает "1" в канал. Если получен "0", то длины всех отрезков, находящихся левее точки $1/2$, умножаются на β, а длины отрезков правее точки $1/2$ умножаются на α. Более формально,

$$\ell(i) := \beta \min\Big(\frac{1}{2}, \ell(i-1)\Big) + \alpha \max\Big(\ell(i-1) - \frac{1}{2}, 0\Big),$$
$$r(i) := \alpha \min\Big(\frac{1}{2}, r(i-1)\Big) + \beta \max\Big(r(i-1) - \frac{1}{2}, 0\Big),$$
$$t(i) := 1 - \ell(i) - r(i).$$

Если получен символ "1", то длины всех отрезков левее точки $1/2$ умножаются на α, а длины всех отрезков правее точки $1/2$ умножаются на β. Таким образом,

$$\ell(i) := \beta \max\Big(\ell(i-1) - \frac{1}{2}, 0\Big) + \alpha \min\Big(\frac{1}{2}, \ell(i-1)\Big),$$
$$r(i) := \alpha \max\Big(r(i-1) - \frac{1}{2}, 0\Big) + \beta \min\Big(\frac{1}{2}, r(i-1)\Big),$$
$$t(i) := 1 - \ell(i) - r(i).$$

В последующих пунктах будет показано, что для произвольного $\varepsilon > 0$, правильно выбранного $\alpha \approx 2\min(\tau, (3-\sqrt{5})/4)$, достаточно большого n и $M = 2^{(R_s(\tau)-\varepsilon)n}$ истинный отрезок $T(n)$ содержит точку $1/2$.

4.2. Дополнительные обозначения. Определим $x(i) := \min(\ell(i), r(i))$ и $y(i) := \max(\ell(i), r(i))$. Будем говорить, что $T(i)$ является *центральным*, если $y(i) \leqslant 1/2$. Также будем говорить, что выполнен *переход* между моментом $i-1$ и моментом i, если либо (1) $\ell(i-1) \leqslant r(i-1)$ и $\ell(i) > r(i)$, либо (2) $\ell(i-1) > r(i-1)$ и $\ell(i) \leqslant r(i)$. Ис-

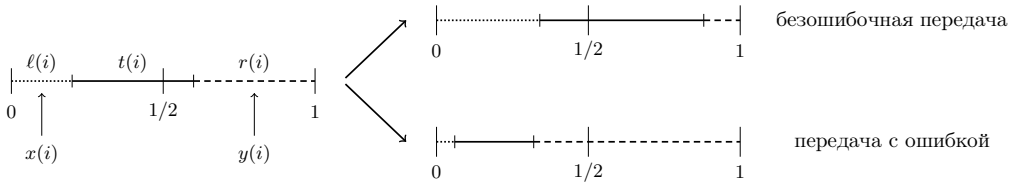

Рис. 4. Пример изменения отрезков $L(i), T(i)$ и $R(i)$ в случае безошибочной передачи и передачи с ошибкой

тинный отрезок $T(i)$ назовем *сбалансированным*, если $y(i)/x(i) \leqslant \beta/\alpha$. Иллюстрация данных понятий приведена на рис. 3.

Пример 1. На рис. 4 можно увидеть отрезки $L(i), R(i)$ и $T(i)$ с $\ell(i) = 0{,}2$, $r(i) = 0{,}4$ и $t(i) = 0{,}4$, а также локальные изменения, которые произойдут в случае ошибочной и безошибочной передачи согласно описанной выше процедуре кодирования при $\tau = 0{,}15$, $\alpha = 2\tau$ и $\beta = 2 - \alpha$. В частности, истинный отрезок $T(i)$ содержит точку $1/2$, и следовательно, является центральным. Более того, выполнено $x(i) = \ell(i)$ и $y(i) = r(i)$, а истинный отрезок $T(i)$ является сбалансированным, поскольку $2 = \dfrac{y(i)}{x(i)} \leqslant \dfrac{\beta}{\alpha} = \dfrac{1{,}7}{0{,}3}$. В этом примере безошибочная передача соответствует отправке и приему "0", что соответствует увеличению всего слева от точки $1/2$ в β раз и уменьшению всего справа в α^{-1} раз. В таком случае происходит переход, так как $\ell(i) \leqslant r(i)$ и $\ell(i+1) > r(i+1)$. Истинный отрезок в момент $i+1$ по-прежнему содержит точку $1/2$, а потому является центральным. Более того, $T(i+1)$ является сбалансированным. Если же при передаче происходит ошибка, то все, что находится слева от $1/2$, увеличивается в β раз, а другая часть уменьшается в α раз. В этом случае не происходит перехода, а истинный отрезок $T(i+1)$ не содержит точку $1/2$, а потому не является центральным. Более того, $T(i+1)$ не является сбалансированным, поскольку $\dfrac{34}{3} = \dfrac{y(i)}{x(i)} > \dfrac{\beta}{\alpha} = \dfrac{1{,}7}{0{,}3}$.

Определим функцию

$$g(i_0, i_1) := e(i_0, i_1) \log \alpha + f(i_0, i_1) \log \beta,$$

где $e(i_0, i_1)$ и $f(i_0, i_1)$ обозначают число ошибочных и безошибочных передач в промежутке времени $(i_0, i_1] = \{i_0 + 1, \ldots, i_1\}$. Отметим, что функция g является аддитивной в том смысле, что выполнено равенство $g(i_0, i_2) = g(i_0, i_1) + g(i_1, i_2)$. Для краткости будем писать $g(n)$, $e(n)$ и $f(n)$ для обозначения $g(0, n)$, $e(0, n)$ и $f(0, n)$. Можно думать о величине $g(i, n)$ как о количестве *энергии*, которая имеется в момент i и расходуется для изменения длины истинного отрезка. Для одной безошибочной передачи нужно потратить количество энергии, равное $\log \beta > 0$, в то время как при ошибочной передаче энергия увеличивается на $-\log \alpha > 0$.

4.3. План доказательства. В следующем утверждении показано, что если количество энергии достаточно велико, то в какой-то момент времени длина истинного отрезка будет отделена от нуля вне зависимости от длины кода n, а также останется некоторое положительное количество энергии, которая будет использоваться в дальнейшем для увеличения длины истинного отрезка.

Лемма 4. *Для любых действительных $\varepsilon_1 > \varepsilon_2 > 0$ существует $\delta > 0$, такое что для почти всех (за исключением конечного числа) $\alpha \in (0, 1)$ выполнено утверждение: для $n \in \mathbb{N}$ условие $g(0, n) > \varepsilon_1 n - \log t(0)$ гарантирует, что существует первый момент времени n_1, при котором $t(n_1) \geqslant \delta$; более того, $g(0, n_1) < \varepsilon_2 n - \log t(0)$ и $g(n_1, n) > (\varepsilon_1 - \varepsilon_2) n$.*

Следующая лемма показывает, что после того как было потрачено достаточное количество энергии, истинный отрезок становится центральным.

Лемма 5. *Пусть α и β удовлетворяют соотношению* (3). *Тогда существует константа $c > 0$, зависящая только от α, β и $t(n_1)$, такая что если $g(n_1, n) > c$, то истинный отрезок $T(n)$ является центральным. Более того, длина истинного отрезка в момент n равна $t(n) = 1 - o(1)$ при $c \to \infty$.*

Наконец, применяя указанные выше леммы, можно получить основной результат.

Теорема 3. *Пусть $\tau \in [0, 1/3)$. Для любого $\varepsilon > 0$ существует $\alpha \in [0, (3-\sqrt{5})/2]$, такое что для достаточно большого n с помощью описанной процедуры кодирования для комбинаторного канала с замещениями и обратной связью можно исправить τn ошибок. При этом скорость передачи при таком кодировании не меньше $R_s(\tau) - \varepsilon$, где*

$$R_s(\tau) = \begin{cases} 1 - h(\tau), & \text{если } 0 \leqslant \tau \leqslant \dfrac{3-\sqrt{5}}{4}, \\ (1-3\tau)\log\left(\dfrac{1+\sqrt{5}}{2}\right), & \text{если } \dfrac{3-\sqrt{5}}{4} < \tau \leqslant 1/3. \end{cases}$$

Доказательство. Выберем M и соответственно $t(0) = 1/M$ так, что выполнены неравенства $2^{(R_s(\tau)-\varepsilon)n} < M < 2^{(R_s(\tau)-\varepsilon/2)n}$ и $-\log t(0) < (R_s(\tau) - \varepsilon/2)n$. По определению имеем $e(0, n) \leqslant \tau n$ и $f(0, n) \geqslant (1 - \tau)n$. Следовательно,

$$g(0, n) = e(0, n)\log\alpha + f(0, n)\log\beta \geqslant (\tau\log\alpha + (1-\tau)\log\beta)n.$$

При условии $\alpha + \beta = 2$ и $\alpha\beta^2 \leqslant 1$ функция $\tau\log\alpha + (1-\tau)\log\beta$ достигает максимального значения $R_s(\tau)$ при $\alpha = 2\min(\tau, (3-\sqrt{5})/4)$ и $\beta = 2 - \alpha$. Для использования леммы 4 выберем α немного меньшим $2\min(\tau, (3-\sqrt{5})/4)$, так что

$$g(0, n) = e(0, n)\log\alpha + f(0, n)\log\beta \geqslant \left(R_s(\tau) - \frac{\varepsilon}{10}\right)n > \frac{2}{5}\varepsilon n - \log t(0).$$

Применяя лемму 4 с $\varepsilon_1 = 2\varepsilon/5$ и $\varepsilon_2 = \varepsilon/5$, получаем, что существует константа $\delta > 0$, для которой для почти всех (за исключением конечного числа) $\alpha \in (0, 1)$ существует первый момент времени n_1, такой что $t(n_1) \geqslant \delta$. Более того,

$$g(n_1, n) = g(0, n) - g(0, n_1) = e(n_1, n)\log\alpha + f(n_1, n)\log\beta > \frac{1}{5}\varepsilon n,$$

и следовательно, для достаточно большого n по лемме 5 можно заключить, что $T(n)$ является центральным. ▲

Наиболее технически сложный результат, используемый при доказательстве теоремы 1, заключен в лемме 5. Для ее доказательства определим несколько вспомогательных функций:

$$u_1(i) := \log(t(i)/x(i)),$$
$$v_1(i) := \log(2t(i)),$$
$$u_2(i) := \begin{cases} -\log(4x(i)y(i)), & \text{если } y(i) \leqslant 1/2, \\ \log((1-y(i))/x(i)), & \text{если } y(i) > 1/2, \end{cases}$$
$$v_2(i) := \begin{cases} -\log(2y(i)), & \text{если } y(i) \leqslant 1/2, \\ \log(2(1-y(i))), & \text{если } y(i) > 1/2. \end{cases}$$

Также определим константы $u_1' := \log(\beta - \alpha)$, $u_1'' := \log(\beta/\alpha - 1)$, $u_2' := \log(\beta/\alpha)$. Очевидно, что $u_1' < u_1''$. Наконец, определим

$$u(i) := \begin{cases} u_1(i), & \text{если } u_1(i) < u_1', \\ u_2(i), & \text{если } u_1(i) \geqslant u_1', \end{cases}$$

$$v(i) := \begin{cases} v_1(i), & \text{если } u_1(i) < u_1'', \\ v_2(i), & \text{если } u_1(i) \geqslant u_1''. \end{cases}$$

Для того чтобы показать корректность леммы 5, мы докажем, что значение $v(n)$ велико, что может быть выполнено лишь тогда, когда $\ell(n)$ и $r(n)$ достаточно малы (см. пример 2).

Предложение 2. *Если $T(i-1)$ является центральным и происходит переход, то $v(i) - v(i-1) \geqslant -\log\beta$. В противном случае выполнено*

$$v(i) - v(i-1) \geqslant \begin{cases} \log\beta, & \textit{если передача безошибочна}, \\ \log\alpha, & \textit{если произошла ошибка}. \end{cases}$$

Изменение $\Delta v(i) := v(i) - v(i-1)$ функции v больше или равно $g(i-1, i)$ за исключением случая, когда $T(i-1)$ является центральным и происходит переход. Если количество подобных центральных переходов достаточно мало, то значение $v(n) - v(n_1)$ достаточно близко к значению $g(n_1, n)$. Поскольку $v(n_1)$ ограничено константой, зависящей от $t(n_1)$, можно показать, что $v(n)$ достаточно велико, и все доказано. Чтобы разобраться со вторым случаем, при котором число центральных переходов велико, мы воспользуемся функцией u и следующим предложением.

Предложение 3. *Если $T(i-1)$ является центральным и происходит переход, то $u(i) - u(i-1) \geqslant \log\beta$. В противном случае $u(i) - u(i-1) \geqslant 0$.*

Таким образом, во втором случае функция u достаточно велика, откуда также следует, что функция u_2 велика. Однако этого недостаточно, чтобы заключить, что $T(n)$ является центральным (см. пример 2). Рассмотрим момент времени, когда произошел последний центральный переход. Можно показать, что в этот момент истинный отрезок является также сбалансированным. Отсюда будет следовать, что значение функции v_2 достаточно близко к значению функции u_2, т.е. тоже достаточно велико. Для того чтобы функция v_2 снова стала мала, должно произойти достаточно много ошибок в силу предложения 4.

Предложение 4. *Если произошел переход и $u_1(i-1) \geqslant u_1''$, то $v_2(i) - v_2(i-1) \geqslant -\log\beta$. Если не произошел переход, то*

$$v_2(i) - v_2(i-1) \geqslant$$

$$\geqslant \begin{cases} \log\beta, & \textit{если передача безошибочна}, \\ \log\alpha, & \textit{если произошла ошибка и } v_2(i-1) < \log\beta, \\ -\log\beta \ (\geqslant \log\alpha), & \textit{если произошла ошибка и } v_2(i-1) \geqslant \log\beta. \end{cases}$$

Большое количество ошибок означает, что осталось большое количество энергии. Можно снова воспользоваться предложением 2, поскольку больше не осталось центральных переходов, и следовательно, можно заключить, что функция v примет большое значение после последней передачи.

Пример 2. Рисунки 5 и 6 демонстрируют различные множества уровней функций $v(i)$ и $u(i)$ как функций, зависящих от $\ell(i)$ и $r(i)$. Множество уровня задается как множество пар $(\ell(i), r(i))$, для которых верно $v(i) = \text{const}$ ($u(i) = \text{const}$). При больших значениях функции $v(i)$ соответствующее множество уровня находится ближе к началу координат, т.е. значения $\ell(i)$ и $r(i)$ довольно малы, а значение $t(i)$ велико.

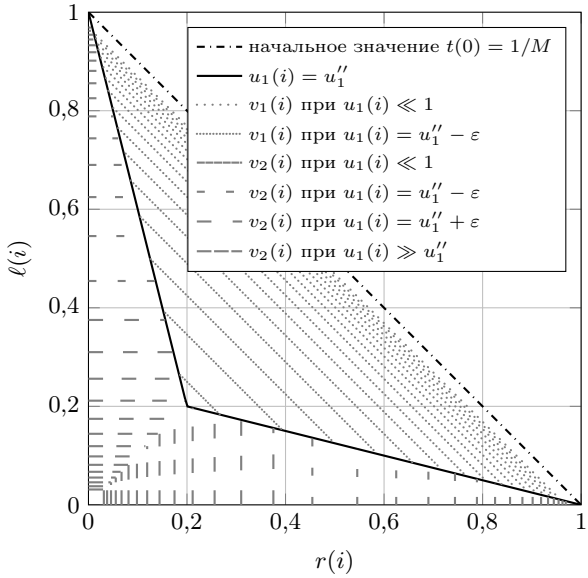

Рис. 5. Множество уровня функции $v(i)$ при $\tau = 0{,}15$, $\alpha = 2\tau$ и $\beta = 2 - \alpha$

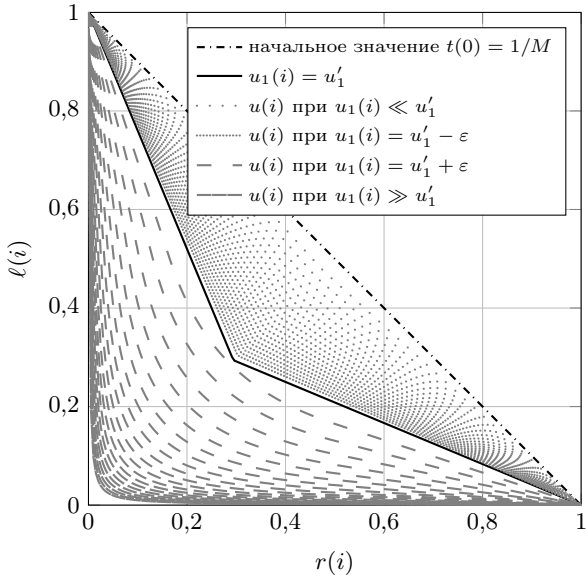

Рис. 6. Множество уровня функции $u(i)$ при $\tau = 0{,}15$, $\alpha = 2\tau$ и $\beta = 2 - \alpha$

В то же время при больших значениях функции $u(i)$ можно лишь утверждать, что множество уровня расположено близко к осям координат, т.е. значение $\ell(i)$ или $r(i)$ мало. Также отметим, что в случае, если $T(i)$ является центральным, то должно быть выполнено неравенство $\ell(i), r(i) < 1/2$. Исходя из приведенных рассуждений, достаточно показать, что значение $v(n)$ велико, чтобы заключить, что истинный отрезок $T(n)$ является центральным.

В вышеприведенных рассуждениях было опущено много технических деталей. Для того чтобы формально доказать лемму 5, нам понадобится несколько вспомогательных предложений.

Предложение 5. *Выполнены следующие (очевидные) свойства*:

1. *Если в какой-то момент произошел переход, то прием был безошибочным*;
2. *Если прием безошибочный, то длина истинного отрезка увеличилась, т.е.* $t(i) > t(i-1)$. *В противном случае длина уменьшилась*;
3. *Если* $T(i-1)$ *является центральным,* $T(i)$ *не является центральным и не произошел переход, то при передаче произошла ошибка*;
4. *Выполнены неравенства* $\alpha t(i-1) \leqslant t(i) \leqslant \beta t(i-1)$;
5. *Для всяких* $x(i)$, $y(i)$ *и* $t(i)$ *верны неравенства* $u_2(i) \geqslant u_1(i)$ *и* $u_2(i) \geqslant u(i)$;
6. *Для всяких* $x(i)$, $y(i)$ *и* $t(i)$ *верны неравенства* $v_2(i) \geqslant v_1(i)$ *и* $v_2(i) \geqslant v(i)$.

Предложение 6. *Выполнены следующие свойства*:

1. *Если* $T(i)$ *является центральным, то* $u_2(i) \geqslant 2v_2(i)$;
2. *Если* $T(i)$ *является центральным и сбалансированным, то* $u_2(i) < 2v_2(i) + \log(\beta/\alpha)$;
3. *Если происходит переход между моментами* $i-1$ *и* i, *то* $T(i-1)$ *и* $T(i)$ *являются сбалансированными*;
4. *Если* $u_1(i-1) < u_1''$ (*или* $u_1(i-1) < u_1'$), $T(i-1)$ *является центральным и передача безошибочна, то происходит переход между моментами* $i-1$ *и* i;
5. *Если* $u_1(i-1) \geqslant u_1'$ (*или* $u_1(i-1) \geqslant u_1''$) *и происходит переход между моментами* $i-1$ *и* i, *то* $T(i)$ *является центральным*;
6. *Если* $u_1(i-1) \geqslant u_1''$ *и происходит переходит между моментами* $i-1$ *и* i, *то* $T(i-1)$ *и* $T(i)$ *являются центральными*;
7. *Если* $u_2(i) \geqslant u_2'$ *и происходит переход между моментами* $i-1$ *и* i *или между моментами* i *и* $i+1$, *то* $T(i)$ *является центральным.*

Предложение 7. *Если* $u_1(i-1) < u_1'$, *то* $u_1(i) - u_1(i-1) \geqslant 0$. *Если вдобавок* $T(i-1)$ *является центральным и происходит переход между моментами* $i-1$ *и* i, *то* $u_1(i) - u_1(i-1) \geqslant \log\beta$. *С другой стороны, если* $u_1(i-1) \geqslant u_1'$, *то* $u_1(i) \geqslant u_1'$, *а если* $u_1(i-1) \geqslant u_1''$, *то* $u_1(i) \geqslant u_1''$.

Предложение 8. *Если* $u_1(i-1) \geqslant u_1'$, *то* $u_2(i) - u_2(i-1) \geqslant 0$. *Если оба отрезка* $T(i-1)$ *и* $T(i)$ *являются центральными, то* $u_2(i) - u_2(i-1) = -\log(\alpha\beta)$.

Предложение 9. *Предположим, что* $u_1(i-1) < u_1''$. *Если происходит переход, то* $v_1(i) - v_1(i-1) > 0$, *в противном случае*

$$v_1(i) - v_1(i-1) \geqslant \begin{cases} \log\beta, & \text{если передача безошибочна,} \\ \log\alpha, & \text{если произошла ошибка.} \end{cases}$$

Предложение 10. *Пусть* $c = -5\log(\alpha\beta)$. *Если оба отрезка* $T(i_0)$ *и* $T(i_1)$ *являются центральными и сбалансированными, а также верно* $u_2(i_0) \geqslant c$, *то*

$$g(i_0, i_1) \leqslant u_2(i_1) - u_2(i_0). \tag{4}$$

Доказательства лемм и предложений приведены в пп. 4.4, 4.5. Наконец, в блок-схеме, приведенной на рис. 7, показана схема доказательства основного результата.

Перед тем как будут даны доказательства, приведем пример 3, в котором рассмотрена передача сообщения с помощью описанной процедуры кодирования. В данном примере отслеживается положение истинного отрезка $T(i)$.

Пример 3. На рис. 8 продемонстрирован пример передачи случайного сообщения m из $M = 2^{14}$ возможных на длине $n' = 27$. Использованы параметры $\tau = 0{,}15$,

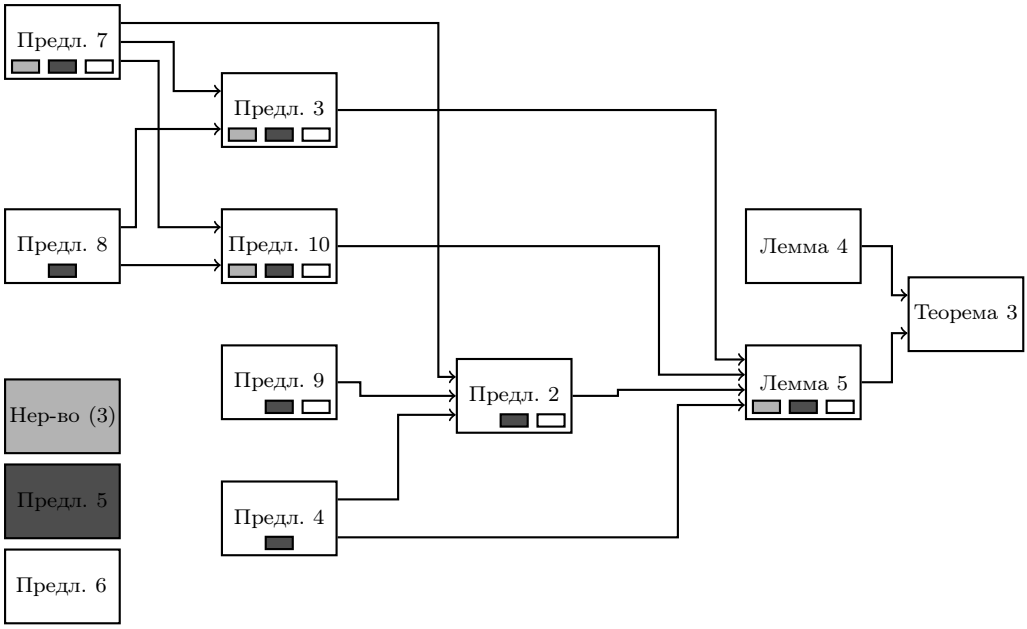

Рис. 7. Иллюстрация схемы доказательства теоремы 3. Для неравенства (3) и предложений 5, 6 не показаны стрелочки для простоты восприятия блок-схемы; маленькие прямоугольники указывают, как используются эти результаты в ходе доказательства

$\alpha = 2\tau$ и $\beta = 2 - \alpha$. Напомним, что $t(i) = 1 - \ell(i) - r(i)$. Три ошибки произошли в моменты $i \in \{16, 21, 22\}$. Поскольку перед началом передачи все отрезки одной длины, положение истинного отрезка $T(0)$, описываемое парой $(\ell(0), r(0))$, близко к прямой $\ell(i) + r(i) = 1$. При увеличении числа переданных символов видно, что положение истинного отрезка становится все ближе к началу координат. Другими словами, длина истинного отрезка увеличивается. Видно, что $T(i)$ становится центральным в момент времени $i = 15$. Поскольку в момент времени $i = 16$ произошла ошибка, истинный отрезок перестает быть центральным. Более того, в этот же момент траектория пересекает множество уровня u_1' для функции u, и в последующих шагах уже не пересекает этот уровень (см. предложение 7). Аналогичное поведение истинного отрезка можно видеть при пересечении множества уровня u_1'' несмотря на то, что ошибки произойдут в моменты времени $i = 21, 22$ (см. предложение 7). Оставшиеся передачи являются безошибочными, и потому можно видеть, что длина $t(i)$ увеличивается до самого последнего момента n'.

4.4. Доказательства лемм.

Доказательство леммы 4. Выберем $k \in \mathbb{N}$ таким, что $k > \dfrac{\log \beta}{\varepsilon_2}$, где $\varepsilon_1 > \varepsilon_2 > 0$. Зафиксируем некоторое значение δ, которое меньше $\dfrac{1}{\beta^2}$ и не превосходит наименьшей по модулю разницы между точкой $1/2$ и ее возможным образом после передачи $1, 2, \ldots, k-1$ символов. Например, после передачи одного символа точка $1/2$ может перейти в одну из точек $\left\{\dfrac{\alpha}{2}, \dfrac{\beta}{2}\right\}$, а после передачи двух – в одну из точек $\left\{\dfrac{\alpha^2}{2}, \dfrac{\alpha\beta}{2}, 1 - \alpha\Big(1 - \dfrac{\beta}{2}\Big), 1 - \beta\Big(1 - \dfrac{\beta}{2}\Big)\right\}$. Легко показать, что $\delta > 0$ для всех (за

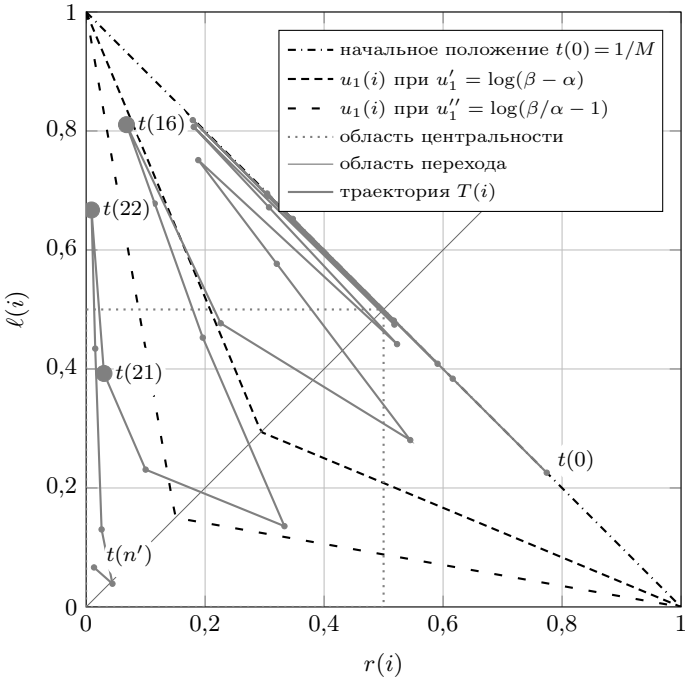

Рис. 8. Иллюстрация траектории значения функции $t(i) = 1 - \ell(i) - r(i)$. Положив $M = 2^{14}$, мы передали случайное сообщение, используя кодирование длины $n' = 27$. Ошибки произошли в моменты времени 16, 21 и 22. Используемые параметры: $\tau = 0{,}15$, $\alpha = 2\tau$ и $\beta = 2 - \alpha$

исключением конечного числа) значений $\alpha \in (0, 1)$. Отметим, что если α является трансцендентным числом, то $\delta > 0$ для любого k.

Предположим, что $t(i) < \delta$ для всех $i \in \{0, 1, \ldots, n\}$. По определению числа δ имеем, что если $T(i)$ является центральным (точка $1/2$ принадлежит отрезку $T(i)$), то $T(i+1), \ldots, T(i+k-1)$ не являются центральными. Обозначим через n' число моментов времени, когда $T(i)$ является центральным. Очевидно, что

$$n' \leqslant \frac{n}{k} + 1 < \frac{\varepsilon_1 n}{\log \beta} + 1.$$

Отсюда можно заключить, что

$$t(n) \geqslant t(0)\alpha^{e(0,n)}\beta^{f(0,n)-n'} \geqslant t(0)\alpha^{e(0,n)}\beta^{f(0,n)-\frac{\varepsilon_1 n}{\log \beta}-1} \geqslant \frac{1}{\beta} > \delta,$$

где мы воспользовались тем, что $g(0, n) = e(0, n)\log\alpha + f(0, n)\log\beta > \varepsilon_1 n - \log t(0)$. Таким образом, пришли к противоречию.

Пусть n_1 обозначает первый момент, при котором $t(n_1) \geqslant \delta$. Используя аналогичные рассуждения, получаем, что

$$\beta\delta > \beta t(n_1 - 1) \geqslant t(n_1) \geqslant t(0)\alpha^{e(0,n_1)}\beta^{f(0,n_1)-\frac{\varepsilon_2 n_1}{\log \beta}-1}.$$

Тогда из вышесказанного следует, что

$$g(0, n_1) = e(0, n_1)\log\alpha + f(0, n_1)\log\beta < \varepsilon_2 n_1 - \log t(0) + \log(\beta^2\delta) < \varepsilon_2 n - \log t(0).$$

Следовательно,

$$g(n_1, n) = g(0, n) - g(0, n_1) > (\varepsilon_1 - \varepsilon_2)n > 0. \quad \blacktriangle$$

Доказательство леммы 5. Определим множество $I := \{i \in (n_1, n] : T(i-1)$ является центральным и происходит переход между моментами $i-1$ и $i\}$. Пусть $m := |I|$, и пусть выбраны числа c, m', v_2', удовлетворяющие соотношению $c \gg m' \gg \gg v_2' \gg 1$. Например, можно выбрать эти числа в виде $c = x^3$, $m' = x^2$, $v_2' = x$, где x достаточно велико по сравнению с величинами α, β, $t(n_1)$. Итак, из условия леммы имеем, что $g(n_1, n) > c$.

Случай $m \leqslant m'$. Из п. 6 предложения 5 и определения функции v можно получить, что $v(n_1) \geqslant v_1(n_1) = \log(2t(n_1))$. Отсюда в силу предложения 2 имеем

$$v(n) \geqslant v(n_1) + e(n_1, n)\log\alpha + (f(n_1, n) - m)\log\beta - m\log\beta \geqslant$$
$$\geqslant \log(2t(n_1)) + g(n_1, n) - 2m'\log\beta > \log(2t(n_1)) + c - 2m'\log\beta \gg 1.$$

Здесь мы воспользовались выбором чисел c и m', а также тем фактом, что $g(n_1, n) = = e(n_1, n)\log\alpha + f(n_1, n)\log\beta$. Из определения функции v и из неравенства $v(n) \gg 1$ получаем, что $T(n)$ является центральным (см. рис. 5).

Случай $m > m'$. Пусть n_2 является m'-м наименьшим элементом в множестве I. Из п. 5 предложения 5 и определения функции u получаем $u_2(n_2) \geqslant u(n_2)$, а также $u(n_1) \geqslant u_1(n_1) = \log(t(n_1)/x(n_1))) \geqslant \log(2t(n_1))$, так как $x(n_1) \leqslant 1/2$. Отсюда в силу предложения 3 имеем

$$u_2(n_2) \geqslant u(n_2) \geqslant u(n_1) + m'\log\beta \geqslant \log(2t(n_1)) + m'\log\beta = \Omega(m').$$

Последнее равенство верно из-за выбора величины m'. Отсюда следует, что в силу п. 7 предложения 6 отрезок $T(n_2)$ является центральным, а в силу п. 3 предложения 6 отрезок $T(n_2)$ является сбалансированным. Из предложения 2, п. 6 предложения 5 и п. 1 предложения 6 имеем

$$g(n_1, n_2) \leqslant v(n_2) - v(n_1) + 2m'\log\beta \leqslant v_2(n_2) - v_1(n_1) + 2m'\log\beta \leqslant$$
$$\leqslant \frac{1}{2}u_2(n_2) - \log(2t(n_1)) + 2m'\log\beta \leqslant \frac{1}{2}u_2(n_2) + O(m'). \tag{5}$$

Пусть n_3 является самым последним элементом в множестве I. Мы знаем, что $T(n_2)$ является центральным и сбалансированным, а также $u_2(n_2) = \Omega(m')$. Аналогичный вывод верен и для отрезка $T(n_3)$, т.е. $T(n_3)$ является центральным и сбалансированным, а $u_2(n_3) = \Omega(m')$. По предложению 10 получаем

$$g(n_2, n_3) \leqslant u_2(n_3) - u_2(n_2). \tag{6}$$

В силу п. 2 предложения 6 имеем

$$v_2(n_3) \geqslant \frac{1}{2}u_2(n_3) - \frac{1}{2}\log(\beta/\alpha) = \Omega(m') \gg v_2'.$$

Если $v_2(n) \geqslant v_2'$, то все доказано. В противном случае пусть $n_4 > n_3$ обозначает первый момент, при котором $v_2(n_4) < v_2'$. Поскольку $v_2(i) > 0$ для всех $i \in [n_3, n_4)$, из определения функции v_2 следует, что отрезок $T(i)$ является центральным для всех $i \in [n_3, n_4)$. По определению множества I нет ни одного перехода между моментами n_3 и n_4. В силу предложения 4 и п. 2 предложения 6, а также неравенства $\alpha\beta^2 < 1$ легко получить, что

$$g(n_3, n_4) = e(n_3, n_4)\log\alpha + f(n_3, n_4)\log\beta \leqslant$$
$$\leqslant 2(-e(n_3, n_4) + f(n_3, n_4))\log\beta \leqslant 2v_2(n_4) - 2v_2(n_3) < -u_2(n_3) + O(v_2'). \tag{7}$$

По определению множества I нет ни одного момента $i \in (n_4, n]$, при котором $T(i-1)$ является центральным и происходит переход между моментами $i-1$ и i. Из предложения 2 можно вывести, что

$$g(n_4, n) \leqslant v(n) - v(n_4). \tag{8}$$

Поскольку не происходит переход между моментами $n_4 - 1$ и n_4, из предложения 4 следует, что $v_2(n_4) \geqslant v_2(n_4 - 1) - \log\beta \geqslant v_2' - \log\beta \gg 1$. По определению значения $v_2(n_4)$ имеем, что $y(n_4) \ll 1$, а также $v_1(n_4) > 0$. Отсюда получаем $v(n_4) \geqslant 0$. Суммируя (5)–(8) и используя тот факт, что $v(n_4) \geqslant 0$, получаем

$$v(n) \geqslant g(n_1, n) - O(m') - O(v_2') \gg 1.$$

Это означает, что отрезок $T(n)$ является центральным. ▲

4.5. Доказательство предложений.

Доказательство предложения 5. 1. Если произошел переход, то меньший отрезок из множества $\{L(i), R(i)\}$ увеличился. Такое может произойти только в случае безошибочной передачи символа.

2. Мы приводим доказательство только для случая безошибочного приема, поскольку случай ошибочного приема рассматривается аналогично.

В случае, если отрезок $T(i-1)$ не является центральным, утверждение выполнено, так как $t(i) = t(i-1)\beta$. В случае, если $T(i-1)$ является центральным отрезком, выполняется

$$t(i) = 1 - \beta x(i-1) - \alpha y(i-1),$$

откуда вытекает следующая цепочка равенств:

$$t(i) - t(i-1) = (1-\beta)x(i-1) + (1-\alpha)y(i-1) = \frac{\beta - \alpha}{2}(y(i-1) - x(i-1)) > 0,$$

где мы воспользовались тем фактом, что $\alpha + \beta = 2$.

3. Предположим, что передача произошла без ошибки и перехода не было. Тогда, так как $T(i-1)$ является центральным отрезком, то

$$\begin{aligned} &x(i-1)\beta = x(i), \\ &y(i-1)\alpha = y(i). \end{aligned} \tag{9}$$

Для того чтобы $T(i)$ не был центральным, необходимо выполнение неравенства $y(i) > 1/2$, но это приводит к противоречию с формулой (9), так как $\alpha < 1$ и $y(i-1) < 1/2$.

4. При безошибочном и ошибочном приеме символа происходит отображение отрезка $[0, 1]$ в отрезок $[0, 1]$, причем длина всякого подотрезка умножается на некоторое действительное число, находящееся в интервале $[\alpha, \beta]$.

5. Вспомним определение функции $u_2(i)$:

$$u_2(i) := \begin{cases} -\log(4x(i)y(i)), & \text{если } y(i) \leqslant 1/2, \\ \log((1-y(i))/x(i)), & \text{если } y(i) > 1/2. \end{cases}$$

Утверждается, что

$$-\log(4x(i)y(i)) \geqslant \log((1-y(i))/x(i)).$$

Действительно, это неравенство эквивалентно следующим двум:

$$\frac{1}{4x(i)y(i)} \geqslant \frac{1-y(i)}{x(i)},$$
$$1 \geqslant 4y(i)(1-y(i)).$$

Последнее неравенство верно, так как его правая часть максимизируется в точке $y(i) = 1/2$, где она принимает значение 1. Неравенство $u_2(i) \geqslant u_1(i) = \log(t(i)/x(i))$ выполняется, так как

$$\frac{1-y(i)}{x(i)} \geqslant \frac{t(i)}{x(i)} = 2^{u_1(i)}.$$

6. Напомним определение функции $v_2(i)$:

$$v_2(i) := \begin{cases} -\log(2y(i)), & \text{если } y(i) \leqslant 1/2, \\ \log(2(1-y(i))), & \text{если } y(i) > 1/2. \end{cases}$$

По аналогии с доказательством п. 5 предложения 5 мы покажем, что

$$-\log(2y(i)) \geqslant \log(2(1-y(i))). \tag{10}$$

Это неравенство эквивалентно следующим двум:

$$\frac{1}{2y(i)} \geqslant 2(1-y(i)),$$
$$1 \geqslant 4y(i)(1-y(i)).$$

Последнее неравенство верно, так как правая часть принимает максимальное значение 1 в точке $y(i) = 1/2$. Неравенство $v_2(i) \geqslant v_1(i) = \log(2t(i))$ выполняется, так как

$$\log(2(1-y(i))) \geqslant \log(2(1-x(i)-y(i))) = v_1(i). \quad \blacktriangle$$

Доказательство предложения 6. 1. Так как $T(i)$ – центральный, то выполняется $y(i) \leqslant 1/2$. Поэтому верно

$$u_2(i) = -\log(4x(i)y(i)) \geqslant -\log(4y^2(i)) = 2v_2(i).$$

2. Так как отрезок $T(i)$ – центральный и сбалансированный, то верны неравенства $y(i) \leqslant 1/2$ и $y(i)/x(i) \leqslant \beta/\alpha$. Следовательно,

$$u_2(i) = -\log(4x(i)y(i)) = -\log(4y^2(i)x(i)/y(i)) =$$
$$= -\log(4y^2(i)) + \log(y(i)/x(i)) \leqslant 2v_2(i) + \log(\beta/\alpha).$$

3. Без ограничения общности предположим, что $\ell(i-1) \leqslant 1/2 \leqslant r(i-1)$ и $\ell(i) > r(i)$. Из п. 1 предложения 5 следуют неравенства $\ell(i) = \beta\ell(i-1)$ и $r(i) \geqslant \geqslant \alpha r(i-1)$. Тогда выполнено

$$\frac{y(i)}{x(i)} = \frac{\ell(i)}{r(i)} \leqslant \frac{\beta\ell(i-1)}{\alpha r(i-1)} \leqslant \frac{\beta r(i-1)}{\alpha r(i-1)} = \frac{\beta}{\alpha}.$$

Полученное неравенство означает, что $T(i)$ сбалансирован. Аналогичным образом покажем, что отрезок $T(i-1)$ сбалансирован:

$$\frac{y(i-1)}{x(i-1)} = \frac{r(i-1)}{\ell(i-1)} \leqslant \frac{r(i)/\alpha}{\ell(i)/\beta} < \frac{\beta\ell(i)}{\alpha\ell(i)} = \frac{\beta}{\alpha}.$$

4. Для начала отметим, что $u_1' < u_1''$. Без ограничения общности можно считать, что $\ell(i-1) < r(i-1) \leqslant 1/2$. Условие $u_1(i-1) \leqslant u_1''$ эквивалентно следующему:

$$\frac{t(i-1)}{x(i-1)} = \frac{1-\ell(i-1)-r(i-1)}{\ell(i-1)} = \frac{1-r(i-1)}{\ell(i-1)} - 1 \leqslant \frac{\beta}{\alpha} - 1.$$

Полученное неравенство можно переписать в виде $\beta\ell(i-1)+\alpha r(i-1) \geqslant \alpha$ и $\beta\ell(i-1) \geqslant \alpha - \alpha r(i-1)$. Так как передача произошла без ошибки, то $\ell(i) = \beta\ell(i-1)$. Следовательно, $\ell(i) \geqslant \alpha - \alpha r(i-1)$, а так как $r(i-1) \leqslant 1/2$, то $\ell(i) > \alpha/2 > \alpha r(i-1) = r(i)$. Это доказывает, что между моментами $i-1$ и i произошел переход.

5. Без ограничения общности предположим, что $\ell(i-1) \leqslant r(i-1)$. Из условия $u_1(i-1) = \log(t(i-1)/x(i-1)) \geqslant u_1'$ выводим

$$\frac{1-2\ell(i-1)}{\ell(i-1)} \geqslant \frac{1-\ell(i-1)-r(i-1)}{\ell(i-1)} = \frac{t(i-1)}{x(i-1)} \geqslant 2^{u_1'} = \beta - \alpha = 2\beta - 2$$

и $\ell(i-1) \leqslant 1/(2\beta)$. Так как произошел переход, то $\beta\ell(i-1) = \ell(i) \geqslant r(i)$, и следовательно, $y(i) = \ell(i) \leqslant 1/2$.

6. Без ограничения общности предположим, что $\ell(i-1) < r(i-1)$ и $\ell(i) \geqslant r(i)$. Для начала отметим, что переход может произойти только в случае правильно принятого символа. Из условия $u_1(i-1) \geqslant u_1''$ получаем, что

$$\frac{t(i-1)}{x(i-1)} = \frac{1-\ell(i-1)-r(i-1)}{\ell(i-1)} = \frac{1-r(i-1)}{\ell(i-1)} - 1 \geqslant \frac{\beta}{\alpha} - 1.$$

Перепишем это неравенство в следующем виде: $\beta\ell(i-1) + \alpha r(i-1) \leqslant \alpha$. Так как передача произошла без ошибки, то $\ell(i) = \beta\ell(i-1)$, а значит, $\ell(i) + \alpha r(i-1) \leqslant \alpha$ или $r(i-1) \leqslant 1 - \ell(i)/\alpha$. Так как $\ell(i) \geqslant r(i)$, то $r(i-1) \leqslant 1 - r(i)/\alpha$. Из условия $r(i) \geqslant r(i-1)\alpha$ получаем неравенство $r(i-1) \leqslant 1 - r(i-1)$, означающее, что отрезок $T(i-1)$ является центральным. Для доказательства того, что отрезок $T(i)$ центральный, заметим, что $u_1(i-1) \geqslant u_1'' \geqslant u_1'$, и поэтому можно воспользоваться п. 5 предложения 6.

7. Предположим, что произошел переход между моментами $i-1$ и i или между моментами i и $i+1$. Также без ограничения общности будем считать, что $\ell(i) \geqslant r(i)$ и $\ell(i-1) < r(i-1)$ или $\ell(i+1) < r(i+1)$. Доказывая от противного, предположим, что отрезок $T(i)$ не централен, а значит, $y(i) = \ell(i) > 1/2$. Условие $u_2(i) \geqslant u_2'$ эквивалентно следующему:

$$\frac{1-y(i)}{x(i)} = \frac{1-\ell(i)}{r(i)} \geqslant \frac{\beta}{\alpha}.$$

Отсюда следует неравенство $\alpha\ell(i) + \beta r(i) \leqslant \alpha$. Так как $\ell(i) > 1/2$, то получаем, что выполняется неравенство $r(i) \geqslant \alpha r(i-1) > \alpha\ell(i-1) = \alpha\ell(i)/\beta \geqslant \alpha/(2\beta)$ или неравенство $\beta r(i) = r(i+1) > \ell(i+1) \geqslant \ell(i)\alpha \geqslant \alpha/2$. Таким образом, $\alpha\ell(i) + \beta r(i) > \alpha/2 + \alpha/2 = \alpha$. Полученное противоречие показывает, что наше предположение было неверно, а значит, отрезок $T(i)$ является центральным. ▲

Доказательство предложения 7. Сначала посмотрим на первую часть предложения, в которой выполняется условие $u_1(i-1) < u_1'$. Придется рассмотреть несколько разных случаев. Предположим, что при передаче произошла ошибка. Тогда $t(i) \geqslant \alpha t(i-1)$ (п. 4 предложения 5) и $x(i) = \alpha x(i-1)$, а значит, $u_1(i) = \log(t(i)/x(i)) \geqslant \log(t(i-1)/x(i-1)) = u_1(i-1)$. Теперь рассмотрим случай безошибочной передачи. Если перехода не было, то из п. 4 предложения 6 следует, что отрезок $T(i-1)$ должен быть не центральным, поэтому $t(i) = \beta t(i-1)$ и $x(i) = \beta x(i-1)$, что влечет $u_1(i) = u_1(i-1)$.

Теперь предположим, что ошибки не было и произошел переход. Сначала рассмотрим случай, в котором отрезок $T(i-1)$ не является центральным. Так как был переход, то $x(i) \leqslant \beta x(i-1)$ и

$$2^{u_1(i)} = \frac{t(i)}{x(i)} \geqslant \frac{\beta t(i-1)}{\beta x(i-1)} = \frac{t(i-1)}{x(i-1)} = 2^{u_1(i-1)}.$$

Остается разобраться со случаем центрального отрезка $T(i-1)$. Нужно доказать следующее неравенство:

$$u_1(i) - u_1(i-1) =$$
$$= \log\left(\frac{1 - x(i-1)\beta - y(i-1)\alpha}{y(i-1)\alpha}\right) - \log\left(\frac{1 - x(i-1) - y(i-1)}{x(i-1)}\right) \geqslant \log\beta.$$

Это неравенство эквивалентно следующим двум:

$$(1 - x(i-1)\beta - y(i-1)\alpha)x(i-1) \geqslant (1 - x(i-1) - y(i-1))y(i-1)\alpha\beta,$$
$$x(i-1)\frac{\beta - \alpha}{2}(y(i-1) - x(i-1)) \geqslant (1 - x(i-1) - y(i-1))(y(i-1)\alpha\beta - x(i-1)).$$

Так как левая часть этого выражения всегда положительна, то достаточно рассмотреть только ситуацию, когда и правая часть положительна. Так как $u_1(i-1) < u_1'$, то для завершения доказательства достаточно показать, что

$$y(i-1) - x(i-1) > 2(y(i-1)\alpha\beta - x(i-1)),$$
$$x(i-1) > y(i-1)(2\alpha\beta - 1).$$

Так как произошел переход, то согласно п. 3 предложения 6 имеем

$$x(i-1) > y(i-1)\frac{\alpha}{\beta}.$$

Заметим, что $2\alpha\beta - 1 < \frac{\alpha}{\beta}$. Действительно, это неравенство эквивалентно следующим:

$$2\alpha\beta - 1 < \frac{\alpha}{\beta},$$
$$2\alpha\beta^2 - \beta < \alpha = 2 - \beta,$$
$$\alpha\beta^2 < 1.$$

Последнее неравенство следует из условия (3). Доказательство первой части предложения завершено.

Теперь предположим, что $u_1(i-1) \geqslant u_1'$, и покажем, что в этом случае $u_1(i) \geqslant u_1'$. Сначала рассмотрим случай передачи с ошибкой. Тогда верно неравенство

$$\frac{t(i)}{x(i)} \geqslant \frac{\alpha t(i-1)}{\alpha x(i-1)} = \frac{t(i-1)}{x(i-1)}.$$

Таким образом, теперь мы можем считать, что передача была безошибочной. Сначала рассмотрим случай нецентрального отрезка $T(i-1)$. Верно следующее:

$$\frac{t(i)}{x(i)} \geqslant \frac{t(i-1)\beta}{x(i-1)\beta} = \frac{t(i-1)}{x(i-1)},$$

где неравенство следует из условия $\beta x(i-1) \geqslant x(i)$. При этом равенство достигается в случае отсутствия перехода, а если же переход произошел, то неравенство строгое. Таким образом, случай нецентрального отрезка $T(i-1)$ полностью разобран.

Теперь приступим к анализу случая центрального отрезка $T(i-1)$. Предположим, что перехода не было. Тогда верно следующее:

$$\frac{t(i)}{x(i)} \geqslant \frac{t(i-1)}{\beta x(i-1)} \geqslant \frac{\beta-\alpha}{\alpha\beta} > \beta-\alpha.$$

Действительно, первое неравенство верно, так как безошибочная передача не может уменьшить длину истинного отрезка. Второе выполнено, так как в противном случае из п. 4 предложения 6 следовало бы наличие перехода. Последнее неравенство следует из того, что $\alpha\beta < 1$.

Осталось рассмотреть случай, когда произошел переход. Заметим, что так как произошел переход, то из п. 3 предложения 6 следует сбалансированность отрезка $T(i-1)$. Следовательно, $y(i-1)/x(i-1) < \beta/\alpha$. Так как произошел переход, то верна цепочка равенств

$$\frac{t(i)}{x(i)} = \frac{1-x(i-1)\beta-y(i-1)\alpha}{y(i-1)\alpha} = \frac{1-x(i-1)\beta}{y(i-1)\alpha} - 1. \tag{11}$$

Из условия $u_1(i-1) \geqslant u_1'$ получаем

$$\begin{aligned}
&\frac{1-x(i-1)-y(i-1)}{x(i-1)} \geqslant \beta-\alpha,\\
&1-x(i-1)-y(i-1) \geqslant (\beta-\alpha)x(i-1),\\
&1-x(i-1)-\frac{\beta-\alpha}{2}x(i-1)-y(i-1) \geqslant \frac{\beta-\alpha}{2}x(i-1),\\
&1-\beta x(i-1)-y(i-1) \geqslant \frac{\beta-\alpha}{2}x(i-1).
\end{aligned}$$

Используя последнее неравенство, выводим

$$\frac{1-x(i-1)\beta}{y(i-1)\alpha} \geqslant \frac{\frac{\beta-\alpha}{2}x(i-1)+y(i-1)}{y(i-1)\alpha} = \frac{1}{\alpha} + \frac{x(i-1)\frac{\beta-\alpha}{2}}{y(i-1)\alpha}. \tag{12}$$

Из сбалансированности отрезка $T(i-1)$ получаем

$$\begin{aligned}
&\frac{1}{\alpha} + \frac{x(i-1)\frac{\beta-\alpha}{2}}{y(i-1)\alpha} > \frac{1}{\alpha} + \frac{\beta-\alpha}{2\beta} = \frac{2\beta+\alpha\beta-\alpha^2}{2\alpha\beta} =\\
&= \frac{(\alpha+\beta)\beta+\alpha\beta+\alpha^2-2\alpha^2}{2\alpha\beta},
\end{aligned} \tag{13}$$

что можно упростить до

$$\frac{(\alpha+\beta)^2-2\alpha^2}{2\alpha\beta} = \frac{2-\alpha^2}{\alpha\beta} = 1 + \frac{2-2\alpha}{\alpha\beta} = 1 + \frac{\beta-\alpha}{\alpha\beta} > \beta-\alpha+1, \tag{14}$$

где последнее неравенство верно, так как $1 > \alpha\beta$. Применяя равенство (11) и неравенства (12)–(14), получаем требуемое.

Теперь покажем, что из неравенства $u_1(i-1) \geqslant u_1''$ следует $u_1(i) \geqslant u_1''$. Доказывая от противного, предположим, что $u_1(i-1) \geqslant u_1''$ и $u_1(i) < u_1''$, т.е. u_1 убывает. Случаи нецентрального положения отрезка $T(i-1)$ или ошибочной передачи разбираются так же, как и в предыдущей части доказательства. Поэтому будем считать, что $T(i-1)$ центральный и передача произошла без ошибки. Следующие неравенства

эквивалентны друг другу:

$$u_1(i-1) \geqslant u_1'' = \log(\beta/\alpha - 1),$$
$$\frac{1 - x(i-1) - y(i-1)}{x(i-1)} \geqslant \beta/\alpha - 1,$$
$$\alpha \geqslant \alpha y(i-1) + \beta x(i-1).$$

Рассуждая похожим образом, можно показать эквивалентность

$$u_1(i) < u_1'',$$
$$\alpha < \alpha y(i) + \beta x(i).$$

Так как отрезок $T(i-1)$ – центральный и передача произошла без ошибки, то выполнено равенство $\alpha y(i-1) + \beta x(i-1) = x(i) + y(i)$. Это равенство и приводит к искомому противоречию

$$\alpha \geqslant \alpha y(i-1) + \beta x(i-1) = y(i) + x(i) \geqslant \alpha y(i) + \beta x(i) > \alpha. \quad \blacktriangle$$

Доказательство предложения 8. Сначала рассмотрим случай, когда оба отрезка $T(i-1)$ и $T(i)$ являются центральными. Вне зависимости от того, происходит ли ошибка, верно следующее:

$$u_2(i) - u_2(i-1) = -\log(4x(i-1)\beta y(i-1)\alpha) + \log(4x(i-1)y(i-1)) =$$
$$= -\log(\alpha\beta) > 0,$$

где последнее неравенство следует из условия $\alpha\beta < 1$.

Перейдем к случаю, когда отрезок $T(i-1)$ центральный, а $T(i)$ – нет. Пункт 5 предложения 6 позволяет утверждать, что перехода не происходило, а из п. 3 предложения 5 мы понимаем, что при передаче произошла ошибка. Преобразуем выражение:

$$u_2(i) - u_2(i-1) =$$
$$= \log\left(\frac{1-y(i)}{x(i)}\right) + \log(4x(i-1)y(i-1)) = \log\left(\frac{4(1-y(i))y(i)}{\alpha\beta}\right).$$

Поскольку $T(i)$ – не центральный, то $1/2 \leqslant y(i) \leqslant \dfrac{\beta}{2}$. Значение $y(i) = \dfrac{\beta}{2}$ минимизирует логарифм в правой части последнего равенства, поэтому

$$\log\left(\frac{4(1-y(i))y(i)}{\alpha\beta}\right) \geqslant \log 1 = 0.$$

Теперь рассмотрим случай, когда отрезок $T(i-1)$ не является центральным, причем произошел переход. Без ограничения общности полагаем $\ell(i-1) < r(i-1)$. Из п. 5 предложения 6 заключаем, что $T(i)$ является центральным. Поэтому верна цепочка преобразований

$$u_2(i) - u_2(i-1) = -\log(4\ell(i)r(i)) - \log\left(\frac{1-r(i-1)}{\ell(i-1)}\right) =$$
$$= -\log\left(\frac{4(1-r(i-1))\ell(i)r(i)}{\ell(i-1)}\right) = -\log\big(4\beta(1-r(i-1))r(i)\big).$$

Используя равенство

$$r(i) = 1 - \beta(t(i-1) + \ell(i-1)) = \frac{\alpha}{2} + \beta\left(r(i-1) - \frac{1}{2}\right),$$

получаем

$$-\log(4\beta(1-r(i-1))r(i)) = -\log\left(4\beta(1-r(i-1))\left(\frac{\alpha}{2}+\beta\left(r(i-1)-\frac{1}{2}\right)\right)\right).$$

Выражение под логарифмом является квадратичной функцией, достигающей максимума при $r(i-1) = \dfrac{3\beta-\alpha}{4\beta}$. Поэтому

$$-\log\left(4\beta(1-r(i-1))\left(\frac{\alpha}{2}+\beta\left(r(i-1)-\frac{1}{2}\right)\right)\right) \geqslant$$
$$\geqslant -\log\left((\beta+\alpha)\left(\frac{\alpha}{2}+\frac{\beta-\alpha}{4}\right)\right) = -\log 1 = 0.$$

Осталось рассмотреть случай, когда отрезок $T(i-1)$ не является центральным и отсутствует переход. Поскольку $\dfrac{1}{4x(i)y(i)} \geqslant \dfrac{1-y(i)}{x(i)}$, можно вывести, что

$$u_2(i) - u_2(i-1) \geqslant \log\left(\frac{1-y(i)}{x(i)}\right) - \log\left(\frac{1-y(i-1)}{x(i-1)}\right) = 0.$$

Равенство нулю выполнено, поскольку нет перехода, откуда следует

$$1-y(i) = \begin{cases}(1-y(i-1))\beta, & \text{если передача безошибочна,}\\ (1-y(i-1))\alpha, & \text{если произошла ошибка,}\end{cases}$$

и

$$x(i) = \begin{cases}x(i-1)\beta, & \text{если передача безошибочна,}\\ x(i-1)\alpha, & \text{если произошла ошибка,}\end{cases}$$

что завершает доказательство. ▲

Доказательство предложения 9. Если произошел переход, то согласно п. 1 предложения 5 прием должен быть безошибочным. В силу п. 2 предложения 5 мы знаем, что в этом случае истинный отрезок увеличивается, что доказывает первое утверждение.

Для доказательства второго утверждения мы сначала рассмотрим случай нецентрального отрезка $T(i-1)$. В этом случае верны равенства

$$v_1(i) - v_1(i-1) = \log t(i) - \log t(i-1) = \begin{cases}\log\beta, & \text{если передача безошибочна,}\\ \log\alpha, & \text{если произошла ошибка.}\end{cases}$$

Теперь рассмотрим случай центрального отрезка $T(i-1)$, причем перехода не было. В этом случае при передаче должна была произойти ошибка, так как иначе мы получим противоречие с п. 4 предложения 6. Получается, что нам надо доказать

$$\log t(i) - \log t(i-1) \geqslant \log\alpha,$$

а это верно в силу п. 4 предложения 5. ▲

Доказательство предложения 4. Сначала рассмотрим случай $u_1(i-1) \geqslant$ $\geqslant u_1''$, причем происходил переход. Из п. 6 предложения 6 мы знаем, что как $T(i-1)$, так и $T(i)$ являются центральными отрезками. Отсюда следует, что

$$v_2(i) - v_2(i-1) = -\log(2y(i)) + \log(2y(i-1)) =$$
$$= -\log(2x(i-1)\beta) + \log(2y(i-1)) \geqslant -\log\beta.$$

Теперь рассмотрим случаи без перехода. Пусть отрезки $T(i-1)$ и $T(i)$ являются центральными. Получаем, что

$$v_2(i) - v_2(i-1) = \log\left(\frac{y(i-1)}{y(i)}\right) =$$
$$= \begin{cases} -\log\alpha \geqslant \log\beta, & \text{если передача безошибочна,} \\ -\log\beta \geqslant \log\alpha, & \text{если произошла ошибка.} \end{cases}$$

Теперь перейдем к случаю, когда отрезок $T(i-1)$ является центральным, а $T(i)$ – нет. Это может произойти только в случае передачи с ошибкой (п. 3 предложения 5), а значит,

$$v_2(i) - v_2(i-1) = \log(2(1-y(i))) + \log(2y(i-1)) = \log(4(1-y(i))y(i)) - \log\beta,$$

но так как $y(i-1) \leqslant 1/2$, то $y(i) \leqslant \dfrac{\beta}{2}$. Таким образом, получаем

$$v_2(i) - v_2(i-1) = \log(4(1-y(i))y(i)) - \log\beta \geqslant \log(\alpha\beta) - \log\beta = \log\alpha.$$

В рассматриваемом случае также выполнено неравенство $v_2(i-1) < \log\beta$, которое следует из цепочки эквивалентных преобразований

$$v_2(i-1) < \log\beta,$$
$$-\log(2y(i-1)) < \log\beta,$$
$$\frac{1}{2} < \beta y(i-1) = y(i).$$

Здесь последнее неравенство следует из того, что отрезок $T(i)$ не является центральным.

Рассмотрим случай, когда оба отрезка $T(i-1)$ и $T(i)$ не являются центральными, причем перехода не происходило. В этом случае выполнена цепочка равенств

$$v_2(i) - v_2(i-1) = \log(2(1-y(i))) - \log(2(1-y(i-1))) =$$
$$= \log\left(\frac{t(i)+x(i)}{t(i-1)+x(i-1)}\right) = \begin{cases} \log\beta, & \text{если передача безошибочна,} \\ \log\alpha, & \text{если произошла ошибка.} \end{cases}$$

Мы покажем, что верно неравенство $v_2(i-1) < \log\beta$, если произошла ошибка. Заметим, что верно неравенство

$$\log(2(1-y(i-1))) \leqslant -\log(2y(i-1)).$$

Тогда неравенство $v_2(i-1) < \log\beta$ следует из цепочки эквивалентных преобразований

$$-\log(2y(i-1)) < \log\beta,$$
$$\frac{1}{2y(i-1)} < \beta,$$
$$\frac{1}{2} < \beta y(i-1) = y(i),$$

где последнее неравенство верно, так как отрезок $T(i)$ не является центральным и произошла ошибка.

Наконец, рассмотрим случай, когда отрезок $T(i)$ является центральным, а отрезок $T(i-1)$ – нет. В этом случае ошибок при передаче не происходило, так как

в противном случае выполнено $y(i) \geqslant y(i-1) \geqslant 1/2$. Поскольку

$$-\log(2y(i)) \geqslant \log(2(1-y(i))),$$

то

$$v_2(i) - v_2(i-1) = -\log(2y(i)) - \log(2(1-y(i-1))) \geqslant \log\left(\frac{1-y(i)}{1-y(i-1)}\right) = \log\beta,$$

что завершает доказательство. ▲

Доказательство предложения 10. Из п. 2 предложения 6 и неравенства (3) можно вывести

$$v_2(i_0) > \frac{u_2(i_0)}{2} - \frac{\log(\beta/\alpha)}{2} \geqslant -\frac{1}{2}\log(\alpha^4\beta^6) \geqslant -\frac{1}{2}\log\beta^{-2} = \log\beta. \tag{15}$$

Поскольку $v_2(i_0) = -\log(2y(i_0)) > \log\beta$, то $y(i_0) < 1/(2\beta)$. Из $y(i_0) < 1/(2\beta)$ получаем

$$u_1(i_0) = \log\left(\frac{1-y(i_0)-x(i_0)}{x(i_0)}\right) \geqslant \log\left(\frac{1-2y(i_0)}{y(i_0)}\right) > u_1'.$$

Из предложения 7 следует, что $u_1(i) \geqslant u_1'$ для всех $i \geqslant i_0$. Предложение 8 влечет неравенство $u_2(i) \geqslant c$ для всех $i \geqslant i_0$. Используя те же рассуждения, что и в (15), получаем неравенство $v_2(i) > \log\beta$ для всех i, для которых отрезок $T(i)$ является центральным и сбалансированным. Отметим, что так как $c \geqslant u_2'$, то выполняется неравенство $u_2(i) \geqslant u_2'$.

Пусть в моменты $j_1, \ldots, j_k$, $i_0 \leqslant j_1 < \ldots < j_k < i_1$, происходили переходы. Представим полуинтервал $[i_0, i_1)$ в виде объединения непересекающихся полуинтервалов $[i_0, j_1) \cup [j_1, j_1+1) \cup [j_1+1, j_2) \cup \ldots \cup [j_k, i_1)$. Из пп. 3 и 7 предложения 6 нам известно, что в моменты, соответствующие концам полуинтервалов, истинный отрезок является центральным и сбалансированным, а значит, все условия для применения предложения 10 выполнены. Более того, выполнение неравенства (4) для этих полуинтервалов влечет выполнение неравенства и для их объединения. Таким образом, достаточно рассмотреть только два случая:

1. $i_1 = i_0 + 1$ и произошел переход;
2. Между моментами i_0 и i_1 переходов не было.

Первый случай тривиален. Так как между моментами i_0 и $i_1 = i_0+1$ был переход, то согласно п. 1 предложения 5 передача произошла без ошибки. В этом случае $g(i_0, i_1) = \log\beta$. С другой стороны, $u_2(i_1) - u_2(i_0) = -\log(\alpha\beta)$ по предложению 8, что не меньше чем $\log\beta$ благодаря неравенству (3).

Перейдем ко второму случаю, в котором между моментами i_0 и i_1 нет переходов. Минимальный отрезок все время остается минимальным, следовательно,

$$g(i_0, i_1) = e(i_0, i_1)\log\alpha + f(i_0, i_1)\log\beta = \log\left(\frac{x(i_1)}{x(i_0)}\right).$$

Обозначим $v_2(i_1) - v_2(i_0)$ и $u_2(i_1) - u_2(i_0)$ через Δv_2 и Δu_2 соответственно. Так как $T(i_0)$ и $T(i_1)$ являются центральными, то

$$\Delta u_2 = -\log(x(i_1)y(i_1)) + \log(x(i_0)y(i_0)) = -\log y(i_1) + \log y(i_0) - \log\left(\frac{x(i_1)}{x(i_0)}\right) = \\ = \Delta v_2 - g(i_0, i_1),$$

что эквивалентно следующему:

$$g(i_0, i_1) = \Delta v_2 - \Delta u_2.$$

Используя пп. 1 и 2 предложения 6 для моментов i_1 и i_0 соответственно, получаем

$$g(i_0, i_1) = \Delta v_2 - \Delta u_2 \leqslant \frac{\Delta u_2 + \log\left(\frac{\beta}{\alpha}\right)}{2} - \Delta u_2 = \frac{-\Delta u_2 + \log\left(\frac{\beta}{\alpha}\right)}{2}.$$

Вспомним неравенство $y(i_0) < 1/(2\beta)$, откуда следует $y(i_0 + 1) < 1/2$, а это значит, что $T(i_0 + 1)$ является центральным. Используя предложение 8, получаем

$$\Delta u_2 = u_2(i_1) - u_2(i_0 + 1) + u_2(i_0 + 1) - u_2(i_0) \geqslant -\log(\alpha\beta).$$

Используя это неравенство вместе с неравенством (3), получаем

$$g(i_0, i_1) \leqslant \frac{-\Delta u_2 + \log\left(\frac{\beta}{\alpha}\right)}{2} \leqslant \frac{\log(\alpha\beta) + \log\left(\frac{\beta}{\alpha}\right)}{2} = \log\beta \leqslant -\log(\alpha\beta) \leqslant \Delta u_2. \quad \blacktriangle$$

Доказательство предложения 3. Вспомним, что согласно п. 5 предложения 5 неравенство $u_2(i) \geqslant u_1(i)$ выполняется для всех $x(i)$, $y(i)$ и $t(i)$.

Если $u_1(i-1) < u_1'$, то $u_1(i) \geqslant u_1(i-1)$ по предложению 7, следовательно, $u(i) \geqslant u_1(i) \geqslant u_1(i-1) = u(i-1)$. Если $T(i-1)$ центральный и произошел переход, то $u_1(i) - u_1(i-1) \geqslant \log\beta$ по предложению 7, значит, $u(i) - u(i-1) \geqslant \log\beta$.

Если же $u_1(i-1) \geqslant u_1'$, то $u_1(i) \geqslant u_1'$ по предложению 7 и $u_2(i) \geqslant u_2(i-1)$ по предложению 8. Это означает, что $u(i) = u_2(i) \geqslant u_2(i-1) = u(i-1)$. Если отрезок $T(i-1)$ центральный и произошел переход, то $T(i)$ тоже центральный согласно п. 5 предложения 6. Поэтому можно использовать предложение 8, что дает $u_2(i) - u_2(i-1) \geqslant -\log(\alpha\beta)$. Так как $\alpha\beta^2 \leqslant 1$ (см. (3)), то это выражение не меньше $\log\beta$. $\blacktriangle$

Доказательство предложения 2. Напомним, что $v_2(i) \geqslant v_1(i)$ для любых $x(i)$, $y(i)$ и $t(i)$ согласно п. 6 предложения 5.

Предположим, что $u_1(i-1) < u_1''$. Если перехода не происходило, то утверждение верно благодаря предложению 9. Если переход был, то предложение 9 дает неравенство $v_1(i) > v_1(i-1)$, следовательно, $v(i) \geqslant v_1(i) > v_1(i-1) = v(i-1)$, т.е. $v(i) - v(i-1) > 0$. Для центрального отрезка $T(i-1)$ эта оценка достаточно хороша. Остается рассмотреть случай, когда $T(i-1)$ не центральный. Из условия $u_1(i-1) < u_1''$ следует $v(i) - v(i-1) \geqslant v_1(i) - v(i-1) = v_1(i) - v_1(i-1)$. Так как произошел переход, то передача произошла без ошибки; условие нецентральности отрезка $T(i-1)$ влечет соотношения $t(i) = \beta t(i-1)$ и $v(i) - v(i-1) \geqslant v_1(i) - v_1(i-1) = \log\beta$.

Предположим, что $u_1(i-1) \geqslant u_1''$. В этом случае $u_1(i) \geqslant u_1''$ по предложению 7. Если не было перехода, то доказываемое предложение следует из предложения 4. Если переход был, то отрезок $T(i-1)$ является центральным согласно п. 6 предложения 6. Тогда $v(i) - v(i-1) = v_2(i) - v_2(i-1) \geqslant -\log\beta$ по предложению 4. $\blacktriangle$

§ 5. Заключение

В данной статье мы рассмотрели новую задачу передачи информации по комбинаторному каналу со вставками и выпадениями и обратной связью. Мы показали, как эта задача может быть сведена к задаче передачи информации по комбинаторному каналу с замещениями. Таким образом, была установлена максимальная асимптотическая скорость кодов для комбинаторного канала со вставками и выпадениями. В частности, скорость положительна, если доля ошибок меньше $1/2$. Мы также напомнили алгоритм Хорштейна [10] для комбинаторного канала с замещениями и привели более подробную версию анализа Зигангирова [9] этого алгоритма.

Подчеркнем, что все результаты, рассматриваемые в данной статье, касаются лишь двоичного канала. Возникает естественный вопрос: можно ли обобщить эти ре-

зультаты для недвоичного случая? Наилучшие на текущий момент результаты для q-ичного канала с обратной связью и замещениями описаны в работе [12]. В частности, если доля ошибок находится в интервале $0 < \tau < 1/q$, то максимальная асимптотическая скорость установлена лишь для счетного числа значений τ. Отметим также, что перенести рассуждения Зигангирова с двоичного случая на q-ичный случай достаточно сложно, поскольку не очевидны аналоги для функций u и v.

Авторы благодарны Цзылинь Цзяну за полезные замечания и комментарии при обсуждении доказательства Зигангирова.

СПИСОК ЛИТЕРАТУРЫ

1. *Левенштейн В.И.* Двоичные коды с исправлением выпадений, вставок и замещений символов // ДАН СССР. 1965. Т. 163. № 4. С. 845–848. http://mi.mathnet.ru/dan31411
2. *Варшамов Р.Р., Тенengольц Г.М.* Код, исправляющий одиночные несимметрические ошибки // АиТ. 1965. Т. 26. № 2. С. 288–292. http://mi.mathnet.ru/at11293
3. *Cheraghchi M., Ribeiro J.* An Overview of Capacity Results for Synchronization Channels // IEEE Trans. Inform. Theory. 2020. V. 67. № 6. P. 3207–3232. https://doi.org/10.1109/TIT.2020.2997329
4. *Schulman L.J., Zuckerman D.* Asymptotically Good Codes Correcting Insertions, Deletions, and Transpositions // IEEE Trans. Inform. Theory. 1999. V. 45. № 7. P. 2552–2557. https://doi.org/10.1109/18.796406
5. *Bukh B., Guruswami V.* An Improved Bound on the Fraction of Correctable Deletions // Proc. 27th Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'2016). Arlington, VA, USA. Jan. 10–12, 2016. P. 1893–1901. https://doi.org/10.1137/1.9781611974331.ch133
6. *Bukh B., Guruswami V., Håstad, J.* An Improved Bound on the Fraction of Correctable Deletions // IEEE Trans. Inform. Theory. 2016. V. 63. № 1. P. 93–103. https://doi.org/10.1109/TIT.2016.2621044
7. *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
8. *Berlekamp E.R.* Block Coding with Noiseless Feedback. PhD Thesis. MIT, Cambridge, USA, 1964.
9. *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
10. *Horstein M.* Sequential Transmission Using Noiseless Feedback // IEEE Trans. Inform. Theory. 1963. V. 9. № 3. P. 136–143. https://doi.org/10.1109/TIT.1963.1057832
11. *Schalkwijk J.* A Class of Simple and Optimal Strategies for Block Coding on the Binary Symmetric Channel with Noiseless Feedback // IEEE Trans. Inform. Theory. 1971. V. 17. № 3. P. 283–287. https://doi.org/10.1109/TIT.1971.1054625
12. *Лебедев В.С.* Кодирование при наличии бесшумной обратной связи // Пробл. передачи информ. 2016. Т. 52. № 2. С. 3–14. http://mi.mathnet.ru/ppi2200

Маринггер Георг
Технический университет Мюнхена, Германия
georg.maringer@tum.de
Полянский Никита Андреевич
Технический университет Мюнхена, Германия
Сколковский институт науки и технологий (Сколтех)
nikita.polyansky@gmail.com
Воробьев Илья Викторович
Сколковский институт науки и технологий (Сколтех)
vorobyev.i.v@yandex.ru
Вельтер Лоренц
Технический университет Мюнхена, Германия
lorenz.welter@tum.de

Поступила в редакцию
14.01.2021
После доработки
16.02.2021
Принята к публикации
20.06.2021