НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2025 Том 25 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2025 Vol. 25 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2025-25-2-286-294
УДК 004.056.4

Построение множества плотных информационных совокупностей для кодов Гилберта и их расширений

Мария Николаевна Исаева✉

Национальный исследовательский университет «Высшая школа экономики», Санкт-Петербург, 190008, Российская Федерация

misaeva@hse.ru✉, https://orcid.org/0009-0007-6228-0617

Аннотация

Введение. При передаче информации по каналам с группирующимися ошибками традиционным подходом является декорреляция канала и использование кодов, исправляющих независимые ошибки. Процедура декорреляции понижает достижимые скорости надежной передачи, поэтому актуальной является задача использования специальных кодов для каналов с памятью и построения эффективных вычислительных методов декодирования для исправления группирующихся ошибок. Для класса случайных кодов известен подход с использованием информационных совокупностей ограниченного диаметра при исправлении пакетов ошибок. Размер множества информационных совокупностей растет линейно с увеличением длины кода, а построение множества описывается вероятностной процедурой. В работе рассматривается построение множества информационных совокупностей для специального класса кодов, исправляющих пакеты ошибок, называемого кодами Гилберта. **Метод.** Рассмотрены множества кодовых позиций наименьшего возможного диаметра. На основе вычисления рангов подматриц проверочной матрицы кода Гилберта оценена вероятность того, что набор позиций является информационной совокупностью. Для заданного расположения информационной совокупности проанализированы позиции исправляемых пакетов. На основании проведенного анализа предложена методика построения множества плотных информационных совокупностей для кодов Гилберта с целью исправления всех пакетов ошибок в пределах корректирующей способности кода. Используя особенности задания параметров кодов Гилберта, проведена оценка размера полученного множества плотных информационных совокупностей. **Основные результаты.** При простом размере блока проверочной матрицы квазициклического кода показано, что для кодов Гилберта на любой позиции находится плотная информационная совокупность. Установлено, что в случае расширенных кодов Гилберта совокупности минимального диаметра существуют только на последней позиции каждого блока. Предложена процедура построения множества плотных информационных совокупностей минимального диаметра для кодов Гилберта и их расширений. Проведено сравнение размера множества информационных совокупностей и вероятность его получения для кодов Гилберта и случайных кодов. Установлено, что количество информационных совокупностей, полученных по предложенной процедуре, не растет с увеличением длины кода. **Обсуждение.** Полученные в работе результаты, показывают возможность разработки вычислительно эффективных декодеров на основе информационных совокупностей при исправлении однократных пакетов ошибок. В отличие от случайных линейных кодов, для которых методы построения информационных совокупностей, в том числе плотных, носят вероятностный характер, для кодов Гилберта определена процедура гарантированного построения множества информационных совокупностей минимального диаметра. Квазициклическая структура кодов Гилберта позволяет строить множества плотных информационных совокупностей меньшей размерности, чем для случайных кодов. Полученные результаты позволяют гарантировать исправление пакетов ошибок в пределах корректирующей способности кодов Гилберта и их расширений с малой вычислительной сложностью. Использование вычислительно эффективных процедур кодирования и декодирования пакетов ошибок позволит повысить надежность доставки сообщений в каналах с памятью.

Ключевые слова

информационные совокупности, корректирующая способность, коды Гилберта, каналы с памятью, пакеты ошибок

Благодарности
Работа подготовлена в результате проведения исследования в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ), лаборатория Интернета вещей и киберфизических систем НИУ ВШЭ в Санкт-Петербурге.

Ссылка для цитирования: Исаева М.Н. Построение множества плотных информационных совокупностей для кодов Гилберта и их расширений // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 2. С. 286–294. doi: 10.17586/2226-1494-2025-25-2-286-294

Development of dense information sets for Gilbert codes and its extensions

Maria N. Isaeva✉

HSE University-St. Petersburg, Saint Petersburg, 190008, Russian Federation

misaeva@hse.ru✉, https://orcid.org/0009-0007-6228-0617

Abstract
When transmitting information over channels with grouping errors, the traditional approach is channel decorrelation and use of codes correcting independent errors. The decorrelation procedure lowers achievable rates of reliable transmission, therefore the problem of using special codes for channels with memory and construction of computationally effective decoding methods for correction of grouping errors is actual. For the class of random codes, an approach is known using information sets of limited diameter to correct error bursts. The size of the set of information sets grows linearly with increasing code length, and the construction of the set is described by a probabilistic procedure. This article considers the construction of a set of information sets for a special class of codes that correct error bursts called Gilbert codes. The sets of code positions of the smallest possible diameter are considered. Based on the calculation of the ranks of the submatrices of the parity-check matrix of the Gilbert code, the probability that the set of positions is an information set is estimated. For a given location of the information set, the positions of the corrected bursts are analyzed. Based on the analysis, a method for constructing a set of dense information sets for Gilbert codes for correcting all error bursts within the code correcting capacity is proposed. Using the features of setting the parameters of Gilbert codes, an estimate of the size of the resulting set of dense information sets is carried out. For a simple block size of the parity-check matrix of a quasi-cyclic code, it is shown that for Gilbert codes a dense information set is located at any position. In the case of extended Gilbert codes, it is shown that sets of minimum diameter exist only at the last position of each block. A procedure for constructing a set of dense information sets of minimum diameter for Gilbert codes and their extensions is proposed. A comparison is made of the set size of information sets and the probability of obtaining it for Gilbert codes and random codes. It is shown that the number of information sets obtained by the proposed procedure does not increase with the length of the code. The results obtained in the paper demonstrate the possibility of developing computationally efficient decoders based on information sets when correcting single error bursts. Unlike random linear codes, for which the methods of constructing information sets including dense ones, are probabilistic, a procedure for guaranteed construction of a set of information sets of minimal diameter is specified for Gilbert codes. The quasi-cyclic structure of Gilbert codes allows constructing sets of dense information sets of smaller dimension than for random codes. The obtained results allow us to guarantee the correction of error bursts within the correcting capacity of Gilbert codes and their extensions with low computational complexity. The use of computationally efficient procedures for encoding and decoding error bursts will improve the reliability of message delivery in channels with memory.

Keywords
information sets, error correcting capability, Gilbert codes, channels with memory, error bursts

Acknowledgements
The article was prepared within the framework of the Basic Research Program at HSE University, Internet of Things and Cyber-Physical Systems Laboratory, St. Petersburg School of Physics, Mathematics, and Computer Science.

For citation: Isaeva M.N. Development of dense information sets for Gilbert codes and its extensions. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 2, pp. 286–294 (in Russian). doi: 10.17586/2226-1494-2025-25-2-286-294

Введение

В задачах управления потоками данных, хранения больших объемов информации и ее передачи по каналам связи необходимо обеспечивать надежность обрабатываемых пользовательских данных. Как при передаче информации, так и в процессе ее обработки могут возникать ошибки. Шум влияет как на достоверность передаваемой информации, так и на вероятность доставки. Исходя из этого, актуальной проблемой является разработка методов обеспечения структурной надежности инфокоммуникационных систем и надежной доставки сообщений [1–4], включающих исправление возникших ошибок на принимающей стороне. Надежность доставки может повышаться путем внесения избыточности в систему связи и репликации передаваемых данных с кратностью, зависящей от требований надежности и своевременности доставки передаваемых сообщений [5, 6]. Одним из способов управления избыточностью является добавление контрольной информации непосредственно в само сообщение. Вопросами восстановления поврежденных данных с использованием этой информации занимается теория помехоустойчивого кодирования [7, 8].

Возникновение ошибок далеко не всегда адекватно описывается моделью случайных независимых событий, чаще всего ошибки сгруппированы внутри передаваемой последовательности [8, 9]. Для борьбы с этим

явлением в каналах с группирующимися ошибками (пакетами ошибок) необходимо построение специфических кодеров и декодеров, которые учитывают особенности таких каналов.

Классические коды Рида–Соломона в каналах, описываемых марковскими цепями, рассматривались в [9], однако сложность кодирования и декодирования этих кодов сравнительно велика для современных систем связи. Более эффективные как по вероятности ошибки, так и по вычислительной сложности коды с малой плотностью проверок на четность применительно к каналам с памятью изучались в [10–12]. В работах [13–15] рассмотрены полярные коды. Следует отметить, что основное внимание исследователей уделяется вопросам построения кодов для каналов с памятью, а не специальным методам их декодирования. В [16] рассмотрен оконный декодер для исправления пакетов ошибок блочно-перестановочными кодами.

В качестве подхода к декодированию можно использовать декодирование по информационным совокупностям, которые, как показано в [17, 18], могут исправлять однократные пакеты ошибок в соответствии с корректирующей способностью случайных кодов. Но случайные коды не обладают какой-либо структурой, поэтому программная и аппаратная реализации процедур кодирования и декодирования может оказаться недостаточно вычислительно эффективной. В [18] представлено декодирование квазициклических кодов с помощью информационных совокупностей, однако исследование ограничено ансамблем случайных кодов, не оптимизированных под исправление пакетов ошибок. В [19] приведен частный случай квазициклических блочно-перестановочных кодов Гилберта и их модификации и доказано, что эти коды способны исправлять пакеты ошибок. Однако нерешенной остается проблема декодирования кодов Гилберта, реализующего их пакетную корректирующую способность.

При использовании информационных совокупностей для исправления пакетов ошибок количество ошибок может быть уменьшено введением ограничений на их диаметр. Для случайных линейных кодов построение информационных совокупностей заданного диаметра является вероятностным. В настоящей работе решается задача построения множества информационных совокупностей для исправления однократных пакетов ошибок с использованием особенностей конструкции кодов Гилберта и их расширений [19]. Необходимо предложить процедуру построения множества плотных информационных совокупностей для кодов Гилберта, оценить размер полученного множества в зависимости от параметров кода и вероятность его построения.

Блочно-циркулянтные конструкции низкоплотностных кодов

Коды с малой плотностью проверок на четность, или низкоплотностные коды, являются одним из наиболее распространенных классов кодов, используемых в современных инфокоммуникационных стандартах [7]. Эти коды характеризуются разреженной проверочной матрицей, что позволяет строить для них крайне вычислительно эффективные алгоритмы кодирования и декодирования, обеспечивающие низкие вероятности ошибки при исправлении независимых ошибок. Одной из наиболее важных конструкций низкоплотностных кодов является блочно-циркулянтная, в этом случае код является квазициклическим. Рассмотрим особенности данной конструкции.

Блочно-циркулянтные коды задаются с помощью базовой матрицы, состоящей из γ строк и ρ столбцов, причем $\gamma < \rho$. Каждый элемент базовой матрицы задает блок, представляющий собой двоичную квадратную матрицу размера $m \times m$. Базовая матрица $\mathbf{H}_{\text{base}}$ блочно-циркулянтного кода имеет вид:

$$\mathbf{H}_{\text{base}} = \begin{bmatrix} t_{11} & \cdots & t_{1\rho} \\ \vdots & \ddots & \vdots \\ t_{\gamma 1} & \cdots & t_{\gamma\rho} \end{bmatrix},$$

где t_{ij} — целые числа. Если каждый элемент $\mathbf{H}_{\text{base}}$ заменить на блок $\mathbf{C}^{t_{ij}}$, где $\mathbf{C}$ — матрица циклической перестановки, размер которой $m \times m$, получим двоичную проверочную матрицу $\mathbf{H}$ кода:

$$\mathbf{H} = \begin{bmatrix} \mathbf{C}^{t_{11}} & \cdots & \mathbf{C}^{t_{1\rho}} \\ \vdots & \ddots & \vdots \\ \mathbf{C}^{t_{\gamma 1}} & \cdots & \mathbf{C}^{t_{\gamma\rho}} \end{bmatrix}.$$

В общем случае в блочно-циркулянтной конструкции в качестве блока может быть выбран любой циркулянт, а в разновидности, называемой блочно-перестановочной конструкцией — произвольная матрица перестановки. Рассмотрим случай использования степеней матрицы $\mathbf{C}$ в качестве блоков. Таким образом, для данного случая термины блочно-перестановочный и блочно-циркулянтный взаимозаменяемы и в дальнейшем под этим термином будем подразумевать только матрицы описанного вида.

Известно, что максимальная длина пакета $b_{\max}$, исправляемого блочно-перестановочными кодами, ограничена размером блока m, или $b_{\max} < m$, поэтому для более эффективного использования избыточности, вносимой помехоустойчивым кодом, необходимо максимизировать размер блока m при фиксированной длине n, т. е. минимизировать значение ρ. Это автоматически приводит и к минимизации значения γ. Потому, в отличие от ситуации с независимыми ошибками, где для получения наилучших кодов рассматриваются матрицы из большого числа блоков (например, в стандарте 5G), для исправления пакетов необходимо использовать блочно-перестановочные коды, в которых количество блоков мало. В результате рассмотрим коды при $\gamma = 2$ или $\gamma = 3$, или, другими словами, с проверочной матрицей из двух или трех полос.

Специальным подклассом блочно-циркулянтных кодов с двумя полосами являются коды Гилберта [19, 20]. Особенность данных кодов — фиксированный способ выбора блоков: в двухполосной матрице кода Гилберта первая полоса состоит из единичных матриц, а вторая — из матриц циклической перестановки со степенями от 0 до $\rho - 1$, где $\rho \le m$. Отметим, что для построения кодов Гилберта используется матрица $\mathbf{C}$, обеспечивающая циклический сдвиг влево, например, при $m = 4$:

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

В современных стандартах при описании базовой матрицы кода обычно предполагается, что матрица **C** обеспечивает сдвиг вправо, однако это дало бы код с совершенно иными (худшими) свойствами с точки зрения исправления пакетов ошибок. Базовая матрица кода Гилберта задается следующим образом:

$$\mathbf{H}_{\text{base}} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & \rho-2 & \rho-1 \end{bmatrix}, \qquad (1)$$

где $\rho \geq 3$. Модификация кода Гилберта для $\rho \geq 4$ может быть получена добавлением третьей строки к базовой матрице [16, 17]:

$$\mathbf{H}_{\text{base}} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & \rho-2 & \rho-1 \\ \rho-1 & \rho-2 & \cdots & 1 & 0 \end{bmatrix}. \qquad (2)$$

Число избыточных символов для кода Гилберта составляет $r = 2m - 1$, а для расширенного кода: $r = 3m - 2$.

Способность кода Гилберта или родственных ему кодов исправлять одиночные пакеты ошибок рассматривались во многих научных работах. В частности, в [19] была предложена процедура вычисления точной корректирующей способности таких кодов при исправлении однократных пакетов ошибок. Кратко, можно сказать, что при $\rho = 3$ код Гилберта исправляет пакеты длиной $m - 1$ и лежит на границе Рейгера (в соответствии с которой для линейного кода $2b_{\max} \leq r$). Отметим, что при увеличении ρ до примерно $m/2$ пакетная корректирующая способность $b_{\max}$ уменьшается практически по линейному закону также до величины около $m/2$, при дальнейшем увеличении значения ρ до максимального значения m величина $b_{\max}$ остается неизменной.

В случае расширенных кодов Гилберта известно, что если m — простое число, то они исправляют все пакеты до $b_{\max} = m - 1$ для любого $\rho \in [4, m]$.

В работах [18, 21] рассматривался вопрос декодирования по информационным совокупностям и предлагалась методика построения множества из небольшого количества T информационных совокупностей, которые гарантировали бы исправление пакетов в пределах корректирующей способности кода. Заметим, что возможность построения такого множества является случайным событием и определяется случайным выбором кода. Проводилась оценка вероятности этого события в предположении, что выбирается случайный линейный двоичный код. Если используется код с выраженной структурой, то полученные в [18, 21] вероятностные оценки могут довольно сильно исказиться, поэтому в дальнейшем рассматривается вопрос разработки методики построения множества плотных информационных совокупностей для блочно-перестановочных конструкций из двух и трех полос, а также оценка вероятности построения такого множества.

Для дальнейшего рассмотрения введем основные понятия информационных совокупностей [22, 23]. Информационной совокупностью называется множество позиций $\chi = \{1 \leq j_1 < j_2 < \ldots < j_k \leq n\}$, если элементы из кодового слова длиной n, соответствующие этим позициям, однозначно определяют кодовое слово. Если на позициях информационной совокупности не оказалось ошибок, то при декодировании по ней можно корректно восстановить принятое слово.

Пусть существует $(k \times n)$-порождающая матрица **G**. Для того чтобы некоторое множество из k позиций было информационной совокупностью, необходимо, чтобы ранг подматрицы $\mathbf{M}_\chi$, составленной из столбцов матрицы **G** с номерами из χ, был равен k (т. е. $\mathbf{M}_\chi$ — невырожденная обратимая матрица). С другой стороны, если рассматривается проверочная $(r \times n)$-матрица кода **H** и χ — информационная совокупность, и $\bar{\chi} = \{1, \ldots, n\} - \chi$ образует дополнение к χ до множества $\{1, \ldots, n\}$, то столбцы проверочной матрицы с номерами из $\bar{\chi}$ формируют невырожденную $(r \times r)$–подматрицу.

При исправлении независимых ошибок выполняется случайный поиск информационной совокупности. Для этого необходимо построить такое множество информационных совокупностей, чтобы при искажении передаваемых символов кодового слова (хотя бы в пределах корректирующей способности кода) нашлась неискаженная информационная совокупность — в предположении, что возможно определить это событие. Для обеспечения вероятностей ошибки декодирования, представляющих практический интерес, мощность такого множества должна быть экспоненциальной. При исправлении однократных пакетов ошибок длиной не более $b_{\max}$ достаточно найти по одной информационной совокупности вне позиций пакета для каждого возможного расположения пакета, а таких расположений может быть $n - b_{\max} + 1$. Тем не менее, можно обеспечить дальнейшее уменьшение числа информационных совокупностей, если заметить, что информационная совокупность с небольшим разбросом позиций (диаметром, т. е. разностью между максимальным и минимальным номерами позиции в информационной совокупности) может исправлять пакеты в нескольких позициях. Это приводит к идее построения информационных совокупностей ограниченного диаметра, можно назвать их плотными [17]. Более точно, назовем Δ-плотными информационными совокупностями такие, чьи позиции расположены внутри ограниченного интервала длиной $k + \Delta$, где $\Delta \in \{0, n - k - b_{\max}\}$. Конечно, при возможности следует минимизировать значение Δ. В дальнейшем в работе будет рассмотрен только случай $\Delta = 0$, и для упрощения использован термин «плотный» без указания значения Δ.

Нахождение множества плотных информационных совокупностей для кодов Гилберта и их расширения

Рассмотрим возможность построения множества плотных информационных совокупностей для кодов Гилберта, проверочная матрица которых задается в соответствии с формулой (1). Понятие плотной инфор-

мационной совокупности связано с заданием некоторой величины Δ. Рассмотрим случай $\Delta = 0$, т. е. множества из k подряд идущих позиций. Исследуем вероятность того, что такие множества образуют информационную совокупность, для этого k подряд идущих столбцов порождающей матрицы кода Гилберта (или, эквивалентно, r подряд идущих столбцов проверочной матрицы) образуют невырожденную подматрицу.

На рис. 1, *a* представлены значения рангов $(r \times r)$-подматриц, составленных из r подряд идущих столбцов проверочной матрицы кода Гилберта в зависимости от положения подматриц (на графике по оси абсцисс отмечены номера их начальных позиций) для $\rho = 5$ и для разных размеров блоков m. На рис. 1, *b* представлены аналогичные зависимости для $\rho = 8$.

Как видно из графиков на рис. 1, большинство рассмотренных подматриц не являются вырожденными, и следовательно, их позиции образуют информационные совокупности. На некоторых графиках можно видеть уменьшение ранга в узком диапазоне значений позиций, тогда как на других любая подматрица невырождена. Можно заметить, что последний случай имеет место, если числа m и $\rho - 1$ взаимно просты, т. е. не имеют общих делителей кроме единицы. В дальнейшем будем рассматривать только простые значения m. Таким образом, с учетом $\rho \le m$ указанное условие всегда выполняется.

Для построения множества плотных информационных совокупностей необходимо указать их местоположение и оценить количество.

В [21] предложена процедура построения множества плотных информационных совокупностей для случайных кодов. Для каждой начальной позиции плотной информационной совокупности диаметром $k + \Delta$ оценивается множество начальных позиций пакетов ошибок длиной $b_{\max}$, не затрагивающих данную информационную совокупность. Такие начальные позиции пакетов ошибок называются «безопасными», а в качестве $b_{\max}$ используется максимальная длина исправляемого кодом пакета. С учетом того, что начальные позиции пакетов ошибок находятся в интервале $[1, n - b_{\max} - 1]$, процедура построения множества плотных информационных совокупностей заканчивается, когда все позиции из указанного интервала становятся «безопасными».

Выбор расположения информационных совокупностей происходит следующим образом: к текущему началу i информационной совокупности (в начальном случае $i = 1$) прибавляется диаметр $k + \Delta$, а затем защитный интервал из $b_{\max} - 1$ позиций. Таким образом, начало следующей информационной совокупности находится в позиции $i + k + \Delta + b_{\max} - 1$ (позиции рассматриваются циклически). В [21] оценена мощность T множества плотных информационных совокупностей, полученных таким образом:

$$T = \left\lfloor \frac{n - b_{\max} + 1}{n - b_{\max} + 1 - (k + \Delta)} \right\rfloor. \qquad (3)$$

Для кода Гилберта значения $b_{\max}$ зависят от конкретных значений ρ, поэтому оценим количество полученных информационных совокупностей экспериментально. На рис. 2 представлены значения T, полученные с помощью описанной процедуры, для кодов Гилберта при $m = 23$ в зависимости от значений ρ.

Из графиков на рис. 2 видно, что полученную кривую можно примерно аппроксимировать как $2\rho/3$. Аналогичный результат был получен и для экспериментов с другими значениями m.

Теперь рассмотрим расширенные коды Гилберта для $\gamma = 3$, заданные в соответствии с (2). На рис. 3 представлены ранги подматриц для $\rho = 5$ и некоторых простых значений m. Пунктирными линиями указаны максимальные ранги (т. е. равные r) для соответствующих кодов.

В каждом из рассмотренных случаев (рис. 3) можно выделить в точности ρ расположений невырожден-

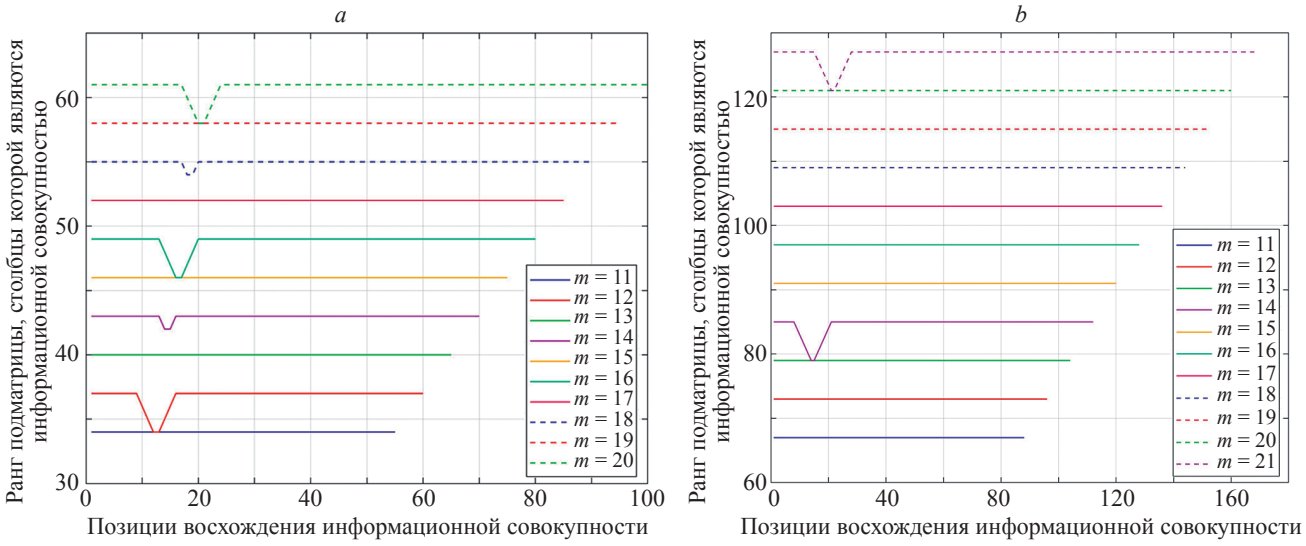

Рис. 1. Графики рангов подматриц для разных размеров блока кода Гилберта с параметром $\gamma = 2$ при $\Delta = 0$ для $\rho = 5$ (*a*) и $\rho = 8$ (*b*)

Fig. 1. Plots of submatrix ranks for different block sizes of the Gilbert code with parameter $\gamma = 2$ at $\Delta = 0$ for $\rho = 5$ (*a*) and $\rho = 8$ (*b*)

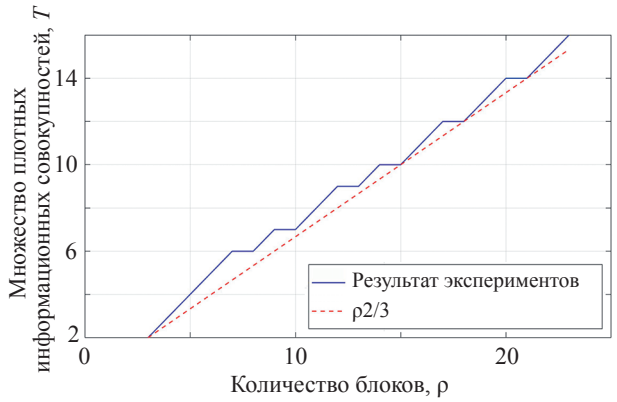

Рис. 2. Число плотных информационных совокупностей для кода Гилберта при $m = 23$

Fig. 2. The number of dense information sets for the Gilbert code at $m = 23$

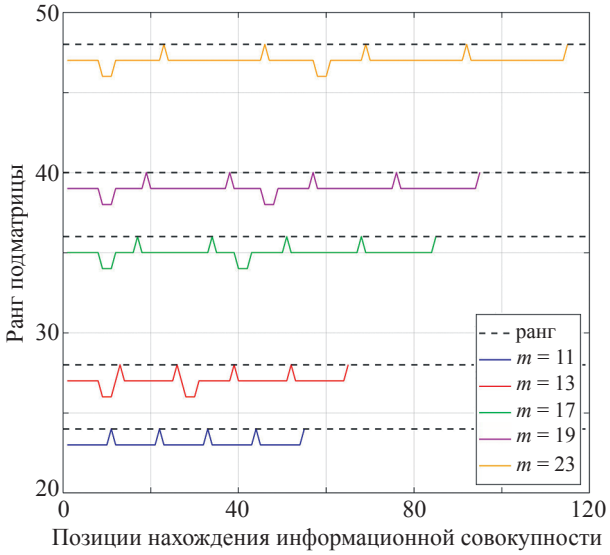

Рис. 3. График рангов подматриц для простых m и $\rho = 5$ в расширенном коде Гилберта

Fig. 3. Graph of the ranks of submatrices for primes m and $\rho = 5$ in the extended Gilbert code

ных подматриц, соответствующих пиковым значениям рангов, достигающих r. Это означает, что при выборе плотных информационных совокупностей ($\Delta = 0$) существует ограничение только позициями, соответствующими пикам: в остальных позициях плотных информационных совокупностей диаметром k не существует. Заметим, что значения аргументов в точках пиков приходятся на последние позиции блоков проверочной матрицы.

Рассмотрим расширенные коды Гилберта, базовая матрица которых задана тремя строками и $\rho \geq 4$ столбцами (2). Если в качестве начала плотной информационной совокупности диаметром k выбрать значение пика, то по описанной методике следующее возможное начало информационной совокупности будет в точности соответствовать пику, отстоящему на $\rho - 2$ блоков (как и позиции ранее, пики рассматриваются циклически). Таким образом, параметры, используемые в выражении (3), принимают следующие значения: для любого простого m и натурального $\rho \in [4, m]$ имеем $n = m\rho$, $k = m\rho - 3m + 2$, $b_{\max} = m - 1$, $\Delta = 0$. Тогда количество плотных информационных совокупностей оценивается выражением

$$T = \left\lceil \frac{m(\rho - 1) + 2}{2m - 1} \right\rceil, \qquad (4)$$

причем, используя тот факт, что $\lceil x \rceil = n$ если и только если $n - 1 < x \leq n$ [24], нетрудно показать, что из (4) справедливо $T = \lceil \rho/2 \rceil$.

Заметим, что для четного ρ построение множества информационных совокупностей после $\rho/2$ шагов приведет к первоначальному пику. Из выражения (3) следует, что для полученного множества все позиции кодовых слов будут «безопасными».

В случае нечетного ρ числа $\rho - 2$ и ρ взаимно просты, и необходимо вернуться в первоначальный пик только после прохождения по всем остальным пикам. Однако из (3) и (4) следует, что достаточно рассмотреть только последовательность из $(\rho + 1)/2$ пиков, отстоящих друг от друга на $\rho - 2$ (с учетом цикличности).

Приведенные выше рассуждения можно сформулировать в виде следующего метода построения множества плотных информационных совокупностей. Для кода Гилберта (1), m – простое, $\rho \in [3, m]$, исправляющего пакеты длиной до $b_{\max}$, вычислим следующую рекуррентную последовательность:

$$\begin{cases} n_1 = 1, \\ n_i = (n_{i-1} - 2m + b_{\max} - 1) \bmod m\rho + 1, \; i = \overline{2, T}, \end{cases}$$

где T рассчитывается в соответствии с (3). Последовательность $n_1, \ldots, n_T$ задает номера начальных позиций множества плотных информационных совокупностей.

Для расширенных кодов Гилберта последовательность $n_1, \ldots, n_T$ имеет вид:

$$\begin{cases} n_1 = m, \\ n_i = (n_{i-1} - 2m - 1) \bmod m\rho + 1, \; i = \overline{2, T}, \end{cases}$$

где $T = \lceil \rho/2 \rceil$.

В таблице приведены значения T, полученные по предложенной методике, для кодов Гилберта, их расширений, а также случайных кодов.

Из таблицы видно, что для случайных кодов нахождение множества информационных совокупностей является вероятностным [21]. Проведенное исследование показывает, что для кодов Гилберта и их расширений множество плотных информационных совокупностей диаметром k может быть построено с вероятностью равной единице для простых значений m. При этом количество информационных совокупностей, необходимых для декодирования пакетов ошибок, меньше, чем при использовании случайных кодов. С учетом того, что длины кодов в ансамблях $(2, \rho)$ и $(3, \rho)$ можно устремить к бесконечности с помощью увеличения m, полученные результаты позволяют строить множества информационных совокупностей, мощность которых не изменяется с ростом длины кода.

Таблица. Размер множеств плотных информационных совокупностей и вероятности их построения для различных кодов
Table. The sizes and construction probabilities of dense information sets for different codes

Используемый код	Длина кода, n	Длина пакета, $b_{\max}$	Параметр плотности, Δ	Размер множества, T	Вероятность построения множества
Скорость кода $R \approx 0{,}33$					
Код Гилберта (γ = 2, ρ = 3)	51	16	0	2	1
Случайный код	51	12	5	3	0,90
Код Гилберта (γ = 3, ρ = 4)	68	16	0	2	1
Случайный код	68	19	7	3	0,97
Скорость кода $R \approx 0{,}5$					
Код Гилберта (γ = 2, ρ = 4)	68	14	0	3	1
Случайный код	68	13	6	4	0,93
Код Гилберта (γ = 3, ρ = 6)	102	16	0	3	1
Случайный код	102	20	8	4	0,97
Скорость кода $R \approx 0{,}6$					
Код Гилберта (γ = 2, ρ = 5)	85	13	0	4	1
Случайный код	85	12	7	5	0,95
Код Гилберта (γ = 3, ρ = 8)	136	16	0	4	1
Случайный код	136	19	9	6	0,97

Заключение

Рассмотрена задача построения множества информационных совокупностей минимального диаметра, состоящего из возможно меньшего числа элементов, для кодов Гилберта и их расширения для исправления пакетов ошибок.

Выполнен анализ возможности нахождения информационных совокупностей диаметром k. Показано, что для простых значений размера блока m кодов Гилберта любые k последовательных позиций являются информационной совокупностью. Это позволило предложить методику выбора плотных информационных совокупностей, количество которых можно примерно оценить, как $2\rho/3$, т. е. их число не зависит от длины кода.

Для расширенных кодов Гилберта было выявлено, что для простых значений m существует в точности ρ информационных совокупностей диаметром k. Предложена процедура выбора плотных информационных совокупностей, отстоящих друг от друга на $\rho - 2$ блока, для исправления любого пакета ошибок в пределах корректирующей способности кода достаточно $\lceil \rho/2 \rceil$ информационных совокупностей.

Полученные результаты позволяют проводить декодирование рассмотренных кодов с низкой сложностью и гарантированным исправлением однократных пакетов ошибок в пределах корректирующей способности кода.

Литература

1. Величко В.В., Попков Г.В., Попков В.К. Модели и методы повышения живучести современных систем связи. М.: Горячая линия–Телеком, 2014. 270 с.
2. Нетес В.А. Основы теории надежности. М.: Горячая линия–Телеком, 2024. 102 с.
3. Половко А.М., Гуров С.В. Основы теории надежности. СПб: БХВ-Петербург, 2006. 704 с.
4. Bogatyrev A.V., Bogatyrev V.A., Bogatyrev S.V. The probability of timeliness of a fully connected exchange in a redundant real-time communication system // Proc. of the Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2020. P. 1–4. https://doi.org/10.1109/weconf48837.2020.9131517
5. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Multipath transmission of heterogeneous traffic in acceptable delays with packet replication and destruction of expired replicas in the nodes that make up the path // Communications in Computer and Information Science. 2023. V. 1748. P. 104–121. https://doi.org/10.1007/978-3-031-30648-8_9

References

1. Velichko V.V., Popkov G.V., Popkov V.K. *Models and Methods of Increasing the Survivability of Modern Communication Systems*. Moscow, Hotline–Telecom, 2014, 270 p. (in Russian)
2. Netes V.A. *Fundamentals of Reliability Theory*. Moscow, Hotline–Telecom, 2024, 102 p. (in Russian)
3. Polovko A.M., Gurov S.V. *Fundamentals of Reliability Theory*. St. Petersburg BHV- Petersburg, 2006, 704 p. (in Russian)
4. Bogatyrev A.V., Bogatyrev V.A., Bogatyrev S.V. The probability of timeliness of a fully connected exchange in a redundant real-time communication system. *Proc. of the Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, 2020, pp. 1–4. https://doi.org/10.1109/weconf48837.2020.9131517
5. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Multipath transmission of heterogeneous traffic in acceptable delays with packet replication and destruction of expired replicas in the nodes that make up the path. *Communications in Computer and Information Science*, 2023, vol. 1748, pp. 104–121. https://doi.org/10.1007/978-3-031-30648-8_9

6. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. Control of multipath transmissions in the nodes of switching segments of reserved paths // Proc. of the International Conference on Information, Control, and Communication Technologies (ICCT). 2022. P. 1–5. https://doi.org/10.1109/ICCT56057.2022.9976839
7. Lin S., Li J. Fundamentals of Classical and Modern Error-Correcting Codes. Cambridge, Cambridge University Press, 2022. 840 p.
8. Moon T.K. Error correction coding: Mathematical methods and algorithms. Wiley, 2020. 992 p.
9. Kulhandjian M., Kulhandjian H., D'Amours C. Improved soft decoding of Reed-Solomon codes on Gilbert-Elliott channels // Proc. of the IEEE International Symposium on Information Theory (ISIT). 2019. P. 1072–1076. https://doi.org/10.1109/ISIT.2019.8849456
10. Xiao X., Vasic B., Lin S., Li J., Abdel–Ghaffar K. Quasi-cyclic LDPC codes with parity-check matrices of column weight two or more for correcting phased bursts of erasures // IEEE Transactions on Communications. 2021. V. 69. N 5. P. 2812–2823. https://doi.org/10.1109/TCOMM.2021.3059001
11. Li L., Lv J., Li Y., Dai X., Wang X. Burst error identification method for LDPC coded systems // IEEE Communications Letters. 2024. V. 28. N 7. P. 1–5. https://doi.org/10.1109/LCOMM.2024.3391826
12. Yang M., Pan Z., Djordjevic I.B. FPGA-based burst-error performance analysis and optimization of regular and irregular SD-LDPC codes for 50G-PON and beyond // Optics Express. 2023. V. 31. N 6. P. 10936–10946. https://doi.org/10.1364/OE.477546
13. Aharoni Z., Huleihel B., Pfister H.D., Permuter H.H. Data-Driven polar codes for unknown Channels with and without memory // Proc. of the IEEE International Symposium on Information Theory (ISIT). 2023. P. 1890–1895. https://doi.org/10.1109/ISIT54713.2023.10206663
14. Fang Y., Chen J. Decoding polar codes for a generalized Gilbert-Elliott channel with unknown parameter // IEEE Transactions on Communications. 2021. V. 69. N 10. P. 6455–6468. https://doi.org/10.1109/TCOMM.2021.3095195
15. Ghaddar N., Kim Y.-H., Milstein L.B., Ma L., Yi B.K. Joint channel estimation and coding over channels with memory using polar codes // IEEE Transactions on Communications. 2021. V. 69. N 10. P. 6575–6589. https://doi.org/10.1109/TCOMM.2021.3098822
16. Ovchinnikov A.A., Veresova A.M., Fominykh A.A. Decoding of linear codes for single error bursts correction based on the determination of certain events // Information and Control Systems. 2022. N 6. P. 41–52. https://doi.org/10.31799/1684-8853-2022-6-41-52
17. Исаева М.Н., Овчинников А.А. Исправление одиночных пакетов ошибок за пределами корректирующей способности кода с использованием информационных совокупностей // Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24. № 1. С. 70–80. https://doi.org/10.17586/2226-1494-2024-24-1-70-80
18. Исаева М.Н. Поиск информационных совокупностей при исправлении пакетов ошибок квазициклическими кодами // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17. № 7. С. 4–12. https://doi.org/10.36724/2072-8735-2023-17-7-4-12
19. Крук Е.А., Овчинников А.А. Точная корректирующая способность кодов Гилберта при исправлении пакетов ошибок // Информационно-управляющие системы. 2016. № 1(80). С. 80–87. https://doi.org/10.15217/issn1684-8853.2016.1.80
20. Veresova A., Ovchinnikov. Burst detection and correction for Gilbert Codes and its QC-LDPC extensions // Proc. of the IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). 2024. P. 47–51. https://doi.org/10.1109/SIBIRCON63777.2024.10758475
21. Исаева М.Н. Разработка и анализ методики построения множества плотных информационных совокупностей для исправления пакетов ошибок // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18. № 10. С. 20–26. https://doi.org/10.36724/2072-8735-2024-18-10-20-26
22. Крук Е.А., Федоренко С.В. Декодирование по обобщенным информационным совокупностям // Проблемы передачи информации. 1995. Т. 31. № 2. С. 54–61.
23. Barg A., Krouk E., van Tilborg H.C.A. On the complexity of minimum distance decoding of long linear codes // IEEE Transactions on Information Theory. 1999. V. 45. N 5. P. 1392–1405. https://doi.org/10.1109/18.771141
24. Грэхем Р., Кнут Д., Паташник О. Конкретная математика. Основание информатики. М.: Мир, 1998. 703 с.

6. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. Control of multipath transmissions in the nodes of switching segments of reserved paths. *Proc. of the International Conference on Information, Control, and Communication Technologies (ICCT)*, 2022, pp. 1–5. https://doi.org/10.1109/ICCT56057.2022.9976839
7. Lin S., Li J. *Fundamentals of Classical and Modern Error-Correcting Codes*. Cambridge, Cambridge University Press, 2022, 840 p.
8. Moon T.K. *Error Correction Coding: Mathematical methods and algorithms*. Wiley, 2020, 992 p.
9. Kulhandjian M., Kulhandjian H., D'Amours C. Improved soft decoding of Reed-Solomon codes on Gilbert-Elliott channels. *Proc. of the IEEE International Symposium on Information Theory (ISIT)*, 2019, pp. 1072–1076. https://doi.org/10.1109/ISIT.2019.8849456
10. Xiao X., Vasic B., Lin S., Li J., Abdel–Ghaffar K. Quasi-cyclic LDPC codes with parity-check matrices of column weight two or more for correcting phased bursts of erasures. *IEEE Transactions on Communications*, 2021, vol. 69, no. 5, pp. 2812–2823. https://doi.org/10.1109/TCOMM.2021.3059001
11. Li L., Lv J., Li Y., Dai X., Wang X. Burst error identification method for LDPC coded systems. *IEEE Communications Letters*, 2024, vol. 28, no. 7, pp. 1–5. https://doi.org/10.1109/LCOMM.2024.3391826
12. Yang M., Pan Z., Djordjevic I.B. FPGA-based burst-error performance analysis and optimization of regular and irregular SD-LDPC codes for 50G-PON and beyond. *Optics Express*, 2023, vol. 31, no. 6, pp. 10936–10946. https://doi.org/10.1364/OE.477546
13. Aharoni Z., Huleihel B., Pfister H.D., Permuter H.H. Data-Driven polar codes for unknown Channels with and without memory. *Proc. of the IEEE International Symposium on Information Theory (ISIT)*, 2023, pp. 1890–1895. https://doi.org/10.1109/ISIT54713.2023.10206663
14. Fang Y., Chen J. Decoding polar codes for a generalized Gilbert-Elliott channel with unknown parameter. *IEEE Transactions on Communications*, 2021, vol. 69, no. 10, pp. 6455–6468. https://doi.org/10.1109/TCOMM.2021.3095195
15. Ghaddar N., Kim Y.-H., Milstein L.B., Ma L., Yi B.K. Joint channel estimation and coding over channels with memory using polar codes. *IEEE Transactions on Communications*, 2021, vol. 69, no. 10, pp. 6575–6589. https://doi.org/10.1109/TCOMM.2021.3098822
16. Ovchinnikov A.A., Veresova A.M., Fominykh A.A. Decoding of linear codes for single error bursts correction based on the determination of certain events. *Information and Control Systems*, 2022, no. 6. pp. 41–52. https://doi.org/10.31799/1684-8853-2022-6-41-52
17. Isaeva M.N., Ovchinnikov A.A. Correction of single error bursts beyond the code correction capability using information sets. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2024, vol. 24, no. 1, pp. 70–80. (in Russian). https://doi.org/10.17586/2226-1494-2024-24-1-70-80
18. Isaeva M.N. Finding information sets when correcting error bursts with quasi-cyclic codes. *T-Comm*, 2023, vol. 17, no. 7, pp. 4–12. (in Russian). https://doi.org/10.36724/2072-8735-2023-17-7-4-12
19. Krouk E.A., Ovchinnikov A.A. Exact burst-correction capability of Gilbert Codes. *Information and Control Systems*, 2016, no. 1(80), pp. 80–87. (in Russian). https://doi.org/10.15217/issn1684-8853.2016.1.80
20. Veresova A., Ovchinnikov. Burst detection and correction for Gilbert Codes and its QC-LDPC extensions. *Proc. of the IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 2024, pp. 47–51. https://doi.org/10.1109/SIBIRCON63777.2024.10758475
21. Isaeva M.N. Development and analysis of a method for constructing dense information sets for error bursts correction. *T-Comm*, 2024, vol. 18, no. 10, pp. 20–26. (in Russian). https://doi.org/10.36724/2072-8735-2024-18-10-20-26
22. Kruk E.A., Fedorenko S.V. Decoding by generalized information sets. *Problemy Peredachi Informatsii*, 1995, vol. 31, no. 2, pp. 54–61. (in Russian)
23. Barg A., Krouk E., van Tilborg H.C.A. On the complexity of minimum distance decoding of long linear codes. *IEEE Transactions on Information Theory*, 1999, vol. 45, no. 5, pp. 1392–1405. https://doi.org/10.1109/18.771141
24. Graham R.L., Knuth D.E., Patashnik O. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Professional, 1994, 672 p.

Автор

Исаева Мария Николаевна — младший научный сотрудник, Национальный исследовательский университет «Высшая школа экономики», Санкт-Петербург, 190008, Российская Федерация, sc 57243599200, https://orcid.org/0009-0007-6228-0617, misaeva@hse.ru

Author

Maria N. Isaeva — Junior Researcher, HSE University-St. Petersburg, Saint Petersburg, 190008, Russian Federation, sc 57243599200, https://orcid.org/0009-0007-6228-0617, misaeva@hse.ru

Статья поступила в редакцию 10.12.2024
Одобрена после рецензирования 19.01.2025
Принята к печати 27.03.2025

Received 10.12.2024
Approved after reviewing 19.01.2025
Accepted 27.03.2025