ПОИСК ИНФОРМАЦИОННЫХ СОВОКУПНОСТЕЙ ПРИ ИСПРАВЛЕНИИ ПАКЕТОВ ОШИБОК КВАЗИЦИКЛИЧЕСКИМИ КОДАМИ

Исаева Мария Николаевна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия,
imn@guap.ru

DOI: 10.36724/2072-8735-2023-17-7-4-12

Manuscript received 02 June 2023;
Accepted 05 July 2023

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003, "Фундаментальные основы построения помехозащищённых систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга"

Ключевые слова: *помехоустойчивое кодирование, декодирование по информационным совокупностям, квазициклические коды, исправление пакетов ошибок, низкоплотностные коды, каналы с памятью*

В данной статье рассматривается вопрос об оценке вероятности нахождения информационных совокупностях в матрицах блочно-перестановочного и блочно-циркулянтного вида. Традиционно в помехоустойчивом кодировании рассматриваются независимые ошибки, однако, в реальных системах они могут быть сгруппированы и образовывать, так называемый, пакет ошибок. Известные оценки вероятности нахождения информационной совокупности проводятся для случайных матриц, а для исправления пакетов ошибок могут использоваться широко распространенные блочно-перестановочные коды с малой плотностью проверок на четность (LDPC-коды) или блочно-циркулянтные квазициклические коды (QC-коды). Для оценки вероятности нахождения информационных совокупностей использовалось математическое моделирование. Были проведены эксперименты, позволяющие выявить параметры для конкретных конструкций, которые дают наибольшую вероятность нахождения информационных совокупностей. В статье представлены результаты, отражающие определенные особенности в значениях вероятности нахождения информационных совокупностей для матриц различного вида, даны предположения и гипотезы о характере таких особенностей. Была выявлена зависимость наличия информационной совокупности от размера и расположения интервала ее поиска внутри блочно-перестановочной матрицы. Результаты данного исследования могут быть использованы для уменьшения сложности декодирования по информационным совокупностям, которая при рассматривании случайных матриц является экспоненциальной.

Информация об авторе:
Исаева Мария Николаевна, *Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных технологий и систем связи, аспирант, г. Санкт-Петербург, Россия*

Для цитирования:
Исаева М.Н. Поиск информационных совокупностей при исправлении пакетов ошибок квазициклическими кодами // T-Comm: Телекоммуникации и транспорт. 2023. Том 17. №7. С. 4-12.

For citation:
Isaeva M.N. (2023) Finding information sets when correcting error bursts with quasi-cyclic codes. *T-Comm*, vol. 17, no.7, pp. 4-12. (*in Russian*)

Введение

Во времена цифровых технологий ежедневно объем информации, циркулирующий по каналам связи, бесконечно возрастает. Информация касается практически все сферы деятельности человека. Из-за различных причин в каналах связи могут возникать ошибки, которые приводят к искажению двоичной передаваемой последовательности, что при декодировании может изменить суть передаваемого сообщения.

Среди алгоритмов декодирования сообщений существует декодирование по информационным совокупностям, которое способно исправлять ошибки. В теории помехоустойчивого кодирования чаще всего рассматривается исправление независимых ошибок [1-3]. Сложность декодирования по информационным совокупностям в данном случае является экспоненциальной для известных алгоритмов. Однако, в реальных каналах связи ошибки часто сгруппированы внутри передаваемой последовательности и образуют пакеты ошибок. При исправлении пакетов ошибок сложность декодирования по информационным совокупностям может быть заметно уменьшена [4].

Известные оценки вероятности нахождения информационной совокупности проводятся для случайных матриц, а, например, для исправления пакетов ошибок могут использоваться широко распространенные блочно-перестановочные LDPC-коды (коды с малой плотностью проверок на четность) и блочно-циркулянтные квазициклические коды. В данной статье рассматривается вопрос об оценке вероятности нахождения информационной совокупности при исправлении пакетов ошибок.

Декодирование по информационным совокупностям

Информационной совокупностью называется множество $\gamma = \{1 \le j_1 < j_2 < \ldots < j_k \le n\}$, при задании компонент $\alpha_{j_1}, \ldots, \alpha_{j_k}$ однозначно определяющее кодовое слово. Если информационная совокупность свободна от ошибок, то есть не имеет на своих позициях ошибок, то принятое слово может быть восстановлено однозначно [5].

Поиск информационной совокупности в порождающей матрице **G** может быть произведен следующим образом: возьмем произвольные k столбцов этой матрицы и составим новую матрицу $\mathbf{M}_\gamma$. Позиции взятых k столбцов будут являться информационной совокупностью γ в том случае, если матрица $\mathbf{M}_\gamma$ будет невырожденной, то есть ее ранг будет равен числу k. Также для $\mathbf{G}_\gamma = \mathbf{M}^{-1} \cdot \mathbf{G}$ на позициях γ должна образоваться единичная матрица.

Для того, чтобы верно декодировать принятое слово, необходимо, чтобы информационная совокупность была свободна от ошибок, для этого необходимо знать минимальное расстояние кода [6]. Если такой возможности нет, то можно провести полный перебор по всему множеству информационных совокупностей. При этом сложность подобного алгоритма будет экспоненциальной. Ниже приведен такой алгоритм декодирования:

1. Генерируется множество информационных совокупностей $\Gamma = \{\gamma_1, \ldots, \gamma_N\}$.

2. По множеству информационных совокупностей формируется множество матриц $\{\mathbf{G}_{\gamma_1}, \ldots, \mathbf{G}_{\gamma_N}\}$.

3. При декодировании принятого слова **b** необходимо осуществить перебор по всем матрицам $\{\mathbf{G}_{\gamma_1}, \ldots, \mathbf{G}_{\gamma_N}\}$, и вычислить на каждой итерации $\mathbf{z}_i = \mathbf{b}(\gamma_i) \cdot \mathbf{G}_{\gamma_i}$, где $\mathbf{b}(\gamma_i)$ – элементы из принятого слова **b** на позициях γ_i.

4. Для каждого $\mathbf{z}_i$ проверяется условие $d(\mathbf{z}_i, \mathbf{b}) \le w_{\min}$, где $d(\mathbf{z}_i, \mathbf{b})$ – расстояние Хэмминга. Если оно выполняется, то $\mathbf{z}_{\min} = \mathbf{z}_i$ и $w_{\min} = d(\mathbf{z}_i, \mathbf{b})$.

5. После того, как был осуществлен перебор по всем информационным совокупностям, принимается решение $\hat{\mathbf{a}} = \mathbf{z}_{\min}$, где $\hat{\mathbf{a}}$ – декодированное слово.

Данный алгоритм актуален при исправлении независимых ошибок. В случае рассмотрения пакетов ошибок необходимо использовать соответствующую метрику, связанную с пакетами (вместо минимального расстояния).

При передаче по каналам с памятью типичная конфигурация ошибок описывается не м помощью их количества, а с помощью понятия пакета ошибок. Пакетом ошибок называется вектор длиной b, в котором первый и последний ненулевой элемент располагаются не далее, чем на b позиций друг от друга. Пакет ошибок может быть циклическим: начинаться в конце принятого слова и заканчиваться в его начале.

При декодировании пакета ошибок все ошибочные позиции группируются и это может быть учтено при поиске информационных совокупностей: при выборе информационной совокупности можно ограничивать поиск k ее элементов позициями, не входящими в предполагаемое расположение пакета. Так как на k подряд идущих позициях может не оказаться информационной совокупности, будем расширять интервал поиска на некоторую величину Δ, таким образом осуществляя поиск информационной совокупности на k +Δ подряд идущих позициях. Поэтому область поиска информационной совокупности также образует собой замкнутый интервал некоторой длины k +Δ (рис. 1).

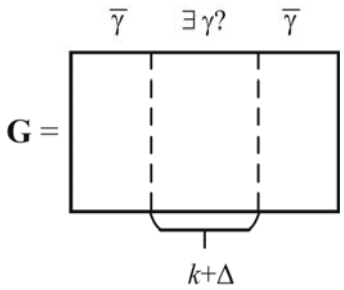

Рис. 1. Поиск информационной совокупности в порождающей матрице **G** на случайных позициях в замкнутом интервале длиной k +Δ

При этом для сокращения числа информационных совокупностей имеет смысл выбирать длину интервала как можно меньшей, то есть значение Δ следует минимизировать.

Известно, что вероятность того, что случайная матрица **M** размера $k \times (k+\Delta)$ будет иметь полный ранг оценивается как [7]:

$$P(rank(\mathbf{M}_{k,k+\Delta}) = k) = Q_\Delta = \prod_{i=\Delta+1}^{\infty}\left(1-\frac{1}{2^i}\right), \Delta \geq 0. \quad (1)$$

Из данной формулы получим, что для Δ=0 значение этой вероятности будет:

$$Q_0 = \prod_{j=1}^{\infty}\left(1-\frac{1}{2^j}\right) = 0,288788... \approx 0,29. \quad (2)$$

С помощью формулы (2) можно посчитать среднее значение Δ:

$$\overline{\Delta} = \sum_{\Delta=0}^{\infty} \Delta \cdot P_\Delta = \sum_{i=0}^{\infty}(1-Q_i) = 1,6066... \approx 1,6. \quad (3)$$

Однако, структура порождающих и проверочных матриц, практически используемых помехоустойчивых кодов может быть далека от случайной. С учетом дополнительного ограничения на интервал поиска при исправлении пакетов ошибок формулы (1), (2) могут оказаться некорректными. Возникает задача оценки вероятности нахождения информационной совокупности с учетом сформулированных ограничений.

Коды с малой плотностью проверок на четность

В настоящей статье в качестве помехоустойчивых кодов рассмотрим коды с малой плотностью проверок на четность, или LDPC-коды. Применение этих кодов для исправления пакетов ошибок рассматривалось, например, в [8-10].

LDPC-коды в 1962 году предложил Р. Галлагер [11]. Такие коды задаются с помощью разреженной проверочной матрицы **H**. Данные коды можно задать на основе блочно-перестановочной конструкции. Такую конструкцию можно описать через базовую матрицу $\mathbf{H_b}$, представленную в формуле (4).

$$\mathbf{H_b} = \begin{bmatrix} t_{11} & \cdots & t_{1\rho} \\ \vdots & \ddots & \vdots \\ t_{\gamma 1} & \cdots & t_{\gamma\rho} \end{bmatrix}, \quad (4)$$

где t_{ij} – степени матрицы циклической перестановки, которые задают блоки $\mathbf{C}^{t_{ij}}$ проверочной матрицы **H**. Размер этих блоков – *m* на *m*, количество блоков – γ на ρ. Структура проверочной матрицы представлена ниже.

$$\mathbf{H} = \begin{bmatrix} \mathbf{C}^{t_{11}} & \mathbf{C}^{t_{12}} & \cdots & \mathbf{C}^{t_{1\rho}} \\ \mathbf{C}^{t_{21}} & \mathbf{C}^{t_{22}} & \cdots & \mathbf{C}^{t_{2\rho}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{C}^{t_{\gamma 1}} & \mathbf{C}^{t_{\gamma 2}} & \cdots & \mathbf{C}^{t_{\gamma\rho}} \end{bmatrix}. \quad (5)$$

Можно обратить внимание, что в матрице вида (5) столбцы двух подряд идущих блоков в сумме всегда образуют нулевой столбец. Это может влиять на поиск информационной совокупности в подряд идущих позициях.

Классическим способом поиска информационных совокупностей является нахождение позиций *k* линейно независимых столбцов, образующих невырожденную подматрицу размера *k*×*k* порождающей матрицы размера *k*×*n*. Однако, поиск информационных совокупностей может быть осуществлен и по проверочной матрице следующим образом: если в проверочной матрице размера *r*×*n* найдены *r* позиций столбцов, образующих невырожденную подматрицу размера *r*×*r*, то эти позиции образуют дополнение: $\gamma \cup \overline{\gamma} = \{1,\ldots,n\}$.

Использование проверочной матрицы вместо порождающей для поиска информационных совокупностей может быть более вычислительно эффективным для кодов со скоростью $R > 1/2$ (рис. 2).

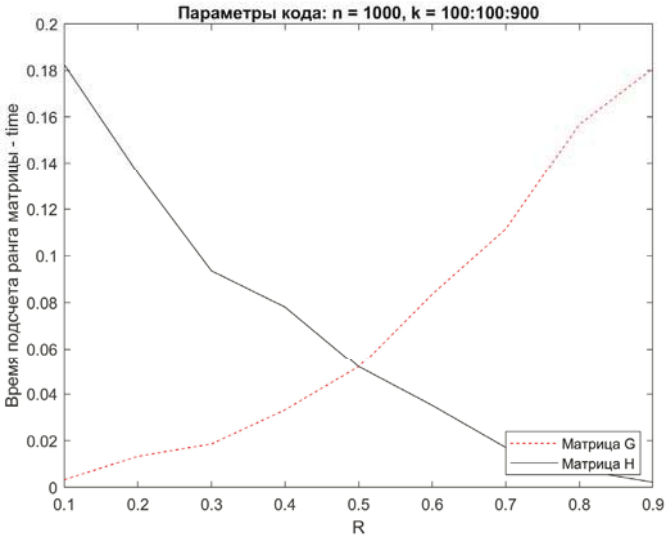

Рис. 2. График зависимости времени подсчета ранга случайных матриц от скорости кода для порождающих и проверочных матриц

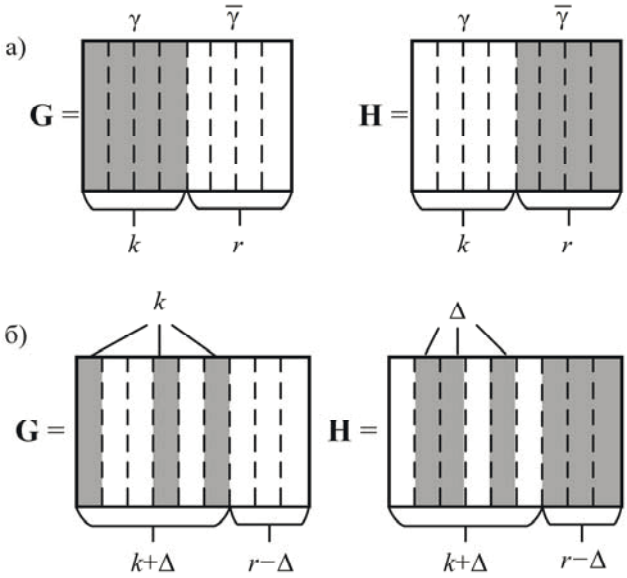

Рис. 3. Схема поиска информационных совокупностей в порождающей матрице **G** и проверочной матрице **H**: а) при Δ = 0; б) при Δ ≠ 0

На рисунке 3, а) и 3, б) представлена схема поиска информационных совокупностей, демонстрирующая соответствие между порождающей матрицей **G** и проверочной матрицей **H**. Соответствующие линейно независимые столбцы порождающей и проверочной матриц обозначены серым цветом.

Поиск информационной совокупности

Рассмотрим случайные блочно-перестановочные конструкции, в которых блоки являются матрицей циклической перестановки, t_{ij} выбираются равномерно из интервала [0:m - 1]. Количество блоков $\gamma = [2; 3; 4]$ (рассматривается несколько случаев) и $\rho = 6$ (значение фиксировано), размер блоков $m = 11$. Кроме этого, будем рассматривать случайные матрицы схожего размера $k = 22$, $n = 66$, в которых ненулевые элементы располагаются с вероятностью 0,5, чтобы проверить правильность выражения (2).

На рисунке 4 изображен график вероятности нахождения информационных совокупностей при Δ=0. Обратим внимание, что при значении $\gamma = 3$ на графике присутствуют только некоторые пики, которые возникают на позициях конца блоков блочно-перестановочной проверочной матрицы. Как говорилось выше, столбцы двух подряд идущих блоков всегда линейно зависимы, таким образом, если интервал поиска невырожденной матрицы содержит в себе два блока целиком – такая матрица всегда вырождена. При длине интервала равного $3m$–1 вероятность этого события равна единице. Также, как можно заметить, значение вероятности для случайной матрицы колеблется в районе отметки 0,3, что соответствует значению из формулы (2).

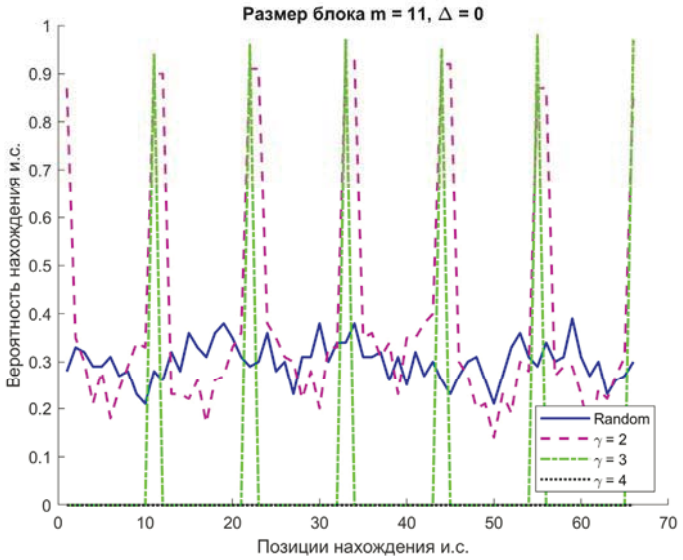

Рис. 4. График вероятности нахождения информационной совокупности при $\Delta = 0$ для случайных матриц размера $k = 22$, $n = 66$ и для блочно-перестановочных матриц с размерами: $\gamma = 2$, $\rho = 6$; $\gamma = 3$, $\rho = 6$; $\gamma = 4$, $\rho = 6$

Рассмотрим интервал длиной $3m$–2, тогда существует единственно возможное положение интервала, не включающее два подряд идущих блока (рис. 5). Оценим параметры кодов для этого случая. Будем считать, что поиск производится по проверочной матрице **H** и рассматриваются интервалы длины r, где r – ранг матрицы **H**.

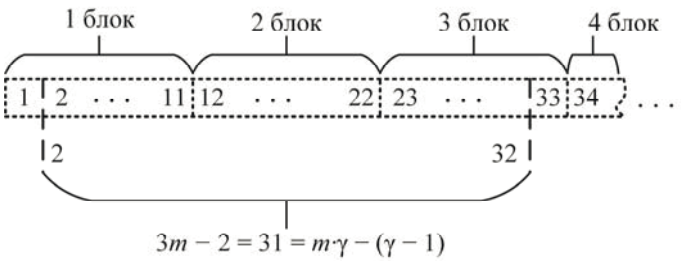

Рис. 5. Схема случая, при котором находится информационная совокупность для $\gamma = 3$, $\rho = 6$ и $\Delta = 0$

В блочно-перестановочной конструкции ранг проверочной матрицы не превышает $m \cdot \gamma - (\gamma - 1)$. Случай, изображенный на рисунке 5 невозможен при длине интервала r превышающего $3m - 2$, тогда $m \cdot \gamma - (\gamma - 1) \geq 3m - 1$, отсюда

$$\gamma \geq \frac{3m-2}{m-1}. \qquad (6)$$

Функция в правой части (6) равна 4 при $m = 2$ и монотонно убывает с ростом m. Таким образом, при $\gamma \geq 4$ блочно-перестановочная конструкция (5) не имеет информационных совокупностей из подряд идущих позиций. При $\gamma = 3$ такая информационная совокупность возможна только для случая из Рисунка 3, при $\gamma = 2$, с учетом $rank(\mathbf{H}) = r = 2m - 1$, попадание $2m$ подряд идущих столбцов в окно размером r невозможно. Это объясняет форму всех кривых на рисунке 4.

Теперь рассмотрим, как изменятся формы кривых, если $\Delta \neq 0$. На Рисунке 6 представлен график вероятности нахождения информационных совокупностей при $\Delta = 1$ для блочно-перестановочных матриц с размерами: $\gamma = 2$, $\rho = 6$; $\gamma = 3$, $\rho = 6$; $\gamma = 4$, $\rho = 6$.

Если сравнить график на рисунках 4 и 6, то можно заметить, что для матрицы с размерами $\gamma = 2$, $\rho = 6$ вероятность нахождения информационных совокупностей на позициях конца блоков и остальных позициях стремятся друг другу, то есть становятся более равномерными. Для остальных блочно-перестановочных матриц значимых изменений пока не наблюдается, а для случайной вероятность все так же находится в пределах значения 0,3.

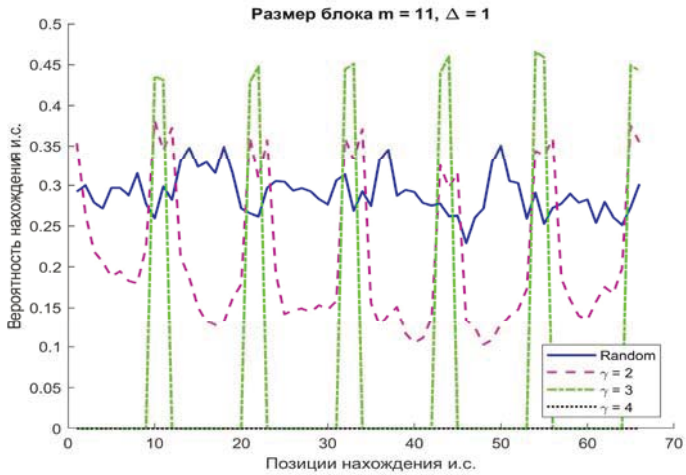

Рис. 6. График вероятности нахождения информационных совокупностей при $\Delta = 1$

На рисунке 7 представлен график вероятности нахождения информационных совокупностей при Δ = 5, а на рисунке 8 – график вероятности нахождения информационных совокупностей при Δ = 10.

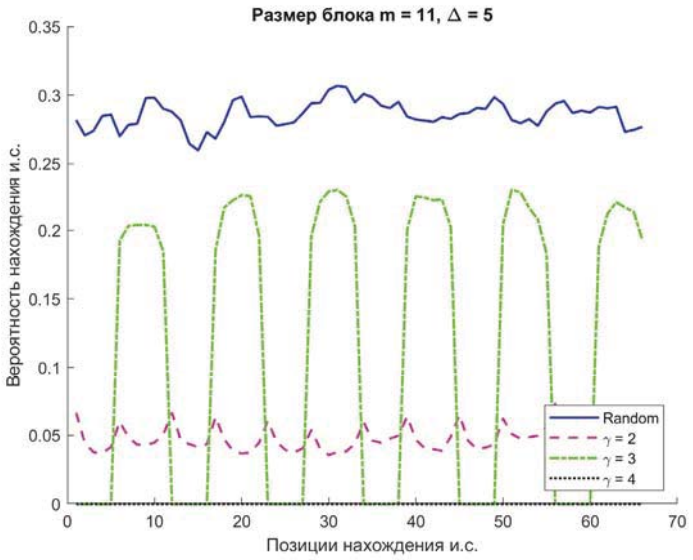

Рис. 7. График вероятности нахождения информационных совокупностей при Δ = 5

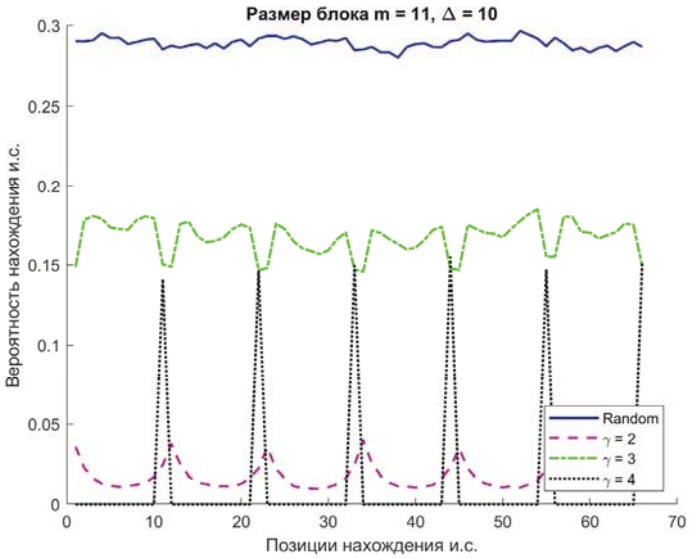

Рис. 8. График вероятности нахождения информационных совокупностей при Δ = 10

Как можно заметить из рисунков 7 и 8 для матрицы с размером γ = 2; ρ = 6 последующее увеличение Δ приводит к уменьшению вероятности нахождения информационной совокупности, что говорит о том, что после какого-то определенного значения, нет смысла увеличивать Δ. Для блочно-перестановочной матрицы с размером γ = 3; ρ = 6 с увеличением Δ вероятность нахождения информационной совокупности появляется не только в позициях конца блоков, но и на других – график становится более равномерным. Для γ = 4; ρ = 6 до значения Δ = 10 вероятность найти информационную совокупность была нулевой. Как только Δ приблизилась к размеру блока *m*, появились характерные пики в районе позиций на концах блока.

Рассмотрим еще один график, изображенный на рисунке 9, чтобы проверить дальнейшие изменение графика для блочно-перестановочной матрицы с размером γ = 4; ρ = 6.

При значении Δ = 20 для γ = 2; ρ = 6 вероятность нахождения информационных совокупностей стремится к нулю. Для γ = 3; ρ = 6, очевидно, вероятность начинает уменьшаться, что говорит о том, что дальнейшее увеличение бессмысленно, а для γ = 4; ρ = 6, наоборот, вероятность нахождения информационных совокупностей выросла, даже относительно пиков из предыдущего графика.

Также стоит отметить, что для любых значений Δ, представленных на графиках, вероятность нахождения информационных совокупностей для случайной матрицы продолжает колебаться на уровне 0,3, что подтверждает выражение (2).

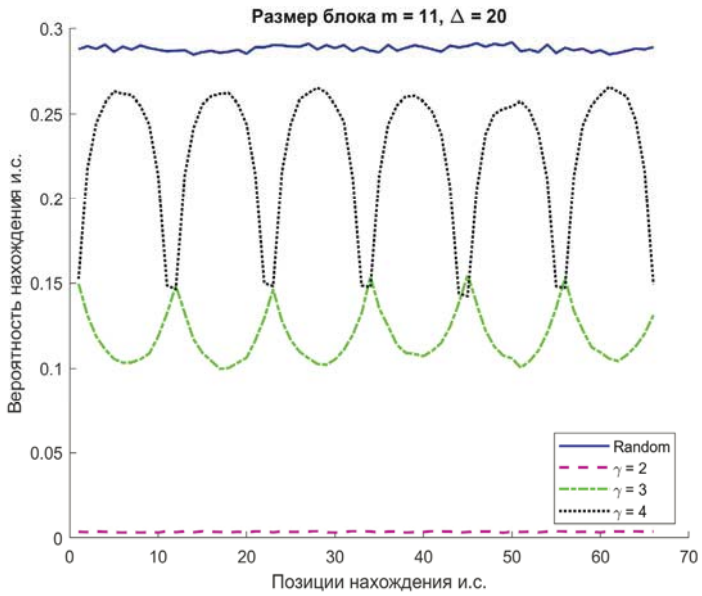

Рис. 9. График вероятности нахождения информационных совокупностей при Δ = 20

Исходя из приведенных графиков, можно сделать следующий вывод: для разных размеров блочно-перестановочных матриц существует свое определенное значение Δ, при котором вероятность нахождения информационной совокупности будет максимальной, причем не только на концах блоков. Для подобных матриц можно получить свое среднее значение Δ, аналогичное полученному в выражении (3) для случайных матриц.

Для матриц, где γ = 2, самая высокая вероятность из приведенных графиков была при Δ = 1. Для матриц, у которых γ = 3, наиболее высокая вероятность была при Δ=1, но только в тех случаях, когда для поиска информационных совокупностей рассматривались позиции, находящиеся в конце блоков. При Δ=10 график зависимости вероятности нахождения информационной совокупности стал похож на равномерный, однако само значение вероятности было значительно ниже, чем при Δ = 1.

Для матриц, у которых γ = 4, при значении Δ >20 график стремится к графику случайной матрицы и становится более равномерным, однако, для матриц, у которых γ = 2 и γ = 3, в данном случае вероятность стремится к нулю.

Квазициклические коды

Квазициклические (quasi-cyclic – QC) коды могут быть заданы аналогично LDPC-кодам с помощью проверочной матрицы вида (5). Каждый блок такой матрицы – циклический сдвиг первой строки, называемый циркулянтом, при этом вес строки может быть больше единицы [12-14]. Рассмотрим блочно-циркулянтные матрицы различного веса t, с размером блока $m = 11$ и размерами: 1 циркулянт, 2×2 и 3×3.

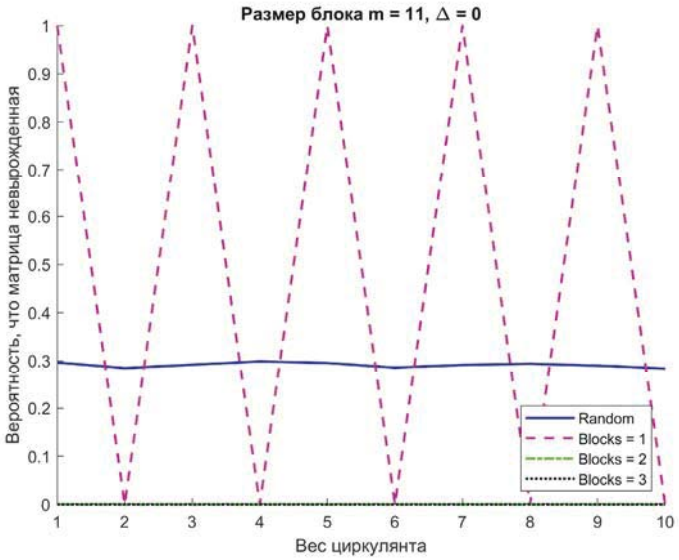

Рис. 10. График вероятности невырожденности для блочно-циркулянтных матриц разного размера и случайной матрицы размера $k = 22$, $n = 66$

Из рисунка 10 видно, что для матриц 2×2 и 3×3 вероятность того, что матрица будет невырожденная всегда равна нулю, а для одного блока циркулянта – она зависит от четности веса.

Таким образом, можно подытожить, что если размер циркулянта m – простой, то для четного веса циркулянта t – матрица всегда будет вырожденная, а для нечетного – всегда невырожденная. Если рассматривать блоки 2×2 – матрица будет всегда вырожденная, так как у нее всегда четное число строк и столбцов. Если рассматривать блоки 3×3 – матрица будет всегда вырожденная, так как есть $2m$ строк четного веса.

Если размер циркулянта – составное число, то для блоков 2×2 и 3×3 справедливо то же самое утверждение, что указано выше. Для одного блока: если вес t четный, то матрица всегда вырождена, если нечетный – то может быть вырождена или невырождена. Таким образом, однозначно можно сделать вывод, что для четного веса циркулянта матрица всегда будет вырождена.

Рассмотрим пример, похожий на пример с блочно-перестановочными конструкциями. Зафиксируем вес циркулянта t =3, размер блока $m = 11$, размеры матрицы $\gamma = 2$, $\rho = 6$; $\gamma = 3$, $\rho = 6$; $\gamma = 4$, $\rho = 6$. Размер циркулянта был выбран как минимальное простое число, иначе матрица будет по свойствам больше походить на случайную, чем блочно-циркулянтную.

На рисунке 11 представлен график вероятности нахождения информационной совокупности для блочно-циркулянтных матриц. Для наглядности также приведен график для случайной матрицы.

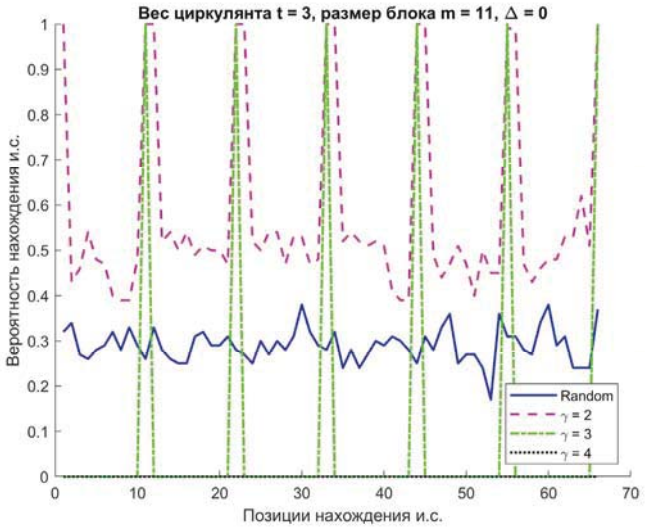

Рис. 11. График вероятности нахождения информационных совокупностей при Δ = 0 для блочно-циркулянтных матриц

Очевидно, что график на рисунке 11 напоминает по своему виду график на рисунке 4. Однако, при увеличении значения Δ разница становится более очевидной.

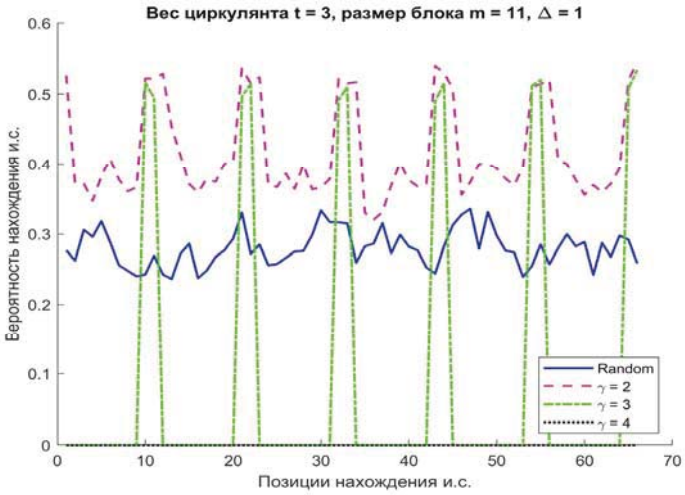

Рис. 12. График вероятности нахождения информационных совокупностей при Δ = 1 для блочно-циркулянтных матриц

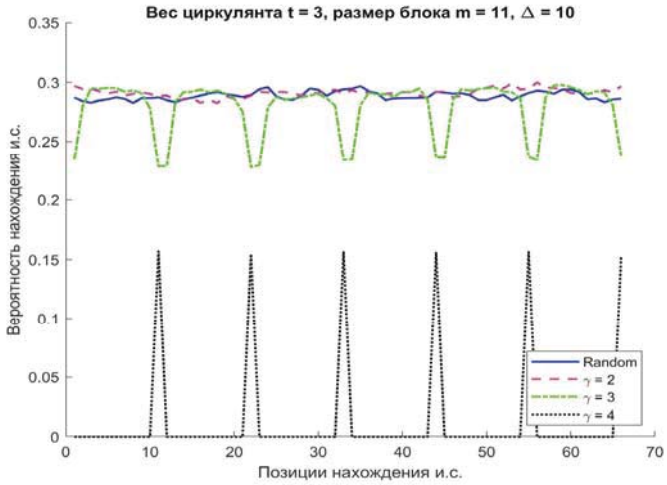

Рис. 13. График вероятности нахождения информационных совокупностей при Δ = 10 для блочно-циркулянтных матриц

На рисунке 12 можно заметить, как график вероятности нахождения информационных совокупностей блочно-циркулянтной матрицы стремится к графику случайно матрицы. Пики, которые были характерны для блочно-перестановочной конструкции, здесь также присутствуют. На рисунке 13 при $\Delta = 10$ можно заметить, как графики вероятности для размеров блочно-циркулянтных матриц $\gamma = 2$, $\rho = 6$ и $\gamma = 3$, $\rho = 6$ становятся более равномерными и близкими к графику случайно матрицы, а для матрицы с размерами $\gamma = 4$, $\rho = 6$ появились характерные пики в районе конца блока.

На рисунке 14 показано, как изменяются графики, если увеличить значение Δ до 20. В отличие от блочно-перестановочной матрицы, для блочно-циркулянтной матрицы значение вероятности с увеличением Δ не падает, а становится более равномерным и колеблется в районе вероятности для случайно матрицы. При дальнейшем увеличении Δ, график вероятности для матрицы с размерами $\gamma = 4$, $\rho = 6$ примет такой же вид и будет колебаться в районе ≈0,28. Для данного типа матриц, очевидно, также возможно найти среднее значение Δ, аналогично выражению (3), где приведено среднее значение Δ для случайных матриц.

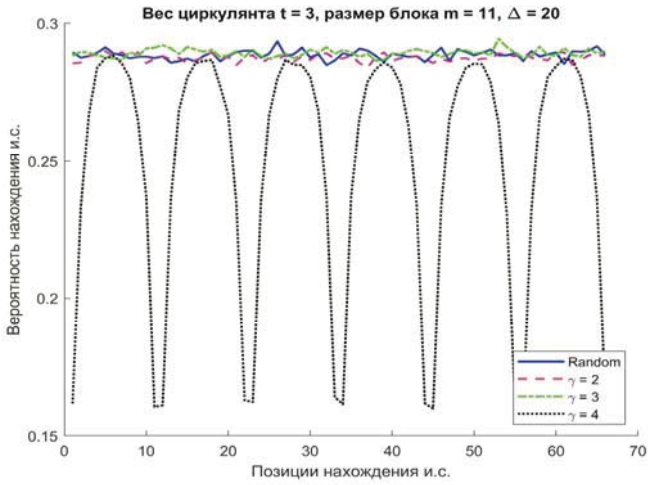

Рис. 14. График вероятности нахождения информационных совокупностей при $\Delta = 20$ для блочно-циркулянтных матриц

В соответствии с утверждением, что блочно-циркулянтные матрицы с числом блоков 2×2 и 3×3 всегда вырождены, если там либо все блоки нечетного веса, либо все блоки четного, рассмотрим блоки, в которых чередуется четный и нечетный вес циркулянта. В ходе экспериментов, было определено, что даже в этом случае такие конструкции не могут быть невырожденными, потому что циркулянт четного веса всегда вырожден, т.к. сумма строк или столбцов всегда будет равна 0. Циркулянт нечетного веса может быть невырожденным, но, если идут два рядом (даже чередуясь через один четный), он всегда вырожденный.

Рассмотрим блочно-циркулянтную матрицу другого вида, изображенной на рисунке 15. Размер такой матрицы 2×4.

Н	Ч	Н	Ч
Ч	Н	Ч	Н

Рис. 15. Схема блочно-циркулянтной матрицы, где Н – циркулянты нечетного веса, Ч – циркулянты четного веса

На рисунке 16 представлен график вероятности нахождения информационной совокупности в матрице вида, представленного на Рисунке 15. Вес циркулянта каждый раз случайный, но проверялся на четность/нечетность. Из графика можно сделать вывод, что при увеличении значения Δ вероятность становится более равномерной и в любой позиции будет равна примерно 0,3. Однако, как можно заметить, для меньшей Δ эта вероятность выше, хоть и заметны пиковые значения на концах блока.

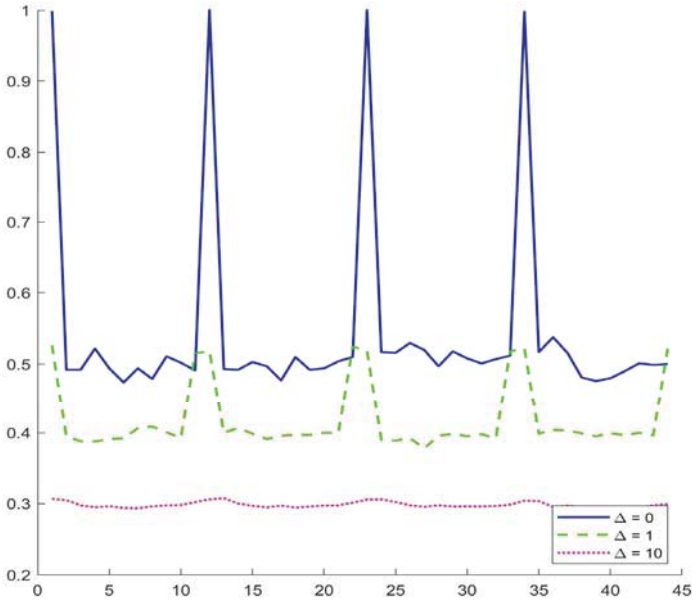

Рис. 16. График зависимости вероятности нахождения информационных совокупностей при различных Δ для блочно-циркулянтных матриц от позиций начала поиска информационных совокупностей

Исходя из графиков, приведенных выше, можно заметить, что независимо от количества циркулянтов (значений γ) при одинаковом весе циркулянтов, вероятность нахождения информационных совокупностей с увеличением Δ стремится к значению вероятности для случайных матриц. Для матриц, у которых количество циркулянтов $\gamma = 2$ необходимо увеличить Δ до 10, для $\gamma = 3$ до 20, а для $\gamma = 4$ до 30. При этом, можно использовать особую структуру построения блочно-циркулянтной матрицы (чередовать четные и нечетные веса), при которых будет сравнительно высокая вероятность нахождения информационных совокупностей, однако, на разных позициях поиска она будет разной.

Заключение

В данной статье была рассмотрена и оценена вероятность нахождения информационных совокупностей для кодов с малой плотностью проверок на четность и квазициклических кодов. Приведены соответствия между порождающей и проверочной матрицами для поиска информационных совокупностей. Были приведены значения Δ, при которых график вероятности нахождения информационных совокупностей достигает своих наивысших значений при различных параметрах матриц. Были найдены и обоснованы закономерности, которые примечательны для матриц, имеющих блочную структуру.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003, «Фундаментальные основы построения помехозащищённых систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга».

Литература

1. *Moon T.K.* Error correction coding: Mathematical methods and algorithms. Wiley, 2020 992 p.

2. *Lin S., Li J.* Fundamentals of Classical and Modern Error-Correcting Codes. Cambridge: Cambridge University Press; 2022, 840 p.

3. *Gazi O.* Forward error correction via channel coding. Cham, Springer, 2020 319 p.

4. *Исаева М.Н., Овчинников А.А.* О применении декодирования по информационным совокупностям при исправлении пакетов ошибок // Радиотехнические, оптические и биотехнические системы. Устройства и методы обработки информации: Четвертая Всерос. Науч. Конф.: сб. докл. СПб.: ГУАП, 2023. С. 188-191.

5. *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. doi:10.31799/1684-8853-2022-6-41-52

6. *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, vol. 45, no. 5, pp. 1392-1405, July 1999, doi: 10.1109/18.771141.

7. *Berlekamp E.R.* The technology of error correcting codes // Proc. IEEE, vol. 68, pp. 564-593, 1980.

8. *Ryan W., Lin S.* Channel Codes: Classical and Modern. New York: Cambridge University Press, 2009. 710 p.

9. *Veresova A.M., Ovchinnikov A.A.* About one algorithm for correcting bursts using block-permutation LDPC-codes // 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2019 P. 1-4.

10. *Krouk E.A., Ovchinnikov A.A.* Block-permutation LDPC codes for distributed storage systems // Smart Innovation, Systems and Technologies. 2015 Vol. 40, pp. 227-238.

11. *Gallager R.G.* Low-Density Parity-Check Codes // IRE Transactions on Information Theory. Jan. 1962. Vol. 8. No. 1, pp. 21-28.

12. *Baldi M.* QC-LDPC Code-Based Cryptography. Springer, 2014. 120 p.

13. *Xiao X., Vasić 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, May 2021. Vol. 69, no. 5, pp. 2812-2823. doi:10.1109/TCOMM.2021.3059001

14. *Fossorier M.P.C.* Quasi-cyclic low-density parity-check codes from circulant permutation matrices // IEEE Transactions on Information Theory. 2004. Vol. 50 Iss. 8, pp. 1788-1793. DOI:10.1109/TIT.2004.831841

FINDING INFORMATION SETS WHEN CORRECTING ERROR BURSTS WITH QUASI-CYCLIC CODES

Maria N. Isaeva, *Saint-Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia,* ***imn@guap.ru***

Abstract

This article discusses the question of assessing the probability of finding information sets in block-permutation and block-circulant matrices. Traditionally, interference-resistant coding is considered independent errors, however, in real systems they can be grouped and generate a so-called error burst. Known estimates of the probability of finding information sets are conducted for random matrices, and for correcting error bursts widespread block-permutation low density parity check codes (LDPC-codes) or block-circulant quasi-cyclic codes (QC-codes) can be used. To estimate the probability of finding information sets mathematical modeling was used. Experiments have been carried out to identify parameters for specific structures that give the greatest probability of finding information sets. The article presents the results reflecting certain features in the values of the probability of finding information sets for matrices of different types, given assumptions and hypotheses about the features. Dependence of the presence of an information set from the size and location of its search interval inside the block permutation matrix was identified. The results of this research may be used to reduce the complexity of decoding by information sets, which, when considering random matrices, is exponential.

Keywords: *noise-resistant coding, decoding by information sets, quasi-cyclic codes, error burst correction, low-density codes, channels with memory.*

References

1. T. K. Moon. Error correction coding: Mathematical methods and algorithms. Wiley, 2020 992 p.

2. S. Lin, J. Li. Fundamentals of Classical and Modern Error-Correcting Codes. Cambridge: Cambridge University Press; 2022, 840 p.

3. O. Gazi. Forward error correction via channel coding. Cham, Springer, 2020 319 p.

4. M.N. Isaeva, A.A. Ovchinnikov. About using of decoding by information sets when correcting error bursts. *Radiotekhnicheskiye. opticheskiye i biotekhnicheskiye sistemy. Ustroystva i metody obrabotki informatsii: IV All-Russian scientific conference: collection of reports*. SPb.:SUAI, 2023, pp. 188-191. (In Russian)

5. A. A. Ovchinnikov, A. M. Veresova, A. A. Fominykh. Decoding of linear codes for single error bursts correction based on the determination of certain events. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 6, pp. 41-52. doi:10.31799/1684-8853-2022-6-41-52
6. A. Barg, E. Krouk and H. C. A. van Tilborg, "On the complexity of minimum distance decoding of long linear codes," *IEEE Transactions on Information Theory,* vol. 45, no. 5, pp. 1392-1405, July 1999, doi: 10.1109/18.771141.
7. E. R. Berlekamp, The technology of error correcting codes, *Proc. IEEE*, vol. 68, pp. 564-593, 1980.
8. W. Ryan, S. Lin. Channel Codes: Classical and Modern. New York: Cambridge University Press, 2009. 710 p.
9. A. M. Veresova, A. A. vchinnikov. About one algorithm for correcting bursts using block-permutation LDPC-codes. *2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*. IEEE. 2019. P. 1-4.
10. E. A. Krouk, A. A. Ovchinnikov. Block-permutation LDPC codes for distributed storage systems. *Smart Innovation, Systems and Technologies*. 2015. Vol. 40, pp. 227-238.
11. R. G. Gallager. Low-Density Parity-Check Codes. *IRE Transactions on Information Theory*. Jan. 1962. Vol. 8. No. 1, pp. 21-28.
12. M. Baldi. QC-LDPC Code-Based Cryptography.Springer, 2014. 120 p.
13. X. Xiao, B. Vasic, S. Lin, J. Li, and K. Abdel-Ghaffar. Quasi-cyclic LDPC codes with parity-check matrices of column weight two or more for correcting phased bursts of erasures. *IEEE Transactions on Communications*, May 2021, vol. 69, no. 5, pp. 2812-2823. doi:10.1109/TCOMM.2021.3059001
14. M.P.C. Fossorier. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Transactionson Information Theory*. 2004 Vol. 50 Iss. 8, pp. 1788-1793. DOI:10.1109/TIT.2004.831841

Information about author:

Maria N. Isaeva, *Saint-Petersburg State University of Aerospace Instrumentation, postgraduate student of the Department of Infocommunication Technologies and Communication Systems (Department 25), St. Petersburg, Russia*