УДК 519.725

В. В. Киен, Н. И. Пилипчук

Московский физико-технический институт (национальный исследовательский университет)

Декодирование двухкомпонентных подпространственных кодов

Построены двухкомпонентные подпространственные коды с заданными параметрами. Проведено декодирование с предварительным определением компоненты. Внесено принципиальное изменение в алгоритм декодирования, связанное с использованием критерия определения компоненты. Вместо ранее используемого рангового критерия предложено использовать числовой критерий. В ранговом критерии было предписано определять ранг префиксной матрицы кода, в числовом критерии подсчитывается число единиц на диагонали. Сравнение критериев показало, что числовой критерий более эффективный в смысле уменьшения вероятности ошибок. К тому же он более простой.

Ключевые слова: кодирование, декодирование, двухкомпонентные коды, ранг, матрица, префикс, пространство, подпространство.

V. V. Kien, N. I. Pilipchuk

Moscow Institute of Physics and Technology

Decoding twocomponent subspace codes

The two component subspace code is constructed. The decoding procedure with preliminary determination components is described. The former decoding algorithm is changed. We propose a new criterion to determine which component is the code word – the first or the second component. Instead of the previously used rank criterion, numerical criteria are recommended. The rank criterion determines the component by the rank of a prefix matrix, while the numerical criterion determines by the number of unit elements on the prefix matrix diagonal. Comparisons of these criteria show that the numerical criterion is more efficient in decreasing the error probability, and can be more easily implemented than the rank one.

Key words: coding, decoding, two-component codes, rank, matrix, prefix, space, subspace.

1. Введение

Многокомпонентные коды с нулевым префиксом (МНП) относятся к классу случайных сетевых подпространственных кодов. Они используют в качестве первой компоненты лифтинговые коды Силвы, Кёттера и Кшишанга (SKK) [1], к которым для увеличения мощности добавляют дополнительные компоненты [2]. Благодаря этому многокомпонентные коды при определённых параметрах достигают верхней границы по мощности. Большая мощность кода означает большую информационную скорость передачи, что является ценным качеством кода.

В то же время многокомпонентность приводит к некоторому недостатку по помехоустойчивости. При итеративном декодировании на первом этапе надо определить компоненту, а затем провести декодирование рангового кода. При передаче по каналу с шумами возможно наложение ошибок на передаваемые сообщения, что может приводить к неправильному определению компоненты. В таком случае применять ранговое декодирование не

имеет смысла, так как найти передаваемое сообщение нельзя. Если правильно определена компонента, то ранговое декодирование по алгоритму [4] правильно определяет сообщение при условии, что количество ошибок и стираний не превосходит корректирующей способности рангового кода, или объявит об отказе от декодирования при превышении границы корректирующей способности.

Предположим, что построен многокомпонентный код, у которого первая компонента представляет собой код SKK [1]. Здесь информационная матрица $X = [I \quad M]$ является конкатенацией единичной матрицы и матрицы рангового кода Габидулина [3]. Дополнительные компоненты в качестве префикса используют нулевую матрицу, то есть все элементы префиксной матрицы – нули. Нулевой префикс повторяется столько раз, каково число дополнительных компонент. В остальной части расположена матрица рангового кода меньшего размера, чем в первой компоненте. В последней компоненте на первом месте нулевая матрица и затем единичная матрица: $X = [O \dots I]$. Число строк, а также число столбцов для всех компонент одинаково.

На первом шаге декодирования надо определить компоненту. Для этого определяем префикс: если это единичная матрица, то это первая компонента. После этого второй шаг – декодируем матрицу рангового кода. Если префикс – нулевая матрица, то это следующая компонента. В двухкомпонентном коде всего две компоненты. Если префикс – нулевая матрица, то решение $X = [O \dots I]$ выдаётся сразу.

2. Двухкомпонентный код

Строим двухкомпонентный подпространственный код с параметрами $(n, d, m) = (8, 6, 3)$ над полем $GF(2)$, где $n = 8$ – длина кода,$m = 3$ – размерность, $d = 6$ – минимальное подпространственное кодовое расстояние.

Используем алгоритм построения рангового кода [5] и, добавив единичный префикс, построим 32 матрицы первой компоненты подпространственного кода. К ним присоединим вторую компоненту с нулевым префиксом. Код состоит из 2 компонент.

► Первая компонента имеет вид $C_1 = [I_3 \quad M]$,

$$C_{\text{первый}} = \begin{bmatrix} 1 & 0 & 0 & M_{11} & M_{12} & M_{13} & M_{14} & M_{15} \\ 0 & 1 & 0 & M_{21} & M_{22} & M_{23} & M_{24} & M_{25} \\ 0 & 0 & 1 & M_{31} & M_{32} & M_{33} & M_{34} & M_{35} \end{bmatrix},$$

где M_{ij} $(i = 1, 2, 3,\ j = 1, 2, 3, 4, 5)$ – элементы матрицы M рангового кода размера 3×5 с ранговым расстоянием $d_{rank} = d/2 = 3$.

Мощность этого кода вычисляется по формуле: $q^{(n-m)(m-d_{rank}+1)} = 2^{5\times 1} = 32$. Первая компонента состоит из 32 кодовых слов.

► Вторая компонента имеет вид $C_2 = [O_3^5 \quad I_3]$,

$$C_{\text{второй}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Мощность этой компоненты равна 1.

Теперь построим ранговый код с матрицей M. Матрица рангового кода M размера 3×5 состоит из линейного подпространства векторов размерности 5 над расширенным полем $GF(2^5)$. Параметры этого кода $(n_r, k_r, d_r) = (3, 1, 3)$, где n_r – длина кодового вектора, k_r-мерное подпространство пространства векторов $GF(2^5)^3$ и d_r – кодовое расстояние. Используем неприводимый полином $\varphi(x) = x^5 + x^2 + 1$ с примитивным элементом α и

соответствующую таблицу поля:

Степенной вид	Базисный вид	Соответствующий вектор
0	0	00000
1	1	00001
α	α	00010
α^2	α^2	00100
α^3	α^3	01000
α^4	α^4	10000
α^5	α^2+1	00101
α^6	$\alpha^3+\alpha$	01010
α^7	$\alpha^4+\alpha^2$	10100
α^8	$\alpha^3+\alpha^2+1$	01101
α^9	$\alpha^4+\alpha^3+\alpha$	11010
α^{10}	α^4+1	10001
α^{11}	$\alpha^2+\alpha+1$	00111
α^{12}	$\alpha^3+\alpha^2+\alpha$	01110
α^{13}	$\alpha^4+\alpha^3+\alpha^2$	11100
α^{14}	$\alpha^4+\alpha^3+\alpha^2+1$	11101
α^{15}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	11111
α^{16}	$\alpha^4+\alpha^3+\alpha+1$	11011
α^{17}	$\alpha^4+\alpha+1$	10011
α^{18}	$\alpha+1$	00011
α^{19}	$\alpha^2+\alpha$	00110
α^{20}	$\alpha^3+\alpha^2$	01100
α^{21}	$\alpha^4+\alpha^3$	11000
α^{22}	$\alpha^4+\alpha^2+1$	10101
α^{23}	$\alpha^3+\alpha^2+\alpha+1$	01111
α^{24}	$\alpha^4+\alpha^3+\alpha^2+\alpha$	11110
α^{25}	$\alpha^4+\alpha^3+1$	11001
α^{26}	$\alpha^4+\alpha^2+\alpha+1$	10111
α^{27}	$\alpha^3+\alpha+1$	01011
α^{28}	$\alpha^4+\alpha^2+\alpha$	10110
α^{29}	α^3+1	01001
α^{30}	$\alpha^4+\alpha$	10010

Число различных ранговых слов и в векторном, и в матричном представлении, включая нулевой вектор (нулевую матрицу), равно $2^{5\times 1}=32$.

Ранговый код $(n_r,k_r,d_r)=(3,1,3)$ задаётся порождающей матрицей G размера (1×3) и ранга 1. Зададим порождающую матрицу G в виде

$$G=\begin{pmatrix} g_1 & g_2 & g_3 \end{pmatrix},$$

где элементы g_1,g_2,g_3 из $GF(2^5)$ линейно независимы над $GF(2)$. Выбираем независимые элементы расширенного поля $GF(2^5)$ в виде $(g_1,g_2,g_3)=(1,\alpha,\alpha^2)$. Тогда порождающая матрица рангового кода такова:

$$G=\begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}. \tag{1}$$

Ранговый код $(n_r,k_r,d_r)=(3,1,3)$ в векторном представлении имеет вид

$$M_1=\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, M_2=\begin{pmatrix} 0 & 1 & \alpha \end{pmatrix}, M_3=\begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix},$$

$$M_4=\begin{pmatrix} \alpha & \alpha^2 & \alpha^3 \end{pmatrix}, M_5=\begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^4 \end{pmatrix}, M_6=\begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix},$$

$$M_7 = \begin{pmatrix}\alpha^4 & \alpha^5 & \alpha^6\end{pmatrix}, M_8 = \begin{pmatrix}\alpha^5 & \alpha^6 & \alpha^7\end{pmatrix}, M_9 = \begin{pmatrix}\alpha^6 & \alpha^7 & \alpha^8\end{pmatrix},$$
$$M_{10} = \begin{pmatrix}\alpha^7 & \alpha^8 & \alpha^9\end{pmatrix}, M_{11} = \begin{pmatrix}\alpha^8 & \alpha^9 & \alpha^{10}\end{pmatrix}, M_{12} = \begin{pmatrix}\alpha^9 & \alpha^{10} & \alpha^{11}\end{pmatrix},$$
$$M_{13} = \begin{pmatrix}\alpha^{10} & \alpha^{11} & \alpha^{12}\end{pmatrix}, M_{14} = \begin{pmatrix}\alpha^{11} & \alpha^{12} & \alpha^{13}\end{pmatrix}, M_{15} = \begin{pmatrix}\alpha^{12} & \alpha^{13} & \alpha^{14}\end{pmatrix},$$
$$M_{16} = \begin{pmatrix}\alpha^{13} & \alpha^{14} & \alpha^{15}\end{pmatrix}, M_{17} = \begin{pmatrix}\alpha^{14} & \alpha^{15} & \alpha^{16}\end{pmatrix}, M_{18} = \begin{pmatrix}\alpha^{15} & \alpha^{16} & \alpha^{17}\end{pmatrix},$$
$$M_{19} = \begin{pmatrix}\alpha^{16} & \alpha^{17} & \alpha^{18}\end{pmatrix}, M_{20} = \begin{pmatrix}\alpha^{17} & \alpha^{18} & \alpha^{19}\end{pmatrix}, M_{21} = \begin{pmatrix}\alpha^{18} & \alpha^{19} & \alpha^{20}\end{pmatrix},$$
$$M_{22} = \begin{pmatrix}\alpha^{19} & \alpha^{20} & \alpha^{21}\end{pmatrix}, M_{23} = \begin{pmatrix}\alpha^{20} & \alpha^{21} & \alpha^{22}\end{pmatrix}, M_{24} = \begin{pmatrix}\alpha^{21} & \alpha^{22} & \alpha^{23}\end{pmatrix},$$
$$M_{25} = \begin{pmatrix}\alpha^{22} & \alpha^{23} & \alpha^{24}\end{pmatrix}, M_{26} = \begin{pmatrix}\alpha^{23} & \alpha^{24} & \alpha^{25}\end{pmatrix}, M_{27} = \begin{pmatrix}\alpha^{24} & \alpha^{25} & \alpha^{26}\end{pmatrix},$$
$$M_{28} = \begin{pmatrix}\alpha^{25} & \alpha^{26} & \alpha^{27}\end{pmatrix}, M_{29} = \begin{pmatrix}\alpha^{26} & \alpha^{27} & \alpha^{28}\end{pmatrix}, M_{30} = \begin{pmatrix}\alpha^{27} & \alpha^{28} & \alpha^{29}\end{pmatrix},$$
$$M_{31} = \begin{pmatrix}\alpha^{28} & \alpha^{29} & \alpha^{30}\end{pmatrix}, M_{32} = \begin{pmatrix}\alpha^{29} & \alpha^{30} & 1\end{pmatrix}.$$

Соответствующее матричное представление :

$$M_1 = \begin{bmatrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix} M_2 = \begin{bmatrix}0&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix} \cdots\cdots\cdots\cdots M_{32} = \begin{bmatrix}0&1&0&0&1\\1&0&0&1&0\\0&0&0&0&1\end{bmatrix}.$$

Двухкомпонентные подпространственные коды с параметрами $(n, d, m) = (8, 6, 3)$ состоят из 33 матриц C_i, $(i = \overline{(1, 33)}$ размера 3×8.

Для краткости записи кодовых матриц представим строки матрицы в виде двоичных чисел и переведём в десятичный вид. Например, запись кодовой матрицы

$$C_2 = \begin{bmatrix}1&0&0&0&0&0&0&1\\0&1&0&0&0&0&1&0\\0&0&1&0&0&1&0&0\end{bmatrix}$$

представим в виде $C_2 = (129, 66, 36)$, где каждое десятичное число – это число, соответствующее двоичному представлению строки матрицы – первой, второй, третьей. Запись сообщения второй компоненты $C_{33} = (4, 2, 1)$ соответствует матрице

$$C_{33} = \begin{bmatrix}0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}.$$

$C_1 = (128, 64, 32)$	$C_2 = (129, 66, 36)$	$C_3 = (130, 68, 40)$	$C_4 = (132, 72, 48)$
$C_5 = (136, 80, 37)$	$C_6 = (144, 68, 42)$	$C_7 = (133, 74, 52)$	$C_8 = (138, 84, 45)$
$C_9 = (148, 77, 58)$	$C_{10} = (141, 88, 49)$	$C_{11} = (154, 81, 39)$	$C_{12} = (145, 71, 46)$
$C_{13} = (137, 78, 60)$	$C_{14} = (142, 92, 61)$	$C_{15} = (156, 93, 63)$	$C_{16} = (157, 95, 59)$
$C_{17} = (159, 91, 51)$	$C_{18} = (155, 83, 35)$	$C_{19} = (147, 67, 38)$	$C_{20} = (131, 70, 44)$
$C_{21} = (134, 76, 56)$	$C_{22} = (140, 88, 53)$	$C_{23} = (152, 84, 47)$	$C_{24} = (149, 79, 62)$
$C_{25} = (141, 94, 57)$	$C_{26} = (158, 89, 55)$	$C_{27} = (153, 87, 43)$	$C_{28} = (151, 75, 54)$
$C_{29} = (139, 86, 41)$	$C_{30} = (150, 73, 50)$	$C_{31} = (137, 82, 33)$	$C_{32} = (146, 65, 34)$
$C_{33} = (4, 2, 1)$			

3. Модель канала и определение префикса

Принимаем модель канала в виде

$$Y = AX + E_{out},$$

где Y – принятое сообщение, A – матрица случайных коэффициентов, E_{out} – матрица внешних ошибок, $X = [I \quad M]$ – информационная матрица как конкатенация единичной

матрицы (префикс) и матрицы рангового кода или $X = [O \dots I]$ – конкатенация нулевой матрицы и единичной.

Представим матрицу внешних помех E_{out} в виде конкатенации $E_{out} = [E_1 \quad E_2]$, где E_1 суммируется с префиксом, а E_2 суммируется с остальной частью матрицы-сообщения.

• Если передано сообщение из первой компоненты, то

$$Y = [A + E_1 \quad AM + E_2].$$

• Если передано сообщение из первой компоненты, то

$$Y = [O \dots I] + E_{out} = [E_1 \quad (O \dots I + E_2)].$$

На первом шаге декодирования надо определить префикс – это единичная или нулевая матрица. Это равнозначно определению компоненты: если единичная, то первая компонента, если нулевая матрица, то это вторая, то есть дополнительная компонента.

Для первого шага декодирования рассматриваем только префикс. Если передавалась первая компонента, то префикс принятого сообщения $Y_1 = A + E_1 = E_A$ или префикс $Y_1 = 0 + E_1 = E_1$, если передавалась вторая компонента, где E_A – суммарная шумовая матрица первой компоненты, E_1 – шумовая матрица второй компоненты. Единичные элементы в каждой из матриц E_A и E_1 считаем ошибками, так как они искажают передаваемые сообщения. Считаем их независимыми. Пусть p_A – вероятность символа «1» и $q_A = 1 - p_A$ – вероятность символа «0» для матрицы E_A и соответственно p, q для E_1.

Поскольку сложение по модулю два, то сложение одноимённых символов даёт нулевой символ, а сложение разноимённых символов даёт единичный символ. Ввиду независимости вероятности символов единичного префикса равны $p_A = 2pq$ и $q_A = p^2 + q^2$. Приведём значения p, q и соответствующие значения p_A, q_A.

p	0	0.001	0.01	0.02	0.03	0.04	0.05	0.1	0.2	0.3
q	1	0.999	0.99	0.98	0.97	0.96	0.95	0.9	0.8	0.7
p_A	0	0.001998	0.0198	0.0392	0.0582	0.0768	0.095	0.18	0.32	0.42
q_A	1	0.998002	0.9802	0.9608	0.9418	0.9232	0.905	0.82	0.68	0.58

Как видно из этих данных, при очень хороших каналах, когда q близко к единице, вероятность символа-ошибки «1» в единичной матрице почти вдвое больше, чем в нулевой матрице. Далее с ухудшением канала (увеличением p) отношение уменьшается и при $p = 0.5$ становится равным единице.

4. Ранговый и числовой критерии

В работе [6] предложен ранговый критерий определения компонент. Если ранг префиксной матрицы больше половины длины диагонали, то считается, что передавалось сообщение с единичным префиксом, в противном случае – с нулевым префиксом. Здесь мы введём ещё один критерий – по числу единиц на диагонали префиксной матрицы. Если число единиц больше половины длины диагонали, то считаем, что передавалось сообщение с единичным префиксом, в противном случае – с нулевым префиксом.

В нашем коде префиксная матрица имеет размер 3×3. В этом случае по ранговому критерию значения ранга 0 или 1 характеризует нулевой префикс. Если ранг 2 или 3, то считаем, что единичный префикс. По числовому критерию аналогично. Если число единиц на диагонали 0 или 1, то считаем, что префикс – нулевая матрица; если число единиц 2 или 3, то префикс – единичная матрица.

Возможное число единиц-ошибок ν в такого размера матрице может быть от $\nu = 0$ до $\nu = 9$. Вероятность события $\nu = i$ есть $C_9^i p^i q^{9-i}$. При значениях $\nu = 0$ и $\nu = 1$ ошибок в определении компоненты нет. Вероятность правильного определения в этих двух случаях $P(0) + P(1) = q^9 + 9pq^8$.

Пример 1. Пусть $p = 0.1 \to P(0) + P(1) \simeq 0.775$. Это значит,что при каждом из используемых критериев имеем правильный ответ в более чем трех четвертях ситуаций для канала с $p = 0.1$. Такой канал в приложениях считается среднего качества.

Пример 2. Пусть $p = 0.01 \to P(0) + P(1) \simeq 0.9965$. Абсолютно безошибочная передача идёт почти постоянно, т.е. в более 99 процентов случаев. В этом случае качество канала считается очень хорошим.

В других случаях при $p \geqslant 0.2 \to P(0) + P(1) < 0.44$, т.е. имеем максимум 44 процента случаев абсолютно безошибочного декодирования. Считается, что такой канал плохого качества. Для совсем плохого канала ($p = 0.5$) вероятность безошибочной работы декодера $P(0) + P(1) \simeq 0,0195$, то есть около лишь двух процентов времени абсолютно безошибочного декодирования.

Покажем, что события с $\nu \geq 2$ вызывают ошибки при определении компонент.

Например, при $p = 0.1$ имеем вероятность P_i события $\nu = i$ такова

i	0	1	2	3	4	5	6
P_i	0.3874	0.3874	0.1721	0.0446	$7 \cdot 10^{-4}$	$1 \cdot 10^{-6}$	$6 \cdot 10^{-9}$

Как видно из этих данных, вероятность суммы событий $\nu = 0$, $\nu = 1$, $\nu = 2$, $\nu = 3$ равна $S = 0.3874 + 0.3874 + 0.1721 + 0.0446 = 0.991$. Ввиду большого значения этой вероятности ограничимся событиями $\nu \leq 3$.

Рассмотрим подробно ситуации, когда число единичных символов в префиксных матрицах $\nu = 2$. Всего $C_9^2 = 36$ таких событий. Записываем 36 нулевых матриц с двумя единичными элементами-ошибками и столько же единичных матриц с двумя ошибками. Определяем ранг каждой матрицы и число единиц на диагонали.

Применяем два критерия: ранговый и числовой. Ранговый критерий считает, что ранг 0 или 1 означает, что передавалась нулевая префиксная матрица; ранг 2 или 3 означает, что передавалась единичная префиксная матрица. Числовой критерий подсчитывает число единиц на главной диагонали префиксной матрицы. Аналогично, если число 0 или 1, то числовой критерий считает, что передавалась нулевая префиксная матрица; если 2 или 3, то единичная матрица.

Оказалось, что среди 36 нулевых матриц ранг больше или равен 2 имеют 18 матриц, то есть ошибок 50 процентов. Учтём вероятность события $\nu = 2$, равную $C_9^i p^i q^{9-i}$, что при $p = 0.1$ равна 0.1721, то есть вклад в общую ошибку определения нулевой компоненты есть $\frac{0.1721}{2} = 0.08605$. Среди такого же числа единичных матриц ранг меньше 2 имеют 12 матриц, то есть ошибок одна треть. Учтём вероятность 0.1721 и получим вклад в общую ошибку $\frac{0.1721}{3} = 0.0574$. По критерию числа единиц на диагонали нулевая матрица имеет 3 ошибочных решения, столько же ошибочных решений, то есть 3 у единичной матрицы, то есть вклад в общую ошибку одинаков и равен $\frac{0.1721}{12} \simeq 0.0143$. Таким образом, для этого случая ранговый критерий даёт большую ошибку для нулевой матрицы, и она больше, чем для единичной матрицы. Критерий числа единиц даёт одинаковые ошибки для обеих матриц, и они меньше, чем при ранговом критерии.

Теперь таким же образом найдём ошибочные решения в случае $\nu = 3$. Всего $C_9^3 = 84$ события с $\nu = 3$, вероятность каждого такого события $p^3 q^6$. Подсчитаем ошибки для каждого из критериев и для каждой из префиксных матриц.

Как и в предыдущем случае, записываем все 84 нулевых матрицы с тремя ошибками и столько же единичных матриц с таким же числом ошибок. Находим ранг и число единиц на диагонали каждой матрицы. Оказалось, что среди 84 нулевых матриц ранг больше или равен 2 имеют 79 матриц. Относительная ошибка $79/84 = 0.940$, то есть очень большое число случаев неправильного определения дополнительной компоненты. При $p = 0.1$ вероятность события с тремя единицами-ошибками в матрице равна 0.0446, так что вклад в общую ошибку равен $0.0446 \times 0.940 = 0.41924$. Среди такого же числа единичных матриц ранг меньше 2 имеют 17 матриц. Относительная ошибка $17/84 = 0.202$, то есть примерно одна пятая часть случаев неправильного определения. Здесь вклад в общую ошибку равен

$0.0446 \times 0.202 = 0.0901$. По критерию числа единиц на диагонали нулевая матрица имеет 21 ошибочное решение из 84 матриц, единичная матрица имеет 23 ошибочных решения из того же количества матриц, то есть относительное число ошибок в нулевой матрице $21/84 = 0.250$, в единичной матрице $23/84 = 0.275$. Вклад в общую ошибку для нулевой матрицы $0.0446 \times 0.25 = 0.0112$ для единичной матрицы $0.0446 \times 0.275 = 0.0123$. Эти цифры не так сильно отличаются, как при ранговом критерии.

Для примера эти данные представим в виде таблицы для относительно хороших каналов, для которых $0.01 \le p \le 0.15$.

Для нулевой матрицы:

p	0	0.01	0.05	0.1	0.15
ε_{R0}	0	0.0018	0.0392	0.1553	0.2610
ε_{d0}	0	0.0003	0.0072	0.0280	0.0607
η_0	–	6	5.44	5.55	4.30

Для единичной матрицы:

p	0	0.01	0.05	0.1	0.15
p_A	0	0.0198	0.095	0.18	0.255
ε_{RI}	0	0.0011	0.0217	0.0588	0.0880
ε_{dI}	0	0.0012	0.02536	0.0855	0.1619
η_I	–	1.09	1.17	1.45	1.84

В этой таблице введены следующие обозначения: p – вероятность ошибки (единицы в префиксной нулевой матрице); p_A – вероятность ошибки (единицы в префиксной единичной матрице); ε_{R0},ε_{RI} – вероятность ошибки при использовании рангового критерия; ε_{d0},ε_{dI} – вероятность ошибки при использовании числового критерия; η_0,η_I – отношение числа ошибок декодирования рангового критерия к такому же числу для числового критерия.

Анализируя данные обеих таблиц, отмечаем, что с увеличением вероятности искажения символов (ухудшением сетевого канала) увеличиваются вероятности ошибок в определении компонент как при ранговом, так и при числовом критерии. Для нулевой матрицы числовой критерий значительно более эффективный, чем ранговый критерий: отношение ошибок для рассматриваемых каналов в 4–6 раз меньше. Чем лучше канал (меньше p), тем более эффективен числовой критерий. Для единичной матрицы более эффективен ранговый критерий, хотя его эффективность η_I по отношению к числовому критерию не превышает 2.

5. Ранговое декодирование

Предположим, что на первом шаге декодирования определена вторая компонента. Тогда сразу выносим решение,что передано сообщение

$$C_{33} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

или $C_{33} = (4, 2, 1)$, что то же самое при десятичном представлении двоичных чисел-строк матрицы.

Если на первом этапе определён префикс в виде единичной матрицы, то переходим ко второму шагу декодирования, когда сообщение передаётся ранговому декодеру. Рассматриваем случай, когда число строк передаваемой матрицы и принятой матрицы одинаковы. Это означает, что нет стираний, возможны только ошибки. Применяем алгоритм рангового декодирования для этих условий [4]. Удалив префикс, передаём возможно

искажённую ранговую матрицу $\widetilde{M}$ размера 3×5 ранговому декодеру. Есть две причины искажений: во первых, умножение передаваемой матрицы M на случайную матрицу A в случайном сетевом канале, во-вторых, сложение со второй частью E_2 размера 3×5 внешней шумовой матрицы. В результате искажённая ранговая матрица $\widetilde{M}$ может быть представлена в виде

$$\widetilde{M} = M + \Delta M_{rest},$$

где M_{rest} – матрица ошибок. Для нас важен ранг ρ этой матрицы. Наш двухкомпонентный код имеет подпространственное расстояние $d_r = 3$, значит, он умеет исправлять только одиночные ранговые ошибки по условию $\frac{(d_r-1)}{2} = 1$ [5].

Предположим, что сообщение передаётся как кодовый вектор вида

$$v = M_8 = \begin{bmatrix} \alpha^5 & \alpha^6 & \alpha^7 \end{bmatrix}. \tag{2}$$

При передаче добавлена ошибка e ранга 1 в виде вектора

$$e = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}. \tag{3}$$

Тогда на принимающей стороне имеем сообщение

$$y = v + e = \begin{bmatrix} \alpha^5 & \alpha^6 & \alpha^7 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha^2 & \alpha^6 & \alpha^{22} \end{bmatrix}.$$

Задача декодирования состоит в том, чтобы найти передаваемое сообщение v. Для этого надо найти вектор ошибки e.

Имеем:
полученное сообщение

$$y = \begin{bmatrix} \alpha^2 & \alpha^6 & \alpha^{22} \end{bmatrix},$$

порождающую матрицу из (1)

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}.$$

Теперь находим проверочную матрицу

$$H = \begin{bmatrix} h_1 & h_2 & h_3 \\ h_1^2 & h_2^2 & h_3^2 \end{bmatrix}$$

из уравнения: $GH^T = 0$.

Получим систему уравнений:

$$\begin{cases} h_1 + \alpha h_2 + \alpha^2 h_3 = 0, \\ h_1^2 + \alpha h_2^2 + \alpha^2 h_3^2 = 0 \end{cases} \Leftrightarrow \begin{cases} h_1 + \alpha h_2 + \alpha^2 h_3 = 0, \\ (\alpha^2 + \alpha) h_2^2 + (\alpha^4 + \alpha^2) h_3^2 = 0 \end{cases} \Leftrightarrow \begin{cases} h_1 + \alpha h_2 + \alpha^2 h_3 = 0, \\ h_3 = \alpha^6 h_2. \end{cases}$$

Положим $h_2 = \alpha$. Тогда $h_3 = \alpha^7$, $h_1 = \alpha^{24}$. Проверочная матрица имеет вид

$$H = \begin{bmatrix} \alpha^{24} & \alpha & \alpha^7 \\ \alpha^{17} & \alpha^2 & \alpha^{14} \end{bmatrix}.$$

Так как $d_r = 3$, то ошибка ранга 1 имеет вид

$$e = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix},$$

где $e_1 \in GF(2^5)$, $u_i \in GF(2)$.

Вычисляем синдром s:

$$s = yH^T = (v + e)H^T = eH^T = \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} \alpha^6 & \alpha^{12} \end{bmatrix} =$$

$$= e_1 \begin{bmatrix} \alpha^{24}u_1 + \alpha u_2 + \alpha^7 u_3 & \alpha^{17}u_1 + \alpha^2 u_2 + \alpha^{14} u_3 \end{bmatrix} = e_1 \begin{bmatrix} x_1 & x_1^2 \end{bmatrix},$$

где $x_1 = \alpha^{24}u_1 + \alpha u_2 + \alpha^7 u_3$.

Приравняем соответствующие компоненты синдрома. Получим систему основных синдромных уравнений:

$$\begin{cases} \alpha^6 = s_0 = e_1 x_1, \\ \alpha^{12} = s_1 = e_1 x_1^2. \end{cases}$$

В этом случае $x_1 = \dfrac{s_1}{s_0} = \alpha^6$, $e_1 = \dfrac{s_0}{x_1} = 1$.

Находим $x_1 = \alpha^6 = \alpha^{24} u_1 + \alpha u_2 + \alpha^7 u_3$.

Вектор ошибки равен

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

Кодовый вектор равен

$$v = y + e = \begin{bmatrix} \alpha^2 & \alpha^6 & \alpha^{22} \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha^2 + 1 & \alpha^6 + 0 & \alpha^{22} + 1 \end{bmatrix} = \begin{bmatrix} \alpha^5 & \alpha^6 & \alpha^7 \end{bmatrix}.$$

Этот кодовый вектор v передан в формуле (2), то есть решение правильное.

6. Заключение

В этой работе представлено двухшаговое декодирование двухкомпонентного кода на примере подпространственного кода-спреда $(8, 6, 3)$. В этом коде всего 33 сообщения, из которых 32 сообщения относятся к первой компоненте и одно сообщение относится к второй компоненте.

На первом шаге определяется компонента. Для этого определяется префикс сообщения. Если префикс единичная матрица, то сообщение принадлежит первой компоненте. Если префикс нулевая матрица, то сообщение принадлежит второй компоненте. Из-за шумов в канале передаваемое сообщение может быть искажено, в том числе и префикс. Определение префикса – это важная часть процедуры декодирования. Так как при неправильном определении префикса ошибку декодирования в последующем исправить не удастся.

Ранее для определения префикса применялся ранговый критерий. Если ранг префиксной матрицы больше (или равен) половине диагонали префикса, то считалось, что префикс – единичная матрица, в противном случае – нулевая матрица. Здесь применён новый и очень простой числовой критерий, при котором считается число единиц на диагонали префиксной матрицы. Если это число больше половины диагонали, то считается, что префикс единичная матрица, в противном случае нулевая. Произведено сравнение обоих критериев и показано, что числовой критерий является более эффективным: если в сообщении единичная матрица, то вероятность ошибки примерно та же, что и у рангового критерия; если нулевая матрица, то вероятность ошибки при числовом критерии меньше, чем при ранговом критерии. Рекомендовано использовать числовой критерий.

На втором шаге декодирования определяется конкретное сообщение. Если оно относится к первой компоненте, то после отделения префикса сообщение-матрица рангового кода передаётся на ранговое декодирование. Применяется стандартный синдромный алгоритм. Если условия определения ошибок выполнены, то есть ранг матрицы ошибки меньше или равен $\frac{d_r - 1}{2}$ (где d_r – ранговое расстояние кода), то декодер исправляет ошибки. Если больше $\frac{d_r - 1}{2}$, то декодер объявляет отказ от декодирования.

Заметим, что в нашем коде всего одно сообщение из 33 имеет нулевой префикс. Поэтому, если источник генерирует свои сообщения с равной вероятностью, то большого отличия в использовании рангового или нулевого критерия не происходит. Другое дело, если мы используем многокомпонентный код, где много раз используются дополнительные компоненты. Кроме того, источник сообщений даже в случае двухкомпонентного кода может специально чаще других использовать сообщение с нулевым префиксом. И в этом случае числовой критерий окажется более эффективным, чем ранговый критерий. К тому же числовой критерий технически легче осуществим.

Литература

1. *Silva D., Koetter R., Kschischang F.* A Rank-Metric Approach to Error Control in RandomNetwork Coding // IEEE Trans. Inform. Theory. 2008. V. 54, N 9. P. 3951–3967.

2. *Gabidulin E.M., Bossert M.* Codes for Network Coding // Proc. 2008 IEEE Int. Sympos. OnInformation Theory (ISIT'2008). Toronto, Canada. July 6–11, 2008. P. 867–870.

3. *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. 1985. Т. 21, вып. 1. С. 3–16.

4. *Габидулин Э.М., Пилипчук Н.И., Боссерт М.* Декодирование случайных сетевых кодов // Проблемы передачи информации. 2010. Т. 46, вып. 4. С. 33–55.

5. *Габидулин Э.М.* Лекции по алгебраическому кодированию. Москва. МФТИ. 2015.

6. *Габидулин Э.М., Пилипчук Н.И.,Колыбельников А.И., Уривский А.В., Владимиров С.М., Григорьев А.А.* Сетевое кодирование // Труды МФТИ. 2009. Т. 1, № 2. С. 3–28.

References

1. *Silva D., Koetter R., Kschischang F.* A Rank-Metric Approach to Error Control in RandomNetwork Coding. IEEE Trans. Inform. Theory. 2008. V. 54, N 9. P. 3951–3967.

2. *Gabidulin E.M., Bossert M.* Codes for Network Coding. Proc. 2008 IEEE Int. Sympos. OnInformation Theory (ISIT'2008). Toronto, Canada. July 6–11, 2008. P. 867–870.

3. *Gabidulin E.M.* Theory of codes with maximal rank distance. Probl. Inform. Transm. 1985. V. 21, N 1. P. 3–16.

4. *Gabidulin E.M., Pilipchuk N.I., Bossert M.* Decoding of random network codes. Probl.Inform. Transm. 2010. V. 46, N 4. P. 33–55. (In Russian).

5. *Gabidulin E.M.* Lectures on algebraic coding. Moscow. MIPT. 2015.

6. *Gabidulin E.M., Pilipchuk N., Kolibelnikov A., Urivskiy A., Vladimirov S., Grigoriev A.* Network coding. Proseedings MIPT. 2009. V. 1, N 2. P. 3–28.

Поступила в редакцию 27.01.2020