ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

УДК 517.19

О ПОСТРОЕНИИ СЛУЧАЙНЫХ КОДИРУЮЩИХ МАТРИЦ СПЕЦИАЛЬНОГО ВИДА ДЛЯ БОРЬБЫ СО СТИРАНИЯМИ В БИНАРНЫХ КАНАЛАХ ПЕРЕДАЧИ ДАННЫХ

Е.Е. Айдаркин, *aidarkinzhenya@mail.ru,* ***В.М. Деундяк***
Южный федеральный университет, г. Ростов-на-Дону
ФГАНУ НИИ "Специализированные вычислительные устройства защиты и автоматика", г. Ростов-на-Дону

Решается проблема борьбы со стираниями в бинарных каналах передачи данных. Информационные векторы длины k умножаются на кодирующие $(k \times n)$ − матрицы. Для декодирования полученных из канала зашумленных кодовых слов применяется метод информационных совокупностей. В качестве кодирующих матриц используются случайные матрицы с равновесными столбцами. Предлагается способ построения таких кодирующих матриц, эффективность которого оценивается с помощью вектора вероятности успешного декодирования (ВВУД). Приведено теоретическое обоснование связи ВВУД и декодирования по информационным совокупностям. Проведены численные эксперименты на основе вычисления ВВУД для кодирующих матриц. На основе результатов экспериментов предлагаются оптимальные параметры генерации кодирующих матриц. Полученные результаты могут быть также использованы в случайных линейных сетях.

Ключевые слова: бинарный канал, стирание в канале, кодирующая матрица, равновесные столбцы матрицы, информационная совокупность.

CONSTRUCTION OF RANDOM ENCODING MATRIX OF SPECIAL TYPE FOR COMBATING ERASURES IN BINARY DATA TRANSMISSION CHANNELS

E.E. Aidarkin, V.M. Deundyak
Southern Federal University, Rostov-on-Don
FSASE SRI «Specialized Security Computing Devices and Automation», Rostov-on-Don

The problem of dealing with erasures in binary data channels is being solved. Information vectors of length k are multiplied by coding $(k \times n)$ − matrices. To decode the noisy codewords obtained from the channel, the method of information sets is used. Random matrices with equal-weight columns are used for coding matrices. A method is proposed for constructing such coding matrices, the effectiveness of which is estimated by using the probability vector of successful decoding (VOSD). A theoretical justification for the connection of the VOSD and decoding of information sets is given. Numerical experiments based on the calculation of VOSD for coding matrices were carried out. Based on the results of these experiments, optimal parameters for the generation of coding matrices are proposed. The results can also be used in random linear networks.

Keywords: binary channel, erasure in channel, encoding matrix, equal-weight matrix columns, information set.

Введение

Развитие сетей мобильной связи и других сетей передачи данных делает актуальной задачу борьбы с помехами, которые вызывают всевозможные ошибки такие как, потеря, вставка, замена и стирание символов.

В настоящее время задача защиты от стираний в каналах решается, как правило, на основе использования кодирующих матриц, например, матриц Коши [1, 5, 10] и Вандермонда [1, 2, 7], а также с помощью вероятностных методов на основе латинских квадратов [12, 13].

ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

Задачей данной работы является создание новых способов построения кодирующих матриц для защиты от стираний в бинарном канале передачи данных на основе использования метода равновесных столбцов. В первом разделе описан матричный метод борьбы со стираниями в канале, основанный на использовании информационных совокупностей и представлен соответствующий алгоритм декодирования. В качестве критерия эффективности выбранной кодирующей матрицы используется вектор вероятностей успешного декодирования, который изучен в разделе 2. Результаты об экспериментальном определении наилучшего веса столбца содержатся в разделе 3. Новый способ построения кодирующих матриц с равновесными столбцами и его модификация представлены в разделе 4.

1. Матричный метод борьбы со стираниями в канале

В работе рассматривается простейшая модель передачи данных: источник кодирует информационное сообщение и передает его через бинарный канал с помехами, далее получатель выполняет декодирование и восстанавливает информационное сообщение. Предполагается, что в канале происходят ошибки типа стирания, поэтому входной алфавит - поле F_2, выходной - $F_2 \cup \{*\}$, где символ "$*$" является индикатором стирания. Например, по каналу передавался вектор (00101011), в канале произошли стирания в первой, третьей и пятой координатах, тогда $(*\,0\,*\,0\,*\,011)$ – полученный из канала вектор. Сообщение разбивается на блоки длины k. Под кодированием понимается умножение информационного блока длины k на $(k \times n)$-матрицу G, $k < n$. Далее будем полагать, что матрица G имеет полный ранг, т.е. $rank(G) = k$, и ее можно рассматривать как порождающую матрицу $[n, k]$-кода C длины n размерности k.

Декодирование осуществляется по методу информационных совокупностей [4, 6], адаптированного для каналов со стираниями в случае отсутствия заранее вычисленного множества информационных совокупностей.

Алгоритм

Вход: полученный из канала вектор $b = (b_1, b_2, \dots, b_n), b_i \in (F_2 \cup \{*\})$, кодирующая матрица G.

Выход: информационное сообщение $a = (a_1, a_2, \dots, a_k)$, где $a_i \in F_2$, или сообщение об ошибке декодирования.

1) Составить множество $J = (j_1, j_2, \dots, j_m)$ нестертых координат вектора b. Если $m < k$, то вернуть сообщение об ошибке и выйти из алгоритма.

2) Составить упорядоченное множество $L = \{l_1, l_2, \dots, l_s\}$, $s = C_m^k$ всех сочетаний по k элементов множества J.

3) $p := 1$.

4) Если $p > s$, то вернуть сообщение об ошибке и выйти из алгоритма. Построить $(k \times k)$-матрицу H_p, столбцы которой являются столбцами матрицы G с номерами из l_p.

5) Вычислить $\text{rank}(H_p)$. Если $\text{rank}(H_p) = k$, то перейти на шаг 6. Если $\text{rank}(H_p) < k$, то $p := p + 1$ и вернуться на шаг 4.

6) Вычислить $a = b_p H_p^{-1}$, где $b_p = \left(b_{i_1}, b_{i_2}, \dots, b_{i_k}\right)$, $i_m \in l_p$, и выйти из алгоритма.

Заметим, что данный алгоритм подходит для случайно сгенерированных матриц полного ранга. Возникает задача нахождения таких условий на генерацию кодирующих матриц, чтобы при декодировании исправлялось как можно больше ошибок типа стираний.

2. Вектор вероятностей успешного декодирования как инструмент априорной оценки результата декодирования

Рассмотрим кодирующую $(k \times n)$ – матрицу G. Будем полагать, что $rank(G) = k$. Обозначим через D_i, $i = k, \dots, n$ множество всех подматриц, полученных из G путем выбора i столбцов (такие подматрицы будем называть столбцовыми подматрицами). Через R_i, $i = k, \dots, n$, обозначим множество подматриц, полученных аналогичным способом, которые имеют ранг k. Заметим, что любому элементу множества R_k соответствует некоторая информационная совокупность, а любой элемент множеств R_i, $i = k+1, \dots, n$ включает в себя столбцовую подматрицу размера $k \times k$, соответствующую информационной совокупности. Нетрудно видеть, что отношение $\rho_i = |R_i|/|D_i|$ соответствует вероятности успешного декодирования [8] информационного сообщения a (алгоритмом декодирования без множества информационных совокупностей) из i полученных без стираний координат вектора b.

Следующий вектор

$$V_G = (\rho_k, \rho_{k+1}, \dots, \rho_n),\ \rho_i = |R_i|/|D_i|,$$

называется вектором вероятностей успешного декодирования для кодирующей $(k \times n) -$ матрицы G [13].

Далее данный вектор используется как инструмент априорной оценки результата декодирования для кодирующей матрицы G.

3. Экспериментальное определение наилучшего веса столбца

В данном разделе экспериментальным способом определяется наилучший вес столбца для построения кодирующих матриц из равновесных столбцов. В качестве веса рассматривается вес Хемминга. В [9] отмечено, что кодирующая матрица, составленная из равновесных столбцов четного веса, является вырожденной. Следовательно, в этой работе рассматриваются матрицы со столбцами нечетного веса.

Первый эксперимент основан на построении матриц из всевозможных столбцов конкретного веса w длины k и вычислении первых координат ρ_i вектора вероятностей успешного декодирования.

Ниже представлена таблица, показывающая результаты вычислений на основе 10 тыс. опытов, проделанных для некоторых длин вектора k и некоторого веса w. Пары (k, w) приведены с тем условием, чтобы векторов с такими параметрами было больше k, т.е. этих векторов достаточно для конструирования «длинных» матриц.

Путем анализа строк таблицы 1 для каждого k можно выделить такой вес w, что все компоненты ρ_i будут больше, чем для других весов (данные строки выделены в таблице жирным шрифтом). Таким весом является «нечетная половина» k. Также можно заметить, что координаты вектора вероятностей успешного декодирования возрастают с увеличением номера координаты. Анализ столбцов таблицы показывает, что с увеличением параметра k, наблюдается уменьшение

ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

вероятностей для ρ_k, что в целом верно и для остальных координат ρ_i. Следовательно, представляется более полезным использовать блоки сравнительно малой длины.

Таблица 1

Первые 10 координат ВВУД, $k = 5, \ldots, 10$

(k, w)	ρ_k	ρ_{k+1}	ρ_{k+2}	ρ_{k+3}	ρ_{k+4}	ρ_{k+5}	ρ_{k+6}	ρ_{k+7}	ρ_{k+8}	ρ_{k+9}
(5, 3)	**0,646**	**0,929**	**1**	**1**	**1**	**-**	**-**	**-**	**-**	**-**
(6, 3)	**0,494**	**0,795**	**0,930**	**0,98**	**0,994**	**0,999**	**0,999**	**1**	**1**	**1**
(7, 3)	**0,411**	**0,722**	**0,886**	**0,952**	**0,982**	**0,992**	**0,997**	**0,999**	**0,999**	**1**
(7, 5)	0,392	0,689	0,849	0,93	0,972	0,989	0,996	0,999	1	1
(8, 3)	0,359	0,665	0,826	0,925	0,967	0,985	0,993	0,998	0,999	0,999
(8, 5)	**0,368**	**0,668**	**0,832**	**0,918**	**0,965**	**0,984**	**0,992**	**0,996**	**0,999**	**0,999**
(9, 3)	0,317	0,611	0,789	0,888	0,938	0,972	0,983	0,993	0,996	0,997
(9, 5)	**0,343**	**0,628**	**0,816**	**0,912**	**0,955**	**0,981**	**0,991**	**0,995**	**0,998**	**0,999**
(9, 7)	0,226	0,468	0,643	0,765	0,847	0,899	0,939	0,961	0,980	0,985
(10, 3)	0,294	0,560	0,748	0,854	0,918	0,954	0,972	0,983	0,990	0,993
(10, 5)	**0,314**	**0,599**	**0,794**	**0,897**	**0,948**	**0,974**	**0,988**	**0,994**	**0,997**	**0,999**
(10, 7)	0,279	0,559	0,741	0,852	0,917	0,95	0,973	0,984	0,987	0,994

Таким образом, для дальнейших исследований будут выбираться столбцы с весом равным «нечетной половине» длины вектора.

4. Способ построения кодирующих матриц с равновесными столбцами

Рассмотрим все равновесные столбцы фиксированного веса w и длины k. Очевидно, что количество таких столбцов равно числу сочетаний C_k^w. Способ построения кодирующих матриц состоит в следующем. Выбирается параметр n ($\leq C_k^w$) – количество столбцов в кодирующей матрице. Случайным образом генерируются n неповторяющихся векторов длины k и веса w, из которых составляется матрица G. Если $rank(G) < k$, то необходимо отказаться от полученной матрицы и повторить процедуру построения матрицы G до достижения ранга k.

Результаты построения матриц на основе применения этого способа анализируются экспериментально с помощью вычисления оценки вектора вероятности успешного декодирования. Эксперимент заключается в следующем:

1) Выбираются параметры (k, w).

2) Строится $(k \times n)$-матрица описанным способом, где $n = k + 5$ (n выбрано для удобства проведения экспериментов).

3) Для этой матрицы вычисляются компоненты ВВУД ρ_i на основе 10 тыс. опытов.

Заметим, что для каждой пары параметров (k, w) проводится 100 экспериментов. Результаты, представленные в таблице 2, вычислены как среднее значение ρ_i среди всех проведенных экспериментов.

Анализируя строки таблицы 2, можно заметить, что вероятности ρ_i возрастают с увеличением i. Отметим, что $\rho_{k+5} = 1$ (следствие полноты ранга матриц). Путем анализа столбцов таблицы 2, можно сделать вывод, что тенденция, описанная в разделе 3 сохраняется.

ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

Заметим, что результаты для матриц с параметрами $(5, 3, 10)$ приблизительно совпадают с наилучшими результатами из статьи [8], полученными другим способом. Данное наблюдение позволяет сделать вывод, что описанный в настоящей работе способ является перспективным.

Таблица 2

Средние значения ВВУД для $\boldsymbol{(k \times (k+5))}$ кодирующих матриц с равновесными столбцами

(k, w, n)	ρ_k	ρ_{k+1}	ρ_{k+2}	ρ_{k+3}	ρ_{k+4}	ρ_{k+5}
(5, 3, 10)	0,643	0,929	1	1	1	1
(6, 3, 11)	0,497	0,802	0,933	0,982	0,997	1
(7, 3, 12)	0,427	0,737	0,895	0,964	0,991	1
(8, 3, 13)	0,364	0,667	0,844	0,935	0,98	1
(9, 5, 14)	0,342	0,647	0,832	0,929	0,978	1
(10, 5, 15)	0,328	0,632	0,822	0,924	0,976	1
(11, 5, 16)	0,306	0,605	0,801	0,912	0,97	1
(12, 7, 17)	0,307	0,607	0,803	0,913	0,971	1
(13, 7, 18)	0,296	0,593	0,791	0,905	0,967	1
(14, 7, 19)	0,295	0,591	0,789	0,904	0,967	1
(15, 7, 20)	0,311	0,614	0,811	0,921	0,975	1

Рассмотрим модификацию описанного выше способа, навеянную [1, 2, 5, 7, 10]. При построении кодирующей матрицы будем использовать конкатенацию единичной матрицы со столбцами одинакового веса. Аналогично базовому способу выбираются параметры k, w, n $(\leq C_k^w + k)$. Первые k столбцов кодирующей матрицы предназначаются для единичной $(k \times k)$-матрицы. Остальные столбцы заполняются векторами длины k веса w. Таким образом, получается что $n \leq C_k^w + k$. Для проведения сравнений модифицированного способа с основным размерности кодирующих матриц совпадают.

Таблица 3

Средние значения ВВУД для $\boldsymbol{(k \times (k+5))}$ кодирующих матриц, построенных с помощью модифицированного способа

(k, w, n)	ρ_k	ρ_{k+1}	ρ_{k+2}	ρ_{k+3}	ρ_{k+4}	ρ_{k+5}
(5, 3, 10)	0,616	0,896	0,98	0,998	1	1
(6, 3, 11)	0,476	0,776	0,915	0,972	0,994	1
(7, 3, 12)	0,355	0,644	0,818	0,917	0,972	1
(8, 3, 13)	0,265	0,53	0,727	0,86	0,947	1
(9, 5, 14)	0,417	0,73	0,889	0,958	0,986	1
(10, 5, 15)	0,385	0,692	0,863	0,946	0,984	1
(11, 5, 16)	0,333	0,628	0,812	0,914	0,97	1
(12, 7, 17)	0,411	0,737	0,905	0,973	0,995	1
(13, 7, 18)	0,376	0,692	0,867	0,951	0,986	1
(14, 7, 19)	0,351	0,657	0,836	0,929	0,975	1
(15, 7, 20)	0,329	0,627	0,813	0,915	0,971	1

Анализируя таблицу 3, можно заметить, что все выводы, полученные из анализа таблицы 2, во многом справедливы и для таблицы 3. Кроме того, сравнивая таблицы 2 и 3, отметим, что вероятности модифицированного способа немного меньше вероятностей базового для маленькой длины вектора k; однако при увеличении длины, наоборот, наблюдается увеличение вероятностей модифицированного способа относительно базового. Данное наблюдение следует учитывать в практических применениях.

Программная реализация для проведения экспериментов создана на языке C++ с помощью библиотеки NTL для работы с полями Галуа [11].

Выводы. В работе предложен новый способ построения кодирующих матриц и его модификация. Проведены эксперименты, направленные на вычисление компонент ВВУД для кодирующих матриц. Результаты экспериментов показывают перспективность этих способов. Следует отметить также, что вектор вероятности успешного декодирования является приемлемым инструментом для оценки качества построения кодирующих матриц для использования в каналах со стираниями. Недостатком этого метода является выполнение априорного полного перебора столбцовых подматриц.

Список цитируемой литературы

1. Айдаркин Е.Е., Деундяк В.М., Позднякова Е.А. Экспериментальное исследование матричных методов защиты от стираний в цифровых каналах передачи данных // Известия вузов. Северо-Кавказский регион. Технические науки. – 2017. – №3, С. 97–104.
2. Деундяк В. М., Михайлова Е. А. Применение матриц Вандермонда при передаче по q-ичному каналу со стираниями // Известия вузов. Северо-Кавказский регион. Естественные науки. – 2012. – №3. – С. 5–9.
3. Деундяк В.М., Маевский А.Э., Могилевская Н.С. Методы помехоустойчивой защиты данных. Ростов-на-Дону: Издательство Южного федерального университета. – 2014. – 309 с.
4. Евсеев Г. С. О сложности декодирования линейных кодов // Пробл. передачи информ. – 1983. – Том 19, №1, С. 3–8.
5. Михайлова Е. А. О реализации схемы В. Пана защиты информации в канале со стираниями // Математика и ее приложения: ЖИМО. – 2011. – №1(8). – с. 75–78.
6. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида–Маллера // Дискрет. матем. – 1994. – Том 6, №2.
7. Al-Shaikhi A., Ilow J. Design of Packet-Based Block Codes with Shift Operators // EURASIP Journal on Wireless Communications and Networking 2010. – V. 2010. – № 263210. – p. 1-12.
8. Gligoroski D., Kralevska K. Families of optimal binary non-MDS erasure codes // ArXiv:1609.02460v1 [cs.IT]. – 2016.
9. K. Kralevska, D. Gligoroski, and H. Øverby. Balanced XOR-ed coding. In Advances in Communication Networking - 19th EUNICE/IFIP, volume 8115 of LNCS, Springer, 2013, p. 161–172.
10. Pan V. Y. Matrix structure and loss-resilient encoding/decoding // Computers and Mathematics with Applications. – 2003. – V. 46. – P. 493-499.
11. Shoup V. NTL: A Library for doing Number Theory // URL:http://shoup.net/ntl/
12. Silva D., Kschischang F.R., and Koetter R. Communication over finite field matrix channels // IEEE Transactions on Information Theory. – 2010. – 56(3):1296–1305.
13. Trullos-Cruces O. Exact Decoding Probability Under Random Linear Network Coding // IEEE Communications Letters. – 2011. – vol. 15, №1.