

А.Г. САРУХАНЫАН, А.Ж. АНОЯН

НОВЫЙ МЕТОД КОДИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАНИЯ АДАМАРА

Разработан метод кодирования и декодирования с использованием повторных прожекторов, основанный на преобразовании Адамара.

Ключевые слова: прожекторы, канал, помехи, кодирование, декодирование, преобразование Адамара.

ВВЕДЕНИЕ. Матрицей Адамара порядка n называется $(-1, +1)$ – матрица H_n размерности $n \times n$, удовлетворяющая условию

$$H_n H_n^T = H_n^T H_n = nI_n,$$

где T – знак транспонирования; I_n – единичная матрица порядка n .

Доказано, что если H_n – матрица Адамара, то $n \equiv 0 \pmod{4}$. Обратная задача, а именно, задача построения или существования матриц Адамара любого порядка n , кратного четырем, до сих пор не решена [1 – 3].

Ниже будем использовать матрицы Адамара порядка 2^k , которые называются также матрицами Сильвестра [1] и строятся согласно следующей рекуррентной формуле:

$$H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix},$$

$k = 1, 2,$

(1)

где $H_1 = (1)$.

Известно также, что из матрицы Сильвестра порядка 2^n строится блочный код мощностью 2^{n+1} , длиной 2^n и минимальным расстоянием 2^{n-1} [4,5], и, следовательно, код Адамара может исправлять $[2^{n-2} - 0,5]$ ошибок (здесь и ниже $[x]$ – целая часть числа x). Построение кодов Адамара с вышеприведенными параметрами не представляет затруднений. В матрице Адамара элементы $+1$ заменяются нулями, а элементы -1 – единицами. Затем к полученным кодовым словам добавляются их дополнения.

Декодирование производится следующим образом. В полученном кодовом слове все нули заменяются единицами, а единицы – минус единицами. Затем к полученному вектору применяется преобразование Адамара, и в его спектре определяется наибольший по модулю коэффициент. Пусть он найден в i -ом месте:

$i = 0, 1,$

2^{n-1} . Если этот коэффициент

положителен, то считается, что было послано кодовое слово под номером i . Если же он отрицателен, то считается, что было послано $i + 2^n$ – е кодовое слово.

1. ПОСТРОЕНИЕ КОДОВ ПОВТОРНЫХ ПРОЖЕКТОРОВ. Пусть $(c_1, c_2, \dots, c_k)$ – двоичное информационное слово, а $\{P_i = (p_{i1}, p_{i2}, \dots, p_{ik}), i=1, 2, \dots, n\}$ – множество двоичных ненулевых векторов, причем мощность множества P равна 2^k-1 . Двоичные слова P_i называются прожекторами кода. Кодовое слово $u = (u_1, u_2, \dots, u_n)$, соответствующее информационному слову $(c_1, c_2, \dots, c_k)$, определяется посредством прожекторов согласно формуле

$$u_i = \bigoplus_{j=1}^k c_j p_{ij}, \quad i = 1, 2, \dots, n, \quad (2)$$

где $\bigoplus$ – знак суммирования по модулю 2.

Процесс декодирования происходит следующим образом. Декодер получает кодовое слово $(u_1, u_2, \dots, u_n)$ и обрабатывает его, записывая результаты в таблицу. Если $u_i=0$, то результат в таблице, соответствующий адресу P_i , увеличивается на 1, если же $u_i=1$, то он уменьшается на 1. После такого заполнения таблицы ее результаты будут представлять собой координаты некоторого вектора V . Размерность вектора V равна 2^k . Далее к вектору V применяется преобразование Адамара $H_k V$. Затем определяется наибольший положительный коэффициент преобразования (т.е. наибольшая положительная координата спектра вектора V). Адрес в таблице декодера, соответствующий этому коэффициенту, и будет являться десятичным представлением исходного информационного слова $(c_1, c_2, \dots, c_k)$.

2. ОЦЕНКА КОЛИЧЕСТВА ИСПРАВЛЯЕМЫХ ОШИБОК. Сперва докажем две теоремы.

Теорема 1. Пусть $H_n = \{h_{ij}\}_{i,j=1}^{2^n}$ – матрица Сильвестра порядка 2^n . Тогда, если строки p и q ($p \neq q$) матрицы H_n совпадают в некоторых столбцах $s_1, s_2, \dots, s_{2^{n-1}}$, т.е. имеет место равенство $h_{ps_i} = h_{qs_i}$, $i=1, 2, \dots, 2^{n-1}$, то для любой k -й строки матрицы H_n существует строка ℓ ($\ell \neq k$) такая, что они совпадают в тех же столбцах, что и строки p и q .

Доказательство. Так как H_n – матрица Адамара типа Сильвестра, то она состоит из четырех матриц Адамара порядка 2^{n-1} и имеет вид (1).

Очевидно, что все столбцы совпадения $s_1, s_2, \dots, s_{2^{n-1}}$ строк p и q не могут находиться в правой части матрицы H_n . Заметим также, что в правой части матрицы H_n не может быть больше совпадений, чем в левой, так же как и в левой части не может быть больше совпадений, чем в правой. В противном случае ортогональность правых и левых матриц Адамара H_{n-1} была бы нарушена.

Таким образом, остается лишь два случая: либо все совпадения находятся в левой части H_n , либо половина – в левой части, а другая половина – в правой части H_n .

Из построения матриц Адамара типа Сильвестра следует, что если все совпадения находятся в левой части H_n , т.е. $s_i=i$, $i=1, 2, \dots, 2^{n-1}$, то для любой строки k существует строка ℓ , которая совпадает с k также в левой части матрицы H_n . Действительно, если все s_i ($i=1, 2, \dots, 2^{n-1}$) находятся в левой половине H_n , то одна из строк p или q должна

находиться в ее верхней половине, а другая – в нижней (если бы обе одновременно находились в верхней или нижней части H_n , то ортогональность левой верхней или левой нижней матрицы Адамара H_{n-1} была бы нарушена). Ясно, что для строки k из верхней половины (нижней половины) H_n существует строка ℓ из ее нижней половины (верхней половины) такая, что совпадает с k в левой части H_n , так как для каждой строки из верхней левой матрицы H_{n-1} существует аналогичная ей в нижней левой матрице H_{n-1} .

Остался случай, когда половина совпадений находится в левой части, а другая половина в правой, т.е. столбцы с номерами $s_1, s_2, \dots, s_{2^{n-2}}$ находятся в левой части, а с номерами $s_{2^{n-2}+1}, s_{2^{n-2}+2}, \dots, s_{2^{n-1}}$ – в правой. Покажем, что утверждение теоремы достаточно доказать для половины совпадений, находящихся в левой части H_n , т.е. для $s_1, s_2, \dots, s_{2^{n-2}}$. Т.е. необходимо доказать, что если две строки совпадают в столбцах $s_1, s_2, \dots, s_{2^{n-2}}$, то совпадения правой части $s_{2^{n-2}+1}, s_{2^{n-2}+2}, \dots, s_{2^{n-1}}$ каким-то образом зависят от $s_1, s_2, \dots, s_{2^{n-2}}$.

Рассмотрим два случая.

1) Строки p и q обе одновременно находятся или в верхней, или в нижней половине матрицы H_n . Покажем, что имеет место равенство

$$s_{2^{n-2}+i} = s_i + 2^{n-2}, \quad i=1, 2, \dots, 2^{n-2}. \quad (3)$$

В самом деле, если обе строки находятся в верхней половине H_n , то в силу того, что в ее верхней части находятся две идентичные матрицы H_{n-1} , ясно, что левым совпадениям $s_1, s_2, \dots, s_{2^{n-2}}$ в левой верхней матрице H_{n-1} соответствуют совпадения верхней правой матрицы H_{n-1} . Т.е. имеет место равенство (3). Пусть теперь обе строки находятся в нижней части матрицы H_n . Так как в матрице $-H_{n-1}$ совпадения сохраняются, то выполнение равенства (3) становится очевидным.

2) Предположим, что одна из строк находится в верхней, а другая – в нижней половине матрицы H_n . Допустим, что в левой части матрицы H_n эти две строки совпадают в столбцах $s_1, s_2, \dots, s_{2^{n-2}}$. Пусть $r_1, r_2, \dots, r_{2^{n-2}}$ – номера тех столбцов, в которых эти строки не совпадают и которые находятся также в левой части H_n . Докажем, что в этом случае имеет место равенство

$$s_{2^{n-2}+i} = r_i + 2^{n-2}, \quad i = 1, 2, \dots, 2^{n-2}. \quad (4)$$

Пусть строка p находится в верхней половине H_n , а строка q – в ее нижней половине. Из вида матриц Сильвестра следует, что для данной строки q существует строка $q' = q - 2^{n-1}$ ($q' \neq p$), находящаяся в верхней части H_n , такая, что строки p и q' совпадают в столбцах $s_1, s_2, \dots, s_{2^{n-2}}$ и,

следовательно, не совпадают в столбцах $\Gamma_1, \Gamma_2, \dots, \Gamma_{2^{n-2}}$. Согласно первому случаю, строки p и q' совпадают также и в столбцах $S_{2^{n-2}+1}, S_{2^{n-2}+2}, \dots, S_{2^{n-1}}$ и различаются в столбцах $\Gamma_{2^{n-2}+1}, \Gamma_{2^{n-2}+2}, \dots, \Gamma_{2^{n-1}}$. Последние, в силу идентичности верхних матриц H_{n-1} , также выражаются через $\Gamma_1, \Gamma_2, \dots, \Gamma_{2^{n-2}}$:

$$\Gamma_{2^{n-2}+i} = \Gamma_i + 2^{n-2}, \quad i = 1, 2, \dots, 2^{n-2}. \quad (5)$$

Строки q и q' различаются только в правой части. Это означает, что в тех столбцах (в правой части H_n), в которых строки p и q' не совпадают, строки p и q совпадают. Совпадения и различия в левой части H_n идентичны. Таким образом: $s_i = r_i$, $i = 2^{n-2}+1, 2^{n-2}+2, \dots, 2^{n-1}$. А отсюда из (5) следует (4).

Осталось доказать условие теоремы для 2^{n-2} совпадений в левой половине матрицы H_n . Так как левые матрицы H_{n-1} идентичны, то любой строке i из нижней левой матрицы H_{n-1} соответствует строка $i' = i - 2^{n-1}$ из верхней левой матрицы H_{n-1} , с которой она совпадает. Доказательство проводится идентично вышесказанному, просто в этом случае имеем матрицу Сильвестра малой размерности. Продолжая таким образом, мы придем к доказательству условия теоремы для матрицы H_1 с одним совпадением в левой части.

Теорема 2. Пусть H_n – матрица Сильвестра порядка k ($k = 2^n$), а действительные векторы-столбцы $A = (a_i)_{i=1}^k$, $B = (b_i)_{i=1}^k$ такие, что $|a_i| = |b_i|$, $i = 1, 2, \dots, k$, при этом знаки координат векторов A и B совпадают соответственно со знаками p -й и q -й строк матрицы Сильвестра H_n . Тогда спектры векторов A и B имеют одинаковые координаты с разным порядком следования.

Доказательство. Предположим, что $H_n A = (u_1, u_2, \dots, u_k)^T$ и $H_n B = (v_1, v_2, \dots, v_k)^T$. Так как знаки всех координат вектора A совпадают со знаками p -й строки, то $u_p = |a_1| + |a_2| + \dots + |a_k|$. Обозначим через $s_1, s_2, \dots, s_{k/2}$ столбцы, в которых строки p и q совпадают, и $r_1, r_2, \dots, r_{k/2}$ – столбцы, в которых они не совпадают. Тогда имеет место равенство:

$$\begin{aligned} u_q &= |a_{s_1}| + \dots + |a_{s_{k/2}}| - |a_{r_1}| - \dots - |a_{r_{k/2}}|. \text{ Аналогичным образом имеем} \\ v_p &= |b_{s_1}| + \dots + |b_{s_{k/2}}| - |b_{r_1}| - \dots - |b_{r_{k/2}}|. \text{ Так как } |a_i| = |b_i|, \text{ то} \\ v_p &= |a_{s_1}| + \dots + |a_{s_{k/2}}| - |a_{r_1}| - \dots - |a_{r_{k/2}}|. \text{ Это означает, что } u_p = v_q \text{ и } u_q = v_p. \end{aligned}$$

Докажем теперь, что для любой строки m существует строка с номером n такая, что $u_m = v_n$ ($m, n = 1, 2, \dots, k$). Согласно теореме 1, для любой строки m матрицы H_n существует такая строка n , что m и n совпадают в тех столбцах, что и строки p и q , т.е. совпадение и несовпадение имеют место соответственно в столбцах с номерами $s_1, s_2, \dots, s_{k/2}$ и $r_1, r_2, \dots, r_{k/2}$. Отсюда следует равенство

$$u_m = |a_{s_1}| + \dots + |a_{s_{k/2}}| - |a_{r_1}| - \dots - |a_{r_{k/2}}| =$$

$$= |b_{s_1}| + \dots + |b_{s_{k/2}}| - |b_{r_1}| - \dots - |b_{r_{k/2}}| = v_n,$$

что и доказывает теорему.

Нетрудно убедиться, что вектор-столбец V , метод определения которого был описан в разделе 1, удовлетворяет условию теоремы 2. То есть, какое бы кодовое слово не передавалось по каналу, векторы преобразования Адамара $H_n V$ всегда будут состоять из одних и тех же чисел, но с различными порядками следования, при условии безошибочной передачи. Это означает также, что вне зависимости от информационного слова, второй по величине коэффициент преобразования всегда будет одним и тем же числом, а в первую очередь, с ним можно спутать максимальный коэффициент, если произошли ошибки при передаче.

Пусть M – число прожекторов и одновременно длина кодового слова, m – второй по величине элемент спектра Адамара. Тогда, с учетом вышеприведенного анализа, можем утверждать, что построенный выше код исправляет

$$t < \frac{M - m}{4} \quad (6)$$

ошибок.

3. ПРИМЕР. В качестве примера рассмотрим действие кодера повторных прожекторов для $M=21$ и $k=3$, где информационное слово имеет вид: $(c_1, c_2, c_3) = (0, 1, 1)$. В качестве прожекторов рассматриваем двоичные наборы, соответствующие десятичным числам $1, 2, \dots, 7$. Каждый из прожекторов повторяется 3 раза. Согласно формуле (2) находим кодовое слово 111111000000111111000 , которое передается через канал. Декодер по методу, описанному в разделе 1, образует вектор $V = (0, -3, -3, +3, +3, -3, -3, +3)^T$. Далее над вектором V производится преобразование Адамара, т.е. $H_3 V = (-3, -3, -3, +21, -3, -3, -3, -3)^T$. Так как наибольший элемент $+21$ имеет индекс 3 в спектральном векторе (нумерация производится с нуля), то декодер решает, что было передано информационное слово $(0, 1, 1)$.

Согласно (6), построенный код длины 21 исправляет 5 ошибок.

В самом деле, пусть в ходе передачи произошло 5 ошибок. В нижеприведенной таблице ошибки выделены жирным шрифтом и подчеркнуты.

Переданное кодовое слово	1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0
Полученное кодовое слово	1 1 <u>0</u> 1 1 1 <u>1</u> <u>1</u> 0 0 0 0 1 1 1 1 1 <u>0</u> <u>1</u> 0 0

В этом случае декодер определяет следующий вектор:
 $V = (0, -1, -3, -1, +3, -3, -1, +1)^T$.

Затем, вычисляя спектральный вектор
 $H_3 V = (-5, +3, +3, +11, -5, -5, +3, -5)^T$,
 декодер снова решает, что было передано информационное слово $(0, 1, 1)$.

Отметим, что при проведении экспериментов использовался также алгоритм быстрого преобразования Адамара [6].

Доказано также, что если какой-либо один из прожекторов повторить только 2 раза (а не три), то получается аналогичный результат. Т.е. фактически построен код длины 20, исправляющий 5 ошибок.

СПИСОК ЛИТЕРАТУРЫ

1. **Wallis W.D., Street A.P., Wallis J.P.** Combinatorics: Room Squares, Sum Free Sets, Hadamard Matrices // Lecture Notes in Mathematics.-1972.- V.292.- 367 p.
2. **Agaian S.S.** Hadamard Matrices and Their Applications // Lecture Notes in Mathematics.-1985.- V.1168.- 280 p.
3. **Sarukhanyan H.G.** Hadamard Matrices: Construction Methods and Applications // First Int. Workshop on Transforms and Filter Banks, (Finland).-1998.- P.95-129.
4. **Питерсон У., Уэлдон Э.** Коды, исправляющие ошибки. - М.: Мир, 1976.- 594с.
5. **Rao Yarlagadda R.K., Hershey John E.** The Hadamard Transform and Error-Correction Coding // Hadamard Matrix Analysis and Synthesis With Applications to Communications and Signal/Image Processing: Kluwer Academic Publishers.- Boston, London, 1997.- P. 39-50.
6. **Ahmed N., Rao K.R.** Orthogonal Transforms for Digital Signal Processing.-Berlin, New York: Springer-Verlag-1975.- 248 p.

ИПИИ НАН РА.

Материал поступил в редакцию 20.03.2000.

Հ.Գ. ՍԱՐԿԻՆՅԱՆ, Ա.Ժ. ԱՆՈՅԱՆ

ՀԱՂԱՄԱՐԻ ՁԵՎԱՓՈԽՈՒԹՅԱՄԲ ԿՈԴԱՎՈՐՄԱՆ ՆՈՐ ՄԵԹՈԴ

Մշակված է կրկնվող պրոյեկտորներով կոդավորման և դեկոդավորման մեթոդ՝ հիմնված Հադամարի ձևափոխության վրա:

H.G. SARUKHANYAN, A.Zh. ANOYAN

NEW CODING METHOD USING HADAMARD TRANSFORMATION

A new coding method using repeated projectors is considered. A decoding method based on the Hadamard transformation is developed.