Две конструкции сверточных МПП-кодов

В. В.Зяблов
Институт проблем передачи информации, Российская академия наук, Москва, Россия
zyablov@iitp.ru

К. А. Кондрашов
Институт проблем передачи информации, Российская академия наук, Москва, Россия
k_kondrashov@iitp.ru

Аннотация

В настоящей работе предлагаются две новые конструкции q-ных сверточных МПП-кодов, предназначенные для построения из коротких слов с малым кодовым расстоянием и простой проверкой длинных каскадных кодов с хорошими дистанционными свойствами. Конструкции строятся на основе 2-х и 4-х кодов с одной q-ной проверкой на четность. Описывается структура кодов и алгоритм кодирования, исследуются дистанционные свойства представленных кодов.

1. Введение

Двоичные сверточные коды с малой плотностью проверок на четность (сверточные МПП-коды) были предложены в [1]. Как и блочные МПП-коды, сверточные (J,K)-МПП-коды описываются проверочной матрицей $\mathbf{H}$, имеющей ровно J единиц в каждом столбце и K единиц в каждой строке. В случае полей $GF(q)$, где $q \neq 2$, на месте единиц могут стоять любые ненулевые элементы поля.

Частным случаем сверточных МПП-кодов являются плетеные коды [2], использующие определенную геометрическую компоновку $J = 2$ кодов-компонентов. Предлагаемые нами конструкции можно рассматривать, как расширение плетеных кодов. В обеих конструкциях в качестве кодов-компонентов используются простые q-ные коды с одной проверкой на четность. В первой конструкции количество кодов-компонентов оставлено неизменным и она представляет из себя сверточный $(2,4)$-МПП-код. Во второй конструкции количество кодов-компонентов увеличено до 4-х, полученный код является сверточным $(4,8)$-МПП-кодом.

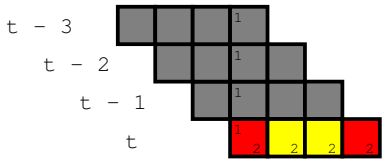

Рис. 1. Представление кодового слова (2,4)-плетеного МПП-кода с помощью массива. Индексами 1 и 2 обозначена принадлежность символов к одному из двух компонентных кодов – вертикальному или горизонтальному. Серым цветом выделены закодированные участки, желтым – места для информационных символов, красным – для проверочных.

2. Первая конструкция

Первая конструкция является прямым обобщением плетеных кодов [2] на случай q-ных кодов с одной q-ной проверкой на четность. Предлагаемую конструкцию $(2,4)$-МПП-кода удобно представить с помощью бесконечного двумерного массива (Рис.1). Кодовые символы помещаются в ячейки массива и проверяются по строкам и по столбцам горизонтальным и вертикальным кодами-компонентами соответственно. В каждый момент времени t символы принятого информационного вектора $\mathbf{u}_t = \left[u_t^0\ u_t^1\right]$ помещаются в выделенную серым область. Вертикальный код кодирует задержанные символы и довершает информационное слово для горизонтального кода. Горизонтальный код кодирует выходной вектор $\mathbf{v}_t = \left[v_t^0\ v_t^1\ v_t^2\ v_t^3\right]$. Скорость кода $R = 0,5$.

3. Вторая конструкция

В плетеных кодах [2] используются два сильных кода-компонента. Двух слабых кодов-

компонентов может быть недостаточно для получения кода с хорошими корректирующими свойствами, поэтому мы предлагаем расширенную конструкцию (Рис.2) с увеличенным числом кодов-компонентов. Мы используем 4 кода-компонента длины 8, что позволяет сохранить общую скорость кода $R = 0,5$. В общем случае скорость сверточного (J,K)-МПП-кода с кодами-компонентами с одной q-ной проверкой на четность определяется как $1 - \frac{J}{K}$. Кодирование выполняется по аналогии с $(2,4)$-кодом: проверочные символы вертикального и диагональных кодов, полученные при кодировании сохраненных в памяти за предыдущие моменты времени символов, вместе с информационными символами образуют информационное слово для горизонтального кода, который завершает кодирование.

4. Кодирование

С предложенными кодами можно работать как с обычными сверточными-МПП кодами, в частности, их можно описать в терминах оператора задержки. Если для всех кодов-компонентов в качестве проверочной матрицы выбрать $\mathbf{H} = (1\ 1\ \ldots\ 1)$, то проверочная матрица внешнего $(4,8)$-кода будет иметь вид:

$$\mathbf{H}^{\mathrm{T}}(D) = \begin{pmatrix} 1 & D^4 & D^6 & 1 \\ D & 1 & D^5 & 1 \\ D^2 & D^5 & D^4 & 1 \\ D^3 & D & D^3 & 1 \\ D^4 & D^6 & D^2 & 1 \\ D^5 & D^2 & D & 1 \\ D^6 & D^7 & 1 & 1 \\ D^7 & D^3 & D^7 & 1 \end{pmatrix}. \qquad (1)$$

При выборе других коэффициентов для любой из проверок на четность эти коэффеценты появятся в соответсвующих позициях в столбце, отвечающем за проверку. Легко увидеть, что представленный сверточный код имеет следующие характеристики: $m_s = 7,\ b = 4,\ c = 8$. Опишем его с помощью полубесконечной проверочной матрицы:

$$\mathbf{H}^{\mathrm{T}} = \begin{pmatrix} \mathbf{H}_0^{\mathrm{T}} & \mathbf{H}_1^{\mathrm{T}} & \cdots & \mathbf{H}_{m_s-1}^{\mathrm{T}} & \mathbf{H}_{m_s}^{\mathrm{T}} & \\ & \mathbf{H}_0^{\mathrm{T}} & \mathbf{H}_1^{\mathrm{T}} & \cdots & \mathbf{H}_{m_s-1}^{\mathrm{T}} & \mathbf{H}_{m_s}^{\mathrm{T}} \\ & \ddots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \qquad (2)$$

где подматрицы $\mathbf{H}_i^{\mathrm{T}}$ – q-ные матрицы размера $c \times (c-b)$, которые легко получить из (1).

$$\mathbf{H}_0^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \ldots \mathbf{H}_7^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Кодирование (m_s,J,K)-кода осуществляется следующим образом. Пусть $\mathbf{v} = [\mathbf{v}_1,\ \mathbf{v}_2,\ \ldots,\ \mathbf{v}_t,\ \ldots]$ – кодовая последовательность, где $\mathbf{v}_t = \left[v_t^0,\ v_t^1,\ \ldots,\ v_t^c\right]$ и $v_t^{p_i} = u_t^i$ для $i = 0,\ldots,b-1$, $p_i \neq p_j$ при $i \neq j$. В любой момент времени эта последовательность должна удовлетворять условию:

$$\mathbf{v}_t\mathbf{H}_0^{\mathrm{T}} + \mathbf{v}_{t-1}\mathbf{H}_1^{\mathrm{T}} + \ldots + \mathbf{v}_{t-m_s}\mathbf{H}_{m_s}^{\mathrm{T}} = 0. \qquad (3)$$

Если из матрицы $\mathbf{H}_0^{\mathrm{T}}$ исключить строки, отвечающие за информационные символы $u^i, i = 0,\ldots b-1$, то полученная $(c-b)\times(c-b)$ матрица $\mathbf{H}_0'^{\mathrm{T}}$ будет иметь полный ранг и решение (3) будет единственным:

$$\mathbf{v}_t'\mathbf{H}_0'^{\mathrm{T}} = -\left(\mathbf{v}_{t-1}\mathbf{H}_1^{\mathrm{T}} + \ldots + \mathbf{v}_{t-m_s}\mathbf{H}_{m_s}^{\mathrm{T}}\right). \qquad (4)$$

Для прямого кодирования по нулевому синдрому требуется $cm_s + b$ ячеек памяти. Этот объем можно уменьшить, используя частичные синдромы. Для кодовой последовательности верно следующее:

$$\mathbf{v}_{[0,\ t-1]}\mathbf{H}_{[0,\ t+m_s-1]}^{\mathrm{T}} = \left[\mathbf{0}_{[0,\ t-1]}|\mathbf{s}_t\right], \qquad (5)$$

где $\mathbf{s}_t = \left[s_t^0,\ s_t^1,\ \ldots,\ s_t^{m_s-1}\right]$

– вектор частичных синдромов. Обновление частичных синдромов происходит в соответствии с рекуррентными соотношениями:

$$s_t^i = \begin{cases} s_{t-1}^{i+1} + \mathbf{v}_t\mathbf{H}_{i+1}^{\mathrm{T}}, & i = 0,\ldots,m_s-2 \\ \mathbf{v}_t\mathbf{H}_{i+1}^{\mathrm{T}}, & i = m_s-1 \end{cases} \qquad (6)$$

А кодовый блок $\mathbf{v}_{t+1}$ получается из следующего уравнения:

$$\mathbf{v}_{t+1}\mathbf{H}_0^{\mathrm{T}} = -s_t^0. \qquad (7)$$

В такой реализации для кодирования потребуется $(c-b)m_s$ ячеек памяти.

5. Дистанционные свойства кодов

Одной из важных характеристик кода, определяющих его корректирующие способности, является минимальное кодовое расстояние d_{min} – минимальное Хеммингово расстояние между кодовыми словами. Так как сверточные коды имеют кодовые слова различной

длины, для них определяется аналог кодового расстояния – свободное расстояние d_{free}. Свободное расстояние – это минимальное расстояние между любыми кодовыми последовательностями сверточного кода. Чтобы определить свободное расстояние кода, мы будем исследовать его активное расстояние

$$d_j = \min\left\{\omega_H\left(\mathbf{v}_{[1,j]}\right)\right\} : \mathbf{v}_{[1,j]}\mathbf{H}^T_{[1,\,j+m_s-1]} = \mathbf{0} \quad (8)$$

– минимальный вес кодовой последовательности, приводящей кодер в нулевое состояние (нулевые частичные синдромы) после j информационных блоков. В таком случае свободное расстояние определяется как минимальное активное расстояние: $d_{free} = \min\limits_j\left\{d_j\right\}$. Для нахождения активных расстояний мы будем для различных j решать систему линейных уравнений

$$x\mathbf{H}^T_{[1,\,j+m_s-1]} = \mathbf{0}, \quad (9)$$

из которой исключены первые несколько строк, отвечающие нулевым символам диагональных кодов первого кодового блока. Система (9) имеет или единственное нулевое решение или множество решений. В последнем случае линейно независимые решения образуют фундаментальную системы решений (ФСР), а все остальные решения получаются из их линейных комбинации. В общем случае минимальный вес решения системы (9) при заданном j определяет точное значение d_j, а минимальный вес векторов ФСР – ее верхнюю границу. Можно показать, что в случае двоичных кодов минимальный вес векторов ФСР будет также давать точное значение d_j. Для этого воспользуемся следующей леммой.

Л е м м а 1. *Кодовые слова двоичных кодов обладают цикличностью.*
Если $\mathbf{v} = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_j]$, *где*
$\mathbf{v}_t = \left[v_t^1, v_t^2, \ldots, v_t^{c-1}, 0\right]$ – *кодовое слово, то и*
$\mathbf{v}' = [\mathbf{v}'_1, \mathbf{v}'_2, \ldots, \mathbf{v}'_j]$, *где*
$\mathbf{v}'_t = \left[0, v_t^1, v_t^2, \ldots, v_t^{c-1}\right]$ – *решение.*

Д о к а з а т е л ь с т в о .
В силу построения, все проверки $x_1 + x_2 + \ldots + x_{c-1} + 0 = 0$ кодов-компонент при единичном сдвиге примут вид $0 + x_1 + x_2 + \ldots + x_{c-1} = 0$. Так как все исходные проверки удовлетворены, то и результирующие проверки будут также удовлетворены. ■

Так как решениями двоичных кодов будут являться вектора ФСР и их сдвиги, а при сдвигах вес слова не меняется, то минимальный вес векторов ФСР будет точным значением активного расстояния d_j. К сожалению, для q-ных кодов этого утверждать нельзя, так как из выполнения условия $x_1\alpha_1 + x_2\alpha_2 + \ldots + x_{c-1}\alpha_{c-1} + 0 = 0$, не следует выполнение $0 + x_1\alpha_2 + x_2\alpha_3 + \ldots + x_{c-1}\alpha_c = 0$ и сдвиги не являются решением.

При решении системы линейных уравнений (9) оказалось, что до некоторого k: $j = 1..k$ у системы нет других решений кроме тривиального. Это означает, что у кодов на длинах $j \le k$ информационных блоков нет кодовых слов, поэтому мы будем считать активное расстояние на этих длинах равным бесконечности. Вычисленные активные расстояния для двоичных и q-ных кодов представлены в Табл. 1 и 2.

Q \ j	1	2	3	4	5
2	∞	4	6	8	
8	∞	∞	≤ 8	≤ 9	≤ 11

Таблица 1. Активные расстояния (2,4)-кодов

Q \ j	3	4	5	6	7
2	∞	12	12	14	
8	∞	∞	∞	≤ 32	≤ 34

Таблица 2. Активные расстояния (4,8)-кодов

6. Заключение

Рассмотрены две кодовые конструкции, представляющие собой обобщения двоичных сверточных МПП-кодов на случай недвоичных конечных полей, описаны алгоритмы кодирования, получены свободные расстояния или их граница сверху. В силу построения оказалось, что двоичные (2,4) и (4,8) коды при декодировании не могут сгенерировать пакеты ошибок длиной вплоть до 1-го и 3-х информационных блоков соответственно, их восмеричные аналоги – до 2-х и 5-и.

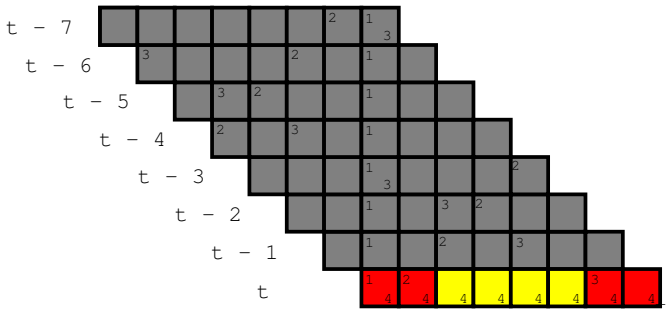

Рис. 2. Представление кодового слова (4,8)-плетеного МПП-кода с помощью массива. Индексами 1 - 4 обозначена принадлежность символов к одному из компонентных кодов. Серым цветом выделены закодированные участки, желтым – места для информационных символов, красным – для проверочных.

Список литературы

[1] *A. Jiménez Feltström and K. S. Zigangirov* Time-varying periodic convolutional codes with low-density parity-check matrix // IEEE Trans. Inform. Theory. 1999. V. IT-45. № 6. P. 2181–2191.

[2] *A. Jiménez Feltström, D. Truchachev, M. Lentmaier, K. S. Zigangirov* Braided Block Codes // IEEE Trans. Inform. Theory submission. May 2008.