ПОЛИНОМИАЛЬНЫЕ КОДЫ И ИХ ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Вражнов Илья Александрович

студент, Самарский национальный исследовательский университет имени Академика С.П. Королева, РФ, Самара

Коновалов Виталий Федорович

студент, Самарский национальный исследовательский университет имени Академика С.П. Королева, РФ, Самара

Додонова Наталья Леонидовна

научный руководитель, канд. физ.-мат. наук, доцент, Самарский национальный исследовательский университет имени Академика С.П. Королева, РФ, г. Самара

Введение. В настоящие время обеспечение высокой достоверности передачи, обработки и хранения информации является актуальной задачей теории и практики электросвязи. Эффективным способом решения данной проблемы является использование избыточного (помехоустойчивого) кодирования информации. Преднамеренное введение избыточной информации в передаваемые информационные сообщения обеспечивает возможность обнаружения и исправления ошибок на приемной стороне. В современных стандартах для кодирования используют такие полиномиальные коды как код Боуза-Чоудхури-Хоквенгема (БЧХ).

При *полиномиальном кодировании* каждое сообщение отождествляется с многочленом, а само кодирование состоит в умножении на фиксированный многочлен. Полиномиальные коды отличаются от других блочных кодов только алгоритмами кодирования и декодирования.

Основные понятия полиномиальных кодов:

При описании полиномиальных кодов n-разрядные кодовые комбинации представляются в виде многочленов с переменной x.

Например, 0011 1000 = $1*x^6+1*x^51*x^4$.

Число информационных символов m - количество разрядов, необходимое для передачи сообщения без использования корректирующих символов.

Число контрольных символов k-количество разрядов, необходимое в данном коде для обеспечения заданной помехоустойчивости.

Длина кодовой комбинации n - комбинация из контрольных и информационных символов, где **n = m + k**.

Неприводимый минимальный многочлен (полином) M(X)-многочлен, делящийся без остатка на себя и на единицу. Неприводимые минимальные многочлены в теории циклических кодов используются для получения образующих многочленов. В таблице 1 приведены некоторые начальные неприводимые многочлены.

Таблица 1.

Начальные неприводимые многочлены

№ п/п	Степень m	Аналитическое представление многочлена	d_{min}	Ко
1.	1	x + 1	2	r =
2.	2	$x^2 + x + 1$	3	r =
3.	3	$x^3 + x + 1$	3	r =
4.		$x^3 + x^2 + 1$	3	r =
5.	4	$x^4 + x + 1$	3	r =
6.		$x^4 + x^2 + 1$	3	r =

Кодовое расстояние d - это расстояние между ближайшими кодовыми комбинациями. Оно определяется числом позиций, в которых их двоичные знаки не совпадают. Это значит, что кодовое расстояние между двоичными комбинациями X и Y равно весу W(Z) некоторой третьей комбинации Z, получаемой поразрядным сложением по модулю 2 этих комбинаций:

Например: x=1000 1011; y=1011 0011;

z= x ⊕ y= 0011 1000, т.о d=3.

Образующий многочлен K(X)-многочлен, при помощи которого происходит построение того или иного кода с заданными помехоустойчивыми параметрами. Образующий многочлен может быть равен неприводимому минимальному многочлену или являться их произведением.

Пример:

K(x) = $m_6(x)$ = = x^4+x^2+1;

K(X) = $m_7(x)*m_{12}(x)$ = 10011*10101 = 110001111 = $x^8+x^7+x^3+x^2+1$.

Теорема: Многочлен $x^{q^m} - x$, где q - степень простого числа, равен произведению всех нормированных неприводимых над GF(q) многочленов, степени которых делят m

Коды БЧХ

В БЧХ-коде построение образующего многочлена, в основном, зависит от двух параметров: от длины кодового слова n=m+k и от числа исправляемых ошибок S.

Алгоритм кодирования (систематического):

1) Задать параметры кода, такие как коррекционная способность t, количество бит в сообщении 5, длина кода 15.

2) Найти порождающий полином.

3) Умножить информационные биты на x^m

4) Вычислить кодовые биты, разделив информационные биты на порождающий полином.

5) Объединить информационные биты с остатком от деления, полученным на предыдущем шаге.

Алгоритм декодирования (расширенным алгоритмом Евклида):

1) Вычислить синдромы $s_1 - s_{2t}$, подставив $\alpha^1 - \alpha^{2t}$ в принятое сообщение Если все синдромы равны 0, сообщение передано без ошибок, и алгоритм завершается. Получить синдромный полином: S(x) = $s_{2t}x^{2t}$ + $s2_{t-1}x^{2t-1}$ +...+ s_1x + 1.

2) Применить алгоритм Евклида для многочленов x^{2t+1} и $S(x)$, чтобы вычислить полином локаторов ошибок.

3) Найти корни полинома методом перебора, определить коэффициенты полинома ошибок x^j , где j=n - k, k - степень α^k - корня полинома-локатора ошибок. Если корней нет, исправить ошибки невозможно, и алгоритм завершается.

4) Сложить полином ошибок и принятое сообщение, получив сообщение без ошибок.

Пример:

Продемонстрируем кодирование сообщения кодом БЧХ. Для начала необходимо задать сообщение B = 10101 длины k, содержащее исходные данные. Если, к примеру, нам нужен код, исправляющий 3 ошибки (t = 3), то нам нужно найти такую степень двойки m, которая бы “покрыла” исходное сообщение и биты четности (т.е. все кодовое слово). Общая длина кодового слова n = 2^m - 1, а количество битов четности – n - k $\leq$ mt. Наименьшая степень двойки, большая k, равна 3 ($2^3 = 8$). Минимальное расстояние равно 2t + 1 = 7. Тогда

минимальное расстояние между двумя кодовыми словами в двоичном представлении как минимум 7 бит, в которых 2 кодовых слова должны различаться. Если мы выберем m=3 с длиной кодового слова n=7, то минимальное расстояние не будет соблюдаться. Для того чтобы это условие выполнялось, необходимо выбрать следующую степень двойки, 4 ($2^4 = 16$).

Таким образом, в данном случае мы используем код БЧХ (15,5), он позволит исправлять 3 ошибки в сообщении длиной 5.

Следующим шагом будет нахождение порождающего полинома. Для этого необходимо сначала выполнить построение поля Галуа GF(2^4), задав его корнем уравнения $\alpha_4 + \alpha + 1 = 0$. Первые 4 элемента поля α_0, α_1, α_2, α_3, будут образующими. Элемент α_4 получим как остаток от деления:

$\frac{\alpha^4}{\alpha^4+\alpha+1} = 1 + \frac{\alpha+1}{\alpha^4+\alpha+1}$. Элементы α_5-α_{14} получим, умножая результат предыдущего шага на α и приводя к образующим элементам, например для α_7:

$\alpha_6 = \alpha_3 + \alpha_2$; $\alpha_7 = \alpha_4 + \alpha_3$ = (так как $\alpha_4 = \alpha + 1$) = $\alpha_3 + \alpha + 1$.

Составим таблицу:

Таблица 2.

Поле Галуа GF(2^4)

Вектор	**Многочлен**	**Степень**
0 0 0 0	0	0
1 0 0 0	1	1
0 1 0 0	α	α
0 0 1 0	α_2	α_2

0 0 0 1	α_3	α_3
1 1 0 0	α_{+1}	α_4
0 1 1 0	$\alpha_2 + \alpha$	α_5
0 0 1 1	$\alpha_3 + \alpha_2$	α_6
1 1 0 1	$\alpha_3 + \alpha_{+1}$	α_7
1 0 1 0	α_{2+1}	α_8
0 1 0 1	$\alpha_3 + \alpha$	α_9
1 1 1 0	$\alpha_2 + \alpha_{+1}$	α_{10}
0 1 1 1	$\alpha_3 + \alpha_2 + \alpha$	α_{11}
1 1 1 1	$\alpha_3 + \alpha_2 + \alpha_{+1}$	α_{12}

1 0 1 1	$\alpha_3 + \alpha_2 + 1$	α_{13}
1 0 0 1	$\alpha_3 + 1$	α_{14}

Затем по теореме для GF(2^4) q=2, m=4:

$x^{2^4} + x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$. Поскольку поле задано корнем уравнения $\alpha_4 + \alpha + 1 = 0$, то минимальный многочлен для каждого из элементов можно найти так:

возьмем к примеру строку α_5 таблицы 3. Подставим α_5 в многочлен $x^2 + x + 1 = \alpha^{10} + \alpha_5 + 1$. Подставляя значения из Таблицы 1 убедимся что $\alpha_{10} + \alpha_5 + 1 = (\alpha_2 + \alpha + 1) + (\alpha_2 + \alpha) + 1 = 0$. Элемент таблицы найден.

Таблица 3.

Минимальные многочлены для элементов α из GF(2^4)

α_0	$x + 1$	f_0
α_1	$x_4 + x + 1$	f_1
α_2	$x_4 + x + 1$	f_2

α_3	$x_4 + x_3 + x_2 + x + 1$	f
α_4	$x_4 + x + 1$	f
α_5	$x_2 + x + 1$	f
α_6	$x_4 + x_3 + x_2 + x + 1$	f

Используя арифметику полей Галуа, а также формулу для порождающего многочлена, находим порождающий многочлен:

$$g(x) = f_1 * f_3 * f_5 = x^{10} + x^8 + x^5 + x^4 + x^2 + x^1 + 1.$$

Дополним исходное сообщение справа 10 нулевыми битами:

10101 0000000000 В виде полинома: $x^{14}+x^{12}+x^{10}$.

Чтобы получить кодовую последовательность, разделим этот полином на порождающий:

$$\frac{x^{14}+x^{12}+x^{10}}{x^{10}+x^8+x^5+x^4+x^2+x+1} = (x^4+1)(x^{10}+x^8+x^5+x^4+x^2+x+1) + x^9+x^6+x^2+x+1$$

Перепишем остаток в векторном виде - 1001000111. Это и есть оставшаяся часть кодового слова. Тогда кодовое слово запишется как:

10101 1001000111.

Допустим, что при передаче произошло 3 ошибки, например

10**0**01 1**1**010**1**0111

Нужно учитывать, что при приеме слова нам неизвестны ни позиции ошибок, ни их количество!

Число t=3, значит синдромов будет 2*t = 6. Их можно найти, подставив в принятое сообщение α в степени номера синдрома:

$S_1 = r(\alpha) = \alpha_3 + 1 = \alpha_{14}$;

$S_2 = r(\alpha_2) = r(\alpha))^2 = (\alpha_{14})^2 = \alpha_3 + \alpha_2 + 1 = \alpha_{13}$;

$S_3 = r(\alpha_3) = \alpha_3 + 1 = \alpha_{14}$;

$S_4 = r(\alpha_4)) = (r(\alpha))^2)^2 = \alpha_3 + \alpha_2 + \alpha = \alpha_{11}$;

$S_5 = r(\alpha_5) = 0$;

$S_6 = r(\alpha_6) = (r(\alpha_3))^2 = \alpha_3 + \alpha_2 + 1 = \alpha_{13}$.

Применим алгоритм Евклида:

Шаг 0. $r_{-2}(x) = x^7$,

$r_{-1}(x) = s(x) = \alpha^{13}x^6 + \alpha^{11}x^4 + \alpha^{14}x^3 + \alpha^{13}x^2 + \alpha^{14}x + 1$,

$y_{-2}(x) = 0$,

$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,

$q_0(x) = \alpha^2x$,

$r_0(x) = \alpha^{13}x^5 + \alpha^1x^4 + x^3 + \alpha^1x^2 + a^2x$,

$y_0(x) = y_{-2}(x) + y_{-1}(x)q_0(x) = q_0(x) = \alpha^2x$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,

$q_1(x) = x+a^3$,

$r_1(x) = \alpha^6x^4 + \alpha^4x^3 + \alpha^9x^2 + \alpha^{12}x + 1$,

$y_1(x) = y_{-1}(x) + y_0(x)q_1(x) = 1+\alpha^2x^2 + \alpha^5x$.

Шаг 3. $r_0(x) = r_1(x)q_2(x) + r_2(x)$,

$q_2(x) = a^7x+1$,

$r_2(x) = \alpha^7x^2+1$,

$y_2(x) = y_0(x) + y_1(x)q_2(x) = \alpha^9x^3 + \alpha^7x^2 + \alpha^{14}x+1$

Тогда полином локаторов ошибок $\sigma(x) =$ $\alpha^9x^3 + \alpha^7x^2 + \alpha^{14}x+1$.

Теперь необходимо подбором найти корни, т.е. значения α^n такие что $\sigma(x)$=0.

$$\sigma(\alpha^3) = \alpha^{18} + \alpha^{13} + \alpha^{17} + 1 = \alpha^3 + \alpha^{13} + \alpha^2 + 1 = 0$$

$$\sigma(\alpha^7) = \alpha^{30} + \alpha^{21} + \alpha^{21} + 1 = 1 + \alpha^{21} + \alpha^{21} + 1 = 0$$

$$\sigma(\alpha^{11}) = \alpha^{42} + \alpha^{29} + \alpha^{25} + 1 = \alpha^{12} + \alpha^{14} + \alpha^{10} + 1 = 0$$

Зная корни, можно легко вычислить полином ошибок. Чтобы получить ненулевые коэффициенты этого полинома, достаточно отнять от 15 степени корней полинома-локатора ошибок:

15-3=12; 15-7=8; 15-11=4. Значит $e(x)=x^{12}+x^8+x^4$ - полином ошибок, а переданное сообщение:

$e(x)+p(x)=x^{12}+x^8+x^4 + x^{14} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^2 + x + 1 =$
$x^{14} + x^{12} + x^{10} + x^9 + x^6 + x^2 + x + 1$.

Описанный код БЧХ (15,5) используется в информации о формате QR- кодов. Обратимся к ГОСТ на QR-коды, чтобы выяснить чему соответствует код из примера. Первые два бита данных содержат уровень исправления ошибок символа, а остальные 3 - уровень маски данных. 10 - последовательность для уровня исправления ошибок H, 101 - последовательность для маски ((i j) mod 2)+((i j) mod 3)=0. К ним добавляют 10 кодовых бит, которые в нашем случае совпадут с полученными в примере 1001000111 .Затем к 15 битам информации о формате 10101 1001000111 применяют операцию XOR с маской 10101 0000010010, чтобы гарантировать, что никакая комбинация уровня исправления ошибок и указателя шаблона маски данных не имеет в результате 15 нулевых битов. В результате получается последовательность 00000 1001010101. Запишем эту последовательность в формат QR-кода, учитывая что черный квадрат означает 1, а белый - 0. В каждом QR коде содержится две копии этих данных, отмеченных на рисунке зелеными и голубыми рамками.

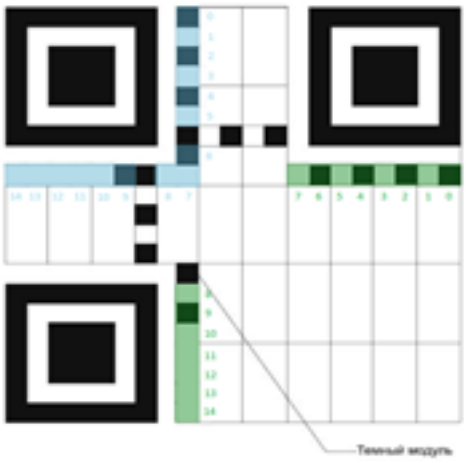

Рисунок. Пример применения БЧХ кода для хранения информации о формате в QR-кодах

Заключение:

БЧХ-коды играют заметную роль в теории и практике кодирования. Интерес к ним определяется следующим: коды БЧХ имеют весьма хорошие свойства; данные коды имеют относительно простые методы кодирования и декодирования.

Теоретически коды БЧХ могут исправлять произвольное количество ошибок, но при этом существенно увеличивается длительность кодовой комбинации, что приводит к уменьшению скорости передачи данных и усложнению приемо-передающей аппаратуры.

В работе были рассмотрены алгоритмы систематического кодирования и декодирования БЧХ кодов, приведен пример создания кодовой последовательности для некоторого слова, а также изучен вопрос практического применения рассмотренного в примере кода.

Список литературы:

1. Р. Морелос-Сарагоса. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2005. – 320 с.

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ./ ред. К. Ш. Зигангирова. – М.: Мир, 1986. – 576 с.

3. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ – М: Связь, 1979. – 744 с.

4. ГОСТ НА QR - коды: ГОСТ Р ИСО/МЭК 18004-2015