УДК 519.725.2

В.О.Дяченко (4 курс, НТФ), О.Н.Дяченко, к.т.н., доц.

АЛЬТЕРНАТИВНЫЙ СПОСОБ ПОСТРОЕНИЯ УКОРОЧЕННЫХ КОДОВ ФАЙРА

В настоящее и обозримое будущее время среди информационных технологий все большую роль будут играть способы помехоустойчивого кодирования, обеспечивающие требуемую достоверность при передаче, обработке и хранении информации. Одними из наиболее эффективных для исправления ошибок являются циклические коды. Эти коды нашли широкое применение благодаря простой аппаратной реализации и высоким корректирующим способностям. В связи с этим вопросы построения и аппаратной реализации циклических кодов являются актуальными, учитывая все большую их популярность и востребованность для различных сфер применения.

В настоящее время получили широкое распространение коды, исправляющие пакеты ошибок: коды Файра, (255, 223, 33) код Рида-Соломона для космической связи NASA, расширенный (128, 122, 7), код Рида-Соломона над полем Галуа $GF(2^7)$ для кабельных модемов и многие другие [1-5].При практической реализации кодов во многих случаях их необходимо укорачивать [1-6]. В данной работе предлагается альтернативный способ построения укороченных кодов Файра, обладающий рядом преимуществ по сравнению с известными.

Из любого (n, k) циклического кода можно получить (n-i, k-i) укороченный код, где n – длина кода, k – количество информационных символов, $0<i<k$ – параметр укорачивания. Одним из способов декодирования укороченных кодов является использование декодеров, построенных для кодов максимальной длины. При этом принятому кодовому слову предпосылаются i нулей, которые кодером не передаются в канал связи. Недостатком такого способа декодирования является несогласованность скоростей передачи кодером кодового слова (длина такого слова n-i, поскольку нули не передаются) и обработки декодером принятого дополненного нулями кодового слова длины n. Кроме того, для формирования синдрома в этом случае необходимо n тактов работы декодера, в то время как при применении другого способа декодирования для этого достаточно n-i тактов.

В отличие от декодера кода максимальной длины, который для формирования синдрома выполняет операции умножения принятого слова на полином X^{n-k} и деления на порождающий полином, декодер укороченного кода умножает на полином, равный остатку от деления полинома X^{n-k+i} на порождающий полином, и полученное произведение делит на порождающий полином. Однако в случае очень большого параметра укорачивания довольно сложно получать остаток от деления полинома X^{n-k+i} на порождающий полином. Так, например, для кода Файра, исправляющего пакет длины 64, получаем такую длину кода, при которой он нереализуем в неукороченном виде. Вместе с тем, его нельзя реализовать при традиционном укорачивании кода. Существует несколько способов определения остатка X^{n-k+i} на порождающий полином. Один из них – аппаратное или программное деление с помощью кодера при подаче на его вход одной единицы и i нулей. Однако, если i мало, нельзя реализовать такой код, поскольку кодовое слово получаем невероятной величины. Таким образом, параметр укорачивания i в любом случае должен быть очень большим, сравнимым с длиной кода. Если i велико, получаем время деления аппаратным способом также невероятной величины. Второй способ – разложение X^{n-k+i} на сомножители для упрощения определения остатка от деления полинома X^{n-k+i} на порождающий полином также не представляется возможным, не говоря уже о третьем способе – деления “уголком”. Тем не менее, с помощью двойственных полиномов такой укороченный код все-таки можно

реализовать.

Основная идея отличия кодирования и декодирования укороченных циклических кодов заключается в следующем. Декодер выполняет исправление принятого слова традиционным способом (применяя умножение на полином, равный остатку от деления полинома X^{n-k+i} на порождающий полином и деление на порождающий полином) Но такой остаток определяется альтернативным способом, при котором параметр укорачивания не участвует. Предлагаемый способ основан на свойстве элементов полей Галуа полученных для двойственных порождающих полиномов. Эти элементы – не что иное как остатки от деления ненулевых полиномов в степенном виде, и кроме того, состояния генератора синдрома в декодере. Анализ таблицы 1 показывает взаимосвязь элементов эти полей. Добавление таблиц на 4 строки ($degp(z)=degp^{*}(z)$) с умножением принятого слова на полином X^{n-k+i}, где $n-k=degp(z)$. Существует зависимость между значениями элементов в двоичном виде. Причем рассматривать их нужно в обратном порядке следования двоичных символов, что соответствует умножению на $X^{degp(z)-1}$. Например, α^4=0011 и $\alpha^{14}=\alpha^{-1}$1100, α^5=0110 и $\alpha^{13}=\alpha^{-2}$=0110, α^6=1100 и $\alpha^{12}=\alpha^{-3}$=0011 и т.д.

Таблица 1. Элементы поля Галуа $GF(2^4)$ с двойственными порождающими полиномами

$p(z)=z^4+z+1$			$p^*(z)=z^4+z^3+1$		
В виде степени	В виде полинома	В двоичном виде	В виде степени	В виде полинома	В двоичном виде
0	0	0000	0	0	0000
α^0	1	0001	$\alpha^0=\alpha^{-15}$	1	0001
α^1	z	0010	$\alpha^1=\alpha^{-14}$	z	0010
α^2	z^2	0100	$\alpha^2=\alpha^{-13}$	z^2	0100
α^3	z^3	1000	$\alpha^3=\alpha^{-12}$	z^3	1000
α^4	z +1	0011	$\alpha^4=\alpha^{-11}$	z^3 +1	1001
α^5	z^2 + z	0110	$\alpha^5=\alpha^{-10}$	z^3 + z + 1	1011
α^6	z^3 + z^2	1100	$\alpha^6=\alpha^{-9}$	z^3 + z^2 + z + 1	1111
α^7	z^3 + z + 1	1011	$\alpha^7=\alpha^{-8}$	z^2 + z + 1	0111
α^8	z^2 + 1	0101	$\alpha^8=\alpha^{-7}$	z^3 + z^2 + z	1110
α^9	z^3 + z	1010	$\alpha^9=\alpha^{-6}$	z^2 + 1	0101
α^{10}	z^2 + z + 1	0111	$\alpha^{10}=\alpha^{-5}$	z^3+ z	1010
α^{11}	z^3 + z^2 + z	1110	$\alpha^{11}=\alpha^{-4}$	z^3 + z^2 + 1	1101
α^{12}	z^3 + z^2 +z + 1	1111	$\alpha^{12}=\alpha^{-3}$	z + 1	0011
α^{13}	z^3 + z^2 + 1	1101	$\alpha^{13}=\alpha^{-2}$	z^2 +z	0110
α^{14}	z^3 + z + 1	1001	$\alpha^{14}=\alpha^{-1}$	z^3 + z^2	1100
α^0	1	0001	$\alpha^{15}=\alpha^0$	1	0001
α^1	z	0010	α^1	z	0010
α^2	z^2	0100	α^2	z^2	0100
α^3	z^3	1000	α^3	z^3	1000

Ненулевые остатки от деления на порождающий полином состоят из двух подмножеств. Общее количество элементов этих подмножеств равны длине исходного кода n(сумме параметра укорачивания іи значения новой длины укороченного кода).Пересекаются эти подмножества на граничных элементах, причем они зеркально равны.

Учитывая эти свойства, можно получить остаток от деления полинома X^{n-k+i} на порождающий полином без явного учета i, а на основе только длины укороченного кода и двойственного полинома.

Пример1. Предположим, что код Файра (511, 499) потребовалось укоротить до (272, 260)-кода [1].Этот код исправляет все пакеты ошибок длины не более 4. В данном случае порождающий полином $g(X)=X^{12}+X^8+X^5+X^3+1$, $X^{n-k+i}=X^{251}$ и необходимо вычислить остатока$(X)= R_{g(X)}[X^{251}]$. В [1] полином X^{251}представлен в виде $X^{251}=(X^{12})^{16}(X^{12})^4 (X^{11})$ для того, чтобы воспользоваться равенством

$$X^{12}=X^8+X^5+X^3+1.$$

Повторяя возведение в квадрат полинома X^{12} и проводя редукцию по модулю g(X), вычисляется $(X^{12})^4$ и$(X^{12})^{16}$, а, следовательно, и X^{251}, так что

$$a(X)=X^{11}+X^9+X^7+X^3+X^2+1.$$

Рассмотрим вычисление для этого же остатка $a(X)= R_{g(X)}[X^{251}]$ с помощью предлагаемого способа. Сначала определяем остаток от деления полинома в степени длины нового укороченного кода уменьшенной на единицу, т.е. X^{271}, на двойственному g(X) полином $g^*(X)= X^{degg(X)}g(X^{-1})=X^{12}(X^{-12}+X^{-8}+X^{-5}+X^{-3}+1)=(X^{12}+X^9+X^7+X^4+1)$ любым известным способом, например, с помощью программы деления полиномов:

$$X^{11}+X^9+X^8+X^4+X^2+1.$$

Получив остаток и умножив его на полином $X^{degg(X)-1}$ находим искомый остаток

$$a(X)=X^{-11}(X^{11}+X^9+X^8+X^4+X^2+1)=X^{11}+X^9+X^7+X^3+X^2+1.$$

Следует отметить важное отличие предлагаемого второго способа от первого и других известных. Из вычислений остатка во втором способе исключается параметр укорачивания i, и таким образом, становится возможной реализация кодов с большим параметром укорачивания и длиной исправляемого пакета ошибок, что наиболее актуально для кодов Файра.

Пример 2. Код Файра с порождающим полиномом

$$(X^{127}+1)(X^{64}+X^4+X^3+X+1)$$

позволяет исправлять пакеты ошибок длины 64 и имеет параметры (18 446 744 073 709 551 615, 18 446 744 073 709 424). Однако такой код нереализуем по известным причинам (длина кода становится равной количеству зёрен из математической задачи о шахматной доске). Вместе с тем, вполне просто построить укороченный код с большим параметром укорачивания, используя простые аппаратные реализации кодера и декодера.

Таким образом, в работе предложен способ построения укороченных кодов Файра, в том числе кодов с большой длиной исправляемого пакета ошибок. Вместе с тем, для таких кодов можно использовать традиционную аппаратную или программную реализацию кодеров и декодеров.

ЛИТЕРАТУРА:

1. Richard E.Blahut. Algebraic Codes for Data Transmission/ Cambridge University Press, 2012. – 498 p.

2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 595 с.: ил.

3. Дяченко В.О., Зинченко Ю.Е., Дяченко О.Н. Исследование способов проектирования кодов Рида-Соломона// Інформаційні управляючі системи та комп'ютерний моніторинг (ІУС КМ-2014) : V Всеукраїнська науково-технічна конференція студентів, аспірантів та молодих вчених, 22-23 квітня 2014 р., м. Донецьк : зб. доп./ Донец. національ. техн. ун-т; редкол. В.А.Світлична. – Донецьк: ДонНТУ, 2014. – в 2 тт. – т.2. – С. 72-78.

4. Зинченко Е.Ю., Дяченко О.Н. Сравнительный анализ способов укорачивания кодов Рида-Соломона// Збірка праць VII міжнародної науково-технічної конференції студентів, аспірантів та молодих науковців – 22-23 листопада 2011 р., Донецьк, ДонНТУ. – 2011. У 2-х томах, Т. 1 – С. 48-52.

5. Дяченко В.О., Дяченко О.Н. Анализ способов реализации кодов Рида-Соломона, исправляющих двойные ошибки// Современные тенденции развития и перспективы внедрения

инновационных технологий в машиностроении, образовании и экономике: материалы Международной научно-практической конференции (Азов, 19 мая 2014 г.). – Ростов н/Д, ДГТУ, 2014. – С. 18-22.
6. Дяченко В.О., Дяченко О.Н. Особенности применения двойственных полиномов для аппаратной реализации циклических кодов // Информационные управляющие системы и компьютерный мониторинг в рамках форума “Инновационные перспективы Донбасса” (ИУС КМ-2015): VI Международная научно-техническая конференция студентов, аспирантов и молодых ученых, 20-22 мая 2015, г.Донецк: / Донец. национал. техн. ун-т; сост.: К.Н.Маренич (председатель) и др. – Донецк: ДонНТУ, 2015. - С. 130–136.