УДК 519.725, 681.3

В.О. Дяченко, О.Н.Дяченко
Донецкий национальный технический университет

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ДВОЙСТВЕННЫХ ПОЛИНОМОВ ДЛЯ АППАРАТНОЙ РЕАЛИЗАЦИИ ЦИКЛИЧЕСКИХ КОДОВ

Аннотация

Дяченко В.О., Дяченко О.Н. Особенности применения двойственных полиномов для аппаратной реализации циклических кодов. *Предлагается применение двойственных полиномов для аппаратной реализации циклических кодов. Рассматриваются особенности альтернативного построения кодирующих и декодирующих схем.*

Внедрение инновационных технологий во всех областях человеческой деятельности приводят к непрерывному увеличению объема накапливаемой информации. Все большее значение приобретают способы помехоустойчивого кодирования, обеспечивающие требуемую достоверность при передаче, обработке и хранении информационных данных. Одними из наиболее эффективных для исправления ошибок и, в особенности, пакетов ошибок, являются циклические коды. В настоящее время существует широчайший спектр разработанных и уже успешно используемых на практике кодов [1-5]: циклические коды Хэмминга, БЧХ, Файра, Рида-Соломона и многие другие. Наиболее известные примеры: (255, 223, 33) код Рида-Соломона для космической связи NASA, укороченные коды Рида-Соломона над полем Галуа GF(28) для CD-ROM, DVD и цифрового телевидения высокого разрешения (формат HDTV), расширенный (128, 122, 7) код Рида-Соломона над полем Галуа GF(27) для кабельных модемов, (255, 239) код рекомендован в качестве внешнего кода в WiMax. Кроме того, циклические коды можно использовать не только для помехоустойчивого

кодирования при передаче данных, а также везде, где есть необходимость в предотвращении искажения информации, например [2]: обнаружение и исправление ошибок в поврежденных или дефектных носителях информации; обнаружение и исправление ошибок при умышленном изменении информационных сообщений с целью дезинформации; обнаружение и исправление модификации информации об авторе или исполняемого кода с целью «взлома» программного обеспечения; защита программного обеспечения или данных от копирования с лицензионного диска; восстановление одного или нескольких томов многотомного архива, искаженных или вообще потерянных при загрузке из сети; обнаружение и исправление ошибок в цепочках ДНК в генной инженерии. Поэтому вопросы построения и аппаратной реализации циклических кодов являются актуальными, учитывая все большую их востребованность для различных сфер применения.

Естественно, что наиболее популярны в настоящее время коды, исправляющие пакеты ошибок. Тем не менее, циклический код Хэмминга, исправляющий одиночные ошибки, заслуживает особого внимания, поскольку является фундаментом для понимания принципов построения более мощных кодов. Одним из примеров может служить аппаратная реализация декодеров двоичного кода Хэмминга и недвоичного кода Рида-Соломона, исправляющего одиночные (недвоичные) ошибки. Кроме того, аппаратная реализация методов компактного тестирования, в частности, генераторы псевдослучайных тестовых последовательностей и сигнатурные анализаторы, построенные на основе декодеров Хэмминга, используются во многих схемах со встроенным самотестированием, в частности, в микропроцессорных СБИС ведущих зарубежных фирм: Pentium Pro (Intel Corporation); S/390 (IBM); Power PC; MC 202-206 (Motorola); AMD-K6 (Advanced Micro Devices).

При построении циклических кодов во многих случаях приходится их укорачивать [1-3]. В данной работе предлагается для кодирования и декодирования кодов применение двойственных полиномов, что в дальнейшем может дать

преимущества при реализации укороченных кодов.

Из любого (n, k) циклического кода можно получить (n-i, k-i) укороченный код, где n - длина кода, k – количество информационных символов, 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^p и деления на порождающий полином, декодер укороченного кода умножает на полином, равный остатку от деления полинома X^{p+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^{p+i} на порождающий полином.

Основная идея отличия применения двойственных полиномов для кодирования и декодирования циклических кодов заключается в том, что декодер выполняет исправление принятого слова по принципу LIFO, а не FIFO, то есть, в обратном порядке следования кодового слова.

Полином $K^*(X) = X^{\deg K(X)} * K(X^{-1})$ называется двойственным полиномом по отношению к полиному K(X).

Коды двойственных полиномов имеют одинаковые характеристики, в частности, одинаковые корректирующие способности, избыточность, аппаратные затраты схемной реализации кодеров и декодеров, быстродействие. В случае

разных полиномов получаем декодер, который обрабатывает биты кодового слова по принципу “последний пришел – первый вышел”.

Пример. Построим два поля Галуа GF(8) как расширения поля GF(2) над примитивными полиномами $p(z)=z^3+z+1$ и $p^*(z)=z^3+z^2+1$ (табл. 1). Элементы поля могут быть представлены в различном обозначении и для ненулевых элементов со степенью большей степени порождающего полинома следуют в обратном порядке.

Таблица 1

Поля Галуа GF(8) с двойственными порождающими полиномами

$p(z)=z^3+z+1$			$p^*(z)=z^3+z^2+1$		
В виде степени	В виде полинома	В двоичном виде	В виде степени	В виде полинома	В двоичном виде
0	0	000	0	0	000
α^0	1	001	α^0	1	001
α^1	z	010	α^1	z	010
α^2	z^2	100	α^2	z^2	100
α^3	z + 1	011	α^3	$z^2 + 1$	101
α^4	$z^2 +z$	110	α^4	$z^2 + z + 1$	111
α^5	$z^2 + z + 1$	111	α^5	$z^2 +z$	110
α^6	$z^2 + 1$	101	α^6	z + 1	011

Рассмотрим более подробно работу кодера и декодера для кода Хэмминга (7,4) с порождающим полиномом кодера $K(X) = X^3 + X + 1$ и порождающим полиномом кодера $K^*(X) = X^3 + X^2 + 1$.

Пусть информационные символы A = 1101 в двоичном виде, или $A(X) = X^3 + X^2 + 1$ в полиномиальном виде. Для систематического кода кодер циклического кода Хэмминга выполняет операцию умножения информационной последовательности на полином X^{n-k} и деление на порождающий полином. Полученный остаток от деления представляет собой

проверочную часть кодового слова. После выполнения этих операций получаем систематический код $X^6 + X^5 + X^3 + 1 = 1101\ 001$, где первая часть 1101 информационная, а вторая 001 – проверочная.

Рассмотрим различные варианты применения порождающих полиномов. В таблице 2: А – кодовое слово, ФС1(А) – формирователь синдрома для K(X), A^* – кодовое слово в обратном порядке следования, ФС2(A^*) – формирователь синдрома для $K^*(X)$, A^*_7 – кодовое слово в обратном порядке следования с ошибкой в 7-м символе кодового слова А, E^*_7 – полином ошибки, ФС2(E^*_7) – формирователь синдрома для $K^*(X)$.

Таблица 2

Различные варианты применения порождающих полиномов

№	А	ФС1(А)	A^*	ФС2(A^*)	A^*_7	ФС2(A^*_7)	E^*_7	ФС2(E^*_7)
	1	2	3	4	5	6	7	8
1	1	100	1	100	0	000	1	100
2	1	110	0	010	0	000	0	010
3	0	011	0	001	0	000	0	001
4	1	011	1	001	1	100	0	101
5	0	111	0	101	0	010	0	111
6	0	101	1	011	1	101	0	110
7	1	000	1	000	1	011	0	011
					*X	100	*X	100
					$*X^2$	010	$*X^2$	010
					$*X^3$	001	$*X^3$	001

ФС представляют собой регистры сдвига с линейной обратной связью (РСЛОС), выполняющие функцию деления кодового слова на порождающий полином. В 5-8 столбцах в дополнительные строках выполняется умножение последовательностей и значение ФС на X, X^2, X^3, а в общем случае – на X^{n-p} (ФС для декодера Меггитта). Анализ таблицы 2 показывает, что, во-первых, результат деления А на K(X) и A^* на $K^*(X)$ равны нулю (остаток от деления кодового слово, записанного в разном порядке и деленного на двойственные полиномы равен нулю, что означает отсутствие ошибки). Во-

вторых, результаты деления реальной последовательности A^*_7 с ошибкой и последовательности ошибки $E^*_7 = A + A^*_7$ совпадают, что позволяет рассматривать только последовательности ошибок вне зависимости от реальных значений кодовых слов (такой же результат будет для любых одиночных ошибок). В-третьих, при реализации ФС в виде РСЛОС, выполняющего функцию умножения на полином X^{n-p} и деления на двойственный полином последовательности кодового слова в порядке обратного следования дает остаток из всех нулей и последней единицы (как и в обычном декодере Меггитта), что дает преимущества при построении схемы исправления в декодере.

Таким образом, при предлагаемой схемной реализации циклических кодов кодер остается прежним. Декодер имеет следующие отличия. В своем составе он содержит реверсивный циклический n-разрядный буферный регистр, формирователь синдрома и схему исправления ошибки. За первые n тактов принятое кодовое слово записывается в буферный регистр и одновременно формируется синдром. Затем направление сдвига в буферном регистре изменяется и за следующие n тактов с помощью формирователя синдрома и схемы исправления декодер устраняет ошибку и кодовое слово уже без ошибки перезаписывается в буферный регистр. За третьи n тактов направление сдвига в буферном регистре снова меняется и на выходе появляется исправленное кодовое слово.

1. Richard E.Blahut. Algebraic Codes for Data Transmission/ Cambridge University Press, 2012. – 498 p.
2. Рахман П.А. Основы защиты данных от разрушения. Коды Рида-Соломона/ Интернет-ресурс. – Режим доступа: URL http://icc.mpei.ru/documents/00000885.pdf Загл. с экрана.
3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 595 с.: ил.
4. 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.

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.