УДК 519.725, 625.7, 681.3

Альтернативный метод укорачивания циклических кодов

Дяченко О.Н., Дяченко В.О
Донецкий национальный технический университет, г. Донецк
кафедра компьютерной инженерии
E-mail: dyachenkoon@gmail.com

Аннотация

Дяченко О.Н., Дяченко В.О. Альтернативный метод укорачивания циклических кодов. *Предлагается использование альтернативного метода укорачивания циклических кодов, исправляющих пакеты ошибок. В статье обоснована актуальность использования укорачивания кодов, в особенности для кодов, исправляющих пакеты ошибок большой длины. Выполнен анализ существующих способов, а также их аппаратной реализации. Рассмотрена идея предлагаемого метода укорачивания, сначала на примере кода Хэмминга, а затем для кодов, исправляющих пакеты ошибок. По сравнению с традиционными подходами укорачивания кодов предлагаемый авторами отличается простотой применения, в том числе для кодов с большим параметром укорачивания.*

Введение. В настоящее и обозримое будущее время динамичные изменения в различных сферах деятельности общества характеризуются лавинообразным ростом объемов самой различной информации: военной, коммерческой, мультимедийной, социально-политической, производственной, научной, технической, культурной и др. Все это признаки информационной революции.

В основе многих выдвинутых ныне теорий и концепций, объясняющих глубинные изменения в экономической и социальной структурах передовых стран мира, начавшиеся в середине XX в., лежит признание нарастания значения информации в жизни общества.

Существует множество различных теорий и классификаций научно-технических революций в истории человечества.

Э. Тоффлер выделяет три «волны» в развитии общества: аграрная при переходе к земледелию; индустриальная во время промышленной революции; информационная при переходе к обществу, основанному на знании (постиндустриальному).

А. И. Ракитов выделяет пять информационных революций: появление и внедрение в деятельность и сознание человека языка; изобретение письменности; изобретение книгопечатания; изобретение телеграфа и телефона; изобретение компьютеров и появление Интернета.

Признанный классик теории постиндустриализма Д. Белл выделяет три технологических революции: изобретение паровой машины в XVIII веке; научно-технологические достижения в области электричества и химии в XIX веке; создание компьютеров в XX веке. Белл утверждал, что, подобно тому, как в результате промышленной революции появилось конвейерное производство, повысившее производительность труда и подготовившее общество массового потребления, так и теперь должно возникнуть поточное производство информации, обеспечивающее соответствующее социальное развитие по всем направлениям.

В последние десятилетия достижения в области внедрения информационных технологий являются одним из определяющих факторов экономического потенциала общества. В результате появляется и развивается информационная инфраструктура, которая предоставляет новые услуги, такие как дистанционное образование, заказ билетов для транспорта, телеработа, телемедицина, электронная торговля, интернет-банкинг, оплата счетов и др.

Тенденция к увеличению количества информации, которую необходимо хранить, обрабатывать и передавать, неизбежно приводит к требованиям обеспечения ее достоверности. Эту задачу призваны выполнять коды, обнаруживающие и исправляющие ошибки.

Одними из наиболее эффективных для исправления ошибок являются циклические коды. Эти коды нашли широкое применение благодаря простой аппаратной реализации и высоким корректирующим способностям. Некоторые специалисты помехоустойчивого кодирования уже давно решили, что все основные теоретические вопросы относительно циклических кодов решены и свое внимание перенесли на совершенствование и разработку других кодовых конструкций [1]. Поэтому инженерам-практикам приходится самим предлагать решения для каждой конкретной технической задачи вне связи с общей стратегией развития циклических кодов.

В связи с этим решение практических вопросов построения и аппаратной реализации циклических кодов являются актуальными, тем более, учитывая все большую их популярность и востребованность для различных сфер применения.

При реализации циклических кодов во многих случаях приходится их укорачивать (например, укороченные коды Рида-Соломона над полем Галуа $GF(2^8)$ для CD-ROM, DVD и цифрового телевидения высокого разрешения - формат HDTV) [2-4, 6]. Существует несколько методов укорачивания кодов. Один из них основан на использовании двойственных порождающих полиномов. В данной работе предлагается альтернативный метод применения двойственных полиномов для кодирования и декодирования укороченных кодов, что дает преимущества при реализации кодов, исправляющих пакеты ошибок большой длины.

Основная идея альтернативного метода применения двойственных полиномов. Наиболее популярны в настоящее время 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]. Вместе с тем, циклический код Хэмминга, исправляющий одиночные ошибки, заслуживает особого внимания, поскольку является фундаментом для понимания принципов построения более мощных кодов. Поэтому, основную идею альтернативного метода применения двойственных полиномов для укорачивания циклически кодов рассмотрим на примере кода Хэмминга.

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 (deg p(z)=deg $p^*(z)$) с умножением принятого слова на полином X^{n-k+i} , где n-k= deg p(z). Существует зависимость между значениями элементов в двоичном виде. Причем рассматривать их нужно в обратном порядке следования двоичных символов, что соответствует умножению элемента от (X^{-1}) на $X^{\deg p(z)-1}$. 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.

Ненулевые остатки от деления на порождающий полином состоят из двух подмножеств. Общее количество элементов этих подмножеств равны длине исходного кода n (сумме параметра укорачивания i и 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.

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

Укороченные коды, исправляющие пакеты ошибок. Предположим, что код (511, 499) потребовалось укоротить до (272, 260)-кода [2]. 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 остаток $a(X) = R_{g(X)}[X^{251}]$. В [2] 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 R и умножив $R(X^{-1})$ 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.

Систематический код, исправляющий пакеты ошибок.

Определение параметров исходного кода.

Параметр укорачивания i = 4

(3*7-4, 3*3-4), исходный код: (7, 3), образующий полином: $C(X) = X^4 + X^3 + X^2 + 1$, b = 2. => j = 3, i = 4, где j параметр перемежения.

Определение параметров кода.

(3*7-4, 3*3-4) = (17, 5)

n = 17, k = 5

Определение длины исправляемого пакета ошибок

b' = j*b = 3*b = 3*2 = 6 (где b – длина исправляемого пакета ошибок для данного кода).

Определение образующего полинома C'(X) и $C^{*'}(X)$.

$C'(X) = X^{j*4} + X^{j*3} + X^{j*2} + 1 = X^{12} + X^9 + X^6 + 1$, $C^{*'}(X) = X^{12}(X^{-12}+X^{-9}+X^{-6}+1)=X^{12}+X^6+X^3+1$

Определение минимального количества проверочных символов (p).

p = n – k = 17 – 5 = 12

Определение остатка от деления $X^{(p+i)}$ на образующий полином $R_{C'(X)}[X^{p+i}]$.

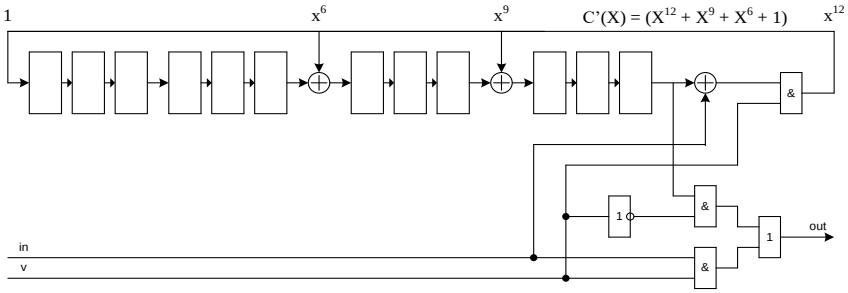
$$\begin{array}{l|l} X^{16} & X^{12}+X^9+X^6+1 \\ \underline{X^{16}+X^{13}+X^{10}+X^4} & X^4+X \\ X^{13}+X^{10}+X^4 & \\ \underline{X^{13}+X^{10}+X^7+X} & \\ X^7+X^4+X & \end{array}$$

$R_{C'(X)}[X^{p+i}] = \mathbf{X^7 + X^4 + X}$, $R_{C^{*'}(X)}[X^{n-1}] = X^{10} + X^7 + X^4$

$R_{C'(X)}[X^{p+i}] = X^{11}(X^{-10}+X^{-7}+X^{-4}) = \mathbf{X^7 + X^4 + X}$

Построение кодера для кода (17, 5).

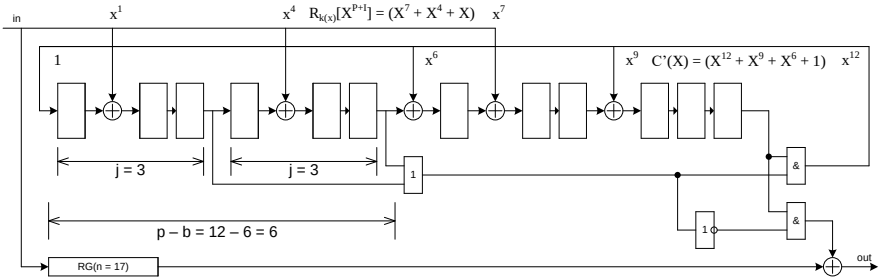
Кодер



Сигнал V используется для переключения ключей кодера. Он должен быть высокого уровня первые k=5 тактов и потом переключаться в низкий уровень.

Построение декодера для кода (17, 5).

Декодер



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

Список литературы

1. Семеренко В. П. Теория и практика CRC кодов: новые результаты на основе автоматных моделей // Восточно-Европейский журнал передовых технологий. – 2015. – 4/9. – С. 38-48.

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

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. націонал. 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.

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.

7. Дяченко В.О., Дяченко О.Н. Циклическое кодирование цифровой информации на основе двойственных полиномов // Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике: материалы II Международной научно-практической конференции (Азов, 19 мая 2015 г.) [Электронный ресурс]. – Ростов н/Д, ДГТУ, 2015. – С. 71-76. – Режим доступа: http://atidstu.ru/atidgtu-rf/node/1163.