ДК 519.725, 625.7, 681.3

О. Н. Дяченко, В. О. Дяченко

Альтернативный метод укорачивания циклических кодов

Обоснована актуальность использования альтернативного метода укорачивания кодов, исправляющих пакеты ошибок большой длины. Выполнен анализ существующих способов и их аппаратной реализации. Предлагаемый авторами метод (по сравнению с традиционными методами укорачивания кодов) отличается простотой применения, в том числе для кодов с большим параметром укорачивания.

Ключевые слова: поле Галуа, циклические коды, укороченные коды, двойственный полином, порождающий полином, пакет ошибок.

O. N. Dyachenko, V. O. Dyachenko

Alternative method for shortening cyclic codes

The applicability of an alternative method for shortening codes to correct large error bursts has been substantiated. Analysis of existing methods and their hardware implementation has been performed. The method suggested by the authors is characterized by simplicity of use (as compared to conventional code shortening methods), including for codes with large shortening parameter.

Key words: Galois field, cyclic codes, shortened codes, dual polynomial, generator polynomial, error burst.

Динамичные изменения в различных сферах деятельности современного общества характеризуются лавинообразным ростом объёма самой различной информации: военной, коммерческой, мультимедийной, социально-политической, производственной, научной, технической, культурной и др.

Основу большинства теорий и концепций, проливающих свет на глубинные изменения в экономической и социальной сферах передовых стран мира, начавшиеся в середине XX в., составляет признание неоспоримой значимости информации в жизни общества.

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

Так, Элвин Тоффлер выделяет три этапа в развитии общества:

– аграрный (переход к земледелию);
– индустриальный (период промышленной революции);
– информационный (переход к обществу, основанному на знании, — постиндустриальному).

Анатолий Ильич Ракитов отмечает пять информационных революций:

– возникновение и внедрение в деятельность и сознание человека языка;
– изобретение письменности;

– изобретение книгопечатания;
– изобретение телеграфа и телефона;
– изобретение компьютеров и появление Интернета.

А признанный классик теории постиндустриализма Дэниел Белл выделяет три технологических революции:
– изобретение паровой машины в XVIII в.;
– научно-технологические достижения в области электричества и химии в XIX в.;
– создание компьютеров в XX в.

По мнению Белла, «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» [1, с. 152].

Достижения в области внедрения информационных технологий служат одним из решающих факторов экономического развития общества в последние десятилетия. Стремительно развивающаяся информационная инфраструктура предоставляет новые услуги — это и дистанционное образование, и покупка билетов онлайн, и телеработа, телемедицина, электронная торговля, интернет-банкинг, оплата счетов и др.

Неуклонный рост количества информации, которую необходимо хранить, обрабатывать и передавать, неизбежно предполагает и обеспечение её достоверности. Это задача для кодов, обнаруживающих и исправляющих ошибки.

Наиболее эффективны для исправления ошибок — циклические коды, которые, благодаря простой аппаратной реализации и высоким корректирующим свойствам, нашли широкое применение в этой сфере. Специалисты в области помехоустойчивого кодирования уже давно переключили свое внимание с циклических кодов на совершенствование и разработку других кодовых конструкций [2]. Поэтому инженеры-практики вынуждены предлагать решения для каждой конкретной технической задачи вне связи с общей стратегией развития циклических кодов.

Отсюда и актуальность решения практических вопросов построения и аппаратной реализации циклических кодов.

При реализации циклических кодов зачастую возникает необходимость их укорачивать (например, укороченные коды Рида — Соломона над полем Галуа $GF(2^8)$ для CD-ROM, DVD и цифрового телевидения высокого разрешения — формат HDTV) [3—5; 6]. Существует несколько методов укорачивания кодов. В основе одного из них —использование двойственных порождающих полиномов.

Мы предлагаем альтернативный метод применения двойственных полиномов для кодирования и декодирования укороченных кодов. Это даёт неоспоримые преимущества при реализации кодов, исправляющих пакеты ошибок большой длины.

Основная идея альтернативного метода применения двойственных полиномов. Сегодня наиболее популярны 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 мн. др. [2—5; 7]. 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 циклических кодов рассмотрим на примере кода Хэмминга.

Основное различие 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 (табл. 1).

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

Окончание таблицы 1

$p(z) = z^4 + z + 1$		$p^*(z) = z^4 + z^3 + 1$	
В виде степени	**В двоичном виде**	**В виде степени**	**В двоичном виде**
α^1	0010	α^1	0010
α^2	0100	α^2	0100
α^3	1000	α^3	1000

Анализ табл. 1 показывает взаимосвязь элементов этих полей. Добавление в таблицу четырёх строк ($\deg p(z) = \deg p^*(z)$) соответствует умножению принятого слова на полином X^{n-k+i}, где $n - k = \deg p(z)$. Существует зависимость между значениями элементов в двоичном виде. Причём рассматривать их нужно в обратном порядке следования двоичных символов, что соответствует умножению элемента от (X^{-1}) на $X^{\deg p(z)-1}$. Например, $\alpha^4 = 0011$ и $\alpha^{14} = \alpha^{-1} = 1100$, $\alpha^5 = 0110$ и $\alpha^{13} = \alpha^{-2} = 0110$, $\alpha^6 = 1100$ 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 равно длине исходного кода n (сумме параметра укорачивания i и значения новой длины укороченного кода). Пересекаются эти подмножества на граничных элементах, и они зеркально равны. Учитывая эти свойства, можно получить остаток от деления полинома X^{n-k+i} на порождающий полином без явного учёта i, а на основе только длины укороченного кода и двойственного полинома.

Укороченные коды, исправляющие пакеты ошибок. Предположим, код (511, 499) необходимо укоротить до (272, 260)-кода [3]. Этот код исправляет все пакеты ошибок длины не более 4. В данном случае порождающий полином $g(X) = X^{12} + X^8 + X^5 + X^3 + 1$, $X^{n-k+i} = X^{251}$, необходимо вычислить остаток $a(X) = R_{g(X)}[X^{251}]$. В работе [3] полином X^{251} представлен в виде $X^{251} = (X^{12})^{16}(X^{12})^4(X^{11})$, чтобы воспользоваться равенством $X^{12} = X^8 + X^5 + X^3 + 1$. Повторив возведение в квадрат полинома X^{12} и проведя редукцию по модулю $g(X)$, вычислим $(X^{12})^4$ 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 определим остаток от деления полинома в степени длины нового укороченного кода, уменьшенной на единицу, т. е. X^{271}, на двойственный $g(X)$ полином

$$g^*(X) = X^{\deg g(X)} g(X^{-1}) = X^{12}(X^{-12} + X^{-8} + X^{-5} + X^{-3} + 1) =$$

$$= (X^{12} + X^9 + X^7 + X^4 + 1)$$

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 $X^{\deg g(X)-1}$, найдём 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. Таким образом, становится возможной реализация кодов с большим параметром укорачивания и длиной исправляемого пакета ошибок.

Систематический код, исправляющий пакеты ошибок:

Определение параметров исходного кода: (7, 3)-код, образующий полином: $C(X) = X^4 + X^3 + X^2 + 1$, длина исправляемого пакета ошибок $b = 2$. Пусть параметр укорачивания $i = 4$; параметр перемежения $j = 3$. Получаем перемежённый укороченный $(3 \cdot 7 - 4, 3 \cdot 3 - 4)$-код.

Определение параметров кода:

$$(3 \cdot 7 - 4, 3 \cdot 3 - 4) = (17, 5);$$

$$n = 17, k = 5.$$

Определение длины исправляемого пакета ошибок:

$$b' = j \cdot b = 3 \cdot b = 3 \cdot 2 = 6,$$

где b — длина исправляемого пакета ошибок для данного кода.

Определение образующего полинома $C'(X)$ и $C^{*\prime}(X)$:

$$C'(X) = X^{j \cdot 4} + X^{j \cdot 3} + X^{j \cdot 2} + 1 = X^{12} + X^9 + X^6 + 1;$$

$$C^{*\prime}(X) = X^{12}(X^{-12} + X^{-9} + X^{-6} + 1) = X^{12} + X^6 + X^3 + 1.$$

Определение минимального количества проверочных символов (p):

$$p = n - k = 17 - 5 = 12.$$

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

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

$$X^{13} + X^{10} + X^4$$

$$\underline{X^{13} + X^{10} + X^7 + X}$$

$$X^7 + X^4 + X$$

$$R_{C'(X)}[X^{p+i}] = X^7 + X^4 + X;$$

$$R_{C^{*}(X)}[X^{n-1}] = X^{10} + X^{7} + X^{4};$$

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

Сигнал V используется для переключения ключей кодера. Он должен быть высокого уровня первые $k = 5$ тактов и потом переключаться в низкий уровень (рис. 1). Построение декодера для кода (17, 5) представлено на рис. 2.

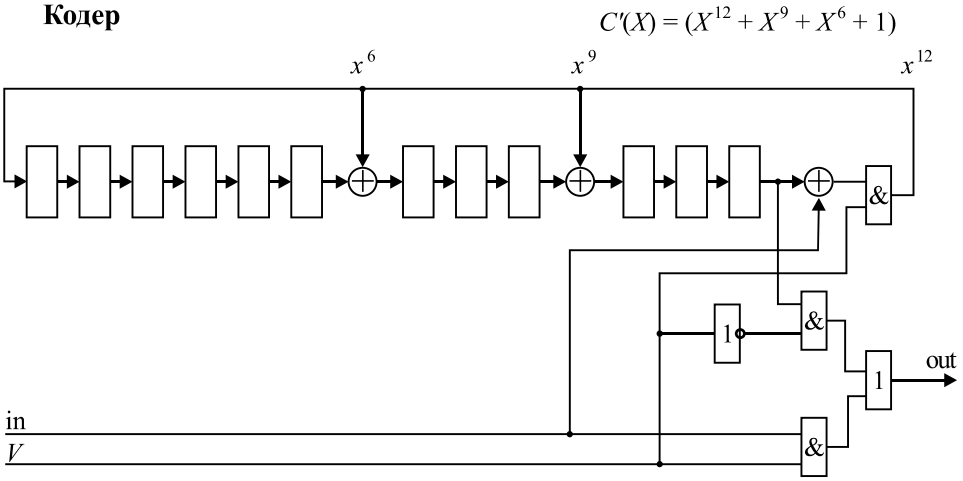

Рис. 1. Построение кодера для кода (17, 5)

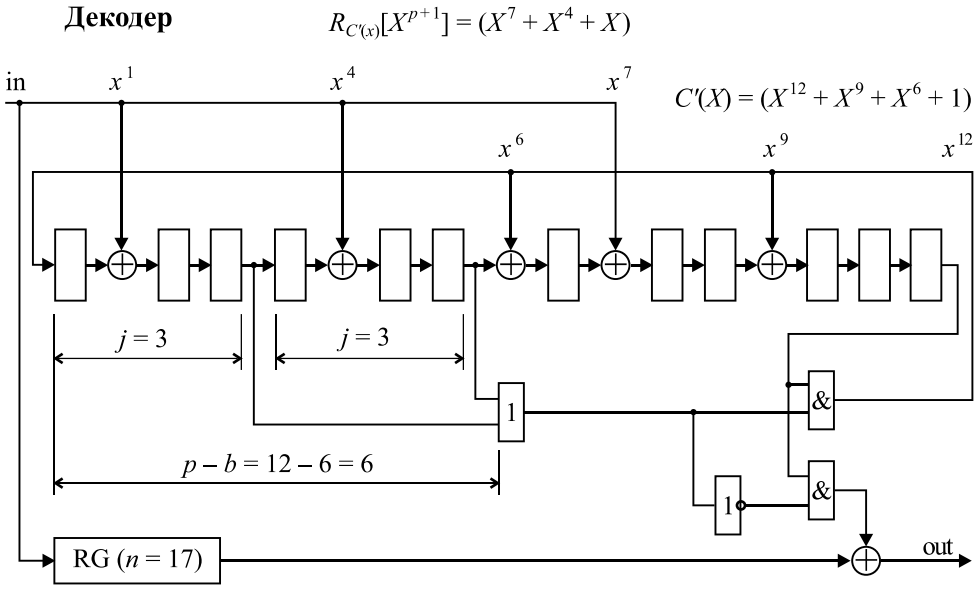

Рис. 2. Построение декодера для кода (17, 5)

Таким образом, предложенный авторами метод построения укороченных циклических кодов (в том числе и кодов с большой длиной исправляемого пакета ошибок) отличается простотой применения. Однако для таких кодов можно использовать и традиционную аппаратную или программную реализацию кодеров и декодеров.

Литература

1. *Белл Д.* Грядущее постиндустриальное общество. Опыт социального прогнозирования: Пер. с англ. 2-е изд., испр. и доп. М.: Academia, 2004. 788 с.
2. *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.
3. *Blahut R. E.* Algebraic codes for data transmission. Cambridge: Cambridge University Press, 2012. 498 p.
4. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976. 595 с.
5. *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, Донецьк, 22—23 квітня 2014 р. Донецьк: ДонНТУ, 2014: в 2 т. Т. 2. С. 72—78.
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, Донецк, 20—22 мая 2015 г. Донецк: ДонНТУ, 2015. С. 130—136.
7. *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: Мат-лы международной научно-практической конференции, Азов, 19 мая 2014 г. Ростов-на-Дону: ДГТУ, 2014. С. 18—22.
8. *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: Мат-лы II международной научно-практической конференции, Азов, 19 мая 2015 г. Ростов-на-Дону: ДГТУ, 2015. С. 71—76.