УДК 621.391.15

Кубицкий В. И.

О ФУНКЦИОНАЛЬНОСТИ КОДОВ ЛАГРАНЖА В ЗАДАЧАХ ПРОГРАММИРОВАНИЯ

ГосНИИ «Аэронавигация» (Россия, Москва)

На примере обобщенных кодов Хэмминга доказывается, что при переходе от кодов Лагранжа к кодам Рида–Соломона теряются функциональные свойства кодов Лагранжа. Показано, как необходимо выбирать узлы интерполирования при переходе от кодов Лагранжа с весом Хэмминга равным 3 к обобщенным кодам Хэмминга.

Работоспособность систем обработки данных в значительной степени зависит от достоверности ввода, хранения и обработки информации, а также от помехоустойчивости передачи ее по каналам связи. Основным средством обеспечения высокой помехоустойчивости сложной системы является введение избыточности, необходимой для коррекции ошибок, возникающих при работе системы и ее звеньев. Одним из способов введения избыточности является помехоустойчивое кодирование.

Идеи избыточного кодирования находят применение не только при передаче информации по каналам связи, но при переработке ее в вычислительных системах. Существует множество алгебраических и арифметических кодов, предназначенных для контроля и исправления ошибок как в процессах передачи и хранения информации, так и в арифметических процедурах и некоторых типах редактирования данных. Результаты исследований Р. Элайса [1], В. Питерсона и М. Рабина [2], С. Винограда [3] говорят о том, что использование групповых (*n*, *k*)-кодов для защиты функциональных преобразований малоэффективно. Расширить рамки классов функциональных преобразований, защищаемых кодами, позволяет использование биноидных кодов [4], частным случаем которых можно рассматривать кольцевые коды. Для защиты информации от ошибок в системах обработки данных лучше всего подходят коды с параллельной структурой, достаточно близкие к технологии побайтовой обработки данных, принятой для большинства вычислительных систем.

К кодам с параллельной структурой относятся коды Лагранжа [5], являющиеся кольцевыми кодами. Эти коды обладают следующими важными свойствами:

- распараллеливание всех важнейших процедур на языке данного кода;
- повышение надежности процессов хранения, передачи и обработки информации;
- экономичность аппаратурных затрат на процедуры кодирования и декодирования;
- сведение к нулю влияния на производительность процессора временных затрат на кодирование и декодирование;
- совместимость с кодами, применяемыми на действующих вычислительных средствах.

В [6] показано, что коды Лагранжа в линейной части изоморфны широко применяемым кодам Рида-Соломона (РС-кодам) [7], но в нелинейной части они выгодно отличаются от РС-кодов. Так коды Лагранжа можно применять для защиты функциональных преобразований [8]÷[10]. Это свойство является важной характеристикой кодов Лагранжа.

Используя линейный изоморфизм между кодами Лагранжа и РС-кодами можно свести код Лагранжа к РС-коду. На примере перехода от кодов Лагранжа к обобщенным кодам Хэмминга покажем, что при этом теряются функциональные свойства кодов Лагранжа. Будем рассматривать параллельный [5] и последовательный [11]÷[12] алгоритмы кодирования кодом Лагранжа.

Пусть:

$S=\{x_o,x_1,\cdots,x_s\}$ – множество информационных узлов мощности k;

$T=\{\beta_1,\beta_2,\cdots,\beta_r\}$ – множество контрольных узлов мощности r;

S,T – подмножества поля F_q (здесь $q=2^m$);

$F_q = (S \cup T)$;

$f_0, f_1, \ldots, f_s$ – информационные символы кодового слова;

$n=2^m$ – длина кодового слова.

1. Параллельный алгоритм кодирования

При параллельном алгоритме кодирования контрольные символы полного кода Лагранжа с весом Хэмминга равным 3 определяются из соотношений:

$$f(\beta_1) = \sum_{i=0}^{s} f_i L_S^{(i)}(\beta_1),$$

$$f(\beta_2) = \sum_{i=0}^{s} f_i L_S^{(i)}(\beta_2),$$

где: f_i – значения кодового полинома в информационных узлах;

$L_S^{(i)}(\beta_1) = -\dfrac{x_i - \beta_2}{\beta_1 - \beta_2}$ – фундаментальные интерполяционные полиномы Лагранжа в контрольном узле β_1;

$L_S^{(i)}(\beta_2) = -\dfrac{x_i - \beta_1}{\beta_2 - \beta_1}$ – фундаментальные интерполяционные полиномы Лагранжа в контрольном узле β_2.

Для преобразования кода Лагранжа в код Хэмминга необходимо информационные символы умножить на коэффициент λ_i, узлы интерполирования подбирать так, чтобы выполнялись условия:

$$\lambda_i L_S^{(i)}(\beta_1) = i + 2\,, \tag{1}$$

$$\lambda_i L_S^{(i)}(\beta_2) = 1\,. \tag{2}$$

Тогда контрольные символы кода Хэмминга будут формироваться по следующему правилу:

$$f'(\beta_1) = \sum_{i=0}^{s} f_i \lambda_i L_S^{(i)}(\beta_1) = \sum_{i=0}^{s} (i+2) f_i,$$

$$f'(\beta_2) = \sum_{i=0}^{s} f_i \lambda_i L_S^{(i)}(\beta_2) = \sum_{i=0}^{s} f_i.$$

Указанные преобразования равносильны следующему:

$(f_0, f_1, \ldots, f_s, f'_{s+1}, f'_{s+2}) \Leftrightarrow f(x)$ – для кода Хэмминга,

$(f_0\lambda_0, f_1\lambda_1, \ldots, f_s\lambda_s, \alpha_{s+1}, \alpha_{s+2}) \Leftrightarrow <f(x)\cdot\lambda(x)|_{p(x)}$ – для кода Лагранжа,

где $p(x)$ – многочлен степени $(n–2)$.

Из [6] известно следующее:

Если кодовым словам $A=(a_0, a_1, \ldots, a_{n-1})$ и $B=(b_0, b_1, \ldots, b_{n-1})$ отвечают полиномы Лагранжа $A(x)$ и $B(x)$, степени которых удовлетворяют условию ст.$A(x)$+ст.$B(x)<n–2t$, то композиция (умножение) кодовых слов $A*B==(a_0 \cdot b_0, a_1 \cdot b_1, \ldots, a_{n-1} \cdot b_{n-1})$ также является кодовым словом, т. е. сохраняется способность обнаруживать и исправлять ошибки кратности $\leq t$.

Для того чтобы установить сохраняются ли функциональные свойства кодов Лагранжа при переходе к кодам Хэмминга, необходимо предварительно определить степень полинома

$$\lambda(x) = \sum_{i=0}^{s} \lambda_i L_S^{(i)}(x), \tag{3}$$

где $L_S^{(i)}(x) = -\prod_{\substack{i=0 \\ j \neq i}}^{s} \dfrac{x - x_j}{x_i - x_j}$, $s=n–3$.

Утверждение 1. Степень полинома $\lambda(x) = \sum_{i=0}^{n-3} \lambda_i L_S^{(i)}(x)$ равна $(n–3)$.

Доказательство. Из выражения (2) определим $\lambda_i = 1/L_S^{(i)}(\beta_2)$ и, подставив в (3), произведем преобразование. В результате получим:

$$\lambda(x) = \sum_{i=0}^{n-3} \frac{L_S^{(i)}(x)}{L_S^{(i)}(\beta_2)} = -\sum_{i=0}^{n-3} \frac{\beta_2 - \beta_1}{x_i - \beta_1} \cdot L_S^{(i)}(x) = -(\beta_2 - \beta_1) \sum_{i=0}^{n-3} \frac{(x-x_0)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_{n-3})}{(x_i-x_0)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_{n-3})} \cdot \frac{1}{(x_i-\beta_1)} \cdot \frac{(x_i-\beta_2)}{(x_i-\beta_2)} =$$

$$= -(\beta_2 - \beta_1) \sum_{i=0}^{n-3} \frac{(x-x_0)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_{n-3})(x_i-\beta_2)}{1} =$$

$$= -(\beta_2 - \beta_1) \sum_{i=0}^{n-3} \varphi_i(x) \cdot (x_i - \beta_2) = -(\beta_1 - \beta_2) \left[\sum_{i=0}^{n-3} \varphi_i(x) \cdot x_i - \sum_{i=0}^{n-3} \varphi_i(x) \cdot \beta_2 \right] = -(\beta_2 - \beta_1)[\Phi_1(x) - \Phi_2(x)]\,.$$

Полином $\Phi_2(x)$ имеет четное $(n–2)$ количество слагаемых полиномов $\varphi_i(x)$ степени $(n–3)$ с одинаковыми коэффициентами β_2 при неизвестных старшей степени. В сумме эти коэффициенты дают 0. Значит, ст. $\Phi_2(x) <n–3$.

Полином $\Phi_1(x)$ имеет четное (n–2) количество слагаемых полиномов $\varphi_i(x)$ степени (n–3) с различными коэффициентами x_i при неизвестных старшей степени. В сумме эти коэффициенты не дают 0, так как сумма любых различных элементов аддитивной группы конечного поля, количество которых равно 2^m–2, всегда не равна 0. Значит, ст. $\Phi_1(x)$ =n–3.

Отсюда, ст. $\left[\Phi_1(x)-\Phi_2(x)\right]$ = n–3. Так как коэффициент $-(\beta_2-\beta_1)$ степени полинома не меняет, то ст. $\lambda(x)$ = n–3.

Этот результат позволяет сделать следующее утверждение:

Утверждение 2. Произведение двух кодовых слов, которым отвечают полиномы $a(x)=\langle f(x)\cdot\lambda(x)|_{p(x)}$ и $b(x)=\langle q(x)\cdot\lambda(x)|_{p(x)}$, где ст. $\lambda(x)$ = n–3, не является кодовым словом.

Доказательство. Для того чтобы произведение кодовых слов $a(x)\cdot b(x)$ было кодовым словом необходимо, чтобы выполнялось равенство:

$$\langle a(x)\cdot b(x)|_{p(x)}=$$
$$=a(x)\cdot b(x)=\langle f(x)\cdot\lambda(x)|_{p(x)}\cdot\langle q(x)\cdot\lambda(x)|_{p(x)}.$$

То есть сумма степеней полиномов *a(x)* и *b(x)* должна быть меньше (n-3). Но

$$\langle a(x)\cdot b(x)|_{p(x)}=\langle\langle f(x)\cdot\lambda(x)|_{p(x)}\cdot\langle q(x)\cdot\lambda(x)|_{p(x)}|_{p(x)}=$$
$$=\langle f(x)\cdot\lambda(x)\cdot q(x)\cdot\lambda(x)|_{p(x)}=\langle A(x)|_{p(x)}.$$

Так как ст.$\lambda(x)$=n-3, ст.$f(x)$≤n-3 и ст.$q(x)$ ≤n-3, то ст.$A(x)$≥2(n-3) и ст.[$a(x)$·ст.$b(x)$] ≥2(n-3).

Значит, ст.$a(x)$+ст.$b(x)$>n-3 и произведение кодовых слов $a(x)$·ст.$b(x)$ не является кодовым словом.

Отсюда следует вывод о том, что при переходе от кодов Лагранжа к обобщенным кодам Хэмминга теряются функциональные свойства кодов Лагранжа.

Покажем, как при переходе от кодов Лагранжа к обобщенным кодам Хэмминга необходимо выбирать узлы интерполирования.

Из выражений (1) и (2) получаем соотношение:

$$i+2=\frac{L_S^{(i)}(\beta_1)}{L_S^{(i)}(\beta_2)}.$$

Подставляя сюда приведенные выше выражения для полиномов $L_S^{(i)}(\beta_1)$ и $L_S^{(i)}(\beta_2)$, получим выражение для выбора интерполяционных узлов:

$$x_i=\frac{(i+2)(\beta_1-\beta_2)\beta_1-(\beta_2-\beta_1)\beta_2}{(i+2)(\beta_1-\beta_2)-(\beta_2-\beta_1)}=\frac{(i+2)\beta_1+\beta_2}{(i+2)+1}.$$

Учитывая, что арифметические операции по кодированию выполняются в конечном поле $GF(2^m)$, имеем:

$$x_i=\frac{(i+2)\beta_1\oplus\beta_2}{(i+2)\oplus 1},$$

где $\oplus$ – операция сложения в конечном поле $GF(2^m)$.

При таком выборе интерполяционных узлов значения фундаментальных интерполяционных полиномов Лагранжа в контрольных узлах будут вычисляться из выражений:

$$L_S^{(i)}(\beta_1)=-\frac{(i+2)(\beta_1-\beta_2)}{(i+2)(\beta_1-\beta_2)\ -(\beta_2-\beta_1)}=-\frac{(i+2)}{(i+2)+1},$$

$$L_S^{(i)}(\beta_2)=\frac{(\beta_2-\beta_1)}{(i+2)(\beta_1-\beta_2)-(\beta_2-\beta_1)}=-\frac{1}{(i+2)+1};$$

или для конечного поля $GF(2^m)$:

$$L_S^{(i)}(\beta_1)=\frac{(i+2)}{(i+2)\oplus 1},$$

$$L_S^{(i)}(\beta_2)=\frac{1}{(i+2)\oplus 1}.$$

2. Последовательный алгоритм кодирования

При последовательном алгоритме кодирования контрольные символы полного кода Лагранжа с весом Хэмминга равным 3 определяются из соотношений [13]:

$$f(\beta_1)=\sum_{i=0}^{s} f_i L_S^{(i)}(\beta_1),$$

$$f(\beta_2)=\sum_{i=0}^{s+1} f_i L_{S_1}^{(i)}(\beta_2),$$

где: $S_1=S\cup\{\beta_1\}$;

$L_S^{(i)}(\beta_1)=-\dfrac{x_i-\beta_2}{\beta_1-\beta_2}$ – фундаментальные интерполяционные полиномы Лагранжа в контрольном узле β_1;

$L_{S_1}^{(i)}(\beta_2) = -1$ – фундаментальные интерполяционные полиномы Лагранжа в контрольном узле β_2.

Для преобразования кода Лагранжа в код Хэмминга необходимо, как и в случае параллельного алгоритма кодирования, информационные символы умножить на коэффициент λ_i. Узлы интерполирования подбираются, исходя из условий:

$$\lambda_i L_S^{(i)}(\beta_1) = i + 2 \ , \qquad (4)$$

$$\lambda_i L_{S_1}^{(i)}(\beta_2) = 1 \ . \qquad (5)$$

Контрольные символы кода Хэмминга вычисляются из соотношений:

$$f'(\beta_1) = \sum_{i=0}^{s} f_i \lambda_i L_S^{(i)}(\beta_1) = \sum_{i=0}^{s} (i+2) f_i,$$

$$f'(\beta_2) = \sum_{i=0}^{s+1} f_i \lambda_i L_{S_1}^{(i)}(\beta_2) = \sum_{i=0}^{s} f_i \quad .$$

Определим степени полиномов:

$$\lambda(x) = \sum_{i=0}^{s} \lambda_i L_S^{(i)}(x) \quad , \qquad (6)$$

где $L_S^{(i)}(x) = -\prod_{\substack{i=0 \\ j \neq i}}^{s} \frac{x - x_j}{x_i - x_j}$;

$$\lambda'(x) = \sum_{i=0}^{s+1} \lambda_i L_{S_1}^{(i)}(x) \quad , \qquad (7)$$

где $L_{S_1}^{(i)}(x) = -\prod_{\substack{i=0 \\ j \neq i}}^{s+1} \frac{x - x_j}{x_i - x_j}$.

Из утверждения 1 следует, что ст.$\lambda(x)$=n–3.

Утверждение 3. Степень полинома $\lambda'(x) = \sum_{i=0}^{n-2} \lambda_i L_{S_1}^{(i)}(x)$ равна (n-3).

Доказательство. Из выражения (5) определим $\lambda_i = 1 / L_{S_1}^{(i)}(\beta_2)$ и, подставив в (7), произведем преобразование. В результате получим:

$$\lambda(x) = \sum_{i=0}^{n-2} \frac{L_{S_1}^{(i)}(x)}{L_{S_1}^{(i)}(\beta_2)} = -\sum_{i=0}^{n-2} L_S^{(i)}(x) = -\sum_{i=0}^{n-2} \frac{(x - x_0)...(x - x_{i-1})(x - x_{i+1})...(x - x_{n-2})}{(x_i - x_0)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_{n-2})} \cdot \frac{(x_i - \beta_2)}{(x_i - \beta_2)} =$$

$$= -\sum_{i=0}^{n-2} \frac{(x - x_0)...(x - x_{i-1})(x - x_{i+1})...(x - x_{n-2})(x_i - \beta_2)}{1} = -\sum_{i=0}^{n-2} \varphi_i'(x) \cdot (x_i - \beta_2) =$$

$$= -\left[\sum_{i=0}^{n-2} \varphi_i'(x) \cdot x_i - \sum_{i=0}^{n-2} \varphi_i'(x) \cdot \beta_2\right] = -\left[\Phi_1'(x) - \Phi_2'(x)\right] .$$

Полином $\Phi_2'(x)$ имеет нечетное (n–1) количество слагаемых полиномов $\varphi_i'(x)$ степени (n–2) с одинаковыми коэффициентами β_2 при неизвестных старшей степени. В сумме эти коэффициенты равны β_2. Значит, ст. $\Phi_2'(x)$ =n–2.

Полином $\Phi_1'(x)$ имеет нечетное (n–1) количество слагаемых полиномов $\varphi_i'(x)$ степени (n-2) с различными коэффициентами x_i при неизвестных старшей степени. В сумме эти коэффициенты равны β_2, так как сумма всех элементов аддитивной группы конечного поля, количество которых равно 2^m (включая элемент β_2), всегда равна 0. Значит, ст. $\Phi_1'(x)$ =n–2.

Так как сумма коэффициентов при неизвестных старшей степени полинома $\Phi_1'(x)$ равна сумме коэффициентов при неизвестных старшей степени полинома $\Phi_2'(x)$, то ст. $\left[\Phi_1'(x) - \Phi_2'(x)\right]$<$n$–2=$n$–3. Значит, ст. $\lambda'(x)$ = n–3.

Полученные результаты подтверждают утверждение 2 о том, что произведение двух кодовых слов $a(x) = < f(x) \cdot \lambda(x)|_{p(x)}$ и $b(x) = < q(x) \cdot \lambda(x)|_{p(x)}$, где ст. $\lambda(x)$ = n–3, не является кодовым словом.

Значит, при переходе от кодов Лагранжа к обобщенным кодам Хэмминга теряются функциональные свойства кодов Лагранжа.

вания для последовательного алгоритма кодирования.

Из выражений (4) и (5) получаем соотношение:

$$i+2=\frac{L_S^{(i)}(\beta_1)}{L_{S_1}^{(i)}(\beta_2)} .$$

Подставляя сюда приведенные выше выражения для полиномов $L_S^{(i)}(\beta_1)$ и $L_{S_1}^{(i)}(\beta_2)$, получим выражение для выбора интерполяционных узлов:

$$x_i=(i+2)(\beta_1-\beta_2)+\beta_2 .$$

Учитывая, что арифметические операции по кодированию выполняются в конечном поле $GF(2^m)$, имеем:

$$x_i=(i+2)(\beta_1\oplus\beta_2)\oplus\beta_2 .$$

При таком выборе интерполяционных узлов значения фундаментальных интерполяционных полиномов Лагранжа в контрольных узлах будут вычисляться из выражений:

$$L_S^{(i)}(\beta_1)=-(i+2) ,$$

$$L_{S_1}^{(i)}(\beta_2)=-1 ,$$

или для конечного поля $GF(2^m)$:

$$L_S^{(i)}(\beta_1)=i+2 ,$$

$$L_{S_1}^{(i)}(\beta_2)=1 .$$

Проведенные исследования показали, что при переходе от кодов Лагранжа к обобщенным кодам Хэмминга теряются функциональные свойства кодов Лагранжа, как для параллельного, так и для последовательного алгоритмов кодирования. При таком переходе соотношения для выбора узлов интерполирования и фундаментальных полиномов Лагранжа проще для последовательного алгоритма кодирования кодом Лагранжа.

Список литературы

1. *Elais P.* Computationin the presence of noise. IBM I, Res. Devel., 1958, 2. – P. 346.

2. *Питерсон В.В., Рабин М.О.* О кодах для контроля логических операций. – В кн.: Кибернетический сборник, вып. 4. – М.: ИЛ, 1962. – С. 105-118.

3. *Vinograd S.* Codingfor logical operation. IBM I, Res. Devel., 1962, 6. – P. 430-437.

4. *Самойленко С.И.* Биноидные коды и их применение. – В сб.: Кодирование в сложных системах. – М.: Наука, 1974. – С. 44-47.

5. *Амербаев В.М., Бияшев Р.Г.* Интерполяция и коды, исправляющие ошибки. – В кн.: Теория кодирования и информационное моделирование. – Алма-Ата: Наука, 1973. – С. 51-64.

6. *Амербаев В.М.* Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976. – 324 с.

7. *Рид И.С., Соломон Г.* Полиномиальные коды над некоторыми конечными полями. – В кн.: Кибернетический сборник. – М.: ИЛ, 1963, вып. 7. – С. 74-79.

8. *Амербаев В.М.* Китайская теорема об остатках и контроль функциональных преобразований. – В кн.: Информационный обмен в вычислительных сетях. – М: Наука, 1980. – С. 150-168.

9. *Бияшев Р.Г.* К вопросу о защите логических операций кодами Лагранжа. – В кн.: Теория кодирования и оптимизация сложных систем. – Алма-Ата: Наука, 1977. – С. 97-108.

10. *Бияшев Р.Г., Черкасов Ю.Н.* Контроль сдвиговых операций в кодах с параллельной структурой. – В сб.: Вопросы кибернетики, вып. 42/2, 1978. – С. 104-109.

11. *Кубицкий В.И.* Модификация процедуры кодирования полиномиальными кодами. (Деп. в ВИНИТИ 10.09.86, № 422 ГА-86, 16 с.). – Библиографический указатель ВИНИТИ «Депонированные научные работы», №1, 1987. – С. 128.

12. *Кубицкий В.И.* Процедуры кодирования и декодирования для полиномиальных кодов. – В сб.: Эксплуатация программного обеспечения систем реального времени, построенных на базе микро- и мини-ЭВМ. – К.: КИИГА, 1989. – С. 67-71.

13. *Кубицкий В.И.* Некоторые алгоритмы коррекции одиночной ошибки кодами с параллельной структурой. – В сб. «Диагностирование электрических и электронных схем» / АН УССР. Ин-т проблем моделирования в энергетике. – К., 1990.