УДК 621.391.251:681.3.06

Кубицкий В.И.

ДЕКОДИРОВАНИЕ МНОГОКРАТНЫХ ОШИБОК КОДАМИ ЛАГРАНЖА

ГосНИИ «Аэронавигация» (Россия, Москва)

Показано, как с помощью кодов Лагранжа можно исправлять многократные недвоичные ошибки. Выводятся ключевые уравнения синдромов для различных алгоритмов кодирования, применяемых при декодировании ошибок

Известно множество кодов для исправления многократных недвоичных ошибок, к которым можно отнести широко известные коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) и коды Рида-Соломона (РС-коды) [1, 2], а также коды Лагранжа [3]. Процедуры декодирования БЧХ- и РС-кодов достаточно полно исследованы и описаны во многих публикациях. Для кодов Лагранжа процедура исправления многократных ошибок приводится в [4].

Покажем, как можно модифицировать эту процедуру, применяя алгоритмы кодирования, разработанные в [5, 6].

Пусть $S=\{x_o,\cdots,x_s\}$ – множество информационных узлов мощности k; $T=\{\beta_1,\cdots,\beta_r\}$ – множество контрольных узлов мощности r. Величина r выбирается в зависимости от количества возникающих в кодовом слове ошибок t и должна быть не меньше, чем $2t$.

Пусть также $S,T\subseteq F_q$ – подмножество поля F_q, $P=S\bigcup T$ – подмножество мощности $n=k+r$.

В процедурах декодирования многократных ошибок кодами Лагранжа используются алгоритмы кодирования этих кодов.

Алгоритмы кодирования для процедур декодирования многократных ошибок

Алгоритм А1: При вычислении значений искаженного полинома $\tilde{f}(x)$ в контрольных узлах используются только информационные символы $\tilde{f}_i$ принятой кодовой последовательности:

$$f^*(\beta_j)=-\sum_{i=0}^{s}\tilde{f}_i\,L_S^{(i)}(\beta_j),\quad j=\overline{1,r},$$

где $L_S^{(i)}(\beta_j)=-\prod\limits_{\substack{l=1\\ l\neq j}}^{r}\dfrac{x_i-\beta_l}{\beta_j-\beta_l}$ – фундаментальные полиномы Лагранжа в контрольных узлах; $S=\{x_o,\cdots,x_s\}$.

Назовем такой алгоритм кодирования *параллельным алгоритмом А1.*

Алгоритм А2: При вычислении значения искаженного полинома $\tilde{f}(x)$ в j-ом контрольном узле кроме информационных символов $\tilde{f}_i$ принятой кодовой последовательности используются вычисленные значения $f^*(\beta_{j-1})$ этого полинома в предыдущих (j-1)-ых контрольных узлах:

$$f^*(\beta_j)=[\sum_{i=0}^{s}\tilde{f}_i+\sum_{\substack{h=1\\ h<j}}^{j-1}f^*(\beta_h)]\,L_{S_{j-1}}^{(i)}(\beta_j),$$

где $L_{S_{j-1}}^{(i)}(\beta_j)=-\prod\limits_{l=j+1}^{r}\dfrac{x_i-\beta_l}{\beta_j-\beta_l}$ – фундаментальные полиномы Лагранжа в контрольных узлах; $S_{j-1}=S\bigcup\{\beta_1,\cdots,\beta_{j-1}\}$; $x_i\in S_{j-1}$.

Назовем такой алгоритм кодирования *последовательным алгоритмом А2.*

Алгоритм А3: При вычислении значения искаженного полинома $\tilde{f}(x)$ в j-ом контрольном узле кроме информационных символов $\tilde{f}_i$ принятой кодовой последовательности используются принятые значения $\tilde{f}(\beta_{j-1})$ этого полинома в предыдущих (j-1)-ых контрольных узлах:

$$f^*(\beta_j)=\sum_{i=0}^{s+j-1}\tilde{f}_i\,L_{S_j}^{(i)}(\beta_j).$$

Назовем такой алгоритм кодирования *последовательным алгоритмом А3.*

Так как контрольные символы, вычисленные согласно параллельному и последовательному алгоритмам, одинаковы, т.е. $\sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) = \sum_{x_i \in S_{j-1}} f_i \, L_{T_j}^{(j)}(x_i)$, то

$$f(\beta_j) + \sum_{x_i \in S_{j-1}} f_i \, L_{T_j}^{(j)}(x_i) = 0 .$$

Что и требовалось доказать.

Равенство (1) справедливо для случая применения последовательного алгоритма вычисления контрольных символов.

Утверждение 2. Кодовый вектор $< f(x)\big|_{P_r(x)}$ принадлежит (n, k)–коду Лагранжа тогда и только тогда, когда для любого $\beta_j \in T$ справедливо равенство:

$$f(\beta_j) + \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) = 0, \quad j = \overline{1, r-1},$$

$$f(\beta_r) + [\sum_{i=0}^{s} f_i + \sum_{j=1}^{r-1} f(\beta_j)] = 0 . \qquad (3)$$

Доказательство. При доказательстве утверждения 1 было показано, что

$$f(\beta_j) + \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) = 0, \quad j = \overline{1, r} .$$

Запишем это равенство в виде двух равенств:

$$f(\beta_j) + \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) = 0, \quad j = \overline{1, r-1},$$

$$f(\beta_r) + \sum_{x_i \in S} f_i \, L_T^{(r)}(x_i) = 0,$$

где $\sum_{x_i \in S} f_i \, L_T^{(j)}(x_i)$ – вычисленные значения контрольных символов в $(r-1)$-ых контрольных узлах;

$\sum_{x_i \in S} f_i \, L_T^{(r)}(x_i)$ – вычисленное значение контрольного символа в r-ом контрольном узле.

Так как контрольные символы, вычисленные по параллельному и параллельно-последовательному алгоритмам кодирования, равны, то получаем:

$$f(\beta_j) + \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) = 0, \quad j = \overline{1, r-1},$$

$$f(\beta_r) + [\sum_{i=0}^{s} f_i + \sum_{j=1}^{r-1} f(\beta_j)] = 0 ,$$

где $[\sum_{i=0}^{s} f_i + \sum_{j=1}^{r-1} f(\beta_j)]$ – вычисленное значение контрольного символа в r-ом контрольном узле.

Что и требовалось доказать.

Равенства (3) справедливы для случая применения параллельно-последовательного алгоритма вычисления контрольных символов.

Докажем ещё одно утверждение.

Утверждение 3. Кодовый вектор $< f(x)\big|_{P_r(x)}$ принадлежит (n, k)–коду Лагранжа тогда и только тогда, когда для любого $\beta_j \in T$ справедливо равенство:

$$\sum_{x_i \in S \cup T} f_i \, x_i^{\mu} = 0, \quad \mu = \overline{0, r-1} . \qquad (4)$$

Доказательство. Умножая обе части равенства (2) на β_j^{μ} $(\mu = \overline{0, r-1})$ и суммируя по $\beta_j \in T$, получаем:

$$\sum_{\beta_j \in T} \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) \, \beta_j^{\mu} + \sum_{\beta_j \in T} f(\beta_j) \, \beta_j^{\mu} =$$

$$= \sum_{x_i \in S} f_i \sum_{\beta_j \in T} L_T^{(j)}(x_i) \, \beta_j^{\mu} + \sum_{\beta_j \in T} f(\beta_j) \, \beta_j^{\mu} = 0 .$$

Так как $\sum_{\beta_j \in T} L_T^{(j)}(x_i) \, \beta_j^{\mu} = x_i^{\mu}$, то имеем $\sum_{x_i \in S \cup T} f_i \, x_i^{\mu} = 0$.

Что и требовалось доказать.

Из доказательства утверждения 2 также следует равенство:

$$\sum_{x_i \in S \cup T} f_i \, x_i^{\mu} = f(\beta_j) + \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) = 0 . \qquad (5)$$

Выражения (1), (2), (3), (4) являются условиями правильности принятого кодового слова для различных вариантов декодирования.

Ключевые уравнения синдромов для декодирования многократных ошибок

Если кодовое слово, закодированное кодом Лагранжа, подвергается воздействию аддитивной ошибки $I \subset S \cup T$, под которой будем понимать полином:

$$\delta_I(x) = \sum_{x_i \in I} \delta_i L_P^{(i)}(x), \qquad |I| = t,$$

то полином, соответствующий искаженному кодовому слову, имеет вид:

$$\tilde{f}(x) = f(x) + \delta_I(x).$$

Уравнение синдрома записывается в виде разности полученных $\tilde{f}(\beta_j)$ и вновь вычисленных $f^*(\beta_j)$ контрольных символов:

$$R_j = \tilde{f}(\beta_j) - f^*(\beta_j), \quad j = \overline{1, r}. \quad (6)$$

Величины $f^*(\beta_j)$ определяются с использованием процедур кодирования. В зависимости от того, какой алгоритм кодирования применяется, меняется вид ключевого уравнения.

В [4] показано, что ключевое уравнение синдрома для декодирования t-кратных ошибок имеет вид:

$$Q_\mu = \sum_{x_i \in I \cap P} \delta_i x_i^\mu, \quad (7)$$

где

$$Q_\mu = \sum_{\beta_j \in T} R_j \beta_j^\mu, \quad \mu = \overline{0, r-1}; \quad (8)$$

δ_i – величины ошибок; x_i – номера ошибочных узлов.

Это ключевое уравнение получено при вычислении значений искаженного полинома $\tilde{f}(x)$ в контрольных узлах с использованием только информационных символов $\tilde{f}_i$ принятой кодовой последовательности (алгоритм А1).

Выведем ключевые уравнения синдромов для декодирования многократных ошибок кодом Лагранжа при использовании последовательных и параллельно-последовательного алгоритмов вычисления контрольных символов. Для этого докажем следующие утверждения.

Утверждение 4. Для последовательного алгоритма А2 вычисления контрольных символов ключевое уравнение синдрома для декодирования t-кратных ошибок имеет вид:

$$Q_\mu = \sum_{x_i \in I \cap P} \delta_i x_i^\mu, \quad (9)$$

где

$$Q_\mu = \sum_{\beta_j \in T} R_j \beta_j^\mu, \quad \mu = \overline{0, r-1}; \quad (10)$$

δ_i – величины ошибок; x_i – номера ошибочных узлов.

Доказательство. Уравнения синдрома (6) для последовательного алгоритма А2 вычисления контрольных символов имеет вид:

$$f(\beta_j) + \sum_{x_i \in S_{j-1}} f_i \, L_{T_j}^{(j)}(x_i) +$$

$$+ \sum_{x_i \in I \cap S_{j-1}} \alpha_i \, L_{T_j}^{(j)}(x_i) + \gamma_j = R_j \neq 0.$$

Так как контрольные символы, вычисленные согласно параллельному и последовательному алгоритмам, одинаковы, то это выражение будет следующим:

$$f(\beta_j) + \sum_{x_i \in S} f_i \, L_T^{(j)}(x_i) +$$

$$+ \sum_{x_i \in I \cap S} \alpha_i \, L_T^{(j)}(x_i) + \gamma_j = R_j \neq 0.$$

С учетом условия правильности принятого кодового слова (2) имеем уравнение:

$$R_j = \sum_{x_i \in I \cap S} \alpha_i L_S^{(i)}(x_i) + \gamma_j,$$

где α_i, γ_j – величины ошибок в информационных и контрольных узлах соответственно.

Умножая обе части уравнения на β_j^μ и, просуммировав по $\beta_j \in T$, получим:

$$\sum_{\beta_j \in T} R_j \, \beta_j^\mu = \sum_{\beta_j \in T} \sum_{x_i \in I \cap S} \alpha_i \, L_T^{(j)}(x_i) \, \beta_j^\mu - \sum_{\beta_j \in T} \gamma_j \, \beta_j^\mu =$$

$$= \sum_{x_i \in I \cap S} \alpha_i \sum_{\beta_j \in T} L_T^{(j)}(x_i) \, \beta_j^\mu + \sum_{\beta_j \in T} \gamma_j \, \beta_j^\mu.$$

С учетом равенств

$$\sum_{\beta_j \in T} L_T^{(j)}(x_i) \beta_j^\mu = x_i^\mu$$

и

$$\alpha_i, \gamma_j = \begin{cases} = 0, & \text{если} \quad x_i, \beta_j \notin I, \\ \neq 0, & \text{если} \quad x_i, \beta_j \in I \end{cases}$$

имеем

$$\sum_{\beta_j \in T} R_j \beta_j^{\mu} = \sum_{x_i \in I \cap S} \alpha_i x_i^{\mu} + \sum_{\beta_j \in I \cap T} \gamma_j \beta_j^{\mu}.$$

Обозначая $Q_{\mu} = \sum_{\beta_j \in T} R_j \beta_j^{\mu}$, получим

$$Q_{\mu} = \sum_{x_i \in I \cap S} \alpha_i x_i^{\mu} + \sum_{\beta_j \in I \cap T} \gamma_j \beta_j^{\mu} = \sum_{x_i \in I \cap (S \cup T)} \delta_i x_i^{\mu}.$$

Что и требовалось доказать.

Утверждение 5. Для последовательного алгоритма А3 вычисления контрольных символов ключевое уравнение синдрома для декодирования t-кратных ошибок имеет вид:

$$Q_{\mu} = \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu}, \qquad (11)$$

где

$$Q_{\mu} = R_j \left[\beta_j^{\mu} + \sum_{m=1}^{\mu} \phi_m^{(\mu)} \beta_j^{\mu - m} \right] - \sum_{m=1}^{\mu} \phi_m^{(\mu)} Q_{\mu - m}, \qquad (12)$$

$$\phi_o^{(\mu)} = 1, \qquad \phi_1^{(\mu)} = - \sum_{z=r-\mu+1}^{r} \beta_z, \ldots,$$

$$\phi_{\mu}^{(\mu)} = (-1)^{\mu} \prod_{z=r-\mu+1} \beta_z, \quad \mu = r - j.$$

Доказательство. При наличии t-кратной ошибки уравнение синдрома (6) записывается в виде:

$$f(\beta_j) + \sum_{x_i \in S_{j-1}} f_i L_{T_j}^{(j)}(x_i) +$$

$$+ \sum_{x_i \in I \cap S_{j-1}} \alpha_i L_{T_j}^{(j)}(x_i) + \gamma_j = R_j \neq 0,$$

где α_i – величины ошибок в информационных и (j-1)-ых контрольных узлах; γ_j – величина ошибки в j-ом контрольном узле.

Учитывая равенство (1), получим:

$$R_j = \sum_{x_i \in I \cap S_{j-1}} \alpha_i L_{T_j}^{(j)}(x_i) + \gamma_j.$$

Произведем преобразования:

$$R_j \prod_{\beta_l \in T_j} (\beta_j - \beta_l) =$$

$$= \sum_{x_i \in I \cap S_{j-1}} \alpha_i \prod_{\beta_l \in T_j} (x_i - \beta_l) + \gamma_j \prod_{\beta_l \in T_j} (\beta_j - \beta_l) =$$

$$= \sum_{x_i \in I \cap S_j} \delta_i \prod_{\beta_l \in T_j} (x_i - \beta_l),$$

$$R_j \sum_{m=0}^{\mu} \phi_m^{(\mu)} \beta_j^{\mu - m} = \sum_{x_i \in I \cap S_j} \delta_i \sum_{m=0}^{\mu} \phi_m^{(\mu)} x_i^{\mu - m}$$

$$\mu = r - j.$$

Так как $\phi_o^{(\mu)} = 1$ при $m = 0$, то запишем:

$$R_j \beta_j^{\mu} + R_j \sum_{m=1}^{\mu} \phi_m^{(\mu)} \beta_j^{\mu - m} =$$

$$= \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu} + \sum_{x_i \in I \cap S_j} \delta_i \sum_{m=1}^{\mu} \phi_m^{(\mu)} x_i^{\mu - m} =$$

$$= \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu} + \sum_{m=1}^{\mu} \phi_m^{(\mu)} \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu} =$$

$$= \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu} + \sum_{m=1}^{\mu} \phi_m^{(\mu)} Q_{\mu - m}.$$

где

$$Q_{\mu - m} = \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu - m}.$$

Отсюда:

$$R_j \left[\beta_j^{\mu} + \sum_{m=1}^{\mu} \phi_m^{(\mu)} \beta_j^{\mu - m} \right] - \sum_{m=1}^{\mu} \phi_m^{(\mu)} Q_{\mu - m} =$$

$$= \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu}.$$

Вводя обозначение

$$Q_{\mu} = R_j \left[\beta_j^{\mu} + \sum_{m-1}^{\mu} \phi_m^{(\mu)} \beta_j^{\mu - m} \right] - \sum_{m-1}^{\mu} \phi_m^{(\mu)} Q_{\mu - m},$$

получим

$$Q_{\mu} = \sum_{x_i \in I \cap S_j} \delta_i x_i^{\mu}.$$

Что и требовалось доказать.

Для фиксированных узлов интерполирования выражение (12) принимает вид:

$$Q_{\mu} = \lambda_j R_j - \sum_{m=1}^{\mu} \phi_m^{(\mu)} Q_{\mu - m}, \qquad (13)$$

где

$$\lambda_j = \beta_j^{\mu} + \sum_{m=1}^{\mu} \phi_m^{(\mu)} \beta_j^{\mu - m} = const$$

и

$$\phi_m^{(\mu)} = const.$$

Утверждение 6. Для параллельно-последовательного алгоритма А4 вычисления контрольных символов ключевое уравнение синдрома для декодирования t-кратных ошибок имеет вид

$$Q_\mu = \sum_{x_i \in I \cap P} \delta_i x_i^\mu , \qquad (14)$$

где

$$Q_\mu = \sum_{\beta_j \in T} R_j \beta_j^\mu , \quad \mu = \overline{0, r-1}; \qquad (15)$$

δ_i – величины ошибок; x_i – номера ошибочных узлов.

Доказательство. Справедливость этого утверждения следует из положения о том, что значения $f^*(\beta_j)$ $(j = \overline{1,r})$, вычисленные согласно алгоритму А4, равны значениям $f^*(\beta_j)$, найденным по алгоритму А1.

Утверждение 7. Ключевое уравнение синдрома для декодирования t-кратных ошибок имеет вид:

$$Q_\mu = \sum_{x_i \in I \cap (S \cup T)} \delta_i x_i , \qquad (16)$$

где

$$Q_\mu = \sum_{x_i \in S \cup T} \tilde{f}_i x_i^\mu , \qquad \mu = \overline{0, r-1} .$$

Доказательство. В силу равенства (5) и при наличии ошибки имеем уравнение:

$$R_j = \tilde{f}(\beta_j) + \sum_{x_i \in S} \tilde{f}_i L_T^{(j)}(x_i),$$

где

$$\tilde{f}(\beta_j) = f(\beta_j) + \gamma_j , \qquad \tilde{f}_i = f_i + \alpha_i .$$

Умножив обе части этого уравнения на β_j^μ и просуммировав по $\beta_j \in T$, получим:

$$\sum_{\beta_j \in T} R_j \beta_j^\mu =$$

$$\sum_{x_i \in S} \tilde{f}_i \sum_{\beta_j \in T} L_T^{(j)}(x_i) \beta_j^\mu + \sum_{\beta_j \in T} \tilde{f}(\beta_j) \beta_j^\mu =$$

$$= \sum_{x_i \in S} \tilde{f}_i x_i^\mu + \sum_{\beta_j \in T} \tilde{f}(\beta_j) \beta_j^\mu ,$$

где

$$x_i^\mu = \sum_{\beta_j \in T} L_T^{(j)}(x_i) \beta_j^\mu .$$

Так как в соответствии с (8) и (10) $\sum_{\beta_j \in T} R_j \beta_j^\mu = Q_\mu$, то имеем соотношение для вычисления величин синдромов

$$Q_\mu = \sum_{x_i \in S \cup T} \tilde{f}_i x_i^\mu , \qquad \mu = \overline{0, r-1}, \qquad (17)$$

которое не требует определения значений $f^*(\beta_j)$ искаженного полинома $\tilde{f}(x)$ в контрольных узлах.

Преобразуем выражение (17). С учётом равенства

$$\alpha_i , \gamma_j = \begin{cases} = 0, & \text{если} \quad x_i , \beta_j \notin I , \\ \neq 0, & \text{если} \quad x_i , \beta_j \in I \end{cases} ,$$

имеем

$$Q_\mu = \sum_{x_i \in S} (f_i + \alpha_i) x_i^\mu + \sum_{\beta_j \in T} [f(\beta_j) + \gamma_j] \beta_j^\mu =$$

$$= \sum_{x_i \in S \cup T} f_i x_i^\mu + \sum_{x_i \in I \cap (S \cup T)} \delta_i x_i^\mu .$$

Учитывая условие правильности принятого кодового слова (4), получим

$$Q_\mu = \sum_{x_i \in I \cap (S \cup T)} \delta_i x_i .$$

Что и требовалось доказать.

Отметим, что соотношение (17) аналогично соотношению для вычисления величин синдромов РС-кодов, а значит, величины Q_μ кода Лагранжа могут быть вычислены теми же способами, которые применяются для определения величин синдромов РС-кодов.

Вычисления в соответствии с (17) назовем *стандартным алгоритмом* определения величин синдромов кода Лагранжа.

Приведенные выше выкладки и уравнения справедливы для полного кода Лагранжа ($F = F_q$, $n = q$). Для неполного кода ($F \subset F_q$, $n < q$) [7] справедливы уравнения, выведенные для декодирования ошибок и стираний кодом Лагранжа [8].