1) Запишем соотношение для параллельного алгоритма кодирования в виде:

+

/=0

+

^=1

откуда находим:

£ /(х г)i?(Д) =
ge=i

/=o

Обозначим правую часть этого равенства через ***F***j . Так как у = 1,***г'***, то получим систему из ***г'*** уравнений для г неизвестных:

-Д т т ^ - Д

= - ъ >

I]*

решая которую определяем значения полинома в стертых информационных узлах.

Для определения значений полинома в стертых информационных узлах х* достаточно иметь ***г*** уравнений.

Введем обозначения:

Ь2, ***Ь3*** - множества коэффициентов Лагранжа в контрольных узлах для набора стертых, оставшихся и всех информационных узлов соответственно.

Множества ***Ь2*** и являются переменными, множество ***Ь5*** - постоянно. Но так как ***Ьг*** и = ***Ь***5, то коэффициенты Лагранжа для множеств ***Ь7*** и можно выбирать из множества ***Ь***5, элементы которого должны храниться в запоминающем устройстве. Это дает возможность не производить вычисления коэффициентов Лагранжа для каждого набора стертых узлов, как это делается в случае восстановления стертых символов посредством применения процедур кодирования.

После вычисления значений стертых информационных символов можно, при необходимости, произвести восстановление стертых контрольных символов, применяя процедуру кодирования. При этом коэффициенты Лагранжа также являются постоянными и принадлежат множеству ***Ь'8***■

2) Аналогично, преобразовывая соотношение для последовательного алгоритма кодирования, получим:

V 1 \TT —Д TT *х%~Рь* -
£=1 /=,41Д*J* - Д А=1 Д - Д

i=0 /=/+iД; *Pi* /?=1 *Hi* Д

или

Ё/(^) **п**|**н** §_ **п**т - §_ = - ^ ■
1=1 ;=y+1Д Д Ж1 Д Д

3) Преобразовывая соотношения для параллельно-последовательного алгоритма кодирования, получим:

1 m №-Д - 4 Й И -
^=1 *I*}*

з - д

1=0

— ***X1~Рь***

/1=1 **А - А**

5+г'-1 *,-Д

- л л) - I / П
/=0 =1Д '- д

или

1 **л г {>** **п** ^ 4 **п** ^ - д
<r=1 /=1 Д ,-Д А=1 Д у-Д

у = и' - 1 ,

Е **л х „) П** ^Д
|=1 *Ий р г<~ Р)*

4) Предложим еще один способ восстановления стертых символов, который основывается на применении ключевого уравнения синдрома при декодировании многократных ошибок для стандартного алгоритма определения величин синдромов кода Лагранжа.

В этом случае имеем систему уравнений:

$$\sum_{\xi=1}^{e} f(\widetilde{x}_\xi)\widetilde{x}_\xi^j = F_j,$$

где $F_j = \sum_{i=0}^{s+r} f_i x_i^j$, $x_i \in S \cup T$, $\widetilde{x}_\xi \in Z \cup \widetilde{T}$, $j = \overline{0, r-1}$.

Определитель этой системы из первых e уравнений ($e \le r$)

$$D = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \widetilde{x}_1 & \widetilde{x}_2 & \cdots & \widetilde{x}_e \\ \vdots & \vdots & & \vdots \\ \widetilde{x}_1^{e-1} & \widetilde{x}_2^{e-1} & \cdots & \widetilde{x}_e^{e-1} \end{vmatrix}$$

является определителем Вандермонда, который не равен 0, так как все $\widetilde{x}_\xi$ различны. Следовательно, такая система уравнений имеет единственное решение, которое может быть найдено либо по методу Гаусса, либо по правилу Крамера.

Решая эту систему уравнений, где неизвестными величинами являются $f(\widetilde{x}_\xi)$, вычисляем значения всех стертых символов.

Здесь при вычислении величин F_j значения f_i в стертых узлах принимаем равными 0. Тогда можно записать:

$F_j = \sum_{i=0}^{s'+r'} f(\text{€}_i)\text{€}_i^j$, где $\text{€}_i \in \text{€} \cup \text{€}$.

2. Ключевые уравнения для исправления ошибок и стираний

Перейдем к процедурам исправления t ошибок, имеющих место одновременно с e стираниями.

Пусть $S, T, V \in F_q$ – подмножества поля F_q. Здесь $V = \{v_1, \ldots, v_e\}$ – подмножество стертых узлов мощности e; $S = \{x_o, x_1, \ldots, x_s\}$ – подмножество узлов мощности k, взятых в качестве информационных после вычеркивания стертых узлов; $T = \{\beta_1, \ldots, \beta_r\}$ – подмножество узлов мощности r, принятых в качестве контрольных после вычеркивания стертых узлов. Пусть также $F = S \cup T \cup V$ – подмножество мощности n.

Докажем справедливость следующих утверждений.

Утверждение 2. Минимальный вес Хэмминга $(n, n-(2t+e))$–кода Лагранжа равен $2t+e+1$.

Доказательство. Пусть $\pi(< f(x)|_{P_F(x)})$ принадлежит кодовому пространству, то есть $< f(x)|_{P_S(x)} = f(x)$, где $P_S(x) = \prod_{x_i \in S}(x - x_i)$.

Тогда $\deg f(x) \le n-(2t+e)-1$, так как $\deg P_S(x) = n-(2t+e)$. Отсюда следует, что число корней многочлена $f(x)$ самое большее равно $n-(2t+e)-1$, то есть любой кодовый вектор имеет самое меньшее $2t+e+1$ ненулевых символов.

Утверждение 3. При любом n $(2(e+2t) \le n \le q)$ для исправления стираний кратности e и для обнаружения и исправления ошибок кратности t кодом Лагранжа необходимо и достаточно $2t+e$ проверочных символов.

Доказательство. Так как минимальное кодовое расстояние для линейного кода равно минимальному весу его ненулевых векторов, то минимальное кодовое расстояние $(n, n-(2t+e))$–кода Лагранжа при $2t+e$ проверочных символах согласно предложению 2 равно $2t+e+1$. А при таком кодовом расстоянии все ошибки, число которых не превышает t, и e стираний могут быть исправлены.

Так как при декодировании стираний и ошибок местоположение стираний будем считать известным, то основная задача заключается в обнаружении и исправлении ошибок.

Можно предложить следующий алгоритм исправления ошибок и стираний:

1. Вычеркиваем все стертые узлы.
2. Выбираем любые r узлов в качестве контрольных.
3. Обнаруживаем и (или) исправляем ошибки, применяя известные процедуры декодирования.
4. По методу декодирования стираний восстанавливаем стертые символы.

Возможность обнаружить и исправить ошибки после вычеркивания стертых символов показывает следующее утверждение.

Утверждение 4. При любом n $(2(e+2t) \le n \le q)$ после вычеркивания e стертых символов получим код Лагранжа, обнаруживающий и исправляющий t ошибок.

Доказательство. Утверждение следует из утверждения 1 и предложения 7.19 [5]. Действительно, вычеркивая комбинацию из e стертых символов искаженного кода, получим $(n-e,\ n-2t-e)$–код Лагранжа, обнаруживающий и исправляющий любую ошибку кратности не выше t.

Выведем ключевые уравнения декодирования ошибок и стираний кодом Лагранжа. Эти уравнения будут справедливы как для случая полного кода Лагранжа $(F = F_q,\ n = q)$, так и для случая неполного кода [6] $(F \subset F_q,\ n < q)$, от которого к полному коду можно перейти, если в недостающих узлах $x_{i_1},\ldots,x_{i_z}$, которые будем считать стертыми, значения кодового полинома принять равными нулю: $f_{i_1} = \ldots = f_{i_z} = 0$, где $z = q - n$.

Утверждение 5. Кодовый вектор $< f(x)\big|_{P_F(x)}$, имеющий стирания, принадлежит (n, k)–коду Лагранжа тогда и только тогда, когда для любого $\beta_j \in T$ справедливо равенство:

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

где $L_T^{(j)}(x_i) = \prod_{\substack{\beta_l \in T \\ l \ne j}} \frac{x_i - \beta_l}{\beta_j - \beta_l}$ – фундаментальный полином Лагранжа в контрольных узлах;

$L_V(x_i) = \prod_{v_\xi} \frac{x_i - v_\xi}{\beta_j - v_\xi}$ – фундаментальный полином Лагранжа в стертых узлах.

Доказательство. Известно [5], что кодовый вектор $< f(x)\big|_{P_F(x)}) \Rightarrow (f_o,\ldots,f_{n-1})$ представляет неискаженное кодовое слово тогда и только тогда, когда:

$$\left[\frac{< f(x)\big|_{P_F(x)}}{P_S(x)}\right] = \frac{< f(x)\big|_{P_F(x)} - < f(x)\big|_{P_S(x)}}{P_S(x)} = 0 \cdot$$

Преобразуем это уравнение с учетом наличия стираний:

$$< f(x)\big|_{P_F(x)} - < f(x)\big|_{P_S(x)} =$$

$$= \sum_{x_i \in F} f_i L_F^{(i)}(x) - \sum_{x_i \in S} f_i L_S^{(i)}(x) =$$

$$= [\sum_{x_i \in S} f_i L_F^{(i)}(x) + \sum_{x_i \in T} f_i L_F^{(i)}(x) +$$

$$+ \sum_{x_i \in V} f_i L_F^{(i)}(x)] - \sum_{x_i \in S} f_i L_S^{(i)}(x) = 0.$$

Так как $\sum_{x_i \in V} f_i L_F^{(i)}(x)$ стерто, то получим: $\sum_{x_i \in S} f_i L_S^{(i)}(x)[L_T(x) L_V(x) - 1] +$

$$+ \sum_{\beta_j \in T} f_i L_S^{(i)}(x) L_T^{(i)}(x) L_V(x) = 0.$$

Для любого $x = \beta_j$ имеем:

$$f(\beta_j) - \sum_{x_i \in S} f_i L_S^{(i)}(\beta_j) = 0$$

или с учетом леммы 1 [6]:

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

Что и требовалось доказать.

Отметим, что равенство (1) справедливо для случая применения параллельного алгоритма вычисления контрольных символов.

В случае применения последовательного алгоритма кодирования справедливо:

Утверждение 6. Кодовый вектор $< f(x)\big|_{P_F(x)}$, имеющий стирания, принадлежит (n, k)–коду Лагранжа тогда и только тогда, когда для любого $\beta_j \in T$ справедливо равенство:

$$f(\beta_j) + \sum_{x_i \in S_{j-1}} f_i L_{T_j}^{(j)}(x_i) L_V(x_i) = 0, \ j = \overline{1,r}, \tag{2}$$

где $L_{T_j}^{(j)}(x_i) = \prod_{\beta_j \in T_j} (x_i - \beta_l)/(\beta_j - \beta_l)$,

$L_V(x_i) = \prod_{v_\xi \in V} (x_i - v_\xi)/(\beta_j - v_\xi)$,

$T_j = T \setminus \{\beta_1,\ldots,\beta_j\}, \quad T = \{\beta_1,\ldots,\beta_r\}$,

$S_{j-1} = S \cup \{\beta_1,\ldots,\beta_{j-1}\}$.

Доказательство. Утверждение следует из леммы 2 [6] и положения о том, что контрольные символы, вычис-

ленные согласно параллельному и последовательному алгоритмам, одинаковы.

Утверждение 7. Кодовый вектор $< f(x)\big|_{P_F(x)}$, имеющий стирания, принадлежит (n, k)–коду Лагранжа тогда и только тогда, когда для любого $\beta_j \in T$ справедливо равенство:

$$\sum_{x_i \in S \bigcup T} f_i x_i^{\mu} \prod_{v_\xi \in V} (x_i - v_\xi) = 0, \quad \mu = \overline{0, r-1}. \quad (3)$$

Доказательство. Произведем преобразование равенства (1).

Запишем:

$$f(\beta_j) + \sum_{x_i \in S} f_i \frac{\prod\limits_{v_\xi \in V} (x_i - v_\xi)}{\prod\limits_{v_\xi \in V} (\beta_j - v_\xi)} L_T^{(j)}(x_i) = 0$$

или

$$f(\beta_j) \prod_{v_\xi \in V} (\beta_j - v_\xi) + \sum_{x_i \in S} f_i L_T^{(j)}(x_i) \prod_{v_\xi \in V} (x_i - v_\xi) = 0.$$

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

$$\sum_{\beta_j \in T} \sum_{x_i \in S} f_i L_T^{(j)}(x_i) \prod_{v_\xi \in V} (x_i - v_\xi) \beta_j^{\mu} +$$

$$+ \sum_{\beta_j \in T} f(\beta_j) \prod_{v_\xi \in V} (\beta_j - v_\xi) \beta_j^{\mu} =$$

$$= \sum_{x_i \in S} f_i \prod_{v_\xi \in V} (x_i - v_\xi) \sum_{\beta_j \in T} L_T^{(j)}(x_i) \beta_j^{\mu} +$$

$$+ \sum_{\beta_j \in T} f(\beta_j) \prod_{v_\xi \in V} (\beta_j - v_\xi) \beta_j^{\mu} = 0.$$

Так как $\sum\limits_{\beta_j \in T} L_T^{(j)}(x_i) \beta_j^{\mu} = x_i^{\mu}$, то имеем $\sum\limits_{x_i \in S \bigcup T} f_i x_i^{\mu} \prod\limits_{v_\xi \in V} (x_i - v_\xi) = 0.$

Что и требовалось доказать.

Выражения (1), (2), (3) являются условием правильности принятого кодового слова.

Пусть кроме стираний в принятом сообщении имеется аддитивная ошибка $I \subset S \bigcup T$, под которой будем понимать полином:

$$\delta_I(x) = \sum_{x_i \in I} \delta_i L_F^{(i)}(x), \quad |I| = t.$$

Синдромные уравнения записываются в виде равенства:

$$R_j = \tilde{f}(\beta_j) - f^*(\beta_j). \quad j = \overline{1, r}, \quad (4)$$

где $\tilde{f}(\beta_j)$ и $f^*(\beta_j)$ принятые и вновь вычисленные контрольные символы.

Справедливо следующее утверждение.

Утверждение 8. Ключевое уравнение для декодирования t ошибок и e стираний имеет вид:

$$T_\mu = \sum_{x_i \in I \cap S} \alpha_i x_i^{\mu} \sum_{u=0}^{e} \sigma_u x_i^{e-u} +$$

$$+ \sum_{\beta_j \in I \cap T} \gamma_j \beta_j^{\mu} \sum_{u=0}^{e} \sigma_u \beta_j^{e-u}, \quad (5)$$

где

$$T_\mu = \sum_{\beta_j \in T} R_j \beta_j^{\mu} \prod_{v_\xi \in V} (\beta_j - v_\xi), \quad \mu = \overline{0, r-1};$$

$$\sigma_o = 1, \quad \sigma_1 = -\sum_{\xi=1}^{e} v_\xi, \ldots, \quad \sigma_e = (-1)^e \prod_{\xi=1}^{e} v_\xi$$

– элементарные симметрические функции номеров стертых узлов;

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

Доказательство. Согласно утверждению 5 имеем соотношение:

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

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

Так как $f(x)$ принадлежит коду Лагранжа, то это отношение можно записать в виде:

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

или $R_j \prod\limits_{v_\xi \in V} (\beta_j - v_\xi) =$

$$= \sum_{x_i \in I \cap S} \alpha_i L_T^{(j)}(x_i) \prod_{v_\xi \in V} (x_i - v_\xi) +$$

$$+ \gamma_j \prod_{v_\xi \in V} (\beta_j - v_\xi).$$

Умножим обе части уравнения на β_j^{μ} и просуммируем по $\beta_j \in T$, получим:

$$\sum_{\beta_j \in T} R_j \beta_j^{\mu} \prod_{v_\xi \in V} (\beta_j - v_\xi) =$$

$$= \sum_{\beta_j \in T} \sum_{x_i \in I \cap S} \alpha_i L_T^{(j)}(x_i) \prod_{v_\xi \in V} (x_i - v_\xi) \beta_j^{\mu} +$$

$$+\sum_{\beta_j\in T}\gamma_j\beta_j^{\mu}\prod_{v_\xi\in V}(\beta_j-v_\xi)=$$

$$=\sum_{x_i\in I\cap S}\alpha_i\prod_{v_\xi\in V}(x_i-v_\xi)\sum_{\beta_j\in T}L_T^{(j)}(x_i)\beta_j^{\mu}+$$

$$+\sum_{\beta_j\in T}\gamma_j\beta_j^{\mu}\prod_{v_\xi\in V}(\beta_j-v_\xi).$$

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

$$\sum_{\beta_j\in T}R_j\beta_j^{\mu}\prod_{v_\xi\in V}(\beta_j-v_\xi)=$$

$$=\sum_{x_i\in I\cap S}\alpha_i x_i^{\mu}\prod_{v_\xi\in V}(x_i-v_\xi)+$$

$$+\sum_{\beta_j\in I\cap T}\gamma_j\beta_j^{\mu}\prod_{v_\xi\in V}(\beta_j-v_\xi).$$

Или

$$T_\mu=\sum_{x_i\in I\cap S}\alpha_i x_i^{\mu}\sum_{u=0}^{e}\sigma_u x_i^{e-u}+$$

$$+\sum_{\beta_j\in I\cap T}\gamma_j\beta_j^{\mu}\sum_{u=0}^{e}\sigma_u\beta_j^{e-u}.$$

Что и требовалось доказать.

Введем обозначение:

$$\Delta_i=\delta_i\sum_{u=0}^{e}\sigma_u x_i^{e-u}.$$

Тогда:

$$T_\mu=\sum_{x_i\in I\cap(S\cup T)}\Delta_i x_i^{\mu}.$$

Это уравнение решается с помощью алгоритма Берлекэмпа.

Отметим, что доказательство утверждения 8 проводилось для случая применения при вычислении контрольных символов параллельного алгоритма кодирования.

Справедливость данного утверждения можно доказать и для случая, когда при вычислении значения искаженного полинома в j-ом контрольном узле кроме информационных символов $\widetilde{f}_i$ кодовой последовательности используются вычисленные значения $f^*(\beta_{j-1})$ в предыдущих (j-1)-ых контрольных узлах (последовательный алгоритм А2). Для этого, используя (2) , запишем:

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

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

С учетом того, что контрольные символы, вычисленные согласно параллельному и последовательному алгоритмам, одинаковы получаем:

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

Дальнейшее доказательство аналогично доказательству утверждения 8.

Если при вычислении значения искаженного полинома в j-ом контрольном узле кроме информационных символов $\widetilde{f}_i$ кодовой последовательности используются значения $f^*(\beta_{j-1})$ полинома $\widetilde{f}(x)$ в (j-1)-ых контрольных узлах принятой последовательности (последовательный алгоритм А3) . то справедливо следующее:

Утверждение 9. Для последовательного алгоритма А3 вычисления контрольных символов ключевое уравнение синдрома декодирования t ошибок и e стираний имеет вид:

$$T_\mu=\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu}\sum_{u=0}^{e}\sigma_u x_i^{e-u},\quad \mu=\overline{0,r-1}, \quad (6)$$

где

$$T_\mu=R_j\left[\beta_j^{\mu}+\sum_{m=1}^{\mu}\phi_m^{(\mu)}\beta_j^{\mu-m}\right]\prod_{v_\xi\in V}(\beta_j-v_\xi)-$$

$$-\sum_{m=1}^{\mu}\phi_m^{(\mu)}T_{\mu-m};$$

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

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

$$\sigma_o=1,\quad \sigma_1=-\sum_{\xi=1}^{e}v_\xi,\ldots,\ \sigma_e=(-1)^e\prod_{\xi=1}^{e}v_\xi.$$

Доказательство. При наличии t ошибок и e стираний синдромное уравнение (4) можно представить в виде соотношения:

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

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

С учетом равенства (2) имеем:

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

Выполним преобразования.

$$R_j=\sum_{x_i\in I\cap S_{j-1}}\alpha_i\prod_{\beta_l\in T_j}\frac{x_i-\beta_l}{\beta_j-\beta_l}\prod_{v_\xi\in V}\frac{x_i-v_\xi}{\beta_j-v_\xi}+\gamma_j;$$

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

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

$$+\gamma_j\prod_{\beta_l\in T_j}(\beta_j-\beta_l)\prod_{v_\xi\in V}(\beta_j-v_\xi)=$$

$$=\sum_{x_i\in I\cap S_j}\delta_i\prod_{\beta_l\in T_j}(x_i-\beta_l)\prod_{v_\xi\in V}(x_i-v_\xi);$$

$$R_j\sum_{m=0}^{\mu}\phi_m^{(\mu)}\beta_j^{\mu-m}\prod_{v_\xi\in V}(\beta_j-v_\xi)=$$

$$=\sum_{x_i\in I\cap S_j}\delta_i\sum_{m=0}^{\mu}\phi_m^{(\mu)}x^{\mu-m}\sum_{u=0}^{e}\sigma_u x_i^{e-u},$$

$$(\mu=r-j),$$

где $\sum_{u=0}^{e}\sigma_u x_i^{e-u}=\prod_{v_\xi\in V}(x_i-v_\xi)$.

Так как $\phi_m^{(\mu)}=1$, то:

$$R_j\left[\beta_j^{\mu}+\sum_{m=1}^{\mu}\phi_m^{(\mu)}\beta_j^{\mu-m}\right]\prod_{v_\xi\in V}(\beta_j-v_\xi)=$$

$$=\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu}\sum_{u=0}^{e}\sigma_u x_i^{e-u}+$$

$$+\sum_{m=1}^{\mu}\phi_m^{(\mu)}\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu-m}\sum_{u=0}^{e}\sigma_u x_i^{e-u}=$$

$$=\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu}\sum_{u=0}^{e}\sigma_u x_i^{e-u}+\sum_{m=1}^{\mu}\phi_m^{(\mu)}T_{\mu-m},$$

где $T_{\mu\text{-}m}=\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu-m}\sum_{u=0}^{e}\sigma_u x_i^{e-u}$.

Далее:

$$R_j\left[\beta_j^{\mu}+\sum_{m=1}^{\mu}\phi_m^{(\mu)}\beta_j^{\mu-m}\right]\prod_{v_\xi\in V}(\beta_j-v_\xi)-$$

$$-\sum_{m=1}^{\mu}\phi_m^{(\mu)}T_{\mu-m}=\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu}\sum_{u=0}^{e}\sigma_u x_i^{e-u}.$$

Обозначая левую часть этого уравнения через T_μ, получим:

$$T_\mu=\sum_{x_i\in I\cap S_j}\delta_i x_i^{\mu}\sum_{u=0}^{e}\sigma_u x_i^{e-u}.$$

Что и требовалось доказать.

Представляется возможным определять правильность декодирования ошибок, а также ошибок и стираний.

Если $n<q$ $(q=p^m)$, то можно выбрать еще один узел интерполирования x_n, принимая его за стертый и полагая значение кодового полинома в нем равным 0. Тогда можно произвести проверку правильности декодирования ошибок до начала исправления стираний. Для этого определяется значение кодового полинома в узлах x_n, которое при правильном декодировании должно быть равным 0:

$$f(x_n)=-\sum_{x_i\in S\cup T}f_i\frac{x_i-v_\xi}{x_n-v_\xi}.$$

Для проверки правильности декодирования ошибок и стираний необходимо просуммировать значения кодового полинома во всех узлах (информационных, контрольных, стертых). Эта сумма в случае правильного декодирования должна быть равна 0.

Примечание. При кодировании наличие узла x_n учитывается (см. выражения (3) и (5) [6]). Значение полинома в этом узле, равное 0, по каналу не передается, поэтому на скорость передачи введение узла x_n не влияет. Но влияет на время кодирования и декодирования, поскольку увеличивается количество операций из-за увеличения мощности множества стертых узлов:

$$V_1=V\cup\{x_n\}=\{v_1,\ldots,v_e,x_n\}.$$

3. Вычисление синдромов

При декодировании ошибок и стираний требуется решать ключевые уравнения синдромов, для чего необходимо знать величины синдромов T_μ.

Рассмотрим несколько способов вычисления величин синдромов.

Утверждение 10. Величины синдромов T_μ при декодировании ошибок и стираний кодом Лагранжа вычисляется из соотношения:

$$T_\mu=\sum_{\beta_j\in T}R_j\beta_j^{\mu}\prod_{v_\xi\in V}(\beta_j-v_\xi),\quad \mu=\overline{0,r-1}.$$

(7)

Справедливость данного утверждения доказывается при выводе ключевого уравнения синдрома (5).

Величины синдромов T_μ следует вычислять по формуле (7) как в случае использования при определении невязок R_j параллельного алгоритма кодирования, так и в случае использования последовательного алгоритма А2.

Приведем выражение для вычисления синдромов T_μ в случае использования при определении невязок R_j последовательного алгоритма А3.

Утверждение 11. При декодировании ошибок и стираний кодом Лагранжа с использованием последовательного алгоритма А3 величины синдромов T_μ вычисляются из соотношения:

$$T_\mu = R_j\left[\beta_j^\mu + \sum_{m=1}^{\mu}\phi_m^{(\mu)}\beta_j^{\mu-m}\right]\prod_{v_\xi\in V}(\beta_j - v_\xi) - \\ -\sum_{m=1}^{\mu}\phi_m^{(\mu)}T_{\mu-m}, \qquad (8)$$

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

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

Справедливость данного утверждения доказывается при выводе ключевого уравнения синдрома (6).

Предложим еще один способ определения величин синдромов T_μ.

Утверждение 12. Величины синдромов T_μ при декодировании ошибок и стираний кодом Лагранжа вычисляются из соотношения:

$$T_\mu = \sum_{x_i\in S\cup T}\tilde{f}_i x_i^\mu\prod_{v_\xi\in V}(x_i - v_\xi), \quad \mu = \overline{0, r-1}. \qquad (9)$$

Доказательство. Запишем синдромное уравнение в виде:

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

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

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

$$\sum_{\beta_j\in T}R_j\beta_j^\mu\prod_{v_\xi\in V}(\beta_j - v_\xi) = \\ = \sum_{x_i\in S}\tilde{f}_i x_i^\mu\prod_{v_\xi\in V}(x_i - v_\xi) + \\ + \sum_{\beta_j\in T}\tilde{f}(\beta_j)\beta_j^\mu\prod_{v_\xi\in V}(\beta_j - v_\xi),$$

где $x_i^\mu = \sum_{\beta_j\in T}\tilde{f}_i\, L_T^{(j)}(x_i)\cdot\beta_j^\mu$.

Условием правильности принятого кодового слова согласно утверждению 7 является равенство:

$$\sum_{x_i\in S\cup T}\tilde{f}_i x_i^\mu\prod_{v_\xi\in V}(x_i - v_\xi) = 0.$$

При наличии ошибки будем иметь:

$$\sum_{x_i\in S\cup T}\tilde{f}_i x_i^\mu\prod_{v_\xi\in V}(x_i - v_\xi) = T_\mu \neq 0.$$

Получили выражение для вычисления синдромов T_μ. Что и требовалось доказать.

Очевидно, что величины синдромов T_μ, вычисленные из (7) и (9), равны.

Вычисление величин синдромов T_μ по формулам (7) и (9) предполагает предварительное определение стертых узлов.

Для того, чтобы иметь возможность определять T_μ в момент приема (поступления) кодовой последовательности воспользуемся следующим утверждением.

Утверждение 13. Величины синдромов T_μ при декодировании ошибок и стираний кодом Лагранжа вычисляются из соотношения:

$$T_\mu = \sum_{u=0}^{e}\sigma_u\sum_{x_i\in S\cup T}\tilde{f}_i x_i^{\mu+e-u}, \qquad (10)$$

где $\sigma_o = 1$, $\sigma_1 = -\sum_{\xi=1}^{e}v_\xi$, ...

..., $\sigma_e = (-1)^e\prod_{\xi=1}^{e}v_\xi$.

Доказательство. Так как справедливо равенство $\prod_{v_\xi\in V}(x_i - v\xi) = \sum_{u=0}^{e}\sigma_u x_i^{e-u}$, то преобразовывая выражение (9) получаем выражение (10).

Аналогичная запись выражения (7) $T_\mu = \sum_{u=0}^{e} \sigma_u \sum_{\beta_i \in T} R_j \beta_j^{\mu+e-u}$ требуемого результата не дает, так как при вычислении невязок R_j все равно необходимо предварительно знать номера стертых узлов.

Утверждение 14. Величины синдромов T_μ при декодировании ошибок и стираний кодом Лагранжа вычисляются из соотношений:

$$T_\mu = \sum_{x_i \in F} \tilde{f}_i x_i^\mu \prod_{v_\xi \in V} (x_i - v_\xi) \qquad (11)$$

или

$$T_\mu = \sum_{u=0}^{e} \sigma_u \sum_{x_i \in F} \tilde{f}_i x_i^{\mu+e-u}, \qquad (12)$$

где $F = S \cup T \cup V$.

Доказательство: Это следует из преобразования выражения (10):

$$T_\mu = \sum_{u=0}^{e} \sigma_u \sum_{x_i \in S \cup T} \tilde{f}_i x_i^{\mu+e-u} =$$

$$= \sum_{x_i \in S \cup T} \tilde{f}_i x_i^\mu \prod_{v_\xi \in V} (x_i - v_\xi) =$$

$$= \sum_{x_i \in S \cup T} \tilde{f}_i x_i^\mu \prod_{v_\xi \in V} (x_i - v_\xi) +$$

$$+ \sum_{v_j \in V} \tilde{f}_{s+r+j} v_j^\mu \prod_{v_\xi \in V} (v_j - v_\xi) =$$

$$= \sum_{x_i \in S \cup T \cup V} \tilde{f}_i x_i^\mu \prod_{v_\xi \in V} (x_i - v_\xi) =$$

$$= \sum_{u=0}^{e} \sigma_u \sum_{x_i \in F} \tilde{f}_i x_i^{\mu+e-u}.$$

Здесь $\prod_{v_\xi \in V} (v_j - v_\xi) = 0$, так как $v_j, v_\xi \in V$.

Что и требовалось доказать.

Это утверждение дает возможность не выбрасывать стертые символы, а задавать им любые ненулевые (или нулевые) значения.

Следствие 1. Величины синдромов T_μ, вычисленные из соотношений (9)÷(12) равны.

Это видно из доказательства утверждения 14.

Вычисления в соответствии с (9)÷(12) назовем *стандартным алгоритмом* определения величин синдромов T_μ.

Следствие 2. Если значения стертых символов принимать не равными нулю и величины синдромов T_μ вычислять из соотношений (11), (12) либо (9) или (10), то ключевое уравнение синдрома для декодирования t ошибок и e стираний имеет вид:

$$T_\mu = \sum_{x_i \in I \cap (S \cup T)} \delta_i x_i^\mu \prod_{v_\xi \in V} (x_i - v_\xi), \qquad (13)$$

где δ_i – величина ошибки, x_i – номер ошибочного узла, v_ξ – номер стертого узла.

Справедливость данного утверждения следует из следствия 1 и утверждения 8.

Список литературы

1. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки: Пер. с англ./Под ред. Р.Л. Добрушина и С.И. Самойленко.– М.: Мир, 1976. – 596 с.

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

3. *Кубицкий В.И.* Последовательный алгоритм декодирования многократных ошибок кодом Лагранжа. – Сб. «Механизация и автоматизация управления». – Киев, №4, 1986. - Деп. №2641-Ук от 5.10.86.

4. *Кубицкий В.И.* Процедуры кодирования и декодирования для полиномиальных кодов. – Сб. научных трудов «Эксплуатация программного обеспечения систем реального времени, построенных на базе микро- и мини-ЭВМ». – Киев: КИИГА, 1989,С. 67-71.

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

6. *Кубицкий В.И.* Кодирование для неполного кода Лагранжа. – Проблеми інформатизації та управління: Збірник наукових праць: Випуск 4 (15). – К.: НАУ, 2005, С. 118-122.