Binary unequal error protection codes as a subclass of generalized (L, G)-codes

Sergey V. Bezzateev and Natalia A. Shekhunova
bsv@aanet.ru sna@delfa.net

Saint Petersburg University of Aerospace Instrumentation,
St.Petersburg, Russia

Linear unequal error protection (UEP) code

Message vector $M = (M_1 M_2 \dots M_f)$, where the length of M_i is equal k_i and

$$k_1+k_2+\dots k_f = k .$$

Codeword $C=(M\ R)$, where the length of R is equal r and

$$k+r = n.$$

Separation vector $S=(s_1 ,s_2 ,..,s_i , \dots ,s_f),$

s_i = dist($C^{(j)}$, $C^{(l)}$) , where $C^{(j)} =(M^{(j)}\ R^{(j)}),\ C^{(l)} =(M^{(l)}\ R^{(l)})$

and $wt(M_i^{(j)})>0,$ $wt(M_i^{(l)})>0.$

Error correcting vector $T=(t_1 ,t_2 , \dots ,t_i, \dots , t_f)$, $t_i= (s_i-1)/2.$

Minimal distance of the code is

$$d = min(s_1, s_2, \dots ,s_f)$$

Optimal (t_1, t_2) UEP codes

Hamming bound for UEP codes

$$r \geq \left]\log\left(1+\sum_{i=1}^{t_2}\binom{n}{i}+\sum_{j=t_2+1}^{t_1}\sum_{i=0}^{t_2}\binom{n-k_1}{i}\binom{k_1}{j-i}\right.\right[$$

Optimal (2, 1) UEP codes

$$H = \begin{bmatrix} 1\ \alpha^{3}\ \alpha^{2\cdot 3} \ldots & \alpha^{2^m\cdot 3} & \alpha^{(2^m+1)\cdot 3} & \alpha^{(2^m+2)\cdot 3} \ldots & \alpha^{(2^{2m}-2)\cdot 3} \\ 1 \qquad \ldots & 0 & \beta & 0 \qquad \ldots & 0 \end{bmatrix}$$

where α - primitive element of GF(2^{2m}) ,

$\beta = \alpha^{2^m+1}$ - primitive element of GF(2^m) ,

m is integer , *m* ł *(*2^m*-1)* , i.e. *m* is odd.

This code has the following parameters:

the length of the code is $n = 2^{2m} - 1$,

the redundancy is $r = 3m$ and

the dimension is $k = 2^{2m} - 3m - 1$, $k_1 = 2^m - m - 1$,

error correcting vector $T=(2 ,1)$, $t_1=2$, $t_2=1$

[1] M. Boyarinov and G. L. Katsman, "Linear Unequal Error Protection Codes", *IEEE Trans. on Information Theory* , Vol. IT-27, No. 2, March 1981, pp. 168-175.

Optimal (t, 1) UEP codes

$$
H = \begin{bmatrix}
1\,\alpha^{2t-1} & \alpha^{2(2t-1)} \ldots & \alpha^{2^m(2t-1)} & \alpha^{(2^m+1)(2t-1)} \ldots & \alpha^{(2^{2m}-2)(2t-1)} \\
1 \quad 0 \quad 0 & \ldots & 0 & \beta^{2t-3} \quad \ldots & 0 \\
\ldots \quad \ldots & & & \ldots. & \ldots \\
1 \quad 0 \quad 0 \ldots & & 0 & \beta^{3} & 0 \\
1 \quad 0 \quad 0 & \ldots & 0 & \beta & 0
\end{bmatrix}
$$

where α - primitive element of GF(2^{2m}) ,

$\beta = \alpha^{2^m+1}$ - primitive element of GF(2^m) ,

m is integer , *m* ł *(2^m-1)* , i.e. *m* is odd.

This code has the following parameters:

the length of the code is $n = 2^{2m} - 1$,

the redundancy is r = (t+1)m and

the dimension is $k = 2^{2m}$ – (t+1)m -1, $k_1 = 2^m - (t-1)m - 1$,

error correcting vector $T=(t, 1)$, $t_1=t$, $t_2=1$

Generalized (L,G) codes

A generalized (L,G)-code is defined by two objects:

- *Locator set L consisting of rational functions* $\frac{v_i(x)}{u_i(x)}, \quad i = 1,\ldots,n$

where $v_i(x)$, $u_i(x)$ *are polynomials with coefficients from* $GF(q^m)$ *such that* $\deg v_i(x) < \deg u_i(x)$ *and* $\gcd(u_i(x); v_i(x)) = 1$; $u_i(x) \neq u_j(x)$ *for any* $i \neq j$;

- *Goppa polynomial* $G(x)$ *with coefficients from* $GF(q^m)$ *such that* $\gcd(u_i(x), G(x)) = 1$.

A vector $a = (a_1\ a_2\ \ldots\ a_n)$ *is a codeword of the generalized (L,G)-code with length n if*

$$\sum_{i=1}^{n} a_i \frac{v_i(x)}{u_i(x)} \equiv 0 \bmod G(x)$$

Generalized (L,G) codes

$$\frac{v_i(x)}{u_i(x)} \equiv f_0^{(i)} + f_1^{(i)}x + \ldots f_{t-1}^{(i)}x^{t-1} \bmod G(x)$$

$$\deg G(x) = t$$

Optimal (2, 1) UEP codes

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{2^m} & \alpha^{2^m+1} & \alpha^{2^m+2} & \ldots & \alpha^{2^{2m}-2} \\ 1 & & & \ldots & 0 & \beta^3 & 0 & \ldots & 0 \end{bmatrix}$$

where α - primitive element of GF(2^{2m}) ,

$\beta = \alpha^{2^m+1}$ - primitive element of GF(2^m) ,

m is integer , m ł (2^m-1) , i.e. m is odd.

[1] M. Boyarinov and G. L. Katsman, "Linear Unequal Error Protection Codes", *IEEE Trans. on Information Theory* , Vol. IT-27, No. 2, March 1981, pp. 168-175.

Optimal (2, 1) UEP codes

By reordering the columns of parity check matrix H it can be rewritten in the following form

$$H = \begin{bmatrix} 1\,\beta\,\beta^2 \ldots \beta^{2^m-2} & \alpha \ldots \alpha^{2^m} & \alpha^{2^m+2} \ldots \alpha^{2^{2m}-2} \\ 1\beta^3\beta^6 \ldots \beta^{3(2^m-2)} & 0 \ldots 0 & 0 \quad \ldots 0 \end{bmatrix}$$

It is possible to update parity check matrix H by two linearly dependent rows:

$$\begin{bmatrix} 1\,\beta^2\beta^4 \ldots \beta^{2(2^m-2)} & \alpha^2 \ldots \alpha^{2\cdot 2^m} & \alpha^{2(2^m+2)} \ldots \alpha^{2(2^{2m}-2)} \end{bmatrix}$$

$$\begin{bmatrix} 1\,\beta^4\beta^8 \ldots \beta^{4(2^m-2)} & \alpha^4 \ldots \alpha^{4\cdot 2^m} & \alpha^{4(2^m+2)} \ldots \alpha^{4(2^{2m}-2)} \end{bmatrix}$$

Optimal (2, 1) UEP codes

Therefore we obtain new parity check matrix H :

$$H = \begin{bmatrix} 1\,\beta\,\beta^{2}\ldots\beta^{2^m-2} & \alpha & \ldots\alpha^{2^m} & \alpha^{2^m+2}\ldots & \alpha^{2^{2m}-2} \\ 1\beta^{2}\beta^{4}\ldots\beta^{2(2^m-2)} & \alpha^{2}\ \ldots & \alpha^{2\cdot 2^m} & \alpha^{2(2^m+2)}\ldots & \alpha^{2(2^{2m}-2)} \\ 1\beta^{3}\beta^{6}\ldots\beta^{3(2^m-2)} & 0 & \ldots\ 0 & 0\ \ldots & 0 \\ 1\beta^{4}\beta^{8}\ldots\beta^{4(2^m-2)} & \alpha^{4} & \ldots\alpha^{4\cdot 2^m} & \alpha^{4(2^m+2)}\ldots & \alpha^{4(2^{2m}-2)} \end{bmatrix}$$

Optimal (2, 1) UEP code as a generalized (L,G)-code

To construct optimal (2,1)UEP code let us choose following objects for generalized (L,G) codes:

- Goppa polynomial $G(x)=x^4$.
- The subset L_1 of numerators for the first $n_1 = 2^m - 1$ positions is

$$L_1 = \left\{ \frac{1}{x+1}, \frac{\beta}{\beta x+1}, \frac{\beta^2}{\beta^2 x+1}, \cdots, \frac{\beta^{n_1-1}}{\beta^{n_1-1} x+1} \right\}, \beta \in GF(2^m)$$

where

$$\frac{\beta^i}{\beta^i x+1} = \beta^i + \beta^{2i} x + \beta^{3i} x^2 + \beta^{4i} x^3 \bmod x^4$$

Optimal (2, 1) UEP code as a generalized (L,G)-code

- The subset L_2 of numerators for the second

$n_2 = 2^{2m} - 2^{\mathrm{m}}$ positions is

$$L_2 = \left\{ \frac{\alpha}{\alpha^2 x^2 + \alpha x + 1}, \frac{\alpha^2}{\alpha^4 x^2 + \alpha^2 x + 1}, \ldots, \frac{\alpha^{2^{2m}-2}}{\alpha^{2(2^{2m}-2)} x^2 + \alpha^{2^{2m}-2} x + 1} \right\},$$

where

$$\frac{\alpha^i}{\alpha^{2i} x^2 + \alpha^i x + 1} = \alpha^i + \alpha^{2i} x + \alpha^{4i} x^3 \bmod x^4,$$

$$\alpha^i \in \{GF(2^{2m}) \setminus GF(2^m)\}.$$

Optimal (2, 1) UEP code as a generalized (L,G)-code

Binary vector

$$a = (a_1^{(1)} a_2^{(1)} \ldots a_{n_1}^{(1)} a_1^{(2)} a_2^{(2)} \ldots a_{n_2}^{(2)})$$

with the length $n = n_1 + n_2$, $n_1 = 2^m - 1$, $n_2 = 2^{2m} - 2^m$
is a codeword of generalized (L, G)-code with (2,1) unequal error protection if

$$\sum_{i=1}^{n_1} a_i^{(1)} \frac{\beta^i}{\beta^i x + 1} + \sum_{j=1}^{n_2} a_j^{(2)} \frac{\alpha^{i_j}}{\alpha^{2i_j} x^2 + \alpha^{i_j} x + 1} \equiv 0 \bmod x^4$$

Decoding algorithm for (2,1) UEP (L,G) codes

Step 1: To calculate a syndrome polynomial *E*(*x*) by the received vector ***b=a+e***:

$$\sum_{i=1}^{n_1} b_i^{(1)} \frac{\boldsymbol{\beta}^i}{\boldsymbol{\beta}^i x + 1} + \sum_{j=1}^{n_2} \mathrm{b}_j^{(2)} \frac{\boldsymbol{\alpha}^{i_j}}{\boldsymbol{\alpha}^{2i_j} x^2 + \boldsymbol{\alpha}^{i_j} x + 1} \equiv$$

$$\sum_{i=1}^{n_1} e_i^{(1)} \frac{\boldsymbol{\beta}^i}{\boldsymbol{\beta}^i x + 1} + \sum_{j=1}^{n_2} \mathrm{e}_j^{(2)} \frac{\boldsymbol{\alpha}^{i_j}}{\boldsymbol{\alpha}^{2i_j} x^2 + \boldsymbol{\alpha}^{i_j} x + 1} \equiv E(x) \bmod x^4$$

Step 2: To find the appropriate rational function $\frac{\boldsymbol{\sigma}(x)}{\boldsymbol{\omega}(x)}$ by using the extended Euclidean algorithm :

$$\frac{\boldsymbol{\sigma}(x)}{\boldsymbol{\omega}(x)} \equiv E(x) \bmod x^4, \deg \boldsymbol{\sigma}(x) < \deg \boldsymbol{\omega}(x) \le 2$$

Decoding algorithm for (2,1) UEP (L,G) codes

Step 3: One or more errors take place in the second part of the codeword with the locator subset L_2 and not more than one error takes place in the first part of the codeword with the locator subset L_1.

To calculate a syndrome polynomial $E^{(1)}(x)$ by the received vector $\boldsymbol{b}^{(1)} = \boldsymbol{a}^{(1)} + \boldsymbol{e}^{(1)}$:

$$\sum_{i=1}^{n_1} b_i^{(1)} \frac{\boldsymbol{\beta}^i}{\boldsymbol{\beta}^i x + 1} \equiv \sum_{i=1}^{n_1} \mathrm{e}_i^{(1)} \frac{\boldsymbol{\beta}^i}{\boldsymbol{\beta}^i x + 1} \equiv \mathrm{E}^{(1)}(x) \bmod x^2$$

Find the appropriate rational function

$$\frac{\boldsymbol{\sigma}^{(1)}(x)}{\boldsymbol{\omega}^{(1)}(x)} \equiv E^{(1)}(x) \bmod x^2 \ , \deg \boldsymbol{\sigma}^{(1)}(x) < \deg \boldsymbol{\omega}^{(1)}(x) \le 1$$

Thank you!

Q & A