Int. J. Appl. Math. Comput. Sci., 2008, Vol. 18, No. 2, 251–257
DOI: 10.2478/v10006-008-0023-x

CREATION OF UNEQUAL ERROR PROTECTION CODES FOR TWO GROUPS OF SYMBOLS

EUGENIUSZ KURIATA

Institute of Control and Computation Engineering
University of Zielona Góra
ul. Podgórna 50, Zielona Góra, Poland
e-mail: E.Kuriata@issi.uz.zgora.pl

This article presents problems of unequal information importance. The paper discusses constructive methods of code generation, and a constructive method of generating asymptotic UEP codes is built. An analog model of Hamming's upper bound and Hilbert's lower bound for asymptotic UEP codes is determined.

Keywords: unequal error protection codes (UEP codes), perfect codes, Hamming's upper bound, Hilbert's lower bound, generation matrix.

1. Importance of information

Even if a small number of symbols is distorted due to information noise in a given information block, such information is rejected regardless of the fact that the remaining symbols in this particular information block are correct. Using detection codes we can only detect the occurrence of a distortion. In order to assure the required level of credibility of any information being sent, correcting codes are applied. Correcting codes can detect errors and reconstruct information that has been distorted provided that the noise level does not exceed the correcting capabilities of the code applied. The most commonly employed codes provide the same level of protection for all the information symbols in an information block. Such an approach assumes that every symbol is of the same importance. As the level of protection should be adequate to the importance of the information, the correcting codes that provide the level of protection required for the most important symbols are in reality applied to the entire information block. However, this solution is not always optimal.

We should now analyse the issue of controlling certain technological processes. The information about the condition of all devices in a managed building is sent to a decision centre (dispatcher). In many cases particular decisions need to be taken, although the acquired information is incomplete or even distorted. In order to avoid such disadvantageous situations, we should guarantee appropriate protection against information distortion and provide a level of credibility which will be appropriate to the importance of the information.

In turn we should now investigate the transfer of information in a railway traffic management system. If we take the safety of railway traffic as the evaluation criterion of information importance, then distorting the "stop" signal (red) into the "go" symbol (green) in a report channel is less dangerous than distorting the "go" signal (green) into the "stop" signal (red). As a result, in the first case the system will force a train in a standstill to stop, whereas in the second case the system will not take any actions to stop a train set in motion. This example shows that information can be of variable importance for a user, depending on the evaluation criterion applied.

The interpretation of an amount of money to be paid for a purchased product can be yet another example of varied information significance in the information block. The figures on the left-hand side are of lesser importance (however, it does not mean that they are not important at all) than the figures on the right-hand side; the longer the sequence is, the more disappointed we are. The above case proves that some symbols in the information block are more important—that is why we should provide the appropriate level of protection with reference to information importance.

In fact, to increase the credibility of information, one usually applies correcting codes. They protect each symbol in the information block against the same number of distortions. Such an approach to information security means that the resources spent on the less important pieces of information are the same as those spent on those parts of information that have higher priority. Hence, the engaged correcting codes protecting every symbol of the information block against the same number of distortions are not always optimal.

It is common knowledge that information has quantitative and qualitative values (Boyarinov and Katsman, 1981; Englund and Hansson, 1997; Masnik and Wolf, 1967). The quantity of information is a constant measure but its importance as a qualitative measure may change. Depending on the chosen criterion, the same piece of information can be of different importance. When evaluating each symbol within the information block, it is reasonable to use correcting codes with unequal error protection codes (UEP codes). These codes provide protection for the symbols or groups of symbols of higher priority against the higher number of distortions and for the remaining symbols they provide a respectively lower level of security. This means that the information received in the transferred information block will be of different level of credibility.

2. Theory of UEP codes

As some data of linear UEP codes will be necessary for further analysis, their basic parameters are specified below.

There exists a linear (n, k, d) code ℓ in the field $GF\,(q)$. $\bar{U} = |u_1 \dots u_k|$ is a registration, and $\bar{X}^{(M)} = \bar{U}\, G_\ell$ is a codeword of ℓ. If the codeword $\bar{X}^{(M)} = |x_1 \dots x_n|$ is distorted, while $wt\,\bar{e} \le t$, then we can define the error vector as

$$\bar{e} = \bar{X}^{(O)} - \bar{X}^{(M)} = |e_1 \dots e_n|\,, \tag{1}$$

where $\bar{X}$ is the obtained distorted codeword.

If the decoding proceeds according to the optimal rule consisting in the search of the nearest codeword (according to Hamming's metric) for the assumed vector $\bar{X}^{(O)}$, and if the i-th symbol in codeword $\bar{X}^{(M)}$ is protected against errors of class $wt\,\bar{E}_i$ whereas the other symbols are protected against errors of class $wt\,\bar{E}_j$, where $wt\,\bar{E}_i > wt\,\bar{E}_j$, then the x_i-th symbol can be decoded correctly if $wt\,\overline{E_i} \ge t > wt\bar{E}_j$ and the error vector distorting the codeword is $\overline{e} \in E_i > E_j$, whereas the other symbols protected against errors of class $wt\,\bar{E}_j$ can be distorted. In general, we can say that if $\bar{E}_i$ is a set of distortion vectors, the magnitude of which is not higher than t_i, then the i-th symbol of the codeword is protected against t_i errors.

Most of the known decoding methods applying Hamming's minimum distance strategy do not use the potential capabilities of the code (Boyarinov, 1980; MacWilliams and Sloane, 1977). If a code provides protection for c_1 symbols against t_1 distortions, for c_2 symbols against t_2 distortions, whereas c_z symbols are protected against t_z distortions, provided that $t_1 < t_2 < \cdots < t_z$, then we can assume that the code protects the codeword against t_1 distortions. This means that if $t < f \le t_j$, then the u_j-th symbol of codeword $\bar{X}$ is protected against $t_j \ge f$ distortions when codeword $\bar{X}$ is protected by the minimum distance of $d_{\min} = 2t + 1$. All other symbols, for which $t_x \ge f$, will be also correctly decoded in this codeword. Hamming's distance between any two codewords with different i-th information symbols should not be lower than $2f_i + 1$ and, as a result, the magnitude of any codeword with a nonzero i-th symbol should not be lower than $2f_i + 1$.

3. Methods of code generation

The structure of concatenating known linear systematic codes mentioned below allows generating of new linear UEP codes (Boyarinov, 1980).

Given rectangular matrices

$$\bar{A} = \left\| \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n_1} \\ a_{21} & a_{22} & \cdots & a_{2n_1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k_1 1} & a_{k_1 2} & \cdots & a_{k_1 n_1} \end{matrix} \right\| \tag{2}$$

and

$$\bar{B} = \left\| \begin{matrix} b_{11} & b_{12} & \cdots & b_{1n_2} \\ b_{21} & b_{22} & \cdots & b_{2n_2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k_2 1} & b_{k_2 2} & \cdots & b_{k_2 n_2} \end{matrix} \right\|, \tag{3}$$

we can form matrices $\bar{A}'$ and $\bar{B}'$ of dimensions $n_1' \times k_1'$ and $n_2' \times k_2'$, respectively, by removing a certain (none if possible) number of rows and columns.

By appropriately concatenating $\bar{A}$ and $\bar{B}$, one can create rectangular matrices

$$\bar{C}_I = \left\| \begin{array}{c|c} \bar{A} & \bar{0}_{\bar{B}} \\ \hline \bar{0}_{\bar{A}} & \bar{B} \end{array} \right\| \tag{4}$$

and

$$\bar{C}_I' = \left\| \begin{array}{c|c} & \bar{0}_{\bar{B}} \\ \bar{A} & \bar{B} \\ & \bar{0}_{\bar{A}} \end{array} \right\| \tag{5}$$

of the following dimensions:

$$\bar{C}_I : n_I \times k_I \,(n_I = n_1' + n_2',\, k_I = k_2' + m,\, 0 \le m \le k_1'),$$
$$\bar{C}_I' : n_I' \times k_I' \,(n_I' = n_1' + n_2',\, k_I' = k_1').$$

Here $\bar{A}'$ is created from $\bar{A}$ after removing $k_1 - k_2$ rows while $k_1 \ge k_2$.

The following matrices will be generated after concatenating matrices $\bar{A}'$ and $\bar{B}'$:

$$\bar{C}_{II} = \left\| \begin{array}{c:c} \bar{A}' & \bar{0}_{\bar{B}'} \\ \hdashline \bar{0}_{\bar{A}'} & \bar{B}' \end{array} \right\| \quad (6)$$

and

$$\bar{C}'_{II} = \left\| \begin{array}{c:c:c} \multicolumn{3}{c}{\bar{A}'} \\ \hdashline \bar{0}_{\bar{B}'} & \bar{B}' & \bar{0}_{\bar{A}'} \end{array} \right\| \quad (7)$$

of the following dimensions:

$$\bar{C}_{II} : n_{II} \times k_{II}\,(n_{II} = m + n'_2,\ k_{II} = k'_1 + k'_2,\ 0 \le m \le n'_1),$$
$$\bar{C}'_{II} : n'_{II} \times k'_{II}\,(n'_{II} = n'_1,\ k'_{II} = k'_1 + k'_2).$$

The presented concatenations of matrices can be used to generate new correcting codes. However, we shall focus on two special cases of concatenation of type I:

$$\bar{C}' = \| \, \bar{A} \,\vdots\, \bar{B} \, \|, \quad (8)$$

$$\bar{C}'' = \left\| \begin{array}{c:c} \bar{A} & \begin{array}{c} \bar{B} \\ \hdashline \bar{0}_{\bar{B}} \end{array} \end{array} \right\|. \quad (9)$$

It is evident that if ℓ_1 and ℓ_2 are linear (n_1, k_1, d_1) and (n_2, k_2, d_2) codes in $GF(q)$, given by generation matrices $\bar{G}_1$ and $\bar{G}_2$, then the concatenation of type $\bar{G}'$ (concatenation of matrices $\bar{G}_1$ and $\bar{G}_2$) generates a linear $(n_1 + n_2, k_2 = k_1, d' = d_1 + d_2)$ code ℓ', while the concatenation of type $\bar{G}''$ will generate a linear $(n_1 + n_2, k_1, d'' \ge d_1)$ code ℓ''. This results from the fact that for code ℓ'' the number of information symbols is $k_1 > k_2$. A particular switch of the rows in $\bar{A}$ can result in generating a code which will protect two groups of symbols: the first group will be protected by Hamming's distance of $d' = d_1 + d_2$ and the second one by $d'' \ge d_1$. It is often possible to select a matrix $\bar{G}_1$ from code ℓ_1 (by removing a number of rows and columns) such that the obtained code ℓ'' will have the minimum distance $d'' > d_1$.

Let us assume that if some rows and columns are switched, it is possible to select a subcode $\tilde{\ell}_1$ of $(n_1,\ \tilde{k}_1)$ from code ℓ_1 whose dimensions are (n_1, k_1) with the minimum distance $\tilde{d}_1 > d_1$, where $\tilde{k}_1 = k_1 - k_2$. We will then create a matrix of code ℓ_1 in such a way that its $\tilde{k}_1$ rows will be the base of subcode $\tilde{\ell}_1$.

The matrix

$$\bar{G}' = \left\| \begin{array}{c:c} \bar{G}_1 & \begin{array}{c} \bar{G}_2 \\ \hdashline \bar{0} \end{array} \end{array} \right\| = \left\| \begin{array}{cc} \hat{G} & \bar{G}_2 \\ \tilde{G}_1 & \bar{0} \end{array} \right\| \quad (10)$$

generates a linear $(n_1 + n_2, k_1)$ code ℓ'' with the minimum distance of $d'' = \min(d_1, d_1 + d_2)$, where matrices $\tilde{G}_1$,

$$\bar{G}_1 = \left\| \begin{array}{c} \hat{G} \\ \tilde{G}_1 \end{array} \right\|,$$

and $\bar{G}_2$ are code generation matrices for $\tilde{\ell}_1$, ℓ_1 and ℓ_2, respectively, whereas $\bar{0}$ is a zero matrix whose dimensions are $n_2 \times (k_1 - k_2)$.

4. Generation of asymptotically perfect UEP codes

The necessary and sufficient conditions to generate linear codes are specified by Lemma 1 (Boyarinov, 1980) and Theorem 2 (Kacman, 1980). Taking into account all the necessary and sufficient conditions for code generation and the above-described methods of matrix concatenation, the optimal linear UEP code with two groups of symbols protected against distortions f_1 and f_2, respectively, can be obtained, where $f_1 > f_2$ (Kuriata, 1982).

The matrix concatenations

$$\bar{C}_{III} = \left\| \begin{array}{c:c} \bar{A} & \bar{0} \\ \hdashline \bar{0} & \bar{B} \end{array} \right\| \quad (11)$$

and

$$\bar{C}'_{III} = \| \, \bar{A} \,\vdots\, \bar{B} \, \|, \quad (12)$$

are analysed below, where the dimensions of matrices $\bar{A}$ and $\bar{B}$ are $n_1 \times k_1$ and $n_2 \times k_2$, respectively. An $(n_1 + n_2) \times (k_1 + k_2)$ matrix of type $\bar{C}_{III}$ generates an $\Re$ code with the minimum distance of $d = \min(d_1, d_2)$, while an $(n_1 + n_2) \times \max(k_1, k_2)$ matrix of type $\bar{C}'_{III}$ generates a λ code with the minimum distance of

(a) $d_{\min} = d_1 + d_2$ if $k_1 = k_2$,

(b) $d_{\min} = d_1$ if $k_1 > k_2$ and $d_1 > d_2$,

(c) $d_{\min} = d_2$ if $k_1 < k_2$ and $d_1 < d_2$.

If the component codes $\bar{A}$ and $\bar{B}$ protect the information against the same number of distortions, then the codes generated on the basis of the structures of type $\bar{C}_{III}$ or $\bar{C}'_{III}$ often have worse parameters than other codes of the same length, number of information symbols, and correcting capabilities (MacWilliams and Sloane, 1977). The structures presented above enable the generation of asymptotically perfect UEP codes.

Now UEP codes will be generated with the use of the presented methods of matrix concatenation, while the matrices of known codes will constitute component matrices. Hamming's code $\overline{H}$ with parameters $n = 2^N - 1$, $k = 2^N - 1 - N$, $d = 3$ and $N \ge 3$ will be used as a base code.

A matrix

$$\bar{C}_{III} = \left\| \begin{array}{c:c} \bar{G}_H & \bar{0} \\ \hdashline \bar{0} & \overline{H}' \end{array} \right\| \quad (13)$$

will be created. The dimensions of the matrix are $(2^N + N) \times (2^{N+1} + N - 1)$, where $\bar{G}_H$ is Hamming's code generation matrix whose dimensions are $k_1 \times (k_1 + r)$, $\overline{H}'$

is Hamming's code orthogonal matrix whose dimensions are $(k_1 + r) \times r$.

After swapping some columns and rows, the following matrix is created:

$$\tilde{\bar{C}}_{III} = \left\| \begin{array}{c|c} \bar{N} & \bar{I} \\ \hline \bar{0} & \bar{H}^T \end{array} \right\|, \tag{14}$$

where $\bar{N}$ is a matrix of Hamming's code control positions whose dimensions are $N \times \left(2^N - 1 - N\right)$, $\bar{I}$ is a matrix of Hamming's code information positions whose dimensions are $N \times N$, $\overline{H}^T$ is Hamming's code transposed control matrix whose dimensions are $\left(2^N - 1 - N\right) \times N$, $\bar{0}$ is a zero matrix whose dimensions are $\left(2^N - 1\right) \times \left(2^N - N - 1\right)$.

If Hamming's extended code ($n = 2^N$, $k = 2^N - 1 - N$, $d = 4$) is used in (14), then a code will be generated as in Fig. 1. We have

$$\Re = \left\| \quad \bar{1} \quad \begin{array}{c|c} \bar{N}_R & \bar{I}_R \\ \hline \bar{0}_R & \bar{N}_R^T \end{array} \right\|, \tag{15}$$

where $\bar{1}$ is a diagonal (all-ones) matrix whose dimensions are $2^N \times 2^N$, $\bar{N}_R$ is a matrix of Hamming's extended code control symbols whose dimensions are $(N+1) \times \left(2^N - 1 - N\right)$, $\bar{I}_R$ is a matrix of Hamming's extended code information symbols whose dimensions are $(N+1) \times (N+1)$, $\overline{N}_R^T$ is a transposed control matrix of Hamming's extended code redundant symbols whose dimensions are $\left(2^N - 1 - N\right) \times (N+1)$, $\bar{0}_R$ is a zero matrix whose dimensions are $\left(2^N - N - 1\right) \times \left(2^N - N - 1\right)$.

$$\Re = \left| \begin{array}{l}
1000000000001111111100000000 \\
0100000000001111000011110000 \\
0010000000001100110011001100 \\
0001000000001010101010101010 \\
0000100000001111111111111111 \\
0000010000000000000100000001 \\
0000001000000000000100000011 \\
0000000100000000000100000101 \\
0000000010000000000100000111 \\
0000000001000000000100010001 \\
0000000000100000000100010011 \\
0000000000010000000100010101 \\
0000000000001000000100010111
\end{array} \right|$$

Fig. 1. $\Re$ code matrix created according to (14) for $N = 4$.

Two groups of symbols protected against various numbers of distortions can be found in the codeword of the code $\Re$: the first group is protected against f_1 errors and the second group against f_2 errors, while $f_1 > f_2$. The matrix (15) generates an $\Re$ code which protects $N + 1$ against f_1 distortions, whereas $2^N - 1$ symbols protect against f_2 distortions.

The parameters of the code $\Re$ are presented below:

(a) length of the code sequence: $n = 2^{N+1}$;

(b) correcting capability of symbols protected against f_1 errors: $d_1 = 2^{N-1} + 2$;

(c) correcting capability of symbols protected against f_2 errors: $d_2 = 3$;

(d) correcting capability of symbols protected against f_2 errors: $k_1 = N + 1$;

(e) number of symbols protected against f_1 errors: $k_2 = 2^N - 1 - N$.

With $n \to \infty$ the code is not trivial (Fig. 2), for

$$D = \frac{d}{n} = \frac{d_1}{n} = \frac{2^{N-1} + 2}{2^{N+1}} = \frac{1}{4}$$

and

$$R = \frac{k}{n} = \frac{(2^N - N - 1) + (N + 1)}{2^{N+1}} = \frac{1}{2}.$$

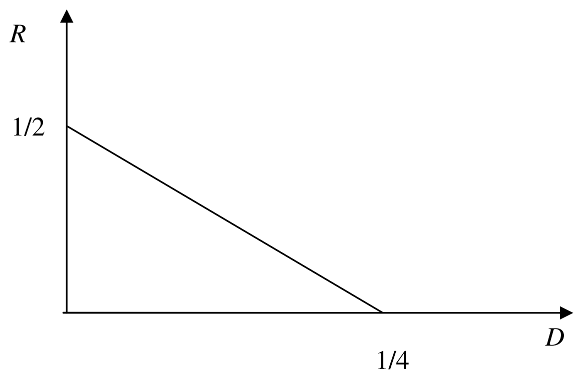

Fig. 2. Asymptotic ($n \to \infty$) bounds of the code $\Re$.

Matrix concatenation will now be using the following rule:

$$\bar{C}_{IV} = \left| \begin{array}{c} \bar{H} \\ \hline \bar{0} \;\big|\; \bar{H}^T \end{array} \right| = \left| \begin{array}{c|c} \bar{N} & \bar{I} \\ \hline \bar{0} & \bar{H}^T \end{array} \right|. \tag{16}$$

The dimensions of the matrix $\bar{C}_{IV}$ will be $\left(2^N + N\right) \times 2^N$, and the component submatrices will be as follows: $\bar{H}$ is a matrix of Hamming's extended code parity tests $(N+1) \times 2^N$, $\bar{H}^T$ is a transposed matrix of Hamming's extended code parity tests $2^N \times (N+1)$, $\bar{N}$ is a submatrix of control symbols in the matrix of Hamming's extended code parity tests whose dimensions are $\big((N+1)\times\big(2^N-1-N\big)\big)$, $\bar{I}$ is a submatrix of information symbols in the matrix of extended Hamming's code parity tests whose dimensions are $(N+1)\times(N+1)$, $\bar{0}$ is a zero matrix whose dimensions are $2^N\times\big(2^N-N-1\big)$.

By means of the structure $\bar{C}_{IV}$ a code can be created as in Fig. 3. We have

$$\Im = \left\| \begin{array}{c|c|c} \bar{1} & \bar{N} & \bar{I} \\ \hline & \bar{0} & \bar{H}^T \end{array} \right\|, \tag{17}$$

where $\bar{1}$ is a diagonal (all-ones) matrix whose dimensions are $\big(2^N+N+1\big)\times\big(2^N+N+1\big)$.

$$\Im = \left| \begin{array}{lll}
100000000000000000000 & 1111111100 & 000000 \\
010000000000000000000 & 1111000011 & 110000 \\
001000000000000000000 & 1100110011 & 001100 \\
000100000000000000000 & 1010101010 & 101010 \\
000010000000000000000 & 1111111111 & 111111 \\
000001000000000000000 & 0000000000 & 000001 \\
000000100000000000000 & 0000000000 & 000011 \\
000000010000000000000 & 0000000000 & 000101 \\
000000001000000000000 & 0000000000 & 000111 \\
000000000100000000000 & 0000000000 & 010001 \\
000000000010000000000 & 0000000000 & 010011 \\
000000000001000000000 & 0000000000 & 010101 \\
000000000000100000000 & 0000000000 & 010111 \\
000000000000010000000 & 0000000100 & 000001 \\
000000000000001000000 & 0000000100 & 000011 \\
000000000000000100000 & 0000000100 & 000101 \\
000000000000000010000 & 0000000100 & 000111 \\
000000000000000001000 & 0000000100 & 010001 \\
000000000000000000100 & 0000000100 & 010011 \\
000000000000000000010 & 0000000100 & 010101 \\
000000000000000000001 & 0000000100 & 010111
\end{array} \right|$$

Fig. 3. $\Im$ code matrix created according to (17) for $N=4$.

According to the theory of codes, $d_{\min} = \min\big(wt\,\big(\bar{X}^{(i)}\big)\big)$. In the generated matrix the magnitude of the $(N+2)$-th row is $wt\,R_p = 2$. As a result, a code $\Im$ with the minimum Hamming distance $d_{\min} = 2$ (symbol) is a detection code. Once we remove the $(N+2)$-th row from this matrix (in this case the sixth), we will obtain a new matrix of the code $d_{\min} = 3$ (symbol) with the minimum distance.

The matrix (17) obtained after the application of the correction will have the following form:

$$\aleph = \left\| \begin{array}{c|c|c} \bar{1} & \bar{N} & \bar{I} \\ \hline & \bar{0} & \bar{H}_m^T \end{array} \right\|, \tag{18}$$

whose dimensions are $\big(2^N+N\big)\times\big(2^{N+1}-1\big)$ (Fig. 4), where: $\bar{N}$ is a submatrix of control symbols in the matrix of Hamming's extended code parity tests whose dimensions are $(N+1)\times\big(2^N-1-N\big)$, $\bar{I}$ is a submatrix of information symbols in the matrix of Hamming's extended code parity tests whose dimensions are $(N+1)\times(N+1)$, $\bar{0}$ is a zero matrix whose dimensions are $\big(2^N-1\big)\times\big(2^N-N-1\big)$, $\bar{H}_m^T$ is a transposed matrix of extended code parity tests.

The code $\aleph$ has the following parameters:

(f) length of the code sequence: $n = 2^N + 2^N + N = 2^{N+1} + N$,

(g) correcting capability of symbols protected against f_1 errors: $d_1 = 2^{N-1} + 2$,

(h) correcting capability of symbols protected against f_2 errors: $d_2 = 3$,

(i) number of symbols protected against f_1 errors: $k_1 = N + 1$;

(j) number of symbols protected against f_2 errors: $k_2 = 2^N - 1$.

$$\aleph = \left| \begin{array}{lll}
10000000000000000000 & 1111111100 & 000000 \\
01000000000000000000 & 1111000011 & 110000 \\
00100000000000000000 & 1100110011 & 001100 \\
00010000000000000000 & 1010101010 & 101010 \\
00001000000000000000 & 1111111111 & 111111 \\
00000100000000000000 & 0000000000 & 000011 \\
00000010000000000000 & 0000000000 & 000101 \\
00000001000000000000 & 0000000000 & 000111 \\
00000000100000000000 & 0000000000 & 010001 \\
00000000010000000000 & 0000000000 & 010011 \\
00000000001000000000 & 0000000000 & 010101 \\
00000000000100000000 & 0000000000 & 010111 \\
00000000000010000000 & 0000000100 & 000001 \\
00000000000001000000 & 0000000100 & 000011 \\
00000000000000100000 & 0000000100 & 000101 \\
00000000000000010000 & 0000000100 & 000111 \\
00000000000000001000 & 0000000100 & 010001 \\
00000000000000000100 & 0000000100 & 010011 \\
00000000000000000010 & 0000000100 & 010101 \\
00000000000000000001 & 0000000100 & 010111
\end{array} \right|$$

Fig. 4. $\aleph$ matrix after removing selected columns and rows created according to (18).

Asymptotic ($n \to \infty$) parameters of the code $\aleph$ are

$$D = \frac{d}{n} = \frac{d_1}{n} = \frac{2^{N-1}+2}{2^{N+1}} = \frac{1}{4}$$

and

$$R = \frac{k}{n} = \frac{(2^N - N - 1) + (N + 1)}{2^{N+1}} = \frac{1}{2}.$$

This code reaches Hamming's upper bound and Hilbert's lower bound (Kuriata, 1982).

5. Bounds of UEP codes

Theorem 1. *There exists a $\bar{G}_1$ generation matrix of a $(2^N - 1, 2^N - N - 1, 3)$ Hamming code ($N \geq 3$). If an $N \times (2^N - 1)$ matrix $\bar{G}_2$ exists, the matrix*

$$\left\| \begin{matrix} \bar{G}_1 \\ \bar{G}_2 \end{matrix} \right\|$$

generates the space of all binary $(2^N - 1)$-vectors and a $(2^N - 1, N)$ matrix $\bar{S}$ with the minimum distance of 2^{N-1}, then the matrix

$$\left\| \begin{matrix} \bar{G}_1 & \bar{0} \\ \bar{G}_2 & \bar{S} \end{matrix} \right\|$$

generates a linear code with the following parameters:

$$(2^{N+1} + N - 2, 2^N + N - 1, \underbrace{2^{N-1}, \dots, 2^{N-1}}_{N}, \underbrace{3, \dots, 3}_{2^N - 1})$$

being at Hamming's upper bound.

Proof. That the code generated by the matrix

$$\left\| \begin{matrix} \bar{G}_1 & \bar{0} \\ \bar{G}_2 & \bar{S} \end{matrix} \right\|$$

is the code

$$(2^{N+1} + N - 2, 2^N + N - 1, \underbrace{2^{N-1}, \dots, 2^{N-1}}_{N}, \underbrace{3, \dots, 3}_{2^N - 1})$$

results directly from the structure of $\bar{G}''$ (10). ■

A new matrix

$$C = \left\| \quad \bar{1} \quad \begin{array}{c|c} \bar{A} & \bar{I} \\ \hline \bar{0} & \bar{G}_{H'} \end{array} \right\|$$

generates a code with the parameters specified in Theorem 1.

The UEP codes presented below asymptotically reach Hilbert's bound

$$R_1 (R_2, \delta_1, \delta_2) \geq \begin{cases} \beta \left(1 - H \left[(\delta_1 - \delta_2) / \beta \right] \right) \\ \Leftarrow 2 (\delta_1 - \delta_2) \leq \beta \leq (\delta_1 - \delta_2) \delta_1, \\ \beta - H (\delta_1) + (1 - \beta) H \left(\dfrac{\delta_2}{1 - \beta} \right) \\ \Leftarrow \dfrac{(\delta_1 - \delta_2)}{\delta_1} < \beta \leq 1 - 2\delta_2, \end{cases} \tag{19}$$

where

$$R_2 = (1 - \beta) \left[1 - H \left(\frac{\delta_2}{1 - \beta} \right) \right], \quad \delta = \lim_{n \to \infty} \left(\frac{d}{n} \right),$$

$$0 \leq \beta \leq 1 - 2\delta_2,$$

and also Griesmer's bound

$$2^{N+1} + N - 2 = \sum_{i=0}^{N-1} \left\lceil \frac{2^{N-1}}{2^i} \right\rceil + \sum_{i=N}^{2^N - 2} \left\lceil \frac{3}{2^i} \right\rceil. \tag{20}$$

A conclusion can be drawn that having a specified length of any linear $(n, k, d_1, d_2, \dots, d_k)$ code, the dependence

$$n \geq \sum_{j=1}^{k} \frac{d_j}{2^{k-j}} \tag{21}$$

can be adopted as an analog model of Plotkin's bound for UEP codes (Kuriata, 1982).

The types of matrix concatenations discussed in the article enable the generation of codes that reach both Hilbert's lower bound and Hamming's upper bound (Kuriata, 1982). The asymptotic bounds of the analysed codes are presented in Fig. 5.

The bounds of codes protecting all symbols in the codeword against the same number of distortions are defined by the following dependences: Hamming's upper bound

$$\sum_{i-o}^{t} C_n^i (q - 1)^i \leq q^r,$$

and Hilbert's lower bound

$$q^r \geq \sum_{i-o}^{d-1} C_n^i (q - 1)^i.$$

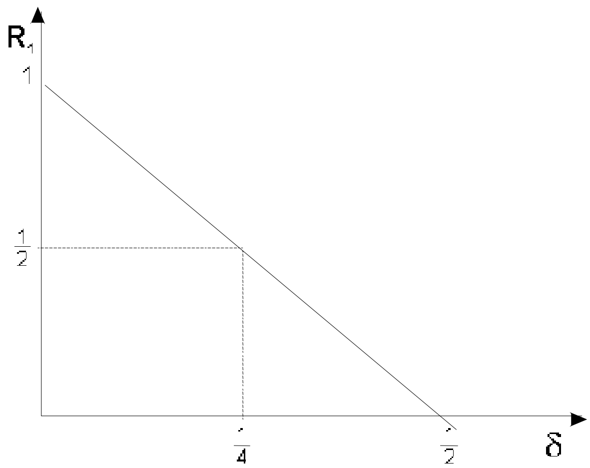

Fig. 5. Asymptotic bounds for UEP codes ($n \to \infty, \delta_2 = 0$) (Kuriata, 1982).

Graphically such bounds are usually presented on graphs of coordinates of $R = k/n$ and $D = d/n$.

In the case of UEP codes a graph of bounds cannot be made in a similar way because here the groups of symbols are protected against various numbers of distortions. Hence, we can determine bounds in the s-dimensional space, where s is the number of symbol groups protected against f_i distortions.

Figure 6 presents the graph of bounds for a family of codes generated by means of (16) with the following parameters:

$$\aleph \Big\{ n = 2^{N+1} + N, k_1 = N+1, k_2 = 2^N - 1, \\ d_1 = 2^{N-1} + 2, d_2 = 3 \Big\}.$$

According to (17) and (18), the generated codes can be taken as broadband codes (Kower, 1974), in which $R_2 = f(R_1)$ (Fig. 6).

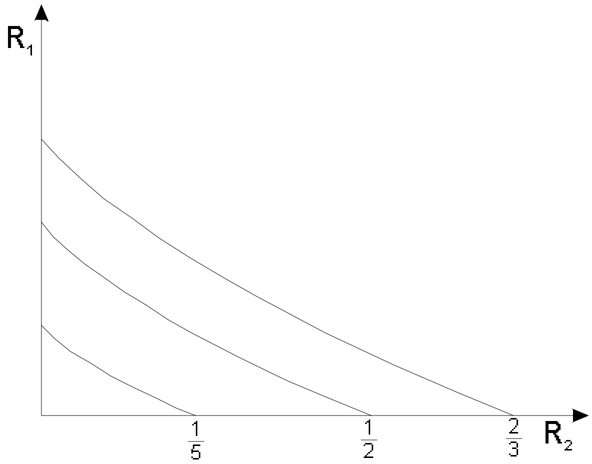

Fig. 6. Analog model of Hilbert's bound for UEP codes ($R_2 = f(R_1)$).

6. Conclusion

The constructive methods of code generation presented in this paper enable the generation of codes with two groups of symbols being differently protected. They are called "floating protection codes" (Kuriata, 1982). It is thus justified to use UEP codes in order to protect information of variable importance, for we can significantly shorten the length of the code block while maintaining the appropriate level of credibility for top-priority information. Such a code block would be longer if we used codes which protect the entire information block against the same number of distortion. Hence, it has been established that the bounds for the asymptotically perfect UEP codes (Hemming's upper bound and Hilbert's lower bound) coincide.

References

Boyarinov I.M. (1980). Constructing linear unequal error protection codes, *Problemy Peredachi Informatsii* **16**(2): 103–107, (in Russian).

Boyarinov I.M and Katsman G.L. (1981). Linear unequal error protection codes, *IEEE Transactions on Information Theory* **IT-27**(2): 168-175.

Englund E.K. and Hansson A.I. (1997). Constructive codes with unequal error protection, *IEEE Transactions on Information Theory* **43**(2): 715–721.

Kacman G. L. (1980). Bounds on volume of linear codes with unequal information symbol protection, *Problemy Peredachi Informatsii* **16**(2): 99–105, (in Russian).

Kower T. M. (1974). *Broadband Information Charnels*, Mir, Moscow, (in Russian).

Kuriata E. (1982). *Investigation and Synthesis Principles of Channel Creation for Dispatcher Centralization Systems, Ph.D. thesis,* Moscow State University of Railway Engineering, MIIT, (in Russian).

MacWilliams F. J. and Sloane N. J. A. (1977). *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam.

Masnik B. and Wolf J. (1967). On linear unequal error protection codes, *IEEE Transactions on Information Theory*, **IT-13**(4): 600–607.

Received: 26 February 2007
Revised: 26 March 2007
Re-revised: 19 December 2007