Mathematica
Balkanica

Mathematical Society of South-Eastern Europe
A quarterly published by
the Bulgarian Academy of Sciences – National Committee for Mathematics

For further information on Mathematica Balkanica visit the website of the journal
http://www.mathbalkanica.info
or contact:
Mathematica Balkanica - Editorial Office;
Acad. G. Bonchev str., Bl. 25A, 1113 Sofia, Bulgaria
Phone: +359-2-979-6311, Fax: +359-2-870-7273,
E-mail: balmat@bas.bg

Mathematica
Balkanica

New series Vol. 4, 1990, Fasc. 2

Some Improvements of a Decoding Algorithm for Linear Codes

Miodrag Živković

Presented by Ž. Mijajlović

A probabilistic method for decoding linear codes is considered, where the a posteriori probabilities of error (APPE) are repeatedly computed. Methods for more precise and more efficient computation of APPE are proposed. These methods are useful when combined with some information set decoding method.

Introduction

Binary linear (n, k) code C with the parity check $r\times n$ matrix H is the null-space of H, where $r=n-k$. Additions, denoted by $\oplus$, and multiplications are operations of the field GF(2). Unless otherwise specified, all vectors will be assumed to be column vectors. Let us introduce the following useful notation. Suppose M is a matrix, and let J be an arbitrary subset of the set of column indices in M. Then M_J will denote the matrix whose columns are all the columns of M with indices in J, in the same order as they appear in M. If M is a column vector, then $((\mathsf{M}^T)_J)^T$ will be written simply as M_J. Here T stands for the operation of the matrix transposition. If $J=\{j\}$, then instead of $\mathsf{M}_{\{j\}}$ it will be written M_j. For a binary vector u the weight of u, i.e. the number of ones among its coordinates will be denoted by $W(\mathsf{u})$.

Let $\mathsf{E}=[E_1, E_2, \dots, E_n]^T$ denote the error-vector, i.e. the n-dimensional binary random vector with pairwise independent coordinates, having the probability distribution given by

$$P\{E_i=1\}=p_i,\ P\{E_i=0\}=q_i=1-p_i,\ 1\leqq i\leqq n.$$

Let $\mathsf{x}\in C$ be an arbitrary codeword. Then the vector $\mathsf{Y}=\mathsf{x}\oplus\mathsf{E}$ is called the received message, because it is formed from the codeword x by including random errors. To decode a received message y, the realization of the random variable Y, means to find a codeword $\hat{\mathsf{x}}\in C$ such that for every $\mathsf{x}'\in C$ the following inequality holds

$$P\{\mathsf{E}=\hat{\mathsf{x}}\oplus\mathsf{y}\}\geqq P\{\mathsf{E}=\mathsf{x}'\oplus\mathsf{y}\}.$$

Symbol-by-symbol decoding method for linear codes [5] consists of complementing those bits of the received message which have the a posteriori probability of error greater than 1/2. It is often practically impossible to compute exactly the a posteriori probabilities of error (APPE), because they depend in a very complicated way on all bits of the received message. The reasonable solution to that problem is to compute the approximate values of APPE, using only a part of parity checks for every bit of the received message. After that, one can replace the a priori probabilities of error by so computed APPE, then to compute the new APPE, and so on (see for example [2, pp. 157], [4]; also [1]). Information set of the code C is any subset of k coordinates of a codeword uniquely determining all other coordinates of the codeword. Using a vector of APPE, one can randomly choose some number of highly reliable information sets (information sets such that the respective coordinates of some APPE-vector are close to 0 or 1) and then to compute the codewords defined by y and these information sets. If there are not many errors in the received message, then all the computed codewords will be equal to the codeword $\hat{\mathsf{x}}$. It is possible to correct all errors in the received message using the APPE-vector.

The a posteriori probabilities of error are the conditional probabilities

$$(1)\qquad \begin{aligned} P_i &= P(\{E_i=1\}\mid\{\mathsf{H}^{(i)}\mathsf{E}=\mathsf{H}^{(i)}\mathsf{y}\}) \\ &= \frac{P\{\mathsf{H}^{(i)}\mathsf{E}=\mathsf{H}^{(i)}\mathsf{y},\ E_i=1\}}{P\{\mathsf{H}^{(i)}\mathsf{E}=\mathsf{H}^{(i)}\mathsf{y}\}},\quad 1\leqq i\leqq n. \end{aligned}$$

The matrix $\mathsf{H}^{(i)}$, $1\leqq i\leqq n$, with r_i rows and n columns, has all ones in the i-th column, and the space C is a subspace of the null-space of the matrix $\mathsf{H}^{(i)}$ (see for example [3]). It is possible to choose $\mathsf{H}^{(i)}=\mathsf{H}$ for all i, $1\leqq i\leqq n$, but in that case the complexity of the computing of the APPE might be inconveniently large.

We are going to describe a decoding algorithm for linear codes. Let $F_{\mathsf{y}}:[0,1]^n\to[0,1]^n$ be the function transforming the probability vector p into the APPE-vector P,

$$F_{\mathsf{y}}(\mathsf{p})=\mathsf{P}.$$

Decoding algorithm under the consideration starts by computing some number $g\geqq 1$ of vectors from the sequence $\{\mathsf{P}^{(j)}\}_{j\geqq 1}$ given by the first member $\mathsf{P}^{(0)}=\mathsf{p}$ and by the recurrent relation

$$\mathsf{P}^{(j+1)}=F_{\mathsf{y}}(\mathsf{P}^{(j)}).$$

The next step is to form the vector $\bar{\mathsf{y}}$, corrected version of the received message y,

$$(2)\qquad \bar{y}_i=\begin{cases} y_i, & P_i^{(g)}\leqq 1/2 \\ 1\oplus y_i, & P_i^{(g)}>1/2 \end{cases},\quad 1\leqq i\leqq n.$$

Under some conditions connected with the error-vector (which will not be considered in this paper, see for example [1]) the vector $\bar{\mathsf{y}}$ is equal to $\hat{\mathsf{x}}$, or at least some of its highly reliable coordinates, forming the information set, are equal to the corresponding coordinates of the vector $\hat{\mathrm{x}}$. That means that the vector $\bar{\mathrm{y}}$ can be taken as the result of decoding of the received message y.

It is well-known that the complexity of the computing the APPE grows exponentially with the exponent min $\{k_i, r_i\}$. A method for reducing this complexity using the equivalent, but smaller, parity check matrices is given in Section 1. The method is a generalization of the method used in [1]. In computing the vectors $\{\mathrm{P}^{(j)}\}_{1\leqq j\leqq g}$, a numerical problem may arise. Namely, the coordinates of these vectors can get very close to 0 or 1, and consequently they cannot be distinguished from that two values. In Section 2. a solution will be given for this problem. The sequence of the algebraic value vectors is computed instead of the APPE-vectors. In Section 3. an example is given.

1. A method for computing the APPE

In the equation (1) it can be supposed without loss of generality that $0\leqq p_i\leqq 1/2$, for all i, $1\leqq i\leqq n$. That can be seen by the following reasoning. Let E' be a random binary vector given by $\mathrm{E}'=\mathrm{E}\oplus\mathrm{d}$, where

$$d_i=\begin{cases}0, & p_i\leqq 1/2\\ 1, & p_i>1/2\end{cases}, \quad 1\leqq i\leqq n.$$

Then for all i, $1\leqq i\leqq n$, it is obviously $P\{E_i'=1\}=p_i'\leqq 1/2$. If the vector y' is defined by $\mathrm{y}'=\mathrm{y}\oplus\mathrm{d}$, then the equalities $\mathrm{H}^{(i)}\mathrm{E}=\mathrm{H}^{(i)}\mathrm{y}$ and $\mathrm{H}^{(i)}\mathrm{E}'=\mathrm{H}^{(i)}\mathrm{y}'$ are equivalent. Thus we have

$$\begin{aligned}P_i'&=P(\{E_i'=1\}\,|\,\{\mathrm{H}^{(i)}\mathrm{E}'=\mathrm{H}^{(i)}\mathrm{y}'\})\\ &=P(\{E_i\oplus d_i=1\}\,|\,\{\mathrm{H}^{(i)}\mathrm{E}=\mathrm{H}^{(i)}\mathrm{y}\})\\ &=\begin{cases}P_i, & p_i\leqq 1/2\\ 1-P_i, & p_i>1/2\end{cases}.\end{aligned}$$

The set C_i of the binary vectors defined by $C_i=\{\mathrm{e}\in B^n\,|\,\mathrm{H}^{(i)}\mathrm{e}=\mathrm{O}^{(r)}\}$ (where $B=\{0, 1\}$ and $\mathrm{O}^{(r)}$ denotes the r-dimensional vector with all coordinates equal to zero) is a group under the operation $\oplus$. For arbitrary $\mathrm{y}\in B^n$ the set $C_{i,\mathrm{y}}$ given by

$$\begin{aligned}C_{i,\mathrm{y}}&=C_i\oplus\mathrm{y}=\{\mathrm{e}\oplus\mathrm{y}\,|\,\mathrm{e}\in C_i\}=\{\mathrm{e}\,|\,\mathrm{e}\oplus\mathrm{y}\in C_i\}\\ &=\{\mathrm{e}\,|\,\mathrm{e}\in B^n,\ \mathrm{H}^{(i)}\mathrm{e}=\mathrm{H}^{(i)}\mathrm{y}\}\end{aligned}$$

is a coset of the group C_i. Let C_i^u denote the set

$$C_i^u=\{\mathrm{e}\in B^n\,|\,\mathrm{H}^{(i)}\mathrm{e}=\mathrm{O}^{(r)},\ e_i=u\},\ u\in B.$$

The set C_i^0 is a subgroup of the group C_i, and the set C_i^1 is its coset. Finally, let

$$C_{i,\mathrm{y}}^u=\{\mathrm{e}\,|\,\mathrm{e}\in C_{i,\mathrm{y}},\ e_i=u\},\ u\in B.$$

Then the equation (1) can be written in the following way

$$P_i = \frac{\Sigma_{\mathsf{e}\in C^1_{i,\mathsf{y}}} P\{\mathsf{E}=\mathsf{e}\}}{\Sigma_{\mathsf{e}\in C_{i,\mathsf{y}}} P\{\mathsf{E}=\mathsf{e}\}}$$

$$(3) \qquad = \left(1+\frac{\Sigma_{\mathsf{e}\in C^0_{i,\mathsf{y}}} \Pi^n_{j=1} p_j^{e_j} q_j^{1-e_j}}{\Sigma_{\mathsf{e}\in C^1_{i,\mathsf{y}}} \Pi^n_{j=1} p_j^{e_j} q_j^{1-e_j}}\right)^{-1}, \quad 1 \leqq i \leqq n.$$

To compute P_i by this equation, it is necessary to perform $n2^{k_i}$ real multiplications (where $k_i = n - r_i$) because $|C_{i,\mathsf{y}}| = 2^{k_i}$.

Obviously, the value of (3) does not depend on those probabilities p_j for which the corresponding column of the parity check matrix $\mathsf{H}^{(i)}$ is a zero vector, $\mathsf{H}^{(i)}_j = \mathsf{O}^{(r)}$. The following theorem shows that the parity-check matrix can be substituted by the equivalent, but smaller matrix.

Theorem 1. *Let i be arbitrary fixed integer, $1 \leqq i \leqq n$, and let the columns of the parity-check matrix $\mathsf{H}^{(i)}$ with the indices from the set $I = \{i_1, i_2, \ldots, i_l\}$ are equal, where $1 \leqq i_1 < i_2 < \ldots < i_l \leqq n$, $l \geqq 2$, and $i \notin I$. Denote by J the complementary set $J = \{1, 2, \ldots, n\} \setminus I = \{j_1, j_2, \ldots, j_{n-l}\}$, $1 \leqq j_1 < j_2 < \ldots < j_{n-l} \leqq n$. Let the binary random vector $\mathsf{E}' = [E'_1 \ldots E'_{n-l} E'_{n-l+1}]^T$ be defined by*

$$E'_s = E_{j_s}, \quad 1 \leqq s \leqq n-l,$$

$$(4) \qquad E'_{n-l+1} = E_{i_1} \oplus E_{i_2} \oplus \ldots \oplus E_{i_l}.$$

In the similar way, let the vector $\mathsf{y}' = [y'_1 \ldots y'_{n-l} y'_{n-l+1}]^T$ be defined by

$$y'_s = y_{j_s}, \quad 1 \leqq s \leqq n \leqq n-l,$$

$$y'_{n-l+1} = y_{i_1} \oplus y_{i_2} \oplus \ldots \oplus y_{i_l}.$$

Denoting by $\mathsf{H}^{(i)\prime}$ the matrix whose columns are that of the matrix $\mathsf{H}^{(i)}$ with the indices $\{j_1, j_2, \ldots, j_{n-l}\}$ and i_1 in this order, APPE P_i can be expressed by the equation

$$(5) \qquad P_i = \frac{P(\{E_i = 1\} \mid \{\mathsf{H}^{(i)\prime}\mathsf{E}' = \mathsf{H}^{(i)\prime}\mathsf{y}'\})}{P\{\mathsf{H}^{(i)\prime}\mathsf{E}' = \mathsf{H}^{(i)\prime}\mathsf{y}'\}}.$$

Proof. Equality (5) follows from the obvious equalities $\mathsf{H}^{(i)}\mathsf{E} = \mathsf{H}^{(i)\prime}\mathsf{E}'$ and $\mathsf{H}^{(i)}\mathsf{y} = \mathsf{H}^{(i)\prime}\mathsf{y}'$ (they are the consequence of the assumption that the columns of the matrix $\mathsf{H}^{(i)}$ with the indices from the set I are equal).□

Observe that the equation (5) is analogous to (1), with $\mathsf{H}^{(i)}$, E, and y substituted respectively by $\mathsf{H}^{(i)\prime}$, E' and y'.

Equivalent probabilities of error are given by the known equality

$$(6) \qquad P\{E'_{n-l+1} = 1\} = \frac{1}{2} - \frac{1}{2} \prod_{s=1}^{l} (1 - 2p_{i_s})$$

(see for example [1, Theorem 1]). Applying Theorem 1, the number of multiplications needed to compute the APPE can be reduced to $n'_i 2^{n'_i - r_i}$, where n'_i is the number of columns in the matrix formed from the matrix $\mathsf{H}^{(i)}$ by deleting all zero- and redundant (repeated) columns. A small number of multiplications needed to compute the equivalent probabilities of error by (6) is neglected. Theorem 1 is a generalization of the statement used in [1], which claims that the redundant columns with exactly one "1" can be deleted from the parity check matrix. In the special case when the matrix $\mathsf{H}^{(i)}$ defines the set of orthogonal parity checks, i. e. when all the columns except the i-th contain exactly one "1", we have $n_i=1+r_i$, and so the number of multiplications needed in (5) is only $2(1+r_i)$. This is a known result, see for example [3].

To achieve more efficient decoding algorithm it is necessary for the number r_i of the independent parity checks (given by the matrix $\mathsf{H}^{(i)}$, $1\leqq i\leqq n$) to be as large as possible. But in that case it is possible (by the use of Theorem 1) to compute the APPE only if the matrices $\mathsf{H}^{(i)}$ have large number of zero- or redundant columns. For every group of redundant columns it is necessary to apply once the equality (6). During the calculation of the sequence of the APPE-vectors, the following problem arises: APPE usually gets close to 0 or 1, and thus it lowers the exactness of the computation. For small value of max $\{p_{i_s}\,|\,1\leqq s\leqq l\}$, it is impossible to compute the probability $P\{E'_{n-l+1}=1\}$ directly by the equation (6). In the following section the method to solve this problem will be given.

2. On the exactness of computing of the APPE

To solve the problem of computing with the probabilities which are very close to 0 or 1, it is useful to transform the probabilities p_i and P_i into the corresponding algebraic values a_i and A_i, given by

$$a_i=\ln\frac{1-p_i}{p_i},\quad A_i=\ln\frac{1-P_i}{P_i},\quad 0<p_i,\ P_i<1,\quad 1\leqq i\leqq n.$$

These transformations are usually used to simplify the expressions like (6) (see for example [3]). Here it will be shown how the a posteriori algebraic values A_i can be computed in the case when some of the probabilities p_i are very close to 0, and therefore they cannot be computed by the use of computers in the standard precision. Probabilities which are close to 1 are transformed according to the note from the beginning of the previous section.

Writing the equality (3) as

$$P_i=\left(1+\frac{\Sigma_{\mathbf{e}\in C^0_{i,\mathbf{y}}}\exp\left(-\Sigma_{j=1}^{n} l_j a_j\right)}{\Sigma_{\mathbf{e}\in C^1_{i,\mathbf{y}}}\exp\left(-\Sigma_{j=1}^{n} l_j a_j\right)}\right)^{-1},\ 1\leqq i\leqq n,$$

we get

$$A_i=\ln\frac{\Sigma_{\mathbf{e}\in C^0_{i,\mathbf{y}}}\exp\left(-\Sigma_{j=1}^{n} l_j a_j\right)}{\Sigma_{\mathbf{e}\in C^1_{i,\mathbf{y}}}\exp\left(-\Sigma_{j=1}^{n} l_j a_j\right)},1\leqq i\leqq n.$$

Here the outer sums are computed dividing all the summands by the greatest among them. Let us denote the algebraic value corresponding to $P\{E'_{n-l+1}=1\}$

(see (4) and (6)) by A'_{n-l+1}. If we suppose that $\max\{p_{i_s} \mid 1 \leqq s \leqq l\} < 1/2$, i.e. $\min\{a_{i_s} \mid 1 \leqq s \leqq l\} > 0$, then the equation (6) can be written as

$$A'_{n-l+1} = \ln \frac{1 + \Pi_{s=1}^{l}(1-2p_{i_s})}{1 - \Pi_{s=1}^{l}(1-2p_{i_s})}$$

$$= \ln \frac{\Pi_{s=1}^{l}(1-p_{i_s}+p_{i_s}) + \Pi_{s=1}^{l}(1-p_{i_s}-p_{i_s})}{\Pi_{s=1}^{l}(1-p_{i_s}+p_{i_s}) - \Pi_{s=1}^{l}(1-p_{i_s}-p_{i_s})}$$

$$(7) \qquad = \ln \frac{\Pi_{s=1}^{l}(e^{a_{i_s}}+1) + \Pi_{s=1}^{l}(e^{a_{i_s}}-1)}{\Pi_{s=1}^{l}(e^{a_{i_s}}+1) - \Pi_{s=1}^{l}(e^{a_{i_s}}-1)} = f\left(\sum_{s=1}^{l} f(a_{i_s})\right),$$

where $f\colon (0, +\infty) \to (0, +\infty)$ is the function defined by the equality [1]

$$(8) \qquad f(z) = \ln \frac{e^z+1}{e^z-1}, \quad z > 0.$$

In the case when $\max\{p_{i_s} \mid 1 \leqq s \leqq l\} = 1/2$, i.e. $\min\{a_{i_s} \mid 1 \leqq s \leqq l\} = 0$, it is natural to take $A'_{n-l+1} = 0$, because $P\{E'_{n-l+1} = 1\} = 1/2$.

Values of the function $f(z)$ for large z cannot be computed by the use of computers in the standard precision because the argument of ln cannot be distinguished from 1. Similarly, for the values of z close to zero $f(z)$ cannot be computed because the number $e^z - 1$ is rounded to zero, by reason of the limitations for the number of bits for the mantissa of real numbers. However the function $\hat{f}(z)$ which is defined in Theorem 2 can be computed for z close to zero and large z, and it is a good approximation of the function $f(z)$. The argument of the outer f in (7) is computed dividing all the summands by $\exp(-\max\{a_{i_s} \mid 1 \leqq s \leqq l\})$. Let ρ denote the relative rounding error for real numbers caused by their representation in the computer. One can take $2^{-56} \simeq 1.39 \times 10^{-17}$ as the typical value for ρ.

Theorem 2. *Let the relative rounding error ρ satisfies the condition $\rho \leqq 2^{-56}$. Define the function $\hat{f}(z)$, $z > 0$ by the following equation*

$$(9) \qquad \hat{f}(z) = \begin{cases} 2e^{-z}, & z_0 \leqq z < +\infty \\ 2e^{-z} + \frac{2}{3}e^{-3z}, & z_1 \leqq z < z_0 \\ \ln \frac{e^z+1}{e^z-1}, & z_2 \leqq z < z_1 \\ \ln \frac{2}{z} + \frac{1}{12}z^2, & z_3 \leqq z < z_2 \\ \ln \frac{2}{z}, & 0 < z < z_3 \end{cases}$$

where $z_0 = \frac{1}{3}\ln\frac{c}{10\rho}$, $z_1 = \frac{1}{5}\ln\frac{3c}{25\rho}$, $z_2 = (48\rho)^{1/3}$, $z_3 = 6\rho$ *and* $c = \frac{2}{3(1-e^{-2})} \simeq 0.771$. *Then*

$$(10)\qquad \frac{1}{z}\,|f(z)-\hat{f}(z)|<\rho.$$

Proof. Let us consider first the case $z>z_0=\frac{1}{3}\ln\frac{c}{10\rho}>12.1$. Using the Taylor expansion

$$(11)\qquad \ln\frac{1+w}{1-w}=2\sum_{k=1}^{\infty}\frac{1}{2k-1}w^{2k-1},\ w<1,$$

we get the inequalities

$$2w\leqq\ln\frac{1+w}{1-w}<2w+\frac{2}{3}\sum_{k=2}^{\infty}w^{2k-1}=2w+\frac{2}{3}\frac{w^3}{1-w^2}$$

$$<2w+\frac{2}{3(1-e^{-2})}w^3=2w+cw^3.$$

Substituting here w by $e^{-z}<1$, we get

$$\frac{1}{z}|\ln\frac{e^z+1}{e^z-1}-2e^{-z}|<\frac{c}{z}e^{-3z}<\frac{c}{10}e^{-3z}<\rho,\ z>z_0,$$

which proves (10) in the case $z>z_0$. In the analogous way, taking the two first members of the expansion (11), we get the inequalities

$$2w+\frac{2}{3}w^3\leqq\ln\frac{1+w}{1-w}\leqq 2w+\frac{2}{3}w^3+\frac{3}{5}cw^5,$$

and consequently, for $z>z_1$ we have

$$\frac{1}{z}\left|\ln\frac{e^z+1}{e^z-1}-2e^{-z}-\frac{2}{3}e^{-3z}\right|<\frac{3}{5}\frac{c}{z}e^{-5z}<\frac{3c}{25}e^{-5z}<\rho.$$

This ends the proof of (10) for the case $z_1\leqq z<z_0$.

The case when z is small, $z<z_2$, is more complicated. Consider the following Taylor expansion of the function $\varphi(z)=f(z)-\ln(\frac{2}{z})$,

$$(12)\qquad \varphi(z)=\ln\frac{e^z+1}{e^z-1}\frac{z}{2}=\frac{z^2}{12}+\frac{\varphi^{\mathrm{IV}}(\theta z)}{4!}z^4,\ 0<\theta<1.$$

We will find the lower and upper bound for $\varphi^{\mathrm{IV}}(z)$ when $0<z<0.01$. These will be also the bounds for $\varphi^{\mathrm{IV}}(\theta z)$, because $0<z<0.01$ implies $0<\theta z<0.01$ Expression for $f(z)$ can be written as

$$(13)\qquad \varphi(z)=\varphi_1(z)+\varphi_2(z),$$

where

$$\varphi_1(z)=\ln\frac{e^z+1}{2},$$

and

$$\varphi_2(z)=\ln\frac{z}{e^z-1}.$$

The fourth derivative of the function $\varphi_1(z)$ is

$$\varphi_1^{\mathrm{IV}}(z)=\frac{1}{1+e^{-z}}-\frac{7}{(1+e^{-z})^2}+\frac{12}{(1+e^{-z})^3}-\frac{6}{(1+e^{-z})^4}.$$

Starting from the inequality

$$\frac{1}{2}\leqq\frac{1}{1+e^{-z}}<\frac{1}{1+e^{-0.01}}=c'\simeq 0.5025$$

the following bounds for $\varphi_1(z)$ are obvious

$$-0.150<2-7c'^2-6c'^4<\varphi_1^{\mathrm{IV}}(z)<c'+12c'^3-\frac{17}{8}<-0.0999,$$

and consequently

$$(14)\qquad |\varphi_1^{\mathrm{IV}}(z)|<0.2,\ 0<z<0.01.$$

The fourth derivative $\varphi_2^{\mathrm{IV}}(z)$ can be written as

$$(15)\qquad \varphi_2^{\mathrm{IV}}(z)=\varphi_3(t)\left(\frac{t}{z}\right)^4,$$

where $t=1-e^{-z}$ and

$$(16)\qquad \varphi_3(t)=\frac{(\ln(1-t))^4(6-12t+7t^2-t^3)-6t^4}{t^8}.$$

Variable t for $0<z\leqq z_2$ obviously satisfies the inequalities $0\leqq t<1-e^{-0.01}<0.01$. To estimate $|\varphi_3(t)|$, we need the Taylor expansion

$$-\ln(1-t)=t+\frac{t^2}{2}+\frac{t^3}{3}+\frac{t^4}{4}+\frac{U}{5}t^5,$$

where $U=(1-\theta_1 t)^{-5}$, $0<\theta_1<1$, and $1\leqq U<(1-t)^{-5}=e^{5z}<e^{0.05}\simeq 1.0513$. Substituting this in (16), we get the expression for $\varphi_3(t)$ in terms of t and U,

$$
\begin{aligned}
\varphi_3(t) = & -\frac{115}{24}+\frac{24}{5}U \\
& +t\left(-\frac{19}{12}-\frac{12}{5}U\right) \\
& +t^2\left(-\frac{145}{144}-\frac{2}{5}U\right) \\
& +t^3\left(-\frac{35}{48}-\frac{1}{5}U\right) \\
& +t^4\left(\frac{125}{144}-3U+\frac{36}{25}U^2\right) \\
& +t^5\left(\frac{35}{72}+\frac{2}{5}U-\frac{36}{25}U^2\right) \\
& +t^6\left(\frac{959}{2592}+\frac{2}{45}U+\frac{3}{25}U^2\right) \\
& +t^7\left(\frac{775}{2592}+\frac{1}{90}U\right) \\
& +t^8\left(\frac{205}{3456}+\frac{31}{54}U-\frac{29}{50}U^2+\frac{24}{125}U^3\right) \\
& +t^9\left(\frac{5}{192}+\frac{47}{540}U+\frac{19}{50}U^2-\frac{36}{125}U^3\right) \\
& +t^{10}\left(\frac{5}{768}+\frac{7}{120}U+\frac{1}{60}U^2+\frac{12}{125}U^3\right) \\
& +t^{11}\left(-\frac{1}{256}+\frac{3}{80}U+\frac{1}{75}U^2\right) \\
& +t^{12}\left(-\frac{1}{80}U+\frac{13}{200}U^2-\frac{14}{375}U^3+\frac{6}{625}U^4\right) \\
& +t^{13}\left(-\frac{3}{200}U^2+\frac{17}{375}U^3-\frac{12}{625}U^4\right) \\
& +t^{14}\left(-\frac{1}{125}U^3-\frac{7}{625}U^4\right) \\
& +t^{15}\left(-\frac{1}{625}U^4\right).
\end{aligned}
$$

The absolute values of the coefficients of t^2, $t^3, \ldots,$ t^{15} in this expansion are obviously smaller than 15 for $0<z<0.01$. This fact allows us to estimate the upper bound for $|\varphi_3(t)|$:

$$|\varphi_3(t)|\leqq\left|-\frac{115}{24}+\frac{24}{5}e^{0.05}\right|+t\left(\frac{19}{12}+\frac{12}{5}e^{0.05}\right)+15(t^2+\ldots+t^{15})$$

$$\leqq 0.255+4.16t+15t^2\frac{1-t^{14}}{1-t}$$

$$\leqq 0.255+0.0416+30t^2<0.3.$$

Using this inequality, (15), and the inequality $t<z$, we conclude that $|\varphi_2^{\mathrm{IV}}(z)|<0.3$ for $0<z<0.01$, and finally, from (13) and (14),

$$|\varphi^{\mathrm{IV}}(z)|<0.5,\ 0<z<0.01.$$

Consider now the case $0<z<z_2=(48\rho)^{1/3}$. We have, see (12),

$$\frac{1}{z}\left|\ln\frac{e^z+1}{e^z-1}-\ln\frac{2}{z}-\frac{z^2}{12}\right|=\left|\varphi^{IV}(\theta z)\frac{z^3}{24}\right|<\frac{z^3}{48}<\rho.$$

Finally, for $0<z<z_3$, the following inequality can be derived

$$\frac{1}{z}\left|\ln\frac{e^z+1}{e^z-1}-\ln\frac{2}{z}\right|=\left|\frac{z}{12}+\varphi^{IV}(\theta z)\frac{z^3}{24}\right|\leqq\frac{z}{12}+\frac{z^3}{48}<\frac{z}{6}<\rho.$$

This completes the proof of Theorem 2. □

In determining the expansion of $\varphi_3(t)$ we used symbolic programming language "MUSIMP". For $\rho=2^{-56}$ parameters in (9) we have the following values: $z_0\simeq 12.1$, $z_1\simeq 7.29$, $z_2\simeq 8.733\times10^{-6}$ and $z_3\simeq 8.33\times10^{-17}$.

3. An example

The following example illustrates the use of $\hat{f}(z)$.

Consider the linear (192, 13) code defined by the following set of parity check equations

$$x_i\oplus x_{i+1}\oplus x_{i+4}\oplus x_{i+6}\oplus x_{i+13}=0,\ 1\leqq i\leqq 179,$$

where x is an arbitrary codeword. Starting from these relations the parity check matrix H can easily be written. Suppose that the received message is the vector

$$\begin{aligned}\mathsf{y}=[\ &11000110100101110000001010001111011111100\\&010110001001101111111111000000000100001111\\&0100110111001010010101011100111000001000\\&10010100110011100001100000001100110111111\\&000011011110110011010000101100111\,]^T.\end{aligned}$$

Table 1. Description of the structure of the parity check matrices $\mathrm{H}^{(i)}$, $1 \leqq i \leqq n$ in the example

	parity check	bounds for i lower	 upper
1	$x_i \oplus x_{i+1} \oplus x_{i+4} \oplus x_{i+6} \oplus x_{i+13} = 0$	1	179
2	$x_i \oplus x_{i+2} \oplus x_{i+8} \oplus x_{i+12} \oplus x_{i+26} = 0$	1	166
3	$x_{i-1} \oplus x_i \oplus x_{i+3} \oplus x_{i+5} \oplus x_{i+12} = 0$	2	180
4	$x_{i-2} \oplus x_i \oplus x_{i+6} \oplus x_{i+10} \oplus x_{i+24} = 0$	3	168
5	$x_{i-4} \oplus x_{i-3} \oplus x_i \oplus x_{i+2} \oplus x_{i+9} = 0$	5	183
6	$x_{i-8} \oplus x_{i-6} \oplus x_i \oplus x_{i+4} \oplus x_{i+18} = 0$	9	174
7	$x_{i-6} \oplus x_{i-5} \oplus x_{i-2} \oplus x_i \oplus x_{i+7} = 0$	7	185
8	$x_{i-12} \oplus x_{i-10} \oplus x_{i-4} \oplus x_i \oplus x_{i+14} = 0$	13	178
9	$x_{i-13} \oplus x_{i-12} \oplus x_{i-9} \oplus x_{i-7} \oplus x_i = 0$	14	192
10	$x_{i-26} \oplus x_{i-24} \oplus x_{i-18} \oplus x_{i-14} \oplus x_i = 0$	27	192

Coordinates of all codewords satisfy also the following family of parity check relation

$$x_i \oplus x_{i+2} \oplus x_{i+8} \oplus x_{i+12} \oplus x_{i+26} = 0; \quad 1 \leqq i \leqq 166.$$

One of the possible set of parity check matrices $\mathrm{H}^{(i)}$, $1 \leqq i \leqq n = 192$ can be described by the Table 1 (the similar construction was used in [4]). For every i, $1 \leqq i \leqq n$, the matrix $\mathrm{H}^{(i)}$ is formed from the parity check relations (second column of the Table 1) for which the respective integer segment (with boundaries given in third and fourth columns) contains i.

In the Table 2 there were listed parameters connected with the matrices $\mathrm{H}^{(i)}$: the number of rows r_i, the number of non-zero columns n_i, the number of non-zero columns after the application of Theorem 1, n'_i, and the numbers $k_i = n_i - r_i$, $k'_i = n'_i - r_i$, $1 \leqq i \leqq n$. It can be seen that the size of the matrix $\mathrm{H}^{(i)\prime}$ is significantly smaller than the size of the matrix $\mathrm{H}^{(i)}$, for the most values of i. Still, this fact does not improve considerably the efficiency of the computation, because $r_i \simeq k'_i$.

The information sets were formed from the set of 40 coordinates with the lowest values of $\min\{P_i^{(8)}, 1 - P_i^{(8)}\}$, $1 \leqq i \leqq n$. Using Theorem 2 and doing the calculations with the algebraic values, the following set of 40 coordinates was obtained

$$\{155, 165, 161, 159, 153, 167, 160, 156, 162, 157,$$
$$166, 164, 168, 163, 154, 158, 169, 105, 152, 172,$$
$$171, 170, 117, 149, 174, 148, 150, 143, 173, 146,$$
$$93, 75, 176, 151, 142, 89, 91, 79, 77, 81\}.$$

Table 2. Parameters connected with matrices $H^{(i)}$

	lower	upper					
	limit for i		r_i	n_i	k_i	n'_i	k'_i
1	1	1	2	9	7	3	1
2	2	2	3	12	9	5	2
3	3	4	4	15	11	7	3
4	5	6	5	18	13	9	4
5	7	8	6	21	15	11	5
6	9	12	7	23	16	14	7
7	13	13	8	26	18	16	8
8	14	26	9	29	20	18	9
9	27	166	10	33	23	19	9
10	167	168	9	31	22	16	7
11	169	174	8	29	21	13	5
12	175	178	7	27	20	10	3
13	179	179	6	25	19	7	1
14	180	180	5	21	16	6	1
15	181	183	4	17	13	5	1
16	184	185	3	13	10	4	1
17	186	192	2	9	7	3	1

Comparing the corresponding coordinates in the vectors x

$$\mathsf{x}=[\,\begin{array}{l}0001011010001111100001000100111011011100\\0100110110011011010011100101010100010111\\0101110011011000111101101101111000001000\\0000010011001011100110000001100101111111\\00011101101111001001000101000111\end{array}\,]^{T}$$

and $\bar{\mathsf{y}}$ (formed using the vector $\mathsf{P}^{(8)}$, see (2)), it can be seen that there is only one error in $\bar{\mathsf{y}}$ among these 40 coordinates.

Corresponding set of 40 coordinates formed without using Theorem 2 is

$$\{\,1,\ 2,\ 4,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 20,\ 21,\ 22,\ 23,\ 24,\ 25,\ 26,\ 27,\ 28,\ 29,\ 30,\ 32,\ 33,\ 34,\ 36,\ 37,\ 38,\ 39,\ 41,\ 42,\ 43,\ 44,\ 45,\ 46,\ 47\,\}$$

In this case there are even 17 errors in these coordinates of the vector $\bar{\mathsf{y}}$. The difference between these two cases can also be illustrated by the following experiment. After each iteration j, $j=1, 2, \ldots, 10$ (computation of the vector $\mathsf{P}^{(j)}$, i.e. $\mathsf{A}^{(j)}$) there were formed 10 random information sets starting from the 40 most reliable coordinates. The number of the information sets without errors (i.e. the number of successful decodings) was respectively 4, 6, 0, 0, 1, 2, 4, 10, 10, 10 for the improved method, and 4, 6, 0, 0, 0, 0, 0, 0, 0, 0 for the usual method of computing the APPE.

Acknowledgement

The author wishes to express his gratitude to professor Ž. Mijajlović for the useful remarks.

References

1. R. G. Gallager. Low-Density Parity-Check Codes. *IEEE Trans. on Inform. Theory*, **IT-8**, 1962, 21-28.
2. G. C. Clark, Jr., J. B. Cain. Error-Correction Coding for Digital Communications. New York, Plenum Press, 1982.
3. G. Battail, M. C. Decouvelaere, P. Godlewski. Replication Decoding. *IEEE Trans. Inform. Theory*, **IT-25**, 1979, 332-345.
4. W. Meier, O. Staffelbach. Fast Correlation Attacks on Stream Ciphers. – In: *Advances in Cryptology, Eurocrypt'*88, C. G. Günter, Ed., Berlin, 1988, 300-314.
5. C. R. P. Hartmann, L. D. Rudolph. An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes. *IEEE Trans. Inform. Theory*, **IT-22**, 1976, 514-517.

Paunova 61/16
11000 Beograd
JUGOSLAVIA

Received 10.07.1989