

2-Stripes Block-Circulant LDPC Codes for Single Bursts Correction

Evgenii Krouk and Andrei Ovchinnikov

Abstract In this paper the low-density parity-check (LDPC) codes are considered applied to correction of error bursts. Errors grouping and forming of so-called bursts are typical effect in real communication and data storage systems, however, this effect is typically ignored, and the coding task is reduced to correction of independent errors, which makes the practical characteristics of coding systems worse comparing to possibly reachable. Nevertheless, LDPC codes are able to protect from burst errors as well as independent ones. The main result of the paper is dedicated to evaluation of maximum correctable burst length of Gilbert codes, which are the 2-stripes special case of LDPC block-permutation codes, the construction which is often used in modern practical applications and research.

Keywords LDPC codes · Bursts-correcting codes · Gilbert codes

1 Introduction

During the development of modern practical communication systems the channel models which are commonly used (binary-symmetric channel or Gaussian channel) are often inadequate since they consider independent errors. At the same time in real communication channels the effect of “memory” occurs (for example due to fading [1]) leading to the dependencies between erroneous symbols. To fight with such errors grouping the interleaving procedure is often used [1].

However, usage of interleaver leads to typical channel behaviour loss, the channel is transformed to memoryless, this decreases the possible transmission rates, and increases the complexity and delay of transmitter and receiver [2, 3]. This is

E. Krouk · A. Ovchinnikov (✉)
Saint-Petersburg State University of Aerospace Instrumentation,
B.Morskaya 67, 190000 Saint Petersburg, Russia
e-mail: mldoc@ieee.org

E. Krouk
e-mail: ekrouk@vu.spb.ru

because the classical coding theory usually proposes code constructions for independent errors which are simpler to analyse. So the important task is to construct coding schemes oriented on typical channel errors, in particular, on correcting the error bursts, that is, the error patterns when first and last erroneous symbols are no far than some value b from each other (and which is called the burst length). Besides, the effect of errors grouping is typical for data storage systems.

In the coding theory the classes of burst-correcting codes are known. For example, these are Fire codes or Reed-Solomon codes [4]. During the last decades a lot attention was given to low-density parity-check (LDPC) codes, particularly block-permutation constructions [5]. Gilbert codes which are considered in this paper are the simple special case of such construction and were proposed initially for burst-correction. However, the exact burst-correction capability of these codes was unknown.

The paper is organized as follows. Section 2 describes Gilbert codes and known estimations of its burst-correction capability. In Sect. 3 the procedure is derived allowing computation of exact value of maximum correctable burst length. The Sect. 4 concludes the paper.

2 Gilbert Codes

LDPC-codes were invented by Gallager [6, 7] and later investigated in many works [8–11]. While possessing comparatively poor minimal distance, these codes, however, provide high error-correction capability with very low decoding complexity. It was shown that LDPC codes may overcome turbo-codes and approach to channel capacity [12]. Additionally, some LDPC constructions (and block-permutation constructions as well) are cyclic or quasi-cyclic, allowing effective coder and decoder implementation.

Block-permutation codes are one of the most prominent and widely used class of LDPC codes [3, 5, 13]. The simple special case of this class are Gilbert codes, which were proposed in [14] as burst-correction codes. Gilbert codes may be defined by the parity-check matrix H_ℓ ,

$$H_\ell = \begin{bmatrix} I_m & I_m & I_m & \dots & I_m \\ I_m & C & C^2 & \dots & C^{\ell-1} \end{bmatrix}, \quad (1)$$

where I_m is $(m \times m)$ -unity matrix, C is $(m \times m)$ -matrix of cyclic permutation:

$$C = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}, \quad (2)$$

and $\ell \leq m$.

Many works were dedicated to estimation of burst-correcting capability of these codes, as well as their modifications and extensions [15–19]. In [20] the estimation of maximum correctable burst length b for the codes defined by matrix (1) is given by inequality

$$b \leq \min_{\gamma \in \{0, \ell-2\}} \max\{\gamma - 1, m - \gamma - 1\}. \quad (3)$$

However, estimation (3) is not correct, giving only the lower bound of the maximum correctable burst length. The exactness of this estimation decreases with growth of ℓ .

In the next section we will give the method of exact evaluation of b .

3 Burst-Correction Capability of Gilbert Codes

The main result of this section and paper is the following theorem.

Theorem 1 *Code with parity-check matrix H_ℓ defined by (1) can correct single bursts of maximal length b_ℓ , where b_ℓ is calculated by the first satisfied condition:*

1. $b_3 = m - 1$, m is odd.
2. If $\ell > \lceil m/2 \rceil + 1$, then

$$\begin{cases} b_\ell = m - \lceil m/2 \rceil + 1, & m \text{ odd,} \\ b_\ell = m/2 - 1, & m \text{ even.} \end{cases}$$

3. If $\ell \leq \lceil m/2 \rceil + 1$, then

$$\begin{aligned} b_\ell &= m - \ell + 1, & \text{if } m \div (\ell - 1), \\ b_\ell &= m - \ell + 1, & \text{if } \exists k > 0 : (m - \ell + 3 - k \cdot (\ell - 1)) \div (\ell - 2), \\ b_\ell &= m - \ell + 2, & \text{if } \exists k > 0 : (m - k \cdot (\ell - 3)) \div (\ell - 2), \\ b_\ell &= m - \ell + 2, & \text{if } \exists k > 0 : (m - k \cdot (\ell - 2)) \div (\ell - 1), \\ b_\ell &= m - \ell + 2, & \text{if } \exists k > 0 : (m - k \cdot (\ell - 1)) \div (\ell - 2). \end{aligned}$$

4. If all preceding conditions are unsatisfied, then:

$$b_\ell = b_{\ell-1}.$$

Proof To prove the statement of the theorem we will introduce some notations and prove some lemmas. Represent the matrix (1) as $H_\ell = [h_0, h_1, \dots, h_{\ell-1}]$, where h_γ — $(2m \times m)$ -block-column, which we will call as block.

The code can correct single error burst of length b , if and only if all packets of length b are in different cosets, i.e. there are no two error vectors e_1 and e_2 (forming the bursts of length no more than b), such that

$$e_1 \cdot H_\ell^T = e_2 \cdot H_\ell^T. \quad (4)$$

Since e_1 and e_2 are error bursts, the analysis of (4) may be reduced to consideration of submatrices of H_ℓ consisting of $2m$ rows and no more than b columns.

Clearly, code with parity-check matrix (1) cannot correct bursts of length m , since the sum of all m columns from any block of H_ℓ gives all-one column.

Each burst B of length $b < m$ affects no more than two adjacent blocks from H_ℓ , let these blocks be γ and $\gamma + 1$. Let us replace in h_γ and $h_{\gamma+1}$ all columns with numbers not from B by zeros and sum obtained matrices h'_γ and $h'_{\gamma+1}$, obtaining

$$Q(B) = (h'_\gamma + h'_{\gamma+1})^T. \quad (5)$$

This matrix has the form

$$Q^T(B) = \left[\begin{array}{cccc|cc|ccc} & & & & i & i+1 & & & & \\ & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \\ & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & \\ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & \\ \hline i & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \\ & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & \\ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & \\ \hline & & & & \tilde{C}^{\gamma+1} & & & & \tilde{C}^\gamma & \\ & & & & \dots & & & & \dots & \\ & & & & 0 & & & & 0 & \end{array} \right], \quad (6)$$

where \tilde{C}^γ and $\tilde{C}^{\gamma+1}$ are parts of matrices C^γ and $C^{\gamma+1}$, and $i + 1$ is the beginning position modulo m of burst B , which we will call as relative beginning of B .

From (4) and (5) it follows that the code with parity-check matrix H_ℓ cannot correct bursts of length $b < m$ if and only if for at least one pair of bursts B_1 and B_2 (of length b) there exists the pair of vectors \bar{x}_1 and \bar{x}_2 of length m such that

$$\bar{x}_1 \cdot Q(B_1) = \bar{x}_2 \cdot Q(B_2). \quad (7)$$

For any burst B the matrix $Q(B)$ may be represented as

$$Q(B) = [Q_1(B), Q_2(B)],$$

where $Q_1(B)$ is $(m \times m)$ -unity matrix with i th row replaced by zeros.

Then the condition (7) may be written as

$$\bar{x}_1 \cdot Q_1(B_1) = \bar{x}_2 \cdot Q_1(B_2), \quad (8)$$

$$\bar{x}_1 \cdot Q_2(B_1) = \bar{x}_2 \cdot Q_2(B_2). \quad (9)$$

Removing the zero row in $Q_1(B)$, we obtain $((m-1) \times (2m))$ -matrix $Q'(B) = [Q'_1(B), Q'_2(B)]$.

Denote as $(\bar{y} \setminus s)$ the vector of length $m-1$ obtained from \bar{y} (of length m) by removing s th position (with correspondent shift of remained digits by one position to the right). Then the following lemma may be formulated.

Lemma 1 *The condition (7) is satisfied if and only if the vector \bar{y} of length m exists such that*

$$\begin{cases} (\bar{y} \setminus i) \cdot Q'_2(B_1) = (\bar{y} \setminus j) \cdot Q'_2(B_2), \\ y_i = y_j = 0. \end{cases} \quad (10)$$

where $i+1, j+1$ are relative beginnings of bursts B_1 and B_2 correspondingly.

Proof Consider the expression (8). Matrices $Q_1(B_1)$ and $Q_1(B_2)$ are unity $(m \times m)$ -matrices with i th and j th zero rows correspondingly. This means that multiplication of \bar{x}_1 by $Q_1(B_1)$ gives the vector \bar{x}_1 with i th position equal to zero. From (8) it follows that \bar{x}_1 and \bar{x}_2 are coincide and contain zeros on positions i and j . That is, the vector $\bar{y} = \bar{x}_1 = \bar{x}_2$ may always be defined with $y_i = y_j = 0$.

Rewrite (8) and (9) as

$$\begin{cases} (\bar{y} \setminus i) \cdot Q'_1(B_1) = (\bar{y} \setminus j) \cdot Q'_1(B_2) \\ (\bar{y} \setminus i) \cdot Q'_2(B_1) = (\bar{y} \setminus j) \cdot Q'_2(B_2) \end{cases}$$

Evidently, first equation is satisfied for any \bar{y} , if $y_i = y_j = 0$, this gives the lemma's statement.

Lemma 2 *For any burst B :*

$$Q'_2(B) = [I_{m-1}, \bar{0}] \cdot C^\gamma, \quad (11)$$

where I_{m-1} is unity $((m-1) \times (m-1))$ -matrix, $\bar{0}$ is zero vector-column of length $m-1$ and γ is integer between 0 and $\ell-1$.

Proof To prove the lemma it is enough to show that for any burst B the correspondent matrix $Q'_2(B)$ is circulant $((m-1) \times m)$ -matrix.

Let B is burst of length $m-1$ containing $s \geq 0$ last columns of block h_i and $m-s-1$ first columns of block h_{i+1} . Then $Q'_2(B) = [q_1(B), q_2(B)]^T$, where $q_1(B)$ is the matrix from first $m-s-1$ columns of C^i and $q_2(B)$ is the matrix from last s columns of C^{i-1} . Matrices $q_1(B)$ and $q_2(B)$ are circulant by construction and we need to show that $(m-s-1)$ th column of C^{i-1} (i.e. first column of $q_1(B)$) is cyclic shift of the $(m-s-1)$ th column of C^i (i.e. the last column of $q_2(B)$) to conclude the proof. This follows from the fact that $(m-s)$ th column of C^{i-1} is equal to $(m-s-1)$ th column of C^i .

From Lemmas 1, 2 and condition (7) it follows that two bursts of length $b < m$ have the same syndrome if and only if there exists \bar{y} of length m , such that for some integer γ the following condition holds:

$$\begin{cases} (\bar{y}\setminus i, 0) = (\bar{y}\setminus j, 0) \cdot C^\gamma, \\ y_i = y_j = 0, \end{cases} \quad (12)$$

where $(\bar{y}\setminus i, 0)$ is vector of length m obtained by adding zero position to $(\bar{y}\setminus i)$.

Let us put in correspondence to vector \bar{y} the polynomial $y(x) = \sum_{k=0}^{m-1} y_k x^k$. Then (12) in polynomial representation will be

$$\begin{cases} (y(x)\setminus i) = (y(x)\setminus j) \cdot x^\gamma \pmod{x^m - 1}, \\ y_i = y_j = 0 \end{cases} \quad (13)$$

(coefficients of $(y(x)\setminus i)$ and $(y(x)\setminus j)$ are defined by vectors $(\bar{y}\setminus i, 0)$ and $(\bar{y}\setminus j, 0)$ correspondingly).

Lemma 3 *If $y(x) = \sum_{k=0}^{m-1} y_k x^k$ —polynomial, satisfying (13), then for any non-zero y_k one of the following holds:*

$$y_k = y_{(k-\gamma) \bmod m}, \quad y_k = y_{(k-\gamma+1) \bmod m}, \quad y_k = y_{(k-\gamma-1) \bmod m}.$$

Proof Polynomial $(y(x)\setminus i)$ may be represented as

$$(y(x)\setminus i) = \sum_{k=0}^{i-1} y_k x^k + \sum_{k=i}^{m-2} y_{k+1} x^k = A^i(x) + B^i(x). \quad (14)$$

Then $((y(x)\setminus j) \cdot x^\gamma) \pmod{x^m - 1}$ may be written as

$$\begin{aligned} ((y(x)\setminus j) \cdot x^\gamma) \pmod{x^m - 1} &= \left(\sum_{k=0}^{j-1} y_k x^{k+\gamma} + \sum_{k=j}^{m-2} y_{k+1} x^{k+\gamma} \right) \pmod{x^m - 1} = \\ &= (A^\gamma(x) + B^\gamma(x)) \pmod{x^m - 1}. \end{aligned} \quad (15)$$

From (13) the equality of coefficients correspondent to the same degrees of polynomials (14) and (15) is follows.

Consider the coefficients for degrees $k = \overline{0, i-1}$ (i.e. from $A^i(x)$). They are correspondent to coefficients of the same degrees either from $A^\gamma(x)$ or from $B^\gamma(x)$. However from (15) it follows that any degree k of $((y(x)\setminus j) \cdot x^\gamma) \pmod{x^m - 1}$ may be represented as $(s + \gamma) \bmod m$. Then

$$\begin{aligned} y_k \in A^i(x) = y_k \in A^\gamma(x) = y_{(k-\gamma) \bmod m}, \text{ or} \\ y_k \in A^i(x) = y_k \in B^\gamma(x) = y_{(k-\gamma+1) \bmod m}. \end{aligned} \quad (16)$$

Similarly for degrees $k = \overline{i, m-2}$

$$\begin{aligned} y_k \in B^i(x) = y_{k-1} \in A^\gamma(x) = y_{(k-\gamma) \bmod m}, \text{ or} \\ y_k \in B^i(x) = y_{k-1} \in B^\gamma(x) = y_{(k-\gamma-1) \bmod m}. \end{aligned} \quad (17)$$

From (16) and (17) we get the lemma's statement.

Corollary 1 For any $y(x)$ satisfying (13) the non-negative integers $\alpha_1, \alpha_2, \alpha_3$ exists such that

$$\alpha_1(\gamma + 1) + \alpha_2\gamma + \alpha_3(\gamma - 1) = m. \quad (18)$$

Proof Let y_k be non-zero element of \bar{y} . Then, according to Lemma 2, one of the elements $y_{(k-\gamma) \bmod m}$, $y_{(k-\gamma+1) \bmod m}$ or $y_{(k-\gamma-1) \bmod m}$ is also non-zero. Continuing these steps the non-zero y_s can be found for which one of the following statements holds:

$$y_s = y_{(s-\gamma) \bmod m} = y_k, y_s = y_{(s-\gamma+1) \bmod m} = y_k, y_s = y_{(s-\gamma-1) \bmod m} = y_k. \quad (19)$$

From this there exists such nonnegative $\alpha_1, \alpha_2, \alpha_3$ that:

$$\alpha_1(\gamma + 1) + \alpha_2\gamma + \alpha_3(\gamma - 1) = 0 \bmod m. \quad (20)$$

To prove the Corollary 1 it is enough to show that there are no other non-zero elements between two non-zero elements of \bar{y} .

If this is not true, then one of the Eqs. (19) is satisfied after more that one passing through the vector \bar{y} (in other words, the value of $k - \gamma$, $k - \gamma - 1$ or $k - \gamma + 1$ becomes negative before satisfying (19), and therefore is taken modulo m more than once). In this case the vector \bar{y} is either all-one vector and the minimal length of uncorrectable burst is m , which is impossible, or it contains zero elements. Then the γ' exists, perhaps less than γ from (20), equal to the number of positions between non-zero elements or differs from it by one, for this γ' the condition (13) also holds, and before satisfying (19) the position number is taken modulo m only once. From this the statement of Corollary 1 follows.

Corollary 1 also means that from all γ , for which (13) holds, the least non-zero value should be chosen.

Lets call as section of \bar{y} the sequence consisting of one and consequent zeros. For example, $\bar{y} = 100010000$ contains two sections of length 4 and 5.

From Corollary 1 it follows that \bar{y} is concatenation of sections of lengths $\gamma, \gamma + 1$ and $\gamma - 1$. Lemma 4 and Corollary 2 specify the locations of these sections.

Lemma 4 For vector, satisfying (13), the following holds:

$$j + \gamma - 1 \leq m - 1. \quad (21)$$

Proof Indeed, let y_{j+1} be the last non-zero element of \bar{y} (otherwise (21) evidently holds). Recall that the element y_{j+1} is always equal to one, since j is relative burst beginning. We will assume that the coefficient y_0 in $y(x)$ is always equal to one. If this is not true, the correspondent \bar{y} may be cyclically shifted, preserving all results of (13), Lemma 3 and Corollary 1. Then from Lemma 3 and Corollary 1, the following cases are possible:

$$\begin{aligned}
y_0 &= y_{m \bmod m} = y_{(m-\gamma-1) \bmod m} = y_{j+1}, \\
y_0 &= y_{m \bmod m} = y_{(m-\gamma+1) \bmod m} = y_{j+1}, \\
y_0 &= y_{m \bmod m} = y_{(m-\gamma) \bmod m} = y_{j+1},
\end{aligned}$$

from this we get $j + \gamma - 1 \leq m - 1$.

Corollary 2 *If $i \leq j + \gamma$, then in sections, forming \bar{y} , the section of length $\gamma - 1$ is either absent, or appeared exactly once and located last.*

Proof From Lemma 4 and inequality (21) the polynomial (15) may be represented as

$$\begin{aligned}
& ((y(x) \setminus j) \cdot x^\gamma) \bmod x^m - 1 = \\
&= \sum_{k=0}^{j-1} y_k x^{k+\gamma} + \sum_{k=j}^{m-\gamma-2} y_{k+1} x^{k+\gamma} + \sum_{k=m-\gamma-1}^{m-2} y_{k+1} x^{(k+\gamma) \bmod m} = \\
&= \sum_{k=0}^{\gamma-2} y_{(k-\gamma+1) \bmod m} x^k + y_j x^{\gamma-1} + \sum_{k=j+\gamma}^{m-2} y_{k-\gamma+1} x^k = \\
&= A^m(x) + y_j x^{\gamma-1} + B^m(x) + C^m(x).
\end{aligned} \tag{22}$$

As we assumed before, let $y_0 = 1$. At first we will not consider cases when relative beginning of one or both bursts coincides with the beginning of correspondent block h_γ of matrix (1), these cases will be considered separately. Then $i + 1 \geq \gamma - 1$ or $i \geq \gamma - 2$. Consider $i = \gamma - 2$ and $i = \gamma - 1$. In the first case from (14) and (22) we get $y_{i+1} = y_{-1 \bmod m} = y_{m-1}$, which is possible only if \bar{y} contains only ones. If there are no other solutions of (13), then the maximal length of correctable burst is $m - 1$. We will exclude such vectors from consideration.

In the second case, for $i = \gamma - 1$ we get $y_{i+1} = y_j$, which is impossible since the element y_{i+1} is always non-zero, while y_j is always zero. From this we get $i \geq \gamma$, i.e. degrees numbers from 0 to $\gamma - 1$ are completely belong to $A^i(x)$, and y_0 is the only non-zero coefficient from coefficients y_k from $A^m(x)$ (this follows from the fact that the minimal number of positions between non-zero elements is $\gamma - 1$, and coefficient of $x^{\gamma-1}$ is zero. Degrees higher than $\gamma - 1$ belong to $B^m(x)$ and $C^m(x)$).

Let $i \leq j + \gamma$. Then from (14) and (22), $C^m(x) \subset B^i(x)$, and the following expressions hold:

$$\begin{aligned}
y_k &= y_{(k-\gamma+1) \bmod m}, & 0 \leq k < \gamma; \\
y_k &= y_{k-\gamma}, & \gamma \leq k < i; \\
y_k &= y_{k-\gamma-1}, & i \leq k < (j + \gamma); \\
y_k &= y_{k-\gamma}, & (j + \gamma) \leq k \leq m - 2.
\end{aligned}$$

So, the expression $y_k = y_{(k-\gamma+1) \bmod m}$ may holds only for one non-zero element of \bar{y} , namely y_0 .

From this also follows that for $i < j + \gamma$ the equation $\alpha_3 = 1$ holds and the only section of length $\gamma - 1$, appeared in \bar{y} , is the last section.

Consider the special case $i = j + \gamma$. Here $C^m(x) = B^i(x)$, and the vector \bar{y} does not contain the sections of length $\gamma + 1$ at all, it has one (last) section of length $\gamma - 1$, and other sections of length γ (in other words, $\alpha_1 = 0$, $\alpha_3 = 1$).

Let us analyse the results of Lemma 3 and its corollaries. Let we have the polynomial $y(x)$, satisfying (13), and correspondent vector \bar{y} . If we denote as i^0 and j^0 the number of zero positions of \bar{y} before $(i + 1)$ and $(j + 1)$ th positions, then the length of incorrecable burst is estimated as $b = \max(m - i^0, m - j^0)$.

However, it is unknown how to solve (13) having only m and ℓ . From the other hand, the properties of polynomial $y(x)$ are known, reflected in Lemma 3 and corollaries. It is clear that, defining the coefficients α_1, α_2 and α_3 of (18), we will define the polynomial $y(x)$ satisfying (13). At the same time for given m there may be several solutions of (18). In this case the worst scenario should be chosen, i.e. polynomials giving the minimal length of incorrecable burst. In the following we will show that coefficients $\alpha_1, \alpha_2, \alpha_3$ of (18), as well as the minimal length of incorrecable burst, are dependent on mutual placement of bursts' relative beginnings i and j .

Consider the case when the beginnings of one or both bursts are coincide with the beginning of the correspondent block of H_ℓ . Then the values $i + 1$ or (and) $j + 1$ should be equal to zero, and from this $i = -1 \pmod m$ or (and) $j = -1 \pmod m$ (since from $i = -1 \pmod m$ follows $(\bar{y} \setminus i, 0) = \bar{y}$).

The following lemma connects the parameters m, γ , coefficients α_1, α_2 , and α_3 from (18) and relative beginnings i and j of error bursts.

Lemma 5 *For the vector \bar{y} of length m and parameters i, j and γ , satisfying (12), the values of coefficients α_1, α_2 , and α_3 of (18) are defined by the values i and j according to the Table 1.*

Proof We will subsequently consider all possible locations of bursts' relative beginnings i and j , using polynomial representations (14) and (22).

1. Let $i \leq j$ and $i = j = -1$. This case corresponds to the first row of Table 1. This means that the equality $y(x) = (y(x) \setminus i) = (y(x) \setminus j)$ holds, that is

$$(y(x) \setminus i) = \sum_{k=0}^{m-1} y_k x^k,$$

$$((y(x) \setminus j) \cdot x^\gamma) \pmod{x^m - 1} = \sum_{k=0}^{m-1} y_k x^{(k+\gamma) \pmod m},$$

Table 1 Relative beginnings of bursts, coefficients of (18) and minimal lengths of incorrecable bursts

#	Condition	Incorr. burst length	Coeff. of (18)	Value of γ
1	$i = -1, j = -1$	$m - \gamma - 1$	$\alpha_1 = 0, \alpha_3 = 0$	$\ell - 1$
2	$-1 < i < (j + \gamma), j \neq -1$	$m - \gamma$	$\alpha_1 \neq 0, \alpha_3 = 1$	$\ell - 2$
3	$i \geq (j + \gamma), j \neq -1$	$m - \gamma + 1$	$\alpha_1 = 0, \alpha_3 \neq 0$	$\ell - 2$
4	$i = -1, j \neq -1$	$m - \gamma + 2$	$\alpha_1 = 0, \alpha_3 \neq 0$	$\ell - 1$
5	$i \neq -1, j = -1$	$m - \gamma + 1$	$\alpha_1 \neq 0, \alpha_3 = 0$	$\ell - 2$

from this $y_k = y_{(k-\gamma) \bmod m}$ for all k . Taking into account (18) we get $\alpha_1 = 0$, $\alpha_3 = 0$. The length b of incorrectable burst in this case is $b = m - \gamma - 1$.

2. Now let $i \leq j$, $i \neq -1$, $j \neq -1$.

In the proof of Corollary 2 it was shown that if $i \neq -1$, then $i \geq \gamma$. Consider different possible values of i and j .

- (a) $i = \gamma$. In this case from (14) and (22) we get $B^m(x) \subset B^i(x)$, $C^m(x) \subset B^i(x)$. In polynomial (14) the coefficient y_{j+1} is always correspondent to degree x^j , and degree x^j in polynomial (22) is always belong to $B^m(x)$, so $y_{i+1} = y_0$, $y_{j+1} = y_{j-\gamma}$. That is, before $(i+1)$ and $(j+1)$ th positions of \bar{y} there is the section of length $\gamma + 1$, then the length of incorrectable burst is $m - \gamma$.
- (b) $(\gamma + 1) \leq i < (j + \gamma)$. In this case the degree x^i belongs to $B^m(x)$, $y_{i+1} = y_{i-\gamma}$, $y_{j+1} = y_{j-\gamma}$, and this is the generalization of the previous case 2a, the length of incorrectable burst is also $m - \gamma$.

These cases are correspondent to the second row of Table 1.

3. Let $i \geq j + \gamma$. As it was shown in the proof of Corollary 2, if $i = j + \gamma$, then \bar{y} consists of one section of length $\gamma - 1$ and other sections of length γ . However, since neither i nor j in considered case are not equal to -1 , there are sections of length γ before relative beginnings of bursts, so $b = m - \gamma + 1$.

If $i > j + \gamma$, degree x^i belongs to $C^m(x)$, and $B^m(x) \subset A^i(x)$, so $y_{i+1} = y_{i-\gamma+1}$, $y_{j+1} = y_{j-\gamma+1}$. In this case in \bar{y} there are sections of length γ before positions y_{i+1} and y_{j+1} , so $b = m - \gamma + 1$.

Now we need to consider cases when i or j equal to -1 .

4. Let $i = -1 = m - 1$, $j \neq -1$. Then (14) and (22) may be written as

$$\begin{aligned} (y(x) \setminus i) &= \sum_{k=0}^{m-1} y_k x^k = A^i(x), \\ ((y(x) \setminus j) \cdot x^j) \bmod x^m - 1 &= A^m(x) + y_j x^{j-1} + B^m(x) + C^m(x). \end{aligned}$$

From this for any k one of the equations is hold: $y_k = y_{(k-\gamma) \bmod m}$, $y_k = y_{(k-\gamma+1) \bmod m}$. In other words, coefficient α_1 in (18) is equal to zero. This corresponds to the previous case, when $B^m(x) \subset A^i(x)$, and there are $\gamma - 1$ zeros before position $(j + 1)$. However, there are $\gamma - 2$ zeros before position $i + 1$, so we should select $b = \max(m - \gamma + 1, m - \gamma + 2) = m - \gamma + 2$. That is, in this case $b = m - \gamma + 2$, $\alpha_3 \neq 0$, $\alpha_1 = 0$.

5. Let $i \neq -1$, $j = -1 = m - 1$. Then

$$\begin{aligned} (y(x) \setminus i) &= \sum_{k=0}^{i-1} y_k x^k + \sum_{k=i}^{m-2} y_{k+1} x^k = A^i(x) + B^i(x), \\ ((y(x) \setminus j) \cdot x^j) \bmod x^m - 1 &= \sum_{k=0}^{m-1} y_{(k-\gamma) \bmod m} x^k. \end{aligned} \tag{23}$$

We get $y_{i+1} = y_{i-\gamma}$, $y_{j+1} = y_0 = y_{(-\gamma) \bmod m}$. This gives $b = m - \gamma + 1$, $\alpha_1 \neq 0$, $\alpha_3 = 0$.

Considered cases give the statement of Lemma 5.

If we know the values of coefficients in (18), we may calculate the minimal length of incorrectable burst. However, in third and fourth rows of Table 1 we have the same coefficients but different burst lengths. But taking into account the value of γ we may see that in fact these values coincide. Let us analyse the relationship between the value of γ (which is unknown during code construction) and ℓ (which is the code's parameter).

First consider $i \neq -1$, $j = -1 = m - 1$ (fifth row of Table 1). As it was shown, \bar{y} for such values i and j consists of sections of lengths γ and $\gamma + 1$, and the last section has the length γ . However, since $i \neq -1$ and $y_0 = 1$, this means that the first error burst occupies blocks h_0 and h_1 , and in the second burst the position correspondent to the column of $Q_2(B_2)$ with one in the first row (counting from zero), or equivalently to the $(m + 1)$ th row of block h_γ , should contain non-zero value. From this it follows that the number of this position is $(0 - \gamma) \bmod m = m - \gamma$. But this is possible only if second burst occupies the block $h_{\gamma+1}$. Then the upper diagonal of $Q_2(B_2)$ contains $\gamma + 1$ ones, and the number of the column containing second non-zero element in this diagonal (i.e. the position of one in the $(m + 1)$ th row of $h_{\gamma+1}$) is $m - \gamma$. So, since the burst B_2 occupies one block, the number of this block is $\gamma + 1$ instead of γ , so the value of γ cannot exceed $\ell - 2$.

Consider in more detail the connection between γ and ℓ . It is clear that $\gamma \leq \ell - 1$, since the burst begins in block h_γ . However, the burst may occupy two blocks and we need to check whether the burst affects the block with number exceeding $\ell - 1$. Let for some ℓ the code can correct bursts of length no more than b_ℓ . Then there are two uncorrectable bursts of length $b_\ell + 1$ occupying the first and last blocks of H_ℓ (it is supposed that the second burst ends in the last block but it may begin in the preceding one). If the second block does not affect the last block, this means that these bursts cannot be corrected by the code with number of blocks less than ℓ , then we may consider this shorter code as the code with bursts in the first and last blocks.

Next, each vector \bar{y} , which is defined by the inincorrectable bursts (see (4) and (12)) and is solution of (12) and (18), has the correspondent value of γ equal either to $\ell - 1$ or to $\ell - 2$. Consider the code with the number of blocks increased by one. The length of inincorrectable burst may either reduced or remain the same. In the first case we have $\gamma' = \gamma + 1$, in the second case $\gamma' = \gamma$. If for $\gamma' = \gamma + 1$ there are no solutions of equation (18) in terms of α_1 , α_2 and α_3 , then $b_{\ell+1} = b_\ell$ (b_ℓ means the maximum length of correctable burst for the code with parameter ℓ).

Continuing the analysis of γ in similar way, we obtain the values given in the last column of Table 1.

Summarizing the analysis, we may formulate the following results.

1. If the condition in the first row of Table 1 is satisfied, this means that $m \div \gamma$, or $m \div (\ell - 1)$ for given m and ℓ , and the code cannot correct bursts of length $b = m - \ell + 2$.

2. $\exists k > 0 : (m - (\gamma - 1) - k \cdot (\gamma + 1)) : \gamma$, or $\exists k > 0 : (m - \ell + 3 - k \cdot (\ell - 1)) : (\ell - 2)$, so $b = m - \ell + 2$.
3. $\exists k > 0 : (m - k \cdot (\gamma - 1)) : \gamma$, or $\exists k > 0 : (m - k \cdot (\ell - 3)) : (\ell - 2)$, so $b = m - \ell + 3$.
4. $\exists k > 0 : (m - k \cdot (\gamma - 1)) : \gamma$, or $\exists k > 0 : (m - k \cdot (\ell - 2)) : (\ell - 1)$, so $b = m - \ell + 3$.
5. $\exists k > 0 : (m - k \cdot (\gamma + 1)) : \gamma$, or $\exists k > 0 : (m - k \cdot (\ell - 1)) : (\ell - 2)$, so $b = m - \ell + 3$.

Given the code parameters m and ℓ we should first consider the conditions giving the least length of uncorrectable burst (i.e. 1 and 2). Then the conditions 3, 4 and 5 should be considered. If there are no satisfied conditions, then the minimal incorrectable burst is not in the last block of H_ℓ , then we should decrease ℓ and repeat the procedure.

The following two lemmas conclude the proof of Theorem 1.

Lemma 6 *If $\ell > \lceil m/2 \rceil + 1$, then the code defined by (1) can correct single bursts of length $b \leq b_\ell$, where*

$$\begin{cases} b_\ell = m - \lceil m/2 \rceil + 1, & m \text{ odd,} \\ b_\ell = m/2 - 1, & m \text{ even.} \end{cases} \quad (24)$$

Proof According to Lemma 5 and its corollaries, for each non-zero element of \bar{y} there are two other non-zero elements at distance γ , $\gamma + 1$ or $\gamma - 1$ positions to the left and to the right (that is, non-zero elements of neighbour sections). If $\ell > \lceil m/2 \rceil + 1$, then the maximum value of γ may exceed $m/2$, this means that the number of sections in \bar{y} is minimal in this case and is equal to 2, so the error burst contains only two ones, which are the beginning and the end of the burst, “moving” to each other by the cyclic shift by γ positions.

Further increasing of ℓ (exceeding $\lceil m/2 \rceil + 1$) will not lead to the decreasing of uncorrectable burst length. It is clear that in this case the maximal length of correctable burst will be defined by (24).

Lemma 7 *For $\ell = 3$ and m odd, the code with parity-check matrix (1) can correct single bursts of length $b = m - 1$.*

Proof It is clear that for $\ell = 3$ the error bursts occupy the first and last blocks of H_3 . Otherwise, γ would be equal to one and \bar{y} would consist of all-ones. Then $\gamma = 2$, which is possible only for $i = -1, j = -1$, and from Table 1 the burst length is $m - \gamma + 1$, which is $m - 1$ for $\gamma = 2$.

It is easy to check that for even m and $\ell = 3$ one may always define the vector \bar{y} satisfying (13) and containing ones on even positions and zeros on others.

From the results given in Table 1, Lemmas 6 and 7 the statement of Theorem 1 follows.

4 Conclusion

In this paper the burst-correcting capability of Gilbert codes is considered, when correcting single error bursts. The procedure is formulated, allowing to calculate the exact value of maximal correctable burst length depending on the parameters of the code. Its worth mentioning that extending Gilbert codes by adding extra parity-checks (or block-rows) to the parity-check matrix may improve the burst-correcting capabilities, however, for any block-permutation LDPC-code this value will be less than the block size.

References

1. Proakis, J., Salehi, M.: Digital Communications. McGraw-Hill (2007)
2. Krouk, E.A., Ovchinnikov, A.A.: Metrics for distributed systems. In: 2014 XIV International Symposium on Problems of Redundancy in Information and Control Systems (REDUNDANCY), pp. 66–70, 1–5 June 2014
3. Krouk, E., Semenov, S., authors.: Krouk, E., Semenov, S. (eds.) Modulation and Coding Techniques in Wireless Communications. Wiley (2011)
4. MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes. North-Holland Publishing Company (1977)
5. Lin, S., Ryan, W.: Channel Codes: Classical and Modern. Cambridge University Press (2009)
6. Gallager, R.G.: Low density parity check codes. IRE Trans. Inf. Theory (1962)
7. Gallager, R.G.: Low Density Parity Check Codes. MIT Press, Cambridge, MA (1963)
8. MacKay, D.: Good error correcting codes based on very sparse matrices. IEEE Trans. Inf. Theory **45** (1999)
9. MacKay, D., Neal, R.: Near shannon limit performance of low-density parity-check codes. IEEE Trans. Inf. Theory **47**(2) (2001)
10. Richardson, T.J., Urbanke, R.L.: The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans. Inf. Theory **47**(2) (2001)
11. Zyablov, V., Pinsker, M.: Estimation of the error-correction complexity for Gallager low-density codes. Probl. Inf. Trans. **XI**(1), 18–28 (1975)
12. Forney, G.D., Richardson, T.J., Urbanke, R.L., Chung, S.-Y.: On the design of low-density parity-check codes within 0.0045 db of the Shannon Limit. IEEE Commun. Lett. **5**(2) (2001)
13. Kozlov, A., Krouk, E., Ovchinnikov, A.: An approach to development of block-commutative codes with low density of parity check. Izvestiya vuzov. Priborostroenie. **8**, 9–14 (2013). (In Russian)
14. Gilbert, E.N.: A problem in binary encoding. Proc. Symp. Appl. Math. **10**, 291–297 (1960)
15. Arazi, B.: The optimal Burst error-correcting capability of the codes generated by $f(x) = (x^p + 1)(x^q + 1)/(x + 1)$. Inf. Contr. **39**(3), 303–314 (1978)
16. Bahl, L.R., Chien, R.T.: On Gilbert Burst-error-correcting codes. IEEE Trans. Inf. Theory **15**(3) (1969)
17. Neumann, P.G.: A note on Gilbert Burst-correcting codes. IEEE Trans. Inf. Theory, IT-11:377 (1965)
18. Zhang, W., Wolf, J.: A class of Binary Burst error-correcting quasi-cyclic codes. IEEE Trans. Inf. Theory, IT-34:463–479 (1988)
19. Krouk, E., Ovchinnikov, A.: 3-Stripes Gilbert low density parity-check codes. US Patent 7,882,415
20. Krouk, E.A., Semenov, S.V.: Low-density parity-check Burst error-correcting codes. In: International Workshop Algebraic and Combinatorial Coding Theory, Leningrad, pp. 121–124 (1990)