An Invariant Subcode of Linear Code

Sergei V. Fedorenko and Eugenii Krouk

Abstract An invariant subcode of a linear block code under the permutation is introduced. The concept of invariant subcode has two types of applications. The first type is decoding of linear block codes given the group of symmetry. The second type is the attack the McEliece cryptosystem based on codes correcting errors. Several examples illustrating the concept are presented.

Keywords Linear code · Permutation matrix · Quadratic residue code · Golay code

1 Introduction

The concept of invariant subcode was proposed by Krouk [1]. The methods for constructing the representation of linear block codes under permutation were reported in [1, Lemma 8.4] (via sequential constructing a basis for an invariant subcode of a linear block code) and in [2–5] (via block circulant representation of a linear block code). The different representations of linear block codes such as double circulant and quasi-cyclic codes are described in [6, Chapter 16.7].

The concept of invariant subcode has two types of applications. The first type is decoding of linear block codes given the group of symmetry [3, 5]. The second type is the attack the McEliece cryptosystem based on codes correcting errors [1].

The remainder of this paper is organized as follows. In Sect. 2, we propose the invariant subcode concept. In Sect. 3, we presented several examples illustrating the concept.

S.V. Fedorenko (✉) · E. Krouk
St. Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia
e-mail: sergei.fedorenko@gmail.com

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

G. De Pietro et al. (eds.), *Intelligent Interactive Multimedia Systems and Services 2016*, Smart Innovation, Systems and Technologies 55,
DOI 10.1007/978-3-319-39345-2_15

2 Invariant Subcode Concept

Let (n, k) code $\mathcal{G}$ be a binary linear block code with a codelength n and k information symbols. The code $\mathcal{G}$ has a generator matrix G and a parity-check matrix H. Let us introduce a permutation matrix for the code. The permutation matrix P for the code $\mathcal{G}$ has a property $GP = MG$ for some nonsingular matrix M. Let codeword $a \in \mathcal{G}$ be an invariant vector under the permutation matrix P such that $aP = a$. Then $aP = aI$ and $a(P - I) = 0$ where I is an identity matrix. All invariant codewords under the permutation matrix P form a subcode $\mathcal{S}$ of the code $\mathcal{G}$. Therefore

$$\begin{cases} aH^T = 0 \\ a(P - I) = 0, \end{cases}$$

$$a \left(\frac{H}{(P - I)^T} \right)^T = 0.$$

The matrix

$$S = \left(\frac{H}{(P - I)^T} \right)^T = 0.$$

is a parity-check matrix of the subcode $\mathcal{S}$. Finally, we obtain an invariant subcode $\mathcal{S} \subset \mathcal{G}$ under the permutation matrix P.

Proposition 1 *If the permutation matrix $P = (p_{i,j}), \quad i, j = 1, \dots, n$, has properties*

1. $p_{i,i} = 0$ *for* $i = 1, \dots, n$,
2. ord $P = l$, *l is a prime,*

then the invariant subcode $\mathcal{S} \subset \mathcal{G}$ under the permutation matrix P consists of l repeating submatrices. Thus a generator matrix G_P of code $\mathcal{S}$ has the form

$$G_P = (\underbrace{C \,|\, C \,|\, \cdots \,|\, C}_{l \text{ times}}).$$

Proof The proof is trivial. □

3 Examples

3.1 The Golay Code Under Order 2 Permutation

The generator matrix of the Golay code is given by

$$G = \begin{pmatrix} G_1 & G_2 \\ C & C \end{pmatrix}$$

$$= \left(\begin{array}{c|c}
1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1 \\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,1 \\
0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 \\
0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0 \\
0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1 \\
0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,1 \\
\hline
1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0 & 1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0 \\
0\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,1 & 0\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,1 \\
0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1 & 0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1 \\
0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0 & 0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,0
\end{array}\right).$$

Let permutation matrix be

$$P = \begin{pmatrix} 0 & I_{12} \\ I_{12} & 0 \end{pmatrix},$$

where I_{12} is the 12×12 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$G_P = (C|C).$$

3.2 The Golay Code Under Order 3 Permutation

Let us consider the Turyn-construction of the Golay code [6, Chapter 18.7.4]. The generator matrix of the Golay code is given by

$$G = \begin{pmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \\ C & C & C \end{pmatrix}$$

$$= \left(\begin{array}{c|c|c}
1\,0\,1\,1\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 1\,0\,1\,1\,0\,0\,0\,1 \\
0\,1\,0\,1\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,1\,0\,1\,1\,0\,0\,1 \\
0\,0\,1\,0\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,1\,0\,1\,1\,0\,1 \\
0\,0\,0\,1\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,1\,1\,1 \\
\hline
0\,0\,0\,0\,0\,0\,0\,0 & 1\,0\,1\,1\,0\,0\,0\,1 & 1\,0\,1\,1\,0\,0\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0 & 0\,1\,0\,1\,1\,0\,0\,1 & 0\,1\,0\,1\,1\,0\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,1\,0\,1\,1\,0\,1 & 0\,0\,1\,0\,1\,1\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,1\,1\,1 & 0\,0\,0\,1\,0\,1\,1\,1 \\
\hline
1\,1\,0\,1\,0\,0\,0\,1 & 1\,1\,0\,1\,0\,0\,0\,1 & 1\,1\,0\,1\,0\,0\,0\,1 \\
0\,1\,1\,0\,1\,0\,0\,1 & 0\,1\,1\,0\,1\,0\,0\,1 & 0\,1\,1\,0\,1\,0\,0\,1 \\
0\,0\,1\,1\,0\,1\,0\,1 & 0\,0\,1\,1\,0\,1\,0\,1 & 0\,0\,1\,1\,0\,1\,0\,1 \\
0\,0\,0\,1\,1\,0\,1\,1 & 0\,0\,0\,1\,1\,0\,1\,1 & 0\,0\,0\,1\,1\,0\,1\,1
\end{array}\right).$$

Let permutation matrix be

$$P = \begin{pmatrix} 0 & I_8 & 0 \\ 0 & 0 & I_8 \\ I_8 & 0 & 0 \end{pmatrix},$$

where I_8 is the 8×8 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$(G_P = C|C|C).$$

3.3 The Golay Code Under Order 4 Permutation

The generator matrix of the Golay code is given by

$$G = \begin{pmatrix} G_1 & G_2 & 0 & G_3 \\ G_3 & G_1 & G_2 & 0 \\ 0 & G_3 & G_1 & G_2 \\ C & C & C & C \end{pmatrix}$$

$$= \left(\begin{array}{c|c|c|c}
0\,1\,1\,0\,0\,1 & 1\,1\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,0 \\
0\,1\,0\,1\,1\,1 & 1\,0\,1\,0\,1\,0 & 0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0 \\
1\,1\,1\,0\,1\,0 & 1\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1 \\
\hline
0\,0\,0\,1\,0\,0 & 0\,1\,1\,0\,0\,1 & 1\,1\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,1\,0 & 0\,1\,0\,1\,1\,1 & 1\,0\,1\,0\,1\,0 & 0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,1 & 1\,1\,1\,0\,1\,0 & 1\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0 \\
\hline
0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,0 & 0\,1\,1\,0\,0\,1 & 1\,1\,1\,1\,0\,0 \\
0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0 & 0\,1\,0\,1\,1\,1 & 1\,0\,1\,0\,1\,0 \\
0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1 & 1\,1\,1\,0\,1\,0 & 1\,0\,1\,0\,0\,1 \\
\hline
1\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,0\,1 \\
1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1 \\
0\,1\,0\,0\,1\,0 & 0\,1\,0\,0\,1\,0 & 0\,1\,0\,0\,1\,0 & 0\,1\,0\,0\,1\,0
\end{array}\right).$$

Let permutation matrix be

$$P = \begin{pmatrix} 0 & I_6 & 0 & 0 \\ 0 & 0 & I_6 & 0 \\ 0 & 0 & 0 & I_6 \\ I_6 & 0 & 0 & 0 \end{pmatrix},$$

where I_6 is the 6×6 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$G_P = (C|C|C|C).$$

3.4 The Golay Code Under Order 6 Permutation

The generator matrix of the Golay code is given by

$$
G = \begin{pmatrix}
G_1 & 0 & 0 & G_2 & G_3 & G_4 \\
G_4 & G_1 & 0 & 0 & G_2 & G_3 \\
G_3 & G_4 & G_1 & 0 & 0 & G_2 \\
G_2 & G_3 & G_4 & G_1 & 0 & 0 \\
0 & G_2 & G_3 & G_4 & G_1 & 0 \\
C & C & C & C & C & C
\end{pmatrix}
$$

$$
= \left(\begin{array}{c|c|c|c|c|c}
0\,1\,1\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,1\,0 & 1\,0\,1\,0 & 0\,1\,1\,1 \\
0\,1\,0\,1 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,1\,1\,1 & 1\,1\,0\,1 \\ \hline
0\,1\,1\,1 & 0\,1\,1\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,1\,0 & 1\,0\,1\,0 \\
1\,1\,0\,1 & 0\,1\,0\,1 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,1\,1\,1 \\ \hline
1\,0\,1\,0 & 0\,1\,1\,1 & 0\,1\,1\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,1\,0 \\
0\,1\,1\,1 & 1\,1\,0\,1 & 0\,1\,0\,1 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \hline
0\,0\,1\,0 & 1\,0\,1\,0 & 0\,1\,1\,1 & 0\,1\,1\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\
0\,0\,0\,0 & 0\,1\,1\,1 & 1\,1\,0\,1 & 0\,1\,0\,1 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \hline
0\,0\,0\,0 & 0\,0\,1\,0 & 1\,0\,1\,0 & 0\,1\,1\,1 & 0\,1\,1\,0 & 0\,0\,0\,0 \\
0\,0\,0\,0 & 0\,0\,0\,0 & 0\,1\,1\,1 & 1\,1\,0\,1 & 0\,1\,0\,1 & 0\,0\,0\,0 \\ \hline
1\,0\,0\,1 & 1\,0\,0\,1 & 1\,0\,0\,1 & 1\,0\,0\,1 & 1\,0\,0\,1 & 1\,0\,0\,1 \\
1\,1\,1\,1 & 1\,1\,1\,1 & 1\,1\,1\,1 & 1\,1\,1\,1 & 1\,1\,1\,1 & 1\,1\,1\,1
\end{array}\right).
$$

Let permutation matrix be

$$
P = \begin{pmatrix}
0 & I_4 & 0 & 0 & 0 & 0 \\
0 & 0 & I_4 & 0 & 0 & 0 \\
0 & 0 & 0 & I_4 & 0 & 0 \\
0 & 0 & 0 & 0 & I_4 & 0 \\
0 & 0 & 0 & 0 & 0 & I_4 \\
I_4 & 0 & 0 & 0 & 0 & 0
\end{pmatrix},
$$

where I_4 is the 4×4 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$
G_P = (C|C|C|C|C|C).
$$

3.5 The (48,24) Quadratic Residue Code Under Order 2 Permutation

The generator matrix of the (48,24) quadratic residue code is given by

$$G = \begin{pmatrix} G_1 & G_2 \\ C & C \end{pmatrix}$$

$$= \left(\begin{array}{c|c}
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,1 \\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0\,0 \\
0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,1\,1\,1 \\
0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1 \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,1\,1\,0\,0 \\
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1 \\
\hline
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0 & 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0 \\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0 & 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0 \\
0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0 & 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0 \\
0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0 & 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0 \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1\,1\,1\,0 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,1\,1\,0\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,1\,1\,0\,1\,0\,1
\end{array}\right).$$

Let permutation matrix be

$$P = \begin{pmatrix} 0 & I_{24} \\ I_{24} & 0 \end{pmatrix},$$

where I_{24} is the 24×24 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$G_P = (C|C).$$

3.6 The (48,24) Quadratic Residue Code Under Order 3 Permutation

The generator matrix of the (48,24) quadratic residue code is given by

$$G = \begin{pmatrix} G_1 & G_2 & 0 \\ 0 & G_1 & G_2 \\ C & C & C \end{pmatrix}$$

$$
= \left(\begin{array}{c|c|c}
1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1 & 0\,0\,1\,1\,1\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0 & 1\,0\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1 & 1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0 & 1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1 & 1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1 & 0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1 & 1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
\hline
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1 & 0\,0\,1\,1\,1\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0 & 1\,0\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1 & 1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0 & 1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1 & 1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1 & 0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1 & 1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,1\,0\,0 \\
\hline
1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,1\,0 & 1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,1\,0 & 1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,1\,0 \\
1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0 & 1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0 & 1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0 \\
1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0 & 1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0 & 1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0 \\
1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0 & 1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0 & 1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0 \\
1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0 & 1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0 & 1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0 \\
0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0 & 0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0 & 0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0 \\
0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1 & 0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1 & 0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1 \\
1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1 & 1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1 & 1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1
\end{array}\right).
$$

Let permutation matrix be

$$
P = \begin{pmatrix} 0 & I_{16} & 0 \\ 0 & 0 & I_{16} \\ I_{16} & 0 & 0 \end{pmatrix},
$$

where I_{16} is the 16×16 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$
G_P = (C|C|C).
$$

3.7 The (48,24) Quadratic Residue Code Under Order 4 Permutation

The generator matrix of the (48,24) quadratic residue code is given by

$$
G = \begin{pmatrix} G_1 & 0 & G_2 & G_3 \\ G_3 & G_1 & 0 & G_2 \\ G_2 & G_3 & G_1 & 0 \\ C & C & C & C \end{pmatrix}
$$

$$
= \left(\begin{array}{c|c|c|c}
1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 & 0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1 \\
0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1 \\
0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 & 0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1 \\
0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 & 0\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0\,1 \\
1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0 \\
1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1 \\
\hline
0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1 & 1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1 & 0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 \\
0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1 & 0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 \\
0\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 \\
1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0 & 1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1 & 1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
\hline
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 & 0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1 & 1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1 & 0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 & 0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1 & 0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 & 0\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0 & 1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1 & 1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
\hline
1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,1 & 1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,1 & 1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,1 & 1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,1 \\
0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0 & 0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0 \\
0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0 & 0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0 & 0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0 & 0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0 \\
0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0 & 0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0 & 0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0 & 0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0 \\
0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0 & 0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0 & 0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0 & 0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0 \\
1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0 & 1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0 & 1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0 & 1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0
\end{array}\right).
$$

Let permutation matrix be

$$
P = \begin{pmatrix} 0 & I_{12} & 0 & 0 \\ 0 & 0 & I_{12} & 0 \\ 0 & 0 & 0 & I_{12} \\ I_{12} & 0 & 0 & 0 \end{pmatrix},
$$

where I_{12} is the 12×12 identity matrix. The generator matrix of the invariant sub-code under the permutation matrix P is

$$
G_P = (C|C|C|C)
$$

3.8 The (48,24) Quadratic Residue Code Under Order 6 Permutation

The generator matrix of the (48,24) quadratic residue code is given by

$$
G = \begin{pmatrix} G_1 & 0 & 0 & G_2 & G_3 & G_4 \\ G_4 & G_1 & 0 & 0 & G_2 & G_3 \\ G_3 & G_4 & G_1 & 0 & 0 & G_2 \\ G_2 & G_3 & G_4 & G_1 & 0 & 0 \\ 0 & G_2 & G_3 & G_4 & G_1 & 0 \\ C & C & C & C & C & C \end{pmatrix}
$$

$$
= \left(\begin{array}{c|c|c|c|c|c}
1\,1\,1\,1\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,1\,1 & 1\,1\,0\,0\,0\,0\,0\,1 \\
1\,1\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0 & 1\,0\,1\,0\,0\,0\,1\,1 & 1\,0\,0\,1\,0\,0\,0\,1 \\
1\,1\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0 & 1\,0\,0\,1\,1\,0\,1\,0 & 0\,0\,1\,1\,1\,0\,1\,0 \\
1\,1\,0\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,1\,0\,0\,1 & 1\,0\,1\,0\,0\,1\,0\,0 \\
\hline
1\,1\,0\,0\,0\,0\,0\,1 & 1\,1\,1\,1\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,1\,1 \\
1\,0\,0\,1\,0\,0\,0\,1 & 1\,1\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0 & 1\,0\,1\,0\,0\,0\,1\,1 \\
0\,0\,1\,1\,1\,0\,1\,0 & 1\,1\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0 & 1\,0\,0\,1\,1\,0\,1\,0 \\
1\,0\,1\,0\,0\,1\,0\,0 & 1\,1\,0\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,1\,0\,0\,1 \\
\hline
0\,0\,0\,0\,1\,0\,1\,1 & 1\,1\,0\,0\,0\,0\,0\,1 & 1\,1\,1\,1\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,0\,0 \\
1\,0\,1\,0\,0\,0\,1\,1 & 1\,0\,0\,1\,0\,0\,0\,1 & 1\,1\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0 \\
1\,0\,0\,1\,1\,0\,1\,0 & 0\,0\,1\,1\,1\,0\,1\,0 & 1\,1\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0 \\
1\,0\,0\,0\,1\,0\,0\,1 & 1\,0\,1\,0\,0\,1\,0\,0 & 1\,1\,0\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1 \\
\hline
0\,0\,0\,0\,1\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,1\,1 & 1\,1\,0\,0\,0\,0\,0\,1 & 1\,1\,1\,1\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,1\,0\,0 & 1\,0\,1\,0\,0\,0\,1\,1 & 1\,0\,0\,1\,0\,0\,0\,1 & 1\,1\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,1\,0 & 1\,0\,0\,1\,1\,0\,1\,0 & 0\,0\,1\,1\,1\,0\,1\,0 & 1\,1\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,1\,0\,0\,1 & 1\,0\,1\,0\,0\,1\,0\,0 & 1\,1\,0\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 \\
\hline
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,0\,0 & 0\,0\,0\,0\,1\,0\,1\,1 & 1\,1\,0\,0\,0\,0\,0\,1 & 1\,1\,1\,1\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,1\,0\,0 & 1\,0\,1\,0\,0\,0\,1\,1 & 1\,0\,0\,1\,0\,0\,0\,1 & 1\,1\,0\,0\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,1\,0 & 1\,0\,0\,1\,1\,0\,1\,0 & 0\,0\,1\,1\,1\,0\,1\,0 & 1\,1\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0\,1 & 1\,0\,0\,0\,1\,0\,0\,1 & 1\,0\,1\,0\,0\,1\,0\,0 & 1\,1\,0\,0\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0 \\
\hline
0\,0\,1\,1\,0\,1\,1\,0 & 0\,0\,1\,1\,0\,1\,1\,0 & 0\,0\,1\,1\,0\,1\,1\,0 & 0\,0\,1\,1\,0\,1\,1\,0 & 0\,0\,1\,1\,0\,1\,1\,0 & 0\,0\,1\,1\,0\,1\,1\,0 \\
1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 \\
0\,1\,1\,0\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,1\,1 & 0\,1\,1\,0\,0\,0\,1\,1 \\
1\,1\,1\,0\,1\,0\,1\,1 & 1\,1\,1\,0\,1\,0\,1\,1 & 1\,1\,1\,0\,1\,0\,1\,1 & 1\,1\,1\,0\,1\,0\,1\,1 & 1\,1\,1\,0\,1\,0\,1\,1 & 1\,1\,1\,0\,1\,0\,1\,1
\end{array}\right).
$$

Let permutation matrix be

$$
P = \begin{pmatrix}
0 & I_8 & 0 & 0 & 0 & 0 \\
0 & 0 & I_8 & 0 & 0 & 0 \\
0 & 0 & 0 & I_8 & 0 & 0 \\
0 & 0 & 0 & 0 & I_8 & 0 \\
0 & 0 & 0 & 0 & 0 & I_8 \\
I_8 & 0 & 0 & 0 & 0 & 0
\end{pmatrix},
$$

where I_8 is the 8×8 identity matrix. The generator matrix of the invariant subcode under the permutation matrix P is

$$
G_P = (C|C|C|C|C|C).
$$

4 Conclusion

The invariant subcode concept is introduced. The two types of applications (decoding of linear block codes and the attack the McEliece cryptosystem) are pointed out.

Acknowledgments The reported study was funded by RFBR according to the research project No. 16-01-00716 a.

References

1. Kabatiansky, G., Krouk, E., Semenov, S.: Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept. Wiley, West Sussex (2005)
2. Krouk, E.A., Fedorenko, S.V.: Decoding by generalized information sets. Problemy Peredachi Informatsii **31**(2), 54–61 (1995) (in Russian); English translation in Problems of Information Transmission **31**(2), 143–149 (1995)
3. Fedorenko, S., Krouk, A.: About block circulant representation of linear codes. In: Proceedings of Sixth International Workshop on Algebraic and Combinatorial Coding Theory at Pskov, Russia, pp. 116–118 (1998)
4. Fedorenko, S.: On the structure of linear block codes given the group of symmetry. In: Proceedings of IEEE International Workshop on Concatenated Codes, Schloss Reisensburg by Ulm, Germany (1999)
5. Fedorenko, S., Krouk, A.: The table decoders of quadratic-residue codes. In: Proceedings of Seventh International Workshop on Algebraic and Combinatorial Coding Theory at Bansko, Bulgaria, pp. 137–140 (2000)
6. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam-New York-Oxford (1977)