Kangweon-Kyungki Math. Jour. **10** (2002), No. 1, pp. 89–95

A DECODING METHOD FOR THE BINARY GOLAY CODE

Jae Yeon Yoon and Young Ho Park

Abstract. We present a simple but new way of decoding the binary Golay code.

1. Introduction

The binay Golay code G_{23} is an important example of a perfect code. It has length 23, dimension 12, and minimum distance 7. Many properties of G_{23} can be deduced from those of the extended Golay code G_{24} having generator matrix $G = [I_{12} \mid A]$, where I_{12} is the identity matrix of rank 12 and

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The *binary Golay code* G_{23} is obtained from G_{24} simply by omitting the last coordinate position from all codewords. In fact, we can omit any one of coordinate positions by the following theorem ([5], [7]).

Received February 14, 2002.
2000 Mathematics Subject Classification: 94B35, 94B15.
Key words and phrases: binary Golay code, decoding.

THEOREM 1.1. *A binary* $[23, 12, 7]$*-code is unique (up to equivalence).*

G_{23} can be constructed in a more natural way as a cyclic code as follows. Let $R = \mathbb{F}_2[x]/(x^{23} - 1)$. The factorization of $x^{23} - 1$ into irreducibles in $\mathbb{F}_2[x]$ is given by

$$x^{23} - 1 = (x - 1)g_1(x)g_2(x)$$

with

$$\begin{aligned} g_1(x) &= x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1, \\ g_2(x) &= x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1. \end{aligned}$$

The cyclic codes $C_1 = \langle g_1(x) \rangle \subset R$ and $C_2 = \langle g_2(x) \rangle \subset R$ can be shown to be all equivalent to G_{23}. The idempotent generator for C_1 may be taken to be

$$n(x) = x^5 + x^7 + x^{10} + x^{11} + x^{14} + x^{15} + x^{17} + x^{19} + x^{20} + x^{21} + x^{22}$$

and the idempotent generator for C_2 to be

$$q(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}.$$

Since the order of 2 modulo 23 is 12, the quadratic residues Q and nonresidues N modulo 23 are

$$\begin{aligned} Q &= \langle 2 \rangle = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}, \\ N &= 5\langle 2 \rangle = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}. \end{aligned}$$

Note that the exponents which appear in $q(x)$ are exactly the quadratic residues and those in $n(x)$ are quadratic nonresidues. Thus G_{23} is also a quadratic residue code. We refer [4], [3], [7], [8] for details about cyclic codes or quadratic codes.

2. The Group of a Code

The group of a code C is useful in determining the structure of the code, computing weight distributions, classifying codes, and devising decoding algorithms.

If $\mathbf{v} = (v_1, \ldots, v_n)$ is a vector and ϕ is a permutation on n objects, then ϕ sends $\mathbf{v}$ into $\mathbf{v}\phi = \mathbf{w} = (w_1, \ldots, w_n)$ with $v_i = w_{i\phi}$. Every permutation of the n coordinate positions sends C onto an equivalent $[n, k]$-code or onto itself. It is easy to check that the set of all permutations that send

C onto itself is a group. This group is called *the group of* C. It is denoted by $G(C)$.

Clearly any element in $G(C)$ applied to the coordinate positions of any generator matrix of C yields another generator matrix of C. The group of C is a subgroup of S_n.

We can now say that a length n code C is cyclic if the group of C contains the cyclic group of order n generated by $\sigma = (0, 1, \ldots, n-1)$. However, $G(C)$ might be, and usually is, larger than this as we see from the following theorem ([7]).

THEOREM 2.1. *Let C be an odd length n binary cyclic code. Let $\sigma \in S_n$ be the cyclic shift, that is, $(i)\sigma = (i+1) \pmod{n}$ and $\tau \in S_n$ be the permutation defined by $(i)\tau = 2i \pmod{n}$. Both σ and τ are considered to act on $0, 1, \ldots, n-1$. Let m be the order 2 mod n. Then $\tau\sigma\tau^{-1} = \sigma^{2^{m-1}}$ and $\tau^{-1}\sigma^i\tau = \sigma^{2i}$ for $0 \leq i \leq n-1$. Furthermore, τ is in $G(C)$, and hence the group P generated by σ and τ is a subgroup of $G(C)$. The order of P is mn.*

3. A decoding method of the Golay code

There are many known decoding methods for G_{23} ([1], [2], [6]). For example, being a cyclic code or, even better, a quadratic residue code, G_{23} can be decoded by the permutation decoding, error-traping decoding or the covering polynomials method. It can be decoded also by using Hexacode. Here we present a simple decoding method using the generator matrix.

DEFINITION 3.1. If G is a generator matrix of an $[n,k]$-code C, then any set of k columns of G that are independent is called an *information set* of C.

Note that any permutation π in $G(C)$ sends an information set into an information set. We may take the information set for G_{23} to be $\{11, 12, \ldots, 22\}$ for an appropriate generator matrix.

THEOREM 3.2. *Let $\sigma : i \to i+1 \pmod{23}$, and $\tau : i \to 2i \pmod{23}$. Then $P = \langle \sigma, \tau \rangle$ is a subgroup of $G(G_{23})$ such that for any error vector e of weight ≤ 3, some $\pi_i \in P$ moves all the 1's in e out of the information places.*

Proof. Let $\mathbf{e} = e_0e_1 \cdots e_{22}$ be an error vector of weight ≤ 3. We need to show that some $\pi \in P$ moves all the 1's in $\mathbf{e}$ out of the information places.

Applying cyclic shift σ, we may assume that $E = \{i \mid e_i = 1\} = \{0, l, k\}$, without loss of generality. As before, the quadratic residues Q and nonresidues N modulo 23 are

$$Q = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\} = \langle 2 \rangle$$
$$N = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\} = 5\langle 2 \rangle.$$

Therefore, if $l \in Q$, then there is some i such that $2^i l = 1$ and if $l \in N$, then there is some i such that $2^i l = 5$. Thus by applying τ^i, we may assume that $E = \{0, 1, k\}$ or $E = \{0, 5, k\}$. Since $\sigma \in P$, it suffices to show that there is i such that $E\tau^i = \{0, a, b\}$ $(a < b)$ satisfying $a > 11$ or $b - a > 11$ or $22 - b > 11$.

1. Suppose $E = \{0, 1, k\}$. If $k \leq 10$ or $k \geq 13$, then we are done. If $k = 10$ or $k = 11$, then apply τ to E to get $E\tau = \{0, 2, 22\}$ or $\{0, 2, 1\}$.
2. Suppose $E = \{0, 5, k\}$. If $k \leq 10$ of $k \geq 17$, then we are done, again. For other cases, one more application of τ is enough as we can see in the table below.

E	$E\tau$
$\{0, 5, 11\}$	$\{0, 10, 22\}$
$\{0, 5, 12\}$	$\{0, 1, 10\}$
$\{0, 5, 13\}$	$\{0, 3, 10\}$
$\{0, 5, 14\}$	$\{0, 5, 10\}$
$\{0, 5, 15\}$	$\{0, 7, 10\}$
$\{0, 5, 16\}$	$\{0, 9, 19\}$

□

Suppose a codeword $\mathbf{x} = x_0x_1 \cdots x_{22}$ is transmitted, an error vector $\mathbf{e} = e_0e_1 \cdots e_{22}$ occurs with weight ≤ 3, and the vector $\mathbf{y} = \mathbf{x} + \mathbf{e} = y_0y_1 \cdots y_{22}$ is received. Let G be the generator matrix of G_{23} such that $\{11, 12, \cdots, 22\}$ is an information set. Hence $\mathbf{x}_L = x_0x_1 \cdots x_{10}$ are the check symbols, and $\mathbf{x}_R = x_{11} \cdots x_{22}$ are information symbols. Write $G = (G_L | G_R)$, where G_L is a (12×11)-matrix and G_R is a (12×12)-matrix. Then G_R is invertible.

Now there exists some $\pi_i \in P$ such that $\mathbf{y}_i = \mathbf{y}\pi_i$ has no errors in the information places. Since $(\mathbf{y}_i)_R$ is the information symbols, there exists a unique codeword $\mathbf{w}$ such that $\mathbf{w}_R = (\mathbf{y}_i)_R$. In fact, $\mathbf{w} = \mathbf{x}\pi_i$ since $\mathbf{x}\pi_i \in G_{23}$ and $d(\mathbf{x}\pi_i, \mathbf{y}\pi_i) = d(\mathbf{x}, \mathbf{y}) \leq 3$. Recall that the encoding map $\mathbf{u} \mapsto \mathbf{u}G$ from $\mathbb{F}_2^{12}$ to G_{23} is bijective. Thus there exists a unique vector $\mathbf{u} \in \mathbb{F}_2^{12}$ such that $\mathbf{u}G = \mathbf{w}$, and then we have

$$(\mathbf{u}G_L|\mathbf{u}G_R) = \mathbf{u}G = \mathbf{w} = (\mathbf{w}_L|\mathbf{w}_R) = (\mathbf{w}_L|(\mathbf{y}_i)_R).$$

Hence $\mathbf{u} = (\mathbf{y}_i)_R G_R^{-1}$ and $\mathbf{w}_L = \mathbf{u}G_L = (\mathbf{y}_i)_R G_R^{-1} G_L$. Consequently,

$$\mathbf{x} = \mathbf{w}\pi_i^{-1} = ((\mathbf{y}_i)_R G_R^{-1} G_L|(\mathbf{y}_i)_R)\pi_i.$$

The decoding procedure is as follows. When $\mathbf{y}$ is received, each $\mathbf{y}_i = \mathbf{y}\pi_i$ and

$$\mathbf{w}_L = \mathbf{y}_i G_R^{-1} G_L$$

in turn is computed, until an i is found for which $d(\mathbf{w}_L, (\mathbf{y}_i)_L) \leq 3$. Then the errors are all in the first 11 places of $\mathbf{y}\pi_i$, and we decode $\mathbf{y}$ as

$$\mathbf{x} = (\mathbf{w}_L|(\mathbf{y}_i)_R)\pi_i^{-1}.$$

If $d(\mathbf{w}_L - (\mathbf{y}_i)_L) > 3$ for all i, we conclude that more than 3 errors have occurred.

Here we provide an explicit example. The generator polynomial for the cyclic code G_{23} is

$$g_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1.$$

This polynomial determines the generator matrix $G = [G_L|G_R]$ for G_{23} with

$$G_L = \begin{bmatrix} 1&0&1&0&1&1&1&0&0&0&1 \\ 0&1&0&1&0&1&1&1&0&0&0 \\ 0&0&1&0&1&0&1&1&1&0&0 \\ 0&0&0&1&0&1&0&1&1&1&0 \\ 0&0&0&0&1&0&1&0&1&1&1 \\ 0&0&0&0&0&1&0&1&0&1&1 \\ 0&0&0&0&0&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&1&0&1&0 \\ 0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix},$$

$$G_R = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0&0&0&0&0\\ 0&1&1&0&0&0&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&0&0&0&0&0&0&0\\ 1&0&0&0&1&1&0&0&0&0&0&0\\ 1&1&0&0&0&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&1&1&0&0&0&0\\ 0&1&1&1&0&0&0&1&1&0&0&0\\ 1&0&1&1&1&0&0&0&1&1&0&0\\ 0&1&0&1&1&1&0&0&0&1&1&0\\ 1&0&1&0&1&1&1&0&0&0&1&1 \end{bmatrix}$$

and so

$$D := G_R^{-1}G_L = \begin{bmatrix} 1&0&1&0&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&1&0&0&1\\ 1&1&0&1&0&0&1&0&1&0&1\\ 1&1&0&0&0&1&1&1&0&1&1\\ 1&1&0&0&1&1&0&1&1&0&0\\ 0&1&1&0&0&1&1&0&1&1&0\\ 0&0&1&1&0&0&1&1&0&1&1\\ 1&0&1&1&0&1&1&1&1&0&0\\ 0&1&0&1&1&0&1&1&1&1&0\\ 0&0&1&0&1&1&0&1&1&1&1\\ 1&0&1&1&1&0&0&0&1&1&0\\ 0&1&0&1&1&1&0&0&0&1&1 \end{bmatrix}.$$

Suppose that $\mathbf{x} = (01000010110|1111000000000)$ was sent and the vector $\mathbf{y} = (01010010110|1110010000000)$ is received. Since $\mathbf{y}_R D = 11100011011$ and $d(\mathbf{y}_L, \mathbf{y}_R D) = 6$, $\mathbf{y}$ have some errors. We compute $\mathbf{y}\pi_i$ for $\pi_i \in P = \langle \sigma, \tau \rangle$ and $\mathbf{w}_L = (\mathbf{y}_i)_R D$ until an i is found for which $d(\mathbf{w}_L, (\mathbf{y}_i)_L) \leq 3$. The existence of such π_i is guaranteed by Theorem 3.2. Note that $E = \{3, 14, 16\}$ and

$$E\sigma^9\tau = \{12, 0, 2\}\tau = \{1, 0, 4\}.$$

At some stage, with $\pi_i = \sigma^9\tau$, we will compute $\mathbf{y}_i = \mathbf{y}\pi_i = \mathbf{y}\sigma^9\tau = (01001001000|101000101110)$ and $\mathbf{w}_L = \mathbf{y}_i D = 10000001000$ and find that $d(\mathbf{w}_L, (\mathbf{y}_i)_L) = 3$. Thus we decode $\mathbf{y}$ as

$$\begin{aligned}\mathbf{x} &= (\mathbf{w}_L|(\mathbf{y}_i)_R)\pi_i^{-1} = (10000001000|101000101110)\tau^{-1}\sigma^{-9} \\ &= (10000000001|000010110111)\sigma^{-9} \\ &= (01000010110|111100000000).\end{aligned}$$

References

[1] N.J.A.Sloane and J.H.Conway, *Soft decoding techniques for codes and lattices*, including the Golay code and the Leech lattice, PGIT 32, 1986, 41–50.

[2] J.H.Conway and M.A.Odlyzko, *Sphere Packings*, Springer-Verlag, 1993.

[3] R.Hill, *A First Course in Coding Theory*, Oxford Alllide Mathematics and Computing Science Series, 1986.

[4] F.J.Macwilliams and N.J.A.Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1977.

[5] V.Pless, *On the uniqueness of the Golay codes*, JCT5, 1968, 215–228.

[6] V.Pless, *Decoding the Golay codes*, PGLT32, 1986, 561–567.

[7] V.Pless, *Introduction to the Theory of Error-Correcting Codes*, A Wiley-Interscience Publication, 1989.

[8] J.Y.Yoon, *On the binary Golay codes*, Master's thesis, Kangwon National University, 2002.

Department of Mathematics
Kangwon National University
Chunchoen 200-701, Korea
E-mail: `yhpark@kangwon.ac.kr`