

# **Golay Code**

蔡尚軒 林耀中

## *Outline*

### **1. Introduction**

### **2. The Golay Code Property**

**Weight Property**

**Weight Distribution**

**Perfect Code**

**Non-Primitive BCH Code**

**Quadratic Residue Code**

### **3. Decode Methods**

**1. Syndrome Decoder**

**2. Error trapping decoder for cyclic codes**

**3. Systematic Search Decoder**

**4. Kasami Decoder**

### **4. Error Rate Performance**

### **5. Conclusion**

### **6. Reference**

# 1. Introduction

There are a total of four Golay codes. Binary  $G_{23}$  (23,12,7),  $G_{24}$  (24,12,8) and Ternary  $G_{12}$  (12, 6, 6),  $G_{11}$  ( 11, 6, 5).

The Golay code  $G_{24}$  (24,12,8) was used to provide error control on the Voyager spacecraft.

They are founded by M.J. Golay in 1949. In the paper he presented, the two semi-perfect code ( 24, 12, 8) and ternary-( 12, 6, 6) is by the following generator matrices.

(24,12,8):  $G = [I_{12}|A]$  where

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

(12,6,6):  $G = [I_6|A]$  where

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

## 2. Properties

Some special properties of the golay code:

1.  $G_{24}$  is a self dual code

Proof? Straight Forward

2. The matrix  $[A|I_{12}]$  is also a generator matrix for  $G_{24}$

Proof? Straight Forward

3. The weight of every codeword in  $G_{24}$  is divisible by 4

Proof? From

$$w(r + s) = w(r) + w(s) - 2w(r \cap s)$$

4. The Golay code  $G_{24}$  has no codewords of weight 4

Proof? Not so intuitive

## Weight distribution

I	$G_{23}$	$G_{24}$
0	1	1
7	253	0
8	506	759
11	1288	0
12	1288	2576
15	506	0
16	253	759
23	1	0
24	0	1

$G_{23}$  is obtained by throwing away the last coordinate of every codeword of the code  $G_{24}$ . (Puncturing the code) The  $G_{24}$  satisfies the sphere sphere-packing condition, therefore, it is a **perfect binary code**.

**$G_{23}$  satisfied Hamming bound.**

Length = 23. For a codeword  $c$ , the span(3) of  $c$  is  $c + (c \text{ with } 1 \text{ bits error}) + (c \text{ with } 2 \text{ bits error}) + (c \text{ with } 3 \text{ bits error})$

$$\begin{aligned}
 |span(c,3)| &= 1 + C_1^{23} + C_2^{23} + C_3^{23} \\
 &= 1 + 23 + 253 + 1771 = 2048 = 2^{11} = 2^{n-k}
 \end{aligned}$$

## **The relationship between $G[23,12,7]$ and $G[24,12,8]$ :**

Extending a Code. Let  $c$  be any  $(n,k,d)$  code with  $d$  odd. By adding a 0 at the end of each codeword of even weight, and 1 at the end of each codeword of odd weight, we obtain a new  $(n+1,k,d+1),c'$ .

Proof:

The distance between any two vectors of  $c'$  is even, The minimum distance cannot be less than  $d$  (which), so must be  $d + 1$ .  $G[24,12,8]$  is the extended code of  $G[23,12,7]$  by adding an overall parity check.

## **Golay Code is Non-Primitive BCH code**

The Golay  $G[23,12,7]$  has length  $n = 23$  and dimension  $k = 12$ . We require an element of order 23.

$$n \mid 2^m - 1$$

$23 \mid 2047, 23 \times 89 = 2047$ . Therefore the element  $\alpha^{89} \in GF(2^{11})$  has order 23.

The cyclotomic coset with respect to 23.

This gives

$$K_1 = \{ 1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12 \}.$$

The dimension  $k = n - |K_1| = 23 - 11 = 12$

The **designed distance** for  $G[23]$  is  $d = 5$  because  $K_1$  contain **4** successive integers. The true minimum distance is 7.

The generator polynomial  $g(x)$  is obtained using

$$g(x) = (x - \beta) (x - \beta^2) (x - \beta^3) (x - \beta^4) (x - \beta^6) (x - \beta^8) (x - \beta^{12}) (x - \beta^{13}) (x - \beta^{16}) (x - \beta^{18})$$

From Table (*Irreducible polynomials of degree=11, j=89*). We select  $m_{89}(x) = 5343_8$ :

$$m_{89}(x)$$

$$=5 \quad 3 \quad 4 \quad 3$$

$$=101 \quad 011 \quad 100 \quad 011$$

$$=x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

## **Golay Code Is Quadratic Residue Code**

In 1968, Vera Pless showed that any binary linear code with the same parameters as  $G_{24}$  must be equivalent to  $G_{24}$ . Later, the other Golay codes are shown to be unique as well. When they were found, Golay did not provide the mathematical structure, which was discovered later as the **Quadratic Residue**

**Code.** Some others also call Golay Code as circulant codes, which parity matrices are circulant.

The Quadratic Residue Sets of the Golay code:

$$\{1,2,3,4,6,8,9,12,13,16,18\}$$

The resulting generator polynomial:

$$g_1(x) = (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \quad \text{or}$$

$$g_2(x) = (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$$

where  $x^{23} + 1 = g_1(x) \cdot g_2(x) \cdot (x + 1)$  [Cyclic code]

For the ternary Golay code, we have

$$x^{11} - 1 = g_1(x) \cdot g_2(x) \cdot (x - 1) \quad \text{where}$$

$$g_1(x) = (x^5 - x^3 + x^2 - x - 1) \quad \text{and} \quad g_2(x) = (-x^5 - x^4 + x^3 - x^2 + 1)$$

### 3. Decoding of Golay Code

Syndrome Decoding [Take it as Linear Code] : Take G[24,12,8] as an example,

$$g(x) = x^{11} + x^9 + x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \quad G = \begin{bmatrix} 101011100011 \\ 111110010010 \\ 110100101011 \\ 110001110110 \\ 110011011001 \\ 011001101101 \\ 001100110111 \\ 101101111000 \\ 010110111100 \\ 001011011110 \\ 101110001101 \\ 010111000111 \end{bmatrix}$$

	Weight of Coset Leader					
Error Inj.	0	1	2	3	Illegal	
0	1	0	0	0	0	0
1	0	24	0	0	0	0
2	0	0	276	0	0	0
3	0	0	0	2024	0	0
4	0	0	0	0	10626	0
5	0	0	0	42504	0	0
6	0	0	21252	0	113344	0
7	0	6072	0	340032	0	0
8	759	0	97152	0	637560	0
9	0	12144	0	1295360	0	0
10	0	0	261096	0	1700160	0
11	0	30912	0	2465232	0	0
12	2576	0	370944	0	2330636	0
13...24	Symmetric					

## Error trapping decoder for cyclic codes

Shift until the numbers of ones in the syndrome register is below or equal to the correctable errors.

Ex: Cyclic code with generator polynomial:

$$x^3 + x + 1$$

If receive  $(1,1,0,0,0,0,0)$  syndrome =  $(1,1,0)$

Shift  $(0,1,1,0,0,0,0)$  syndrome =  $(0,1,1)$

Shift  $(0,0,1,1,0,0,0)$  syndrome =  $(1,1,1)$

Shift  $(0,0,0,1,1,0,0)$  syndrome =  $(1,0,1)$

Shift  $(0,0,0,0,1,1,0)$  syndrome =  $(1,0,0)$

**FOUND!!**

The decoded word is  $(1,1,0,0,0,0,0) +$

$$(0,0,0,1,0,0,0) = (1,1,0,1,0,0,0)$$

There are possible error conditions that the decoder cannot decode

Ex: The error patterns that make burst errors longer than the generator polynomial are the ones that cannot be trapped. Below are two examples of the three-error pattern for  $G_{23}$  that cannot be trapped.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
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								
	1								1							1							
		1								1							1						
			1								1							1					
				1								1							1				
					1								1							1			
						1								1							1		
							1								1							1	

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
					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		
					1										1						1	
						1										1						1
							1										1					
								1										1				
									1										1			
										1										1		
											1										1	
												1										1

Kasami's error-trapping technique  
(introduced later)

## Decoding of the $G_{23}$ code:

Basic idea:

Error Trapping

Exceptional Cases

### Systematic Search Decoder:

A. Compute Syndrome

B. Shift and repeat A, if syndrome weight  $\leq 3$ , the error pattern is found

C. If after 23 shifts and no error patterns found. Guess error location! Invert first bit and repeat A & B except check for syndrome weight  $\leq 2$ .

D. Repeat C for the 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> ...and the 12<sup>th</sup> bit.

## Kasami Decoder

Kasami's error-trapping technique: finds a set of polynomials  $[\phi_j(X)]_{j=1}^N$  of degree  $k-1$  or less, such that, for any correctable error pattern  $e(X)$ , there is one polynomial  $\phi_j(X)$  such that  $X^{n-k} \cdot \phi_j(X)$  matches the message section of  $e(X)$  or the message section of a cyclic shift of  $e(X)$ . The polynomials  $\phi_j(X)$ 's are called the covering polynomials.

For the (23,12,7) Golay code, the selected set of covering polynomials are as follow:

$$\phi_1(X) = 0, \phi_2(X) = x^5, \phi_3(X) = x^6$$

Dividing  $x^5 \cdot x^{11}$  by the generator polynomial, the following remainder can be acquired:

$$\begin{aligned} x^5 \cdot x^{11} &= g(x) \cdot q_1(x) + \rho_1(x) \\ \rho_1(x) &= x^9 + x^8 + x^6 + x^5 + x^2 + x \end{aligned}$$

Similarly,  $x^6 \cdot x^{11}$  the following remainder can be acquired:

$$x^6 \cdot x^{11} = g(x) \cdot q_2(x) + \rho_2(x)$$

$$\rho_2(x) = x^{10} + x^9 + x^7 + x^6 + x^3 + x^2$$

Idea:

1. Check syndrome threshold
2. Added  $\rho_1(x)$  to the syndrome, then check syndrome threshold
3. Added  $\rho_2(x)$  to the syndrome, then check syndrome threshold

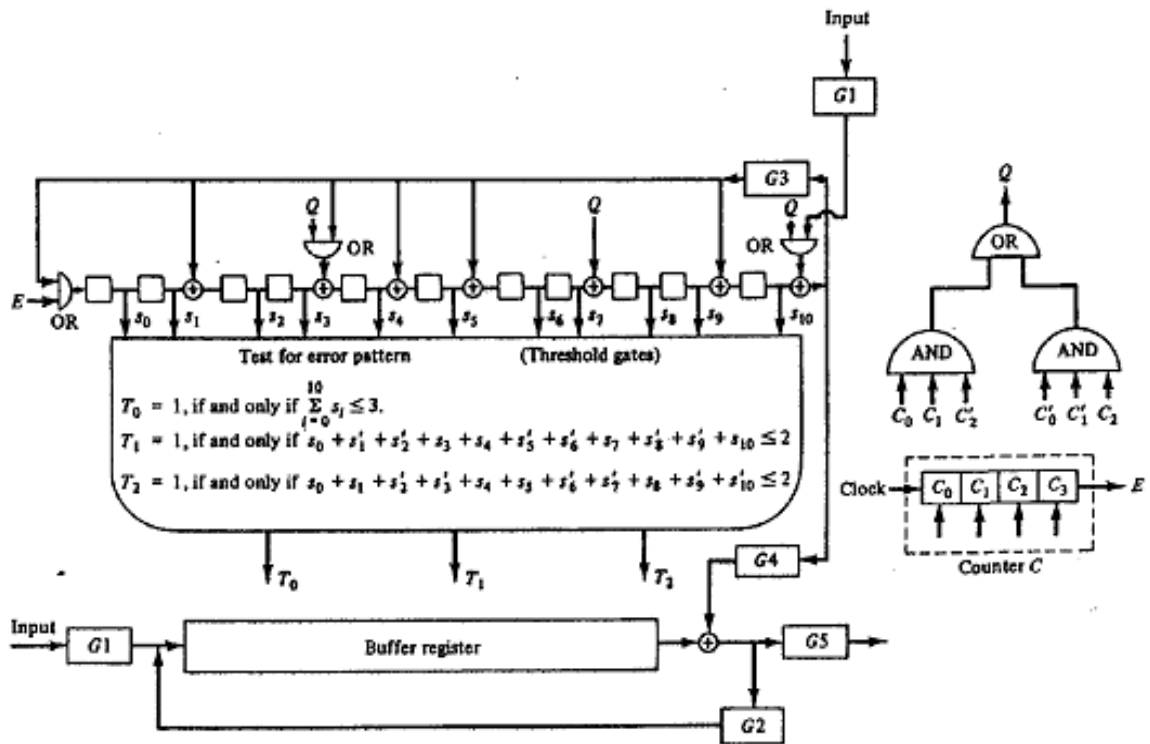


Figure 5.5 Error-trapping decoder for the Golay code.

A. Shift receive into syndrome and buffer register. (G1 G3 G5 on, G2 G4 off)

B. Syndrome test for following conditions (G2 G3 on, G1 G4 G5 off):

1.  $\sum_{i=0}^{10} s_i \leq 3$  : if success, the syndromes are added to the code to correct it; if not, the next test is used.

2.  $s_0 + s_1' + s_2' + s_3 + s_4 + s_5' + s_6' + s_7 + s_8' + s_9' + s_{10} \leq 2$ : if success, the resulting syndrome is outputted to the buffer input

3.  $s_0 + s_1 + s_2' + s_3' + s_4 + s_5 + s_6' + s_7' + s_8 + s_9' + s_{10}' \leq 2$ : if success, the resulting syndrome is outputted to the buffer input

D. If success (G3 off, G4 on) the error value is summed with the received code.

E. The corrected code is then found in the buffer register after 46 cycles

## 4. Error Rate Performance

It can be shown that for a BSC the performance of the Golay code G23 can be expressed in terms of the probability of an error at the output of the decoder as a function of the probability  $P$  of a symbol error of the channel.

$$P_b = \sum_{v=0}^3 \binom{23}{v} (1-P)^v \cdot P^{23-v} + \sum_{j=7}^{16} \frac{j \cdot W_j}{23} \left[ \sum_{v=0}^3 \sum_{r=0}^v \binom{j}{v-r} \binom{23-j}{r} (1-P)^{j-v+2r} \cdot P^{23-j+v-2r} \right]$$

**first term:** The channel introduces a 20-23 error,

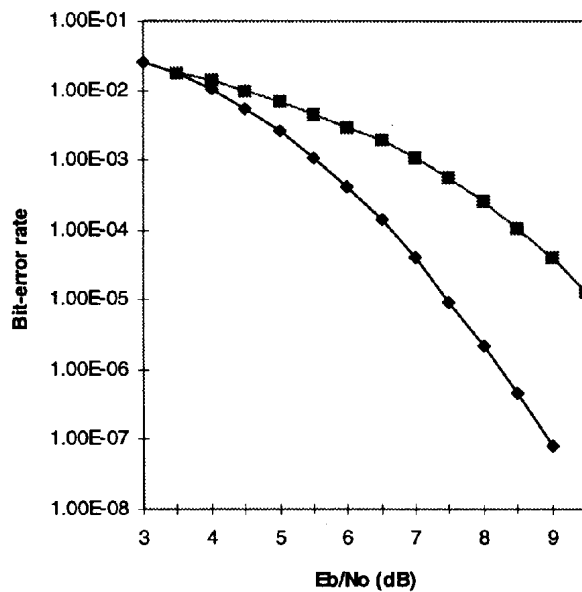
**second term:** The channel introduces a error that is equivalent to another code (or within the distance 3 of a code) [ex: if 011 is a code word distance 1 of this codeword would be 111, 001, 010]

**Basic concept:** The channel introduces a error that would cause the decoder to generate a undetectable error.

For binary phase-shift keyed modulation, a communication channel is a model of BSC for white Gaussian noise with

$$P = Q\left(\sqrt{R \cdot \frac{E_b}{N_0}}\right)$$

where  $R=k/n$  is the data rate.  $R=12/23$  for the code G23. The performance curve is given as below:



The line with squares are pure BPSK without coding. The line with diamonds are BPSK with Golay Coding. By the use of the Golay code, approximately 2.15dB coding gain is achieved by with  $P \approx 10^{-5}$ , while 1.33dB coding gain is obtained at  $P \approx 10^{-3}$ .

## **5. Conclusion**

1. The Golay  $(23,12,7)$  is the only multiple-error-correcting binary perfect code.
2. The Golay code has abundant and beautiful algebraic structure. Since its discovery by Golay in 1949 [12], it has become a subject of study by many coding theorists and mathematicians.

## **6. Reference:**

1. Irving S.Reed & Xuemin Chen,  
“*Error-Control Coding for Data Network*”,  
Kluwer Academic Pulishers, 1999.
2. Shu Lin & Daniel J. Costello, JR, “Error  
Control Coding Fundamentals and  
Applicatoins”, Prentice-Hall, 1983
3. NJ. Sloane, Partial of “A Short Course on  
Error Control Coding” – Topic: “Golay  
Code”
4. Martin Bossert, “Channel Coding for  
Telecommunications”, John Willey & Sons,  
1999
5. S. Roman, "Introduction to coding and  
Information Theory", Springer
6. M.J Golay, "Notes on Digital Coding", IRE,  
1949