V4a THE BINARY GOLAY CODE (1949)

- Let $\hat{B} = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&0&1&1&1&0&0&0&1&0 \\ 1&0&1&1&1&0&0&0&1&0&1 \\ & & & & & \vdots & & & & & \\ 0&1&1&0&1&1&1&0&0&0&1 \end{bmatrix}_{12\times 11}.$ each row is the left cyclic shift of the previous row.

- Let $\boxed{\hat{G} = [I_{12} \mid \hat{B}]_{12\times 23}}$. $\hat{G}$ is a GM for a $(23,12)$-binary code called the (binary) Golay code C_{23}. In fact, $d(C_{23}) = 7$. [proof later]

$\boxed{\text{CLAIM } C_{23} \text{ is a perfect code.}}$

PROOF We have $e = \lfloor (d-1)/2 \rfloor = 3$, and

$$M \cdot \sum_{i=0}^{e} \binom{n}{i}(q-1)^i = 2^{12}\left[\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}\right] = 2^{23}. \quad \square$$

THE EXTENDED GOLAY CODE C_{24}

- C_{24} is the binary code with GM $G = [I_{12} \mid B]_{12\times 24}$, where

$$B = \left[\begin{array}{c|c} 0 & \\ 1 & \\ 1 & \hat{B} \\ \vdots & \\ 1 & \end{array}\right]_{12\times 12} \quad \left(\text{so } B = \left[\begin{array}{c|ccccccccccc} 0 & 1&1&1&1&1&1&1&1&1&1&1 \\ 1 & 1&1&0&1&1&1&0&0&0&1&0 \\ \vdots & &&&&& \vdots &&&&& \\ 1 & 0&1&1&0&1&1&1&0&0&0&1 \end{array}\right]_{12\times 12} \right).$$

- **PROPERTIES OF C_{24}**

1) C_{24} is a $(24,12)$-binary code.
2) $GG^T = 0$ [check this]. Hence $C_{24} \subseteq C_{24}^{\perp}$, so C_{24} is self-orthogonal. $C \subseteq C^{\perp}$
3) Since $\dim(C_{24}) = \dim(C_{24}^{\perp}) = 12$, we have $C_{24} = C_{24}^{\perp}$. So, C_{24} is self-dual. $C = C^{\perp}$
4) $B = B^T$ (so B is symmetric).
5) A PCM for C_{24} is $H = [-B^T \mid I_{12}] = [B \mid I_{12}]$.
6) Since $C_{24} = C_{24}^{\perp}$, H is also a GM for C_{24}.

THEOREM $d(C_{24}) = 8$.

$$G = \begin{array}{c} \left[\begin{array}{c|c} & 011111111111 \\ & 111011100010 \\ I_{12} & 110111000101 \\ & \vdots \\ & 101101110001 \end{array}\right] \end{array} \begin{array}{l} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_{12} \end{array}$$

PROOF Let the rows of G be $r_1, r_2, \ldots, r_{12}$.

i) Note that $w(r_1) = 12$ and $w(r_i) = 8$ for $2 \le i \le 12$. Hence $4 \mid w(r_i)$ for all i. Now, $r_i \cdot r_j = 0$ since $GG^T = 0$, and so the number of coordinates of r_i and r_j that are both 1 is even. Hence, $4 \mid w(r_i + r_j)$, and so every codeword has weight divisible by 4. Thus, $d(C_{24}) = 4$ or 8.

ii) Next, we'll show that no codeword has weight 4 (so $d(C_{24}) = 8$).

- Each row of G has weight ≥ 8.
- Adding two rows of G: $w(r_1 + r_j) = 8$ for $2 \le j \le 12$. [Check this]

  $w(r_i + r_j) = 8$ for $2 \le i < j \le 12$. [Check this]

- Adding 3 rows of G: Let $c = r_i + r_j + r_k$, where $1 \le i < j < k \le 12$. Let $c = (x, y)$, where x, y have length 12. Suppose $w(c) = 4$. Since $w(x) = 3$, we have $w(y) = 1$. Since $H = [B \mid I_{12}]$ is also a GM for C_{24}, c must be a single row of H. This is impossible since each row of H has weight 8 or 12. Hence, $w(c) \neq 4$.

- Adding 4 rows of G: Let $c = r_i + r_j + r_k + r_l$, where $1 \le i < j < k < l \le 12$. Let $c = (x, y)$, and suppose $w(c) = 4$. Then $w(x) = 4$ and $w(y) = 0$. But H does not have any such vector in its row space. Thus, $w(c) \neq 4$.

- Adding ≥ 5 rows of G: If $c = (x, y)$ is the sum of 5 or more rows of G, then $w(x) \geq 5$, so $w(c) \neq 4$. □

$\boxed{\text{COROLLARY } d(C_{23}) = 7.}$

V4b A DECODING ALGORITHM FOR C_{24}

RECALL $n=24$, $k=12$, $d=8$, $e=3$.

$G=[I_{12} \mid B]$ and $H=[B \mid I_{12}]$ are both GMs and PCMs for C_{24}.

DECODING STRATEGY (IMLD) Compute a syndrome s of the received word r. Find a vector e of weight ≤ 3 that has syndrome s. If such a vector e exists, then decode r to $c=r-e$; else reject r.

CORRECTNESS If the error vector has weight ≤ 3, then the decoder always make the correct decision. If the error vector has weight ≥ 4, the decoder will either reject r, or will decode r to a codeword different from the transmitted one.

DECODING ALGORITHM FOR C24 (WITH JUSTIFICATION)

- Let $r = (x, y)$ and $e = (e_1, e_2)$, where x, y, e_1, e_2 have length 12.
- There are 5 cases (not mutually exclusive) in the event $w(e) \le 3$:

  (A) $w(e_1) = 0$ and $w(e_2) = 0$.

  (B) $1 \le w(e_1) \le 3$ and $w(e_2) = 0$.

  (C) $w(e_1) = 1$ or 2, and $w(e_2) = 1$.

  (D) $w(e_1) = 0$ and $1 \le w(e_2) \le 3$.

  (E) $w(e_1) = 1$ and $w(e_2) = 1$ or 2.

1) Compute the syndrome $s_1 = [I_{12} \mid B]\, r^T$.
   If $s_1 = 0$, then accept r and STOP. [case A]
2) [Note: $s_1 = [I_{12} \mid B]\, r^T = [I_{12} \mid B]\, e^T = e_1^T + B e_2^T = e_1^T$. So, if we are in case B, then $1 \le w(s_1) \le 3$.] If $w(s_1) \le 3$, then set $e = (s_1^T, 0)$. [case B]
   Correct x in the positions corresponding to the 1's in s_1 and STOP.

3) [Recall: $s_1 = e_1^T + Be_2^T$. If we are in case (C), then s_1 is equal to a column of B with one or two bits flipped (depending on which bits of e_1 are 1)]. Compare s_1 with the columns (or rows) of B. [Case C]
If any column of B, say column i, differs in exactly one (say j) or two (say j and k) positions from s_1, then decode $r=(x,y)$ as follows:

Correct x in position j, or in positions j,k.

Correct y in position i, and STOP.

4) Compute the syndrome $s_2 = [B \mid I_{12}]r^T = [B \mid I_{12}]e^T = Be_1^T + e_2^T = e_2^T$.
If $w(s_2) \leq 3$, then correct y in the positions corresponding to the 1's in s_2 and STOP. [Case D]

5) Analogous to step 3. [Case E]

6) Reject r (since $w(e) \geq 4$).

DECODING ALGORITHM FOR C24

Suppose $r=(x,y)$ is received.

1) Compute $s_1=[I_{12}|B]r^T$. If $s_1=0$, then accept r and STOP. (A)
2) If $\omega(s_1)\leq 3$, then set $e=(s_1^T,0)$ and decode r to $c=r-e$ and STOP. (B)
3) Compare s_1 to the rows of B. If row i of B differs in exactly one position (say j) or two positions (say j and k), then:
   Correct x in position j, or positions j and k; Correct y in position i; STOP. (C)
4) Compute $s_2=[B|I_{12}]r^T$,
   If $\omega(s_2)\leq 3$, then set $e=(0,s_2^T)$ and decode r to $c=r-e$ and STOP. (D)
5) Compare s_2 to the rows of B. If row i of B differs in exactly one position (say j) or two positions (say j and k), then:
   Correct y in position j, or positions j and k; Correct x in position i; STOP. (E)
6) Reject r.

- **EXAMPLE** Decode $r = (1000\ 1000\ 0000\ 1001\ 0001\ 1101)$.

  SOLUTION Compute $s_1 = [I_{12} | B] r^T = (0100\ 1000\ 0000)^T$.

  Since $w(s_1) = 2$, we set $e = (s_1^T, 0)$ and decode r to

  $c = r - e = (1100\ 0000\ 0000\ 1001\ 0001\ 1101)$. [Check: $Hc^T = 0$]

- **EXAMPLE** Decode $r = (1000\ 0010\ 0000\ 1000\ 1101\ 0010)$.

  SOLUTION Compute $s_1 = [I_{12} | B] r^T = (1011\ 1110\ 1011)^T$.

  Then $w(s_1) > 3$. We see that s_1 differs in positions 6 and 7 from row 4 of B. So, we set $e = (0000\ 0110\ 0000\ 0001\ 0000\ 0000)$ and decode r to $c = r - e = (1000\ 0100\ 0000\ 1001\ 1101\ 0010)$.

  [Check: $Hc^T = 0$]

$$B = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{array}\right]_{12 \times 12}.$$

NOTES (decoding algorithm for C_{24})

1) The decoding algorithm only needs to store B (144 bits).
   In contrast, a syndrome table has size $2^{12} \times 24 = 98{,}304$ bits.
2) Decoding is efficient and simple $\Rightarrow$ good for hardware implementation.
3) C_{24} was used in the Voyager space mission to transmit photos of Jupiter and Saturn to earth.

V4c RELIABILITY OF C_{24}

- **QUESTION** Is C_{24} better than simpler codes such as the binary replication codes and the Hamming codes?

- Let p = symbol error probability, and $C = \{c_1, c_2, \ldots, c_M\}$.
- Let ω_i = prob. that the decoding algorithm makes an incorrect decision or rejects if c_i is sent.
- $P_C = \frac{1}{M}\sum_{i=1}^{M}\omega_i = \omega_1$ = error probability of C.
- $1 - P_C$ = reliability of C = prob. that r is decoded correctly.

(1) For C_{24}, $1 - P_{C_{24}} = (1-p)^{24} + \binom{24}{1}p(1-p)^{23} + \binom{24}{2}p^2(1-p)^{22} + \binom{24}{3}p^3(1-p)^{21}$.

(2) If no channel encoding is used, the prob. that a 12-bit message is transmitted with no errors is $(1-p)^{12}$.

(3) Suppose the binary triplication code T is used to encode 12-bit messages. Then $1 - P_T = [(1-p)^3 + 3p(1-p)^2]^{12}$.

(4) Suppose that a (15,11)-binary Hamming code H is used to encode 11-bit messages. Then $1 - P_H = (1-p)^{15} + 15p(1-p)^{14}$.

p	$(1-p)^{12}$	$1-P_T$	$1-P_H$	$1-P_{C_{24}}$
0.1	0.282429	0.711206	0.549043	0.785738
0.01	0.886385	0.996480	0.990378	0.999909
0.001	0.988066	0.999964	0.999896	0.9999999895
Rate	1	$\frac{1}{3} \approx 0.33$	$\frac{11}{15} \approx 0.73$	$\frac{1}{2} = 0.5$