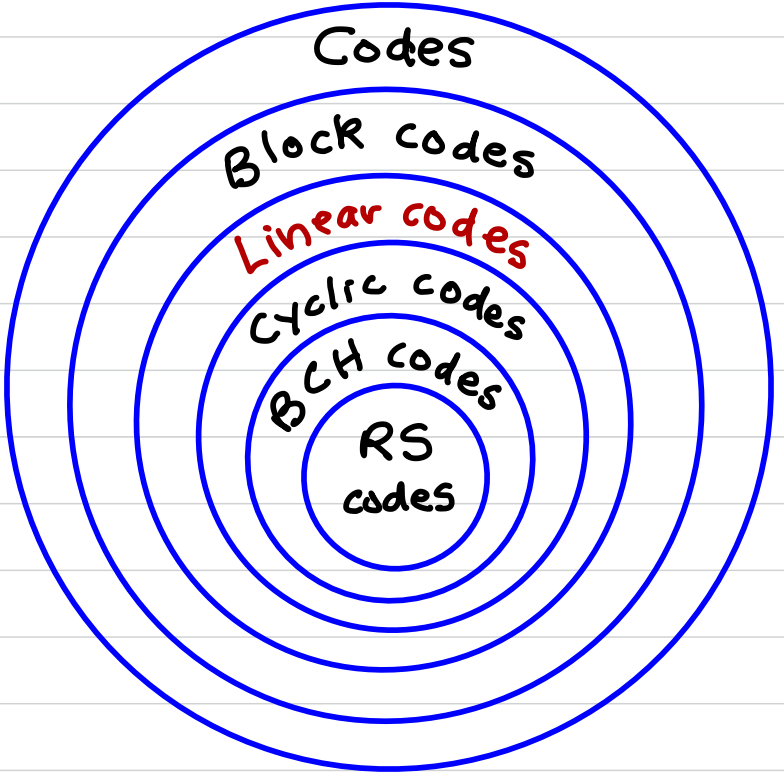
V3a Linear Codes



Linear codes

- Weight
- Generator matrix
- Dual code
- Parity-check matrix
- Distance
- Perfect codes
- Hamming codes
- Syndrome decoding

DEFINITION OF A LINEAR CODE

- Let $F = GF(q)$, and let $V_n(F) = F^n = \overbrace{F \times F \times \cdots \times F}^{n}$.
  $V_n(F)$ is an n-dimensional vector space over F, with $|V_n(F)| = q^n$.

DEFINITION A linear (n,k)-code over F is a k-dimensional subspace of $V_n(F)$.

RECALL A subspace S of a vector space V over F is a non-empty subset $S \subseteq V$ such that (i) $a, b \in S \Rightarrow a+b \in S$, and (ii) $a \in S, \lambda \in F \Rightarrow \lambda a \in S$.
If S is a subspace of V, then S is itself a vector space over F; in particular $0 \in S$. A basis of S is a linearly independent, spanning subset of S. All bases of S have the same size, called the dimension of S.

PROPERTIES OF LINEAR CODES

Let C be an (n,k)-code over $F=GF(q)$, and let $v_1, v_2, \ldots, v_k$ be an ordered basis for C.

1) **NUMBER OF CODEWORDS** The codewords in C are precisely $m_1v_1 + m_2v_2 + \cdots + m_kv_k$, where $m_i \in F$.

Thus, $|C| = M = \boxed{q^k}$.

2) **RATE** The rate of C is $R = \frac{\log_q M}{n} = \frac{\log_q q^k}{n} = \boxed{\frac{k}{n}}$.

3) WEIGHT

DEFINITION The weight $\omega(v)$ of a vector $v \in V_n(F)$ is the number of nonzero coordinates in v. The weight of a linear code C is

$$\omega(C) = \min\{\omega(c) : c \in C, c \neq 0\}.$$

THEOREM If C is a linear code, then $\omega(C) = d(C)$.

PROOF We have $d(C) = \min\{d(x,y) : x,y \in C, x \neq y\}$

$= \min\{\omega(x-y) : x,y \in C, x \neq y\}$ (since $d(x,y) = \omega(x-y)$)

$= \min\{\omega(c) : c \in C, c \neq 0\}$ (since C is linear, $x-y \in C$)

$= \omega(C)$. □

NOTATION An (n,k,d)-code C over F is a linear code of length n, dimension k, and distance d.

4) ENCODING

- Since there are q^k codewords, there are also q^k source messages.
- We shall assume that the source messages are the elements of F^k.
- Then, a convenient and natural bijection between F^k and C, i.e. an encoding rule, is defined by

$$m = (m_1, m_2, \ldots, m_k) \longmapsto c = m_1 v_1 + m_2 v_2 + \cdots + m_k v_k.$$

- NOTE Different ordered bases for C yield different encoding rules.

5) GENERATOR MATRIX: A convenient way to describe C.

DEFINITION A generator matrix (GM) for an (n,k)-code C is a $k \times n$ matrix whose rows form a basis for C: $G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}$

NOTE The encoding rule is $\boxed{c = mG.}$

EXAMPLE (linear code) Consider the $(5,3)$-binary code
$C = \langle \underbrace{10011}_{c_1}, \underbrace{01001}_{c_2}, \underbrace{00110}_{c_3} \rangle$. (NOTE: c_1, c_2, c_3 are l.i. over $\mathbb{Z}_2$.)

- A generator matrix for C is $G_1 = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right]_{3\times 5}$.

- The encoding rule w.r.t. the GM G is $c = mG_1$.

$000 \longrightarrow 00000$		$100 \longrightarrow 10011$	
$001 \longrightarrow 00110$		$101 \longrightarrow 10101$	
$010 \longrightarrow 01001$		$110 \longrightarrow 11010$	
$011 \longrightarrow 01111$		$111 \longrightarrow 11100$	
$\underbrace{011}_{m}$	$\underbrace{01111}_{c}$	$\underbrace{111}_{m}$	$\underbrace{11100}_{c}$

- $M = |C| = 2^3 = 8$, $R = 3/5$, $d(C) = w(C) = 2$.
  So, C is a $(5,3,2)$-binary code.

STANDARD FORM GM

DEFINITION Let C be an (n,k)-code over F. A GM G for C of the form $G = [I_k | A]_{k \times n}$ is said to be in standard form.
If C has a GM in standard form, then C is a systematic code.

EXAMPLE $C = \langle 100011, 001001, 000110 \rangle$ is a non-systematic $(6,3)$-binary code.
However, $C' = \langle 100011, 001001, 010010 \rangle$ obtained by swapping the 2^{nd} and 4^{th} coordinates of every codeword in C, is systematic.
A GM for C' is

$$G' = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right]_{3 \times 6}.$$

EQUIVALENT CODES

DEFINITION Two codes C, C' of length n are equivalent if C' can be obtained from C by choosing a permutation of coordinate positions $\{1, 2, \ldots, n\}$, and then consistently rearranging every codeword in C according to this permutation.

FACTS (equivalent codes)

1. If C is linear and C' is equivalent to C, then C' is linear.
2. Equivalent linear codes have the same length, dimension, distance.
3. Every linear code is equivalent to a systematic code.

V3b Dual Code and Parity Check Matrices

DEFINITION Let $x=(x_1,x_2,\ldots,x_n)$, $y=(y_1,y_2,\ldots,y_n)\in V_n(F)$.
The inner product of x and y is $x\cdot y=x_1y_1+x_2y_2+\cdots+x_ny_n\in F$.
x,y are orthogonal if $x\cdot y=0$.

PROPERTIES For all $x,y,z\in V_n(F)$ and $\lambda\in F$:

(i) $x\cdot y=y\cdot x$.

(ii) $x\cdot(y+z)=x\cdot y+x\cdot z$.

(iii) $(\lambda x)\cdot y=\lambda(x\cdot y)$.

(iv) $x\cdot x=0$ does not imply that $x=0$.

EXAMPLE Let $x=111100\in V_6(\mathbb{Z}_2)$. Then $x\cdot x=0$, but $x\neq 0$.
More generally, if $x\in V_n(\mathbb{Z}_2)$, then $x\cdot x=0$ iff $\omega(x)$ is even.

THE DUAL CODE

DEFINITION Let C be an (n,k)-code over F. The dual code of C is $C^\perp = \{x \in V_n(F) : x \cdot y = 0 \ \forall y \in C\}$. "$C^\perp$ = C perp"

THEOREM If C is an (n,k)-code over F, then $C^\perp$ is an $(n,n-k)$-code over F.

PROOF Let G_1 be a GM for C, and let the rows of G_1 be $v_1, v_2, \ldots, v_k$.

CLAIM Let $x \in V_n(F)$. Then $x \in C^\perp$ iff $v_1 \cdot x = v_2 \cdot x = \cdots = v_k \cdot x = 0$.

PROOF OF CLAIM ($\Rightarrow$) is clear since $v_1, v_2, \ldots, v_k \in C$.

($\Leftarrow$) Suppose $v \in C$. Then we can write $v = \lambda_1 v_1 + \cdots + \lambda_k v_k$, where $\lambda_i \in F$. Then $v \cdot x = (\lambda_1 v_1 + \cdots + \lambda_k v_k) \cdot x = \lambda_1 (v_1 \cdot x) + \cdots + \lambda_k (v_k \cdot x) = 0$. □

Thus, $C^\perp = \{x \in V_n(F) : G_1 x^T = 0\}$ = null space of G_1.

Since G_1 has rank k, its null space is a subspace of $V_n(F)$ of dim $n-k$. □

PARITY-CHECK MATRIX

THEOREM If C is a linear code, then $(C^\perp)^\perp = C$.

PROOF Let C be an (n,k)-code. Then $C^\perp$ is an $(n,n-k)$-code. Furthermore, $(C^\perp)^\perp$ is an (n,k)-code, and $C \subseteq (C^\perp)^\perp$. Since $\dim(C) = \dim((C^\perp)^\perp)$, it follows that $C = (C^\perp)^\perp$. □

DEFINITION If C is a linear code, then a generator matrix H for $C^\perp$ is called a parity-check matrix (PCM) for C.

NOTES (i) H is an $(n-k) \times n$ matrix.
(ii) C has many PCMs.

CONSTRUCTING A PCM FOR C (A GM FOR $C^\perp$)

THEOREM Let C be an (n,k)-code with GM $G_1 = [I_k | A]$.
Then $H = [-A^T | I_{n-k}]$ is a GM for $C^\perp$.
NOTE: A is a $k \times (n-k)$ matrix.

PROOF Since $\text{rank}(H) = n-k$, H is a GM for an $(n, n-k)$-code $\overline{C}$.
Also, $GH^T = [I_k | A] \begin{bmatrix} -A \\ \hline I_{n-k} \end{bmatrix} = -A + A = 0$.

Thus, $\overline{C} \subseteq C^\perp$. Since $\dim(\overline{C}) = \dim(C^\perp) = n-k$, we have $\overline{C} = C^\perp$.
Hence, H is a GM for $C^\perp$. □

EXAMPLE Consider the $(5,2)$-code C over $\mathbb{Z}_3$ with GM $G = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$. Find a PCM for C.

SOLUTION First find a GM for C in standard form.

$$G \xrightarrow{R_1 \leftarrow 2R_1} \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{R_2 \leftarrow R_2 - R_1} \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 2 & 1 & 1 \end{array}\right]$$

A

$$H = \left[\begin{array}{cc|ccc} 2 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{array}\right].$$

- We have $C = \{00000, 20210, 10120, 11001, 22002, 01211, 02122, 21121, 12212\}$.
- $d(C) = w(C) = 3$, and $R = 2/5$.

NOTES ON PCMs

Let C be an (n,k)-code over F with GM G.

1) An $(n-k)\times n$ matrix H over F is a PCM for C iff $GH^T = 0$ and $\text{rank}(H) = n-k$.

2) $G_\perp$ is a PCM for $C^\perp$ (since $(C^\perp)^\perp = C$).

3) Let H be a PCM for C. Then H is a GM for $C^\perp$, so C = null space of H.

4) Let H be a PCM for C, and let $x \in V_n(F)$. Then $x \in C$ iff $Hx^T = 0$.

V3c Distance of a Linear Code

C	$C^\perp$
(n,k)-code over F	$(n,n-k)$-code over F
G: GM for C	H: GM for $C^\perp$
C = row space of G	$C^\perp$ = row space of H
H: PCM for C	G: PCM for $C^\perp$
C = null space of H	$C^\perp$ = null space of G
$x \in C$ iff $Hx^T = 0$	$x \in C^\perp$ iff $Gx^T = 0$

$$(C^\perp)^\perp = C$$

THEOREM (distance of a linear code) Let H be a PCM for an (n,k)-code C over F. Then $d(C) \geq s$ iff every $s-1$ columns of H are linearly independent over F.

PROOF Let $H = [h_1 | h_2 | \cdots | h_n]$.

($\Leftarrow$) Suppose $d(C) \leq s-1$. Let $c = (c_1, c_2, \ldots, c_n) \in C$ with $c \neq 0$ and $w(c) \leq s-1$. Without loss of generality, suppose that $c_j = 0$ for $s \leq j \leq n$. Then, since $Hc^T = 0$, we have

$$c_1 h_1 + c_2 h_2 + \cdots + c_{s-1} h_{s-1} + c_s h_s + \cdots + c_n h_n = 0,$$

so $c_1 h_1 + \cdots + c_{s-1} h_{s-1} = 0$. Since at least one of $c_1, c_2, \ldots, c_{s-1}$ is nonzero, the $s-1$ columns $h_1, h_2, \ldots, h_{s-1}$ of H are linearly dependent.

→

($\Rightarrow$) Suppose there is a set of $s-1$ columns of H that are linearly dependent over F. Without loss of generality, let them be $h_1, h_2, \ldots, h_{s-1}$. So, $\exists\ \lambda_i \in F$, not all 0, such that

$$\lambda_1 h_1 + \lambda_2 h_2 + \cdots + \lambda_{s-1} h_{s-1} = 0.$$

Let $c = (\lambda_1, \lambda_2, \ldots, \lambda_{s-1}, 0, \ldots, 0) \in V_n(F)$. Then $c \in C$ since $Hc^T = \lambda_1 h_1 + \lambda_2 h_2 + \cdots + \lambda_{s-1} h_{s-1} = 0$. But $1 \le w(c) \le s-1$, so $1 \le d(C) \le s-1$. □

COROLLARY Let H be a PCM for a linear code C over F. Then $d(C)$ is the smallest number of columns of H that are linearly dependent over F.

EXAMPLE In the example on slide 64, $F = \mathbb{Z}_3$ and $H = \begin{bmatrix} 2 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{bmatrix}$.

- No single column of H is l.d. over $\mathbb{Z}_3$ (i.e. no zero column), so $d(C) \geq 2$.

- No two columns of H are l.d. over $\mathbb{Z}_3$ (i.e. scalar multiples of each other), so $d(C) \geq 3$.

- There exist three columns of H that are l.d. over $\mathbb{Z}_3$:

$$\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} - 2\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \text{ so } d(C) \not\geq 4.$$

- Hence $d(C) = 3$.

EXAMPLE Let H be a PCM for a binary linear code C.

1) $d(C) = 1$ iff H has a zero column.

2) $d(C) = 2$ iff H has no zero column, and two columns of H are identical.

3) $d(C) = 3$ iff the columns of H are nonzero and distinct, and some column of H is the sum of two other columns.

4) etc.

EXAMPLE Find a $(7,4,3)$-binary code C. (n, k, d)

SOLUTION Construct a PCM for C: $H = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]_{3\times 7}$.

Then a GM for C is $\left[\begin{array}{ccc|c} 1 & 1 & 0 & \\ 0 & 1 & 1 & \\ 1 & 0 & 1 & I_4 \\ 1 & 1 & 1 & \end{array}\right]_{4\times 7}$.

C has $n=7$, $k=4$, $d=3$, $q=2$, $M=16$.

NOTE C is a Hamming code of order 3 over $\mathbb{Z}_2$.

V3d HAMMING CODES

- Hamming codes are an infinite family of single-error correcting codes discovered by Richard Hamming in 1950.

- EXAMPLE Recall that $H = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$ is a PCM for a $(7,4,3)$-binary code C, called the Hamming code of order 3 over $\mathbb{Z}_2$.

DEFINITION A Hamming code of order r over $F = GF(q)$ is an (n,k)-code over F with $n = \frac{q^r-1}{q-1}$ and $k = n-r$, and with PCM H_r, an $r \times n$ matrix whose columns are nonzero, and no two of whose columns are scalar multiples of each other.

EXAMPLE A PCM for a Hamming code of order 3 over $\mathbb{Z}_3$ is:

$$H_3 = \left[\begin{array}{ccc|ccc|c|ccc|ccc} 1&0&0&1&1&0&1&2&1&0&1&1&2 \\ 0&1&0&1&0&1&1&1&0&2&1&2&1 \\ 0&0&1&0&1&1&1&0&2&1&2&1&1 \end{array}\right]_{3\times 13}.$$

$n = 13$
$k = 10$
$d = 3$

NOTES (Hamming codes)

1) If $v \in V_r(F)$, $v \neq 0$, then exactly one nonzero scalar multiple of v must be column of H_r, giving $n = (q^r-1)/(q-1)$ columns in total.

2) H_r has rank r, since among the columns of H_r are scalar multiples of the unit vectors. Hence Hamming codes of order r over GF(q) do indeed have dimension $n-r$.

3) By design, Hamming codes of order r over GF(q) have distance 3, and so are single-error correcting codes.

DECODING SINGLE-ERROR CORRECTING CODES

- Let H be a PCM for an (n,k,d)-code C over F with $d \geq 3$.

DEFINITION Suppose $c \in C$ is sent and $r \in V_n(F)$ is received. The error vector is $e = r - c$ (so $r = c + e$).

EXAMPLE Over $\mathbb{Z}_3$: If $c = 100101$ and $e = 020000$, then $r = 120101$.

KEY OBSERVATIONS

1) $Hr^T = H(c+e)^T = Hc^T + He^T = He^T$ (since $Hc^T = 0$).
2) If $e = 0$, then $He^T = 0$. (The converse is not true.)
3) If $w(e) = 1$, say $e = (0, \ldots, 0, \alpha, 0, \ldots, 0)$ (α in the i^{th} position), then $He^T = \alpha h_i$, where

h_i is the i^{th} column of H. (The converse is not true.)

DECODING ALGORITHM FOR SINGLE-ERROR CORRECTING CODES

INPUT PCM H and a received word $r \in V_n(F)$.

1) Compute $s = Hr^T$.
2) If $s=0$, then accept r as the transmitted word (so $e=0$); STOP.
3) Compare s with the columns of H. If $s = \alpha h_i$ for some i, then set $e = (0, \ldots, 0, \alpha, 0, \ldots, 0)$, and decode to $c = r - e$; STOP.
   (i^{th} position)
4) Report that more than one error has occurred.

CORRECTNESS If $w(e)=0$ or $w(e)=1$, the decoding algorithm is guaranteed to make the correct decision.

EXAMPLE Consider the $(7,4,3)$-binary Hamming code with PCM

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{3\times 7}.$$

Suppose that $r = 0111110$.

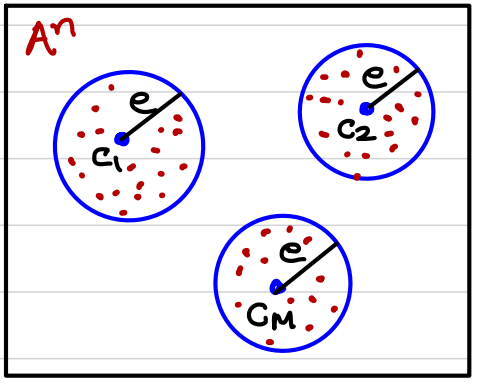
We compute $s = Hr^T = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$, which is the 6^{th} column of H.

So, we set $e = (0000010)$ and decode r to $c = r - e = 0111100$.

6^{th} position

CHECK Verify that $Hc^T = 0$.

V3e Perfect Codes



DEFINITION Let C be an $[n, M]$-code of distance d over A, with $|A| = q$ and $e = \lfloor \frac{d-1}{2} \rfloor$. Then C is perfect if each $x \in A^n$ is in the sphere of radius e centered at some $c \in C$.

- Equivalently, C is perfect if $$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n.$$

- For fixed q, n, d, a perfect code has maximum possibe M. In other words, a perfect code has maximum possible rate $R = \frac{\log_q M}{n}$ for fixed q, n, d.

- **EXAMPLE** $C = A^n$ is a (trivial) perfect code with distance $d = 1$.
- **EXAMPLE** Let n be odd. Then $C = \{\underbrace{000\cdots0}_{n}, \underbrace{111\cdots1}_{n}\}$ is a perfect binary code with distance n.

  PROOF Let $e = (n-1)/2$. Then

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = 2\left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}\right]$$

$$= \left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{e}\right] + \left[\binom{n}{e+1} + \binom{n}{e+2} + \cdots + \binom{n}{n}\right] \quad \left[\text{since } \binom{n}{k} = \binom{n}{n-k}\right].$$

$$= (1+1)^n = 2^n. \quad \square$$

- **EXERCISE** Prove that every perfect code has odd distance.
- **EXERCISE** Show that IMLD = CMLD for perfect codes.

EXAMPLE All Hamming codes of order r over $GF(q)$ are perfect.

PROOF We have $n = \frac{q^r - 1}{q-1}$, $k = n - r$, $d = 3$, $e = 1$.

Now, $M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^k \left[\binom{n}{0} (q-1)^0 + \binom{n}{1} (q-1)^1 \right]$

$$= q^k [1 + n(q-1)]$$

$$= q^{n-r} \left[1 + \frac{q^r - 1}{q-1} (q-1) \right]$$

$$= q^n. \quad \square$$

CLASSIFICATION OF PERFECT CODES

THEOREM (Tietäväinen, 1973) The only perfect codes are:

1) $V_n(GF(q))$ [trivial codes].
2) The binary replication codes of odd lengths.
3) The Hamming codes, and all codes with the same $[n, M, d]$ parameters.
4) The $(23, 12, 7)$-binary Golay code C_{23}, and all codes equivalent to it [see V4a].
5) The $(11, 6, 5)$-ternary Golay code and all codes equivalent to it.

A GM for this code is

$$G = \left[\begin{array}{c|ccccc} & 1 & 1 & 1 & 1 & 1 \\ & 0 & 1 & 2 & 2 & 1 \\ I_6 & 1 & 0 & 1 & 2 & 2 \\ & 2 & 1 & 0 & 1 & 2 \\ & 2 & 2 & 1 & 0 & 1 \\ & 1 & 2 & 2 & 1 & 0 \end{array}\right]. \quad 6 \times 11$$

V3f Syndrome Decoding

Let C be an (n,k)-code over $F=GF(q)$ with PCM H.

DEFINITION Let $x,y \in V_n(F)$. We write $x \equiv y \pmod{C}$ if $x-y \in C$.

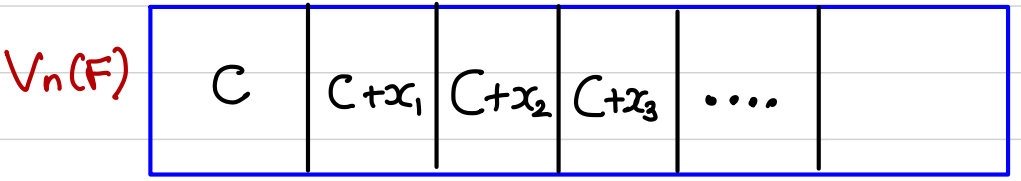
FACTS 1) $\equiv \pmod{C}$ is an equivalence relation.

2) The set of equivalence classes partitions $V_n(F)$.

3) The equivalence class containing $x \in V_n(F)$ is

$$C+x = \{y \in V_n(F) : y \equiv x \pmod{C}\} = \{c+x : c \in C\},$$

and is called a coset of C.



EXAMPLE (cosets) Consider the (5,2)-binary code C with GM $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$.

Find all cosets of C.

SOLUTION The cosets of C are:

$C = C + 00000 = \{00000, 10111, 01110, 11001\} = C + 10111 = C + 01110 = C + 11001.$

$C + 10000 = \{10000, 00111, 11110, 01001\} = C + 00111 = C + 11110 = C + 01001.$

$C + 01000 = \{01000, 11111, 00110, 10001\}.$

$C + 00100 = \{00100, 10011, 01010, 11101\}.$

$C + 00010 = \{00010, 10101, 01100, 11011\}.$

$C + 00001 = \{00001, 10110, 01111, 11000\}.$

$C + 10100 = \{10100, 00011, 11010, 01101\}.$

$C + 10010 = \{10010, 00101, 11100, 01011\}.$

FACTS (cosets)

1) $C + 0 = C$.
2) If $y \in C + x$, then $C + y = C + x$.
3) All cosets of C have the same size, namely $|C| = q^k$.
4) The number of distinct cosets is q^{n-k}.

DEFINITION Let H be a PCM for an (n,k)-code C over F. Let $x \in V_n(F)$. The syndrome of x (w.r.t. H) is $s = Hx^T$.

NOTES 1) $s \in V_{n-k}(F)$.

2) All codewords have syndrome 0.

THEOREM Let $x, y \in V_n(F)$. Then $x \equiv y \pmod{C}$ iff $Hx^T = Hy^T$. So, cosets are characterized by their syndromes.

PROOF We have $x \equiv y \pmod{C}$ iff $x - y \in C$ iff $H(x-y)^T = 0$ iff $Hx^T = Hy^T$. □

DECODING Recall that $c \in C$ is sent and $r \in V_n(F)$ is received. The (unknown) error vector is $e = r - c$. Since $r - e = c$, we have $r \equiv e \pmod{C}$. Thus, r and e are in the same coset of C.

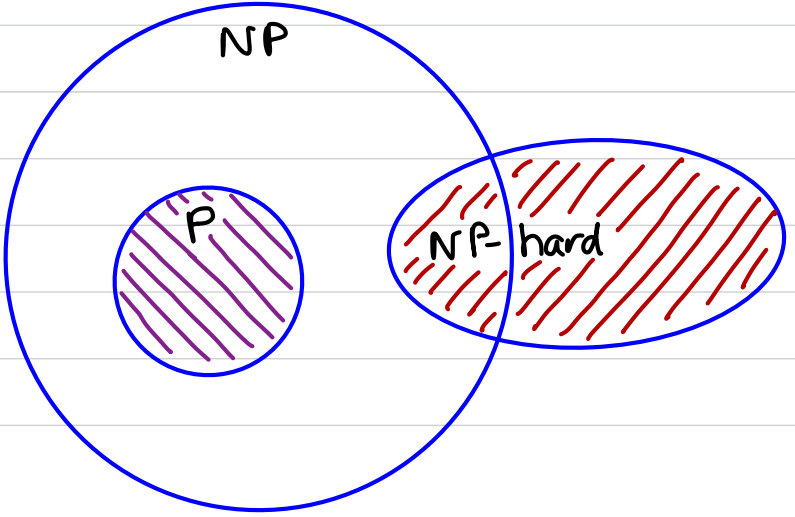
DECODING STRATEGY Given r, find a vector e of smallest weight that has the same syndrome as r: $He^T = Hr^T$.

CMLD: Decode r to $c = r - e$.

IMLD: If e is unique, decode r to $c = r - e$; else reject r.

QUESTION Given H and r, can one efficiently find a vector e of smallest weight such that $He^T = Hr^T$? [syndrome decoding problem]

FACT This problem is NP-hard, which strongly suggests that no general-purpose efficient algorithm exists.



If any NP-hard problem can be solved efficiently, then all problems in NP can be solved efficiently, so "P = NP".

SYNDROME DECODING ALGORITHM (CMLD)

SETUP For each coset of C, select an arbitrary vector of smallest weight in that coset, and call it the coset leader of that coset. Store a table of coset leaders and their syndromes.

coset leader	syndrome

q^{n-k} rows

DECODING ALGORITHM (CMLD)

Given $r \in V_n(F)$, compute $s = Hr^T$. Let the corresponding coset leader be e. Then decode r to $c = r - e$.

NOTE The decoding algorithm is guaranteed to make the correct decision if the error vector is a coset leader; otherwise, it is guaranteed to make an incorrect decision.

SELECTING COSET LEADERS

THEOREM Let C be an (n, R, d)-code over F. Let $x \in V_n(F)$ be a vector of weight $\leq \lfloor \frac{d-1}{2} \rfloor$. Then x is a coset leader.

PROOF Suppose y is in the same coset as x, with $y \neq x$ and $w(y) \leq w(x) \leq \lfloor \frac{d-1}{2} \rfloor$. Then $x \equiv y \pmod{C}$, so $x - y \in C$ and $x - y \neq 0$. But

$$w(x-y) = w(x+(-y)) \leq w(x) + w(-y) = w(x) + w(y) \leq \lfloor \tfrac{d-1}{2} \rfloor + \lfloor \tfrac{d-1}{2} \rfloor \leq d-1.$$

This contradicts $d(C) = d$, so no such y exists.
Hence, x is the unique vector of smallest weight in its coset, so must be a coset leader. □

EXAMPLE (syndrome decoding for the code on slide 82)

- For the (5,2)-binary code C with GM $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$, we have a PCM $H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$. Note that $d(C) = 3$.

- SYNDROME TABLE

coset leader	syndrome
00000	000
10000	111
01000	110
00100	100
00010	010
00001	001
10100	011
10010	101

DECODING

- Suppose $r = 11011$.
- Compute $s = Hr^T = 010$.
- The corresponding coset leader is $e = 00010$.
- Decode r to $c = r - e = 11001$.

NOTE Syndrome decoding is not efficient in general since the syndrome table is exponentially large.
For an (n,k)-binary code, the syndrome table has size

$$2^{n-k}\big(n + (n-k)\big) = \boxed{2^{n-k}(2n-k) \text{ bits.}}$$

2^{n-k}: # cosets; n: coset leader; $(n-k)$: syndrome

[Actually, only $2^{n-k}n$ bits are needed since the table can be sorted by syndrome, and then the syndromes do not need to be stored.]