Math 127, Wed Mar 17

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 6.4, 7.1. For Mon: 7.2–7.3.
- PS06 outline due Wed night, full version due Mon.
- Problem session Fri Mar 19, 10am–noon.
- **Exam 2 in one week**, on 3.5–3.6, 4.2–4.3, 5.3–5.6, and 6.1–6.4 (PS04–06). Review session Mon night (recorded to YouTube).

The Hamming 7-code $\mathcal{H}_7$

$\mathcal{H}_7$ is the nullspace of the parity check matrix

$$H_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Col i of H_7 is the binary digits of the number i (written backwards/upwards).

$[1\ 1\ 0\ 1\ 1\ 1\ 0]^T = y$

- Data bits x_3, x_5, x_6, and x_7, and

$$x_1 = x_3 + x_5 + x_7$$
$$x_2 = x_3 + x_6 + x_7$$
$$x_4 = x_5 + x_6 + x_7.$$

- Transmit $\mathbf{x}$, receive $\mathbf{y}$.
- Let $\mathbf{s} = H_7\mathbf{y} \in \mathbf{F}_2^3$. syndrome of y
  If $\mathbf{s} = \mathbf{0}$, $\mathbf{y} \in \mathcal{H}_7$;
  else $\mathbf{s}$ is binary digit of bit to correct.

An example

Msg: 0110
$\;\;\;\;\;\;\;\;\;\;$ 3 5 6 7

$x_1 = 0+1+0 = 1$

$x_2 = 0+1+0 = 1$

$x_4 = 0+1+1 = 0$

Transmit $\underline{x} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \underline{y}$ Rec'd

$H\underline{y} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \longrightarrow 100 = 4$
bin.

Fix bit 4.

How to mult mat·vec (mod 2)

$$\begin{array}{c} H_7 \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \\ \begin{matrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{matrix} \end{array} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \begin{array}{l} \text{two 1s} \\ \text{two 1s} \\ \text{three 1s} \end{array}$$

Take the l.c. of columns of H_7 corresponding to the coefficients of the vector.

Extension: The Hamming 8-code $\mathcal{H}_8$

$\mathcal{H}_8$ is defined to be the nullspace of the parity check matrix

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

All $\underline{x} \in \mathbb{F}_2^8$ s.t. $H_8 \underline{x} = \underline{0}$

Note:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \leftarrow H_7$$

So to be consistent with the Hamming 7-code, we write $\mathbf{x} \in \mathcal{H}_8$ as

$$\mathbf{x} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_7 \end{bmatrix}.$$

So the last three rows of parity check matrix H_8 say precisely that bits x_1...x_7 are a codeword from Hamming 7.

Key properties of $\mathcal{H}_8$

Theorem

The Hamming 8-code $\mathcal{H}_8$ is the Hamming 7-code $\mathcal{H}_7$, extended by a parity check bit x_0; and $\mathcal{H}_8$ corrects 1 error and detects 2 errors.

See PS06.

Hamming 8-code is often used in ECC plug-in memory:

Generalizations?

Can we find other, similar codes, but maybe better?

Definition

An $[n, k, d]$ **binary code** is a binary linear code $\mathcal{C}$ such that:

- $\mathcal{C}$ has length n; # of bits in each codeword
- $\dim \mathcal{C} = k$; and # of vectors in a basis for C = # of data bits in the message m
- d is the smallest number of nonzero coordinates appearing in a nonzero codeword of $\mathcal{C}$.

The numbers n, k, and d are called the **length**, **dimension**, and **minimum distance** of **C**, respectively. $\mathcal{C}$

Examples

$\text{Null}([1 \cdots 1])$

Example: Parity check code of length $n+1$.

$[n+1, n, 2]$ high dim, less EC

$\text{Span}\left(\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}\right)$

Example: Repetition code of length n.

$[n, 1, n]$ low dim, more EC

Example: Hamming code $\mathcal{H}_7$.

$[7, 4, 3]$ min dist 3

$\Rightarrow \frac{3-1}{2}$ EC $= 1$

Example: Hamming code $\mathcal{H}_8$.

$[8, 4, 4]$

An IDEA: Look at a code using geometry

Ex: x = 1100101
y = 0011011

So d(x,y) = 6.

Definition

$\mathbf{x}, \mathbf{y} \in \mathbf{F}_2^n$; **Hamming distance** between $\mathbf{x}$ and $\mathbf{y}$ is:

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= \text{the number of coordinates in which } \mathbf{x} \text{ and } \mathbf{y} \text{ differ} \\ &= \text{the number of nonzero coordinates in } \mathbf{x} - \mathbf{y} \\ &= \text{the number of coordinate changes needed to go from } \mathbf{x} \text{ to } \mathbf{y}. \end{aligned}$$

Hamming weight $\mathrm{wt}(\mathbf{x})$ is the number of nonzero coordinates of $\mathbf{x}$, i.e.:

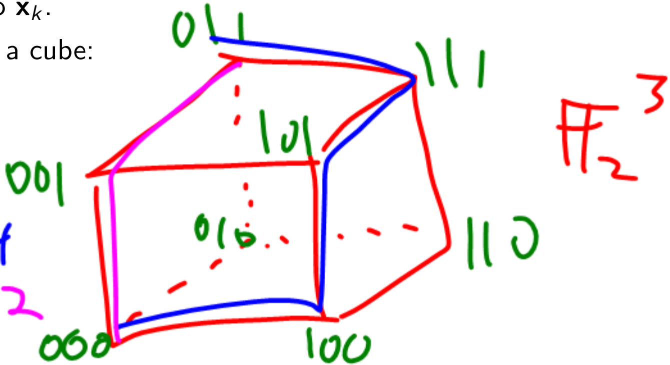
$$\mathrm{wt}(\mathbf{x}) = d(\mathbf{x}, 0), \qquad d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y}).$$

Why is Hamming distance a distance?

Definition

A **Hamming path of length** k in $\mathbf{F}_2^n$ is a sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbf{F}_2^n$ such that for $1 \leq i \leq k$, the vectors $\mathbf{x}_{i-1}$ and $\mathbf{x}_i$ differ in exactly one coordinate (i.e., $\mathbf{x}_i - \mathbf{x}_{i-1}$ has exactly one nonzero coordinate). We also say that the path $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_k$ goes from $\mathbf{x}_0$ to $\mathbf{x}_k$.

Picture in a cube:



— len 4

— len 2

Hamming distance is a path distance

Theorem

For $\mathbf{x}, \mathbf{y} \in \mathbf{F}_2^n$, the Hamming distance $d(\mathbf{x}, \mathbf{y})$ is precisely the length of a shortest Hamming path from $\mathbf{x}$ to $\mathbf{y}$.

Proof: Can only change one coord in each step of a Hamming path, so the length of a Hamming path from x to y is at least d(x,y).

Conversely, by changing one coordinate at a time, we can get from x to y in a path of length d(x,y).

Consequence: Distances to any codeword $\mathbf{x}$ are same as distances to $\mathbf{0}$, so if d is **minimum distance**

$$d = \min \{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}\},$$

then d is smallest distance between any two codewords in $\mathcal{C}$.

Hamming distance is a metric

Definition

A **metric** on a set X is a function $d : X \times X \to \mathbf{R}$ (i.e., two inputs in X, output is a real number) that satisfies the following four axioms for all $x, y, z \in X$:

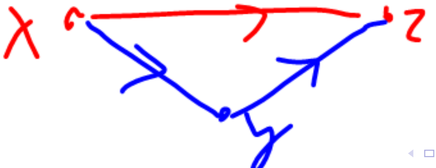
1. $d(x, y) \geq 0$.
2. $d(x, y) = 0$ if and only if $x = y$.
3. $d(x, y) = d(y, x)$.
4. (Triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$.

No shortcuts thru third location y.

Theorem

Hamming distance $d(\mathbf{x}, \mathbf{y})$ is a metric on $\mathbf{F}_2^n$.

Proof of triangle:



If the red path is shortest path from x to z, then d(x,y)+d(y,z) can't be < d(x,z), otherwise there would be a shorter path.

Nearest neighbor correction

(Lookup table algorithm)

Xavier transmits $\mathbf{x}$, Yolanda receives $\mathbf{y}$.

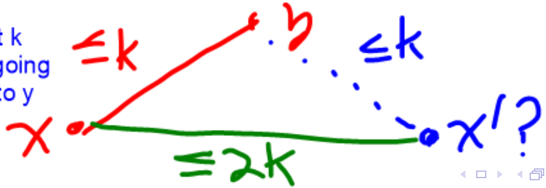
- If there is a unique $\mathbf{y}' \in \mathcal{C}$ such that $d(\mathbf{y}, \mathbf{y}')$ is minimized, we correct $\mathbf{y}$ to $\mathbf{y}'$. (E.g., if $\mathbf{y} \in \mathcal{C}$, then $\mathbf{y}' = \mathbf{y}$ minimizes $d(\mathbf{y}, \mathbf{y}')$, as $d(\mathbf{y}, \mathbf{y}) = 0$.)
- If there is more than one vector $\mathbf{y}' \in \mathcal{C}$ such that $d(\mathbf{y}, \mathbf{y}')$ is minimized, we state that $\mathbf{y}$ has been detected as an erroneous transmission, but cannot be corrected.

Theorem

Let $\mathcal{C}$ be a binary linear code with minimum distance d. Then the nearest neighbor method, applied to $\mathcal{C}$, corrects $\lfloor (d-1)/2 \rfloor$ errors and detects $\lfloor d/2 \rfloor$ errors.

Proof of correction: Assume $d = 2k+1$, so $k = (d-1)/2$.

At most k errors going from x to y



But shortest dist between two codewords is at most 2k+1. So nearest nbr x unique.

Ideals

Maybe the most important definition in ring theory:

Definition

Let R be a (commutative) ring. An **ideal** of R is $I \subseteq R$ s.t.:

1. (Zero) The zero element of R is contained in I.
2. (Closed under addition) If $x, y \in I$, then $x + y \in I$.
3. (Closed under R-multiplication) If $x \in I$ and $r \in R$, then $rx \in I$.

For a ring R:

- The set $\{0\}$ is an ideal of R called the **zero ideal**.
- R is an ideal of itself.

More interesting examples

Let $R = \mathbf{Z}$, $I = \{3n \mid n \in \mathbf{Z}\}$.

Classes of examples

R a ring.

- For fixed $a \in R$, the set

$$(a) = \{ra \mid r \in R\}$$

  is called the **principal ideal generated by** a.
- For fixed $a, b \in R$, the set

$$(a, b) = \{ra + sb \mid r, s \in R\}$$

  is called the **ideal generated by** a **and** b.
- For F a field and $a \in F$, the set

$$I_a = \{f(x) \in F[x] \mid f(a) = 0\}$$

  is an ideal of $F[x]$.