Today

- Administrivia
- Introduction

4 test cases

CSS.318.1

Coding Theory

Lecture 1 (2022-8-29)

Instructor: Prahladh Harsha.

Administrivia:

Grading Policy: 4 problem sets - 80%

Project / Paper Presentation - 20%
/ Final Exam

Coding Theory:

Error Correcting Codes

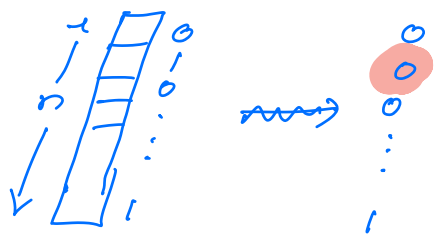
- Shannon (1948)
- Hamming (1950)

Toy Examples:

Example 1: Guessing Hats Game

Example 2: Hamming's Problem

- Store n bits
- Corruptions happen (not exactly.
  (at most t corruptions) $t \ll n$.
  $(0 \to 1, 1 \to 0)$
- $n = 63$; $t = 1$ corruptions



Questions:
How to handle corruptions

① Detection:
2^{n-1} strings
w/ parity bit

② Recovery

Example 2a Data Centers

n bits

n data centers

$n = mt$

$\leq l$ local corruptions

$\leq g$ - global corruptions

$l >> g$

Example 3: Secret Sharing.

n - parties.

- Share a secret among n people.
- t or more people should be able to recover secret using their share
- (t-1) or less - cannot recover

(t-1) vs t . 55.

Example 4: Pool testing

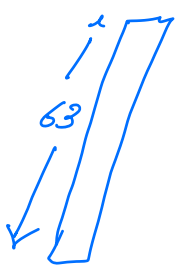
n = 384 health workers

48 tests

detected 4 positive among 384

Return to Hamming's Problem

n = 63 ; t = 1

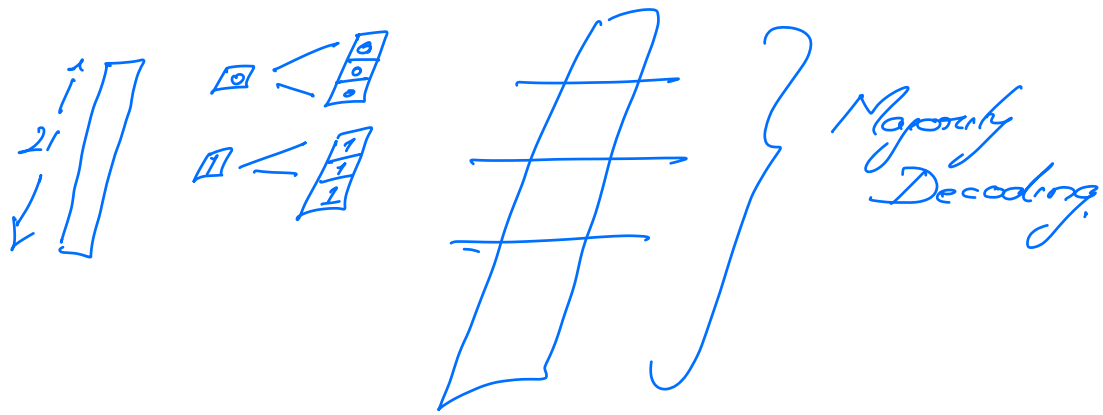


- Store 63 bits
- Atmost one corruption

0 → 1 } but don't know
1 → 0 } location of corruption.

Qn: What is the max # of strings that can be stored on device such that it can be recovered?

Soln 1: Repeat each bit 3 times



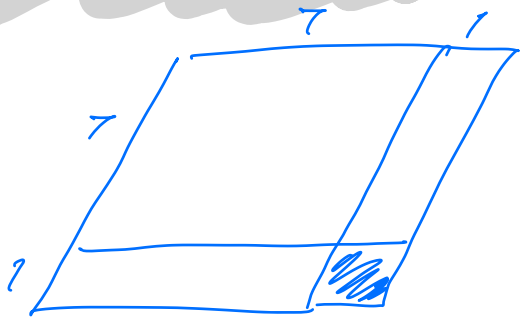
Encoding / Decoding – simple.

Store 21 "message" bits in 63 bits

$$\text{Rate} = \frac{\text{message length}}{\text{block length}} = \frac{21}{63} = \frac{1}{3}$$

Qn: Can one do better than 1/3?

Soln 2: View 63 locations as 8×8 less corner

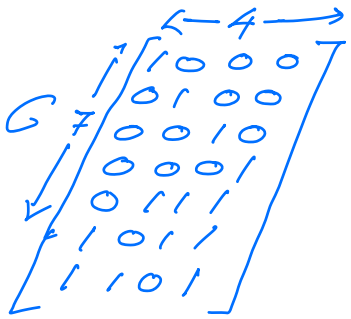


message - 7×7

$$\text{Rate} = \frac{49}{63} \checkmark$$

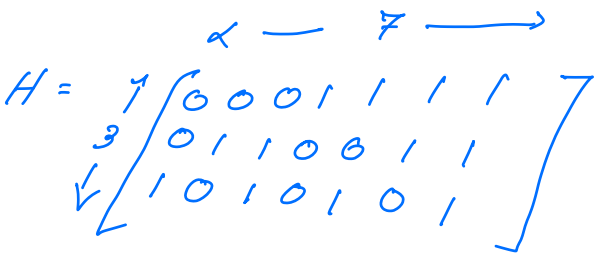
Qn: Can one do even better?

Soln 3*: Starters scale down $n=63$ to $n=7$ yet. $t=1$



$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{bmatrix} \longmapsto Gm$$

$$m \in \{0,1\}^4 \longmapsto \{0,1\}^7$$



Surprising Observations:

1. $\forall\, m_1 \neq m_2 \in \{0,1\}^4$, Gm_1 & Gm_2 differ in at least 3 locations

   [will prove later]

2. $y \in \{0,1\}^7$

   Suppose y is Gm for some $m \in \{0,1\}^4$

   or $Gm + e_i$ for some $m \in \{0,1\}^4$ & $i \in [4]$

then $Hy = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$ Magically $b_1 b_2 b_3 = \bar{0}$, $\Rightarrow$ no errors

else $b_1 b_2 b_3$ – index of the corrupted bit

[will prove later]

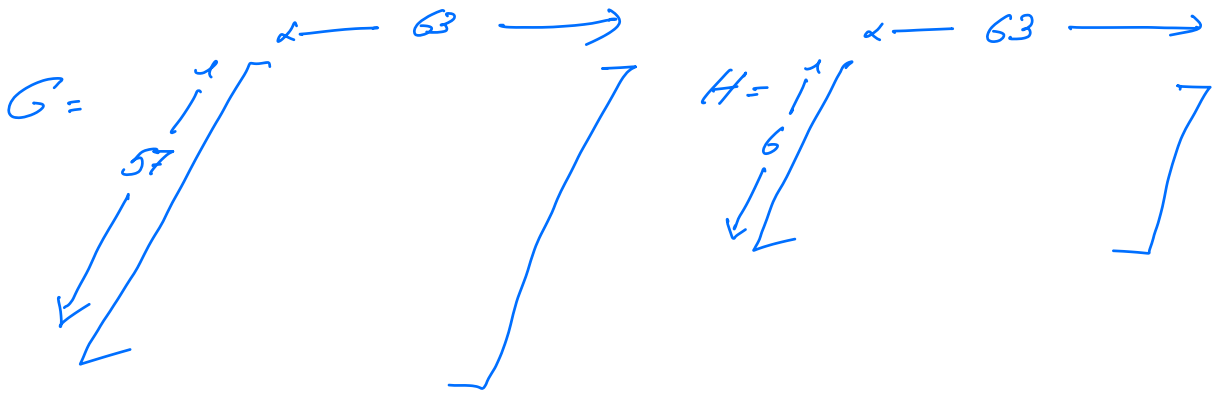
Rate = $4/7$.

To extend to 63, naively just repeat 9 times

Rate = 4/7

Soln 3. [Hamming Soln].

Constructed 2 matrices



— Properties [will prove later]

1. $\forall m_1 \neq m_2 \in \{0,1\}^{57}$, $Gm_1 \neq Gm_2$ differ in ≥ 3 location

2. $y \in \{0,1\}^{63}$ obtained by corrupting at most one bit

Hy - index of the corrupted bit.

— Rate = $\frac{57}{63}$

[Hamming] cannot do any better

—

Hamming:

① Constructed a Code

② Limitations of any code that has property

③ Efficient Decoding Alg.

④ Relates to the halts problem

} Broad Outline of the rest of the course