EE5350 Error Correcting Codes

Course webpage:

https://people.iith.ac.in/shashankvatedka/html/courses/2022/EE5350/course_details.html

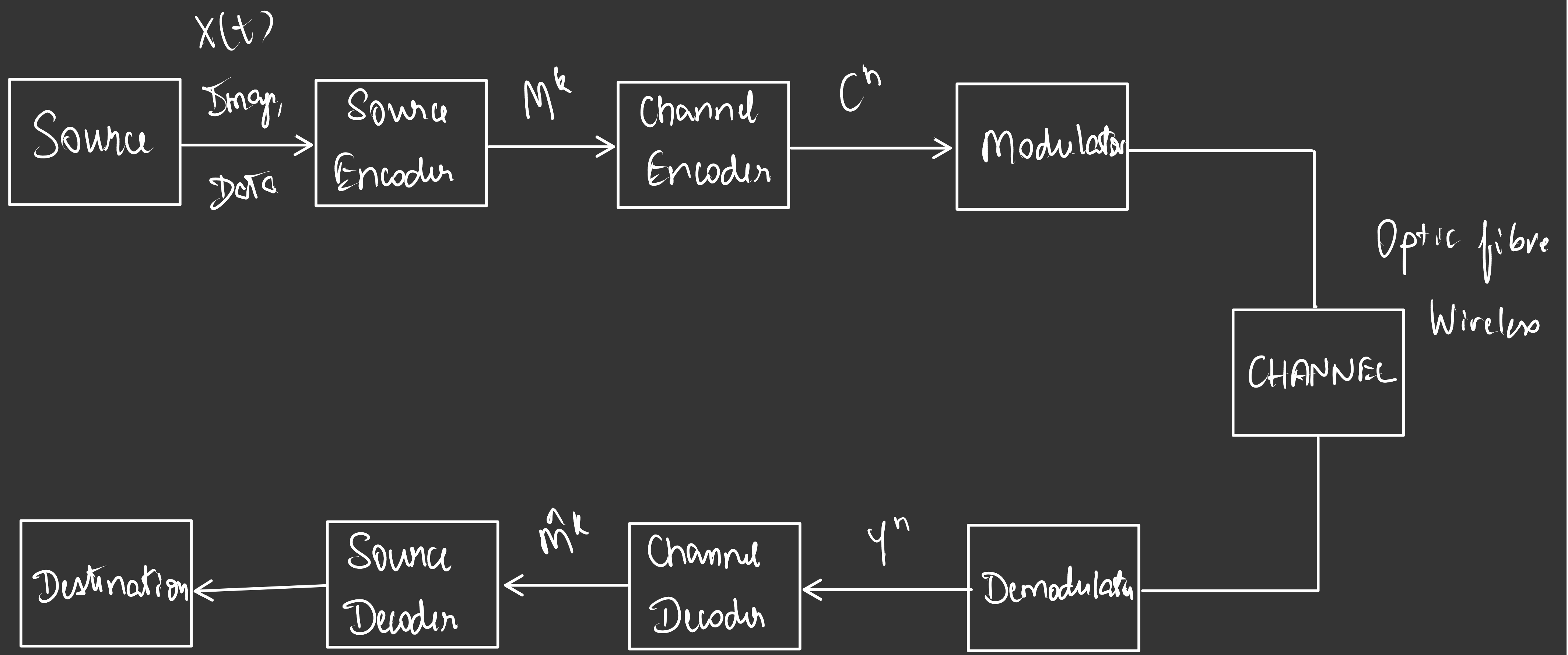
Homework submissions/announcements:

Google classroom

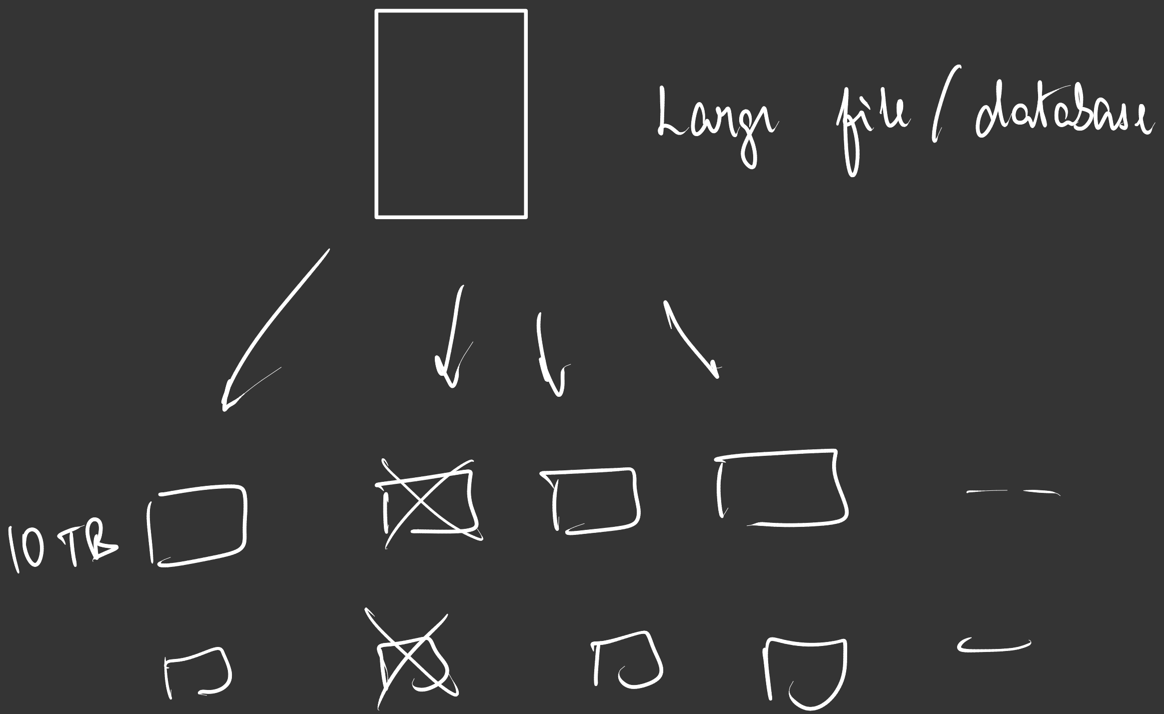
You should take this course if:

1. You like math & programming
2. You are interested in storage/communication systems, or
3. You are interested in theoretical computer science/cryptography

Example 1: Digital communication system



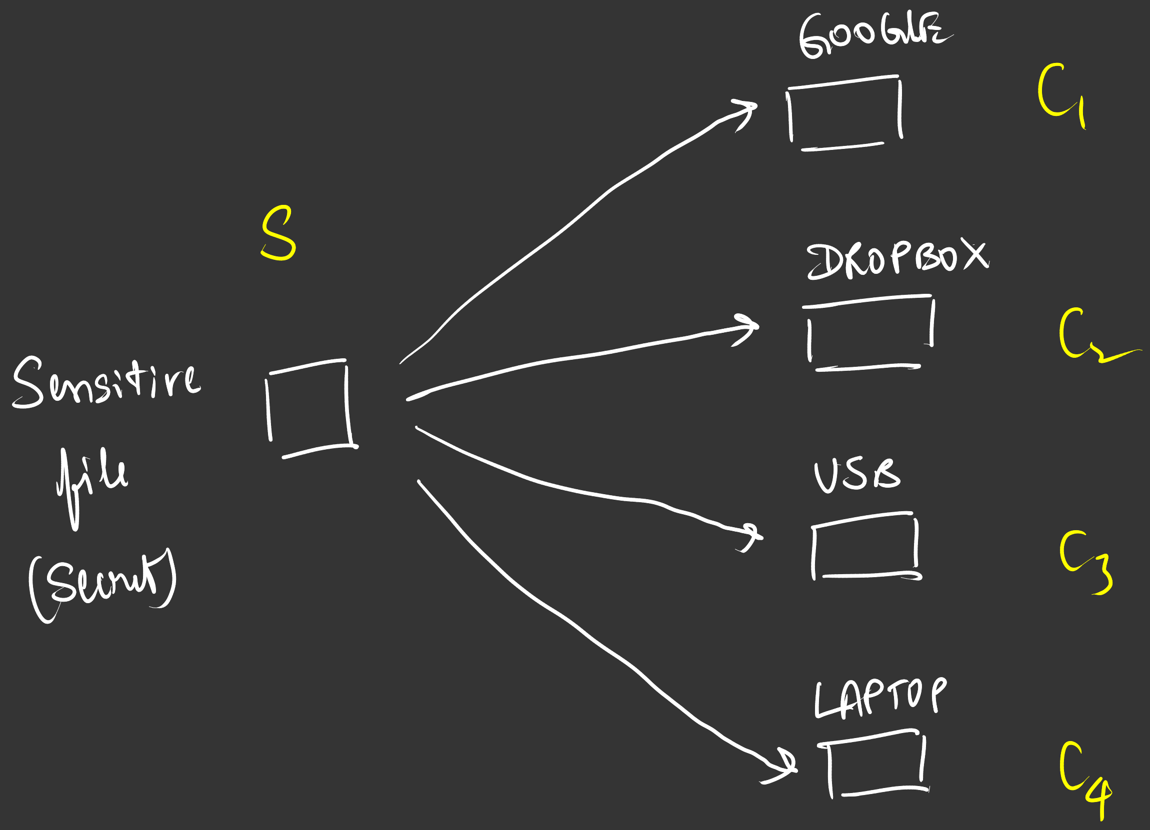
Example 2: Distributed storage systems



RAID

Example 3: Bar codes/QR codes/CDs/DVDs/blue-ray discs

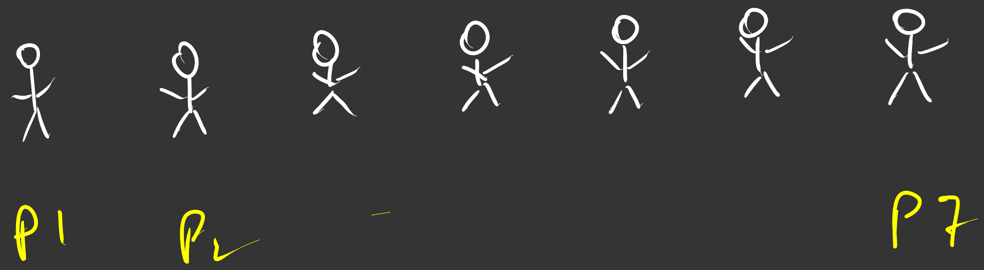
Example 4: Secret sharing



① S can be recovered from any 3 of $\{C_1, C_2, C_3, C_4\}$

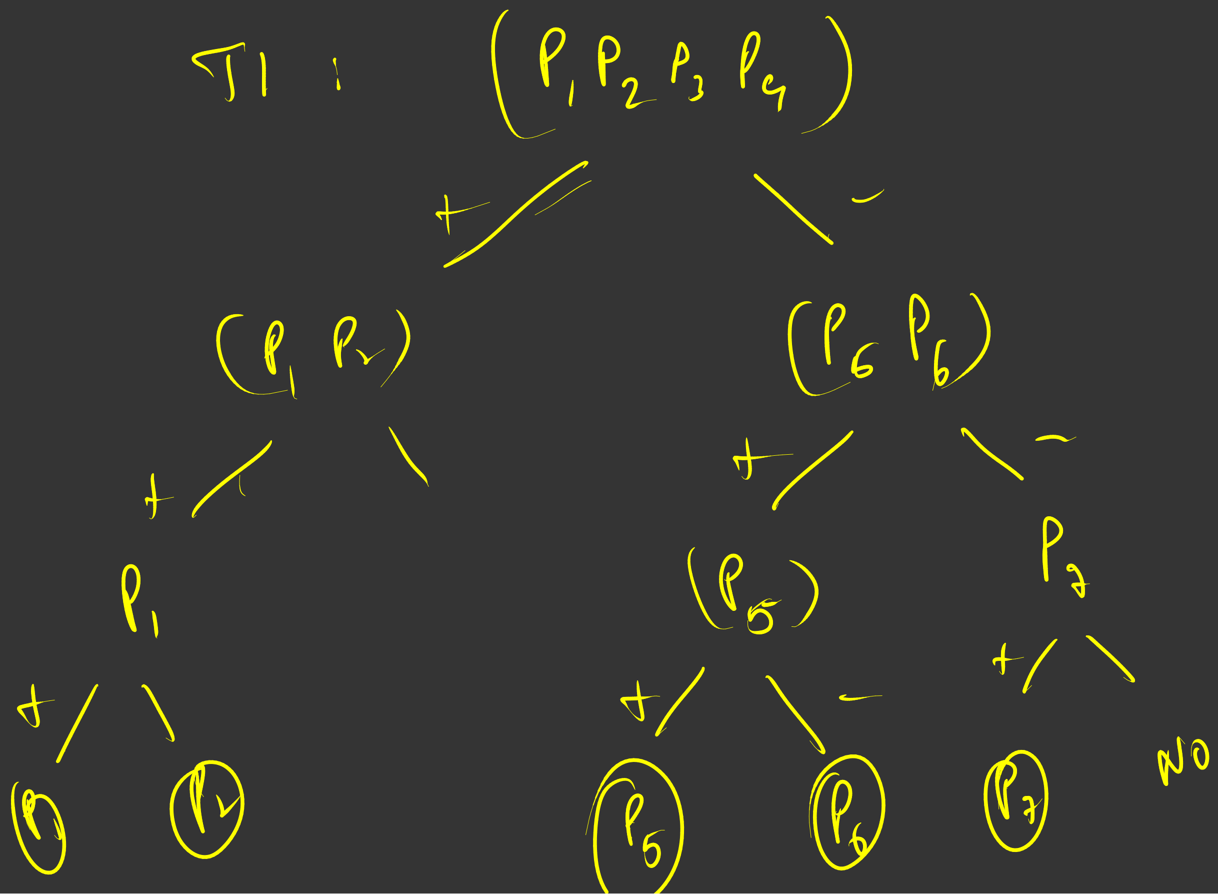
② Any 2 of $\{C_1, C_2, C_3, C_4\}$ gives NO info about S

Example 5: Group testing



≤ 1 infected

Only 3 testing kits.



$$
\begin{array}{c|c}
\begin{array}{c} T_1 \\ T_2 \\ T_3 \end{array} &
\begin{bmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{bmatrix} \\
 & \begin{array}{ccccccc} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 \end{array}
\end{array}
$$

$(7, 4, 3)$ Hamming Code

$$\begin{array}{cc}
\begin{matrix} T_1 \\ T_2 \\ T_3 \end{matrix} &
\begin{bmatrix}
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1
\end{bmatrix} \\
 & \begin{matrix} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 \end{matrix}
\end{array}$$

Example 6: Cryptography

- Postquantum cryptosystems based on ECCs
- Basic idea:
  * Decoding random codes is hard
  * Specific codes can be decoded efficiently

... and many others (hashing, compressed sensing, etc.)

The basic model

Causes errors /

Introduces "NOISE"

Message

k-bit

$\{1, 2, --, M\}$

$m_i \in \mathcal{M}$

Codeword

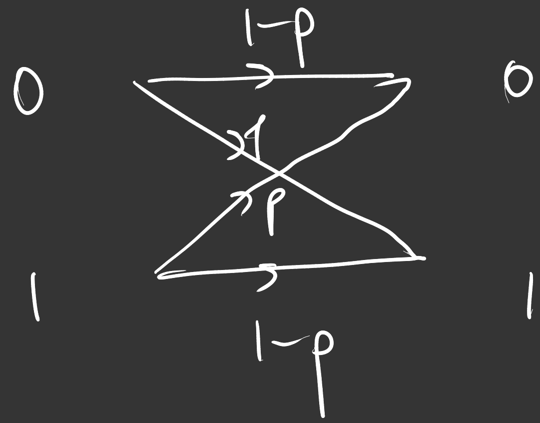
$X_i \in \mathbb{F}$

Rate : $R = \dfrac{\log|\mathcal{M}^k|}{\log|\mathbb{F}^n|}$

(Some use $\dfrac{\log|\mathcal{M}^k|}{n}$)

Example channel 1: Binary symmetric channel

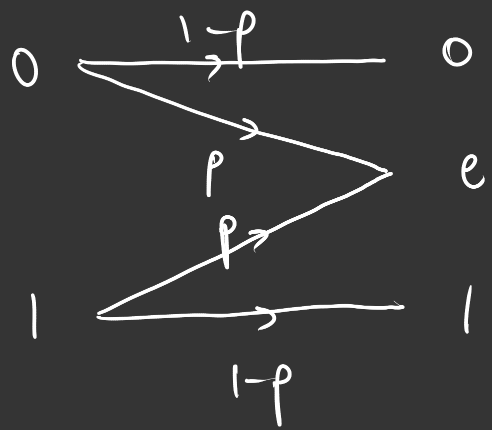
BSC(p)



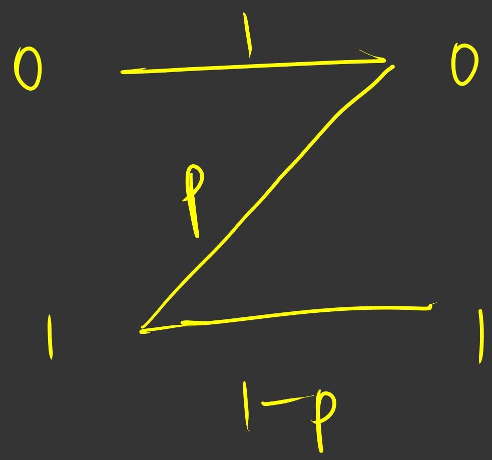
0	1	0	1	1
↓	↓	↓	↓	↓
1	0	0	1	1

Example channel 2: Binary Erasure Channel

BEC(p)

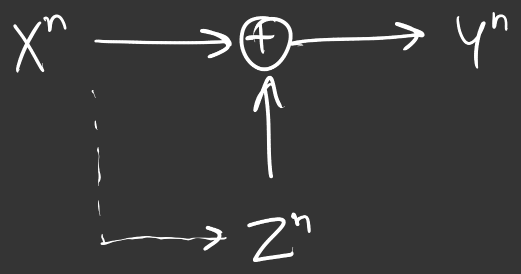


0 0 1 1



0
1
0
p
1
1
1-p

Example channel 3: Adversarial bit-flip channel



$\#$ of 1's in $Z^n \le np$.

$m^k = \underline{01101}$

1 0 1 0 1 1 0

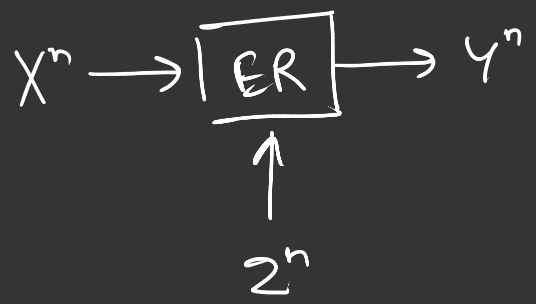
For $i = 1, 2, 3 \ldots n$

$Y_i = X_i \oplus Z_i$

Adversarial

BSC : $Z_i \sim$ iid $\mathrm{Ber}(p)$

Example channel 4: Adversarial erasure channel



\# of locations erased $\leq np$.

1 0 1 0 1 1

(n, M) block code

(Codebook)

Definition: An (n, M) block code over $\mathcal{Y}$ is a set $C \subseteq \mathcal{Y}^n$

s.t. $|C| = M$.

Each $c^n \in C$ is called a codeword.

$n \rightarrow$ Code length / blocklength

$M \rightarrow$ Code size.

Encoder

Given an (n, M) code C over $\mathbb{F}_q$, an encoder is a mapping from $\{1, 2, \ldots, M\}$ to C.

$$\text{ENC} : \{1, 2, \ldots, M\} \to C$$

$(3, 4)$

C

$1 \longmapsto 000$

$2 \longmapsto 010$

$3 \longmapsto 111$

$4 \longmapsto 100$

Linear encoders:

Those for which $C^n = AM^k$ for some matrix A.

(Not all codes have linear encoders)

			C_1	C_2
m_1	00	$\mapsto$	000	000
m_2	01	$\mapsto$	110	100
m_3	10	$\mapsto$	111	001
m_4	11	$\mapsto$	100	101

$C_2 + C_3 = C_4$

$Am_2 + Am_3 = Am_4$

$A(m_2 + m_3)$

Decoder

For an (n, M) code over $\mathcal{X}$ & a channel with input alphabet $\mathcal{X}$ & output alphabet $\mathcal{Y}$, a decoder is a map from $\mathcal{Y}^n$ to C.

$$\mathrm{DEC}: \mathcal{Y}^n \to C$$

C (3, 2) code

$0 \longmapsto 000$

$1 \longmapsto 111$

$\mathcal{Y}^n$

$000 \to 000$

$001 \to 000$

$010 \to 000$

$100 \to 000$

$011 \to 111$

$101 \to 111$

$110 \to 111$

$111 \to 111$

$000 \to 0$

$111 \to 1$

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

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

A : Generator matrix of C

Maximum likelihood decoder and MAP decoder

Channel : $p(y^n | x^n)$

$p_{Y^n|X^n}$: Channel transition pmf.

ML decoder : Given $y^n \in \mathcal{Y}^n$, $\quad x^*_{ML} = \underset{x^n \in \mathcal{C}}{\arg\max}\; p(y^n | x^n)$

Maximum A-posteriori Probability (MAP) : Given $y^n \in \mathcal{Y}^n$, $\quad x^*_{MAP} = \underset{x^n \in \mathcal{C}}{\arg\max}\; p(x^n | y^n)$

BSC(p):

000

111

$y^n = (y_1\ y_2\ y_3)$

Given y^n, $x^*_{ML} = \underset{x^n \in \{000, 111\}}{\arg\max}\ p(y^n | x^n)$

$= p(y^n | 000)$ or $p(y^n | 111)$

$p(y^n | 000) = p^k (1-p)^{n-k}$ if y^n has k 1's

Generate x^n, y^n

$p(y^n | x^n) =$

x^n 0 1 0 1 1

$\downarrow \quad \downarrow \qquad\qquad \downarrow$ $\qquad k = 3$

y^n 1 0 0 1 0

$$p(y^n | x^n) = p^k (1-p)^{n-k}$$

If # of 1's in $y^n = k$,

$$C = \begin{Bmatrix} 0\,0 \cdots 0 \\ 1\,1 \cdots 1 \end{Bmatrix}$$

$$p(y^n | 0 \cdots 0) = p^k (1-p)^{n-k}$$

$$p(y^n | 1 \cdots 1) = p^{n-k} (1-p)^k$$

$p < \frac{1}{2}$, $\quad \hat{x}_{ML} = \begin{cases} 0\,0 \cdots 0 & \text{if } \operatorname{maj}(y^n) = 0 \\ 1 \cdots 1 & \text{if } \operatorname{maj}(y^n) = 1 \end{cases}$

Declare $(0\cdots0)$ if $p(y^n|0\cdots0) > p(y^n|1\cdots1)$

$\Leftrightarrow p^k(1-p)^{n-k} > p^{n-k}(1-p)^k$

$$\left(\frac{p}{1-p}\right)^k > \left(\frac{p}{1-p}\right)^{n-k}$$

If $p<\frac{1}{2}$, $\underbrace{\frac{p}{1-p}}_{\alpha} < 1$

$\alpha^k > \alpha^{n-k} \Leftrightarrow n-k > k$ # of 0's > # of 1's

$p > \frac{1}{2}$, $\frac{p}{1-p} > 1$ # of 1's > # of 0's

$\Leftrightarrow k > n-k$

MAP decoder:

$$x^*_{MAP} = \underset{x^n \in C}{\arg\max}\ p(x^n | y^n)$$

$$= \underset{x^n \in C}{\arg\max}\ \frac{p(y^n | x^n)\, p(x^n)}{p(y^n)}$$

$$= \underset{x^n \in C}{\arg\max}\ p(y^n | x^n)\, p(x^n)$$

$= x^*_{ML}$ if all $x^n \in C$ are equiprobable.

$$\left\{ \underline{p(y^n \mid x^n(1))}\ \underline{p(x^n(1))},\quad \underline{p(y^n \mid x^n(2))}\ \underline{p(x^n(2))},\ \ldots \right\}$$

Error detection and correction capability

For a code C, (& a decoder DEC), we say that C is

k- error correctable (error correcting capability is k)

if :

$DEC(y^n) = x^n$ as long as at most k

symbols are replaced.

$\forall \; x^n \in C$

$$y = \{0, 1, 2\}$$

$$C = \begin{Bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 2 \end{Bmatrix}$$

$$\begin{matrix} 2 & 1 & 2 \end{matrix}$$

$$\begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$$

$$\begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{Bmatrix}$$

Defn: A code C has an error detection capability of k (C can detect k errors) if any sequence of $\leq k$ substitution errors do not result in a valid codeword.

The Hamming distance

$d_H(x^n, y^n)$ is the number of coordinates in which x^n & y^n differ

$wt_H(x^n) = d_H(0^n, x^n)$ is called the Hamming weight of x^n

$$
\begin{array}{lccccc}
x^n: & 1 & 0 & 1 & 1 & 0 \\
y^n: & 0 & 1 & 0 & 0 & 0 \\
z^n: & e & 1 & 0 & e & 1
\end{array}
$$

$d_H(x^n, y^n) = 4$

$d_H(y^n, z^n) = 3$

Substitution errors:

x^n 0 1 0 1 1 0

y^n 0 $\underline{0}$ 0 $\underline{0}$ 1 $\underline{1}$

$$y^n = x^n \oplus w^n$$

$$w^n = 0\ 1\ 0\ 1\ 0\ 1$$

Given $\underline{\text{any}}$ $x^n, y^n \in \{0,1\}^n$

we can write $y^n = x^n \oplus w^n$

$(w^n = x^n \oplus y^n)$

Moreover, $wt_H(w^n) = d_H(x^n, y^n)$

$$\begin{tikzcd} x^n \arrow[r] \arrow[dr, dashed] & \oplus \arrow[r] & y^n \\ & w^n \arrow[u] & \end{tikzcd} \quad , \; wt_H(w^n) \leq \ell$$

Adversarial error channel

* A code C is ℓ-error correctable if $\exists$ a decoder that can recover x^n from y^n as long as $wt_H(w^n) \leq \ell$ or $d_H(x^n, y^n) \leq \ell$, $\forall x^n \in C$

* A code C is ℓ-error detectable if $x^n \oplus w^n \notin C \setminus \{x^n\}$ as long as $wt_H(w^n) \leq \ell$.

Defn Minimum distance of a code:

$$d_{min}(C) = \min_{\substack{x^n, y^n \in C \\ x^n \neq y^n}} d_H(x^n, y^n)$$

Suppose C can detect l errors.

$$l < d_{min}(C)$$

$$\begin{array}{l} c_1 \\ c_2 \\ c_3 \end{array} \left\{ \begin{array}{ccccc} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array} \right\}$$

$c_1 \oplus [0\ 1\ 0\ 1\ 1] = c_3$

$c_1 \oplus [0\ 1\ 0\ 1\ 0] = [0\ 0\ 0\ 1\ 0]$

$c_3 \oplus [0\ 0\ 0\ 0\ 1] = [0\ 0\ 0\ 1\ 0]$

* $d_{min}(C) = 3 \longrightarrow$ code

* For every $x^n \in C$

$$d_H(x^n, y^n) \leq 1 \longrightarrow \text{Channel}$$

Decoder: Minimum Hamming distance decoder

- Compute $d_H(y^n, c^n) \quad \forall c^n \in C$
- Choose the c^n that minimizes the

$$\hat{x}^n = \underset{c^n \in C}{\arg\min}\ d_H(c^n, y^n)$$

What can we say abt $d_H(c^n, y^n)$ for $c^n \in C \setminus \{x^n\}$

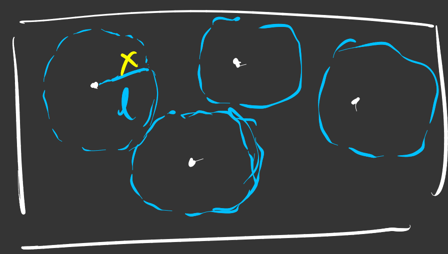
$$3 \le d_H(c^n, x^n) \le d_H(x^n, y^n) + d_H(y^n, c^n)$$

$$d_H(y^n, c^n) \ge 3 - d_H(x^n, y^n)$$

$$\ge 3 - 1 = 2$$

If $l \ge d_{min}/2$!

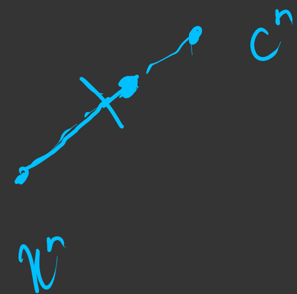
$\exists\ x^n, c^n$ st $d_H(x^n, c^n) = d_{min}$



$e^n = x^n \oplus c^n$ $\qquad wt_H(e^n) = d_{min}$

$y^n = \tilde{e}^n + x^n$ $\qquad d_H(y^n, x^n) = l$

$d_H(y^n, c^n)$



☆ # of errors that C can correct $< d_{min}/2$

The Hamming distance is a metric

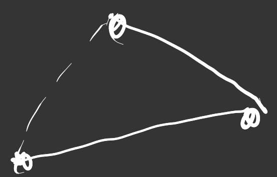
Metric : $d : \mathcal{Y}^n \times \mathcal{Y}^n \to \mathbb{R}$ is a metric if

① $d(x^n, y^n) \geq 0 \quad \forall\, x^n, y^n \in \mathcal{Y}^n$

& $d(x^n, y^n) = 0$ iff $x^n = y^n$

② $d(x^n, y^n) = d(y^n, x^n)$

③ $d(x^n, y^n) \leq d(x^n, z^n) + d(z^n, y^n) \quad \forall\, x^n, y^n, z^n$



The Hamming distance is a metric

Prop. 1 & 2 are easy

Prop 3: For every x^n, y^n, z^n,

$$d_H(x^n, z^n) \le d_H(x^n, y^n) + d_H(y^n, z^n)$$

$d_H(x^n, z^n)$: min # substitutions req to go from x^n to z^n

$$\begin{tikzcd}
x^n \arrow[rr, "\text{sub}"] \arrow[dr] & & z^n \\
& y^n \arrow[ur] &
\end{tikzcd}$$

The parity code

$$(n, M) = (k+1, 2^k)$$

Message

$$(m_1, m_2, \dots, m_k) \longrightarrow (m_1, m_2, \dots, m_k, m_1 \oplus m_2 \oplus \dots \oplus m_k)$$

Q: ① What is d_{min} for the parity code?

② What is the error detection/correction capability.

The repetition code

n — # repetitions

$$m \longmapsto m, m, m, \ldots m$$

$$(n, 2)$$

Q: ① What is d_{min}?

② What is the error detection/correction capability.

Proposition: Given a code C, the following are equivalent:

① $d_{min}(C) = d \geq 2$

② If d is odd, then C can correct $\frac{d-1}{2}$ errors

③ C can detect $d-1$ errors

④ C can correct $d-1$ erasures.

0 1 e e 1

1 e e 0 0

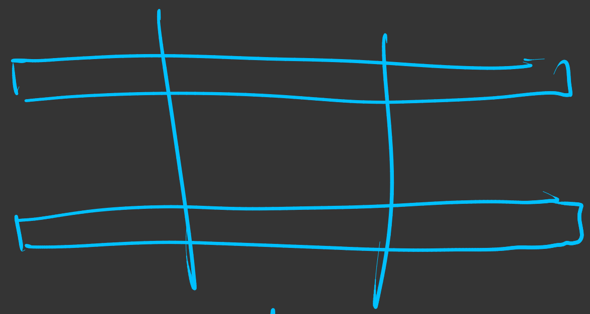
$$\left\{ \begin{matrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{matrix} \right\}$$

① - ③ : clear

④ : Declare C^n if $\exists$ unique $C^n \in C$ matching in unerased locations

Take any c_1^n, c_2^n

$$d_H(c_1^n, c_2^n) \geq d$$



l

If $\tilde{c}_1^n$ $\tilde{c}_2^n$ are obtained by erasing l locations

$$d_H(\tilde{c}_1^n, \tilde{c}_2^n) \geq d-l$$

Any erasure pattern of $l \leq d-1$ erasures can be corrected

$$\left\{ \begin{matrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{matrix} \right\}$$

$0 \quad 1 \quad 0$

In general, Suppose $d-1$ loc are erased.

& $\exists \ \underline{c}_1, \underline{c}_2$ which match in all unerased locations

$$n-(d-1) = n-d+1$$

$$\Rightarrow d_H(\underline{c}_1, \underline{c}_2) \leq d-1$$

The Hamming code

$$(m_1, m_2, m_3, m_4) \longmapsto (m_1, m_2, m_3, m_4, m_2 \oplus m_3 \oplus m_4, m_1 \oplus m_3 \oplus m_4, m_1 \oplus m_2 \oplus m_4)$$

What is a field?

$(\mathbb{F}, \oplus, \cdot)$

$\oplus : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

$\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

Addition & multiplication:

$\forall a, b \in \mathbb{F}$

1. Closure $a \oplus b \in \mathbb{F}$ & $a \cdot b \in \mathbb{F}$

2. Commutativity $a \oplus b = b \oplus a$ & $a \cdot b = b \cdot a$

3. Associativity $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ & $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

4. Existence of identity $\exists\, 0, 1 \in \mathbb{F}$ st

$a \oplus 0 = a$ $\quad a \cdot 1 = a \quad \forall a \in \mathbb{F}$

5. Existence of inverse

$\forall a \in \mathbb{F}, \exists\, \bar{a} \in \mathbb{F}$ st $a \oplus \bar{a} = 0$ & $\forall a \in \mathbb{F} \setminus \{0\}, \exists\, a^{-1}$

$a \cdot a^{-1} = 1$

Others

Distributivity

$a \cdot (b \oplus c) = (a \cdot b) \oplus (a \cdot c)$

Which of the following are fields?

1. $(\mathbb{R}, +, \cdot)$ is a field

2. $(\mathbb{Q}, +, \cdot)$ is a field

3. $(\mathbb{Z}, +, \cdot)$ No (3 does not have a multiplicative inverse)

4. $(\mathbb{R} \setminus \mathbb{Q}, +, \cdot)$ Not closed under $\cdot$

5. $(\mathbb{C}, +, \cdot)$ Yes

(6) $(\mathbb{Z}_q, \oplus_q, \odot_q)$ $\quad q \in \mathbb{Z}$ $\quad$ Set of integers modulo-q

$$\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$$

$$a \oplus_q b = [a+b] \bmod q$$

$$a \odot_q b = [ab] \bmod q$$

$\mathbb{Z}_2$

XOR

$\oplus$	0	1
0	0	1
1	1	0

AND

$\odot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Additive inverse:

$\mathbb{Z}_q$

For any $a \in \mathbb{F}_q$

$$a \oplus_q \bar{a} = 0$$

Happens if $[a + \bar{a}] \bmod q = 0$

$$a + \bar{a} = qm \quad \text{for } m \in \mathbb{Z}$$

$$0 \leq a + \bar{a} \leq 2(q-1)$$

$$\Rightarrow \boxed{\bar{a} = q - a}$$

β

$\bar{\alpha} = \gamma$

$\bar{\gamma} = \alpha$

$\oplus$	α	β	γ
α	γ	α	β
β	α	β	γ
γ	β	γ	α

α

$\alpha^{-1} = \alpha$

$\gamma^{-1} = \gamma$

$\odot$	α	β	γ
α	α	β	γ
β	β	β	β
γ	γ	β	α

Multiplicative inverse

$a \odot_q a^{-1} = 1$

$[a\, a^{-1}] \bmod q = 1$

$a a^{-1} = mq + 1$

Suppose that $q = 4$

$2 \cdot a^{-1} = m \times 4 + 1$

$\therefore \mathbb{Z}_4$ is not a field

$q = 15$

$a = 3$

$3 a^{-1} = m \times 15 + 1$

Suppose q is composite

then $q = \alpha\beta$ for $\alpha, \beta \in \{0, 1, \ldots q-1\}$

$$\alpha\alpha^{-1} = mq + 1$$
$$= m\alpha\beta + 1$$

$\Rightarrow$ α does not have an inverse.

$\Rightarrow$ $(\mathbb{Z}_q, \oplus_q, \odot_q)$ is NOT a field.

HW: Prove that $\mathbb{Z}_q$ is a field for prime q.

(f) Set of all polynomials (coeff from $\mathbb{R}$)

$$\{ \quad x(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots) \neq 1$$

NOT a field.

Eg 1 $\{0, 1, x, 1+x\}$

$\oplus$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\odot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

$\{0, 1, 1+x, x\}$ mod $(1+x+x^2)$

mod $(1+x^2)$

8. Set of all $n \times n$ matrices

No

9) $\left\{ \begin{bmatrix} x & -y \\ y & x \end{bmatrix} : x, y \in \mathbb{R} \right\}$ with st matrix addition & multiplication

Closure

Identity $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Inverse

Commutativity

$$\begin{bmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{bmatrix} \begin{bmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{bmatrix} = \begin{bmatrix} x_1x_2 - y_1y_2 & -(x_1y_2 + y_1x_2) \\ x_1y_2 + y_1x_2 & x_1x_2 - y_1y_2 \end{bmatrix}$$

$$\begin{bmatrix} x & -y \\ +y & x \end{bmatrix}^{-1} = \frac{1}{x^2+y^2} \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

$$(x_1, y_1) \oplus (x_2, y_2) \longmapsto (x_1 + x_2 \quad y_1 + y_2)$$

$$(x_1, y_1) \odot (x_2, y_2) \longmapsto (x_1 x_2 - y_1 y_2 \, , \, x_1 y_2 + y_1 x_2)$$

$$\begin{bmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{bmatrix} \longmapsto (x_1, y_1)$$

$$(x_1 + i y_1)(x_2 + i y_2)$$

(15) $\{x + y\sqrt{2} \; : \; x, y \in \mathbb{Q}\}$

Homework

Vector space $(V, +, \circ)$ over $(\mathbb{F}, \oplus, \cdot)$

① Commutativity $\quad \underline{v}_1 + \underline{v}_2 = \underline{v}_2 + \underline{v}_1 \quad \forall\, \underline{v}_1, \underline{v}_2 \in \mathbb{V}$

② Associativity $\quad \underline{v}_1 + (\underline{v}_2 + \underline{v}_3) = (\underline{v}_1 + \underline{v}_2) + \underline{v}_3$

③ Existence of identity element

$$\exists\, \underline{0} \in \mathbb{V} \text{ st } \underline{0} + \underline{v} = \underline{v}$$

④ Existence of inverses

$$\forall\, \underline{v} \in \mathbb{V},\ \exists\, \underline{\bar{v}} \text{ st } \underline{v} + \underline{\bar{v}} = \underline{0}$$

⑤ Compatibility of multiplications

$$b \cdot (a \cdot \underline{v}) = (b \cdot a) \cdot \underline{v} = a \cdot (b \cdot \underline{v})$$

⑥ Multiplicative identity

$$1 \cdot \underline{v} = \underline{v} \qquad 0 \cdot \underline{v} = \underline{0}$$

$$0 \cdot v + \cancel{\alpha v} = (0 + \alpha)\underline{v} = \cancel{\alpha \underline{v}}$$

1. Distributivity

(i) $(a+b)\underline{v} = a\underline{v} + b\underline{v}$

(ii) $a(\underline{v}_1 + \underline{v}_2) = a\underline{v}_1 + a \cdot \underline{v}_2$

Examples of vector spaces

(1) Set of all polynomials $(\leq k)$

(2) $\mathbb{R}^n$ over $\mathbb{R}$

$\mathbb{F}^n$ over $\mathbb{F}$

$\mathbb{C}^n$ over $\mathbb{C}$

(3) Set of all differentiable fns over $\mathbb{R}$

(4) $\mathbb{R}$ over $\mathbb{Q}$

$\sqrt{2} = \alpha \sqrt{3}$