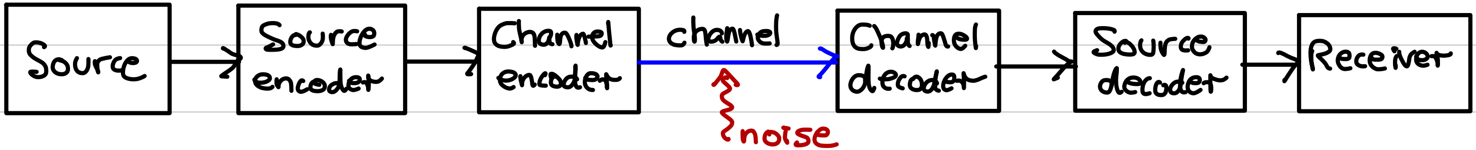
V1a Basic Definitions and Concepts



Definitions

- An alphabet A is a finite set of $q \geq 2$ symbols.
- A word is a finite sequence of symbols from A (also: vector, tuple).
- The length of a word is the number of symbols it has.
- A code C over A is a finite set of words (with $|C| \geq 2$).
- A codeword is a word in the code C.
- A block code is a code in which all codewords have the same length.
- A block code of length n containing M codewords over A is a subset $C \subseteq A^n$ with $|C| = M$. C is called an $[n, M]$-code over A.

• **EXAMPLE**

$C = \{00000, 11100, 00111, 10101\}$ is a $[5,4]$-code over $\{0,1\}$.

Source messages	Codewords
00	00000
01	11100
10	00111
11	10101

• The channel encoder only transmits codewords. However, what is received may not be a codeword.

• **EXAMPLE**

$r = 11000$ is received.

What should the channel decoder do?

ASSUMPTIONS ABOUT THE CHANNEL

(1) Only symbols from A are transmitted ("hard decision coding").

(2) No symbols are lost/added/interchanged during transmission.

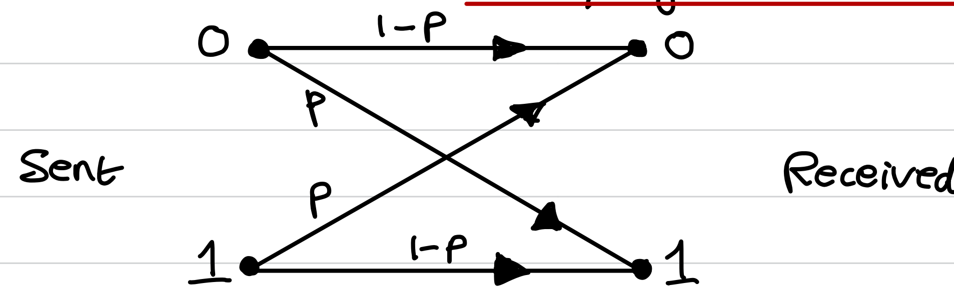
(3) The channel is a q-symmetric channel:

- Let $A = \{a_1, a_2, \ldots, a_q\}$.
- Let $X_i = i^{th}$ symbol sent.
- Let $Y_i = i^{th}$ symbol received.
- For all $i \geq 1$, $1 \leq j, k \leq q$, $Pr(Y_i = a_k \mid X_i = a_j) = \begin{cases} 1-p, & \text{if } j = k, \\ \frac{p}{q-1}, & \text{if } j \neq k. \end{cases}$

p is called the symbol error probability of the channel $(0 \leq p \leq 1)$.

BINARY SYMMETRIC CHANNEL (BSC)

- A 2-symmetric channel is called a binary symmetric channel.



- For a BSC:

  (1) If $p=0$, the channel is perfect.

  (2) If $p=1/2$, the channel is useless.

  (3) If $1/2 < p < 1$, then flipping all received bits converts the channel to a BSC with $0 < p < 1/2$.

  (4) Henceforth, we will assume that $\boxed{0 < p < 1/2 \text{ for a BSC}}$.

EXERCISE

- For a q-symmetric channel, show that one can take
$$0 < p < \frac{q-1}{q}$$
without loss of generality.
Hint: First consider the case $q=3$.

- In the remainder of the course, we shall assume that
$$\boxed{0 < p < \frac{q-1}{q}}$$

INFORMATION RATE

DEFINITION The information rate (or rate) R of an $[n,M]$-block code C over an alphabet A of size q is $R = (\log_q M)/n$.

- If C encodes messages that are the k-tuples over A (so $|C| = q^k$), then $\boxed{R = k/n.}$

- Note: $0 < R \leq 1$. Ideally, R should be close to 1.

- **EXAMPLE** The rate of the binary code $C = \{00000, 11100, 00111, 10101\}$ is $R = 2/5$.

HAMMING DISTANCE

DEFINITION The Hamming distance (or distance) between two n-tuples in A^n is the number of coordinate positions in which they differ.

THEOREM (properties of Hamming distance)

For all $x, y, z \in A^n$: (1) $d(x,y) \geq 0$, with $d(x,y) = 0$ iff $x = y$.

(2) $d(x,y) = d(y,x)$.

(3) $d(x,y) + d(y,z) \geq d(x,z)$ (Δ inequality)

DEFINITION The Hamming distance (or distance) of an $[n,M]$-code C is $d(C) = \min\{d(x,y) : x,y \in C, x \neq y\}$.

EXAMPLE The distance of $C = \{00000, 11100, 00111, 10101\}$ is $d(C) = 2$.

V1b DECODING STRATEGIES

EXAMPLE Let $C = \{00000, 11100, 00111, 10101\}$.

C is a $[5,4]$-code over $\{0,1\}$ (a binary code) with $R = 2/5$ and $d(C) = 2$.

> **ERROR DETECTION** If C is used for error detection only, the strategy is the following: A received word $r \in A^n$ is accepted iff $r \in C$.

ERROR CORRECTION Let C be an $[n, M]$-code over A with distance d.

Suppose that $c \in C$ is transmitted and $r \in A^n$ is received.

The (channel) decoder must decide one of the following:

(i) No errors have occurred; accept r.

(ii) Errors have occurred; correct (or decode) r to a codeword $c \in C$.

(iii) Errors have occurred; correction is not possible.

NEAREST NEIGHBOUR DECODING

INCOMPLETE MAXIMUM LIKELIHOOD DECODING (IMLD)

If there is a unique codeword $c \in C$ such that $d(r,c)$ is a minimum, then decode r to c. If no such c exists, then reject r (ask for retransmission or disregard the information).

COMPLETE MAXIMUM LIKELIHOOD DECODING (CMLD)

Same as IMLD, except that if there are two or more $c \in C$ for which $d(r,c)$ is minimum, decode r to an arbitrary one of these.

IS IMLD A REASONABLE STRATEGY?

THEOREM IMLD chooses the codeword $c \in C$ for which the conditional probability $P(r|c) = P(r \text{ is received} \mid c \text{ is sent})$ is largest.

PROOF Suppose $c_1, c_2 \in C$ with $d_1 = d(c_1, r)$, $d_2 = d(c_2, r)$. Suppose that $d_1 > d_2$.

Now, $P(r|c_1) = (1-p)^{n-d_1}\left(\frac{p}{q-1}\right)^{d_1}$ and $P(r|c_2) = (1-p)^{n-d_2}\left(\frac{p}{q-1}\right)^{d_2}$.

And, $\dfrac{P(r|c_1)}{P(r|c_2)} = (1-p)^{d_2-d_1}\left(\frac{p}{q-1}\right)^{d_1-d_2} = \left(\frac{p}{(1-p)(q-1)}\right)^{d_1-d_2}$.

Now, $\dfrac{p}{(1-p)(q-1)} < 1 \iff p < (1-p)(q-1) \iff p < q - pq - 1 + p \iff pq < q-1 \iff p < \frac{q-1}{q}$.

Thus, $\dfrac{P(r|c_1)}{P(r|c_2)} < 1$, so $P(r|c_1) < P(r|c_2)$, and the result follows. $\square$

MINIMUM ERROR PROBABILITY DECODING (MED)

- An ideal strategy would be to decode r to a codeword $c \in C$ for which $P(c|r) = P(c \text{ is sent} \mid r \text{ is received})$ is largest. This is MED.

- EXAMPLE (IMLD/CMLD is not the same as MED)

  Consider $C = \{\overset{c_1}{000}, \overset{c_2}{111}\}$, and suppose that $P(c_1) = 0.1$ and $P(c_2) = 0.9$.

  Suppose $p = 1/4$ (for a BSC).

  Suppose $r = 100$ is the received word.

  Then $P(c_1|r) = P(r|c_1) \cdot P(c_1)/P(r) = p(1-p)^2 \times 0.1/P(r) = \frac{9}{640} \cdot \frac{1}{P(r)}$.

  And $P(c_2|r) = P(r|c_2) \cdot P(c_2)/P(r) = p^2(1-p) \times 0.9/P(r) = \frac{27}{640} \cdot \frac{1}{P(r)}$.

  So, $\boxed{\text{MED decodes } r \text{ to } c_2,}$ whereas $\boxed{\text{IMLD decodes } r \text{ to } c_1.}$

$$\boxed{\textbf{BAYES THEOREM: } P(A \wedge B) = P(A) \cdot P(B|A) = P(B) \cdot P(A|B).}$$

IMLD/CMLD vs. MED

- **IMLD** maximizes $P(r|c)$.
- **MED** maximizes $P(c|r)$.

(i) MED has the drawback that the decoding algorithm depends on the probability distribution of source messages.

(ii) If all source messages are equally likely, then CMLD and MED are identical: $P(c_i|r) = P(r|c_i) \cdot \frac{P(c_i)}{P(r)} = P(r|c_i) \cdot \frac{1}{\underbrace{M \cdot P(r)}_{\text{does not depend on } i}}$.

(iii) In practice, IMLD/CMLD is used.

$\boxed{\text{In this course, we will use IMLD/CMLD.}}$

V1c Error Correcting and Detecting Capabilities

Detection only

STRATEGY If r is received, then accept r iff $r \in C$.

DEFINITION A code C is an e-error detecting code if the decoder always makes the correct decision if e or fewer errors per codeword are introduced by the channel.

EXAMPLE Consider $C = \{000, 111\}$.

- C is a 2-error detecting code.
- C is not a 3-error detecting code.

THEOREM A code C of distance d is a $(d-1)$-error detecting code, but is not a d-error detecting code.

PROOF Suppose $c \in C$ is sent.

- If no errors occur, then c is received and is accepted.
- Suppose that the number of errors introduced is ≥ 1 and $\leq d-1$; let r be the received word. Then $1 \leq d(r, c) \leq d-1$, so $r \notin C$. Thus, r is rejected.
- Since $d(C) = d$, there exist $c_1, c_2 \in C$ with $d(c_1, c_2) = d$.

  If c_1 is sent and c_2 is received, the decoder accepts c_2; the d errors go undetected. $\square$

CORRECTION

STRATEGY : IMLD / CMLD

DEFINITION A code C is an e-error correcting code if the decoder always makes the correct decision if e or fewer errors per codeword are introduced by the channel.

EXAMPLE Consider $C = \{000, 111\}$.

- C is a 1-error correcting code.
- C is not a 2-error correcting code.

THEOREM A code C of distance d is an e-error correcting code, where $e = \lfloor \frac{d-1}{2} \rfloor$. ($\lfloor x \rfloor$ is the largest integer $\leq x$.)

PROOF Suppose that $c \in C$ is sent, at most $(d-1)/2$ errors are introduced, and r is received. Then $d(r,c) \leq (d-1)/2$. On the other hand, if c' is any other codeword, then

$$\begin{aligned} d(r,c') &\geq d(c,c') - d(r,c) \quad \text{(by } \Delta \text{ inequality)} \\ &\geq d - (d-1)/2 \\ &= (d+1)/2 \\ &> (d-1)/2 \geq d(r,c). \end{aligned}$$

Hence, c is the unique codeword at minimum distance from r, so the IMLD/CMLD decoder correctly concludes that c was sent. $\square$

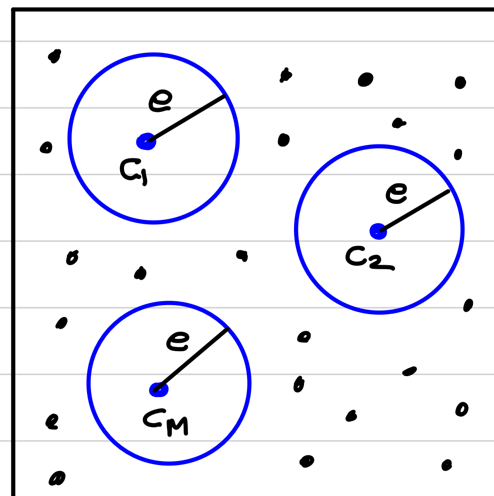
EXERCISE Suppose $d(C)=d$, and let $e=\lfloor \frac{d-1}{2} \rfloor$. Show that C is not an $(e+1)$-error correcting code.

SPHERE PACKING A natural question to ask is: Given A, n, M, d, does there exist an $[n,M]$-code C over A of distance $\geq d$?

This question can be phrased as an equivalent sphere packing problem:

> Can we place M spheres of radius $e=\lfloor \frac{d-1}{2} \rfloor$ in A^n, so that no two spheres overlap?

A^n



$C=\{c_1, c_2, \ldots, c_M\}$, $e=\lfloor \frac{d-1}{2} \rfloor$.

S_c = sphere of radius e centered at $c \in C$
= all words within distance e of c.

> We proved: If $c_1, c_2 \in C$, $c_1 \neq c_2$, then $S_{c_1} \cap S_{c_2} = \phi$.

- **QUESTION** Let $q=2$, $n=127$, $M=2^{64}$.
  Does there exist an $[n,M]$-binary code with $d \geq 21$?
  If so, can encoding and decoding be done efficiently?

- We will construct such a code in V6.
  The main tools used will be linear algebra (over finite fields) and abstract algebra (rings and fields).