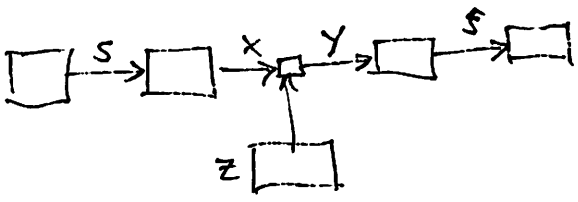
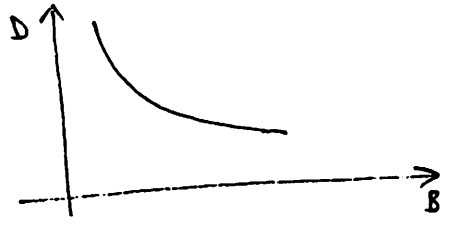
The problem of communication



$(P_S, d(S,\hat{S}), P_{Y|X}, b(X))$

$D = E[d(S,\hat{S})]$

$B = E[b(X)]$



what is the best tradeoff that can be achieved and how do we do it.

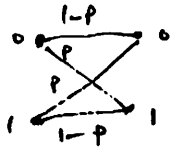
Last time we considered the setting of a binary symmetric source, so

$\mathcal{S} = \{0,1\}$, with S s.t. $\sim \text{Bern}(\frac{1}{2})$.

$$d(s,\hat{s}) = \begin{cases} 0, & s=\hat{s} \\ 1, & s\neq\hat{s} \end{cases}, \text{ Hamming distance}$$

Also the $BSC(p)$, so

$$P_{Y|X} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$



$$b(x) = \begin{cases} b_0, & x=0 \\ b_0, & x=1. \end{cases}$$

we saw that uncoded transmission achieved $(D,B) = (p, b_0)$.

is there a way to reduce the distortion by incurring more cost?

→ consider error-control codes.

A simple strategy: repeat three times and perform majority voting.

↳ repetition code

Now clearly $B = 3b_0$.

D is governed by a binomial random variable:

$$D = \sum_{k=2}^{3} \binom{3}{k} p^k (1-p)^{3-k} = 3p^2(1-p) + p^3.$$

This is less than p.

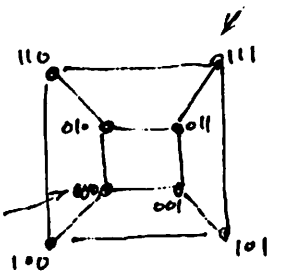
In general, as $B = n b_0$ for large n, D starts to approach 0.

So repetition coding allows one to drive the expected distortion to zero with expending more and more cost.

Are there more clever coding strategies that yield better (D, B) tradeoffs?

Better ways of introducing redundancy than just repetition?

Look geometrically in Hamming space:



Can we combine the binary symbols in an intelligent way so that every extra symbol checks whether there is error in some subset of the information-bearing symbols?

First design the optimal decoder:

inputs to channel chosen from set of binary codewords of length n.

→ since BSS, all codewords occur with equal probability.

Since errors can occur in any position, all 2^n possible sequences possible as output.

Let coded input words be $x_1, x_2, \dots, x_M$ and outputs $y_1, \dots y_{2^n}$.

optimal decoder will associate each received sequence y with a codeword x to maximize $p(x|y)$, which since all codewords are equally likely is $\max p(y|x)$.

By direct computation : $p(y|x) = p^{d_H(x,y)} (1-p)^{n-d_H(x,y)}$

Letting $d_i = d_H(x_i, y)$, it is easy to see

$$p(y|x_1) > p(y|x_2) \text{ iff } d_1 < d_2.$$

Thm: optimal decoder is minimum distance decoder.

ex: Suppose codewords are $x_1 = 00000$, $x_2 = 10011$, $x_3 = 11100$, $x_4 = 01111$ and $y = 01011$ is received.

Then decoded to x_4 since $d(x_4, y) = 1$ and $d(x_i, y) > 1$ for $i \neq 4$.

notice that distance properties of codes are quite fundamental.

Lemma: Let $x_1, x_2, \dots, x_M$ be binary codewords of length n s.t. for given positive integer e,

$$d_H(x_i, x_j) \geq 2e+1 \quad \text{for } i \neq j$$

then all single, double, ..., e-tuple errors can be corrected.

Sphere-packing bound: If a code consisting of M binary sequences of length n corrects all single, double, ..., e-tuple errors, then

$$M \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}.$$

Sphere of radius e associated with codeword x_i has

$$1 + n + \binom{n}{2} + \cdots + \binom{n}{e} = \sum_{i=0}^{e} \binom{n}{i}$$ sequences in it.

need to fit M such spheres in the space of volume 2^n.

A class of codes that are computationally easy to encode/decode are linear codes, and in particular parity check codes.

Given a set of simultaneous linear equations of the form

$$a_{11} r_1 + a_{12} r_2 + \cdots + a_{1n} r_n = 0 \pmod 2.$$
$$\vdots$$
$$a_{m1} r_1 + a_{m2} r_2 + \cdots + a_{mn} r_n = 0$$

Solutions to this are called a parity check codes where codewords lie in linear subspace of ambient space and the $n \times n$ matrix A is the parity-check matrix

Example: Hamming code.

Consider the set of all non-zero binary vectors of length 3, arrange them in columns to form a matrix

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

Consider set of vectors of length 7 in null space of A, ie.
vectors that when multiplied by A give 000.

Since A^t has rank 3, null space of A will have dimension 4, ie.

2^4 codewords.

See list.

Since set of codewords is null space of a matrix, it is linear in the sense that sum of any two codewords is also a codeword.

⇒ one can note that any two codewords differ in at least 3 places.

→ in fact the distance spectrum is equal for all codewords, and code meets the sphere-packing bound with equality (perfect code).

→ Golay code, Hamming code, repetition code are the only binary perfect codes.

The encoding/decoding operations are linear, i.e. matrix multiplication

↳ when doing by hand, use Venn diagram approach

→ demo.

How many parity checks are needed?

Gilbert-Varshamov bound: An e-tuple error correcting parity check code with words of length n may be constructed if number of check digits m satisfies:

$$2^m > \sum_{i=0}^{2e-1} \binom{n-1}{i}$$

[sufficient but not necessary]

This bound says nothing about distortion (error probability), which is more basic than # errors corrected.

→ for linear codes, multiset of distances from a given codeword to all other codewords is identical to multiset of distances from any other given codeword to all other codewords, including all-zeros codeword (which is any linear code)

→ So rather than distances, weights are sufficient.

Let A_ℓ be # of codewords of weight ℓ in linear code.

Then $(n+1)$-dimensional vector with components A_ℓ is weight distribution.

for Hamming code:

$$[1, 0, 0, 7, 7, 0, 0, 1].$$

For Hamming code, we find probability of correct reception of all-zeros codeword under minimum distance decoding is

$$(1-p)^7 + 7p(1-p)^6$$

so $\tilde{D} = 1 - (1-p)^7 - 7p(1-p)^6$, which is probability of correct word reception.

and $B = \frac{7}{4} b_0$.

more generally, let $N_\ell^h(s)$ be # of error patterns of weight h that are distance $\leq s$ from a codeword of length ℓ.

since decoding limited to p apparent errors, error probability is

$$D = \sum_{h=0}^{n} \binom{n}{h} p^h (1-p)^{n-h} \sum_{s=0}^{p} \sum_{\ell=1}^{n} A_\ell N_\ell^h(s)$$

where

$$N_\ell^h(s) = \sum_{\substack{0 \le i \le n \\ 0 \le j \le n \\ i+2j+h = s+1}} \binom{n-\ell}{j+h-\ell} \binom{\ell}{i} \binom{\ell-i}{j},$$

by combinatorics.