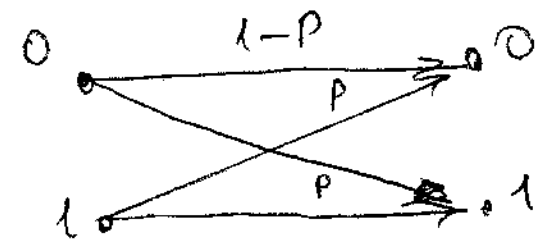
STATISTICAL DESCRIPTION OF CHANNELS (COMMUNICATION AND COMPUTATION)

q-ary symmetrical channels:

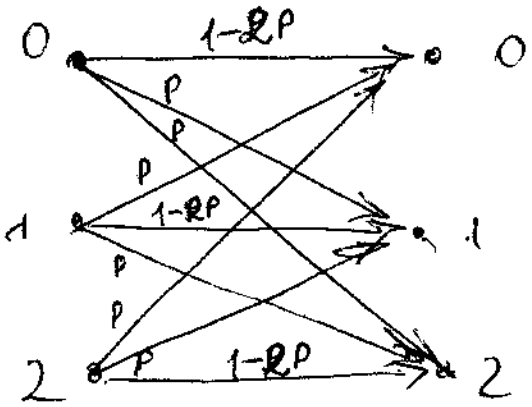
Every symbol from Z_q at the output of the channel can be distorted into any other symbol with the same probability.

EXAMPLE 1. BINARY SYMMETRICAL CHANNEL (BSC)



P is a bit distortion rate.

EXAMPLE 2 TERNARY SYMMETRICAL CHANNEL (TSC)



$q=3$

ERROR FREE $f(x)$ ACTUAL $f(x)$

FOR q-ary symmetrical channel

$$i \xrightarrow{1-(q-1)P} i \qquad i \in \mathbb{Z}_q$$

FOR BSC when $f(x) \in Z_2^n$ (n-bits in the output)

Prob. of no errors — $(1-p)^n$

Prob. of 1-bit errors (single error) — $\binom{n}{1}(1-p)^{n-1}p$

Prob. of 2-bit errors (double errors) — $\binom{n}{2}(1-p)^{n-2}p^2$

Prob. of i-bit errors — $\binom{n}{i}(1-p)^{n-i}p^i$

$(i = 0, 1, \cdots, n)$

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!} \qquad i! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots i$$

$4! = 24$.

Prob of at most ℓ errors

$$P_\ell = \sum_{i=0}^{\ell} \binom{n}{i}(1-p)^{n-i}p^i$$

EXAMPLE BSC $n=3$, $\ell=1$

$$P_1 = (1-p)^3 + 3p(1-p)^2 = (1-p)^2(1+2p)$$

FOR TSC $(q=3)$ for $f(x) \in Z_3^n$

Prob of 0 errors — $(1-2p)^n$

Prob of 1 errors — $\binom{n}{1}(1-2p)^{n-1}2p$

Prob of 2 errors — $\binom{n}{2}(1-2p)^{n-2}4p^2$

Prob of i errors — $\binom{n}{i}(1-2p)^{n-i}2^i p^i$

$(i=0,1,\ldots,n)$

For q-ary channel

Prob. of (exactly) i errors —

$$\binom{n}{i}\left(1-(q-1)p\right)^{n-i}(q-1)^i p^i$$

THE HAMMING DISTANCE in Z_q^n = $d(x,y)$

$(x \in Z_q^n, y \in Z_q^n)$

NUMBER OF PLACES where they differ.

Examples 1) $q=2$, $n=5$

$d(11011, 10001) = 2$

2) $q=3$, $n=3$

$d(011, 201) = 2$

1) $0 \leq d(x,y) \leq n$

2) $d(x,y) = 0 \Rightarrow x = y$

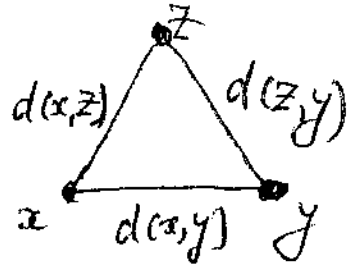
for $q=2$ $d(x,y) = n \Rightarrow x = \bar{y}$

$\bar{0} = 1$, $\bar{1} = 0$.

3) $d(x,y) = d(y,x)$

4. Δ inequality

$$d(x,z) + d(z,y) \geq d(x,y)$$



T1.

$$d(x,y)+d(z,y)+d(x,y) \leq \begin{cases} 2n, & q=2 \\ 3n, & q>2 \end{cases}$$

↑ obvious

EXAMPLE $q=3$, $n=3$

$x = 012$ $y = 101$ $z = 220$

$d(x,z)=3$, $d(z,y)=3$, $d(x,y)=3$

HAMMING DISTANCE OF CODE $C \subseteq \mathbb{Z}_q^n$

$$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y)$$

EXAMPLE: $q=2$ $n=5$ $C=\{00000, 01011, 10110, 11101\}$

$d(C)=3$

DECODING (ERROR DETECTION / ERROR CORRECTION)

SUPPOSE THAT SET OF ALL ERROR FREE OUTPUTS IS A SELECTED CODE C

$f(x) \in C$

$f(x) \xrightarrow{\text{ERROR}} \hat{f}(x)$

$f(x)$: ERROR FREE OUTPUTS OF THE CHANNEL

$\hat{f}(x)$: distorted (possibly) output. (ACTUAL OUTPUT)

TO detect errors IS SUFFICIENT TO VERIFY THAT $\hat{f}(x) \stackrel{?}{\in} C$

ERROR CORRECTION

EXAMPLE 1. BINARY CHANNEL. $q=2$ $n=5$

1) $\left(f(x) = 01011 \xrightarrow{\text{error}} 01\overset{*}{0}01 = \hat{f}(x)\right) \Rightarrow$

single error $\Leftrightarrow d(f(x), \hat{f}(x)) = 1 \Rightarrow$

Prob of this error $(1-p)^4 p$

2) $\left(f(x) = 11101 \xrightarrow{\text{error}} \overset{*}{0}1\overset{*}{0}01 = \hat{f}(x)\right) \Rightarrow$

double error $\Leftrightarrow d(f(x), \hat{f}(x)) = 2$

Prob of this error $(1-p)^3 p^2$

For $p < 1/2$ $(1-p)^4 p > (1-p)^3 p^2 \Rightarrow$

SINGLE ERRORS ARE MORE PROBABLE THAN DOUBLE ERRORS

IN GENERAL FOR $p < 0.5$

$i+1$ ERRORS ARE LESS PROBABLE THAN i ERRORS (FOR A GIVEN SET OF $i+1$ positions where all the errors occur)

EXAMPLE $C = \{00000, 01011, 10110, 11101\}$

$\hat{f}(x) = 01001$

$d(00000, \hat{f}(x)) = 2$, $d(01011, \hat{f}(x)) = 1$ $\Rightarrow$

$d(10110, \hat{f}(x)) = 5$, $d(11101, \hat{f}(x)) = 2$

$\Rightarrow$ error correction

$\hat{f}(x) = 01011$

SINCE SINGLE ERRORS ARE MORE PROBABLE THAN DOUBLE ERRORS

IN GENERAL. FOR ERROR CORRECTION:

$$\hat{f}(x) = A \iff \min_{a \in C} d(\hat{f}(x), a) = d(\hat{f}(x), A)$$

$A = f(x)$ - error free output is a codeword $A \in C$ nearest to $\hat{f}(x)$ (nearest to distorted output) $\Rightarrow$

nearest neighbour decoding = maximum likelihood decoding =

= MINIMUM distance decoding

HAMMING NORM (weight)

$$A \in Z_q^n \Rightarrow \|A\| = d(\underbrace{00\ldots0}_{n}, A)$$

$$0 \le \|A\| \le n$$

$$\|A\| = 0 \Rightarrow A = \overbrace{00\ldots0}^{n}$$

SPHERE OF RADIUS ℓ $\quad S_\ell \subseteq Z_q^n$

$$S_\ell = \{ A \mid \|A\| = \ell \}$$

BALL OF RADIUS ℓ $\quad B_\ell \subseteq Z_q^n$

$$B_\ell = \{ A \mid \|A\| \le \ell \} = \bigcup_{i=0}^{\ell} S_i$$

EXAMPLE. 1) $q=2$, $n=4$

$S_0 = \{0000\}$, $|S_0|=1$

$S_1 = \{0001, 0010, 0100, 1000\}$, $|S_1|=4$

$S_2 = \{0011, 0101, 1001, 0110, 1010, 1100\}$

$|S_2|=6$

$B_2 = S_0 \cup S_1 \cup S_2$ $\quad |B_2|=11$

EXAMPLE 2) $q=3$, $n=3$

$S_0 = \{000\}$, $|S_0|=1$

$S_1 = \{001, 002, 010, 020, 100, 200\}$, $|S_1|=6$

$S_2 = \{011, 012, 021, 022,$
$101, 102, 201, 202,$
$110, 120, 210, 220\}$ $\quad |S_2|=12$

$|B_2| = 19.$

Area of a ~~sper~~ sphere

FOR $q=2 \Rightarrow |S_\ell| = \binom{n}{\ell}$

FOR q-ary case $S_\ell \subseteq Z_q^n$

$$|S_\ell| = \binom{n}{\ell} (q-1)^\ell$$

Volume of a Ball $B_\ell = \bigcup_{i=0}^{\ell} S_i \subseteq Z_q^n$

$$|B_\ell| = \sum_{i=0}^{\ell} |S_i| = \sum_{i=0}^{\ell} (q-1)^i \binom{n}{i}$$

EXAMPLE $q=2$, $n=100$

$|S_0|=1$, $|S_1|=100$, $|S_2|=4950$ etc

$|S_0| << |S_1| \leq\!< |S_2| << \cdots$

$|B_\ell| \simeq |S_\ell|$ for large n and small ℓ.

Skin-effect:

FOR ANY $q \geq 2$ and large n

if $\ell < n/2$

$$|B_\ell| \simeq |S_\ell| \Rightarrow$$

ALMOST ALL VOLUME OF A BALL

IS CONCENTRATED NEAR ~~IT~~ ITS

SURFACE.

SPHERE OF RADIUS ℓ and center v

$$S_\ell(v) = \{ A \mid d(v, A) = \ell \} \qquad v \in Zq^n$$

$$S_\ell(v) \subseteq Zq^n$$

$S_\ell(00\ldots0) = S_\ell$

$|S_\ell(v)| = |S_\ell|$ AREA OF A SPHERE does not depend on a position of it's center.

(INVARIACE OF AREA FOR TRANSLATIONS OR SHIFTS)

BALL OF RADIUS ℓ and center v

$$B_\ell(v) = \{ A \mid d(v, A) \leq \ell \}$$

$B_\ell(00\ldots0) = B_\ell$

$|B_\ell(v)| = |B_\ell|$ - volume of a ball does not depend on a position of its center

EXAMPLE $q=2$, $n=4$, $v=1011$

$S_0(1011) = 1011$, $|S_0(1011)| = 1$

$S_1(1011) = \{0011, 1111, 1001, 1010\}$, $|S_1(1011)| = 4$

$S_2(1011) = \{1000, 1110, 0010, 1101, 0001, 0111\}$

$|S_2(1011)| = 6.$

$B_2(1011) = S_0(1011) \cup S_1(1011) \cup S_2(1011)$

$|B_2(1011)| = 11.$