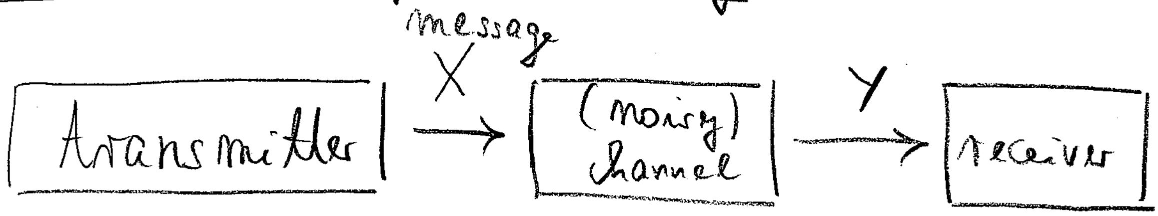
§4 Shannon capacity

Claude E. Shannon (1916–2001): founder of (mathematical) information theory.

basic model in information theory



problem: usually $Y \neq X$

goal: recover X from Y.

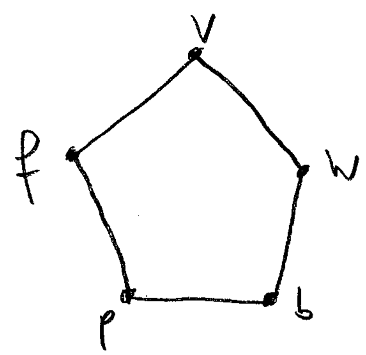
message: X sequence of symbols from alphabet V.

noisy channel: can confuse similar looking symbols.

similarity / confusion graph $G = (V, E)$

two symbols i, j can be confused $\iff \{i, j\} \in E$

example



C_5

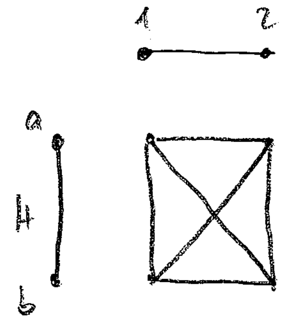
information rate for zero error communication:

$\alpha(G)$ independence number $\quad (\alpha(C_5) = 2)$.

approach to improve information rate: send more symbols at the same time, i.e. use V^k instead of V.

<u>Def. 1</u> $G = (V, E)$, $H = (W, F)$ graphs. Define the <u>strong graph product</u>

$$G \boxtimes H = (V \times W, \{\{v_1, w_1\}, \{v_2, w_2\}\} : \begin{array}{l} v_1 = v_2 \text{ and } \{w_1, w_2\} \in F \text{ or} \\ w_1 = w_2 \text{ and } \{v_1, v_2\} \in E \text{ or} \\ \{v_1, v_2\} \in E,\ \{w_1, w_2\} \in F \end{array}).$$



G

G ⊠ H.

Notation: $G^{\boxtimes k} = \underbrace{G \boxtimes \cdots \boxtimes G}_{k\text{-times}}$.

<u>Lemma 2</u> $\alpha(G \boxtimes H) \geq \alpha(G)\,\alpha(H)$,

in particular $\sqrt[k]{\alpha(G^{\boxtimes k})} \geq \alpha(G)$.

<u>Proof</u> Let $I \subseteq V$ be independent in G, and let $J \subseteq W$ be independent in H, then $I \times J$ independent in $G \boxtimes H$.

$\boxtimes$

Def 3 **Shannon capacity** of G:

$$\Theta(G) = \sup_{k \in \mathbb{N}} \sqrt[k]{\alpha(G^{\boxtimes k})} \qquad (\geq \alpha(G) \text{ by Lemma 2}).$$

Example $\Theta(C_5) \geq \sqrt{5} > 2$

Because $\alpha(C_5^{\boxtimes 2}) \geq 5$: $\{(1,1), (2,3), (3,5), (4,2), (5,4)\}$ is independent in $C_5^{\boxtimes 2}$

Shannon (1956): 1) Is $\Theta(C_5) = \sqrt{5}$?

2) How to compute $\Theta(G)$?

Answer 1) Lovász (1979): YES (this lecture).

2) No algorithm is known, even the value $\Theta(C_7)$ is not known.

Theorem 4 $\vartheta(G \boxtimes H) = \vartheta(G) \cdot \vartheta(H)$.

Proof Recall Kronecker product $A \otimes B \in \mathbb{R}^{mp \times nq}$ of two matrices $A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{p \times q}$ defined by

$$(A \otimes B)_{(ih,jk)} = A_{ij} B_{hk}$$

(see Chapter III, 2 Def. 11).

$\vartheta(G \boxtimes H) \geq \vartheta(G)\,\vartheta(H)$:

Consider primal SDP defining

$$\vartheta(G) = \max \langle J, X \rangle$$
$$X \succeq 0,\ \mathrm{Tr}(X) = 1,$$
$$X_{ij} = 0 \text{ for } \{i,j\} \in E.$$

Let X be feasible solution for $\vartheta(G)$, Y feasible for $\vartheta(H)$.
Then $X \otimes Y$ is feasible for $\vartheta(G \boxtimes H)$ (check it!) and

$$\langle J, X \otimes Y \rangle = \langle J, X \rangle \cdot \langle J, Y \rangle.$$

$\vartheta(G \boxtimes H) \leq \vartheta(G)\,\vartheta(H)$:

Consider dual SDP

$$\vartheta(G) = \min t$$
$$Z - J \succeq 0$$
$$Z_{ii} = t$$
$$Z_{ij} = 0 \text{ if } \{i,j\} \notin E.$$

Let X be feasible for $\vartheta(G)$, Y feasible for $\vartheta(H)$. Then $X \otimes Y$ feasible for $\vartheta(G \boxtimes H)$:

- $(X \times Y)_{(ih,ih)} = X_{ii} \cdot Y_{hh} = \vartheta(G)\,\vartheta(H)$.

- $\{\{i,j\},\{h,k\}\} \notin E(G \boxtimes H)$

$$(X \times Y)_{(ih,jk)} = X_{ij} Y_{hk} = 0$$

- $X \otimes Y - J \succeq 0$

We know $X - J \succeq 0$ and $Y - J \succeq 0$.

Hence (Proposition III.2.12): $(X-J)\otimes(Y-J) \succeq 0$.

Therefore $X \otimes Y - X \otimes J - J \otimes Y + J \otimes J \succeq 0$. $\quad (*)$

We also know

$$(X-J)\otimes J + J \otimes (Y-J) \succeq 0$$

Therefore

$$X \otimes J - J \otimes J + J \otimes Y - J \otimes J \succeq 0 \qquad (**)$$

Summing $(*)$ and $(**)$:

$$X \otimes Y - J \otimes J \succeq 0.$$ $\boxtimes$

<u>Corollary 5</u> $\vartheta(G) \geq \Theta(G)$.

<u>Proof</u> $\sqrt[k]{\alpha(G^{\boxtimes k})} \leq \sqrt[k]{\vartheta(G^{\boxtimes k})} = \sqrt[k]{\vartheta(G)^k} = \vartheta(G)$. $\boxtimes$

In particular: $\Theta(G)$ is finite.

Theorem 6 $\vartheta(C_5) = \sqrt{5}$.

Proof → use computer; similar to Exercise 5.4)

→ We will show $\vartheta(C_n)\,\vartheta(\overline{C_n}) = n$;

hence $\vartheta(C_5) = \sqrt{5}$ because $C_5 = \overline{C_5}$.

Def. 7 Let $G = (V, E)$ be a graph.

a) The automorphism group of G is

$$\mathrm{Aut}(G) = \{\sigma : V \to V : \sigma \text{ permutation and } \{i,j\} \in E \Leftrightarrow \{\sigma(i), \sigma(j)\} \in E\}.$$

b) G is called homogeneous (vertex transitive) if for all $i, j \in V$ there is $\sigma \in \mathrm{Aut}(G)$ so that $\sigma(i) = j$.

Decision problem "Given G, is $\mathrm{Aut}(G) = \{id\}$?" is very interesting. We know that it lies in P, but probably it is not NP-complete.

Very recent breakthrough: Babai (12/2015) announced quasipolynomial algorithm, running time $2^{O((\log n)^c)}$ for $c > 1$.