ALGO

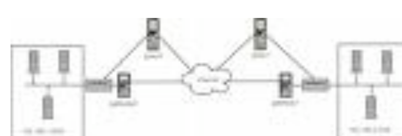
EPFL

Coding Theory: Achievements and Challenges




ISBN 978-0-7334-2609-4

9780733426094


Amin Shokrollahi
EPFL

AIMC 40, 2009

Noisy Channel

Channel Model (Simplified)

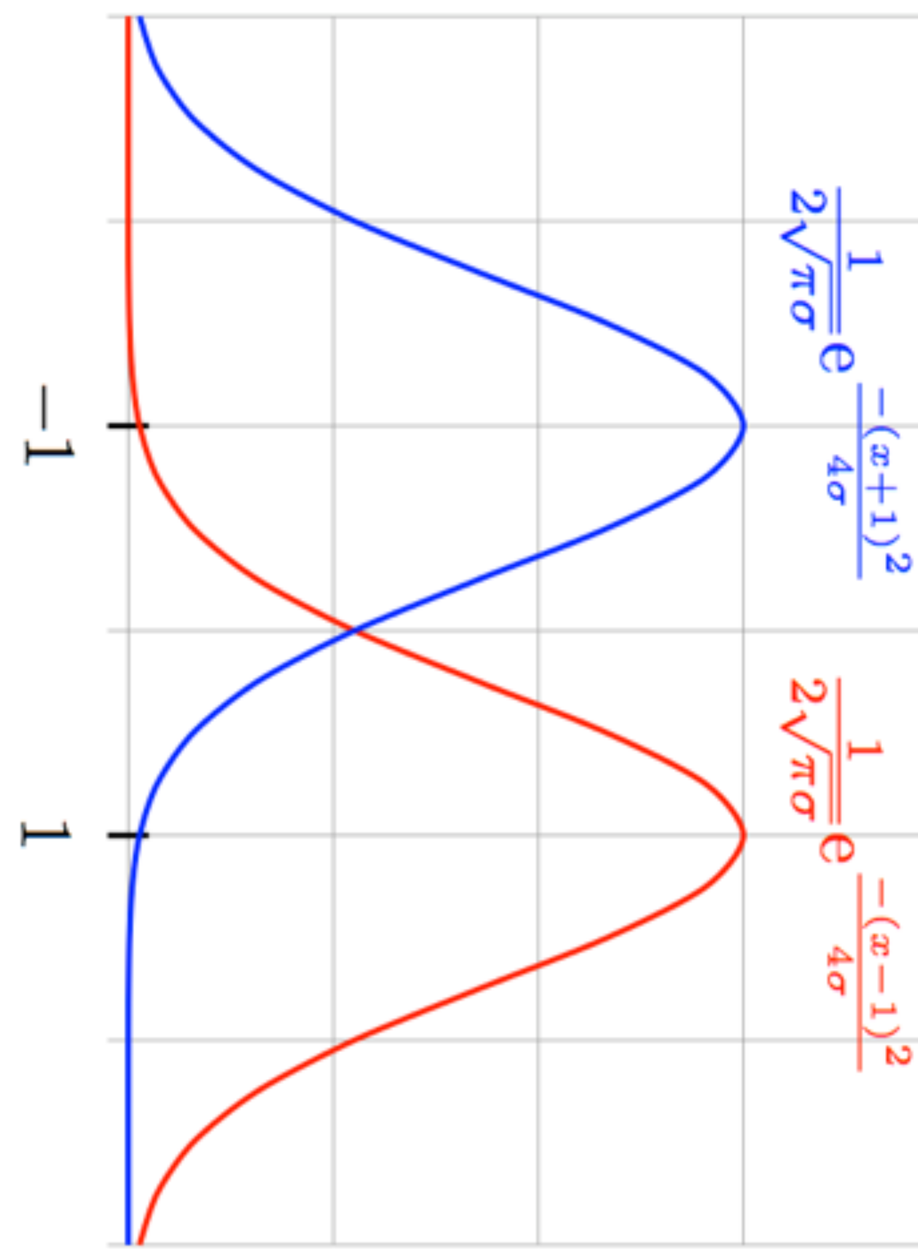
Σ, Γ finite alphabets

$p\colon \Sigma \times \Gamma \to \mathbb{R}$ Conditional probability distribution

$p(x \mid y)$ Probability that *x* is sent given that *y* is received

For fixed *x* $p(x \mid y)$ is a probability distribution on Σ

Examples (Σ = GF(2))



AWGN(σ)

Entropy, Mutual Information, Capacity

X r.v. on Σ, Y r.v. on Γ

$$H(X) = -\sum_{x \in X} \Pr[X = x] \log_2(\Pr[X = x])$$

Entropy

How many "bits of uncertainty" does X have?

Entropy, Mutual Information, Capacity

X r.v. on Σ, Y r.v. on Γ

$$H(X) = -\sum_{x \in X} \Pr[X = x] \log_2(\Pr[X = x])$$

$$H(X|Y) = -\sum_{x \in \Sigma, y \in \Gamma} \Pr[X = x, Y = y] \log_2(\Pr[X = x|Y = y])$$

Conditional Entropy

How many "bits of uncertainty" does *X* have, if we know *Y*?

Entropy, Mutual Information, Capacity

X r.v. on Σ, *Y* r.v. on Γ

$$H(X) = -\sum_{x \in X} \Pr[X = x] \log_2(\Pr[X = x])$$

$$H(X|Y) = -\sum_{x \in \Sigma, y \in \Gamma} \Pr[X = x, Y = y] \log_2(\Pr[X = x | Y = y])$$

$$I(X;Y) := H(X) - H(X|Y)$$

Mutual Information

What is the reduction of "bits of uncertainty" of *X* if we know *Y*?

Entropy, Mutual Information, Capacity

X r.v. on Σ, $\mathcal{C}$ channel with law $p(x \mid y)$

Y r.v. induced on Γ by X.

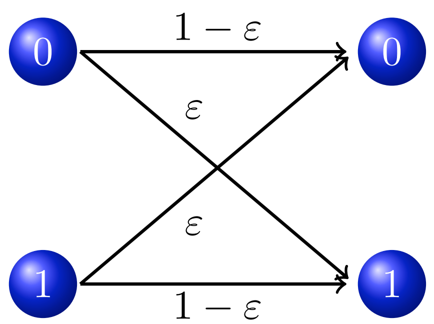
$q(x) = \Pr[X = x]$

$$\mathrm{Cap}(\mathcal{C}) = \max_q I(X;Y)$$

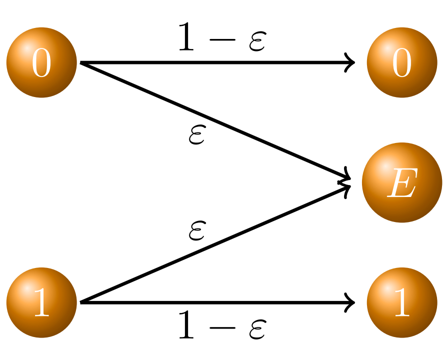
Channel Capacity

Best “reduction of uncertainty” of X given Y

Examples



$$\mathrm{Cap}(\mathrm{BSC}(\varepsilon)) = 1 + \varepsilon \log_2(\varepsilon) + (1-\varepsilon)\log_2(1-\varepsilon)$$
$$= 1 - h(\varepsilon)$$



$$\mathrm{Cap}(\mathrm{BEC}(\varepsilon)) = 1 - \varepsilon$$

Shannon's Channel Coding Theorem

Reliable communication over channel $\mathcal{C}$ is possible for any rate $R < \mathrm{Cap}(\mathcal{C})$

Average number of bits sent per channel use

Impossible if $R > \mathrm{Cap}(\mathcal{C})$

Claude E. Shannon
1916-2001

Example: BSC

$$(x_1, \ldots, x_k) \in \mathrm{GF}(2)^k$$

Not explicit — Encoding — $\cdot$ A ($k \times n$) Random

$$(y_1, \ldots, y_n) \in \mathrm{GF}(2)^n$$

Transmission — $\mathcal{C}$ — $e_i \in \mathrm{Bernoulli}(\varepsilon)$ Indepenent

$$z = (y_1 + e_1, \ldots, y_n + e_n) \in \mathrm{GF}(2)^n$$

Exp-time — Decoding

$$y' = \mathrm{argmin}_{c \in \mathrm{Im}(A)} d_H(z, c) \qquad d_H(z, c) = |\{i \mid z_i \neq c_i\}|$$

Example: BSC

If A is chosen randomly, and $k/n < 1 - h(\varepsilon)$ then

$$\frac{1}{2^k} \sum_{x \in \mathrm{GF}(2)^k} \Pr[y' \neq x \cdot A] \leq \exp(-\gamma n)$$

Positive, depends on ε and k/n

Shannon's Channel Coding Theorem

→ Not constructive

→ Polynomial time algorithms

Not practical

Forney, 1967: Concatenated Codes

Open Problem

For any given channel, design "practical" codes that come arbitrarily close to the capacity of that channel

Linear Codes

Bounds

RS-Codes

WB-Decoder

List-Decoding

AG-Codes

LDPC Codes

ALGO

Decoding on the BEC

EPFL

Theory

Theory

Theory

Achieving Capacity

Other Channels

Other Channels

Other Channels

Further Developments