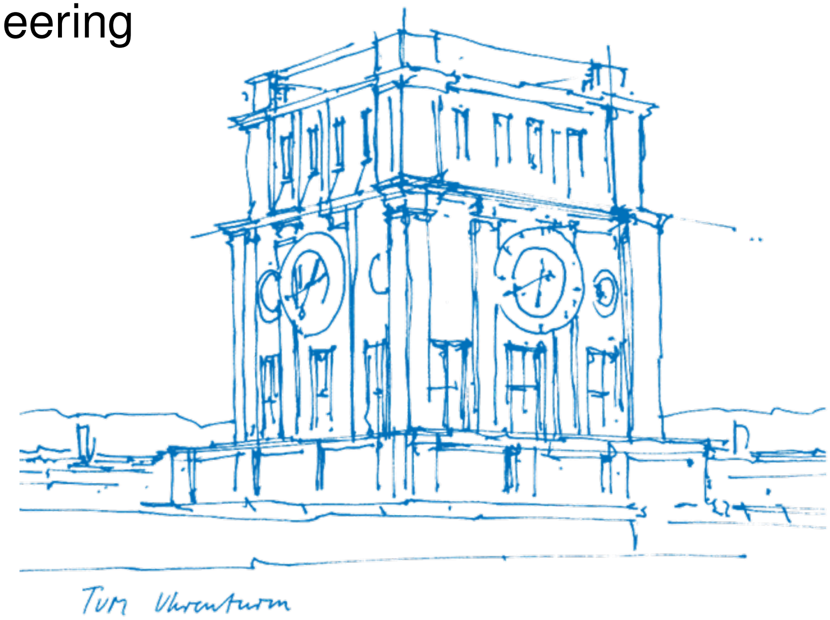
An Introduction to the **ID**entification

Mohammad Javad Salariseddigh
Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich
4th Feb 2020



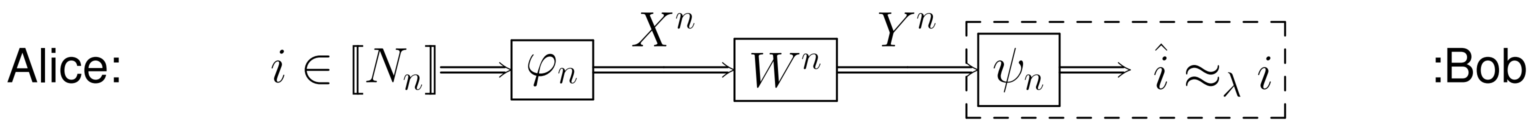
Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Outline

- Transmission
- **ID**entification
- ID Codes
- Remarks

Transmission

(Shannon 1948):



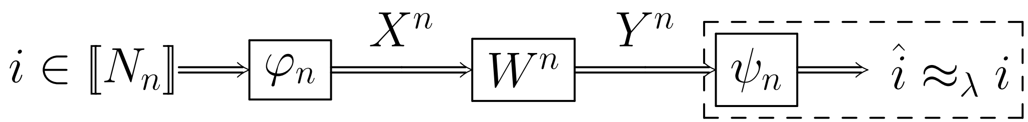
Transmission (n, N_n, λ) code for W is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Transmission

(Shannon 1948):

Alice:



:Bob

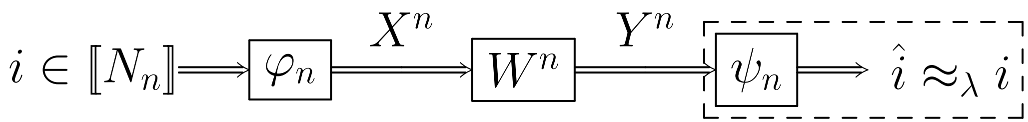
Transmission (n, N_n, λ) code for W is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$\boldsymbol{u_i} \in \mathcal{X}^n, \mathcal{D}_i \subset \mathcal{Y}^n$$

Transmission

(Shannon 1948):

Alice:



:Bob

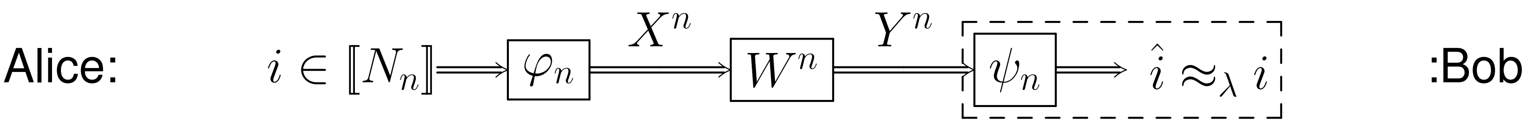
Transmission (n, N_n, λ) code for W is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$\boldsymbol{u_i} \in \mathcal{X}^n, \mathcal{D}_i \subset \mathcal{Y}^n$$

$$W^n(\mathcal{D}_i | \boldsymbol{u_i}) \geq 1 - \lambda$$

Transmission

(Shannon 1948):

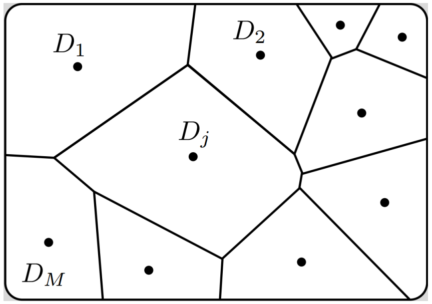


Transmission (n, N_n, λ) code for W is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$\boldsymbol{u_i} \in \mathcal{X}^n, \mathcal{D}_i \subset \mathcal{Y}^n$$

$$W^n(\mathcal{D}_i | \boldsymbol{u_i}) \geq 1 - \lambda$$

$$\mathcal{D}_i \bigcap_{i \neq j} \mathcal{D}_j = \emptyset$$

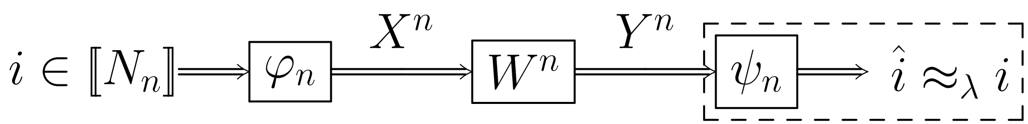


Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Transmission

(Shannon 1948):

Alice:



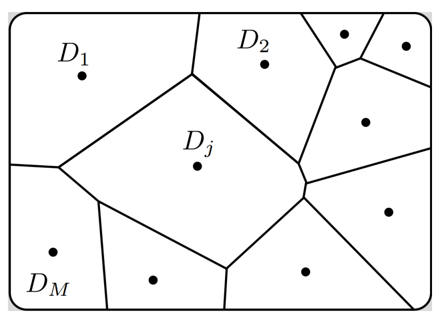
:Bob

Transmission (n, N_n, λ) code for W is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$\boldsymbol{u_i} \in \mathcal{X}^n, \mathcal{D}_i \subset \mathcal{Y}^n$$

$$W^n(\mathcal{D}_i | \boldsymbol{u_i}) \geq 1 - \lambda$$

$$\mathcal{D}_i \bigcap_{i \neq j} \mathcal{D}_j = \emptyset$$

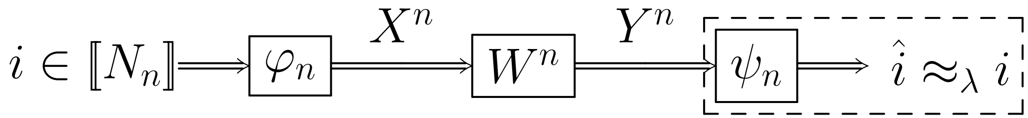


Capacity

$$\lim_{n \to \infty} \frac{1}{n} \log N_{max}(n, \lambda) = C_T \qquad \forall \lambda \in (0, 1)$$

Transmission

(Shannon 1948):

Alice: 

:Bob

Transmission (n, N_n, λ) code for W is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

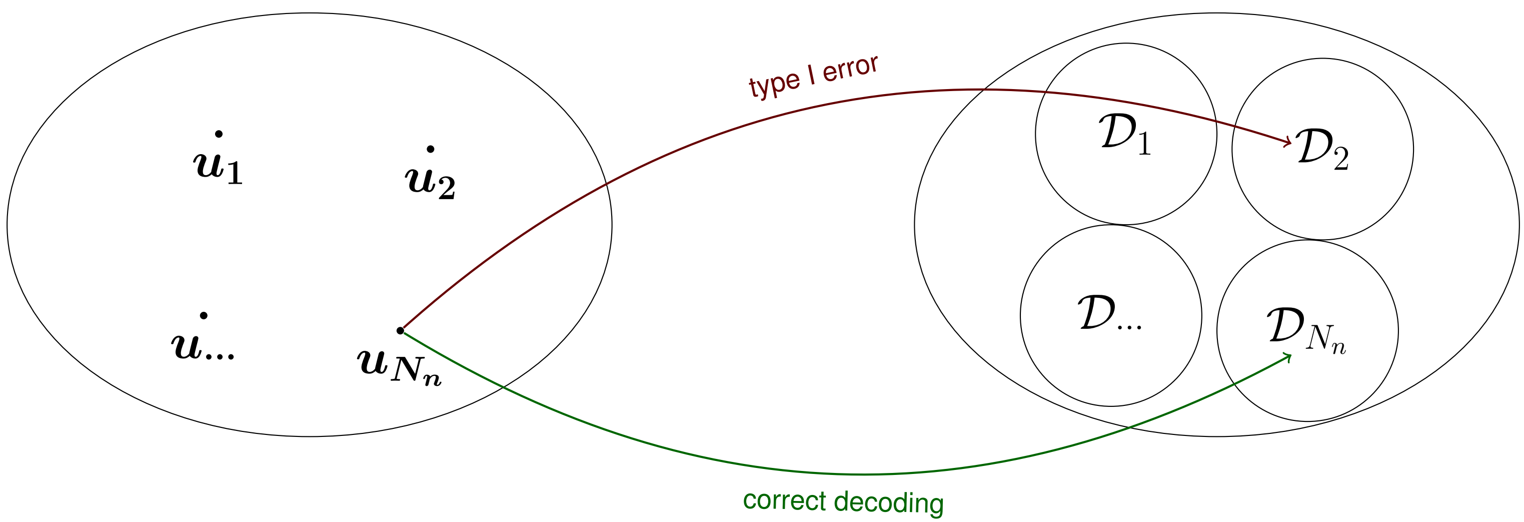


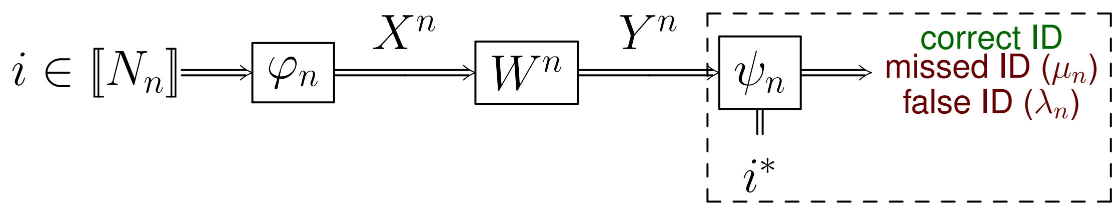
Figure: Geometric depiction of Transmission code

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

IDentification

(Ahlswede & Dueck 1989):

Alice:

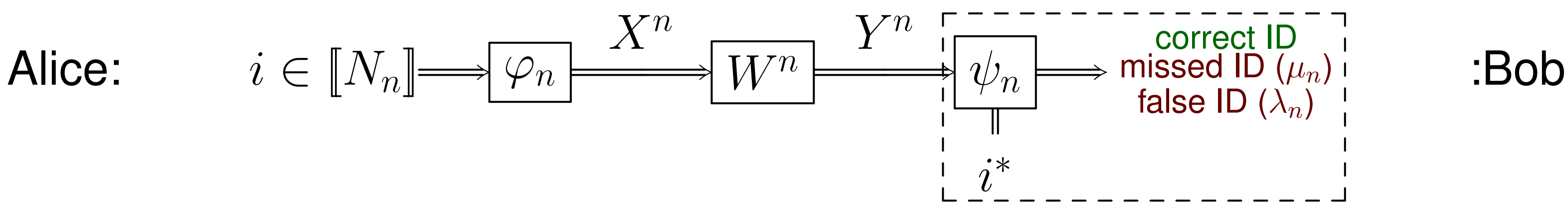


:Bob

$(n, N_n, \mu_n, \lambda_n)$ ID code for W is a system $\{(Q_i, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

IDentification

(Ahlswede & Dueck 1989):



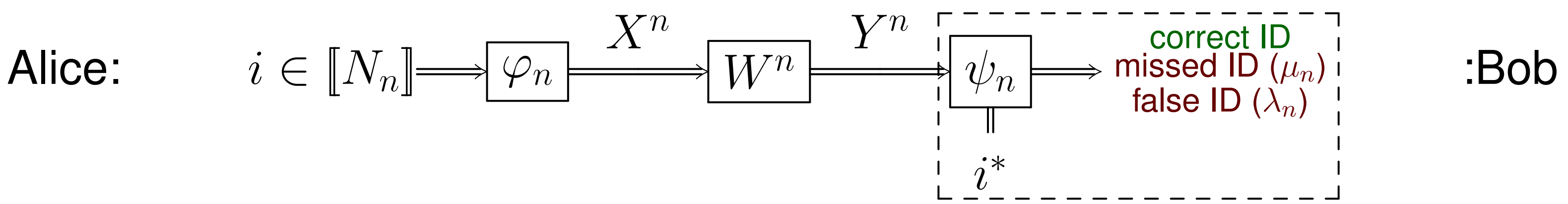
$(n, N_n, \mu_n, \lambda_n)$ ID code for W is a system $\{(Q_i, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$Q_i = \varphi_n(i) \rightarrow \text{codeword of message } i$$

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

IDentification

(Ahlswede & Dueck 1989):



$(n, N_n, \mu_n, \lambda_n)$ ID code for W is a system $\{(Q_i, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$Q_i = \varphi_n(i) \rightarrow \text{codeword of message } i$$

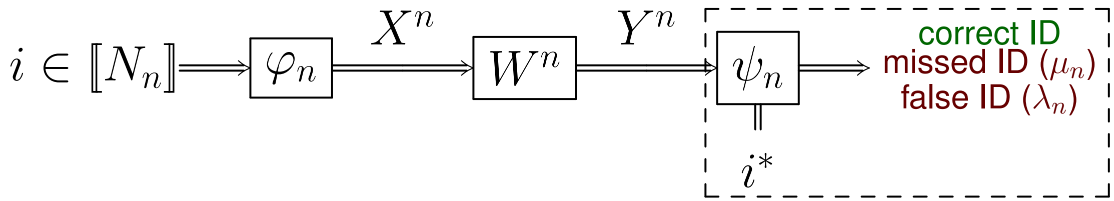
$$Q_i(x^n) = Pr\{X^n(i) = x^n\},\ x^n \in \mathcal{X}^n,\ \mathcal{D}_i \subset \mathcal{Y}^n$$

$$Q_i W^n \rightarrow Pr\{Y^n(i) = y^n\} \text{ (response of } Q_i)$$

IDentification

(Ahlswede & Dueck 1989):

Alice:



:Bob

$(n, N_n, \mu_n, \lambda_n)$ ID code for W is a system $\{(Q_i, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$Q_i = \varphi_n(i) \rightarrow \text{codeword of message } i$$

$$Q_i(x^n) = Pr\{X^n(i) = x^n\},\ x^n \in \mathcal{X}^n,\ \mathcal{D}_i \subset \mathcal{Y}^n$$

$$Q_i W^n \rightarrow Pr\{Y^n(i) = y^n\} \text{ (response of } Q_i\text{)}$$

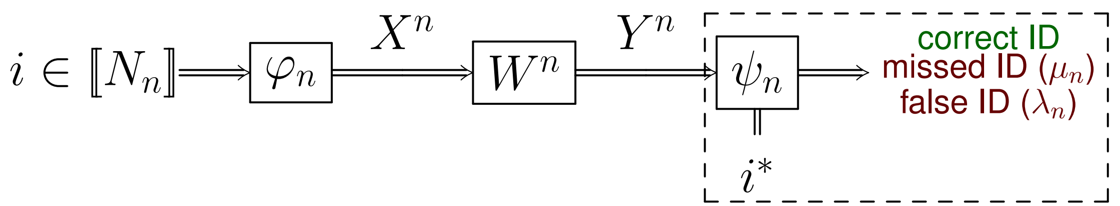
$$\mu_n^{(i)} = Q_i W^n(\mathcal{D}_i^c) = Pr\{Y^n(i) \in \mathcal{Y}^n \setminus \mathcal{D}_i\} \xrightarrow{\text{type I error}} \quad \mu_n = \max_{1 \le i \le N_n} \mu_n^{(i)}$$

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

IDentification

(Ahlswede & Dueck 1989):

Alice:



:Bob

$(n, N_n, \mu_n, \lambda_n)$ ID code for W is a system $\{(Q_i, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$Q_i = \varphi_n(i) \rightarrow \text{codeword of message } i$$

$$Q_i(x^n) = Pr\{X^n(i) = x^n\},\ x^n \in \mathcal{X}^n,\ \mathcal{D}_i \subset \mathcal{Y}^n$$

$$Q_i W^n \rightarrow Pr\{Y^n(i) = y^n\} \text{ (response of } Q_i)$$

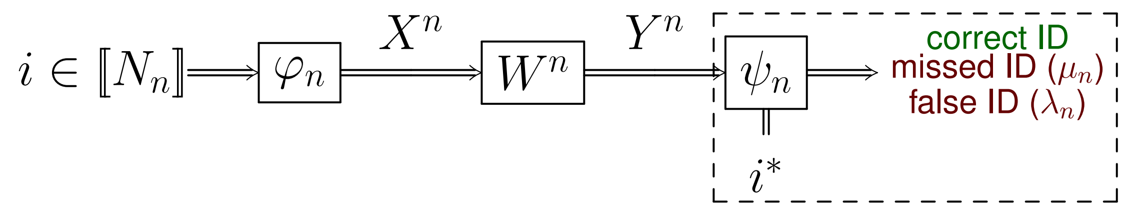
$$\mu_n^{(i)} = Q_i W^n(\mathcal{D}_i^c) = Pr\{Y^n(i) \in \mathcal{Y}^n \setminus \mathcal{D}_i\} \xrightarrow{\text{type I error}} \mu_n = \max_{1 \le i \le N_n} \mu_n^{(i)}$$

$$\lambda_n^{(i,j)} = Q_j W^n(\mathcal{D}_i) = Pr\{Y^n(j) \in \mathcal{D}_i\}(j \neq i) \xrightarrow{\text{type II error}} \lambda_n = \max_{1 \le j, i \le N_n, j \neq i} \lambda_n^{(j,i)}$$

IDentification

(Ahlswede & Dueck 1989):

Alice:



:Bob

$(n, N_n, \mu_n, \lambda_n)$ ID code for W is a system $\{(Q_i, \mathcal{D}_i)\}_{i \in [\![N_n]\!]}$:

$$Q_i = \varphi_n(i) \rightarrow \text{codeword of message } i$$

$$Q_i(x^n) = Pr\{X^n(i) = x^n\}, \; x^n \in \mathcal{X}^n, \; \mathcal{D}_i \subset \mathcal{Y}^n$$

$$Q_i W^n \rightarrow Pr\{Y^n(i) = y^n\} \text{ (response of } Q_i)$$

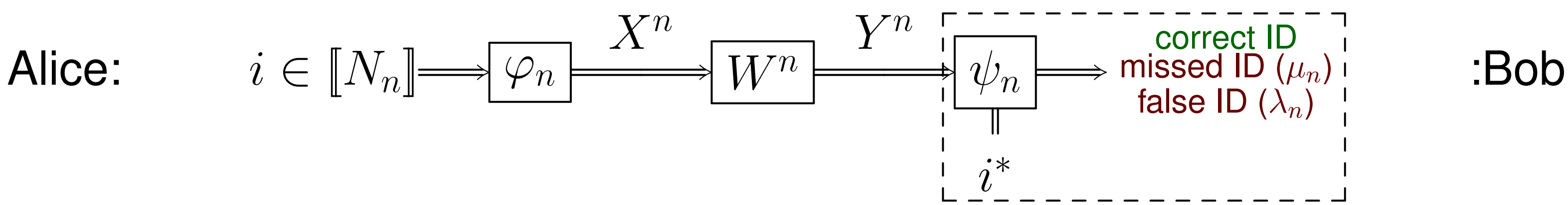
$$\mu_n^{(i)} = Q_i W^n(\mathcal{D}_i^c) = Pr\{Y^n(i) \in \mathcal{Y}^n \setminus \mathcal{D}_i\} \xrightarrow{\text{type I error}} \mu_n = \max_{1 \le i \le N_n} \mu_n^{(i)}$$

$$\lambda_n^{(i,j)} = Q_j W^n(\mathcal{D}_i) = Pr\{Y^n(j) \in \mathcal{D}_i\} (j \neq i) \xrightarrow{\text{type II error}} \lambda_n = \max_{1 \le j, i \le N_n, j \neq i} \lambda_n^{(j,i)}$$

$$N_n \le 2^{|\mathcal{Y}|^n}$$

IDentification

(Ahlswede & Dueck 1989):



missed ID (due to channel noise)

Alice sent message i, Bob who is interested in test message i^* can decide i^* was not sent

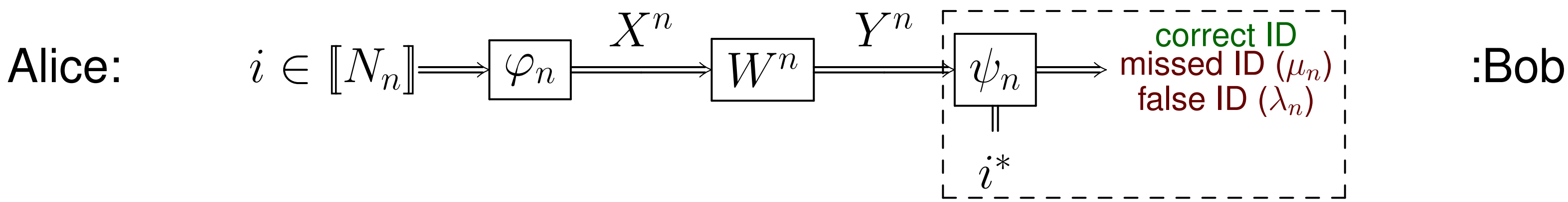
false ID (inherent to the code)

Alice sent message j, Bob who is interested in test message j^* can decide message $i \neq j$ was sent

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

IDentification

(Ahlswede & Dueck 1989):



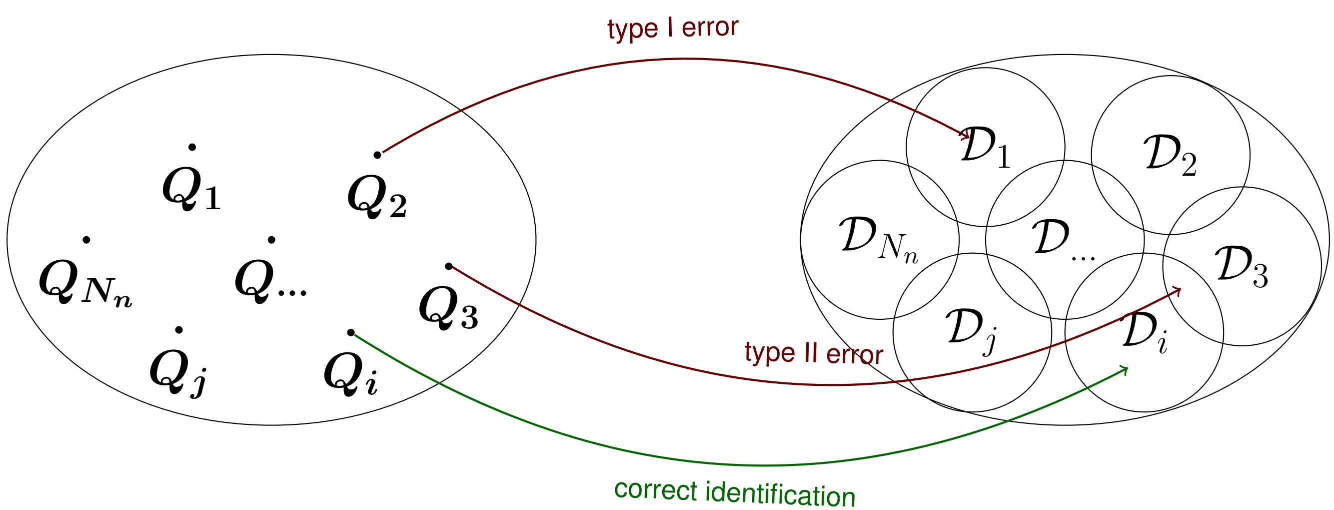


Figure: Geometric depiction of ID code

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

IDentification Theorems

Rate

$$r_n \triangleq \frac{1}{n} \log \log N(n, \mu_n, \lambda_n) \tag{1}$$

Capacity

$$C_{ID} = \lim_{n \to \infty} \frac{1}{n} \log \log N_{max}(n, \mu_n, \lambda_n) \tag{2}$$

Direct Part

$$\liminf_{n \to \infty} r_n \geq C_T \quad \forall \mu_n, \lambda_n \in (0, 1] \tag{3}$$

Soft Converse

$$\limsup_{n \to \infty} r_n \leq C_T \quad \mu_n, \lambda_n \leq 2^{-n\varepsilon} \quad \forall \varepsilon > 0 \tag{4}$$

Strong Converse (Han & Verdu 1992)

$$C_{ID} \leq C_T \quad \forall \mu_n, \lambda_n \geq 0 \quad \& \quad \limsup_{n \to \infty} (\mu_n + \lambda_n) < 1 \tag{5}$$

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Transmission vs **ID**entification

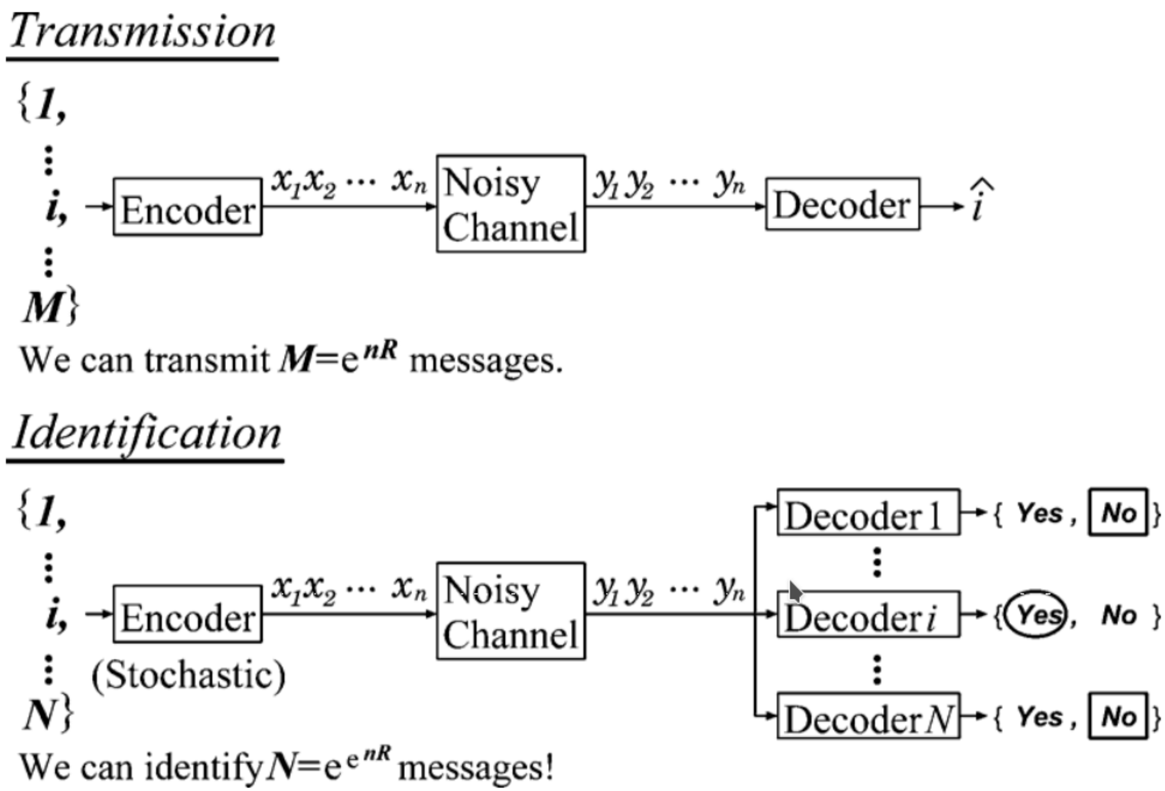


Figure: difference between Transmission and **ID**entification [1]

[1] Y. Oohama, "Converse coding theorems for identification via channels," IEEE Trans. Inform. Theory, vol. 59, pp. 744-759, Feb. 2013.

Application

- Scenario → Radio Networks, LAN, and Downlink Satellite Communications
- Goal → Delivery a sequences of messages, each intended for one receiver

Application

- Scenario → Radio Networks, LAN, and Downlink Satellite Communications
- Goal → Delivery a sequences of messages, each intended for one receiver

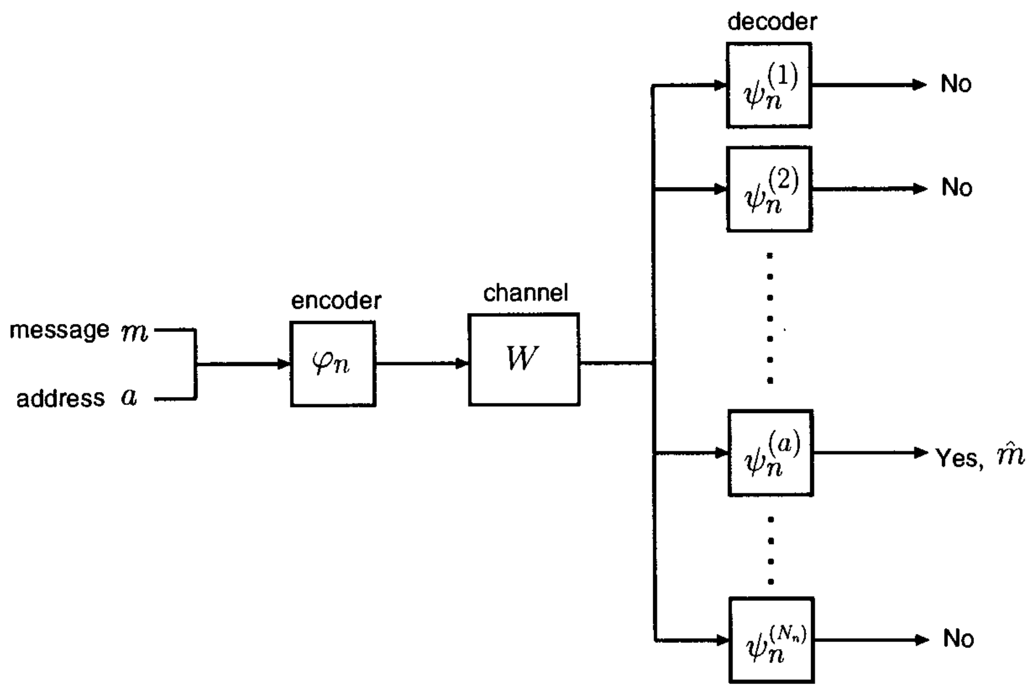


Figure: realization of identification-transmission communication [2]

[2] adopted from "Information-Spectrum Methods in Information Theory", T. S. Han, Tokyo, 2003, p. 436.

Construction 1 (Random Coding Argument)

(Ahlswede & Dueck):

- Shannon's coding theorem gaurantees existence of two transmission codes:
  - $\mathcal{L}' = \{(\boldsymbol{u}'_j, \mathcal{D}'_j) | j \in [\![M']\!]\}$ / $(n, \lceil 2^{n(C-\varepsilon)} \rceil, 2^{-n\delta})$
  - $\mathcal{L}'' = \{(\boldsymbol{u}''_k, \mathcal{D}''_k) | k \in [\![M'']\!]\}$ / $(\lceil \sqrt{n} \rceil, \lceil 2^{\varepsilon\sqrt{n}} \rceil, 2^{-\sqrt{n}\delta})$

- Let $\mathcal{T}$ be a family of maps $\mathcal{T} = \{T_i | i \in [\![N]\!]\}$ where $T_i : [\![M']\!] \to [\![M'']\!]$
- Let $\mathcal{U}_i := \{\boldsymbol{u}'_j.\boldsymbol{u}''_{T_i(j)} | j \in [\![M']\!]\}$ and $\mathcal{D}_i = \bigcup_{j=1}^{M'} \mathcal{D}'_j \times \mathcal{D}''_{T_i(j)}$
- Let $Q(i)$ be uniform distribution on set of codewords $\mathcal{U}_i$

- Obviously $\mathcal{ID}_{\mathcal{L}',\mathcal{L}''} = \{(Q_i, \mathcal{D}_i)\}_{i \in [\![N]\!]}$ is an $(n + \sqrt{n}, N, \lambda_1^{\mathbb{L}',\mathbb{L}''}, \lambda_2^{\mathbb{L}',\mathbb{L}''})$ ID code.

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Construction 1 (Random Coding Argument)

(Ahlswede & Dueck):

- Let $\forall i \in [\![N]\!]$ and $\forall j \in [\![M']\!]$, U_{ij} be independent RVs s.t. $\Pr\{U_{ij} = \boldsymbol{u}'_j.\boldsymbol{u}''_k\} = \frac{1}{M''}$, $\quad \exists T^* \in$ **T** s.t. $T^*_i(j) = k \in [\![M'']\!]$
- Let random set $\overline{\mathcal{U}}_i = \{U_{i1}, \cdots, U_{iM'}\}$ be a vector of concatenated codeword
- Let random decoding set $\mathcal{D}(\overline{\mathcal{U}}_i) = \bigcup_{j=1}^{M'} \mathcal{D}(U_{ij})$ where $\mathcal{D}(U_{ij}) = \mathcal{D}'_j \times \mathcal{D}''_k$
- System $\{(\overline{Q}(i),\mathcal{D}(\overline{\mathcal{U}}_i))|i \in [N]\}$ is $(M'(n + \lceil\sqrt{n}\rceil), N, \lambda_1, \lambda_2)$ ID code and achieves acceptible maximal error probabilities

Construction 2 (Concatenation)

(Verdu & Wei):

- Sequence of binary constant-weight code $\{C_i\} = (S_i, N_i, M_i, \mu_i M_i)$ with weight factor β_i, second order rate ρ_i and pairwise overlap fraction μ_i is optimal for identification if:
  - $\beta_i \to 1$, $\rho_i \to 1$, $\mu_i \to 0$

- 3 layer concatenated code $C_1 \circ C_2 \circ C_3$ denoted by $[q, k, t]$ with:
  - $C_1 = [q]$ PPM (all binary q-vectors of unit weight)
  - $C_2 = [q, k]$ RS Code
  - $C_3 = [q^k, q^t]$ RS Code
  - $t \leq k \leq q =$ prime

  is a $(q^{k+2}, (q^k)^{q^t}, q^{k+1}, kq^k + q^{1+t})$ binary constant-weight code

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Construction 2 (Concatenation)

(Verdu & Wei):

- Let $\{C_i\} = [q_i, k_i, t_i]$ be sequence of 3 layer concatenated codes, then $\{C_i\}$ is optimal for identification if:
  - $t_i \to \infty$
  - $\frac{t_i}{k_i} \to 1$
  - $\frac{k_i}{q_i} \to 0$
  - $q_i^{t_i - k_i} \to 0$
- Coupling 3 layer concatenated code with a transmission code (n, e^{nR}, λ) gives an IT code which subsequently ID code can be extracted from !
- Error exponents of resulting ID code $\to$ $(\frac{1}{n}\log\frac{1}{\lambda}, \frac{1}{n}\log\frac{1}{\lambda+\mu})$

Construction 3 (1 Layer RS Code)

(Moulin & Koetter):

- Let $C = (n, |C|, d)_q$ be an EC code
- For word $c_i = (c_i^1, \cdots, c_i^n)$ let enc/dec set $A_i = D_i$ is $\{(u, c_i^u) | u \in [n]\}$
- $|A_i| = n, \quad |A_i \cap A_j| \leq n - d, \quad \forall i, j \in [|C|] \quad \rightarrow \mu_n = 1 - \frac{d}{n}$
- Let RS code $(n \leq q - 1, k)$ over $\mathbb{F}_q$ map $(x_0, \cdots, x_{k-1}) \in \mathbb{F}_q^k$ to $(y_1, \cdots, y_n) \in \mathbb{F}_q^n$ where $y_i = \sum_{j=0}^{k-1} x_j \alpha_i^j$ where $\alpha_i \in F = \{\alpha_1, \cdots, \alpha_n\} \subset \mathbb{F}_q$
- $(x_0, \cdots, x_{k-1}) \sim P = \sum_{j=0}^{k-1} x_j X^j \in \mathbb{F}_q[X]$
- Set $A_P = \{(j, P(\alpha_j))\} | j \in [n]\} \quad$ for $P \in \mathbb{F}_q[X]$
- Now M-K-RS ID code is defined by $\{(A_p, A_p) | P \in \mathbb{F}_q[X], deg(P) < k\}$
- Corresponding ID code is $(\log_2 n + \log_2 q, q^k, 0, \frac{k-1}{n})$
- Application in ContactLess Device (RFID tags) identification [**Private Interrogation**]

Institute For Communications Engineering
Department of Electrical and Computer Engineering
Technical University of Munich

Construction 3 (1 Layer RS Code)

(Moulin & Koetter):

- Let message set $\mathbb{M}$ have cardinality 2^{rK}, where $r = \varepsilon n$, for some $\varepsilon \in (0,1)$
- Partition message m into K submessages $m_1, \cdots, m_K$
- Binary representation of m as $r \times K$ matrix where m_u sits in the u-th coloumn.

$$\mathbf{m} \sim \left.\underbrace{\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}}_{K}\right\} r$$

- Encoding:
  - Generate RV u uniformly distributed over $\{1, \cdots, K\}$
  - Transmit ID word (u, m_u)
- Parameters:
  - # of bits to represent **a** $= (u, m_u) = \log K + r$ where $\log K = \frac{1-\varepsilon}{\varepsilon} r$
  - $\frac{1}{n} \log\log \mathbb{M} = 1 - \varepsilon + \frac{\log(\varepsilon n)}{n}$

Construction 3 (1 Layer RS Code)

(Moulin & Koetter):

- Decoding:
  - RX observes output of noiseless channel **b** = **a** $= (u, m_u)$
  - To test for the presence of message m^*, decoder compares if $m_u = m_u^*$
- Performance:
  - $\mu_n = 0$ ☺
  - $\lambda_n = 1 - \frac{1}{K}$ ☹
- The need for redundancy $\rightarrow$ representation of message s.t. increase distance between different messages (measured via distinct coloumns)
- Simple idea $\rightarrow$ apply (L, K) RS code with alphabet size $q = 2^r$ to message m
- Performance:
  - $\mu_n = 0$ ☺
  - $\lambda_n = \frac{K}{L}$ ☺

Remarks

- ID codes outperform one exponential order more than transmission codes by gaining reliable transmission of double exponential messages in bloklength
- Double Exponent Coding Theorem have been developed
- ID performance is measured by two errors namely type I and type II
- ID application $\rightarrow$ P2MP, remote alarm service,
- For infinite alphabet channel (white Gaussian with bandwith constraint) or DMC ID and Shannon capacity coincide
- ID code for noisy channel $\rightarrow$ concatenation of standard transmission code and an ID code for noiseless channel
- Need for explicit construction of ID codes and Practical algorithms for implementation continues!

Questions

Thanks For Attendance