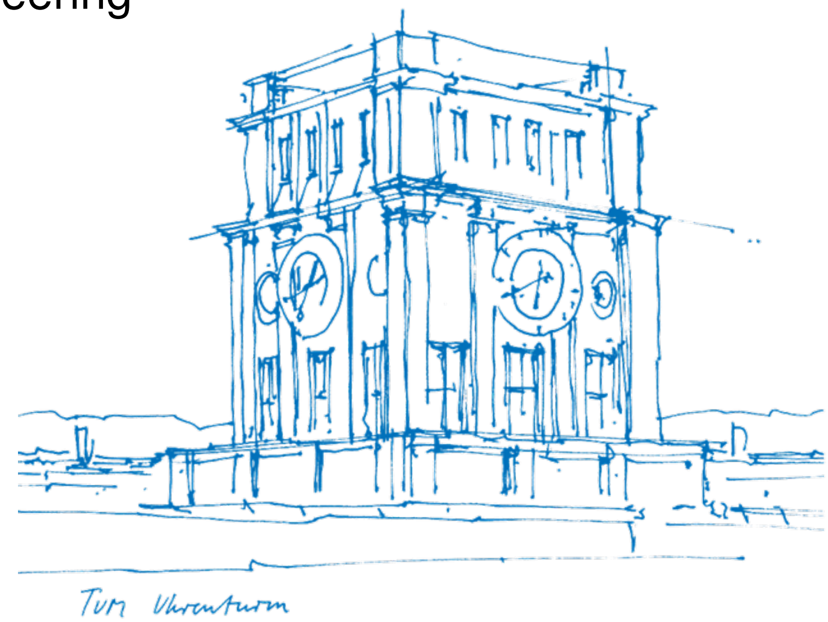
An Introduction to IDentification

Mohammad Javad Salariseddigh
Technical University of Munich
Department of Electrical and Computer Engineering
Institute For Communications Engineering
29th October 2019



Outline

- Transmission (Shannon)
- IDentification (Ahlswede & Dueck)
- Construction of ID code
- Summary

Transmission

Transmission (Shannon) over W^n:

Alice: $i \in \{1, ..., N_n\} \Longrightarrow \boxed{\text{Enc}} \xRightarrow{X^n} \boxed{W^n} \xRightarrow{Y^n} \boxed{\text{Dec}} \Longrightarrow \hat{i} \approx_\lambda i$:Bob

Classical (n, N_n, λ) code for W is a system $\{(u_i, D_i)\}_{i\in[N_n]}$ such that:

Transmission

Transmission (Shannon) over W^n:

Alice: $i \in \{1, \ldots, N_n\} \Longrightarrow \boxed{\text{Enc}} \xRightarrow{X^n} \boxed{W^n} \xRightarrow{Y^n} \boxed{\boxed{\text{Dec}} \Longrightarrow \hat{i} \approx_\lambda i}$:Bob

Classical (n, N_n, λ) code for W is a system $\{(u_i, D_i)\}_{i \in [N_n]}$ such that:

$$u_i \in \mathcal{X}^n, D_i \subset \mathcal{Y}^n$$

Transmission

Transmission (Shannon) over W^n:

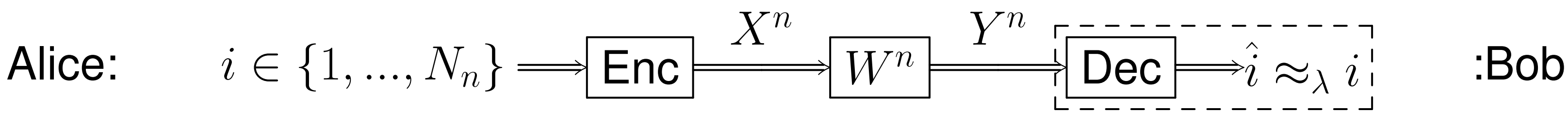
$$\text{Alice:} \quad i \in \{1, \ldots, N_n\} \Longrightarrow \boxed{\text{Enc}} \xRightarrow{X^n} \boxed{W^n} \xRightarrow{Y^n} \boxed{\text{Dec}} \Longrightarrow \hat{i} \approx_\lambda i \quad \text{:Bob}$$

Classical (n, N_n, λ) code for W is a system $\{(u_i, D_i)\}_{i \in [N_n]}$ such that:

$$u_i \in \mathcal{X}^n, D_i \subset \mathcal{Y}^n$$
$$W^n(D_i|u_i) \geq 1 - \lambda$$

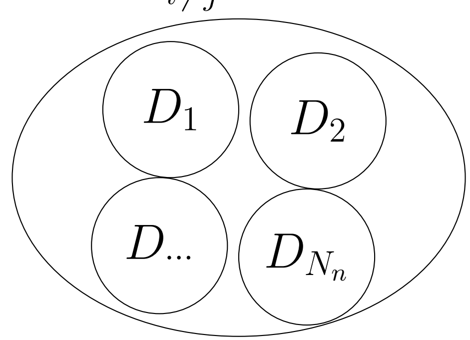
Transmission

Transmission (Shannon) over W^n:



Classical (n, N_n, λ) code for W is a system $\{(u_i, D_i)\}_{i \in [N_n]}$ such that:

$$u_i \in \mathcal{X}^n, D_i \subset \mathcal{Y}^n$$
$$W^n(D_i | u_i) \geq 1 - \lambda$$
$$D_i \bigcap_{i \neq j} D_j = \emptyset$$



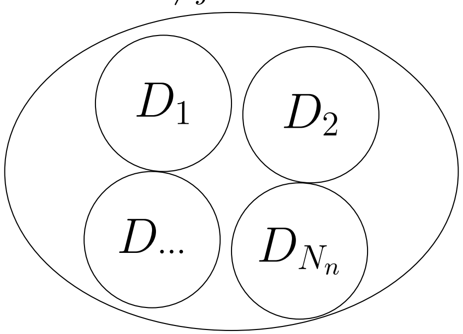
Transmission

Transmission (Shannon) over W^n:

Alice: $i \in \{1, ..., N_n\} \Longrightarrow \boxed{\text{Enc}} \xrightarrow{X^n} \boxed{W^n} \xrightarrow{Y^n} \boxed{\boxed{\text{Dec}} \Longrightarrow \hat{i} \approx_\lambda i}$:Bob

Classical (n, N_n, λ) code for W is a system $\{(u_i, D_i)\}_{i \in [N_n]}$ such that:

$$u_i \in \mathcal{X}^n, D_i \subset \mathcal{Y}^n$$
$$W^n(D_i|u_i) \geq 1 - \lambda$$
$$D_i \underset{i \neq j}{\cap} D_j = \emptyset$$



Transmission capacity (Shannon)

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

Transmission

Transmission (Shannon) over W^n:

Alice: $\quad i \in \{1, ..., N_n\} \Longrightarrow \boxed{\text{Enc}} \xRightarrow{X^n} \boxed{W^n} \xRightarrow{Y^n} \boxed{\text{Dec}} \Longrightarrow \hat{i} \approx_\lambda i \quad$:Bob

Classical (n, N_n, λ) code for W is a system $\{(u_i, D_i)\}_{i\in[N_n]}$ such that:

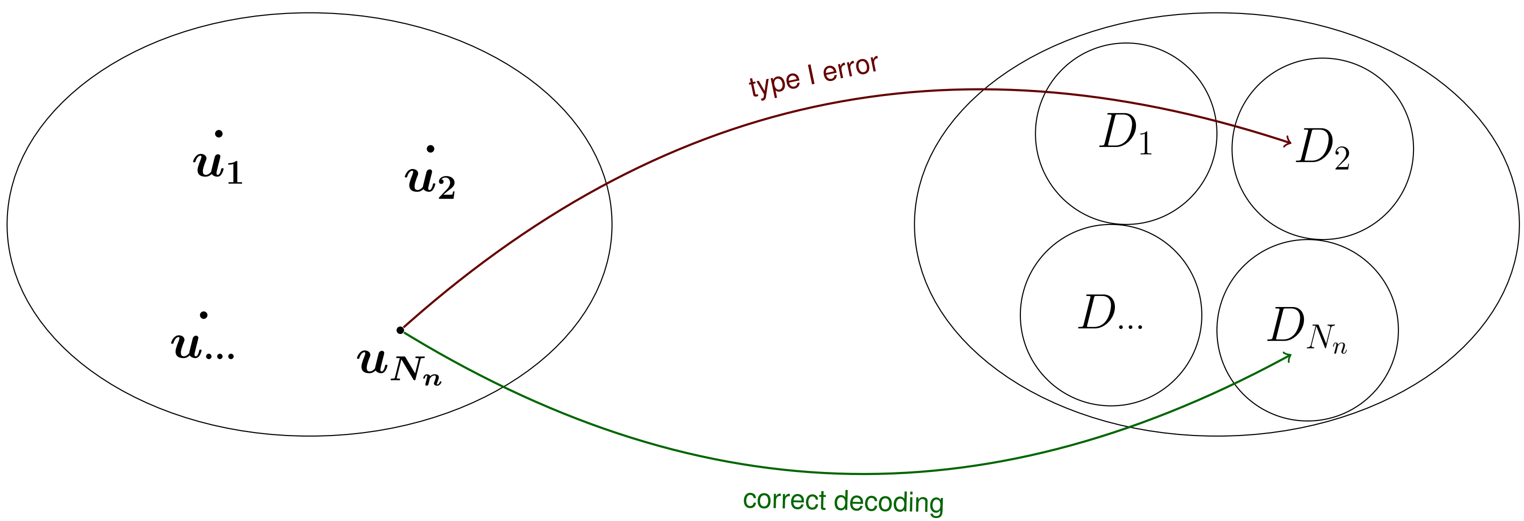
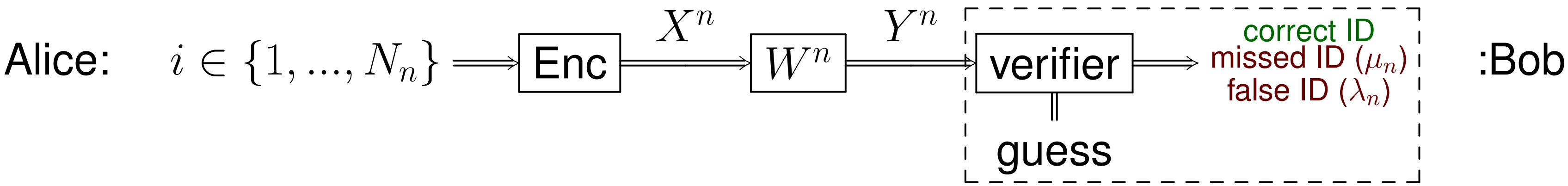


Figure: Geometric depiction of Transmission code

IDentification

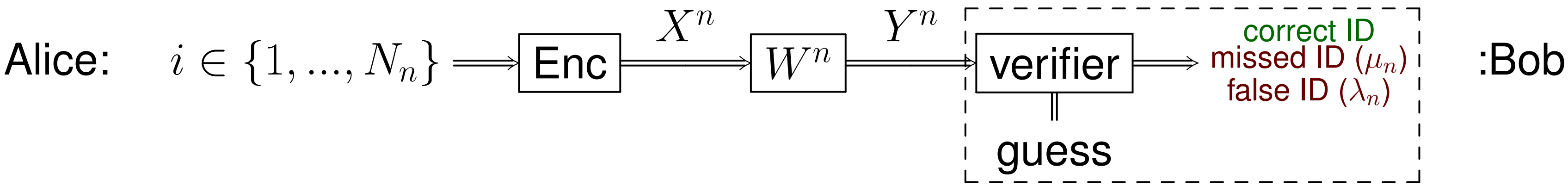
IDentification (Ahlswede-Dueck) over W^n:



Randomized $(n, N_n, \mu_n, \lambda_n)$ identification code for W is a system $\{(Q_i, D_i)\}_{i\in[N_n]}$ such that:

IDentification

IDentification (Ahlswede-Dueck) over W^n:

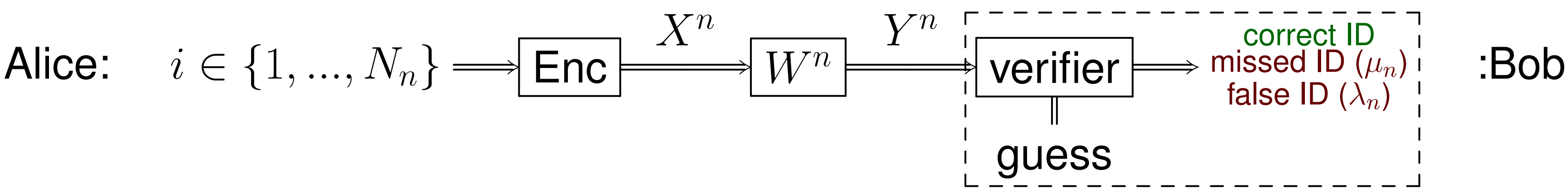


Randomized $(n, N_n, \mu_n, \lambda_n)$ identification code for W is a system $\{(Q_i, D_i)\}_{i\in[N_n]}$ such that:

random codeword $X^n(i) \rightarrow$ generated by randomized encoder $\varphi_n(i)$

IDentification

IDentification (Ahlswede-Dueck) over W^n:

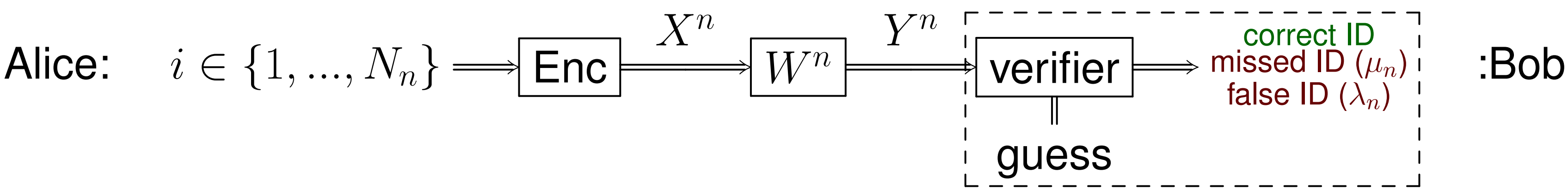


Randomized $(n, N_n, \mu_n, \lambda_n)$ identification code for W is a system $\{(Q_i, D_i)\}_{i \in [N_n]}$ such that:

$$\text{random codeword } X^n(i) \rightarrow \text{generated by randomized encoder } \varphi_n(i)$$
$$Q_i(x^n) = Pr\{X^n(i) = x^n\}, \; x^n \in \mathcal{X}^n, \; D_i \subset \mathcal{Y}^n$$

IDentification

IDentification (Ahlswede-Dueck) over W^n:



Randomized $(n, N_n, \mu_n, \lambda_n)$ identification code for W is a system $\{(Q_i, D_i)\}_{i \in [N_n]}$ such that:

random codeword $X^n(i) \rightarrow$ generated by randomized encoder $\varphi_n(i)$

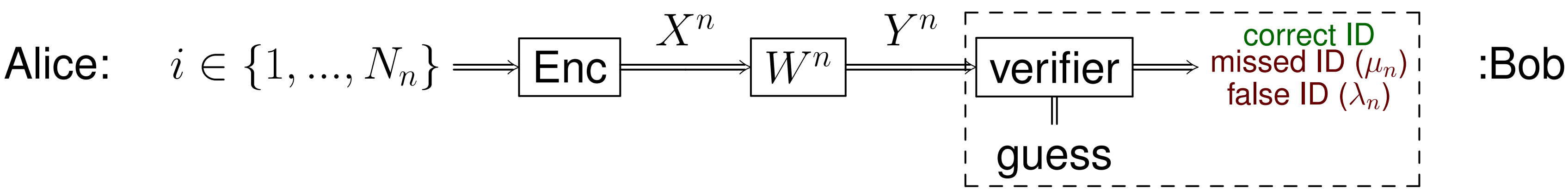
$$Q_i(x^n) = Pr\{X^n(i) = x^n\},\ x^n \in \mathcal{X}^n,\ D_i \subset \mathcal{Y}^n$$

$Y^n(i) \rightarrow$ output of W^n when input is $X^n(i)$

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

IDentification

IDentification (Ahlswede-Dueck) over W^n:



Randomized $(n, N_n, \mu_n, \lambda_n)$ identification code for W is a system $\{(Q_i, D_i)\}_{i \in [N_n]}$ such that:

random codeword $X^n(i) \rightarrow$ generated by randomized encoder $\varphi_n(i)$

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

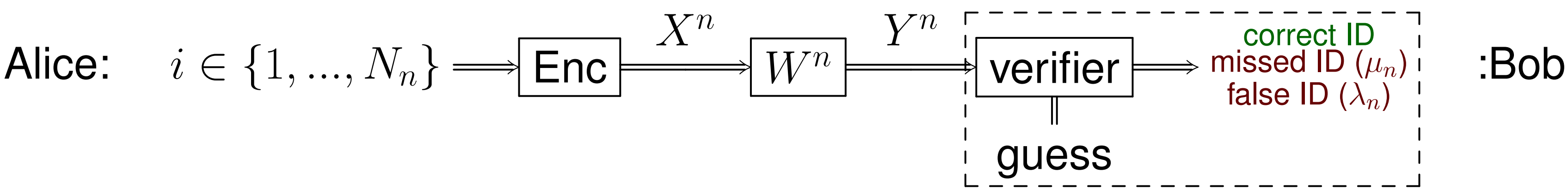
$Y^n(i) \rightarrow$ output of W^n when input is $X^n(i)$

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

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

IDentification

IDentification (Ahlswede-Dueck) over W^n:



Randomized $(n, N_n, \mu_n, \lambda_n)$ identification code for W is a system $\{(Q_i, D_i)\}_{i \in [N_n]}$ such that:

random codeword $X^n(i) \rightarrow$ generated by randomized encoder $\varphi_n(i)$

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

$Y^n(i) \rightarrow$ output of W^n when input is $X^n(i)$

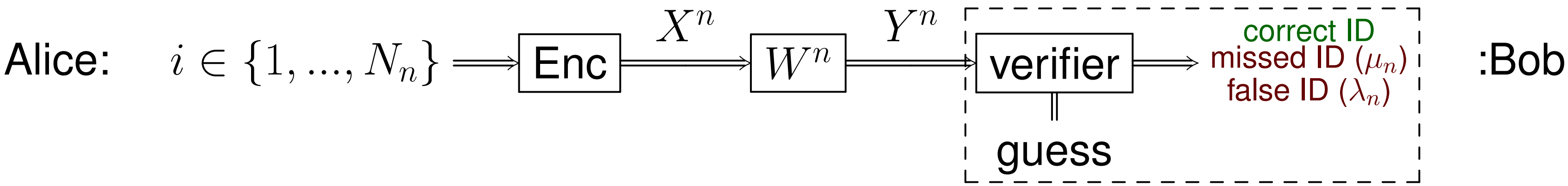
$$Q_i W^n \rightarrow Pr\{Y^n(i) = y^n\}$$

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

$$\lambda_n^{(i,j)} = Q_j W^n(D_i) = Pr\{Y^n(j) \in D_i\} (j \neq i) \xrightarrow{\text{type II error}} \qquad \lambda_n = \max_{1 \leq j, i \leq N_n, j \neq i} \lambda_n^{(j,i)}$$

IDentification

IDentification (Ahlswede-Dueck) over W^n:



missed identification

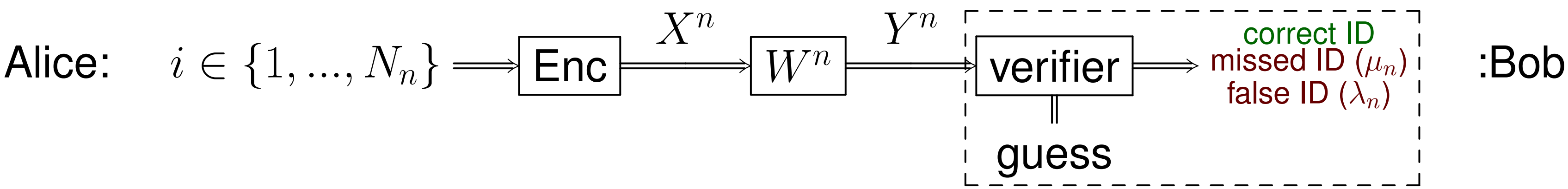
Alice sent message i, Bob who is interested in message i (guess i) can decide his message was not sent / caused by transmission errors

false identification

Alice sent message i, Bob who is interested in message $j \neq i$ (guess j) can decide message j was sent / inherent to the code

IDentification

IDentification (Ahlswede-Dueck) over W^n:



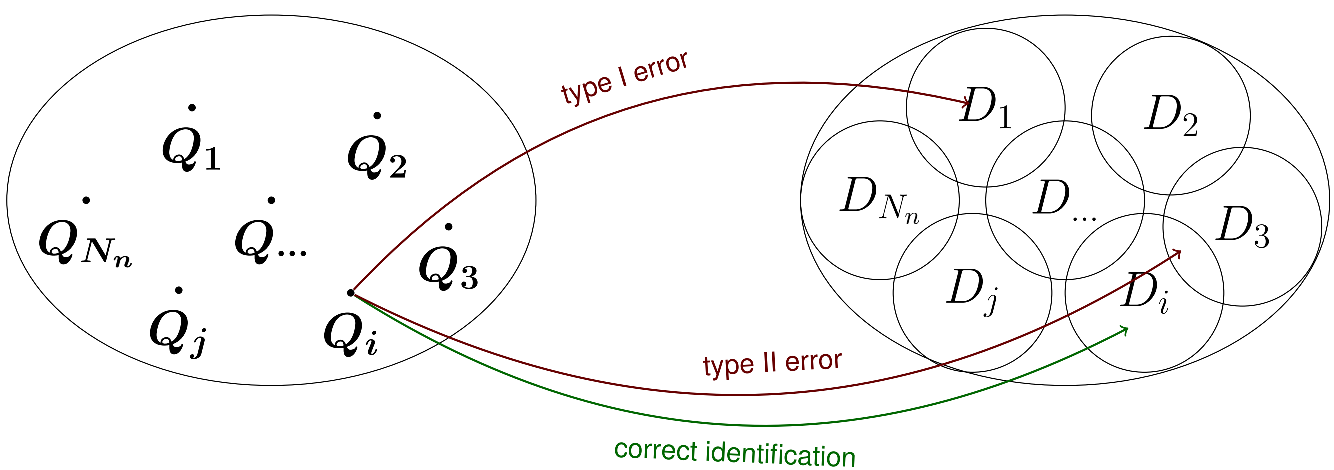
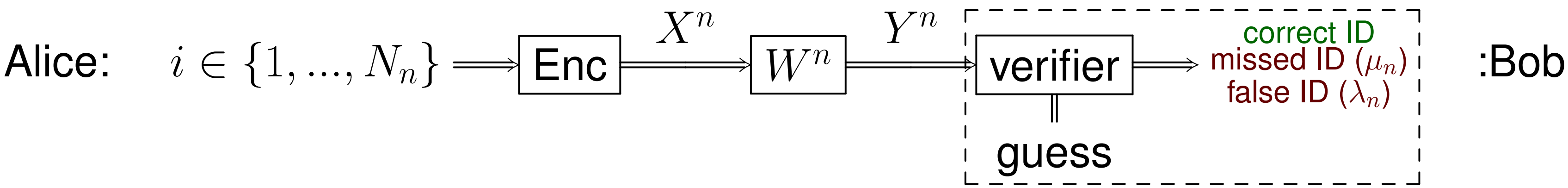


Figure: Geometric depiction of IDentification code

IDentification

IDentification (Ahlswede-Dueck) over W^n:



Rate

$$r_n = \frac{1}{n} \log \log N_n \tag{1}$$

Capacity

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

ID Coding Theorem

$$C_{ID} = C_T \tag{3}$$

Theorem

ID capacity of any channel is greater than or equal its Shannon capacity

Technical Application of IDentification

- Scenario $\rightarrow$ local-area/radio networks and downlink satellite communications
- Goal $\rightarrow$ centeral station wants to deliver sequences of messages, each intended for one of the receivers

Technical Application of IDentification

- Scenario $\rightarrow$ local-area/radio networks and downlink satellite communications
- Goal $\rightarrow$ centeral station wants to deliver sequences of messages, each intended for one of the receivers

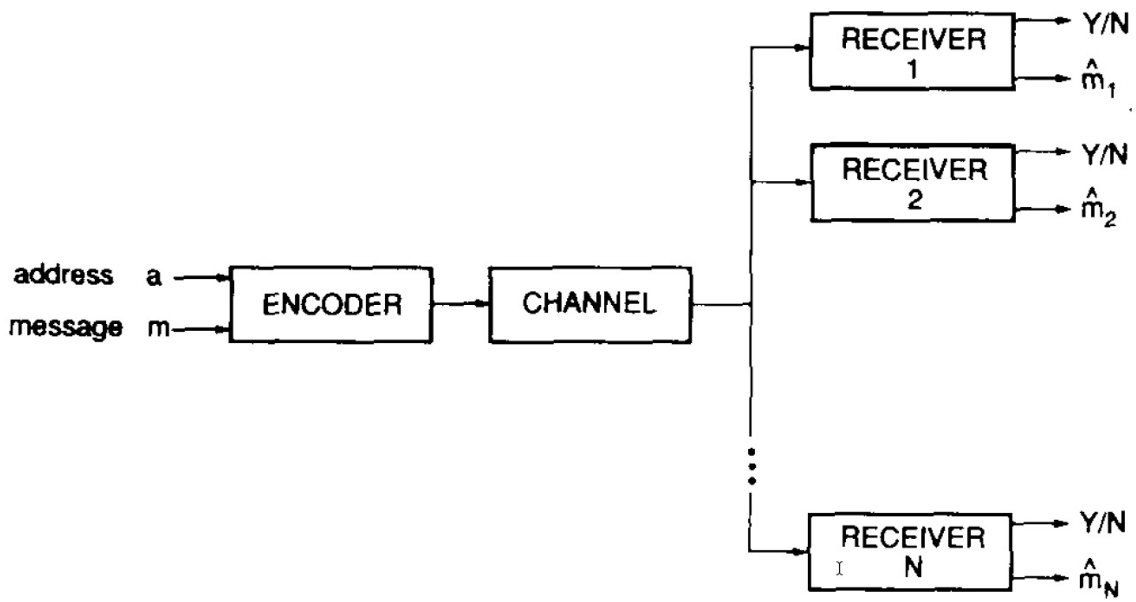


Figure: Identification plus transmission through a noisy channel [2]

[2] T. S. Han and S. Verdb, "New results in the theory and applications of identification via channels," IEEE Trans. Inform. Theory, vol. 38, pp. 14-25, Jan. 1992.

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

Technical Application of IDentification

- Scenario $\rightarrow$ local-area/radio networks and downlink satellite communications
- Goal $\rightarrow$ centeral station wants to deliver sequences of messages, each intended for one of the receivers

- (Decoupled Coding) $\rightarrow$
  juxtaposing ID code and transmission code to send address and message respectively
  - (address identification rate) $\frac{1}{n}\log\log N_n \rightarrow C_T$ is achievable if $\frac{1}{n}\log M \rightarrow 0$
  - (message transmission rate) $\frac{1}{n}\log M \rightarrow C_T$ is achievable if $\frac{1}{n}\log\log N_n \rightarrow 0$
- (Coupled Coding) $\rightarrow$
  IDentification plus Transmission problem code (IT) can achieve both rates simultaneously

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

Construction of ID Code (random selection)

1. Let $\mathscr{L}'$ and $\mathscr{L}''$ be two transmission codes, $\xrightarrow[\text{gaurantees existence of}]{\text{Shannon's coding theorem}}$
   - $(n, M', 2^{-n\delta})$ code $\mathscr{L}' = \{(u_j^{'}, D_j^{'})|j \in [M']\}$ with $M' = \lceil 2^{n(C-\varepsilon)} \rceil$
   - $(\lceil \sqrt{n} \rceil, M'', 2^{-\sqrt{n}\delta})$ code $\mathscr{L}'' = \{(u_k^{''}, D_k^{''})|k \in [M'']\}$ with $M'' = \lceil 2^{\varepsilon\sqrt{n}} \rceil$

2. Let T be a family of maps $T = \{T_i|i \in [N]\}$ where $T_i : [M'] \to [M'']$
3. Let $\mathscr{U}_i := \{u_j^{'}.u_{T_i(j)}^{''}|j \in [M']\}$ and $D_i = \bigcup_{j=1}^{M'} D_j^{'} \times D_{T_i(j)}^{''}$
4. System $\{(Q(.|i), D_i)|i \in [N]\}$ is an ID code constructed from $\mathscr{L}'$ and $\mathscr{L}''$
5. Let U_{ij} be independent RV s.t. $Pr\{U_{ij} = u_j^{'}.u_k^{''}\} = \frac{1}{M''}$
   $i \in [N], j \in [M'], k \in [M'']$
6. Let $\overline{\mathscr{U}}_i = \{U_{i1}, \cdots, U_{iM'}\} \qquad \forall i \in [N]$
7. Let $D(\overline{\mathscr{U}}_i) = \bigcup_{j=1}^{M'} D(U_{ij})$ where $D(U_{ij}) = D_j^{'} \times D_k^{''}$
8. System $\{(\overline{Q}(.|i), D(\overline{\mathscr{U}}_i))|i \in [N]\}$ achieves small maximal error probabilities

Construction of ID Code (concatenation)

- 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:
- $\beta_i \to 1$, $\rho_i \to 1$, $\mu_i \to 0$
- Three-layer concatenated code $C_1 \circ C_2 \circ C_3$ denoted by $[q, k, t]$ with:
  - $C_1 = [q]PPM$
  - $C_2 = [q, k]$ Reed-Solomon
  - $C_3 = [q^k, q^t]$ Reed-Solomon
  - $t \leq k \leq q =$ prime

  is a $(q^{k+2}, q^{kq^t}, q^{k+1}, kq^k + q^{1+t})$ binary constant-weight code
- Let $\{C_i\} = [q_i, k_i, t_i]$ be sequence of three-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 three-layer concatenated code with a transmission code (n, e^{nR}, λ) gives an IT code which subsequently ID code can be constructed from

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

Concluding Remarks

1. In contrast to single exponential behavior of conventional transmission codes, in IDentification for any channel (not necessarily discrete or memoryless) ID codes can asymptotically gaurantee transmission of $e^{e^{nC}}$ messages with n uses of a noisy channel while keeping error probabilities arbitrarily zero
2. Transmission capacity and IDentification capacity coincides (DMC)
3. Despite of Shannons's formulation, ID decoder selects a list of messages
4. List size grows doubly exponential in block length
5. Decoding reliability is expressed in terms of type I/II errors probabilities
6. IDentification can be used where the recipient is only interested in verify if a certain message is the transmitted message or not (P2MP, remote alarm service)

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

Questions

Thanks For Attendance