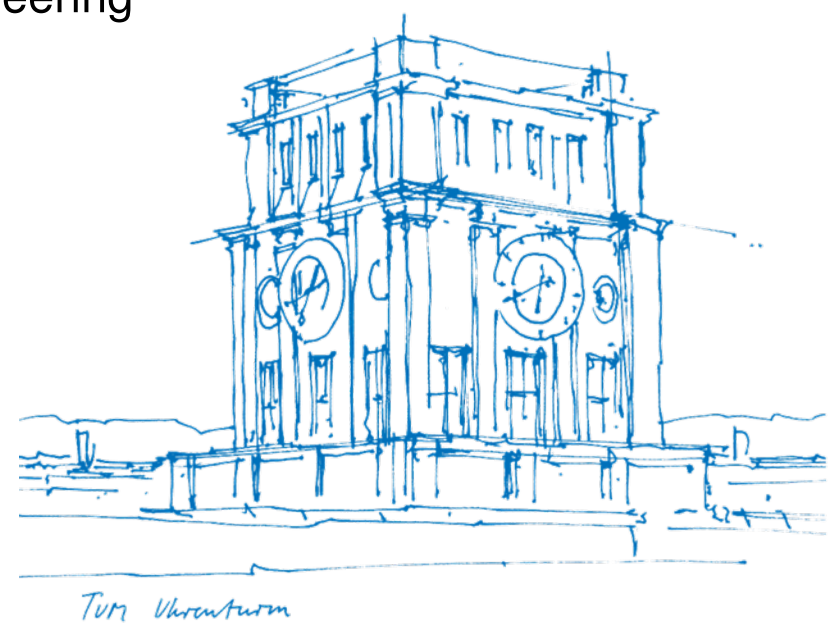
IDentification, Tag codes end Error-correction codes (or "A different way of using Error-correction codes")

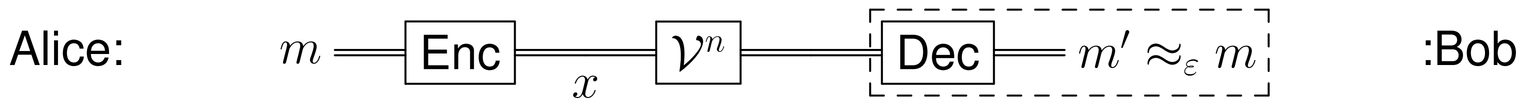
Roberto Ferrara
Technical University of Munich
Department of Electrical and Computer Engineering
Institute for Communications Engineering

13th March 2019



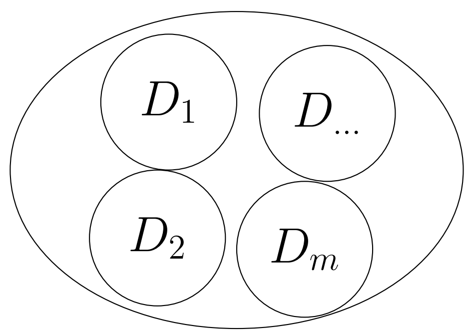
Transmission vs Identification

Transmission (Shannon coding) over $\mathcal{V}^n$:



(n, M, ε) code $\{x_m, D_m\}_{m\in[M]}$:

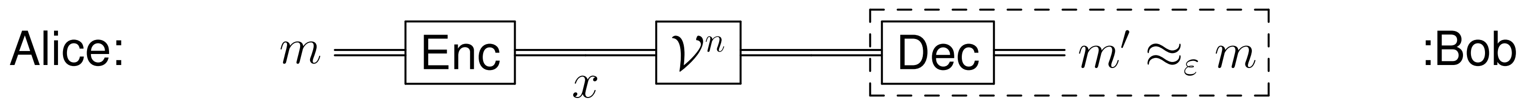
$$\frac{1}{M}\sum \mathcal{V}^n(D_m|x_m) \geq 1-\varepsilon$$

The decoding sets are disjoint: 

The transmission capacity is the optimal $C = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\log M/n$.

Transmission vs Identification

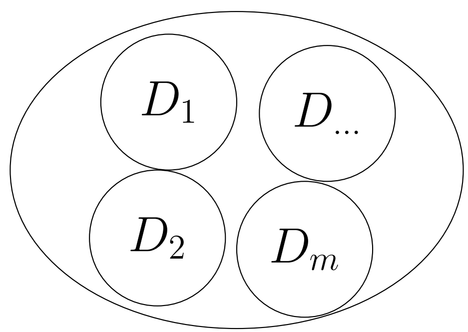
Transmission (Shannon coding) over $\mathcal{V}^n$:



(n, M, ε) code $\{\boldsymbol{X_m}, D_m\}_{m\in[M]}$:

$$\frac{1}{M}\sum \mathcal{V}^n(D_m|\boldsymbol{X_m}) \geq 1-\varepsilon$$

The decoding sets are disjoint:



The transmission capacity is the optimal $C = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\log M/n$.

Transmission vs Identification

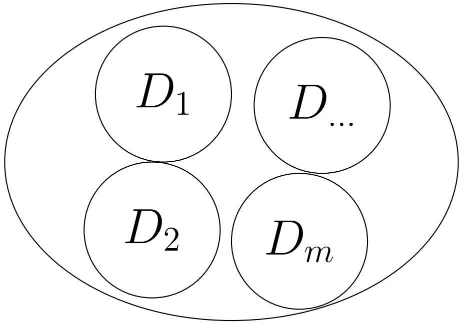
Transmission (Shannon coding) over $\mathcal{V}^n$:

Alice: $m \Longrightarrow \boxed{\text{Enc}} \xrightarrow[x]{} \boxed{\mathcal{V}^n} \Longrightarrow \boxed{\text{Dec}} \Longrightarrow m' \approx_\varepsilon m$:Bob

(n, M, ε) code $\{\boldsymbol{X_m}, D_m\}_{m \in [M]}$:

$$\mathbf{min}\, \mathcal{V}^n(D_m | \boldsymbol{X_m}) \geq 1 - \varepsilon$$

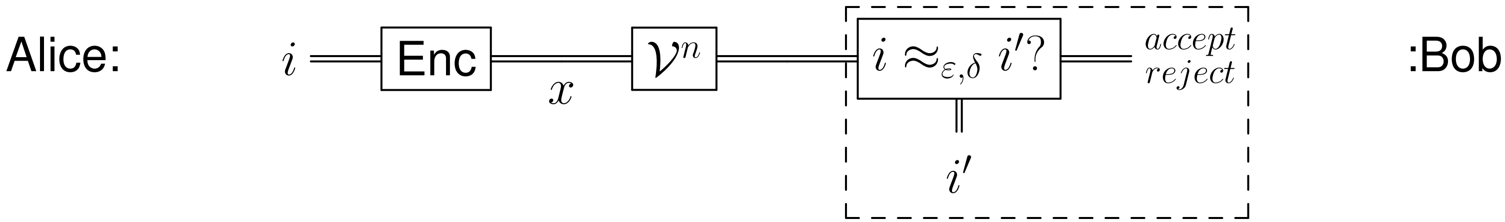
The decoding sets are disjoint:



The transmission capacity is the optimal $C = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \log M/n$.

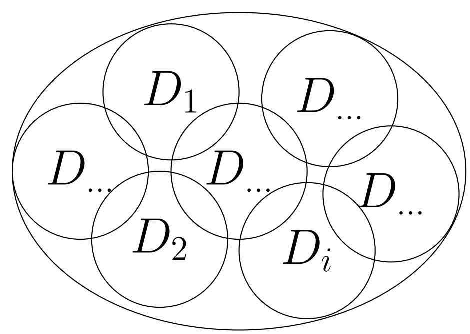
Transmission vs Identification

Identification (Ahlswede-Dueck coding?) over $\mathcal{V}^n$:



(n, I, ε) code $\{\boldsymbol{X_i}, D_i\}_{i\in[I]}$:

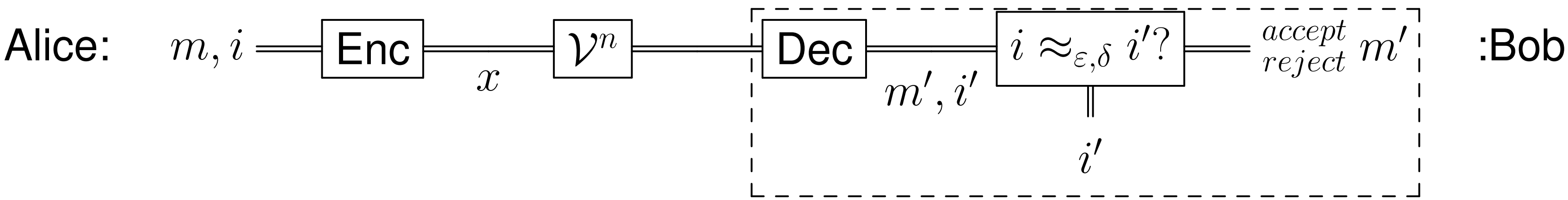
$$\min \mathcal{V}^n(D_i|\boldsymbol{X_i}) \geq 1-\varepsilon \qquad\qquad \boldsymbol{\max \mathcal{V}^n(D_i|X_j) \leq \varepsilon}$$

The "decoding"/testing sets can overlap: 

The identification capacity is the optimal $C_{ID} = \lim_{\varepsilon\to 0}\lim_{n\to\infty} \mathbf{\log\log I}/n$. $\mathbf{C_{ID} = C}$!.
Asymptotically small pairwise overlap, but exponentially many overlaps.
Pairwise overlap is more stringent than pairwise distinguishability.

Transmission AND Identification

Transmission-Identification (Han-Verdù coding?) over $\mathcal{V}^n$:



(n, M, I, ε) code $\{x_{m,i}, D_{m,i}\}_{i\in[I]}$: $D_{m,i} \perp D_{m',i}$ and

$$\min_i \frac{1}{M}\sum_m \mathcal{V}^n(D_{m,i}|x_{m,i}) \geq 1-\varepsilon \qquad \max \mathcal{V}^n(D_i|X_j) \leq \varepsilon$$

$$\Big(\Rightarrow \quad \min_i \mathcal{V}^n(D_i|X_i) \geq 1-\varepsilon\Big)$$

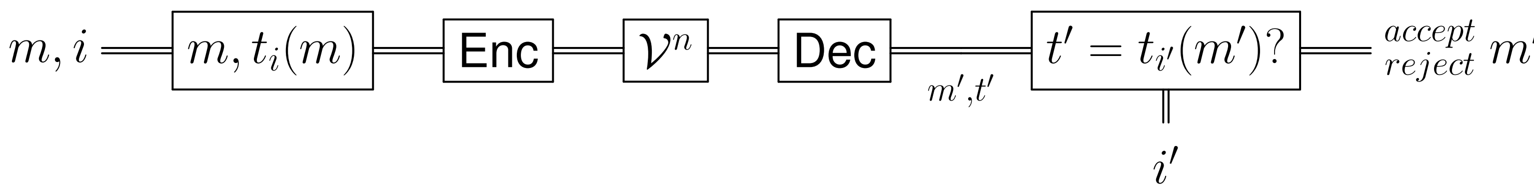
The transmission-identification capacity is the optimal

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}(\log M, \log\log I).$$

(C, C) is achievable!.

Tag codes

Separation coding: converting a good transmission code into a good identification code is enough.
Given a capacity achieving transmission code, an transmission-identification capacity is achieved choosing tag (labelling) functions $t_i : [M] \to [q]$:



A $[I, M, q, \Omega/M]$ tag code is a collection of I functions from $[M]$ to $[q]$ with pairwise overlap at most Ω.

Need tag codes $[I, M, q, \varepsilon]$ with:

1. size I exponential in M
2. bits of output $\log q$ sublinear in bits of input $\log M$
3. asymptotically zero ε

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

Tag codes = Error-correction codes

$(M =$ blocklength, $I =$ size, $d)_q$ error-correction codes (without decoding) are tag codes

$$I \text{ codewords} \left\{ \begin{array}{l} \overbrace{\vec{c}_1 = c_{11} \dots c_{1M}}^{M \text{ symbols of size } s} \\ \vec{c}_{\dots} = \dots \\ \vec{c}_I = c_{I1} \dots c_{IM} \end{array} \right. \qquad d = M - \Omega$$

For identification we need

$$\frac{\log \log I}{\log M} \to 1 \qquad \frac{\log q}{\log M} \to 0 \qquad \frac{d}{M} \to 1.$$

From the Gilbert-Varshamov bound

$$I > \frac{q^M}{\sum_{k=0}^{d-1} \binom{M}{k} (q-1)^k} > \frac{q^M}{2^M q^d} = \frac{q^\Omega}{2^M}$$

Choosing $\Omega = M - d = \lfloor \frac{2}{\log q} M \rfloor$ then

$$I > 2^M \qquad \varepsilon \leq 2/\log q$$

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

Tag codes = Error-correction codes

$(M =$ blocklength, $I =$ size, $d)_q$ error-correction codes (without decoding) are tag codes

$$I \text{ codewords} \begin{cases} \overbrace{\vec{c}_1 = c_{11} \dots c_{1M}}^{M \text{ symbols of size } s} \\ \vec{c}_{\dots} = \dots \\ \vec{c}_I = c_{I1} \dots c_{IM} \end{cases} \qquad d = M - \Omega$$

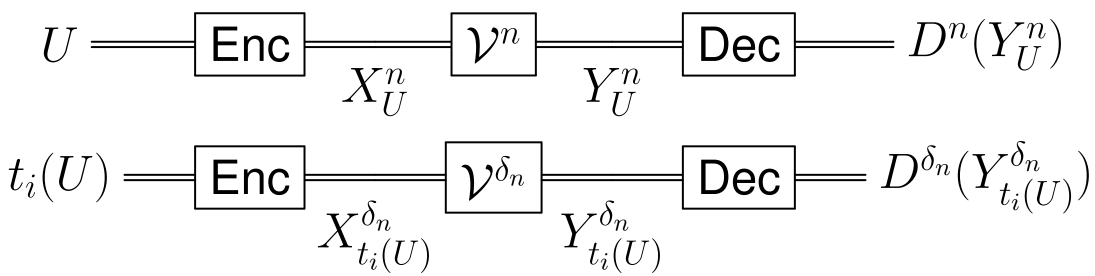
For identification we need

$$\frac{\log \log I}{\log M} \to 1 \qquad \frac{\log q}{\log M} \to 0 \qquad \frac{d}{M} \to 1.$$

There always exist

- $(M, 2^M, M(1 - 2/\log q))_q$ error-correction codes, or equivalently
- $[2^M, M, q, 2/\log q]$ tag codes.

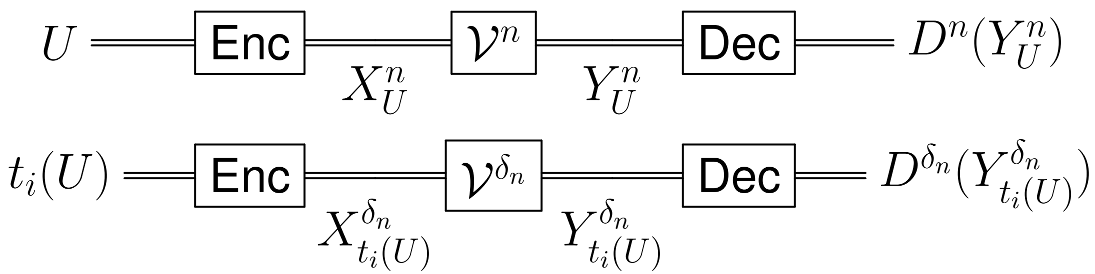
Achievability: proof sketch (for identification)



$\delta_n \in o(n)$

$$
\begin{aligned}
\mathcal{V}^{n+\delta_n}(D_j^{n+\delta_n}|X_i^{n+\delta_n}) &= Pr\Big[t_j \circ D^n(Y_U^n) \neq D^{\delta_n}\big(Y_{t_i(U)}^{\delta_n}\big)\Big] \\
&\leq Pr[D^n(Y_U^n) \neq U] + Pr\Big[t_j \circ D^n(Y_U^n) \neq D\big(Y_{t_i(U)}^{\delta_n}\big)|D^n(Y_U^n) = U\Big] \\
&\leq Pr[D^n(Y_U^n) \neq U] + Pr\Big[t_j(U) \neq D^{\delta_n}\big(Y_{t_i(U)}^{\delta_n}\big)\Big] \\
&\leq Pr[D^n(Y_U^n) \neq U] + Pr\Big[D^{\delta_n}\big(Y_{t_i(U)}^{\delta_n}\big) \neq t_i(U)\Big] + Pr[t_j(U) \neq t_i(U)] \\
&\leq \varepsilon_n + \varepsilon_{\delta_n} + \frac{2}{\log q_{\delta_n}} \\
&\leq \varepsilon_n + \varepsilon_{\delta_n} + \frac{2}{\delta_n(C - \varepsilon_{\delta_n})}
\end{aligned}
$$

Achievability: proof sketch (for identification)



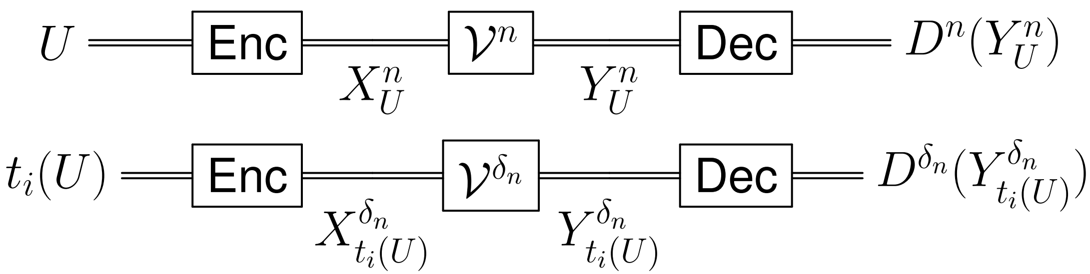
$\delta_n \in o(n)$

$$
\begin{aligned}
\mathcal{V}^{n+\delta_n}(D_j^{n+\delta_n} | X_i^{n+\delta_n}) &= Pr\left[t_j \circ D^n(Y_U^n) \neq D^{\delta_n}\left(Y_{t_i(U)}^{\delta_n}\right)\right] \\
&\leq Pr[D^n(Y_U^n) \neq U] + Pr\left[D^{\delta_n}\left(Y_{t_i(U)}^{\delta_n}\right) \neq t_i(U)\right] + Pr[t_j(U) \neq t_i(U)] \\
&\leq \varepsilon_n + \varepsilon_{\delta_n} + \frac{2}{\delta_n(C - \varepsilon_{\delta_n})}
\end{aligned}
$$

$$
\mathcal{V}^{n+\delta_n}(D_i^{n+\delta_n} | X_i^{n+\delta_n}) \geq 1 - \varepsilon_n - \varepsilon_{\delta_n}
$$

$$
\frac{1}{n+\delta_n} \log\log I = \frac{n}{n+\delta_n} \frac{1}{n} \log M \geq \frac{n}{n+\delta_n}(R - \varepsilon_n) \to R
$$

Randomness and (Transmission-)Identification

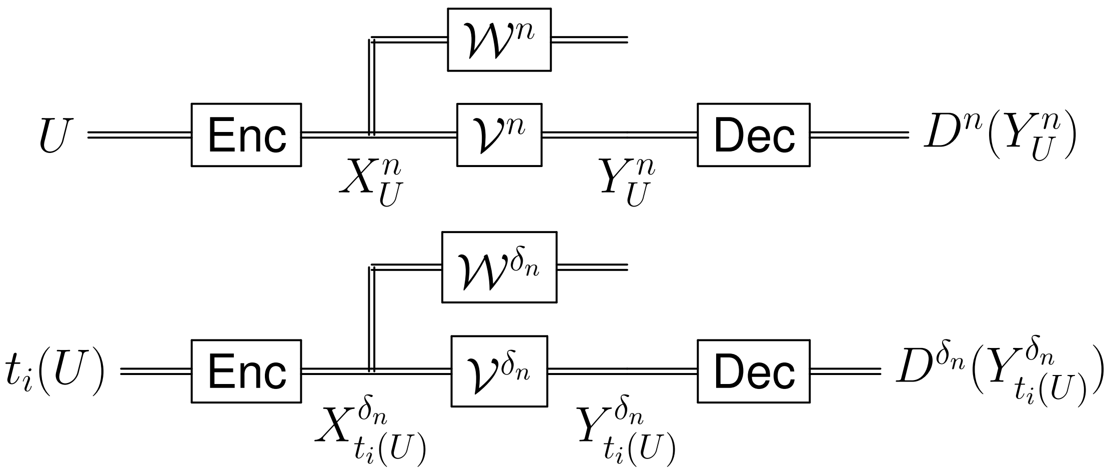


- The achievable rate depends only on the size of the common randomness.
- If non-transmission sources of common randomness are present, the identification rate increases (unlike for transmission)
- However, identification capacity is zero if transmission capacity is zero.

Existing conjecture: Identification and common-randomness capacities are always equal when transmission capacity is non-zero.

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

Secrecy of Identification



- if secrecy of U is not needed (e.g., U is randomness, not a message) we can ignore the wiretap channel $\mathcal{W}^n$.
- to ensure the secrecy of the identity only non-zero secret capacity is needed against $\mathcal{W}^{\delta_n}$.

Secret identification capacity is still common-randomness capacity, even if secret key/transmission capacity are significantly lower (but non-zero).

Motivation

- (transmission-identification) Communication to a specific receiver among many receivers listening to the same channel with feedback
- (transmission-identification) watermarking
- (identification) Potential for very low-latency were only few outcomes among many are relevant (automotive, ...)

Could be easy to provide in already implemented codes...

Closing remarks

Previous work:

- Analog results for compound and arbitrarily-varying channels, with and without wiretap, PUFs, etc.
- Analog results for quantum outputs with no advantage from incompatible "decodings"/tests.
- All proofs relied on a random tag code argument.
- Partial results for quantum channels (missing converses,)

Future Work:

- Exploit the connection to channel resolvability to prove that common-randomness cost is an upper bound.
- Prove equivalence of distillable common-randomness and common-randomness cost to prove the common-randomness$=$identification conjecture.