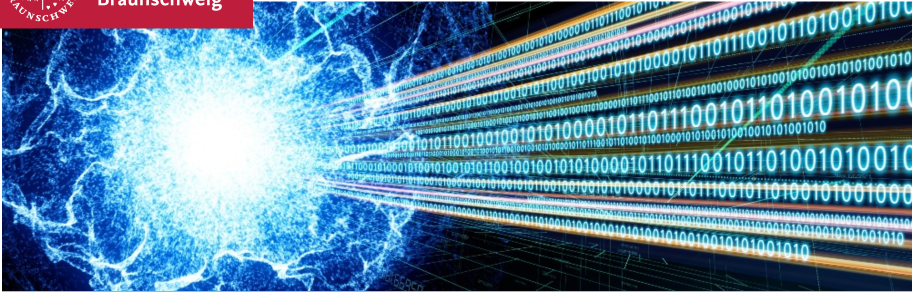
Technische Universität Braunschweig

Institut für Nachrichtentechnik



Message Identification for Future Communication Systems

Christian Deppe

Algorithmic Structures for Uncoordinated Communications and Statistical Inference in Exceedingly Large Spaces, BIRS, March 10-15, 2024

Overview

1. Shannon's Channel Coding
2. Deterministic Identification
3. Randomized Identification
4. Gaussian Channels
5. Feedback as a Resource for Randomness
6. Further Research

Shannon's Channel Coding

- Alice has to transmit a message $m \in \mathcal{M} = \{1, 2, \dots, M\}$ to Bob
- Alice uses a block code $\mathcal{X}^n = \{0, 1, \dots, q-1\}^n$
- $W = \{W(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ is a stochastic matrix.
- The probability for a sequence $y \in \mathcal{Y}^n$ to be received if $x^n \in \mathcal{X}^n$:

$$W^n(y^n|x^n) = \prod_{t=1}^{n} W(y_t|x_t)$$

- Bob receives a word in $\mathcal{Y}^n$.

Goal: Bob has to decode the correct message with a small decoding error

$\Longrightarrow$ Finding the correct answer to: "What was Alice's message?"

Shannon's Channel Coding

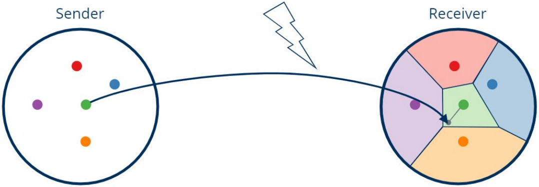
Definition

A (deterministic) $(\mathrm{n}, \mathrm{M}, \lambda)$ code for W is a set of pairs $\{(\mathrm{u_i}, \mathcal{D}_\mathrm{i}) : \mathrm{i} \in \mathcal{M}\}$

$$\mathrm{u_i} \in \mathcal{X}^\mathrm{n}, \mathcal{D}_\mathrm{i} \subset \mathcal{Y}^\mathrm{n} \quad \text{for all } \mathrm{i} \in \mathcal{M} \tag{1}$$

$$\mathcal{D}_\mathrm{i} \cap \mathcal{D}_\mathrm{j} = \emptyset \text{ for all } 1 \leq \mathrm{i}, \mathrm{j} \leq \mathrm{n}, \mathrm{i} \neq \mathrm{j} \tag{2}$$

$$\mathrm{W^n}\left(\mathcal{D}_\mathrm{i} | \mathrm{u_i}\right) \geq 1 - \lambda \forall \mathrm{i} \in \mathcal{M} \tag{3}$$



Bob decided that message i was send if he receive a word in $\mathcal{D}_\mathrm{i}$.

Which triples (n, M, λ) are possible?

- We require, that a certain number $M(n)$ of messages can be transmitted over the channel. It is reasonable to set them exponential in n $\left(M(n) = e^{R \cdot n}\right)$, since in the noiseless case $(w(y|x) = 0 \text{ for } y \neq x)$ $|\mathcal{X}|^n$ messages are possible. R is denoted as the rate of the code. Let $\lambda(R, n)$ be the smallest error probability for (n, e^{Rn}) codes and define the largest error exponent as $E(R) = \lim_{n \to \infty} \frac{1}{n} \log \lambda(R, n)$.
- We require that $\lambda \in (0, 1)$ is fixed. Let $M(n, \lambda)$ denote the maximum number of messages that can be transmitted over the channel for given word length n and probability of error λ.

Shannon's Channel Coding

In his Fundamental Theorem Shannon proved that $M(n, \lambda)$ grows exponentially in n. More exactly, he proved that

$$\liminf_{n \to \infty} \frac{\log M(n, \lambda)}{n}$$

exists and does not depend on $\lambda \in (0, 1)$. Shannon defined this limit as the capacity of the channel.

Transmission and local randomness

Definition

A randomized (n, M, λ) for a DMC W transmission code is a family of pairs

$$\{(Q_i, D_i)\,|i = 1, \ldots, M\} \quad \text{with}$$

$$Q_i \in \Pr(\mathcal{X}^n), \quad D_i \subset \mathcal{Y}^n \forall 1 = 1, \cdots, M \tag{4}$$

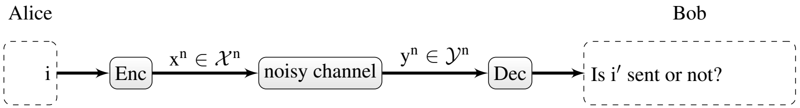
$$D_i \cap D_j = \emptyset \forall i \neq j \tag{5}$$

$$\sum_{x^n \in \mathcal{X}^n} Q_i(x^n) W^n(D_i|x^n) \geq 1 - \lambda \forall i = 1, \ldots, M \tag{6}$$

Lemma

Let W be a DMC. A deterministic (n, M, λ) transmission code for W exists if and only if a randomised (n, M, λ) transmission code exists.

Post-Shannon: Identification (ID)



hypothesis testing problem

Ahlswede/Dueck Picture 1989[1]

[1] R. Ahlswede and G. Dueck, "Identification via channels," in IEEE Transactions on Information Theory, vol. 35, no. 1, pp. 15-29, Jan. 1989, doi: 10.1109/18.42172.

Complexity of Communication and Identification

Model:

- Alice chooses $i \in \{1, 2, \ldots, 2^m\}$.
- Bob chooses $j \in \{1, 2, \ldots, 2^m\}$.
- Goal: Bob want to calculate $f(i, j)$ with small error.
- Alice and Bob are connected via a channel.

In message identification one consider:

$$f = (i, j) \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Deterministic Identification (DI) over DMCs

Definition

An $(\mathrm{M}, \mathrm{n}, \lambda_1, \lambda_2)$-DI code for DMC $\mathcal{W}$ is a system $\{(\mathrm{u}_\mathrm{i}, \mathcal{D}_\mathrm{i})\}_{\mathrm{i} \in [1:\mathrm{L}(\mathrm{n},\mathrm{R})]}$ subject to

1. Code size: $\mathrm{M} = 2^{\mathrm{nR}}$
2. Code-word: $\mathrm{u}_\mathrm{i} \in \mathcal{X}^\mathrm{n}$, decoding regions: $\mathcal{D}_\mathrm{i} \subset \mathcal{Y}^\mathrm{n}$
3. Input constraint: $\mathrm{n}^{-1} \sum_{\mathrm{t}=1}^{\mathrm{n}} \phi(\mathrm{u}_{\mathrm{i},\mathrm{t}}) \leq \mathrm{A}$ with $\phi : \mathcal{X} \to [0, \infty)$
4. Error requirement type I: $\mathrm{W}^\mathrm{n}(\mathcal{D}_\mathrm{i} | \mathrm{u}_\mathrm{i}) > 1 - \lambda_1$
5. Error requirement type II: $\mathrm{W}^\mathrm{n}(\mathcal{D}_\mathrm{i} | \mathrm{u}_\mathrm{j}) \underset{\mathrm{i} \neq \mathrm{j}}{<} \lambda_2$

DI Capacity of DMC

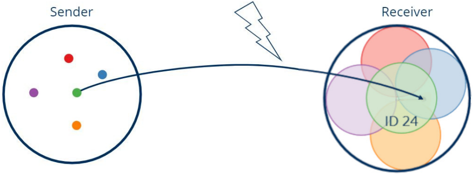
Theorem

Let $\mathcal{W}$ be a DMC with distinct rows in channel matrix. Then the DI capacity with exponential code size and under input constraint is given by

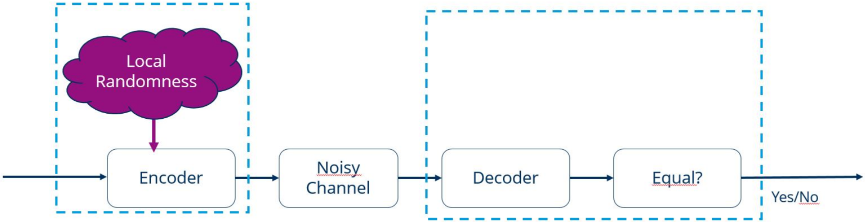
$$\mathbb{C}_{\mathrm{DI}}(\mathcal{W}) = \max_{p_X \,:\, \mathbb{E}\{\phi(X)\} \leq A} H(X)$$

M. J. Salariseddigh, U. Pereg, H. Boche, and C. Deppe, "Deterministic identification over channels with power constraints," IEEE Int'l Conf. Commun. (ICC), 2021

Deterministic Identification



Randomized Identification [1]



- Originally introduced by Ahlswede and Dueck (1989)
- Capacity was established with randomness at encoder

[1] R. Ahlswede and G. Dueck, "Identification via Channels", IEEE Trans. Inf. Theory, 1989

Randomized Identification (ID)-Code

Randomized ID-code

A randomized $(n, N, \lambda_1, \lambda_2)$ ID-code for a discrete memoryless channel (DMC) W is a family of pairs $\{(Q_i, \mathcal{D}_i) | i = 1, \dots, N\}$ with $\lambda_1, \lambda_2 \leq \lambda < \frac{1}{2}$ and $\forall i \in \{1, \dots, N\}$:

- $Q_i \in \mathcal{P}(\mathcal{X}^n),\ \mathcal{D}_i \subseteq \mathcal{Y}^n$
- $\sum_{x^n \in \mathcal{X}^n} Q_i(x^n) W^n(\mathcal{D}_i^c | x^n) \leq \lambda_1 \Longleftarrow$ channel noise
- $\sum_{x^n \in \mathcal{X}^n} Q_j(x^n) W^n(\mathcal{D}_i | x^n) \leq \lambda_2 \Longleftarrow$ ID-code

$\Rightarrow$ Randomization is crucial to establish capacity!

ID Coding Theorem [1] [2]

Theorem

Let W be a finite DMC and $\mathrm{N}(\mathrm{n}, \lambda)$ the maximal number s.t. an $(\mathrm{n}, \mathrm{N}, \lambda_1, \lambda_2)$ ID-code for W exists with $\lambda_1, \lambda_2 \leq \lambda$ then:

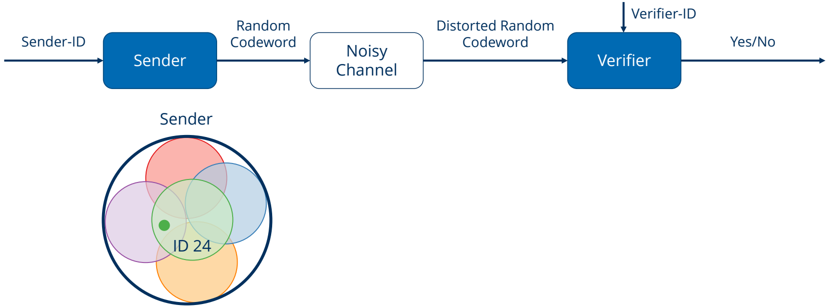
$$\mathrm{C_{ID}}(\mathrm{W}) = \mathrm{C}(\mathrm{W}), \quad \forall \lambda \in (0, \frac{1}{2}),$$

where $\mathrm{C}(\mathrm{W})$ denotes the Shannon transmission capacity of W, $\mathrm{C_{ID}}(\mathrm{W}) \triangleq \lim_{\mathrm{n}\to\infty} \frac{1}{\mathrm{n}} \log\log \mathrm{N}(\mathrm{n}, \lambda)$

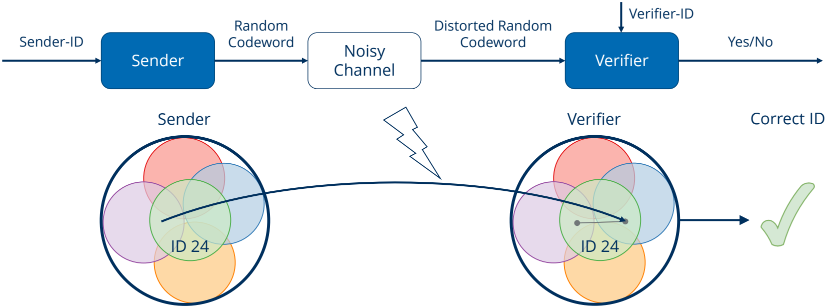
[1] R. Ahlswede and G. Dueck, "Identification via channels," in IEEE Transactions on Information Theory, vol. 35, no. 1, pp. 15-29, Jan. 1989

[2] T. S. Han and S. Verdu, "New results in the theory of identification via channels," in IEEE Transactions on Information Theory, vol. 38, no. 1, pp. 14-25, Jan. 1992.

Identification Codes



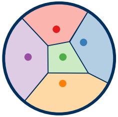
Identification Codes



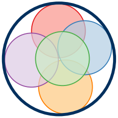
Each ID has set of codewords, one is picked **randomly**
Codeword sets **overlap** and don't have to be convex
Sender and verifier are identical → **ID doesn't require decoding**, only encoding

Identification Capacity

Transmission: $N = 2^{nR}$



ID: $N = 2^{2^{nR}}$

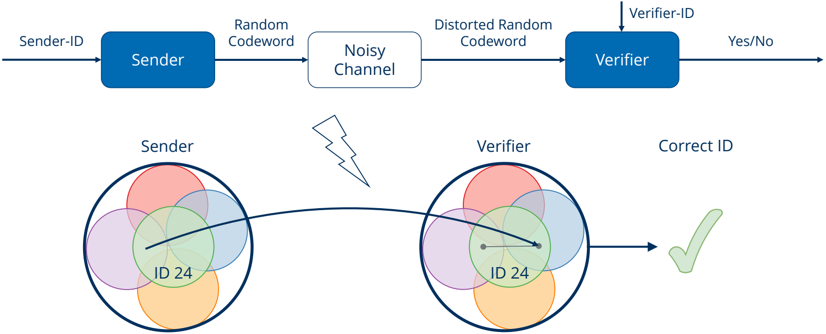


Discrete Memoryless Channel (DMC):

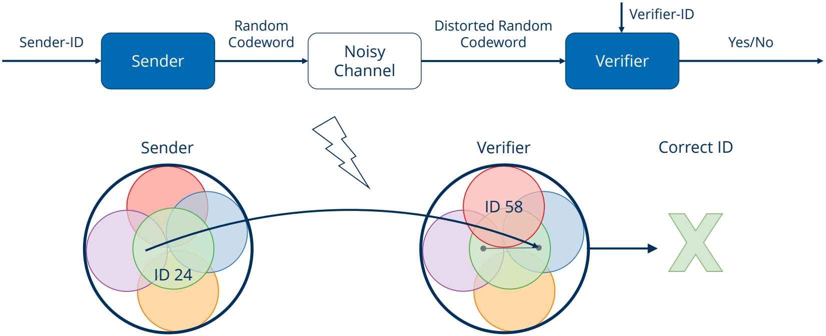
N	number of entities
n	number of bits
R	rate (0.0-1.0)

→ The number of identifiable entities **grows double exponentially** in block size, at the cost of a **new kind of error**

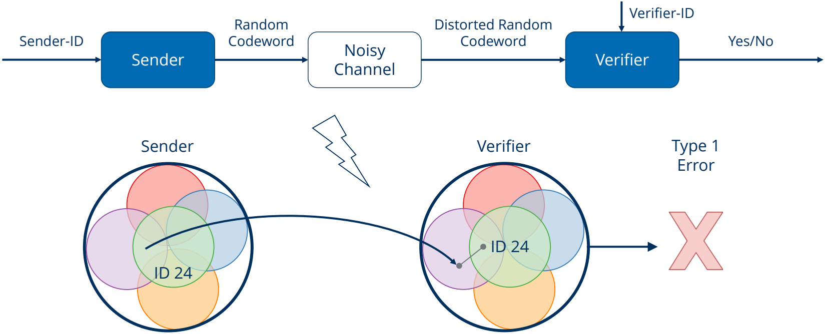
Identification - Correct Positive



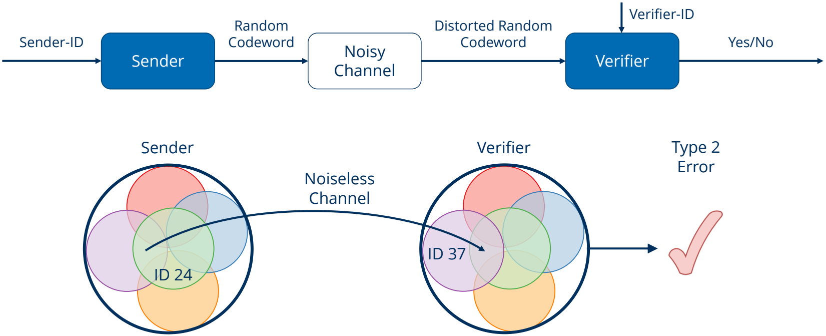
Identification - Correct Negative



Identification - False Negative



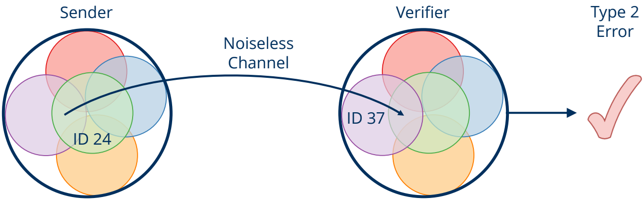
Identification - False Positive



→ **Hypothesis testing** of {maybe, no}

Identification - Error Types

	Caused by	Reduced by	Removed by
Type 1 errors	Noisy channel	Shannon channel coding	Shannon channel coding
Type 2 errors	Overlapping codeword sets	Identification codes	-



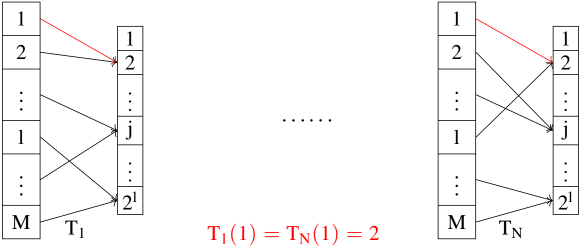
Achievability with functions

To send a message i, we prepare a set of coloring functions $\{T_i,\ i = 1, \ldots, N\}$ known by the sender and the receiver

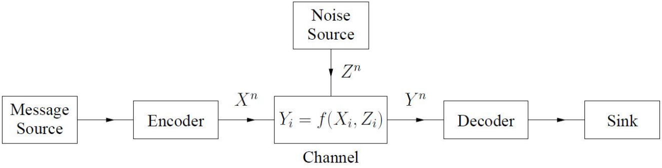
Achievability with functions

To send a message i, we prepare a set of coloring functions $\{T_i,\ i = 1, \ldots, N\}$ known by the sender and the receiver

$$
\begin{aligned}
T_i : \{1, \ldots, M\} &\longrightarrow \{1, \ldots, 2^l\} \\
: \quad \underbrace{l}_{\text{coloring number}} &\mapsto \underbrace{T_i(l)}_{\text{color, depend on } f_i}
\end{aligned}
$$



The Gaussian Channel



- We consider the AWGN (additive white Gaussian noise) channel.
- The signal at the receiver contains, in addition to the useful signal, additive noise, which represents a realization of a white Gaussian process.
- "Power" constraint: For a codeword $(x_1, x_2, \ldots, x_k)$ transmitted through the channel, we have:

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P.$$

Transmission Capacity of the Gaussian Channel

The channel capacity for the power-constrained channel is given by:

$$C(G) = \max\left\{I(X;Y) : f \text{ s.t. } E\left(X^2\right) \leq P\right\} = \frac{1}{2}\log\left(1 + \frac{P}{N}\right)$$

RI Coding Theorem [1]

Theorem

For the AWGN holds

$$C_{\mathrm{ID}}(G) = C(G), \quad \forall \lambda \in (0, \frac{1}{2}).$$

[1] Labidi, W., Deppe, C., Boche, H. (2020). Secure identification for Gaussian channels and identification for multi-antenna gaussian channels. arXiv preprint arXiv:2011.06443.

DI Capacity of the Gaussian Channel

Theorem

The DI capacity of the Gaussian channel $\mathscr{G}$ is given by

$$\mathbb{C}_{\mathrm{DI}}(\mathscr{G}) = \infty \; . \tag{7}$$

Proof Sketch (Achievability)

Codebook construction: Choose codewords in spheres such that the distance is "big enough" and that the power constraint is fullfilled!

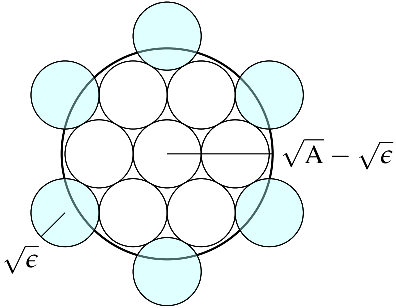


Illustration of a sphere packing, where small spheres of radius $r_0 = \sqrt{\epsilon}$ cover a bigger sphere of radius $r_1 = \sqrt{A} - \sqrt{\epsilon}$. The small spheres are disjoint from each other and have a non-empty intersection with the big sphere.

Proof Sketch (Achievability)

Encoding Given a message $\mathrm{i} \in [\![2^{\mathrm{nR}}]\!]$, transmit $\bar{\mathrm{x}} = \bar{\mathrm{u}}_{\mathrm{i}}$.

Decoding Let $\delta > 0$. To identify whether a message $\mathrm{j} \in \mathcal{M}$ was sent, the decoder checks whether the channel output y belongs to the following decoding set,

$$\mathcal{D}_{\mathrm{j}} = \left\{ \bar{\mathrm{y}} \in \mathbb{R}^{\mathrm{n}} \,:\, \|\bar{\mathrm{y}} - \bar{\mathrm{u}}_{\mathrm{j}}\| \leq \sqrt{\sigma_{\mathrm{Z}}^2 + \delta} \right\} . \tag{8}$$

Coding Scale: Deterministic Identification

$L(n, R)$

$2^{2^{nR}}$ $\mathbb{C}_{DI}(\mathcal{W}, L_{\text{d-exp}}) = 0$

2^{nR} $\mathbb{C}_{DI}(\mathcal{W}, L_{\exp}) = \infty$

S., Pereg, Boche & Deppe, ICC 2021

Coding Scale: Deterministic Identification

$L(n, R)$

$2^{2^{nR}}$ $\mathbb{C}_{DI}(\mathcal{W}, L_{\text{d-exp}}) = 0$

What is the correct scale?

2^{nR} $\mathbb{C}_{DI}(\mathcal{W}, L_{\exp}) = \infty$

S., Pereg, Boche & Deppe, ICC 2021

DI Capacity of the Gaussian Channel

Theorem

The DI capacity of the Gaussian channel $\mathscr{G}$ in the $2^{n\log(n)}$-scale, i.e., for $L(n,R) = 2^{(n\log n)R}$ is bounded by

$$\frac{1}{4} \leq \mathbb{C}_{\mathrm{DI}}(\mathscr{G}, L) \leq 1 \; . \tag{9}$$

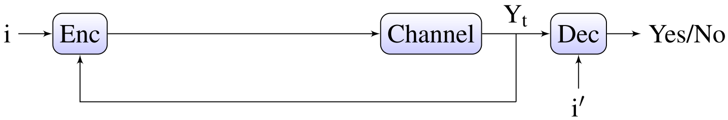
Hence, the DI capacity is infinite in the exponential scale and zero in the double-exponential, i.e.,

$$\mathbb{C}_{\mathrm{DI}}(\mathscr{G}, L) = \begin{cases} \infty & \text{for } L(n,R) = 2^{nR} \; , \\ 0 & \text{for } L(n,R) = 2^{2^{nR}} \; . \end{cases} \tag{10}$$

The Power of Randomness

If we have no direct access to randomness, can we use resources to get randomness?

DI with Noiseless Feedback



- Ahlswede and Dueck considered channels with discrete alphabets
- The results is extended to the Gaussian channel

R. Ahlswede and G. Dueck, "Identification in the presence of feedback-a discovery of new capacity formulas," IEEE Trans. Inf. Theory, 1989 W. Labidi, H. Boche, C. Deppe and M. Wiese, "Identification over the Gaussian Channel in the Presence of Feedback," IEEE Int'l Symp. Inf. Theory (ISIT), 2021 [arXiv:2102.01198, 2021]

DIF Capacity of a DMC

Theorem

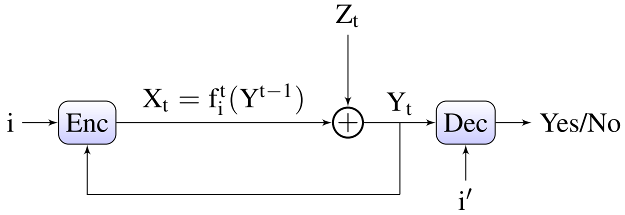
Let $\mathbb{C}_{\text{DIF}}(\mathcal{W})$ and $\mathbb{C}(\mathcal{W})$ be the DIF capacity and the Shannon capacity of the DMC $\mathcal{W}$, respectively. Then the deterministic identification capacity with feedback is given by

$$\mathbb{C}_{\text{DIF}}(\mathcal{W}) = \begin{cases} \max_{x \in \mathcal{X}} H\left(W(\cdot|x)\right) & \text{if } \mathbb{C}(\mathcal{W}) > 0 \\ 0 & \text{iff } \mathcal{W} \text{ is noiseless or } \mathbb{C}(\mathcal{W}) = 0 \end{cases}$$

- Feedback allows a double exponential growth of the identities
- Noise can increase the identification feedback capacity

R. Ahlswede and G. Dueck, "Identification in the presence of feedback-a discovery of new capacity formulas," IEEE Trans. Inf. Theory, 1989

DIF Over Gaussian Channels: System Model



- $Z_t,\ t = 1, \ldots, n \overset{\text{iid}}{\sim} \mathcal{N}\left(0, \sigma^2\right)$
- The channel is denoted by W_{σ^2}

DIF code for Gaussian channels under average power constraint

A $(L(n,R), n, \lambda_1, \lambda_2)$-DIF code for W_{σ^2} with $\lambda_1 + \lambda_2 < 1$ is a system $\{(f_i, \mathcal{D}_i)\}_{i \in [1:L(n,R)]}$ subject to

1. Code size: $L(n,R)$
2. Feedback strategy: $f_i = [f_i^1, f_i^2 \ldots, f_i^n] \in \mathcal{F}_n$, decoding region: $\mathcal{D}_i \subset \mathcal{Y}^n$
3. $\sum_{t=1}^{n} (f_i^t)^2 \leq n \cdot P_{tot}, \quad \forall i \in \{1, \ldots, N\}$
4. Error requirement type I: $W^n(\mathcal{D}_i | u_i) > 1 - \lambda_1$
5. Error requirement type II: $W^n(\mathcal{D}_i | u_j) \underset{i \neq j}{<} \lambda_2$

- $\mathcal{F}_n$ is set of all encoding functions f_i, where $f_i^1 \in \mathcal{X}$ and $f_i^t : \mathcal{Y}^{t-1} \to \mathcal{X}$ for $t > 1$

DIF Capacity of Gaussian Channel

Theorem

Let $\lambda \in (0,1)$, $\sigma^2 \geq 0$ and $P_{tot} > 0$. Then for all $R > 0$, there exists a blocklength n_0 such that for every $n \geq n_0$ there exists a deterministic identification feedback code $(L(n,R), n, \lambda_1, \lambda_2)$ for W_{σ^2} of blocklength n with $L(n,R) = 2^{2^{nR}}$ identities and with $\lambda_1, \lambda_2 \leq \lambda$, i.e.,

$$\mathbb{C}_{DIF}(\sigma^2, P_{tot}) = +\infty$$

- Change the scaling? Choose higher scaling?
- Without feedback, code size growth $\sim 2^{(n \log n)R}$

W. Labidi, H. Boche, C. Deppe and M. Wiese, "Identification over the Gaussian Channel in the Presence of Feedback," IEEE Int'l Symp. Inf. Theory (ISIT), 2021 [arXiv:2102.01198, 2021] M. J. Salariseddigh, U. Pereg, H. Boche, and C. Deppe, "Deterministic identification over channels with power constraints," IEEE Int'l Conf. Commun. (ICC), 2021 [arXiv:2010.04239, 2021]

Infinite DIF Capacity regardless of the Scaling

Theorem

Let $\lambda \in (0,1)$, $\sigma^2 \geq 0$ and $P_{\text{tot}} > 0$. Then there exists a blocklength n_s such that for every positive integer $L(n,R)$ and every $n \geq n_s$ there exists a deterministic identification feedback code $(L(n,R), n, \lambda_1, \lambda_2)$ for W_{σ^2} of blocklength n with $L(n,R)$ identities and with $\lambda_1, \lambda_2 \leq \lambda$

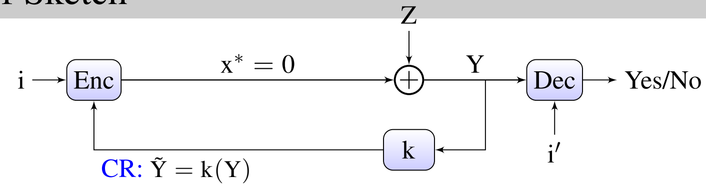
W. Labidi, H. Boche, C. Deppe and M. Wiese, "Identification over the Gaussian Channel in the Presence of Feedback," IEEE Int'l Symp. Inf. Theory (ISIT), 2021 [arXiv:2102.01198, 2021]

Proof Sketch ($\sigma^2 > 0$)

1. To send a message i, we prepare a set of coloring functions $\{F_i, \quad i = 1, \dots, L(n,R)\}$ known by the sender and the receiver

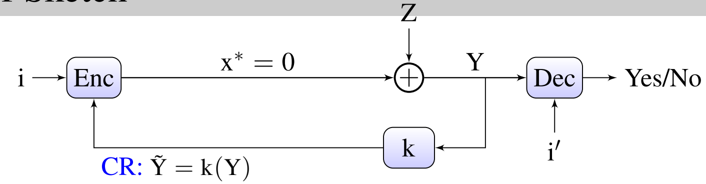
$$F_i : \{1, \dots, |\mathcal{L}|\} \longrightarrow \{1, \dots, M\}$$
$$: \underbrace{l}_{\text{coloring}} \mapsto \underbrace{F_i(l)}_{\text{color}}$$

Proof Sketch



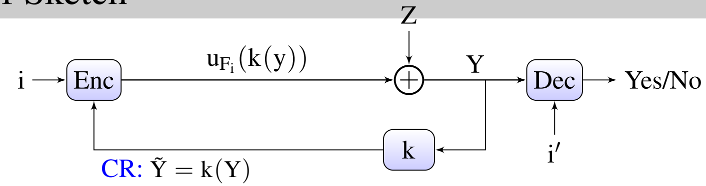
2. We send one symbol $x^* = 0$ over the forward channel

Proof Sketch



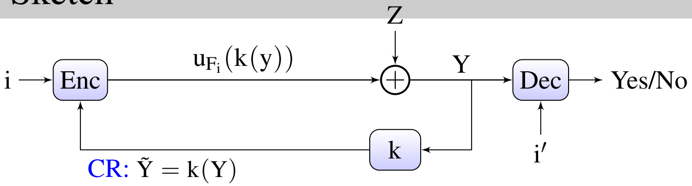
3. We generate the RV $\tilde{Y} = k(Y) \sim \mathrm{Unif}(\mathcal{L})$, $|\mathcal{L}|$ determines the growth of $L(n, R)$

Proof Sketch



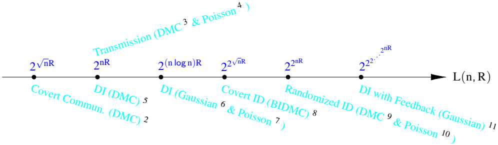
4. $\mathcal{C} = \{(u_j, \mathcal{D}_j),\ j = 1, \ldots, M\}$ is an $(m, M, 2^{-m\delta})$ transmission code, we send $u_{F_i(k(y))}$, $k(y) \in \mathcal{L} \implies (n, L(n, R), \lambda_1, \lambda_2)$ DIF code with $n = 1 + m$

Proof Sketch



5. If $F_i(k(y)) = F_{i'}(k(y))$, then $i = i'$

Coding Scale



---

2 Bloch, "Covert Communication over Noisy Channels: A Resolvability Perspective", T-IT, 2016

3 Shannon, "A Mathematical Theory of Communication", Bell Sys. Tech. J., 1948

4 Lapidoth and Moser, "On the Capacity of the Discrete-Time Poisson Channel", T-IT, 2009

5 Salarisedigh et al., "Deterministic Identification Over Channel With Power Constraints", T-IT, 2021

6 Salarisedigh et al., "Deterministic Identification Over Fading Channels", Proc. ITW, 2020

7 Salarisedigh et al., "Deterministic Identification Over Poisson Channels", Proc. GC, 2021

8 Zhang and Tan, "Covert Identification over Binary-Input Discrete Memoryless Channels", arXiv, 2021

9 Ahlswede and Dueck, "Identification via Channels", T-IT, 1989

10 Burnashev, "On Identification Capacity of Infinite Alphabets or Continuous-Time Channels", T-IT, 2000

11 Labidi et al., "Identification over the Gaussian Channel in the Presence of Feedback", Proc. ISIT, 2021

18 M. J. Salariseddigh, U. Pereg, H. Boche, and C. Deppe, "Deterministic identification over channels with power constraints," IEEE Int'l Conf. Commun. (ICC), 2021 [arXiv:2010.04239, 2021]

19 W. Labidi, H. Boche, C. Deppe and M. Wiese, "Identification over the Gaussian Channel in the Presence of Feedback," IEEE Int'l Symp. Inf. Theory (ISIT), 2021 [arXiv:2102.01198, 2021]

I did not talk about ......

- K-Identification
- Construction of RI-Codes
- Construction of DI-Codes
- Joint Identification and Sensing
- Molecular Comunication and Identification
- Quantum Communication and Identification
- Source Identification
- PUFs and Identification
- Function Compression and Identification
- Security and Identification
- Covert Communication and Identification
- Common Randomness Capacity and Identification
- Resolvability and Identification

Thank you to Coauthors working on Identification

Thank you to the financial supporters

- Joint project 6G-life (2021-2025): Support by the Federal Ministry of Education and Research of Germany in the programme of Souverän. Digital. Vernetzt..
- NEWCOM (2019-2024): Support by the Federal Ministry of Education and Research of Germany.
- "General Theory of Information Transfer" (2007-2012): supported by DFG (German Research Foundation)