Deterministic Identification: From Theoretical Analysis to Practical Identification Codes

Ilya Vorobyev[1], Christian Deppe[2], Luis Torres-Figueroa[1], Holger Boche[1]
[1]Technical University of Munich, Germany
[2]Technical University of Braunschweig, Germany

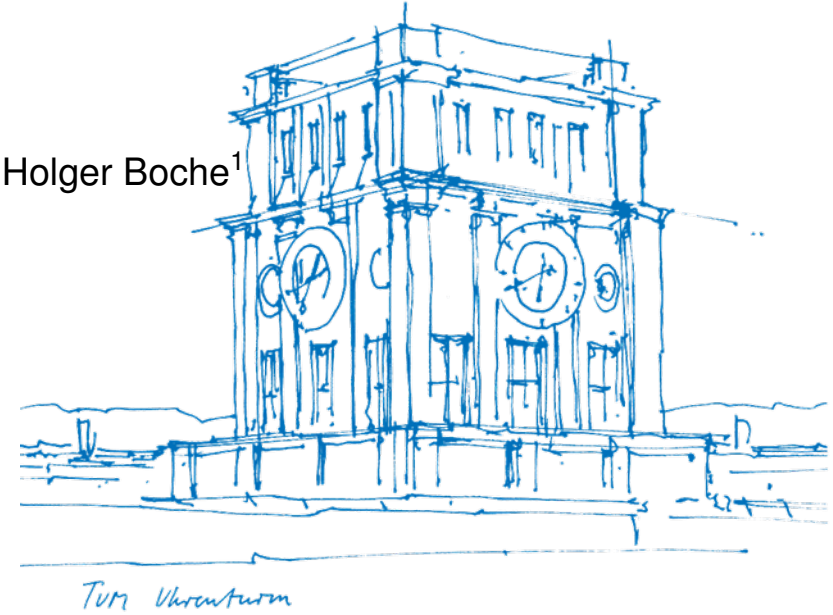


Table of Contents

Decoding

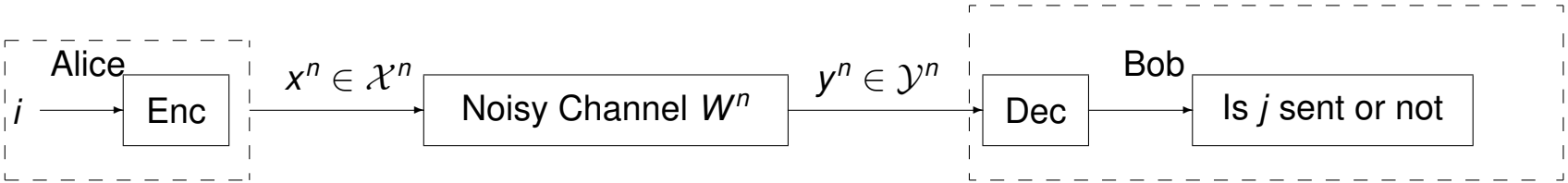
Shannons Channel Coding:

- Alice has to transmit a message $m \in \mathcal{M} = \{1, 2, \ldots, M\}$ to Bob
- Alice uses a block code $\mathcal{X}^n = \{0, 1, \ldots, q-1\}^n$
- $W = \{W(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ 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 $\mathcal{Y}^n$.

Identification



- Alice has to transmit a identity $i \in \mathcal{M} = \{1, 2, \ldots, M\}$
- Alice sends $x^n \in \mathcal{X}^n = \{0, 1, \ldots, q-1\}^n$
- $W = \{W(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ 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 $\mathcal{Y}^n$.

Deterministic and Randomized

Two types of identification:

- Randomized. Up to $2^{2^{C_{tr}n}}$ identities.
- Deterministic. Up to $2^{C_{ID}n}$ for DMC, but the capacity is higher than for transmission.

Definitions

Definition

A (M, n) DI code for a DMC $\mathcal{W}$ under input constraint A is defined as a system $(\mathcal{U}, \mathcal{D})$ that consists of a codebook $\mathcal{U} = \{\mathbf{u}_i\}_{i\in[M]}$, $\mathcal{U} \subset \mathcal{X}^n$, such that

$$\phi^n(\mathbf{u}_i) \leq A, \text{ for all } i \in [M], \tag{1}$$

and a collection of decoding regions $\mathcal{D} = \{D_i\}_{i\in[M]}$, $D_i \subset \mathcal{Y}^n$. The error probabilities are given by

$$P_{e,1}(i) = W^n(D_i^c|\mathbf{u}_i) \quad \text{(missed-identification error)}, \tag{2}$$
$$P_{e,2}(i,j) = W^n(D_j|\mathbf{u}_i) \quad \text{(false identification error)}. \tag{3}$$

A $(M, n, \lambda_1, \lambda_2)$ DI code satisfies

$$P_{e,1}(i) \leq \lambda_1, \tag{4}$$
$$P_{e,2}(i,j) \leq \lambda_2, \tag{5}$$

for all $i, j \in [M]$, $i \neq j$.

More Definitions

A rate R is called achievable if for any $\lambda_1, \lambda_2 > 0$ and sufficiently large n there exists a $(M, n, \lambda_1, \lambda_2)$ DI code with $M \geq 2^{Rn}$. The capacity is defined as the supremum of all achievable rates and denoted as $C_{DI}(\mathcal{W})$.

We consider cost function of the following form.

$$\phi^n(x^n) = \frac{1}{n} \sum_{t=1}^{n} \phi(x_t). \tag{6}$$

The type $\hat{P}_{x^n}$ of a given sequence x^n is defined as the empirical distribution $\hat{P}_{x^n}(a) = N(a|x^n)/n$ for all $a \in \mathcal{X}$, where $N(a|x^n)$ is the number of occurrences of the symbol a in the sequence x^n. For a given distribution p_X type class $\mathcal{T}(p_X)$ is defined as a set of all sequences $x^n \in \mathcal{X}^n$ such that for every $a \in \mathcal{X}$ an equality $\hat{P}_{x^n}(a) = p_X(a)$ holds.

Table of Contents

Known results

In paper [1] the authors prove the following Theorem.

Theorem

For reduced DMC (all rows of matrix W are different) $\mathcal{W}$ its identification capacity equals

$$C_{DI}(\mathcal{W}) = \max_{p_X : \mathbb{E}\{\phi(X)\} \leq A} H(X).$$

If there are no constraints then

$$C_{DI}(\mathcal{W}) = \log_2 |\mathcal{X}|.$$

Theorem is proved with random coding method, so it doesn't provide efficient method of construction or encoding.

[1] Mohammad J. Salariseddigh; Uzi Pereg; Holger Boche; Christian Deppe "Deterministic Identification Over Channels With Power Constraints", 2021

Key Lemma

The proof is based on the following lemma.

Lemma

Let X be a random variable with a distribution $p_X(x)$, $x \in \mathcal{X}$, and R be a positive number such that $R < H(X)$. Then for sufficiently small $\varepsilon \in (0, 1)$ and sufficiently large n, there exists a codebook $U^* = \{\mathbf{u}_i, i \in \mathcal{M}\}$, which consists of $|\mathcal{M}|$ sequences in $\mathcal{X}^n$, such that the following holds:

1) All the codewords belong to the type class $\mathcal{T}(p_X)$.

2) The distance between any two codewords is at least $n\varepsilon$.

3) The codebook size is at least $\frac{1}{2} \cdot 2^{nR}$.

Construction

Theorem

For reduced DMC $\mathcal{W}$ there exists a sequence of DI codes $(M_i = 2^{n_i R}, n_i, \lambda_{1,i}, \lambda_{2,i})$ such that $\lambda_{1,i}, \lambda_{2,i} \to 0$, $n_i \to \infty$, $R \to C_{DI}(\mathcal{W}) = \max_{p_X : \mathbb{E}\{\phi(X)\} \leq A} H(X)$. The construction complexity and encoding complexity are both polynomial in codelength n_i.

Sketch of the proof

We construct a code of rate $R < H(X)$. Concatenated construction:

- Inner code of rate R_1, $R > R_1$, length n_1, alphabet $q_1 = q$, and Hamming distance $d_1 \geq \varepsilon_1 n_1$.
- Outer code is a Reed-Solomon code of rate $R_2 \geq (1 - \varepsilon_2)$, length $n_2 = q_2$, alphabet size $q_2 \sim q_1^{R_1 n_1}$, and Hamming distance $d_2 \geq \varepsilon_2 n_2$.
- Final code has rate $\geq R_1(1 - \varepsilon_2)$, length $n = n_1 n_2$, alphabet size q, and Hamming distance $d \geq \varepsilon_1 \cdot \varepsilon_2 \cdot n$.

Complexity of constructions is $O(q_1^{n_1} \cdot n_1) = O(M_1^{1/R_1} \cdot n_1) = O(n_2^{1/R} \cdot n_1)$ operations and $O(q^{n_1})$ memory.

Complexity of encoding is also polynomial.

Table of Contents

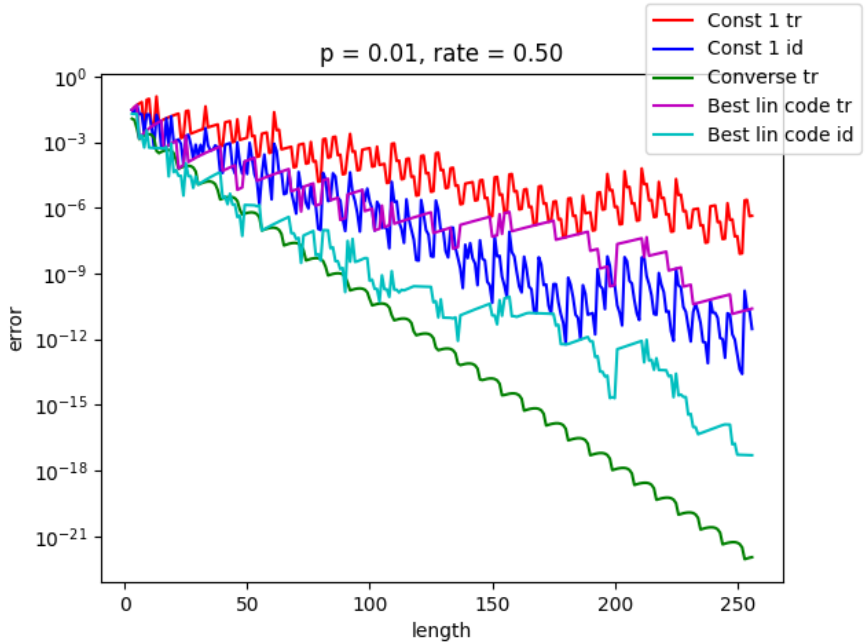
Simulations for DMC

- We use our Construction to obtain DI codes of finite length for the binary symmetric channel (BSC) without power constraints.
- As inner codes we take either all possible codewords, all possible codewords of even weight, Hamming code, or extended Hamming code. As outer codes we use Reed-Solomon codes with field size $q_2 = M_1$.
- We calculate the error ε for $(n, M, \varepsilon, \varepsilon)$ identification code, i.e. we have the same constraint for the errors of the first and the second type. As decoding regions for each identity i we use balls of radius r with a center at corresponding codeword $\mathbf{u}_i$. The radius is chosen for each length to minimize the error.
- We also provide a transmission error for the same codes from Construction, and converse bound for transmission error[2]
- At last, we compute identification and transmission errors for the linear codes with the best known distance.[3]

[2] Yury Polyanskiy; H. Vincent Poor; Sergio Verdu "Channel Coding Rate in the Finite Blocklength Regime"

[3] M. Grassl, “Bounds on the minimum distance of linear codes and quantum codes,” Online available at http://www.codetables.de

Simulation results 1



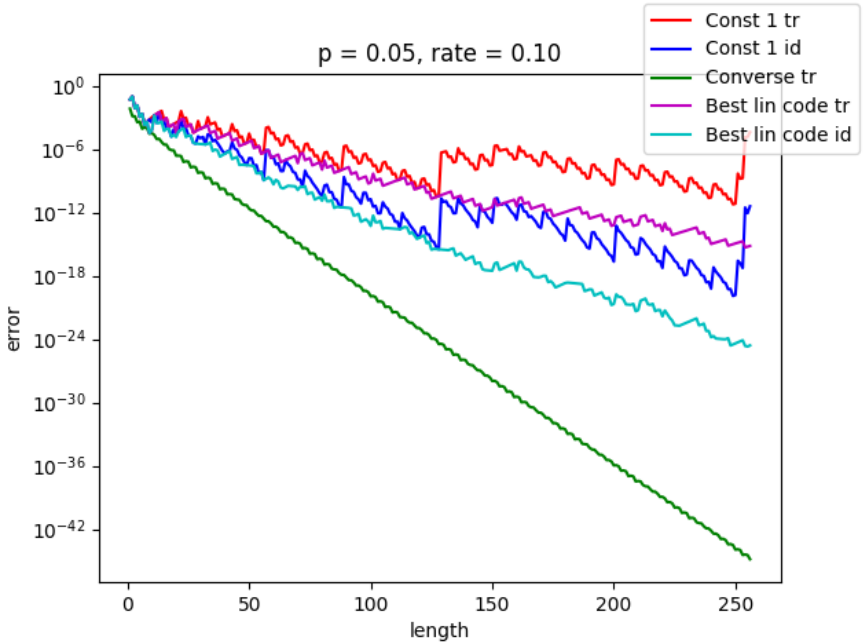


Figure: Identification and transmission errors for the codes of length up to 256

Simulation results 2

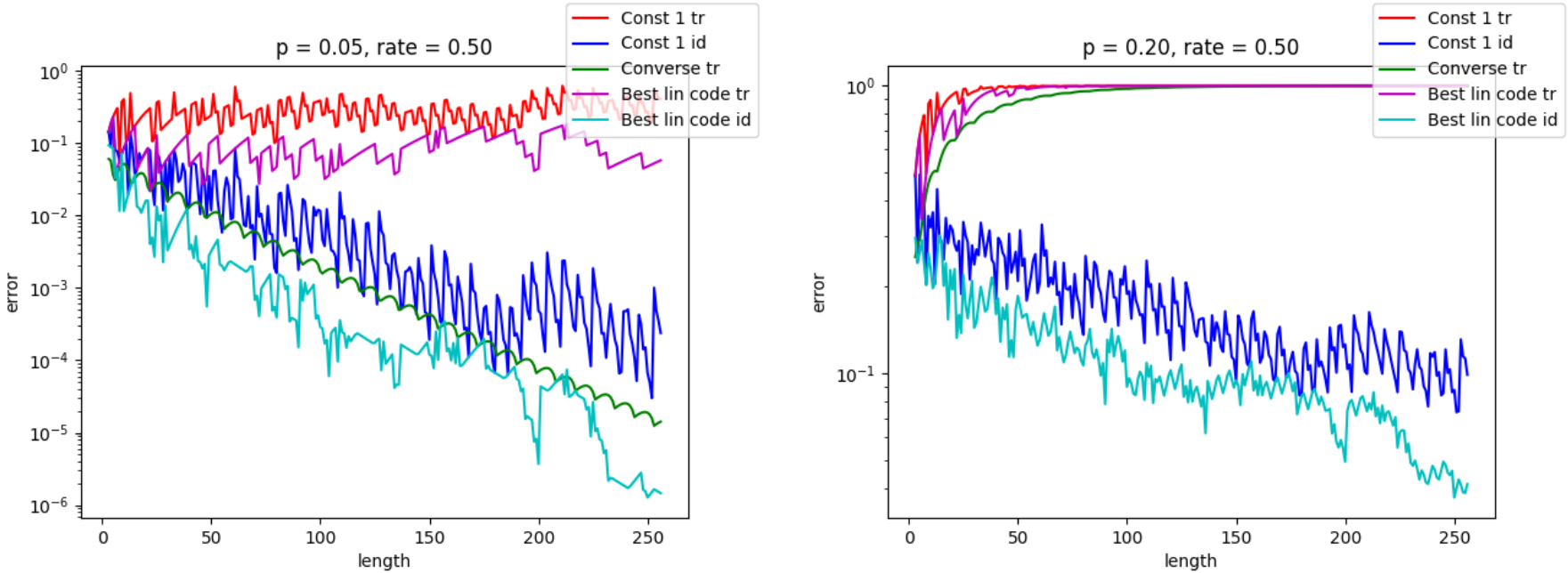


Figure: Identification and transmission errors for the codes of length up to 256

Table of Contents

Hardware simulations

We investigate BSC channels by using BPSK modulation for the transmission of codewords $\mathbf{u}_i$ via Gaussian channels at different signal-to-noise ratio (SNR) levels for a fixed transmit signal power. Thus, we increase the AWGN power in 1 dB steps after 1000 measurements.

In our experiments we consider two cases. “Scenario 1” consists of a receiver interested in the transmitter’s identity ($j = i$), which is used in the DI verification process, V_{DI}. Here we are interested in evaluating the *missed-identification errors*, $P_{e,1}(i)$, caused by transmission errors.

“Scenario 2” contemplates the case when the receiver is interested in a different identity, j, than the transmitter’s one, i. We investigate the scenario when the codewords corresponding to identities i and j are located at the minimum possible distance between them, i.e., the decoding region radius r. Here we focus on the analysis of the *false identification errors*, $P_{e,2}(i, j)$ that occur for different SNR levels and BER.

Table: Key parameters of the four experiments we conducted.

Element	Parameter	Exp. 1	Exp. 2	Exp. 3	Exp. 4
Inner Code	Code	SPC	SPC	EH	SPC
	length n_1	8	8	8	8
	dimension k_1	7	7	4	7
	distance d_1	2	2	4	2
Outer Code	Code	RS	RS	RS	RS
	alphabet q_2	128	128	16	128
	length n_2	32	16	16	32
	dimension k_2	19	10	3	4
	distance d_2	14	7	14	29
Concatenated Code	length n	256	128	128	256
	dimension k	133	70	12	28
	distance d	28	14	56	58
Verifier	radius r	19	9	32	42

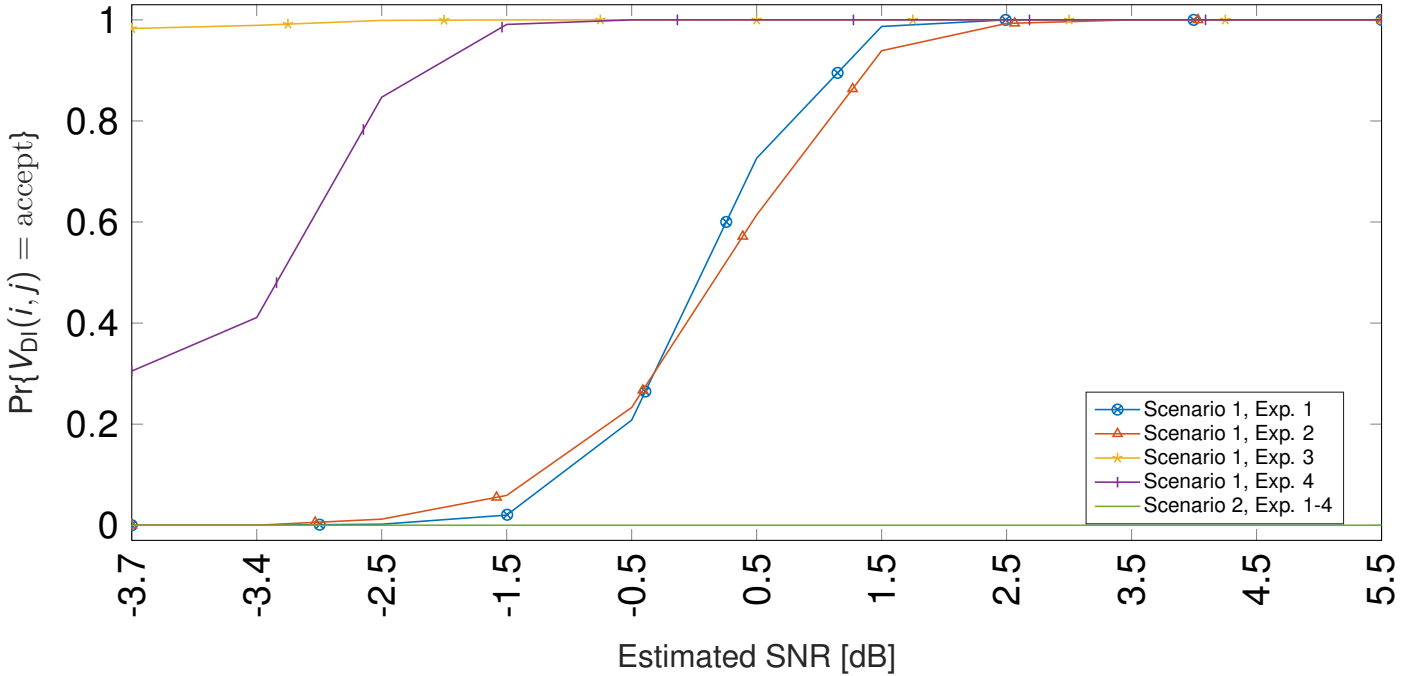


Figure: Probability of accept responses after DI verification at the receiver.

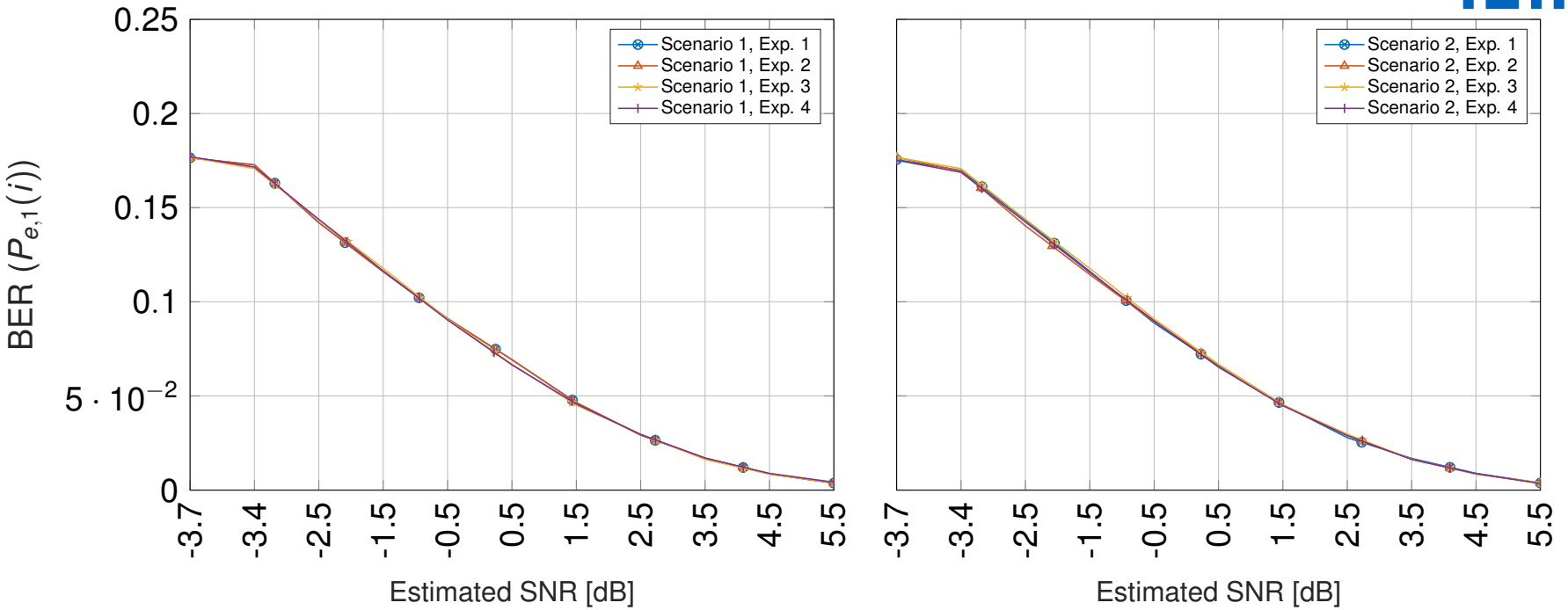


Figure: Errors of the first kind, $P_{e,1}(i)$ as in Eq. (4), caused by the channel transmission, measured using the bit error rate for different SNR levels.

Conclusion and future work

- The construction of identification codes with optimal capacity was proposed. The complexity of construction and encoding are polynomial in length n.
- For finite lengths deterministic identification codes were constructed. For the binary symmetric channel we confirm that the identification codes achieve rate bigger than the rate of transmission codes. Hardware simulation verifies these results.

Future directions

- Finite lengths identification codes for other channel, for example, binary asymmetric channel.
- Construction of identification codes for AWGN and Fading channels. (We have some results available at arxiv.)

Thank you for your attention!