Finite Blocklength Performance of Capacity-achieving Codes in the Light of Complexity Theory

Holger Boche*, Andrea Grigorescu*, Rafael F. Schaefer†, H. Vincent Poor‡
*Technical University of Munich
†Technische Universität Dresden
‡Princeton University
boche@tum.de, andrea.grigorescu@tum.de,rafael.schaefer@tu-dresden.de, poor@princeton.edu

Since the work of [1] on the finite blocklength performance of capacity-achieving codes for discrete memoryless channels, many papers have developed further results for several practically relevant channels, see [2]–[4]. However, the complexity of computing capacity-achieving codes has not been investigated until now. We study this question for one of the simplest of non-trivial Gaussian channels, i.e., the additive colored Gaussian noise (ACGN) channel.

In this context, it is essential to have a well-defined concept of complexity. In particular, the "parameters" of the communication system should be of low complexity, meaning they should be easy to describe. We focus on a point-to-point ACGN channel. This system is fully characterized by the transmission power P of the transmitter and the noise power spectral density N. Therefore, both the transmission power P and the power spectral density N should be easy to compute. The central question is how complex it is to compute key performance metrics of the communication system. Of particular practical importance are the Shannon capacity and sequences of capacity-achievable codes.

To assess computational complexity, we consider the classes FP, FP_1, and $\#\mathrm{P}_1$. For this, we first need to introduce the set of all finite strings over the binary alphabet, denoted by $\{0,1\}^*$.

Definition 1 (Class FP)**.** *A function $f\colon \{0,1\}^* \to \mathbb{N}$ is in* FP *if it can be computed by a deterministic Turing machine in polynomial time.*

In this work, we are also interested in studying functions that are defined on the singleton alphabet, i.e., $\{0\}^* \subset \{0,1\}^*$. In other words, these functions are defined solely on the set of finite words composed of the symbol 0. The class analog to FP defined on singleton sets are denoted by FP_1. We further introduce the class $\#\mathrm{P}_1$ also defined on the singleton alphabet. $\#\mathrm{P}_1$ encompasses functions that count the number of solutions verifiable by a Turing machine in polynomial time.

Definition 2 (Classes FP_1 and $\#\mathrm{P}_1$)**.** *A function $f\colon \{0\}^* \to \mathbb{N}$ is said to be in FP_1 if it can be computed by a deterministic Turing machine in polynomial time.*

A function $f\colon \{0\}^* \to \mathbb{N}$ is said to be in $\#\mathrm{P}_1$ if there exists a polynomial $p\colon \mathbb{N} \to \mathbb{N}$ and a polynomial time Turing machine M so that for every string $x \in \{0\}^*$

$$f(x) = |\{y \in \{0\}^{p(|x|)}\colon M(x,y) = 1\}|.$$

In [5], it has been shown that there exists an infinitely differentiable, strictly positive noise power spectral density N_*, which is computable in polynomial time and such that for every sufficiently large rational power constraint P under the widely accepted assumption $\mathrm{FP}_1 \neq \#\mathrm{P}_1$, the capacity $C(P, N_*)$ cannot be computed in polynomial time, demonstrating a complexity-blowup phenomenon.

Let $\epsilon > 0$, $\epsilon \in \mathbb{Q} \cap (0,1)$ be the admissible decoding error and $\{R_n(\epsilon)\}_{n\in\mathbb{N}}$ be a sequence of achievable rates of capacity achieving codes. It is of interest to determine the conditions under which, for a given $M \in \mathbb{N}$, where M describes the precision of the deviation of $C(P,N)$, for a certain blocklength n_M, when the following holds:

$$R_{n_M}(\epsilon) > C(P,N) - \frac{1}{2^M}. \tag{1}$$

This is visualized in Figure 1.

Next we introduce the definition of time complexity of a computable real number.

Definition 3. *Let t be an integer function. The* time complexity *of a computable real number x is bounded by t if there exists a Turing machine that computes, on each input $n \in \mathbb{N}$, a dyadic rational number d in $t(n)$ moves such that $|d - x| \leq 2^{-n}$.*

Further, we introduce the concept of a polynomial time computable number.

Definition 4. *A real number x is* polynomial time computable *if its time complexity is bounded by a polynomial function p.*

We now follow with the introduction of a polynomial time computable sequence.

Definition 5. *Let $\{\alpha_n\}_{n\in\mathbb{N}}$ be a computable sequence of computable numbers. This sequence is computable in polynomial time if there exists a polynomial $p\colon N\times\mathbb{N}\to\mathbb{N}$, such that for all $n\in\mathbb{N}$ and for each $M\in\mathbb{N}$, a number $\alpha_{n,M}\in\mathbb{Q}$ is computed in at most $p(n,M)$ steps such that*

$$|\alpha_n-\alpha_{n,M}|\leq\frac{1}{2^M}$$

holds.

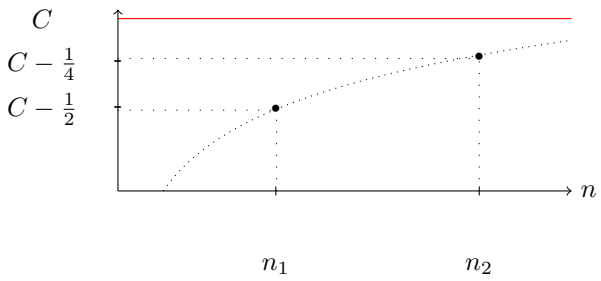


Fig. 1: The red line represents the band-limited ACGN capacity $C=C(P,N_*)$ for the power spectral density. N_* and the power constraint P in the asymptotic regime. The black curve represents the finite blocklength achievable rate $R_n(\epsilon)$ for some fixed $\epsilon>0$. For n_1 we have $R_{n_1}(\epsilon)>C-\frac{1}{2}$ and for n_2 we have $R_{n_2}(\epsilon)>C-\frac{1}{4}$. Fig. from [5].

Remark 1. *It holds that $R_n(\epsilon)=\frac{1}{n}\log_2\mathcal{M}_n(\epsilon)$ for $n\in\mathbb{N}$. Hence, for every $n\in\mathbb{N}$ the achievable rate $R_n(\epsilon)$ is a polynomial time computable number.*

The following theorem is discussed in the rest of the abstract.

Theorem 1. *Let B be a polynomial time computable number representing the bandwidth. There exists a strictly positive and polynomial time computable noise power spectrum N_* such that for all sufficient large rational power constraint P_* and for all rational $\epsilon>0$, the computation of achievable rate sequence $\{R_{n_M}(\epsilon)\}_{M\in\mathbb{N}}$ fulfilling:*

$$R_{n_M}(\epsilon)>C(P_*,N_*)-\frac{1}{2^M}. \tag{2}$$

is in $\#\mathrm{P}_1$.

If $\mathrm{FP}_1\neq\#\mathrm{P}_1$, then for N_* and for every sufficiently large $P_*\in\mathbb{Q}$, none of the sequences $\{R_{n_M}\}_{n_M\in\mathbb{N}}$ satisfying (2) *can be computed in polynomial time.*

Remark 2. *For every $M\in\mathbb{N}$ we have that $R_{n_M}(\epsilon)$ is a polynomial time computable number. The complexity of computing the sequence $\{R_{n_M}(\epsilon)\}_{n_M\in\mathbb{N}}$ grows faster than any polynomial as M increases.*

Remark 3. *Consequently, determining the blocklengths $\{n_M\}_{M\in\mathbb{N}}$, that satisfy* (1) *is not feasible in polynomial time for an ACGN channel with noise power spectral density N_*.*

Remark 4. *We show that either the sequence of achievable rates $\{R_{n_M}(\epsilon)\}_{n_M\in\mathbb{N}}$ as a function of the blocklength is not a polynomial time computable sequence, or the sequence of blocklength $\{n_M\}_{M\in\mathbb{N}}$ corresponding to the achievable rates with guaranteed distance to capacity is not a polynomial time computable sequence, see [5].*

Remark 5. *Note that Theorem 1 is valid for any computable sequence of achievable rates satisfying the relation* (1)*. In theoretical computer science, a distinction is made between computable and non-computable solutions. For strictly positive, computable continuous spectral densities N and computable $P>0$, $C(P,N)$ is always a computable number. However, in computer science, there is a further distinction between feasible and unfeasible problems within the realm of computable solutions. The feasibility thesis states that a natural problem has a feasible algorithm if and only if the problem has a polynomial time algorithm; see [6, p. 90] and [7]. Therefore, if $\mathrm{FP}_1\neq\#\mathrm{P}_1$, then the problem of computing achievable rates under the performance constraint* (1) *is not algorithmically feasible, even for very easily computable performance parameters of the communication system, i.e., N computable in polynomial time and $P\in\mathbb{Q}$.*

Finding important performance metrics for communication systems is an important task in information and communication theory. Computer-assisted search and optimization play a crucial role here. Important questions, such as the computation of the optimal input distribution for discrete memoryless channels or code constructions, cannot be solved algorithmically on Turing machines depending on the communication parameters; see [8]–[10] . It is interesting to see that even for simple communication systems, such as point-to-point ACGN channels, the complexity of important performance metrics is very high under typical complexity assumptions, even for fixed and easily computable communication parameters.

REFERENCES

[1] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, Apr. 2010.

[2] ——, "Dispersion of the Gilbert-Elliott channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1829–1848, Mar. 2011.

[3] ——, "Feedback in the non-asymptotic regime," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4903–4925, Aug. 2011.

[4] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

[5] H. Boche, A. Grigorescu, R. F. Schaefer, and H. V. Poor, "Characterization of the complexity of computing the capacity of colored Gaussian noise channels," *IEEE Trans. Commun.*, 2024, early Access.

[6] J. A. Carlson, A. Jaffe, and A. Wiles, *The millennium prize problems*. American Mathematical Soc., 2006.

[7] S. A. Cook, "Computational complexity of higher type functions," in *Int. Congress Math.* Kyoto, Japan: Springer -Verlag, Berlin, 1991, pp. 55–69.

[8] Y. Lee, H. Boche, and G. Kutyniok, "Computability of optimizers," *IEEE Trans. Inf. Theory*, vol. 70, no. 4, pp. 2967–2983, Apr.

[9] H. Boche, R. F. Schaefer, and H. V. Poor, "Turing meets Shannon: On the algorithmic construction of channel-aware codes," *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2256–2267, Apr. 2022.

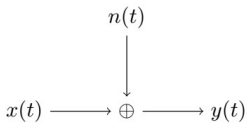
[10] ——, "Algorithmic computability and approximability of capacity-achieving input distributions," *IEEE Trans. Inf. Theory*, vol. 69, no. 9, pp. 5449–5462, Sep. 2023.

Finite Blocklength Performance of Capacity-achieving Codes in the Light of Complexity Theory

Holger Boche[1], Andrea Grigorescu[1], Rafael F. Schaefer[2] , H. Vincent Poor[3]

[1]Chair of Theoretical Information Technology, Technical University of Munich,
[2]Chair of Information Theory and Machine Learning, Technische Universität Dresden
[3]Dept. of Electrical and Computer Engineering, Princeton University

Band Limited ACGN Channel



- $x(t)$ Band-limited input signal with p.s.d. $P_x(f)$
- $y(t)$ Band-limited output signal
- $n(t)$ Band-limited Gaussian noise with noise spectrum $N(f)$
- Band $B > 0$

Capacity band-limited ACGN channel

The capacity of the band-limited ACGN channel with bandwidth B, and continuous noise power spectrum N on the interval $[0, B]$ subject to a power constraint $P > 0$ is given by

$$C(P, N) = \int_0^B \ln\left(1 + \frac{P_x^*(f)}{N(f)}\right) df.$$

The capacity-achieving power spectrum density is given by

$$P_x^*(f) = \begin{cases} \Big[\nu - N(f)\Big]_+ & \text{for } f \in [0, B] \\ 0 & \text{f} \notin [0, B], \end{cases}$$

where ν is chosen such that $\int_0^B P_x^*(f)\, df = P$ is satisfied [4].

Complexity Classes

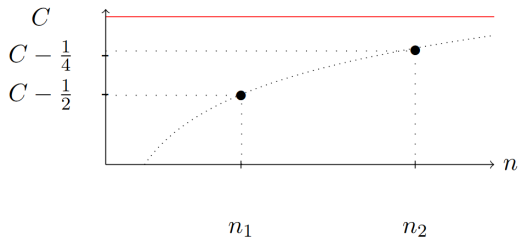
Definition 1 (Class FP_1)**.** A function $f\colon \{0\}^* \to \mathbb{N}$ is in FP if it can be computed by a deterministic TM in polynomial time

Definition 2 (Class $\#\mathrm{P}_1$)**.** A function $f\colon \{0\}^* \to \mathbb{N}$ is in #P if there exists a polynomial $p\colon \mathbb{N} \to \mathbb{N}$ and a polynomial time TM M, such that for every string $x \in \{0\}^*$,

$$f(x) = |\{y \in \{0\}^{p(|x|)} \colon M(x, y) = 1\}|$$

$$\mathbf{FP_1 \neq \#P_1?}$$

Computing Finite Blocklength Performance



- $\{R_n(\epsilon)\}_{n\in\mathbb{N}}$ blocklength-dependent sequence of achievable rates when allowing error $\epsilon \in \mathbb{Q}$ [3]
- $\{R_n(\epsilon)\}_{n\in\mathbb{N}}$ converges to the capacity

$$R_{n_M}(\epsilon) \geq C(P, N) - \frac{1}{2^M}. \tag{1}$$

- For a fixed n, the achievable rate is always a polynomial-time computable number

Polynomial Time Sequence

Definition 3. Let $\{\alpha_n\}_{n\in\mathbb{N}}$ be a computable sequence of computable numbers. This sequence is computable in polynomial time if there exists a polynomial $P\colon N \times \mathbb{N} \to \mathbb{N}$, such that for all $n \in \mathbb{N}$ for each $M \in \mathbb{N}$ a number $\alpha_{n,M} \in \mathbb{Q}$ is computed in at most $P(n, M)$ steps such that it holds:

$$|\alpha_n - \alpha_{n,M}| \leq \frac{1}{2^M}.$$

This notion precisely takes into account the blocklength dependence!

What is the complexity of computing the blocklength-dependent sequence of achievable rates for the band-limited ACGN channel with polynomial time computable continuous noise power spectrum N?

Results

Theorem 1 ([2])**.** *Let B be a polynomial time computable number. There exists a strictly positive and polynomial time computable noise power spectrum N_* such that for all sufficient large rational power constraint P_* and for all rational $\epsilon > 0$, the computation of achievable rate sequence $\{R_{n_M}(\epsilon)\}_{n_M\in\mathbb{N}}$ fulfilling:*

$$R_{n_M}(\epsilon) > C(P_*, N_*) - \frac{1}{2^M}. \tag{2}$$

is in $\#\mathrm{P}_1$. If $\mathrm{FP}_1 \neq \#\mathrm{P}_1$, then for N_* and for every sufficiently large $P_* \in \mathbb{Q}$, none of the sequences $\{R_{n_M}\}_{M\in\mathbb{N}}$ satisfying (2) can be computed in polynomial time.

Complexity Blowup!

Computing the Band-limited ACGN Capacity

- There are computable noise spectrum, for which the capacity yields a **non-computable number** [1]

  ⇒ Shannon's coding approach is not effective, i.e., cannot be solved algorithmically

- If the continuous noise power spectrum is **strictly positive and computable**, then the capacity will always be a **computable number** [2]

Conclusions

- Determining the blocklengths $\{n_M\}_{M\in\mathbb{N}}$, that satisfy (1) is not feasible in polynomial time for an ACGN channel with noise power spectrum N_*
- Either the sequence of achievable rates is not a polynomial-time computable sequence
- Or the minimum blocklength n_M corresponding to the capacity approximation

  $$R_{n_M}(\epsilon) > C(P, N) - \frac{1}{2^M}$$

  grows faster than any polynomial

References

[1] Holger Boche et al. "Algorithmic Computability of the Capacity of Gaussian Channels with Colored Noise". In: *IEEE Global Telecommun. Conf.* 2023

[2] Holger Boche et al. "Characterization of the Complexity of Computing the Capacity of Colored Noise Gaussian Channels". In: *IEEE Trans. Commun.* (2024). Early Access

[3] Yury Polyanskiy, H Vincent Poor, and Sergio Verdú. "Channel coding rate in the finite blocklength regime". In: *IEEE Trans. Inf. Theory* 56.5 (Apr. 2010), pp. 2307–2359

[4] Claude E Shannon. "Communication in the presence of noise". In: *Proc. IRE* 37.1 (1949), pp. 10–21