Technical University of Munich
TUM School of Computation, Information and Technology
Chair of Theoretical Information Technology

December, 2024

Research internship / Bachelor / Master thesis: Computer-Aided Formalization and Verification of Information Theory

The problem
When proving new results, a large share of the time of the authors as well as the reviewers of papers is spent on checking the proofs for errors and fixing them, even if the argument is conceptually correct. Even Shannon awardees had mistakes in published papers (see the discussion in [1, Section 2.4] on [2], and the comment in [3, p. 513] on [4, Theorem 6]). Sometimes mistakes have turned out to be (probably) fundamental errors [2], and sometimes to be correctable, with the high level idea being correct (see [5, 6] on [7]). The review process of even the most reputable journal in our field, the *IEEE Transactions on Information Theory* does not always catch these mistakes [4, 7].

The idea
Interactive proof assistants and proof checkers, like Lean, Isabelle, or Coq check if a proof is correct and also help users to find proofs, e.g., by automating some proof steps like simplifications of expressions, and by showing the “holes” of a proof, i.e., what remains to be shown. More sophisticated aids, sometimes based on neural networks are currently under development, and there are also stronger proof automations.

The work
Students are invited to join us in formalizing information theoretic models and results in Lean. We aim to first prove simple results like typicality bounds and historical (coding) theorems, but ultimately, the goal is to prove our new results.
The first task is to learn the basics of Lean, e.g., by playing the set theory game other Lean games, and to get somewhat familiar with the necessary parts of the standard library, mathlib4, especially the probability theory module. Then, students should work on formalizing simple and accessible results, e.g., on typicality and concentration of measures, which are crucial tools to prove coding theorems. Depending on the type of work (internship, Bachelor/Master thesis) and the progress of the student, the scope can be extended to actual coding theorems.
It may well be that theorems from the standard literature must be translated into more general mathematical terms to be formalized, since mathlib4 is not specific to the information theoretic domain. Also, possibly, theorems will be generalized on the way.

Your qualifications
Required: Strong motivation to

1. learn to do information theoretic proofs,
2. gain a deeper understanding of the mathematical foundations of information theory,
3. to learn and work with the functional, dependently typed, programming language Lean.

Helpful:

1. Knowledge in probability theory, e.g., from the lecture “Stochastische Signale”.
2. Knowledge in information theory, e.g. from the lectures “Information Theory” or “Informationstheoretische Sicherheit”.
3. Programming experience, in particular with functional, very strongly typed programming languages like Haskell, ML, or even dependently typed languages.
4. Some experience with LaTeX and/or Typst

To apply

Please send your application by e-mail to Johannes Rosenberger (johannes.rosenberger@tum.de) with the following documents:

- Curriculum vitae
- Academic transcript
- Short motivation

General information

TUM is aiming to increase the number of women employees, and applications from women are expressly welcomed. People with disabilities, with essentially the same suitability and qualification, will be preferred. As you apply for a position at the Technical University of Munich (TUM), you provide personal data. Please note our data protection information according to Art. 13 Data Protection Basic Regulation (DSGVO) on the collection and processing of personal data in connection with your application http://go.tum.de/554159. By submitting your application, you confirm that you have taken note of the data protection information of the TUM.

Technical University of Munich
TUM School of Computation, Information and Technology
Chair of Theoretical Information Technology
Prof. Holger Boche
Theresienstrasse 90, 80333 Munich

References

[1] A. Bracher, “Identification and Zero-Error Codes,” Ph.D. dissertation, ETH Zurich, Konstanz, 2016, ISBN: 3-86628-574-4, DOI: 10.3929/ethz-a-010739015.

[2] R. Ahlswede, “General theory of information transfer: Updated,” vol. 156, no. 9, pp. 1348–1388, May 2008, DOI: 10.1016/j.dam.2007.07.007.

[3] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer Berlin Heidelberg, 2003, DOI: 10.1007/978-3-662-12066-8.

[4] T. Han and S. Verdú, “Approximation theory of output statistics,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May 1993, DOI: 10.1109/18.256486.

[5] M. Hayashi, “General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, 2006, DOI: 10.1109/TIT.2006.871040.

[6] S. Watanabe, “Minimax converse for identification via channels,” *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 25–34, Jan. 2022, ISSN: 1557-9654, DOI: 10.1109/TIT.2021.3120033.

[7] Y. Steinberg, “New converses in the theory of identification via channels,” *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 984–998, 1998, DOI: 10.1109/18.669139.