Polar Codes: Reliable Communication with Complexity Polynomial in the Gap to Shannon Capacity

Venkatesan Guruswami

Computer Science Department
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh PA 15213, USA.
guruswami@cmu.edu

Abstract

Shannon's monumental 1948 work laid the foundations for the rich fields of information and coding theory. The quest for *efficient* coding schemes to approach Shannon capacity has occupied researchers ever since, with spectacular progress enabling the widespread use of error-correcting codes in practice. Yet the theoretical problem of approaching capacity arbitrarily closely with polynomial complexity remained open except in the special case of erasure channels.

In 2008, Arikan proposed an insightful new method for constructing capacity-achieving codes based on channel polarization. In this talk, I will begin with a self-contained survey of Arikan's celebrated construction of polar codes, and then discuss our recent proof (with Patrick Xia) that, for all binary-input symmetric memoryless channels, polar codes enable reliable communication at rates within $\epsilon > 0$ of the Shannon capacity with block length (delay), construction complexity, and decoding complexity all bounded by a *polynomial* in the gap to capacity, i.e., by $\mathrm{poly}(1/\epsilon)$. Polar coding gives the *first explicit construction* with rigorous proofs of all these properties; previous constructions were not known to achieve capacity with less than $\exp(1/\epsilon)$ decoding complexity.

We establish the capacity-achieving property of polar codes via a direct analysis of the underlying martingale of conditional entropies, without relying on the martingale convergence theorem. This step gives rough polarization (noise levels ϵ for the *good channels*), which can then be adequately amplified by tracking the decay of the channel Bhattacharyya parameters. Our effective bounds imply that polar codes can have block length bounded by $\mathrm{poly}(1/\epsilon)$. We also show that the generator matrix of such polar codes can be constructed in polynomial time by algorithmically computing an adequate approximation of the polarization process.

1998 ACM Subject Classification E.4 Coding and Information Theory, F.2 Analysis of Algorithms and Problem Complexity

Keywords and phrases Error-correction algorithms, Linear Codes, Shannon capacity, Martingale convergence, Computational complexity

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2013.1

Category Invited Talk

33rd Int'l Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2013).
Editors: Anil Seth and Nisheeth K. Vishnoi; pp. 1–1

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany