De-randomizing Shannon: The Design and Analysis of a Capacity-Achieving Rateless Code

Hari Balakrishnan, Peter Iannucci, Jonathan Perry, Devavrat Shah

(Submitted on 3 Jun 2012)

This paper presents an analysis of spinal codes, a class of rateless codes proposed recently. We prove that spinal codes achieve Shannon capacity for the binary symmetric channel (BSC) and the additive white Gaussian noise (AWGN) channel with an efficient polynomial-time encoder and decoder. They are the first rateless codes with proofs of these properties for BSC and AWGN. The key idea in the spinal code is the sequential application of a hash function over the message bits. The sequential structure of the code turns out to be crucial for efficient decoding. Moreover, counter to the wisdom of having an expander structure in good codes, we show that the spinal code, despite its sequential structure, achieves capacity. The pseudo-randomness provided by a hash function suffices for this purpose. Our proof introduces a variant of Gallager's result characterizing the error exponent of random codes for any memoryless channel. We present a novel application of these error-exponent results within the framework of an efficient sequential code. The application of a hash function over the message bits provides a methodical and effective way to de-randomize Shannon's random codebook construction.

Subjects: **Information Theory (cs.IT)**; Networking and Internet Architecture (cs.NI)
Cite as: **arXiv:1206.0418 [cs.IT]**
(or **arXiv:1206.0418v1 [cs.IT]** for this version)

Submission history

From: Devavrat Shah [view email]
[v1] Sun, 3 Jun 2012 03:25:18 GMT (60kb,D)

Which authors of this paper are endorsers?