Random codes

Aleksandra Popovska, aleksandrap@ii.edu.mk

Institute of Informatics, Faculty of Natural Sciences and Mathematics, P.O.Box 162, Skopje, Republic of Macedonia

Keywords: random codes, probabilistic models.

AMS: 94B60

Abstract

The non-constructive proof of the noisy-channel coding theorem shows that good block codes exist for any noisy channel, and moreover that nearly all block codes are good. However, writing down an explicit and practical encoder and decoder that are as good as proved by Shannon in his seminal work A Mathematical Theory of Communication is still an unsolved problem. Recently, it has been recognized that two classes of codes, namely turbo codes and low-density parity-check (LDPC) codes, perform at rates extremely close to the Shannon limit. Turbo and LDPC codes are based on a similar philosophy: constrained random code, described by some fixed parameters plus randomness, decoded using iterative algorithms or message passing decoders. My plains for future work are investigations to probabilistic models in coding theory, especially in random codes.

References

[1] Gligoroski, D., Markovski, S., Kocarev, Lj. (2005) *Efficiently Decodable Almost Random Codes*, Submitted to IEEE Information Theory

[2] Barg,A., Forney,D. (2002) *Random Codes: Minimum Distances and Error Exponents*, IEEE Transactions on Information Theory, VOL. 48, NO 9, p.2568-2573

[3] MacKay,D.,(2003) *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press 2003,

[4] Vanstone, S.A., van Ooschot, P.S. (1989) *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, Boston.