COMPLEXITY ISSUES IN CODING THEORY

Alexander Barg

Bell Laboratories, Lucent Technologies
600 Mountain Avenue, Room 2C-375
Murray Hill, NJ 07974, USA
abarg@research.bell-labs.com

and

Insitute for Information Transmission Problems
Russian Academy of Sciences
Moscow, Russia

Abstract. This paper deals with complexity issues in the theory of linear error-correcting codes. Algorithmic problems that we study are constructing good codes, encoding and decoding them. According to their complexity. problems are divided into easy, i.e., polynomial in the length n of the code, and difficult, i.e., exponential ones. The first part deals with easy problems. We present a construction of codes that correct a linear fraction of errors with complexity $n \log n$. The construction is based on well-known since the late 80ies explicit constructions of good expanding graphs. Another group of problems in this part is related to codes for non-Hamming errors, namely, erasures, defects (codes for memories with defective cells), and localized errors.

The second part, which forms the core of this paper, deals with difficult problems, first and foremost, maximum likelihood decoding of linear codes. We study separately the complexity of hard-decision and soft-decision decoding. For the hard-decision decoding case we present algorithms grouped in two classes, gradient-like decoding and information-set decoding. It turns out that this general approach is sufficient to study most if not all known general decoding methods. In the soft-decision decoding context, we first discuss possible problem settings and then implementations of decoding with reduced complexity.

The last part of the paper overviews most known NP-hard decoding problems including some recent nonapproximability results.

The supporting material includes many general properties of linear codes from well-known to rather sophisticated, and a brief discussion of models of computations and relevant settings for the study of complexity issues in coding theory. We also give examples of many methods studied. Sometimes they just illustrate concepts and definitions, but sometimes capture the most essential features of the proofs and on occasion even replace them.

Generally we give complete and self-contained proofs of the results.

The coverage is extended from classical algorithms up to very recent developments. We thoroughly study and compare different algorithms, especially those applicable to several seemingly non-related problems. This unified approach to algorithmic coding problems enables us to organize previously independent results in a self-contained part of coding theory.

This paper will appear as a chapter in Handbook of Coding Theory, V. Pless, W. Cary Huffman and R. Brualdi, Eds., Elsevier Science, to be published.

Keywords: linear code, complexity, encoding, regular-graph codes, maximum likelihood decoding, Gilbert–Varshamov bound, soft-decision decoding, NP-hard problems.

Contents