Chiesa, Alessandro; Gur, Tom; Shinkar, Igor

Relaxed locally correctable codes with nearly-linear block length and constant query complexity. (English) [Zbl 07672197]
SIAM J. Comput. 51, No. 6, 1839-1865 (2022)

Summary: Locally correctable codes (LCCs) are error correcting codes $C : \Sigma^k \to \Sigma^n$ which admit local algorithms that correct any individual symbol of a corrupted codeword via a minuscule number of queries. For systematic codes, this notion is stronger than that of locally decodable codes (LDCs), where the goal is to only recover individual symbols of the message. One of the central problems in algorithmic coding theory is to construct $O(1)$-query LCCs and LDCs with minimal block length. Alas, state-of-the-art of such codes requires super-polynomial block length to admit $O(1)$-query algorithms for local correction and decoding, despite much attention during the last two decades. The study of relaxed LCCs and LDCs, which allow the correction algorithm to abort (but not err) on a small fraction of the locations, provides a way to circumvent this barrier. This relaxation turned out to allow constant-query correcting and decoding algorithms for codes with polynomial block length. Focusing on local correction, T. Gur et al. [LIPIcs – Leibniz Int. Proc. Inform. 94, Article 27, 11 p. (2018; Zbl 1462.68050)] showed that there exist $O(1)$-query relaxed LCCs that achieve nearly-quartic block length $n = k^{4+\alpha}$, for an arbitrarily small constant $\alpha > 0$. We construct an $O(1)$-query relaxed LCC with nearly-linear block length $n = k^{1+\alpha}$, for an arbitrarily small constant $\alpha > 0$. This significantly narrows the gap between the lower bound which states that there are no $O(1)$-query relaxed LCCs with block length $n = k^{1+o(1)}$. In particular, our construction matches the parameters achieved by E. Ben-Sasson et al. [SIAM J. Comput. 36, No. 4, 889–974 (2006; Zbl 1118.68071)], who constructed relaxed LDCs with the same parameters. This resolves an open problem raised by Gur et al. [loc. cit].

MSC:
68P30 Coding and information theory (compaction, compression, models of communication, encoding schemes, etc.) (aspects in computer science)
68Q17 Computational difficulty of problems (lower bounds, completeness, difficulty of approximation, etc.)
68Q87 Probability in computer science (algorithm analysis, random structures, phase transitions, etc.)

Keywords:
algorithmic coding theory; sublinear algorithms; tensor codes; consistency tests using random walks

Full Text: DOI

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically extracted.