Abstract

Locally-correctable codes (LCCs) and locally-testable codes (LTCs) are special families of error-correcting codes that admit highly efficient sub-linear time algorithms for error correction and detection, respectively, while making a small number of queries to the received word.

LCCs and LTCs were originally studied in complexity theory because of their close relationship to program checking and probabilistically-checkable proofs (PCPs), but in recent years there has been a new incentive for their study due to their potential use for massive data transmission and storage purposes and the successful implementation of related families of local codes in cloud storage systems.

We show constructions of LCCs and LTCs with constant rate, constant relative distance, and sub-polynomial number of queries and running time of the form $\exp(\sqrt{\log n})$ where $n$ is the codeword length. Prior to our work, such codes were known to exist only with polynomial number of queries and running time of the form $n^{\beta}$ and there were several, quite different, constructions known.

Along the way, we also construct LCCs and LTCs over large (but constant) size alphabets, with the same number of queries and running time, which additionally have the property of approaching the Singleton bound: they have almost the best-possible relationship between their rate and distance. Such a result was previously not known for any sub-linear number of queries and running time.

If time permits I will also discuss a very recent work that improves the running time and number of queries of LTCs to a quasi-polylogarithmic function of the form $(\log n)^{O(\log \log n)}$.

Joint work with Swastik Kopparty, Or Meir and Shubhangi Saraf