Lower Bounds for Matching Vector Codes

Abhishek Bhowmick

Abstract

We prove new lower bounds on the encoding length of Matching Vector (MV) codes. These recently discovered families of Locally Decodable Codes (LDCs) originate in the works of Yekhanin and Efremenko and are the only known families of LDCs with a constant number of queries and sub-exponential encoding length. The systematic study of these codes, and their limitations, was initiated by Dvir, Gopalan and Yekhanin [DGY] where quasi-linear lower bounds were proved on their encoding length. Our work makes another step in this direction by proving two new lower bounds. The first is an unconditional quadratic lower bound, conjectured in [DGY], which is the first bound to exceed the known lower bounds for general constant-query LDCs (when the number of queries is greater than four). The second result is a *conditional* super-polynomial lower bound for constant-query MV codes, assuming a well-known conjecture in additive combinatorics–the Polynomial Freiman Rusza conjecture (over Z_m). At the heart of MV codes are families of vectors in Z_m^n with restricted inner products modulo m. More precisely, families $U = (u_1...u_t)$, $V = (v_1...v_t)$ with u_i, v_j in Z_m^n such that $\langle u_i, v_i \rangle = 0 \bmod m$ for all i in $[t]$ and $\langle u_i, v_j \rangle ! = 0 \bmod m$ for $i ! = j$. Our lower bounds for MV codes are obtained by improving the known *upper bounds* on such families–a question that arises independently in combinatorics in the context of set systems with restricted modular intersections. In the course of our proofs we develop certain tools for working with matrices over Z_m that might be of independent interest.

This is joint work with Zeev Dvir and Shachar Lovett.