January 19, 2024

BOUNDED DEGREE- LOW RANK PARITY CHECK CODES.

Low Rank Parity Check Codes (LRPC codes) are the rank-metric analogue of low density parity check codes. We introduced a new constrain on the support of the parity check matrix. In particular we require that the parity check matrix has its support in the $\mathbb{F}_q$-linear space $\mathcal{V}_{a,d} = \langle 1, a, a^2, ..., a^{d-1} \rangle_{\mathbb{F}_q}$.

It is easy to show that LRPC codes of density 2 (i.e. LRPC such that the support of their parity check matrix has dimension 2) correspond to BD-LRPC of bounded degree 2.

Thanks to the special structure of the subspace $\mathcal{V}_{a,d}$, we proved that BD-LRPC codes with bounded degree d can uniquely correct errors of rank weight r when $n - k \geq r + u$ for certain $u \geq 1$, in contrast to the condition $n - k \geq dr$ required for the standard LRPC codes. The probability of failure of the algorithm we propose is exponential in q^{-u+1}.

As the code length n approaches infinity, when $\frac{n}{m} \to 0$, it is shown that u can be chosen as certain constant, which indicates that the BD-LRPC codes with a code rate of R can be, with a high probability, uniquely decodable with the decoding radius $\rho = \frac{r}{n}$ attaining the Singleton bound $1 - R$.