Contribution ID: **126** Type: **not specified**

List Decoding of Rank-Metric Codes with Row-to-Column Ratio Bigger Than 1/2

Friday, July 14, 2023 11:20 AM (20 minutes)

Shu Liu, Chaoping Xing and Chen Yuan

Abstract: Despite of numerous results about the list decoding of Hamming-metric codes, development of list decoding on rank-metric codes is not rapid as its counterpart. The limit on list decoding obeys the Gilbert-Varshamov bound in both the metrics. In the case of the Hamming-metric, the Gilbert-Varshamov bound is a trade-off among rate, decoding radius and alphabet size, while in the case of the rank-metric, the Gilbert-Varshamov bound is a trade-off among rate, decoding radius and column-to-row ratio (i.e., the ratio between the numbers of columns and rows). Hence, alphabet size and column-to-row ratio play the similar role for list decodability in each metric. In the case of the Hamming-metric, it is more challenging to list decode codes over smaller alphabets. In contrast, in the case of the rank-metric, it is more difficult to list decode codes with large column-to-row ratio. In particular, it is extremely difficult to list decoding of square matrix rank-metric codes (i.e., the column-to-row ratio is equal to 1).

The main purpose of this paper is to explicitly construct a class of rank-metric codes mC of rate R with the column-to-row ratio up to $2/3$
and efficiently list decode these codes with decoding radius beyond the decoding radius $(1-R)/2$ (note that $(1-R)/2$ is at least half of relative minimum distance Gd). In literatures, the largest column-to-row ratio of rank-metric codes that can be efficiently list decoded beyond half of minimum distance is $1/2$. Thus, it is greatly desired to efficiently design list decoding algorithms for rank-metric codes with the column-to-row ratio bigger than $1/2$ or even close to 1.
Our key idea is to compress an element of the field F_{q^n} into a smaller F_q-subspace via a linearized polynomial. Thus, the column-to-row ratio gets increased at the price of reducing the code rate. Our result shows that the compression technique is powerful and it has not been employed in the topic of list decoding of both the Hamming and rank metrics.
Apart from the above algebraic technique, we follow some standard techniques to prune down the list. The algebraic idea enables us to pin down the messages
into a structured subspace of dimension linear in the number n of columns. This "periodic" structure allows us to pre-encode the messages to prune down the list.

Presenter: XING, Chaoping

Session Classification: Track A-3