JING HAO, Georgia Institute of Technology
Minimum distance of random linear codes

In coding theory, the trade-off between information rate R and error-correcting ability δ of a code is a central topic of study. Classical work by Gilbert and Varshamov has showed that with high probability, the minimum distance of a random linear code can achieve the G-V bound given by $R = 1 - H_2(\delta)$, where H_2 is the binary entropy function. In this work, we give a full characterization for the minimum distance of a random linear code by comparing it to the random code ensemble where every coordinate of a codeword are taking values uniformly in $\mathbb{F}_q$.