

MINIMAL CODEWORDS IN LINEAR CODES

Y. Borissov, N. L. Manev

The sets of minimal codewords in linear codes were considered for the first time in connection with a decoding algorithm (Tai-Yang Hwang [2]). Additional interest to them was sparked by a work of J. Massey [3], where it was shown that they describe minimal access structures in secret-sharing based on linear codes.

Definition. Let C be a q -ary linear code. A nonzero codeword $\mathbf{c} \in C$ is called **minimal** if its support does not contain the support of any other nonzero codeword as proper subset.

It seems to be quit difficult to describe the set of minimal codewords for an arbitrary linear code even in the binary case. The problem is completely solved only for q -ary Hamming code and for the second order binary Reed-Muller code $RM(2, m)$ [1]. For the general case of the r^{th} order binary Reed-Muller codes as well as for other types of codes only partial results are obtained till now.

In a linear $[n, k, d]$ code any codeword of weight $\leq 2d - 1$ is minimal, and any one of weight $\geq n - k + 1$ is non-minimal. Hence, the interest weights are w :

$$2d \leq w \leq n - k + 1.$$

In this talk we present some recent results about minimal codewords for a class of cyclic codes and r^{th} order binary Reed-Muller codes $R(r, m)$.

References

- [1] A. Ashikhmin, A. Barg, Minimal Vectors in Linear Codes, *IEEE Trans. Inf. Theory*, IT-44, 1998, 5, 2010–2017.
- [2] Tai-Yang Hwang, *Decoding linear block codes for minimizing word error rate*, IEEE Trans. on Information Theory, IT-25 (1979), 6, 733–737.
- [3] J. Massey, *Minimal Codewords and Secret Sharing*, in Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory, Molle, Sweden, 1993, 246–249.