Minimal codewords in Reed-Muller codes

J. Schillewaert, L. Storme and J.A. Thas
Department of Pure Mathematics and Computer Algebra
Ghent University
Krijgslaan 281-S22, B-9000 Gent, Belgium
{jschille, ls, jat}@cage.ugent.be

April 16, 2008

Abstract

Minimal codewords were introduced by Massey [5] for cryptographical purposes. They are used in particular secret sharing schemes, to model the access structures. We study minimal codewords of weight smaller than $3 \cdot 2^{m-r}$ in binary Reed-Muller codes $RM(r, m)$ and translate our problem into a geometrical one, using a classification result of Kasami, Tokura, and Azumi [3, 4] on Boolean functions. In this geometrical setting, we calculate numbers of non-minimal codewords. So we obtain the number of minimal codewords in the cases where we have information about the weight distribution of the code $RM(r, m)$.

The presented results improve previous results obtained theoretically by Borissov, Manev, and Nikova [2], and computer aided results of Borissov and Manev [1].

References

[1] Y. Borissov and N. Manev. Minimal codewords in linear codes. *Serdica Math. J.*, 30(2-3):303–324, 2004.

[2] Y. Borissov, N. Manev, and S. Nikova. On the non-minimal codewords in binary Reed-Muller codes. *Discrete Appl. Math.*, 128(1):65–74, 2003. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[3] T. Kasami and N. Tokura. On the weight structure of Reed-Muller codes. *IEEE Trans. Information Theory*, IT-16:752–759, 1970.

[4] T. Kasami, N. Tokura, and S. Azumi. On the weight enumeration of weights less than 2.5d of Reed-Muller codes. *Information and Control*, 30(4):380–395, 1976.

[5] J. L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.