

A construction of Reed-Muller codes from Boolean functions

Bianca Liana Bercea

Ovidius University from Constanta, bianca.bercea@365.univ-ovidius.ro, ORCID:
0009-0008-0828-0293

Keywords: Boolean functions, Reed-Muller codes, cryptography

Abstract. Boolean functions have important applications in cryptography and coding theory. A famous class of binary codes derived from Boolean functions are the Reed-Muller (RM) codes. These were defined by Reed, and Muller built the way of decoding and implicitly detecting and correcting errors. One of these codes (RM(1,5)) was used in 1969 by the Mariner probe to transmit images from the Moon. Each pixel in the image was assigned one of $2^6 = 64$ degrees of shade, and the six bits of information were encoded in a word of length 32. The RM(1,5) code can correct up to 7 independent errors.

References

- [1] A. Atanasiu, Theory of error correcting codes, Publisher: University of Bucharest. (in Romanian).
- [2] C. Gherghe, D. Popescu, *Cryptography. Codes. Algorithms*. Publisher: University of Bucharest. (in Romanian).
- [3] E. Abbe, A. Shpilka, M. Ye, Reed-Muller Codes: Theory and Algorithms. Arxiv: 2002.03317v2 [cs.IT].