Abstract

Binomial presentation of modular integer programming and applications to coding theory

Irene Márquez-Corbella

imarquez@agt.uva.es

SINGACOM Group
University of Valladolid, Spain
http://www.singacom.uva.es/

The set of minimal codewords in linear codes is related with decoding algorithms and the so-called gradient-like decoding algorithms, which for binary codes can be regarded as an integer programming with binary arithmetic conditions.

Conti and Traverso in [2] proposed an efficient algorithm which uses Gröbner bases to solve integer programming with ordinary integer arithmetic conditions. Then in [3] Ikegami and Kaji extended the Conti-Traverso algorithm to solve integer programming with modulo arithmetic conditions. It seems natural to consider for those problems the Graver basis associated to them which turns to be the set of codewords of minimal support of codes defined on $\mathbb{Z}_q^n$, which in the binary case correspond to the set of minimal codewords. This provides us an universal test set that allows us gradient decoding in those codes related to the test set stated in [1] which we will see that is equivalent to the approach in [2].

Additional interest to the set of minimal codewords is associated to different topics in cryptography. In particular the set of minimal codewords of a code is one to one related to the minimal access structure of secret sharing schemes based on linear codes as J. Massey show in [4].

References

[1] M. Borges-Quintana, M. A. Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro. *Gröbner bases and combinatorics for binary codes*. Appl. Algebra Engrg. Comm. Comput. vol. 19, no. 5, pp. 393–411, 2008.

[2] P. Conti and C. Traverso. *Buchberger algorithm and integer programming*. Proceedings AAECC-9 (new Orleans), Springer LNCS, vol. 539, pp. 130-139, 1991.

[3] D. Ikegami and Y. Kaji. *Maximum Likelihood Decoding for Linear Block Codes Using Grobner Bases*. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. E86-A, no. 3, pp. 643-651, 2003.

[4] J. L. Massey. *Minimal Codewords and Secret Sharing*. Proceedings of the 6th joint Swedish-Russian International Workshop on Information Theory, pp. 276-279, 1993.