MAGMA software development. Optimal codes

Mercè Villanueva

Classical coding theory [5, 8] is concerned about the representation of information that can be transmitted over some noisy channel. In many engineering products, developed using results of the coding theory, optimal codes are used.

Let $\mathbb{F}_q^n$ be the set of all vectors of length n over an alphabet $\mathbb{F}_q$ of size q. The (Hamming) distance between two vectors $u, v \in \mathbb{F}_q^n$, denoted by $d(u, v)$, is the number of coordinates in which they differ. An (n, M, d) q-ary code C is a subset of $\mathbb{F}_q^n$ with cardinality M and minimum (Hamming) distance d. The vectors of a code are called codewords and the minimum distance of C, d, is the minimum value of $d(u, v)$ for all $u, v \in C$ and $u \neq v$. If C is a subgroup of $\mathbb{F}_q^n$, then we say that C is linear. Finally, we say that C is optimal if it has the best possible parameters q, n, d, M, that is, at the same time we cannot increase M for given values q, n, d, and we cannot increase d for given values q, n, M. Optimal codes have being studied intensively [9, 7, 12, 10].

With the extensive use of high performance computers, several new research lines have arisen in the border between mathematics and computer science: the study of algorithmic to manipulate efficiently different mathematical structures and its applications. Nowadays, there exist many tools of symbolic calculation that perform exact calculations (in opposition to approximate) with a great variety of mathematical objects. Typical examples are the commercial products such as Mathematica, MAPLE and MAGMA; though we can also find noncommercial products like Sage, GAP and Macaulay.

For the research and development of applications based on error-correcting codes, it is necessary to have software tools to simulate such codes. Nowadays, MAGMA is the best software designed to solve computational difficult problems in algebra, combinatorics, and especially, in coding theory, since it has very complete and efficient packages to work with them. More specifically, MAGMA has functions to work with linear error correcting codes over finite fields, modular rings and Galois rings [3]. Moreover, the members of our research group have implemented recently a new package in MAGMA with all the necessary functions to work with $\mathbb{Z}_2\mathbb{Z}_4$-additives codes [2]; and have also added new functionalities to the already existing package for linear codes over finite rings [1]. These two new packages can be downloaded from the web page http://ccsg.uab.cat, and the second one has already been integrated inside MAGMA system. For more information on the software MAGMA in general, visit its official web page http://magma.maths.usyd.edu.au/.

It is known that for many parameters, the best codes are nonlinear [4, 6], that is, for given values q, n, d, the codes with the maximum number of codewords M, are nonlinear. However, currently, neither MAGMA nor any symbolic computation system have functions to manipulate such codes in a efficient way and without storing all codewords. We have started the development of a new

MAGMA package to work with nonlinear codes over finite fields [11, 13], with the double purpose of being able to analyse new optimal codes for both previous applications and to offer a new research tool in the coding theory field. The main aim of the project is to contribute on the development of this package. Specifically, the objectives are the study of the main properties of nonlinear codes: size, minimum distance, kernel, coset representatives; the study of the MAGMA software and the new package to work with nonlinear codes; and the construction of some optimal nolinear codes to be included in the MAGMA database connected with the package.

References

[1] R. D. Barrolleta, J. Pernas, J. Pujol, and M.Villanueva, "Codes over Z4. A Magma package," version 2.0, Universitat Autònoma de Barcelona, 2016. http://ccsg/uab.cat.

[2] J. Borges, C. Fernández, J. Pujol, J. Rifà, and M. Villanueva, "Z2Z4-linear codes. A Magma package," version 3.5, Universitat Autònoma de Barcelona, 2012. http://ccsg/uab.cat.

[3] W. Bosma, J. J. Cannon, C. Fieker and A. Steel (Eds.) *Handbook of* MAGMA *Functions*, Edition 2.22, 5669 pages, 2016.

[4] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, "The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes", *IEEE Trans. on Information Theory*, vol. 40, pp. 301-319, 1994.

[5] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[6] M. Kiermaier, A. Wassermann, and J. Zwanzger, "New upper bounds on binary linear codes and a Z4-code with a better-than linear Gray image," 2016. arXiv:1503.03394.

[7] A. Laaksonen and P.R.J. Östergård, "New lower bounds on error-correcting ternary, quaternary and quinary codes," In: Barbero Á., Skachek V., Ytrehus Ø. (eds) Coding Theory and Applications. ICMCTA 2017. Lecture Notes in Computer Science, vol 10495.

[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, New York, 1977.

[9] P.R.J. Östergård, "On the structure of optimal error-correcting codes," *Discrete Mathematics*, vol. 179, no. 1-3, 1998.

[10] J. Pujol, J. Rifà and F. Solov'eva, "Construction of Z_4-Linear Reed-Muller Codes", *IEEE Transactions on Information Theory*, vol. 55, no. 1, pp. 99-104, 2009.

[11] J. Pujol and M. Villanueva, "Binary codes. A Magma package," version 2.0, Universitat Autònoma de Barcelona, 2014. http://ccsg/uab.cat.

[12] J. Rifà, F.I. Solov'eva and M. Villanueva, "On the intersection of $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard codes," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1766-1774, April 2009.

[13] M. Villanueva, F. Zeng, and J. Pujol, "Efficient representation of binary nonlinear codes: constructions and minimum distance computation," Des. Codes and Cryptogr., vol. 76, pp. 3-21, 2015.