Classification of $\mathbb{Z}_{2^s}$-linear Hadamard codes by using MAGMA software

Cristina Fernández-Córdoba, Mercè Villanueva

February 16, 2018

This project is included in the context of algebraic coding theory. In the scheme of communication through noisy channels, error-correcting codes deals with the reliable transmission of information. Initially, these codes were defined over finite fields [11] and, from the paper [9], it started to grow up the study of codes over rings.

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 1$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. The elements of $\mathbb{Z}_{2^s}^n$ will also be called vectors over $\mathbb{Z}_{2^s}$ of length n. A binary code of length n is a nonempty subset of $\mathbb{Z}_2^n$, and it is linear if it is a subspace of $\mathbb{Z}_2^n$. Equivalently, a nonempty subset of $\mathbb{Z}_{2^s}^n$ is a $\mathbb{Z}_{2^s}$-additive if it is a subgroup of $\mathbb{Z}_{2^s}^n$.

The Hamming weight of a binary vector $\mathbf{u} \in \mathbb{Z}_2^n$, denoted by $\mathrm{wt}_H(\mathbf{u})$, is the number of nonzero coordinates of $\mathbf{u}$. The Hamming distance of two binary vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$, denoted by $d_H(\mathbf{u}, \mathbf{v})$, is the number of coordinates in which they differ. Note that $d_H(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_H(\mathbf{v} - \mathbf{u})$. The minimum distance of a binary code C is $d(C) = \min\{d_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$.

In [9], a Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined as $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$ and $\phi(3) = (1, 0)$. There exist different generalizations of this Gray map, which go from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ [6, 7, 10, 12]. Then, we define $\Phi : \mathbb{Z}_{2^s}^n \to \mathbb{Z}_2^{n2^{s-1}}$ as the component-wise Gray map of a generalization of ϕ.

Let $\mathcal{C}$ be a $\mathbb{Z}_{2^s}$-additive code of length n. We say that its binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_{2^s}$-linear code of length $2^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{2^s}^{t_1} \times \mathbb{Z}_{2^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_4^{t_{s-1}} \times \mathbb{Z}_2^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(n; t_1, \ldots, t_s)$.

A binary code of length n, $2n$ codewords and minimum distance $n/2$ is called a Hadamard code. Hadamard codes can be constructed from normalized Hadamard matrices [1, 11]. The $\mathbb{Z}_{2^s}$-additive codes that, under some specific Gray map Φ, give a Hadamard code are called $\mathbb{Z}_{2^s}$-additive Hadamard codes and the corresponding binary images are called $\mathbb{Z}_{2^s}$-linear Hadamard codes, [8].

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 [5]. 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 [3, 4], which are a generalization of linear codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$; and have also added new functionalities to the already existing package for linear codes over finite rings [2]. 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/.

The objectives of this project are to study the $\mathbb{Z}_{2^s}$-linear Hadamard codes; work with the MAGMA software to deal with this family of codes; and use this software in order to classify these codes for some values of their parameters.

References

[1] Assmus, E. F., Key, J. D.: Designs and their codes. Cambridge University Press, Great Britain (1992).

[2] 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.

[3] 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.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, "Z2Z4-linear codes: generator matrices and duality," *Designs, Codes and Cryptography*, vol. 54, no. 2, pp. 167-179, 2010.

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

[6] Carlet, C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inform. Theory, 44, no. 4, pp. 1543–1547 (1998).

[7] Dougherty, S. T., Fernández-Córdoba, C.: Codes Over $\mathbb{Z}_{2^k}$, Gray Map and Self-Dual Codes. Advances in Mathematics of Communications, 5, no. 4, pp. 571–588 (2011).

[8] C. Fernndez-Crdoba, C. Vela, M. Villanueva, "On $\mathbb{Z}_{2^s}$-Linear Hadamard Codes: kernel and partial classification," submitted to *Designs, Codes Cryptogr.*, arXiv:1801.05189, 2017.

[9] Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory, 40, no. 2, pp. 301–319 (1994).

[10] Krotov, D. S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Trans. Inf. Theory, 53, no. 4, pp. 1532–1537 (2007).

[11] MacWilliams, F. J., Sloane, N. J. A.: The theory of error-correcting codes. 16, Elsevier (1977).

[12] Honold, T., Nechaev, A. A.: Weighted modules and representations of codes. Probl. Inf. Transm., 35, no. 3, pp. 1839 (1999).