

On the permutation decoding for binary linear and Z_4 -linear Hadamard codes

R. D. Barrolleta¹, **M. Villanueva¹**

Permutation decoding is a technique, introduced in [3] by MacWilliams, that strongly depends on the existence of special subsets, called PD-sets, of the permutation automorphism group PAut(C) of a linear code C. In [2], it is shown how to find s-PD-sets of minimum size s + 1 for partial permutation decoding for the binary simplex code S_m of length $2^m - 1$, for all $m \ge 4$ and $1 < s \le \lfloor \frac{2^m - m - 1}{m} \rfloor$. In [1], an alternative permutation decoding method is presented, which can be applied to any binary systematic code (not necessarily linear), in particular to any \mathbb{Z}_4 -linear code. Nevertheless, this alternative method assumes that we know an appropriate PD-set for such codes.

In this talk, we obtain s-PD-sets of size s + 1 for binary linear Hadamard codes (extended codes of S_m), following the techniques described in [2]. Furthermore, we provide a criterion to obtain s-PD-sets of the same size for partial permutation decoding for \mathbb{Z}_4 -linear codes. As particular examples, we apply this criterion to (nonlinear) Hadamard \mathbb{Z}_4 -linear codes, where we also prove that such sets are of minimum size. Finally, we present two recursive constructions to obtain s-PD-set for this family of Hadamard \mathbb{Z}_4 -linear codes.

Referencias

- J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva: Permutation decoding of Z₂Z₄-linear codes, *Des. Codes and Cryptogr.*, DOI 10.1007/s10623-014-9946-4, (2014),
- [2] W. Fish, J. D. Key, and E. Mwambene: Partial permutation decoding for simplex codes, Adv. Math. Commun. 6 (4) (2012), 505–516.
- [3] F. J. MacWilliams: Permutation decoding of systematics codes, Bell System Tech. J. 43 (1964), 485-505.

¹Departament d'Enginyeria de la Informació i de les Comunicacions Universitat Autònoma de Barcelona Edifici Q, 08193, Bellaterra (Barcelona) {rolanddavid.barrolleta, merce.villanueva}@uab.cat