Efficient computation of a parity-check matrix for $\mathbb{Z}_{p^s}$-additive codes and $\mathbb{Z}_p\mathbb{Z}_{p^2}\mathbb{Z}_{p^3}$-additive codes

Adrián Torres-Martín, Cristina Fernández-Córdoba, Carlos Vela, Mercè Villanueva

Departament d'Enginyeria de la Informació i de les Comunicacions,
Universitat Autònoma de Barcelona

adrian.torres@uab.cat

Resumen. A linear code over the ring $\mathbb{Z}_{p^s}$ of length n is a submodule of $\mathbb{Z}_{p^s}^n$, where p is a prime and $s \geq 1$. These codes are also called $\mathbb{Z}_{p^s}$-additive codes and can be seen as a generalization of linear codes over $\mathbb{Z}_2$, $\mathbb{Z}_4$, or, more generally, over $\mathbb{Z}_{2^s}$, which have been extensively studied (see, e.g., [3, 4, 5]). We present an efficient method for computing a parity-check matrix of a $\mathbb{Z}_{p^s}$-additive code from a generator matrix in standard form. This generalizes a result given for linear codes over $\mathbb{Z}_4$ in [5]. We also compare the performance of our results, implemented in Magma, with the currently available function in Magma for codes over finite rings in general. Finally, we outline some ideas to generalize these results to $\mathbb{Z}_p\mathbb{Z}_{p^2}\mathbb{Z}_{p^3}$-additive codes, which are submodules of $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2} \times \mathbb{Z}_{p^3}^{\alpha_3}$, for some non-negative integers $\alpha_1, \alpha_2, \alpha_3$, following some of the ideas presented in [1, 2] for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Keywords: $\mathbb{Z}_{p^s}$-additive codes, $\mathbb{Z}_p\mathbb{Z}_{p^2}\mathbb{Z}_{p^3}$-additive codes, parity-check matrix.

References

[1] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva (2010). $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. *Designs, Codes and Criptography*, 54(2), 167–179.

[2] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva (2022). $\mathbb{Z}_2\mathbb{Z}_4$-*Linear Codes*. Springer.

[3] C. Fernández-Córdoba, C. Vela, M. Villanueva (2022). Nonlinearity and kernel of $\mathbb{Z}_2\mathbb{Z}_4$-linear simplex and MacDonald codes. *IEEE Transactions on Information Theory*, 68(11), 7174–7183.

[4] M. K. Gupta (2005). On linear codes over $\mathbb{Z}_{2^s}$. *Designs, Codes and Criptography*, 36, 227–244.

[5] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé (1994). The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2), 301–319.

Agradecimientos. This work has been partially supported by the Spanish MCIN under Grant PID2022-137924NB-I00 (AEI / 10.13039/501100011033 / FEDER, UE).

Indicar la preferencia (subrayar la opción elegida): póster o charla.

Indicar la preferencia (subrayar la opción elegida): Lunes/Martes o Jueves/Viernes.