Additive Complementary Dual Codes Over $\mathbb{F}_{q^2}$

Gyanendra K. Verma* and R. K. Sharma†

Extended Abstract

Coding theory has several uses in areas such as communication theory, information theory, computer theory, and cryptography. Different researchers studied linear codes over finite fields and finite rings due to its linear structure. In particular, linear complimentary dual (LCD) codes over finite fields were extensively investigated because they have applications in many areas like consumer electronics, data storage communication systems and LCD codes can be implemented against side channel attack as well as fault injection attack.

A linear code which intersect its dual trivially is called LCD code. In order to shed further light on this literature, we looked at the incremental work done throughout time in this area. LCD codes were defined and characterised by Massey [4]. LCD codes offer the optimal linear coding solution for the binary adder channel with two users in [5]. In 2010, Borges et al. [3] defined $\mathbb{Z}_2\mathbb{Z}_4$-additive codes as submodules of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ over $\mathbb{Z}_4$. Later, these additive codes were generalized to codes over $\mathbb{Z}_2 \times \mathbb{Z}_{2^s}$ by Aydogdu and Siap [2]. Again Aydogdu et al. [1] introduced $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes and established standard form of generator and parity check matrices for these codes.

Recently, Shi et al.[7, 6] studied additive cyclic complimentary dual and additive complimentary dual (ACD) codes over finite field $\mathbb{F}_4$. They constructed ACD codes over $\mathbb{F}_4$ from binary codes with respect to trace Euclidean and trace Hermitian inner products. Taking inspiration form this,

*Department of Mathematics, Indian Institute of Technology Delhi, India, *email*: gkvermaiitdmaths@gmail.com

†Department of Mathematics, Indian Institute of Technology Delhi, India, *email*: rksharmaiitd@gmail.com

we generalize the additive code over finite field $\mathbb{F}_{q^2}$ where, q is prime power. An additive subgroup of $\mathbb{F}_{q^2}^n$ is said to be an additive code over $\mathbb{F}_{q^2}$ of length n.

In this paper, we define additive codes over finite field $\mathbb{F}_{q^2}$ as additive subgroups where q is prime power. We associate an additive code with a matrix called generator matrix. We characterise trace Euclidean ACD and trace Hermitian ACD codes in terms of generator matrices over the finite field. Also, we construct trace Euclidean ACD and trace Hermtian ACD codes over $\mathbb{F}_{q^2}$ from linear LCD codes over $\mathbb{F}_q$.

References

[1] I. Aydogdu, T. Abualrub, and I. Siap. On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. *International Journal of Computer Mathematics*, 92:1806 – 1814, 2015.

[2] I. Aydogdu and I. Siap. The structure of z 2 z 2 s-additive codes: Bounds on the minimum distance. *Applied Mathematics & Information Sciences*, 7:2271–2278, 2013.

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

[4] J. L. Massey. Reversible codes. *Inf. Control.*, 7:369–380, 1964.

[5] J. L. Massey. Linear codes with complementary duals. *Discret. Math.*, 106-107:337–342, 1992.

[6] M. Shi, N. Liu, J.-L. Kim, and P. Solé. Additive complementary dual codes over $\mathbb{F}_4$. *Designs, Codes and Cryptography*, 2022.

[7] M. Shi, N. Liu, F. Özbudak, and P. Solé. Additive cyclic complementary dual codes over $\mathbb{F}_4$. *Finite Fields Their Appl.*, 83:102087, 2022.