1 LCD codes

Linear complementary dual codes

Lecture 1: Linear complementary dual codes. In this first part of the lectures will introduce the notion of linear complementary dual codes (or codes with complementary duals) in short LCD. These are codes whose intersections with their dual codes are trivial and give an optimum linear coding solution for the two user binary adder channel. They are also used in counter measures to passive and active side channel analyses on embedded cryptosystems, see Carlet and Guilley [3] for a detailed description. We also give a combinatorial construction of LCD codes based on orthogonal matrices, which are essentially equivalent to systematic generator matrices of self-dual codes.

Lecture 2: Some bounds on LCD codes. In [13] Massey showed that there exist asymptotically good LCD codes. In [5] Dougherty et all gave a few bounds on $LCD[n,k]$ and exact values of $LCD[n,k]$ for $k = 1$ only. Later, in [6] the authors study exact values of $LCD[n,k]$ which is the maximum of possible values of d among $[n,k,d]$ binary LCD codes.

Lecture 3: Binary LCD codes with largest minimum weight. Drawing from results obtained in [7] we examine binary linear complementary dual $[n,k]$ codes with the largest minimum weight among all binary linear complementary dual $[n,k]$ codes. We study a characterization of binary linear complementary dual codes with the largest minimum weight for small dimensions. A complete classification of binary linear complementary dual $[n,k]$ codes with the largest minimum weight is also given for $1 \leq k \leq 16$.

Lecture 4: Applications. Special LCD codes. The second part of the lectures will concern LCD codes of a particularly applicable variety that can be obtained from the adjacency matrices of graphs, [8]. We show how LCD [13] codes with a particularly useful feature can be found from the row span over a finite field of adjacency matrices of graphs by considering these together with the codes from the associated reflexive graphs and complementary graphs. Application is made to some particular classes, including uniform subset graphs and strongly regular graphs.

Some additional material on special LCD codes will deal with results obtained in [9]. The authors examine binary and ternary LCD codes from adjacency matrices of the strongly regular Peisert self-complementary graphs $\mathcal{P}^*(q)$ [15], and the strongly regular generalized Peisert $G\mathcal{P}^*(q)$ [14] graphs, where $q = p^{2t}$, $t \geq 1$,

and $p \equiv 3 \pmod 4$ is a prime, in the case when the dual code is the code of the reflexive graph; these graphs have the same parameters as those of Paley graphs, $P(q)$ [2, p.35], *viz.* $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. Small words of small weight are found in the binary and ternary codes of these, and some indications from computations that the square root bound holds for the codes, as it is shown to hold for those from Paley graphs when q is a prime: see [1, Chapter 2], for example. In addition, a decoding algorithm that can be feasible for these LCD codes is proposed by the authors.

Finally, and related to the material presented in Lecture 4, the reader should consider the discussion on codes from adjacency matrices from the Hamming graphs $H^k(n, m)$ which are examined for the property of being special LCD codes. The special property involves being able to propose a feasible decoding algorithm for the binary codes, and also to deduce the dimension of the code from the eigenvalues of an adjacency matrix, which are known for these graphs [10]. In this piece of research the authors discuss some positive results, in particular for the binary and ternary codes of this class of graphs.

References

[1] E. F. Assmus, Jr and J. D. Key, *Designs and their codes*, Cambridge: Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] P. J. Cameron and J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge: Cambridge University Press, 1991, London Mathematical Society Student Texts 22.

[3] Carlet, C. and Guilley, S. Complementary dual codes for counter-measures to side-channel attacks. Proceedings of the 4th ICMCTA Meeting, Palmela, Portugal, (2014). In Coding Theory and Applications. Springer International Publishing, 97-105 (2015).

[4] D Crnković, Ronan Egan, B G Rodrigues and A Švob, LCD codes from weighing matrices. Appl. Algebra Eng. Commun. Comput. **32** (2) (2021), 175–189.

[5] Dougherty, S.T, Kim, J.-L., Ozkaya, B., Sok, L., Sole, P. The combinatorics of LCD codes: linear programming bound and orthogonal matrices. Int. J. Information and Coding Theory, Vol. 4, Nos. 2/3, 2017

[6] Lucky Galvez, Jon-Lark Kim, Nari Lee, Young Gun Roe and Byung-Sun Won. Some bounds on binary LCD codes. Cryptogr. Commun. **10** (2018),719—728.

[7] Masaaki Harada and Ken Saito, Binary linear complementary dual codes. Cryptography and Communications **11** (4) (2019), 677—696.

[8] J D Key and B G Rodrigues. LCD codes from adjacency matrices of graphs. Appl. Algebra Eng. Commun. Comput. **29** (3) (2018), 227–244.

[9] J D Key and B G Rodrigues. Special LCD codes from Peisert and generalized Peisert graphs. Graphs and Combin. **35**(3) (2019) 633–652.

[10] W Fish, J D Key, E Mwambene and B G Rodrigues. Hamming graphs and special LCD codes. Journal of Applied Mathematics and Computing, **61** (1-2) (2019) 461— 479.

[11] T. Le and B. G. Rodrigues, On some codes from rank-3 representations of the simple Chevalley group $G_2(q)$, *Adv. Math. Comm.,* **17** (1) (2023), 207–226.

[12] D. Leemans and B. G. Rodrigues. Linear codes with complementary duals from some strongly regular subgraphs of the McLaughlin graph. *Math. Commun.* **21** (2) (2016), 239–249.

[13] J. Massey. Linear codes with complementary duals. *Disc. Math.*, **106/107** (1992), 337–342.

[14] Natalie Mullin, *Self-complementary arc-transitive graphs and their imposters*, Master's thesis, University of Waterloo, 2009.

[15] Wojciech Peisert, *All self-complementary symmetric graphs*, J. Algebra **240** (2001), 209–229.

[16] B. G. Rodrigues. Linear codes with complementary duals related to the complement of the Higman-Sims graph. Bull. Iranian Math. Soc. **43** (7) (2017), 2183 – 220

[17] B. G. Rodrigues. On special LCD codes related to the Hoffman-Singleton graph. In progress.

[18] N. Sendrier. Linear codes with complementary duals meet the Gilbert-Varshamov bound *Discrete Math.*, **285** (2004), 345–347.