Optimal Linear Codes From Projective Groups

Michael Braun, Axel Kohnert, Alfred Wassermann

Department of Mathematics, University of Bayreuth
95440 Bayreuth, Germany
{Michael.Braun,Axel.Kohnert,Alfred.Wassermann}@uni-bayreuth.de

We explicitly construct linear codes over $\mathbb{F}_q$ with an approach based on work by Hill [3] and Braun [2]. It is based on the following theorem which shows the equivalence between the construction of codes with a prescribed minimum distance and solving a linear system of equations with bounded integral solutions.

Theorem 1 *Let Ω be a maximal set of pairwise lineary independent vectors of $\mathbb{F}_q^k$ unequal to zero. Let $M_{k,q} = (m_{v,w})$ be the $|\Omega| \times |\Omega|$ matrix whose rows resp. columns correspond to the elements of Ω and whose entry $m_{v,w}$ corresponding to the row v and column w is defined to be*

$$m_{v,w} := \begin{cases} 1 & \text{if } \langle v, w \rangle = 0 \\ 0 & \text{else.} \end{cases}$$

Then there is an (n, k, d', q)-code with minimum distance $d' \geq d$ if and only if there is a vector $x \in \{0, \ldots, n\}^{|\Omega|}$ and a vector $y \in \{0, \ldots, n-d\}^{|\Omega|}$ satisfying

$$\text{(1)} \qquad (M_{k,q}| - I) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 0$$

$$\text{(2)} \qquad \sum_{v \in \Omega} x_v = n,$$

where I is the identity matrix. □

Since for interesting parameters these Diophantine linear systems are quite big and can not be solved by contemporary computer methods, we further reduce the size of the system by restricting the search to codes with a prescribed group of automorphisms, see also [1]. Then, in many cases the resulting systems can be solved by algorithms for lattice point enumeration [4]. With this approach many new optimal codes for $\mathbb{F}_q$, $q \in \{2, 3, 5, 7, 8\}$, have been constructed.

References

[1] A. Betten, A. Kerber, A. Kohnert, R. Laue, and A. Wassermann, *The discovery of simple 7-designs with automorphism group PΓL(2,32)*, AAECC 11, LNCS 948, Springer-Verlag, 1995, 131–145.

[2] M. Braun: *Construction of Linear Codes with Large Minimum Distance*. IEEE Transactions on Information Theory, to appear.

[3] R. Hill: *Optimal Linear Codes*. Cryptography and Coding II, Oxford University Press, 1992, 41–70.

[4] A. Wassermann, *Attacking the market split problem with lattice point enumeration*, J. Combinatorial Optimization **6**, 2002, 5–16.