CONSTRUCTION OF (SOMETIMES) OPTIMAL LINEAR CODES

MICHAEL BRAUN, AXEL KOHNERT AND ALFRED WASSERMANN

1. INTRODUCTION

For the purpose of error correcting linear codes over a finite field $GF(q)$ and fixed dimension k we are interested in codes with high minimum distance d as these allow the correction of up to $\lfloor (d-1)/2 \rfloor$ errors. On the other hand we are interested in codes with minimum redundancy, i.e. codes of small length n. High minimum distance and small length are controversial goals for the optimization of codes. A linear code C is called *optimal* in this context if there is no linear code of the same length and higher minimum distance. There are bounds [8] giving limits for the optimal minimum distance of a linear code of fixed length n. There is a lower bound, saying there is a known linear code having this minimum distance. The upper bound is given by theoretic results, for example the Griesmer bound. The known upper bounds are not always exact, meaning that for many parameters $[n, k]$ there are no known codes over $GF(q)$ whose minimal distance is equal to the upper bound. In many cases there is a gap between lower and upper bound. As we are constructing codes we shorten the gap by improving the lower bound. First results obtained with our method were given in [5]. In this paper we report on refinements which allowed the construction of several new codes, in two cases they are optimal.

2. LINEAR CODES WITH PRESCRIBED MINIMUM DISTANCE AND PPRESCRIBED GROUP OF AUTOMORPHISMS

The main theorem for the construction of 'good' (i.e. improving the known lower bound) linear codes is the following one, see [5] and also [1]. We call an $[n, k]$-code over $GF(q)$ with minimum distance d an $[n, k, d; q]$-code.

Theorem 1. *Let G be a subgroup of $GL(k, q)$, let $\omega_0, \ldots, \omega_{m-1}$ be the orbits of G on the 1-subspaces of $GF(q)^k$ and let $\Omega_0, \ldots, \Omega_{m-1}$ be the orbits of G on the*

Key words and phrases. optimal linear code, incidence matrix, group of automorphisms .

set of $k-1$-subspaces with representatives $K_i \in \Omega_i$. Let $M^G_{k,q} = (m^G_{i,j})$ be the $m \times m$ matrix with entries

$$m^G_{i,j} := |\{T \in \omega_j \mid T \subseteq K_i\}|,$$

Then there is an $[n, k, d'; q]$-code with minimum distance $d' \geq d$ such that a generator matrix of this code has G as a group of automorphisms if and only if there is a vector $x \in \{0, \ldots, n\}^m$ and a vector $y \in \{0, \ldots, n-d\}^m$ satisfying

$$\textit{(1)} \qquad (M^G_{k,q}| - I) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = 0$$

$$\textit{(2)} \qquad \sum_{j=0}^{m-1} |\omega_j| \cdot x_j = n,$$

where I is the identity matrix. □

The correspondence between a solution x_i of the linear system of equations and a linear code C is given by the selection of x_i copies of the generators of the $1-$dimensional subspaces in ω_i as columns of the generator matrix. In the case of $0/1$ solutions $(x_1, \ldots, x_m)$ the resulting code is a projective code, i.e. there are no repeated columns in the generator matrix. The above correspondence reduces the problem to a system of Diophantine linear equations, which are solved here by ehaustive enumeration based on lattice basis enumeration, see [13] and [1].

3. Related Work

The matrix M^G defined in the previous section is an incidence matrix reduced by an incidence preserving group action [12]. This construction is a general approach that works for many discrete structures for example designs [2, 3], q-analogs of designs [7], parallelisms in projective geometries [6]. The construction of linear codes with prescribed automorphisms has a long history [9]. Especially the case of cyclic codes or quasi-cyclic codes [10, 11]. The advantage of our method is that we can prescribe the minimum distance. In [4] and [5] this method was applied to the construction of linear codes and already helped to find many new codes. In this article we describe further new sets of parameters of new linear codes improving the previously known lower bounds for the maximal minimum distance. Using different methods there is a lot work to close the gap between the upper bound and lower bound. There are constructive methods which allow the construction of better codes and theoretic considerations which allow to show the non-existence of certain codes, and therefore improve the upper bounds.

4. SEARCH FOR CODES

The construction problem for good linear codes (i.e. codes with a minimum distance near to the upper bound) is now to find a subgroup $G \leq GL(k,q)$ which is large enough to reduce the size of systems of equations such that it can be handled by the solver. But on the other hand there should still be a linear code with these properties, i.e. the system of equations should have a solution. We generated random subgroups using generators of the following types:

- permutation matrix
- block diagonal matrix
- monomial matrix
- random matrix

Taking a single generator we compute the orbits on the points and hyperplanes. If the number of orbits too large we add a further generator to increase the order of the group G, which corresponds to the fusion of orbits, i.e. the reduction of the size of the matrix M^G. On the other hand in the case of a group which was nearly good enough (i.e. there was a code attaining the lower bound) one may try to decrease the order of the group by for example substituting one generator $g \in G$ by g^i with i dividing the order of g. Finally we construct the matrix $M^G_{k,q}$. This work has to be done for fixed k and q. Afterwards we can try to compute solutions for all possible lengths n.

4.1. **Systematic Search for Good Groups.**

For a systematic search of good groups (i.e. groups which appear as a group of automorphisms of a good linear code) we build a table of subgroups $G \leq GL(k,q)$. We only store groups which differ in the orbit sizes, so we forget about non conjugated subgroups, with equal orbit sizes. This method should be improved as the following example shows:
In the case of the recently (see [5]) found $[98,5,80;8]$-code we used the group generated by the following two matrices:

$$\begin{pmatrix} 7 & & & & \\ & 7 & & & \\ 7 & & & & \\ & & & 7 & \\ & & 7 & & \end{pmatrix}, \begin{pmatrix} 4 & & & & \\ & 5 & & & \\ & & 6 & & \\ & & & 5 & \\ & & & & 4 \end{pmatrix}$$

where the non-zero field elements are represented by the numbers $1,\ldots,7$ which are the exponents of a primitive element. The missing entries are all zero. The group is generated by a permutation matrix and a diagonal matrix. Another group with same orbits sizes but only carrying a $[98,5,78;8]$-code is generated by the

very similiar generators:

$$\begin{pmatrix} 7 & & & & \\ & 7 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 7 \end{pmatrix}, \begin{pmatrix} 7 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 1 & \\ & & & & 7 \end{pmatrix}.$$

The difference is that the second diagonal matrix has fixpoints.
Together with the orbit sizes we store the best minimum distance (for a given length n of the code) we found using the stored group and the maximum number of repetitions for the columns of the generator matrix.

4.2. **Improving Results.** Given above information for each group there are several methods available to produce codes with higher minimum distance starting with a given group G from the table:

- Take a subgroup $H < G$. This allows to construct a code with may be larger minimum distance, as at least the same minimum distance can be reached for a fixed n.
- Switch from a projective to a non projective code. This also allows to construct better codes for a larger n, as now we allow repetitions of columns.
- Check simliar groups. One example was the above $[98, 5; 8]-$code.

4.3. **Limits.** The limits for the use of this method are given by the limits of the algorithm for the solution of the system linear equations. We can handle systems with up to about 200 equations. This number corresponds to the number of orbitson the hyper planes. In the case of the original problem this corresponds to the search of a code with a high minimum distance and an automorphism group with at most 200 orbits. On the other hand we construct the generator matrix by taking the generators of the one-dimensional spaces in an orbit, so we are looking for small orbits, which gives us the chance to combine the generator matrix from several orbits. This shows the controversial aims: small number of orbits and small orbit-sizes. Altogether this shows that the problem becomes more difficult the larger the number of code words is. The results of our method show that the biggest case where we found a new code (in [5]) was in the case of $k = 5$ and $q = 8$. This is a code with 32768 code words.

5. RESULTS

The following table we only give codes, which are not in [5] . The two optimal codes are marked using boldface for the minimum distance. In the last column we give the previously known bounds from [8].

q	k	n	d	bounds
2	11	80	33	$32-35$
3	7	46	26	$25-27$
		60	**36**	$35-36$
		243	156	$154-159$
	8	200	126	$124-129$
		205	128	$126-133$
4	6	215	156	$154-159$
5	5	95	72	$71-74$
		126	97	$96-99$
7	5	30	22	$21-23$
		46	35	$34-36$
8	4	112	**96**	$95-96$
9	4	125	108	$107-109$

In the case of the optimal $[60, 7, 36; 3]$ and $[112, 4, 96; 8]$ codes, the upper bound were given by the Griesmer bound and a one-step Griesmer bound, respectively.

REFERENCES

[1] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann: *Error Correcting Linear Codes*, Springer 2005.

[2] A. Betten, R. Laue and A. Wassermann: *Simple* 7*-Designs with Small Parameters*. Journal of Combinatorial Designs 7, pp. 79-94, 1999.

[3] A. Betten, A. Kerber, A. Kohnert, R. Laue and A. Wassermann: *The discovery of simple 7-designs with automorphism group* $P\Gamma L(2, 32)$. Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. 11th international symposium, AAECC-11, Paris, France, July 17-22, 1995, Lect. Notes Comput. Sci. 948, pp. 131-145, 1995.

[4] M. Braun: *Construction of Linear Codes with Large Minimum Distance*. IEEE Transactions on Information Theory, Vol.50, No. 8, August 2004.

[5] M. Braun, A. Kohnert, A. Wassermann: *Optimal Linear Codes From Matrix Groups*, 5p, to appear in IEEE Transactions on Information Theory.

[6] M. Braun and J. Sarmiento: *Parallelisms in Projective Geometries with a Prescribed Group of Automorphisms*, submitted to Journal of Combinatorial Designs.

[7] M. Braun, A. Kerber and R. Laue: *Systematic Construction of* q*-Analogs of Designs*, to appear in Designs, Codes, Cryptography.

[8] A. Brouwer: *Linear Code Bounds*. Online Server http://www.win.tue.nl/~aeb/voorlincod.html

[9] P. Camion: *Linear codes with given automorphism groups*, Discrete Math. 3, pp. 33-45, 1972.

[10] T. A. Gulliver: *Two new optimal ternary two-weight codes and strongly regular graphs*, Discrete Math. 149, pp. 83-92, 1996.

[11] T. A. Gulliver: *A new two-weight code and strongly regular graph*, Appl. Math. Lett. 9, pp. 17-20, 1996.

[12] A. Kerber: *Applied Finite Group Actions*, Springer, 1999.

[13] A. Wassermann: *Attacking the market split problem with lattice point enumeration*, Journal of Combinatorial Optimization 6, pp. 5-16, 2002.

UNIVERSITY OF BAYREUTH, DEPARTMENT OF MATHEMATICS, D-95440 BAYREUTH, GERMANY