Update on the Extension of Good Linear Codes

Axel Kohnert

Lehrstuhl Mathematik II
Universität Bayreuth
95440 Bayreuth
Deutschland

Abstract

In this short note we state how we construct new good linear codes C over the finite field with q elements. We start with already good (= high minimum distance d for given length n and dimension k) codes which we got for example by our method [2,3,4,5]. The advantage of this method is that we explictly get the words of minimum weight d. We try to extend the generator matrix of C by adding columns with the property that at least s of the letters added to the codewords are different from 0. Using this we know that the minimum distance of the extended code is $d + s$ as long as the second smallest weight was $\geq d + s$.

In this note we only state the method and the results. A full version [8] is submitted to the proceedings of Combinatorics 2006.

Key words: finite projective geometry, coding theory, linear codes, minimum weight

Method

A linear $[n, k]_q-$code C is connected (see e.g. [1]) to its generator matrix Γ by the identity:

$$C = \{v\Gamma : v \in GF(q)^k\}.$$

The minimum distance d measures the error correction capability of C. We call C an $[n, k, d]_q$ code. We want to know which vectors $v_1, \ldots, v_s$ from $GF(q)^k$ correspond via multiplication with the generator matrix to codewords of minimum weight d. We call these vectors the *minimum weight generators* of the code C. Denote by $V = \{v_1, \ldots, v_s\}$ the set of elements from $GF(q)^k$ which is the minimum weight generator of C. Our aim is to find a extension of the generator matrix Γ by

Email address: Axel.Kohnert@uni-bayreuth.de (Axel Kohnert).

l columns in a way such that the corresponding extended code C' has minimum distance $> d$. If this is possible we call C' an $l-$extension of C.

We define the following intersection matrix D, which is a $t \times h$ matrix with entries equal to 0 or 1. The rows are labelled by the t minimum weight generators $g_1, \ldots, g_t$ and the columns are labelled by the h possible columns $\gamma_1, \ldots, \gamma_h$ of the generator matrix. The entries are defined as ($<,>$denotes the inner product):

$$D_{i,j} := \begin{cases} 1 & \text{if } < g_i, \gamma_j > \neq 0 \\ 0 & \text{if } < g_i, \gamma_j > = 0 \end{cases}.$$

Using this matrix D, the problem of an good extension is a covering problem and we get the following theorem which in a certain sense is an inverse result to the special puncturing in [7]:

Theorem 1 *$l-$Extension*

Let C be a linear $[n,k,d]_q$ code. We get an $[n+l,k,d+1]_q$ code if we find l columns of the matrix D, such that for each row there is at least one non-zero entry among the l columns.

In the case of a large enough gap between the minimum weight of C and the second smallest weight we get:

Corollary 2 *$(l,s)-$Extension*

Let C be a linear $[n,k,d]_q$ code with a second smallest weight $d+s$. We get an $[n+l,k,d+s]_q$ code if we can find l columns of the matrix D, such that for each row there are at a least s non-zero entries among the l columns.

To solve this problem we use the following equivalent formulation:

Corollary 3 *$l-$Extension as Diophantine inequality*

Let C be a linear $[n,k,d]_q$ code. If there is a $(0/1)-$solution $x = (x_1, \ldots, x_h)$ of the Diophantine system of inequalities:

$$\begin{array}{|c|} \hline \\ D \\ \\ \\ \hline 1 \ldots 1 \ldots 1 \ldots 1 \\ \hline \end{array} \quad x \quad \begin{array}{|c|} \hline \geq 1 \\ \vdots \\ \\ \vdots \\ \geq 1 \\ \hline = l \\ \hline \end{array}$$

then there is an $[n+l,k,d+1]_q$ code.

Computational Problems

The size of the problem is given by the size of the matrix D. We can handle systems with about 500000 entries. The typical linear codes C, where we can apply this method are in the range of codes with about 5000 codewords. In [8] we describe several methods to reduce the size of D.

To apply $l-$extension to a code C, we need to know the minimum weight generator of the code. It is known [9] that already the computation of the minimum weight (which is less information) is $NP-$hard.

But if we apply the corresponding extension algorithm to a code C, we have constructed using the methods described in [2,3,4,5] we already got during this construction the minimum weight generator.

On the other hand codes which can be handled using this method are in most cases small enough, so that it is not difficult to compute the minimum weight generator using complete enumeration or more sophisticated algorithms based on advanced methods for the computation of the minimum distance [1,7].

Results

We found a new $[n = 82, k = 8, d = 49]_{q=3}$ code, which is a $2-$extension of a previously computed $[80, 8, 48]_3$ code with 1320 codewords of minimum weight.

This new code can be extended twice using $1-$extension, giving also new $[83, 8, 50]_3$ and $[84, 8, 51]_3$ codes. For the last one we again apply $2-$extension and afterwards $1-$extension and get new $[86, 8, 53]_3$ and $[87, 9, 54]_3$ codes.

More codes found using $l-$extension have the following parameters:

$[130, 8, 79]_3$

$[187, 6, 135]_4$, $[197, 6, 142]_4$, $[212, 6, 153]_4$, $[227, 6, 165]_4$,
$[232, 6, 169]_4$, $[242, 6, 177]_4$, $[247, 6, 181]_4$

$[191, 7, 134]_4$, $[192, 7, 135]_4$

Here we do not list the derived codes. All these codes are improvements of Brouwers online table [6] of codes, where one can look up the largest known minimum distance for given triples of (n, k, q).

References

[1] A. BETTEN, M. BRAUN, H. FRIPERTINGER, A. KERBER, A. KOHNERT, AND A. WASSERMANN, *Error correcting codes*, Springer, 2006.

[2] M. BRAUN, *Construction of linear codes with large minimum distance*, IEEE Transactions on Information Theory, 50 (2004), pp. 1687–1691.

[3] M. BRAUN, A. KOHNERT, AND A. WASSERMANN, *Construction of (n, r)-arcs in PG$(2, q)$*, Innovations in Incidence Geometry, 1 (2005), pp. 133–141.

[4] ——, *Construction of (sometimes) optimal linear codes*, Bayreuther Mathematische Schriften, 74 (2005), pp. 69–75.

[5] ——, *Optimal linear codes from matrix groups*, IEEE Transactions on Information Theory, 12 (2005), pp. 4247–4251.

[6] A. BROUWER, *Linear code bounds*. *http://www.win.tue.nl/˜aeb/voorlincod.html*.

[7] M. GRASSL AND G. WHITE, *New good linear codes by special puncturing*, in Proceedings International Symposium on Information Theory, 2004. ISIT 2004, 2004, p. 454.

[8] A. KOHNERT, *Extension of good linear codes*, submitted, (2006), p. 6.

[9] A. VARDY, *The intractability of computing the minimum distance of a code.*, IEEE Trans. Inf. Theory, 43 (1997), pp. 1757–1766.