Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 309 (2009) 412–417
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

(l, s)-extension of linear codes

Axel Kohnert

Angewandte Informatik, Universität Bayreuth, 95440 Bayreuth, Deutschland, Germany

Received 26 June 2006; accepted 10 December 2007
Available online 18 January 2008

Abstract

We construct new linear codes with high minimum distance d. In at least 12 cases these codes improve the minimum distance of the previously known best linear codes for fixed parameters n, k. Among these new codes there is an optimal ternary $[88, 8, 54]_3$ code.

We develop an algorithm, which starts with already good codes C, i.e. codes with high minimum distance d for given length n and dimension k over the field $GF(q)$. The algorithm is based on the newly defined (l, s)-extension. This is a generalization of the well-known method of adding a parity bit in the case of a binary linear code of odd minimum weight. (l, s)-extension tries to extend the generator matrix of C by adding l columns with the property that at least s of the l letters added to each of the codewords of minimum weight in C are different from 0. If one finds such columns the minimum distance of the extended code is $d + s$ provided that the second smallest weight in C was at least $d + s$. The question whether such columns exist can be settled using a Diophantine system of equations.

Keywords: Finite projective geometry; Coding theory; Linear codes; Extendable codes; Minimum weight; Diophantine system of equations

1. Introduction

The most prominent example of an extension of a linear code which increases the minimum weight is the addition of a parity bit to a binary linear code of odd minimum weight. There are several papers in which the authors try to generalize this situation.

A code is called *extendable*, if it is possible to find an extension which also increases the minimum distance. Extendability was studied by Hill and Lizak [1,2], van Eupen and Lisonek [3], Simonis [4] and in recent years by Maruta and his coworkers [5–8]. A common theme in this line of work is the study of the weight distribution of a linear code C. The authors derive certain conditions on the weight distribution which are sufficient for the extendability of the code.

We generalize this approach, as we no longer search for one-step extensions only. We try to increase the length of the codewords by l letters in a way such that the minimum distance increases by at least 1. We call this a *good* extension.

This is different from the previous work by Van Eupen and Lisonek [3] where they prove that in certain situations a ternary code is two-fold extendable, this says that it is possible to increase the length and also the minimum distance by

E-mail address: axel.kohnert@uni-bayreuth.de.

0012-365X/$ - see front matter
doi:10.1016/j.disc.2007.12.028

2. The sufficient conditions ensure that the resulting code is self-orthogonal. Two-fold extendability was also studied in [6] and [8].

Concepts used but not defined in this text can be found in any book on linear codes (e.g. [9,10]).

2. (l, s)-extension

Let C be a linear $[n, k]_q$ code of minimum distance d with generator matrix Γ. We call this an $[n, k, d]_q$ code. The C is described by its generator matrix Γ via the relation:

$$C = \{v\Gamma : v \in GF(q)^k\}. \tag{1}$$

Let $c_1, \ldots, c_g$ be the codewords in C of minimum weight d. There are vectors $v_1, \ldots, v_g$ from $GF(q)^k$ such that $c_i = v_i\Gamma$ for all the minimum weight codewords c_i. We call the set $V := \{v_1, \ldots, v_g\} \subset GF(q)^k$ the *minimum weight generator* of the code C. We are looking for an extension of the generator matrix Γ by l columns in a way such that the corresponding extended code has minimum distance larger than d. For an increase in the minimum distance it is necessary that all minimum weight codewords in C are extended by at least one nonzero letter. This will be used to characterize a good extension.

The possible columns for the extension of the generator matrix are the nonzero vectors of $GF(q)^k$. We are interested in the minimum weight of the extended code. Therefore we are only interested in the zero/nonzero property of the letters to be added to the codewords. This property is invariant under scalar multiplication of the possible column by a nonzero element from $GF(q)$, therefore we restrict to columns

$$\gamma_1, \ldots, \gamma_h \tag{2}$$

which are representatives of the one-dimensional subspaces of $GF(q)^k$. In order to have canonical representatives the first nonzero entry of γ_i is assumed to be 1. The number h of possible canonical columns is $\frac{q^k-1}{q-1}$.

We have to check whether the extension by a possible column increases the weight of the actual minimum weight codewords. The minimum weight property, as in the case of the columns is invariant under scalar multiplication by a nonzero element, therefore the number s of the minimum weight codewords in C is a multiple of $(q-1)$ and we have to check only $t := \frac{s}{q-1}$ elements from the minimum weight generator, which again are representatives

$$g_1, \ldots, g_t \tag{3}$$

of certain one-dimensional subspaces of $GF(q)^k$. Here we also use canonical representatives.

For a systematic search by computer defines the *intersection matrix* D, which is a $t \times h$ matrix with entries equal to 0 or 1. The rows are labeled by the t canonical representatives $g_1, \ldots, g_t$ and the columns are labeled by the h possible canonical columns $\gamma_1, \ldots, \gamma_h$. The entries of D are defined as

$$D_{i,j} := \begin{cases} 1 & \text{if } \langle g_i, \gamma_j \rangle \neq 0 \\ 0 & \text{if } \langle g_i, \gamma_j \rangle = 0 \end{cases}. \tag{4}$$

where $\langle , \rangle$ denotes the usual inner product. An entry 1 at the position i, j says that there is a nonzero letter in the codeword $c = g_i\Gamma'$ at position m if a generator matrix Γ' has γ_j as the mth column. An entry 0 says that this letter is 0. Using this we have the following theorem:

Theorem 1 (*Good Extension*). *Suppose that C is a linear $[n, k, d]_q$ code.*

There is a code C' with minimum distance at least $d + 1$ built by l-fold extension of C, if and only if, there are l columns of the matrix D, such that for each row of D there is at least one nonzero entry among the l columns.

Proof. This equivalence follows from the above description of the link between the matrix D and the encoding of the codewords via multiplication by a generator matrix. □

We call such an $[n + l, k]_q$ code C' with minimum distance at least $d + 1$ an $(l, 1)$-*extension* of C. We added l columns to a generator matrix and got an increase in the minimum distance of at least 1. The generator matrix of the code C' is given by the extension of the generator matrix of C by the columns corresponding to the selected l columns