Discrete Mathematics 331 (2014) 22–26

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

New ternary linear codes from projectivity groups

Nicola Pace

Universidade de São Paulo, Inst. de Ciências Matemáticas e de Computação, Av. do Trabalhador São-Carlense, 400, São Carlos, SP 13560-970, Brazil

ARTICLE INFO

Article history:
Received 12 December 2013
Received in revised form 20 March 2014
Accepted 25 April 2014
Available online 14 May 2014

Keywords:
Finite projective space
Group orbit
Projectivity
Linear code

ABSTRACT

In this note, the existence of $[66, 10, 36]_3$ and $[55, 15, 24]_3$ linear codes is proven. These ternary codes are constructed from orbits of a projectivity group of $PG(k-1, F_3)$, for $k = 10, 15$. These new codes and their punctured subcodes improve the best known lower bounds on the largest possible minimum distance.

1. Introduction

Let F_q be a finite field with q elements and F_q^n the vector space of n—tuples over F_q. A q—*ary linear code* $\mathcal{C}$ of length n and dimension k is a k—dimensional subspace of F_q^n. The number of non-zero positions in a vector $x \in \mathcal{C}$ is called the Hamming weight $w(x)$ of x; the *Hamming distance* $d(x, y)$ between two vectors $x, y \in \mathcal{C}$ is defined by $d(x, y) := w(x-y)$. The *minimum distance* of $\mathcal{C}$ is $d(\mathcal{C}) := \min\{w(x) \mid x \in \mathcal{C}, x \neq 0\}$, and a q—ary linear code of length n, dimension k and minimum distance d is indicated as a $[n, k, d]_q$ code. The *dual* $C^\perp$ of a code C consists of all the vectors of F_q^n orthogonal to every codewords in C: $C^\perp := \left\{x \in F_q^n \mid \langle x, y\rangle = 0 \text{ for any } y \in C\right\}$, where $\langle , \rangle$ denotes the inner product in F_q^n. An important bound is the *Griesmer bound*: $n \geq g_q(k, d)$, where $g_q(k, d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$.

Two $[n, k]_q$—codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over F_q are *equivalent* if there exists an n by n monomial matrix M such that $\mathcal{C}_1 M = \mathcal{C}_2$. The automorphism group of a linear code $\mathcal{C}$ is the set of all monomial matrices M such that $\mathcal{C} = \mathcal{C}M$, and it is denoted by $Aut(\mathcal{C})$. Every monomial matrix M can be written as a product $M = D \cdot P$, where D is a diagonal matrix with nonzero diagonal elements and P is a permutation matrix.

In this note, the following problem is considered: given q, n, k, one needs to find the $[n, k, d]_q$—code with largest possible d. In [4], M. Grassl keeps track of the progress on this problem for $q \leq 9$ and maintains a table with the lower bounds on the largest possible minimum distance. Some entries correspond to optimal codes, that is, their minimum distance is known to be the largest possible for the given parameters n, k, q. The codes in this note improve some entries for the case $q = 3$, and the improvements are summarized in Table 1.

E-mail address: nicolaonline@libero.it.

http://dx.doi.org/10.1016/j.disc.2014.04.027

Table 1
New lower bounds on the minimum distance.

$[n, k]$	Previous value	New value
[64, 10]	33	34
[65, 10]	34	35
[66, 10]	35	36
[53, 15]	21	22
[54, 15]	21	23
[55, 15]	22	24
[56, 15]	23	24

2. Geometric description of linear codes

Let $PG(k-1, q)$ be the projective space over the field F_q. Let $\mathcal{C}$ be a q—ary linear code described by a generator matrix G. If there is no 0—column in G, then one can consider the columns of G as points in $PG(k-1, q)$. Vice versa, given a multiset $\mathcal{P} = \{P_1(x_{1,1}, \dots, x_{k,1}), \dots, P_n(x_{1,n}, \dots, x_{k,n})\}$ of points in $PG(k-1, q)$, one can consider the matrix

$$G = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ x_{k,1} & x_{k,2} & \cdots & x_{k,n} \end{pmatrix}.$$

The matrix G is the generating matrix of a q—ary linear code $\mathcal{C}$. If there is no hyperplane containing the points in $\mathcal{P}$, then $\mathcal{C}$ is a linear $[n, k, d]_q$ code, where the minimum distance d is the minimum number of points from $\mathcal{P}$ outside a hyperplane (in the multiset sense), see [1, Theorem 16.1].

A linear $[n, k]_q$—code $\mathcal{C}$ is called *projective* if there is a generator matrix whose columns generate different projective points. The following definitions are equivalent, see [1, Proposition 16.2].

- $\mathcal{C}$ is a projective code.
- The columns of a generator matrix describe different projective points.
- $\mathcal{C}^{\perp}$ does not contain words of weight 2.

Let A be a projectivity group. Then, one can consider orbits of the group A acting on the points of $PG(k-1, q)$. If the projective points in the previous definition constitute an orbit of A, then the code is called *A—transitive*. If the projectivity group is unspecified, then one can simply speak of a *transitive* projective linear code. Many examples known in the literature can be described as transitive projective linear codes. For example, a *simplex code* $\mathcal{S}_k(q)$ is a $\left[(q^k-1)/(q-1), k, q^{k-1}\right]_q$—code, where the columns of the generator matrix are all the points of $PG(k-1, q)$. Since the projective linear group $PGL(k, q)$ acts transitively on the points of $PG(k-1, q)$, every simplex code $\mathcal{S}_k(q)$ is a transitive projective linear code. In $PG(2, q)$ and $PG(3, q)$, orbits of projectivity groups produce interesting arcs, that are geometrical objects equivalent to particular optimal codes, see [6–8] and references therein. For further examples and details, the reader can refer to [1, Section 2.16] and [5, Chapter 13].

Since this approach works for $k = 3$ and $k = 4$, it is reasonable to look for transitive projective linear codes as a source of new linear codes with large minimum distance. In the next sections, new ternary linear codes are constructed. The GAP and Magma code [3,2] and their generator matrices are available at the permanent address:

http://www.nicolapace.it/pub/gf3codes.html.

3. New ternary linear codes

Every linear projectivity $t : PG(k-1, q) \to PG(k-1, q)$ can be identified by a suitable non-singular matrix $T \in GL(k, q)$. The action of the projectivity on the points of $PG(k-1, q)$ is considered: let $P(x_1, \dots, x_k)$ be a point in $PG(k-1, q)$, the point P^t is obtained by multiplying the row-vector $(x_1, \dots, x_k)$ and the matrix T. Namely, if $Q(y_1, \dots, y_k)$ and $\lambda \in F_q^*$ are such that $(x_1, \dots, x_k) \cdot T = (\lambda y_1, \dots, \lambda y_k)$, then $P^t = Q$.

Let $A \leq P\Gamma L(k, q)$ be a projectivity group of $PG(k-1, q)$. The orbit of a point P in A is denoted by P^A. Let $\mathcal{C}$ be a projective linear A—transitive linear code, where the columns of the generator matrix are the points of P^A. Any two such codes are equivalent, hence they have the same length, dimension and minimum distance. Then, w.l.g. any such a code is denoted by $\mathcal{C}(P, A)$.