Linear Algebra and its Applications 433 (2010) 356–364

Contents lists available at ScienceDirect

Linear Algebra and its Applications

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

Some constructions of linearly optimal group codes

Elena Couselo [a,1], Santos González [a,1], Victor Markov [b,2], Consuelo Martínez [a,1,*], Alexander Nechaev [b,2]

[a] Department of Mathematics, University of Oviedo, Spain
[b] Center of New Information Technologies of Moscow State University, Russia

ARTICLE INFO

Article history:
Received 2 March 2009
Accepted 25 February 2010
Available online 3 April 2010

Submitted by R.A. Brualdi

AMS classification:
94B05
94B15
94B60
94B65

Keywords:
Group code
Linearly optimal code
Reed–Solomon code
Group ring

ABSTRACT

We continue here the research on (quasi)group codes over (quasi)group rings. We give some constructions of $[n, n-3, 3]_q$-codes over $\mathbb{F}_q$ for $n = 2q$ and $n = 3q$. These codes are linearly optimal, i.e. have maximal dimension among linear codes having a given length and distance. Although codes with such parameters are known, our main results state that we can construct such codes as (left) group codes. In the paper we use a construction of Reed–Solomon codes as ideals of the group ring $\mathbb{F}_q G$ where G is an elementary abelian group of order q.

1. Introduction

We will extensively use some notions related to group rings. We refer the reader to [4, Appendix 2].

(Quasi-)group codes over a finite ring R are linear codes obtained from left ideals of a (quasi-)group ring $A = RG$ of a finite (quasi-)group G in the following way. Let $G = \{g_1, \ldots, g_n\}$ and $I \leqslant_A A$ be a left

* Corresponding author.
E-mail address: cmartinez@uniovi.es (C. Martínez).

1 Partially supported by Grant MTM2007-67884-C04-01 and IB-08-147.
2 This work was supported by the grants of the President of RF: SS-4.2008.10, SS-1983.2008.1, and by the Grant of RFFR: 08-01-00693-a, 02-01-00687. V. Markov and A. Nechaev thank also Oviedo University for the hospitality.

0024-3795/$ - see front matter
doi:10.1016/j.laa.2010.03.002

ideal of A. Then the set $\mathcal{K} = \mathcal{K}(I)$ of all words $(r_1, \ldots, r_n) \in R^n$ such that $\sum r_i g_i \in I$ is a linear n-code over the ring R, i.e. a submodule of the module $_R R^n$. Such codes will be also called *G-codes over R*, and will be said to be contained in the group ring. Moreover, a left ideal $I \leqslant_A A$ will be identified with the code $\mathcal{K}(I)$ and, for shortness, we will say that I is an $[n, k, d]_q$-code to mean that $\mathcal{K}(I)$ is a code of length n, cardinality q^k and code distance d. This identification allows to define for every $x = \sum r_i g_i \in A$ its *Hamming weight* $\|x\|$ by $\|x\| = \|(r_1, \ldots, r_n)\|$.

There are many results about such codes in the case $R = \mathbb{F}$ a finite field and G an abelian group (mainly a cyclic group with order coprime to $|\mathbb{F}|$) see e.g. [8,3]. In the case of non-abelian groups there are some results in [9–11], where ideals of a semisimple $\mathbb{F}$-algebra $\mathbb{F}G$ were considered.

Let us notice that codes considered in this paper sometimes are referred as left group codes, using the name group code when I is a two-sided ideal of the group algebra.

A natural and first step in the research of loop-codes is the computation of parameters for all possible codes $\mathcal{K} = \mathcal{K}(I)$ and left ideals I of loop-algebras $\mathbb{F}G$ of small orders and to search for the best codes among them. This was carried out in [2].

Following [3], a (generally nonlinear) $[n, k, d]$-code $C \subseteq \mathbb{F}_q^n$ is said to be *optimal* if $|C| = q^k$ is maximal among sizes of all possible n-codes with a given distance d. Remind that any code C satisfies the inequality $k \leqslant n - d + 1$ (Singleton bound) and the code C is called MDS-code if $k = n - d + 1$. Evidently, any MDS-code is optimal.

For any quasi-group ring $A = RG$ there is an important example of a linked quasigroup MDS-code: its *fundamental ideal*

$$\Delta(A) = \left\{ \sum_{g \in G} r(g)g : \sum_{g \in G} r(g) = 0 \right\}. \tag{1}$$

The fundamental ideal $\Delta(A)$ is an $[n, n-1, 2]$-code and can be described also as the R-submodule of A spanned by all differences $e - g,\ g \in G$.

According to the definition of optimal code we will say that a linear $[n, k, d]_q$-code over a field $\mathbb{F}_q$ is *linearly optimal* if k is the maximum of the dimensions of all $\mathbb{F}_q$-linear n-codes with a fixed distance d.

Let $n(k, q)$ (resp. $m(k, q)$) be the maximal length of all MDS-codes C with combinatorial dimension $k = \log_q |C|$ over an alphabet of q elements (resp., for a primary q, the maximal length of all linear MDS codes over the field $\mathbb{F}_q$). Clearly $m(k, q) \leqslant n(k, q)$.

The following simple remark helps to prove that some codes are linearly optimal.

Proposition 1.1 (see [2])**.** *Let n, k, q be natural numbers, q primary, such that*

$$n > m(k + 1, q).$$

Then any $\mathbb{F}_q$-linear $[n, k, n - k]_q$-code is linearly optimal.

Indeed, in other case there exists a linear $[n, k + 1, n - k]_q$-code. But it is an MDS-code. So $n \leqslant m(k + 1, q)$. This is a contradiction.

Corollary 1.2. *Any linear $[tq, tq - 3, 3]_q$ code for $t \geqslant 2$ is linearly optimal.*

Proof. If $q \leqslant k$ then $n(k, q) = k + 1$ by [3]. Now for $k = tq - 3 \geqslant q - 1$ we have

$$m(k + 1, q) = m(tq - 2, q) \leqslant n(tq - 2, q) = tq - 1 < tq. \quad \square$$

In this paper we will give constructions of $[tq, tq - 3, 3]_q$ group codes over $\mathbb{F}_q$ for $t = 2$ and $t = 3$. Linear algebra technics will play a key role in the proofs of our results.

Let us note that linear $[n, n - 3, 3]_q$-codes over $\mathbb{F}_q$ can be easily constructed as a shortcut Hamming $[N, N - 3, 3]$-code for $N = q^2 + q + 1$ [1]. Our main results state that we can construct such codes as group codes over $\mathbb{F}_q$.