Linear Algebra Appl. 457 (2014) 114–153

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Dual codes of product semi-linear codes

Luis Felipe Tapia Cuitiño, Andrea Luigi Tironi *

Departamento de Matemática, Universidad de Concepción, Casilla 160-C, Concepción, Chile

ARTICLE INFO

Article history:
Received 2 January 2014
Accepted 6 May 2014
Available online 29 May 2014
Submitted by R. Brualdi

MSC:
primary 12Y05, 16Z05
secondary 94B05, 94B35

Keywords:
Finite fields
Dual codes
Skew polynomial rings
Semi-linear maps

ABSTRACT

Let $\mathbb{F}_q$ be a finite field with q elements and denote by $\theta : \mathbb{F}_q \to \mathbb{F}_q$ an automorphism of $\mathbb{F}_q$. In this paper, we deal with linear codes of $\mathbb{F}_q^n$ invariant under a semi-linear map $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ for some $n \geq 2$. In particular, we study three kinds of their dual codes, some relations between them and we focus on codes which are products of module skew codes in the non-commutative polynomial ring as a subcase of linear codes invariant by a semi-linear map T. In this setting we give also an algorithm for encoding, decoding and detecting errors and we show a method to construct codes invariant under a fixed T.

0. Introduction

Recently there has been a lot of interest on algebraic codes in the setting of skew polynomial rings which form an important family of non-commutative rings. Skew polynomial rings have found applications in the construction of algebraic codes, where codes are defined as ideals (submodules) in the quotient rings (modules) of skew polynomial rings.

* Corresponding author.
E-mail addresses: ltapiac@udec.cl (L.F. Tapia Cuitiño), atironi@udec.cl (A.L. Tironi).

http://dx.doi.org/10.1016/j.laa.2014.05.011
0024-3795/

The main motivation for considering these codes is that polynomials in skew polynomial rings exhibit many factorizations and hence there are many more ideals in a skew polynomial ring than in the commutative case.

Furthermore, the research on codes in this setting has resulted in the discovery of many new codes with the better Hamming distance than any previously known linear code with same parameters.

Inspired by the recent works [2–4], in Section 1 we introduce the notion of T-codes, that is, linear codes invariant under a semi-linear transformation T, and we characterize them from an algebraic point of view (see Theorem 6). In Section 2, as a consequence of Theorem 12 and Proposition 13, we introduce the definition of *product semi-linear T-codes*, a generalization of the module skew codes and a subcase of linear codes invariant under a semi-linear transformation T (see Definitions 14 and 16, and Remark 18). In particular, we show that in the commutative case any invariant code by means of an invertible linear transformation is isomorphic as a vector space to a product of module codes (see Theorem 12). In Section 3 we study the main properties of the Euclidean dual codes (Theorem 23, Proposition 25 and Remark 24), the quasi-Euclidean and the Hermitian dual codes (Definitions 39 and 51, Theorems 40 and 56) and the main relations among them (Theorem 53 and Corollaries 55 and 57). Finally, in Section 4 we give an algorithm for encoding, decoding and detecting errors by a product semi-linear code (Algorithm 2), while in Section 5 we show a method to construct codes invariant under a semi-linear transformation (e.g., see Proposition 66 for the commutative case).

1. Notation and background material

Let $\mathbb{F}_q$ be a finite field with q elements and denote by θ an automorphism of $\mathbb{F}_q$. Let us recall here that if $q = p^s$ for some prime number p, then the map $\tilde{\theta} : \mathbb{F}_q \to \mathbb{F}_q$ defined by $\tilde{\theta}(a) = a^p$ is an automorphism on the field $\mathbb{F}_q$ which fixes the subfield with p elements. This automorphism $\tilde{\theta}$ is called the *Frobenius automorphism* and it has order s. Moreover, it is known that the cyclic group it generates is the full group of automorphisms of $\mathbb{F}_q$, i.e. $\mathrm{Aut}(\mathbb{F}_q) = \langle\tilde{\theta}\rangle$. Therefore, any $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ is defined as $\theta(a) := \tilde{\theta}^t(a) = a^{p^t}$, where $a \in \mathbb{F}_q$ and t is an integer such that $0 \leq t \leq s$. Furthermore, when θ will be the identity automorphism $id : \mathbb{F}_q \to \mathbb{F}_q$, we will write simply $\theta = id$.

If $n \geq 2$ is an integer, then we denote by $\mathbb{F}_q^n$ the vector space

$$\mathbb{F}_q^n := \underbrace{\mathbb{F}_q \times \ldots \times \mathbb{F}_q}_{n\text{-times}}.$$

It is well known that a semi-linear map $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is the composition of an automorphism θ of $\mathbb{F}_q$ with an $\mathbb{F}_q$-linear transformation M, i.e. $(\vec{v})T := (\vec{v})\Theta \circ M$, where $(v_1, \ldots, v_n)\Theta := (\theta(v_1), \ldots, \theta(v_n))$ and M is an $n \times n$ matrix with coordinates in $\mathbb{F}_q$. In this case we call T a *θ-semi-linear map*, or a *θ-semi-linear transformation*.

For any $\vec{v} \in \mathbb{F}_q^n$ and any T as above, let $[\vec{v}]$ denote the T-cyclic subspace of $\mathbb{F}_q^n$ spanned by $\{\vec{v}, (\vec{v})T, (\vec{v})T^2, \ldots\}$.