Journal of Pure and Applied Algebra 219 (2015) 1031–1044

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

A zero-dimensional approach to Hermitian codes

Edoardo Ballico [a,1], Alberto Ravagnani [b,*]

[a] *Department of Mathematics, University of Trento, Via Sommarive 14, 38123 Povo (TN), Italy*
[b] *Institut de Mathématiques, Université de Neuchâtel, Emile-Argand 11, CH-2000 Neuchâtel, Switzerland*

ARTICLE INFO

Article history:
Received 31 August 2012
Received in revised form 12 December 2013
Available online 19 May 2014
Communicated by I.M. Duursma

MSC:
94B27; 14C20; 11G20

ABSTRACT

We study the algebraic geometry of a family of evaluation codes from plane smooth curves defined over any field. In particular, we provide a cohomological characterization of their dual minimum distance. After having discussed some general results on zero-dimensional subschemes of the plane, we focus on the interesting case of Hermitian s-point codes, describing the geometry of their dual minimum-weight codewords.

1. Introduction

Let $\mathbb{F}$ be any finite field and let $n \geq 1$ be an integer. A **linear code** of length n and dimension k over $\mathbb{F}$ is a k-dimensional vector subspace $\mathscr{C} \subseteq \mathbb{F}^n$. The elements of $\mathscr{C}$ are called **codewords**. For any $v, w \in \mathscr{C}$ define the **distance** between v and w by $d(v,w) := |\{1 \leq i \leq n : v_i \neq w_i\}|$. The **weight** of a codeword $v \in \mathscr{C}$ is defined as $\mathrm{wt}(v) := d(v,0)$. The **minimum distance** of a code $\mathscr{C} \subseteq \mathbb{F}^n$ of at least two elements is the positive integer

$$d(\mathscr{C}) := \min_{v \in \mathscr{C} \setminus \{0\}} \mathrm{wt}(v) = \min_{v \neq w \in \mathscr{C}} d(v,w).$$

A code of minimum distance d corrects $\lfloor (d-1)/2 \rfloor$ errors: the higher is the minimum distance, the higher is the correction capability. Define the inner product in $\mathbb{F}^n$ by $v \cdot w := \sum_{i=1}^n v_i w_i$. The **dual code** of $\mathscr{C}$ is the $(n-k)$-dimensional code $\mathscr{C}^\perp := \{u \in \mathbb{F}^n : u \cdot v = 0 \text{ for any } v \in \mathscr{C}\}$.

Definition 1. We say that codes $\mathscr{C}, \mathscr{D} \subseteq \mathbb{F}^n$ are **strongly isometric** if the codewords of $\mathscr{C}$ are obtained multiplying component-wise the codewords of $\mathscr{D}$ by a vector of $\mathbb{F}^n$ whose components are all nonzero.

* Corresponding author.
E-mail addresses: edoardo.ballico@unitn.it (E. Ballico), alberto.ravagnani@unine.ch (A. Ravagnani).
[1] Partially supported by MIUR and GNSAGA.

http://dx.doi.org/10.1016/j.jpaa.2014.05.031
0022-4049/

Remark 2. The strong isometry is an equivalence relation on the set of codes in $\mathbb{F}^n$. Strongly isometric codes have the same dimension and the same minimum distance. Moreover, a strong isometry preserves the support of the codewords and, in particular, the number of minimum-weight codewords of a code. Codes $\mathscr{C}$ and $\mathscr{D}$ are strongly isometric if and only if their dual codes $\mathscr{C}^\perp$ and $\mathscr{D}^\perp$ are strongly isometric.

Let $\mathbb{P}^r$ be the projective r-dimensional space over $\mathbb{F}$, and let $C \subseteq \mathbb{P}^r$ be a connected smooth curve defined[2] over $\mathbb{F}$. Assume that C is a complete intersection. Choose any subset $B \subseteq C(\mathbb{F})$ of $\mathbb{F}$-rational points of C and an integer $d > 0$. Finally, consider the linear map

$$\mathrm{ev} : H^0\big(C, \mathscr{O}_C(d)\big) \to \mathbb{F}^{|B|}$$

($|B|$ denotes the cardinality of B) which evaluates a degree d homogeneous form on C at the points appearing in B. Being a vector subspace of $\mathbb{F}^{|B|}$, the image of ev, say $\mathscr{C}$, is a linear code of length $|B|$ over the finite field $\mathbb{F}$.

Recently, A. Couvreur showed in [2] that a lower bound on the minimum distance of $\mathscr{C}^\perp$ can be expressed in terms of d and the projective geometry of B (for instance, the existence in B of $d+2$ collinear points). Codes arising from geometric constructions are known to have good parameters for applications and a wide literature on the topic is available (see in particular [15] and [16]).

In this paper we focus on the case $r = 2$ of the described approach (i.e., on the case of plane smooth curves) and provide an improvement of Couvreur's method in this specific context. More precisely, we introduce zero-dimensional schemes in the setup, and study codes obtained evaluating vector spaces of the more general form $H^0(C, \mathscr{O}_C(d)(-E))$, where $E \subseteq \mathbb{P}^2$ is a zero-dimensional scheme whose support avoids the set B in the notation above. This class of codes includes many classical Goppa codes (see Remark 14 on page 1036). Then we apply the results for arbitrary curves to the special case of codes from the Hermitian curve, providing a geometric characterization of the dual minimum-weight codewords of many Hermitian s-point codes (see [15], Chapter 10 for the definitions).

1.1. Layout of the paper

The paper is organized in three main parts. In Section 2 we characterize the dual minimum distance of codes arising from smooth plane curves, and establish a key lemma to control zero-dimensional plane schemes from a cohomological point of view. In Section 3 we describe some geometric properties of Hermitian s-point codes. In Section 4 we prove our main results on Hermitian s-point codes.

1.2. Main references

One-point codes from the Hermitian curve are well-studied, and efficient methods to decode them are known [16–18]. The minimum distance of Hermitian two-point codes has been first determined by M. Homma and S.J. Kim [6–9] and more recently S. Park gave explicit formulas for the dual minimum distance of such codes (see [14]) using different techniques. The second and the third Hamming weight of one-point codes on the Hermitian curve are studied in [12,18] and [13]. The second Hamming weight of Hermitian two-point codes is treated in [10].

[2] The curve C could be not defined over $\mathbb{F}$, but only over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$.