Journal of Symbolic Computation 73 (2016) 27–45

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On the small-weight codewords of some Hermitian codes

Chiara Marcolla[a], Marco Pellegrini[b], Massimiliano Sala[a]

[a] Department of Mathematics, University of Trento, Italy
[b] Department of Mathematics, University of Firenze, Italy

ARTICLE INFO

Article history:
Received 28 April 2014
Accepted 19 February 2015
Available online 5 March 2015

Keywords:
Affine-variety code
Hamming weight
Hermitian code
Hermitian curve
Linear code
Minimum-weight words

ABSTRACT

For any affine-variety code we show how to construct an ideal whose solutions correspond to codewords with any assigned weight. We are able to obtain geometric characterizations for small-weight codewords for some families of Hermitian codes over any $\mathbb{F}_{q^2}$. From these geometric characterizations, we obtain explicit formulas. In particular, we determine the number of minimum-weight codewords for all Hermitian codes with $d \leq q$ and all second-weight codewords for distance-3, 4 codes.

1. Introduction

Let q be a power of a prime, then the *Hermitian curve* $\mathcal{H}$ is the plane curve defined over $\mathbb{F}_{q^2}$ by the affine equation $x^{q+1} = y^q + y$, where $x, y \in \mathbb{F}_{q^2}$.

This curve has genus $g = \frac{q(q-1)}{2}$ and has q^3 $\mathbb{F}_{q^2}$-rational affine points, plus one point at infinity, so it has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$ and therefore it is a maximal curve (Ruck and Stichtenoth, 1994). This is the best known example of maximal curve and there is a vast literature on its properties, see Hirschfeld et al. (2008) for a recent survey. Moreover, the Goppa code (Goppa, 1981, 1988) constructed on this curve is by far the most studied, due to the simple basis of its Riemann–Roch space (Stichtenoth, 1993), which can be written explicitly. The Goppa construction has been generalized in

E-mail addresses: chiara.marcolla@unitn.it (C. Marcolla), pellegrin@math.unifi.it (M. Pellegrini), maxsalacodes@gmail.com (M. Sala).

http://dx.doi.org/10.1016/j.jsc.2015.03.003
0747-7171/© 2015 Elsevier Ltd. All rights reserved.

Vlăduţ and Manin (1984) to higher dimensions. A simpler description can be found in Fitzgerald and Lax (1998) for the so-called affine-variety codes.

In this paper we provide an algebraic and geometric description for codewords of a given weight belonging to any fixed affine-variety code. In Augot (1996) the solving of a (multivariate) polynomial equation system was proposed for the first time to determine minimum-weight codewords of cyclic codes, while in Sala (2007) a more efficient system was proposed. Our proposal can be seen as a generalization to the affine-variety case of Sala (2007). A similar approach can be used to decode codes, as described, for example, in de Boer and Pellikaan (1999) and surveyed in Mora and Orsini (2009). The specialization of our results to the Hermitian case allows us to give explicit formulas for the number of some small-weight codewords. Codes over the Hermitian curve have been studied along the years and in Høholdt et al. (1998), along with a survey of known results, a new challenging approach as explicit evaluation codes is proposed. We expand on our 2006 previous result, presented orally as Sala and Pellegrini (2006), where we proved the intimate connection between curve intersections and minimum-weight codewords.

The paper is organized as follows:

- In Section 2 we provide our notation, our first preliminary results on the algebraic characterization of fixed-weight codewords of any affine-variety code and some easy results on the intersection between the Hermitian curve and any line.
- In the beginning of Section 3 we provide a division of Hermitian codes in four phases, which is a slight modification of the division in Høholdt et al. (1998), and we give our algebraic characterization of fixed-weight codewords of some Hermitian codes. We study in depth the first phase (that is, $d \leq q$) in Section 3.2 and we use these results to completely classify geometrically the minimum-weight codewords for all first-phase codes in Section 3.3. In Section 3.4 we can count some special configurations of second weight codewords for any first-phase code and finally in Section 3.5 we can count the exact number of second-weight codewords for the special case when $d = 3, 4$. A result in this section relies on our results (Marcolla et al., 2014) on intersection properties of $\mathcal{H}$ with some special conics, firstly presented at Effective Method in Algebraic Geometry, MEGA 2013.
- In Section 4 we draw some conclusions and propose some open problems.

2. Preliminary results

2.1. Known facts on Hermitian curve and affine-variety codes

From now on we consider $\mathbb{F}_q$ the finite field with q elements, where q is a power of a prime and $\mathbb{F}_{q^2}$ the finite field with q^2 elements. Also, $\overline{\mathbb{F}}_{q^2}$ will denote the algebraic closure of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. Let α be a fixed primitive element of $\mathbb{F}_{q^2}$, and we consider $\beta = \alpha^{q+1}$ as a primitive element of $\mathbb{F}_q$. From now on q, q^2, α and β are understood as above.

The *Hermitian curve* $\mathcal{H} = \mathcal{H}_q$ is defined over $\mathbb{F}_{q^2}$ by the affine equation

$$x^{q+1} = y^q + y \quad \text{where } x, y \in \mathbb{F}_{q^2}. \tag{1}$$

This curve has genus $g = \frac{q(q-1)}{2}$ and has $n = q^3$ rational affine points, denoted by $P_1, \ldots, P_n$. For any $x \in \mathbb{F}_{q^2}$, Eq. (1) has exactly q distinct solutions in $\mathbb{F}_{q^2}$. The curve contains also one point at infinity P_∞, so it has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$ (Ruck and Stichtenoth, 1994).

Let $t \geq 1$. For any ideal I in the polynomial ring $\mathbb{F}_q[X]$, where $X = \{x_1, \ldots, x_t\}$, we denote by $\mathcal{V}(I) \subset (\overline{\mathbb{F}}_q)^t$ its variety, that is, the set of its common roots. For any $Z \subset (\overline{\mathbb{F}}_q)^t$ we denote by $\mathcal{I}(Z) \subset \mathbb{F}_q[X]$ the vanishing ideal of Z, that is, $\mathcal{I}(Z) = \{f \in \mathbb{F}_q[X] \mid f(Z) = 0\}$.

Let $g_1, \ldots, g_s \in \mathbb{F}_q[X]$, we denote by $I = \langle g_1, \ldots, g_s \rangle$ the ideal generated by the g_i's. Let $\{x_1^q - x_1, \ldots, x_t^q - x_t\} \subset I$. Then I is zero-dimensional and radical (Seidenberg, 1974). Let $\mathcal{V}(I) = \{P_1, \ldots, P_n\}$.