21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

# ON THE DUAL MINIMUM-WEIGHT CODEWORDS OF ONE-POINT GOPPA CODES

ALBERTO RAVAGNANI[1]

*Department of Mathematics, University of Neuchâtel*
*Emile-Argand 11, CH-2000 Neuchâtel (Switzerland)*

EDOARDO BALLICO[2]

*Department of Mathematics, University of Trento*
*Via Sommarive 14, 38100 Povo, TN (Italy)*

ABSTRACT. One-point Goppa codes are among the most studied algebraic geometric codes. They are obtained evaluating vector spaces of rational functions on curves defined over finite fields at appropriate sets of points. In some relevant cases (e.g., for codes from norm-trace curves) the dual minimum-weight codewords of such codes are characterized by the intersections of the underlying curve with lines and conics in the plane. We describe a geometric method to determine the dual minimum distance of such codes and explicitly count their dual minimum-weight codewords.

## 1. MOTIVATIONS

Goppa codes are error-correcting codes for which we have efficient decoding algorithms. They are becoming more and more interesting for their possible applications in cryptography through the McEliece cryptosystem (see [13]). The minimum distance and the minimum-weight codewords play an important role in the decoding performance of a code.

## 2. ONE-POINT CODES

Let us briefly recall the definition of one-point Goppa code. See [14] for a geometric introduction to Goppa codes and [15] for a more number-theoretic approach.

**Definition 1.** Let $X \subseteq \mathbb{P}^r$ be an algebraic curve defined over a finite field $\mathbb{F}_q$, and let $P \in X(\mathbb{F}_q)$ be a raional point of $X$. For $m \in \mathbb{Z}$, denote by $\mathscr{L}(mP)$ the Riemann-Roch space associated to the divisor $mP$ on $X$. Set $\{P_1,...,P_n\} := X(\mathbb{F}_q) \setminus \{P\}$. The **one-point code** $\mathscr{C}(X,mP)$ is defined as the image of the evaluation map of rational functions

$$\mathrm{ev} : \mathscr{L}(mP) \to \mathbb{F}_q^n, \qquad f \mapsto (f(P_1),...,f(P_n)).$$

The dual code of $\mathscr{C}(X,mP)$ will be denoted by $\mathscr{C}^{\perp}(X,mP)$.

Among the most commonly used curves for constructing one-point codes there are norm-trace curves (in particular, Hermitian curves) and curves which are covered by the Hermitian curve. See [15], Section 8.3, [10] and [6] among the others. This talk is concerned with the parameters of codes

*E-mail addresses*: alberto.ravagnani@unine.ch[1], edoardo.ballico@unitn.it[2].

ISBN: 978-90-367-6321-9

of type $\mathscr{C}^{\perp}(X,mP)$ arising from such curves. In particular, we are interested in their minimum distance and in the number of their minimum-weight codewords.

## 3. From intersections of curves to minimum-weight codewords

When studying a code of type $\mathscr{C}^{\perp}(X,mP)$ a simple description of the Riemann-Roch space $\mathscr{L}(mP)$ on $X$ is very useful. For many curves employed in coding theory (e.g., for Hermitian curves and norm-trace curves) the Riemann-Roch space $\mathscr{L}(mP)$ turns out to be a vector space of homogeneous forms with some prescribed zeroes. For example, if $\mathscr{H}_q$ is the Hermitian curve[1] and $P_\infty := (0:1:0)$ is its point at infinity then, for any $m \in \mathbb{Z}_{>0}$,

$$L(mP_\infty) = H^0(\mathscr{H}_q, \mathscr{O}_{\mathscr{H}_q}(d)(-aP_\infty)),$$

where $m = d(q+1)-a$ with $0 \leq a \leq q$ (see [4], Remark 7). Analogous results hold for norm-trace curves and for curves covered by the Hermitian curve (see [3] and [2] for details). As a consequence, it is natural to study codes obtained evaluating vector spaces of the form

$$H^0(X, \mathscr{O}_X(d)(-E)),$$

where $X$ is a plane curve defined over a finite field, $E \subseteq X$ is a zero-dimensional scheme whose support consists of rational points, and $d$ is a positive integer. To construct codes as long as possible, we simply evaluate the elements of $H^0(X, \mathscr{O}_X(d)(-E))$ at all the rational points of $X$ avoiding the support of $E$. We denote such a code by $\mathscr{C}(X,d,E)$ and its dual by $\mathscr{C}^{\perp}(X,d,E)$. See [1], Lemma 1 for the dimension of codes of this form.

In many relevant cases (for example, when $X = \mathscr{H}_q$) a support $S$ of a minimum-weight codeword of $\mathscr{C}^{\perp}(X,d,E)$ is characterized (see [4], Lemma 17 and Proposition 13 for a detailed proof) by the non-vanishing condition

$$\dim\, H^1(\mathbb{P}^2, \mathscr{I}_{E\cup S}(d)) > 0.$$

Classical results on zero-dimensional schemes in the plane (e.g., [9]) provide a geometric description of such a condition in terms on the intersections of $E \cup S$ with low degree curves in the plane. As a straightforward consequence, the possible supports $S$ of the minimum-weight codewords of $\mathscr{C}^{\perp}(X,d,E)$ are completely determined by the rational intersections of $X$ with low degree curves in the plane. Determining such intersections is a well-studied problem in discrete geometry, and very precise results are available for curves of degree one and two, i.e., for lines and conics (see in particular [11] and [12]).

**Remark 2.** Notice that for any linear code over a finite field $\mathbb{F}_q$ the number of minimum-weight codewords, say $m$, and the number of their possible supports, say $s$, are related by $m = s(q-1)$. Hence the knowledge of all the possible supports gives, in particular, the number of the minimum weight codewords.

**Remark 3.** A. Couvreur studied codes obtained evaluating homogeneous forms on curves and surfaces first. In particular, he provided in [8] a geometric method to lower bound the dual minimum distance of codes obtained evaluating vector spaces of the form $H^0(X, \mathscr{O}_X(d))$, where $X$ is a projectively connected and smooth complete intersection. Introducing zero-dimensional schemes in the framework of [8], we improved the method for the special case of plane curves.

[1] Let $\mathbb{P}^2$ be the projective plane of coordinates $(x:y:z)$ over the algebraic closure of a finite field $\mathbb{F}_{q^2}$. The Hermitian curve $\mathscr{H}_q \subseteq \mathbb{P}^2$ is defined over $\mathbb{F}_{q^2}$ by the affine equation $y^q + y = x^{q+1}$.

## 4. SOME EXPLICIT RESULTS

Here we state two of the main results we obtained for codes from an Hermitian curve $\mathscr{H}_q$ defined over $\mathbb{F}_{q^2}$. In the notation of Definition 1, we provide a characterization (and in many cases the exact number) of the minimum-weight codewords of any code $\mathscr{C}^\perp(\mathscr{H}_q, mP_\infty)$ with $0 < m \leq q^2+q$.

**Theorem 4** ([4], Theorem 18)**.** Let $m \in \mathbb{Z}_{>0}$. Write $m = d(q+1)-a$, with $0 \leq a \leq q$. Assume $d \leq q-1$. Set $\mathscr{C} := \mathscr{C}(\mathscr{H}_q, mP_\infty)$. Denote by $\delta$ the minimum distance of $\mathscr{C}^\perp$ and by $A_\delta$ the number of its minimum-weight codewords.

(1) If $a > d$ then $\mathscr{C}^\perp$ is isometric to $\mathscr{C}^\perp(\mathscr{H}_q, (d-1)(q+1)P_\infty)$, which is studied in the next case.
(2) Assume $a = 0$. Then $\delta = d+2$. Distinct points $P_1, ..., P_\delta$ of $\mathscr{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ are the support of a minimum-weight codeword of $\mathscr{C}^\perp$ if and only if they are collinear. Moreover,

$$\frac{A_\delta}{q^2-1} = \begin{cases} (q^4-q^3) & \text{if } d = q-1, \\ q^2\binom{q}{\delta} + (q^4-q^3)\binom{q+1}{\delta} & \text{if } d < q-1. \end{cases}$$

(3) If $0 < a \leq d$ then $\delta = d+1$. Distinct points $P_1, ..., P_\delta$ in $\mathscr{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ are the support of a minimum-weight codeword of $\mathscr{C}^\perp$ if and only if $P_\infty, P_1, ..., P_\delta$ are collinear. Moreover,

$$\frac{A_\delta}{q^2-1} = q^2\binom{q}{\delta}.$$

**Theorem 5** ([4], Theorem 19)**.** Fix an integer $a$ with $0 \leq a \leq q$ and set $m := q(q+1)-a$. Denote by $\delta$ the minimum distance of $\mathscr{C}^\perp := \mathscr{C}^\perp(\mathscr{H}_q, mP_\infty)$, and by $A_\delta$ the number of its minimum-weight codewords.

(1) If $a = 0$ then $\delta = 2q+2$. Distinct points $P_1, ..., P_\delta$ in $\mathscr{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ are the support of a minimum-weight codeword of $\mathscr{C}^\perp$ if and only if they lie on a conic of $\mathbb{P}^2$.
(2) If $a = 1$ then $\delta = 2q+1$, and distinct points $P_1, ..., P_\delta$ in $\mathscr{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ are the support of a minimum-weight codeword of $\mathscr{C}^\perp$ if and only if $P_\infty, P_1, ..., P_\delta$ lie on a conic of $\mathbb{P}^2$.
(3) If $2 \leq a < q$ then $\delta = 2q$, and the following two facts hold.
   (a) Assume $q$ even. Then points $P_1, ..., P_\delta$ in $\mathscr{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ are the support of a minimum-weight codeword of $\mathscr{C}^\perp$ if and only if they lie on two lines intersecting at $P_\infty$. Moreover,

$$A_\delta = (q^2-1)\binom{q^2}{2}.$$

   (b) Assume $q$ odd. Then distinct points $P_1, ..., P_\delta$ in $\mathscr{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ are the support of a minimum-weight codeword of $\mathscr{C}^\perp$ if and only if either they lie on two lines intersecting at $P_\infty$, or they lie on a smooth conic of $\mathbb{P}^2$ which is tangent to $X$ at $P_\infty$. Moreover,

$$A_\delta = (q^2-1)\left[q^2(q+1)(q-1)/2 + \binom{q^2}{2}\right].$$

Analogous results (even if less detailed) can be obtained for codes from more general norm-trace curves and quotients of the Hermitian curve ([3] and [2]). In some cases two-point Goppa codes can be studied using the same method (see [5]).

## REFERENCES

[1] E. Ballico, A. Ravagnani, *A zero-dimensional cohomological approach to Hermitian codes*. `http://arxiv.org/abs/1202.0894`.

[2] E. Ballico, A. Ravagnani, *On the dual minimum distance and minimum weight of codes from a quotient of the Hermitian curve*. Applicable Algebra in Engineering, Communication and Computing, 24 (2013), pp. 343 – 354.

[3] E. Ballico, A. Ravagnani, *On the duals of geometric Goppa codes from norm-trace curves*. Finite Fields and their Applications, vol. 20 (2013), pp. 30 – 39.

[4] E. Ballico, A. Ravagnani, *On the geometry of Hermitian one-point codes*. Journal of Algebra (to appear).

[5] E. Ballico, A. Ravagnani, *The dual geometry of Hermitian two-point codes*. Discrete Mathematics, 313 (2013), 23, pp. 2687 – 2695.

[6] M. A. Coleman, N. Drake, G. L. Matthews, *Codes from a quotient of the Hermitian curve attaining the designed distance*. Congressus Numerantium, 182 (2006), 161–170.

[7] A. Couvreur, *Differential Approach for the Study of Duals of algebraic-Geometric Codes on Surfaces*. Journal de Théorie des Nombres de Bordeaux, 23 (2011), 2, pp. 95 – 120.

[8] A. Couvreur, *The dual minimum distance of arbitrary dimensional algebraic-geometric codes*. Journal of Algebra, 350 (2012), 1, pp. 84 – 107.

[9] P. Ellia, C. Peskine: Groupes de points de $\mathbf{P}^2$: caractère et position uniforme. Lecture Notes in Mathematics, 1417, Springer Berlin (1990).

[10] O. Geil, *On codes from norm-trace curves*. Finite Fields and their Applications, 9 (2003), 351 – 371.

[11] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Clarendon Press, Oxford, 1979.

[12] C. Marcolla, M. Pellegrini, M. Sala *On the Hermitian curve, its intersections with some conics and their applications to affine-variety codes and Hermitian codes*. `http://arxiv.org/abs/1208.1627` (2012).

[13] R. J. McEliece, *A Public-Key Cryptosystem Based On Algebraic Coding Theory*. Jet Propulsion Laboratory, DSN Progress Report (1978), pp. 114 – 116.

[14] S. A. Stepanov, *Codes on Algebraic Curves*. Springer, 1999.

[15] H. Stichtenoth, *Algebraic function fields and codes*, Second Edition. Springer-Verlag, 2009.

[16] K. Yang, P. V. Kumar, *On the True Minimum Distance of Hermitian Codes*. Coding Theory and Algebraic Geometry (Stichtenoth and Tsfasman editors), Springer-Verlag, 1992.