Algebraic Geometry codes from Castle curves

C. Munuera[1], A. Sepúlveda[2] and F. Torres[2]

[1] Dept. of Applied Mathematics, University of Valladolid
Avda Salamanca SN, 47012 Valladolid, Castilla, Spain
[2] IMECC-UNICAMP, Cx.P. 6065, 13083-970, Campinas-SP, Brasil

Abstract. The quality of an algebraic geometry code depends on the curve from which the code has been defined. In this paper we consider codes obtained from *Castle curves*, namely those whose number of rational points attains Lewittes' bound for some rational point Q and the Weierstrass semigroup at Q is symmetric.

1 Introduction

Goppa constructed error correcting linear codes by using tools from Algebraic Geometry: a nonsingular, projective, geometrically irreducible, algebraic curve $\mathcal{X}$ of genus g defined over $\mathbf{F}_q$, the finite field with q elements, and two rational divisors D and G on $\mathcal{X}$; see [12, 13, 30]. These divisors are chosen in such a way that they have disjoint supports and D equals to a sum of pairwise distinct rational points, $D = P_1 + \ldots + P_n$. The *algebraic geometry* (or simply AG) code defined by the triple $(\mathcal{X}, D, G)$ is the q-ary linear space

$$C(\mathcal{X}, D, G) := \{ev(f) := (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\},$$

where $\mathcal{L}(G) = \{f \in \mathbf{F}_q(\mathcal{X})^* : G + \operatorname{div}(f) \succeq 0\} \cup \{0\}$ is the Riemann-Roch space associated to G. Soon after its introduction, AG codes become an important instrument in Coding Theory; for example, Tsfasman, Vlăduţ and Zink showed that the Gilbert-Varshamov bound can be improved by using them, [32]. Later, Pellikaan, Shen and van Wee [28] noticed that any arbitrary linear code is in fact an AG-code.

The study of AG codes, which is based on resources from algebraic geometry, is usually difficult. For example, it is well known that the parameters k and d (the dimension and the minimum distance) of $C(\mathcal{X}, D, G)$ verify

1. $k = \ell(G) - \ell(G - D)$, where $\ell(\cdot)$ denotes the dimension of the Riemann-Roch space $\mathcal{L}(\cdot)$; and
2. $d \geq d(\mathcal{X}, D, G) := n - \deg(G)$ (the *Goppa bound*).

However the exact determination of k and d is often not possible. If $2g - 2 < \deg(G) < n$ then the code $C(\mathcal{X}, D, G)$ is called *strongly* AG; in this case, the Riemann-Roch theorem gives $k = \deg(G) - 1 + g$. In other cases $\ell(G)$ and/or $\ell(G - D)$ are rather difficult to compute. On the other hand, if $\deg(G) \geq n$, the above bound on d does not give any information; nevertheless, Munuera [24] improved (2) by using another geometric invariant of the curve, see (1) below. For an integer $r \geq 1$, set

$$\gamma_r = \gamma_r(\mathcal{X}, q) := \min\{\deg(A) : A \text{ is a } \mathbf{F}_q\text{-rational divisor on } \mathcal{X} \text{ with } \ell(A) \geq r\}\,.$$

The number $\gamma(\mathcal{X}, q) := \gamma_2$ and the sequence $(\gamma_r)_{r\geq 1}$ are called respectively the *gonality* (resp. *gonality sequence*) of $\mathcal{X}$ over $\mathbf{F}_q$; cf. [34]. We have

$$d \geq n - \deg(G) + \gamma_{a+1}\,, \tag{1}$$

where a is the *abundance* of the code, namely $a := \ell(G - D)$; unfortunately both the genus and the gonality sequence of curves are usually very hard to compute.

Other lower bounds on the minimum distance on AG-codes have been developed by several authors; it seems that the more interesting of them is the *order* (or *Feng-Rao*) bound cf. [19], but it can be applied only to the duals of *one-point* AG codes; i.e., those AG codes for which G is a multiple of a rational point (although there is an analogous for "two-point" AG codes, see [5, 27]). We stress that, in general, the minimum distance of the dual $C^\perp$ of C does not give information on the minimum distance of C.

Let $C(\mathcal{X}, D, mQ)$ be a one-point AG code. The space $\mathcal{L}(G)$ is closely related to the Weierstrass semigroup at Q

$$S(Q) = \{0 = \rho_1(Q) < \rho_2(Q) < \ldots\} = \{-v_Q(f) : f \in \cup_{r=0}^{\infty}\mathcal{L}(rQ)\}$$

where v_Q is the valuation at Q. The element $\rho_2(Q)$ is usually called the *multiplicity* at (resp. of) Q (resp. $S(Q)$). As we mentioned above, $k = m - 1 + g$ for $2g - 2 < m < n$. In any case, if $\rho_i(Q) \leq m < \rho_{i+1}(Q)$ then $k = i$, so $S(Q)$ gives the dimension of $C(\mathcal{X}, D, mQ)$. Annalogously, the computation of the order bound of the code $C(\mathcal{X}, D, mQ)^\perp$ depends also on the semigroup $S(Q)$, see [19]. Therefore, the problems of computing the dimension and the minimum distance of (the duals of) one-point AG codes go through the problem of computing Weierstrass semigroups, which is not an easy problem at all.

Fortunately, we know some curves that combine the good properties of having a reasonable handling and giving one-point codes with excellent parameters (some times records in the tables [18]); such curves include the Deligne-Lusztig varieties of dimension one [6] (namely the projective line, the Hermitian curve, the Suzuki curve and the Ree curve), the generalized Hermitian curves [9], the Norm-Trace curves [10], etc. It is natural to ask if these curves share some common characteristic that motives all these good properties. At the first look, all the aforementioned curves have 'many' rational points; as a matter of fact, the Deligne-Lusztig curves are *optimal* in the sense that they have the maximum number of rational points that curves of its genus defined over the same ground field can have, see [15]. Several bounds on the number of rational points of curves are available in the literature, see e.g. [30]. For our purposes it is relevant the one given by Lewittes in [21]: if Q is a rational point of $\mathcal{X}$, then

$$\#\mathcal{X}(\mathbf{F}_q) \leq q\rho_2(Q) + 1\,. \tag{2}$$

This bound was proved by using the theory of Algebraic Function Fields of one variable (or see Theorem 1 below). It was recently improved by Geil and Matsumoto in [11].

In this paper we are interested in curves reaching equality in (2) and for which the semigroup $S(Q)$ is symmetric (in the sense that $\rho \in S(Q)$ if and only if $2g-1-\rho \notin S(Q)$). We shall refer to these curves as *Castle curves* (here the word 'castle' is used to honoring the place where this meeting is realized!). The aforementioned Norme-Trace curve, the generalized Hermitian curve and Deligne-Lusztig curves are all of them Castle curves. Also we shall show some common properties of one-point Goppa codes arising from Castle curves.

2 Castle curves

Let $\mathcal{X}$ be a curve over $\mathbf{F}_q$ with $(n+1)$ $\mathbf{F}_q$-rational points. Write $\mathcal{X}(\mathbf{F}_q) = \{Q, P_1, \ldots, P_n\}$. The following Theorem, due to Geil and Matsumoto [11, Thm. 1], gives an upper bound on $\#\mathcal{X}(\mathbf{F}_q)$. It generalizes a previous result of Lewittes [21, Thm. 1]. For the convenience of the reader we shall include a short proof of the Lewittes bound.

Theorem 1. *Let $S(Q)$ be the Weierstrasas semigroup at Q. Set $s + S(Q) := \{s+\rho : \rho \in S(Q)\}$ and $S^*(Q) := S(Q) \setminus \{0\}$. Then*

$$\#\mathcal{X}(\mathbf{F}_q) \leq \#(S(Q) \setminus (qS^*(Q) + S(Q))) + 1\,.$$

In particular $\#\mathcal{X}(\mathbf{F}_q) \leq q\rho_2(Q) + 1$.

Proof. Set $\rho_2 = \rho_2(Q)$ and let $f \in \mathcal{L}(\rho_2 Q)$ be a rational function such that $\rho_2 = -v_Q(f)$. Then $f^q \in \mathcal{L}(q\rho_2 Q)$ and $ev(f^q) = ev(f)$. Since ev is injective for $m = q\rho_2 < n = \#\mathcal{X}(\mathbf{F}_q) - 1$ and $f^q \neq f$, we have $q\rho_2 \geq n$, which is the Lewittes' bound. A similar reasonning leads to the Geil-Matsumoto bound.

Example 1. A rational curve is clearly a Castle curve. A hyperelliptic curve is a Castle curve if and only if it has just one hyperelliptic rational point and attains equality in the hyperelliptic bound $\#\{$rational nonhyperelliptic points$\} + 2\#\{$rational hyperelliptic points$\} \leq 2q+2$.

Example 2. (The Norm-Trace curve). Let us consider the curve defined over $\mathbf{F}_{q^r}$ by the affine equation

$$x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y$$

or equivalently by $N_{\mathbf{F}_{q^r}|\mathbf{F}_q}(x) = T_{\mathbf{F}_{q^r}|\mathbf{F}_q}(y)$, where the maps N and T are respectively the norm and trace from $\mathbf{F}_{q^r}$ to $\mathbf{F}_q$. This curve has $2^{2r-1}+1$ rational points and the Weierstrass semigroup at the unique pole Q of x is given by

$$S(Q) = \langle q^{r-1}, (q^r-1)/(q-1)\rangle\,.$$

Since every semigroup generated by two elements is symmetric, this is a Castle curve. Codes on these curves have been studied by Geil, [10].

Example 3. (Generalized Hermitian curves) For $r \geq 2$ let us consider the curve $\mathcal{X}_r$ over $\mathbf{F}_{q^r}$ defined by the afine equation

$$y^{q^{r-1}} + \ldots + y^q + y = x^{1+q} + \ldots + x^{q^{r-2}+q^{r-1}}$$

or equivalently by $s_{r,1}(y, y^q, \ldots, y^{q^{r-1}}) = s_{r,2}(x, x^q, \ldots, x^{q^{r-1}})$, where $s_{r,1}$ and $s_{r,2}$ are respectively the first and second symmetric polynomials in r variables. Note that $\mathcal{X}_2$ is the Hermitian curve. These curves were introduced by Garcia and Stichtenoth in [9] and they have $q^{2r-1}+1$ rational points. Let Q be the only pole of x. Then $S(Q) = \langle q^{r-1}, q^{r-1}+q^{r-2}, q^r+1\rangle$. This semigroup is telescopic (loc. cit.) and hence symmetric (see e.g. [22]). Therefore, $\mathcal{X}_r$ is a Castle curve. AG-codes based on these curves were studied by Bulygin [4] in the binary case and by Sepúlveda [29] in the general case.

To show that the Deligne-Lusztig curves are Castle curves, we shall point out an interesting interplay beetween Castle curves and Jacobian Varieties of curves (cf. [8]). Let $L(t)$ be the numerator of the Zeta function of $\mathcal{X}$ over $\mathbf{F}_q$. Set

$$h(t) := t^{2g} L(t^{-1}) .$$

Then $h(t)$ is monic of degree $2g$ and its independent term is nonzero. Moreover it is the characteristic polynomial of the Frobenius morphism $\Phi_{\mathcal{J}}$ on the Jacobian $\mathcal{J}$ of $\mathcal{X}$ (here we see $\Phi_{\mathcal{J}}$ as an endomorphism acting on the Tate module). Let

$$h(t) = \prod_j h_j^{r_j}(t)$$

be the factorization of $h(t)$ in $\mathbf{Z}[t]$. Since $\Phi_{\mathcal{J}}$ is semisimple and the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithfully (see [33, Thm. 2], [20, VI§3]), it follows that

$$\prod_j h_j(\Phi_{\mathcal{J}}) = 0 . \tag{3}$$

Let $\Phi : \mathcal{X} \to \mathcal{X}$ denote the Frobenius morphism on $\mathcal{X}$. Let $\pi : \mathcal{X} \to \mathcal{J}$ be the natural morphism given by $P \mapsto [P - Q]$, $Q \in \mathcal{X}(\mathbf{F}_q)$. Since $\pi \circ \Phi = \Phi_{\mathcal{J}} \circ \pi$, (3) implies the following equivalence of divisors on $\mathcal{X}$

$$\prod_j h_j(\Phi)(P) \sim mQ , \quad \text{with} \quad P \in \mathcal{X} \text{ and } m = \textstyle\prod_j h_j(1) . \tag{4}$$

This suggests to study the linear series $\mathcal{C} := |mQ|$. Remark that $\mathcal{C}$ is independent of the rational point Q, and $|m|$ belongs to the Weierstrass semigroup at any rational point. Let us write

$$\prod_j h_j(t) = t^U + \alpha_1 t^{U-1} + \ldots + \alpha_{U-1} t + \alpha_U .$$

Proposition 2. *Notation as above. Suppose that* (i) $\alpha_1 \geq 1$, (ii) $\alpha_{j+1} \geq \alpha_j$ *for* $j = 1, \ldots, U-1$, *and* (iii) $\#\mathcal{X}(\mathbf{F}_q) \geq q\alpha_U + 1$. *Then, for any* $P \in \mathcal{X}(\mathbf{F}_q)$ *we have*

1. $\#\mathcal{X}(\mathbf{F}_q) = q\rho_2(P) + 1$;
2. $\rho_2(P) = \alpha_U$;
3. $\gamma(\mathcal{X}, q) = \alpha_U$.

Proof. We first show that α_U is a generic non-gap (that is, a non-gap at a point which is not a Weierstrass point). In fact, by applying Φ_* to (4) we get

$$\alpha_U R \sim \Phi^{U+1}(R) + (\alpha_1 - 1)\Phi^U(R) + (\alpha_2 - \alpha_1)\Phi^{U-1}(R) + \ldots + (\alpha_U - \alpha_{U-1})\Phi(R).$$

By (i) and (ii), α_U is a non-gap at any point R such that $\phi^{U+1}(R) \neq R$, i.e., at any point which is not a fixed point of ϕ^{U+1}. Since the number of fixed points of this morphism is finite, the claim follows. By standard Weierstrass point theory, it holds that $\rho_2(P) \le \alpha_U$. Thus from (iii) and the Lewittes' bound (2), we have

$$q\alpha_U + 1 \le \#\mathcal{X}(\mathbf{F}_q) \le q\rho_2(P) + 1 \le q\alpha_U + 1$$

and (1), (2) follow. Now set $\gamma = \gamma(\mathcal{X}, q)$. Then, as $\gamma \le \alpha_U$ by definition of γ and $\#\mathcal{X}(\mathbf{F}_q) \le (q+1)\gamma$, (iii) holds as $\alpha_U \le q$.

The polynomials $h(t)$ for the Hermitian, $\mathcal{H}$, the Suzuki, $\mathcal{S}$, and the Ree curve, $\mathcal{R}$, are as follows see e.g. [15]:

(I) $h_{\mathcal{H}}(t) = (t + \ell)^{2g}$, where $q = \ell^2$ and $g = \ell(\ell - 1)/2$;
(II) $h_{\mathcal{S}}(t) = (t^2 + 2q_0 t + q)^g$, where $q = 2q_0^2 > 2$ and $g = q_0(q - 1)$;
(III) $h_{\mathcal{R}}(t) = (t^2 + q)^A (t^2 + 3q_0 t + q)^B$, where $q = 3q_0^2 > 3$, $A = q_0(q-1)(q + 3q_0 + 1)/2$, $B = q_0(q^2 - 1)$ and $g = 2A + 2B$.

By using these polynomials, and after some computations, we obtain the following data for any rational point P

Curve $\mathcal{X}$	Hermitian	Suzuki	Ree
$\rho_2(P) = \gamma(\mathcal{X}, q)$	ℓ	q	q^2
$\#\mathcal{X}(\mathbf{F}_q)$	$\ell^3 + 1$	$q^2 + 1$	$q^3 + 1$
m	$1 + \ell$	$1 + 2q_0 + q$	$(1 + q)(1 + 3q_0 + q))$
$\mathcal{C}$	$\lvert(1 + \ell)P\rvert$	$\lvert(1 + 2q_0 + q)P\rvert$	$\lvert(1 + q)(1 + 3q_0 + q)P\rvert$

.

In order to study the symmetry of the Weierstrass semigroups associated to these curves, let us first recall some facts from the Stöhr-Voloch theory, concerning to a geometric bound on the number of rational points of curves over finite fields [31]. Let x, y be rational functions such that

$$\operatorname{div}_\infty(x) = \rho_2(P)P \quad \text{and} \quad \operatorname{div}_\infty(y) = mP.$$

Consider the morphism $\phi = (1 : x : y) : \mathcal{X} \to \mathbf{P}^2(\overline{\mathbf{F}}_q)$. The linear series $\mathcal{E}$ associated to ϕ is given by the divisors $\{\operatorname{div}(\ell) + mP : \ell = a + bx + cy\,, (a : b : c) \in \mathbf{P}^2(\overline{\mathbf{F}}_q)\}$. Let $v = v_Q$ denote the valuation at $Q \in \mathcal{X}$. For all but finitely many points Q, there exist lines $\ell_0 = \ell_0(Q), \ell_1 = \ell_1(Q)$ and $\ell_2 = \ell_2(Q)$, such that $v(\ell_0) = 0$, $v(\ell_1) = 1$ and $v(\ell_2) = \epsilon_2 > 1$, this number being independent of Q [31, Thm. 1.5]. To deal with rational points, we consider the sequence

$0 = \nu_0 < \nu_1$ where $\nu_1 = 1$ or $\nu_1 = \epsilon_2 > 1$. According to [31, Sect. 2], the last case occurs if and only if $\Phi(Q) \in \mathrm{div}(\ell_2) + mP$ for all but finitely many points Q. In our case, the last condition holds true by (4). Thus it holds that

$$y^q - y = \frac{dy}{dx}(x^q - x)\,. \tag{5}$$

Proposition 3. *Let P be a rational point of the Hermitian, Suzuki or Ree curve. Then the Weierstrass semigroup at P is symmetric.*

Proof. For Hermitian and Suzuki curves the Weierstrass semigroups are known and the symmetry follows after some arithmetical computations (although alternative conceptual proofs can be done by using the above reasonning). We shall omit them. For the Ree curve it seems that the structure of $S(P)$ $(P \in \mathcal{X}(\mathbf{F}_q))$ is no available; nevertheless, we can still prove the symmetry property via the linear series $\mathcal{E}$. Here we have $\rho_2(P) = q^2$ and $m = (1+q)(1+3q_0+q)$. Let t be a local parameter at P. We will show that $v(\frac{dx}{dt}) = 2g-2$. Remark that $\#\mathcal{X}(\mathbf{F}_q) = q^3+1 = (q-3q_0+1)m$ and $2g-2 = (3q_0-2)m$. By applying the chain rule to (5), and since $\gcd(m,q) = 1$, we have

$$v(\frac{dx}{dt}) - qm = -m - 1 - q\rho_2(P) = -m - \#\mathcal{X}(\mathbf{F}_q)$$

or equivalently

$$v(\frac{dx}{dt}) = (q-1)m - m - (q-3q_0+1)m = (3q_0-2)m.$$

Example 4. (Castle maximal curves) Let $\mathcal{X}$ be a maximal curve of genus g over $\mathbf{F}_q$, $q = \ell^2$. Then $\mathcal{X}$ is a Castle curve if and only if there exists $Q \in \mathcal{X}(\mathbf{F}_q)$ such that $1+\ell^2+2g\ell = 1+\ell^2\rho_2(Q)$. Thus $\mathcal{X}$ must be a curve of genus $g = \ell(\rho_2(Q)-1)/2$. Apart from the Hermitian curve, such curves do exist. For example:

- The curve defined by $y^{\ell/2} + y^{\ell/2^2} + \ldots + y^2 + y = x^{\ell+1}$ with ℓ even; here the genus is $\ell(\ell-2)/4$ and $\rho_2(Q) = \ell/2$ where Q is the unique pole of x (see [2]);
- The curve defined by $y^{\ell/3} + y^{\ell/9} + \ldots + y^3 + y = ax^{\ell+1}$, where ℓ is a power of three, $a \in \mathbf{F}_q$ with $a^{\ell-1} = -1$; here the genus is $\ell(\ell-3)/6$ and $\rho_2(Q) = \ell/3$ at P the unique pole of x (see [3]).

Further examples can be find in [1].

The next Proposition colects some properties of Castle curves. Let us remember that by $\gamma_r = \gamma_r(\mathcal{X}, q)$ we denote the r-th gonality of $\mathcal{X}$ over $\mathbf{F}_q$.

Proposition 4. *Let $\mathcal{X}$ be a Castle curve with respect to a point $Q \in \mathcal{X}(\mathbf{F}_q)$, where the multiplicity at Q satisfy $\rho_2(Q) \leq q+1$. Then*

1. $\gamma_2 = \rho_2(Q)$;

2. $\gamma_i = \rho_i(Q)$ for $i \geq g - \gamma + 2$; that is,

$$\gamma_i = \rho_i(Q) = \begin{cases} i + g - 2 & \text{if } g - \gamma + 2 \leq i \leq g; \\ i + g - 1 & \text{if } i > g; \end{cases}$$

3. We have the equivalence of divisors on $\mathcal{X}$

$$\sum_{P \in \mathcal{X}(\mathbf{F}_q)} P \sim (q\rho_2(Q) + 1)Q\,.$$

Proof. Set $\rho_i := \rho_i(Q)$. (1) We have $\rho_2 - (\rho_2 - 1)/(q+1) \leq \gamma \leq \rho_2$ and the hypothesis on ρ_2 implies the result. (2) The statement about the gonalities of high order follows from the fact that both, the semigroup $S(Q)$ and the set of gonalities $GS(\mathcal{X}) = (\gamma_r)_{r \geq 1}$ verify the same symmetry property: for every integer a, it holds that $a \in S(Q)$ (resp. $a \in GS(\mathcal{X})$) if and only if $2g - 1 - a \notin S(Q)$ (resp. $2g-1-a \notin GS(\mathcal{X})$), cf. [26]. (3) As we have seen in the proof of Theorem 1, the code $C(\mathcal{X}, P_1 + \ldots + P_n, nQ)$ is abundant, hence $\ell(nQ - D) = 1$.

3 Codes on Castle curves

Let $\mathcal{X}$ be a curve of genus g over $\mathbf{F}_q$ with $(n+1)$ $\mathbf{F}_q$-rational points, $\mathcal{X}(\mathbf{F}_q) = \{Q, P_1 \ldots, P_n\}$. Consider the sequence of codes $(C_m)_{m \geq 1}$, where $C_m = C(\mathcal{X}, P_1 + \ldots + P_n, mQ)$, and let k_m, d_m be the dimension and the minimum distance of C_m, respectively. Let $S(Q) = \{0 = \rho_1 < \rho_2 < \ldots\}$ be the Weierstrass semigroup at Q. Define the function $\iota = \iota_Q : \mathbf{N}_0 \to \mathbf{N}$ by $\iota(m) = \max\{i : \rho_i \leq m\}$. Note that $\iota(m) = \ell(mQ)$. Let us remember that two $\mathbf{F}_q$-codes C_1 and C_2 of the same length n, are *isometric* if there is an n-uple $\mathbf{x}$ of nonzero elements in $\mathbf{F}_q$ such that $C_1 = \mathbf{x} * C_2 := \{\mathbf{x} * \mathbf{c} : \mathbf{c} \in C_2\}$, where $*$ stands for the coordinatewise product, see [25].

Proposition 5. *If $\mathcal{X}$ is a Castle curve with respect to Q, then*

1. *For $m < n$, the dimension of C_m is $k_m = \iota(m)$;*
2. *For $m \geq n$, C_m is an abundant code of abundance $\iota(m-n)$ and dimension $k_m = \iota(m) - \iota(m-n)$;*
3. *The dual of C_m is isometric to $C_{n+2g-2-m}$;*
4. *For $1 \leq m < n$, d_m reaches Goppa bound if and only if d_{n-m} does;*
5. *The minimum distance of C_n verifies $d_n \geq \rho_2(Q)$.*

Proof. (1) Since ev is injective over $\mathcal{L}(mQ)$ for $m < n$, the result follows from the fact that $\iota(m) = \ell(mQ)$. (2) We have already seen that C_n is abundant. Thus, in view of Proposition 4, if $m \geq n$ the abundance of C_m for $m \geq n$ is $\ell(mQ-D) = \ell(mQ-nQ) = \iota(m-n)$. The statement about the dimension follows trivially. (3) The dual of C_m is $C(D, D + W - mQ)$, where W is a differential form with simple poles and residue 1 at each P_i (see [25]). Now, in view of Proposition 4, $P_1 + \ldots + P_n \sim nQ$ and $(2g-2)Q \sim W$ (as the semigroup S is symmetric). Thus $P_1 + \ldots + P_n + W - mQ \sim (n + 2g - 2 - m)Q$ and codes C_m,

$C_{n+2g-2-m}$ are isometric, see [25]. (4) For $m < n$, C_m reaches equality in the Goppa bound if and only if then there exists $D', 0 \leq D' \leq D$ such that $mQ \sim D'$. Let $D'' = D - D'$. Thus $mQ \sim D - D'' \sim nQ - D''$, hence $(n-m)Q \sim D''$ and the code C_{n-m} also reaches equality in the Goppa bound. (5) Since $\gamma_2 = \rho_2$, this is just the improved Goppa bound on the minimum distance.

Remark. Since isometric codes have the same parameters, property 3 of the above Proposition allows us to use the order bound to estimate the minimum distance of these codes.

Example 5. Let us consider codes on the Suzuki curve $\mathcal{S}$ over $\mathbf{F}_8$. Here $g = 2(8-1) = 14$ and $\#\mathcal{S}(\mathbf{F}_8) = 8^2 + 1 = 65$.

Let $m = 50$. We have $k_{50} = 50 + 1 - 14 = 37$. The Goppa bound gives $d_{50} \geq 14$ and by applying the order bound we in fact obtain a $[64, 37, \geq 16]$ code over $\mathbf{F}_8$. Note that according to the Grassl tables [14], it is not known a $[64, 37]$ code over $\mathbf{F}_8$ having minimum distance $d > 16$.

Analogously, for $m = 73$ we obtain a $[64, 58, \geq 4]$ which have the best known parameters.

Finally, by applying now the bound stated in item 5 of the above proposition for $m = 63$, we get a $[64, 50, \geq 8]$ code, which is again a record. All these facts were unkown up the the moment (even if the codes are known longtime ago). By the way, note that the order bound on the minimum distance of this last code gives $d([64, 50]) \geq 6$. This shows that the order bound is not always better that the improved Goppa bound.

4 A worked example

In [7], Deolalikar constructed a subcover of the Garcia-Stichtenoth curve (see Example 3) in the particular case $r = 3$. In this section, we generalize his construction obtaining Castle curves.

Proposition 6. *Let $\mathcal{X}_r$ be a Garcia-Stichtenoth curve over $\mathbf{F}_{q^r}$ and let $b \in \mathbf{F}_{q^r}^*$ such that $T_{\mathbf{F}_{q^r}|\mathbf{F}_q}(b) = 0$, being T the trace function. Then for $j = 1, \ldots, r-2$, the curve $\mathcal{X}_r^j$ defined over $\mathbf{F}_{q^r}$ by the affine aquation*

$$s_{r,2}(x, x^q, \ldots, x^{q^{r-1}}) =$$

$$y_j^{q^j} - \left(\frac{1}{b^{q^j - q^{j-1}}} + \cdots + \frac{1}{b^{q^j-1}}\right) y_j^{q^{j-1}} - \cdots - \left(\frac{1}{b^{q^2-q}} + \frac{1}{b^{q^2-1}}\right) y_j^q - \frac{1}{b^{q-1}} y_j,$$

where $s_{r,2}$ is the second symmetric polynomial, is covered by $\mathcal{X}_r$.

Proof. A covering map $c : \mathcal{X}_r \to \mathcal{X}_r^j$ is given by $c(x, y) =$

$$(x, y^{q^{r-j-1}} + (b^{q^{r-1}-1} + \cdots + b^{q^{r-j}-1} + 1) y^{q^{r-j-2}} + \cdots + (b^{q^{r-1}-1} + \cdots + b^{q^2-1} + 1) y)$$

Let $Q^j \in \mathcal{X}_r^j$ be the only pole of x.

Proposition 7. *The curve $\mathcal{X}_r^j$, $j = 1, \dots, r-2$, verifies the following properties.*

1. *Q^j is totally ramified.*
2. *The genus of $\mathcal{X}_r^j$ is $g = (q^j - 1)q^{r-1}/2$.*
3. *The number of rational points of $\mathcal{X}_r^j$ is $q^{r+j} + 1$.*
4. *The Weierstrass semigroup at $Q^j \in \mathcal{X}_r^j$ is $S(Q^j) = \langle q^j, q^{r-1} + 1 \rangle$.*

Proof. (1) $Q \in \mathcal{X}_r$ is totally ramified. (2) and (3) follow from [7, Thm. 3.5]. (4) It is clear that $-v_Q(x) = q^j$. Let us consider the rational function $z := x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^{r-2}} - y_j^{q^{j-1}}$. Then $z^q = x^{q+q^2} + x^{q+q^3} + \cdots + x^{q^{r-2}+q^{r-1}} - y^{q^j}$ and, by using the defining equation of $\mathcal{X}_r^j$, we obtain $-v_Q(z) = q^{r-1} + 1$. Now, since the genus of $\langle q^j, q^{r-1} + 1 \rangle$ is g, we get the equality.

In particular, $\mathcal{X}_r^j$ is a Castle curve. Other consequence of the above Proposition is the following.

Proposition 8. *Let $z = x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^{r-2}} - y_j^{q^{j-1}}$. Then $\mathcal{L}(mQ^j) = \langle \{x^i z^k : i \cdot q^j + k \cdot (q^{r-1} + 1) \leq m, 0 \leq i$ and $0 \leq k < q^j\} \rangle$, for all $m \geq 0$.*

For $m = 0, 1, 2, \dots$, we can consider the codes $\mathcal{C}_{r,m}^j := C(\mathcal{X}_r^j, D, mQ_\infty^j)$, where D is the sum of all rational points of $\mathcal{X}_r^j$ except Q^j. The length of these codes is $n = q^{r+j}$. The dimension and minimum distance can be estimated as shown in Proposition 5.

Example 6. For $q = 2$ and $r = 3$, the curve $\mathcal{X}_3^1$ is hiperelliptic of genus 2 over $\mathbf{F}_8$. It has 17 rational points. By using the order bound, we show that for $m = 13$ we get a $[16, 12, 4]$ code over $\mathbf{F}_8$. Note that, according to the main conjecture on MDS codes, there is no $[16, 12, > 4]$ code over $\mathbf{F}_8$.

When $q = 2$ and $j = 1$, then $\mathcal{X}_r^j$ is a hyperelliptic curve and Q_∞^j a hyperelliptic point. Let us consider the code $\mathcal{C}_{r,m}^1 = C(\mathcal{X}_r^1, D, mQ_\infty^1)$. Assume $m < n$. If m is even then there exists a divisor $D' \leq D$ such that $D' \sim sQ$ (simply write D' as a sum of $s/2$ pairs of conjugated points). Then the minimum distance of $\mathcal{C}_{r,m}^1$ is $d = n - m$. Thus, for m odd we have $n - s \leq d(\mathcal{C}_{r,m}^1) \leq n - m + 1$. In particular, for $m \leq 2^{r-1}$, if m even then $\mathcal{C}_{r,m}^1$ has dimension $(m/2) + 1$ and if m is odd then $\mathcal{C}_{r,m}^1 = \mathcal{C}_{r,m-1}^1$. Since this code does not meet the Goppa bound, according to Proposition 5, item (4), the same happens for $m' = n - m$. We conclude that for m odd, $n - 2^{r-1} \leq m < n$, the code $\mathcal{C}_{r,m}^1$ has dimension $m + 1 - 2^{r-2}$ and minimum distance $n - m + 1$.

References

1. M. Abdón and A. Garcia: On a characterization of certain maximal curves. *Finite Fields Appl.* **10** (2004) 133–158.
2. M. Abdón and F. Torres: On maximal curves in characteristic two. Manuscripta Math. **99** (1999) 39–53.
3. M. Abdón and F. Torres: On $\mathbf{F}_{q^2}$-maximal curves of genus $q(q-3)/6$. Beitr. Algebra Geom. **46** (2005) 241–260.

4. S.V. Bulygin: Generalized Hermitian codes over $GF(2^r)$. IEEE Trans. Inform. Theory **52** (2006) 4664–4669.
5. C. Carvalho, C. Munuera, E. Silva and F. Torres: Near orders and codes. IEEE Trans. Inform. Theory **53** (2009) 1919–1924.
6. P. Deligne and G. Lusztig: Representations of reductive groups over finite fields. Ann. of Math. **103** (1976) 103–161.
7. V. Deolalikar: Determining irreducibility and ramification groups for an additive extension of the rational function fields. J. Number Theory **97** (2002) 269–286.
8. R. Fuhrmann and F. Torres: On Weierstrass points and optimal curves. Supplemento ai Rendiconti del Circolo Matematico di Palermo **51** (1998) 25–46.
9. A. Garcia and H. Stichtenoth: A class of polynomials over finite fields. Finite Fields Their Applic. **5** (1999) 424–435.
10. O. Geil: On codes from norm-trace curves. Finite fields and their Applications **9** (2003) 351–371.
11. O. Geil and H. Matsumoto: Bounding the number of rational places using Weierstrass semigroups. preprint, 2007.
12. V.D. Goppa: Geometry and Codes. Kluwer (Mathematics and its applications 24), Dordrecht, 1991.
13. V.D. Goppa: Codes associated with divisors. Problems Inform. Transmission **13** (1977) 22–26.
14. M. Grassl: Bounds on the minimum distance of linear codes. available online at http://www.codetables.de.
15. J.P. Hansen: Deligne-Lusztig varieties and group codes. Lect. Notes Math. **1518** (1992) 63–81.
16. J.P Hansen and J.P. Pedersen: Automorphism group of Ree type, Deligne-Lusztig curves and function fields. J. Reine Angew. Math. **440** (1993) 99–109.
17. J.P. Hansen and H. Stichtenoth: Group codes on certain algebraic curves with many rational points. Applicable Algebra Eng. Comm. Comput. **1** (1990) 67–77.
18. H.W. Henn: Funktionenkörper mit grosser Automorphismgruppen. J. Reine Angew Math. **302** (1978) 96–115.
19. T. Høholdt, J.H. van Lint and R. Pellikaan: Algebraic-Geometry codes. In V.S. Pless and W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998
20. S. Lang: Abelian Varieties. Interscience Pub., New York, 1959.
21. J. Lewittes: “Places of degree one in function fields over finite fields. J. Pure Appl. Algebra **69** (1990) 177–183.
22. C. Kirfel and R. Pellikaan: The minimum distance of codes in an array coming from telescopic semigroups. IEEE Trans. Inform. Theory **41** (1995) 1720–1732.
23. G. Matthews: Codes from the Suzuki function field. IEEE Trans. Inform. Theory **50** (2004) 3298–3302.
24. C. Munuera: On the generalized Hamming weights of geometric Goppa codes. IEEE Trans. Inform. Theory **40**(6) (1994) 2092–2099.
25. C. Munuera and R. Pellikaan: Equality of geometric Goppa codes and equivalence of divisors. J. Pure Appl. Algebra **90** (1993) 229–252.
26. C. Munuera and F. Torres: Bounding the trellis state complexity of algebraic geometric codes. Applicable Algebra Eng. Comm. Computing **15** (2004) 81–100.
27. C. Munuera and F. Torres: The structure of algebras admitting well agreeing near weights. J. Pure Appl. Algebra **212** (2007) 910–918.
28. R. Pellikaan, B.Z. Shen and G.J.M. van Wee: Which Linear Codes are Algebraic-Geometric. IEEE Trans. Inform. Theory **37** (1991) 583–602.

29. A. Sepúlveda: Generalized Hermitian codes over $GF(q^r)$. preprint, 2007.
30. H. Stichtenoth: Algebraic Funtion Fields and Codes. Springer Verlag, New York-Berlin, 1993.
31. K.O. Stöhr and J.F. Voloch: Weierstrass points and curves over finite fields. Proc. London Math. Soc. (1986) 1–19.
32. M.A. Tsfasman, S. Vlăduţ and T. Zink: Modular curves, Shimura curves and Goppa codes better that Varshamov-Gilbert bound. Math. Nachr. **109** (1982) 21–28.
33. J. Tate: Endomorphisms of abelian varieties over finite fields. Inventiones Math. **2** (1966) 134–144.
34. K. Yang, P.V. Kumar and H. Stichtenoth: On the weight hierarchy of geometric Goppa codes. IEEE Trans. Inform. Theory **40** (1994) 913–920.

This article was processed using the LaTeX macro package with LLNCS style