CASTLE CURVES AND CODES

XVIII LATIN-AMERICAN ALGEBRA COLLOQUIUM
SÃO PEDRO, SÃO PAULO, SP, 3-8, AUGUST, 2009

FERNANDO TORRES

(WITH CARLOS MUNUERA AND ALONSO SEPÚLVEDA)

INSTITUTE OF MATHEMATICS, STATISTIC AND COMPUTER SCIENCES
UNIVERSITY OF CAMPINAS, P.O. BOX 6065, 13083-970, CAMPINAS, SP, BRAZIL
FTORRES AT IME.UNICAMP.BR

Abstract. The quality of an Algebraic Geometry Goppa code depends on the curve from which the code has been defined. In this talk we introduce two types of curves of interest for such codes: the so-called Castle and weak Castle curves. We subsume the main properties of codes arising from these curves.

References:

(I) "Algebraic Curves over a Finite Field", J.W.P. Hirschfeld, G. Korchmáros and F. Torres, Princenton University Press, USA, 2008.
(II) "Algebraic geometric codes: basic notions", M. Tsfasman, S. Vladut and D. Nogin, American Mathematical Society, Vol. **139**, USA, 2007.
(III) "Many Rational Points, Coding Theory and Algebraic Geometry", N.E. Hurt, Kluwer Academic Publishers, Dordrecht, Boston, London, 2003.
(IV) "Function Fields and Codes", H. Stichtenoth, Springer, Berlin 1993.
(V) *Castle curves and codes*, C. Munuera, A Sepúlveda and F. Torres, preprint, 2009.
(VI) *Algebraic Geometry codes from Castle curves*, Coding Theory and Applications, Second International Castle Meeting, ICMCTA 2008. (A. Barbero Ed.), C. Munuera, A. Sepúlveda and F. Torres, 117–127, Lecture Notes Comput. Sci. **5228**, Springer-Verlag, Berlin Heidelberg 2008.

Main Problem. Find curves that combine the good properties of having a reasonably handling and giving Algebraic Geometry Goppa codes with excellent parameters.

2000 Math. Subj. Class.: Primary 05B, Secondary 14H.

Keywords: finite field, curves with many points, one-point geometrical Goppa codes, Weierstrass semigroups, numerical semigroups.

Here the word 'Castle' is used to honoring "El Castillo de la Mota, Medina del Campo"; see Reference (VI) above.

July 31, 2009.

Throughout, by a curve we mean a 'projective, non-singular geometrically irreducible algebraic curve '.

Set up.

- Let $\mathbb{F}_\ell$ be the finite field of order ℓ. Let $\mathcal{X}$ be a curve of genus g defined over $\mathbb{F}_\ell$;
- Let G be a $\mathbb{F}_\ell$-divisor on $\mathcal{X}$ and $P_1, \ldots, P_n$ be pairwise distints $\mathbb{F}_\ell$-rational points in $\mathcal{X}$ such that $P_i \notin \mathrm{Supp}(G)$ for all i. Thus

$$ev(f) := (f(P_1), \ldots, (f_n)) \in {\mathbb{F}_\ell}^n$$

for all f in the Riemann-Roch space of G, namely

$$\mathcal{L}(G) = \{\mathbb{F}_\ell\text{-rational functions } f \neq 0 : G + \mathrm{div}(f) \succeq 0\} \cup \{0\}\,.$$

Recall the 'Riemann-Roch theorem': let g and K be, respectively, the genus and a canonical divisor of $\mathcal{X}$; then

$$\ell(G) = \deg(G) + 1 - g + \ell(K - G)\,,$$

where $\ell(\cdot)$ denotes the $\mathbb{F}_\ell$-dimension of $\mathcal{L}(\cdot)$.

Definition 1. The $\mathbb{F}_\ell$-vector space

$$E = E_{\mathcal{X},D,G} := \{ev(f) : f \in \mathcal{L}(G)\} \subseteq {\mathbb{F}_\ell}^n$$

is the *Algebraic Geometry Goppa* code (AGG-code for short) associated to the triple $(\mathcal{X}, G, D)$, where we set $D := P_1 + \ldots + P_n$.

A very basic problem in Coding Theory is regarding the parameteres: lenght, dimension and minimun distance. For AGG-codes, the lenght equals n. Let k and d denote, respectively, its ($\mathbb{F}_\ell$) dimension and minimum distance d. Here

$$d := \min\{w(ev(f)) : ev(f) \neq (0, \ldots, 0) \quad \text{where } w(e(f)) = \#\{i : f(P_i) \neq 0\}\,.$$

By the very definiton of E, it follwos that:

- $k = \ell(G) - a$, where $a = \ell(G - D)$ is the "abundance of the code";
- $d \geq d_{GOPPA} := n - \deg(G)$.

Computing k and d is often a hard problem. Let us consider the special case:

$$2g - 2 < \deg(G) < n\,. \tag{1}$$

Thus $a = 0$, $\ell(K - G) = 0$ and Riemann-Roch computes k: we have $k = \deg(G) + 1 - g$. However, the invariant g is often difficult to compute. If $\deg(G) \geq n$, we can improve the upper bound on d (Munuera). For $r \geq 1$ an integer, set (Kummar, Stichtenoth, Yang)

$$\gamma_r = \gamma_r(\mathcal{X}, r) := \min\{\deg(A) : A \text{ is a } \mathbb{F}_\ell\text{-divisor with } \ell(A) \geq r\}\,.$$

Definition 2. $(\gamma_r)_{r \geq 1}$ is *the $\mathbb{F}_\ell$-gonality sequence* of $\mathcal{X}$; γ_2 is *the $\mathbb{F}_\ell$-gonality.*

Thus if $\deg(G) \geq n$, then

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

One again, both the genus and the gonality sequence of curves, are often very hard to compute.

Other lower bounds concerning the minimum distance have been development by several authors; it seems that the more interesting is the so called *order* or *Feng-Rao* bound; such a number is associate to any (numerical) semigroup.

In the case of an 'one-point' AGG-codes E (i.e., when G is the multiple of a single $\mathbb{F}_\ell$-rational point), the order bound $d_{ORD}(E)$ can be applied only to lower bound the minimum distance $d^\perp$ of the dual of E (Feng, Rao, Høholdt, van Lint, Pellikaan). We stress that, in general, $d^\perp$ does not give information on d.

Let E_m denotes the AGG-code associated to $(\mathcal{X}, D, G_m)$, $G_m = mQ$, and k_m its dimension. Let $C_m = E_m^\perp$. E_m. To deal with $\mathcal{L}(G_i)$, we are led to consider the Weierstrass semigroup at Q

$$S(Q) = \{0 = \rho_1(Q) < \rho_2(Q) < \ldots\} = \{-v_Q(f) : f \in \cup_r^\infty \mathcal{L}(rQ)\}\,, \tag{2}$$

where v_Q is the evaluation at Q. As we mention above, under the restriction (1) we only obtain $k_m = m - g + 1$. Hovewer from (2) we compute k_m (for all m) as follows:

$$\text{If } \rho_\iota(Q) \leq m < \rho_{\iota+1}(Q)\ ,\quad \text{then } k_m = \iota\,. \tag{3}$$

Now let C_m is associated to $(\mathcal{X}, D, D + K - G_m)$ with K an appropiate canonical divisor on $\mathcal{X}$. We compute $d_{ORD}(E_m)$ by taking into consideration the Weierstrass semigroup $S(Q)$. It holds that

$$d^\perp(E_m) \geq d_{ORD}(E_m) \geq d_{GOPPA}(E_m\ \perp) = \ . \tag{4}$$

A very interesting fact is that the computation of the order bound does no depend on the divisor D neither on the selection of the basis of $\mathcal{L}(E_m)$. Thus we consider this computation on an arbitrary semigroup H. Let

$$H = \{0 = \rho_1 < \rho_2 < \ldots\}\,.$$

For $\ell \geq 1$ an integer, consider the sets

$$A(\ell) = A(\rho_\ell) := \{(s,t) \in \mathbb{N}^2 : \rho_s + \rho_t = \rho_\ell\}$$

and their cardinals

$$\nu_\ell = \#A(\ell)\,.$$

Then the order bound for H at $m \in \mathbb{N}$ is defined by

$$d_{ORD,H}(m) := \min\{\nu_\ell : \ell \geq m\}\,;$$

in the case of codes, $d_{ORD}(E_m)$ is defined throught $S(Q)$. In general it is not easy to compute orders of semigroups. Campillo, Farrán, Munuera, Bras-Amorós, Oneto, Tamone,

Oliveira, Villanueva, ... worked out several types of semigroups: in fact in many cases they obtained a closed formula for the order.

However, in my opinion a harder problem arises (which is open in characteristic zero): It is an arbitrary semigroup realized as a Weierstrass semigroup? Shall we apply the usual techniques in characteristic zero to positive characteristic?

It is worth to mention that, e.g., Bras-Amorós, Oneto, Tamone, ... compute the order bound of semigroups generated by less than 5 elements or semigroups ordinaries; Munuera, Oliveira and Villanueva examples have small weight: thus by reduction module p all of them are Weiertrass.

Remark 1. Carvalho, Munuera, Silva,... obtained a formula of 'order type' (as in the case of one variable) for codes with $\#\mathrm{Supp}(G) > 1$.

We conclude the following:

- If (1) holds, computing the parameters of an AGG-code would be very restricted by the geometry of the curve;
- If we even consider one-point AGG-codes we have the restiction of computing Weierstrass semigroups or the combinatorial computation of the orders.

In this talk we consider curves, a particular solution to the main problem formulated above, that combine the properties of having a reasonable handling and giving one-point AGG-codes with exellent parameters; some time they are record in the known tables.

From now we only consider one-point AGG-codes, says $E = E_{\mathcal{X},D,G}$ with

$$D = P_1 + \ldots + P_n, \ , \quad \text{and} \quad G = mQ\,. \tag{5}$$

Let n, k, d be the parameters of E. By a pointed curve $(\mathcal{X}, Q)$ defined over $\mathbb{F}_\ell$, we mean a curve $\mathcal{X}$ over $\mathbb{F}_\ell$ together with a $\mathbb{F}_\ell$-rational point $Q \in \mathcal{X}$. We let $(X : Y : Z)$ be the projectives coordenates of $\mathbb{P}^2$ and $x = X/Z$ and $y = Y/Z$ the affine coordentes of $\mathbb{A}^2$. We let $N := \#\mathcal{X}(\mathbb{F}_\ell)$ and thus $n + 1 \leq N$.

Example 1. (Hermitian curve over $\mathbb{F}_{q^2}$), $\ell = q^2$. It is well known that $N = q^3 + 1$. Let Q the unique point in $Z = 0$. The usual "Hermitian " codes are defined on this curve with $n = q^3$. Let $\mathcal{H} : y^q + y = x^{q+1}$ be the affine equation of the curve. We notice the following properties:

(I) $H(Q) = \langle q, q+1 \rangle$ and hence $(2g-2)Q$ is canonical;
(II) The morphism $x : \mathcal{H} \to \mathbb{P}^1$ is unramified of order q except at Q;
(III) $x^{-1}(\alpha) \subseteq \mathcal{X}(\mathbb{F}_{q^2})$ for all $\ell \in \mathbb{F}_{q^2}$;
(IV) $\#x^{-1}(\alpha) = q$ for all $\ell \in \mathbb{F}_{q^2}$.

Let $x^{-1}(\alpha) = R_1^\alpha + \ldots + R_q^\alpha$. Then

$$D = \mathrm{div}(x^q - x) \sim nQ\,.$$

with $n = N-1 = qs$. For the one-point AGG-code E_m over $\mathcal{H}$, D as above and $G_m = mQ$ we obtain:

(1) $E_m^\perp$ is isometric to $E_{n+2g-2-mQ}$;
(2) We already noticed that k_m follows from $H(Q)$; observe that $a = \ell(mQ - D) = \ell(m-n)Q$.
(3) (the most important matter) The distance $d_m \geq n - m + \gamma_{a+1}$ and moreover the gonality sequence equals $H(Q)$.

Example 2. ($\ell = q^2$) Let $\mathcal{X}$ be the curve over $\mathbb{F}_{q^2}$ defined by $y^q + y = x^{(q+1)/2}$. Let Q be the unique commom pole of x and y (Notice that the curve is $\mathbb{F}_{q^2}$-maximal of genus $(q-1)^2/2$.) Then:

(1) Property (I) above is true as $H(Q) = \langle (q+1)/2, q, q+1\rangle$ is symmetric since x is unramified over any $\alpha \in \mathbb{P}^1(\mathbb{F}_\ell)$, $\alpha \neq \infty$;
(2) Property (II) reads: the morphism $y : \mathcal{X} \to \mathbb{P}^1$, of order $(q+1)/2$, is unramified except at the points over the roots of $Y^q + Y = 0$;
(3) Property (III) becomes: $y^{-1}(\alpha) \subseteq \mathcal{X}(\mathbb{F}_{q^2})$ for all $\alpha \in \mathbb{F}_{q^2}$ such that $\alpha^q + \alpha = 0$;
(4) Property (IV) also holds for $\alpha \in \mathbb{F}_{q^2}$ such that $\alpha^q + \alpha = 0$.

Here we take D as follows. For each $\alpha_i \in \mathbb{F}_{q^2}$ with $\alpha_i^q + \alpha_i \neq 0$, write

$$\mathrm{div}(y - \alpha_i) = \sum_{j=1}^{(q+1)/2} P_j^i - \frac{q+1}{2}Q$$

so that

$$D := \sum_{i=1}^{N-q}\sum_{j=1}^{(q+1)/2} P_j^i \sim (\frac{q+1}{2}(N-q)Q\,,$$

where $N - q = (q^2 + q2g) - q = (q^3 - q)(q+1)/4$. Thus we obtain a code on $\mathcal{X}$ satisfying properties of type (I)-(IV), (1)-(3) in the previous example.

Remark 2. One also can consider less points than n in the above examples.

Definition 3. A pointed curve $(\mathcal{X}, Q)$ over $\mathbb{F}_\ell$ is called *weak Castle* if

(1) the Weierstrass semigroup $H(Q)$ at Q is symmetric;
(2) there exists a morphism $\phi : \mathcal{X} \to \mathbb{P}^1 := \bar{\mathbb{F}}_\ell \cup \{\infty\}$ with $\mathrm{div}_\infty(\phi) = hQ$, and elements $\alpha_1, \ldots, \alpha_a \in \mathbb{F}_\ell$ such that for all $i = 1, \ldots, a$, we have $\phi^{-1}(\alpha_i) \subseteq \mathcal{X}(\mathbb{F}_\ell)$ and $\#\phi^{-1}(\alpha_i) = h$.

In the above situation note that $h \in H(Q)$. Furthermore, since ϕ is unramified over each α_i, if we write $\phi^{-1}(\alpha_i) = \{P_1^i, \ldots, P_h^i\}$, then $\mathrm{div}(\phi - \alpha_i) = \sum_{j=1}^{h} P_j^i - hQ$. We set $z := \prod_{i=1}^{a}(\phi - \alpha_i)$ and

$$D = D_{\mathcal{X},\phi} := \sum_{i=1}^{a}\sum_{j=1}^{h} P_j^i \,.$$

Hence D is an effective rational divisor of degree ah with $D \sim ahQ$ since $\mathrm{div}(z) = D - ahQ$.

Now let us show an interesting family of weak Castle curves that can be defined in simple terms. This family is closely related to a bound on the number of rational points of $\mathcal{X}$.

Theorem 1. *(Lewittes, Geil, Matsumoto) Let $\mathcal{X}$ be a curve over $\mathbb{F}_\ell$ and let Q be a rational point on $\mathcal{X}$. Let $H = H(Q)$ be the Weierstrass semigroup at Q and $\rho_2 = \rho_2(Q)$ the first positive element of H. Then*

$$\#\mathcal{X}(\mathbb{F}_\ell) - 1 \leq \#(H \setminus (\ell H^* + H)) \leq \ell\rho_2(Q)\,.$$

The inequality $\#\mathcal{X}(\mathbb{F}_\ell) - 1 \leq \ell\rho_2$ above was already known by Lewittes. Having bounds on $\mathcal{X}(\mathbb{F}_\ell)$ - which in ganeral is a challenging matter - it is related to the relative parameters R and δ of an AGG-code, $C_{\mathcal{X},D,G}$, with $\deg(G) < 2g - 2$: Riemann-Roch gives

$$R + \delta \geq 1 - (g-1)/n\,;$$

thus would of interest that $\#\mathcal{X}(\mathbb{F}_\ell) >> g$.

The family of weak Castle curves we refer is the following.

Definition 4. A pointed curve $(\mathcal{X}, Q)$ over $\mathbb{F}_\ell$ is called *Castle* if $H(Q)$ is symmetric and equality holds in the Lewittes-Geil-Matsumoto bound; i.e, $\#\mathcal{X}(\mathbb{F}_\ell) = \ell\rho_2(Q) + 1$, where $\rho_2(Q)$ is the first positive element of $H(Q)$.

They are indeed weak Castle as the following Proposition shows.

Proposition 1. *Every Castle curve $(\mathcal{X}, Q)$ is weak Castle.*

Proof. Takes ϕ such that $\mathrm{div}_\infty(\phi) = \rho_2 Q$. □

Examples of Castle and weak Castle curves.

Example 3. Rational curves are clearly Castle. Then Reed-Solomon codes are Castle codes.

Example 4. Let $\mathcal{X}$ be a hyperelliptic curve of genus g over $\mathbb{F}_q$ having a hyperelliptic rational point Q. A plane model of $\mathcal{X}$ is given by the equation $y^2 + r(x)y = p(x)$, where $p(x)$ and $r(x)$ are polynomials of degrees $\deg p(x) = 2g + 1$ and $\deg r(x) \leq g$. Then the morphism $\phi = x : \mathcal{X} \to \mathbb{P}^1$ makes $(\mathcal{X}, Q)$ a weak Castle curve. $D_{\mathcal{X},\phi}$ is the sum of all non-hyperelliptic rational points on $\mathcal{X}$. Thus, it is a Castle curve iff Q is the only hyperelliptic rational point on $\mathcal{X}$ and $a = q$.

Example 5. (Norm-Trace curves)It is defined over $\mathbf{F}_q = \mathbf{F}_{\ell^r}$ by the affine equation

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

or $N(y) = T(x)$, where N and T are respectively the norm and trace from $\mathbf{F}_q$ to $\mathbf{F}_\ell$. This curve has $\ell^{2r-1}+1$ rational points and the Weierstrass semigroup at the unique pole Q of y is $H(Q) = \langle \ell^{r-1}, (\ell^r-1)/(\ell-1)\rangle$. Then it is Castle. Codes from this curve have been studied by Geil.

In subsequent examples we shall introduce new types of norm-trace curves.

Example 6. (Hermitian and Generalized Hermitian curves) Let $q = \ell^r$ with $r \geq 2$ and consider the curve $\mathcal{X}$ over $\mathbb{F}_q$ defined by the affine equation

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

or equivalently, by $s_{r,1}(y, y^\ell, \ldots, y^{\ell^{r-1}}) = s_{r,2}(x, x^\ell, \ldots, x^{\ell^{r-1}})$, where $s_{r,1}$ and $s_{r,2}$ are respectively the first and second symmetric polynomials in r variables. This curve was introduced by Garcia and Stichtenoth. It has genus $g = (\ell^{r-1}(\ell^{r-1}-1)/2$ and $\ell^{2r-1}+1$ rational points. Let Q be the only pole of x. Then $H(Q) = \langle \ell^{r-1}, \ell^{r-1}+\ell^{r-2}, \ell^r+1\rangle$. This semigroup is telescopic (loc. cit.) and hence symmetric (Kirfel, Pellikaan). Therefore $\mathcal{X}$ is a Castle curve. Codes arising from these curves have been studied by Bulygin in the binary case and by Munuera, Sepúlveda, ... in the general case. Note that when $r = 2$, then $\mathcal{X}$ is the Hermitian curve.

Example 7. (Another generalization of Hermitian curves) Let q be a square, $q = \ell^{2r}$, and $m \geq 2$ be an integer such that $m|(\ell^r+1)$. Let $\mathcal{X}$ be the non-singular model over $\mathbb{F}_q$ of the plane curve given by the equation

$$y^m = p(x) := x + x^\ell + \ldots + x^{\ell^{2r-1}} .$$

Since $\gcd(m, \ell) = 1$, there is just one point Q over $x = \infty$. For $r = 1$ and $m = \ell+1$ we obtain again the Hermitian curve. (The case $r = 1$ and other values of m were treated by Yang, Kummar and Stichtenoth) . Let us show some properties of $\mathcal{X}$:

(1) The genus of $\mathcal{X}$ is $g = (m-1)(\ell^{2r-1}-1)/2$. This follows directly from the Riemann-Hurwitz genus formula.
(2) The functions x and y have order m and ℓ^{2r-1}, respectively, at Q. Then $H(Q) \supseteq \langle m, \ell^{2r-1}\rangle$. Taking into account the genus of $\mathcal{X}$ we conclude the equality. Thus $H(Q)$ is generated by two elements and hence it is symmetric.
(3) The pointed curve $(\mathcal{X}, Q)$ is weak Castle. Furthermore $\deg(D_{\mathcal{X},\phi}) = m(\ell-1)\ell^{2r-1}$. To see this, let $\phi = x$, $h = m$ and $a = \ell^{2r} - \ell^{2r-1}$. For $\alpha \in \mathbb{F}_q$ with $p(\alpha) \neq 0$, we shall show that ϕ is unramified over α and that $\phi^{-1}(\alpha) \subseteq \mathcal{X}(\mathbb{F}_q)$. The first condition is clear as $\gcd(m, \ell) = 1$. For the later we have to prove that $y^m = p(\alpha)$ has m solutions in $\mathbb{F}_q$. Since $p(\alpha)$ is the trace of α from $\mathbb{F}_q$ to $\mathbb{F}_\ell$, we conclude that

$$y^m = p(\alpha) = p(\alpha)^{\ell m} .$$

From the hypothesis $m|(\ell^r+1)$ we have $y^{\ell^r+1} = y^{\ell(\ell^r+1)}$. Then by induction $y^{\ell^r+1} = y^{\ell^r(\ell^r+1)}$ and the result follows.

(4) Note that we can also prove the above result by considering $\phi = y$ and $h = \ell^{2r-1}$. The weak Castle property is equivalent to study $\mathbb{F}_q$-rational roots of $\beta^m = p(x)$ for a fixed $\beta \in \mathbb{F}_q^*$. We have that $x \in \mathbb{F}_q$ iff $p(x) = p(x^\ell)$ iff $\beta^{(\ell-1)m} = 1$. A subgroup of $\mathbb{F}_q^*$ order $(\ell-1)m$ exists as $m \mid (\ell^r+1)$. Thus by taking $a = (\ell-1)m$, the pointed curve is weak Castle. Notice that the degrees of the corresponding divisors D in the definition, associated to the morphisms x and y, are the same.

(5) A simple computation shows that the number of rational points of $\mathcal{X}$ is $\#\mathcal{X}(\mathbb{F}_q) = 1 + \ell^{2r-1} + m(\ell-1)\ell^{2r-1}$. In particular, $\mathcal{X}$ is maximal iff $r = 1$.

(6) The curve $(\mathcal{X}, Q)$ is Castle when $r = 1$ and $m = \ell + 1$ (the Hermitian case).

Example 8. (Plane non-Frobenius classical curves) Now we consider certain plane curves arising in the context of curves with infinitely many non-singular points whose Frobenius image lies on the respective tangent lines. Let $p(X) \in \mathbb{F}_q[X]$ and let $\mathcal{X}$ be the curve defined by

$$y^m = p(x) \quad \text{such that} \quad y^q - y = \frac{dy}{dx}(x^q - x) \quad (*)\,.$$

Furthermore we shall assume that the polynomial $Y^m - p(X)$ is absolute irreducible (this is true for example if $p(x)$ has at least a root whose multiplicity is coprime with m), where ℓ is the characteristic of q. This curve was studied by Garcia when $\ell > 2$. The following properties below can be proved as in such a paper.

(1) $\deg p(X) = m$.

(2) There are exactly m $\mathbb{F}_q$-rational points over $x = \alpha$ for all $\alpha \in \mathbb{F}_q$ with $p(\alpha) \neq 0$. In addition, there are exactly m $\mathbb{F}_q$-rational points over $x = \infty$. Thus $\#\mathcal{X}(\mathbb{F}_q) \geq m + m(q - \#\{\alpha \in \mathbb{F}_q : p(\alpha) = 0\})$.

(3) If $p(X)$ is a separable polynomial (i.e.,the plane curve of equation $y^m = p(x)$ is non-singular), then it has all its roots in $\mathbb{F}_q$ and hence $\#\mathcal{X}(\mathbb{F}_q) = (q - m + 2)m$.

(4) Assume that $p(X)$ is separable and let α be a root. Let $Q \in \mathcal{X}$ be the unique point over $x = \alpha$ and v the valuation at Q. Then $H(Q) = \langle m-1, m\rangle$. In fact, $\mathrm{div}(1/(x-\alpha)) = \mathrm{div}_\infty(x) - mQ$. Since $v(y) = 1$ we have $\mathrm{div}(y) = Q + E - \mathrm{div}_\infty(x)$ for some $E \geq 0$ with $Q \notin \mathrm{Supp}(E)$, and hence $m - 1 \in H(Q)$ by using $y/(x-\alpha)$. Since $\mathcal{X}$ is non-singular, its genus is $(m-1)(m-2)/2$ and the assertion follows.

(5) If $p(X)$ is separable and α, Q, are as in the previous item, then $(\mathcal{X}, Q)$ is weak Castle with $\deg(D_{\mathcal{X},\phi}) = (q + 1 - m)m$. In order to see this, take $\phi = 1/(x-\alpha)$, $h = m$ and $a = q + 1 - m$. The proof follows directly from the above properties.

We can give concrete examples of these curves.

(a) The Fermat curve $y^m = ax^m + b$ over $\mathbb{F}_q$ with $q = \ell^r$, satisfies the property $(*)$ iff $m = (\ell^r - 1)/(\ell^i - 1)$ with $i \mid r$ (Garcia-Voloch).

(b) (A new Norm-Trace curve). Let $\mathcal{X}$ be the plane curve

$$y^{\ell^2+\ell+1} = p(x) = (x^{\ell+1}+1)^\ell x + (x^\ell + x)^\ell = x^{\ell^2+\ell+1} + x^{\ell^2} + x^\ell + x$$

over $\mathbb{F}_{\ell^3}$. This curve is non-singular and a direct computation shows that property $(*)$ holds true (Garcia). In particular, $(\mathcal{X}, Q)$ is weak Castle, where $Q = (0:0:1)$ and $\phi = 1/x$. It has $\#\mathcal{X}(\mathbb{F}_q) = (\ell^2+\ell+1)(\ell+1)(\ell-1)^2 = \ell^5 + 1 - \ell^2(\ell+1)$ rational points.

More generally, let $q = \ell^r$ $(r \geq 2)$ and let $N_{\mathbb{F}_q|\mathbb{F}_\ell}$ and $T_{\mathbb{F}_q|\mathbb{F}_\ell}$ be, respectively, the norm and trace maps from $\mathbb{F}_q$ to $\mathbb{F}_\ell$. We can consider the plane curve $\mathcal{X}$ given by

$$\begin{aligned} N_{\mathbb{F}_q|\mathbb{F}_\ell}(y) &= N_{\mathbb{F}_q|\mathbb{F}_\ell}(x) + T_{\mathbb{F}_q|\mathbb{F}_\ell}(x) \\ &= (N_{\mathbb{F}_{\ell^{r-1}}|\mathbb{F}_\ell}(x)+1)^\ell x + (T_{\mathbb{F}_{\ell^{r-1}}|\mathbb{F}_\ell}(x))^\ell . \end{aligned}$$

In the same way $\mathcal{X}$ satisfies property $(*)$ above and it is a weak Castle curve with

$$\#\mathcal{X}(\mathbb{F}_q) = \ell^{2r-1} + 1 - \frac{\ell^2(\ell^{r-2}-1)(\ell^{r-1}-1)}{(\ell-1)^2} .$$

As a matter of fact, the curves above over $\mathbb{F}_q$, $q = \ell^r$ are a particular case of curves of type $N_{\mathbb{F}_q|\mathbb{F}_\ell}(y) = p(x)$, where $p(x)$ satisfies the property $p(a) \in \mathbb{F}_\ell$ for any $a \in \mathbb{F}_q$. Here it is not necessary to verify condition $(*)$ in order to obtain week Castle curves. For example we may take $p(x) = x^{\ell^2+\ell} + x^{\ell^2+1} + x^{\ell+1} + \alpha$ with $\alpha \in \mathbb{F}_\ell$ where $q = \ell^3$.

Example 9. (Deligne-Lusztig curves) There are three outstanding types of curves of positive genus over $\mathbb{F}_q$, whose number of rational points attains the maximum number of rational points that curves of their genus over $\mathbb{F}_q$ can have. The case $r = 2$ gives the Hermitian curve and in fact this curve attains the Hasse-Weil upper bound. The other two types are Suzuki and Ree curves. All of them are Castle.

(a) The *Suzuki curve* $\mathcal{S}$ is characterized as being the unique curve over $\mathbb{F}_q$, $q = 2q_0$, $q_0 = 2^r > 2$, of genus $g = q_0(q-1)$ having q^2+1 $\mathbb{F}_q$-rational points (Furhmann, ...). A plane model is given by $y^q - y = x^{q_0}(x^q - x)$. Thus, there is just one point Q over $x = \infty$ which is $\mathbb{F}_q$-rational, and $H(Q) = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$ (Hansen, Sticthenoth, ...). This semigroup is telescopic and hence symmetric.

(b) The *Ree curve* $\mathcal{R}$ is defined over $\mathbb{F}_q$ with $q = 3q_0$, $q_0 = 3^r > 3$. It is birational to the space curve $y^q - y = x^{q_0}(x^q - x)$, $z^q - z = x^{2q_0}(x^q - x)$. $\mathcal{R}$ is characterized by means of its number of rational points q^3+1, its genus $g = q_0(q-1)(q+q_0+1)/3$, and the fact that its group of automorphism equals the Ree group (Hansen, Pederson). There is just one point Q over $x = \infty$ which is $\mathbb{F}_q$-rational. The multiplicity of the Weierstrass semigroup at Q is known to be $h = q^2$ (loc. cit.). In order to show that $\mathcal{R}$ is Castle we have to show that $H(Q)$ is symmetric. This fact is already known (Munuera, Sepúlveda, ...). For the sake of completeness we sketch the proof. We use rudiments of Jacobians (Tate) and Stöhr-Voloch theory concerning bounds on the number of rational points of curves via the

Frobenius morphism. The starting point is our knowledge of the enumerator of the Zeta function of $\mathcal{R}$, namely

$$p(t) = (1 + qt^2)^A (1 + 3q_0 t + qt^2)^B$$

whit $A = q_0(q-1)(q+3q_0+2)/2$ and $B = q_0(q^2-1)$ (Hansen, ...). Since $t^{2g}p(t^{-1})$ is the characteristic polynomial of the Frobenius $\tilde{\mathbf{\Phi}}$ morphism of the Jacobian of $\mathcal{X}$, we obtain the following linear equivalence on $\mathcal{X}$:

$$\mathbf{\Phi}^4(P) + 3q_0\mathbf{\Phi}^3(P) + 2q\mathbf{\Phi}^2(P) + 3q_0\phi(P) + q^2P \sim mQ\,,$$

where $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ is the Frobenius morphism on $\mathcal{X}$, $m := q^2 + 3q_0q + 2q + 3q_0 + 1$, P an arbitrary point of $\mathcal{X}$ and Q an arbitrary $\mathbb{F}_q$-rational point. In particular, $m \in H(Q)$. Let x and y be the rational functions such that $\mathrm{div}_\infty(x) = q^2Q$ and $\mathrm{div}_\infty(y) = m$. We consider the morphism $\pi = (1 : x : y) : \mathcal{X} \to \mathbb{P}^2(\bar{\mathbb{F}})$. After some computations via invariants defined in Stöhr-Voloch theory, we can show that for a generic $P \in \mathcal{X}$, $\mathbf{\Phi}(P)$ belongs to the osculating line at P. This means that $\mathbf{\Phi}(P)$ satisfies a linear equation

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

If v and t are respectively the valuation and a local parameter at Q, it follows that

$$-qm = v(\frac{dy}{dt}) - v(\frac{dx}{dt}) - q^3 = -m - 1 - v(\frac{dx}{dt}) - q^3$$

and hence $v(\frac{dx}{dt}) = 2g - 2$. This shows that $H(Q)$ is symmetric.

Examples of AGG-codes arising from weak Castle curves have nice properties concerning duality and the dimension, one works as in Examples 1, 2. Concerning the minimum distance we recall that

$$d \geq n - \deg(G) + \gamma_{a+1}\,, \quad \text{being } a = \ell(G - D) \text{ the abundance}\,;$$

For these curves, we obtain the following properties of the gonality sequence $GS(\mathcal{X}) = (\gamma_i)_{i\geq 1}$.

Lemma 1. (Munuera, Sepúlveda, ...) *Notation as above. Let $(\mathcal{X}, Q)$ be a Castle curve over $\mathbb{F}_q$ and $H(Q) = \{0 = h_1, 0 < h_2, h_3, \ldots\}$ be the Weierstrass semigroup at Q. If $h_2 \leq q + 1$, then*

(1) $\gamma_2 = h_2$;
(2) *Let $\gamma = \gamma_2$. Then $\gamma_i = h_i$ for $i \geq g - \gamma + 2$; i,e,*

$$\gamma_i = h_i = \begin{cases} i + g - 2 & \text{if } g - \gamma + 2 \leq i \leq g, \\ i + g - 1 & \text{if } i > g. \end{cases}$$

Proof. (Hint) Use the simmetry of $H(Q)$ and the symmetry of $GS(\mathcal{X})$ (Carvalho): $t \in GS(\mathcal{X})$ iff $2g - 1 - t \notin GS(\mathcal{X})$). □

Proposition 2. *Let $(\mathcal{X}, Q)$ be a weak Castle curve. Let d_m be the minimum distance of $C_m = C(\mathcal{X}, D, mQ)$.*

(1) *If $m = th$, $t = 1, \ldots, a-1$, then C_m reaches equality in the Goppa bound, i.e., $d_m = n - m$.*
(2) *For $m < n$, then C_m reaches equality in the Goppa bound if and only if C_{n-m} does;*
(3) *If $h = h_2$ then for $n - h_2 \leq m \leq n$, we have $h_2 \geq d_m \geq \gamma_2$. In particular, if $(\mathcal{X}, Q)$ is Castle and $h_2 \leq q + 1$, then $d_m = h_2$.*

An extension of the minimum distance is given by the generalized Hamming weights. Let us remember that, for a code C of dimension k, we define the r-th generalized Hamming weight as

$$d^r = d^r(C) =: \min\{\mathrm{supp}(L) : L \text{ is a } r\text{-dimensional vector subspace of } C\}$$

$r = 1, \ldots, k$, where $\mathrm{supp}(L) = \{i : \text{ there is } \mathbf{x} \in L \text{ with } x_i \neq 0\}$. In the next Proposition, we calculate bounds of the generalized Hamming weights for weak Castle codes. We denote the r-th generalized Hamming weight of the $C_m = C(\mathcal{X}, D, mQ)$ code by d^r_m.

Proposition 3. *Let $(\mathcal{X}, Q)$ be a weak Castle curve. Let $C_m = C(\mathcal{X}, D, mQ)$ be a code of dimension k_m and abundance $\alpha = \alpha_m$. Then for every r, $1 \leq r \leq k_m$:*

(1) $n - m + \gamma_{r+\alpha} \leq d^r_m \leq d_{m-h_{r+\alpha}}$
(2) *If $m - h_{r+\alpha} = th$ or $n - m + h_{r+\alpha} = th$, $t = 1, \ldots, a-1$, then $d^r_m \leq n - m + h_{r+\alpha}$.*

Finally we consider

The order bound. Let $(\mathcal{X}, Q)$ be a weak Castle curve and let $H(Q) = \{0 = h_1, h_2, \ldots\}$ be the Weierstrass semigroup at Q. For $\ell = 1, 2, \ldots$, recall the sets

$$A(\ell) := \{h_s \in H(Q) : \ h_{l+1} - h_s \in H(Q)\}\,,$$

The ℓ-th *order bound* of $H(Q)$ is defined as

$$d_{ORD}(\ell) := \min\{\#A(r) : r \geq \ell\}\,.$$

This bound can be extended to all generalized Hamming weights as follows (Heijnen, Pellikaan, Munuera, Farrán). For $\ell_1 < \ldots < \ell_r$, define the set $A(\ell_1, \ldots, \ell_r) = A(\ell_1) \cup \ldots \cup A(\ell_r)$. Let ℓ be a positive integer. The number $d^r_{ORD}(\ell) = \min\{\#A(\ell_1, \ldots, \ell_r) : \ell \leq \ell_1 < \ldots < \ell_r\}$ is called the ℓ-th *order bound* on the r-th generalized weight of $H(Q)$.

Proposition 4. *$d(C(\mathcal{X}, D, mQ)) \geq d_{ORD}(\iota(n + 2g - 2 - m))$. More generally, for all r, $1 \leq r \leq k_m$, we have $d^r_m(C(\mathcal{X}, D, mQ)) \geq d^r_{ORD}(\iota(n + 2g - 2 - m))$.*

Example 10. Let us consider the new Norm-Trace curve introduced above with $\ell = 3$ and $r = 2$; i.e, the curve is given by $y^{\ell+1} = x^{\ell+1} + x^\ell + x$. It has 28 $\mathbb{F}_{28}$-rational points and thus it is the Hermitian. Here with $\phi = 1/x$ and taking 6 points in $\mathbb{F}_9$ we find a code of lenght 24. The dimension can be stimated by the Weierstrass semigroup which equals $\langle 3, 4\rangle$ (thus $24 = \rho_{22}$) and hence $k = 22$. The minimum distances can be estimated via the order bound. According to the Grassl tables, we obtain $[24, k, d]$ codes with the best (already) known parameters for all values of k, $1 \leq k \leq 24$, except $k = 4, 18, 19, 20$.