AG Goppa Codes from Maximal Curves over determined Finite Fields of characteristic 2

Robert J. McEliece
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125, USA
Email: rjm@systems.caltech.edu

M. C. Rodriguez-Palánquex
E.U. Estadística
Universidad Complutense de Madrid
Avda. Puerta de Hierro s/n, 28040 Madrid, Spain
Email: mcrodri@mat.ucm.es

Abstract. **In AG coding theory is very important to work with curves with many rational points, to get good codes. In this paper, from curves defined over $\mathbb{F}_2$ with genus $g \geq 1$ we give sufficient conditions for getting maximal curves over $\mathbb{F}_{2^{2g}}$**

I. Introduction

Curves with many rational points are very interesting in Coding theory. In particular, *Goppa geometric codes* obtained from *Hermitian curves* have been extensively studied [9],[10].

If C is a smooth projective curve over the finite field $\mathbb{F}_q$, with genus g, then by the Hasse-Weil Theorem, the number of rational points is bounded by

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$$

We have studied properties of *Quasihermitian curves* and the Goppa codes obtained from them [6], [7].

We present here some results about sufficient conditions for getting maximal curves over $\mathbb{F}_{2^{2g}}$, and we apply these results to *Quasihermitian curves*.

Quasihermitian curves are defined over $\mathbb{F}_q$, with $q = 2^j$, $\forall a, b \in \mathbb{Z}$, being $a \geq 2$, $b > -a, \beta_1, \beta_2 \in \mathbb{F}_q - \{0\}$, by the affine equation

$$y^a + \beta_1 y + \beta_2 x^{a+b} = 0$$

If C is the curve the equation

$$y^a + y + x^{a+b} = 0$$

with $a, b \in \mathbb{Z}$, being $a \geq 2$, $b > -a$ then its genus is [6]

$$g(C) = \frac{s_0(b_0 - 1)}{2} - \alpha_0$$

where

$$a + b = 2^n b_0 \text{ with } n \geq 0 \text{ and } b_0 \geq 1 \text{ odd}$$
$$a - 1 = 2^s s_0 \text{ with } s \geq 0 \text{ and } s_0 \geq 1 \text{ odd}$$
$$\alpha = \gcd(a, b_0),\ \alpha = 2\alpha_0 + 1$$

Among these *Quasihermitian curves* there are many maximal curves, i.e., for the non-singular models of these curves, the number of $\mathtt{i}_q$ -rational points attains the *Hasse-Weil upper bound*

$$q + 1 + 2g\sqrt{q}$$

Quasihermitian curves include some types of known maximal curves. If $j = 2j_0$ we have the maximal curves

$$y^{2^{j_0}} + y = x^m$$

where m is a divisor of $(2^{j_0}+1)$ ([1]). When $m = 2^{j_0}+1$, we have the *Hermitian Curves,*

$$y^{2^{j_0}} + y = x^{2^{j_0}+1}$$

Maximal *Quasihermitian curves* are, for example:

$$y^2 + y = x^{13} \text{ (maximal over } \mathbb{F}_{2^{12}})$$
$$y^4 + y = x^6 \text{ (maximal over } \mathbb{F}_{2^6})$$

II. Zeta Function

Let C be a non-singular curve of genus g defined over $\mathbb{F}_q$, $s \in \mathbb{N}$ and $Pic_s(C)$ is the set of equivalent class of divisors of degree s. We suppose that $\#Pic_0(C)=h$. Then, for each s is $\#Pic_s(C)=0$ or h. If a_s is the number of effective divisors of degree s on C, we define the *Zeta function* [3]

$$z(C,t) = \sum_{s=0}^{\infty} a_s t^s$$

this series converges if $|t| < \sqrt{q}$ and $z(C, t)$ is the rational function in t

$$z(C,t) = \frac{p(t)}{(1-t)(1-qt)}$$

being $p(t) \in \} [t]$, such that

$$p(t) = \prod (1 - z_i t)(1 - \bar{z}_i t)$$

with $z_1, ..., z_g \in \} [i]$ and $|z_i| = \sqrt{q}$.

The *Zeta function* satisfies

$$\log(z(C,t)) = \sum_{r=1}^{\infty} N_r \frac{t^r}{r}$$

So,

$$\#C(\mathbb{i}_q^r) = q^r + 1 - \sum_{i=1}^{g} (z_i^r + \bar{z}_i^r)$$

III. Maximal Curves over $\mathbb{F}_{2^{2g}}$

In this section, we present the main theorem with the sufficient conditions for obtaining maximal curves.

Lemma *Let C be a defined curve over $\mathbb{F}_2$ with genus g. If $\forall j \le g$, $\#C(\mathbb{F}_{2^j}) = 2^j + 1$, then*

$$\sum_{i=1}^{g} (z_i^{2g} + \bar{z}_i^{2g}) = -2^{g+1} g$$

Proof.

According to the definition of *Zeta function*, we have that

$$\forall r, \#C(\mathbb{i}_{2^r}) = 2^r + 1 - ((z_1^r + \bar{z}_1^r)) + (z_2^r + \bar{z}_2^r) + ... + (z_g^r + \bar{z}_g^r))$$

Moreover,

$$\forall j \le g, \ \#C(\mathbb{F}_{2^j}) = 2^j + 1$$

Then

$$(z_1 + \bar{z}_1) + ... + (z_g + \bar{z}_g) = 0$$
$$(z_1^2 + \bar{z}_1^2) + ... + (z_g^2 + \bar{z}_g^2) = 0$$
$$\vdots$$
$$(z_1^g + \bar{z}_1^g) + ... + (z_g^g + \bar{z}_g^g) = 0$$

Thus, if

$$p(t) =$$
$$= (1 - z_1 t)(1 - \bar{z}_1 t)...(1 - z_g t)(1 - \bar{z}_{g1} t) =$$
$$= 1 + \sigma_1 t + ... + \sigma_{2g-1} t^{2g-1} + \sigma_{2g} t^{2g}$$

then, we have proved that

$$\sigma_1 = \sigma_2 = ... = \sigma_{2g-1} = 0$$

Using for this proof the *Newton Identy* [4] [5]

So, we have that

$$\sum_{i=1}^{g}(z_i^{2g}+\bar{z}_i^{2g})=-2^{g+1}g$$

And

$$p(t)=1+(-1)^{2g}(z_1\bar{z}_1...z_g\bar{z}_g)t^{2g}=$$
$$=1+2^g t^{2g}$$

being

$$z(C,t)=\frac{1+2^g t^{2g}}{(1-t)(1-2t)}$$

Theorem *Let g be the genus of the curve C defined over* $\mathbb{F}_2$.
If $\forall j \le g$, $\#C(\mathbb{F}_{2^j})= 2^j+1$, *then C is maximal over* $\mathbb{F}_{2^{2g}}$.

Proof.

According to *Hasse-Weil bound*

$$\#C(\mathbb{F}_{2^{2g}})$$

By the Lemma

$$z(C,t)=\frac{1+2^g t^{2g}}{(1-t)(1-2t)}$$

Moreover

$$\#C(\mathbb{F}_{2^g})=2^g+1-\sum_{i=1}^{g}(z_i^g+\bar{z}_i^g)$$

By hypothesis

$$\forall j \le g,\ \#C(\mathbb{F}_{2^j})=2^j+1$$

Therefore, by the Lemma

$$(z_1^{2g}+\bar{z}_1^{2g})+...+(z_g^{2g}+\bar{z}_g^{2g})=-2^{g+1}g$$

So,

$$\#C(\mathbb{F}_{2^{2g}})=2^{2g}+1-\sum_{i=1}^{g}(z_i^{2g}+\bar{z}_i^{2g}) \Rightarrow$$
$$\Rightarrow \#C(\mathbb{F}_{2^{2g}})=2^{2g}+1+2^{g+1}g$$

The curve *C* is maximal on $\mathbb{F}_{2^{2g}}$.

IV. Conclusion

Let *g* be the genus of *C* and let $\#C(\mathbb{F}_q)$ be the number of $\mathbb{F}_q$-rational points of *C* (i.e., for the non-singular model of *C*). We can compute the values $\#C(\mathbb{F}_q)$ using *Zeta function program*, so we can present, for example, the following maximal *Quasihermitian curves* according to the sufficient conditions of this Theorem.

$C: y^2+y+x^{13}=0$
with $g=6$ and $\#C(\mathbb{F}_{2^{12}})=4{,}865$

$C: y^2+y+x^{11}=0$
with $g=5$ and $\#C(\mathbb{F}_{2^{10}})=1{,}345$

$C: y^4+y+x^3=0$
with g =3 and $\#C(\mathbb{F}_{2^6})=113$

$C: y^3+y+x^5=0$
with $g=2$ and $\#C(\mathbb{F}_{2^4})=33$

V. References

[1] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros, F.Torres. *On plane maximal curves*. Math. AG/9802113. (Feb. 1998).

[2] R. Hartshorne. *Algebraic geometry*. GTM 76, Springer-Verlag, New York. (1982).

[3] J.H. van Lint, G. van der Geer. *Introduction to coding theory and algebraic geometry*. DMV Seminar, 12. Birkhäuser Verlag, Basel. (1988).

[**4**] F.J. MacWilliams, N.J.A. Sloane.*The Theory of Error Correcting Codes*. Amsterdam, North-Holland. 1977.

[**5**] R.J.McEliece, M.C. Rodríguez-Palánquex. *Results to get Maximal Quasihermitian Curves*. *New possibilities for AG Codes*. Information, Coding and Mathematics. Kluwer Academic Publishers.2002.

[**6**] M. C. Rodríguez-Palánquex, L.J. García-Villalba, I. Luengo-Velasco. *Computing the Genus of a Class of Curves*. LNCS 2227, pp. 182-191. Springer-Verlag 2001

[**7**] L.J. García-Villalba, M. C. Rodríguez-Palánquex, F. Montoya-Vitini. *An Algorithm for Computing the Minimum Distance*. Electronics Letters, Vol. 35, No. 18, pp.1534-1535. 1999

[**8**] J. H. Silverman. *The arithmetic of elliptic curves*. GTM 106, Springer-Verlag, New York (1986).

[**9**] H. Stichtenoth. *A note on Hermitian codes over GF*(*q*2). IEEE Trans. Inf. Theory, vol. 34 (5), pp. 1345-1347. (September 1988).

[**10**] H. J. Tiersma. *Remarks on codes from Hermitian curves*. IEEE Trans. Inform. Theory, vol. IT-33 (4). (July 1987).