Multiplicative character sums and non linear geometric codes

Marc Perret[1]

Abstract. Let q be a power of a prime number, F_q the finite field with q elements, n an integer dividing q - 1, $n \geq 2$, and χ a character of order n of the multiplicative group F_q^*. If X is an algebraic curve defined over F_q and if G is a divisor on X, we define a non linear code $\Gamma(q, X, G, n, \chi)$ on an alphabet with n + 1 letters.We compute the parameters of this code, through the consideration of some character sums.

Introduction. If f is a rational function on the curve X, define

$$W(f) = \sum_{P \in X_*(F_q)} \chi(f(P)),$$

where $X_*(F_q)$ is the set of rational points on the curve X which are neither a zero or a pole of f. The study of such a character sum, or more precisely of a slightly different sum, enables us to derive some estimations for the number of points of a Kummer covering [3].

In an other way, the extra data of a divisor G on X, prime to the F_q-rational points of X, allows to define, both following Goppa [1] and Tietäväinen [6], some non linear codes, whose parameters can be bounded via some estimates for the above mentioned modified character sums.

In the first part, we study the modified character sums and their related Kummer coverings. The genus of a Kummer covering is given in § I. 1, Theorem 1. In § I. 2, we define the modified character sums, and obtain a bound for them (Theorem 2), from which we deduce a generalized Weil's inequality for Kummer coverings (§ I. 3, Theorem 3).

We construct in the second part the non linear geometric codes (§ II. 1), compute their parameters in § II. 2 (Theorem 4), and give some more explicit examples in § II. 3.

[1] Equipe CNRS "Arithmetique & Théorie de l'Information"
C.I.R.M. Luminy Case 916
13288 Marseille Cedex 9
France.

No proofs are given here. The proofs of the first part can be found in [3], and those of the second part in a forthcoming paper [4].

I. Multiplicative character sums

1. Kummer coverings. Let X be a smooth irreducible algebraic projective curve defined over $\mathbf{F}_q$, K its rational function field and n an integer dividing q - 1. If P is a point of X, we denote by v_P the normalised valuation of K defined by P. Namely, for $f \in K$

$$v_P(f) = \begin{cases} m \text{ if P is a zero of order m of f,} \\ -m \text{ if P is a pole of order m of f,} \\ 0 \text{ if P is not a zero nor a pole.} \end{cases}$$

We then define the reduced order of f at P by

$$v'_P(f) = \operatorname*{Min}_{g \in K^*} (|v_P(fg^n)|),$$

(where $|x|$ is the absolute value of $x \in \mathbf{R}$), in such a way that $0 \leq v'_P(f) < n$. This number $v'_P(f)$ is the remainder of the euclidean division of $v_P(f)$ by n.

Let H_0 be a subgroup of K^* containing K^{*n} as a subgroup of finite index, let Y be the smooth model of $L = K(H_0^{1/n})$, and assume that L and K have the same constant field : we then say that H_0 is regular. The extension L/K is a Kummer extension [3], so that the corresponding covering $\pi : Y \to X$ is a Kummer covering. The following theorem gives the genus g_Y of Y, where

$$U'(f) = \{P \in X(\overline{\mathbf{F}_q}), v'_P(f) \neq 0\},$$

and where $\overline{\mathbf{F}_q}$ is an algebraic closure of $\mathbf{F}_q$.

Theorem 1. *Let $r = (H_0 : K^{*n})$, g_X and g_Y the genus of X and Y. Then*

$$2g_Y - 2 = r(2g_X - 2) + \sum_f \sum_{u \in U'(f)} \deg u,$$

where the first sum runs over a system of representatives of H_0/K^{*n}.

2. Character sums. Let χ be a character of F_q^* of order n, and $k = F_q$. For $f \in K^*$, we define the sum

$$W(f) = \sum_{P \in X_*(F_q)} \chi(f(P)) \;;$$

here, $X_*(F_q) = \{ P \in X(F_q), f(P) \neq 0, \infty\}$. A modified sum is more closely related to the Kummer covering $Y \to X$ defined in I.1. For $f \in K$ and $P \in X(F_q)$, let

$$\chi'(f(P)) = \chi(h(P)) \qquad \text{if } f = g^n.h, \text{ h invertible at P,}$$
$$\chi'(f(P)) = 0 \qquad \text{if } v_P'(f) = 0\;;$$

then define

$$W'(f) = \sum_{P \in X(F_q)} \chi'(f(P)).$$

Theorem 2. *Let H_0 be a regular subgroup of K^*, containing K^{*n} as a subgroup of finite index, and H' a system of representatives of the non vanishing classes of H_0 (mod K^{*n}). Then*

$$\left| \sum_{f \in H'} W'(f) \right| \leq \frac{B(H_0)}{2} [2\sqrt{q}],$$

with

$$B(H_0) = (r - 1)(2g_X - 2) + \sum_{f \in H'} \;\sum_{u \in U'(f)} \deg u\ .$$

The proof of this theorem involves the theory of abelian L-function and the Riemann hypothesis for curves (the Weil theorem), by considering the L function related to f :

$$L'(T,f) = \exp\Big(\sum_{s=1}^{\infty} \frac{T^s}{s} W_s'(f)\Big),$$

with

$$W_s'(f) = \sum_{P \in X(F_{q^s})} \chi'(N_{F_{q^s}/F_q}(f(P))).$$

In the particular case where H_0 is the subgroup of K^* generated by $\phi \in K^*$ and K^{*n}, it is easyly seen that H_0 is regular if ϕ is not a constant function, so we obtain

Corollary 1. *Let ϕ be a non constant rational function on X. Then*

$$\left|\sum_{i=1}^{n-1} W'(\phi^i)\right| \leq (n-1)(g_X - 1 + \sum_{P\in U'(\phi)} \deg P)[2\sqrt{q}].$$

3. Number of points of a Kummer covering. As a consequence of theorem 2, we obtain the following

Theorem 3. *Let X as above, K its rational function field, and $\pi : Y \to X$ be the Kummer covering defined by a subgroup H_0 of K^* containing K^{*n} as a subgroup of finite index. Then*

$$|\#Y(F_q) - \#X(F_q)| \leq \frac{B(H_0)}{2}[2\sqrt{q}].$$

Because of theorem 1, this estimate can also be written

$$|\#Y(F_q) - \#X(F_q)| \leq (g_Y - g_X)[2\sqrt{q}].$$

This is an improvement, in this case, of Weil's inequality $|\#Y(F_q) - \#P_1(F_q)| \leq g_Y[2\sqrt{q}]$. The same inequality has been proved by Lachaud in the case of a general abelian covering $\pi : Y \to X$ (see [2]).

II. Non linear geometric codes

1. The codes. Let X be as above and set $N = \#X(F_q)$. Let G be a divisor on X prime to $X(F_q)$, and χ a character of order n of F_q^* with value in the group $\mu_n(C)$ of n-th roots of unity in C. Consider the map

$$c : L(G) \to (\mu_n(C)\cup\{0\})^N$$
$$f \to (c_P(f))_{P\in X(F_q)},$$

where

$$c_P(f) = \chi'(f(P)),$$

and χ' is as defined in I.2. We define the code $\Gamma = \Gamma(q, X, G, n, \chi)$ as the image of L(G) under c.

2. Parameters of Γ. The following is a lower bound for the Hamming distance between two codewords in terms of the above character sum :

Lemma 1. *For $f, g \in L(G)$, letting $\phi = f.g^{n-1}$; then*

$$d(c(f), c(g)) \geq \frac{n-1}{n} N - \frac{1}{n} \sum_{i=1}^{n-1} W'(\phi^i) - \deg G.$$

Remark. It is possible to give an upper bound for $d(c(f), c(g))$.

Corollary 1 and Lemma 1 enable to give an estimate for the parameters of Γ :

Theorem 4. *If*

$$N > (g - 1 + 2 \deg G)[2\sqrt{q}]) + \frac{n}{n-1} \deg G,$$

then $\Gamma(X, G, \chi)$ is a non linear code of length $N = \#X(F_q)$ on an alphabet with $(n + 1)$ elements, of minimum distance

$$d_{min}(\Gamma) \geq \frac{n-1}{n} (N - (g - 1 + 2 \deg G)[2\sqrt{q}]) - \deg G,$$

and of cardinality

$$M = \#\Gamma \geq q^{\deg G + 1 - g}.$$

3. Examples. Let $N_g(q)$ (resp $n_g(q)$) be the maximum (resp. minimum) number of $\mathbf{F}_q$-rational points of an algebraic smooth projective irreducible curve of genus g defined over $\mathbf{F}_q$. Such a curve will be called maximal (resp. minimal) if it reaches this bound. Moreover, let $k = \frac{\log M}{\log (n+1)}$ be the "dimension" of the $(N, M, d)_{n+1}$ code.

a. Codes from the projective line. The projective line $\mathbf{P}^1_{\mathbf{F}_q}$ has genus 0 and q + 1 rational points over $\mathbf{F}_q$. If we choose a divisor G of degree m and a quadratic character χ of $\mathbf{F}_q^*$, (that is for n = 2 and q odd), we obtain the following

Proposition 1. *For all powers q of an odd prime number and all integers $m < \frac{q + 1 + [2\sqrt{q}]}{2([2\sqrt{q}] + 1)}$, there exists a F_3 non linear code with parameters*

$$\left(q + 1, k = (m + 1) \frac{\log q}{\log 3}, d \geq \frac{q + 1 + [2\sqrt{q}]}{2} - m([2\sqrt{q}] + 1)\right)_3.$$

b. Codes on elliptic curves. The above construction on an extremal elliptic curve X over $\mathbf{F}_q$, n = 2, a divisor G of degree m and a quadratic character χ of $\mathbf{F}_q^*$, gives

Proposition 2. *For all powers q of an odd prime number and all integers* $m < \frac{N_1(q)}{2([2\sqrt{q}]+1)}$, *there exists a* F_3 *non linear code with parameters*

$$\left(N_1(q),\ k \geq m\,\frac{\log q}{\log 3},\ d \geq \frac{N_1(q)}{2} - m([2\sqrt{q}]+1)\right)_3,$$

and a similar result holds if we replace $N_1(q)$ *by* $n_1(q)$.

Note that the exact values of $N_1(q)$ and $n_1(q)$ are known (cf for example [5]).

Examples.

1) For q = 127, $N_1(127) = 150$ and $n_1(127) = 106$.

$m = 2$ gives a $(150,\ k \geq 2\frac{\log 127}{\log 3},\ d \geq 29)_3$ and a $(106,\ k \geq 2\ \frac{\log 127}{\log 3},\ d \geq 7)_3$ code.

2) q = 1033 $N_1(1033) = 1098$ $n_1(1033) = 970$

$m = 6$ $(1098,\ k \geq 6\frac{\log 1033}{\log 3},\ d \geq 159)_3$ $(970,\ k \geq 6\frac{\log 1033}{\log 3},\ d \geq 95)_3$

c. Codes over $\mathbf{F}_4$ from curves of genus 2. If we consider extremal curves of genus 2 over $\mathbf{F}_q$ for $q \equiv 1 \pmod 3$, and multiplicative characters of $\mathbf{F}_q^*$ of order 3, we obtain

Proposition 3. *For all powers q of a prime number,* $q \equiv 1 \pmod 3$, *all integers* $g \in N$, *and all integer m such that*

$$m < \frac{N_2(q) - [2\sqrt{q}]}{2[2\sqrt{q}] + 3/2},$$

there exists a non linear F_4*-code with parameters*

$$\left(N_2(q),\ k \geq (m-1)\,\frac{\log q}{\log 4},\ d \geq \frac{2}{3}(N_2(q) - (1+2m)[2\sqrt{q}]) - m\right)_4,$$

and a similar result holds if we replace $N_2(q)$ by $n_2(q)$.

A general formula for $N_2(q)$ and $n_2(q)$ can be found in [5].

Examples.

1) $q = 511$	$N_2(511) = 602$	$n_2(511) = 422$
$m = 2$	$(602, k \geq \frac{1}{2}\frac{\log 511}{\log 2}, d \geq 210)_4$	$(422, k \geq \frac{1}{2}\frac{\log 511}{\log 2}, d \geq 100)_4$
$m = 5$	$(602, k \geq 2\frac{\log 511}{\log 2}, d \geq 37)_4$	
2) $q = 1033$	$N_2(1033) = 1162$	$n_2(511) = 906$
$m = 5$	$(1162, k \geq 2\frac{\log 1033}{\log 2}, d \geq 263)_4$	$(906, k \geq 2\frac{\log 1033}{\log 2}, d \geq 87)_4$
$m = 6$	$(1162, k \geq \frac{5}{2}\frac{\log 1033}{\log 2}, d \geq 178)_4$	

4. Conclusion. The above construction gives non linear codes on any alphabet with $n + 1 \geq 3$ elements. Lemma 1 links the Hamming distance and some character sums, and estimations on these character sums enable us to give a lower bound for the minimum distance, and to compute the cardinality of these codes under a technical assumption (theorem 4). Because of the generality of the estimations we used, one can expect the true minimum distance to be much greater than the given lower bound in many cases. Numerical computations could give information, for example, in the case of the code constructed from the space of polynomials of given bounded degree on the projective line, and from the quadratic character.

Bibliography

[1] Goppa, V. D.*Algebraico-geometric codes*, Math. USSR Izv., **21** (1983), pp.75-91.

[2] Lachaud, G. *Artin-Schreier curves, exponential sums and the Carlitz-Uchiyama bound for geometric codes*, accepted in Jour. of Number Theory.

[3] Perret, M. *Multiplicative Character Sums and Kummer Coverings*, accepted in Acta Arithmetica.

[4] Perret, M. *Non linear geometric codes*, in preparation.

[5] Serre, J. P. *Nombre de points des courbes algébriques sur* F_q, Sém de Theorie des Nombres de Bordeaux 1982/83, n° **22** = Œuvres, n° 129, vol. III, pp. 664-668, Springer, New york 1986.

[6] Tietäväinen, A. *Character sums and applications of coding theory,* Ann. Univ. Turkuensis, Ser. A I, **186** (1984), pp. 110-117.