Binary spherical geometric codes.

Marc Perret
Equipe C.N.R.S. "Arithmétique & Théorie de l'information"
C.I.R.M. Luminy Case 916, 13288 Marseille Cedex 9
France.

Abstract. Let q be a power of an odd prime number and $\mathbf{F}_q$ be the finite field with q elements. We will construct a binary spherical code from an algebraic curve C defined over $\mathbf{F}_q$ and a rational divisor G on C, as the twist by the quadratic character η of the Goppa code L(G). The computation of the parameters of this code is based on the study of some character sums.

0. Introduction. In a previous paper ([3]), we have constructed some non linear geometric codes on any alphabet having $n \geq 3$ elements from a smooth projective irreducible algebraic curve C defined over $\mathbf{F}_q$, a rational divisor G on C and a multiplicative character χ of order n - 1 of $\mathbf{F}_q^*$ as a twist of the Goppa code L(G). Unfortunately, we were unable to construct a binary code in this way : this is what we will do here. In order to compute the parameters of these codes, it is convenient to define them as spherical codes. As in the case studied in [3], these parameters can be computed from estimations on certain character sums.

In the first section, we give the useful definitions and result (proposition 1) on character sums ; the proofs can be found in [2]. In the second section, we recall the basic concepts for spherical codes. For more informations on this topic, see [1] for example. In the third section, we define the geometric spherical code, and give its parameters in the fourth section (theorem 1). This theorem follows from an estimation for the angle between two codewords in term of a character sum (proposition 2). In the fifth section, we deduce from this study the Hamming parameters of this code (theorem 2). Finally, we ask in the sixth section some open questions.

in this paper, #X will denote the cardinality of the set X.

1. Multiplicative Character Sums. Let C be a smooth projective irreducible curve of genus $g(C)$ defined over $\mathbf{F}_q$, G a rational divisor on C prime to $X(\mathbf{F}_q)$, and η the quadratic character of the multiplicative group $\mathbf{F}_q^*$ (that is, $\eta(x) = 1$ if $x \in \mathbf{F}_q^*$ is a square, and $\eta(x) = -1$ if not). If $P \in C$ and $f \in K = K(C)$ the function field of C, we define the P-adic valuation $v_P(f)$ as follows :

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

Let

$$v_P'(f) := \operatorname{Min}_{g \in K^*} (| v_P (fg^2) |)$$

be the *reduced order of f at P*. Notes that this reduced order is always obtained for a certain $g \in K^{*2}$. Let

$$\eta'(f(P)) := \begin{cases} \eta(g(P)) \text{ if } v_P'(f) = v_P(g) = 0 \text{ and } f \equiv g \bmod K^{*2}, \\ 1 \text{ if } v_P'(f) \neq 0. \end{cases}$$

Defines $C'(f) = \{P \in C(\mathbf{F}_q) / v_P'(f) = 0\}$, and $U'(f) = \{P \in C(\mathbf{F}_q) / v_P'(f) \neq 0\}$, in such a way that $C(\mathbf{F}_q) = C'(f) \cup U'(f)$ (disjoint union), and

$$W'(f) := \sum_{P \in C'(\mathbf{F}_q)} \eta'(f(P)).$$

Then, $\overline{\mathbf{F}_q}$ being an algebraic closure of $\mathbf{F}_q$, we have

Proposition 1. *If $f \in K$, then*

$$| W'(f) | \leq c(f)\sqrt{q},$$

with

$$c(f) = 2g(C) - 2 + \sum_{P \in C(\overline{\mathbf{F}_q}) / v_P'(f) = 0} \deg P.$$

2. Spherical codes. for more details, see [1]. We denote by S_{n-1} the unit sphere of $\mathbf{R}^n$. If $x, y \in S_{n-1}$, let

$$\varphi(x, y) = \arccos(x, y)$$

be the angle between x and y (in such a way that $(x \mid y) = \cos \varphi(x, y)$, where $(. \mid .)$ denotes the usual scalar product), and

$$\rho(x, y) = \| x - y \|^2$$

be the euclidean distance between x and y. If $X \subset S_{n-1}$ is a finite set, we say that X is a *spherical code* of *length* n. Its *minimum angle* is

$$\varphi(X) = \text{Min } \{ \varphi(x, y), x, y \in X, x \neq y\}$$

and its *minimum distance* (in the euclidean sense) is

$$\rho(X) = \text{Min } \{\rho(x - y), x, y \in X, x \neq y\}.$$

It is easily seen that

$$\rho(X) = 2 - 2 \cos \varphi(X) = 4 \frac{\sin^2 \varphi(X)}{2}.$$

Let us denote by $\theta(X)$ the ratio

$$\theta(X) = \frac{\log_2 \#X}{n}.$$

Remark. When X is a binary spherical code, that is, a spherical code whose points have the form $\frac{1}{\sqrt{N}}(\pm 1, \ldots, \pm 1)$, it is clear that $\theta(X) = k(X)$ is the usual dimension of the code X.

3. The geometric spherical code. Let $N = \#C(\mathbf{F}_q)$, S_{N-1} the unit sphere of $\mathbf{R}^N$ and x the map

$$\begin{aligned} x : L(G) &\to S_{N-1} \\ f &\to (x_P(f))_{P \in C(\mathbf{F}_q)}, \end{aligned}$$

with

$$x_P(f) := \frac{1}{\sqrt{N}} \eta'(f(P)).$$

It is easy to check that for $f \in L(G)$, we have $x(f) \in S_{N-1}$. Indeed,

$$\|x(f)\| = \sum_{P \in C(\mathbf{F}_q)} x_P^2(f) = \frac{1}{N} \sum_{P \in C(\mathbf{F}_q)} \left(\eta'(f(P))\right)^2 = 1.$$

We define the code $X = X(q, C, G)$ as the image of L(G) under x. This is a spherical code, whose parameters can be computed as follows.

4. Parameters of X.

Theorem 1. *Suppose that* $N > 2(g(C) - 1 + \deg G)\sqrt{q} + 2 \deg G$. *Then X is a spherical code of length* $N = \#C(F_q)$, *with parameters*

$$\rho(X) \geq 2 - \frac{4}{N}((g(C) - 1 + \deg G)\sqrt{q} + \deg G)$$

and

$$\theta(X) \geq (\deg G + 1 - g(C))\frac{\log_2 q}{N}.$$

This theorem follows from the following proposition.

Proposition 2. *For* $f, g \in L(G), f \neq g$, *we have*

$$|(x(f) \mid x(g))| \leq \frac{1}{N}(|W'(fg)| + 2 \deg G).$$

Proof.

$$N(x(f) \mid x(g)) = N \sum_{P \in C(F_q)} x_P(f)x_P(g) = \sum_{P \in C(F_q)} \eta'(f(P))\ \eta'(g(P))$$

$$= \sum_{P \in C'(fg)} \eta'(fg(P)) + \sum_{P \in U'(f) \cap C'(g)} \eta'(g(P)) + \sum_{P \in C'(f) \cap U'(g)} \eta'(f(P))$$

since $C(F_q) = C'(fg) \cup U'(fg)$, and $U'(fg) = \big(U'(f) \cap C'(g)\big) \cup \big(C'(f) \cap U'(g)\big)$. Thus,

$$N\,|(x(f) \mid x(g))| \leq |W'(fg)| + \#U'(f) \cap C'(g) + \#C'(f) \cap U'(g)$$

$$\leq |W'(fg)| + \#U'(f) + \#U'(g).$$

But for $f, g \in L(G)$, we have $\#U'(f) \leq \deg G$ and $\#U'(g) \leq \deg G$, which proves the proposition 2.

Corollary 1. *For* $f, g \in L(G), f \neq g$, *we have*

$$|(x(f) \mid x(g))| \leq \frac{2}{N}((g(C) - 1 + \deg G)\sqrt{q} + \deg G)).$$

Proof. This is clear from propositions 1 and 2, and the fact that for $f \in L(G)$,

$$\sum_{P \in C(\overline{F_q}) \,/\, v_P'(f) = 0} \deg P \le 2 \deg G.$$

Remark. Corollary 1 can be slightly improved by

$$| (x(f) | x(g)) | \le \frac{1}{N} [(2g(C) - 2 + \deg G + \kappa)\sqrt{q} + 2\deg G)]$$

where $\kappa = \deg \mathrm{Supp}(G)$ is the degree of the support of G : if $G = \sum_P m_P P$ with $m_P \neq 0$, then $\kappa = \sum_P \deg P \le \deg G$. Moreover, $\kappa = \deg G$ if and only if $m_P = 1$ for all P such that $m_P \neq 0$.

Proof of Theorem 1. Under the hypothesis $N > 2(g(C) - 1 + \deg G)\sqrt{q} + 2 \deg G$, corollary 1 shows that for all $f, g \in L(G)$ such that $f \neq g$, we have $| (x(f) | x(g)) | < 1$. Thus, the map x is one-one, so that $\log_2 \#X = \log_2 \#L(G) = \dim_{F_q}(L(G)) \log_2 q \le (\deg G + 1 - g(C)) \log_2 q$ by Riemann-Roch theorem, hence the bound for $\theta(X)$. Moreover, the lower bound for $\rho(X)$ follows from the definition and corollary 1.

5. The Hamming parameters. Since the coordinates of the codeword $x(f) \in X(q, C, G)$ are of form

$$x_P(f) = \frac{1}{\sqrt{N}} \eta'(f(P)) \in \{-\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}\},$$

X(q, C, G) is a binary (non linear) code. The following theorem gives the dimension and Hamming minimum distance of X(q, C, G).

Theorem 2. *Suppose that* $N > 2(g(C) - 1 + \deg G)\sqrt{q} + 2 \deg G$. *Then X is a binary non linear code with parameters*

$$\textit{length} = N = = \#C(F_q)$$
$$\textit{minimum distance} = d(X) \ge \frac{N}{2} - ((g(C) - 1 + \deg G)\sqrt{q} + \deg G)$$
$$\textit{dimension} = k(X) \ge (\deg G + 1 - g(C)) \log_2 q.$$

Proof. The statement on the dimension follows from theorem 1 and the remark at the end of section 2, and the statement on the Hamming minimum distance from theorem 1 and the following lemma :

Lemma 1. *If X is a spherical binary code, then*

$$\frac{d(X)}{N} = \frac{\rho(X)}{4}.$$

Proof. It is an easy computation to verify that for $x, y \in X$, we have $\rho(x, y) = \frac{4d(x, y)}{N}$.

6. Open problems.

6.1. It is possible to define some spherical geometric codes on any alphabet : consider a smooth projective irreducible curve C of genus $g(C)$ defined over $\mathbf{F}_q$, G a rational divisor on C prime to $X(\mathbf{F}_q)$, and χ multiplicative character of of order n (so that, n divides q - 1). We can define a reduced order as in § 1 by $v_P'(f) = \underset{g \in K^*}{\text{Min}} (| v_P (fg^n) |)$ and a modified character (which is not a character !)

$$\chi'(f(P)) := \begin{cases} \chi(g(P)) \text{ if } v_P'(f) = v_P(g) = 0 \text{ and } f \equiv g \bmod K^{*2}, \\ 1 \text{ if } v_P'(f) \neq 0. \end{cases}$$

Notes that this is not the same χ' as in [3]. If $N = \#C(\mathbf{F}_q)$ and if Σ_{N-1} is the unit sphere of $\mathbf{C}^N$, let y be the map

$$y : L(G) \to \Sigma_N$$
$$f \to \left(\frac{1}{\sqrt{N}} \chi'(f(P))\right)_{P \in C(\mathbf{F}_q)}$$

What about the parameters of the code $Y(C, G, \chi) := y(L(G))$?

6.2. As in [3], because of the generality of the estimation on character sums we used, one can expect the true parameters of X(q, C, G) to be much greater than the given lower bound in many cases, and to avoid the technical hypothesis of theorems 1 and 2. Here too, numerical computations could give informations, for example, in the case of the code constructed from the space of polynomials of given bounded degree on the projective line.

Bibliography.

[1] Conway, J. H. and Sloane, N. J. A. "Sphere packing, Lattices and Groups", *Springer-Verlag*, New-York, 1988.

[2] Perret, M. *"Multiplicative character sums and Kummer coverings"*, Acta Arithmetica, **59** n°3 (1991), p. 75-86.

[3] Perret, M. *"Multiplicative character sums and non linear geometric codes"*, symposia of Eurocode 90, to appear in Lecture Notes in Computer Sciences, *Springer*.