On The Weights of Irreducible Cyclic Codes

Yves Aubry and Philippe Langevin
G.R.I.M.
Université du Sud Toulon-Var
France
e-mail: {yaubry, langevin}@univ-tln.fr

February 14, 2005

Abstract

The paper is devoted to the study of the weight distribution of irreducible cyclic codes. We start from the interpretation due to McEliece of these weights by means of Gauss sums. Firstly, a p-adic analysis using Stickelberger congruences and Gross-Koblitz formula enable us to improve the divisibility theorem of McEliece by giving results on the multiplicity of the weights. Secondly, in connection with a conjecture of Schmidt and White, we focus on index 2 binary irreducible cyclic codes. We show, assuming the generalized Riemann hypothesis, that there are infinitely many such codes. Furthermore, we consider a subclass of this family of codes, called Quadratic Residue codes. The parameters of these codes are related to class numbers of some imaginary quadratic number fields. We give an elementary proof of the non-existence of two-weight binary irreducible cyclic codes of index 2.

1 Introduction

Very recently, Wolfmann proved that a two-weight binary cyclic code is necessary irreducible (see [Wolf]). On the other hand, it is well known that there exists two infinite class of irreducible cyclic codes with at most two nonzero weights: the subfield codes and the semiprimitive ones. Apart from these two families, 11 exceptional codes have been found by Langevin (see [Lan]) and Schmidt and White (see [S-W]). It has been conjectured in this last paper that this is the whole story. We investigate here this kind of questions.

In the first part of this article, we recall the interpretation due to McEliece of the weights of an irreducible cyclic code by means of linear combinations of Gauss sums. The McEliece theorem on the divisibility of the weights plays a significant role in the study of weight distributions. In particular, Schmidt and White deduce from it a necessary and sufficient condition for an irreducible cyclic code to be a two-weight code.

In the second part, we use the Stickelberger congruences and the Gross-Koblitz formula to obtain two new results that improve the theorem of McEliece. We study the functions that appear in the p-adic expansion of the weight of a codeword. The estimation of their algebraic degree lead us to results on the divisibility concerning the multiplicity of the weights by means of Ax and Katz theorems.

In the last part, we are interested in the conjecture of Schmidt and White on irreducible cyclic codes $c(p, m, v)$. Since they proved that it holds for index 2 codes (conditionally on the Generalized Riemann Hypothesis), we focus our attention on this class of codes. We prove that, conditionally on G.R.H., there are infinitely many index 2 binary irreducible cyclic codes $c(2, m, v)$ with v prime. This result can be seen as an analogue of the Artin conjecture on primitive roots. Thus, this family of codes seems to be interesting in view of the result of Schmidt and White. However, combining a result of Langevin in [Lan] with an upper bound on the class number of imaginary quadratic number fields derived from a result of Louboutin in [Lou], we are enable to prove, and without assuming G.R.H., that there doesn't exist any two-weight index 2 irreducible cyclic code $c(2, m, v)$ with $v > 3$ prime and $v \equiv 3 \pmod 4$.

2 McEliece theorem

Let K be a finite field with p elements, p prime, and L be an extension of K of degree $[L : K] = m$, of order say q. Let n be a divisor of $q - 1$ and write $v = (q - 1)/n$. Let ζ be a primitive n-th root of unity in L. Consider the following map Φ:

$$\begin{array}{rccl} \Phi: & L & \longrightarrow & K^n \\ & a & \longmapsto & \left(Tr_{L/K}(a\zeta^{-i})\right)_{i=0}^{n-1} \end{array}$$

where $Tr_{L/K}$ is the trace of the field L over K. It is easy to see that the image $\Phi(L)$ of L by Φ is an irreducible cyclic code, of length n, denoted $c(p, m, v)$ in [S-W], its dimension is equal to $\mathrm{ord}_n(p)$ the multiplicative order of p modulo n. These are the codes we are interested by. For an element t of L, let us denote by $w(t)$ the weight of $\Phi(t)$. The well known McEliece formula gives the weight of $\Phi(t)$ in term of Gauss sums

$$w(t) = \frac{n(p-1)}{p(q-1)}(q - \sum_{\chi \in \Gamma \setminus \{1\}} \tau_L(\chi)\bar{\chi}(t)) \tag{1}$$

where Γ is the group of characters that are trivial over K^* and ζ, see [S-W]. The Gauss sum $\tau_L(\chi)$ is implicitly defined with respect to the canonical additive character, say μ_L, of L. By definition,

$$\tau_L(\chi) = \sum_{x \in L^*} \chi(x)\mu_L(x).$$

Note that a change of additive character produces a permutation of weights. As in [S-W], let us denote by θ the greatest integer such that, for all non trivial $\chi \in \Gamma$, p^θ divides $\tau_L(\chi)$. The famous Stickelberger theorem (see next section) claims

$$\theta = \frac{1}{p-1} \min_{0<j<v} S(jn)$$

where $S(jn)$ is the sum of the p-digits of jn.

Theorem 1 (McEliece) *All the weights of the irreducible cyclic code* $c(p, m, v)$ *are divisible by* $p^{\theta-1}$. *Moreover, one of them is not divisible by* p^θ.

Sketch of the proof. It suffices to group together the terms of minimal p-adic valuation in (1) to get the first part of the theorem. The second part comes from the independence (modulo p) of the multiplicative characters of L. □

A two-weight code is a code with two nonzero Hamming weights. In order to classify the irreducible cyclic codes, we may assume that v divides $(q-1)/(p-1)$ i.e. n is a multiple of $p-1$. In that case, the order of Γ is $(q-1)/n$ and the McEliece formula appears as the Fourier inversion formula of the map $t \mapsto f(t) = \frac{qz(t)-n}{p-1}$, where $z(t)$ denotes the number of zero components of the codeword $\Phi(t)$. Moreover if G denotes the group of order n in L^*, the map $f(t)$ is defined over the quotient group $V = L^*/G$. Let us set $f := \mathrm{ord}_v(p)$, and since $nv = p^m - 1$, f divides m and we set $m = fs$.

Theorem 2 (Schmidt-White) *The irreducible cyclic code* $c(p, m, v)$ *is a two-weight code if and only if there exists an integer* k *satisfying the three conditions*

(1) k *divides* $v - 1$

(2) $kp^{s\theta} \equiv \pm 1 \pmod{v}$

(3) $k(v - k) = (v - 1)p^{s(f-2\theta)}$

Sketch of the proof. Using Fourier analysis, one can prove that

$$D = \{t \in V \mid p^\theta \text{ divides } w(t)\}$$

is a difference set of order $p^{f-2\theta}$ implying (3). This set or its complementary is a (v, k, λ) difference set satisfying (1) & (2). Surprisingly, the three conditions are sufficient. □

Traditionally, one says that p is semiprimitive modulo v when -1 is in the group generated by p in $(\mathbf{Z}/v\mathbf{Z})^*$. In this case, all the Gauss sums are rationals, $\theta = f/2$, the code $c(p, m, v)$ is a two-weight code with $k = 1$. Each of these assertions characterizes the semiprimitivity.

3 p-adic weight formula

In this section, we p-analyse the function

$$f(t) = \sum_{1 \neq \chi \in \Gamma} \tau_L(\chi)\bar{\chi}(t). \tag{2}$$

The condition $v \mid \frac{q-1}{p-1}$ implies $\Gamma \perp K^*$ whence the algebraic integer $f(t)$ is in fact rational. Let us consider the p-adic expansion of f:

$$f(t) = p^\theta \sum_{i=0}^{+\infty} f_i(t) p^i \tag{3}$$

where each f_i maps L into $\{0, 1, \ldots, p-1\}$ the set of representatives of $\mathbf{F}_p$. In the first part of this section, we use the Stickelberbger's congruences to determine the algebraic degree of f_0. In the second part, we will use the Gross-Koblitz formula to give an upper bound on the degree of f_1.

In what follows, the notations are those of Koblitz [Kob], see also [Kob] for the case $p = 2$. We realize the finite field L as the quotient ring $\mathbf{Z}_p[\xi]/(\pi)$, where ξ is a $(q-1)$-root of unity in an algebraic extension of $\mathbf{Q}_p$ the field of p-adic numbers and π is the root of $X^{p-1} + p$. The Teichmüller character of L, denoted by ω, is the multiplicative character of L defined by the relation

$$\omega(\xi \pmod{\pi}) = \xi.$$

It is important to remark that $t \mapsto \omega(t) \pmod{\pi}$ is nothing but the identity of L^*. The Gross-Koblitz formula claims the existence of an additive character ψ_π such that, for any residue a modulo $q-1$, the following holds:

$$\tau_L(\bar{\omega}^a, \psi_\pi) = \pi^{S(a)} \prod_{j=0}^{f-1} \Gamma_p(1 - \langle \frac{p^j a}{q-1} \rangle) \tag{4}$$

where $S(a) = a_0 + a_1 + \ldots + a_{f-1}$ is the sum of the p-digits of $a = \sum_{i=0}^{f-1} a_i p^i$, $\langle x \rangle$ is the fractional part of x, and Γ_p the p-adic gamma function defined by

$$\forall k \in \mathbf{N}, \quad \Gamma_p(k) = (-1)^k \prod_{j<k,\, p \not| j} j, \qquad \forall s \in \mathbf{Z}_p, \quad \Gamma_p(s) = \lim_{k \to s} \Gamma_p(k).$$

3.1 The function f_0.

The first approximation of the p-adic gamma function:

$$\Gamma_p(1 - \frac{a}{q-1}) \equiv \Gamma_p(1 + a_0) \equiv (-1)^{1+a_0} a_0! \pmod{p}$$

gives the famous Stickelberger's congruences

$$\tau_L(\bar{\omega}^a, \psi_\pi) \equiv R(a)(-1)^{S(a)} \pi^{S(a)} \pmod{p\pi^{S(a)}}$$

where $R(a)$ is essentialy the product of factorials of the digits of a

$$R(a) = (-1)^f \prod_{i=0}^{f-1} a_i!\,.$$

By definition, the parameter θ satisfies $(p-1)\theta = \min_{0<j<v} S(jn)$. We introduce the set

$$J = \{j \mid S(jn) = (p-1)\theta\},$$

so that

$$f_0(t) \equiv \sum_{j \in J} R(jn) t^{jn} \pmod{p}.$$

Using any K-basis of L, the function f_0 becomes a mapping from K^f into K. Since all the exponents jn have a constant p-ary weight equal to θ, the algebraic degree of f_0 is less or equal to θ. The previous theorem of McEliece claims that the weights of an irreducible cyclic code of parameter θ are divisible by $p^{\theta-1}$. The next theorem specifies the multiplicities of the weights.

Theorem 3 *Let $w_0 p^{\theta-1}$ be a weight of an irreducible cyclic code of parameter θ. The number of codewords of weight of the form $w p^{\theta-1}$ with $w \equiv w_0 \pmod p$ is divisible by $p^{\lceil f/\theta \rceil - 1}$.*

Proof. The codeword $\Phi(t)$ has weight $w(t) = w p^{\theta-1}$ with $w \equiv w_0 \pmod p$ if and only if $f_0(t) \equiv w_0 \pmod p$. By Ax theorem (see [Ax]) the number of solutions is divisible by $p^{\lceil f/\theta \rceil - 1}$. □

Example 4 *The weights of the binary* $[23, 11]$ *Golay code are :* 0, 8, 12 *and* 16 *whence $\theta = 3$ and Theorem 3 claims that the number of codewords of weight* 12 *is divisible by* $2^{\lceil 11/3 \rceil - 1} = 8$. *According to [MWS], this number is* 56×89.

Remark 5 *In the case of a two-weight code, the condition (3) of the theorem of Schmidt and White implies a divisibility by a large power of p. It seems very interesting to study the function f_0 by means of the tools exposed in [A-S].*

3.2 The function f_1

All along this subsection, we assume that $p = 2$. The first values of the 2-adic gamma function are: $\Gamma_2(0) = 1$, $\Gamma_2(1) = -1$, $\Gamma_2(2) = +1$, $\Gamma_2(3) = -1$, and $\Gamma_2(4) = 3 \equiv -1 \pmod 4$. In particular,

$$\Gamma_2((1 - \langle \frac{a}{q-1} \rangle) \equiv \Gamma_2(1 + a_0 + a_1 2) \equiv (-1)^{1+a_0+a_0 a_1} \pmod 4$$

and we get the congruence

$$\tau_L(\bar{\omega}^a, \psi) \equiv (-1)^{Q(a)} 2^{S(a)} \pmod{2^{2+S(a)}} \tag{5}$$

where $Q(a) = f + a_0 a_1 + a_1 a_2 + \ldots + a_{f-1} a_0$. To improve our approximation of $f(t)$, we introduce the set $\Upsilon = \{k \in \mathbf{N} \mid 1 \leq k < v, \quad S(kn) = \theta + 1\}$ and the partition $J_\epsilon = \{j \in J \mid Q(jn) \equiv \epsilon \pmod 2\}$. We have

$$f_0(t) + 2 f_1(t) \equiv \sum_{j \in J_0} \omega^{jn}(t) - \sum_{j \in J_1} \omega^{jn}(t) + 2 \sum_{k \in \Upsilon} \omega^{kn}(t) \pmod 4.$$

The Boolean function f_1 depend on the sets Υ and J_1 but also of the "carry function" $g(t)$ corresponding to the relation

$$\sum_{j \in J} \omega^{jn}(t) \equiv f_0(t) + 2 g(t) \pmod 4.$$

By classical 2-adic tricks, we get:

$$\begin{aligned} g(t) &= \frac{1}{2}\Big(\sum_{j \in J} \omega^{jn}(t) - \big(\sum_{j \in J} \omega^{jn}(t)\big)^2 \Big) \\ &\equiv \sum_{j < j'} \omega^{(j+j')n}(t) \pmod 2. \end{aligned}$$

Reducing modulo 2, gluing all pieces together, we get:

$$f_1(t) = \sum_{j < j'} t^{(j+j')n} + \sum_{j \in J_1} t^{jn} + \sum_{k \in \Upsilon} t^{kn}$$

Theorem 6 *Let $w_0\,2^{\theta-1}$ be a weight of a binary irreducible cyclic code. The number of codewords with weight of the form $w\,2^{\theta-1}$ with $w \equiv w_0 \pmod 4$ is divisible by $2^{\lfloor \frac{f-3\theta}{2\theta} \rfloor}$.*

Proof. Let $a + 2b + \cdots$ be the 2-adic decomposition of w_0. The weight of $\Phi(t)$ is of the form $w\,p^{\theta-1}$ if and only if t is a solution of the system

$$f_0(t) = a, \qquad f_1(t) = b.$$

The result is a consequence of the theorem of Katz in [Kat] since the algebraic degrees of f_0 and f_1 are respectively less or equal to θ and 2θ. □

Example 7 *A sufficient condition to obtain a non trivial result is $n > 1$ and $5\theta < f$. The first instance is the $[11, 10]$-code ($v = 93$, $\theta = 2$), and the second is the $[6765, 20]$-code ($v = 155$, $\theta = 4$).*

4 Binary Irreducible Cyclic Codes

4.1 Primes which generate squares and index 2 codes

Is there infinitely many primes p such that 2 generates the squares modulo p ? Before answering this question, recall that the Artin conjecture asserts that 2 is a primitive root for infinitely many primes (the conjecture is proved by Hooley assuming the Generalized Riemann Hypothesis). In other words, there is infinitely many primes p such that the order of 2 modulo p is equal to $p - 1$.

We consider here an analogue question : is there infinitely many primes p such that 2 generates exactly the squares modulo p ? We can give an another formulation of this question : is there infinitely many primes p such that the order of 2 modulo p is equal to $\frac{p-1}{2}$ or equivalently such that 2 has index 2 modulo p ? Indeed, it is equivalent since the group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic and since the subgroup of squares has index 2 (p odd).

Consider the set

$$H(x) := \sharp\{p \leq x \mid p \text{ prime and } \operatorname{ord}_p(2) = \frac{p-1}{2}\}.$$

Murata has proved (see [Mur]) that G.R.H. implies that for every $\varepsilon > 0$,

$$H(x) = \frac{3}{8}\delta\pi(x) + O\Big(\frac{2^{\varepsilon} x \log\log x}{\log^2 x}\Big),$$

where

$$\delta = \prod_{\ell \text{ prime}} \Big(1 - \frac{1}{\ell(\ell-1)}\Big)$$

is the Artin constant.

Then, under G.R.H., we can conclude positively to our question: there is infinitely many primes p such that 2 has index 2 modulo p.

Recall that a code $c(p, m, v)$ is said to have index 2 if the multiplicative order of p modulo v is equal to $\varphi(v)/2$, where φ is the Euler function. In particular, we have shown that:

Proposition 8 *Conditionally on G.R.H., there are infinitely many index 2 binary irreducible cyclic codes $c(2, m, v)$ with v prime.*

Remark 9 *Recall that an index 2 binary irreducible cyclic codes $c(2, m, v)$ with v prime has at most three different nonzero weights. Thus, this codes are good candidates to be two-weight codes. By the way, we can state that, conditionally on G.R.H., there are infinitely many binary codes with at most three different nonzero weights.*

4.2 The residue quadratic case

For the study of a special class of three-weight codes, Langevin in [Lan] introduced more restrictive conditions on our integer v which lead us to the quadratic residue case for v, namely the index 2 case with the additional conditions that v is an odd prime greater than 3 with $v \equiv 3 \pmod 4$. In other words, the integer v satisfies the QR-case if:

(i) v is a prime greater than 3,

(ii) $\mathrm{ord}_v(p) = \frac{v-1}{2}$,

(iii) $v \equiv 3 \pmod 4$.

This case is of particular interest because of an explicit relation between the class number h of the imaginary quadratic number field $\mathbf{Q}(\sqrt{-v})$ and the Gauss sums (see [Lan]).

An irreducible cyclic $c(p, m, v)$-code with v satisfying the QR-conditions is called a QR-code. Recall that for such a code, the order of p modulo v divides m and the quotient is denoted by s (see section 2). We have:

Theorem 10 *There does not exist two-weight binary QR-code.*

Proof. By theorem 3.3 of [Lan], we know that the code $c(p, m, v)$ has at most two weights if and only if

$$\frac{v+1}{4} = p^{hs}. \tag{6}$$

The previous relation implies that:

$$4p^{hs} \equiv 1 \pmod v.$$

If $p = 2$, we have that p^{hs+2} is 1 modulo v, which implies that the order of p modulo v divides $hs + 2$. But, by hypothesis, we have $\mathrm{ord}_v(p) = (v - 1)/2$. Then, taking the logarithm in (6), we have the inequalities:

$$\frac{v-1}{2} \leq hs + 2 = \log(\frac{v+1}{4}) + 2. \tag{7}$$

implying $v = 7$.

$\square$

References

[A-S] A. Adolphson and S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley-Warning, *Ann. scient. Éc. Norm. Sup.*, t.20 , (1987) pp. 545–556.

[Ax] J. Ax, Zeroes of polynomial over finite fields, *Amer. J. Math.*, Vol. 86, (1964), pp 255–261.

[Kat] N. Katz, On a theorem of Ax, *Amer. J.Math.*, Vol.93, (1971), pp 485–499.

[Kob] N. Koblitz, p-adic Analysis: a Short Course on Recent Work, *LMS*, LNS-46, 1980.

[Lan] Ph. Langevin, A new class of two weight codes, *Finite field and their applications, Glasgow 1995, London Math. Soc.* Lecture Note Ser. 233, 181-187 (1996).

[Lang] S. Lang, Cyclotomic Fields I and II, *Springer-Verlag*, GTM-121, 1990.

[Lou] S. Louboutin, Majorations explicites de $|L(1, \chi)|$ (suite), *C. R. Acad. Sci. Paris*, t. 323, Série I, p. 443-446, 1996.

[Mur] L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, *Arch. Math.* **57** (1991), 555–565.

[S-W] B. Schmidt and C. White, All two-weight irreducible cyclic codes ?, *Finite Fields and Their Applications* **8** (2002), 1-17.

[MWS] J. MacWilliams and J. Seery, The weight distributions of some minimal cyclics codes, *IEEE transactions on information theory* , IT-27:6, (1981).

[Wolf] J. Wolfmann, Are two-weight projective cyclic codes irreducible ? *IEEE transactions on information theory*, to appear.