On The Weights of Binary Irreducible Cyclic Codes

Yves Aubry and Philippe Langevin

Université du Sud Toulon-Var, Laboratoire GRIM F-83270 La Garde, France,
{langevin,yaubry}@univ-tln.fr,
WWW home page: http://{langevin,yaubry}.univ-tln.fr

Abstract. This paper is devoted to the study of the weights of binary irreducible cyclic codes. We start from McEliece's interpretation of these weights by means of Gauss sums. Firstly, a dyadic analysis, using the Stickelberger congruences and the Gross-Koblitz formula, enables us to improve McEliece's divisibility theorem by giving results on the multiplicity of the weights. Secondly, in connection with a Schmidt and White's conjecture, we focus on binary irreducible cyclic codes of *index two*. We show, assuming the generalized Riemann hypothesis, that there are an infinite of such codes. Furthermore, we consider a subclass of this family of codes satisfying the quadratic residue conditions. The parameters of these codes are related to the class number of some imaginary quadratic number fields. We prove the non existence of such codes which provide us a very elementary proof, without assuming G.R.H, that any two-weight binary irreducible cyclic code $c(m, v)$ of index two with v prime greater that three is semiprimitive.

1 Introduction

In a recent paper [9], Wolfmann has proved that a two-weight binary cyclic code is necessarily irreducible. On the other hand, it is well-known that there exist two infinite classes 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 [4]) and, Schmidt and White (see [6]). It has been conjectured in the later paper that this is the whole story. This question is investigated in this paper in the case of the characteristic two.

In the first part of this article, we recall the McEliece interpretation of the weights of an irreducible cyclic code by means of linear combinations of Gauss sums. McEliece's divisibility theorem plays a significant role in the study of weight distributions of irreducible cyclic codes. In particular, Schmidt and White deduce 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 McEliece's theorem. We study the Boolean functions that appear in the dyadic expansion of the weight of a codeword. The estimation of their algebraic degree leads us to results on the divisibility concerning multiplicities by means of Ax's and Katz's theorems.

In the last part, we are interested in Schmidt and White's conjecture on irreducible cyclic $c(m,v)$ codes. Since they proved that it holds for codes of index two (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 an infinity of binary irreducible cyclic $c(m,v)$ codes of index two 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 Schmidt and White's result. Then, we use a result of Langevin in [4] to prove that there does not exist any two-weight irreducible cyclic $c(m,v)$ code of index two with $v > 3$ prime and $v \equiv 3 \pmod 4$. This provides us an elementary proof, without assuming G.R.H, of a particular instance of the Schmidt and White conjecture, namely that any two-weight binary irreducible cyclic $c(m,v)$ code of index two with v prime greater that 3 is semiprimitive.

2 McEliece's theorem

Let L be a finite field of order $q = 2^m$. 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:

$$\begin{aligned} \Phi : L &\longrightarrow \mathbf{F}_2^n \\ a &\longmapsto \left(\mathrm{Tr}_{L/\mathbf{F}_2}(a\zeta^{-i})\right)_{i=0}^{n-1} \end{aligned}$$

where $\mathrm{Tr}_{L/\mathbf{F}_2}$ is the trace of the field L over $\mathbf{F}_2$. The image $\Phi(L)$ of L by Φ is an irreducible cyclic code of length n, denoted $c(m,v)$, see [6] for the material about these codes. Its dimension is equal to the multiplicative order of 2 modulo n, denoted $\mathrm{ord}_n(2)$. Any binary irreducible cyclic code can be viewed as a $c(m,v)$ code, so let us consider such codes. 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

$$w(t) = \frac{n}{2(q-1)}\left(q + \sum_{\chi \in \Gamma\setminus\{1\}} \tau_L(\chi)\bar{\chi}(t)\right) \tag{1}$$

where Γ is the subgroup of multiplicative characters of L^* that are orthogonal to ζ, see [6]. 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 [6], let us denote by θ the greatest integer such that, for all non trivial $\chi \in \Gamma$, 2^θ divides $\tau_L(\chi)$. The famous Stickelberger theorem (see next section) claims

$$\theta = \min_{0<j<v} S(jn)$$

where $S(k)$ denotes the sum of the bits in the binary expansion of the natural integer k.

Theorem 1 (McEliece). *All the weights of the irreducible cyclic code $c(m,v)$ are divisible by $2^{\theta-1}$. Moreover, one of them is not divisible by 2^{θ}.*

Sketch of the proof. It suffices to group together the terms of minimal 2-adic valuation in (1) to get the first part of the theorem. The second part comes from the independence (modulo 2) of the multiplicative characters of L. $\square$

A two-weight code is a code with two nonzero Hamming weights. The McEliece formula appears as the Fourier inversion formula of the map $t \mapsto f(t) = qz(t) - n$, 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 $f := \mathrm{ord}_v(2)$, and since $nv = 2^m - 1$, f divides m and we set $m = fs$.

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

(i) k *divides* $v-1$
(ii) $k2^{s\theta} \equiv \pm 1 \pmod{v}$
(iii) $k(v-k) = (v-1)2^{s(f-2\theta)}$

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

$$D = \{t \in V \mid 2^{\theta} \text{ divides } w(t)\}$$

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

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

3 Dyadic weight formula

In this section, we analyse dyadicaly the function

$$f(t) = \sum_{1 \neq \chi \in \Gamma} \tau_L(\chi)\bar{\chi}(t) = 2^{\theta} \sum_{i=0}^{+\infty} f_i(t) 2^i \tag{2}$$

where the f_i are Boolean functions i.e. map L into $\{0,1\}$. By definition, see [7], the degree of a Boolean function f defined over a $\mathbf{F}_2$-space E of dimension m is equal to the smallest degree of a polynomial $p \in \mathbf{F}_2[X_1, X_2, \ldots, X_m]$ such that

$\forall (x_1, x_2, \ldots, x_m) \in \mathbf{F}_2^m$

$$p(x_1, x_2, \ldots, x_m) \equiv f(x_1\beta_1 + x_2\beta_2 + \cdots + x_m\beta_m) \pmod 2,$$

where $(\beta_1, \beta_2, \ldots, \beta_m)$ is any basis of L considered has a vector space over $\mathbf{F}_2$.

In the first part of this section, we use the Stickelberger'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. For this, we realize the finite field L as the quotient ring $\mathbf{Z}_2[\xi]/(2)$, where ξ is a $(q-1)$-root of unity in an algebraic extension of $\mathbf{Q}_2$ the field of 2-adic numbers. The Teichmüller character of L, denoted by ω, is the multiplicative character of L defined by the relation

$$\omega(\xi \pmod 2) = \xi.$$

It is important to remark that $t \mapsto \omega(t) \pmod 2$ is nothing but the identity of L^*. The Gross-Koblitz formula below (see [3]) claims the existence of an additive character ψ such that, for any residue a modulo $q-1$, the following holds:

$$\tau_L(\bar{\omega}^a, \psi) = (-2)^{S(a)} \prod_{j=0}^{f-1} \Gamma_2\big(1 - \langle \frac{2^j a}{q-1} \rangle\big) \tag{3}$$

where $S(a) = a_0 + a_1 + \ldots + a_{f-1}$ is the sum of the bits of $a = \sum_{i=0}^{f-1} a_i 2^i$, $\langle x \rangle$ is the fractional part of x, and Γ_p the 2-adic gamma function defined by

$$\forall k \in \mathbf{N}, \quad \Gamma_2(k) = (-1)^k \prod_{j<k,\, 2 \nmid j} j, \qquad \forall s \in \mathbf{Z}_2, \quad \Gamma_2(s) = \lim_{k \to s} \Gamma_2(k).$$

3.1 The function f_0.

The first approximation of the 2-adic gamma function gives the famous Stickelberger's congruences

$$\tau_L(\bar{\omega}^a, \psi) \equiv 2^{S(a)} \pmod{2^{1+S(a)}}.$$

We introduce the set

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

so that

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

Using any $\mathbf{F}_2$-basis of L, the function f_0 becomes a mapping from $\mathbf{F}_2^f$ into $\mathbf{F}_2$. Since all the exponents jn have a constant 2-ary weight equal to θ, the algebraic degree of f_0 is less or equal to θ. The previous McEliece theorem claims that the weights are divisible by $2^{\theta-1}$. The next result gives precisions concerning the multiplicities of the weights. Let us recall that by Ax's theorem (see [1]), for any polynomial $f \in \mathbf{F}_2[X_1, X_2, \ldots, X_m]$ of degree k, the number of solutions in $\mathbf{F}_2^m$ of the equation :

$$f(x_1, x_2, \ldots, x_m) = 0$$

is divisible by $2^{\lceil \frac{m}{k} \rceil - 1}$ where $\lceil r \rceil$ denotes the smallest integer greater or equal to r.

Theorem 3. *The number of codewords of weight of dyadic valuation $\theta - 1$ is divisible by $2^{\lceil f/\theta \rceil - 1}$.*

Proof. The weight of $\Phi(t)$ has valuation $\theta - 1$ if and only if $f_0(t) = 1$. By Ax's theorem the number of solutions is divisible by $2^{\lceil f/\theta \rceil - 1}$ since the degree of the Boolean function f_0 is less or equal to θ.

Example 1. The weights of the binary $[23, 11]$ (subcode of the 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 [8], this number is $56 \times 23 = 8 \times 161$.

Remark 1. 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 2. It seems very interesting to study more precisely the function f_0.

3.2 The function f_1

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,

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

and we get the congruence

$$\tau_L(\bar{\omega}^a, \psi) \equiv (-1)^{Q(a)} 2^{S(a)} \pmod{2^{2+S(a)}} \tag{4}$$

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 $K = \{k \in \mathbf{N} \mid 1 \leq k < v, \quad S(kn) = \theta + 1\}$ and the partition $J_\epsilon = \{j \in J \mid Q(jn) \equiv \epsilon \pmod 2\}$. We have

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

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

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

By classical 2-adic tricks, we get:

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

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

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

Let us recall that Katz's divisibility theorem (see [2]) implies that for any pair of polynomials f_1 and $f_2 \in \mathbf{F}_2[X_1, X_2, \ldots, X_m]$ of degree $k_1 \leq k_2$, the number of solutions in $\mathbf{F}_2^m$ of the system of equations :

$$\begin{cases} f_1(x_1, x_2, \ldots, x_m) = 0 \\ f_2(x_1, x_2, \ldots, x_m) = 0 \end{cases}$$

is divisible by $2^{\lfloor \frac{m-k_1-k_2}{k_2} \rfloor}$ where $\lfloor r \rfloor$ denotes the largest integer smaller or equal to r.

Theorem 4. *Let w_0 be an integer. 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 $w\,2^{\theta-1}$ 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 above Katz divisibility theorem since the algebraic degrees of f_0 and f_1 are respectively less or equal to θ and 2θ.

Example 2. 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 one is the $[6765, 20]$-code ($n = 6765$, $v = 155$, $\theta = 4$). According to [8], the weight distribution is given by Tab. (1). All the weight are divisible by 8, and the number A_w of codewords of weight w satisfy:

$$\sum_{w\equiv 0 \pmod 4} A_w = 1 + 25n \qquad \equiv 0 \mod 2,$$
$$\sum_{w\equiv 1 \pmod 4} A_w = (5 + 45)n \qquad \equiv 0 \mod 2,$$
$$\sum_{w\equiv 2 \pmod 4} A_w = (5 + 20 + 20 + 5)n \qquad \equiv 0 \mod 2,$$
$$\sum_{w\equiv 3 \pmod 4} A_w = (4 + 25 + 1)n \qquad \equiv 0 \mod 2.$$

Table 1. Weight distribution of the [6765, 20] irreducible cyclic code. The number of codewords of weight w is equal to $\mu \times n$, $\bar{w}$ denotes the congruence of $\frac{w}{8}$ modulo 4.

w	3272	3280	3320	3352	3376	3392	3400	3408	3448	3504
$\bar{w}$	1	2	3	3	2	0	1	2	3	2
μ	5	5	4	25	20	25	45	20	1	5

4 Two-weight Binary Irreducible Cyclic Codes

4.1 Primes which generate squares and index 2 codes

Is there infinitely many primes v such that 2 generates the squares modulo v ? 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 v such that the order of 2 modulo v is equal to $v-1$.

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

For a positive integer x, let $H(x)$ be the cardinality of the set

$$\{v \leq x \mid v \text{ prime and } \operatorname{ord}_v(2) = \frac{v-1}{2}\}.$$

Murata has proved (see [5]) 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 use the previous result of Murata to conclude positively to our question: there is infinitely many primes v such that 2 has index 2 modulo v.

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

Proposition 1. *Conditionally on G.R.H., there are infinitely many index 2 binary irreducible cyclic codes $c(m, v)$ with v prime.*

Remark 2. Recall that an index 2 binary irreducible cyclic codes $c(m,v)$ with v prime has at most three different nonzero weights. Thus, these 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 cyclic codes with at most three different nonzero weights.

4.2 The residue quadratic case and the semiprimitivity

For the study of a special class of three-weight codes, Langevin in [4] 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 quadratic residue conditions if:

(i) v is a prime greater than 3,
(ii) $\mathrm{ord}_v(2) = \frac{v-1}{2}$,
(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 [4]).

Proposition 2. *There does not exist a two-weight binary irreducible cyclic code satisfying the quadratic residue conditions.*

Proof. Let s be the integer introduced in the section (2). By theorem 3.3 of [4], we know that the code $c(m,v)$ has at most two weights if and only if

$$\frac{v+1}{4} = 2^{hs}. \tag{5}$$

The previous relation implies that:

$$2^{hs+2} \equiv 1 \pmod v.$$

This implies that the order of 2 modulo v divides $hs+2$. But, by hypothesis, we have $\mathrm{ord}_v(2) = (v-1)/2$. Then, taking the logarithm in (5), we have the inequalities:

$$\frac{v-1}{2} \le hs + 2 = \log(\frac{v+1}{4}) + 2 \tag{6}$$

implying $v = 7$. But this leads to a code with only one nonzero weight: the proposition follows.

The conjecture of Schmidt and White in even characteristic states that an irreducible cyclic code $c(m,v)$ is a two-weight code if and only if it is a semiprimitive code. They proved it, conditionally on G.R.H. for all index 2 codes. We can now prove it also for all index 2 codes with v prime greater than 3 but without assuming G.R.H.:

Theorem 5. *A binary irreducible cyclic code $c(m, v)$ of index 2 with v prime greater than 3 is a two-weight code if and only if it is a semiprimitive code.*

Proof. The odd prime v is congruent to 1 or 3 modulo 4. The last congruence comes to the quadratic residue case and the previous proposition implies that the code has three weights. The first congruence $v \equiv 1 \pmod 4$ implies that -1 is a square modulo v and thus is a power of 2 modulo v since 2 has index 2 modulo v and then generates the squares. Thus, the code is semiprimitive.

The converse is a well-known result: the semiprimitivity implies that the code has two weights.

References

1. J. Ax, Zeroes of polynomial over finite fields, *Amer. J. Math.*, Vol. 86, (1964), pp 255–261.
2. N. Katz, On a theorem of Ax, *Amer. J. Math.*, Vol.93, (1971), pp 485–499.
3. N. Koblitz, p-adic Analysis: a Short Course on Recent Work, *LMS*, LNS-46, 1980.
4. Ph. Langevin, A new class of two weight codes, *Finite Fields and Their Applications, Glasgow 1995, London Math. Soc.* Lecture Note Ser. 233, 181-187 (1996).
5. L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, *Arch. Math.* **57** (1991), 555–565.
6. B. Schmidt and C. White, All two-weight irreducible cyclic codes ?, *Finite Fields and Their Applications* **8** (2002), 1-17.
7. F.J. MacWilliams and N.J.A. Sloane. The Theory of Error-Correcting Codes, Elsevier Science Publisher, 1991.
8. J. MacWilliams and J. Seery, The weight distributions of some minimal cyclics codes, *IEEE transactions on information theory* , IT-27:6, (1981).
9. J. Wolfmann, Are 2-weight projective cyclic codes irreducible ? *IEEE transactions on information theory*, Vol. **51**, N. 2 (2005), 733-737.