On the semiprimity of cyclic codes
Yves Aubry, Philippe Langevin

To cite this version:
ON THE SEMIPRIMITIVITY OF CYCLIC CODES

YVES AUBRY AND PHILIPPE LANGEVIN

Abstract. We prove, without assuming the Generalized Riemann Hypothesis, but with at most one exception, that an irreducible cyclic code $c(p, m, v)$ with $v$ prime and $p$ of index 2 modulo $v$ is a two-weight code if and only if it is a semiprimitive code or it is one of the six sporadic known codes. The result is proved without any exception for index-two irreducible cyclic $c(p, m, v)$ codes with $v$ prime not congruent to 3 modulo 8. Finally, we prove that these two results hold true in fact for irreducible cyclic code $c(p, m, v)$ such that there is three $p$-cyclotomic cosets modulo $v$.

1. Introduction

Irreducible cyclic codes are extensively studied in the literature. They can be defined by three parameters $p$, $m$ and $v$ and are denoted $c(p, m, v)$ (see section 2 for a precise definition). Such codes with only few different (Hamming) weights are highly appreciated, especially those with exactly two non-zero weights, called two-weight codes. The classification of two-weight codes is a classical problem in coding theory (see [3]); it is still an open problem but recent progress has been made. An infinite family, namely the semiprimitive codes (i.e. when $-1$ is a power of $p$ modulo $v$), and eleven sporadic examples are known. Schmidt and White in [9] provided evidence to conjecture that this is the whole story:

Conjecture 1. An irreducible cyclic code $c(p, m, v)$ is a two-weight code if and only if it is a semiprimitive code or it is one of the eleven sporadic known codes.

They proved their conjecture, conditional on the Generalized Riemann Hypothesis (G.R.H.), for index-two codes, that is when $p$ has index 2 modulo $v$. Note that semiprimitive codes have two non-zero weights and thus only the “only if” part had to be proved.

We considered in [1] the conjecture in the binary case and we proved it in a particular case without assuming G.R.H.. Our main result here is a proof of this conjecture without assuming G.R.H. but with at most one exception in the case where $p$ has index 2 and $v$ is prime. We prove before, using near-primitive root densities and conditionally on G.R.H., that for any prime number $p$ there are infinitely many such codes namely index-two irreducible cyclic codes $c(p, m, v)$ with $v$ prime.
We prove the conjecture without any exception (and without assuming G.R.H.) in the case where \( p \) has index 2 and \( v \) is a prime not congruent to 3 modulo 8. Finally, we remark that the results hold true in fact for irreducible cyclic codes \( c(p, m, v) \) with \( v \) an integer such that there is three \( p \)-cyclotomic cosets modulo \( v \).

2. IRREDUCIBLE CYCLIC CODES AND McELIECE WEIGHT-FORMULA

Let us introduce irreducible cyclic codes over a prime finite field (indeed, it is enough for our purpose, namely the classification of two-weight irreducible cyclic codes, to consider such codes over prime fields, as remarked in [9]).

Let \( p \) be a prime number and consider the finite field \( K \) with \( p \) elements. Let \( L \) be the extension of degree \( m \) of \( K \), consider a divisor \( n \) of \( p^m - 1 \) and write \( v = (p^m - 1)/n \) (thus \( v \) and \( p \) are coprime). Let \( \zeta \) be a primitive \( n \)-th root of unity in \( L \) (i.e. \( \zeta \) is a generator of the cyclic subgroup of order \( n \) of the multiplicative group \( L^* \)). We define the \( c(p, m, v) \) code to be the image of the following map \( \Phi_m \):

\[
\Phi_m : \quad L \rightarrow K^n
\]

\[
t \mapsto (\text{Tr}_{L/K}(t \zeta^{-i}))_{i=0}^{n-1}
\]

where \( \text{Tr}_{L/K} \) is the trace of the field \( L \) over \( K \).

It is a code of length \( n \) and dimension \( \text{ord}_n(p) \), the multiplicative order of \( p \) modulo \( n \). Every irreducible cyclic code over \( K \) can be viewed as a \( c(p, m, v) \) code (see [9]), so we can take \( c(p, m, v) \) as the definition of irreducible cyclic codes over \( K \) of length \( n \). The \( c(p, m, v) \) codes are known to be projective or saturated according to whether \( \gcd(n, p - 1) = 1 \) or \( \gcd(n, p - 1) = p - 1 \). As remarked in [9], we may assume the saturated situation.

Now we are interested in the weight \( w(t) \) of a codeword \( \Phi_m(t) \) of such a code, for \( t \in L^* \). Let \( \chi \) be a character of the multiplicative group \( L^* \) and let

\[
\tau_L(\chi) = -\sum_{x \in L^*} \chi(x)e^{2\pi i \text{Tr}_{L/K}(x)}
\]

be the Gauss sum associated with \( \chi \).

Let \( V \) be the subgroup of \( L^* \) of index \( v \) and let \( \Gamma \) be the subgroup of characters of \( L^* \) which are trivial both on \( V \) and \( K^* \). Note that the order of \( \Gamma \) is equal to \( v \gcd(n, p - 1)/(p - 1) \) which is just equal to \( v \) in the saturated situation. We have the following McEliece formula:

**Proposition 2.** For any \( t \in L^* \), the weight \( w(t) \) of the codeword \( \Phi_m(t) \) is given by:

\[
w(t) = \frac{p - 1}{pv} \left(p^m + \sum_{\chi \in \Gamma \setminus \{1\}} \tau_L(\chi) \bar{\chi}(t)\right).
\]

And, conversely by Fourier inversion
\begin{equation}
\tau_L(\chi) = \frac{p}{p-1} \sum_{t \in L^*/V} w(t) \chi(t).
\end{equation}

One says that $p$ is semiprimitive modulo $v$ when $-1$ is in the group generated by $p$ in $(\mathbb{Z}/v\mathbb{Z})^*$, i.e. when $\text{ord}_v(p)$ is even. Note that in this case all the Gauss sums are rational and a $c(p, m, v)$ code is a two-weight code. In the paper we investigate the reciprocal: besides some sporadic known examples, is any two-weight irreducible cyclic code semiprimitive?

3. The case $v$ small

Before going further let us treat the case where $v$ is small, i.e. $v = 2$ or 3. We know that a $c(p, m, 2)$ code is a two-weight code, and that the weights can be expressed in term of quadratic Gauss sum (see [7]). In the same way, the weights of a $c(p, m, 3)$ code can be expressed by means of cubic Gauss sums. However, it is hard to give the exact values of the cubic Gauss sums (see [6]), and thus also the weights of such a code. Nevertheless, we have the following characterization:

Proposition 3. A $c(p, m, 3)$ code has two weights if and only if it is semiprimitive (that is here, if and only if $p \equiv 2 \mod 3$).

Proof. Let $\chi$ be a multiplicative character of $L$ of order 3. The number of weights of a $c(p, m, 3)$ code is equal to the number of distincts values taken by the mapping:

$$L^* \ni t \mapsto f(t) = \tau_L(\chi)(t) + \tau_L(\bar{\chi})(t).$$

Let $1 \neq j$ be a cubic root of unity. Let $t$ be such that $\chi(t) = j$. It is easy to see that $f(1) = f(t)$ implies $\tau_L(\chi) = j\tau_L(\bar{\chi})$, that $f(t) = f(t^2)$ implies $\tau_L(\chi) = \tau_L(\bar{\chi})$ and that $f(1) = f(t^2)$ implies $\tau_L(\bar{\chi}) = j^2\tau_L(\chi)$. Therefore, the code has two weights if and only if there exists a cubic root of unity $\omega$ such that

\begin{equation}
\tau_L(\bar{\chi}) = \omega \tau_L(\chi).
\end{equation}

In particular, since $\tau_L(\chi)^3$ is an algebraic integer of degree 2 and norm $p^{3m}$, we deduce that $\tau_L(\chi)^6 = \tau_L(\bar{\chi})^6 = p^{6m}$. Hence the Gauss sums $\tau_L(\chi)$ are pure Gauss sums (see [7] for a definition of a pure Gauss sum). It follows by a theorem of Baumert, Mills and Ward (see Theorem 11.6.4 of [7] for example) that $p$ is semiprimitive modulo 3. \hfill \Box

4. Infinitely many index-two $c(p, m, v)$ codes with $v$ prime

For the study of $c(p, m, v)$ codes with $v$ prime and $p$ of index two modulo $v$, we are interested in primitive and near-primitive root densities.
In 1927, Emil Artin made the following conjecture (called now the Artin’s primitive root conjecture): for any integer $\alpha \neq \pm 1$ not a square, the natural density

$$\lim_{x \to +\infty} \frac{\#\{v \text{ prime } | \ v \leq x \text{ and } \alpha \text{ generates } \mathbb{F}_v^*\}}{\#\{v \text{ prime } | \ v \leq x\}}$$

exists and is positive. In 1967, Hooley proved this conjecture under the assumption of G.R.H.. In particular, he proved that if $\alpha$ is neither $\pm 1$ nor a perfect square, then there are infinitely many primes $v$ for which $\alpha$ is a primitive root modulo $v$.

If we ask $\alpha$ to generate only the squares of $\mathbb{F}_v^*$ and not the whole group $\mathbb{F}_v^*$, i.e. to have index 2 and not index 1 modulo $v$, we come to the notion of near-primitive roots. Precisely, fix $\alpha \neq \pm 1$ not a perfect power and let $v$ be a prime and $t$ be an integer such that $v \equiv 1 \pmod{t}$. Consider

$$N_{\alpha,t}(x) = \#\{v \text{ prime } | \ v \leq x \text{ and } v \nmid \alpha \text{ and } \text{ind}_v(\alpha) = t\}.$$ 

Notice that for $t = 1$ this quantity is just the previous one studied by Artin and Hooley. In 2000, Moree introduced in [8] a weighting function depending on $\alpha$ and $t$ and gave an estimation of $N_{\alpha,t}(x)$ assuming G.R.H.. In particular, for $\alpha = p$ a prime number and $t = 2$, he proved that

$$N_{p,2}(x) = \sum_{v \text{ odd prime } v \leq x} \frac{\varphi\left(\frac{v-1}{2}\right)}{v-1} + O\left(\frac{x \log \log x}{\log^2 x}\right).$$

This implies that there exist infinitely many primes $v$ such that $p$ has index 2 modulo $v$.

In particular, we have:

**Proposition 4.** Conditionally on G.R.H., for any prime number $p$ there are infinitely many index-two irreducible cyclic codes $c(p, m, v)$ with $v$ prime.

5. Necessary conditions on two-weight codes

The irreducible cyclic codes $c(p, m, v)$, with $v$ a prime number and with $p$ of index 2 modulo $v$, range in two families: the first one with $v \equiv 1 \pmod{4}$ and the second one with $v \equiv 3 \pmod{4}$. If $v \equiv 1 \pmod{4}$, then $-1$ is a square modulo $v$ and since $p$ generates the squares modulo $v$, we are reduced to the semiprimitive case. This lead us to consider the second case, where $-1$ is not a square modulo $v$. Moreover, in view of Proposition 3, we can suppose that $v$ is greater than 3.

Hence, let us consider a prime number $p$ and an integer $v$ satisfying the following (2) conditions:

(a) $v$ is a prime greater than 3,
(b) $\text{ord}_v(p) = (v-1)/2$ i.e. $p$ has index 2 modulo $v$,
(c) $v \equiv 3 \pmod{4}$.
Let $f$ be the multiplicative order of $p$ modulo $v$. Note that $f$ divides $m$, and we set $s = m/f$. It is shown in [4] that if a $c(p, m, v)$ code with $v$ satisfying the $(\sharp)$ conditions has two weights then:

\begin{equation}
\frac{v + 1}{4} = p^{hs}.
\end{equation}

We give, now, a more precise result:

**Theorem 5.** If a $c(p, m, v)$ code with $v$ satisfying the $(\sharp)$ conditions is a two-weight code then we have:

$$m = \text{ord}_v(p).$$

**Proof.** Since $p$ has index 2 modulo $v$, then $p$ is a square modulo $v$, and $(p) = PP'$ splits in the extension $\mathbb{Q}(\sqrt{-v})/\mathbb{Q}$. We have that the norm

$$N_{\mathbb{Q}(\sqrt{-v})/\mathbb{Q}}(P) = p$$

and that $P^h = (\alpha)$ is a principal ideal (since $h$ is the ideal class number of $\mathbb{Q}(\sqrt{-v})$, with $\alpha = (a + b\sqrt{-v})/2$ (with $a, b \in \mathbb{Z}$) an algebraic integer of $\mathbb{Q}(\sqrt{-v})$. Taking norms, we obtain $p^h = (a^2 + bv^2)/4$ and since $a$ and $b$ cannot be zero in this situation, we conclude that

$$\frac{v + 1}{4} \leq p^h.$$

But by (5) a $c(p, m, v)$ code with $v$ satisfying the $(\sharp)$ conditions has two weights if and only if

\begin{equation}
\frac{v + 1}{4} = p^{hs}.
\end{equation}

Thus, $p^{hs} \leq p^h$ and $s = 1$. \qed

Then, the previously defined parameter $s$ appearing in [4] and [9] is equal to 1 under the $(\sharp)$ conditions. In particular, we have:

**Corollary 6.** If a $c(p, m, v)$ code with $v$ satisfying the $(\sharp)$ conditions is a two-weight code then

\begin{equation}
\frac{v + 1}{4} = p^h.
\end{equation}

where $h$ is the class number of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-v})$. In particular, such a code is completely defined by the parameter $v$.

Furthermore, we have the following necessary condition on $p$ for two-weight $c(p, m, v)$ code with $v$ satisfying the $(\sharp)$ conditions:

**Corollary 7.** If a $c(p, m, v)$ code with $v$ satisfying the $(\sharp)$ conditions has two weights, then $p$ is the least prime which totally splits in the extension $\mathbb{Q}(\sqrt{-v})/\mathbb{Q}$, i.e. $p$ is the least prime which is a square modulo $v$. 
Proof. Indeed, if \( \ell \) is a prime which totally splits in \( \mathbb{Q}(\sqrt{-v})/\mathbb{Q} \), then the previous proof implies that \( \ell^h \geq \frac{v+1}{4} = p^h \) which gives \( \ell \geq p \). \( \square \)

6. Main results

Using the previous section, we can state the following result which can also be derived from the proof of lemma 4.1. of [4].

**Theorem 8.** There is no two-weight \( c(p, m, v) \) code with \( v \) satisfying the \((\sharp)\) conditions and with \( v \equiv 7 \pmod{8} \). Hence, Conjecture 1 holds true for index-two irreducible cyclic \( c(p, m, v) \) codes with \( v \) a prime not congruent to 3 modulo 8.

*Proof.* Since \( v \equiv 7 \pmod{8} \), it follows that 2 is a square modulo \( v \), and the ideal \((2)\) splits in the extension \( \mathbb{Q}(\sqrt{-v})/\mathbb{Q} \). By Corollary 7, we conclude that \( p = 2 \). But we proved in [1] that there exists no two-weight binary \( c(p, m, v) \) code with \( v \) satisfying the \((\sharp)\) conditions, so we get the non-existence of such codes. Hence, this proves the conjecture since the case \( v \equiv 1 \pmod{4} \) is trivial, as quoted in the previous section, and the last case \( v \equiv 3 \pmod{4} \) is divided in two subcases: when \( v \equiv 7 \pmod{8} \), which is now solved, and when \( v \equiv 3 \pmod{8} \) which is the remainder case. \( \square \)

Actually, we will consider now a more general approach using the identity of Corollary 6 but with at most one exception.

If a \( c(p, m, v) \) code with \( v \) satisfying the \((\sharp)\) conditions has two weights then we have the following relation

\[
\frac{v+1}{4} = p^h,
\]

where \( h \) is the class number of the imaginary quadratic number field \( \mathbb{Q}(\sqrt{-v}) \) (see Corollary 6).

In 1935, Siegel gave a non-effective lower bound on the residue at \( s = 1 \) of the L-function \( L(s, \chi_v) \) associated to the primitive odd Dirichlet character \( \chi_v \) of \( \mathbb{Q}(\sqrt{-v}) \). Tatzawa, in 1951, proved an effective lower bound of \( L(1, \chi_v) \) but with at most one exception (see [10] and see also [5] for a simple proof): if \( 0 < \varepsilon < 1/2 \) and \( v \geq \max(e^{1/\varepsilon}, e^{11/2}) \), then

\[
L(1, \chi_v) \geq 0.655\varepsilon v^{-\varepsilon}.
\]

Since the class number \( h \) of \( \mathbb{Q}(\sqrt{-v}) \) with \( -v \equiv 1 \pmod{4} \) is linked to \( L(1, \chi_v) \) by the following Dirichlet class number formula:

\[
L(1, \chi_v) = \frac{\pi h}{\sqrt{v}},
\]

we can use Tatzawa theorem to get an upper bound on \( v \).

**Proposition 9.** There exists at most one two-weight \( c(p, m, v) \) code with \( v \geq 10^8 \) satisfying the \((\sharp)\) conditions.
Table 1. Sporadic \(c(p, m, v)\) codes with \(v\) satisfying the \((\varepsilon)\) conditions and \(v \leq 10^8\).

<table>
<thead>
<tr>
<th>(v)</th>
<th>11</th>
<th>19</th>
<th>67</th>
<th>107</th>
<th>163</th>
<th>499</th>
</tr>
</thead>
<tbody>
<tr>
<td>(p)</td>
<td>3</td>
<td>5</td>
<td>17</td>
<td>3</td>
<td>41</td>
<td>5</td>
</tr>
<tr>
<td>(h)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

Proof. Let \(\varepsilon = 1/\log(10^8) \in (0, 1/2)\). For \(v \geq \max(e^{1/\varepsilon}, e^{11.2}) = 10^8\), we have, with at most one exception:

\[
L(1, \chi_v) \geq 0.655\varepsilon v^{-\varepsilon} = 0.035v^{-0.054}.
\]

Now, \(v^2/4 = p^h \geq 2^h\) implies that \(\log v^2/4 \geq h \log 2\). By the Dirichlet class number formula, we get:

\[
\log \frac{v + 1}{4} \geq \sqrt{\frac{\pi}{v}} L(1, \chi_v) \log 2.
\]

But, for \(v \geq 10^8\), we have on one hand \(\log \frac{v + 1}{4} \geq 17.03\) and on the other hand \(\sqrt{\frac{\pi}{v}} L(1, \chi_v) \log 2 > 28.55\) by Tatuzawa theorem. Thus, there exists no \(v \geq 10^8\) such that \(\frac{v + 1}{4} = p^h\), with at most one exception. \(\square\)

Now, we make an exhaustive research of the primes \(v \leq 10^8\) such that \((v + 1)/4\) is a power of a prime \(p\). Then, for such primes \(v\), we check whether \((v + 1)/4 = p^h(v)\) holds true or not, with \(h(v)\) the class number of \(\mathbb{Q}(\sqrt{-v})\). Actually, we recover the following sporadic known examples of Table 1.

Thus, we have proved the following theorem:

**Theorem 10.** Any two-weight irreducible cyclic \(c(p, m, v)\) code where \(p\) has index two modulo a prime \(v\) and which is not one of the six sporadic examples of Table 1 is semiprimitive, with at most one exception. Hence, Conjecture 1 is true, with at most one exception, for all index-two \(c(p, m, v)\) codes with \(v\) prime.

7. **Cyclotomic cosets**

Let \(p\) be a prime. For any integer \(v\) prime to \(p\), consider on the ring \(\mathbb{Z}/v\mathbb{Z}\) the equivalence relation given by: for \(a, b \in \mathbb{Z}/v\mathbb{Z}\), we set \(a \sim b\) if and only if there exists \(t \in \mathbb{Z}\) such that \(a = bp^t\). The equivalence classes for this equivalence relation are the so-called \(p\)-cyclotomic cosets modulo \(v\).

Recall that the order \(\text{ord}_v(g)\) of an element \(g\) of the multiplicative group \((\mathbb{Z}/v\mathbb{Z})^*\) divides the order \(\varphi(v)\) of this group, where \(\varphi\) is the Euler function. We denote by \(\text{ind}_v(g)\) the index of \(g\) modulo \(v\) i.e.

\[
\text{ind}_v(g) = \frac{\varphi(v)}{\text{ord}_v(g)}.
\]

Then \(\text{ind}_v(g) = [\langle g \rangle : \langle g \rangle]\) where \(\langle g \rangle\) denotes the subgroup of \((\mathbb{Z}/v\mathbb{Z})^*\) generated by \(g\). But the number \(\gamma(p, v)\) of \(p\)-cyclotomic cosets
modulo \( v \) is also equal to the number of irreducibles polynomials in the
decomposition of the polynomial \( X^v - 1 \) over \( F_p \), thus it is equal to
\[
\gamma(p, v) = \sum_{d \mid v} \frac{\varphi(d)}{\text{ord}_d(p)} = \sum_{d \mid v} \text{ind}_d(p)
\]
with the convention that \( \text{ind}_1(p) = 1 \). For example, the condition \( \gamma(p, v) = 2 \)
is equivalent to \( \text{ind}_v(p) = 1 \), that is \( p \) is a primitive root modulo \( v \).

**Proposition 11.** Let \( v \) be an integer. The ring \( \mathbb{Z}/v\mathbb{Z} \) contains exactly
3 \( p \)-cyclotomic cosets if and only if one of the following holds:

(i) \( v \) is a prime and \( p \) has index \( 2 \) mod \( v \);

(ii) \( v \) is the square of a prime and \( p \) has index \( 1 \) mod \( v \).

**Proof.** By (8) we have \( \gamma(p, v) = 3 \) if and only if \( \text{ind}_v(p) = 2 \) and \( v \) has
no proper divisor, or \( \text{ind}_v(p) = 1 \) and \( v \) has a unique proper divisor.
The proposition is then proved. \( \square \)

**Proposition 12.** Let \( v \) be an integer. If the ring \( \mathbb{Z}/v\mathbb{Z} \) contains exactly
three \( p \)-cyclotomic cosets then any \( c(p, m, v) \) code has at most three non-zero weights.

**Proof.** The result is in fact much general: the number of weights is
less or equal than the number of cyclotomic cosets. It follows from the
fact that the weight of a codeword of a \( c(p, m, v) \) code is invariant
under \( t \mapsto t\zeta \) and under \( t \mapsto t^p \); see Theorem 2.5 of [2] for a detailed proof.

The case (ii) of Proposition 11 falls into the semiprimitive case since
\( p \) generates the whole group \( (\mathbb{Z}/v\mathbb{Z})^* \) and thus contains \(-1\).

Finally, we have proved the following result:

**Theorem 13.** If \( v \) is an integer such that there is three \( p \)-cyclotomic cosets modulo \( v \) then any two-weight irreducible cyclic code \( c(p, m, v) \)
which is not one of the six sporadic examples of Table 1 is semiprimitive,
with at most one exception. Hence, Conjecture 1 holds true, with
at most one exception, for all \( c(p, m, v) \) codes with \( v \) an integer such that
there is three \( p \)-cyclotomic cosets modulo \( v \).

**Proof.** If a binary irreducible cyclic code with three-cyclotomic cosets
has two weights then it is semiprimitive. Indeed, by Proposition 11, an
irreducible cyclic code with three-cyclotomic cosets leads to two cases.
The first one leads \( c(p, m, v) \) codes with \( v \) a square of a prime and \( p \) of
index 1 modulo \( v \) which gives a semiprimitive code.

The other case leads to \( c(p, m, v) \) codes with \( v \) a prime and \( p \) of index
2 modulo \( v \) (the so-called index-two codes). When \( v \equiv 1 \pmod{4} \), we
saw that we obtain a semiprimitive code. When \( v \equiv 3 \pmod{4} \), we
obtain \( c(p, m, v) \) codes with \( v \) satisfying the (\( \sharp \)) conditions. In the case
where \( p = 2 \), i.e. the binary case, we found in [1] that there is no two-weight codes. When \( p \neq 2 \), theorem 10 gives the result. □

REFERENCES


Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France.

E-mail address: {yaubry, langevin}@univ-tln.fr