 doi:10.3934/amc.2021002

THE WEIGHT DISTRIBUTION OF IRREDUCIBLE CYCLIC CODES ASSOCIATED WITH DECOMPOSABLE GENERALIZED PALEY GRAPHS

Ricardo A. Podestá* and Denis E. Videla

FaMAF-CIEM (CONICET), Universidad Nacional de Córdoba
Av. Medina Allende 2144, Ciudad Universitaria
Córdoba (5000), República Argentina

(Communicated by Dianhua Wu)

Abstract. We use known characterizations of generalized Paley graphs which are Cartesian decomposable to explicitly compute the spectra of the corresponding associated irreducible cyclic codes. As applications, we give reduction formulas for the number of rational points in Artin-Schreier curves defined over extension fields and to the computation of Gaussian periods.

1. Introduction

In a recent work [20] (see also [19]) we have related the spectra of generalized Paley graphs with the weight distribution of certain associated irreducible cyclic codes. In this work we will compute the weight distribution of irreducible cyclic codes whose associated generalized Paley graphs are Cartesian decomposable. We now recall the basic definitions and results about these codes and graphs.

Generalized Paley graphs. Let k and q be integers, with q a prime power, say $q = p^m$. A *generalized Paley graph* is a Cayley graph (*GP-graph* for short) of the form

(1) $$\Gamma(k,q) = X(\mathbb{F}_q, R_k) \quad \text{with} \quad R_k = \{x^k : x \in \mathbb{F}_q^*\}.$$

That is, $\Gamma(k,q)$ is the graph with vertex set $\mathbb{F}_q$ and two vertices $u, v \in \mathbb{F}_q$ are neighbors (directed edge) if and only if $v - u = x^k$ for some $x \in \mathbb{F}_q^*$. Notice that if ω is a primitive element of $\mathbb{F}_q$, then $R_k = \langle \omega^k \rangle = \langle \omega^{(k,q-1)} \rangle$. This implies that $\Gamma(k,q) = \Gamma((k,q-1),q)$ and that it is a $\frac{q-1}{(k,q-1)}$-regular graph. Thus, we will always assume that $k \mid q-1$. Although the graphs $\Gamma(k,q)$ were denoted as $GP(q, \frac{q-1}{k})$ in [16], our notation is more suited to our purposes because of the relation with the codes $\mathcal{C}(k,q)$ that will be defined later. The graph $\Gamma(k,q)$ is undirected if q is even or if $k \mid \frac{q-1}{2}$ for p odd, and it is connected if the regularity degree

$$n = \tfrac{q-1}{k}$$

is a primitive divisor of $q-1$ (see [16]). For $k = 1, 2$ we get the complete graph $\Gamma(1,q) = K_q$ and the classic Paley graph $\Gamma(2,q) = P(q)$.

2020 *Mathematics Subject Classification:* Primary: 94B15, 05C25; Secondary: 05C50, 05C76.
Key words and phrases: Irreducible cyclic codes, generalized Paley graphs, weight distribution, spectra, Cartesian decomposable.
Partially supported by CONICET, FonCyT (BID-PICT 2018-02073) and SECyT-UNC.
* Corresponding author: Ricardo A. Podestá.

The spectrum $Spec(\Gamma)$ of a graph Γ is the spectrum of its adjacency matrix. If Γ has different eigenvalues $\lambda_0, \ldots, \lambda_t$ with multiplicities $m_0, \ldots, m_t$, we write as usual

$$Spec(\Gamma) = \{[\lambda_0]^{m_0}, \ldots, [\lambda_t]^{m_t}\}$$

with $\lambda_0 > \cdots > \lambda_t$. It is well-known that an n-regular graph Γ has n as it biggest eigenvalue, with multiplicity equal to the number of connected components of Γ.

There are few cases of explicitly known spectrum of Cayley graphs. For instance: unitary Cayley graphs over rings $X(R, R^*)$, where R is a finite abelian ring and R^* is the group of units ([1], this includes the classic unitary graphs $X(\mathbb{Z}_n, \mathbb{Z}_n^*)$) and generalized Paley graphs $X(\mathbb{F}_{q^m}, S_\ell)$ with $S_\ell = \{x^{q^\ell+1} : x \in \mathbb{F}_{q^m}^*\}$ where $\ell \mid m$ ([19], this includes the classic Paley graphs).

The eigenvalues of the GP-graphs $\Gamma(k, q)$, being Cayley graphs, are given by

$$\lambda_\gamma = \sum_{y \in R_k} \chi_\gamma(y) \tag{2}$$

for each $\gamma \in \mathbb{F}_q$, where $\{\chi_\gamma\}$ are the irreducible characters of $\mathbb{F}_q$. In [20], we studied the spectrum of $\Gamma(k, q)$ and showed that these eigenvalues λ_γ coincide with the Gaussian periods

$$\eta_i^{(N,q)} = \sum_{x \in C_i^{(N,q)}} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}(x)} \in \mathbb{C}, \qquad 0 \le i \le N-1, \tag{3}$$

where $C_i^{(N,q)} = \omega^i \langle \omega^N \rangle$ is the coset in $\mathbb{F}_q$ of the subgroup $\langle \omega^N \rangle$ of $\mathbb{F}_q^*$ and

$$N = \gcd(\tfrac{q-1}{p-1}, k). \tag{4}$$

More explicitly, we showed that

$$Spec(\Gamma(k, q)) = \{[n]^{1+\mu n}, [\eta_{i_1}]^{\mu_{i_1} n}, \ldots, [\eta_{i_s}]^{\mu_{i_s} n}\}.$$

for some integers $\mu, \mu_{i_1}, \ldots, \mu_{i_s}$ (see Theorem 2.1 in [20]).

Cartesian graph product. There are many different kind of products in graph theory. The most common ones are the tensor product (also called Kronecker product or direct product), the strong product and the Cartesian product (also called box product or sum of graphs). These products allow, in different contexts, to determine some graphs invariants such as: chromatic, clique and independence numbers, diameter, eigenvalues and energy, and also the automorphism group. A complete study of these products can be found in [12]. It is remarkable that they are particular cases of another graph operation called NEPS (non-complete extended p-sum, see [4]). In this work, we will only deal with the Cartesian product.

The *Cartesian product* of the graphs $\Gamma_1, \ldots, \Gamma_t$ with $t > 1$, is the graph

$$\Gamma = \Gamma_1 \square \cdots \square \Gamma_t, \tag{5}$$

with vertex set $V(\Gamma) = V(\Gamma_1) \times \cdots \times V(\Gamma_t)$, such that $(v_1, \ldots, v_t)$ and $(w_1, \ldots, w_t)$ in $V(\Gamma)$ form an edge in Γ if and only if there is only one $j \in \{1, \ldots, t\}$ such that $\{v_j, w_j\}$ is an edge in Γ_j and $v_i = w_i$ for all $i \ne j$. For instance, $K_2 \square K_2 = C_4$, the Cartesian product of K_2 and a path graph is a ladder graph and the Cartesian product of two path graphs is a grid graph. Also, the Cartesian product of n edges is an n-hypercube $(K_2)^{\square n} = Q_n$, the Cartesian product of two hypercube graphs is another hypercube: $Q_n \square Q_m = Q_{n+m}$, and the Cartesian product of two complete graphs $K_n \square K_m$ is the $n \times m$ rook's graph. Another important class of Cartesian product graphs is given by the Hamming graphs. A *Hamming graph* $H(b, m)$ is any graph with vertex set all the b-tuples with entries from a set V of size m, and two b-tuples form an edge if and only if they differ in exactly one coordinate. Clearly,

$$H(b,m) = (K_m)^{\Box b} \tag{6}$$

for positive integers b, m such that $b, m > 1$. Notice that $Q_n = H(n,2)$.

It is a classic result of Sabidussi ([23]) from 1957 that the chromatic number of the Cartesian product satisfies $\chi(G\Box H) = \max\{\chi(G), \chi(H)\}$. Hence, a Cartesian product is bipartite if and only if each of its factors is. More recently in 2000, Imrich and Klavźar proved that a Cartesian product is vertex transitive if and only if each of its factors is ([13]). If a connected graph is a Cartesian product, it can be factorized uniquely as a product of prime factors; that is, graphs that cannot themselves be decomposed as products of graphs ([24]).

Irreducible cyclic codes. A linear code of length n over $\mathbb{F}_q$ is a vector subspace $\mathcal{C}$ of $\mathbb{F}_q^n$. The weight of a codeword $c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ is the number $w(c)$ of its nonzero coordinates. The weight distribution of $\mathcal{C}$, denoted

$$Spec(\mathcal{C}) = (A_0, \ldots, A_n),$$

is the sequence of frequencies $A_i = \#\{c \in \mathcal{C} : w(c) = i\}$. If $w_0 = 0 < w_1 < \cdots < w_t$ are the non-zero weights, then $\mathcal{C}$ is called a *t-weight* code and w_1 is the minimum distance of $\mathcal{C}$.

A linear code $\mathcal{C}$ is cyclic if for every $(c_0, \ldots, c_{n-1})$ in $\mathcal{C}$ the shifted codeword $(c_1, \ldots, c_{n-1}, c_0)$ is also in $\mathcal{C}$. An important subfamily of cyclic codes is given by the irreducible cyclic codes. For $k \mid q-1$ we will be concerned with the weight distribution of the p-ary irreducible cyclic codes

$$\mathcal{C}(k,q) = \big\{ c_\gamma = \big(\operatorname{Tr}_{q/p}(\gamma\, \omega^{ki}) \big)_{i=0}^{n_{\mathcal{C}}-1} : \gamma \in \mathbb{F}_q \big\} \tag{7}$$

where ω is a primitive element of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $\operatorname{Tr}_{q/p}$ denotes the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. This code has zero ω^{-k} and length

$$n_{\mathcal{C}} = \tfrac{q-1}{N} \tag{8}$$

with N as in (4). Sometimes, we will need to further assume that $k \mid \frac{q-1}{p-1}$. This extra assumption implies that $N = k$ and $n_{\mathcal{C}} = n = \frac{q-1}{k}$.

The computation of the spectrum of (irreducible) cyclic codes is in general a difficult task. There are several papers on the computation of the spectra of some of these cyclic codes by using exponential sums (see for instance [2], [9], [14], [15] and [17]). A complete survey on this topic can be found in [8] (see also [7] for the irreducible case). A different approach for irreducible cyclic codes can be found in [26]. It is well-known that the weights of irreducible cyclic codes can be calculated in terms of Gaussian periods (see for instance [3], [5], [6] and [17]). In fact, using Gaussian periods we have recently showed in [20] that if $\Gamma(k,q)$ is connected and $k \mid \frac{q-1}{p-1}$, then the eigenvalue λ_γ of $\Gamma(k,q)$ and the weight of $c_\gamma \in \mathcal{C}(k,q)$ for γ in $\mathbb{F}_q$ are related by the simple expression

$$\lambda_\gamma = n - \tfrac{p}{p-1} w(c_\gamma) \tag{9}$$

where $n = \frac{q-1}{k}$ is both the length of $\mathcal{C}(k,q)$ and the regularity degree of $\Gamma(k,q)$. Moreover, the frequency of the weight $w(c_\gamma)$ coincides with the multiplicity of λ_γ. We notice that the relation between cyclic codes and graphs is not new. In [14] and [29] the spectra of Hermitian form graphs is used to compute the weight distribution of some cyclic codes with an arbitrary number of zeros.

We will assume henceforth that $q = p^m$ for some natural m with p prime and that k is a positive integer such that $k \mid q-1$. We next give a brief summary of the results of the paper.

Outline and results. In Section 2, we consider the weight distribution of the code $\mathcal{C} = \mathcal{C}(k,q)$ associated with the graph $\Gamma = \Gamma(k,q)$ which is Cartesian decomposable. In this case it was proved by Pearce and Praeger ([18]) that $\Gamma = \square^b \Gamma_0$ for some fixed GP-graph Γ_0. In Theorem 2.2, we show that the weight distribution of $\mathcal{C}$ can be computed from the corresponding one of the smaller code $\mathcal{C}_0$ associated with Γ_0. In fact, the weights of $\mathcal{C}$ are certain integral linear combinations $w = \ell_1 w_1 + \cdots + \ell_s w_s$ of the weights $w_1, \ldots, w_s$ of $\mathcal{C}_0$.

In the next two sections we obtain the weight distributions of irreducible cyclic codes $\mathcal{C}$ constructed from 1-weight and 2-weight irreducible cyclic codes. In the 1-weight case, the weight distribution of $\mathcal{C}$ is obtained from the code $\mathcal{C}(1,q)$, which in the binary case is the simplex code (see Proposition 3.1). In the case of irreducible 2-weight cyclic codes, they are of three different kind: subfield, semiprimitive and exceptional. Subfield subcodes are not connected and hence cannot be considered by our methods. The semiprimitive case is studied in Proposition 4.1. The computations of the exceptional cases can be done in the same way, but are left over because of the size of the numbers involved.

Section 5 deals with the weight distribution of the irreducible cyclic codes constructed from the codes $\mathcal{C}(3,q)$ and $\mathcal{C}(4,q)$. We have that $\Gamma(1,q)$ and $\Gamma(2,q)$ are the complete graphs and the classic Paley graphs, respectively. The next graphs to consider are $\Gamma(3,q)$ and $\Gamma(4,q)$. The weight distributions of the associated codes $\mathcal{C}(3,q)$ and $\mathcal{C}(4,q)$ are known (see Theorems 19–21 in [7]). In Theorems 5.1 and 5.3 we give the weight distributions of the irreducible cyclic codes constructed from $\mathcal{C}(3,q)$ and $\mathcal{C}(4,q)$, respectively.

The final two sections are devoted to applications of the reduction result given in Theorem 2.2 In Section 6, we consider Artin-Schreier curves $C_{k,\beta}(p^m)$ with affine equations

$$y^p - y = \beta x^k$$

where $k \mid \frac{p^m-1}{p-1}$ and $\beta \in \mathbb{F}_{p^m}$. In Proposition 6.1 we obtain the direct relationship

$$\#C_{k,\beta}(p^m) = 2p^m + k(p-1)\lambda_\beta$$

between the the number of $\mathbb{F}_{p^m}$-rational points of the curve $C_{k,\beta}(p^m)$ and the eigenvalues of the graph $\Gamma(k,p^m)$. Then, via this connection between curves and graphs and the reduction result for graphs, we express the number of rational points of an Artin-Schreier curve over a field $\mathbb{F}_{p^{ab}}$ in terms of linear combinations of the number of rational points of Artin-Schreier curves over a subfield $\mathbb{F}_{p^a}$ (see Corollary 6.2).

Finally, as a second application, we give an expression for Gaussian periods in terms of Gaussian periods of smaller parameters (Proposition 7.1). In fact, we show that, under the same hypothesis of Cartesian decomposability of GP-graphs used in Theorem 2.2, each Gaussian period $\eta_i^{(k,p^{ab})}$ is an integral linear combination of Gaussian periods $\eta_j^{(u,p^a)}$. In the particular case that the smaller pair is semiprimitive, we get the simple explicit expression of Proposition 7.3.

2. Spectrum of cyclic codes associated with decomposable GP-graphs

A graph Γ is *Cartesian decomposable* if it can be written as a product of smaller graphs $\Gamma_1, \ldots, \Gamma_t$ as in (5) with $t > 1$. Recently, Pearce and Praeger ([18]) characterized those generalized Paley graphs which are Cartesian decomposable. They proved that a Cartesian decomposable GP-graph is a product of copies of a single graph, which is necessarily another GP-graph.

More precisely, if $\Gamma = \Gamma(k, p^m)$ is simple and connected, that is if k divides $\frac{q-1}{2}$ when p is odd and $n = \frac{p^m-1}{k}$ is a primitive divisor of $p^m - 1$, the following conditions are equivalent:

$$(10) \qquad \begin{aligned} &(a) \quad \Gamma = \Gamma(k, p^m) \text{ is Cartesian decomposable.} \\ &(b) \quad n = bc \text{ with } b > 1,\ b \mid m \text{ and } c \text{ is a primitive divisor of } p^{\frac{m}{b}} - 1. \\ &(c) \quad \Gamma \cong \square^b \Gamma_0, \text{ where } \Gamma_0 = \Gamma(u, p^{\frac{m}{b}}) \text{ with } u = \tfrac{p^{\frac{m}{b}}-1}{c} \text{ for } b, c \text{ as in } (b). \end{aligned}$$

We recall that n is a *primitive divisor* of $p^m - 1$ if $n \mid p^m - 1$ and $n \nmid p^t - 1$ for all $t < m$. To denote this fact, for convenience, we will use the following notation

$$(11) \qquad n \dagger p^m - 1.$$

We want to point out the following structural consequence of the previous result of Pearce and Praeger for those GP-graphs which are strongly regular.

Proposition 2.1. *Let $\Gamma(k, q)$ be a connected GP-graph which is strongly regular. Then, $\Gamma(k, q)$ is Cartesian decomposable if and only if it is a Hamming graph and q is a perfect square. In this case we have*

$$(12) \qquad \Gamma(k, q) = K_{q'} \square K_{q'} = H(2, q')$$

with $k = \frac{\sqrt{q}+1}{2}$ and $q' = \sqrt{q}$.

Proof. Suppose that $\Gamma = \Gamma(k, q)$, with $q = p^m$, is a Cartesian decomposable strongly regular graph. Since Γ is connected, by (10) we have $\Gamma \cong \square^b \Gamma_0$, where $\Gamma_0 = \Gamma(u, p^a)$ with $c = \frac{p^a-1}{u} \dagger p^a - 1$, $m = ab$ and $n = \frac{p^m-1}{k} = bc$. Also, since every connected strongly regular graph has only two non-trivial eigenvalues, necessarily $b = 2$ and Γ_0 is a complete graph. Otherwise, Γ would have more than two nontrivial eigenvalues because all of the eigenvalues of the Cartesian product of graphs are sums of eigenvalues of its factors. Thus, Γ_0 must have only two eigenvalues and $b = 2$. But the graphs with only two eigenvalues are exactly disjoint unions of two copies of the same complete graph. As $c = \frac{p^a-1}{u} \dagger p^a - 1$ then Γ_0 is connected. Therefore, Γ_0 is the complete graph with p^a vertices, since $b = 2$, and then $q' = p^a = \sqrt{q}$. On the other hand, we have

$$k = \tfrac{p^m-1}{n} = \tfrac{p^{2a}-1}{2(p^a-1)} = \tfrac{p^a+1}{2} = \tfrac{\sqrt{q}+1}{2},$$

as desired. The second equality in (12) follows by (6).

The converse is clear from the fact that the eigenvalues of $K_{q'} \square K_{q'}$ are $2q' - 2$, $q' - 2$ and -2, with multiplicities 1, $2(q' - 1)$ and $(q' - 1)^2$, respectively. $\square$

We next show that if Γ is a Cartesian decomposable GP-graph, say $\Gamma \cong \square^b \Gamma_0$, then the computation of the spectrum of the cyclic code $\mathcal{C}$ associated with Γ reduces to the one of the smaller code $\mathcal{C}_0$ associated with Γ_0. We will use a recent result in [20] relating the spectra of $\mathcal{C}_0$ with the one of Γ_0.

In the sequel we assume that p is a prime and k, m are positive integers such that

(13) $$q = p^m, \qquad k \mid q-1 \qquad \text{and put} \qquad n = \tfrac{q-1}{k}.$$

In addition, sometimes we will also require that

(14) $$m = ab, \qquad n = bc \qquad \text{and} \qquad u = \tfrac{p^a-1}{c},$$

for non-negative integers a, b, c with $b > 1$ and $c \mid p^a - 1$. Notice that if $p-1 \mid c$ (or, equivalently, if $u \mid \frac{p^a-1}{p-1}$), then $k \mid \frac{q-1}{p-1}$.

We are now in a position to state and prove our main result.

Theorem 2.2. *Let $p, q, k, m, n, a, b, c, u$ be positive integers as in (13)–(14) with $c \dagger p^a - 1$ and $n \dagger p^m - 1$. Consider the irreducible cyclic codes $\mathcal{C} = \mathcal{C}(k, p^m)$ and $\mathcal{C}_0 = \mathcal{C}(u, p^a)$. If $p-1 \mid c$, then Spec($\mathcal{C}$) is determined by Spec($\mathcal{C}_0$). More precisely, if the weights of $\mathcal{C}_0$ are $0 = w_0 < w_1 < \cdots < w_s$ with frequencies $A_{w_i} = m_i$ for $i = 0, \ldots, s$, then the weights of $\mathcal{C}$ are given by*

(15) $$w_{\ell_0,\ldots,\ell_s} = \ell_1 w_1 + \cdots + \ell_s w_s$$

where $(\ell_0, \ldots, \ell_s) \in \mathbb{N}_0^{s+1}$ such that $\ell_0 + \cdots + \ell_s = b$, with frequencies

(16) $$A_{\ell_0,\ldots,\ell_s} = \tbinom{b}{\ell_0,\ldots,\ell_s} m_1^{\ell_1} \cdots m_s^{\ell_s}.$$

In particular, $\mathcal{C}$ has the same minimum distance as $\mathcal{C}_0$.

Proof. We have $k \mid \frac{p^m-1}{p-1}$ and $u \mid \frac{p^a-1}{p-1}$ since $p-1 \mid c$. Also, the graphs $\Gamma = \Gamma(k, p^m)$ and $\Gamma_0 = \Gamma(u, p^a)$ are connected because of the primitiveness of n and c, respectively. Thus, we can apply Theorem 5.1 in [20] to the codes $\mathcal{C}$ and $\mathcal{C}_0$ of lengths n and c, respectively.

By hypothesis, since conditions (10) are satisfied, we have that $\Gamma \cong \square^b \Gamma_0$ and therefore $\mathrm{Spec}(\Gamma) = \mathrm{Spec}(\square^b \Gamma_0)$. It is known that the eigenvalues of the Cartesian product of graphs is the sum of the eigenvalues of its factors (see for instance [4]). Now, if $\mathrm{Spec}(\Gamma_0) = \{[\lambda_0]^{m_0}, [\lambda_1]^{m_1}, \ldots, [\lambda_s]^{m_s}\}$ where $\lambda_0 = c$ is the trivial eigenvalue with multiplicity $m_0 = 1$, then the eigenvalues of Γ are

(17) $$\Lambda_{\ell_0,\ldots,\ell_s} = \ell_0 \lambda_0 + \cdots + \ell_s \lambda_s$$

where the $(s+1)$-tuple of integers $(\ell_0, \ldots, \ell_s)$ satisfies

$$\ell_0 + \cdots + \ell_s = b$$

and $\ell_i \geq 0$ for every i, with corresponding multiplicity

(18) $$\tbinom{b}{\ell_0,\ldots,\ell_s} m_1^{\ell_1} \cdots m_s^{\ell_s}$$

since $m_0 = 1$, where $\binom{b}{\ell_0,\ldots,\ell_s}$ stands for the multinomial coefficient. The hypothesis $p-1 \mid c$ is equivalent to $u \mid \frac{p^a-1}{p-1}$. Thus, we can apply Theorem 5.1 in [20] (i.e. (9)) to the graph Γ_0 and the code $\mathcal{C}_0$ and, hence, we have

$$\lambda_i = c - \tfrac{p}{p-1} w_i$$

for each $i = 0, \ldots, s$. Therefore, we get

$$\Lambda_{\ell_0,\ldots,\ell_s} = \sum_{i=0}^{s} \ell_i (c - \tfrac{p}{p-1} w_i) = n - \tfrac{p}{p-1} \sum_{i=1}^{s} \ell_i w_i,$$

since $c(\ell_0 + \cdots + \ell_s) = bc = n$ and $w_0 = 0$. Also, the frequency of w_i in $\mathcal{C}_0$ is m_i for all $i = 0, \ldots, s$. Since $p-1 \mid c$ we have $k \mid \frac{q-1}{p-1}$ and hence by (9) again applied to $\mathcal{C}$ and Γ, we have that the weights of $\mathcal{C}$ are given by

$$w_{\ell_0,\ldots,\ell_s} = \tfrac{p-1}{p}(n - \Lambda_{\ell_0,\ldots,\ell_s}) = \ell_1 w_1 + \cdots + \ell_s w_s$$

with frequencies $\binom{b}{\ell_0,\ldots,\ell_s} m_1^{\ell_1} \cdots m_s^{\ell_s}$, as desired.

The last assertion is straightforward from (15), and the result follows. $\square$

Remark 2.3. Suppose that $\Gamma \simeq \square^b \Gamma_0$. Then Γ and Γ_0 have associated irreducible cyclic codes $\mathcal{C}$ and $\mathcal{C}_0$. Under the hypothesis of the theorem, we can only assure that the spectrum of $\mathcal{C}$ equals the spectrum of the direct sum code

$$\mathcal{C}_0^b = \mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_0,$$

with $\mathcal{C}_0$ repeated b-times, which is not cyclic in general. Thus, one may wonder if there is some code operation $*$ such that $\mathcal{C} = \mathcal{C}_0 * \cdots * \mathcal{C}_0$, with $\mathcal{C}_0$ repeated b-times.

3. Cyclic codes from 1-weight cyclic codes

In this and the next two sections we will apply Theorem 2.2 to compute the spectra of irreducible cyclic codes constructed from irreducible cyclic codes with few weights. We consider 1-weight irreducible cyclic codes here and 2-weight irreducible cyclic codes in the next section. In Section 5 we will deal with some codes that are 3-weight and 4-weight irreducible cyclic codes.

One-weight irreducible cyclic codes are already characterized when $k \mid q-1$ (see [7], [28]). In fact, by Theorem 16 in [7], we have that if $k \mid q-1$, then the cyclic code $\mathcal{C}(k,q)$ is irreducible if and only if

$$N = \gcd(\tfrac{q-1}{p-1}, k) = 1.$$

In our case, the restriction $k \mid \frac{q-1}{p-1}$ implies that $k = 1$ and hence, the only irreducible cyclic code that we can take into account is

$$\mathcal{C}(1,q) = \{(\mathrm{Tr}_{q/p}(\gamma\omega^i))_{i=0}^{q-1} : \gamma \in \mathbb{F}_q\}$$

over $\mathbb{F}_p$ of length $q-1$, where ω is a primitive element of $\mathbb{F}_q$. Note that in the binary case $p = 2$, $\mathcal{C}(1, 2^m)$ is just the simplex code (i.e. the dual of the Hamming code).

From now on, it will be useful to use the following notation

$$\Psi_b(x) = \tfrac{x^b-1}{x-1} = x^{b-1} + \cdots + x^2 + x + 1. \tag{19}$$

Proposition 3.1. *Let $q = p^a$ with p prime, $a \geq 1$ and $b > 1$ an integer dividing $\Psi_b(q)$. Put $k = k_b = \frac{1}{b}\Psi_b(q)$. Then, $\mathcal{C} = \mathcal{C}(k, q^b)$ is an irreducible b-weight cyclic code with weights $0, w, 2w, \ldots, bw$ and frequencies given by*

$$Spec(\mathcal{C}) = \{A_{\ell w}(\mathcal{C}) = \tbinom{b}{\ell} {A_w}^{\ell}\}_{0\leq \ell \leq b} \tag{20}$$

where $w = (p-1)p^{a-1}$ and $A_w = p^a - 1$ is the weight distribution of the code $\mathcal{C}_0 = \mathcal{C}(1,q)$.

Proof. Notice that $k = \frac{q^b-1}{b(q-1)}$ and thus $k \mid \frac{q^b-1}{p-1}$. Clearly $c = q-1$ is a primitive divisor of itself. By Theorem 2.2, the spectrum of the irreducible cyclic code $\mathcal{C}$ is determined by the spectra of the code $\mathcal{C}_0 = \mathcal{C}(1,q)$ if $n = \frac{q^b-1}{k} = b(q-1)$ is a primitive divisor of $q^b - 1$. Equivalently, if the GP-graph $\Gamma(k, q^b)$ is connected.

Thus, we will show that $\Gamma(k, q^b)$ is connected by showing that it is a Hamming graph. For integers d, q with $d > 1$ and $q > 1$, recall that a Hamming graph $H(d, q)$ is any graph with vertex set all the d-tuples with entries from a set V of size q, and two d-tuples form an edge if and only if they differ in exactly one coordinate.

In [16], Lim and Praeger characterized all the GP-graphs which are Hamming graphs. They proved that $\Gamma(\frac{p^m-1}{n}, p^m)$ is Hamming if and only if $n = b(p^{\frac{m}{b}} - 1)$ for some divisor $b > 1$ of m. Clearly, n satisfies this last condition and then $\Gamma(k, q^b)$ is a Hamming graph, which is connected by definition. This implies that n is a primitive divisor of $q^b - 1$.

We have that $\mathcal{C}_0 = \mathcal{C}(1, p^a)$. By Theorems 15 and 16 in [7], $\mathcal{C}_0$ is a 1-weight $[p^a, a, (p-1)p^{a-1}]$-code with weight distribution given by $w = (p-1)p^{a-1}$ with $A_w = p^a - 1$. The proposition thus follows from Theorem 2.2.

By (15) the weights are $w_{\ell_0,\ell_1} = \ell_1 w_1$ with $(\ell_0, \ell_1) \in \mathbb{N}_0^2$ such that $\ell_0 + \ell_1 = b$. Thus, the weights are

$$w_\ell = \ell w \qquad \text{with} \qquad 0 \leq \ell \leq b.$$

By (16) the frequencies are given by

$$A_{\ell w} = A_{\ell_0,\ell_1} = \tbinom{b}{\ell_0,\ell_1} m_1^{\ell_1} = \tfrac{b!}{\ell_0!\ell_1!} m_1^{\ell_1} = \tbinom{b}{\ell_1} A_w^{\ell_1}.$$

Since ℓ_1 runs from 0 to b, we get the desired result. □

Notice that one can check that (20) is correct by adding the frequencies

$$\sum_{0\leq\ell\leq b} \tbinom{b}{\ell} A_w^\ell = (1 + A_w)^b = p^{ab} = q^b.$$

Example 3.2. Consider $p = 2$ and $a = 3$, hence $q = 8$. One can check that if $b = 7$ then $b \mid 8^6 + \cdots + 8^2 + 8 + 1 = 299.593$. The simplex code $\mathcal{C}_0 = \mathcal{C}(1, 8)$ has weights $w_0 = 0$, $w_1 = 4$, with frequencies $A_0 = 1$, $A_4 = 7$. Now, $k_b = \frac{1}{7}\Psi_7(8) = 42.799$. By the previous proposition, the irreducible cyclic code

$$\mathcal{C}(\tfrac{1}{7}\Psi_7(8), 8^7) = \mathcal{C}(42.799, 2.097.152)$$

has weight distribution

$$w_0 = 0,\ w_1 = 4,\ w_2 = 8,\ w_3 = 12,\ w_4 = 16,\ w_5 = 20,\ w_6 = 24,\ w_7 = 28$$

with frequencies

$$\begin{aligned}
&A_0 = 1, && A_4 = \tbinom{7}{1}7 = 7^2 = 49,\\
&A_8 = \tbinom{7}{2}7^2 = 3\cdot 7^3 = 1.029, && A_{12} = \tbinom{7}{3}7^3 = 5\cdot 7^4 = 12.005,\\
&A_{16} = \tbinom{7}{4}7^4 = 5\cdot 7^5 = 84.035, && A_{20} = \tbinom{7}{5}7^5 = 3\cdot 7^6 = 352.947,\\
&A_{24} = \tbinom{7}{6}7^6 = 7^7 = 823.543, && A_{28} = 7^7 = 823.543.
\end{aligned}$$

By Theorem 17 in [7], if $\frac{q-1}{p-1}$ is even, then $\mathcal{C}(2, q)$ is a 2-weight irreducible cyclic code with non-zero weights $w^\pm = \frac{(p-1)(q\pm\sqrt{q})}{qN}$ with frequencies $A_{w^\pm} = \frac{q-1}{2}$. The next result exhibits another infinite family of 2-weight irreducible cyclic codes.

Corollary 3.3. *If q is a power of an odd prime p, then $\mathcal{C}(\frac{q+1}{2}, q^2)$ is a 2-weight irreducible cyclic code with weights $0, w, 2w$ with corresponding frequencies $A_0 = 1$, $A_w = 1(q-1)$, $A_{2w} = (q-1)^2$ where $w = \frac{p-1}{p}q$.*

Proof. Taking $b = 2$, we clearly have that $2 \mid \Psi_2(q) = q + 1$ since q is odd. Thus, the statement follows directly from Proposition 3.1. $\square$

Remark 3.4. The code $\mathcal{C}(\frac{q+1}{2}, q^2)$ belongs to the class of semiprimitive 2-weight irreducible cyclic codes. In the following section, we will use this kind of codes to find other weight distributions. The GP-graph Γ associated with this code is the one given in Proposition 2.1, that is $\Gamma = K_q \square K_q = H(2, q)$.

By Proposition 3.1, to get the weight distribution of $\mathcal{C}(\frac{1}{b}\Psi_b(q), q^b)$ we only need to check that $b \mid \Psi_b(q)$. In the next result we give some sufficient conditions for this to happen, based on previous results on [21].

Corollary 3.5. *Let p be a prime and let a, b, k, m, x be positive integers such that $m = ab$ with $b > 1$, $k = \frac{1}{b}\Psi_b(p^a)$ and $x = p^a$. The weight distribution of $\mathcal{C}(k, p^m)$ is given by (20) in the following cases:*

(a) *If $b = r$ is a prime different from p and $x \equiv 1 \pmod r$.*

(b) *If $b = 2r$ with r an odd prime, x coprime with b and $x \equiv \pm 1 \pmod r$.*

(c) *If $b = rr'$ with $r < r'$ odd primes such that $r \nmid r' - 1$ and $x \equiv 1 \pmod{rr'}$.*

(d) *If $b = r_1 r_2 \cdots r_\ell$ with $r_1 < r_2 < \cdots < r_\ell$ primes different from p with $x \equiv 1 \pmod{r_1}$ and $x^{b/r_i} \equiv 1 \pmod{r_i}$ for $i = 2, \ldots, \ell$.*

(e) *If $b = r^t$ with r prime such that $ord_b(x) = r^h$ for some $0 \le h < t$.*

(f) *If $b = r_1^{t_1} \cdots r_\ell^{t_\ell}$ with $r_1 < \cdots < r_\ell$ primes different from p where $ord_{r_i^{t_i}}(x) = r_i^{h_i}$ with $0 \le h_i \le t_i - 1$ for all i.*

Proof. Clearly (a)–(d) are direct consequences of Proposition 3.1 and the divisibility properties of $\Psi_b(x)$ in the square-free case given in Lemma 5.1 of [21]. On the other hand, (e) follows from Proposition 3.1 and Lemma 5.2 of [21]. The remaining assertion is straightforward from Proposition 3.1 and Lemma 5.3 of [21]. $\square$

4. Cyclic codes from 2-weights cyclic codes

In [25], Schmidt and White conjectured that all two-weight irreducible cyclic codes of length n over $\mathbb{F}_p$, with $p - 1 \mid n$, belong to one of the following disjoint families:

• The *semiprimitive codes*, which are those $\mathcal{C}(u, p^a)$ such that -1 is a power of p modulo u. Equivalently, (k, q) with $q = p^m$ is a *semiprimitive pair*, that is $k \mid p^t + 1$ for some t such that $t \mid m$ and $m_t = \frac{m}{t}$ even, and $k \neq p^{\frac{m}{2}} + 1$.

• The *subfield subcodes*, corresponding to $\mathcal{C}(u, p^a)$ where $u = \frac{p^a - 1}{p^t - 1}$ with $t < a$.

• The *exceptional codes*, i.e. irreducible 2-weight cyclic codes which are neither subfield subcodes nor semiprimitive codes.

If one does not require the condition $p - 1 \mid n$, Pinnawala and Rao ([22]) has given a family of 2-weight irreducible cyclic codes which are not of the previous kind.

Notice that in the subfield subcode case, the graph $\Gamma(u, p^a)$ is not connected since $c = \frac{p^a - 1}{u}$ is not a primitive divisor of $p^a - 1$; and thus we cannot apply Theorem 2.2. Hence, we are only interested in the other two cases.

We now compute the spectrum of the code $\mathcal{C}$ associated with the decomposable graph $\Gamma \simeq \square^b \Gamma_0$, where Γ_0 is a semiprimitive GP-graph.

Proposition 4.1. *Let $p, q, k, m, n, a, b, c, u$ be positive integers as in (13)–(14) such that $n \dagger p^m - 1$. If (u, p^a) is a semiprimitive pair then the weights of the code $\mathcal{C} = \mathcal{C}(k, p^m)$ are given by*

$$w_{\ell_1,\ell_2} = \tfrac{(p-1)p^{\frac{a}{2}-1}}{u}\big\{\ell_1(p^{\frac{a}{2}} - \sigma(u-1)) + \ell_2\big(p^{\frac{a}{2}} + \sigma\big)\big\} \tag{21}$$

for every pair of non-negative integers ℓ_1, ℓ_2 such that $0 \le \ell_1 + \ell_2 \le b$, where we put $\sigma = \pm 1$ if $u \mid p^{\frac{a}{2}} \pm 1$, with frequencies

$$A_{\ell_1,\ell_2} = \tbinom{b}{\ell_1}\tbinom{b-\ell_1}{\ell_2} c^{\ell_1+\ell_2}(u-1)^{\ell_1}. \tag{22}$$

Proof. Consider the semiprimitive irreducible cyclic code $\mathcal{C}_0 = \mathcal{C}(u, p^a)$. Thus, we have that $u \mid p^\ell + 1$ for some $\ell \mid a$ with $\frac{a}{\ell}$ even and that $\mathcal{C}_0$ is a 2-weight code. By Remark 5.6 in [20] the weights of $\mathcal{C}_0$ are

$$w_1 = \tfrac{(p-1)p^{\frac{a}{2}-1}}{u}(p^{\frac{a}{2}} - \sigma(u-1)) \qquad \text{and} \qquad w_2 = \tfrac{(p-1)p^{\frac{a}{2}-1}}{u}(p^{\frac{a}{2}} + \sigma)$$

where $\sigma = (-1)^{\frac{m}{2\ell}+1}$ with ℓ the minimal positive integer such that $u \mid p^\ell + 1$.

Since (u, p^a) is a semiprimitive pair then $u \mid \frac{p^a-1}{p-1}$ and $k \mid \frac{p^m-1}{p-1}$. Indeed, assume that $u \mid p^\ell + 1$ with $\frac{a}{\ell}$ even, then if we denote by $v = v_2(\frac{a}{\ell})$ the 2-adic value of $m\ell$ we obtain that $\frac{a}{2^v} = h\ell$ for some h odd. On the first hand, by taking into account that $p^\ell \equiv -1 \pmod{p^\ell + 1}$ we obtain that

$$p^{\frac{a}{2^v}} = p^{h\ell} \equiv (-1)^h \equiv -1 \pmod{p^\ell + 1}$$

i.e we have that $p^\ell + 1 \mid p^{\frac{a}{2^v}} + 1$ and thus $u \mid p^{\frac{a}{2^v}} + 1$. On the other hand, it is easy to see that

$$p^a - 1 = (p^{\frac{a}{2^v}} - 1)\prod_{j=1}^{v}(p^{\frac{a}{2^j}} + 1).$$

Notice that $p - 1 \mid p^{\frac{a}{2^v}} - 1$ and therefore $u \mid \frac{p^a-1}{p-1}$, as desired. Now, since $u \mid \frac{p^a-1}{p-1}$ and $\Psi_b(p^a) = \frac{p^{ab}-1}{p^a-1}$ then $u\Psi_b(p^a) \mid \frac{p^{ab}-1}{p-1}$. Using that $k = \frac{u}{b}\Psi_b(p^a)$ we obtain that $k \mid \frac{p^m-1}{p-1}$, as we wanted. Thus, by Remark 5.6 in [20] the frequencies of w_1, w_2 are $m_1 = c$ and $m_2 = c(u-1)$, respectively.

Now, by hypothesis we have that $m = ab$ and $n = bc$ is a primitive divisor of $p^m - 1$. Hence, by Theorem 2.2 the weights of $\mathcal{C}(k, p^m)$ are $w_{\ell_0,\ell_1,\ell_2} = \ell_1 w_1 + \ell_2 w_2$ where $(\ell_0, \ell_1, \ell_2) \in \mathbb{N}_0^3$ with $\ell_0 + \ell_1 + \ell_2 = b$, with frequencies

$$A_{w_{\ell_0,\ell_1,\ell_2}} = \tbinom{b}{\ell_0,\ell_1,\ell_2} m_1^{\ell_1} m_2^{\ell_2} = \frac{b!}{\ell_1!\ell_2!(b-(\ell_1+\ell_2))!} m_1^{\ell_1} m_2^{\ell_2}.$$

Thus, disregarding ℓ_0 we have that

$$w_{\ell_1,\ell_2} = \ell_1 w_1 + \ell_2 w_2 = \tfrac{(p-1)p^{\frac{a}{2}-1}}{u}\big\{\ell_1(p^{\frac{a}{2}} - \sigma(u-1)) + \ell_2\big(p^{\frac{a}{2}} + \sigma\big)\big\}$$

with corresponding multiplicities

$$A_{w_{\ell_1,\ell_2}} = \tbinom{b}{\ell_1}\tbinom{b-\ell_1}{\ell_2} c^{\ell_1+\ell_2}(u-1)^{\ell_1},$$

where (ℓ_1, ℓ_2) runs over all 2-tuples of non-negative integers such that $0 \le \ell_1 + \ell_2 \le b$, and therefore we obtain (21) and (22), as we wanted. □

The proposition implies that one knows the weight distribution of the cyclic code $\mathcal{C} = \mathcal{C}(k, p^{ab})$ associated to the decomposable graph $\Gamma(k, p^{ab}) = \square^b \Gamma(u, p^a)$ without need to know the weight distribution of the smaller cyclic code $\mathcal{C}_0 = \mathcal{C}(u, p^a)$ associated to $\Gamma_0(u, p^a)$.

Example 4.2. Let p be an odd prime and take $a = u = 2$ and $b = 3$. The graph $\Gamma_0 = \Gamma(2, p^2)$ is the classic Paley graph over $\mathbb{F}_{p^2}$ with spectrum

$$Spec(\Gamma_0) = \{[\tfrac{p^2-1}{2}]^1, [\tfrac{p-1}{2}]^{\frac{p^2-1}{2}}, [-\tfrac{p+1}{2}]^{\frac{p^2-1}{2}}\}$$

(see for instance [10]). Then, the two nonzero weights of the code $\mathcal{C}_0 = \mathcal{C}(2, p^2)$, that can be obtained from (9), have multiplicity $\frac{p^2-1}{2}$. We have $m = ab = 6$ and $c = \frac{p^2-1}{2}$ and thus

$$n = bc = \tfrac{3(p^2-1)}{2}.$$

Clearly, c is a primitive divisor of $p^2 - 1$. Notice that if $p \neq 3$ ($p = 2t + 1$ prime and $t \not\equiv 1 \pmod 3$), then $9 \mid n$. In particular, if $p \equiv 2, 5, 7 \pmod 9$, then n is a primitive divisor of $p^6 - 1$, since in these cases the order of p modulo 9 is 6 and then 9 does not divide $p^a - 1$ when $1 \leq a < 6$. This implies that n does not divide $p^a - 1$, either.

In this case one can choose $\sigma = 1$ or -1 indistinctly in the formula (21). Therefore the code

$$\mathcal{C} = \mathcal{C}(\tfrac{2(p^6-1)}{3(p^2-1)}, p^6) = \mathcal{C}(\tfrac{2}{3}(p^4 + p^2 + 1), p^6)$$

has weights

$$w_{\ell_1,\ell_2} = \tfrac{(p-1)}{2}\{\ell_1(p-1) + \ell_2(p+1)\} = \tfrac{(p-1)^2}{2}\ell_1 + c\ell_2$$

for every pair $0 \leq \ell_1 + \ell_2 \leq 3$, with frequencies

$$A_{\ell_1,\ell_2} = \tbinom{3}{\ell_1}\tbinom{3-\ell_1}{\ell_2}(\tfrac{p^2-1}{2})^{\ell_1+\ell_2}.$$

If $\ell_2 = 0$, then $w_{1,0} = \frac{(p-1)^2}{2}$, $w_{2,0} = (p-1)^2$, and $w_{3,0} = \frac{3(p-1)^2}{2}$. If $\ell_1 = 0$, then $w_{0,1} = \frac{p^2-1}{2}$, $w_{0,2} = p^2 - 1$, and $w_{0,3} = \frac{3(p^2-1)}{2}$. Also, if ℓ_1 and ℓ_2 are nonzero, then $w_{1,1} = p(p-1)$, $w_{2,1} = \frac{(p-1)}{2}(3p-1)$ and $w_{1,2} = \frac{(p-1)}{2}(3p+1)$. One can check that if $p \neq 5$, all these weights are different and hence the spectrum of $\mathcal{C}$ is given by Table 1.

TABLE 1. Weight distribution of $\mathcal{C}$ with $p \equiv 2, 5, 7 \pmod 9$ and $p > 5$.

weight	frequency
$w_{0,0} = 0$	$A_{0,0} = 1$
$w_{1,0} = \frac{(p-1)^2}{2}$	$A_{1,0} = 3(\frac{p^2-1}{2})$
$w_{2,0} = (p-1)^2$	$A_{2,0} = 3(\frac{p^2-1}{2})^2$
$w_{3,0} = \frac{3(p-1)^2}{2}$	$A_{3,0} = (\frac{p^2-1}{2})^3$
$w_{0,1} = \frac{p^2-1}{2}$	$A_{0,1} = 3(\frac{p^2-1}{2})$

weight	frequency
$w_{0,2} = p^2 - 1$	$A_{0,2} = 3(\frac{p^2-1}{2})^2$
$w_{0,3} = \frac{3(p^2-1)}{2}$	$A_{0,3} = (\frac{p^2-1}{2})^3$
$w_{1,1} = p(p-1)$	$A_{1,1} = 6(\frac{p^2-1}{2})^2$
$w_{2,1} = \frac{p-1}{2}(3p-1)$	$A_{2,1} = 3(\frac{p^2-1}{2})^3$
$w_{1,2} = \frac{p-1}{2}(3p+1)$	$A_{1,2} = 3(\frac{p^2-1}{2})^3$

Notice that adding all the frequencies we get

$$\sum_{0 \leq i+j \leq 3} A_{i,j} = 1 + 6c + 12c^2 + 8c^3 = p^6$$

and therefore the code $\mathcal{C}$ has dimension 6 and minimum distance $\frac{(p-1)^2}{2}$. That is, $\mathcal{C}$ has parameters $[\frac{3(p^2-1)}{2}, 6, \frac{(p-1)^2}{2}]$.

For instance, if $p=5$, we have $\mathcal{C} = \mathcal{C}(\frac{2}{3}(5^4+5^2+1), 5^6) = \mathcal{C}(434, 15.625)$ with parameters $[36, 6, 8]$ defined over $\mathbb{F}_5$. The weights of $\mathcal{C}$ are given by

$$w_{1,0} = 8, \;\; w_{2,0} = 16, \;\; w_{3,0} = w_{0,2} = 24, \;\; w_{0,1} = 12,$$
$$w_{0,3} = 36, \;\; w_{1,1} = 20, \;\; w_{2,1} = 28, \;\; w_{1,2} = 32,$$

with frequencies

$$A_8 = A_{12} = 3c = 36, \quad A_{16} = 3c^2 = 432, \quad A_{20} = 6c^2 = 864,$$
$$A_{24} = (c+3)c^2 = 2.160, \quad A_{28} = A_{32} = 3c^3 = 5.184, \quad A_{36} = c^3 = 1.728.$$

since $c = 12$. $\lozenge$

Remark 4.3. The weight distribution of irreducible cyclic codes constructed from exceptional 2-weight irreducible cyclic codes can be obtained from Theorem 2.2 and from the spectrum of the associated GP-graphs, which are computed in [20].

5. Cyclic codes from $\mathcal{C}(3,q)$ and $\mathcal{C}(4,q)$

In general, 3-weight or 4-weight irreducible cyclic codes are not classified. In this section we will use the irreducible cyclic codes $\mathcal{C}(3,q)$ and $\mathcal{C}(4,q)$ to find new weight distributions of irreducible cyclic codes via the reduction formula obtained in Section 2. More precisely, for $u=3,4$, if $\mathcal{C}_0 = \mathcal{C}(u,q)$ is the code associated to $\Gamma_0(u,q)$, we will compute the weight distributions of codes $\mathcal{C}(k,q^r)$ associated to the Cartesian product graph $\Gamma(k,q^r) = \square^r \Gamma(u,q)$.

We begin with cyclic codes constructed from $\mathcal{C}(3,q)$.

Theorem 5.1. *Let p and r be different primes with $p \equiv 1 \pmod 3$ and let c, k, m, q, t be integers such that $m = 3t$, $q = p^m$, $c = \frac{q-1}{3}$ and $k = \frac{3}{r}\Psi_r(q)$. If $q \equiv 1 \pmod r$ and $(3,r)=1$, then the weights of $\mathcal{C}(k,q^r)$ are given by*

$$w_{\ell_1,\ell_2,\ell_3} = \tfrac{p-1}{3p}\{hq + (a(\tfrac{\ell_2+\ell_3}{2} - \ell_1) + \tfrac{9b}{2}(\ell_2-\ell_3))p^t\}$$

where $(\ell_1,\ell_2,\ell_3) \in \mathbb{N}_0^3$ such that $0 \le h = \ell_1+\ell_2+\ell_3 \le r$, and a, b are the unique integers satisfying

$$4p^t = a^2 + 27b^2, \qquad a \equiv 1 \pmod 3 \qquad \text{and} \qquad (a,p) = 1,$$

with corresponding frequencies

$$A_{\ell_1,\ell_2,\ell_3} = \tbinom{r}{h}\tbinom{h}{\ell_1,\ell_2,\ell_3} c^h.$$

Proof. The spectrum of $\mathcal{C}(3,q)$ is given in Theorems 19 and 20 in [7], with different notations (r for our q, N for our k, etc).

If $p \equiv 1 \pmod 3$, by Theorem 19 in [7], the four weights of $\mathcal{C}(3,q)$ are $w_0 = 0$,

$$w_1 = \tfrac{(p-1)(q-a\sqrt[3]{q})}{3p}, \;\; w_2 = \tfrac{(p-1)(q+\frac12(a+9b)\sqrt[3]{q})}{3p}, \;\; w_3 = \tfrac{(p-1)(q+\frac12(a-9b)\sqrt[3]{q})}{3p}, \tag{23}$$

with frequencies $A_0 = 1$ and $A_1 = A_2 = A_3 = \frac{q-1}{3} = c$; where a and b are the only integers satisfying $4\sqrt[3]{q} = a^2+27b^2$, $a \equiv 1 \pmod 3$ and $(a,p)=1$. Clearly, $3 \mid \frac{q-1}{p-1}$, since $p \equiv 1 \pmod 3$ and $m = 3t$. Moreover, c is a primitive divisor of $p^m - 1$, since the associated graph $\Gamma(3,p^m)$ is connected.

Assume now that $(3,r) = 1$ and $q \equiv 1 \pmod r$, we will show now that $n = rc = r(\frac{q-1}{3})$ is a primitive divisor of $q^r - 1$. Notice that the statement $n \mid q^r - 1$

is equivalent to $r \mid 3\,\Psi_r(q)$, since $\Psi_r(q) = \frac{q^r-1}{q-1}$. By hypothesis $q \equiv 1 \pmod r$, this implies that

$$\Psi_r(q) = \sum_{i=0}^{r-1} q^i \equiv r \equiv 0 \pmod r.$$

Thus $n \mid q^r - 1$ as desired.

It is enough to show that $n \not| p^l - 1$ for all $1 \le l \le r-1$. Assume first that $m \mid l$, i.e $l = hm$ for some $1 \le h \le r-1$, then the statement $n \not| p^{hm} - 1$ is equivalent to $r \not| 3\,\Psi_h(q)$ and this is equivalent to $r \not| \Psi_h(q)$ since $(3,r) = 1$. By hypothesis $q \equiv 1 \pmod r$, then $\Psi_h(q) \equiv h \not\equiv 0 \pmod r$, therefore $n \not| p^{hm} - 1$ for all $1 \le h \le r-1$.

On the other hand, if $l < m$ then n cannot divide $p^l - 1$, since c divides n and c is a primitive divisor of $p^m - 1$. On the other hand, if $m \le l \le rm$ and $n \mid p^l - 1$ we necessarily have that $m \mid l$. Indeed, if $l = md + e$ with $0 \le e < m-1$ then

$$p^l \equiv p^e \pmod c.$$

But $p^l \equiv 1 \pmod c$ since $c \mid n$. The primitive divisibility of c implies that $e = 0$, therefore $m \mid l$, that is $l = hm$ with $1 \le h \le r-1$. By the last case $n \not| p^{hm} - 1$ for all $1 \le h \le r-1$, therefore n is a primitive divisor of $q^r - 1$, as desired.

The statement now follows from Theorem 2.2 proceeding as in the proofs of Propositions 3.1 and 4.1. □

Example 5.2. In the notation of the previous theorem, let $p = 7$, $r = 2$, $t = 1$, $m = 3t = 3$, $q = p^3 = 343$, and hence $c = \frac{q-1}{3} = 114$. Clearly $p \equiv 1 \pmod 3$, $(r,3) = 1$ and $q \equiv 1 \pmod r$. In this case, it is not difficult to see that $a = b = 1$ satisfying $4\sqrt[3]{q} = a^2 + 27b^2$ with $(a,p) = 1$ and $a \equiv 1 \pmod 3$.

By the last theorem, the weights of the irreducible cyclic code $\mathcal{C}(\frac{3(q+1)}{2}, q^2) = \mathcal{C}(516, 7^6)$, after routine calculations, are given by

$$w_{\ell_1,\ell_2,\ell_3} = 2\,(49\,h - \ell_1 + 5\ell_2 - 4\ell_3)$$

for $0 \le h = \ell_1+\ell_2+\ell_3 \le 2$ with ℓ_i's non-negative integers, with frequencies A_{ℓ_1,ℓ_2,ℓ_3}. By a simple analysis of cases, we obtain that the weight distribution of $\mathcal{C}(516, 7^6)$ is given by Table 2. ◊

TABLE 2. Weight distribution of $\mathcal{C}(516, 7^6)$.

weight	frequency	weight	frequency
$w_{0,0,0} = 0$	$A_{0,0,0} = 1$	$w_{0,2,0} = 216$	$A_{0,2,0} = 114^2$
$w_{1,0,0} = 96$	$A_{1,0,0} = 228$	$w_{0,0,2} = 180$	$A_{0,0,2} = 114^2$
$w_{0,1,0} = 108$	$A_{0,1,0} = 228$	$w_{1,1,0} = 204$	$A_{1,1,0} = 2 \cdot 114^2$
$w_{0,0,1} = 90$	$A_{0,0,1} = 228$	$w_{1,0,1} = 186$	$A_{1,0,1} = 2 \cdot 114^2$
$w_{2,0,0} = 192$	$A_{2,0,0} = 114^2$	$w_{0,1,1} = 198$	$A_{0,1,1} = 2 \cdot 114^2$

Proceeding similarly as in the proof of the previous theorem, one can obtain the weight distribution of irreducible cyclic codes obtained from $\mathcal{C}(4, q)$. We leave the details to the reader.

Theorem 5.3. *Let p, and r be different primes with $p \equiv 1 \pmod 4$ and let c, k, m, q, t be integers such that $m = 4t$, $q = p^m$, $c = \frac{q-1}{4}$ and $k = \frac{4}{r}\Psi_r(q)$. If $q \equiv 1 \pmod r$ and $(4, r) = 1$, then the weights of $\mathcal{C}(k, q^r)$ are given by*

$$w_{\ell_1,\ell_2,\ell_3,\ell_4} = \tfrac{p-1}{4p}\{hq + (\ell_1 + \ell_2 - \ell_3 - \ell_4)\sqrt{q} + (2a(\ell_1 - \ell_2) + 4b(\ell_3 - \ell_4))p^t\}$$

for $0 \le h = \ell_1 + \ell_2 + \ell_3 + \ell_4 \le r$ with $(\ell_1, \ell_2, \ell_3, \ell_4) \in \mathbb{N}_0^4$, where a, b are the unique integers satisfying

$$\sqrt{q} = a^2 + 4b^2, \qquad a \equiv 1 \pmod 4 \qquad \text{and} \qquad (a, p) = 1.$$

with frequencies

$$A_{\ell_1,\ell_2,\ell_3,\ell_4} = \tbinom{r}{h}\tbinom{h}{\ell_1,\ell_2,\ell_3,\ell_4}c^h.$$

Remark 5.4. The condition $k \mid \frac{q-1}{p-1}$, which allows us to switch between the spectrum of the graph $\Gamma(k, q)$ and the weight distribution of the code $\mathcal{C}(k, q)$, implies that $p \equiv \pm 1 \pmod k$ for $k = 3, 4$. The cases not covered by Theorems 5.1 and 5.3, that is $p \equiv -1 \pmod k$ with $k = 3, 4$, are semiprimitive ones and fall into the case of Theorem 4.1.

6. Number of rational points of Artin-Schreier curves

In this section we consider Artin-Schreier curves $C_{k,\beta}(p^m)$ with affine equations

$$C_{k,\beta}(p^m): \qquad y^p - y = \beta x^k, \quad \beta \in \mathbb{F}_{p^m} \tag{24}$$

with $k \mid p^m - 1$. A good treatment of Artin-Schreier curves can be found in Chapter 3 by Güneri-Özbudak in [11].

We begin by establishing a direct relationship between the number of rational points of $C_{k,\beta}(p^m)$ and the eigenvalue λ_β of $\Gamma(k, p^m)$ –see equation (2)–.

Proposition 6.1. *Let p be a prime and let k, n, m be positive integers such that $k \mid \frac{p^m-1}{p-1}$ and $n = \frac{p^m-1}{k}$. If n is a primitive divisor of $p^m - 1$ then*

$$\#C_{k,\beta}(p^m) = 2p^m + k(p-1)\lambda_\beta \tag{25}$$

for all $\beta \in \mathbb{F}_{p^m}$.

Proof. The code $\mathcal{C}_k = \{c_k(\beta) = (\mathrm{Tr}_{p^m/p}(\beta x^k))_{x \in \mathbb{F}_{p^m}^*} : \beta \in \mathbb{F}_{p^m}\}$ is obtained from k-copies of $\mathcal{C}(k, p^m)$. This implies that

$$w(c_k(\beta)) = k\, w(c(\beta)) \qquad \text{where} \qquad c_k(\beta) = \big(\mathrm{Tr}_{p^m/p}(\beta\omega^{ik})\big)_{i=1}^n.$$

On the other hand, the weight of the codeword $c_k(\beta)$ is related to the number of $\mathbb{F}_{p^m}$-rational points of the curve $C_{k,\beta}(p^m)$. In fact, by Theorem 90 of Hilbert we have

$$\mathrm{Tr}_{p^m/p}(\beta x^k) = 0 \qquad \Leftrightarrow \qquad y^p - y = \beta x^k \quad \text{for some } y \in \mathbb{F}_{p^m}.$$

Since $C_{k,\beta}(p^m)$ is a p-covering of $\mathbb{P}^1$, considering the point at infinity, we get

$$\#C_{k,\beta}(p^m) = 1 + p\,\#\{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_{p^m/p}(\beta x^k) = 0\} = p^{m+1} - p\, w(c_k(\beta)) + 1.$$

Then, equation (25) follows directly from the last equality and (9). $\square$

Artin-Schreier curves over extensions. As an application of Theorem 2.2, we will next obtain a relationship between the rational points of Artin-Schreier curves as in (24) defined over two different fields

$$\mathbb{F}_{p^a} \subset \mathbb{F}_{p^m},$$

with p a fixed prime. We recall the notation $\Psi_b(x) = \frac{x^b-1}{x-1} = x^{b-1} + \cdots + x^2 + x + 1$.

Corollary 6.2. *Let p be a prime and let $k, m = ab, n, a, b, c, u$ as in Theorem 2.2. Then, for each $\beta \in \mathbb{F}_{p^m}$ there are $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{p^a}$ such that*

$$\#C_{k,\beta}(p^m) = \tfrac{1}{b}\Psi_b(p^a) \sum_{i=1}^{b} \#C_{u,\alpha_i}(p^a) - (p+1)p^a \Psi_{b-1}(p^a). \tag{26}$$

Conversely, given $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{p^a}$ there exists $\beta \in \mathbb{F}_{p^m}$ satisfying (26).

Proof. Consider the cyclic codes $\mathcal{C}_k$ and $\mathcal{C}(k, p^m)$ as before and the analogous ones $\mathcal{C}_u$ and $\mathcal{C}(u, p^a)$. Proceeding similarly as in the the proof of Proposition 6.1, we have that

$$\#C_{u,\alpha}(\mathbb{F}_{p^a}) = 1 + p \cdot \#\{x \in \mathbb{F}_{p^a} : \mathrm{Tr}_{p^a/p}(\alpha x^u) = 0\} = p^{a+1} - p\, w(c_u(\alpha)) + 1.$$

First notice that $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^m}$. Now, by Theorem 2.2, for each element $\beta \in \mathbb{F}_{p^m}$ there exist elements $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{p^a}$ such that $w(c(\beta)) = w(c(\alpha_1)) + \cdots + w(c(\alpha_b))$. Moreover, given $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{p^a}$, $w(c(\alpha_1)) + \cdots + w(c(\alpha_b))$ defines a weight in $\mathcal{C}(k, p^m)$, i.e. there must be some $\beta \in \mathbb{F}_{p^m}$ such that

$$w(c(\beta)) = w(c(\alpha_1)) + \cdots + w(c(\alpha_b)).$$

Therefore, the number $\#C_{k,\beta}(p^m)$ equals

$$p^{m+1} + 1 - pk \sum_{i=1}^{b} w(c(\alpha_i)) = p^{m+1} + 1 - \tfrac{k}{u} \sum_{i=1}^{b} (p^{a+1} + 1 - \#C_{u,\alpha_i}(p^a)). \tag{27}$$

Since $\frac{k}{u} = \frac{p^m-1}{b(p^a-1)} = \frac{1}{b}\Psi_b(p^a)$, after straightforward calculations we get (26) as desired. □

In particular, from (26) we have

$$\#C_{k,\beta}(p^m) \equiv \tfrac{1}{b}\Psi_b(p^a) \sum_{i=1}^{b} \#C_{u,\alpha_i}(p^a) \pmod{M}$$

with $M = p+1$, $M = p^a$ or $\Psi_{b-1}(p^a)$. Since $\Psi_{t+1}(x) = x^t + \Psi_t(x)$, taking $x = p^a$ and $t = b-1$ we also have

$$b \cdot \#C_{k,\beta}(p^m) \equiv p^{a(b-1)} \sum_{i=1}^{b} \#C_{u,\alpha_i}(p^a) \qquad (\mathrm{mod}\ \Psi_{b-1}(p^a)).$$

Example 6.3. In the notations of Theorem 2.2, take $p = 2$ and $u = 1$. Hence, $c = 2^a - 1$, $n = b(2^a - 1)$ and $m = ab$. Obviously $2^a - 1$ is a primitive divisor of itself and it can be shown that if b is odd and $x = 2^a \equiv 1 \pmod{b}$ then n is a primitive divisor of $2^m - 1$. If $k = \Psi_b(x)$, by the last corollary the $\mathbb{F}_{2^m}$-rational points of the curve

$$C_{k,\beta}(2^m): \quad y^2 + y = \beta x^k \tag{28}$$

with $\beta \in \mathbb{F}_{2^m}$ can be calculated in terms of the $\mathbb{F}_{2^a}$-rational points of the curves

$$C_{1,\alpha_i}(2^a): \quad y^2 + y = \alpha_i x$$

for some $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{2^a}$.

The simplex code $\mathcal{C}(1, 2^a)$ has only one nonzero weight, which is 2^{a-1}. Taking into account that

$$\#C_{1,\alpha}(2^a) = 2^{a+1} - 2w(c_1(\alpha)) + 1$$

with $w(c_1(\alpha)) \in \mathcal{C}(1, 2^a)$ we have that $\#C_{1,\alpha}(2^a) = 2^{a+1}+1$ or 2^a+1 for all $\alpha \in \mathbb{F}_{2^a}$. By (27) and Corollary 6.2, we have that the number of $\mathbb{F}_{2^m}$-rational points of each curve in (28) is given by $2^{m+1} + 1 - k\ell 2^a$ for some ℓ depending on β ranging over all the interval $0 \leq \ell \leq b$, that is

$$\{\#C_{k,\beta}(2^m)\}_{\beta \in \mathbb{F}_{2^m}} = \{2^{m+1} + 1 - k\ell 2^a : 0 \leq \ell \leq b\}.$$

7. A reduction formula for Gaussian periods

The Gaussian periods $\eta_i^{(N,q)}$ defined in (3) satisfy some arithmetic relations. From Theorem 14 in [7], we have the following integrality results:

$$\eta_i^{(N,q)} \in \mathbb{Z} \qquad \text{and} \qquad N\eta_i^{(N,q)} + 1 \equiv 0 \pmod p \tag{29}$$

where $q = p^m$ and $N = gcd(\frac{q-1}{p-1}, k)$. Furthermore, if $k \mid \frac{q-1}{p-1}$ then $N = k$ and we have

$$\sum_{i=0}^{k-1} \eta_i^{(k,q)} = -1 \qquad \text{and} \qquad \sum_{i=0}^{k-1} \eta_i^{(k,q)} \eta_{i+j}^{(k,q)} = q\theta_j - n \quad (0 \leq j \leq k-1) \tag{30}$$

with $n = \frac{q-1}{k}$ and where $\theta_j = 1$ if and only if $-1 \in C_j^{(k,q)}$ and $\theta_j = 0$ otherwise (see [27]). Equivalently, $\theta_j = 1$ if and only if either n is even and $j = 0$ or else n is odd and $j = \frac{k}{2}$. Apart from (29) and (30), there are not many known relations for Gaussian periods (to our best knowledge).

As another application of Theorem 2.2, we next give a relation between Gaussian periods defined over two different fields $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^m}$, showing that one can reduce the computation of $\eta_i^{(k,q)}$ to integral linear combinations of Gaussian periods $\eta_j^{(u,a)}$ with smaller parameters, namely $u \mid k$ and $a \mid m$.

Proposition 7.1. *Let p be a prime and let k, m, n, a, b, c, u be integers as in Theorem 2.2. Then, for each $i = 0, \ldots, k-1$ there exist integers $s \in \mathbb{N}$ and $\ell_0, \ell_1, \ldots, \ell_s \in \mathbb{N}_0$ such that*

$$\eta_i^{(k,p^m)} = c\ell_0 + \sum_{j=1}^{s} \ell_j \eta_{i_j}^{(u,p^a)} \tag{31}$$

where the ℓ_i's run over all possible $(s+1)$-tuples $(\ell_0, \ldots, \ell_s)$ such that $\ell_0 + \cdots + \ell_s = b$ different from $(b, 0, \ldots, 0)$.

Proof. By hypothesis, $\Gamma = \Gamma(k, p^m)$ decomposes as $\Gamma = \Box^b \Gamma_0$ where $\Gamma_0 = \Gamma(u, p^a)$. Let $q = p^m$ and $z = p^a$. We know that the spectra of Γ and Γ_0 are given in terms of Gaussian periods. In fact, by Theorem 2.1 in [20] we have that

$$\begin{aligned} Spec(\Gamma(k,q)) &= \{\Lambda_0 = n, \quad \Lambda_1 = \eta_1^{(k,q)}, \quad \ldots, \quad \Lambda_{k-1} = \eta_{k-1}^{(k,q)}\}, \\ Spec(\Gamma(u,z)) &= \{\lambda_0 = c, \quad \lambda_1 = \eta_1^{(u,z)}, \quad \ldots, \quad \lambda_{u-1} = \eta_{u-1}^{(u,z)}\}. \end{aligned} \tag{32}$$

By (17) in the proof of Theorem 2.2, the eigenvalues of Γ and of Γ_0 are related by the expression

$$\Lambda_{\ell_0,\ldots,\ell_s} = \ell_0\lambda_0 + \cdots + \ell_s\lambda_s \tag{33}$$

where $\ell_0, \ldots, \ell_s$ are integers satisfying $\ell_0 + \cdots + \ell_s = b$. By (32) and (33) we have (31). It remains to rule out all the cases giving

$$\eta_i^{(k,q)} = n = bc.$$

But the only way to have $\eta_i^{(k,q)} = n$ is given by $(\ell_0, \ell_1, \ldots, \ell_s) = (b, 0, \ldots, 0)$, since $\ell_0 + \cdots + \ell_s = b$, and the result thus follows. □

Remark 7.2. The Gaussian periods $\eta_0^{(k,q)}, \ldots, \eta_{k-1}^{(k,q)}$ with (k,q) a semiprimitive pair are explicitly known (see Lemma 13 in [7]).

We now show that if $\Gamma = \Gamma(k, p^m)$ is Cartesian decomposable, say $\Gamma \simeq \square^b \Gamma_0$, with $\Gamma_0 = \Gamma(u, p^a)$ a semiprimitive GP-graph then we can explicitly compute the Gaussian periods $\eta_i^{(k,p^m)}$.

Proposition 7.3. *Let $q = p^m$ with p prime and $k \mid q-1$ such that $n = \frac{q-1}{k} = bc$ where $m = ab$, $u = \frac{p^a-1}{c}$ and (u, p^a) is a semiprimitive pair. Then, the different Gaussian periods modulo q are given by*

$$\eta_i^{(k,q)} = \ell_0 c + \ell_1 \tfrac{(u-1)\sigma\sqrt{p^a}-1}{u} - \ell_2 \tfrac{\sigma\sqrt{p^a}+1}{u} \tag{34}$$

where the non-negative integers ℓ_0, ℓ_1, ℓ_2 run in the set

$$\{(\ell_0, \ell_1, \ell_2) : \ell_0 + \ell_1 + \ell_2 = b\} \setminus \{(b, 0, 0)\}$$

and $\sigma = (-1)^{\frac{a}{2t}+1}$ with t the least integer j such that $u \mid p^j + 1$.

Proof. By Corollary 7.1 we have an expression for each $\eta_i^{(k,q)}$ in terms of the $\eta_j^{(u,p^a)}$'s. Since (u, p^a) is a semiprimitive pair, there are only two different such periods, given by (3.4) and (3.5) of [20], depending the case. In case (a), that is $p, \alpha = \frac{p^t+1}{u}$ and $s = \frac{a}{2t}$ odd, we have

$$\eta_0^{(u,p^a)} = \tfrac{(u-1)\sqrt{p^a}-1}{u} \qquad \text{and} \qquad \eta_1^{(u,p^a)} = -\tfrac{\sqrt{p^a}+1}{u}$$

while in case (b) we have

$$\eta_0^{(u,p^a)} = -\tfrac{\sigma\sqrt{p^a}+1}{u} \qquad \text{and} \qquad \eta_1^{(u,p^a)} = \tfrac{\sigma(u-1)\sqrt{p^a}-1}{u}.$$

Now, by (31) we get

$$\eta_i = \ell_0\, c + \ell_1\, \eta_0^{(u,p^a)} + \ell_2\, \eta_1^{(u,p^a)}.$$

Since the triples (ℓ_0, ℓ_1, ℓ_2) satisfying $\ell_0 + \ell_1 + \ell_2 = b$ are symmetric, the above expression is the same no matter if we are in case of (a) or (b), or if σ is 1 or -1, and hence we get (34). □

Example 7.4. Take $u = 2$, $a = 2$, $b = 3$ and $p = 5$. Then $(u, p^a) = (2, 5^2)$ is a semiprimitive pair and $\Gamma_0 = \Gamma(2, 5^2) = P(25)$, a classic Paley graph. Thus, we have $m = ab = 6$, $q = 5^6 = 15.625$, $c = \frac{p^a-1}{u} = \frac{5^2-1}{2} = 12$ and $n = bc = 36$; hence $k = \frac{q-1}{n} = 434$.

By (34), the Gaussian periods for $(k, q) = (434, 15.625)$ are given by

$$\eta_i^{(434,15.625)} = 12\ell_0 + 2\ell_1 - 3\ell_2$$

where $\ell_0 + \ell_1 + \ell_2 = 3$ and $(\ell_0, \ell_1, \ell_2) \neq (3, 0, 0)$; compare with (3). There are 9 such triples, namely $(2,1,0)$, $(2,0,1)$, $(1,2,0)$, $(1,1,1)$, $(1,0,2)$, $(0,3,0)$, $(0,2,1)$, $(0,1,2)$ and $(0,0,3)$. Thus, we have that

$$\eta_1 = 26,\ \eta_2 = 21,\ \eta_3 = 16,\ \ \eta_4 = 11,\ \ \eta_5 = \eta_6 = 6,\ \ \eta_7 = 1,\ \ \eta_8 = -4,\ \ \eta_9 = -9.$$

Note that $\eta_i \equiv 1 \pmod 5$ for $1 \le i \le 9$ as it should be, since $k\eta_i \equiv -1 \pmod p$ by (29).

We now check the expressions in (30). If $\eta_i^{(k,q)}$ is associated with (ℓ_0, ℓ_1, ℓ_2), then its frequency is given by $\mu_i = \frac{1}{n} A_i$ where

$$A_i = A_{\ell_0,\ell_1,\ell_2} = \tbinom{3}{\ell_0,\ell_1,\ell_2} m_0^{\ell_0} m_1^{\ell_1} m_2^{\ell_2},$$

with m_0, m_1, m_2 the multiplicities of the Paley graph $P(25)$. The spectrum of $P(q)$ is well-known and it is given by

$$Spec(P(p^2)) = \{[\tfrac{p^2-1}{2}]^1, [\tfrac{p-1}{2}]^n, [\tfrac{-p-1}{2}]^n\}$$

with $n = \frac{p^2-1}{2}$. Hence, $Spec(P(25)) = \{[12]^1, [2]^{12}, [-3]^{12}\}$ and we thus have $m_0 = 1$ and $m_1 = m_2 = 12$. In this way we obtain

$$\begin{gathered} A_{2,1,0} = A_{2,0,1} = 3 \cdot 12 = 36, \qquad A_{1,2,0} = A_{1,0,2} = 3 \cdot 12^2 = 432, \\ A_{1,1,1} = 6 \cdot 12^2 = 684, \qquad A_{0,2,1} = A_{0,1,2} = 3 \cdot 12^3 = 5184, \\ A_{0,3,0} = A_{0,0,3} = 1 \cdot 12^3 = 1728, \end{gathered}$$

and hence

$$\mu_1 = \mu_2 = 1, \quad \mu_3 = \mu_5 = 12, \quad \mu_4 = 24, \quad \mu_6 = \mu_9 = 48, \quad \mu_7 = \mu_8 = 144.$$

Therefore we have

$$\sum_{i=0}^{433} \eta_i^{(434,5^6)} = \sum_{i=1}^{9} \mu_i \eta_i$$

and hence

$$\begin{aligned} \sum_{i=0}^{433} \eta_i^{(434,5^6)} &= \mu_1(\eta_1+\eta_2) + \mu_3(\eta_3+\eta_5) + \mu_4\eta_4 + \mu_6(\eta_6+\eta_9) + \mu_7(\eta_7+\eta_8) \\ &= (26+21) + 12(16+6) + 24 \cdot 11 + 48(6-9) + 144(1-4) = -1. \end{aligned}$$

One can also check that

$$\sum_{i=1}^{9} \mu_i \eta_i^2 = 15.589 = q - n \qquad \text{and} \qquad \sum_{i=1}^{9} \mu_i \mu_{i+j} \eta_i \eta_{i+j} = -36 = -n$$

for $j = 1, \ldots, 9$, and hence the second identity of (30) holds. ♢

References

[1] R. Akhtar, T. Jackson-Henderson, R. Karpman, M. Boggess, I. Jiménez, A. Kinzel and D. Pritikin, On the unitary Cayley graph of a finite ring, *Electron. J. Combin.* **16** (2009), 117–130.

[2] L. D. Baumert and R. J. McEliece, Weights of irreducible cyclic codes, *Information and Control*, **20** (1972), 158–175.

[3] B. Berndt, R. J. Evans and K. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[4] D. Cvetkovic, M. Doobs and H. Sachs, *Spectra of Graphs*, Pure and Applied Mathematics, Academic Press, 1980.

[5] C. Ding, The weight distribution of some irreducible cyclic codes, *IEEE Trans. Inform. Theory*, **55** (2009), 955–960.

[6] C. Ding, A class of three-weight and four-weight codes, *Lecture Notes in Computer Science*, **5557**, Springer Verlag, (2009) 34–42.

[7] C. Ding and J. Yang, Hamming weights in irreducible cyclic codes, *Discrete Mathematics*, **313** (2013), 434–446.

[8] H. Q. Dinh, C. Li and Q. Yue, Recent progress on weight distributions of cyclic codes over finite fields, *J. Algebra Comb. Discrete Struct. Appl.*, **2** (2015), 39–63.

[9] K. Feng and J. Luo, Weight distribution of some reducible cyclic codes, *Finite Fields Appl.*, **14** (2008), 390–409.

[10] C. D. Godsil and G. F. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, Springer, 2001.

[11] A. Garcia and H. Stichtenoth, *Topics in Geometry, Coding Theory and Cryptography*, Algebra and Applications, Springer, 2007.

[12] R. Hammack, W. Imrich and S. Klavžar, *Handbook of Product Graphs*, CRC Press 2nd edition, 2011.

[13] W. Imrich and S. Klavžar, *Product Graphs: Structure and Recognition*, Wiley-Interscience, 2000.

[14] S. Li, S. Hu, T. Feng and G. Ge, The weight distribution of a class of cyclic codes related to Hermitian forms graphs, *IEEE Trans. Inform. Theory*, **59** (2013), 3064–3067.

[15] C. Li, Q. Yue and F. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements, *Finite Fields Appl.*, **28** (2014), 94–114.

[16] T. K. Lim and C. Praeger, On Generalised Paley Graphs and their automorphism groups, *Michigan Math. J.*, **58** (2009), 293–308.

[17] R. J. McEliece, Irreducible cyclic codes and Gauss sums, Combinatorics in: Proc. NATO Adv. Study Inst., Breukelen, 1974. Math. Centre Tracts 55, Math. Centrum, Amsterdam, 1974.

[18] G. Pearce and C. Praeger, Generalised Paley graphs with a product structure, *Ann. Comb.*, **23** (2019), 171–182.

[19] R. A. Podestá and D. E. Videla, The spectra of generalized Paley graphs of $q^\ell + 1$ powers and applications, preprint, `arXiv:1812.03332`.

[20] R. A. Podestá and D. E. Videla, Spectral properties of generalized Paley graphs and of their associated irreducible cyclic codes, preprint, `arXiv:1908.08097v2`.

[21] R. A. Podestá and D. E. Videla, The Waring's problem over finite fields through generalized Paley graphs, *Discrete Mathematics*, **344** (2021), 112324.

[22] A. Rao and N. Pinnawala, A family of two-weight irreducible cyclic codes, *IEEE Trans. Inform. Theory*, **56** (2010), 2568–2570.

[23] G. Sabidussi, Graphs with given group and given graph-theoretical properties, *Canadian Journal of Mathematics*, **9** (1957), 515–525.

[24] G. Sabidussi, Graph multiplication, *Mathematische Zeitschrift*, **72** (1960), 446–457.

[25] B. Schmidt and C. White, All two weight irreducible cyclic codes, *Finite Fields Appl.*, **8** (2002), 1–17.

[26] A. Sharma and G. K. Bakshi, The weight distribution of some irreducible cyclic codes, *Finite Fields Appl.*, **18** (2012), 144–159.

[27] T. Storer. *Cyclotomy and Difference Sets*, Markham Publishing Co., Chicago, 1967.

[28] G. Vega and J. Wolfmann, New classes of 2-weight cyclic codes, *Des. Codes Cryptogr.*, **42** (2007), 327–334.

[29] Z. Zhou, A. Zhang, C. Ding and M. Xiong, The weight enumerator of three families of cyclic codes, *IEEE Trans. Inform. Theory*, **59** (2013), 6002–6009.

Received February 2020; revised February 2021.

E-mail address: `podesta@famaf.unc.edu.ar`
E-mail address: `devidela@famaf.unc.edu.ar`