UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

Master's Thesis
(Magistrsko Delo)

Strongly regular Cayley graphs over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$

(Krepko regularni Cayleyjevi grafi nad $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$)

Ime in Priimek: Luigi Fatigato
Študijski program: Matematične znanosti, 2. stopnja
Mentor: prof. dr. István Kovács

Koper, oktober 2020

Ključna dokumentacijska informacija

Ime in PRIIMEK: Luigi FATIGATO

Naslov zaključne naloge: Krepki regularni Cayleyjevi grafi nad $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$

Kraj: Koper

Leto: 2020

Število listov: 71 Število slik: 15 Število tabel: 4

Število prilog: 1 Število strani prilog: 11 Število referenc: 19

Mentor: prof. dr. István Kovács,

UDK: 519.17 (043.2)

Ključne besede: Cayleyjevi grafi, Schurjeva metoda, Krepko regularni Cayleyjevi grafi, Schurjevi obroči

Math. Subj. Class. (2010): 05C25, 05C60, 20B25

Izvleček:
To magistrsko delo predstavlja klasifikacijo krepkih regularnih Cayleyjevih grafov nad grupah $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$, pridobljeno v [14] po Schurjevi metodi, kjer je p liho pravštevilo. V primeru ko je $p = 2$, je zbranih tudi nekaj rezultatov numerične analize.

Key document information

Name and SURNAME: Luigi FATIGATO

Title of final project paper: Strongly regular Cayley graphs over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$

Place: Koper

Year: 2020

Number of pages: 71 Number of figures: 15 Number of tables: 4

Number of appendices: 1 Number of appendix pages: 11
Number of references: 19

Mentor: Prof. István Kovács, PhD

UDC: 519.17 (043.2)

Keywords: Cayley graphs, Schur's method, Strongly regular Cayley graphs, Schur rings

Math. Subj. Class. (2010): 05C25, 05C60, 20B25

Abstract:

This master thesis presents the classification of strongly regular Cayley graphs over the groups $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ obtained in [14] using the Schur's method, where p is an odd prime. For the case when $p = 2$, some results from numerical analysis are also collected.

Acknowledgement

I want to thank my mentor, Prof. István Kovács, PhD, for his patient review of this work and for his precious hints and suggestions. I thank my wife for her daily presence in my life and finally I thank my parents for their love.

List of Contents

List of Tables

List of Figures

Appendices

Appendix A: Octave subroutines

1 Introduction

The concept of a strongly regular graph and that one of a finite commutative groups are both well known. Let (ν, k, λ, μ) be an ordered quadruple of integer numbers. A *strongly regular graph* with parameters (ν, k, λ, μ) is a non-complete, regular graph of ν nodes with valency k, such that for each pair (a, b) of adjacent nodes, there are λ nodes adjacent to both a and b, and for each pair (a, b) of not-adjacent nodes, there are μ nodes adjacent to both a and b, see e.g. the book [9]. Such graph is also called a (ν, k, λ, μ)-strongly regular graph. Let G be a finite group. A subset S of G is called symmetric if for each $s \in S$, $s^{-1} \in S$ also holds. Let us consider a symmetric subset S of G, S not containing the neutral element e. We can build a graph having elements of G as nodes; and given elements $a, b \in G$ are adjacent if $ab^{-1} \in S$. This graph is known in literature as *Cayley graph*, denoted by $\Gamma_G(S)$, see [9].

Strongly regular Cayley graphs are the main subjects of this thesis, and the abbreviation SRCG for strongly regular Cayley graph, and SRG for strongly regular graphs, will be used throughout the text. For instance, it was proved that SRCG's with so called Paley parameters over an abelian p-group do exist if and only if the corresponding group is isomorphic to $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. Then Y. I. Leifman and M. E. Muzychuk [14] studied the structure of SRCG's over the group $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ using the Schur ring method, assuming that p is an odd prime. That study led to a classification of these graphs. Their paper [14] is the basis of this work.

More precisely, they studied the *Schur ring* $W(G)$ whose basic quantities consist of the generators of cyclic subgroups of the group $G = \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. This was previously proved by Bridges and Mena [3], [4] to be the unique maximal Schur ring over G for which the irreducible characters of G take rational values on the basic quantities. The main tools are the *Hasse diagrams* of cyclic and co-cyclic subgroups of $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$, which turn out to be trees. Given an abelian group G, a co-cyclic subgroup is defined as a subgroup H of G such that G/H is a cyclic group. The tree of cyclic subgroups is denoted by the symbol Δ, the tree of co-cyclic groups is denoted by the symbol ∇.

Classes of equivalence are set up among irreducible characters having the same kernel, and it is proved that kernels are co-cyclic groups. The first massive result is a precise evaluation of the characters on the nodes of Δ.

For each element $F \in \Delta$, those character value are positive if $F \subseteq H$, negative if

$|F| = p|F \cap H|$, and 0 otherwise. This result is crucial to prove many other theorems and lemmas.

The key property that a subset S of Δ not containing the trivial subgroup could have or not is *homogeneity*. This property regards the evaluation of the cardinality of the set resulting from the intersection between S and the set of the sons of a generic element H chosen into an appropriate subset of Δ. In the main theorem Y. I. Leifman and M. E. Muzychuk characterize all the subsets of Δ that correspond to strongly regular graphs in terms of homogeneity, see [14, Theorem 1.6].

There are essentially two aims in this thesis:

1. To create coding tools for calculating SRCG's over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ (characters and eigenvalues, calculation of cyclic and co-cyclic subgroups in a tree) based on the results of Y. I. Leifman and M. E. Muzychuk [14].

2. To investigate SRCG's over the group $\mathbb{Z}_{2^n} \oplus \mathbb{Z}_{2^n}$.

2 Strongly regular Cayley graphs and rational S-rings over finite abelian groups

In this chapter we will introduce some important and general concepts. Since there are different topics from algebra and combinatorics involved together in this thesis, we split this chapter in five sections. In the first one, we will discuss strongly regular graphs. In the second one, we will define S-rings and S-modules. We will need to introduce some notations and terminologies about trees, since we will do operations on trees to manage the rational S-rings over finite commutative groups. Finally, in the last two sections we will fix some concepts from representation theory and then we will introduce strongly regular Cayley graphs.

2.1 Strongly regular graphs

Main references: the readers will receive more information on strongly regular graphs from [9] and [2].

Definition 2.1.1. Let (ν, k, λ, μ) be an ordered quadruple of integer numbers. A *strongly regular graph* is a non-complete, regular graph of ν nodes with valency k, such that for each pair (a, b) of adjacent nodes, there are λ nodes adjacent to both a and b, and for each pair (a, b) of not-adjacent nodes, there are μ nodes adjacent to both a and b.

If Γ is a (ν, k, λ, μ)-strongly regular graph, then its complement $\overline{\Gamma}$ is also strongly regular, the parameters of which are $(\nu, \nu - 1 - k, \nu - 2k - 2 + \mu, \nu - 2k + \lambda)$.

Definition 2.1.2. Let Γ be a (ν, k, λ, μ)-strongly regular graph. Then Γ is said to be *trivial* if one between Γ and $\overline{\Gamma}$ is not connected.

Lemma 2.1.1. Let Γ be a (ν, k, λ, μ)-strongly regular graph. Then the following equality holds:

$$(\nu - k - 1)\mu = k(k - 1 - \lambda). \tag{2.1}$$

Proof. Let (u, v) be an edge of Γ. There are λ vertices adjacent to both u and v, hence there are $k-1-\lambda$ vertices adjacent to u but not to v. Then there are exactly $k(k-1-\lambda)$ edges in Γ which connects vertices non-adjacent to v with vertices adjacent to v. On the other hand, if (u, v) is not an edge of Γ, then u, v have μ common neighbours. Then the numbers of edges connecting vertices non-adjacent to v with vertices adjacent to v are $\mu(\nu - k - 1)$. □

Lemma 2.1.2. A strongly regular graph Γ is trivial if and only if $\mu = k$ or $\mu = 0$. Moreover, a trivial graph or its complementary graph is isomorphic to a disjoint union of complete graphs K_n.

Proof. Γ is connected if and only if $\mu > 0$ and its complement is connected if and only if $\overline{\mu} = \nu - 2k + \lambda > 0$.

It follows from eq.(2.1) that, if $\mu = k$, then $\nu - 2k + \lambda = 0$ and the graph $\overline{\Gamma}$ is disconnected. Equation (2.1) implies also that, if $\mu = 0$, then $k = 0$ (i.e. the set of edges is the empty set) or $\lambda = k - 1$ (i.e. disjoint union of complete graphs K_n). If $\mu = k$ then we reply the proof about the complementary graph. □

Proposition 2.1.1. Let Γ be a graph with adjacency matrix A, which is neither complete nor empty. Then Γ is strongly regular if and only if A^2 is a linear combination of A, I and J.

Proof. The ij-entry of A^2 is equal to the number of walks of length 2 from i to j. If Γ is strongly regular, then this number is k, λ or μ according to the fact whether i and j are the same vertex, two adjacent vertices or two non-adjacent vertices. Then we can write:

$$A^2 = k \cdot I + \lambda \cdot A + \mu \cdot (J - I - A).$$

The converse is almost the definition of strongly regular graph. □

Corollary 2.1.1. Let Γ be a (ν, k, λ, μ)-strongly regular graph. Let $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$. Then the eigenvalues of the adjacency matrix A are

$$k, \ \frac{(\lambda - \mu + \sqrt{\Delta})}{2}, \ \frac{(\lambda - \mu - \sqrt{\Delta})}{2}.$$

Definition 2.1.3. Let $\mathbb{F}_q$ be the finite field of q elements with $q \equiv 1(\text{mod } 4)$. The *Paley graph $P(q)$* is a strongly regular graph with parameters

$$(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}).$$

The nodes of $P(q)$ are the elements of $\mathbb{F}_q$, and given elements $a, b \in \mathbb{F}_q$ are adjacent if and only if their difference $a - b$ is a non-zero square in $\mathbb{F}_q$.

2.2 S-rings and S-modules

Definition 2.2.1. Let G be a multiplicative group. A *group ring* $R[G]$ is a free R-module with basis G and multiplication defined distributively using the given multiplication in G. In other words:

$$\left(\sum_{x\in G} a_x x\right)\left(\sum_{y\in G} b_y y\right) = \sum_{x,y\in G} (a_x b_y)(xy),$$

where $a_x, b_y \in K$.

Definition 2.2.2. Let R be a ring with unit 1. If K is a subset of a finite group G, then the group ring element $\sum_{g\in K} g \in R[G]$ is called a *simple quantity* and will be denoted by $\underline{K}$.

Definition 2.2.3. An *R-submodule* of $R[G]$ with a basis $\{\underline{T}_1 \ldots \underline{T}_k\}$ where $T_1, \ldots, T_k$ are mutually disjoint sets whose union is equal to G is called an *S-module over G* with standard basis $\{\underline{T}_1, \ldots, \underline{T}_k\}$.

Definition 2.2.4. An S-module C over G is called a *Schur ring* (or *S-ring* for short) over G if the following conditions are satisfied:

1. C is a subring of $R[G]$,
2. $1 \in C$,
3. $\sum_{g\in G} c_g g \in C \implies \sum_{g\in G} c_g g^{-1} \in C$.

A subset S of a group G is called *symmetric* if $x \in S \implies x^{-1} \in S$.

Definition 2.2.5. Let G be a group and let S be a symmetric subset of G, not containing the neutral element of G. The *Cayley graph* with generating set S over G, denoted by $\Gamma_G(S)$, is the graph having the elements of G as nodes, and two nodes f, g are adjacent if and only if $fg^{-1} \in S$.

The following theorem is well known:

Theorem 2.2.1. The Cayley graph $\Gamma_G(S)$ is a strongly regular graph if and only if $\langle 1, \underline{S}, \underline{G} - \underline{S} - 1\rangle$ is an S-ring over G.

It is easy to prove that, if either $\{S\} \cup \{e\}$ or $G \setminus S$ is a subgroup of G, then $\Gamma_G(S)$ is a trivial strongly regular graph. We conclude this subsection with the definition of a primitive S-ring.

Definition 2.2.6. An S-ring C over G is called *primitive* if $K = \{e\}$ and $K = G$ are the only subgroups of G for which $\underline{K} \in C$ holds.

2.3 Trees

Let us analyse the following rooted tree:

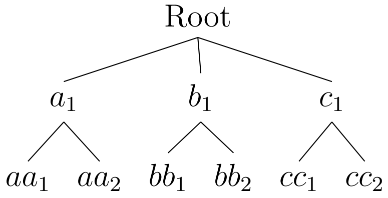


Figure 1: A tree

We fix some general terminology. The *length* of a node of the tree is the number of edges in the minimal path between the root and the node. If the node has a label N, then we indicate its length as $l(N)$.

Example 2.3.1. Consider the rooted tree shown above. Then we have:
$l(Root) = 0$,
$l(a_1) = l(b_1) = l(c_1) = 1$,
$l(aa_1) = l(aa_2) = l(bb_1) = l(bb_2) = l(cc_1) = l(cc_2) = 2$.

If two nodes S and P of a rooted tree are adjacent and $l(S) = l(P) + 1$, then S is called a *son* of P and P is called the *father* of S. This is also written as $P = Father(S)$.

A subset B consisting of all the sons of a common father is said to be a *block* and it is denoted by $B = Sons(P)$ if the common father is P. In this case P is also said to be the father of the block B and we write $P = Father(B)$.

Example 2.3.2. In the example above, bb_1 is son of b_1 and cc_1 is not son of b_1 since it is not adjacent to b_1. Furthermore, $\{cc_1, cc_2\} = Sons(c_1)$ is a block. But $\{cc_1\}$ is not a block since this does not consists of all sons of c_1. Note that, neither $\{cc_1, bb_1\}$ is a block.

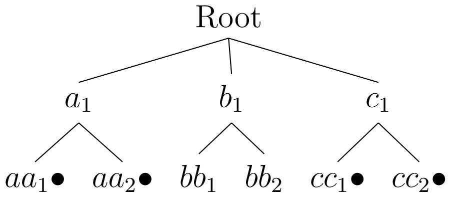
Definition 2.3.1. A *block set* is a union of blocks.

Example 2.3.3. In the example above, $\{bb_1, bb_2\} \cup \{a_1, b_1, c_1\}$ is a block set and $\{aa_1, aa_2\} \cup \{bb_1, bb_2\}$ is also a block set.

Definition 2.3.2. Two subsets of a rooted tree are said to be *block equivalent* if their symmetric difference is a block set.

Example 2.3.4. We put bullets next to nodes belonging to two subsets A and B which are block equivalent.

A:



B:

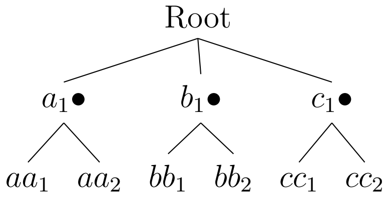


Figure 2: Block equivalent sets

Let T be a rooted tree. Then we denote with T_i its subset collecting all the nodes of T having length less or equal to i.

Example 2.3.5. If T is the one shown in the figure 3, then T_1 is the one shown in the figure 4

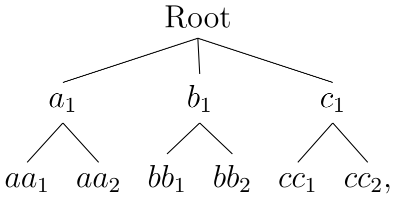


Figure 3: A tree T of length 2

Definition 2.3.3. Let T be a rooted tree and let N be a node of T. We define the *descendents* $Des_j(N)$ of N inductively as follows:

$Des_1(N) = Sons(N)$, and

$Des_j(N) = \{F : Father(F) \in Des_{j-1}(N)\}$ if $j > 1$.

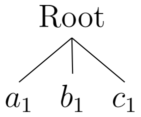


Figure 4: Subset of the previous tree T - nodes of length ≤ 1

Example 2.3.6. The block set $\{aa_1, aa_2\} \cup \{bb_1, bb_2\} \cup \{cc_1, cc_2\} = T_2 \backslash T_1$ is $Des_2(Root)$.

Definition 2.3.4. Let T be a rooted tree. Then we can build up another tree T^j. Its notes are the sets $Des_j(N)$, $N \in T$. Define the relation $\subseteq^j$ of T^j by letting $Des_j(N_1) \subseteq^j Des_j(N_2)$ if and only if $N_1 \subseteq N_2$. This relation is partial order, and the Hasse diagaram of the induced poset defines the tree T^j.

Example 2.3.7. If T is the tree in fig. 5, then the T^1 is the tree in fig. 6.

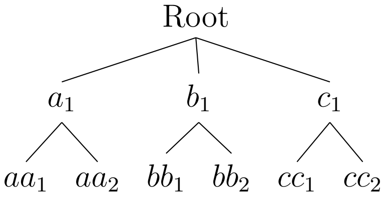


Figure 5: A Tree with leaves of length 2

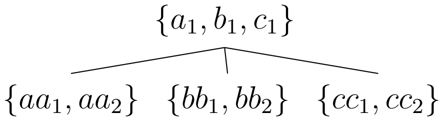


Figure 6: T^1 referred to the previous Tree

All the trees we will consider in this work are rooted, and the valency of each node of T, except the leaves which have valency 1, is $p+1$, where p is a certain prime number.

2.4 Representations, characters and abelian groups

Main references: the readers can find more information on these topics from [12].

Definition 2.4.1. Let G be a group. A *representation* of G over a field $\mathbb{F}$ is an homomorphism

$$\phi : G \to \mathrm{GL}(n, \mathbb{F})$$

for some n. The degree of a representation is the integer n.

Example 2.4.1. The dihedral group $D_8 = \langle a, b \mid a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle$ has the following representation:

$$\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \phi(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \phi(a^2) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \ \phi(a^3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\phi(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \phi(ab) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \phi(a^2b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \ \phi(a^3b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Definition 2.4.2. A representation ϕ is *faithful* if $\ker(\phi) = \{1\}$.

Definition 2.4.3. Two representations ϕ, ρ are *equivalent* if they have the same degree and if there exists an invertible matrix T such that $\forall g \in G : T^{-1} \cdot \phi(g) \cdot T = \rho(g)$.

Definition 2.4.4. Given a representation ϕ, the corresponding *character* χ is the function from G to $\mathbb{F}$ such that $\chi(g) = tr(\phi(g))$ for each $g \in G$.

We now introduce the concept of $\mathbb{F}[G]$-*module* and we show there is a close connection between $\mathbb{F}[G]$-modules and representations of G over $\mathbb{F}$.

Definition 2.4.5. Let V be a vector space over $\mathbb{F}$ and let G be a group. Then V is an $\mathbb{F}[G]$-*module* if a multiplication $v \cdot g$ $(v \in V, g \in G)$ is defined satisfying the following conditions for all $u, v \in V, \lambda \in \mathbb{F}, g, h \in G$:

- $v \cdot g \in V$,
- $(v \cdot g) \cdot h = v \cdot (gh)$,
- $v \cdot 1 = v$,
- $(\lambda v) \cdot g = \lambda(v \cdot g)$,
- $(u + v) \cdot g = u \cdot g + v \cdot g$,

We observe that the function $f : V \to V, v \mapsto v \cdot g, g \in G$ is an endomorphism of V.

Definition 2.4.6. Let V be an $\mathbb{F}[G]$-module, and let $\mathcal{B}$ be a basis for V. For each $g \in G$, let $[g]_{\mathcal{B}}$ denote the matrix of the endomorphism $v \to v \cdot g$ of V, relative to the basis $\mathcal{B}$.

The following theorem puts in relationship the concept of a representation and the one of an $\mathbb{F}[G]$-module.

Theorem 2.4.1. 1. If $\rho : G \to \mathrm{GL}(n, \mathbb{F})$ is a representation of G over $\mathbb{F}$, then $V = \mathbb{F}^n$ is an $\mathbb{F}[G]$-module whose multiplication $v{\cdot}g$ is defined by $v\rho(g)$. Moreover, there is a basis $\mathcal{B}$ such that $\rho(g) = [g]_{\mathcal{B}}$ for all $g \in G$.

2. Assume that V is an $\mathbb{F}[G]$-module and $\mathcal{B}$ a basis for V. Then the function $\rho : G \to \mathrm{GL}(n, \mathbb{F})$ defined by $\rho(g) = [g]_{\mathcal{B}}$, $g \in G$ is a representation of G over $\mathbb{F}$.

Given an $\mathbb{F}[G]$-module V, an $\mathbb{F}[G]$-*submodule* of V is a subspace W of V for which $w \cdot g \in W$ for all $g \in G, w \in W$.

Definition 2.4.7. an $\mathbb{F}[G]$-module V is said to be *irreducible*, if the only two $\mathbb{F}[G]$-submodules of V are $\{0\}$ and V. Similarly, a representation $\rho : G \to \mathrm{GL}(n, \mathbb{F})$ is irreducible if the corresponding $\mathbb{F}[G]$-module $V = \mathbb{F}^n$ is irreducible.

Definition 2.4.8. Let V and W be $\mathbb{F}[G]$-modules. A function $\theta : V \to W$ is an $\mathbb{F}[G]$-*homomorphism* if it is a linear trasformation and

$$\theta(v) \cdot g = \theta(v \cdot g).$$

An $\mathbb{F}[G]$-*isomorphism* is an invertible $\mathbb{F}[G]$-homomorphism.

The following two theorems are two milestones in the theory of representations. They are the Maschke Theorem and the Schur's Lemma.

Theorem 2.4.2. (Maschke Theorem) Let G be a finite group, let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, and let V be an $\mathbb{F}[G]$-module. If U is an $\mathbb{F}[G]$-submodule of V, then there exists an $\mathbb{F}[G]$-submodule W such that $V = U \oplus W$.

Lemma 2.4.1. (Schur's Lemma) Let V and W be two irreducible $\mathbb{C}[G]$-modules and let $\theta : V \to W$ be an $\mathbb{C}G$-homomorphism.

1. Then either θ is a $\mathbb{C}G$-isomorphism or $\theta v = 0$ for all $v \in V$.

2. If θ is a $\mathbb{C}G$-isomorphism, then θ is a scalar multiple of the identity endomorphism $\mathbf{1}_V$.

One of the consequences of the Schur's Lemma is that an irreducible representation of an abelian group G has degree 1. Indeed, if V is irreducible and G is abelian, then for $v \in V$ and $x, g \in G$, $vxg = vgx$, and so the mapping $f : v \mapsto vx$ is an $\mathbb{C}[G]$-homomorphism from V to itself. Then, by the Schur's lemma,

$$vx = \lambda_x v \text{ forall } v \in V.$$

This implies that every subspace of V is a $\mathbb{C}[G]$-submodule and by the hypotesis of irreducibility, $\dim(V) = 1$.

2.5 Cayley graphs

Main references: The readers can find more information on the topics of this section from [3], [15], [14], [17].
Let Irr(G) denote the set of all irredicuble caharacters of a group G. A character is irreducible if its representation is irreducible. We have already defined the concept of a Cayley graph. It is interesting to find the conditions on G and on S, such that the Cayley graph $\Gamma_G(S)$ turns out to be a strongly regular graph. A first great hypothesis on G is if is it abelian or not. In this work, since now, we will consider only finite abelian groups. Under this hypothesis, we can prove a first result: the following lemma.

Lemma 2.5.1. Let G be an abelian group, let S be a symmetric subset of G not containing the neutral element. Let A be the adjacency matrix of the Cayley graph $\Gamma_G(S)$. Then the rows of the character table of G form a complete set of eigenvectors for A, and the eigenvector belonging to the character ψ has the eigenvalue $\psi(\underline{S})$.

An important consequence of this lemma is that, if the Cayley graph is also strongly regular, for the Corollary 2.1.1 and for the Lemma 2.5.1, the Theorem 5.0.1 is proved. The following theorem shows the shape of a SRCG (strongly regular Cayley graph) over a commutative group with non-rational eigenvalues.

Theorem 2.5.1. Let G be an abelian group of order ν and S be a symmetric subset of $G \setminus \{e\}$. Suppose that there exists an (ν, k, λ, μ)-SRCG $\Gamma_G(S)$ such that $\delta = (\lambda-\mu)^2+4(k-\mu)$ is not a square. Then $\Gamma_G(S)$ is the Paley graph $P(\nu)$ with parameters $(\nu, \frac{\nu-1}{2}, \frac{\nu-5}{4}, \frac{\nu-1}{4})$ and $\nu = p^{2\eta+1}$ for some $p \equiv 1(\text{mod } 4)$ and integer η.

Definition 2.5.1. Let G be a finite abelian group of exponent m. Let $\mathbf{P}$(G) be the group of automorphisms of G of the form $x \to x^t$ where t ranges through all residues which are relatively prime to m. The orbits of this action are in a bijection with the cyclic subgroups of G. If $H \leqslant G$, then the set O_H of generators of H is an orbit of $\mathbf{P}$(G). Denote the S-module (with $\mathbb{C}$ as ring R) with standard basis of simple quantities $\underline{O_H}$ by W(G).

Theorem 2.5.2. Let G be a finite abelian group. Then the S-module $W(G)$ is an S-ring over G. Moreover, $W(G)$ is the unique maximal S-ring over G for which the values of the irreducible characters of G on its standard basis are rational.

Definition 2.5.2. Let G be a finite abelian group. Any S-ring over G contained in $W(G)$ is called a *rational S-ring* over G.

Definition 2.5.3. Let $\lambda : G \times G \to \mathbb{C}^*$ satisfy

1. $\lambda(g, h) = \lambda(h, g)$,

2. $\lambda(g, h_1h_2) = \lambda(g, h_1)\lambda(g, h_2)$,

3. $\forall g \in G : \lambda(g, h) = 1 \implies h = e$.

Then $g \mapsto \lambda(g, -)$ is called a *symmetric isomorphism* of G with its character group.

Definition 2.5.4. Let $\Gamma_G(S)$ be an SRCG and λ be a symmetric isomorphism of G with its character group. Define S^+ such that $e \notin S^+$ and, for each $g \in G, g \neq e$ it holds that $g \in S^+$ if and only if $\sum_{h \in S} \lambda(g, h) = r$, where r is the largest non-principal eigenvalue of $\Gamma_G(S)$. Then $\Gamma_G(S^+)$ is called the *dual graph* to $\Gamma_G(S)$ with respect to λ.

Theorem 2.5.3. $\Gamma_G(S^+)$ is a non-trivial SRCG if and only if $\Gamma_G(S)$ is a non trivial SRCG and in this case $(r - s)(r^+ - s^+) = |G|$, where r^+, s^+ are the non-principal eigenvalues of $\Gamma_G(S^+)$.

3 Complex characters of rational S-rings over finite abelian groups

In this chapter, we will prove some properties of characters of rational S-rings over finite abelian groups, giving also some examples. The most important result is a direct calculation of a character of the set of generators of a cyclic subgroup H of G, that strictly depends on the order of H

We remind that φ is the *Euler function* and that μ is the *Möbius function:*

$$\mu(n) = \begin{cases} 1 & \text{if } n = p_1 \cdots p_i, i \text{is odd}, \\ 0 & \text{if } \exists p^k \ s.t.\ p^k \mid n, k \neq 1, p^k > 1, \\ -1 & \text{if } n = p_1 \cdots p_i, i \text{ is even}. \end{cases}$$

We remind also the *Möbius inversion formula*:

$$F(n) = \sum_{d|n} f(d) \implies f(n) = \sum_{d|n} \mu(\frac{n}{d})F(d) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \tag{3.1}$$

We continue with an alternative definition of a *character* of an abelian group G (compare with Definition 2.16).

Definition 3.0.1. Let G be an abelian group of order n. A *character* of G is an homomorphism from G into the non-zero complex numbers, viewed as a multiplicative group.

Now, if an element g of G has order n, then it is easy to prove that each character σ sends that element g to some n-th root of unity. Indeed $1 = \sigma(e) = \sigma(g^n) = (\sigma(g))^n$, where e is the neutral element of G.

We know that characters are homomorphisms. This implies that there is a binary operation $\circ$ on $\mathrm{Irr}(G)$ defined by

$$[\chi \circ \psi](g) = \chi(g) \cdot \psi(g),\ g \in G,$$

where $\cdot$ is the multiplication on complex numbers.

Theorem 3.0.1. The set $\mathrm{Irr}(G)$ together with the multiplication $\circ$ is a group, which is isomorphic to G.

In order to show some important properties of characters, we give some examples.

Example 3.0.1. Let H be the following subgroup of $\mathbb{Z}_{3^3} \oplus \mathbb{Z}_{3^3}$:

$$H = \{(a, a) : a \in \{0, 1, \dots, 26\}\},$$

and let $\psi \in \mathrm{Irr}(H)$ be the character sending all elements in the form $(3a, b)$, $a, b \in \{0, \dots, 26\}$ to 1, all elements in the form $(3a-1, b)$ to $(\sqrt{3}i - 1)/2$, and all elements in the form $(3a-2, b)$ to $-(\sqrt{3}i + 1)/2$. Then

$$\psi(\underline{H}) = 9 \cdot (1 - 1) = 0.$$

Indeed, it is easy to check that the image $\psi(H) = \{1, (\sqrt{3}i - 1)/2, -(\sqrt{3}i + 1)/2\}$, and that each element of this image has correspondence with 9 members of H.

Example 3.0.2. Let us consider now another subgroup $K \leqslant \mathbb{Z}_{3^3} \oplus \mathbb{Z}_{3^3}$ defined as:

$$\begin{aligned} K = \{&(0,0),(6,1),(12,2),(18,3),(24,4),(3,5),(9,6),(15,7),(21,8),(0,9)\\ &(6,10),(12,11),(18,12),(24,13),(3,14),(9,15),(15,16),(21,17),(0,18),\\ &(6,19),(12,20),(18,21),(24,22),(3,23),(9,24),(15,25),(21,26)\}. \end{aligned}$$

If we calculate $\psi(\underline{K})$, we get $\psi(\underline{K}) = 27 = |K|$. Indeed $\psi(K) = \{1\}$ and the only element of the image has correspondence with all elements of K.

Proposition 3.0.1. The set of simple quantities which correspond to cyclic subgroups of G forms a basis of $W(G)$ called the subgroup basis.

Proof. Let C_i be a cyclic subgroup of G of order i. Then we can write $\underline{C_i} = \sum_{k|i} \underline{O_k}$, where $\underline{O_k}$ is the simple quantity corresponding to the cyclic subgroup C_k of C_i. Then we apply the the Möbius inversion formula on that sum and we get the proof. □

Let us consider now the groups and the character ψ we already introduced in the previous example. If we define the character ρ, having the same kernel as ψ but sending all elements in the form $(3a-1, b)$ to $-(\sqrt{3}i + 1)/2$ and all elements in the form $(3a-2, b)$ to $(\sqrt{3}i - 1)/2$, we will find that $\psi(H) = \rho(H)$ and $\psi(K) = \rho(K)$. This is not a random result. Whatever we choose a character ψ, then the following sentence is true for a any cyclic subgroup $H \leqslant G$ of order $|H| = n$ and any character $\psi \in \mathrm{Irr}(H)$:

$$\exists\, m \text{ s.t. } \forall g \in H, \psi^m(g) = 1 \to m \mid n. \tag{3.2}$$

Now, if $m \mid n$ and $m \neq 1$, then the group H is transformed into a $\frac{n}{m}$ copies of the identical set A of m elements, where

$$A = \{e^{\frac{2a\pi i}{m}} : a \in \{1, \dots, m\}\}.$$

If we sum together all the elements of A we find the complex number $e^{\frac{2\pi i}{m}} \cdot (\sum_{a=0}^{m-1} e^{2\pi i \frac{a}{m}})$. Now, $(\sum_{a=0}^{m-1} e^{2\pi i \frac{a}{m}}) = \frac{(e^{2\pi i}-1)}{e^{2\pi i/m}-1} = 0$. If $m = 1$, then all the elements of H are sent to 1 and $\psi(\underline{H}) = |H| = n$. We obtain that:

$$\psi(\underline{H}) = \begin{cases} |H| & \text{if } H \subseteq \ker(\psi), \\ 0 & \text{if } H \not\subseteq \ker(\psi). \end{cases} \tag{3.3}$$

This important result is emphasized in the following proposition.

Proposition 3.0.2. Let ρ, $\sigma \in \mathrm{Irr}(G)$. Then ρ and σ are equal on $W(G)$ if and only if $\ker(\rho) = \ker(\sigma)$.

Proof. It follows from Proposition 3.0.1 that the subgroup basis is a basis for $W(G)$. This means that, if we find a property for the subgroup basis, we can extend the result to $W(G)$. It follows from equation 3.3 that that, if $\ker(\sigma) = \ker(\rho)$, then $\rho(\underline{H}) = \sigma(\underline{H})$ for each $H \leqslant G$. If $\ker(\sigma) \neq \ker(\rho)$, then there exists a $h \in G$ such that $h \in \ker(\sigma)\,, h \notin \ker(\rho)$ or $h \in \ker(\rho)\, h \notin \ker(\sigma)$. In any case, if $H = \langle h \rangle$ will be such that $\sigma(\underline{H}) \neq \rho(\underline{H})$. It will be $|H|$ for the character with h in its kernel and 0 for the other one. □

Definition 3.0.2. A subgroup $H \leqslant G$ is called a *co-cyclic subgroup* if and only if G/H is a cyclic group.

The introduction of the Definition 3.0.2 is crucial for the subsequent parts of this work. Let us consider a character ψ_H such that $H = \ker(\psi_H)$. Let $h \in H$, $g \in G$ and let $f \in G \setminus H$. Let $+$ be the binary operation of the group G. Then $\psi_H(g + h) = \psi_H(g)$, $\psi_H(f + g) = \psi_H(f) \cdot \psi_H(g)$. Let us consider the coset $g + H$. Then $\psi_H(g + H) = \psi_H(g) \cdot \psi_H(H)$. We have to prove the next proposition.

Proposition 3.0.3. There exists a bijection between the set of equivalence classes of $\mathrm{Irr}(G)$, where two characters belong to the same class if and only if they have the same kernel, and the set of co-cyclic subgroups of G.

Proof. Let H be a subgroup of G and let G/H be the quotient group according to H (we know it is a group since G is abelian). Two elements of G belong to the same coset of H if and only if their difference is a member of H.

Then we consider H as the kernel of a character ψ. Then

$$H + a = H + b \iff a - b = h \in H, \iff \psi(a) = \psi(b) \tag{3.4}$$

Therefore, we can conclude that the image of ψ is isomorphic to G/H and so G/H is cyclic since the image of ψ is cyclic. Then H is indeed a co-cyclic group. □

Definition 3.0.3. A proper subgroup $H \leq G$ is *maximal* if $H \leqslant K \leqslant G$ implies $K = H$ or $K = G$.

We give some examples to show the validity of Proposition 3.0.3.

Example 3.0.3. Let K be the following subgroup of $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^3}$:

$$\begin{aligned} K &= \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),(2,0),(2,1),(2,2),\\ &\quad (2,3),(2,4),(2,5),(2,6),(2,7),(4,0),(4,1),(4,2),(4,3),(4,4),(4,5),\\ &\quad (4,6),(4,7),(6,0),(6,1),(6,2),(6,3),(6,4),(6,5),(6,6),(6,7)\}. \end{aligned}$$

This subgroup is cocyclic on G. Indeed G/K consists of two elements, let us say a and b, such that the Cayley table is:

+	a	b
a	a	b
b	b	a

Table 1: Cayley table of G/K introduced in this Example

where $a = K$ and $b = (1,0)+K$. This group is cyclic. Now, we can also define the class of characters in $Irr(G)$ having the kernel equal to K. We have seen, through equation 3.3, what are the values of the characters applied to the whole cyclic subgroup $H \leqslant G$. We are interested to find the values of the characters applied to the set of generators of such H.

Example 3.0.4. Let us consider the cyclic group

$$F = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7)\}$$

of $G = \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^3}$. The set of its generators is $O_F = \{(0,1),(0,7),(0,3),(0,5)\}$. Then the set difference $F \setminus O_F = \{(0,0),(0,2),(0,4),(0,6)\}$, that is a maximal subgroup of F. If we keep K the cocyclic group in the previous example, then we can find that $\psi_K(O_F) = \psi_K(F) - \psi_K(F \setminus O_F) = 8 - 4 = 4$.

Definition 3.0.4. The intersection of all maximal subgroups of a group G is called the *Frattini subgroup* of G and denoted by $\Phi(G)$. If G has no maximal subgroups, then $\Phi(G) = G$ by definition.

If G is a cyclic group of order $p_1^{a_1} \dots p_s^{a_s}$ then $\Phi(G)$ has the index $p_1 \cdots p_s$.

Lemma 3.0.1. Let $\chi \in \mathrm{Irr}(G), h \in G, H = \langle h \rangle$ and $F = H \cap \ker(\chi)$. Denote by O_H the set of all generators of H. Then:

$$\chi(\underline{O_H}) = |\Phi(H)|\mu\left(\frac{|H|}{|F|}\right)\varphi\left(\frac{|F|}{|\Phi(H)|}\right).$$

In the previous example, $\Phi(H) = F, |F| = 4, |H| = 8$ and if we apply the lemma, we obtain $\psi_K(\underline{O_F}) = 4$.

4 The characters of the S-ring $W(\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n})$

In the following chapters G will stand for $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. Let us begin with some examples.

Example 4.0.1. Let us fix $p = 3$, $n = 3$. Let us examine the cyclic subgroups of G, starting from the non trivial ones with the least order. We find that they are:
$\{(9,0),(18,0),(0,0)\}$, $\{(0,9),(0,18),(0,0)\}$,
$\{(9,9),(18,18),(0,0)\}$ and $\{(9,18),(18,9),(0,0)\}$.

The total amount of generators of such sets is $2 \cdot 4 = 8$. A second family of subgroups of G is the following:
$\{(3,0),(6,0),(9,0),(12,0),(15,0),(18,0),(21,0),(24,0),(0,0)\}$
$\{(3,9),(6,18),(9,0),(12,9),(15,18),(18,0),(21,9),(24,18),(0,0)\}$
$\{(3,18),(6,9),(9,0),(12,18),(15,9),(18,0),(21,18),(24,9),(0,0)\}$.

These three subgroups contains $\{(9,0),(18,0),(0,0)\}$. The subgroups $\langle(0,3)\rangle$, $\langle(9,3)\rangle$ and $\langle(18,3)\rangle$ contain $\{(0,9),(0,18),(0,0)\}$. The subgroups $\langle(3,3)\rangle$,$\langle(21,3)\rangle$ and $\langle(3,21)\rangle$ contain $\langle(9,9)\rangle$, whistle $\langle(3,6)\rangle$, $\langle(24,3)\rangle$, $\langle(6,3)\rangle$ contain $\{(9,18), (18,9), (0,0)\}$. The last set of cyclic subgroup is built up by 36 sets. We list only three of them for lacking of space: $\langle(0,1)\rangle, \langle(9,1)\rangle, \langle(18,1)\rangle$ containing $\langle(0,3)\rangle$. Each of the 12 sets of order 9 previously found is included in three different subgroups of order 27. Now, if we represent the inclusion order of all these subgroups with an Hasse diagram, we will find that the diagram is a tree.

Proposition 4.0.1. The subgroups $\{H = \langle p^m, ap^m\rangle,\ 0 \leqslant m \leqslant n-1, 0 \leqslant a \leqslant p^{n-m}-1\} \cup \{H = \langle bp^{m+1}, p^m\rangle, 0 \leqslant m \leqslant n-1, 0 \leqslant b \leqslant p^{n-m-1}-1\} \cup \{(0,0)\}$ exhaust the set of cyclic subgroups of G. The set of cyclic subgroups is partially ordered by inclusion. The Hasse diagram of this poset is a tree, where the trivial subgroup is the root.

Proof. $\{(0,0)\}$ is a cyclic subgroup of order 1. All the cyclic subgroups of order p declared in hypotesis are of the kind:$\langle(p^{n-1}, p^{n-1}a)\rangle, 0 \leqslant a \leqslant p-1; \langle(0, p^{n-1})\rangle$. They are all distinct and the total number of the generators is: $(p-1)\cdot(p+1) = p^2-1$. The set of cyclic subgroups of order p^m is $\langle(p^{n-m}, p^{n-m}a)\rangle \cup \langle(0, p^{n-m})\rangle$. The total number of generators is $(p^2-1)\cdot p^{2(m-1)}$. Then, we sum the number of generators of $\langle(0,0)\rangle$, that is 1, with the number of generators of subgroups of order p (that number is (p^2-1)), with number of all these distinct generators of groups of order p^n: $1+(p^2-1)\sum_{i=1}^{n} p^{2(i-1)} = p^{2n} = |G|$. The lattice of subgroups of a cyclic p-group is a chain, therefore the Hasse diagram of the poset of cyclic subgroups of a p-group is a tree. □

The Hasse diagram of the poset of cyclic subgroups of $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ will be denoted denoted by Δ. Let us do some further examples of such Δ.

Example 4.0.2. Let $p=2$ and $n=3$. Then we get the following Hasse diagram:

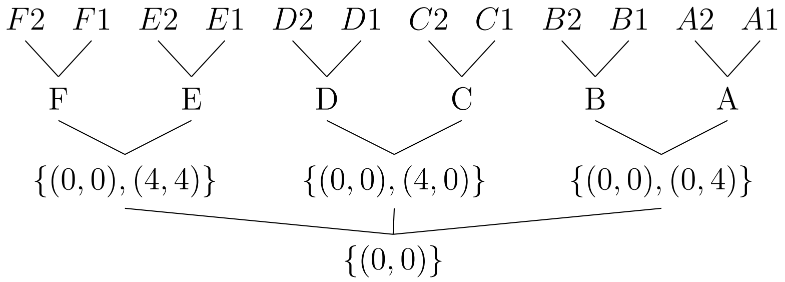


Figure 7: Hasse Diagram of the poset of the cyclic subgroups of $\mathbb{Z}_8 \oplus \mathbb{Z}_8$

Where:
$A=\{(0,0),(0,2),(0,4),(0,6)\}$,
$B=\{(0,0),(4,2),(0,4),(4,6)\}$,
$C=\{(0,0),(2,0),(4,0),(6,0)\}$,$D=\{(0,0),(2,4),(4,0),(6,4)\}$,
$E=\{(0,0),(2,2),(4,4),(6,6)\}$,$F=\{(0,0),(6,2),(4,4),(2,6)\}$,
$A1=\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7)\}$,
$A2=\{(0,0),(4,1),(0,2),(4,3),(0,4),(4,5),(0,6),(4,7)\}$,
$B1=\{(0,0),(2,1),(4,2),(6,3),(0,4),(2,5),(4,6),(6,7)\}$,
$B2=\{(0,0),(6,1),(4,2),(2,3),(0,4),(6,5),(4,6),(2,7)\}$,
$C1=\{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0),(7,0)\}$,
$C2=\{(0,0),(1,4),(2,0),(3,4),(4,0),(5,4),(6,0),(7,4)\}$,
$D1=\{(0,0),(1,2),(2,4),(3,6),(4,0),(5,2),(6,4),(7,6)\}$,
$D2=\{(0,0),(1,6),(2,4),(3,2),(4,0),(5,6),(6,4),(7,2)\}$,
$E1=\{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7)\}$,
$E2=\{(0,0),(1,5),(2,2),(3,7),(4,4),(5,1),(6,6),(7,3)\}$,
$F1=\{(0,0),(3,1),(6,2),(1,3),(4,4),(7,5),(2,6),(5,7)\}$,
$F2=\{(0,0),(3,5),(6,2),(1,7),(4,4),(7,1),(2,6),(5,3)\}$.

Let us now find the cocyclic subgroups of G. The trivial cocyclic subgroup is $\{G\}$.

Example 4.0.3. To have a clear idea, let us do the calculation of the cocyclic subgroups of $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^3}$. They shall be collected in the following Hasse diagram (the ordering now is according to $\supseteq$):

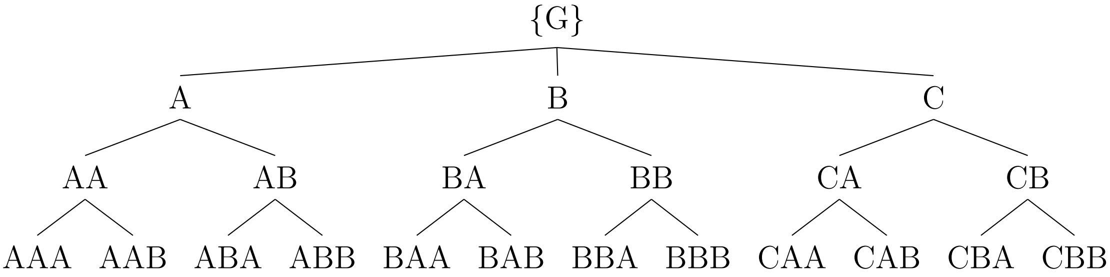


Figure 8: Poset of cocyclic groups on $\mathbb{Z}_8 \oplus \mathbb{Z}_8$

Where:
$A = \{(a, b) : a \text{ even}\}$
$B = \{(a, b) : (a + b) \text{ even}\}$
$C = \{(a, b) : b \text{ even}\}$
$AA = \{(0, 0), (0, 1) \dots (0, 7), (4, 0), (4, 1) \dots (4, 7)\}$
$AB = \{(0, 0), (0, 2), (0, 4), (0, 6), (2, 1), (2, 3), (2, 5), (2, 7), (4, 0), (4, 2), (4, 4), (4, 6), (6, 1), (6, 3), (6, 5), (6, 7)\}$
$BA = \{(0, 0), (0, 4), (1, 1), (1, 5), (2, 2), (2, 6), (3, 3), (3, 7), (4, 0), (4, 4), (5, 1), (5, 5), (6, 2), (6, 6), (7, 3), (7, 7)\}$
$BB = \{(0, 0), (0, 4), (1, 3), (1, 7), (2, 2), (2, 6), (3, 1), (3, 5), (4, 0), (4, 4), (5, 3), (5, 7), (6, 2), (6, 6), (7, 1), (7, 5)\}$
$CA = \{(0, 0), (0, 4), (1, 0), (1, 4), (2, 0), (2, 4), (3, 0), (3, 4), (4, 0), (4, 4), (5, 0), (5, 4), (6, 0), (6, 4), (7, 0), (7, 4)\}$
$CB = \{(0, 0), (0, 4), (1, 2), (1, 6), (2, 0), (2, 4), (3, 2), (3, 6), (4, 0), (4, 4), (5, 2), (5, 6), (6, 0), (6, 4), (7, 2), (7, 6)\}$
Then $AAA, ..., CBB$ are both cocyclic and cyclic groups, and:
$AAA = \{(0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (0, 5), (0, 6), (0, 7)\}$
$AAB = \{(0, 0), (4, 1), (0, 2), (4, 3), (0, 4), (4, 5), (0, 6), (4, 7)\}$
$ABA = \{(0, 0), (2, 1), (4, 2), (6, 3), (0, 4), (2, 5), (4, 6), (6, 7)\}$
$ABB = \{(0, 0), (6, 1), (4, 2), (2, 3), (0, 4), (6, 5), (4, 6), (2, 7)\}$
$BAA = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7)\}$
$BAB = \{(0, 0), (1, 5), (2, 2), (3, 7), (4, 4), (5, 1), (6, 6), (7, 3)\}$

$BBA = \{(0,0),(1,3),(2,6),(3,1),(4,4),(5,7),(6,2),(7,5)\}$
$BBB = \{(0,0),(1,7),(2,6),(3,5),(4,4),(5,3),(6,2),(7,1)\}$
$CAA = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0),(7,0)\}$
$CAB = \{(0,0),(1,4),(2,0),(3,4),(4,0),(5,4),(6,0),(7,4)\}$
$CBA = \{(0,0),(1,2),(2,4),(3,6),(4,0),(5,2),(6,4),(7,6)\}$
$CBB = \{(0,0),(1,6),(2,4),(3,2),(4,0),(5,6),(6,4),(7,2)\}$

Let us compute now, for example, G/AA. It is made of four elements: $AA, (1,0)+AA, (2,0)+AA, (3,0)+AA$ and it is obviously cyclic. If we compute now, for example, G/BB, we obtain that it is also made of four elements: $BB, (0,1)+BB, (0,2)+BB, (0,3)+BB$. Generally talking, the following inferences are true:

$$\begin{aligned} K = \langle (b\cdot p, 1), (p^m, 0)\rangle,\ 1 \leqslant m \leqslant n,\ 0 \leqslant b \leqslant p^{m-1}-1 \implies \\ G/K = \{K, (1,0)+K, ..., (p^m-1, 0)+K\} \\ G/K \cong \mathbb{Z}_{p^m} \end{aligned}$$

$$\begin{aligned} K = \langle (1, a), (0, p^m)\rangle,\ 1 \leqslant m \leqslant n,\ 0 \leqslant a \leqslant p^m-1 \implies \\ G/K = \{K, (0,1)+K, ..., (0, p^m-1)+K\} \\ G/K \cong \mathbb{Z}_{p^m} \end{aligned} \tag{4.1}$$

Proposition 4.0.2. The subgroups $\{K = \langle (b\cdot p, 1), (p^m, 0)\rangle,\ 1 \leqslant m \leqslant n,\ 0 \leqslant b \leqslant p^{m-1}-1\} \cup \{K = \langle (1,a), (0,p^m)\rangle,\ 1 \leqslant m \leqslant n,\ 0 \leqslant a \leqslant p^m-1\} \cup \{G\}$ exhaust the set of cocyclic subgroups of G.

Proof. G is a trivial cocyclic group. Excluding this case, the element $(p,0)$ should stay or should not stay in the cocyclic group. If it does not, then their elements will be generated by $(1,a),(0,c)$: we can properly say that $a \leq p^{m-1}$ and $c = p^m$. If $(p,0)$ stays in the cocyclic group, then it cannot stay with $(0,p)$ otherwise the cocyclic group will be isomorphic to $\mathbb{Z}_{p^{n-1}} \oplus \mathbb{Z}_{p^{n-1}}$ and the quotient group will not be cyclic (contradiction). Then the cocyclic group will be generated by $(p\cdot b, 0)$ and by $(p^m, 0)$. □

Proposition 4.0.3. Let H be a cocyclic subgroup of $G = \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ isomorphic to $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^m}$. Define $H^{\Delta} = \{p^m h \mid h \in H\}$. Then the mapping $H \to H^{\Delta}$ is a bijection between the set of cocyclic groups of G and the set of cyclic subgroups of G. Moreover, $H_1 \subseteq H_2 \iff H_1^{\Delta} \supseteq H_2^{\Delta}$. The set of cocyclic subgroups is partially ordered by inclusion. The Hasse diagram of this poset is a tree, where G is the root.

Proof. If we have $H = \langle (1,a), (0, p^{n-m})\rangle$, then the operation $p^m \cdot H = \langle (p^m, ap^m)\rangle = K$ has an inverse: $K^{\nabla} = H$. If we have $H = \langle (b\cdot p, 1), (p^{n-m}, 0)\rangle$, then the operation

$p^m \cdot H = \langle(b \cdot p^{m+1}, p^m\rangle$ has an inverse $K^{\triangledown} = H$. $K_1 = \{\langle(1, a_1), (0, p^{m_1})\rangle \supseteq K_2 = \{\langle(1, a_2), (0, p^{m_2})\rangle\} \iff a_1 \equiv a_2\ (\mathrm{mod}\ (p^{m_1}) \wedge m_1 \leqslant m_2 \iff K_1^{\Delta} \subseteq K_2^{\Delta}$. This implies that also the Hasse diagram of cocyclic groups is a tree. □

We will denote the Hasse diagram of the poset of cocyclic subgroups of $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ by ∇. The operation bringing a cocyclic group H into a cyclic group will be denoted H^{Δ}, its inverse will be denoted $H^{\triangledown}$.

Let us consider again the tree of cyclic subgroups of $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^3}$. We will denote as "sons of X" the elements Y of Δ such that X is a maximal subgroup in Y. In a similar way, we can define "sons of X the Y elements of ∇ such that Y is a maximal subgroup for X. Inductively, we can define *j-descendants* of X by letting $Des_1(X) = Sons(X)$ and $Des_{j+1}(X) = Sons(Des_j(X))$ if $j \geqslant 1$.

We can build up the "tree of the sons" of the tree of cyclic subgroups in $\mathbb{Z}_8 \oplus \mathbb{Z}_8$:

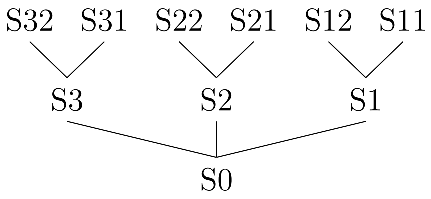


Figure 9: "Tree of sons" - Δ^1 on $\mathbb{Z}_8 \oplus \mathbb{Z}_8$

Where:
$S0 = \{\langle(4,0)\rangle \wedge \langle(4,4)\rangle \wedge \langle(0,4)\rangle\}$
$S1 = \{\langle(0,2)\rangle \wedge \langle(4,2)\rangle\}$
$S2 = \{\langle(2,2)\rangle \wedge \langle(6,2)\rangle\}$
$S3 = \{\langle(2,0)\rangle \wedge \langle(2,4)\rangle\}$
$S11 = \{\langle(0,1)\rangle \wedge \langle(4,1)\rangle\}$
$S12 = \{\langle(2,1)\rangle \wedge \langle(6,1)\rangle\}$
$S21 = \{\langle(1,1)\rangle \wedge \langle(5,1)\rangle\}$
$S22 = \{\langle(3,1)\rangle \wedge \langle(7,1)\rangle\}$
$S31 = \{\langle(1,0)\rangle \wedge \langle(1,4)\rangle\}$
$S32 = \{\langle(1,2)\rangle \wedge \langle(1,6)\rangle\}$
We have also a "tree of grand sons":

We denote the poset of j-descendants by Δ^j. To be clear: we have plotted Δ^1 and Δ^2 of $\mathbb{Z}_8 \oplus \mathbb{Z}_8$ in sequence. Moreover, we define Δ_i, Δ_i^j, ∇_i, ∇_i^j as those subsets of

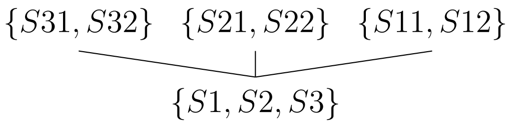


Figure 10: ”Tree of grandsons” - Δ^2 on $\mathbb{Z}_8 \oplus \mathbb{Z}_8$

their trees, such that their elements have length $l \leqslant i$. If $S \subseteq \Delta_i^j$ then $[S]$ will denote the simple quantity of its generators. The notation $\chi_H[S]$ will mean the value of the character χ_H with kernel H on $[S]$.

Lemma 4.0.1. Let $F \in \Delta$ and $H \in \nabla$. Then $F \subseteq H \iff l(F) - l(F \cap H^\Delta) \leqslant n - l(H^\Delta)$.

Proof. Let $F \subseteq H$. If $l(H) = l + m$, then $l(H^\Delta) = l - m$. Then our goal is to prove that $l(F) - l(F \cap H^\Delta) \leqslant m$. $H^\Delta = p^m \cdot H \supseteq p^m F$, but also $F \supseteq p^m F$, then $F \cap H^\Delta \supseteq p^m F$. F is cyclic and $[F : p^m F] \leqslant p^m$. But $[F : p^m F] = \frac{|F|}{|p^m F|} \rightarrow \frac{|F|}{|F \cap H^\Delta|} \leqslant p^m$. Then $p^{l(F) - l(F \cap H^\Delta)} \leqslant p^m \rightarrow l(F) - l(F \cap H^\Delta) \leqslant m$ as desired.

Let $l(F) - l(F \cap H^\Delta) \leqslant m$. If $l(F) \leqslant m$, then $F \subseteq H$. If $l(F) \leqslant m$, we know that F is cyclic and so the inequality $[F : F \cap H^\Delta] \leqslant p^m$ implies $F \cap H^\Delta \supseteq p^m F$. If $H = \langle (1,0), (0, p^{n-m}) \rangle$, then $H^\Delta = \langle (p^m, 0) \rangle$. Let $f = (f_1, f_2)$ be a generator of F. Now $p^m F \subseteq H^\Delta$ implies that $f_2 = 0 \mod (p^{n-m})$. Therefore $f = (f_1, f_2' p^{n-m}) \in \langle (1,0), (0, p^{n-m}) = H$ □

Remark 4.0.1. The following conditions are equivalent:

(a): $l(F) - l(F \cap H^\Delta) = n - l(H^\Delta) + 1$

(b): $Father(F) \subseteq H \wedge F \nsubseteq H$.

Indeed, if (a) does hold, then $F \nsubseteq H$ by Lemma 4.0.1 and $F \cap H^\Delta \supseteq Father(F) \cap H^\Delta$ implies $l(F \cap H^\Delta) \geqslant l(Father(F) \cap H^\Delta)$. Moreover, the intersection between two cyclic subgroups is the common ancestor, in the tree Δ. If this result is properly F, then $l(F) - l(F) = 0$ in contradiction with the hypothesis. Then (a) is the same as:
$l(Father(F)) - l(H^\Delta \cap Father(F)) = n - l(H^\Delta) \implies (b)$.

Conversely, if (b) does hold, then we can apply Lemma 4.0.1 and we obtain the proof.

The following corollary is crucial, since it gives the possibility to calculate irreducible characters in an easy way.

Corollary 4.0.1. Let $F \in \Delta$ and $H \in \nabla$. Then:

$$\chi_H[F] = \begin{cases} \frac{|F|(p-1)}{p} & \text{if } F \subseteq H, \\ \\ -\frac{|F|}{p} & \text{if } l(F) - l(F \cap H^{\Delta}) = n - l(H^{\Delta}) + 1, \\ \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We use the results of equation (3.3) and use the fact that $O_F = \{F\} \backslash \{Father(F)\}$. Then $\chi_H(\underline{O_F}) = \chi_H(\underline{F}) - \chi_H(\underline{Father(F)})$.
In the first case, $\chi_H(\underline{F}) = |F|$, $\chi_H(\underline{Father(F)}) = \frac{|F|}{p}$, and the case is proved. In the second case, $\chi_H(\underline{F}) = 0$, $\chi_H(\underline{Father(F)}) = \frac{|F|}{p}$, and also this case is proved. In the third case, $\chi_H(\underline{F}) = 0$, $\chi_H(\underline{Father(F)}) = 0$ and also this case is proved. □

Proposition 4.0.4. Let $X, Y \subseteq \Delta_i^j$, such that $(X \cup Y) \cap \Delta_0^j = \emptyset$ and for each l, $1 \leq l \leq i$, either $X \cap (\Delta_l^j \setminus \Delta_{l-1}^j) = \emptyset$ or $Y \setminus (\Delta_l^j \setminus \Delta_{l-1}^j) = \emptyset$. Then for each $H_1, H_2 \in \nabla_{n-j} \setminus \nabla_{n-j-1}$ it holds that

$$|(\chi_{H_1}[X] - \chi_{H_1}[Y]) - (\chi_{H_2}[X] - \chi_{H_2}[Y])| \leq (2p^i - 1)p^{2j}.$$

Proof. We claim that $-p^{2j+1} \leq \chi_H[X \cap \Delta_1^j \setminus \Delta_0^j] \leq (p-1)p^{2j}$ and $-(p^m - p^{m-1})p^{2j} \leq \chi_H[X \cap \Delta_m^j \setminus \Delta_{m-1}^j] \leq (p^m - p^{m-1})p^{2j}), 2 \leq m \leq i$.

Case $m = 1$: For $i = 1$, if there is a node N of $\Delta_1 \setminus \Delta_0$ s.t. $N = (H^{\Delta} \cap X)$ for all the nodes $X = Des_j(N)$, then this is the scenario we can have the maximum χ_H and the minimum χ_H. The minimum χ_H is if we pick all the largest block set X such that$X \cap H^{\Delta} = \{(0,0)\}$. The cardinality of the largest block set is pp^j. Indeed there are $p+1$ nodes $\in \Delta_1^j \setminus \Delta_0^j$, but one of them is out (let us call it P) of this calculation since it is the only one such that $Des_j(P) \cap H^{\Delta} \neq \{(0,0)\}$. Therefore, we can conclude that: $\chi_H(X) \geq pp^j(-1/p)p^{(j+1)} = -p^{(2j+1)}$, $X \in \Delta_1^j \setminus \Delta_0^j$. Instead, the maximum χ_H is reached if we pick all and only the $p^{(j+1)}$ nodes $N \in Des_j(P)$. In that case, $\chi_H(N) = p^{2j} \cdot (p-1)$. So $\chi_H(N) \leq p^{2j} \times (p-1)$. This part is represented in the following tree, where the $\oslash$ stands for the only element in $\Delta_1 \setminus \Delta_0$ ancestor of H^{Δ}, the $\bullet$ stands for the nodes in $\Delta_1^j \setminus \Delta_0^j$ having a $H^{\Delta} \cap X \neq \{(0,0)\}$, the stars are the nodes having $H^{\Delta} \cap X = \{(0,0)\}$ (This is only a scheme):

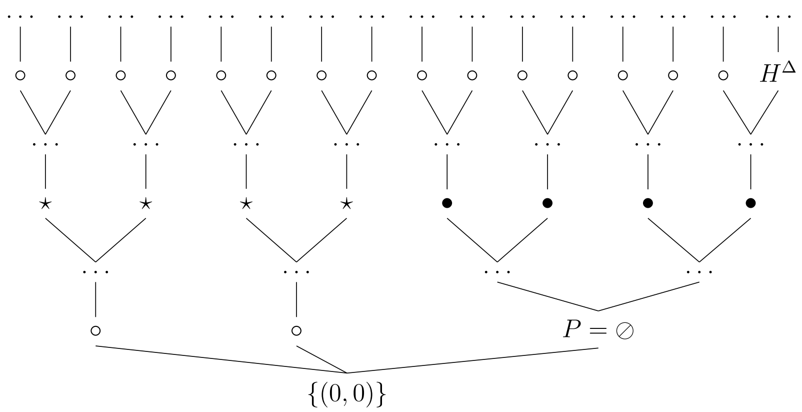


Figure 11: Proof of Proposition 4.0.4

Case $m > 1$: The scenario is: $X \subseteq H$ (this occurring for all the nodes descending from only one fixed P, $X \in Des_j(P)$, $P \in \Delta_m \setminus \Delta_{m-1}$)
or $l(X) - l(H^{\Delta} \cap X) = n - l(H) + 1$ that means: $l(X \subseteq H^{\Delta}) = m - 1$ (this occurring for X descending from the $p - 1$ nodes N s.t. $Father(N) = Father(P) \wedge N \neq P$)
or: $\chi_H(X) = 0$ (all the remaining nodes in $\Delta^j_m \setminus \Delta^j_{m-1}$). The lower bound is when we collect into a set S all the $p^j(p-1) \times p^j$ having negative χ_H, plus maybe some nodes with $\chi_H = 0$. Then: $\chi_H[S] = -(p-1) \cdot p^j \cdot p^{(m+j)}/p = -(p-1) \cdot p^{(m-1)} \cdot p^{2j}$. The upper bound is when we collect into a set S the p^j nodes having positive character, plus maybe some nodes having $\chi_H = 0$. Then: $\chi_H[S] = p^j(p-1)p^{(j+m)}/p$ and this is the upper bound. Summarizing the inequalities we claimed and proved valid, we obtain: $-p^{1+2j} \leqslant \chi_H[X] - \chi_H[Y] \leqslant (p^i - 1) \cdot p^{2j}$ if $Y \cap (\Delta^j_1 \setminus \Delta^j_0) = \emptyset$ and $-p^{1+2j} \leqslant \chi_H[X] - \chi_H[Y] \leqslant (p^i - 1) \cdot p^{2j+i}$ if $(X \cap \Delta^j_1 \setminus \Delta^j_0) = \emptyset$. Writing these inequalities for H_1 and H_2 we proved this proposition. □

5 Homogeneous strongly regular graphs over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$

We define what is an homogeneous subset of Δ. According to this property, it is possible to classify all the Strong Regular Cayley Graphs over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$.

Definition 5.0.1. Let $(a_1, \dots, a_i)$ be an integer vector, $0 \leq a_1 \leq p+1, 0 \leq a_2, \dots, a_i \leq p-1$. We say that $S \subseteq \Delta_i^j$ is $(a_1, \dots, a_i)$-*homogeneous* if $\Delta_0^j \not\subseteq S$ and for each $H \in \Delta_{i-1}^j$ it holds that:

$$|Sons(H) \cap S| = \begin{cases} a_{l(H)+1} + 1 & \text{if } H \in S, \\ a_{l(H)+1} & \text{if } H \notin S. \end{cases}$$

A less general definition of homogeneity is found, if j is set equal to 0. Let us now illustrate an example of homogeneous graph. The bullet means: "the node belongs to S" and the circle means "the node does not belong to S".

Example 5.0.1. This is a $(2, 1, 0)$-homogeneous S $(p = 3, n = 3 + j)$. It is a general case since this tree could be Δ or Δ^j.

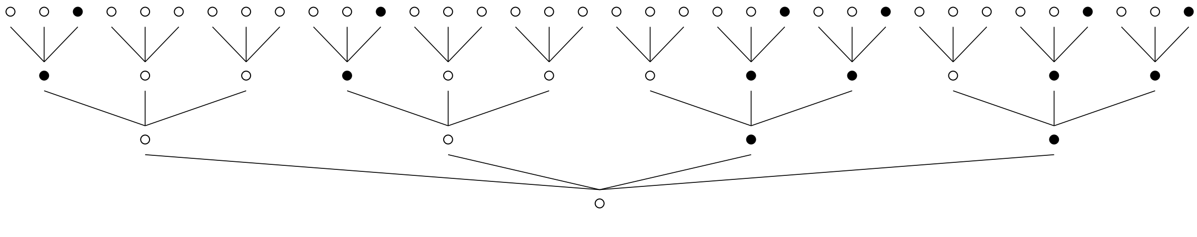


Figure 12: A $(2, 1, 0)$-homogeneous S $(p = 3, n = 3 + j)$

Another important definition is the latin square type strongly regular graph.

Definition 5.0.2. A (ν, k, λ, μ)-SRG is said to be *latin square type* if $\exists q, m$ such that: $\nu = m^2$, $k = q(m-1)$, $\lambda = m - 2 + (q-1)(q-2)$, $\mu = q(q-1)$. It is instead said to be *negative latin square type* if $\nu = m^2$, $k = q(m+1)$, $\lambda = -m - 2 + (q+1)(q+2)$, $\mu = q(q+1)$

Example 5.0.2. $2K_2$ is of latin square type with $m = 2$, $q = 1$, C_4 is latin square type with $m = 2$, $q = 2$.

Example 5.0.3. A negative latin square type is the complement of the Clebsch graph, with parameters $m = 4$ and $q = 2$. That is, the unique $(16, 10, 6, 6)$-SRG.

Let us only list some theorems, useful to prove an important property of any not trivial Strongly Regular Cayley Graph.

Theorem 5.0.1. *Let G an abelian group of order ν and S be a subset of G with $e \notin S$ and $S^{-1} = S$. Then $\Gamma_G(S)$ is an (ν, k, λ, μ)-SRCG over G if and only if for any irreducible character χ of G,*

$$\chi(\underline{S}) = \begin{cases} k & \text{if}\, \chi \,\text{principal on}\, G, \\ (\lambda - \mu \pm \sqrt{\delta})/2 & \text{if}\, \chi \,\text{NOT principal on}\, G. \end{cases}$$

where $\chi(\underline{S}) = \sum_{g \in S} \chi(g)$, $\delta = (\lambda - \mu)^2 + 4(k - \mu)$. These values are equal to the Strongly Regular Cayley Graph's eigenvalues k, r, s correspondingly.

Proof. It is a consequence of Corollary 2.1.1 and Lemma 2.5.1. □

Proposition 5.0.1. *Let Γ be a strongly regular graph. If one of its eigenvalues is 0 or -1, then Γ is a trivial strongly regular graph.*

Proposition 5.0.2. *An SRCG over G defined by a block set $S \subseteq \Delta$ is trivial. (i.e. it is a union of complete graphs or a complementer of such graph).*

Proof. Let $H \in \nabla \setminus \nabla_{n-1}$. Corollary 4.0.1 and $H = H^{\Delta}$ imply that, if a block set is $B = \Delta_1 \setminus \Delta_0$ then $\chi_H[B] = \frac{p-1}{p} \cdot p - \frac{p^2}{p} = -1$. If instead B is a block set in any $\Delta_i \setminus \Delta_{i-1}\, i \neq 1$, then

$$\chi_H(B) = n \cdot \left(p^{i-1} \frac{p-1}{p} - (p-1)p^{j-1}\frac{1}{p} \right) = n \cdot 0 = 0,$$

where n is the number of blocks in B. The proposition is then a consequence of Proposition 5.0.1 □

Example 5.0.4. Let us pick $\{(2, 2), (6, 6), (6, 2), (6, 6)(4, 2), (4, 6), (0, 2), (0, 6)\}$ from $\mathbb{Z}_8 \oplus \mathbb{Z}_8$. This is a trivial graph.

Proposition 5.0.3. *If $S \subseteq \Delta$ is not a block set, then there exists m, $1 \leqslant m \leqslant n$, and H_1, $H_2 \in \nabla \setminus \nabla_{n-1}$ such that $\chi_{H_1}[S] - \chi_{H_2}[S] = p^m$.*

Proof. Let m be the maximal number for which, if $B \subseteq \Delta$ is any block in $\Delta_m \setminus \Delta_{m-1}$ such that $B \cap S \neq \emptyset \wedge B \setminus S \neq \emptyset$. Let $F_1 \in B \cap S$ and let $F_2 \in B \setminus S$. Then set $H_1^{\Delta} \in Des_{n-m}(F_1)$ and $H_2^{\Delta} \in Des_{n-m}(F_2)$. Then $\chi_{H_1}[S \cap \Delta_m \setminus \Delta_{m-1}] - \chi_{H_2}[S \cap \Delta_m \setminus \Delta_{m-1}] = p^m$. If we pick the level $\Delta_j \setminus \Delta_{j-1}\; j \leq m-1$, the elements X of S laying there, which are not ancestors of H_1, H_2, have $\chi_{H_1}[X] = \chi_{H_2}[X] = 0$, whistle the only element P ancestor of H_1,H_2 is such that $\chi_{H_1}[P] = \chi_{H_2}[P] = |P|\frac{p-1}{p}$ and anyway we obtain: $\chi_{H_2}[S \setminus (\Delta_m \setminus \Delta_{m-1})] - \chi_{H_2}[S \setminus (\Delta_m \setminus \Delta_{m-1})] = 0$. Then $\chi_{H_1}[S] - \chi_{H_2}[S] = p^m$ □

This last result is crucial to prove the following proposition:

Proposition 5.0.4. If $\Gamma_G(S)$ is a non trivial Strong Regular Cayley Graph with non principal eigenvalues r and s, then $r - s = p^n$. Moreover, $\Gamma_G(S)$ is latin square or negative latin square type, respectively.

Proof. We recall the result of Lemma 2.1.1:

$$(\nu - k - 1)\mu = k(k - 1 - \lambda).$$

As a consequence of Proposition 5.0.3, we have that $r - s = p^m$, with $0 \leq m \leq n$ and by Theorem 2.5.3, remembering that $|G| = p^{2n}$ we can conclude that $r - s = p^n$.

Then, by Theorem 5.0.1, we have that: $\lambda - \mu = r + s$ and $k - \mu = -rs$. Then we obtain that:

$$(\nu - k - 1)(k + rs) = k(-1 - rs - (r + s)) \rightarrow$$

$$k^2 - k(\nu + (r + s)) - rs(\nu - 1) = 0 \rightarrow$$

$$(k - r)(k - s) = \mu\nu = \nu(k + rs)$$

$$(k - s - p^n)(k - s) = p^{2n}(k + s(p^n + s)).$$

Then:

$$k^2 - (p^{2n} + p^n + 2s)k + s(s + p^n)(1 - p^{2n}) = 0.$$

This yields to:

$$k = \frac{p^{2n} + p^n + 2s \pm (p^{2n} + p^n(1 + 2s))}{2}.$$

Let us examine now the two solutions $k(s, p^n)$. We have $k = k' = s - sp^n$. With this value, $\mu = s - sp^n + s(s + p^n) = s + s^2 = s(1 + s)\, \lambda = s^2 + 3s + p^n$. If we put $q = -s$ and $m = p^n$ we prove that such graph is latin square type. Then we have $k = k'' = s + sp^n + p^n + p^{2n}$. With this value, $\mu = s + sp^n + p^n + p^{2n} + s(p^n + s) = (p^n + s)(1 + p^n + s)$. If $q = p^n + s$, then $\lambda = q(q + 1) + 2s + p^n = q(q + 1) + 2q - p^n = q^2 + 3q - m$ with $m = p^n$, and that is a negative latin square type. □

Let S be now $(a_1 \dots a_k) - \textit{homogeneous}$. Fix $F \in \Delta_k^j$, $F \notin S$. If $l(F) = 0$, then $|Des_1(F) \cap S| = a_1$. Let us calculate $|Des_j(F) \cap S|$. We claim that $|Des_j(F) \cap S| = A_{0,j} = a_1 + \sum_{i=2}^{j} a_i(p^{i-1} + p^{i-2})$. The proof is by induction. For $i = 2$, it is evident:a_1 nodes belonging to S will generate $(a_2 + 1)a1$ nodes still belonging to S and $(p + 1 - a_1)$ nodes will generate $(p + 1 - a_1)a_2$ nodes still belonging to S. Then $|Des_2(F) \cap S| = (a_2a_1 + a_1 + (p + 1)a_2 - a_1a_2) = a_1 + (p + 1)a_2$. Let this claim be valid until $j - 1$. Then $|Des_j(F) \cap S| = |Des_{j-1}(F) \cap S|(a_j + 1) + (p^{j-2}(p + 1) - |Des_{j-1}(F) \cap S|)a_j = |Des_{j-1}(F) \cap S| + p^{j-2}(p + 1)a_j = a_1 + \sum_{i=2}^{j-1} a_i(p^{i-1} + p^{i-2}) + (p^{j-2} + p^{j-1})a_j \rightarrow$ *proof*. Similarly, it can be proved that, if $l(F) \neq 0$, then $|Des_{m-l(F)}(F) \cap S| =$

$A_{l(F),m} = \sum_{i=l(F)+1}^{m} a_i p^{i-l(F)-1}$. So, we set:$A0, m = a_1 + \sum_{i=2}^{m} a_i(p^{i-1} + p^{i-2})$, $A_{l,m} = \sum_{i=l+1}^{m} a_i p^{i-l-1}$ and$A_{m,m} = 0$. We underline that these numbers depend only on $l(F)$. If $F \in \Delta_k^j$, then $|Des_{m-l(F)} F \cap S| = A_{l(F),m} + 1$. We can conclude that $|Des_{m-l(F)} F \cap S| = A_{l(F),m} + \delta_S(F)$ where $\delta_S(F) = 1$ if $F \in S$ and it is 0 otherwise. Formalize these results with the following:

Definition 5.0.3. Let S be a $(a_1, \dots, a_n)-$homogeneous set. Then we define the following functions of the vector $\underline{a} = (a_1, \dots a_n)$:

$$A_{0,m} = a_1 + \sum_{i=1}^{m} a_i(p^{i-1} + p^{i-2})$$

and:

$$A_{l,m} = \sum_{i=l+1}^{m} a_i p^{i-l-1}$$

It turn to be:

$$|Des_{m-l(F)} \cap S| = A_{l(F),m} + \delta_S(F)$$

where $\delta_S(F) = 1 if F \in S, 0\, otherwise$

Lemma 5.0.1. Let S be an $(a_1 \dots a_n)-$homogeneous set. Let $H \in \nabla_t \setminus \nabla_t - 1, 0 \leq t \leq n$. Then the following equation holds:

$$\begin{gathered}\chi_H[S] = \sum_{i=1}^{n-t} A_{0,i}(p^i - p^{i-1}) - A_{0,n-t+1}p^{n-t} \\ + \sum_{i=1}^{t-1}(A_{i,n-t+i} - A_{i,n-t+i+1})p^{n-t+i} + (A_{t,n} + \delta_S(H^\Delta))p^n\end{gathered} \tag{5.1}$$

Proof. The first element on the right side of this equation is $\chi_H[S \cap \Delta_{n-t}]$. We know that all the elements $F \in S$ having length less or equal to $n-t$ are such that $\chi_H[F] > 0$. Let us analyse the level $\Delta_{n-t+1} \setminus \Delta_{n-t}$: at this level, there will be elements giving a positive or negative contribute (not null, since their parents give a positive contribute). Let us say that there exists a number x, such that $\chi_H[S \cap (\Delta_{n-t+1} \setminus \Delta_{n-t})] = x \cdot (p^{n-t+1} - p^{n-t}) + (A_{0,n-t+1} - x) \cdot (-p^{n-t})$. The number x represents the cardinality of the subset of the largest $X_0 \subseteq \Delta_{n-t+1} \setminus \Delta_{n-t}$ such that $\chi_H[X_0] > 0$. Let us call X_0 the set collecting all these x elements. Let us claim that exists F_1 s.t. $X_0 = Des_{n-t}(F_1) \cap S$, where F_1 is a certain element belonging to $\Delta_1 \setminus \Delta_0$. This claim is proved, since F_1 is the ancestor of H^Δ. Then: $x = |Des_{n-t}(F_1) \cap S| = A_{1,n-t+1} + \delta_S(F_1)$. Let us now analyse the subset $\Delta_{n-t+2} \setminus \Delta_{n-t+1}$. Here, we have a set X_1 such that $\chi_H[X_1] > 0$. Then we can write, as we did for X_0, tat $X_1 = Des_{n-t}(F_2) \cap S$, where F_2 is some element $F_2 \in \Delta_2 \setminus \Delta_1$, such that $F_2 \in Sons(F_1)$, F_2 ancestor of H^Δ, and a set $Y_0 = \bigcup_{F \in X_0} Sons(F) \setminus X_1$. Then $\chi_H[Y_0] <$

0. Then $|X_1| = A_{2,n-t+2}+\delta_S(F_2)$, $|Y_0| = -(A_{2,n-t+2}+\delta_S(F_2)-A_{1,n-t+1}-\delta_S(F_1))$. Then $\chi_H[S \cap (\Delta_{n-t+2} \setminus \Delta_{n-t+1})] = (A_{2,n-t+2}+\delta_S(F_2))p^{n-t+2} - p^{n-t+1}(A_{1,n-t+1}+\delta_S(F_1))$. At each level $\Delta_{n-t+i} \setminus \Delta_{n-t+i-1}$ we have a subset of that level $X = Des_{n-t}(F_i) \cap S$ where $F_i \in \Delta_i \setminus \Delta_{i-1}$ and F_i ancestor of H^Delta, such that $\chi_H[X] > 0$ and also a subset $Y = Des_{n-t}(F_{i-1}) \cap S \setminus X$, with $F_i \in Sons(F_{i-1})$, such that $\chi_H[Y] < 0$. Summing up $\chi_H[S \cap \Delta_{n-t}] + \sum_{i=1}^{t} \chi_H[S \cap (\Delta_{n-t+i} \setminus \Delta_{n-t+i-1}]$ we prove the lemma. □

Proposition 5.0.5. Let S be an $(a_1 \dots a_n)-$homogeneous set. Then for all t, $1 \leq t \leq n$

1. $|\chi_H[S] s.t. l(H) = t| \leqslant 2$

2. $\chi_{H_1}[S] \equiv \chi_{H_2}[S](mod p^n) \forall H_1, H_2 \in \nabla_t \setminus \nabla_{t-1}$

3. if $(a_1 \dots a_t) \neq (0 \dots 0) \wedge (a_1 \dots a_t) \neq (p+1, p-1 \dots p-1)$ then $\exists X, Y \in \nabla_t \setminus \nabla_{t-1} such\, that\, \chi_X[S] - \chi_Y[S] = p^n$

4. if $(a_1 \dots a_t) = (0 \dots 0) \vee (a_1 \dots a_t) = (p+1, p-1 \dots p-1)$ then $\forall X, Y \in \nabla_t \setminus \nabla_{t-1}$ it holds that $\chi_X[S] = \chi_Y[S]$

Proof.

1. According to the equation 5.1, there are only two possibilities for the value $\chi_H[S]$, depending on the fact if H^Δ does or does not belong to S.

2. We can observe that we can write the equation 5.1 as the sum of two parts: $\chi_H[S] = L + p^n \cdot \delta_S[H^\Delta)$. Then $\chi_{H_2}[S] - \chi_{H_1}[S] = L - L + (\delta_S(H_2) - \delta_S(H_1)) \cdot p^n = \delta_S(H_2) - \delta_S(H_1)) \cdot p^n$

3. In that case, there exists a block $B \subsetneq (\nabla_t \setminus \nabla_{t-1})$such that $B^\Delta \cap S \neq \emptyset$,$B^\Delta \setminus S \neq \emptyset$. We set $X \in B \cap S^\Delta$ and $Y \in B \setminus S^\Delta$

4. The validity of this point is self evident.

□

Definition 5.0.4. Let $S \subseteq \Delta$ or $S \subseteq \Delta_i^j$. Denote $x_m[S] = min\{\chi_H[S] | H \in \nabla_m \setminus \nabla_{m-1}\}$

The following Proposition is related to the general definition of homogeneous set (S $\in \Delta^j$: we consider the tree of j-descendants). The importance of this Proposition stays on the fact that Sets S s.t. $S = homogeneousset \cup blockset$ have very interesting properties.

Proposition 5.0.6. Let $S \subseteq \Delta_i^j\, \Delta_0^j \cap S = \emptyset$. If $\chi_H[S] \equiv \chi_{H'}[S](mod\, p^{i+2j})$, for every $H, H' \in \nabla_{n-j} \setminus \nabla_{n-j-1}$, then:

1. $|\chi_H[S]|\, H \in \nabla_{n-j} \setminus \nabla_{n-j-1}| \leq 2$

2. there exists a unique homogeneous set $S^h \subseteq \Delta_i^j$ which is block equivalent to S and satisfies $x_{n-j}[S] = x_{n-j}[S^h]$for all $H \in \nabla_{n-j} \setminus \nabla_{n-j-1}$

3. $x_{n-j}[S] = -p^{2j} \sum_{l=1}^{i} a_l p^{l-1}$ whenever S is an $(a_1, a_2 \dots a_n)$homogeneous set and $(a_1, a_2 \dots a_i) \neq (p+1, p-1 \dots p-1)$

Proof. 1. it is proved: by Proposition 4.0.4 we have $|\chi_H[S] - \chi_{H'}[S]| \leqslant (2p^i - 1)p^{2j}$ whenever H, $H' \in \nabla_{n-j} \setminus \nabla n - j - 1$

2. This is by induction on i, fixed j. For $i = 1$, set $S = S^h$ and this is the only possible choice, since the complement of $S \cap (\Delta_1^j \setminus \Delta_0^j)$ cannot have the same x_{n-j}, except the case we have p odd and $a_1 = \frac{p+1}{2}$, but in that case the complement is equal to the set. Assume now $i > 1$, and the proposition holds until $i - 1$. Consider the set $S_{i-1} = S \cap \Delta_{i-1}^j$. We know by the corollary 4.0.1 that $\chi_H[F] \equiv 0 mod(p^{i+2j})$ whenever $l(F) = i$ (length in the sense of Δ^j), then we can conclude that $\chi_H[S_{i-1}] \equiv \chi_H[S] mod(p^{2j+i-1})$. We know that a block B has character $\chi_H[B] = p^{2j}$ if $B = \Delta_1^j \setminus \Delta_0^j$ and it has a character $\chi_H[B] = 0$ if $B \subsetneq \Delta_i^j \setminus \Delta_{i-1}^j$, then $S_{i-1} = S_{i-1}^h$, $\chi_H[S_{i-1}] = \chi_H[S_{i-1}^h]$. Let $F = Des_j(F^*)$,where F^* is the only forefather of H^Δ of length i. Let $F' = Father(F)$ and $B = sons(F')$. Then:

$$\chi_H[S] = \chi_H[S_{i-1}] + \chi_H[S \setminus \Delta_{i-1}^j] =$$

$$x_{n-j}[S_{i-1}^h] + \delta_{S_{i-1}}(F')p^{i-1+2j} - |S \cap B| p^{i-1+2j} + p^{i+2j} \delta_S(F).$$

Now, the hypothesis $\chi_H[S] \equiv \chi_{H'}[S] (mod\, p^{i+2j})$, for every $H, H' \in \nabla_{n-j} \setminus \nabla_{n-j-1}$ implies that

$$\exists a_i \in [0, p-1]\, s.t. - \delta_{S_{i-1}}(F') + |S \cap B| \equiv a_i mod(p).$$

The left hand side is $\in [-1, p]$, then or $0 < a_i = |S \cap B| - \delta_{S_{i-1}}(F') < p - 1$ or $a_i = 0$ or $a_i = p - 1$. In the first case, the homogeneous set is $S \setminus \Delta_{i-1}^j \cup (S_{i-1}^h)$. In the second case, we can obtain S^h from S by removing all the blocks s.t. $|S \cap B| = p\, \delta_{S_{i-1}}(F') = 0$. In the third case, we can obtain S^h by adding all the blocks s.t. $|S \cap B| = 0\, \delta_{S_{i-1}}(F') = 1$.

3. The equation is a straightforward consequence of corollary 4.0.1

□

Corollary 5.0.1. If $S \subseteq \Delta_i^j, S \cap \Delta_0^j = \emptyset$ and S^h is an $(a_1 \dots a_i)-$homogeneous set, then:

1. if $0 < a_l < p - 1$, then $S \cap (\Delta_l^j \setminus \Delta_{l-1}^j) = S^h \cap (\Delta_l^j \setminus \Delta_{l-1}^j)$ for each l, $1 \leqslant l \leqslant i$;

2. if S^h is neither $(0\dots0)-$ or $(p+1, p-1\dots p-1)$ homogeneous set, then there exists a B block such that $B \cap S \neq \emptyset$ and $B \setminus S \neq \emptyset$

Corollary 5.0.2. If $S \subseteq \Delta$ defines a non trivial SRCG over G, then there exists a unique $(a_1\dots a_n)-$homogeneous set $S^h \subseteq \Delta$ such that S is block equivalent to S^h.

Proposition 5.0.7. Let $S \subseteq \Delta$ be an $(a_1\dots a_n)-$homogeneous set. Then S defines an SRCG if and only if $a_2 = \dots = a_n$.

Proof. S defines a strongly regular graph. Let us consider two cases:

- the homogeneous set is a $(a_1, 0\dots0, a_n)$ set or its complementary. If S is an $(a_1, 0\dots0, a_n)$ - homogeneous set, then we can write:

$$k = \chi_G[S] = a_1(p^{n-1}-1) + \big(a_1(a_n+1)((p+1)p^{n-2}-a_1)a_n\big)\,(p^n - p^{n-1})$$

  if the corresponding graph is an SRG, then $(p^n - 1|k\, or\, p^n + 1|k)$ and the only possibility for that is $a_n = 0$.

- the homogeneous set is not $(a_1, 0\dots0, a_n)$ set nor its complementary. If the corresponding graph is an SRG, then there are only three possible values for any character $\chi_H[S]$. Since we have two possible values of $\chi_H[S]$ both if $H \in \nabla_n \backslash \nabla_{n-1}$ or if $H \in \nabla_{n-1} \setminus \nabla_{n-2}$, then $x_n[S] = x_{n-1}[S]$. We recall that:$A_{0,1} = a_1\; A_{0,2} = a_1 + a_2 p\; A_{i,i+1} = a_{i+1}\; A_{i,i+2} = a_{i+1} + a_{i+2}p$. We apply the equation 5.1 to find that:

$$x_n[S] = -\sum_{i=0}^{n-1} a_{i+1}p^i$$

$$x_{n-1}[S] = -a_1 - a_2 p - \sum_{i=2}^{n-2} a_i p^i$$

  Then we have:

$$a_2 p + \sum_{i=2}^{n-1} a_i p^i = \sum_{i=2}^{n} a_i p^{i-1}$$

  and that proves $a_2 = \dots = a_n$

Conversely, if S is a $(a_1, a_2\dots, a_2)$ homogeneous set, then, applying the equation 5.1, all the characters with kernel $H \in \nabla_t \setminus \nabla_{t-1}, t > 0$ are $s = -a_1 - a_2\sum_{i=2}^{n} p^{i-1}$ or $r = s + p^n$, and $\chi_G[S] = k = s(1-p^n)$. This proves that the corresponding graph is strongly regular. □

6 Non homogeneous strongly regular Cayley graphs over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$

Proposition 5.0.7 states the conditions under which a homogeneous set S corresponds to a strongly regular Cayley graph. Let us give some examples of strongly regular Cayley graphs over G, say $\Gamma_G(S)$,with S a non homogeneous set. Take $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$. The graph defined by a union of $(2,0)-$ homogeneous set and the unique block $B \in (\Delta_2 \backslash \Delta_1) \backslash S$ is a $(16,10,6,6)-SRCG$. Denote the class of such graphs by Γ_2. The complementary graph of a graph belonging to Γ_2 is the unique $(16,5,0,2)-$strongly regular graph, known in literature as Clebsch graph. We illustrated, in the picture 13, a set S corresponding to a graph belonging to Γ_2.

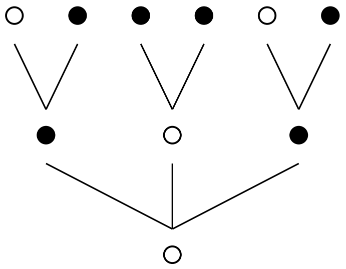


Figure 13: S corresponding to a graph member of Γ_2

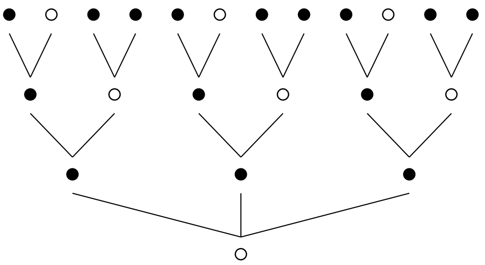


Figure 14: S corresponding to a graph member of Γ_3

Similarly, take $\mathbb{Z}_8 \oplus \mathbb{Z}_8$. The graph which is defined by a union of $(3,0,0)$-homogeneous set S and all the blocks $(B \subseteq (\Delta_3 \setminus \Delta_2) \setminus S$ is an $(64,45,32,30)-SRCG$ and we denote the class of such graphs Γ_3. We illustrated, in the picture 14, a set S corresponding to a graph belonging to Γ_3. We can argue that both the graphs from Γ_2 and the graphs corresponding to their $S^h = (2,0)-$ homogeneous sets are strongly regular (together with their complementary graphs Γ_2^c) and, similarly, both graphs from Γ_3 (or from the complementary family Γ_3^c) and the graphs corresponding to their $S^h = (3,0,0)$ homogeneous sets are strongly regular. The following proposition states that we cannot find, with the exception of these four families of graphs (Γ_2, Γ_3 and their complementaries) other situations in which :

- $S \neq S^h$,
- $\Gamma_G(S)$, $\Gamma_G(S^h)$ are both non trivial strongly regular graphs.

Proposition 6.0.1. If S and S^h define non trivial strongly regular Cayley graphs, then $S = S^h$ or $\Gamma_G(S) \in \Gamma$, with $\Gamma \in \{\Gamma_2, \Gamma_2^c, \Gamma_3, \Gamma_3^c\}$.

Proof. The Proposition 5.0.7 states that an S^h is homogeneous set if and only if $a_2 = \ldots = a_n$. If $(a_2 \neq 0 \wedge a_1 \neq 0) \vee (a_2 \neq p-1 \wedge a_1 \neq p+1)$ then Corollary 5.0.1 implies here that $S = S^h$. If $a_1 = a_2 = 0 \vee a_1 = a_2 = p-1$ then we have S^h corresponding to a trivial strongly regular graph and then we are out of the hypothesis of this proposition. The remaining cases are $a_2 = p-1 \wedge a_1 \neq a_2$ or the complementary case $a_2 = 0 \wedge a_1 \neq a_2$. We examine only the last case. We have $\chi_G[S] > \chi_G[S^h]$ since $|S| \geqslant |S^h|$. Let $B = \bigcup\{D\, block \subseteq \Delta | D \cap S^h = \emptyset\}$. Then:

$$\chi_G[B] = \sum_{i=2}^{n} \left(p^i + p^{i-1} - A_{0,i-1}p\right)\left(p^i - p^{i-1}\right) = p^{2n} - p^2 + a_1(p^2 - p^{n+1}).$$

Moreover, we have:

$$\chi_G[S^h] = a_1(p^n - 1)$$

and $s = -a_1$. The condition $\chi_G[S] > \chi_G[S^h]$ implies $\chi_G[S] \neq \chi_G[S^h]$, hence $\chi_G[S] = k" = s + sp^n + p^{2n} + p^n$, with $s = -a_1$ since $s(S) = s(S^h)$. At the end, we can write: $\chi_G[S] - \chi_G[S^h] = -2a_1p^n + p^n + p^{2n} \leqslant p^{2n} - p^2 + a_1p^2 - a_1p^{n+1}$ that implies $a_1 - 1 \geqslant p^{n-2}(a_1(p-2)+1)$. Hence $n = 2, p = 2, a_1 = 2$ or $n = 3, p = 2, a_1 = 3$. In the first case $S^h \cup B$ defines a graph from Γ_2 and in the second case $S^h \cup B$ defines a graph from Γ_3. □

Proposition 6.0.2. Let $H \in \nabla_1 \setminus \nabla_0$. Denote $\Omega_H = (\Delta \setminus \Delta_{n-1}) \setminus Des_{n-1}(H^{\Delta})$. Then for each subset $S \subseteq \Delta$ it is fulfilled that $\chi_G[S] - \chi_H[S] = p^n |\Omega_H \cap S|$

Proof. If $l(H) = l(H^\Delta) = 1$ then by Corollary 4.0.1 each element $F \in S$ is such that $\chi_H[F] > 0$ or $\chi_H[F] < 0$. Let T be the subset of S such that $\chi_H[F] < 0 \forall F \in T \wedge \chi_H[F'] > 0 \forall F' \notin T$. We prove that $T = \Omega_H \cap S$. The fact that $l(T \cap H^\Delta) = 0$ implies that $T \subseteq (\Omega_H \cap S)$ and the fact that T is the maximal set containing all the nodes $d : \chi_H[d] < 0$ implies that $\Omega_H \cap S \subseteq T$. Then $\chi_H[\Omega_H \cap S] = -p^{n-1}|\Omega_H \cap S| = \chi_G[\Omega_H \cap S] - |\Omega_H \cap S|p^n$. Then $\chi_H[S] = \chi_G[S \setminus (\Omega_H \cap S)] + \chi_H[\Omega_H \cap S] = \chi_G[S] - p^n|\Omega_H \cap S|$. □

Proposition 6.0.3. Let $\Gamma_G(S)$ be a non trivial $(p^{2n}, k, \lambda, \mu)-$strongly regular Cayley graph over G with $k = s + sp^n + p^n + p^{2n}$. If $p > 2$, then S is a $(\frac{p+1}{2}, \frac{p-1}{2} \dots \frac{p-1}{2})$- homogeneous set which defines an SRCG with Paley parameters. Moreover, $(\frac{p+1}{2}, \frac{p-1}{2} \dots \frac{p-1}{2})$ - homogeneous sets exhaust the set of strongly regular Cayley graphs with Paley parameters over G. If $p = 2$, then S or its complement satisfy $S \setminus S_{n-1} = (S^h \setminus S^{h-1}) \cup (\bigcup(block D \in \Delta \setminus \Delta_{n-1}|D \cap S^h = \emptyset)$.

Proof. Let $H \in \nabla_1 \setminus \nabla_0$. Then by Proposition 6.0.3 $\chi_G[S] - \chi_H[S] = p^n|\Omega_H \cap S|$. Since the graph is strongly regular, $\chi_H[S] \in \{s, s + p^n\}$. Then we have:

$$|\Omega_H \cap S| = \begin{cases} s + p^n + 1 & \text{if}\, \chi_H[S] = s \\ s + p^n & \text{if}\, \chi_H[S] = s + p^n \end{cases}$$

Let now $S^* = S_{n-1} \cup (S^h \setminus S^h_{n-1})$. Then $\Omega_H \cap S = \Omega_H \cap S^*$ and $|\Omega_H \cap S^*| = A_{0,n} - (A_{1,n} + \delta_{S^h}(H^\Delta))$. But $A_{0,n} - A_{1,n} = a_1 + \sum_{i=2}^n a_i(p^{i-1} + p^{i-2}) - \sum_{i=2}^n a_i p^{i-2} = a_1 + \sum_2^n a_i p^{i-1} = -s$. If $0 < a_n < p - 1$, then $S^* = S$, $\delta_{S^h}(H^\Delta) = \delta\{s + p^n\}(\chi_H[S])$ whence $s + p^n + 1 = -s \implies s = -\frac{(p^n+1)}{2}$.We can write:

$$-s = \frac{p^n + 1}{2} = \sum_{i=1}^n a_i p^{i-1} = a_1 + \sum_{i=2}^n a_2 p^{i-1} + \sum_{a_i \in A} (a_i - a_2)p^{i-1}$$

where A is the set of $a_j \neq a_2, 1 \leq j \leq n$. Then we can write: $\frac{(p^n+1)}{2} = a_1 + \frac{a_2}{p-1}(p^n - p) + \sum_{a(i) \in A}(a - a_2)p^{i-1} \implies a_2 = \frac{p-1}{2}$, $a_1 = \frac{p+1}{2}, A = \emptyset$. Since $a_2 = \ldots = a_n < p - 1 \wedge 0 < a_1 < p + 1$, then S^h is a Strongly regular Cayley graph and $S = S^h$. Verify the corresponding graph is a Paley graph. See the proof of the Proposition 5.0.4. In the case of $k = (s + p^n)(1 + p^n)$ we have: $k = \frac{p^{2n}-1}{2}$, $\mu = \frac{p^n-1}{2}\frac{p^n+1}{2} = \frac{p^{2n}-1}{4}$, $\lambda = \frac{p^n-1}{2}\frac{p^n+1}{2} = \frac{p^{2n}-5}{4}$. If S is a Paley graph, then $\lambda - \mu = -1 = r + s = 2s + p^n$ and $s = -(\frac{p^n+1}{2})$. Using the same arguments, we conclude that S is a $(\frac{p+1}{2}, \frac{p-1}{2} \dots \frac{p-1}{2})$ and that is the only possible Paley graph if $0 < a_n < p-1$. Consider the case of $a_n = 0$. Let $B := \bigcup\{block\, D \in \Delta | D \subseteq \Omega_H, D \cap S^h = \emptyset\}$ There are $(p + 1 - 1)p^{n-1} = p^n$ elements in Ω_H. Show the following tree:

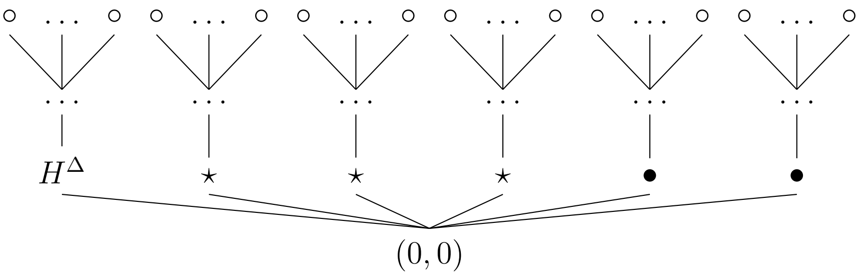


Figure 15: Proof of Proposition 6.0.3

where the star stands for an element of $\Delta_1 \setminus \Delta_0$ not belonging to S^h and a bullet stands for an element of $\Delta_1 \setminus \Delta_0$ belonging to S^h. We do not assign a bullet or a star to H^{Δ} since we use $\delta_{S^h}(H^{\Delta})$. Since $a_n = 0$, then for each block K whose intersection with $S^h_n \setminus S^h_{n-1}$ is not the empty set, we can write $|K \cap (S^h)| = 1$. To obtain $|B|$, we must subtract $p^n - \sum_{K:K\in S^h_n\setminus S^h_{n-1}} p$. It follows that,to obtain $|B|$, we have to subtract $p|\star|\cdot|Des_{n-1}(\star)\cap S^h| = (p-a_1+\delta_{S^h}H^{\Delta})pA_{1,n}$ and $p|\bullet|\cdot|Des_{n-1}\bullet\cap S^h| = (a_1 - \delta_{S^h}(H^{\Delta}))p(A_{1,n}+1)$. We get: $|B| = p^n - p(a_1 - \delta_{S^h}H^{\Delta} + pA_{1,n})$. We can write the following inequality:

$$\begin{aligned}
&0 = |\Omega_H \cap S| - |\Omega_H \cap S^*| - |B \cap S| \geqslant |\Omega_H \cap S| - |\Omega_H \cap S^*| - |B| = \\
&s + p^n + 1 - \delta_{\{s+p^n\}}(\chi_H[S]) + s + \delta_{S^h}(H^{\Delta}) - p(p^{n-1} - A_{1,n}p) + a_1 p - \delta_{S^h}(H^{\Delta})p = \\
&(p-2)\sum_{i=1}^{n} a_i p^{i-1} + 1 - \delta_{\{s+p^n\}}(\chi_H[S]) - (p-1)\delta_{S^h}(H^{\Delta})
\end{aligned} \tag{6.1}$$

If $p \neq 2$ then we have a contradiction. Indeed if there exists $a_j \neq 0, 1 \leq j \leq n-1$, then the quantity in the right hand of the inequality (6.1) is strictly positive, but the inequality states it must be null or negative. If all the parameters of S^h are 0, then by Proposition 6.0.1 $S = S^h$ and $k = s - sp^n$. Since $s - sp^n = s + sp^n + p^n + p^{2n}$ this implies $s = -\frac{p^n+1}{2}$ and this contradicts with $a_n = 0$. If instead $a_n = 0$ and $p = 2$, the inequality (6.1) is:

$$1 - \delta_{\{s+p^n\}}(\chi_H[S]) - \delta_{S^h}(H^{\Delta}) \leqslant 0.$$

This last inequality turns to be an equality: both $|B \cap S|$ and $|B|$ are divisible by p. We remind that:

$$0 = |\Omega_H \cap S| - |\Omega_H \cap S^*| - |B \cap S| = 2s + 2^n + 1 - (\delta_{\{s+p^n\}}\chi_H[S] + \delta_{S^h}(H^{\Delta})) - |B \cap S|.$$

Now: $2s + 2^n - |B\cap S|$ is an even number. It means that the number $1 - (\delta_{\{s+p^n\}}\chi_H[S] + \delta_{S^h}(H^{\Delta}))$ must be even (0 is the only even value it can assume) as well. Therefore $(\delta_{\{s+p^n\}}\chi_H[S] + \delta_{S^h}(H^{\Delta})) = 1$ and $B \cap S = B$. Since $\Delta \setminus \Delta_{n-1} = \bigcup_{H\in\nabla_1\setminus\nabla_0} \Omega_H$, it holds that $\bigcup\{block\, D \in \Delta \setminus \Delta_{n-1} | D \cap S^h = \emptyset\} \subseteq S$. If $\Gamma_G(S)$ is an SRCG with the valency $s + sp^n + p^n + p^{2n}$ then its complement has the valency of the same type. Then the case $a_n = p - 1$ is complement to the case $a_n = 0$. □

Remark 6.0.1. If $p = 2$ we cannot have any SRCG with Paley parameters over G. Indeed, to have Paley parameters, $s = \frac{p^n+1}{2}$, but s is an integer. This agrees with the results of [15], who proved that a SRCG over a finite abelian group of rank 2 exists if and only if G is isomorphic to $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$, p odd prime.

Proposition 6.0.4. Let S define a non-trivial SRCG over G. If $k = s - sp^n$ then $S \setminus S_{n-1} = S^h \setminus S^h_{n-1}$

Proof. Let $H \in \nabla_1 \setminus \nabla_0$. Let $S^* = S_{n-1} \cup (S^h \setminus S^h_{n-1})$. Then

$$\chi_G[S^*] = \chi_G[S_{n-1}] + A_{0,n}(p^n - p^{n-1})$$

and

$$\chi_H[S^*] = \chi_G[S_{n-1}] + (A_{1,n} + \delta_{H^\Delta}(S^h))p^n - A_{0,n}p^{n-1}.$$

Therefore by Proposition 6.0.3:

$$|\Omega_H \cap S^*| = A_{0,n} - A_{1,n} - \delta_{H^\delta}(S^h) = -s - \delta_{H^\delta}(S^h).$$

Again by Proposition 6.0.3 and by $k = s - sp^n$ we have $|\Omega_H \cap S| = -s - \delta_{\{s+p^n\}}(\chi_H[S])$. By construction of S^h either $S^* \subseteq S$ or$S \subseteq S^*$. From which it follows that $|\Omega_H \cap S \div \Omega_H \cap S^*| = ||\Omega_H \cap S| - |\Omega_H \cap S^*|| \in \{0, 1\}$, where $\div$ denotes the symmetric difference. Since $\Omega_H \cap S$ and $\Omega_H \cap S^*$ are block equivalent, the cardinality of their symmetric difference is divisible by p. It follows that $|\Omega_H \cap S| = |\Omega_H \cap S^*|$ and $\Omega_H \cap S = \Omega_H \cap S^*$.Since $\Delta \setminus \Delta_{n-1} = \bigcup_{H \in \nabla_1 \setminus \nabla_0} \Omega_H$, we obtain $(\Delta \setminus \Delta_{n-1}) \cap S = (\Delta \setminus \Delta_{n-1}) \cap S^* \implies S \setminus S_{n-1} = S^h \setminus S^h_{n-1}$ □

Proposition 6.0.5. Let S define a non-trivial SRCG over G, $p > 2$. Then either S is an
$(a_1, a_2 \ldots a_2)$-homogeneous set or S^h is an $(a_1, \ldots, a_n)-$homogeneous set with $a_{n-1} = 0$ or $a_{n-1} = p - 1$

Proof. Now we can assume that $n \geqslant 3$. According to Corollary 5.0.2there exists a block set U such that $S = S^h \div U$. Denote $R = S^h \cap U$, $T = U \setminus S^h$. Let $F \in \nabla_{n-1} \setminus \nabla_{n-2}$.Then $\chi_F[S] = \chi_F[S^h] + \chi_F[T] - \chi_F[R]$. We have that, by Proposition 5.0.5 $|\{residue\, of\, \chi_F[S^h]$ mod $p^n | l(F) = n-1\}| = 1$. Furthermore, $|\{residue\, of\, \chi_F[S] mod\, p^n | l(F) = n-1\}| = 1$. By Proposition 6.0.4 $S \setminus S_{n-1} = S^h \setminus S^h_{n-1}$. Then $T^1 \subseteq \Delta^1_{n-2}, R^1 \subseteq \Delta^1_{n-2}$. Denote $\overline{R} = \bigcup_{\{m | a_m = p-1, 2 \leqslant m \leqslant n-1\}} (\Delta_m \setminus \Delta_{m-1}) \setminus R$. Since $\chi_F[\Delta_m \setminus \Delta_{m-1}] = -p^2\delta_2(m)$ for $n \geqslant m \geqslant 2$, it follows that $\chi_F[\overline{R}] = -p^2\delta_{\{m|a_m=p-1\}}(2) - \chi_F[R]$. Denote $Q = T \cup \overline{R}$

and $\rho = \delta_{\{m|a_m=p-1\}}(2)$. By Proposition 5.0.6, Q^1 is block equivalent to the unique $\{b_1, b_2, \dots, b_2\}-$ homogeneous set $Q^{1h} \subseteq \Delta^1_{n-2}$ with $Q^{1h} \cap \Delta^1_1 = Q^1 \cap \Delta^1_1$. Therefore

$$\chi_F[Q] = \chi_F[Q^{1h}] = x_{n-1}[Q] + \delta_{Q^{1h}}(Sons(Father(F^{\Delta})))p^n.$$

If Q^{1h} is not a $(p+1, p-1, \dots, p-1)$-homogeneous set:

$$\begin{aligned} &\chi_F[S] = s + \delta_{\{s+p^n\}}(\chi_F[S])p^n = \\ &\chi_F[S^h] + \chi_F[T] - \chi_F[R] = \chi_F[S^h] + \chi_F[Q] + \rho p^2 = \\ &x_{n-1}[S^h] + \delta_{S^h}(F^{\Delta})p^n + x_{n-1}[Q] + \delta_{Q^{1h}}(Sons(Father(F^{\Delta})))p^n + \rho p^2. \end{aligned} \tag{6.2}$$

If Q^{1h} is a $(p+1, p-1, \dots, p-1)$- homogeneous set, then $\chi_F[Q^{1h}] = \chi_F[S] = x_{\{n-1\}}[S^h] + \delta_{S^h}(F^{\Delta})p^n - p^2 + \rho p^2$. Consider the cases when Q^{1h} is a $(0, \dots, 0)-$homogeneous set and $\rho = 0$ or $Q^{1h}$is a $(p+1, p-1, \dots p-1)$ - homogeneous set and $\rho = 1$. If $a_{n-1} = 0$ or $a_{n-1} = p-1$ there is nothing to prove. If $a_{n-1} \neq 0 \wedge a_{n-1} \neq p-1$ then $\chi_F[S] = s + \delta_{S^h}(F^{\Delta})$, $s = x_{n-1}[S]$ and this implies that S is $(a_1, a_2, \dots, a_2)$ - homogeneous. Then by Proposition 6.0.1 $S = S^h$. If Q^{1h} is a $(p+1, p-1, \dots, p-1)-$homogeneous set and $\rho = 0$ then (let us remember that $\rho = 0 \iff a_2 \neq p-1 \wedge \rho = 1 \iff a_2 = p-1$) $a-2 \neq p-1$. Let us recall the definition of $\overline{R} = \bigcup_{\{m|a_m=p-1, 2\leqslant m\leqslant n-1\}}(\Delta_m \setminus \Delta_{m-1}) \setminus R$. It follows that, if $\rho = 0$, $(\Delta_2 \setminus \Delta_1) \cap \overline{R} = \emptyset$. Then $Q = T \cup \overline{R} \implies Q \cap (\Delta_2 \setminus \Delta_1 \cap Q = (\Delta_2 \setminus \Delta_1) \cap T$. This clearly implies that $a_1 = 0$: $(\Delta_2 \setminus \Delta_1) \cap T$ is a block set. But $a_2 = 0$ as well (by Corollary 5.0.1). Now recall the Equation (5.1). In this case, $t = n-1, A_{0,1} = A_{0,2} = 0, A_{i,i+1} = a_{i+1}, A_{i,i+2} = a_{i+1} + a_{i+2}p$. Thus, $x_{n-1}[S] = -\sum_{i=1}^{n-3} a_{i+2}p^{i+2} = \sum_{i=3}^{n-1}(-a_i p^i)$. The equality $s = x_{n-1}[S] - p^2$ implies that: $s = -\sum_{i=3}^{n} a_i p^{i-1} = -\sum_{i=3}^{n-1} a_i p^i - p^2$, that is equivalent to:$\sum_{i=3}^{n-1}(p-1)a_i p^{i-1} = a_n p^{n-1} - p^2$. We can adjust the right-hand part of the equality in this way: $a_n p^{n-1} - p^2 = a_n p^2(p^{n-3} - 1) + a_n p^2 - p^2 = a_n p^2 \sum_{i=1}^{n-3} p^{i-1}(p-1) + p^2(a_n - 1) = a_n \sum_{i=3}^{n-1} p^{i-1}(p-1) + p^2(a_n - 1)$. Then we can write:

$$\sum_{i=3}^{n-1}(p-1)a_i p^{i-1} = a_n \sum_{i=3}^{n-1} p^{i-1}(p-1) + p^2(a_n - 1).$$

This implies that $a_i = 1 \forall 3 \leq i \leq n$ or that S^h is a $(0, 0, 1, \dots, 1)-$homogeneous set and $S = S^h \cup (\Delta_2 \setminus \Delta_1)$. The equality $k = s(1-p^n) = \chi_G[S^h] + \chi_G[\Delta_2 \setminus \Delta_1]$ implies $n = 4$. We obtain a contradiction, since in that case $x_2[S] \neq s$ and the graph cannot be strongly regular. We should do similar passages to examine the case Q^{1h} is $(0, \dots, 0) - homogeneous$ with$\rho = 1$ to get a similar contradiction. Last sub-hypothesis: Q^1 block equivalent to a homogeneous set that is nor $(0, \dots, 0)-$ nor $(p+1, p-1, \dots, p-1)-$ homogeneous. In this case $a_{n-1} = 0$ or $a_{n-1} = p-1$ as a consequence of Corollary 5.0.1. □

Lemma 6.0.1. Let S define a non-trivial SRCG over G, $p > 2$. Then either S is an $(a_1, a_2, \dots, a_2)-$ homogeneous set or one of the sets S^h or $(\Delta \setminus \Delta_0) \setminus S^h$ is an $(a_1, 0, \dots, 0, a_n)-$homogeneous set.

Theorem 6.0.1. Let p be a prime number. Every strongly regular Cayley graph over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ is defined by a subset of Δ. Let $p > 2$ and let $\varphi : \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}/\langle (p^{n-1}, 0), (0, p^{n-1})\rangle$ be the canonical homomorphism, $S \subseteq \Delta$ and $S \neq \emptyset$, $S \neq \Delta \setminus \{e\}$. S defines a non-trivial strongly regular Cayley graph over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$ if and only if one of the following conditions is true:

1. S is an $(a_1, a_2, \dots, a_2)-$homogeneous set and S is not a $(1, 0, \dots 0)$ or a $(p, p-1, \dots, p-1)-$ homogeneous set;

2. if $n > 3$, then S^h is an $(a_1, 0, \dots, 0, a_n)-$ homogeneous set with $a_n > 0$, $S^h \subseteq S$ and $Q = \varphi(S \setminus S^h)$ defines a non trivial strongly regular Cayley graph over $\varphi(p(\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n})$ for which Q^h is a $(0, \dots, 0, a_n)-$ or a$(p, p-1, \dots, p-1, a_n - 1)-$ homogeneous set. If $n = 3$, then S^h is an $(a_1, 0, a_3)-$homogeneous set with $a_3 > 0$, $S^h \subseteq S$ and $Q = \varphi(S \setminus S^h)$ is an $(a_3)-$homogeneous set which defines a strongly regular Cayley graph over $\varphi(p(\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^3}) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$;

3. S is a complement of the mentioned in the previous item.

Proof. If $S \neq S^h$ and it is corresponding to an SRCG, then by Proposition 6.0.1 and by Lemma 6.0.1 S^h, does not correspond to an SRCG and it is an $(a_1, 0, \dots, a_n)$- homogeneous set, or $(\Delta \setminus \Delta_0) \setminus S^h$ is an $(a_1, 0, \dots, 0, a_n)$- homogeneous set. By Proposition 6.0.3 the valency k of the SRCG associated to S is $k = s(1 - p^n)$ and by Proposition6.0.4 $(S \setminus S^h) \cap (\Delta_n \setminus \Delta_{n-1}) = \emptyset$. Let us consider the case $S^h = (a_1, 0, \dots, 0, a_n)-$ homogeneous set. In this case, according to the equation (5.1), $x_n[S^h] = -a_1 - a_n p^{n-1}$ and, for each $2 \leq t \leq n-1$, $x_{n-1}[S^h] = -a_1$. By this and, again, by Proposition 6.0.4, $Q = \varphi(S \setminus S^h)$ corresponds to an SRCG over $\varphi(pG)$ with $s = -a_n p^{n-3}$ and $r = s + p^{n-2}$ (Theorem 5.0.1). If $n > 3$, $0, -1$ are not eigenvalues of Q. Then Q^h is a $(0, \dots, a_n)-$homogeneous set or a $(p, p-1, \dots, p-1, a_n - 1)$-homogeneous set. If $a_n = 3$, then Q is an $(a_3)-$ homogeneous set. If $a_3 > 1$, then an a_3-homogeneous set defines a non trivial SRCG over $\mathbb{Z}_p \oplus \mathbb{Z}_p$. For Proposition 6.0.3, $x_0[Q] = -a_n p^{n-3}(1 - p^{n-2})$. In addition, $x_0[S \setminus S^h] = x_1[S \setminus S^h] = p^2 x_0[Q] = -a_n p^{n-1} + a_n p^{2n-3}$ and $x_1[S^h] = -a_1 - a_n p^{2n-3}$. Then $x_1[S] = x_1[S \setminus S^h] + x_1[S^h] = -a_1 - a_n p^{n-1} = x_i[S], \forall\, i : 1 \leq i \leq n$. Then all the graphs cited in this Theorem are strongly regular. □

7 Strongly regular Cayley graphs over $\mathbb{Z}_{2^n} \oplus \mathbb{Z}_{2^n}$

In this chapter we show some numerical results. They are interesting, since we cannot apply the Theorem 6.0.1. We will analyse the following cases: $p = 2$ and $n = 2$, $n = 3\, n = 4$. A numerical research, held by [17] gave some very important results. M.E. Malandro and K. W. Smith split the SRCG over $\mathbb{Z}_{2^n} \oplus \mathbb{Z}_{2^n}$ in three categories:

1. Partial congruent partitions;

2. Reversible Hadamard partial difference sets (of type A or of type B);

3. A remaining category, they called "sporadic".

Definition 7.0.1. Suppose that a group of order m^2 has t subgroups $H_1, \dots, H_t$, each of order m, such that each pair meets only in the identity. Then the set S consisting of the union of these subgroups, less the identity, gives a strongly regular Cayley graph. These classes of graphs are said to be *partial congruent partitions* and labeled as *PCP(t).*

In particular, [17] fixed the attention to PCP(2) and PCP(3).

Definition 7.0.2. Let G be a group of order $4m^2$. A *Hadamard difference set* (HDS) in G is a subset $D \subseteq G$ such that the multiset $\{g_1 g_2^{-1}, g_1 \wedge g_2 \in D\}$ has exact $\lambda = m^2 - m$ occurrences for every non identity member $g \in G$. A Hadamard difference set is said to be *reversible* if $D = D^{-1}$ the set of its inverses.

Remark 7.0.1. if the identity is in D, then D is a reversible HDS if and only if D^c is a symmetric subgroup of G with degree $2m^2 + m$. If the identity is not in D, then it is a reversible HDS if and only if D is a symmetric subgroups of G with degree $2m^2 - m$.

Definition 7.0.3. A *reversible Hadamard partial difference set of type A* (RHPDSA) is a Hadamard Difference set of degree $2m^2 - m$. A *reversible Hadamard partial difference set of type B* (RHPDSB) is a complementary of a Hadamard difference set, with a degree $2m^2 + m$.

Helped by an intense numerical research, Malandro and Smith formulated the following conjecture:

Conjecture 1.2 [17]: The total number of reversible Hadamard partial difference sets in $G_n = \mathbb{Z}_{2^n} \oplus \mathbb{Z}_{2^n}$ of:

- type A: $(2^{2^n-2})(2^n - 1)$
- type B: $(2^{2^n-2})(2^n + 1)$

7.1 p=2, n=2

All the homogeneous sets correspond to strongly regular graphs. There are two families of $\Gamma_G(S)$ which are strongly regular graphs and such that S is a non homogeneous set: they are Γ_2 and Γ_2^c. The following tables collects all those homogeneous sets:

S^h	s	k
$(0,1)$	-2	6
$(1,1)$	-3	9
$(2,0)$	-2	6
$(3,0)$	-3	9

Table 2: Homogeneous sets corresponding to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$

We did not list $(0,0) - S^h$,$(1,0) - S^h$, $(2,1) - S^h$ and $(3,3) - S^h$ since they correspond to trivial strongly regular graphs.

7.2 p=2, n=3

All the homogeneous sets such that $\Gamma_G(S)$ is a non trivial SRCG are of the type $(a_1, 0, 0)$ or $(a_1, 1, 1)$, with $0 \leq a_1 \leq p+1$. Now we proceed to list all the non-homogeneous sets corresponding to a non trivial SRCG. Read the table in the following way: S^h stands for the array identifying the homogeneous set block equivalent to S. To identify S, add the number blocks in $\Delta_2 \setminus \Delta_1$ and in $\Delta_3 \setminus \Delta_2$ indicated in the table (if that number is negative, it means you have to subtract blocks belonging to S^h to obtain S).

Remark 7.2.1. The graphs corresponding to the $(0,1,0)-$homogeneous sets and to the $(3,0,1)-$ homogeneous sets are not strongly regular and, in addition, there does not exist any S block equivalent to one of them such that $\Gamma_G(S)$ is an SRCG.

S^h	blocks $\in \Delta_2 \setminus \Delta_1$	blocks $\in \Delta_3 \setminus \Delta_2$	s	k
$(0,0,1)$	1	–	-4	28
$(0,0,1)$	3	–	-4	36
$(0,1,1)$	–	-3	-6	18
$(1,0,1)$	1	–	-5	35
$(1,0,1)$	1	-1	-5	27
$(1,1,0)$	-1	–	-3	21
$(2,0,1)$	1	–	-6	42
$(2,1,0)$	-1	–	-4	28
$(2,1,0)$	-1	1	-4	36
$(3,0,0)$	–	3	-3	45
$(3,1,0)$	-1	–	-5	35
$(3,1,0)$	-3	–	-5	27

Table 3: Non homogeneous sets corresponding to $\mathbb{Z}_8 \oplus \mathbb{Z}_8$

7.3 p=2, n=4

We performed a numerical analysis of the S sets which are block equivalent to an S^h s.t. $a_1 \ldots, a_n \in \{0,1\}$. This is not a loss of generality, since a graph is strongly regulr if and only if its complementary graph is strongly regular. We arranged all the homogeneous sets block equivalent to a set S s.t $\Gamma_G(S)$ is strongly regular. We can exclude from that table the following S^h sets:

- $(0,0,0,0)-S^h$,$(1,0,0,0)-S^h$: their corresponding graphs are trivial;
- $(0,0,1,0)-S^h$: $k=72$. All the blocks forming $\Delta_2 \setminus \Delta_1$ do not belong to S^h.But 15 does not divide $72,76,80,84$. In addition, there are 6 blocks from $\Delta_4 \setminus \Delta_3$ totally out of S^h. But 17 does not divide $168,172,176,180$;
- $(0,1,0,0)-S^h$:$k=42$. Three blocks from $\Delta_3 \setminus \Delta_2$ are totally out of S^h. But 15 does not divide $42,50,58,66$. In addition, there are 9 blocks from $\Delta_4 \setminus \Delta_3$ totally out of S^h. But 17 does not divide $138,146,154,162$;
- $(0,1,0,1)-S^h$:$k=138$. There are three blocks from $\Delta_3 \setminus \Delta_2$ out of S^h.But 15 does not divide $138,146,154,162$. In addition, there are three blocks from $\Delta_4 \setminus \Delta_3$ belonging to S^h. But 17 does not divide $90,98,106,114$;
- $(1,0,1,0)-S^h$:$k=87$. There is a block in $\Delta_3 \setminus \Delta_2$ belonging to S^h and there are two blocks from $\Delta_2 \setminus \Delta_1$ not belonging to S^h. But 15 does not divide

$79, 83, 87, 91, 95$. In addition, there are 5 blocks from $\Delta_4 \setminus \Delta_3$ out of S^h. But 17 does not divide $159, 163, 167, 171, 175$;

- $(1,0,1,1) - S^h$:$k = 183$. There is a block in $\Delta_3 \setminus \Delta_2$ belonging to S^h and there are two blocks from $\Delta_2 \setminus \Delta_1$ not belonging to S^h. But 15 does not divide $175, 179, 183, 187, 191$. In addition, there are 7 blocks blocks from $\Delta_4 \setminus \Delta_3$ belonging to S^h. But 17 does not divide $63, 67, 71, 75, 79$;

- $(1,1,0,0) - S^h$:$k = 57$. There is one block from $\Delta_2 \setminus \Delta_1$ belonging to S^h and there are two blocks from $\Delta_3 \setminus \Delta_1$ not belonging to S^h. But 15 does not divide $53, 57, 61, 65, 69, 73$. In addition, there are 8 blocks from $\Delta_4 \setminus \Delta_3$ not belonging to S^h, but 17 does not divide $181, 185, 189, 194, 198, 202$.

The remaining sets are arranged in the following table.

S^h	blocks $\in \Delta_2 \setminus \Delta_1$	blocks $\in \Delta_3 \setminus \Delta_2$	blocks$\in \Delta_4 \setminus \Delta_3$	s	k
$(0,0,0,1)$	$-$	$B_1 \in Des_2(\langle(0,8)\rangle) \cup B_2 \in Des_2(\langle(8,8)\rangle) \cup B_3 \in Des_2(\langle(8,0)\rangle)$	$-$	-8	120
$(0,0,0,1)$	C_1, C_2	$B_1\, B_2\, s.t\, Father(B_1) \in C_1\, Father(B_2) \in C_2$	$-$	-8	120
$(0,0,0,1)$	C_1, C_2	$B_1\, B_2\, s.t\, Father(B_1) \in C_1\, Father(B_2) \in C_2, B_3, B_4 : Father(B_3) = Father(B_4) \wedge \neq (Father(B_1) \vee Father(B_2))$	$-$	-8	136
$(0,0,1,1)$	add all blocks	$-$	$-$	-12	180
$(0,1,1,0)$	$-$	remove all blocks	$-$	-6	90
$(0,1,1,1)$	$-$	$-$	$-$	-14	210
$(1,0,0,1)$	$-$	$A, B, C\, s.t. A \cap B = A \cap C = B \cap C = \langle(0,0)\rangle$	$-$	-9	135
$(1,0,0,1)$	C_1, C_2	$B_1\, B_2\, s.t\, Father(B_1) \in C_1\, Father(B_2) \in C_2$	$-$	-9	135
$(1,0,0,1)$	$-$	$A, B, C\, s.t. A \cap B = A \cap C = B \cap C = \langle(0,0)\rangle$	remove block	-9	119
$(1,0,0,1)$	C_1, C_2	$B_1\, B_2\, s.t\, Father(B_1) \in C_1\, Father(B_2) \in C_2$	remove block	-9	119
$(1,1,0,1)$	remove block	add all blocks	$-$	-11	165
$(1,1,1,0)$	$-$	remove $A, B, C\, s.t. A \cap B = A \cap C = B \cap C = \langle(0,0)\rangle$	$-$	-7	105
$(1,1,1,1)$	$-$	$-$	$-$	-15	225

Table 4: Non homogeneous sets corresponding to SRCG over $Z_{16} \oplus \mathbb{Z}_{16}$ and S^h with $a_i \in \{0,1\}$

Remark 7.3.1. A classification of SRCGs on $G - \mathbb{Z}_{2^n} \oplus \mathbb{Z}_{2^n}$ is quite difficult, since we have homogeneous sets of the form $(a_1, \ldots 1, \ldots 0, \ldots a_n) - S^h$ or $(a_1, \ldots 0, \ldots 1, \ldots a_n) - S^h$ which are block equivalent to a set S such that $\Gamma_G(S)$ is a SRCG. We listed two of them in the previous table: $(1,1,0,1) - S^h$, $(0,0,1,1) - S^h$.

8 Octave subroutines

We show the subroutines we accomplished in order to inquiry on the SRCG over $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$.

8.1 Adjacency matrices and eigenvalues of an SRCG

We arranged a subroutine which turned to be very useful to check the correctness of the calculation of the characters of a SRCG. We called it "*Cayley_Matrix.m*". The great efficiency of the function "eig.m", together with the same efficiency of the function "ismember.m", subroutines both defined in the Matlab/Octave environment, allowed us to manage matrices of a not pretty small size. The subroutine was tested for Adjacency matrices 256 × 256 sized, giving the response in a pair of minutes. This subroutine takes a matrix S, a prime p and a positive integer as inputs. Each cell (a, b) of the Adjacency matrix is defined as $ismember((a-b) \mod p^n, S, "rows")$, so that the boolean value "1" is assigned, if $(a-b) \mod p^n$ does belong to the rows of S, the boolean "0" is assigned otherwise. After the conversion from boolean type to double type, the list of eigenvalues of the Adjacency matrix is calculated by *eig.m*.

Example 8.1.1. We want to calculate the eigenvalues of $\Gamma_G(S)$ with $G = \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2}$ and $S = \{(2,2), (1,0), (3,0), (1,1), (3,3), (1,3), (3,1), (0,1), (0,3)\}$. We arrange S into an array, defined (according to the syntax of Matlab, a semicolon defines a new row and a comma a new column), in the following way:
$[[2,2];[1,0];[3,0];[1,1];[3,3];[1,3];[3,1];[0,1];[0,3]]$. We obtain the expected result: $\lambda_1 = -3$, $\lambda_2 = 1$, $\lambda_3 = 9$.

8.2 Construction of Δ tree

The first subroutine is "cyclic.m". This file accepts three inputs: generator, p and n. Its aim is to calculate the cyclic group generated by generator, an element of $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. The output is: subgroup, a structure array containing all the elements of the cyclic group. This file works with a built-in function of Octave, which is rem. That function accepts an ordered couple of integers x, y and returns the reminder of the division $\frac{x}{y}$. Another built-in function used in the file is "norm". The control is when the neutral element is generated: at that moment, we know all the elements of the cycle are stored in the output structure array (in Octave or Matlab environment, that data structure is known as *cell*).

Example 8.2.1. Let us try to use the array $[4,4]$ corresponding to the couple $(4,4)$ as generator, $p = 2$, $n = 4$. The output is the following structure array:
$\{[1,1] = 4\ 4, [1,2] = 8\ 8, [1,3] = 12\ 12, [1,4] = 0\ 0\}$ corresponding to the subgroup:
$\{(0,0), (4,4), (8,8), (12,12)\}$

The second subroutine is ”*cyclic_gen.m*”. This function calls the previous one,and it accepts p,m and n as inputs in order to calculate all the members of $\Delta_{n-m} \setminus \Delta_{m-n-1}$.

Example 8.2.2. We want to calculate $\Delta_2 \backslash \Delta_1$ of Δ on $\mathbb{Z}_8 \oplus \mathbb{Z}_8$. We give the inputs: $p = 2, n = 3, m = 1$ and we obtain the structure array as output of ”*cyclic_gen*”:$\{[1,1] = \{[1,1] = 2\ 0[1,2] = 4\ 0, [1,3] = 6\ 0, [1,4] = 0\ 0\}[1,2] = \{[1,1] = 2\ 2, [1,2] = 4\ 4, [1,3] = 6\ 6[1,4] = 0\ 0\}[1,3] = \{[1,1] = 2\ 4, [1,2] = 4\ 0[1,3] = 6\ 4[1,4] = 0\ 0\}, [1,4] = \{[1,1] = 2\ 6[1,2] = 4\ 4, [1,3] = 6\ 2, [1,4] = 0\ 0\}[1,5] = \{[1,1] = 0\ 2, [1,2] = 0\ 4, [1,3] = 0\ 6, [1,4] = 0\ 0\}[1,6] = \{[1,1] = 4\ 2, [1,2] = 0\ 4, [1,3] = 4\ 6[1,4] = 0\ 0\}\}$

The output of ”*cyclic_gen*” is the whole block set $\Delta_{n-m} \setminus \Delta_{m-n-1}$. The problem of the cell generated as output is that there is no partition in blocks. To get the output more readable, other two subroutines are accomplished. One of them is ”intersection.m”. It accepts as input two cells, and it returns the elements present in both of them. This function uses a function defined in Octave environment, which is ”intersect”.

Example 8.2.3. Let x be $x = \{[1,1] = [4,4], [1,2] = [8,8], [1,3] = [12,12], [1,4] = [0,0]\}$ and let y be $y = \{[1,1] = [8,8], [1,2] = [0,0]\}$. Then $z = intersection(x,y)$ turns to be $z = y$.

A function accomplished to find the Father of each node of the block set $\Delta_{n-m} \setminus \Delta_{m-n-1}$ is *blocks.m*. It intersects $\Delta_{n-m} \setminus \Delta_{m-n-1}$ with $\Delta_{n-m-1} \setminus \Delta_{m-n-2}$ and stores the Father of each set, element of $\Delta_{n-m} \setminus \Delta_{m-n-1}$ into a Matlab cell. It is easier to illustrate the output by an example.

Example 8.2.4. $p = 2, m = 1, n = 3$. The output of *cyclic_gen* is: $\{[1,1] = \{[1,1] = [2,0], [1,2] = [4,0], [1,3] = [6,0], [1,4] = [0,0]\}[1,2] = \{[1,1] = [2,2], [1,2] = [4,4], [1,3] = [6,6], [1,4] = [0,0]\}[1,3] = \{[1,1] = [2,4], [1,2] = [4,0], [1,3] = [6,4], [1,4] = [0,0]\}[1,4] = \{[1,1] = [2,6], [1,2] = [4,4], [1,3] = [6,2], [1,4] = [0,0]\}, [1,5] = \{[1,1] = [0,2], [1,2] = [0,4], [1,3] = [0,6], [1,4] = [0,0]\}[1,6] = \{[1,1] = [4,2], [1,2] = [0,4], [1,3] = [4,6], [1,4] = [0,0]\}\}$, the output of blocks is: $\{[1,1] = \{[1,1] = [4,0], [1,2] = [0,0]\}[1,2] = \{[1,1] = [4,4], [1,2] = [0,0]\}[1,3] = \{[1,1] = [4,0], [1,2] = [0,0]\}[1,4] = \{[1,1] =$

$[4,4], [1,2] = [0,0]\}[1,5] = \{[1,1] = [0,4], [1,2] = [0,0]\}[1,6] = \{[1,1] = [0,4], [1,2] = [0,0]\}\}$

8.3 Construction of ∇ tree

The subroutine *two_generated.m* calculates the subgroup $\langle v_1, v_2\rangle$ of $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. The subroutine *cocyclic_gen.m* calculates the cocyclic groups belonging to a fixed level $\Delta_m \setminus \Delta_{m-1}$. This subroutine is built up but not widely used.

8.4 Characters of homogeneous sets

In this subsection we introduce three subroutines: *characters.m*, *A.m* and *charactershomo.m*. The first one selects a level $\Delta_i \setminus \Delta_{i-1}$, the H^Δ corresponding to a co-cyclic group H and calculates $\chi_H[S]$ for each element $S \in \Delta_i \setminus \Delta_{i-1}$.

Example 8.4.1. We define $H^\Delta = \langle(1,0)\rangle$, $p = 3$,$m = 2$,$n = 3$. In other words, we are searching the characters of the members of the first level of Δ corresponding to $H = \langle(1,0)\rangle$. As we expect, the response is that $\chi = 2$ for only one member (the only one being subset of H) and $\chi = -1$ for the other three.

The subroutine $A.m$ calculates the coefficients $A_{l,m}$ of a given homogeneous set. The only difficulty is a little matter of indices: Matlab and Octave do not accept arrays with a position indexed by 0. In other words, $A(0)$ is a mistake, if A is an array. Therefore, $A_{l,m}$ is stored into the $l+1, m$ cell of a matrix.

Example 8.4.2. We ask the coefficients of $(1,1,0) - S^h$, with $p = 3$. The output is a matrix: $\begin{bmatrix} 1 & 5 & 5 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$.
The side i in the first row is $A_{0,i}$, the side i in the second row is $A_{1,i}$, the side i in the third row is $A_{2,i}$.

The subroutine *charactershomo.m* takes as input $A(a,p)$, δ (its value is 1 if $H^\Delta \in S^h$,0 otherwise), the level t and n, and calculates the characters of an homogeneous group according to the equation (5.1).

9 Conclusion

We examined, using the Schur's method, the classification of the strongly regular $\Gamma_G(S)$ Cayley graphs. The tree-structure of $S\Delta$ and the same corresponding arrangement ∇, the Hasse diagram of the co-cyclic groups forming the kernel of the characters $\in \mathrm{Irr}(G)$, led us to inquiry on the homogeneous S subsets of Δ. We found some very interesting results. We proved that, for each $H, \in \nabla_t \setminus \nabla_t - 1$, $t \geq 1$, the corresponding character $\chi_H[S]$ has only two possible values, say u and $v = p^n + u$, according to the fact if $H^\Delta \notin S$ or $H^\Delta \in S$. We proved that a Strongly regular Cayley graph could be a latin square type or a negative latin square type. We proved that, if S corresponds to an SRCG, then there exists a block set which is the symmetric difference of an homogeneous set S^h and the S set. We reported the proof that, if S is homogeneous, then it corresponds to a Strongly Regular Graph if and only if its defining array is of the form $(a_1, 0, \ldots, 0)$ or of the form $(a_1, p-1, \ldots, p-1)$. We went through the case $p = 2$, $n = 2$ and $p = 2$, $n = 3$ and we defined the classes of SRCG Γ_2 and Γ_3. We proved that if S correspond to an SRCG and the corresponding homogeneous set S^h $(S \div S^h = blockset)$corresponds to an SRCG as well, then or $S = S^h$, or $\Gamma_G(S) \in \Gamma_2$, or $\Gamma_G(S) \in \Gamma_3$. We examined the occurrence when S corresponds to a Paley graph and finally, collecting all the previous results, we came to the proof of the theorem 6.0.1 which classifies SRCG when p is odd. Then we led a numerical inquiry on the cases p is 2 and we reported some results obtained by [17] in those cases.

10 Povzetek naloge v slovenskem jeziku

To delo je *š*tudija krepkih regularnih Cayleyjevih grafov nad abelskah grupah $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. Dejansko je pokazalo v literaturi, da lahko dobimo krepko regularne grafe na grupah $\mathbb{Z}_{p^k} \oplus \mathbb{Z}_{p^h}$ in samo, *če* je $k = h$. atančneje, preučili smo Schurove kolobarje $W(G)$, katerih osnovne količine sestavljajo generatorji cikličnih podgrup grupe $G = \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$. To sta pred tem dokazala Bridges in Mena [3], [4] kot edinstven maksimum Schurovi kolobar nad G, nerazcepni karakteri od grupe G prevzamejo racionalne vrednosti na osnovnih količinah. Glavna orodja so *Hassejevi diagrami* cikličnih in kocikličnih podgrup od $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}$, ki se izkažejo za drevesa. Glede na abelovo grupo G je kociklična podgrupa opredeljena kot podgrupa H v G, tako da je G/H ciklična grupa. Drevo cikličnih podgrup je označeno s simbolom Δ, drevo kocikličnih grup pa s simbolom ∇. Razredi enakovrednosti so postavljeni med nezdružljiv, ki imajo isto jedro, in dokazujejo, da so jedra kociklične grupe. Prvi množični rezultat je natančna ocena znakov na vozliščih Δ. Za vsak element $F \in \Delta$ so te vrednosti karakterjev pozitivne, če je $F \subseteq H$, negativne, če $|F| = p|F \cap H|$ in 0 drugače.Ta rezultat je ključnega pomena za dokazovanje številnih drugih izrek in lem. Ključna lastnost, ki jo lahko ima podmnožica S v Δ, ki ne vsebuje trivialne podgrupe, ali ne, *homogenost.* Ta lastnost se nanaša velikost množice, ki izhaja iz presečišča med S in množico sinov generičnega elementa H, izbranega v ustrezno podgrupoo Δ. V glavnem izreku Y. I. Leifman in M. E. Muzychuk opisujeta vse podvrsti Δ, ki glede na homogenost ustrezajo krepko reularnim grafom, glej [14, Teorem 1.6]. Z Schurjevo metodo smo preučili klasifikacijo krepko regularnega grafa$\Gamma_G(S)$. Drevesna struktura $S \in \Delta$ in enaka ustrezna razporeditev cikličnih grup, ki tvorijo jedro karakterjev $\in \mathrm{Irr}(G)$, so nas privedle do poizvedovanja o homogenih podmnožicah S v Δ. Našli smo nekaj zelo zanimivih rezultatov. Videli smo, da ima za vsak $H, \in \nabla_t \setminus \nabla_{t-1}$, $t \geq 1$ ustrezen karakter $\chi_H[S]$ le dve možni vrednosti, recimo u in $v = p^n + u$, glede na dejstvo, da je $H^\Delta \notin S$ ali $H^\Delta \in S$. Dokazali smo, da je krepko regularen Cayleyjev graf lahko biti latinski kvadratni tip ali negativen latinski kvadratni tip. Dokazali smo, da če S ustreza SRCG, potem je S simetrična razlika homogene množiceS^h in blokovske množice. Poročali smo o dokazu, da če je S homogen, potem ustreza krepko regularnem grafu, če in samo, če je njegova definirajoča množica oblike $(a_1, 0, \ldots, 0)$ ali oblike $(a_1, p-1, \ldots, p-1)$. Šli smo skozi primer $p = 2$, $n = 2$ in $p = 2$, $n = 3$ in smo opredelili razrede SRCG Γ_2 in Γ_3. Dokazali smo, da če S ustrezata SRCG in ustrezna homogena množica S^h $(S \; divS^h = blok)$ ustrezata tudi SRCG, potem ali $S = S^h$, ali $\Gamma_G(S) \in \Gamma_2$ ali $\Gamma_G(S) \in \Gamma_3$. Pregledali smo pojav, ko S ustreza grafu Paleyja in na koncu zbrali vse prejšnje rezultate ter prišli do dokaza izrek 6.0.1, ki razvrsti SRCG, kadar je p odd. Nato smo vodili številčno poizvedovanje o primerih p je 2 in poročali smo o nekaterih rezultatih, ki jih je za iste primere pridobil [17].

11 References

[1] N.L. Biggs, A.T.White,Permutation Groups and Combinatorial Structures, Cambridge University Press, 1979 *(Not cited.)*

[2] R.C. Bose, Strongly regular graphs, partial geometries, and partially balanced designs, Pacific J. Math. 13 (1963) 389–419. *(Cited on page 3.)*

[3] W.G. Bridges, R.A. Mena, Rational circulants with rational spectra and cyclic strongly regular graphs, Ars Combin. 8 (1979) 143–161 *(Cited on pages 1, 11, and 48.)*

[4] W.G.Bridges,R.A.Mena,Rational G-matrices with rational eigenvalues,J.Combin.TheorySer.A32(1982) 264–280 *(Cited on pages 1 and 48.)*

[5] A.E. Brouwer,A.M. Cohen,A. Neumaier,Distance-regular graphs,Springer, Berlin, 1989 *(Not cited.)*

[6] J.A. Davis, Partial difference sets in p-groups, Arch. Math. 63 (1994) 103- *(Not cited.)*

[7] Delsarte, An algebraic approach to the association schemes of coding theory,Philips Res. Reports, (suppl.10)(1973)1-97 *(Not cited.)*

[8] I.A.Faradzev,A.A.Ivanov,M.H.Klin,Galois correspondence between permutation groups and cellular rings (association schemes), Graphs Combin. 6 (1992) 202–224. *(Not cited.)*

[9] G.D. Godsil Algebraic Combinatorics Chapman & Hall, 1993 *(Cited on pages 1 and 3.)*

[10] J.J.Golfand,A.A.Ivanov,M.H.Klin,Amorphic cellular rings,in:I.A.Faradzev ,A.A.Ivanov, M.H.Klin,A.J. Woldar(Eds.),Investigations in Algebraic Theory of Combinatorial Objects, Mathematics and Its Applications (Soviet Series), vol. 84, KluwerAcademic Publishers, Dordrecht, 1994, pp. 167–187. *(Not cited.)*

[11] W.H.Haemers,E.Spence,The pseudo-geometric graphs for generalized quadrangle of order(3,t),European J. Combin. 22 (6) (2001) 839–845 *(Not cited.)*

[12] G.James, M. Liebeck Representations and characters of Groups, second Edition, Cambridge University Press, 2001 *(Cited on page 9.)*

[13] R. Kochendorfer, Untersuchungen über eine Vermutung von W. Burnside, Schr. Math. Sem. Inst. Angew. Math. Univ. Berlin 3 (1937) 155–180 *(Not cited.)*

[14] Y. I. Leifman, M. E. Muzychuk Strongly regular Cayley graphs over the group $\mathbb{Z}_p^n \oplus \mathbb{Z}_p^n$, Discrete Mathematics, Elsevier 305(2005) 219-239 *(Cited on pages 1, 2, 11, and 48.)*

[15] K.H. Leung, S.L. Ma, Partial difference sets with Paley parameters, Bull. London Math. Soc. 27 (1995) 553–564 *(Cited on pages 11 and 37.)*

[16] S.L.Ma, On association schemes,Schur rings, strongly regular graphs and partial difference sets, ArsCombin. 27 (1989) 211–220. *(Not cited.)*

[17] M.Malandro, K.W. Smith Partial difference sets in $C_{2^n} \times C_{2^n}$ Discrete Mathematics, Elsevier 2019 *(Cited on pages 11, 40, 41, 47, and 49.)*

[18] J.J.Seidel,Strongly regular graphs,in:W.T.Tutte(Ed.),Recent Progress in Combinatorics,Academic Press, NewYork, 1969, pp. 185–197 *(Not cited.)*

[19] H.Wielandt, Finite Permutation Groups,Academic Press, NewYork, 1964. *(Not cited.)*

Appendices

Appendix A: Octave subroutines

In this section, we write attach the sheets of the Octave subroutines we have built. There are some subroutines (functions, in Matlab/Octave environment), which are internal to the environment and are called by the subroutines (functions) we built up. In particular:
ismember.m receives two arrays and checks if elements in the first array are in the second one. The result is a logical 1 or a logical 0. This function is very useful to build the adjacency matrices. *eig.m* is a function calculating the eigenvalues of a matrix. It is a very powerful and smart function, capable of a quick computation of large sized matrices. *rem.m* calculates the reminder of a division between integers. *factor.m* factorizes integers. *length.m* and *size.m* return the size of a vector or a matrix. *zeros.m*, *ones.m* and *eye.m* define the $\underline{\mathbf{0}}$,$\mathbf{J}$,$\mathbf{I}$ matrices.

```
function [G,A_matr,lambdas]=Cayley_Matrix(p,n,S)
  G=[0,0];
  for i=0:p^n-1
    for j=0:p^n-1
      if (norm([i,j])>=10^-5)
      G=[G;[i,j]];
      endif
    endfor
  endfor
  s=size(G);
  for c1=1:s(1)
    for c2=1:s(1)
      x1=G(c1,:);
      x2=[p^n,p^n]-G(c2,:);
      x=x1+x2;
      x(1)=rem(x(1),p^n);
      x(2)=rem(x(2),p^n);function [G,A_matr,lambdas]=Cayley_Matrix(p,n,S)
  G=[0,0];
  for i=0:p^n-1
    for j=0:p^n-1
      if (norm([i,j])>=10^-5)
      G=[G;[i,j]];
      endif
    endfor
  endfor
  s=size(G);
  for c1=1:s(1)
    for c2=1:s(1)
      x1=G(c1,:);
      x2=[p^n,p^n]-G(c2,:);
      x=x1+x2;
      x(1)=rem(x(1),p^n);
      x(2)=rem(x(2),p^n);
      A_matr(c1,c2)=ismember(x,S,"rows");
    endfor
  endfor
  A_matr=double(A_matr);
  lambdas=eig(A_matr);
endfunction

      A_matr(c1,c2)=ismember(x,S,"rows");
    endfor
  endfor
  A_matr=double(A_matr);
  lambdas=eig(A_matr);
endfunction
```

```
function subgroup =cyclic(generator, p,n)

  % this subroutine calculates the cyclic group generated by "generator"
  %in Zpn + Zpn
  % cfr. "Strongly regular Cayley graphs over the group Zpn + Zpn
 % by Ye?m I. Leifman, Mikhail E. Muzychuk -
 % Elzevier Discrete Mathematics 305 (2005) 219-239

  control = 0;
  s=generator;
  c1=1;
  subgroup{1}=generator;
  while control ==0
    c1=c1+1;
    s=generator+s;
    s(1)=rem(s(1),p^n);
    s(2)=rem(s(2),p^n);
    subgroup{c1}=s;
    if norm(s)<=10^-6
      control=1;
    endif
##    if c1>10000
##      control=1;
##    endif
  endwhile
endfunction

```

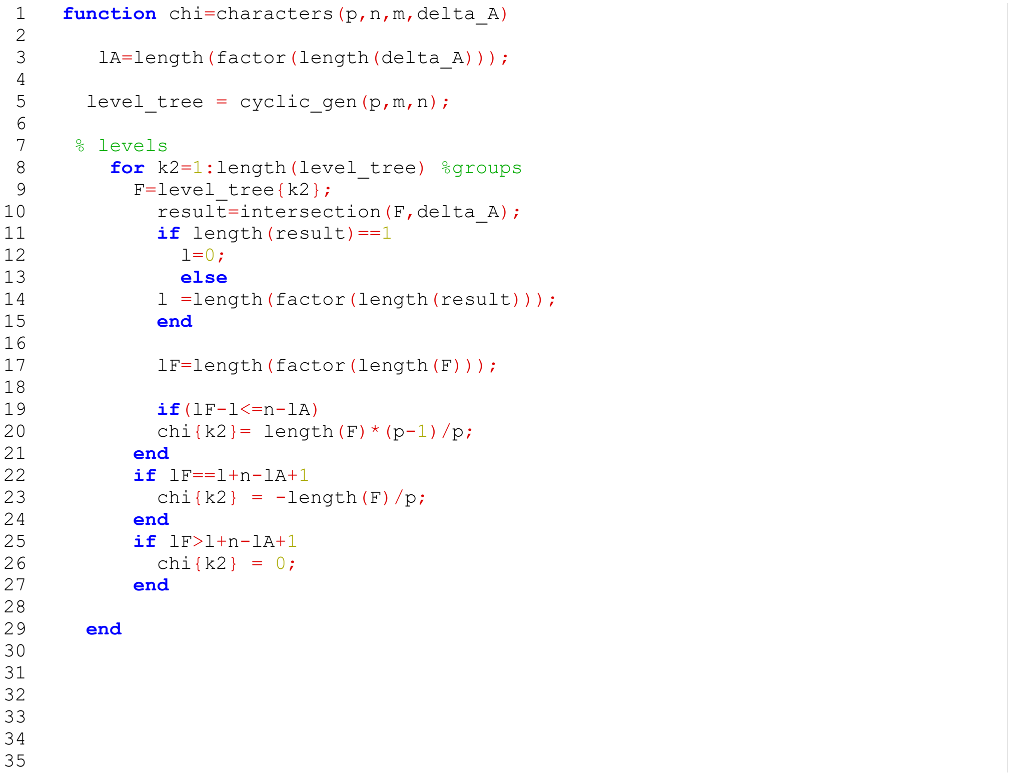
```
function level_tree = cyclic_gen(p,m,n)
  %this subroutine calculates the level "n-m" of the cyclic tree (delta)
  %if m =n then the output is {[0,0]}
  % cfr. "Strongly regular Cayley graphs over the group Zpn + Zpn
 % by Ye?m I. Leifman, Mikhail E. Muzychuk -
 % Elzevier Discrete Mathematics 305 (2005) 219-239


  if m<0
    'error'
    error
  end
  if m>n
    'error'
    error
  end



for c1=1:p^(n-m)
  generator=p^(m)*[1,c1-1];
  level_tree{c1}=cyclic(generator,p,n);
end

for c1=p^(n-m)+1:p^(n-m)+p^(n-m-1)
b=c1-p^(n-m)-1;
generator=p^m*[b*p,1];
level_tree{c1}=cyclic(generator,p,n);
end

if m==n
    level_tree={[0,0]};
  end

endfunction
```

```
function subgroup = two_generated(v1,v2,p,n)
 %This subroutine calculates the subgroup of Zpn +Zpn generated by
 % v1 and v2
 % cfr. "Strongly regular Cayley graphs over the group Zpn + Zpn
 % by Ye?m I. Leifman, Mikhail E. Muzychuk -
 % Elzevier Discrete Mathematics 305 (2005) 219-239
  s1=cyclic(v1,p,n);
  s2=cyclic(v2,p,n);
  l1=length(s1);
  l2=length(s2);
  c=0;
  for c1=1:l1
    for c2=1:l2
      c=c+1;
      s3=s1{c1}+s2{c2};
      s3(1)=rem(s3(1),p^n);
      s3(2)=rem(s3(2),p^n);
      subgroup{c}=s3;
    end
  end


endfunction

```

```
function level= cocyclic_gen(p,m,n)
 %this subroutine calculates the m-level of reverse-delta tree
%cocyclic groups in Zpn+Zpn
 % cfr. "Strongly regular Cayley graphs over the group Zpn + Zpn
 % by Ye?m I. Leifman, Mikhail E. Muzychuk -
 % Elzevier Discrete Mathematics 305 (2005) 219-239
  if m!=n
  v1=[p^m,0];
  v3=[0,p^m];
  for c1=1:p^m
    a=c1-1;
    v2=[1,a];
    level{c1}=two_generated(v2,v3,p,n);
  endfor
  for  c1=p^(m)+1:p^m + p^(m-1)
    b=c1-p^m-1;
    v4=[b*p,1];
    level{c1}=two_generated(v1,v4,p,n);
  endfor
end
%I split these two cases because otherwise members of the base were
%calculated twice
if m==n
  level=cyclic_gen(p,0,n);
endif
if n<m
  'error'
  error
endif
if m<0
  'error'
  error
endif
endfunction

```

```
function result = intersection(A,B)
  A1=[];
  B1=[];
  result={};
for i=1:length(A)
  K=A{i};
  A1=[A1;K];
end

  for i=1:length(B)
  B1=[B1;B{i}];
end
  result1=intersect(A1,B1, "rows");
  for i=1:length(result1(:,1))
    result{i}=result1(i,:);
  endfor
endfunction

```

```
function Father = blocks(p,m,n)
  level_tree = cyclic_gen(p,m,n);
  if m !=n-1
  level_parent=cyclic_gen(p,m+1,n);



  for i=1:length(level_parent)
    for j=1:length(level_tree)
      A=intersection(level_parent{i},level_tree{j});
      B=level_parent{i};
    if length(A)==length(B)
    Father{j}=level_parent{i};
    endif
    endfor
  endfor
end
if m==n-1
  Father={[0,0]};
endif
endfunction

```



```
function chi=characters(p,n,m,delta_A)

   lA=length(factor(length(delta_A)));

  level_tree = cyclic_gen(p,m,n);

 % levels
    for k2=1:length(level_tree) %groups
      F=level_tree{k2};
        result=intersection(F,delta_A);
        if length(result)==1
          l=0;
          else
        l =length(factor(length(result)));
        end

        lF=length(factor(length(F)));

        if(lF-l<=n-lA)
        chi{k2}= length(F)*(p-1)/p;
      end
      if lF==l+n-lA+1
        chi{k2} = -length(F)/p;
      end
      if lF>l+n-lA+1
        chi{k2} = 0;
      end

  end
```

```
function coeff = A(a,p)

 n=length(a);
 coeff=zeros(n,n);
 if length(factor(p))>1
   error
   end
 if a(1)<0||a(1)>p+1
   error
 endif
 for i=2:n
   if a(i)<0||a(i)>p-1
     error
   endif
 endfor
 coeff(1,1)=a(1);
 for j=2:n
   coeff(1,j)=a(1);
   for k=2:j
     coeff(1,j)=coeff(1,j)+a(k)*(p^(k-1)+p^(k-2));
     endfor
 endfor
 for i=2:n
   for j=i:n

    for k=i:j
      coeff(i,j)=coeff(i,j)+a(k)*p^(k-i);
     endfor

   endfor
 endfor
endfunction

```

```
function chi = charactershomo(p,n,delta,coeff,t)

  if t<n && t>=1
    sum_1=0;
    sum_2=0;
    for i=1:n-t
      sum_1=sum_1+coeff(1,i)*(p^i-p^(i-1));
    endfor
    for i=1:t-1
      sum_2=sum_2+(coeff(i+1,(n-t+i))-coeff(i+1,n+i-t+1))*p^(n-t+i);
    endfor
    chi=sum_1-coeff(1,n-t+1)*p^(n-t)+sum_2+(coeff(t+1,n)+delta)*p^n;
  endif
  if t==n
    sum_1=0;
    for i=1:n-1
      sum_1=sum_1+(coeff(i+1,i)-coeff(i+1,i+1))*p^(i);
    endfor
    chi=sum_1+delta*p^n-coeff(1,1);
  endif
  if t==0
    sum_1=0;
    for i=1:n
      sum_1=sum_1+coeff(1,i)*(p^i-p^(i-1));
    endfor
    chi=sum_1;
  endif

  if t<0||t>n
    error
  endif
endfunction
```