Universidade de Lisboa
Faculdade de Ciências
Departamento de Matemática

Low-dimensional Affine Synchronizing Groups

Ana Filipa Costa da Silva

Dissertação
Mestrado em Matemática

2012

Universidade de Lisboa
Faculdade de Ciências
Departamento de Matemática

Low-dimensional Affine Synchronizing Groups

Ana Filipa Costa da Silva

Dissertação
Mestrado em Matemática

Orientador: Doutor Csaba Schneider

2012

Abstract

The synchronization property emerged from finite state automata and transformation semigroup theory. Synchronizing permutation groups were introduced by Arnold and Steinberg to study the Černý Conjecture. In this thesis we study the synchronization property in affine permutation groups of low-dimensions. J.E. Pin proved that one-dimensional affine groups are synchronizing. Hence our main results concern affine groups in dimension 2.

We used the characterization given by Neumann of synchronization using graph theory, which relies on the study of the equality between the clique number and the chromatic number of certain graphs invariant under the actions of a group, called the suitability property. It turned out that some of such graphs for two-dimensional affine groups have an interesting geometry and are part of a widely studied class of graphs, the generalized Paley graphs.

Further, we used the properties of the theta-function defined by Lovász connected to eigenvalues of a graph to obtain a necessary condition for the suitability in edge-transitive and vertex-transitive graphs. In this thesis we stated a criterion to decide if a generalized Paley graph is suitable. Then we used the tools referred to above and we presented conditions for two-dimensional affine groups to be synchronizing.

Resumo

A propriedade de sincronização surgiu no contexto da teoria de autómatos e semigrupos de transformação. Arnold and Steinberg definiram os grupos de permutação sincronizantes com o objectivo de estudar a Conjectura de Černý por outra perspectiva. Nesta tese estudamos a propriedade de sincronização em grupos afins de pequenas dimensões. Dado que J.E. Pin provou que os grupos afins de dimensão 1 são sempre sincronizantes, os resultados principais desta tese aplicam-se a grupos afins bidimensionais.

Peter Neumann estudou os grupos sincronizantes usando teoria de grafos. Esta caracterização consiste no estudo de grafos invariantes sobre a acção de um grupo e em determinar se os seus números cromático e de clique coincidem. Descobrimos que alguns grafos invariantes sobre a acção de grupos afins bidimensionais tinham uma geometria simétrica e que faziam parte de uma classe amplamente estudada de grafos, conhecidos como grafos de Paley generalizados.

Como ferramenta extra, estudámos a função-teta, um número invariante num grafo, que foi definida por Lovász. Esta função possui uma caracterização que utiliza os valores próprios da matriz de adjacência do grafo e que nos permitiu concluir uma condição suficiente para a igualdade no número cromático e de clique em grafos cujo grupo de automorfismos é transitivo nas arestas e nos vértices.

Nesta tese estabelecemos um critério para a igualdade no número cromático e de clique nos grafos de Paley generalizados e usámos esse resultado, bem como as ferramentas anteriormente referidas, para obter uma caracterização dos grupos afins bidimensionais sincronizantes.

Acknowledgment

I would like to express my gratitude to everyone that in one way or the other was important for the elaboration of this dissertation. I apologize in advance for the names that I might have forgotten to mention.

First of all, I want to present my deepest thanks to my supervisor Doutor Csaba Schneider for all guidance and support during my Master's degree. Citing his Master's thesis,

"(. . .) the personality of the supervisor is of fundamental importance."

I could not agree more. His enthusiasm with the research work has been fundamental for my motivation during this year. His new ideas and suggestions for approaches to the problems increased my desire to further my knowledge of mathematics. I am also thankful for his realistic perspective of the work since he pushed me when it was necessary and he read carefully the awful preliminary versions of the dissertation. His guidance in the research, during courses and seminars and even his advices about giving classes, made me a much better mathematician. Thank you very much.

I express my sincere gratitude to João Araújo and Benjamin Steinberg for their help on the history of the synchronization property. I was very surprised by their willingness to answer my emails and explain to me the origin and motivation for the study of the synchronization property on group theory. Their contribution was fundamental to position synchronization across this area of Algebra.

I would like to thank my professors from the mathematics department of Faculdade de Ciências, in particular, professor Owen Brisson and professor Carlos André, for their availability for answering my doubts and questions on group and number theory. Some of our discussions were the key for some proofs in this dissertation. I also thank the support of the Center of Algebra of the University of Lisbon, which allowed me to attend to several seminars and workshops.

I also want to sincerely thank professors Gracinda Gomes and Maria João Gouveia. However, it is not just enough for me to thank them for being my teachers, since I am grateful to them for reasons beyond their academic position. They are the ones who probably listened to most of my existential problems while pursuing my Master's and who (always full of patience) wisely advised me. Their support and understanding were very important for me.

I would also like to show my gratitude to all the people that, in spite of their little understanding of the work of my dissertation, were an essential support for me, in particular for my mental and psychological health. First, I want to sincerely thank my mother and my grandparents for tolerating my ill-mannered behavior and lack of patience in the low days and for their infinite kindness and love.

I am happy to thank all my friends who have constantly been around, caring about my work, celebrating my small victories and trying to cheer me up when I was stuck with some problem. Thanks to Filipe, Marta, Raquel, Mariana and Joana, the cute group, as they call. Thanks to Catarina and Mafalda that, besides the jokes and parties for making me happy, taught me that at some point we have to face the issues we are dealing with. Thanks to Jeronimo for the interest in my work and also for encouraging me to have higher prospects for the future, regardless of my fears. Thanks to Joana, Marta, Catia, Beatriz and Tatah, the fancy girl's group, for all the sharing which was an important part of my emotional growth.

Finally, and trying to avoid a silly sentence, I deeply thank Ricardo for being present all the time.

Contents

Notation

$\bar{\partial}(\Gamma)$ Average degree of the vertices of the graph Γ

Ω^k k-th Cartesian power of Ω

$\mathsf{Sym}(\Omega)$ Symmetric group on a set Ω

D_n Dihedral group of order n

$[G : H]$ Set of right cosets of H in G

αG Orbit of α under G

$\alpha(\Gamma)$ Independence number of the graph Γ

$\mathsf{Alt}(n)$ Alternating group on the set $\{1, \ldots, n\}$

$\mathsf{Aut}(\Gamma)$ Automorphism group of the graph Γ

$\chi(\Gamma)$ Chromatic number of the graph Γ

$\mathbb{F}^*$ Mutiplicative group of the field $\mathbb{F}$

$\mathbb{F}_q$ Field with q elements

Γ' Complement graph of the graph Γ

$\Gamma(\alpha)$ Neighborhood of the element α on the graph Γ

Γ_Δ Undirected orbital graph associated with the undirected orbital Δ

$\Gamma_{q,m}$ Generalized Paley graph of the field $\mathbb{F}_q$ with index m

$\mathsf{GL}(n, p)$ General linear group of dimension n over $\mathbb{F}_p$

$\mathsf{GL}(V)$ Group of linear transformations of the vector space V

$\ker \psi$ Kernel of the action ψ

λ_1^Γ Largest eigenvalue of the graph Γ

λ_n^Γ Smallest eigenvalue of the graph Γ

$\mathsf{M}(n,p)$ Monomial group of $\mathsf{GL}(2,p)$

$\omega(\Gamma)$ Clique number of the graph Γ

$\Omega^{(k)}$ k-tuples of pairwise distinct points of Ω

$\Omega^{\{k\}}$ k-pairwise distinct subsets from Ω

$\partial_{\max}(\Gamma)$ Maximum degree of a vertex in the graph Γ

ρ_1 Right regular action

ρ_H Right coset action

$\mathsf{Sym}(n)$ Symmetric group on the set $\{1,\ldots,n\}$

φ Frobenius automorphism

$\vartheta(\Gamma)$ Theta-function of the graph Γ

A_Γ Adjacency matrix of the graph Γ

G_α Stabilizer of α under the elements of G

G_Δ Setwise stabilizer of Δ under G

$G_{(\Delta)}$ Pointwise stabilizer of Δ under G

Hg Right coset of H in G

K_n Complete graph with n vertices

$S_{q,m}$ Set of m-powers of the non-zero elements of $\mathbb{F}_q$

Z_{p^2} Singer cycle of the field $\mathbb{F}_{p^2}$

C_n Cyclic group of order n

List of Figures

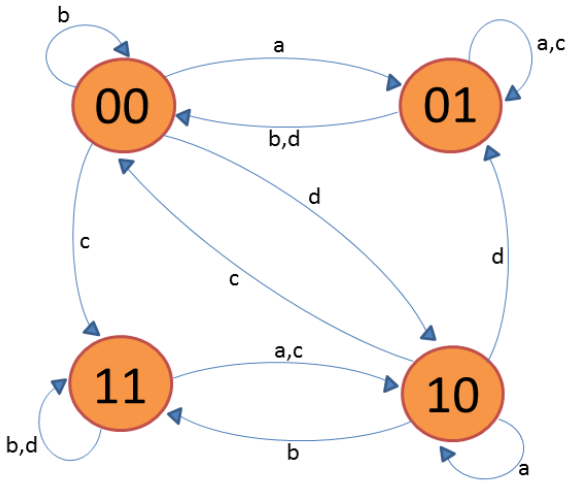
Chapter 1

Introduction

Synchronization is a concept which involves several areas of mathematics, such as automata theory, semigroup theory and group theory. This concept was implicitly present in some work of mathematicians in the beginning of the study of automata and semigroups. For instance in 1956 Ashby [Ash56] presented a puzzle involving two ghostly noises, Singing and Laughter, in a haunted mansion. Each of the noises can be either on or off and their behavior depends on combinations of two possible actions, playing the piano or burning the incense. The objective of the puzzle is to find a combination of the actions which puts the haunted mansion into silence. The mansion has 4 different states since there are 4 possible combinations of the ghostly noises. Further, combining the actions of playing the piano and burning the incense, we get 4 different combinations of the actions, which have different effects on the haunted mansion.

A mathematical model of the enigma is displayed in Figure 1.1. States of the mansion are encoded by the strings $00, 01, 10, 11$ and the combinations of the actions are encoded by the letters a, b, c, d. The string 00 encodes the complete silence; that is, when both noises are off. The string 01 represents the case when Laughter is on and Singing is off. The other two strings correspond to similar situations. Analogously, the letters encode the possible combinations of the actions. For instance the letter b stands for the action that the piano is played but the incense is not burned.

The challenge of this puzzle, which is related to the synchronization concept, is to find a combination of the actions of playing the piano and burning the incense which puts the haunted mansion into silence, no matter what ghostly noises are on. In Figure 1.1, the enigma is translated into the prob-



Action	Play the piano	Burn the Incense
a	No	No
b	Yes	No
c	No	Yes
d	Yes	Yes

Figure 1.1: The haunted mansion

lem of finding a sequence of letters that, when applied to every state of the diagram, takes it to state 00. At that time Ashby solved this problem under the assumption that both noises were on; that is, the haunted mansion was in state 11. He realized that if he applied the sequence *abc*, then the diagram switched from state 11 to state 00, where the haunted mansion was in silence. However, it is easy to check that the sequence *abc* always puts the haunted mansion in silence, no matter what ghostly noises are on. Thus the sequence *abc* solves our enigma.

This puzzle posed by Ashby illustrates the synchronization concept in a less mathematical context and shows also how it appeared in automata theory.

1.1 Synchronization and Automata and Semigroup Theory

Despite of the occurrence of synchronization in some mathematical problems, this property was only defined in 1964 by Černý in his paper [Čer64] about synchronizing automata.

A finite and deterministic automaton $\mathscr{A}$ is a triple (Q, A, δ), where Q is

a finite set of states and A is a finite set of symbols, called *letters*, which form the *alphabet* of the automaton. The third component is the *transition function* $\delta : Q \times A \to Q$, which applies the letters of the alphabet and switches the states of the automaton. A *word* in an automaton is a sequence of concatenated letters of its alphabet. The *length* of a word w is the number of concatenated letters used to form it and the *image* of w is the subset of states resulting from applying w to every state of the automaton. The size of the image of a word is called the *rank* of the word. Given a state x and a word w, the image of x under w is denoted by xw. Given an alphabet A, the set of words built from the letters of A is denoted by A^*.

A word in an automaton is called a *reset-word* if when applied to every state of the automaton it results in the same state. In other words, the rank of a reset-word is one. An automaton is said to be *synchronizing* if it has a reset-word. The example of the haunted mansion describes a synchronizing automaton with a reset-word abc. However, let us consider a simpler example.

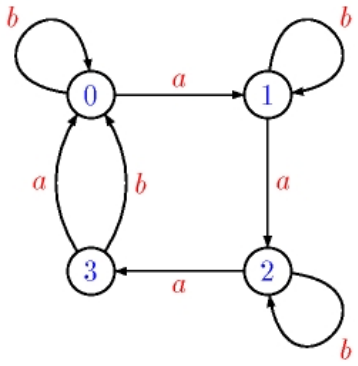


Figure 1.2: A synchronizing automata

In Figure 1.2, we consider the automaton $\mathscr{A} = (Q, A, \delta)$, where we have that $Q = \{0, 1, 2, 3\}$, $A = \{a, b\}$ and the transition function acts on the states as in the diagram. It is easy to verify that the word ba^3ba^3b is a reset-word for $\mathscr{A}$, since it switches every state of Q to the state 0.

Characterizing synchronizing automata and estimating the length of their reset-words has been a challenge in automata theory. In 1964, Černý [Čer64] conjectured that every synchronizing automaton with n states has a reset-word with length smaller or equal to $(n-1)^2$. This conjecture remains open after almost 50 years.

Several approaches to the Černý Conjecture were made in the last decades. In particular, for circular automata, this conjecture was solved. An automaton $\mathscr{A} = (Q, A, \delta)$, where Q has n states, is said to be *circular* if there exists a word $w \in A^*$ such that $\{x_0 w^i : 1 \leq i \leq n\} = Q$, for all $x_0 \in Q$. This means that the word w acts as a permutation of the states of Q. In 1978, J. E. Pin [Pin78] proved the Černý Conjecture for circular automata with a prime number of states and about 20 years later, L. Dubuc generalized the result for every circular automata [Dub98].

The set of transitions of a finite state deterministic automaton is a semigroup under the operation of concatenation, called the *transition semigroup*. In this terminology, an automaton is synchronizing if its transition semigroup contains a constant map. The Černý Conjecture is equivalent to the assertion that in the transition semigroup of a synchronizing automaton a constant map can be written as a word of length at most $(n-1)^2$. Therefore the study of the synchronization property can be approached from semigroup theory.

1.2 Synchronization and Permutation Groups

In the middle of the last decade, João Araújo and Benjamin Steinberg, mathematicians interested in the study of group theory and semigroup theory, suggested that the synchronization property could be studied in the context of permutation groups. This observation gave rise to the study of synchronizing permutation groups, a new field within permutation group theory.

The study of permutation groups arose from polynomial equations in the end of 18th century. The problem of finding the solutions of such equations was the motivation for the study of these groups by mathematicians such as Lagrange, Ruffini or Galois. In 1854, Arthur Cayley, a British mathematician, proved that every group is isomorphic to a permutation group. This result is known as Cayley's Theorem [Cay54] and shows the importance of permutation groups within group theory.

One of the mathematicians who suggested the study of the synchronization property was Benjamin Steinberg. His motivation for this approach stems from a paper by Y. Zalcstein [Zal71] about the representation theory of semigroups. In this paper of 1971, Zalcstein attributes a result to John Rhodes which states that a 2-transitive group is synchronizing, though

Rhodes did not use this name in 1966, since it was not yet defined. Steinberg thought that the study of synchronizing groups, as such groups form a class between 2-transitive and primitive groups, could be a step towards attacking the Černý Conjecture. Besides, Steinberg realized that he could generalize Rhodes' and Pin's results.

At the same time, another mathematician, namely João Araújo got interested in the study of groups with the synchronization property. In [LM94] Levi and McFadden proved that $\langle a, \mathsf{Sym}(n)\rangle \setminus \mathsf{Sym}(n)$ is idempotent generated and regular. Later Levi in [Lev96] proved that the same result holds for the semigroup $\langle a, \mathsf{Alt}(n)\rangle \setminus \mathsf{Alt}(n)$. These papers were the most important references in João Araújo's PhD thesis, and at a certain point they prompted him to try to classify the groups $G \leq \mathsf{Sym}(n)$ that satisfy the property
"for all $a \in T(n) \setminus \mathsf{Sym}(n)$ we have that $\langle a, G\rangle \setminus G$ is idempotent generated";

or (1.1)

"for all $a \in T(n) \setminus \mathsf{Sym}(n)$ we have that $\langle a, G\rangle \setminus G$ is regular".

When James Mitchell told Araújo in September of 2003 that he was about to leave for the US to work with Levi, Araújo stated the problems above and claimed that he had a classification of the groups that satisfy these properties. In addition he expressed his belief that classifying the groups that together with any singular map generate a semigroup with given properties would be the most important topic in the near future of semigroup theory.

While João Araújo was deeply involved in this line of research, The Center of Algebra of The University of Lisbon organized a workshop in November 2002 where M. Volkov introduced synchronizing automata and Eppstein's results on them [Epp90]. This talk led João Araújo to think about the classification of groups that together with any singular map generate a constant map.

Let G be a permutation group acting on a set Ω and let $\mathscr{P}$ be a partition of Ω into a disjoint union of non-empty subsets. We define a *section* of $\mathscr{P}$ as a subset S of Ω which contains precisely one element from each part of $\mathscr{P}$. If, given a partition $\mathscr{P}$, there exists a section S such that

$$Sg \text{ is a section of } \mathscr{P}, \text{ for every } g \in G, \tag{1.2}$$

then $\mathscr{P}$ is called a *G-regular* partition or a *section-regular* partition. João Araújo defined $G \leq \mathsf{Sym}(\Omega)$ to be a *synchronizing permutation group* if G is

a non-trivial group and it does not admit G-regular partitions beyond the trivial ones $\{\Omega\}$ and $\{\{\alpha\} : \alpha \in \Omega\}$.

However, unlike the classification referred to in Equation (1.1), this one totally defeated Araújo. He was convinced that this problem was much more difficult than the others based on McFadden's and Levi's work, and hence the idea was left dormant.

The ICALP 2005 (International Colloquium on Automata, Languages and Programming) Conference held in Lisbon in July of 2005 had a satellite workshop on Semigroups and Automata organized by Vitor Fernandes, Gracinda Gomes, Jean-Eric Pin, and Mikhail Volkov. There Steinberg presented a talk based on his joint work with one of his Master's students, Fredrick Arnold, in which he stated his definition of synchronizing groups. He called a group synchronizing if the semigroup generated by the group and by any non-invertible transformation contained a constant map. It is not hard to show that Steinberg's definition of synchronizing groups is equivalent to Araújo's definition given above. In the talk he proved that synchronizing groups were primitive and asked if the converse was true. Araújo did not attend workshop, for he was on that day taking Laci Márki, who participated in another meeting held in Lisbon, to a trip on a sailboat showing him the river Tejo. The extended abstract of Steinberg's talk focused on representation theory proving that QI-groups (groups whose deleted modules are irreducible over the rationals) were synchronizing without actually stating the definition of synchronizing groups. Hence the two protagonists of our story did not realize at that time how closely their works were related. The results of Arnold and Steinberg were published in [AS06].

In 2006 Araújo went to the Fountainsfest, a conference in honour of his supervisor John Fountain, and there he presented the classification discussed in Equation (1.1). Benjamin Steinberg was in the first row and in the end he asked Araújo if he could classify the groups that together with any map generate a constant. Araújo said "I already thought about that, but it is a very difficult problem". He recalled later (totally unaware of the paper by Arnold and Steinberg[AS06]) that he thought that that idea had just occurred to Steinberg during the talk. Nevertheless, if Steinberg found the idea worth a question, maybe the problem was worth a new look.

By accident, in the night of the conference's banquet Araújo sat next to S. Donkin. As soon as Donkin introduced himself, Araújo commented: "that is funny because I have a number of problems in group theory that I would like to discuss with a group theorist". "Try me" was Donkin's simple reply.

Araújo picked the toughest of the questions: "I need the classification of the primitive permutation groups that admit a partition and a section, such that every element in the orbit of the section, is a section for the original partition". Donkin said: "This seems a very interesting question. Write to Peter Neumann in Oxford. I am sure he is going to be interested".

After returning to Lisbon, Araújo wrote to Neumann who replied in less than two hours showing indeed strong interest in the problem and asking for more information on its origins. Then Neumann made some impressive progress very quickly, and gave some talks on the topic to group theorists, attracting the attention of Peter Cameron, Jan Saxl, Cheryl Preager, John Bamberg, Csaba Schneider, and many other. The solutions for the problems in Equation (1.1) were finally published in [AMS11].

Although being formally different, the definitions of synchronizing groups given by Steinberg and Araújo are equivalent. This equivalence is proved in [Neu09, Appendix]. We note that in this dissertation we will use the definition suggested by João Araújo.

As noted before, Fredrick Arnold and Benjamin Steiberg proved in [AS06] that synchronizing groups are primitive. Then they combined this result with Pin's [Pin78, Théorème 2] and concluded that a permutation group with prime degree has the synchronization property if and only if it is primitive. The main result of [AS06] states that QI-groups (that is, groups whose deleted modules are irreducible over $\mathbb{Q}$) are synchronizing.

Peter Cameron defined basic groups, as the ones that do not preserve a power structure of the underlying set [Cam99, Section 4.3]. Peter Neumann in [Neu09, Example 3.4] constructs a section-regular partition from a power structure to prove that a certain group is non-synchronizing. Cameron generalized this example and prove that non-basic groups are not synchronizing.

Neumann proved that a section-regular partition for a transitive group is uniform [Neu09, Theorem 2.1]; that is, all the parts have the same size. Further, he showed that a non-trivial section-regular partition for a primitive group has at least 2 parts and that every part has at least 2 elements. It follows from this last result that a primitive group of degree double of a prime is synchronizing. In [Neu09] Peter Neumann presented a series of examples of primitive non-synchronizing groups. In the he gave a graph theoretic characterization of synchronizing groups. This characterization, which is one of the main tools of this dissertation, has been widely used to verify that certain groups are synchronizing.

Araújo, Bentz and Cameron in a recent paper [ABC12] investigated the

conjecture that a primitive group and an arbitrary transformation with non-uniform kernel generate a constant map. They verify this conjecture in some special cases.

1.3 Main Results

The focus of this dissertation is the study of the synchronization property in low-dimensional affine groups. The result of J. E. Pin, namely Théorème 2 of [Pin78], implies that 1-dimensional affine groups are always synchronizing. Hence the next step in this direction is to study 2-dimensional affine groups.

These groups are semidirect products of the group of translations by the elements of a 2-dimensional vector space over a prime field $\mathbb{F}_p$ and a subgroup of $\mathsf{GL}(2,p)$ (see the definition of these groups on Section 6.1). The main results of this dissertation are the following.

Theorem 1. *Suppose that H is an irreducible subgroup of $\mathsf{GL}(2,p)$, let T denote the group of translations of the vector space $V = (\mathbb{F}_p)^2$ and let $G = T \rtimes H$ be the corresponding subgroup of $\mathsf{Sym}(V)$.*

(1) If H is an imprimitive linear group then G is non-synchronizing.

(2) Suppose that H is primitive.

- *(2.1) If $\mathsf{SL}(2,p) \leq H$ then G is 2-transitive and hence synchronizing.*
- *(2.2) Suppose that H is either isomorphic to a cyclic group C_r or to a group of the from $C_r \rtimes C_2$. Set $m = (p^2-1)/r$. Then the following hold.*
  - *(a) If $m = 1$ then G is 2-transitive and hence synchronizing.*
  - *(b) If $m > 1$ and $m \mid p+1$ then G is non-synchronizing.*
  - *(c) If $m = 3$ then G is non-synchronizing if and only if $3 \mid p+1$.*
- *(2.3) Suppose that H contains a cyclic normal subgroup C_r of index 2 but H is not a semidirect product $C_r \rtimes C_2$. Set $m = (p^2-1)/r$. Then the following are valid.*
  - *(a) If $m = 2$ then G is 2-homogeneous and hence synchronizing.*
  - *(b) If $m > 2$ and $m \mid p+1$ then G is non-synchronizing.*

(c) *Set* $i \in \mathbb{N}$ *such that* $2^i \mid \gcd(r, p-1)$ *but* $2^{i+1} \nmid \gcd(r, p-1)$. *Suppose that* $(p-1)/2^i \equiv m/2 \pmod{m}$. *If* $m > 2$ *and* $(m/2) \mid p+1$ *then* G *is non-synchronizing.*

Theorem 1 can be found in this thesis as Theorem 6.5.1 and we remark that in Chapter 6 we prove a stronger statement than Statement (2.2). In the proof of this theorem we mostly use the characterization by Peter Neumann [Neu09] of the synchronization property using graph theory. This characterization is discussed in Section 4.2 and relies on the study of clique and chromatic numbers of certain graphs associated with the group actions. In particular we are interested in such graphs whose clique number and chromatic number coincide.

It turns out that some graphs associated with the affine groups described in Statements (2.2) and (2.3) of Theorem 1 are isomorphic to graphs built from finite fields and known as generalized Paley graphs (see Chapter 5). We denote by $\Gamma_{p^2,m}$ the generalized Paley graph of the field with p^2 elements with index m (see Section 5.2). Using Neumann's characterization, we are interested in determining when a generalized Paley graph has the same clique number and chromatic number. The next theorem gives a solution to this problem.

Theorem 2. *In a generalized Paley graph* $\Gamma_{p^2,m}$, *the clique number and the chromatic number coincide if and only if* $m \mid p+1$.

This theorem is stated as Theorem 5.3.2 in the dissertation. If $m \mid p+1$ then we can find a nice clique and coloring for such generalized Paley graphs (see Proposition 5.3.3). However, in the case when $m \nmid p+1$, the situation is harder and we follow a different approach to this problem. We use spectral graph theory; that is, the theory of eigenvalues of graphs, in order to bound the clique number and the chromatic number of a graph. One bound thus obtained is the Lovász theta-function defined by László Lovász [Lov79] (see Section 4.4). This function is the key for the proof of the next theorem, which gives us a necessary condition for the equality of the clique and chromatic numbers for an edge-transitive and vertex-transitive graph. In particular, the case $m \nmid p+1$ in Theorem 2 is proved using Theorem 3.

Theorem 3. *Suppose that* Γ *is a vertex-transitive and edge-transitive graph whose clique number is equal to the chromatic number. Assume that this number is* k. *Then* $k-1$ *divides the degree* $\bar{\partial}(\Gamma)$ *of* Γ. *Suppose further that* λ *is the smallest eigenvalue of* Γ. *Then* $\lambda = -\bar{\partial}(\Gamma)/(k-1)$.

Theorem 3 can be found as Theorem 4.4.3 in this dissertation.

1.4 Methodology

The main results of this dissertation are proved unsing techniques of permutation group theory and graph theory. In Chapter 2 we start with a review of the basic concepts of permutation group theory. The subsequent chapters consider different aspects of the synchronization property.

It is known that a synchronizing group must belong to one of just three classes of the O'Nan-Scott Theorem. An interesting O'Nan-Scott class of groups, since this class contains both synchronizing and non-synchronizing groups, is formed by affine groups. Hence the objective of this dissertation is to better understand when an affine group is synchronizing. As explained before Theorem 1, our main results concern primitive affine groups in dimension 2. Such a group is built from a 2-dimensional vector space over $\mathbb{F}_p$, where p is a prime, and an irreducible subgroup of $\mathsf{GL}(2,p)$ (See Sections 6.1 and 6.2).

Therefore to study such affine groups we use a characterization of irreducible subgroups of $\mathsf{GL}(2,p)$ given in Flannery and O'Brien [FO05]. Some of these irreducible subgroups are monomial and their structures are described in Short [Sho92]. The different classes of irreducible subgroups of $\mathsf{GL}(2,p)$ are described in Theorem 6.3.4. This way we will classify primitive affine permutation groups in dimension 2 into different classes according to their irreducible matrix group components, as done in Theorem 1, in order to obtain results about the synchronization property.

For the proof of Statement (1) of Theorem 1, we use the concept of Cartesian decompositions, defined in [PBS03]. These structures are very useful for our goal, since we rephrase the result by Peter Cameron which states that a non-basic group is non-synchronizing in terms of Cartesian decompositions. Hence we prove that a group which preserves a Cartesian decomposition is non-synchronizing (see Theorem 3.2.2). Furthermore, the affine groups whose matrix group components are imprimitive preserve Cartesian decompositions (see Theorem 6.2.4) and hence we obtain that such affine groups are not synchronizing. For more details on Cartesian decompositions we refer to Section 3.2, while imprimitive matrix groups are defined in Section 6.2.

In the proof that some of the groups described in Theorem 1 are synchronizing, we use the fact that 2-homogeneous and 2-transitive groups are

synchronizing (see Theorem 3.1.1). These properties are discussed in Section 2.3.

For proving the remaining statements of Theorem 1, which is the most complex part, we used the characterization of synchronization given by Peter Neumann using graph theory [Neu09]. Neumann proved that a group acting on a set Ω is non-synchronizing if and only if there exists a graph with vertex-set Ω and G-invariant edge-set whose clique number is equal to the chromatic number (see Theorem 4.2.4). In this case we call this graph suitable. Therefore, using this characterization, the problem of verifying if a group is synchronizing is reduced to analyzing the clique and chromatic numbers of such graphs and checking if these numbers coincide.

It turns out that certain graphs for some affine permutation groups are isomorphic to generalized Paley graphs. These graphs are natural generalizations of Paley graphs defined by Paley in 1933 [Pal33] and we investigate them in Chapter 5. Therefore we are interested in determining conditions for generalized Paley graphs to be suitable. We reach a conclusion for these graphs over fields with p^2 elements, where p is a prime, as stated in Theorem 2. In the case when $m \mid p+1$, the assertion of Theorem 2 follows from [BDR88], a paper which obtains bounds for the clique and chromatic numbers of generalized Paley graphs of finite fields.

Finding the clique number and the chromatic number of a general graph is an NP-hard problem. Therefore mathematicians interested in this subject try to establish bounds for these numbers. One of these bounds was found by László Lovász in 1979 [Lov79] and is called the theta-function. We discuss this bound for the clique number and the chromatic number in Section 4.4. The theta-function of an edge-transitive and vertex-transitive graph can be determined by the eigenvalues of its adjacency matrix (see Statement 4 of Proposition 4.4.2). This result implies Theorem 3 and, in turn, the case when $m \nmid p+1$ in Theorem 2 was obtained using Theorem 3.

Thus, from the characterization of suitable generalized Paley graphs of Theorem 2, we obtain conclusions about the synchronization property in the remaining 2-dimensional affine groups described in Theorem 1.

Unfortunately, a class of primitive irreducible subgroups of $\mathsf{GL}(2,p)$ is not studied in this dissertation, namely the subgroups described in Proposition 4.4 of [FO05] which have central quotients isomorphic either to $\mathsf{Sym}(4)$, $\mathsf{Alt}(4)$ or to $\mathsf{Alt}(5)$. We were not able to apply the techniques discussed in this dissertation to this class of groups.

Chapter 2

Permutation Groups

In this thesis we are interested in the synchronization property in affine permutation groups. In this chapter we give the elementary and necessary background on finite permutation groups. We start with the definition of a permutation group, orbits and stabilizers. Then we define a transitive and a multiple transitive permutation group and discuss the concept of primitivity. The permutation group theory discussed in this chapter can be found in the first chapters of [DM96] and [Cam99].

2.1 Basic Concepts

The *symmetric group* on a set Ω, denoted by $\mathsf{Sym}(\Omega)$, is the set of all permutations of Ω under the operation of composition. A *permutation group* is a subgroup of $\mathsf{Sym}(\Omega)$. We define the *degree* of a permutation group as the cardinality of the set Ω. The image of $\alpha \in \Omega$ under a permutation $\pi \in \mathsf{Sym}(\Omega)$ is written as $\alpha\pi$. If $\Omega = \{1, \ldots, n\}$ then we write $\mathsf{Sym}(n)$ for $\mathsf{Sym}(\Omega)$.

Any permutation can be written as a product of *transpositions*, which are cycles of length 2. The number of transpositions that are in such a product can be odd or even and the parity of this number does not depend on the particular decomposition. We call a permutation *odd* if it can be written as an odd number of transpositions and in a similar way we define *even permutations*. The identity permutation is an even permutation. The *alternating group*, denoted by $\mathsf{Alt}(n)$, is the group of all even permutations of the set $\{1, \ldots, n\}$ and it is a normal subgroup of $\mathsf{Sym}(n)$.

An *action* of a group G on a set Ω is a homomorphism ψ from G to

$\mathsf{Sym}(\Omega)$. For $\alpha \in \Omega$ and $g \in G$, the point $\alpha\psi(g)$ is usually denoted by αg. Let us consider the *kernel*

$$\ker \psi = \{g \in G : \alpha g = \alpha \text{ for all } \alpha \in \Omega\}$$

of the homomorphism ψ. The kernel is a normal subgroup of G. If ψ is injective, then $\ker \psi = 1$, and we say that the action is *faithful*.

Suppose that G and H are permutation groups acting on the sets Ω and Δ, respectively. We say that G and H are *permutationally isomorphic* if there exists a bijection $\psi : \Omega \to \Delta$ and an isomorphism $\phi : G \to H$ such that $(\alpha g)\psi = (\alpha\psi)(g\phi)$ for all $\alpha \in \Omega$ and $g \in G$. The pair (ψ,ϕ) is called a *permutational isomorphism*. In other words, permutationally isomorphic groups only differ in the labeling of their elements and in the labeling of the elements of the sets they act upon.

If G is a group and H is a subgroup of G, then for an element $g \in G$, the set

$$Hg = \{hg : h \in H\}$$

is called a *right coset* of H in G. The set of right cosets of H in G is denoted by $[G : H]$. A *left coset* is defined in an analogous way. All the left and right cosets have the same cardinality, that is equal to the cardinality of H, which is itself a coset considering $g = 1$. Furthermore, the number of left cosets is equal to the number of right cosets and this number is known as the *index* of H in G and is denoted by $|G : H|$. By Lagrange's Theorem, we have that $|G| = |G : H||H|$.

Let us define an action on cosets. If G is a group and H is a subgroup of G then we can define the *right coset action*, denoted by ρ_H, of G on the set of right cosets $[G : H]$ by right multiplication as follows. If $g \in G$ and $Hg' \in [G : H]$ then $(Hg')(g\rho_H) = Hg'g$. The action ρ_1 of G on itself is called the *right regular action* of G. In a similar way we can define an action of G on the set of left cosets.

2.2 Orbits and Stabilizers

When a group G acts on a set Ω, a typical point α of Ω is moved by the elements of G to other points. The set of these images is called the *orbit* of α under G, or the G-orbit of α, and we denote it by αG. Hence

$$\alpha G := \{\alpha g : g \in G\}.$$

A *partition* of a set Ω is a set $\{P_1, \ldots, P_k\}$ of subsets of Ω such that

1. $\bigcup_{i=1}^{k} P_i = \Omega$;
2. $P_i \cap P_j = \emptyset$ if $i \neq j$.

The following lemma is well-known and it is a consequence of the definition of a G-orbit.

Lemma 2.2.1 (Theorem 1.4A of [DM96])**.** *Suppose that G is a group acting on a set Ω. Then the G-orbits form a partition of Ω.*

By Lemma 2.2.1, the orbits of a group can be considered as equivalence classes as follows. Let G be a group acting on a set Ω and define a relation $\sim$ on Ω:

$$\alpha \sim \beta \text{ if and only if there exists } g \in G \text{ such that } \alpha g = \beta. \tag{2.1}$$

This is an equivalence relation and the equivalence classes are the orbits of G.

A group G is said to be *transitive* on Ω if it has only one orbit, that is $\alpha G = \Omega$ for all $\alpha \in \Omega$. In other words, we say that G is transitive if for every pair of points α and β belonging to Ω there exists $g \in G$ such that $\alpha g = \beta$. In the terminology of the equivalence relation $\sim$ in Equation (2.1), the group G is transitive if and only if there is just one equivalence class.

Let us now consider the elements of G that fix the point $\alpha \in \Omega$ under their action on the set Ω. These elements form the *stabilizer* G_α of α:

$$G_\alpha = \{g \in G : \alpha g = \alpha\}.$$

The stabilizer of a point is always a subgroup of the original group G and if $\alpha, \beta \in \Omega$ with $\beta = \alpha g$ for some $g \in G$, then $G_\beta = (G_\alpha)^g$.

The definition of a stabilizer can also be extended to subsets of the underlying set Ω. Furthermore, we can define such stabilizers setwise or pointwise. Let G be a group acting on a set Ω and let Δ be a subset of Ω. Then the *setwise stabilizer* of Δ is the set

$$G_\Delta = \{g \in G : \delta g \in \Delta \text{ for all } \delta \in \Delta\},$$

while the *pointwise stabilizer* of Δ is defined as

$$G_{(\Delta)} = \{g \in G : \delta g = \delta \text{ for all } \delta \in \Delta\}.$$

A permutation group G is called *semiregular* if $G_\alpha = 1$ for all $\alpha \in \Omega$ and it is *regular* if it is transitive and semiregular.

Proposition 2.2.2. *A transitive abelian permutation group is regular.*

Proof. Let G be a transitive abelian permutation group acting on a set Ω and let $\alpha \in \Omega$. Let us consider the stabilizer G_α. Let $\beta \in \Omega$. Since G is transitive, there exists an element $g \in G$ such that $\beta = \alpha g$. Therefore, by a remark above, we have that $G_\beta = (G_\alpha)^g$. As G is abelian, each of its subgroups is a normal subgroup. Hence we obtain that $(G_\alpha)^g = G_\alpha$, for all $g \in G$. This means that $G_\beta = (G_\alpha)^g = G_\alpha$ and as β was taken arbitrarily, we obtain that G_α stabilizes all points of Ω. Since G is a permutation group, this implies that $G_\alpha = 1$. Hence we conclude that G is semiregular and as G is transitive by assumption, we obtain that G is a regular group. □

The following theorem links the stabilizers and the orbits of a transitive permutation group.

Theorem 2.2.3 (Corollary 1.4A of [DM96])**.** *Suppose that G is transitive in its action on a set Ω. Then the following hold.*

1. *The stabilizers G_α, for $\alpha \in \Omega$, form a single conjugacy class of subgroups of G.*
2. *The G-action on Ω is equivalent to the right coset action ρ_{G_α} for each $\alpha \in \Omega$. In particular, $|G : G_\alpha| = |\Omega|$ for each $\alpha \in \Omega$.*
3. *The action of G is regular if and only if $|G| = |\Omega|$.*

Proof. Let us prove the first statement. Since the group G is transitive, for all $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $\alpha g = \beta$. Hence we have, by an observation above, that $(G_\alpha)^g = G_\beta$ which means that all stabilizers are conjugate. Thus the stabilizers form a conjugacy class.

For the proof of the Statement 2, fix $\alpha \in \Omega$ and consider the stabilizer G_α. Let us define a map $\psi : \Omega \to [G : G_\alpha]$ as follows. For all $\omega \in \Omega$, set $\omega\psi = G_\alpha g$, where $g \in G$ is an element such that $\alpha g = \omega$. Such an element exists as G is a transitive group. Let us first show that ψ is a well defined map from Ω to $[G : G_\alpha]$. If $g_1, g_2 \in G$ such that $\alpha g_1 = \alpha g_2$ then $g_1 g_2^{-1} \in G_\alpha$ which means that $G_\alpha g_1 = G_\alpha g_2$. Thus ψ is well defined. Now we prove that it is injective. Let $\omega_1, \omega_2 \in \Omega$ such that $\omega_1\psi = \omega_2\psi$. Let $g_1, g_2 \in G$, such that $\alpha g_1 = \omega_1$ and $\alpha g_2 = \omega_2$. Then $G_\alpha g_1 = G_\alpha g_2$. Hence $g_1 g_2^{-1} \in G_\alpha$ and we have that

$\omega_1 = \alpha g_1 = \alpha g_1 g_2^{-1} g_2 = \alpha g_2 = \omega_2$. Thus ψ is injective. From the definition of ψ, it follows that it is surjective. Hence ψ is a bijection, which gives that $|G : G_\alpha| = |\Omega|$. Next we prove that (ψ, id) is a permutational isomorphism from the G-action on Ω to the G-action on $[G : G_\alpha]$. Let $\omega \in \Omega$ and $g \in G$. Then $(\omega\psi)g = (G_\alpha h)g$ where $h \in G$ is an element such that $\alpha h = \omega$. Now $(G_\alpha h)g = G_\alpha(hg) = (\omega g)\psi$ since from $\alpha h = \omega$ it follows that $\alpha hg = \omega g$. Thus (ψ, id) is a permutational isomorphism as claimed and the actions of G on these two sets are equivalent.

Let us now prove the third statement. By Lagrange's Theorem, given any subgroup H of G, we have that $|G| = |G : H||H|$. In particular, the equality $|G| = |G : G_\alpha||G_\alpha|$ holds for any $\alpha \in \Omega$. Hence the condition $|G| = |\Omega|$ is equivalent to $|\Omega| = |G : G_\alpha||G_\alpha|$. From Statement 2 we know that $|G : G_\alpha| = |\Omega|$, for all $\alpha \in \Omega$. Therefore $|G| = |\Omega|$ if and only if $|\Omega| = |\Omega||G_\alpha|$, which means that $|G_\alpha| = 1$ for all $\alpha \in \Omega$. Thus, as G is transitive, we conclude that $|G| = |\Omega|$ is equivalent to G being regular. □

2.3 Multiple Transitivity

Suppose that G is a permutation group acting on a set Ω. The group G is called *k-homogeneous* if G is transitive on the set

$$\Omega^{\{k\}} = \{\{\alpha_1, \ldots, \alpha_k\} : \alpha_i \in \Omega, \text{ and } \alpha_i \neq \alpha_j \text{ if } i \neq j\}.$$

Let G be a group acting on a set Ω and denote by Ω^k the k-th Cartesian power of Ω. The subset $\Omega^{(k)}$ of Ω^k consisting of k-tuples of pairwise distinct ordered points is clearly G-invariant for every k. A group G is said to be *k-transitive* if G is transitive on $\Omega^{(k)}$. Note that if G is k-transitive for some $k \in \mathbb{N}$ then G is n-transitive for all $n \leq k$.

It is clear that a k-transitive group is k-homogeneous. However, these two properties are not equivalent, as shown by the next example.

Example 2.3.1. Consider the cyclic group of order 3. Set $\mathrm{C}_3 = \langle(123)\rangle$, acting on the set $\Omega = \{1, 2, 3\}$. This group is clearly transitive on the set $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ of unordered pairs of Ω and hence the group C_3 is 2-homogeneous. However, C_3 is not a 2-transitive group. Consider, for instance, the elements $(1, 2), (2, 1) \in \Omega^{(2)}$. As $\mathrm{C}_3 = \{(123), (132), \mathrm{id}\}$, there is no element $g \in \mathrm{C}_3$ such that $(1, 2)g = (2, 1)$.

Thus, the cyclic group C_3 is an example of a 2-homogeneous but not a 2-transitive group.

Lemma 2.3.2 (Section 1.8 of [Cam99]). *Suppose that G is a transitive permutation group acting on a set Ω. Then G is k-transitive if and only if G_α is $(k-1)$-transitive on $\Omega\backslash\{\alpha\}$, for all $\alpha \in \Omega$.*

Proof. Let us suppose that G is k-transitive on Ω and let $\alpha \in \Omega$. We want to prove that the stabilizer G_α is $(k-1)$-transitive on the set $\Omega\backslash\{\alpha\}$. Let $(\alpha_1, \ldots, \alpha_{k-1}), (\beta_1, \ldots, \beta_{k-1}) \in (\Omega\backslash\{\alpha\})^{(k-1)}$. By definition, we have that $\alpha \neq \alpha_i, \beta_i$, for $i \in \{1, \ldots, k-1\}$. Therefore the k-tuples $(\alpha_1, \ldots, \alpha_{k-1}, \alpha)$, $(\beta_1, \ldots, \beta_{k-1}, \alpha)$ are elements of $\Omega^{(k)}$. As G is a k-transitive group, there exists an element $g \in G$ such that

$$(\alpha_1, \ldots, \alpha_{k-1}, \alpha)g = (\beta_1, \ldots, \beta_{k-1}, \alpha).$$

Since $\alpha g = \alpha$, it follows that $g \in G_\alpha$. Hence there exists $g \in G_\alpha$ such that $(\alpha_1, \ldots, \alpha_{k-1})g = (\beta_1, \ldots, \beta_{k-1})$, which means that G_α is $(k-1)$-transitive on $\Omega\backslash\{\alpha\}$.

Conversely, let us now assume that G_α is $(k-1)$-transitive on $\Omega\backslash\{\alpha\}$ for all $\alpha \in \Omega$. Let $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^{(k)}$. Since G is a transitive group, there exists $g \in G$ such that $\alpha_1 g = \beta_1$. Set, for $i \in \{2, \ldots, k\}$, $\gamma_i = \alpha_i g$. As g is a permutation, $\gamma_2, \ldots, \gamma_k \neq \beta_1$. By assumption, the stabilizer G_{β_1} is $(k-1)$-transitive on $\Omega\backslash\{\beta_1\}$. Therefore there exists $h \in G_{\beta_1}$ such that $(\gamma_2, \ldots, \gamma_k)h = (\beta_2, \ldots, \beta_k)$ and in particular $\beta_1 h = \beta_1$. Thus we have that $(\alpha_1, \ldots, \alpha_k)gh = (\beta_1, \ldots, \beta_k)$ and $gh \in G$. Hence G is k-transitive on Ω. □

In the next chapter we will use these definitions in the particular case when $k = 2$. A group G is called 2-*homogeneous* if G is transitive on the set

$$\Omega^{\{2\}} = \{\{\alpha, \beta\} : \alpha, \beta \in \Omega, \alpha \neq \beta\},$$

and G is said to be 2-*transitive* if G is transitive on

$$\Omega^{(2)} = \{(\alpha, \beta) : \alpha, \beta \in \Omega, \alpha \neq \beta\}.$$

2.4 Primitive Permutation Groups

The definition of a primitive permutation group comes from the concept of blocks. Suppose that G is a group acting transitively on a set Ω. For a subset B of Ω and $g \in G$, set

$$Bg = \{\gamma g : \gamma \in B\}.$$

A nonempty subset B of Ω is called a *block* for G if for each $g \in G$ either $Bg = B$ or $Bg \cap B = \emptyset$. We observe that the singletons $\{\alpha\}$, with $\alpha \in \Omega$, and Ω itself are always blocks, which are called *trivial blocks*. The set $\{Bg : g \in G\}$, where B is a block for G, is called a *block-system* for the group G.

With this notion it is possible to define a primitive group. A transitive group G is said to be *primitive* if it has no non-trivial blocks. Otherwise G is *imprimitive*. The definitions of primitive and imprimitive groups require that the group in question is already transitive. Hence these notions are not defined for intransitive groups.

If H is a transitive subgroup of an imprimitive group G acting on a set Ω, then H is also imprimitive. This comes from the fact that if B is a non-trivial block for G then it is clearly a non-trivial block for H. Therefore the property of imprimitivity is inherited by transitive subgroups.

As was done before with the concept of orbits, it is possible to characterize blocks in terms of equivalence relations. Let G act transitively on a set Ω. A *congruence* on Ω is an equivalence relation $\approxeq$ which is G-invariant. This means that

$$\text{for all } \alpha, \beta \in \Omega \text{ and } g \in G, \text{ if } \alpha \approxeq \beta \text{ then } \alpha g \approxeq \beta g.$$

The equivalence classes of a congruence are blocks for G. If $|\Omega| \geq 2$, then there are two trivial congruences, the equality relation, whose blocks are singletons, and the universal relation, with a single block Ω. In this terminology, G is said to be primitive if there is no non-trivial congruence of Ω preserved by G.

To study further a primitive group, we will need another notion, namely that of the G-invariant partitions. Suppose $G \leq \mathsf{Sym}(\Omega)$ is a transitive permutation group. If $\{P_1, \ldots, P_k\}$ is a partition of Ω such that

$$\text{for all } P_i \text{ and } g \in G,\ P_i g = P_j \text{ for some } j,$$

then the partition $\{P_1, \ldots, P_k\}$ is called a *G-invariant partition* of Ω. As with blocks, the G-invariant partitions $\{\{\alpha\} : \alpha \in \Omega\}$ and $\{\Omega\}$ are said to be *trivial*.

There is a straight relation between blocks and invariant partitions. Suppose that G is a transitive group on a set Ω and $B \subseteq \Omega$ is a block for G. Then $\{Bg : g \in G\}$ is a G-invariant partition. Conversely, if $\{P_1, \ldots, P_k\}$ is a G-invariant partition of Ω then P_i is a block for G for all $i \in \{1, \ldots, k\}$.

It follows from this relation between partitions and blocks that the size of a G-block divides $|\Omega|$.

We can give a new characterization of primitive groups using G-invariant partitions and their connection to block-systems.

Lemma 2.4.1. *Let G be a transitive subgroups of $\mathsf{Sym}(\Omega)$. Then G is primitive if and only if there are only trivial G-invariant partitions of Ω.*

As noted before, if B is a block for a transitive group $G \leq \mathsf{Sym}(\Omega)$, then $|B| \mid |\Omega|$. This implies the following Corollary.

Corollary 2.4.2. *A transitive group of prime degree is primitive.*

Example 2.4.3. Let us analise an example of an imprimitive group.

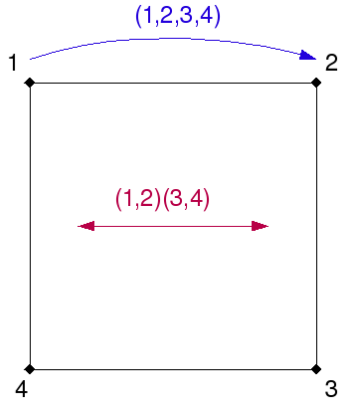


Figure 2.1: The group D_8 acting on the vertices of a square.

Consider the dihedral group D_8 acting on the vertices of a square as in Figure 2.1. In this example $\Omega = \{1, 2, 3, 4\}$ and $D_8 = \langle (12)(34), (1234) \rangle$. It is clear that D_8 is a transitive group. The two pairs of opposite vertices of the square form non-trivial blocks for the group. Hence $\mathscr{P} = \{\{1, 3\}, \{2, 4\}\}$ is a non-trivial partition of Ω which is invariant under D_8. Therefore the group D_8 is an imprimitive group.

After giving the definition of a primitive group, using congruence classes and G-invariant partitions, we will present some important properties of such groups to link primitivity to other concepts of group theory, for instance with

maximal subgroups. Let G be a group. A subgroup H of G is said to be a *maximal subgroup* of G if H is a proper subgroup of G and no proper subgroup of G contains H properly.

Theorem 2.4.4 (Corollary 1.5A of [DM96]). *Let G be a group acting transitively on a set Ω with at least two points. Then G is primitive if and only if each point stabilizer G_α is a maximal subgroup of G.*

Proof. Let us suppose first that G is primitive and let $\alpha \in \Omega$. Then G_α is a proper subgroup of G since Ω contains at least two elements. Let $H \leq \mathsf{Sym}(\Omega)$ such that $G_\alpha \leq H \leq G$ and set $B = \{\alpha h : h \in H\}$. By definition, B is an H-orbit. We claim that B is a block for G. Let $g \in G$ and $\beta \in \Omega$ such that $\beta \in Bg \cap B$. Then $\beta = \alpha h_1 g = \alpha h_2$ for some $h_1, h_2 \in H$. This means that $h_1 g h_2^{-1} \in G_\alpha$. As $G_\alpha \leq H$, we obtain that $g \in H$. Therefore $Bg = B$, and so B is a block for G. Since G is primitive, $B = \{\alpha\}$ or $B = \Omega$. Let us suppose first that $B = \{\alpha\}$ and let $h \in H$. Then $\alpha h = \alpha$ since $\alpha h \in B$ and so $h \in G_\alpha$. Thus we obtain in this case that $G_\alpha = H$. Let us now assume that $B = \Omega$ and let $g \in G$. Then $\alpha g \in \Omega = B$ so $\alpha g = \alpha h$ for some $h \in H$. It follows that $gh^{-1} \in G_\alpha \leq H$ and so $g \in H$. Hence we conclude that $H = G$. Therefore our argument implies that a subgroup H such that $G_\alpha \leq H \leq G$ must be equal either to G_α or to G. Thus G_α is a maximal subgroup of G.

Next, we prove the reverse direction of the statement. Let $\alpha \in \Omega$ and let us suppose that G_α is a maximal subgroup of G. Let B be a block for G such that $\alpha \in B$. We aim to prove that $B = \{\alpha\}$ or $B = \Omega$. First we observe that $G_\alpha \leq G_B$. Indeed, if $g \in G$ such that $\alpha g = \alpha$ then $Bg \cap B \neq \emptyset$, which means that $Bg = B$, and hence $g \in G_B$. As we assumed that G_α is a maximal subgroup of G, either $G_B = G_\alpha$ or $G_B = G$. Let us assume first that $G_B = G_\alpha$ and let $\beta \in B$. Since G is a transitive group, there exists $g \in G$ such that $\beta = \alpha g$. Then $Bg \cap B \neq \emptyset$ which implies that $Bg = B$. Therefore $g \in G_B = G_\alpha$ and so $\beta = \alpha g = \alpha$. Hence we obtain in this case that $B = \{\alpha\}$. Let us now suppose that $G_B = G$ and let $\beta \in \Omega$. By the transitivity of G, there exists $g \in G$ such that $\beta = \alpha g$. Then $\beta \in Bg = B$. Since β was chosen arbitrarily, we conclude in this case that $B = \Omega$. In both cases we obtain that G has no non-trivial blocks. Hence G is primitive. □

As we saw in Statement 1 of Theorem 2.2.3, if a group is transitive then its point stabilizers are all conjugate. Therefore, if one of the point stabilizers is maximal then all the point stabilizers are maximal. Thus in the

previous result it is only necessary to verify the maximality of one of the point stabilizers.

Theorem 2.4.5. *Suppose that G is a 2-homogeneous group acting on a set Ω. Then G is primitive.*

Proof. First note that a 2-homogeneous group is transitive. We argue by contradiction and assume that $\mathscr{P} = \{P_1, \ldots, P_k\}$ is a non-trivial G-invariant partition of Ω. Then $k \geq 2$ and $|P_i| \geq 2$. Pick $\alpha, \beta \in P_1$ such that $\alpha \neq \beta$ and $\gamma \in P_2$. As G is 2-homogeneous, there is $g \in G$ such that $\{\alpha, \beta\}g = \{\alpha, \gamma\}$. Hence $P_1 g \cap P_1 \neq \emptyset$ but $P_1 g \neq P_1$ since $\gamma \in P_1 g$ and $\gamma \notin P_1$. Therefore P_1 is not a block, which is a contradiction to the G-invariant property of $\mathscr{P}$. Thus G does not preserve non-trivial partitions of Ω. Consequently, G is primitive. □

The converse statement of Theorem 2.4.5 is not true. To support this claim, let us present a simple example of a primitive group which is not 2-homogeneous.

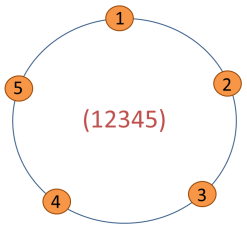


Figure 2.2: The cyclic group of order 5.

Example 2.4.6. Let C_5 be the cyclic group of order 5 acting on the set $\Omega = \{1, \ldots, 5\}$ as in Figure 2.2.

We have that $\mathrm{C}_5 = \langle (12345) \rangle$ and therefore, this group is transitive. Since C_5 has prime degree, by Proposition 2.4.2, it follows that it is a primitive group.

On the other hand, the set $\Omega^{\{2\}}$ has 10 elements, while C_5 has only 5 elements. Hence it follows that C_5 is not transitive on $\Omega^{\{2\}}$, which means that this group in not 2-homogeneous. Thus C_5 is an example of a primitive but not 2-homogeneous group.

The following diagram in Figure 2.3 shows the relationship among the classes of permutation groups defined so far. The Examples 2.3.1, 2.4.3 and 2.4.6 discussed in this chapter show that these classes of permutation groups are properly contained in each other.

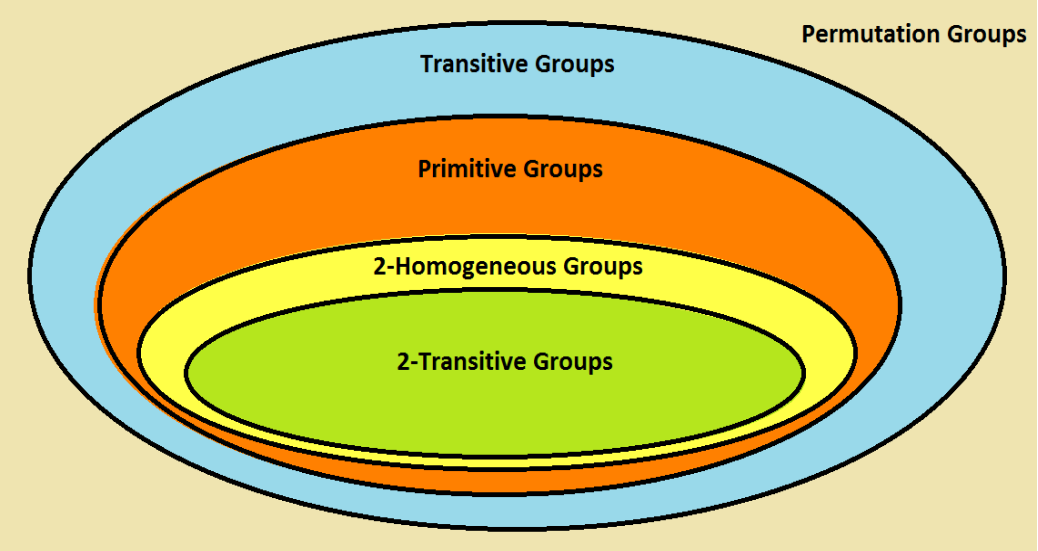


Figure 2.3: The relation between some classes of permutation groups.

Chapter 3

Synchronization and Separation

Synchronization is a recently defined property for permutation groups motivated by a concept in automata and semigroup theory and is related to the Černý Conjecture [Čer64]. João Araújo and Benjamin Steinberg suggested an approach to Černý Conjecture using permutation groups. This approach has not solved the problem, but it was the beginning of the study of synchronizing permutation groups.

The aim of this chapter is to introduce the class of synchronizing groups and to present their most elementary properties.

3.1 Synchronizing Groups

Let Ω be a finite set and let $G \leq \mathsf{Sym}(\Omega)$. Let $\mathscr{P}$ be a partition of Ω to a disjoint union of non-empty subsets of Ω. We define a *section* of $\mathscr{P}$ as a subset S of Ω that contains precisely one element from each part of $\mathscr{P}$.

If given a partition $\mathscr{P}$ there is a section S which verifies

$$Sg \text{ is a section of } \mathscr{P} \text{ for all } g \in G,$$

then $\mathscr{P}$ will be called a *section-regular* or a *G-regular* partition. A permutation group G acting on a set Ω is called *synchronizing* if $G \neq 1$ and there are no non-trivial G-regular partitions of Ω. It follows from the definition that a subgroup H of a non-synchronizing group G is non-synchronizing, since any section-regular partition for G is clearly a section-regular partition for H.

Theorem 3.1.1. *1. A synchronizing permutation group is transitive and primitive.*

2. A 2-homogeneous group is synchronizing.

Proof. Let G be a permutation group acting on a set Ω. To prove the first statement, we only need to observe that if G is intransitive or imprimitive then G preserves a non-trivial partition of the underlying set and it is clear that this partition is section-regular.

Now let us prove Statement 2. Suppose $G \leq \mathsf{Sym}(\Omega)$ is a 2-homogeneous permutation group. Let $\mathscr{P} = \{P_1, \ldots, P_k\}$ be a non-trivial partition of Ω and let S be a section of $\mathscr{P}$. Let $\alpha_1, \alpha_2 \in S$ such that $\alpha_1 \neq \alpha_2$. Assume, without loss of generality, that $\alpha_1 \in P_1$ with $|P_1| \geq 2$. Let $\beta \in P_1 \backslash \{\alpha_1\}$. Such elements exist since $\mathscr{P}$ is non-trivial. As G is 2-homogeneous, there exists $g \in G$ such that $\{\alpha_1, \alpha_2\}g = \{\alpha_1, \beta\}$. Then $\alpha_1, \beta \in Sg$ which implies that Sg is not a section. Therefore no non-trivial section-regular partition exists for G, which means that the group is synchronizing. □

Since a 2-transitive group is 2-homogeneous, it follows from Statement 2 of Theorem 3.1.1 that every 2-transitive group is synchronizing. We obtain in particular that $\mathsf{Sym}(n)$ and the alternating group $\mathsf{Alt}(n)$ are always synchronizing.

Next we will characterize the G-regular partitions for transitive and primitive groups. In particular, we will prove that a G-regular partition is uniform, which means that every part of the partition has the same size. For proving this, we will need a result by Peter Neumann known as Neumann's Separation Lemma, stated as follows.

Proposition 3.1.2 (Neumann's Separation Lemma)**.** *Let G be a transitive permutation group acting on a set Ω and let A and B be finite subsets of Ω with $|\Omega| > |A||B|$. Then there exists $g \in G$ such that $Ag \cap B = \emptyset$.*

Proposition 3.1.2 can be found as Lemma 2.3 of [Neu76]. Statement 1 of the following proposition can be found in [Neu09, Theorem 2.1] and the proof we present follows Cameron [Cam10, Theorem 9 of Chapter 3].

Proposition 3.1.3. *1. A section-regular partition for a transitive permutation group is uniform*

2. A transitive group of prime degree is synchronizing.

Proof. Let us prove the first statement. Let G be a transitive group and $\mathscr{P}= \{P_1, \ldots, P_k\}$ be a section-regular partition for G with section S which witnesses its regularity. We have that $|S| = k$. The partition $\mathscr{P}$ is uniform if $|\Omega| = k|P_i| = |S||P_i|$ for all $i \in \{1, \ldots, k\}$. If there exists $P_i \in \mathscr{P}$ such that $|P_i||S| < |\Omega|$ then by Proposition 3.1.2, there exists $g \in G$ such that $P_i g \cap S = \emptyset$, which is a contradiction since S is a section that witnesses the G-regularity of $\mathscr{P}$. Using this argument we also conclude that cannot exist $P_i \in \mathscr{P}$ such that $|P_i||S| > |\Omega|$ otherwise there would exist a part $P_j \in \mathscr{P}$ such that $|P_j||S| < |\Omega|$, which cannot happen. Therefore we conclude, for all $P_i \in \mathscr{P}$, that $|P_i||S| = |\Omega|$. Hence $\mathscr{P}$ is a uniform section-regular partition for G.

Next, we prove Statement 2. Let G be a transitive permutation group acting on a set Ω of prime order. Let $\mathscr{P}$ be a G-regular partition of Ω. By Statement 1, we have that $\mathscr{P}$ is uniform. As $|\Omega|$ is a prime number, it follows that $\mathscr{P}$ is a trivial partition of Ω. Hence G is a synchronizing group. □

3.2 Synchronization and Cartesian Decompositions

There are primitive groups which preserve Cartesian decompositions of the sets they act upon. The main result of this section is that a primitive group which preserves a Cartesian decomposition is non-synchronizing. This fact was observed by Peter Neumann. In Example 3.4 of [Neu09], in order to prove that a group is non-synchronizing, Neumann constructs a G-regular partition using a direct decomposition of the set on which the group acts upon. Below we present the definition of a Cartesian decomposition and prove the result, which allow us to conclude in Chapter 6 that certain primitive groups are non-synchronizing.

A *Cartesian decomposition* of a set Ω is a set $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_t\}$ of non-trivial partitions of Ω such that

$$|P_1 \cap \cdots \cap P_t| = 1 \text{ for all } P_1 \in \mathscr{P}_1, \ldots, P_t \in \mathscr{P}_t.$$

Let $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_t\}$ be a Cartesian decomposition of a set Ω. Then the map $\omega \mapsto (P_1, \ldots, P_t)$, where for $i \in \{1, \ldots, t\}$ the part $P_i \in \mathscr{P}_i$ is chosen so that $\omega \in P_i$, is a well defined bijection between the set Ω and $\mathscr{P}_1 \times \cdots \times \mathscr{P}_t$. Thus we can naturally identify the set Ω with the Cartesian product $\mathscr{P}_1 \times \cdots \times \mathscr{P}_t$.

A Cartesian decomposition Σ of Ω is said to be *homogeneous* if we have that $|\mathscr{P}_i| = |\mathscr{P}_j|$ for all $\mathscr{P}_i$, $\mathscr{P}_j \in \Sigma$. Note that if Σ is homogeneous then $|\Omega|$ can be identified with$|\mathscr{P}|^t$ for all $\mathscr{P} \in \Sigma$.

Example 3.2.1. Let us consider an example of a Cartesian decomposition.

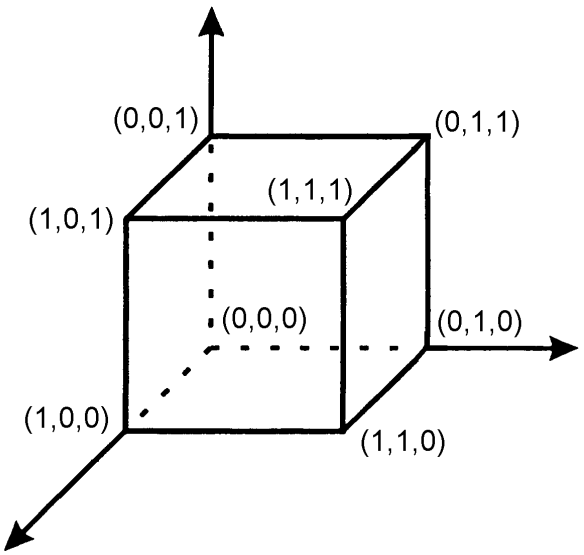


Figure 3.1: The 3-dimensional cube.

Let Ω be the set of vertices the 3-dimensional cube as in Figure 3.1. Let $\mathscr{P}_1$ be the partition

$$\{(1,0,0),(1,1,0),(0,1,0),(0,0,0)\},\{(1,0,1),(1,1,1),(0,1,1),(0,0,1)\},$$

let $\mathscr{P}_2$ be the partition

$$\{(0,0,0),(0,0,1),(1,0,1)(1,0,0)\},\{(1,1,0),(0,1,0),(0,1,1),(1,1,1)\},$$

and let $\mathscr{P}_3$ be the partition

$$\{(0,0,0),(0,1,0),(0,1,1),(0,0,1)\},\{(1,0,0),(1,1,0),(1,1,1),(1,0,1)\}.$$

We have, for $P_i \in \mathscr{P}_i$, that $\left|\bigcap_{i\in\{1,2,3\}} P_i\right| = 1$. Hence $\Sigma = \{\mathscr{P}_1,\mathscr{P}_2,\mathscr{P}_3\}$ is an example of a Cartesian decomposition.

After the definition of Cartesian decompositions, we define basic groups. Let G be a primitive permutation group acting on a set Ω. We say that G is *non-basic* if G preserves a Cartesian decomposition of Ω. Otherwise G is called a *basic* group. We remark that the definition of basic groups given by Peter Cameron in [Cam99, Section 4.3] does not require the primitivity of the group. However, we will only consider this notion for primitive groups. In Example 6.2.5 we present a non-basic, primitive group.

Next we state the main theorem of this section, a result that gives a necessary condition for the synchronization property in permutation groups.

Theorem 3.2.2. *Let G be a primitive group acting on a finite set Ω. If G is non-basic then G is a non-synchronizing group.*

Proof. Let $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_t\}$ be a Cartesian decomposition of Ω which is invariant under G. We start by showing that the group G must be transitive on Σ. Assume by contradiction that G is intransitive on Σ. Then we may assume without loss of generality that $\Sigma_1 = \{\mathscr{P}_1, \ldots, \mathscr{P}_s\}$, with $s < t$, is a G-orbit.

Let, for $i \in \{1, \ldots, s\}$, $P_i \in \mathscr{P}_i$, and set $B = P_1 \cap \cdots \cap P_s$. We claim that B is a non-trivial block for G. Since the partitions $\mathscr{P}_i$ are non-trivial for all $i \in \{1, \ldots, t\}$, we have that $B \neq \Omega$. Next, we assert that $|B| > 1$. Let $P_r, P_r' \in \mathscr{P}_r$ with $r > s$ and such that $P_r \neq P_r'$. Then, since Σ is a Cartesian decomposition of Ω, it follows that $B \cap P_r \neq \emptyset$ and $B \cap P_r' \neq \emptyset$. As $P_r \cap P_r' = \emptyset$, we obtain that $B \cap P_r$ and $B \cap P_r'$ are disjoint sets, and so B contains at least two elements, as was claimed. Now let $g \in G$. Then we have that either $Bg = B$ or $Bg = P_1' \cap \cdots \cap P_s'$, with $P_i' \in \mathscr{P}_i$ for $i \in \{1, \ldots, s\}$ and $P_{i_0} \neq P_{i_0}'$ for some $i_0 \in \{1, \ldots, s\}$. Therefore if $\alpha \in B \cap (P_1' \cap \cdots \cap P_s')$ then in particular $\alpha \in P_{i_0} \cap P_{i_0}'$. As $P_{i_0} \neq P_{i_0}'$, we obtain a contradiction to the condition that $\mathscr{P}_{i_0}$ is a partition. Thus $B = P_1 \cap \cdots \cap P_s$ is a non-trivial block for G, which is a contradiction since we assume that G is primitive. Hence G is transitive on Σ.

Next, we want to show that there exists a G-regular partition of Ω. We will prove that $\mathscr{P}_1$ is a section-regular partition for G. By the first part of the proof we may assume that G is transitive on Σ. Then $|\mathscr{P}_i| = |\mathscr{P}_j|$ for all $\mathscr{P}_i, \mathscr{P}_j \in \Sigma$. For all $i \in \{1, \ldots, t\}$, fix a bijection $\alpha_i : \mathscr{P}_1 \to \mathscr{P}_i$. We have, for each part P of $\mathscr{P}_1$ and for $j \in \{2, \ldots, t\}$, that $P\alpha_j$ is a part of $\mathscr{P}_j$. Therefore we can consider the tuple $(P, P\alpha_2, \ldots, P\alpha_t) \in \mathscr{P}_1 \times \cdots \times \mathscr{P}_t$ and the element $\omega_P = P \cap P\alpha_2 \cap \cdots \cap P\alpha_t$ of Ω. Let us consider the set $S = \{\omega_P : P \in \mathscr{P}_1\}$. Note that S is a section for $\mathscr{P}_1$ and that S is also a section for all $\mathscr{P}_i \in \Sigma$.

We will show that S witnesses the G-regularity of $\mathscr{P}_1$. Let $g \in G$. We claim that Sg is section for $\mathscr{P}_1$. Since Σ is a G-invariant Cartesian decomposition, there exists $i \in \{1, \ldots, t\}$ such that $\mathscr{P}_i g = \mathscr{P}_1$. As S is a section for $\mathscr{P}_i$, we obtain that Sg is a section for $\mathscr{P}_i g = \mathscr{P}_1$. Therefore S witnesses the section-regular property for $\mathscr{P}_1$. Thus $\mathscr{P}_1$ is a non-trivial section-regular partition. Hence G is a non-synchronizing group. □

3.3 Synchronization and Separating Groups

The separation property stems from Neumann's Separation Lemma stated in Proposition 3.1.2. In this section we study separating groups and their basic characteristics since the separation property is a sufficient condition for synchronization (see Proposition 3.3.1).

Let G be a transitive permutation group acting on a set Ω with $|\Omega| = n$. We call G a *non-separating group* if there exist subsets A and B of Ω, with $|A|, |B| > 1$ and $|A||B| = n$, such that for all $g \in G$ we have that $Ag \cap B \neq \emptyset$. Otherwise G is said to be *separating*, which means that for any two subsets of Ω satisfying the conditions above, there is an element $g \in G$ such that $Ag \cap B = \emptyset$. For instance a group acting transitively on a set with prime number of elements is always separating since it is not possible to find sets A and B satisfying the desired conditions.

Next, we link the concept of separation with the properties of permutation group theory studied before, in particular with the synchronization property.

Proposition 3.3.1 (Theorem 7 of [Cam10])**.** *Let G be a transitive group acting on a set Ω.*

1. *If G is separating then G is a synchronizing group.*

2. *If G is 2-homogeneous then G is separating.*

Proof. Let us prove the first statement. Assume that G is non-synchronizing. Then there exists a non-trivial section-regular partition $\mathscr{P}$ with section S which witnesses the G-regularity of $\mathscr{P}$. We have that $\mathscr{P}$ is uniform by the first statement of Proposition 3.1.3. If we consider S and a part P of $\mathscr{P}$ then $|S||P| = |\Omega|$ and $|S|, |P| > 1$. Therefore, as $\mathscr{P}$ is G-regular, for all $g \in G$, Sg is also a section for $\mathscr{P}$. Hence $Sg \cap P \neq \emptyset$ for all $g \in G$. Thus G is a non-separating group and hence Statement 1 is proved.

The proof of the second statement is analogous to the proof of Statement 2 of Theorem 3.1.1 replacing S by A and P_1 by B. □

We know that a synchronizing group is primitive. Thus, by Statement 1 of Proposition 3.3.1, we obtain also that every separating group is primitive. Next, we present an example of a group which shows that the converse of Statement 1 of Proposition 3.3.1 is not true.

Example 3.3.2. The orthogonal classical group $P\Omega(5,3)$ acting on 40 points is an example of a synchronizing and non-separating group. For the details of this example, we refer to Chapter 6 of [Cam10], Section "Some conclusions".

3.4 The Automorphism Group of the Petersen Graph

In this section we discuss an example of a primitive separating but not 2-homogeneous group. This example connects the properties studied in this and in the previous chapters and justifies that the converses of Statement 2 of Theorem 3.1.1 and Statement 2 of Proposition 3.3.1 are not true. In order to study this group we introduce two graphs. One can find this example in Chapter 3 of the lecture notes of Peter Cameron [Cam10].

Let us consider the set Ω of all 2-element subsets of $\{1,\dots,5\}$; that is, $\Omega = \{\{1,2\},\{1,3\},\dots,\{3,5\},\{4,5\}\}$ and $|\Omega| = 10$. Consider the sets $E_P = \{\{A,B\} \in \Omega^{\{2\}} : A \cap B = \emptyset\}$ and $E_J = \Omega^{\{2\}} \backslash E_P$. Then $\Gamma_P = (\Omega, E_P)$ and $\Gamma_J = (\Omega, E_J)$ are undirected graphs with vertex-set Ω. These graphs are usually referred to as the Petersen graph and the (5,2)-Johnson graph and are displayed in Figure 3.2. Note that $|E_P| = 15$ and $|E_J| = 30$.

We define a *clique* in a graph Γ as a complete subgraph of Γ; that is, a set of vertices, such that any two of them are joined by an edge. We say that Γ has *clique number* n, denoted by $\omega(\Gamma)$, if the maximal clique size in Γ is n. A set of vertices not involving any edges is called an *independence set* in the graph. Analogously to the clique number, the size of a largest subset of vertices of Γ involving no edges is called the *independence number* of Γ and is denoted by $\alpha(\Gamma)$. From the definition of the Petersen graph and the (5,2)-Johnson graph we obtain that a clique in Γ_P is an independence set in Γ_J and the converse is also true.

Lemma 3.4.1. *1. The group* $\mathsf{Sym}(5)$ *acts transitively on the set* Ω*, on* E_P *and on* E_J*.*

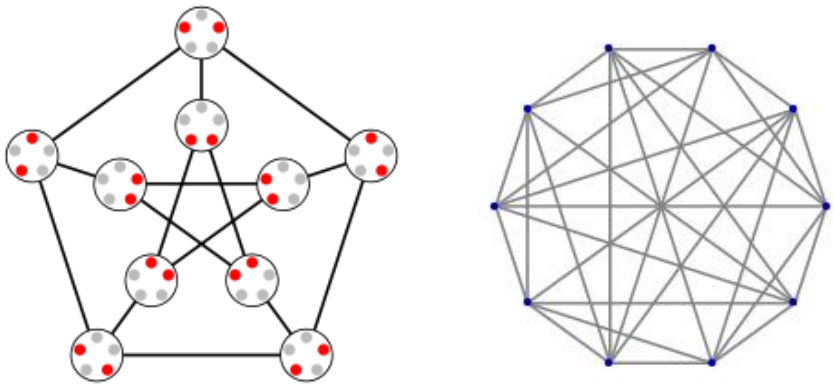


Figure 3.2: The Petersen graph and the (5,2)-Johnson graph.

2. *We have that* $\omega(\Gamma_P) = 2$ *and* $\omega(\Gamma_J) = 4$.

Proof. To prove that $\mathsf{Sym}(5)$ is transitive on Ω, we remark that $\mathsf{Sym}(5)$ is 2-homogeneous on the set $\{1, \ldots, 5\}$ therefore for every pair of elements $\{a, b\}, \{c, d\}$ in Ω there is an element $g \in \mathsf{Sym}(5)$ such that $\{a, b\}g = \{c, d\}$. Hence $\mathsf{Sym}(5)$ is transitive on the set Ω.

Let us now show that the group $\mathsf{Sym}(5)$ is transitive on the sets E_P and E_J. Let $e_1 = \{\{a, b\}, \{c, d\}\}$ and $e_2 = \{\{e, f\}, \{g, h\}\}$ be elements of E_P. By the definition of E_P, we have that $|\{a, b, c, d\}| = 4$ and that $|\{e, f, g, h\}| = 4$. Since $\mathsf{Sym}(5)$ is 5-transitive on $\{1, \ldots, 5\}$, it is 4-transitive on that set. Hence there is $g \in \mathsf{Sym}(5)$ such that $(a, b, c, d)g = (e, f, g, h)$ and so $e_1 g = e_2$. Thus $\mathsf{Sym}(5)$ is transitive on E_P. A similar argument shows that this group is also transitive on the set E_J.

Next, we prove Statement 2. We first have to show that a maximal complete subgraph of Γ_P has only 2 vertices. Indeed, in Ω the maximum number of pairwise disjoint 2-sets is 2 since the elements of Ω are built from the set $\{1, \ldots, 5\}$. Hence the clique number of Γ_P is 2. Now let us consider the graph Γ_J. By definition of Ω, there exist at most 4 pairs which pairwise intersect each other non-trivially. Hence a clique in Γ_J has size at most 4. On the other hand the set of vertices $\{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}\}$ is a complete subgraph of Γ_J . Therefore the clique number of Γ_J is 4. □

Using Lemma 3.4.1, we are ready to show that the group $\mathsf{Sym}(5)$ acting on the set Ω is a primitive separating but not 2-homogeneous group.

Proposition 3.4.2. *Let* Ω *be defined as above. Then the following hold.*

1. $\mathsf{Sym}(5)$ *is primitive on* Ω*;*

2. $\mathsf{Sym}(5)$ *is separating on* Ω*;*

3. $\mathsf{Sym}(5)$ *is not 2-homogeneous on* Ω*.*

Proof. Let us prove that $\mathsf{Sym}(5)$ is primitive on Ω. Let B be a block for $\mathsf{Sym}(5)$. Without loss of generality, we can assume that B contains the element $\{1,2\}$ from Ω. Suppose first that B contains an element disjoint from $\{1,2\}$, for instance $\{4,5\}$. Since $\{1,2\}(345) = \{1,2\}$ and B is a block for $\mathsf{Sym}(5)$, we have that $B(345) = B$. Hence $\{3,5\} = \{4,5\}(345)$, $\{3,4\} = \{3,5\}(345) \in B$. Similarly, as $\{3,5\}(124) = \{3,5\}$, we obtain that $\{2,4\} = \{1,2\}(124)$, $\{1,3\} = \{3,4\}(124) \in B$. Thus $|B| \geq 6$ and since $|B|$ divides $|\Omega|$ (see the observation made before Lemma 2.4.1 about G-invariant partitions and blocks), we conclude that $|B| = 10$. Hence B is a trivial block. Let us now assume that B contains an element that intersect $\{1,2\}$ non-trivially, for instance $\{1,3\}$. As $\{1,2\}(345) = \{1,2\}$ we obtain that $\{1,4\}$, $\{1,5\} \in B$. Furthermore, since $\{1,4\}(134) = \{1,3\}$ which is an element of B, we obtain that $B = B(134)$. Using a similar argument, we have that $\{3,4\} = \{1,3\}(134), \{3,5\} = \{1,5\}(134) \in B$. Thus $|B| \geq 6$, which gives that $B = \Omega$. Therefore $\mathsf{Sym}(5)$ does not admit non-trivial blocks on Ω which implies that $\mathsf{Sym}(5)$ is primitive on that set.

Next, we prove that $\mathsf{Sym}(5)$ is a separating group on Ω. Let A and B be subsets of Ω such that $|A|, |B| > 1$ and $|A||B| = |\Omega|$. We want to show that there exists $g \in \mathsf{Sym}(5)$ such that $Ag \cap B = \emptyset$. Since $|\Omega| = 10$, we have that $\{|A|, |B|\} = \{2,5\}$. Without loss of generality, we can assume that $|A| = 2$ and $|B| = 5$. If $A \cap B = \emptyset$ then we can choose $g = 1$ and the claim is proved. Therefore we may assume that $A \cap B \neq \emptyset$. First we suppose that the two elements of A form an edge in Γ_P. Then we have that $A = \{\{a,b\},\{c,d\}\}$ with $|\{a,b,c,d\}| = 4$. On the other hand, by second statement of Lemma 3.4.1, the clique number of the (5,2)-Johnson graph Γ_J is 4. As $|\Omega \backslash B| = 5$, there exist two pairs $\{c_1,c_2\},\{c_3,c_4\}$ in $\Omega \backslash B$ that are not connected in Γ_J, which means that they form an edge in Γ_P. By Statement 1 of Lemma 3.4.1, the group $\mathsf{Sym}(5)$ is transitive on E_P, and so there exists $g \in \mathsf{Sym}(5)$ such that $\{\{a,b\},\{c,d\}\}g = \{\{c_1,c_2\},\{c_3,c_4\}\}$. Therefore there is $g \in G$ such that $Ag \cap B = \emptyset$. Next, we want to consider the case when the elements of A are not connected in Γ_P. Then, without loss of generality, we have that $A = \{\{a,b\},\{a,c\}\}$. By the second statement of Lemma 3.4.1, the clique number of Γ_P is 2. Hence, as $|\Omega \backslash B| = 5$, there exist

$\{c_1, c_2\}, \{c_3, c_4\} \in \Omega \backslash B$ that form an edge in Γ_J. By the first statement of Lemma 3.4.1, we have that $\mathsf{Sym}(5)$ is transitive on E_J. Thus we conclude that there exists $g \in G$ such that $\{\{a, b\}, \{a, c\}\}g = \{\{c_1, c_2\}, \{c_3, c_4\}\}$. This means that there is $g \in G$ such that $Ag \cap B = \emptyset$. In each case we proved the existence of an element $g \in \mathsf{Sym}(5)$ which separates the sets A and B. Therefore $\mathsf{Sym}(5)$ is a separating group on Ω.

By Statement 1 of Lemma 3.4.1, $\mathsf{Sym}(5)$ has 2 orbits on $\Omega^{\{2\}}$, namely E_P and E_J which means that $\mathsf{Sym}(5)$ is not 2-homogeneous in Ω. □

Example 3.4.3. Inspired by the example of Section 3.4, we give an example that shows that the converse Statement of Theorem 3.2.2 is not true; that is, there exists a basic non-synchronizing group.

Let Ω be the set of all 2-element subsets of $\{1, \ldots, 6\}$. Then $|\Omega| = 15$ and $\Omega = \{\{1, 2\}, \{1, 3\}, \ldots, \{4, 5\}, \{5, 6\}\}$. Consider the group $\mathsf{Sym}(6)$ acting on Ω. We claim that, acting on Ω, the group $\mathsf{Sym}(6)$ is basic and non-synchronizing. Using an analogous argument to the last section, we can easily show that this group is primitive.

Next, we prove that $\mathsf{Sym}(6)$ is basic. Let $\Sigma = \{\mathscr{P}_1, \ldots \mathscr{P}_n\}$ be a non-trivial Cartesian decomposition preserved by $\mathsf{Sym}(6)$. Since we can identify Ω with $\mathscr{P}_1 \times \cdots \times \mathscr{P}_n$, we have that $|\Omega| = |\mathscr{P}_1| \times \cdots \times |\mathscr{P}_n|$. This implies that $n = 2$ and $\{|\mathscr{P}_1|, |\mathscr{P}_2|\} = \{3, 5\}$. Therefore, since $|\mathscr{P}_1| \neq |\mathscr{P}_2|$, we obtain that $\mathsf{Sym}(6)$ preserves these two partitions. This is a contradiction to the primitivity of $\mathsf{Sym}(6)$. Thus this group is basic.

Let us prove that $\mathsf{Sym}(6)$ is non-synchronizing. The complete graph K_6 is edge-colored with 5 colors; that is, there exists a coloring of the edges of K_6 with the rule that two edges with common vertices get different colors which uses 5 colors. Therefore, considering a partition $\mathscr{P}$ of Ω by that edge-coloring, we obtain that $\mathscr{P}$ has 5 parts of size 3, with the property that any two pairs in the same part are disjoint. Now consider the set S of all pairs of Ω containing the element 1. By the way $\mathscr{P}$ was defined, we have that S is a section for $\mathscr{P}$ and also by the action of $\mathsf{Sym}(6)$ on Ω, we obtain that Sg is a section for $\mathscr{P}$ for all $g \in \mathsf{Sym}(6)$. Therefore this group preserves a non-trivial section-regular partition. Thus $\mathsf{Sym}(6)$ acting on Ω is non-synchronizing.

To finish this chapter on the synchronization property, we can now extend the diagram of permutation groups displayed on Figure 2.3. The diagram of Figure 3.3 shows us a picture of how these diverse properties fit into each other. Furthermore, we can also read off which of these properties are sufficient for synchronization and which of them are necessary.

We observe that the examples described in this and in the previous chapters support the fact that these classes of groups are properly contained in each other.

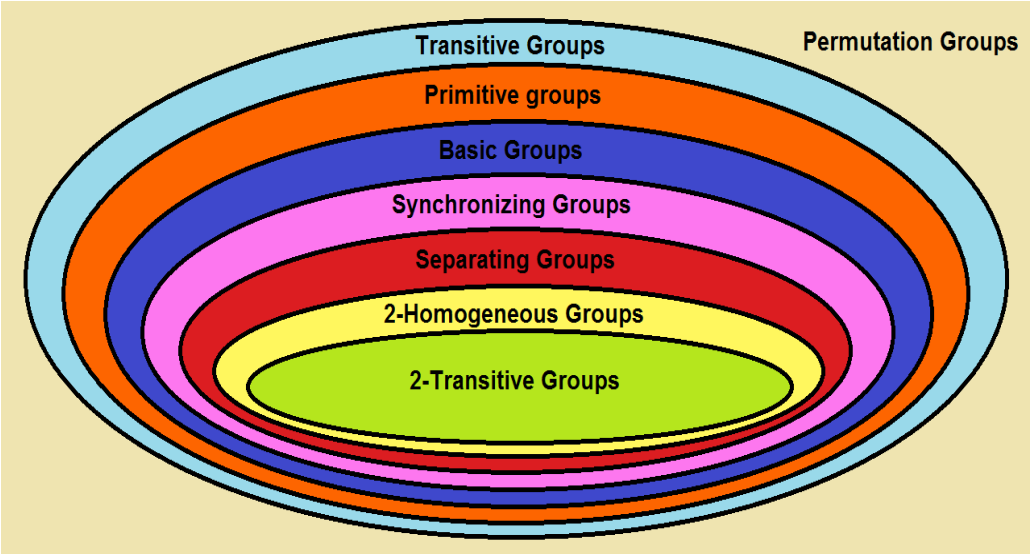


Figure 3.3: The synchronization property among the classes of permutation groups.

Chapter 4

Synchronization, Separation and Graphs

The synchronization property in permutation groups has a close relationship with some properties of certain graphs that arise from the group action. In this chapter we will be concerned with this relationship. We will start with the necessary background on graph theory, in particular with the construction and properties of undirected orbital graphs. Then we will state Theorem 4.2.4, which gives necessary and sufficient conditions for the separation and the synchronization properties. Next, we generalize the results for vertex-transitive graphs and in Section 4.4 we discuss a graph invariant, the Lovász theta-function, which turns out to be useful in our characterization of synchronizing groups.

4.1 Undirected Orbital Graphs

In this section we study undirected graphs built from the action of a group on a certain set. This construction is analogous to the orbital graph construction (see Section 3.2 of [DM96]). Let G be a permutation group acting on a set Ω. An *undirected orbital* of G is an orbit of G on the set

$$\Omega^{\{2\}} = \{\{\alpha, \beta\} : \alpha, \beta \in \Omega \text{ and } \alpha \neq \beta\}.$$

Given an undirected orbital Δ of G, the *undirected orbital graph* associated with Δ, denoted by $\Gamma_\Delta = (\Omega, \Delta)$, is the undirected graph with vertex-set Ω and edge-set Δ; that is, there exists an edge from α to β in Γ_Δ if and only if

$\{\alpha, \beta\} \in \Delta$. For any graph Γ, we denote the neighborhood of a vertex α in Γ by $\Gamma(\alpha)$.

Example 4.1.1. We showed in Section 3.4 that $\mathsf{Sym}(5)$ has two undirected orbitals with respect to its action on a set with 10 points. The corresponding undirected orbital graphs are the Petersen graph and the (5,2)-Johnson graph, displayed in Figure 3.2.

An *automorphism of a graph* Γ is a permutation g of the vertex-set of Γ such that for any two vertices v_1, v_2, we have that $v_1 g$ and $v_2 g$ form an edge in Γ if and only if v_1 and v_2 form an edge in Γ. Hence the edges are preserved by a graph automorphism. The set of all automorphisms of a graph Γ, with the operation of composition, is a group which is the *automorphism group* of Γ and is denoted by $\mathsf{Aut}(\Gamma)$. A graph Γ is said to be *vertex-transitive* if given two vertices v_1 and v_2 of Γ there is a graph automorphism that maps v_1 to v_2. In a similar way we can define *edge-transitive* graph. We say that a graph Γ is *regular* if every vertex of Γ has the same number of neighbors. In particular a vertex-transitive graph is always regular.

A graph is said to be *connected* if there is a path between any two vertices, otherwise the graph is called *disconnected*. Let us define a relation $\sim$ in the set of vertices Ω of a graph Γ as follows.

Given $\alpha, \beta \in \Omega$, $\alpha \sim \beta$ if and only if there exists a path in Γ from α to β.

The relation $\sim$ is an equivalence relation and the equivalence classes of $\sim$ are called the *connected components* of the graph Γ. If a graph is connected then it has just one connected component.

This concept of connectivity in a graph leads us to a result to test if a transitive permutation group is primitive.

Theorem 4.1.2 (Higman's Theorem)**.** *Let G be a transitive permutation group acting on a set Ω. Then G is primitive if and only if the graph $\Gamma_\Delta = (\Omega, \Delta)$ is connected for all undirected G-orbitals Δ in $\Omega^{\{2\}}$.*

Proof. Let us assume that all graphs associated with undirected orbitals for G are connected. Let B be a block for G with at least two elements. We want to show that $B = \Omega$. Let $\alpha, \beta \in B$ such that $\alpha \neq \beta$ and consider the undirected orbital Δ for G that contains $\{\alpha, \beta\}$. Let $\gamma \in \Omega$. Since the graph associated with Δ is connected, there is a path $\alpha = \alpha_0, \ldots, \alpha_k = \gamma$ from α to γ. We show by induction that, for all $i \in \{0, \ldots, k\}$, we have

$\alpha_i \in B$. The claim is true for $i = 0$. Thus let us assume by inductive hypothesis that $\alpha_{i-1} \in B$. Since $\{\alpha_{i-1}, \alpha_i\} \in \Delta$ there exists $g \in G$ such that $\{\alpha g, \beta g\} = \{\alpha_{i-1}, \alpha_i\}$. As we assume that $\alpha_{i-1} \in B$ either $\alpha g \in B$ or $\beta g \in B$. Therefore, since B is a block, we have that $B = Bg$ which implies that $\alpha_i \in B$. Thus we obtain that $\alpha_i \in B$ for all $i \in \{1, \ldots, k\}$. In particular $\gamma \in B$. Hence for all $\gamma \in \Omega$ we conclude that $\gamma \in B$ which means that $B = \Omega$. Therefore G has no non-trivial blocks and so it is a primitive group.

Conversely let us suppose that there exists an undirected orbital Δ for G such that the graph Γ_Δ associated with Δ is not connected. The connected components of Γ_Δ form a G-invariant partition of Ω, which is non-trivial since Γ_Δ is non-trivial and Γ_Δ is not connected. This fact implies that G is an imprimitive group by Lemma 2.4.1. □

A *bipartite graph* Γ is a graph whose vertices can be divided into disjoint sets U_1, U_2 such that every edge of Γ connects a vertex in U_1 to a vertex in U_2. The subsets U_1 and U_2 are called the *bi-parts* of Γ. An example of a bipartite graph is shown in Figure 4.1. Since the automorphisms of graphs preserve distance (the length of a shortest path between two connected points), it follows that an automorphism of a connected bipartite graph either preserves the bi-parts or swaps them.

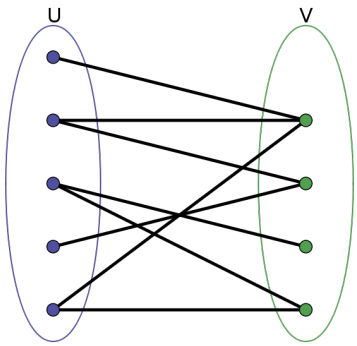


Figure 4.1: A bipartite graph with 9 vertices

As an application of Higman's Theorem, we can characterize the section regular partitions for primitive permutation groups.

Proposition 4.1.3 (Lemma 2.4 of [Neu09]). *Suppose that G is a primitive group acting on a set Ω and let $\mathscr{P}$ be a non-trivial section-regular partition for G. Then we have that $|\mathscr{P}| > 2$ and for every part P of $\mathscr{P}$, $|P| > 2$.*

Proof. Since $\mathscr{P}$ is a non-trivial section-regular partition of Ω, we have that $|P| > 1$ and $|\mathscr{P}| > 1$. Therefore, we assume by contradiction that $|P| = 2$ or $|\mathscr{P}| = 2$.

Let us suppose first that $|\mathscr{P}| = 2$. Let S be a section for $\mathscr{P}$ which witnesses its G-regularity. Then S is a unordered pair $\{\alpha, \beta\}$ and we can consider the undirected orbital $\{\alpha, \beta\}G$ containing S and denote it by Δ. Since the group G is primitive, we have, by Theorem 4.1.2, that the undirected orbital graph Γ_Δ associated with Δ is connected. Let P_1, P_2 be the two parts of $\mathscr{P}$. Since for all $g \in G$, Sg is a section for $\mathscr{P}$, every edge in Γ_Δ connects an element from P_1 to an element from P_2. This fact means that Γ_Δ is a bipartite graph with bi-parts P_1 and P_2. As Γ_Δ is connected, we have that any graph automorphism of Γ_Δ either fixes P_1 and P_2 setwise or interchanges them (see the remark before Proposition 4.1.3). By definition, G is a group of automorphisms of Γ_Δ. This means that $\mathscr{P}$ is a non-trivial G-invariant partition, which contradicts the primitivity of the group G. Hence the case $|\mathscr{P}| = 2$ cannot occur. Thus $|\mathscr{P}| > 2$.

Now let us assume that every part P of $\mathscr{P}$ has size 2. Let S be a section for $\mathscr{P}$ which witnesses its G-regularity. Let $S' = \Omega \backslash S$ and $\mathscr{Q} = \{S, S'\}$. Then $\mathscr{Q}$ is a partition of Ω. Since S is a section for $\mathscr{P}$ we have that any part of $\mathscr{P}$ is a section for $\mathscr{Q}$. Let $P = \{\alpha, \beta\}$ be a part of $\mathscr{P}$ and g be an element of G. We want to show that Pg is a section for $\mathscr{Q}$. Let us assume that $Pg \subset S$. As $\{\alpha, \beta\}g \subseteq S$, we have that $\alpha, \beta \in Sg^{-1}$ which is a contradiction to the fact that S witnesses section-regularity of $\mathscr{P}$ and so Sg^{-1} is a section for $\mathscr{P}$. Next we assume that $Pg \subset S'$. Since g is a permutation, $Sg^{-1} \cap S'g^{-1} = \emptyset$. On the other hand, we have that α, β are in $S'g^{-1}$. This fact means that $P \cap Sg^{-1} = \emptyset$, which is again a contradiction since Sg^{-1} must be a section for $\mathscr{P}$. Hence we obtain that $|Pg \cap S| = 1$ and $|Pg \cap S'| = 1$. Therefore Pg is a section for $\mathscr{Q}$ which implies that $\mathscr{Q}$ is a G-regular partition. Hence by the previous paragraph, this case cannot happen since $\mathscr{Q}$ has only two parts. Therefore $|P| > 2$, for every part P of $\mathscr{P}$ and the proof is complete. □

The next corollary, concerned about the synchronization property, is a direct consequence of Proposition 4.1.3.

Corollary 4.1.4. *A primitive group of degree $2p$, where p is a prime, is*

synchronizing.

Proof. Let $G \leq \mathsf{Sym}(\Omega)$ be a primitive group with $|\Omega| = 2p$, where p is a prime. By Proposition 4.1.3, a non-trivial G-regular partition of Ω has more than 2 parts and each part has more than 2 elements. By Statement 1 of Proposition 3.1.3 we know that a G-regular partition is uniform. By assumption, we have that $|\Omega| = 2p$, and as the only proper divisors of $2p$ are 2 and p, we obtain that there cannot exist a non-trivial section-regular partition of G. Hence G is a synchronizing group. □

4.2 Synchronization, Cliques and Colors

In this section, we prove a necessary and sufficient condition for the synchronization and separation properties using the clique and the chromatic numbers of the graphs discussed above. We start by defining some concepts of graph theory before stating the results about these properties.

Given a graph $\Gamma = (\Omega, E)$, we denote by $\Gamma' = (\Omega, E')$ the *complement graph* of Γ; that is, the graph with the same vertex-set Ω and edge-set $E' = \Omega^{\{2\}} \backslash E$. It follows from the definition of the complement graph that a clique in Γ' is an independence set in Γ and that the converse is also true. Given a graph Γ, $\omega(\Gamma)$ is the clique number and $\alpha(\Gamma)$ is the independence number of Γ. Recall the definitions of these numbers from Section 3.4.

Proposition 4.2.1. *Let $\Gamma = (\Omega, E)$ be a vertex transitive graph and suppose that C is a clique and I is an independence set in Γ such that $|C||I| = |\Omega|$. Then $\omega(\Gamma) = |C|$ and $\alpha(\Gamma) = |I|$.*

For the proof of this proposition we need an auxiliary Lemma that can be found as Theorem 8 of [Cam10].

Lemma 4.2.2. *Let G be a transitive permutation group acting on a set Ω and let A, B be subsets of Ω satisfying $|A||B| = \lambda|\Omega|$ for some integer λ. Then the following are equivalent:*

1. *for all $g \in G$, $|Ag \cap B| = \lambda$;*
2. *for all $g \in G$, $|Ag \cap B| \leq \lambda$;*
3. *for all $g \in G$, $|Ag \cap B| \geq \lambda$.*

Proof of Proposition 4.2.1. Let $\Gamma = (\Omega, E)$ be a vertex-transitive graph and set $G = \mathsf{Aut}(\Gamma)$. Assume that C is a clique and I is an independence set for Γ such that $|C||I| = |\Omega|$. We claim that $\omega(\Gamma) = |C|$. Let us suppose by contradiction that there exists a clique $A \in \Omega$ such that $|A| > |C|$. Without loss of generality, we can assume that $|A| = |C| + 1$. Let $\beta \in A$ and let us consider $A_1 = A \backslash \{\beta\}$. Then $|A_1| = |C|$ and we have, for all $g \in G$, that $|A_1 g \cap I| \leq 1$. Hence, by Lemma 4.2.2, we obtain, for all $g \in G$, that $|A_1 g \cap I| = 1$. Let $\gamma \in I$. Since G is a transitive group in Ω, there exists $g \in G$ such that $\beta g = \gamma$. On the other hand, we have that $|A_1 g \cap I| = 1$ and as $\beta \notin A_1$, it follows that $\gamma = \beta g \notin A_1 g$. Therefore $|Ag \cap I| = |(\{\beta g\} \cup A_1 g) \cap I| = 2$. This is a contradiction since A is a clique and I is an independence set. Thus there is no clique with size greater than C and so $\omega(\Gamma) = |C|$. Exchanging Γ with its complement graph Γ', we obtain that $|I| = \omega(\Gamma') = \alpha(\Gamma)$. □

The *chromatic number* of a graph Γ, denoted by $\chi(\Gamma)$ is the smallest number of colors needed to color the vertices of Γ so that no two adjacent vertices share the same color. It is a trivial observation that $\omega(\Gamma) \leq \chi(\Gamma)$ holds in any graph Γ.

Let Γ be a vertex-transitive graph with vertex-set Ω. Then Γ is called a *pseudo-suitable* graph if $\omega(\Gamma)\omega(\Gamma') = |\Omega|$. If we have that $\omega(\Gamma) = \chi(\Gamma)$, then Γ will be called a *suitable* graph.

Proposition 4.2.3. *Let Γ be a vertex-transitive graph. Then the following are valid.*

1. *Γ is pseudo-suitable if and only if Γ' is pseudo-suitable.*
2. *If Γ is suitable then Γ is pseudo-suitable.*

Proof. The first statement is a consequence of the definition of pseudo-suitable graphs.

Let us prove Statement 2. Let $\Gamma = (\Omega, E)$ be a vertex-transitive graph and set $G = \mathsf{Aut}(\Gamma)$. Assume that Γ is suitable, such that $\omega(\Gamma) = \chi(\Gamma) = k$. Let $\mathscr{P}$ be a partition of Ω according to a colouring with k colors and let C be a clique for Γ with size k. Since the edge-set of Γ is G-invariant, we have, for all $g \in G$, that the image Cg is a clique for Γ with k vertices. Thus, for all $g \in G$, the set Cg contains precisely one vertex of each color. Thus Cg is a section for $\mathscr{P}$ for each $g \in G$, which shows that $\mathscr{P}$ is a G-regular partition. By the first statement of Proposition 3.1.3, we obtain that $\mathscr{P}$ is uniform, which means that every part of $\mathscr{P}$ has $|\Omega|/k$ vertices. Let P be a part

of $\mathscr{P}$. We observe that by the way $\mathscr{P}$ was defined with the colors, P is an independence set for Γ and by the last argument it has size $|\Omega|/k$. Therefore, applying Proposition 4.2.1 to C and P, we conclude that $\alpha(\Gamma) = |\Omega|/k$ and hence $|\omega(\Gamma)||\alpha(\Gamma)| = |\Omega|$. As observed before, an independence set in a graph is a clique in its complement graph. Thus we obtain that $|\omega(\Gamma)||\omega(\Gamma')| = |\Omega|$. Therefore Γ is a pseudo-suitable graph. □

Now we present the main result of this chapter, that gives necessary and sufficient conditions for the separation and synchronization properties in terms of graphs whose edge-sets are invariant under the action of a group.

Theorem 4.2.4. *Let G be a transitive permutation group acting on a set Ω. Then the following hold.*

1. *G is non-separating if and only if there is a G-invariant subset E of $\Omega^{\{2\}}$ such that $\Gamma = (\Omega, E)$ is pseudo-suitable.*

2. *If G is primitive then G is non-synchronizing if and only if there is a proper non-empty G-invariant subset $E \subseteq \Omega^{\{2\}}$ such that the graph $\Gamma_E = (\Omega, E)$ is suitable.*

Proof. Let us prove the first statement. Assume that G is non-separating and let A and B be subsets of Ω which witness its non-separability. Consider the graph Γ with vertex-set Ω and set of edges $\{\{ag, bg\} : a, b \in A \text{ and } a \neq b\}$. It is clear that A is a clique in Γ. If any pair of elements of B was an image of a pair of points of A by an element $g \in G$, we had that $|Ag \cap B| \geq 2$ which contradicts the Lemma 4.2.2 since we assume that $|A||B| = 1|\Omega|$. Hence B is an independence set of Γ. Hence by Proposition 4.2.1 we have that $\omega(\Gamma)\,\alpha(\Gamma) = |A||B| = |\Omega|$. This equation is equivalent to $\omega(\Gamma)\,\omega(\Gamma') = |\Omega|$ and hence Γ is a pseudo-suitable graph.

Conversely, assume that there exists a pseudo-suitable graph Γ for G. Let us observe that a clique and an independence set in Γ can intersect in at most one point. Indeed, if the intersection contains two points, they must be connected and unconnected at the same time. Then, in particular, any clique C of size $\omega(\Gamma)$ and independence set I with size $\omega(\Gamma')$ must meet in at most one point. Thus, by Lemma 4.2.2, they meet at exactly one point. Therefore for all $g \in G$ we obtain that $Cg \cap I \neq \emptyset$. Hence G is a non-separating group.

Next we prove Statement 2. Let us suppose first that G is a primitive non-synchronizing group. Let $\mathscr{P} = \{P_1, \ldots, P_k\}$ be a non-trivial section-regular partition of Ω for G, witnessed by a section S and consider the following set:

$$E = \{\{\alpha g, \beta g\} : g \in G, \alpha, \beta \in S, \alpha \neq \beta\}.$$

Since $E \subseteq \Omega^{\{2\}}$, the graph $\Gamma_E = (\Omega, E)$ is undirected. Further, the set E is G-invariant. Therefore using Theorem 4.1.2, we conclude that the graph Γ_E is connected. We have that every pair of elements of the section S is connected in Γ_E since this graph has edge-set E. Therefore the clique number of Γ_E is bigger or equal to $|S|$. On the other hand, if P is a part of the partition $\mathscr{P}$ and $\alpha, \beta \in P$, then α and β are not connected in Γ_E. Indeed, if they were connected, there would exist $g \in G$ and $\alpha_1, \beta_1 \in S$ such that $\alpha = \alpha_1 g$ and $\beta = \beta_1 g$. Since $\alpha_1, \beta_1 \in S$, these elements belong to different parts of the partition $\mathscr{P}$ and as $\mathscr{P}$ is G-regular, so do α and β. This contradicts the fact that $\alpha, \beta \in P$. Hence Γ_E is colorable with k colors, where $k = |S| = |\mathscr{P}|$. Therefore we conclude that $\chi(\Gamma_E) \leq k \leq \omega(\Gamma_E)$. Since the clique number is smaller or equal that the chromatic number, we obtain that $\chi(\Gamma_E) = \omega(\Gamma_E) = k$. This means that Γ_E satisfies the conditions of the theorem.

Conversely, assume that $\Gamma_E = (\Omega, E)$ is a graph with the same clique and chromatic number k, where $E \subseteq \Omega^{\{2\}}$ is a G-invariant set. Let $g \in G$, and C be a clique of size k in Γ_E. Consider a partition $\mathscr{P}$ of Ω according to a coloring with k colors. Since the graph Γ_E is G-invariant, Cg is also a clique for the graph. Then $|Cg| = |\mathscr{P}|$ and for all part P of $\mathscr{P}$ we have that $|Cg \cap P| = 1$. Indeed, this intersection must be non-empty since Cg must contain one vertex of each color. Further, if $\alpha, \beta \in Cg \cap P$, with $\alpha \neq \beta$, then they must be connected and unconnected at the same time. Hence Cg is a section for $\mathscr{P}$. Thus C witnesses the G-regularity of $\mathscr{P}$. Therefore $\mathscr{P}$ is a non-trivial section-regular partition of Ω which means that G is a non-synchronizing group. □

Theorem 4.2.4 shows us a shortcut on the road of determining if a permutation group is synchronizing. Since a separating group is synchronizing, we should start our search of synchronization by investigating the separation property. Therefore, by Statement 1 of Theorem 4.2.4, this is reduced to the problem of determining the clique number of a graph. Thus, if we do not find a pseudo-suitable graph for the group, then we can conclude that the group is separating and hence synchronizing.

In the other hand, if we find a pseudo-suitable graph for the group then that graph and its complement graph are good candidates for being suitable, meaning that the group in study can be non-synchronizing. This fact is

justified by Statement 2 of Proposition 4.2.3, which states that a suitable graph is pseudo-suitable.

4.3 Vertex-Transitive Automorphisms of a Graph

Combining the results in the previous sections, we can obtain interesting properties of graphs with vertex-transitive automorphism groups.

Theorem 4.3.1. *Let $\Gamma = (V, E)$ be a vertex-transitive graph such that $\omega(\Gamma) = \chi(\Gamma) = k$. Then the following hold.*

1. *The number k divides the number of vertices of Γ.*

2. *Every colour of a colouring with size k, colours the same number of vertices.*

Proof. For the proof of the first statement, we just observe that the graph Γ is suitable by hypothesis. Hence, from Statement 2 of Proposition 4.2.3 it follows that Γ is a pseudo-suitable graph, which means that $\omega(\Gamma)\omega(\Gamma') = |V|$. As $\omega(\Gamma) = k$, it implies that k divides the number of vertices.

Next we prove the second statement. Let $\mathscr{P}$ be a colouring for Γ with k colours and C be a clique of Γ with size k. As the graph Γ is invariant under $\mathrm{Aut}(\Gamma)$, we obtain, for all $g \in \mathrm{Aut}(\Gamma)$, that Cg is also a clique for Γ. Then $|Cg| = |\mathscr{P}|$ and for all part P of $\mathscr{P}$ we have that $|Cg \cap P| = 1$. This argument implies that Cg is a section for the partition $\mathscr{P}$. Hence this partition is a section-regular partition. Thus, by the first statement of Proposition 3.1.3, we conclude that $\mathscr{P}$ is a uniform partition. Therefore in a colouring of Γ with k colours, each colour is applied to the same number of vertices. □

4.4 The Lovász Theta-function

The problem of determining the clique and the chromatic number of certain graphs is a hard task and it is not always possible to solve efficiently. In the aim of solving this problem, there were developments in order to establish bounds for the clique and chromatic number of graphs. One of these bounds was defined by László Lovász [Lov79]. In his article about the Shannon

capacity of a graph, Lovász defined a function, called theta-function, which gives some bounds for these numbers.

In this section we will define this function and present a summary of its properties, in order to get more tools for analyzing the synchronization property using graphs. For the theory of the theta-function we refer to Chapter 3 of [GM12]. To simplify notation, we will assume that a graph with n vertices has vertex-set $\{1, \ldots, n\}$.

An *orthogonal representation* of a graph $\Gamma = (V, E)$ with n vertices, is a sequence $\mathcal{U} = (u_1, \ldots, u_n)$ of unit vectors in a Euclidean space $\mathbb{R}^m$ for some m, such that

$$u_i^T u_j = 0 \text{ if } \{i, j\} \notin E.$$

It follows from the definition that every graph has an orthogonal representation, since we can consider an orthogonal basis of $\mathbb{R}^{|V|}$. We define the *value* of an orthogonal representation $\mathcal{U}$ of a graph Γ as

$$\vartheta(\mathcal{U}) = \min_{\|c\|=1} \max_{1 \le i \le n} \frac{1}{(c^T u_i)^2}.$$

The minimum value over all orthogonal representations of a graph Γ is called the *theta-function* of Γ and is denoted by $\vartheta(\Gamma)$.

After the definition of the theta-function, we are interested in its properties; in particular the ones that connect this function to the clique and the chromatic number of a graph. For these results we refer to the paper of Lovász [Lov79].

Proposition 4.4.1. *Let $\Gamma = (V, E)$ be an undirected graph with edge-set E and vertex-set V of size n. Then the following hold.*

1. $\omega(\Gamma) \le \vartheta(\Gamma') \le \chi(\Gamma)$.
2. *If Γ is vertex-transitive then $\vartheta(\Gamma)\vartheta(\Gamma') = n$.*

From this proposition we conclude that for suitable graphs, Statement 1 implies that $\omega(\Gamma) = \vartheta(\Gamma') = \chi(\Gamma)$.

Given a graph Γ with n vertices, we define the *adjacency matrix* of the graph Γ, denoted by A_Γ, as the $n \times n$ matrix with entries 0 and 1, where the entry a_{ij} is 1 if the vertices i and j are connected by an edge and it is 0 otherwise. As we consider in our study finite undirected simple graphs, the adjacency matrix has zero-diagonal and is symmetric. From the symmetric

property of these matrices we conclude that their eigenvalues are real. On the other hand, as A_Γ has integer entries, its characteristic polynomial has integer coefficients and is monic. Since every eigenvalue is a root of the characteristic polynomial, we obtain from the rational root test (Proposition 5.1 of [Mor96]), that any rational eigenvalue of A_Γ must be an integer.

Let Γ be an undirected simple graph with n vertices and A_Γ be the adjacency matrix for Γ. Let us denote the eigenvalues of the matrix A_Γ by $\lambda_1^\Gamma \geq \lambda_2^\Gamma \geq \ldots \geq \lambda_n^\Gamma$. These eigenvalues are independent of the ordering of the vertices of the graph and therefore we refer to the eigenvalues of the adjacency matrix as the eigenvalues of the graph Γ. The smallest and the largest eigenvalues of a graph Γ, respectively denoted by λ_n^Γ and λ_1^Γ, are particularly interesting since they exhibit some special properties and represent some characteristics of the graph.

We define the *degree* of a vertex v as the number of edges incident to v. Let $\partial_{\max}(\Gamma)$ denote the maximum degree of a vertex in a graph Γ and $\bar{\partial}(\Gamma)$ denote the average degree of the vertices of Γ. If Γ is regular, since every vertex has the same degree, then $\bar{\partial}(\Gamma)$ denotes the degree of the graph.

Next we present a summary of the properties of the theta-function connected to the eigenvalues of a graph and with its clique and chromatic number. We observe that in the following chapters we will study graphs with the property of regularity. Therefore the last two statements of the next proposition have results that apply for those graphs.

Proposition 4.4.2. *Let Γ be a graph with vertex-set of size n. Then we have that:*

1. $1 - (\lambda_1^\Gamma/\lambda_n^\Gamma) \leq \chi(\Gamma)$;
2. $\max\{\bar{\partial}(\Gamma), \sqrt{\partial_{max}(\Gamma)}\} \leq \lambda_1^\Gamma \leq \partial_{max}(\Gamma)$;
3. *If Γ is regular then* $\lambda_1^\Gamma = \bar{\partial}(\Gamma)$;
4. *If Γ is regular and edge-transitive then* $\vartheta(\Gamma) = -n\lambda_n^\Gamma/(\lambda_1^\Gamma - \lambda_n^\Gamma)$.

Proof. For the proof of this proposition we refer to the paper of Lovász [Lov79]. Statement 1 can be found as Corollary 3 and Statement 2 as Proposition 2.1. The third statement is a consequence of Statement 2. The last statement can be found as Theorem 9 in the same paper. □

Since every vertex-transitive graph is regular, applying the formula for the Lovász theta-function given by Statement 4 of Proposition 4.4.2, we obtain a necessary condition for the suitability in vertex-transitive graphs which are edge-transitive.

Theorem 4.4.3. *Let Γ be a vertex-transitive and edge-transitive suitable graph with n vertices such that $\omega(\Gamma) = \chi(\Gamma) = k$. Then we have that $k-1$ divides $\bar{\partial}(\Gamma)$. Further $\lambda_n^\Gamma = -\bar{\partial}\Gamma/(k-1)$.*

Proof. Let Γ be a graph in the conditions of the theorem. From the first statement of Proposition 4.4.1, we know that $\omega(\Gamma) \leq \vartheta(\Gamma') \leq \chi(\Gamma)$. Since Γ is a suitable graph, it implies that $\omega(\Gamma) = \vartheta(\Gamma') = \chi(\Gamma)$ and therefore $\vartheta(\Gamma') = k$. As Γ is vertex-transitive, from Statement 2 of Proposition 4.4.1 we know that $\vartheta(\Gamma')\vartheta(\Gamma) = n$. Hence we obtain that $\vartheta(\Gamma) = n/k$. Also from the vertex-transitive property of Γ, we have that Γ is regular and therefore we can apply Statement 3 of Proposition 4.4.2 which states that λ_1^Γ coincides with to the degree of Γ. Now by Statement 4 of Proposition 4.4.2 we know that $\vartheta(\Gamma) = (-n\lambda_n^\Gamma)/(\lambda_1^\Gamma - \lambda_n^\Gamma)$. Using the observations made above, we obtain that

$$\vartheta(\Gamma) = \frac{n}{k} = \frac{-n\lambda_n^\Gamma}{\bar{\partial}(\Gamma) - \lambda_n^\Gamma}$$

and after some calculations we get

$$\lambda_n^\Gamma(1-k) = \bar{\partial}(\Gamma). \tag{4.1}$$

Hence λ_n^Γ is a rational number. However, since λ_n^Γ is an eigenvalue from the adjacency matrix of Γ, it follows, using the rational root test, that λ_n^Γ is an integer. Thus $(k-1)$ divides $\bar{\partial}(\Gamma)$.

Further from Equation (4.1) we conclude that $\lambda_n^\Gamma = -\bar{\partial}(\Gamma)/(k-1)$. □

Chapter 5

Synchronization and Generalized Paley Graphs

In this chapter we will present an interesting class of graphs, the Paley graphs, constructed from finite fields. These graphs are named after Raymond Paley, a mathematician who died young in 1933 in an avalanche in Canada. After the definition made by Paley [Pal33], a generalization of these graphs was developed. See for instance [LP09].

Paley graphs are very important for our study of synchronization in affine groups since some undirected orbital graphs in Chapter 4 associated with these groups are generalized Paley graphs. Hence we will study these graphs, in particular their clique and chromatic numbers, which are the properties involved in the characterization in Theorem 4.2.4 of synchronizing groups using graphs.

Since generalized Paley graphs are built using finite fields, we start this chapter by summarizing the general theory of finite fields necessary for the construction of these graphs and further, in Chapter 6, to describe some subgroups of $\mathsf{GL}(2, p)$.

5.1 Finite Fields

For any field $\mathbb{F}$, we denote by $\mathbb{F}^*$ the set $\mathbb{F}\backslash\{0\}$ viewed as an abelian multiplicative group. We present a proposition which states the properties of finite fields that will be used in this dissertation. These properties can be found in Chapter 5.5 of [Hun80].

Proposition 5.1.1. *1. The order of a finite field is a power of a prime.*

2. For every prime-power q there exists a field with q elements.

3. If $\mathbb{F}$ and $\mathbb{K}$ are finite fields with q elements then $\mathbb{F} \cong \mathbb{K}$.

4. A field $\mathbb{F}$ of p^k elements, where p is a prime and $k \in \mathbb{N}$, contains a subfield $\mathbb{K}$ of p^d elements if and only if d is a divisor of k. In this case $\mathbb{K}$ is unique and $\mathbb{F}$ can be considered as a (k/d)-dimensional vector space over $\mathbb{K}$.

5. A finite subgroup of the multiplicative group of every field is cyclic.

For a prime power q, we let $\mathbb{F}_q$ denote the field of q elements, which, by the third statement of Proposition 5.1.1, is uniquely determined up to isomorphism. If p is a prime then $\mathbb{F}_p$ is usually identified with the set $\{0, \ldots, p-1\}$, in which the addition and the multiplication are performed modulo p.

To set up notation, we proceed to the construction of finite fields with p^k elements. Let $\mathbb{F}_p$ be the finite field with p elements and consider an irreducible polynomial $f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0$ over $\mathbb{F}_p$. Then the quotient ring $\mathbb{F}_p[x]/(f)$, where (f) is the ideal generated by f, is a field with p^k elements. By the third property of Proposition 5.1.1, the isomorphism type of this field is independent of f. Hence we identify $\mathbb{F}_{p^k}$ with the ring $\mathbb{F}_p[x]/(f)$. The elements of $\mathbb{F}_{p^k}$ are cosets of the form $g+(f)$ and let us denote such a coset by $[g]_f$. Every coset $[g]_f$ contains a unique element g_1 with degree at most $k-1$ and so $[g]_f = [g_1]_f$. Hence $\mathbb{F}_{p^k} = \{[\alpha_{k-1}x^{k-1} + \ldots + \alpha_0]_f : \alpha_{k-1}, \cdots, \alpha_0 \in \mathbb{F}_p\}$.

Example 5.1.2. Let us present the construction of the field $\mathbb{F}_9$. Since $9 = 3^2$, we consider the field $\mathbb{F}_3$ and an irreducible polynomial of degree two over $\mathbb{F}_3$. For instance, consider $f(x) = x^2 + 1$. Then $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$ is a field with 9 elements. Denoting by i, as in $\mathbb{C}$, a root in $\mathbb{F}_9$ of x^2+1 we write the elements of $\mathbb{F}_9$ in the form $\alpha + \beta i$, with $\alpha, \beta \in \mathbb{F}_3$.

By Statement 5 of Proposition 5.1.1, we have that $\mathbb{F}_9^*$ is cyclic. Since $i^2 = -1$ it follows that $i^4 = 1$ which means that i generates a proper subgroup of order 4 in $\mathbb{F}_9^*$. Since $\mathbb{F}_9^*$ has only one maximal subgroup, namely $\langle i \rangle$, and $1 + i \notin \langle i \rangle$, we obtain that $\mathbb{F}_9^* = \langle 1 + i \rangle$.

Multiplication of elements of the form $\alpha + \beta i$ is performed using the fact that $i^2 = -1$. For instance $2i(1 + 2i) = 2i + 4i^2 = 2i - 4 = 2i + 2$.

Continuing with the notation introduced before Example 5.1.2 we have that the elements of the form $[0x^{k-1}+\ldots+0x+\beta]_f$ form a subfield of $\mathbb{F}_{p^k}$ with p elements and by Statement 4 of Proposition 5.1.1, $\mathbb{F}_{p^k}$ is a k-dimensional vector space over $\mathbb{F}_p$. The set $\{[1]_f, [x]_f, [x^2]_f, \ldots, [x^{k-1}]_f\}$ is an $\mathbb{F}_p$-basis for $\mathbb{F}_{p^k}$. In the case where $k = 2$, if $\gamma \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ the set $\{1, \gamma\}$ is an $\mathbb{F}_p$-basis for $\mathbb{F}_{p^2}$.

If $\mathbb{F}_q$ is the field with q elements, where $q = p^n$ and p is a prime, then we have that $\beta^q = \beta$ for all $\beta \in \mathbb{F}_q$. Furthermore the map

$$\varphi : \mathbb{F}_q \to \mathbb{F}_q \text{ defined by } \beta \mapsto \beta^p$$

is an automorphism of the field $\mathbb{F}_q$. This automorphism is called the *Frobenius automorphism* after Ferdinand Frobenius. We have that φ is a $\mathbb{F}_p$-linear map; that is, a map that satisfies the following properties:

1. $(\beta_1 + \beta_2)\varphi = \beta_1\varphi + \beta_2\varphi$, for all $\beta_1, \beta_2 \in \mathbb{F}_q$.

2. $(\alpha\beta)\varphi = \alpha(\beta\varphi)$, for all $\beta \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_p$.

We have, by Statement 4 of Proposition 5.1.1, that $\mathbb{F}_q$ can be regarded as a n-dimensional vector space over the prime field $\mathbb{F}_p$. Hence, if we fix a basis for $\mathbb{F}_q$ over $\mathbb{F}_p$, as the Frobenius automorphism is an $\mathbb{F}_p$-linear map, then we can consider φ as an element of $\mathsf{GL}(n, p)$, the group of $n \times n$ invertible matrices over $\mathbb{F}_p$. We will use the Frobenius automorphism in our further study of irreducible subgroups of the general linear group in Chapter 6.

5.2 Generalized Paley Graphs

Let q be a prime-power number such that $q \equiv 1 \pmod 4$. Let $\mathbb{F}_q$ be the field with q elements and set $S = \{\alpha^2 : \alpha \in \mathbb{F}_q^*\}$, the set of non-zero square elements of $\mathbb{F}_q$. Let $V = \mathbb{F}_q$ and $E = \{\{\alpha, \beta\} \in \mathbb{F}_q^{\{2\}} : \alpha - \beta \in S\}$. We observe that since $q \equiv 1 \pmod 4$, we have that $-1 \in S$. Therefore the set S is well defined because $\alpha - \beta = -1(\beta - \alpha)$, which means, as -1 is a square in $\mathbb{F}_q$, that $\alpha - \beta$ is a square in $\mathbb{F}_q$ if and only if $\beta - \alpha$ is a square in $\mathbb{F}_q$. The *Paley graph of the finite field* $\mathbb{F}_q$, denoted by $\Gamma_{q,2}$, is the graph with vertex-set V and edge-set E. Some examples of Paley graphs are displayed in Figure 5.1.

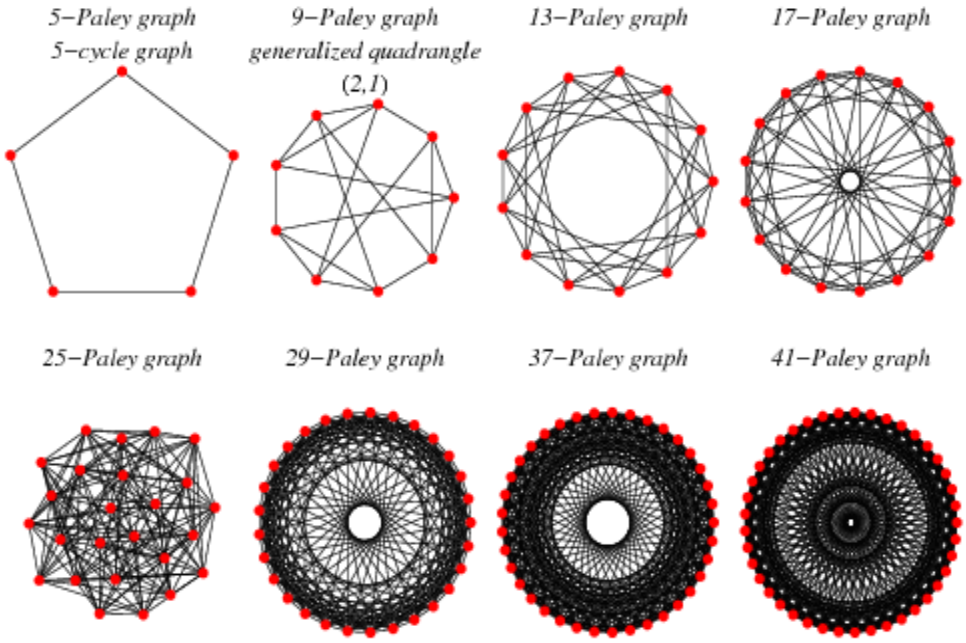


Figure 5.1: The Paley graphs of the fields with small number of elements. **Source:** Weisstein, Eric W. "Paley Graph." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/PaleyGraph.html

Let q be a prime-power and $m \geq 2$ be a divisor of $q-1$ such that $2m|q-1$. Set $S_{q,m} = \{\alpha^m : \alpha \in \mathbb{F}_q^*\}$. Then $S_{q,m} \leq \mathbb{F}_q^*$ and $|S_{q,m}| = (q-1)/m$. Since $2m$ divides $q-1$, we have that $-1 \in S_{q,m}$. Consider the graph $\Gamma_{q,m}$ with vertex-set $\mathbb{F}_q$ and edge-set E defined by $\{\alpha, \beta\} \in E$ if and only if $\alpha - \beta \in S_{q,m}$. As before, this set is well defined because $-1 \in S_{q,m}$. We call $\Gamma_{q,m}$ the *generalized Paley graph of the field* $\mathbb{F}_q$ *with index* m. We remark that the two definitions of $\Gamma_{q,2}$ given in this section are identical.

In the next proposition we present some properties of generalized Paley graphs. As observed before, these graphs will turn out to be undirected orbital graphs for some affine permutation groups. Therefore we must verify that these graphs are symmetric for applying the theory of Chapter 4. In particular, in this proposition, we prove that these graphs are vertex-transitive and edge-transitive (see Section 4.1, after Example 4.1.1, for the definitions).

Proposition 5.2.1. *Let q be a prime-power and $m \in \mathbb{N}$ such that the generalized Paley graph $\Gamma_{q,m}$ is defined. Then*

1. *$\Gamma_{q,m}$ is isomorphic to a subgraph of its complement graph $\Gamma'_{q,m}$.*
2. *If $\alpha \in \mathbb{F}_q$ and $\beta \in S_{q,m}$ then the map $\psi_{\alpha,\beta}$ defined by $\delta \mapsto \beta\delta + \alpha$ is an automorphism of $\Gamma_{q,m}$.*
3. *$\Gamma_{q,m}$ is vertex-transitive and edge-transitive.*
4. *$\Gamma_{q,m}$ is a regular graph and $\bar{\partial}(\Gamma_{q,m}) = (q-1)/m$.*

Proof. Let q and m be parameters such that the generalized Paley graph $\Gamma_{q,m}$ is defined and let γ be a generator of $\mathbb{F}^*_{p^2}$.

We prove Statement 1. Define the map $\varsigma : \mathbb{F}_q \to \mathbb{F}_q$ as $\alpha \mapsto \alpha\gamma$ for every element $\alpha \in \mathbb{F}_q$. It is easy to see that ς is a bijection. Now we observe that if δ_1, δ_2 are connected vertices in $\Gamma_{q,m}$ then $\delta_1 - \delta_2 \in S_{q,m}$. Therefore we have that $\delta_1\varsigma - \delta_2\varsigma = (\delta_1 - \delta_2)\gamma \in S_{q,m}\gamma$. Since $\gamma \notin S_{q,m}$, we obtain that $S_{q,m}\gamma$ is a non-trivial coset of $S_{q,m}$ in $\mathbb{F}^*_q$. Thus $S_{q,m} \cap S_{q,m}\gamma = \emptyset$. This means that $\delta_1\varsigma$ and $\delta_2\varsigma$ are not connected in $\Gamma_{q,m}$. Hence they are connected in its complement graph $\Gamma'_{q,m}$. Therefore ς is a injective homomorphism from $\Gamma_{q,m}$ to $\Gamma'_{q,m}$. Thus the generalized Paley graph $\Gamma_{q,m}$ is isomorphic to a subgraph of $\Gamma'_{q,m}$.

Next, we prove the second statement. Let us fix $\alpha, \beta \in \mathbb{F}_q$ such that $\beta \in S_{q,m}$ and define the map $\psi_{\alpha,\beta} : \mathbb{F}_q \to \mathbb{F}_q$ by $\delta \mapsto \beta\delta + \alpha$. We will prove that $\psi_{\alpha,\beta}$ is a graph automorphism. We claim that $\psi_{\alpha,\beta}$ is injective. Let $\delta_1, \delta_2 \in \mathbb{F}_q$ such that $\delta_1\psi_{\alpha,\beta} = \delta_2\psi_{\alpha,\beta}$. Then

$$0 = \delta_1\psi_{\alpha,\beta} - \delta_2\psi_{\alpha,\beta} = (\beta\delta_1 + \alpha) - (\beta\delta_2 + \alpha) = \beta(\delta_1 - \delta_2).$$

Since $\beta \neq 0$ we find that $\delta_1 = \delta_2$. On the other hand, for every $\delta \in \mathbb{F}_q$, we have that $\beta^{-1}\delta - \beta^{-1}\alpha \in \mathbb{F}_q$ and $(\beta^{-1}\delta - \beta^{-1}\alpha)\psi_{\alpha,\beta} = \delta$. Therefore $\psi_{\alpha,\beta}$ is onto. To conclude that $\psi_{\alpha,\beta}$ is a graph automorphism, it remains to show that it is a graph homomorphism. Let $\delta_1, \delta_2 \in \mathbb{F}_q$. We have that

$$\delta_1\psi_{\alpha,\beta} - \delta_2\psi_{\alpha,\beta} = (\beta\delta_1 + \alpha) - (\beta\delta_2 + \alpha) = \beta(\delta_1 - \delta_2) + \alpha - \alpha = \beta(\delta_1 - \delta_2).$$

As $\beta \in S_{q,m}$, we have that $\delta_1\psi_{\alpha,\beta} - \delta_2\psi_{\alpha,\beta} \in S_{q,m}$ if and only if $\delta_1 - \delta_2 \in S_{q,m}$. Hence $\delta_1\psi_{\alpha,\beta}$ and $\delta_2\psi_{\alpha,\beta}$ are connected in $\Gamma_{q,m}$ if and only if δ_1 and δ_2 are connected in $\Gamma_{q,m}$. Thus $\psi_{\alpha,\beta} \in \mathrm{Aut}(\Gamma_{q,m})$.

Let us prove Statement 3. We begin by proving that the graph $\Gamma_{q,m}$ is vertex-transitive. Let $\delta_1, \delta_2 \in \mathbb{F}_q$. Then $\psi_{\delta_2-\delta_1,1}$ defined in Statement 2,

is an automorphism of the graph $\Gamma_{q,m}$ such that $\delta_1\psi_{\delta_2-\delta_1,1} = \delta_2$. Therefore the graph $\Gamma_{q,m}$ is vertex-transitive. Next, we prove that this graph is edge-transitive. Let $\{\alpha_1, \delta_1\}, \{\alpha_2, \delta_2\}$ be edges of the graph $\Gamma_{q,m}$. We already proved that this graph is vertex-transitive, therefore we can assume without loss of generality that $\alpha_1 = \alpha_2 = 0$. Hence it is suffice to prove that given two edges $e_1 = \{0, \delta_1\}$ and $e_2 = \{0, \delta_2\}$ there exists an element $g \in \mathrm{Aut}(\Gamma_{q,m})$ such that $e_1 g = e_2$. By the definition of $\Gamma_{q,m}$, there exists i and $j \in \mathbb{N}$ such that $\delta_1 = \gamma^{mi}$ and $\delta_2 = \gamma^{mj}$. Then the map $\psi_{0,\gamma^{m(j-i)}}$ defined in Statement 2 is an automorphism of $\Gamma_{q,m}$ such that $e_1\psi_{\alpha,\beta} = \{0, \delta_1\}\psi_{\alpha,\beta} = \{0, \delta_2\} = e_2$. Thus the graph $\Gamma_{q,m}$ is edge-transitive.

Now we prove the last statement. Since $\Gamma_{q,m}$ is vertex-transitive, we obtain that this is a regular graph. We claim that $\bar{\partial}(\Gamma_{q,m}) = (q-1)/m$. By definition of $\Gamma_{q,m}$ we have that α is a neighbor of 0 if and only if $\alpha \in S_{q,m}$. Hence the vertex 0 has $|S_{q,m}| = (q-1)/m$ neighbors. Since this graph is regular, every vertex has the same number of neighbors as the vertex 0. Thus $\bar{\partial}(\Gamma_{q,m}) = (q-1)/m$. □

The study of graphs developed in Chapter 4 in terms of the synchronization property was about the clique and chromatic numbers. Thus we present the next results which give us some properties of this numbers in generalized Paley graphs.

Theorem 5.2.2 (Theorem 1 of [BDR88])**.** *Let p be an odd prime and $n \in \mathbb{N}$. Let $m \neq 1$ such that $m \mid (p^n-1)/(p-1)$. Then*

$$p^d \leq \omega(\Gamma_{p^n,m})) \leq \chi(\Gamma_{p^n,m})) \leq \chi(\Gamma'_{p^n,m}) \leq p^{n-d},$$

where d is any divisor of n such that $m \mid (p^n-1)/(p^d-1)$.

Proof. Let γ be a generator of $\mathbb{F}^*_{p^n}$. Since d divides n, by Statement 4 of Proposition 5.1.1, there exists a subfield $\mathbb{K}$ of $\mathbb{F}_{p^n}$ such that $\mathbb{K}$ has p^d elements. Further, we have that $\mathbb{K}^*$ is a multiplicative subgroup of $\mathbb{F}^*_{p^n}$ with index $(p^n-1)/(p^d-1)$. As $\mathbb{F}^*_{p^n}$ is cyclic and generated by γ, it follows that $\mathbb{K}^* = \left\langle \gamma^{(p^n-1)/(p^d-1)} \right\rangle$.

We have that $m \mid (p^n-1)/(p^d-1)$ by assumption, therefore the elements of $\mathbb{K}^*$ lie in the set $S_{p^n,m}$. In particular, since $-1 \in \mathbb{K}$ it follows that $-1 \in S_{p^n,m}$ and so the graph $\Gamma_{p^n,m}$ is defined. As $\mathbb{K}$ is additively closed, the elements of $\mathbb{K}$ form a clique on $\Gamma_{p^n,m}$. Thus $p^d \leq \omega(\Gamma_{p^n,m})$. By the first statement of

Proposition 5.2.1, $\Gamma_{p^n,m}$ is isomorphic to a subgraph of $\Gamma'_{p^n,m}$ and therefore $\chi(\Gamma_{p^n,m}) \leq \chi(\Gamma'_{p^n,m})$.

To complete the proof of the theorem we want to get an upper bound for the chromatic number of $\Gamma'_{p^n,m}$. As observed before, $\mathbb{K}$ is a clique in $\Gamma_{p^n,m}$. Hence $\mathbb{K}$ is an independence set in $\Gamma'_{p^n,m}$. Similarly, every additive coset $\mathbb{K} + \gamma^i$ of $\mathbb{K}$ in $\mathbb{F}_{p^n}$ is an independence set of vertices in $\Gamma'_{p^n,m}$. Therefore the p^{n-d} cosets of $\mathbb{K}$ in $\mathbb{F}_{p^n}$ form a colouring on $\Gamma'_{p^n,m}$, which implies that $\chi(\Gamma'_{p^n,m}) \leq p^{n-d}$. Since we have that $\omega(\Gamma_{p^n,m}) \leq \chi(\Gamma_{p^n,m})$, it follows that $p^d \leq \omega(\Gamma_{p^n,m}) \leq \chi(\Gamma_{p^n,m}) \leq \chi(\Gamma'_{p^n,m}) \leq p^{n-d}$. □

5.3 Synchronization and Generalized Paley Graphs

In Chapter 6 we will mainly be interested in the study of synchronization in 2-dimensional affine groups, which are groups that act on a set with p^2 elements, where p is a prime. Therefore in this section we will consider generalized Paley graphs constructed from fields with p^2 elements.

In Section 4.2 we established a criterion which connects the synchronization property to the suitability in graphs. Thus we present a result about the suitability in generalized Paley graphs.

Proposition 5.3.1. *Let p be an odd prime and $m \in \mathbb{N}$ such that the generalized Paley graph $\Gamma_{p^2,m}$ is defined. If $\Gamma_{p^2,m}$ is non-suitable then its complement graph $\Gamma'_{p^2,m}$ is non-suitable.*

Proof. Let us assume that the generalized Paley graph $\Gamma_{p^2,m}$ is non-suitable. Then either $\omega(\Gamma_{p^2,m}) \neq p$ or $\chi(\Gamma_{p^2,m}) \neq p$. If $\omega(\Gamma_{p^2,m}) \neq p$ then since p is the only proper divisor of p^2, we have that $\omega(\Gamma_{p^2,m})\omega(\Gamma'_{p^2,m}) \neq p^2$. Hence the graph $\Gamma_{p^2,m}$ is not pseudo-suitable and by Statement 1 of Proposition 4.2.3, we obtain that $\Gamma'_{p^2,m}$ is not pseudo-suitable. It follows from Statement 2 of the same proposition that $\Gamma'_{p^2,m}$ is a non-suitable graph since a suitable graph is pseudo-suitable.

Now let us suppose that $\omega(\Gamma_{p^2,m}) = p$ and $\chi(\Gamma_{p^2,m}) \neq p$. As the chromatic number of a graph is greater or equal to its clique number, we obtain that $\chi(\Gamma_{p^2,m}) > p$. From Statement 1 of Proposition 5.2.1, we have that $\Gamma_{p^2,m}$ is isomorphic to a subgraph of $\Gamma'_{p^2,m}$. Hence there is a subgraph of $\Gamma'_{p^2,m}$ with chromatic number bigger than p. Thus $\chi(\Gamma'_{p^2,m}) > p$ which implies that

graph $\Gamma'_{p^2,m}$ is non-suitable. In both cases we concluded the non-suitability of $\Gamma'_{p^2,m}$. □

Next, we present a necessary and sufficient condition for suitability in generalized Paley graphs of fields with p^2 elements.

Theorem 5.3.2. *Let p be an odd prime and $m \in \mathbb{N}$ such that the generalized Paley graph $\Gamma_{p^2,m}$ is defined. We have that $\Gamma_{p^2,m}$ is suitable if and only if $m \mid p+1$.*

Proof. If $m \mid p+1$ then it follows from Theorem 5.2.2, considering $n = 2$ and $d = 1$, that $\Gamma_{p^2,m}$ is a suitable graph. Let us now prove the other direction. Let us assume that $\Gamma_{p^2,m}$ is a suitable graph. Since the graph $\Gamma_{p^2,m}$ is not complete and p is the only proper divisor of p^2, from Statement 1 of Theorem 4.3.1 we obtain that $\omega(\Gamma_{p^2,m}) = p$. Since $\Gamma_{p^2,m}$ is suitable, we also conclude that $\chi(\Gamma_{p^2,m}) = p$. By Statement 3 of Proposition 5.2.1, the graph $\Gamma_{p^2,m}$ is vertex-transitive and edge-transitive. Therefore we can apply Theorem 4.4.3, which states that $p-1$ divides $\bar{\partial}(\Gamma_{p^2,m})$, where $\bar{\partial}(\Gamma_{p^2,m})$ is the number of neighbors of a vertex in $\Gamma_{p^2,m}$. By the last statement of Proposition 5.2.1, we know that $\bar{\partial}(\Gamma_{p^2,m}) = (p^2-1)/m$. Therefore we obtain that $p-1$ divides $(p^2-1)/m$, which means that $(p-1)a = (p^2-1)/m = (p-1)(p+1)/m$ for some $a \in \mathbb{Z}$. Thus we conclude that $ma = p+1$ for some $a \in \mathbb{Z}$ and hence m divides $p+1$. □

After an arithmetic condition for suitability in generalized Paley graphs, we will describe a maximal clique and a minimal coloring for these suitable graphs.

Proposition 5.3.3. *Let p be an odd prime and consider the generalized Paley graph $\Gamma_{p^2,m}$ such that $m \mid p+1$. Let γ be a generator of $\mathbb{F}_{p^2}^*$. Then*

1. *The subfield $\mathbb{F}_p$ is a clique in $\Gamma_{p^2,m}$.*
2. *The partition $\{\{\alpha + \beta\gamma : \beta \in \mathbb{F}_p\} : \alpha \in \mathbb{F}_p\}$ of $\mathbb{F}_{p^2}$ is a coloring for the graph $\Gamma_{p^2,m}$.*

Proof. We first observe that if $m \mid p+1$ then the generalized Paley graph $\Gamma_{p^2,m}$ is defined. Indeed, as p is odd, $p-1$ is even and hence $2 \mid p-1$. Therefore $2m \mid p^2-1$ which is the condition for the graph to be defined.

As $p^2-1=(p-1)(p+1)$, we have that $\mathbb{F}_p^* = S_{p^2,p+1}$. Since $m \mid p+1$, we obtain that $\mathbb{F}_p^* \leq S_{p^2,m}$. The argument in the proof of Theorem 5.2.2 with $n=2$ and $d=1$ implies that the subfield $\mathbb{F}_p$ is a clique in $\Gamma_{p^2,m}$.

Next, we prove that the partition

$$\{\{\alpha+\beta\gamma : \beta \in \mathbb{F}_p\} : \alpha \in \mathbb{F}_p\}$$

of $\mathbb{F}_{p^2}$ is a coloring for the graph $\Gamma_{p^2,m}$. We must show that for every element $\alpha \in \mathbb{F}_p$ the elements of the set $\{\alpha+\beta\gamma : \beta \in \mathbb{F}_p\}$ are not connected in $\Gamma_{p^2,m}$. Let us fix $\alpha \in \mathbb{F}_p$ and consider the set $A = \{\alpha+\beta\gamma : \beta \in \mathbb{F}_p\}$. Let $\delta_1, \delta_2 \in A$. We claim that $\{\delta_1, \delta_2\}$ is not an edge of $\Gamma_{p^2,m}$. We have that $\delta_1 = \alpha+\beta_1\gamma$ and $\delta_2 = \alpha+\beta_2\gamma$ with $\beta_1, \beta_2 \in \mathbb{F}_p$ such that $\beta_1 \neq \beta_2$. Then $\delta_2 - \delta_1 = (\beta_2-\beta_1)\gamma$. Since $\beta_2-\beta_1 \in \mathbb{F}_p^*$, by the argument above, we obtain that $\beta_2-\beta_1 \in S_{p^2,m}$. Hence $\delta_2-\delta_1 \in S_{p^2,m}\gamma$. Since $\gamma \notin S_{p^2,m}$, we have that $S_{p^2,m}\gamma$ is a non-trivial coset of $S_{p^2,m}$ in $\mathbb{F}_{p^2}^*$. Thus $S_{p^2,m}\gamma \cap S_{p^2,m} = \emptyset$. Therefore $\{\delta_1, \delta_2\}$ is not an edge in the graph $\Gamma_{p^2,m}$. Then for all $\alpha \in \mathbb{F}_p$ the elements of the set $\{\alpha+\beta\gamma : \beta \in \mathbb{F}_p\}$ form a color for the graph $\Gamma_{p^2,m}$. Hence the partition $\{\{\alpha+\beta\gamma : \beta \in \mathbb{F}_p\} : \alpha \in \mathbb{F}_p\}$ is a coloring for this graph. □

In this dissertation we are interested in generalized Paley graphs associated with maximal subgroups of the multiplicative group of a field. This particular interest is justified by the fact that the absence of synchronization is preserved by the subgroups of a given group. We now present the lattice diagrams of the subgroups of the multiplicative groups of the fields with p^2 elements, with p under 25. For each maximal subgroup, we consider the corresponding generalized Paley graph. The green arrows mean that the corresponding generalized Paley graph is suitable while the red crosses mean that this graph is non-suitable.

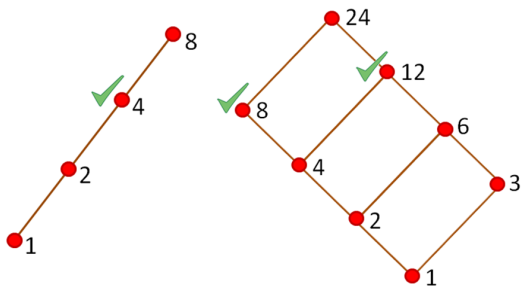


Figure 5.2: The lattice of the divisors of 8 and 24.

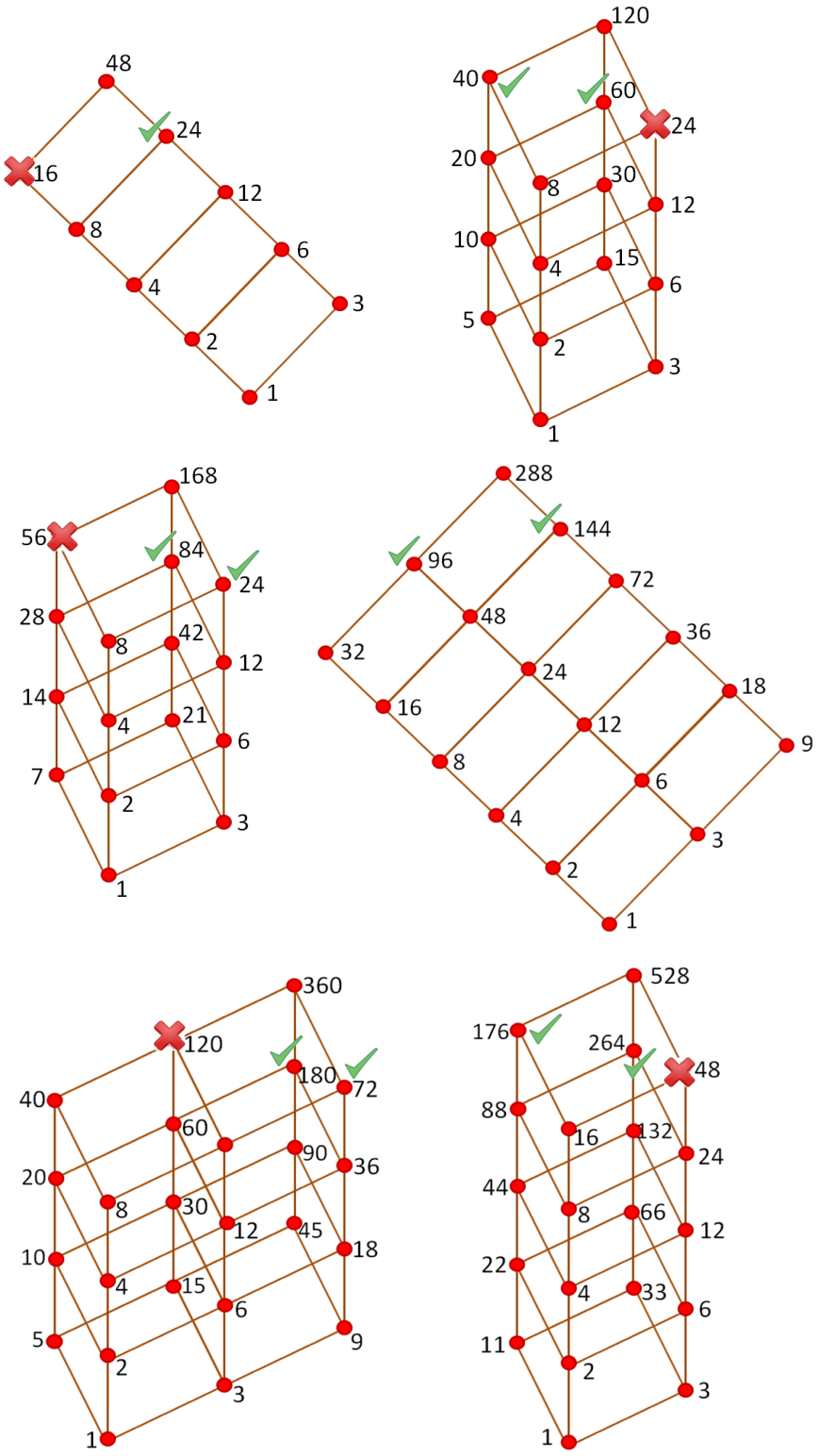


Figure 5.3: The lattice of the divisors of 48, 120, 168, 288, 360 and 528.

Chapter 6

Low-Dimensional Affine Synchronizing Groups

In this chapter we will study low-dimensional permutation groups of affine type. The affine permutation groups constitute an infinite family which arise naturally from affine geometries and are built using a vector space and a matrix group component.

We will construct these groups and present some of their elementary properties. Since we are concerned with the synchronization property in these groups, we must consider primitive affine groups. Therefore we state Theorem 6.2.1, that connects the primitivity property of these groups to the irreducibility of their matrix group components. Then we briefly describe the irreducible subgroups of $\mathsf{GL}(2, p)$ in order to characterize the affine groups in dimension 2.

From a result of Pin stated as [Pin78, Théorème 2], we obtain that the one-dimensional affine groups are always synchronizing. Therefore, the next task in the the study of this class of groups is the study of two-dimensional affine groups, which will be carried out in Section 6.5.

6.1 Construction of an Affine Group

Let V be an n-dimensional vector space over the field $\mathbb{F}_q$, where q is a prime-power. Let H be a subgroup of $\mathsf{GL}(V)$, the group of invertible transformations of the vector space V, which can be considered as a subgroup of $\mathsf{Sym}(V)$. For any element $v \in V$, define $\sigma_v \in \mathsf{Sym}(V)$ as follows: $u\sigma_v = u + v$ for all $u \in V$.

The set $T = \{\sigma_v : v \in V\}$ is a subset of $\mathsf{Sym}(V)$ and since we have, for all $v_1, v_2 \in V$, that

$$\sigma_{v_1}\sigma_{v_2} = \sigma_{v_1+v_2}, \tag{6.1}$$

the set T is closed under composition and therefore $T \leq \mathsf{Sym}(V)$. Then the affine group corresponding to V and H is

$$G = \langle T, H \rangle.$$

Thus G is a subgroup of $\mathsf{Sym}(V)$. An *affine permutation group* is a group that is constructed this way.

We will prove in the next lemma that the affine groups are internal semidirect products. If H and K are subgroups of a group G then G is a *semidirect product of K by H*, denoted by $G = K \rtimes H$, if K is normal in G, $H \cap K = 1$ and $G = KH$.

Example 6.1.1. Let us consider the group $D_6 = \langle (12), (123) \rangle$ and its subgroups $K = \langle (123) \rangle$ and $H = \langle (12) \rangle$. We have that H normalizes K, K is normal in D_6, $H \cap K = 1$ and $D_6 = KH$. Hence $D_6 = K \rtimes H$.

Lemma 6.1.2. *Let $T, H \leq \mathsf{Sym}(V)$ defined as above and let G be the corresponding affine group. Then the following hold:*

1. *T is an abelian regular normal subgroup of G, which is isomorphic to V, regarded as an abelian group;*
2. *H normalizes T;*
3. *$T \cap H = 1$;*
4. *$G = TH = HT$ and $|G| = |T||H| = |V||H|$. Further $G = T \rtimes H$;*
5. *The stabilizer of the zero vector, G_0, is equal to H.*

Proof. Let us prove the first statement. The map $v \mapsto \sigma_v$ is a homomorphism by Equation (6.1) and it is easy to see that this map is a bijection. Hence V is isomorphic to T. Therefore, as V is abelian, we conclude that the group T is also abelian. On the other hand, the group T is transitive since for all $u, v \in V$, we have that $u\sigma_{v-u} = v$. As T is a transitive and abelian group, by Proposition 2.2.2 we conclude that T is a regular group.

Next, we prove Statement 2. Let $\sigma_v \in T$ and $h \in H$. For any $u \in V$, we have that

$$u(h^{-1}\sigma_v h) = (uh^{-1} + v)h = u + vh = u\sigma_{vh}.$$

Thus $h^{-1}\sigma_v h = \sigma_{vh}$ and T is normalized by H.

Let us now prove Statement 3. Since the elements of H fix the zero vector, $T \cap H$ must stabilize 0. By Statement 1, T is a regular group and hence $T_0 = 1$. Thus, we obtain that $H \cap T \leq T_0 = 1$. Hence $H \cap T = 1$. Statement 4 is a consequence of Statements 2 and 3 and the definition of the semidirect product.

To prove that $G_0 = H$ we observe that $H \leq G_0$. Conversely let $g \in G_0$. By Statement 4 we have that $g = \sigma_v h$ for some $\sigma_v \in T$ and $h \in H$. Then $0 = 0g = 0(\sigma_v h) = (0 + v)h = vh$. If $v \neq 0$ then $vh \neq 0$. Hence $g \in H$ and we conclude that $G_0 = H$. □

From Statement 2 of Lemma 6.1.2, if we consider $T, H \leq \mathsf{Sym}(V)$ defined as above, then the corresponding affine group G can be written simply by

$$G = HT = \{x \mapsto xh + v : h \in H, v \in V\}.$$

Since T is a transitive group, the affine permutation group G is also transitive. Further, if V is an n-dimensional vector space over $\mathbb{F}_p$ then fixing a basis for V over $\mathbb{F}_p$, we have that $\mathsf{GL}(V) \cong \mathsf{GL}(n, p)$. Therefore, in the construction of an affine group, we can consider H as a subgroup of $\mathsf{GL}(n, p)$.

Since a vector space over the field $\mathbb{F}_{p^k}$ can be regarded as a vector space over $\mathbb{F}_p$, where p is a prime, we will usually consider the underlying vector space of an affine group over $\mathbb{F}_p$.

6.2 Primitive and Synchronizing Affine Groups

From Statement 1 of Theorem 3.1.1, we know that a synchronizing permutation group is primitive. Therefore, to study synchronization, we are interested in primitive affine groups. Hence we must start by a criterion for deciding if an affine group is primitive.

Let V be an n-dimensional vector space over $\mathbb{F}_p$, with a prime p. As observed before, if we choose a basis for V over $\mathbb{F}_p$ then $\mathsf{GL}(V) \cong \mathsf{GL}(n, p)$. Hence, in this dissertation, we will consider subgroups of $\mathsf{GL}(n, p)$. Let $H \leq \mathsf{GL}(n, p)$ be a linear group and W be a subspace of V. We say that W is an *H-invariant subspace* of V if for all $h \in H$ and $w \in W$ we have that

$wh \in W$. For instance $W = 0$ and $W = V$ are always invariant subspaces for every subgroup of the general linear group which are called the *trivial subspaces* of V. A matrix group $H \leq \mathsf{GL}(2, p)$ is said to be *reducible* if there is a non-trivial H-invariant subspace W of V. Otherwise, H is called *irreducible*.

The next theorem states a criterion for an affine group to be primitive.

Theorem 6.2.1. *Let V be an n-dimensional vector space over the field $\mathbb{F}_p$, with a prime p. Let $H \leq \mathsf{GL}(n, p)$ and consider the corresponding affine group $G = T \rtimes H$. Then G is primitive if and only if H is irreducible.*

Proof. First let us suppose that G is a primitive group and let $W \leq V$ be an invariant subspace under H. It is required to prove that $W = 0$ or $W = V$. We claim that W is a block for G. Since W is H-invariant, we have that if $w \in W$ then $wh \in W$ for all $h \in H$. This implies that $Wh = W$. If $g \in G$ such that $g = h\sigma_v$, with $v \in V$ and $h \in H$, then

$$Wg = \{wh + v : w \in W\} = W + v.$$

Since $W + v$ is a coset of W in V, we know that either $W + v = W$, in the case that $v \in W$, or $(W + v) \cap W = \emptyset$, when $v \notin W$. This implies that W is a block for G. Since we assume that G is primitive, either $W = 0$ or $W = V$. Hence there are only trivial H-invariant subspaces of V. Thus H is irreducible.

Now let us prove the reverse direction. Assume that H is irreducible and let $B \subseteq V$ be a block for G. Without loss of generality, we can assume that $0 \in B$. We claim that B is a subspace of V. To prove that, as $0 \in B$ by assumption, it is necessary to show that B is closed under sum of vectors and multiplication by scalars. Let $u, v \in B$. We have that $0\sigma_v = v$. Hence $B \cap B\sigma_v \neq \emptyset$. As B is a block and $\sigma_v \in G$, we obtain that $B = B\sigma_v$. On the other hand, the vector $u + v = u\sigma_v$, therefore $u + v \in B\sigma_v$, which means that $u+v \in B$. Now suppose that $u \in B$ and let $\alpha \in \mathbb{F}_p$. Then $\alpha u = u+u+\ldots+u$, a sum of α terms. Since B is closed under addition of vectors, we have that $\alpha u \in B$. Therefore B is a subspace of V which is H-invariant since $0h = 0$ for all $h \in H$. Hence $Bh = B$ for all $h \in H$. Thus, as H is irreducible, it follows that $B = 0$ or $B = V$. Therefore G is a primitive group. □

By Theorem 6.2.1 the characterization of the affine primitive permutation groups is reduced to the study of irreducible subgroups of $\mathsf{GL}(n, p)$, with a prime p. The discussion of these irreducible subgroups of $\mathsf{GL}(2, p)$ will briefly be presented in the next section.

Next we state two results about the synchronization property in affine permutation groups.

Theorem 6.2.2 (Théorème 2 of [Pin78])**.** *An affine group acting on the elements of a one-dimensional vector space over a prime field is synchronizing.*

Proof. Let G be a group in the conditions of the theorem. Then the degree of G is equal to p, where p is a prime. Hence by Statement 1 of Proposition 3.1.3 a section-regular partition for G must be trivial. Therefore G is synchronizing. □

Theorem 6.2.2 was first proved in Pin's paper [Pin78] that was published long before Neumann's paper [Neu09] that contains the result that a section-regular partition is uniform. Thus the original proof given by Pin is significantly more complex.

Let V be an n-dimensional vector space over a field $\mathbb{F}_p$ and $H \leq \mathsf{GL}(n,p)$ be an irreducible matrix group. If the vector space V can be written as a direct sum $V = W_1 \oplus \cdots \oplus W_n$ of non-trivial subspaces W_i of V, with $n \geq 2$, such that for any W_i and $h \in H$ there exists W_j such that $W_i h \subset W_j$, then H is called an *imprimitive matrix group*. Otherwise H is said to be a *primitive matrix group*. Hence the imprimitive matrix groups are the ones which preserve a direct sum decomposition of the underlying vector space.

Example 6.2.3. Let $\mathbb{F}_p$ be the field with p elements, where p is a prime. Let V be a two-dimensional vector space over the field $\mathbb{F}_p$ and $\{e, f\}$ be a basis of V over $\mathbb{F}_p$. Let us consider the full monomial group of $\mathsf{GL}(2,p)$, which is denoted by $\mathsf{M}(2,p)$ and is defined as follows:

$$\mathsf{M}(2,p) = \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} : \alpha, \beta \in \mathbb{F}_p^* \right\} \cup \left\{ \begin{bmatrix} 0 & \alpha \\ \beta & 0 \end{bmatrix} : \alpha, \beta \in \mathbb{F}_p^* \right\}.$$

We claim that the group $\mathsf{M}(2,p)$ preserves a direct sum decomposition of the vector space V. Indeed, we have, for $g \in \mathsf{M}(2,p)$, that $eg = \alpha e$ and $fg = \beta f$ or $eg = \alpha f$ and $fg = \beta e$, for $\alpha, \beta \in \mathbb{F}_p$. Hence we obtain that $\mathsf{M}(2,p)$ preserves the direct sum decomposition $V = \langle e \rangle \oplus \langle f \rangle$. Thus, the group $\mathsf{M}(2,p)$ is an imprimitive matrix group.

From this definition of primitivity in matrix groups, we can conclude that in some cases the affine permutation groups are always non-synchronizing.

Theorem 6.2.4. *Let V be an n-dimensional vector space over the field $\mathbb{F}_p$, where p is a prime, and H be a subgroup of $\mathsf{GL}(n,p)$. Consider the group T of translations by elements of V and the corresponding affine group $G = \langle T, H\rangle$. If H is an imprimitive matrix group then G is non-basic and hence a non-synchronizing group.*

Proof. Let H be an imprimitive subgroup of $\mathsf{GL}(n,p)$. Let T be the group of translations by elements of V and consider the affine group $G = \langle T, H\rangle$. Since H is an imprimitive matrix group, we have that H preserves a decomposition $V = W_1 \oplus \cdots \oplus W_n$. Hence every element $v \in V$ can be written uniquely as $v = w_1 + \cdots + w_n$, where $w_i \in W_i$ and $i \in \{1, \ldots, n\}$.

Let $i \in \{1, \ldots, n\}$ and $w \in W_i$. Set

$$P_{i,w} = \{w_1 + \cdots + w_n \in V : w_i = w\}$$

and consider the partition $\mathscr{P}_i = \{P_{i,w} : w \in W_i\}$. Then consider the set of partitions $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_n\}$.

We claim that Σ is a Cartesian decomposition which is preserved by G. By the uniqueness of the decomposition of the elements of the vector space V as a sum of elements of the subspaces W_i, with $i \in \{1, \ldots, n\}$, we have, for $P_{i,w_i} \in \mathscr{P}_i$, that

$$\bigcap_{i \in \{1,\ldots,n\}} P_{i,w_i} = \{w_1 + \cdots + w_n\},$$

which has size one. Hence Σ is a Cartesian decomposition.

Now let us prove that the group G preserves Σ. Let $i \in \{1, \ldots, n\}$ and $P_{i,w} \in \mathscr{P}_i$, with $w \in W_i$. Let $v \in V$ and $\sigma_v \in T$. As observed before, v is uniquely written as $v = u_1 + \cdots + u_n$, with $u_j \in W_j$, for $j \in \{1, \ldots, n\}$. Then

$$\begin{aligned}
&P_{i,w}\sigma_v = \\
&= \{(w_1 + \cdots + w + \cdots + w_n) + (u_1 + \cdots + u_n) : w_j \in W_j \text{ for all } j \neq i\} \\
&= \{w_1 + \cdots + (w + u_i) + \cdots + w_n : w_j \in W_j \text{ for all } j \neq i\} \\
&= P_{i,w+u_i}.
\end{aligned}$$

Therefore σ_v preserves the partition $\mathscr{P}_i$, which means that the elements of T preserve Σ.

Now let $h \in H$. We have that

$$(w_1 + \cdots + w_i + \cdots + w_n)h = (w_1h + \cdots + w_ih + \cdots + w_nh).$$

Let $j \in \{1,\dots,n\}$ such that $W_i h = W_j$. This subspace exists since H preserves the direct sum decomposition $W_1 \oplus \cdots \oplus W_n$. Hence $P_{i,w}h = P_{j,w_i h}$, which is a part of the partition $\mathscr{P}_j$. Thus $\mathscr{P}_i h = \mathscr{P}_j$ and Σ is preserved by the elements of H. Therefore $G = \langle T, H\rangle$ preserves the Cartesian decomposition Σ and G is not basic. Thus, by Theorem 3.2.2, we conclude that G is a non-synchronizing group. □

Example 6.2.5. Let $\mathsf{M}(2,p)$ be the subgroup of $\mathsf{GL}(2,p)$ in Example 6.2.3 and let T be the group of translations of a 2-dimensional vector space over $\mathbb{F}_p$. Set $G = T \rtimes \mathsf{M}(2,p)$. Since $\mathsf{M}(2,p)$ is irreducible, the group G is primitive by Theorem 6.2.1. However, as $\mathsf{M}(2,p)$ is imprimitive, we have that G is non-basic by Theorem 6.2.4.

6.3 Irreducible Subgroups of $\mathsf{GL}(2,p)$

By Theorem 6.2.2, a one-dimensional affine group is synchronizing. The next step in our study is to consider 2-dimensional affine groups. From Theorem 6.2.1, we know that the 2-dimensional primitive affine groups are constructed from irreducible subgroups of $\mathsf{GL}(2,p)$. Flannery and O'Brien classified the irreducible subgroups of $\mathsf{GL}(n,q)$ for $n = 2, 3$ [FO05] and separated them in different types, based on Short's contribution to this subject [Sho92]. In this thesis we are interested in the case when $q = p$ and $n = 2$ in order to use their results for $\mathsf{GL}(2,p)$. We will follow the characterization of [FO05] as well as some properties given in Short [Sho92], and we will separate the irreducible subgroups of $\mathsf{GL}(2,p)$ into the classes of primitive and imprimitive matrix groups.

Let $\mathbb{F}_p$ be the field with p elements. We observe that from Statement 4 of Proposition 5.1.1 the field $\mathbb{F}_{p^2}$ can be regarded as a two-dimensional vector space over the prime field $\mathbb{F}_p$. Therefore, from now on, instead of considering a general two-dimensional vector space over $\mathbb{F}_p$, we will consider the vector space $\mathbb{F}_{p^2}$.

Let δ be an element of $\mathbb{F}_{p^2}^*$, the multiplicative group of the field $\mathbb{F}_{p^2}$, which is cyclic by the last statement of Proposition 5.1.1. Consider the transformation $\mu_\delta : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ defined by $\beta \mapsto \beta\delta$ for all $\beta \in \mathbb{F}_{p^2}$. Then μ_δ is an invertible $\mathbb{F}_p$-linear map on $\mathbb{F}_{p^2}$ and so, fixing a basis for $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, it can be considered as an element of $\mathsf{GL}(2,p)$. The subgroup $\{\mu_\delta : \delta \in \mathbb{F}_{p^2}^*\}$ of $\mathsf{GL}(2,p)$, denoted by Z_{p^2} is called a *Singer cycle* in $\mathsf{GL}(2,p)$ and has order

p^2-1. The group Z_{p^2} is isomorphic to $\mathbb{F}_{p^2}^*$ via the isomorphism $\delta \mapsto \mu_\delta$, and hence it is cyclic (see Statement 5 of Proposition 5.1.1).

Example 6.3.1. Let us show how to build a Singer cycle for the field $\mathbb{F}_9$. From Example 5.1.2 we know that $\mathbb{F}_9^* = \langle 1+i \rangle$, where $i^2 = -1$. Therefore we consider the map $\mu_{1+i} : \mathbb{F}_9 \to \mathbb{F}_9$ defined by $\beta\mu_{1+i} = \beta(1+i)$ for all $\beta \in \mathbb{F}_9$. It is clear that μ_{1+i} is an invertible $\mathbb{F}_3$-linear map.

Then as $\{1, i\}$ is a basis for $\mathbb{F}_9$ regarded as a 2-dimensional vector space over $\mathbb{F}_3$, if we consider the images of 1 and i under μ_{1+i}, we obtain a 2 by 2 matrix that generates Z_9 as a subgroup of $\mathsf{GL}(2,3)$. We have that $1\mu_{1+i} = 1+i$ and that $i\mu_{1+i} = i + i^2 = i + (-1) = 2 + i$. Therefore the matrix corresponding to μ_{1+i} is $\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$, which has order 8. The group $Z_9 = \left\langle \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \right\rangle$ is a Singer cycle in $\mathsf{GL}(2,3)$.

For each divisor m of Z_{p^2}, we can define $Z_{p^2,m}$ as $(Z_{p^2})^m$ and we set $r = (p^2-1)/m$ so that $|Z_{p^2,m}| = r$. Further, we have that $Z_{p^2,m}$ is an irreducible subgroup of $\mathsf{GL}(2,p)$ if and only if $r \nmid p-1$ [Sho92, Proposition 4.4.2] and it is primitive if and only if $r \nmid 2(p-1)$ [Sho92, Proposition 4.2.1].

Let us now consider another class of subgroups of $\mathsf{GL}(2,p)$. Let φ be the Frobenius automorphism $\beta \mapsto \beta^p$. As observed in Section 5.1, since φ is an $\mathbb{F}_p$-linear map, if we fix a basis for $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, then we can regard φ as an element of order 2 of $\mathsf{GL}(2,p)$. Let r be a divisor of p^2-1. Set $m = (p^2-1)/r$ and consider $Z_{p^2,m}$ as above. Further, define $\overline{Z_{p^2,m}} = \langle Z_{p^2,m}, \varphi \rangle$.

Lemma 6.3.2. *Let p be a prime and r be a divisor of p^2-1. Consider $\overline{Z_{p^2,m}}$ as above. Then the following hold:*

1. *φ normalizes $Z_{p^2,m}$;*
2. *$\langle \varphi \rangle \cap Z_{p^2,m} = 1$;*
3. *$\overline{Z_{p^2,m}} = Z_{p^2,m} \langle \varphi \rangle = Z_{p^2,m} \rtimes \langle \varphi \rangle$;*
4. *$|\overline{Z_{p^2,m}}| = 2r$;*
5. *$\overline{Z_{p^2,m}}$ is irreducible if and only if $r \nmid p-1$ and it is primitive if and only if $r \nmid 2(p-1)$.*

Proof. We start by proving that φ normalizes the full Singer cycle Z_{p^2}. Let $\beta \in \mathbb{F}_{p^2}$ and $\delta \in \mathbb{F}_{p^2}^*$. Since $\varphi^{-1} = \varphi$, we have that

$$\beta(\mu_\delta)^\varphi = \beta(\varphi^{-1}\mu_\delta\varphi) = \beta(\varphi\mu_\delta\varphi) = \beta^p(\mu_\delta\varphi) = (\beta^p\delta)\varphi = \beta^{p^2}\delta^p = \beta\mu_{\delta^p}.$$

Therefore we obtain, for all $\delta \in \mathbb{F}_{p^2}^*$, that $(\mu_\delta)^\varphi = \mu_{\delta^p} \in Z_{p^2}$. Hence φ normalizes the Z_{p^2}. Since Z_{p^2} is a cyclic group and for all m such that $m \mid p^2-1$, the subgroup $Z_{p^2,m}$ is the unique subgroup of Z_{p^2} with index m, we obtain that φ must normalize $Z_{p^2,m}$ for all such m.

Let us now prove that $\langle\varphi\rangle \cap Z_{p^2,m} = 1$. We claim that $\langle\varphi\rangle \not\leq Z_{p^2,m}$. Indeed, since $Z_{p^2,m}$ is a cyclic group it has at most one subgroup of order 2. If $|Z_{p^2,m}|$ is odd then there is no such subgroup. If $|Z_{p^2,m}|$ is even then it has a unique subgroup of order 2, namely $\langle\mu_{-1}\rangle$ and it is clear that $\langle\mu_{-1}\rangle \neq \langle\varphi\rangle$ since φ leaves the elements of $\mathbb{F}_p$ invariant and μ_{-1} does not. Therefore $\langle\varphi\rangle \cap Z_{p^2} = 1$. Statement 3 is a consequence from Statements 1 and 2.

For proving the statement about the order of $\overline{Z_{p^2,m}}$, we observe that

$$|\overline{Z_{p^2,m}}| = |\langle\varphi\rangle||Z_{p^2,m}|/|\langle\varphi\rangle \cap Z_{p^2}| = 2(p^2-1)/m = 2r.$$

Statement 5 is a consequence of Propositions 4.2.1 and 4.2.4 of [Sho92]. □

We note that if $S_{p^2,m}$ is the subgroup of $\mathbb{F}_{p^2}^*$ with index m, as defined in Section 5.2, then the Frobenius automorphism φ stabilizes $S_{p^2,m}$.

Next, we study another class of irreducible subgroups of $\mathsf{GL}(2,p)$. Let r be a divisor of p^2-1 such that r is even, $m = (p^2-1)/r$ is even and $r \nmid p-1$. Let i be the natural number such that $\gcd(r, p-1)$ is divisible by 2^i but not by 2^{i+1}. Since r is even, we obtain that $i \geq 1$. Let γ be a fixed generator of $\mathbb{F}_{p^2}^*$ and set $d_{p^2,m} = \varphi\mu_{\gamma^{(p-1)/2^i}}$. Then define the subgroup $\widetilde{Z_{p^2,m}} = \langle Z_{p^2,m}, d_{p^2,m}\rangle$ of $\mathsf{GL}(2,p)$.

As observed before, we will separate the irreducible subgroups of $\mathsf{GL}(2,p)$ into the classes of primitive and imprimitive groups. Therefore, in this discussion of subgroups of $\mathsf{GL}(2,p)$, we want to consider different classes of primitive irreducible subgroups of the general linear group. Hence the conditions required for the definition of $\widetilde{Z_{p^2,m}}$ guarantee that this type of subgroups of $\mathsf{GL}(2,p)$ is distinct from the previous ones. Indeed, $r \nmid p-1$ assures that these groups are primitive ([Sho92, Proposition 4.2.4]) and the parity of m and r guarantees that this class of subgroups is distinct from the previous ones ([Sho92, Lemmas 4.1.5 and 4.1.8]).

Lemma 6.3.3. *Let r be an even divisor of p^2-1 such that $m=(p^2-1)/r$ is even and $r \nmid p-1$. Consider the group $\widetilde{Z_{p^2,m}}$ and the element $d_{p^2,m}$ as above. Then the following hold:*

1. *$d_{p^2,m}$ normalizes $Z_{p^2,m}$;*
2. *$\widetilde{Z_{p^2,m}} = Z_{p^2,m}\langle d_{p^2,m}\rangle$;*
3. *$(d_{p^2,m})^2 \in Z_{p^2,m}$;*
4. *$|\widetilde{Z_{p^2,m}}| = 2|Z_{p^2,m}| = 2r$.*

Proof. Let us prove that $d_{p^2,m}$ normalizes $Z_{p^2,m}$. By the first statement of Lemma 6.3.2, we know that φ normalizes $Z_{p^2,m}$. Since Z_{p^2} is an abelian group, $Z_{p^2,m} \leq Z_{p^2}$, and $\mu_{\gamma^{(p-1)/2^i}} \in Z_{p^2}$, we obtain that $\mu_{\gamma^{(p-1)/2^i}}$ normalizes $Z_{p^2,m}$, and so does the product $d_{p^2,m} = \varphi\mu_{\gamma^{(p-1)/2^i}}$. Statement 2 is a consequence of the first statement.

Now we prove that $(d_{p^2,m})^2 \in Z_{p^2,m}$ in Statement 3. We have that

$$\begin{aligned}(d_{p^2,m})^2 &= \varphi\mu_{\gamma^{(p-1)/2^i}}\varphi\mu_{\gamma^{(p-1)/2^i}} = \varphi^{-1}\mu_{\gamma^{(p-1)/2^i}}\varphi\mu_{\gamma^{(p-1)/2^i}} \\ &= (\mu_{\gamma^{(p-1)/2^i}})^{\varphi}\mu_{\gamma^{(p-1)/2^i}}.\end{aligned}$$

Using the same argument of the proof of Statement 1 of Lemma 6.3.2, we have that

$$(\mu_{\gamma^{(p-1)/2^i}})^{\varphi} = \mu_{(\gamma^{(p-1)/2^i})_{\varphi}} = \mu_{\gamma^{p(p-1)/2^i}}.$$

Hence $(d_{p^2,m})^2 = \mu_{\gamma^{p(p-1)/2^i}}\mu_{\gamma^{(p-1)/2^i}}$. Since $\delta \mapsto \mu_\delta$ is a homomorphism, we obtain that

$$(d_{p^2,m})^2 = \mu_{\gamma^{p(p-1)/2^i}}\mu_{\gamma^{(p-1)/2^i}} = \mu_{\gamma^{p(p-1)/2^i+(p-1)/2^i}} = \mu_{\gamma^{(p^2-1)/2^i}}.$$

Therefore $\mu_{\gamma^{(p^2-1)/2^i}}$ is an element of order 2^i. By definition of i, we have that 2^i divides r, which is the order of $Z_{p^2,m}$. Thus we obtain that $(d_{p^2,m})^2 \in Z_{p^2,m}$.

Next, we prove Statement 4. We know that

$$|\widetilde{Z_{p^2,m}}| = \frac{|Z_{p^2,m}||\langle d_{p^2,m}\rangle|}{|Z_{p^2,m} \cap \langle d_{p^2,m}\rangle|}.$$

On the other hand, by Statement 3 we know that $d_{p^2,m}^2 \in Z_{p^2,m}$. Therefore we have that $|Z_{p^2,m} \cap \langle d_{p^2,m}\rangle| = |\langle d_{p^2,m}\rangle|/2$. Thus

$$|\widetilde{Z_{p^2,m}}| = \frac{|Z_{p^2,m}||\langle d_{p^2,m}\rangle|}{|\langle d_{p^2,m}\rangle|/2} = 2|Z_{p^2,m}| = 2r.$$

□

We remark that, as with the Frobenius automorphism, if $S_{p^2,m}$ is the subgroup of $\mathbb{F}_{p^2}^*$ with index m defined in Section 5.2 then the element $d_{p^2,m}$ in its action on $\mathbb{F}_{p^2}$ stabilizes $S_{p^2,m}$.

After describing some primitive irreducible subgroups of $\mathsf{GL}(2,p)$, we can state the next theorem, which, up to conjugacy, classifies all irreducible subgroups of $\mathsf{GL}(2,p)$. This theorem is a summary of the results from Chapter 4 of [FO05]

Theorem 6.3.4. *Let p be an odd prime and H be an irreducible subgroup of $\mathsf{GL}(2,p)$. Then precisely one of the following hold:*

1. $\mathsf{SL}(2,p) \leq H$.
2. *H is an imprimitive linear group.*
3. *H is conjugate to a subgroup of the form $Z_{p^2,m}$, $\overline{Z_{p^2,m}}$, where $(p^2-1)/m$ does not divide $2(p-1)$, or to a subgroup of the form $\widetilde{Z_{p^2,m}}$, where both m and $r = (p^2-1)/m$ are even and $r \nmid p-1$.*
4. *$H/Z(H)$ is isomorphic to one of the groups $\mathsf{Alt}(4)$, $\mathsf{Sym}(4)$ or $\mathsf{Alt}(5)$.*

6.4 Undirected Orbital Graphs of Affine Groups

From Statement 2 of Theorem 4.2.4, a primitive group on Ω is synchronizing if and only if there is no suitable undirected generalized orbital graph for the group; that is, a graph with vertex-set Ω and edge-set invariant under the group, whose clique number is equal to the chromatic number. Thus we must start our study of the synchronization property by describing the undirected orbitals of primitive affine groups built using different types of irreducible subgroups of $\mathsf{GL}(2,p)$.

Let p be an odd prime and consider the field $\mathbb{F}_{p^2}$. Let γ be a fixed generator of $\mathbb{F}_{p^2}^*$. Let $Z_{p^2,m}$ be the subgroup of a Singer cycle Z_{p^2} with index m and set $r = |Z_{p^2,m}| = (p^2-1)/m$. Let T be the group of translations by

elements of $\mathbb{F}_{p^2}$ and consider the corresponding affine group $G = T \rtimes Z_{p^2,m}$, acting on the elements of $\mathbb{F}_{p^2}$.

We define r_1, m_1 as follows.

$$\begin{array}{l} \text{If } r \text{ is even, then } r_1 = r \text{ and } m_1 = m. \\ \text{If } r \text{ is odd, then } r_1 = 2r \text{ and } m_1 = m/2. \end{array} \tag{6.2}$$

Note that $S_{p^2,m} \leq S_{p^2,m_1}$, where $S_{p^2,m}$ and S_{p^2,m_1} are the subgroups of $\mathbb{F}_{p^2}^*$ with indexes m and m_1, respectively, whose definitions we recall from Section 5.2. For $i \in \{0, \ldots, m_1 - 1\}$ let

$$\Delta_i = \left\{ \{\alpha, \beta\} : \beta - \alpha \in S_{p^2,m_1}\gamma^i \right\}. \tag{6.3}$$

The sets Δ_i are well defined. Indeed, if $\beta - \alpha \in S_{p^2,m_1}\gamma^i$ then we have that $\alpha - \beta = -(\beta - \alpha) \in (-1)S_{p^2,m_1}\gamma^i$. Since S_{p^2,m_1} has always even order, we obtain that $-1 \in S_{p^2,m_1}$ and hence $\alpha - \beta \in S_{p^2,m_1}\gamma^i$.

In the next lemma we will present some properties of the undirected orbital graphs of affine groups. In Section 4.1 we defined Γ_Δ as the graph (Ω, Δ), where $\Delta \subseteq \Omega^{\{2\}}$, and in Section 5.2 we denoted by $\Gamma_{p^2,m}$ the generalized Paley graph of the field $\mathbb{F}_{p^2}$ with index m.

Lemma 6.4.1. *Let p be an odd prime. Let m be a divisor of $p^2 - 1$ and let $Z_{p^2,m}$ be as above. Consider the affine group $G = T \rtimes Z_{p^2,m}$. Then the following hold:*

1. *$\Delta_0, \cdots, \Delta_{m_1-1}$ are precisely the G-orbits on $(\mathbb{F}_{p^2})^{\{2\}}$;*
2. *$\Gamma_{\Delta_i} \cong \Gamma_{\Delta_j}$ for all $i, j \in \{0, \ldots, m_1 - 1\}$;*
3. *$\Gamma_{\Delta_0} = \Gamma_{p^2,m_1}$.*

Proof. Let us prove Statement 1. Let γ be the generator of $\mathbb{F}_{p^2}^*$ fixed above. For $i \in \{0, \ldots m_1 - 1\}$, consider the G-orbit $\overline{\Delta_i} = \{0, \gamma^i\}G$. We claim that $\Delta_i = \overline{\Delta_i}$. Let us start by proving that $\Delta_0 = \overline{\Delta_0}$. First we show that $\overline{\Delta_0} \subseteq \Delta_0$. Let $g \in G$, such that $g = \sigma_\beta \mu_{\delta^m}$, with $\beta \in \mathbb{F}_{p^2}$ and $\delta \in \mathbb{F}_{p^2}^*$. Then

$$\{0,1\}g = \{0,1\}\sigma_\beta\mu_{\delta^m} = \{\beta, 1+\beta\}\mu_{\delta^m} = \{\beta\delta^m, \delta^m + \beta\delta^m\}.$$

We have that $(\delta^m + \beta\delta^m) - \beta\delta^m = \delta^m \in S_{p^2,m}$. Thus we obtain that $(\delta^m + \beta\delta^m) - \beta\delta^m \in S_{p^2,m_1}$. Hence $\overline{\Delta_0} \subseteq \Delta_0$. Conversely, let $\{\alpha, \beta\} \in \Delta_0$. Then $\{\alpha, \beta\}\sigma_{-\alpha} = \{0, \beta - \alpha\}$. Since $S_{p^2,m}$ is a subgroup of S_{p^2,m_1} with index 1 or 2, either $\beta - \alpha \in S_{p^2,m}$ or $\alpha - \beta \in S_{p^2,m}$ (or both, in the case when the

index is 1). Without loss of generality, we can assume that $\beta - \alpha \in S_{p^2,m}$. Then $\{\alpha,\beta\}\sigma_{-\alpha}\mu_{(\beta-\alpha)^{-1}} = \{0,1\}$. This means that $\{\alpha,\beta\} \in \overline{\Delta_0}$. Therefore $\Delta_0 \subseteq \overline{\Delta_0}$.

Now let $i \in \{1,\ldots,m_1-1\}$. We want to prove that $\Delta_i = \overline{\Delta_i}$. We have that $\beta-\alpha \in S_{p^2,m_1}$ is equivalent to $(\beta-\alpha)\gamma^i \in S_{p^2,m_1}\gamma^i$. Therefore $\Delta_i = \Delta_0\gamma^i$. Thus we conclude that $\Delta_i = \Delta_0\gamma^i = \overline{\Delta_0}\gamma^i$. Hence we have to prove that $\overline{\Delta_0}\gamma^i = \overline{\Delta_i}$. This is equivalent to showing that $\overline{\Delta_0}\gamma^i = \Delta_0\gamma^i$ is a G-orbit. Let $\{\alpha,\beta\} \in \Delta_0$ and $g \in G$. We want to conclude that $\{\alpha,\beta\}\gamma^i g \in \Delta_0\gamma^i$. Indeed, we have that $\{\alpha,\beta\}\gamma^i g = \{\alpha,\beta\}g^{\gamma^{-i}}\gamma^i$ and that $g^{\gamma^{-i}} \in G$. Since $\Delta_0 = \overline{\Delta_0}$ is a G-orbit in $(\mathbb{F}_{p^2})^{\{2\}}$ we obtain that $\{\alpha,\beta\}g^{\gamma^{-i}}\gamma^i \in \Delta_0\gamma^i$. Hence $\Delta_0\gamma^i$ is G-invariant. It remains to show that if $\{\alpha,\beta\}\gamma^i \in \Delta_0\gamma^i$ then there exists $g \in G$ such that $\{\alpha,\beta\}\gamma^i g = \{0,\gamma^i\}$. As $\{\alpha,\beta\} \in \Delta_0$ there exists $h \in G$ such that $\{\alpha,\beta\}h = \{0,1\}$. Therefore $\{\alpha,\beta\}\gamma^i h^{\gamma^i} = \{\alpha,\beta\}h\gamma^i = \{0,1\}\gamma^i = \{0,\gamma^i\}$. Since $h \in G$ and $\gamma^i \in S_{p^2}$ we obtain that $h^{\gamma^i} \in G$. Thus we have that $\{\alpha,\beta\}\gamma^i \in \{0,\gamma^i\}G = \overline{\Delta_i}$. Hence $\Delta_0\gamma^i$ is a G-orbit. Further, $\{0,1\} \in \Delta_0$ and so $\{0,\gamma^i\} \in \Delta_0\gamma^i$. By definition, it means that $\overline{\Delta_i} = \Delta_0\gamma^i = \overline{\Delta_0}\gamma^i$. Thus $\Delta_i = \overline{\Delta_i}$. On the other hand, we have that $\bigcup_{i\in\{0,\ldots,m_1-1\}} \overline{\Delta_i} = (\mathbb{F}_{p^2})^{\{2\}}$ and these undirected orbitals are distinct since if $\{\alpha,\beta\} \in \Delta_i \cap \Delta_j$ then $\beta-\alpha \in S_{p^2,m_1}\gamma^i \cap S_{p^2,m_1}\gamma^j$. This is a contradiction as $S_{p^2,m_1}\gamma^i$ and $S_{p^2,m_1}\gamma^j$ are distinct cosets of S_{p^2,m_1} on $\mathbb{F}_{p^2}^*$. Therefore $\Delta_0,\ldots,\Delta_{m_1-1}$ are precisely the G-orbits on $(\mathbb{F}_{p^2})^{\{2\}}$.

Next, we prove Statement 2. From the argument in the last paragraph, we have that $\Delta_0\gamma^i = \Delta_i$. Hence μ_{γ^i} is an isomorphism between the graphs Γ_{Δ_0} and Γ_{Δ_i} for all $i \in \{0,\ldots,m_1-1\}$.

Now we prove the last statement. We first remark that the vertex-sets of Γ_{Δ_0} and Γ_{p^2,m_1} coincide. On the other hand, both Γ_{Δ_0} and Γ_{p^2,m_1} are vertex-transitive graphs (see Proposition 5.2.1). Therefore it is enough to show that the neighborhoods $\Gamma_{\Delta_0}(0)$ and $\Gamma_{p^2,m_1}(0)$ of zero in Γ_{Δ_0} and Γ_{p^2,m_1}, respectively, are the same. By the way these graphs are built, we have that

$$\Gamma_{\Delta_0}(0) = \{\alpha \in \mathbb{F}_{p^2} : \{0,\alpha\} \in \Delta_0\} = \{\alpha \in \mathbb{F}_{p^2} : \alpha - 0 \in S_{p^2,m_1}\} = \Gamma_{p^2,m_1}(0).$$

Hence we conclude that $\Gamma_{\Delta_0} = \Gamma_{p^2,m_1}$. □

The next step is to describe the undirected orbitals for the affine groups constructed from the other types of irreducible subgroups of $\mathsf{GL}(2,p)$ described in Statement 3 of Theorem 6.3.4, namely $\overline{Z_{p^2,m}}$ and $\widetilde{Z_{p^2,m}}$. From the fact that $\varphi^2 = 1$ and from Statement 3 of Lemma 6.3.3, we know that φ^2

and $(d_{p^2,m})^2$ are elements of the the group $Z_{p^2,m}$ for all divisor m of p^2-1. Therefore the undirected orbitals of the corresponding affine groups are either undirected orbitals as in Equation (6.3) or are unions of two such undirected orbitals. Thus, to describe the orbits of the groups $\overline{G} = T \rtimes \overline{Z_{p^2,m}}$ and $\widetilde{G} = T \rtimes \widetilde{Z_{p^2,m}}$ on the set $(\mathbb{F}_{p^2})^{\{2\}}$, we just have to see what is the action of the elements φ and $d_{p^2,m}$ on the set of orbits in Equation (6.3).

Lemma 6.4.2. *Let $\Delta_0, \ldots, \Delta_{m_1-1}$ be the undirected orbitals displayed in Equation (6.3) and let $j,\ k \in \{0, \ldots, m_1-1\}$. Then*

1. *$\Delta_j\varphi = \Delta_k$ if and only if $m_1 \mid jp-k$.*
2. *$\Delta_j d_{p^2,m} = \Delta_k$ if and only if $jp + (p-1)/2^i \equiv k \pmod{m_1}$, where i is as in the definition of the element $d_{p^2,m}$.*

Proof. Let $\{\alpha, \beta\} \in \Delta_j$. By Equation (6.3), we know that $\beta - \alpha \in S_{p^2,m_1}\gamma^j$.

Let us prove Statement 1. We have that $(\beta-\alpha)\varphi \in (S_{p^2,m_1}\gamma^j)\varphi$. By an observation after Lemma 6.3.2, we know that φ normalizes S_{p^2,m_1}. Thus $(S_{p^2,m_1})\varphi = S_{p^2,m_1}$ and hence $(\beta-\alpha)\varphi \in S_{p^2,m_1}\gamma^{jp}$. Therefore, we conclude that $\Delta_j\varphi = \Delta_k$ if and only if $S_{p^2,m_1}\gamma^{jp}$ is the same coset of S_{p^2,m_1} in $\mathbb{F}_{p^2}^*$ as $S_{p^2,m_1}\gamma^k$. This is equivalent to

$$S_{p^2,m_1}\gamma^{jp-k} = S_{p^2,m_1},$$

which is the same as $\gamma^{jp-k} \in S_{p^2,m_1}$; that is, it is equivalent to $m_1 \mid jp-k$.

Next, we regard the action of the element $d_{p^2,m}$ on the undirected orbital Δ_j. We have that $(\beta-\alpha)d_{p^2,m} \in (S_{p^2,m_1}\gamma^j)d_{p^2,m}$ and recall that $d_{p^2,m} = \varphi\mu_{\gamma^{(p-1)/2^i}}$. Using a remark after Lemma 6.3.3, we obtain that $d_{p^2,m}$ normalizes S_{p^2,m_1}. Hence $(\beta-\alpha)d_{p^2,m} \in S_{p^2,m_1}\gamma^{jp+(p-1)/2^i}$. Using an analogous argument to the one in the previous statement, we conclude that $\Delta_j d_{p^2,m} = \Delta_k$ if and only if $m_1 \mid jp + (p-1)/2^i - k$. This statement is equivalent to $jp + (p-1)/2^i \equiv k \pmod{m_1}$. □

We remark that by the definition of the action of the elements φ and $d_{p^2,m}$ on the set of undirected orbitals of Equation (6.3), we have that $\Delta_i\varphi = \Delta_j$ is equivalent to $\Delta_j\varphi = \Delta_i$ and the same happens with the element $d_{p^2,m}$.

Using Statement 1 of Lemma 6.4.2 we obtain that the undirected orbital Δ_0 described in Equation (6.3) is always an undirected orbital for the group $\overline{G} = T \rtimes \overline{Z_{p^2,m}}$. Hence from Statement 3 of Lemma 6.4.1 we conclude that

the generalized Paley graph Γ_{p^2,m_1} is an undirected orbital graph for both $G = T \rtimes Z_{p^2,m}$ and $\overline{G}$.

From Statement 2 of Lemma 6.4.2, we can obtain further properties of the undirected orbitals of the groups of the form $\widetilde{G} = T \rtimes \widetilde{Z_{p^2,m}}$ as well as of their undirected orbital graphs. We remark that in the definition of $\widetilde{Z_{p^2,m}}$, the order of $Z_{p^2,m}$ is always even. Therefore, in Equation (6.2), we have that $m_1 = m$ and $r_1 = r$.

Let us introduce an equivalence relation on the set $\{0, \ldots, m_1 - 1\}$ defined as follows:

$$i \approx j \quad \text{if and only if } i = j \text{ or } \Delta_i d_{p^2,m} = \Delta_j. \tag{6.4}$$

A numerical expression to verify if $i \approx j$ is given in the second statement of Lemma 6.4.2. Then the equivalence classes of $\approx$ have size at most 2 and it is proved in the next lemma that these classes have size precisely 2. Let $\mathscr{C}$ denote the set of equivalence classes of $\approx$. For $\alpha \in \mathscr{C}$ such that $\alpha = \{j, k\}$, we define $\widetilde{\Delta_\alpha} = \Delta_j \cup \Delta_k$. We set α_0 to be the element of $\mathscr{C}$ that contains 0.

Proposition 6.4.3. *Let p be an odd prime and m be a divisor of $p^2 - 1$ such that $\widetilde{Z_{p^2,m}}$ is a primitive irreducible subgroup of $\mathsf{GL}(2,p)$. Consider the affine group $\widetilde{G} = T \rtimes \widetilde{Z_{p^2,m}}$. Then the following hold.*

1. *Every class of $\mathscr{C}$ has size 2 and hence $\widetilde{G}$ has $m/2$ orbitals.*
2. *If $(m/2) \in \widetilde{\Delta_{\alpha_0}}$ then $\Gamma_{\widetilde{\Delta_{\alpha_0}}} = \Gamma_{p^2,m/2}$.*

Proof. Let us prove the first Statement. As observed before, each equivalence class of $\approx$ has at most 2 elements. Therefore we need to prove that no class has just one element. This is equivalent to showing, for every $j \in \{0, \ldots, m-1\}$, that $jp + (p-1)/2^i \not\equiv j \pmod m$ holds. Hence we will prove, for every $j \in \{0, \ldots, m-1\}$, that

$$m \nmid j(p-1) + (p-1)/2^i. \tag{6.5}$$

For an integer x, let $[x]_2$ denote the largest 2-power that divides x. Note that, given $x, y \in \mathbb{Z}$ such that $[x]_2 \neq [y]_2$, we have that

$$[x + y]_2 = \min\{[x]_2, [y]_2\}. \tag{6.6}$$

Let $j \in \{0, \ldots, m-1\}$. As we want to prove Equation (6.5) it suffices to show that $[m]_2 > [j(p-1) + (p-1)/2^i]_2$. Using the notation above, the

definition of i can be rephrased as $2^i = [\gcd(p-1, r)]_2$. Hence precisely one of the following holds:

$$\text{a) } [p-1]_2 = 2^i \qquad \text{b) } [p-1]_2 > 2^i \text{ and } [r]_2 = 2^i.$$

Suppose that case a) holds. Then $(p-1)/2^i$ is odd. Since $p-1$ is even, we have that $j(p-1)+(p-1)/2^i$ is odd. By definition, m is even and therefore $m \nmid j(p-1)+(p-1)/2^i$ as desired.

Now assume case b). Set $2^k = [p^2-1]_2$. We have that $mr = p^2-1$ and hence we conclude that $[m]_2 = 2^{k-i}$. On the other hand, it is clear that $[j(p-1)]_2 > [(p-1)/2^i]_2$. Therefore, using Equation (6.6), we obtain that

$$[j(p-1)+(p-1)/2^i]_2 = [(p-1)/2^i]_2.$$

As $p+1$ is even it follows that $[(p-1)(p+1)/2^i]_2 > [(p-1)/2^i]_2$. Hence we conclude that

$$\begin{aligned}[m]_2 &= 2^{k-i} = [(p^2-1)/2^i]_2 = [(p-1)(p+1)/2^i]_2 \\ &> [(p-1)/2^i]_2 = [j(p-1)+(p-1)/2^i]_2.\end{aligned}$$

This implies that in case b) $m \nmid j(p-1)+(p-1)/2^i$. In both cases we proved the claim of Equation (6.5). Thus, for every $j \in \{0, \ldots, m-1\}$, we have that $jp + (p-1)/2^i \not\equiv j \pmod m$. This means that every equivalence class of $\approx$ has precisely two elements.

Next, we prove Statement 2. Assume that $\alpha_0 = \{0, m/2\}$. Then we have that $\widetilde{\Delta_{\alpha_0}} = \Delta_0 \cup \Delta_{m/2}$ is an undirected orbital for $\widetilde{G}$ and

$$\widetilde{\Delta_{\alpha_0}} = \{\{\alpha, \beta\} \in (\mathbb{F}_{p^2})^{\{2\}} : \beta - \alpha \in S_{p^2,m} \cup S_{p^2,m}\gamma^{m/2}\},$$

where γ is a generator of $\mathbb{F}_{p^2}^*$. We claim that $S_{p^2,m} \cup S_{p^2,m}\gamma^{m/2} = S_{p^2,m/2}$. It is clear that $S_{p^2,m} \cup S_{p^2,m}\gamma^{m/2} \subseteq S_{p^2,m/2}$. Since $|S_{p^2,m} \cup S_{p^2,m}\gamma^{m/2}| = |S_{p^2,m/2}|$, we obtain that $S_{p^2,m/2} = S_{p^2,m} \cup S_{p^2,m}\gamma^{m/2}$. Thus we can write the undirected orbital $\widetilde{\Delta_{\alpha_0}}$ as

$$\Delta_0 \cup \Delta_t = \big\{\{\alpha, \beta\} : \beta - \alpha \in S_{p^2,m/2}\big\},$$

which is the edge-set of the generalized Paley graph $\Gamma_{p^2,m/2}$. Hence the undirected orbital graph $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$ is the generalized Paley graph $\Gamma_{p^2,m/2}$. □

6.5 Synchronization of Two-Dimensional Affine Groups

In this section we will be concerned with the synchronization property in 2-dimensional affine groups. We will consider the different classes of irreducible subgroups of $\mathsf{GL}(2,p)$, having Theorem 6.3.4 as a reference, and then we will construct the respective affine groups in order to find out if they are synchronizing.

Theorem 6.5.1. *Let p be and odd prime. Let T be the group of translations by elements of $\mathbb{F}_{p^2}$ and H be an irreducible subgroup of $\mathsf{GL}(2,p)$. Consider the affine group $G = T \rtimes H$.*

(1). If H is imprimitive then G is non-synchronizing.

(2). Suppose that H is primitive.

- *(2.1). If $\mathsf{SL}(2,p) \leq H$ then G is 2-transitive and hence synchronizing.*
- *(2.2). If H is is a conjugate to $Z_{p^2,m}$ or $\overline{Z_{p^2,m}}$, for some divisor m of p^2-1, then the following are valid:*
  - *(a). If $m = 1$ then G is 2-transitive and hence synchronizing.*
  - *(b). Set m_1 as in Equation (6.2). If $m_1 > 1$ and $m_1 \mid p+1$ then the group G is non-synchronizing. In particular, if $m = 2$ then G is non-synchronizing.*
  - *(c). If $m = 3$ then G is synchronizing if and only if $3 \nmid p+1$.*
- *(2.3). If H is conjugate to $\widetilde{Z_{p^2,m}}$ for some m such that $\widetilde{Z_{p^2,m}}$ is a primitive subgroup of $\mathsf{GL}(2,p)$ then the following are valid:*
  - *(a). If $m = 2$ then G is 2-homogeneous and hence synchronizing.*
  - *(b). If $m > 2$ and $m \mid p+1$ then G is non-synchronizing.*
  - *(c). Suppose that $(p-1)/2^i \equiv m/2 \pmod{m}$. If $m > 2$ and $(m/2) \mid p+1$ then G is non-synchronizing.*

Proof. (1). See Theorem 6.2.4.

(2.1). By Statement 5 of Lemma 6.1.2, we have that $G_0 = H$ and by assumption $\mathsf{SL}(2,p) \leq H$. Since $\mathsf{SL}(2,p)$ is transitive on $\mathbb{F}_{p^2}\backslash\{0\}$, it follows that G is 2-transitive by Lemma 2.3.2. From Statement 2 of Theorem 3.1.1 we conclude that G is a synchronizing group.

(2.2). Let Δ_0 be as in Equation (6.3). Then by Statement 3 of Lemma 6.4.1 we have that $\Gamma_{\Delta_0} = \Gamma_{p^2,m_1}$ and that Γ_{Δ_0} is an undirected orbital graph for G (see the remark after Lemma 6.4.2). Further Γ_{p^2,m_1} is suitable if and only $m_1 \mid p+1$ by Theorem 5.3.2

(2.2)(a). If $m = 1$ then G contains $Z_{p^2,1}$ which is transitive on $\mathbb{F}_{p^2}\backslash\{0\}$. Hence we obtain as in the proof of Statement 1 that G is 2-transitive and hence synchronizing.

(2.2)(b). Suppose that $m_1 > 2$. If $m_1 \mid p+1$ then Γ_{p^2,m_1} is a suitable graph by Theorem 5.3.2. Therefore, using the characterization of Statement 2 of Theorem 4.2.4, we obtain that G is non-synchronizing. In the particular case when $m = 2$ then $m_1 = 2$ and $\Gamma_{p^2,2}$ is a suitable graph since $2 \mid p+1$. Thus if $m = 2$ then G is non-synchronizing.

(2.2)(c). If $3 \mid p+1$ then $m = m_1 = 3$ and G is non-synchronizing by Statement (2.2)(b). Suppose that $3 \nmid p+1$. Let $\Delta \subseteq (\mathbb{F}_{p^2})^{\{2\}}$ be a G-invariant set. It suffices to prove that $\Gamma_\Delta = (\mathbb{F}_{p^2}, \Delta)$ is a non-suitable graph. We have that either Δ is one of $\Delta_0, \Delta_1, \Delta_2$ in Equation (6.3) or Δ is the union of two such sets (see Statement 1 of Lemma 6.4.1 and the remark before Lemma 6.4.2). If $\Delta = \Delta_i$ for some $i \in \{0,1,2\}$ then by Statement 2 of Lemma 6.4.1 we obtain that $\Gamma_\Delta \cong \Gamma_{p^2,3}$ and this graph is non-suitable by Theorem 5.3.2. Assume now that $\Delta = \Delta_i \cup \Delta_j$ with $i,j \in \{0,1,2\}$ and $i \neq j$. Then Γ_Δ is the complement graph $\Gamma'_{p^2,3}$ of Γ_{Δ_k} where $\{k\} = \{0,1,2\}\backslash\{i,j\}$ that is isomorphic to $\Gamma_{p^2,3}$. However, by Proposition 5.3.1, $\Gamma'_{p^2,3}$ is non-suitable and neither is Γ_Δ. In both cases we concluded the non-suitability of Γ_Δ. Thus if $3 \nmid p+1$ then G is a synchronizing group.

(2.3)(a). If $m = 2$ then from Statement 1 of Proposition 6.4.3 we obtain that G has only 1 orbit on the set $(\mathbb{F}_{p^2})^{\{2\}}$ and hence it is 2-homogeneous. Thus by the second statement of Theorem 3.1.1, we conclude that G is a synchronizing group.

(2.3)(b). Suppose that $m \mid p+1$. Let $\alpha_0 = \{0,t\}$ as in the equivalence relation of Equation (6.4). By definition, $\Gamma_{\widetilde{\Delta_{\alpha_0}}} = (\mathbb{F}_{p^2}, \Delta)$ where

$$\Delta = \Delta_0 \cup \Delta_t = \{\{\alpha,\beta\} : \beta - \alpha \in S_{p^2,m} \cup S_{p^2,m}\gamma^t\},$$

where γ is a fixed generator of $\mathbb{F}^*_{p^2}$. Let $s \in \{0,\dots m-1\}\backslash\{0,t\}$. Such an element exist since $m > 2$. Then we have

$$S_{p^2,m}\gamma^s \cap (S_{p^2,m} \cup S_{p^2,m}\gamma^t) = \emptyset \tag{6.7}$$

We claim that $\mathbb{F}_p$ is a clique and $C = \{\{\delta_1 + \delta_2\gamma^s : \delta_2 \in \mathbb{F}_p\} : \delta_1 \in \mathbb{F}_p\}$ is a coloring of $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$. Since $m \mid p+1$, using an analogous argument to the one

in the proof of Statement 1 of Proposition 5.3.3, we obtain that $\mathbb{F}_p^* \leq S_{p^2,m}$. Therefore if $\nu_1, \nu_2 \in \mathbb{F}_p$ and $\nu_1 \neq \nu_2$ then $\nu_2 - \nu_1 \in S_{p^2,m}$. Thus $\mathbb{F}_p$ is a clique in $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$. Next, we prove that C is a coloring. It is clear that C is a partition of $\mathbb{F}_{p^2}$. Hence we only need to show that each part of C is an independence set on $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$. If α, β are distinct elements of the same part then $\beta - \alpha$ is of the form $\nu\gamma^s$, with $\nu \in \mathbb{F}_p^*$. Since $\mathbb{F}_p^* \leq S_{p^2,m}$, we have that $\beta - \alpha \in S_{p^2,m}\gamma^s$. Therefore, by Equation (6.7), α is not connected to β in the graph $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$ and thus C is a coloring for that graph. Hence we proved that $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$ has a clique with p elements and a coloring with p colors, which mean that it is a suitable graph. Thus, using Statement 2 of Theorem 4.2.4, we conclude that G is non-synchronizing.

(2.3)(c). Now assume that $(p-1)/2^i \equiv m/2 \pmod{m}$. Then we have that $\alpha_0 = \{0, m/2\}$. Hence by Statement 2 of Proposition 6.4.3, we obtain that $\Gamma_{\widetilde{\Delta_{\alpha_0}}} = \Gamma_{p^2,m/2}$. Assume that $m > 2$. If $m/2 \mid p+1$ then by Theorem 5.3.2 the graph $\Gamma_{p^2,m/2}$ is suitable and so is the undirected orbital graph $\Gamma_{\widetilde{\Delta_{\alpha_0}}}$ for G. Thus G is non-synchronizing. □

Bibliography

[ABC12] João Araújo, Wolfram Bentz, and Peter J Cameron. Groups synchronizing a transformation of non-uniform kernel. Technical Report arXiv:1205.0682, May 2012.

[AMS11] J. Araújo, J. D. Mitchell, and Csaba Schneider. Groups that together with any transformation generate regular semigroups for idempotent generated semigroups. *J. Algebra*, 343:93–106, 2011.

[AS06] Fredrick Arnold and Benjamin Steinberg. Synchronizing groups and automata. *Theoret. Comput. Sci.*, 359(1-3):101–110, 2006.

[Ash56] W. Ross Ashby. *An introduction to cybernetics*. Chapman and Hall Ltd., London, 1956.

[BDR88] I. Broere, D. Döman, and J. N. Ridley. The clique numbers and chromatic numbers of certain Paley graphs. *Quaestiones Math.*, 11(1):91–93, 1988.

[Cam99] Peter J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[Cam10] Peter J. Cameron. Synchronization . see http://www.maths.qmul.ac.uk/∼pjc/LTCC-2010-intensive3/, 2010.

[Cay54] A. Cayley. On the theory of groups as depending on the smbolic equation $\theta^n = 1$. *Phil. Mag.*, 7:40–47, 1854.

[Čer64] J. Černý. Poznámka k homogénnym eksperimentom s konecnými avtomatami. *Mat.-Fyz. Cas. Solvensk. Akad.*, 14:208–216, 1964.

[DM96] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[Dub98] L. Dubuc. Sur les automates circulaires et la conjecture de Černý. *RAIRO Inform. Théor. Appl.*, 32(1-3):21–34, 1998.

[Epp90] David Eppstein. Reset sequences for monotonic automata. *SIAM J. Comput.*, 19(3):500–510, 1990.

[FO05] D. L. Flannery and E. A. O'Brien. Linear groups of small degree over finite fields. *Internat. J. Algebra Comput.*, 15(3):467–502, 2005.

[GM12] Bernd Gartner and Jiri Maousek. *Approximation Algorithms and Semidefinite Programming*. Springer, New York, 2012.

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[Lev96] Inessa Levi. On the inner automorphisms of finite transformation semigroups. *Proc. Edinburgh Math. Soc. (2)*, 39(1):27–30, 1996.

[LM94] I. Levi and R. B. McFadden. S_n-normal semigroups. *Proc. Edinburgh Math. Soc. (2)*, 37(3):471–476, 1994.

[Lov79] László Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25(1):1–7, 1979.

[LP09] Tian Khoon Lim and Cheryl E. Praeger. On generalized Paley graphs and their automorphism groups. *Michigan Math. J.*, 58(1):293–308, 2009.

[Mor96] Patrick Morandi. *Field and Galois theory*, volume 167 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[Neu76] Peter M. Neumann. The structure of finitary permutation groups. *Arch. Math. (Basel)*, 27(1):3–17, 1976.

[Neu09] Peter M. Neumann. Primitive permutation groups and their section-regular partitions. *Michigan Math. J.*, 58(1):309–322, 2009.

[Pal33] R.E.A.C. Paley. On orthogonal matrices. *J. Math. Phys. Inst. Tech.*, 12:311–320, 1933.

[PBS03] Cheryl E. Praeger, Robert W. Baddeley, and Csaba Schneider. Transitive simple subgroups of wreath products in product action. 2003.

[Pin78] J.-E. Pin. Sur un cas particulier de la conjecture de Černý. In *Automata, languages and programming (Fifth Internat. Colloq., Udine, 1978)*, volume 62 of *Lecture Notes in Comput. Sci.*, pages 345–352. Springer, Berlin, 1978.

[Sho92] M. W. Short. *The primitive soluble permutation groups of degree less than* 256, volume 1519 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.

[Zal71] Yechezkel Zalcstein. Studies in the representation theory of finite semigroups. *Trans. Amer. Math. Soc.*, 161:71–87, 1971.

Index