SYNCHRONISING AND SEPARATING PERMUTATION GROUPS THROUGH GRAPHS

Mohammed Hamoud Aljohani

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews

2022

Identifiers to use to cite or link to this thesis:

DOI: https://doi.org/10.17630/sta/227
http://hdl.handle.net/10023/26470

Synchronising and separating permutation groups through graphs

Mohammed Hamoud Aljohani

This thesis is submitted in partial fulfilment for the degree of

Doctor of Philosophy (PhD)

at the University of St Andrews

November 2021

بسم الله الرحمن الرحیم

Dedication

I would like to dedicate my work to

my parents,

siblings,

and my wife and children.

Declaration

Candidate's declaration

I, Mohammed Hamoud Aljohani, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 42000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree. I confirm that any appendices included in my thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

I was admitted as a research student at the University of St Andrews in November 2016.

I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date: 29 /11/21 Signature of Candidate:

Supervisor's declaration I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree. I confirm that any appendices included in the thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

Date: 29 /11/21 Signature of Supervisor 1:

Date: 29 /11/21 Signature of Supervisor 2:

Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand, unless exempt by an award of an embargo as requested below, that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Mohammed Hamoud Aljohani, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

Printed copy No embargo on print copy.

Electronic copy No embargo on electronic copy.

Date: 29 /11/21 Signature of Candidate:

Date: 29 /11/21 Signature of Supervisor 1:

Date: 29 /11/21 Signature of Supervisor 2:

Underpinning Research Data or Digital Outputs

Candidate's declaration

I, Mohammed Hamoud Aljohani, hereby certify that no requirements to deposit original research data or digital outputs apply to this thesis and that, where appropriate, secondary data used have been referenced in the full text of my thesis.

Date: 29 /11/21 Signature of Candidate:

Acknowledgements

First and foremost, I would like to express my thanks to Almighty Allah, the Most Gracious and the Most Merciful, for giving me strength and well-being and for his blessing in finishing this thesis.

It is a great pleasure to express my deep sense of thanks and gratitude to all of the people who helped me throughout my postgraduate study.

I would like to offer my special thanks to Prof. Peter Cameron, my principle supervisor, for his advice and guidance throughout my postgraduate experience. I deeply appreciate his patience and encouragement. Also, my grateful thanks are extended to Prof. James Mitchell for his valuable comments and suggestions as supervisor and director of postgraduate study.

During my study I have contacted some people, from inside and outside the school, who provided me with information and insights. I would like to thank them all, especially John Bamberg, Ian Wanless, Leonard Soicher and Sean Eberhard.

With great gratitude, I want to thank my family for believing in me. I highly appreciate their tutelage and support.
This work was supported by the Ministry of Higher Education in Saudi Arabia (Taibah University) and the Saudi Cultural Bureau in London.

Abstract

About 15 years ago, Araújo, Arnold and Steinberg introduced the notion of synchronisation to the theory of finite permutation groups. Synchronisation property is closely related to another property which is called separation, but they are not the same. Interestingly, the study of the two properties for finite groups involves many combinatorial problems. In this thesis, we tried to extend the current knowledge about synchronising and separating groups and suggest some questions. The introduction and the background are represented in Chapter 1 and Chapter 2, respectively. The main work is divided into three chapters.

In Chapter 3, we started by extending the notions of synchronisation and separation to association schemes. Then, we considered two important families of almost simple permutation groups. Firstly, the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$ (we call this the first group). Secondly, the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of uniform l-partitions of an n-set, $\{1, ..., n\}$, into subsets of size k where $n = kl$ (we call this the second group).

For first group, when $k = 2, 3, 4$ and 5, we showed that for large enough n the group

is non-separating (resp. non-synchronizing) if and only if there is a Steiner system $S(t, k, n)$ (resp. large set) for some $t < k$. In general, we stated a conjecture that is if true would be a crucial extension of the remarkable result by Peter Keevash that considers the existence of Steiner systems. For the second group, we gave similar results to the first group when $K = 2, 3, 4, 5, 6$ and $l = 2$. We stated conjecture for $k > 6$ and $l = 2$. Also, we showed that the group is non-synchronising when $l > 2$.

In Chapter 4, the synchronisation property of affine distance transitive permutation groups is considered. We showed that the separation and the synchronising properties are equivalent for affine groups. We determined when some groups are synchronising, for example, automorphism groups of Hamming graphs, halved graphs, folded halved graphs, bilinear form graphs, some alternating form graphs and cosets graphs of some Golay codes. In addition, we stated a conjecture for distance regular graphs which connects this chapter and the previous one.

In Chapter 5, we started by defining the diagonal factorisation of finite groups and proved some related basic results. Then, we showed that the diagonal group $D(T, 2)$ is non-separating if and only if T admits a diagonal factorisation. Also, we showed that the group $D(T, 2)$ is non-separating when $T = A_n$. We proved that the diagonal group $D(T, d)$ for $d \geq 3$, is non-synchronising. In the last section, we showed the equivalence between the separation and the synchronisation properties for groups of diagonal types.

Contents

Dedication **i**

Declaration **i**

Acknowledgements **v**

Abstract **vii**

1 Introduction **1**

1.1 Synchronising automaton and Černý conjecture 2

1.2 From synchronising automata to synchronising groups 5

1.3 Motivation and Aim 6

2 Background **7**

2.1 Permutation groups and transformation monoids 7

2.1.1 Permutation groups 8

2.1.1.1 Transitive permutation groups 10

2.1.1.2 Primitive permutation groups 12

2.1.1.3 Basic permutation groups 14

2.1.2 Transformation monoids 15

2.2 Synchronisation and separation in permutation groups 16

2.2.1 Synchronising groups 17

2.2.2 Separating groups 18

2.3 Graphs and association schemes 20

2.3.1 Graphs 20

2.3.2 Graph homomorphisms 22

2.3.3 Orbitals and orbital graphs 23

2.3.4 Association schemes 25

2.4 Methods and results 30

2.4.1 O'Nan & Scott theorem 30

2.4.2 Results and outline 31

3 Almost simple permutation groups **35**

3.0.1 Summary of the results 36

3.1 First group and Johnson association schemes 37

3.1.1 Intersecting systems and Steiner systems 42

3.1.2 $k = 2, 3, 4$ and 5 48

3.1.2.1 The case $k = 2$ 48

3.1.2.2 The case $k = 3$ 50

3.1.2.3 The case $k = 4$ 55

3.1.2.4 The case $k = 5$ 66

3.1.3 The main conjecture 69

3.1.4 A way towards a proof of the main conjecture 72

3.1.4.1 The case $\bar{I}$ is singleton 72

3.1.4.2 The case $I = \{1, k\}$ 74

3.1.5 Projective planes 77

3.2 The second group 78

3.2.1 The case $l = 2$ and folded Johnson schemes 79

3.2.1.1 The case $k = 2$ or $k = 3$: 80

3.2.1.2 The case $k = 4$: 80

3.2.1.3 The case $k = 5$: 81

3.2.1.4 The case $k = 6$: 82

3.2.1.5 The conjecture 83

3.2.2 The case $l > 2$ 85

3.3 Conclusion and future work 87

4 Affine permutation groups **88**

4.0.1 Summary of the results 89

4.1 Permutation groups of affine type 90

4.1.1 Primitive affine groups and irreducible linear groups 92

4.1.2 Basic affine permutation groups and primitive linear groups 93

4.2 Coding theory 96

4.3 Imprimitive distance-regular graphs 103

4.4 Hamming graphs 104

4.5 Halved n-cube and folded halved n-cube 106

4.5.1 Halved n-cube and folded n-cube 106

4.5.2 Folded halved n-cube 111

4.6 Bilinear forms graph 113

4.6.1 Basic definitions 113

4.6.2 Maximal sets of rank 1 115

4.6.3 Clique and co-cliuqe numbers 116

4.7 Alternating forms graph 117

4.8 Hermitian forms graph 121

4.9 Coset graphs of some Golay codes 125

4.9.1 The coset graph of the extended ternary Golay code 125

4.9.2 The coset graph of the truncated binary Golay code 126

4.9.3 The coset graph of the binary Golay code 128

4.10 Conjecture 130

4.11 Conclusion and future work 130

5 Diagonal permutation groups **132**

5.0.1 Summary of the results 133

5.1 Factorisation of finite groups 133

5.1.1 Basic definitions and results 133

5.2 Diagonal groups with two factors $D(T, 2)$ 142

5.2.1 Conjugacy classes association scheme 143

5.2.2 The factorisation of finite groups and the separation property 146

5.2.3 The diagonal groups $D(T, 2)$ where $T = A_n$, and $n \geq 5$ . . . 149

5.2.4 Related problems 154

5.2.4.1 The proportion of all-even Latin squares 155

5.2.4.2 Equivalent Latin squares and monoids 156

5.3 Diagonal groups $D(T, d)$ when $d \geq 3$ 158

5.3.1 The separation and synchronisation property for $D(T, d)$, when $d \geq 3$ 159

5.4 The equivalence of separation and synchronisation properties 162

5.5 Conclusion and future work 164

A Appendix 166

A.1 The proof of Theorem 3.10 166

Bibliography 201

List of Figures

1.1 Digraph representing Cameron's automaton. 3

1.2 Digraph representing Černý's automaton. 4

5.1 The decomposition of the complete digraph with three vertices into three directed cycles of length 2 and into two directed cycles of length 3. 150

List of Tables

1.1 A reset word for Cameron's automaton. 3

1.2 A reset word for Černý automaton. 4

4.1 Weight distribution of the binary Golay code 109

5.1 Example of Latin square of size 5. 153

5.2 Example of all-even Latin square of size 6. 153

5.3 The proportion of all-even-Latin squares for $3 \leq n \leq 9$. 155

5.4 Example of inequivalent Latin squares of size 4. 156

Chapter 1

Introduction

The classification of finite permutation groups into various classes is an important and interesting topic in group theory. There are two crucial questions to be asked; first, when does a group belong to a specific class? Second, what are the relations between these classes?

A permutation group G on a finite set Ω is ***synchronising*** if every semigroup generated by G and a non-permutation transformation f on Ω contains a constant function. The concept of synchronisation, in permutation groups, was defined around 15 years ago by Araújo in [3] and Steinberg with Arnold in [8]. Its original context is the theory of automata, particularly the theory of deterministic finite automata.

Another class are ***separating*** permutation groups. A permutation group G on a finite set Ω is separating if for any two subsets A and B of Ω, each of which contains at least two elements, with the properties that the product of their cardinalities equals the cardinality of Ω and $|Ag \cap B| = \varnothing$ for some $g \in G$. The concept of separation can be traced back to the work of Peter Neumann [57]. The two notions of synchronisation and separation coincide in some groups and differ in others.

This chapter gives a very brief discussion of deterministic finite automata. Also, it explains the reason mathematicians introduced the notion of synchronisation to permutation groups. Moreover, it states the motivation and the aim of our study.

1.1 Synchronising automaton and Černý conjecture

A (finite, deterministic) automaton DFA consists of a finite set Ω of states and a finite set of transitions, each transition being a function from Ω to itself [21]. A DFA can be represented by a directed graph. In this directed graph, the vertex set is Ω and for each transition $a \in \Sigma$, there is a unique out-arc from each vertex labelled a. The Figures 1.1 and 1.2 are examples of finite deterministic automata.

A ***reset word*** in a deterministic finite automaton is a sequence of transitions such that the composition of the transitions, applied to any starting state brings you to a specific state. An automaton that contains a reset word is called synchronising. Figure 1.1 is an example of a synchronising automaton. It can be seen as a dungeon with four rooms (states) and coloured arcs that (transitions) represent paths. Assume that, each room contains a door that leads to instant death except in room 3 the door leads to freedom. Also, suppose that we are inside one of these rooms without knowing which one it is. If we only have a map of the dungeon and a reset word, for example (red, blue, red), then this reset word brings us to room 1 and from there we can reach room 3 and then reach freedom. According to Volkov

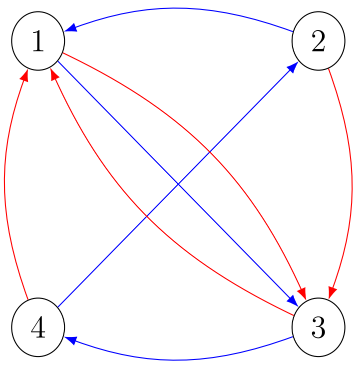

Figure 1.1: Digraph representing Cameron's automaton.

states	red	blue	red
1	3	4	1
2	3	4	1
3	1	3	1
4	1	3	1

Table 1.1: A reset word for Cameron's automaton.

[77], Jan Černý (1964) was the first person to define the concept of synchronisation explicitly but the name directable automaton was used instead of synchronising automaton. Černý observeed that $(n-1)^2$ is an upper bound on the length of the shortest reset word in any synchronising automata he encountered. Also, he provided an infinite family of synchronising automata with the property that their shortest reset word has length $(n-1)^2$. Figure 1.2 is a synchronising automaton on four states, it is a member of the family that was described by Černý. He stated his observation as a conjecture, which can be stated as follows:

Conjecture 1. *[25] Suppose that an automaton with n states is synchronising. Then it admits a reset word of length bounded above by $(n-1)^2$.*

This conjecture regarded as one of the longest standing conjectures in the theory of automata. Despite effort and time, Černý's conjecture is proved to be true for only partial cases. One of these cases is the case of aperiodic [1] automata. In 2007, Trahtman save an affirmative proof for the conjecture when the automata is aperiodic [74]. For more information about the Černý's conjecture and related problems the survey [77] is recommended.

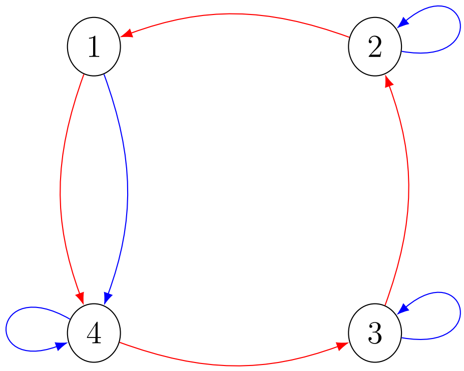

Figure 1.2: Digraph representing Černý's automaton.

states	blue	red	red	red	blue	red	red	red	blue
1	4	3	2	1	4	3	2	1	4
2	2	1	4	3	3	2	1	4	4
3	3	2	1	4	4	2	1	4	4
4	4	3	2	1	4	3	2	1	4

Table 1.2: A reset word for Černý automaton.

[1] A semigroup without non-trivial subgroups is called aperiodic. A DFA with ***aperiodic*** transition semigroup is called aperiodic too [74].

1.2 From synchronising automata to synchronising groups

Let DFA be a deterministic finite automaton on an n-set of states Ω,$n > 1$. Then the set of transitions Σ, with the operation of composition, generates a submonoid M of the full transformation monoid T_n. Now, if the DFA is synchronising, a reset word will be represented by a constant transformation in M. In view of this, we can define the notion of synchronisation for any transformation monoid (semigroup) as follows: a transformation monoid is said to be synchronising if it contains a constant function. If the set of transitions in a finite automaton generates a permutation group then the automaton is non-synchronising.

After Trahtman's result, it remains to check the conjecture for monoids (semigroups) with non-trivial subgroups. One way is to consider the monoids with non-trivial groups of units. In this particular case, Araújo in [3] and Steinberg and Arnold in [8] proposed that if we introduce the notion of synchronisation to permutation groups, we would be able to use our knowledge about groups and generators to prove the conjecture in the case of monoids with a non-trivial subgroup of units. For more ideas about how this could be done see [6, 21]. Although this approach has not helped to prove the conjecture, it motivated many interesting problems in group theory.

The new idea of studying synchronising permutation groups caught the attention of group and semigroup theorists specially after the paper of Peter Neumann [58], for example [4, 5, 7, 22, 52, 64, 66]. In addition, there are two theses on the topic of synchronising groups. First, a PhD thesis [64], where the author did not consider the classification of synchronising permutation groups. However, he studied some related problems such as ranks not synchronised by groups of permutation rank 3 and the singular endomorphisms (not automorphisms) of the Hamming graph and related graphs. Second, the Masters thesis [67], is devoted studying 2-dimensional affine groups. For more information, the survey [6] provides a wide range of background on the theory of synchronising groups.

1.3 Motivation and Aim

Cameron and Kazanidis [22] found a combinatorial necessary and sufficient condition for a finite permutation group to be synchronising. A similar condition can be found for separating permutation groups (These results are presented in Chapter 2). Therefore, it is possible to combine group theoretic and combinatorial approaches to determine if a group is synchronising (separating) or not. Also, the study of synchronising (separating) permutation groups results in some interesting combinatorial problems. Furthermore, the synchronisation and separation properties refine the class of primitive permutation groups. These facts provide us with the motivation to conduct this research.

The goal is to investigate and extend the current knowledge of synchronising and separating permutation groups. In this study, we consider some important examples of permutation groups and attempt to find out when they are synchronising or separating. Also, we study the relationship between these two properties. In particular, when they are equivalent and when they are not. In addition, we would like to understand how these properties are related to properties in other branches of mathematics, for example, design theory and association schemes.

The outline of this thesis will be represented in the next chapter.

Chapter 2

Background

The purpose of this chapter is to introduce the general background for this thesis. We state notions, concepts and basic results that are necessary for our study. Also, we fix notation and conventions. The results are provided without proofs. They can be found in standard books such that [20, 31, 62] for permutation groups, [6] for synchronisation and separation properties, [37] for graph theory and [10, 36] for association schemes.

2.1 Permutation groups and transformation monoids

A ***group*** $(G, \circ)$ is an algebraic structure consisting of a set G and a binary operation $\circ$ such that;

- $\circ$ is associative, i.e., $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ for all $g_1, g_2, g_3 \in G$.
- G has a unique identity.
- Every element in G has an inverse.

This is the abstract definition of a group. The group $(G, \circ)$ will be just denoted by G if the operation is clear.

Let $(G, \circ)$ be a group, A subset H of G is called a ***subgroup*** of G if $(H, \circ)$ is group. H is called a ***normal subgroup*** if $gHg^{-1} = H$ for all $g \in G$. The ***centraliser*** of H in G, denoted by $C_G(H)$, is the subgroup containing all elements $g \in G$ such that $gh = hg$ for all $h \in H$. If H and K are subgroups in G, then K ***centralises*** H if $K \leq C_G(H)$. It is not difficult to see that if H is a normal subgroup of G then $C_G(H)$ is a normal subgroup of G too. The ***normaliser*** of H in G, denoted by $N_G(H)$, is the subgroup of all $g \in G$ such that $gH = Hg$. It is the largest subgroup of G that containing H as a normal subgroup. If H and K are subgroups of G, then K ***normalises*** H if $K \leq N_G(H)$. If $H = N_G(H)$, we say that H is ***self normalising*** in G. The centraliser of a subgroup is a normal subgroup of its normaliser. The subgroup of G that contains all elements $g \in G$ that commute with all elements of G is called the ***centre*** of the group G and denoted by $Z(G)$. It is clear that $Z(G)$ is a normal subgroup of G and G is abelian if and only if it equals its centre. Therefore, non-abelian simple groups have trivial centres. The centre of a subgroup H of G is equal to the intersection of H and its centraliser $C_G(H)$.

2.1.1 Permutation groups

For a non-empty set Ω, the symmetric group $\mathrm{Sym}(\Omega)$ consists all bijective maps from Ω to itself. It is a group with the operation of composition. Elements of $\mathrm{Sym}(\Omega)$ are called permutations and a subgroup G of $\mathrm{Sym}(\Omega)$ is called a permutation group. When Ω is finite, say $\Omega = \{1, \cdots, n\}$, the symmetric group is denoted by $\mathrm{Sym}(n)$ or S_n.

In this thesis, we deal only with finite groups and write permutations on the right of their argument. Let G be a permutation group, we compose from left to right, for example if $\alpha \in \Omega$ and $g_1, g_2 \in G$ we have $\alpha(g_1 g_2) = (\alpha g_1)g_2$. The symbol of composition is omitted as it is obvious from the context.

Let G be a group and Ω be a non-empty set. An ***action of*** G ***on*** Ω is a homomorphism φ from G to $\mathrm{Sym}(\Omega)$.

Equivalently, G ***acts on*** Ω, if there is a function

$$\mu : \Omega \times G \longrightarrow \Omega,$$

satisfying the following:

- (i) $\mu(\alpha, e) = \alpha$ for all $\alpha \in \Omega$ (where e represents the identity element of G); and
- (ii) $\mu(\mu(\alpha, g), h) = \mu(\alpha, gh)$ for all $\alpha \in \Omega$ and $g, h \in G$.

If Ω is finite, $|\Omega|$ is called the degree of the action and the image of G under φ, denoted by G^{Ω}, is called the permutation group induced on Ω by G. The ***kernel*** of the action is defined as

$$\ker(\phi) = \{g \in G : \alpha(g\varphi) = \alpha \text{ for all } \alpha \in \Omega\}.$$

The action is called ***faithful*** if its kernel contains only the identity. Every abstract group is isomorphic to a transitive permutation group (Cayley's Theorem). If an action φ of a group G is faithful, then $\mathrm{Im}(G\varphi)$ is isomorphic to G.

Example 2.1. *(a) Let G be a group. Then G acts on itself by right multiplication via $\mu(h, g) = hg$ for all $h, g \in G$. It is a faithful action.*

(b) *Let H be a subgroup of a group G. If we let H/G indicate the set of right cosets of H in G, then G acts on H/G by the rule $\mu(Hg_1, g) = H(g_1 g)$ for all $Hg_1 \in H/G$ and $g \in G$. It is faithful if and only if $\cap_{g\in G}\, g^{-1}Hg = \{e\}$.*

(c) *Let H, K be subgroups of a group G such that K normalises H. Then K acts on H by conjugation. That is, $\mu(x, k) = k^{-1}xk$ for all $x \in H$ and $k \in K$. The kernel of this action is the centraliser of H in K.*

2.1.1.1 Transitive permutation groups

Let G be a group acting on a set Ω. We define a relation $\equiv$ on Ω by $\alpha \equiv \beta$ if $\beta = \alpha g$ for some $g \in G$; this is an equivalence relation (this follows from the group axioms). The equivalence classes are called ***orbits***. So the orbit of $\alpha \in \Omega$, denoted O_α, contains all elements of the form αg. Also, if β is in the orbit O_α, then it follows that $O_\alpha = O_\beta$.

G is said to be ***transitive*** on Ω (or the action is transitive) if for any two elements $\alpha, \beta \in \Omega$, there is $g \in G$ such that $\alpha g = \beta$, that is, G has only one orbit and we say that G is ***intransitive*** otherwise. Intransitive groups preserve non-trivial equivalence relations. The action of a group G on the right cosets of one of its subgroups is an example of transitive action. On the other hand, the action of a non-trivial group G on itself by conjugation is intransitive and the conjugacy classes are its G-orbits.

A crucial concept is the ***point stabiliser*** of an element $\alpha \in \Omega$, it is the subgroup G_α of G, which contains all $g \in G$ such that $\alpha g = \alpha$. Let G be a group acting on a set Ω, we say that the action is ***semi-regular*** if $|G_\alpha| = 1$ for all $\alpha \in \Omega$. The action is said to be ***regular*** if it is transitive and semi-regular.

Theorem 2.2. *[31, Theorem 1.4A. (ii)] Let G be a group acting transitively on a* *set Ω, then any two point stabilisers are conjugate.*

Theorem 2.3. *[31, Theorem 1.4A. (iii)](**Orbit-Stabiliser property**) Let G be a group acting transitively on a set Ω, then $|\Omega|= |G : G_\alpha|$ for all $\alpha \in \Omega$. In particular, $|\Omega||G_\alpha|= |G|$ if G is finite.*

Let G_1 and G_2 be groups acting on the sets Ω_1 and Ω_2, respectively, we say that $G_1^{\Omega_1}$ is ***isomorphic*** to $G_2^{\Omega_2}$ if there are:

- a bijection $\phi : \Omega_1 \to \Omega_2$;
- an isomorphism $\psi : G_1 \to G_2$.

such that $(\alpha g)\phi = (\alpha\phi)(g\psi)$ for all $\alpha \in \Omega_1$ and $g \in G_1$.

Theorem 2.4. *[20, Theorem 1.3 (a)] Let G be a group acting transitively on a set Ω, then the action is isomorphic to the action of G on the set H/G, where H is the point stabiliser of $\alpha \in \Omega$.*

Theorem 2.5. *[20, Theorem 1.3 (b)] Let G be a group with two subgroups H and K, then the actions on H/G and K/G are isomorphic if and only if H and K are conjugate.*

Theorem 2.6. *[62, Lemma 2.4] A transitive abelian permutation group is regular.*

Let H and K be groups. The ***direct product*** of H and K, denoted by $H \times K$, is the set $\{(h, k) : h \in H, k \in K\}$ with the group operation $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$ and (e, e) as an identity. The inverse of an element (h, k) is given by (h^{-1}, k^{-1}).

Let G be a permutation group acting intransitively on the finite set Ω. Then there is more than one orbit. Assume that there are r and call them $\Omega_1, \cdots, \Omega_r$. Then

G is a subgroup of the direct product $\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_r) \leq \mathrm{Sym}(\Omega)$ which contains all permutations that permute the elements of each orbits but do not send an element from one orbit to a different one. Therefore, any intransitive permutation group can be embedded in a direct product of symmetric groups [81].

2.1.1.2 Primitive permutation groups

Let G be a group acting transitively on a finite set Ω. A non-empty subset B of Ω is called a ***block*** for the group G if for each $g \in G$ either $Bg = B$ or $Bg \cap B = \varnothing$. The underlying set Ω and the singletons $\{\alpha\}$, where $\alpha \in \Omega$, are examples of blocks and they are called ***trivial blocks***. Let $\Sigma = \{Bg : g \in G\}$. It is clear that Σ is a partition of Ω and Σ is called the ***block-system*** containing B. It is non-trivial when B is non-trivial.

The action of G on Ω is called ***primitive*** if G has no non-trivial blocks on Ω, and it is called ***imprimitive*** otherwise. When the action is imprimitive the block system Σ for a block B is called a ***system of imprimitivity***. It can be shown that if G is imprimitive on Ω with Σ as a non-trivial system of imprimitivity, then G acts transitively on Σ and all blocks in Σ have the same size.

Let G be a group acting transitively on a set Ω, then a G-***congruence*** on Ω is an equivalence relation R on Ω with the property that

$$\alpha R\beta \Longleftrightarrow \alpha g \ R \ \beta g \ for \ all \ g \in G.$$

If G is imprimitive, then G preserves a non-trivial G-***congruence*** on Ω.

Theorem 2.7. *[37, Lemma 2.5.1] Let G be a group acting transitively on a set Ω, with $|\Omega| \geq 2$. Then G is primitive if and only if the point stabilizer G_α is maximal for all $\alpha \in \Omega$.*

A regular permutation group is primitive if and only if it has prime degree. Therefore, by Theorem 2.6, a primitive abelian group has prime degree. A ***minimal normal subgroup*** of a group G is a normal subgroup N such that there is no non-trivial normal subgroup H such that $H < N$.

Proposition 2.8. *[6, Proposition 2.4.] A non-trivial normal subgroup of a primitive group is transitive.*

Let H and K be groups. Assume that

$$\Phi : K \to \mathrm{Aut}(H)$$

corresponds to an action of K on H that respects the structure of H. The ***semi-direct product*** of H by K is the set $H \rtimes K = \{(h, k) : h \in H, k \in K\}$ with identity (e, e) and group operation:

$$(h_1, k_1)(h_2, k_2) = (h_1(h_2(k\Phi)), k_1k_2), \text{ where } (h)(k\Phi) = khk^{-1}$$
$$(h, k)^{-1} = ((k^{-1}h^{-1}k), k^{-1}).$$

H is isomorphic to a normal subgroup of $H \rtimes K$.

Let H and K be finite groups acting on Δ and Γ, respectively. The ***top group*** is a group isomorphic to K. The ***base group*** B is defined as the set $\mathrm{Fun}(\Gamma, H)$ of all functions from Γ to H. It is a group with the operation $(\gamma)fg = (\gamma)f(\gamma)g$, where $\gamma \in \Gamma$ and $f, g \in \mathrm{Fun}(\Gamma, H)$. It is isomorphic to the direct product of $|\Gamma| = n$ copies of H.

The ***wreath product*** of H by K, denoted by $H \wr K$, is the semi-direct product $B \rtimes K$, acting on n copies of Δ as follows:

B acts on n copies of Δ coordinate-wise while K permutes the coordinates. The size of the group $HwrK$ is $|H|^n|K|$ and its degree is $n|\Delta|$. If we assume $|\Delta|= m$, then the group $H \wr K$ is a subgroup of $S_m \wr S_n$.

Let G be a transitive imprimitive group on a finite set Ω with $|\Omega|= n$ and system of imprimitivity $\Sigma = \{P_1, \cdots, P_m\}$. Then all blocks have the same size, say $k = n/m$, and G is a subgroup of $\mathrm{Sym}(k) \wr \mathrm{Sym}(m)$ which contains all permutations with the property that they permute the elements in a partition or send a partition to a different partition[81].

2.1.1.3 Basic permutation groups

A ***Cartesian decomposition***, Λ of a set Ω is a finite set of partitions, $\Lambda = \{P_1, \cdots, P_l\}$, of Ω such that $|P_i|\geq 2$ for each i and

$$|p_1 \cap p_2 \cap \cdots \cap p_l|= 1$$

for all $p_1 \in P_1, \cdots, p_l \in P_l$. A Cartesian decomposition is said to be *trivial* if it contains only one partition, namely the partition into singletons. A Cartesian decomposition is said to be ***homogeneous*** if all the P_i have the same cardinality. Let G be a group acting primitively on a set Ω. Then the action is called ***non-basic*** if it preserves a non-trivial homogeneous Cartesian decomposition. It is ***basic*** otherwise[62].

Let H and K be finite group acting on Δ and Γ, respectively. The ***product action*** of the wreath product of H by K, denoted by $HwrK$, is the action of $H \wr K$ on the set $\mathrm{Fun}(\Gamma, \Delta)$ (the Cartesian product of $|\Gamma|$ copies of Δ) of all functions from Γ to Δ, where the base group acts coordinate-wise and the ***top group*** permutes the coordinates. The group $HwrK$ is a subgroup of $\mathrm{Sym}(m)wr\,\mathrm{Sym}(n)$, when $|\Gamma|= n$

and $|\Delta|= m$. It has degree m^n.

If $\{P_1, \cdots, P_l\}$ is a Cartesian decomposition of a set Ω, then the defining property yields a well defined bijection between Ω and $P_1 \times \cdots \times P_l$, given by

$$\omega \to (p_1, \cdots, p_l)$$

where, for $i = 1, \cdots, l$, the part $p_i \in P_i$ is the unique part of P_i which contains ω. Thus the set Ω can be naturally identified with the Cartesian product $P_1 \times \cdots \times P_l$ [62]. Therefore, a group G is non-basic if it is contained in a wreath product with product action.

2.1.2 Transformation monoids

A ***semigroup*** $(S, \circ)$ is an algebraic structure consisting of a set S and a binary operation $\circ$ such that

- $\circ$ is associative, i.e., $(s_1 \circ s_2) \circ s_3 = s_1 \circ (s_2 \circ s_3)$ for all $s_1, s_2, s_3 \in S$.

This is the abstract definition of a semigroup. The semigroup $(S, \circ)$ is just denoted by S if the operation is clear. A **monoid** is a semigroup with an identity.

For a non-empty set Ω, the ***full transformation monoid*** $T(\Omega)$ on Ω consists of all maps from Ω to itself. It is a monoid (semigroup) with the operation of composition. The group $\mathrm{Sym}(\Omega)$ is a submonoid of $T(\Omega)$. Also, any subset M of $T(\Omega)$, which is a monoid with the composition operation, is called a transformation monoid. When Ω is finite, say $\Omega = \{1, \cdots, n\}$, the full transformation monoid is denoted by T_n. The order of T_n is n^n. Let M be a monoid and Ω a non-empty finite set. An action of a monoid M on Ω can be defined as a homomorphism ϕ from M to the full transformation monoid T_n. The action is transitive if for any

α and β in Ω, there exists $f \in M$ such that $\alpha f \phi = \beta$. A monoid (semigroup) is called **synchronising** if it contains a constant map.

In analogy with Cayley's Theorem, we have the following:

Theorem 2.9. *[34, Theorem 2.4.3] An n-element semigroup is isomorphic to a sub-semigroup of T_{n+1}.*

Let Ω be a finite set and f a map from Ω to itself. The **image** of f is the set of the following form:

$$\mathrm{Im}(f) = \{\alpha f : \alpha \in \Omega\},$$

also, the **kernel** of f, $\ker(f)$, is the equivalence relation R_f defined by

$$\alpha R_f \beta \iff \alpha f = \beta f.$$

The kernel is uniform means that all equivalence classes have the same size. The rank of f, $\mathrm{rank}(f)$, is the cardinality of $\mathrm{Im}(f)$.

2.2 Synchronisation and separation in permutation groups

Although the synchronisation property was introduced to permutation group theory to help prove Černý's conjecture, the goal has not been achieved yet. Instead, it became an important topic in group theory. Another crucial concept is separating permutation groups. This is closely related to the synchronisation notion but they are not equivalent in general. One of the reasons that synchronization and separation are important is that they lie between primitivity and 2-transitivity, that is, they refine the class of primitive groups. Also, in many cases, the study of these properties leads to interesting (complicated) combinatorial problems. Here, we restate the concepts of synchronisation and separation with some basic related results.

2.2.1 Synchronising groups

Let G be a transitive group acting on a set Ω. We say that G **synchronises** a non-permutation f if the monoid $\langle G, f\rangle$ contains a map of rank 1 (constant function). The group G is called ***non-synchronising*** if there exists a non-permutation f such that $\langle G, f\rangle$ contains no constant map. The group G is ***synchronising***, otherwise. We assume that $|G| \neq 1$. A permutation group of prime degree is an example of synchronising group, by Corollary 2.12.

Let G be a permutation group on a set Ω and P be a partition of Ω. A ***section*** of P is a subset S of Ω such that the intersection of S and any part of P contains exactly one element. The partition P is said to be ***section regular*** or G-***regular partition*** if there is a section S of P such that

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

Theorem 2.10. *[6, Theorem 3.8.] A permutation group G on a set Ω is synchronising if and only if there is no non-trivial section regular partitions of Ω.*

Peter Neumann showed that if there is a regular partition it must be uniform, that is all parts have the same size.

Theorem 2.11. *[6, Theorem 3.9.] A section regular partition of a transitive permutation group is uniform.*

As a consequence of this theorem we get Pin's Theorem.

Corollary 2.12. *[60, Theorem 2] A transitive permutation group of prime degree is synchronising.*

Corollary 2.13. *[6, Corollary 3.11.] Let M be a transformation monoid on a finite set Ω with a transitive group of units. Then each element of M of minimal rank has a uniform kernel.*

It turns out that synchronising groups are basic, which is indicated by the following proposition.

Theorem 2.14. *[6, Proposition 3.7] Let G be a permutation group acting on Ω. If G is synchronising then G is basic.*

The converse is not always true. In fact, there are many basic permutation groups which are non-synchronising. For example, we will consider in the next chapter groups induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set of all k-subsets of an n-set. For $n > 2k$, this group is basic, but in some cases it is non-synchronising. For particular examples see Theorem 3.22.

The following result provides a connection between primitive groups and the synchronisation of monoids $\langle G, f\rangle$, where f is a transformation of rank $n-1$.

Theorem 2.15. *[5, Theorem 1] Let G be a transitive permutation group on Ω, where $|\Omega|= n$. Then G is primitive if and only if for any map $f : \Omega \longrightarrow \Omega$ of rank $n-1$, the monoid $\langle G, f\rangle$ contains an element of rank 1.*

2.2.2 Separating groups

Let G be a transitive permutation group on a finite set Ω, the group G is said to be ***non-separating*** if, given two subsets $A, B \subset \Omega$ (each contains at least two elements) with $|A|, |B| > 1$, and $|A| \cdot |B| = |\Omega|$ such that $|A \cap Bg| \neq \varnothing$ for all $g \in G$. The group G is said to be ***separating***, otherwise.

Theorem 2.16. *[6, Corollary 5.5] Let G be a transitive group acting on a finite set Ω, if G is separating then it is synchronising.*

The converse is also not true in general. In the dissection in Chapter 3, after Theorem 3.34 we show that the group induced by Sym(10) on 4-subsets of a 10-set is synchronising but non-separating.

Let G be a permutation group a set Ω. We say that G is 2-***transitive*** if for any (δ_1, β_1) and (δ_2, β_2) in $\Omega \times \Omega$ such that $\delta_1 \neq \delta_2$ and $\beta_1 \neq \beta_2$, there is g in G such that $(\delta_1, \beta_1)g = (\delta_2, \beta_2)$.

Theorem 2.17. *Let G be a group acting on a finite set Ω, if G is 2-transitive then it is separating.*

In our study, we will encounter many separating groups which are not 2-transitive. All 2-transitive permutation groups are known. A list of all such groups can be found in the books [62] and [31] by Cameron and Dixon & Mortimer, respectively. From previous discussions in this chapter, there is a classification in a hierarchy structure for finite permutation groups as follows:

2-transitive $\Longrightarrow$ separating $\Longrightarrow$ synchronising $\Longrightarrow$ basic $\Longrightarrow$ primitive $\Longrightarrow$ transitive.

The converse is not always true. Therefore, the study of synchronising (separating) permutation groups is reduced to these which are basic but not 2-transitive.

2.3 Graphs and association schemes

In this section, we list some definitions and results from graph theory. Also, we see how graph theory provides good tools to study the properties which are under consideration.

2.3.1 Graphs

A ***directed graph*** (digraph) D is an ordered pair $(V(D), E(D))$, where $V = V(D)$ is a set of vertices (points), called the ***vertex set*** and $E = E(D) \subseteq V \times V$, is a set of ordered pairs and called the ***arc (directed edge) set***. A vertex β is ***adjacent*** to a vertex α if there is an edge $e = (\alpha, \beta)$ from α to β and we say that β and α are ***incident*** to e. We consider only ***finite directed graphs*** $D = (V, E)$, that is V is a finite set. A ***directed path*** P from a vertex α to a vertex β of length d is a sequence of $d + 1$ vertices:

$$\alpha = \alpha_0, ..., \alpha_d = \beta$$

such that

$$(\alpha_{i-1}, \alpha_i) \in E \text{ for all } i \in \{1, ..., d\}.$$

If we relax the previous condition to either $(\alpha_{i-1}, \alpha_i) \in E$ or $(\alpha_i, \alpha_{i-1}) \in E$ for all $i \in \{1, ..., d\}$, then we call P an **undirected path**. If P is a path which has no repetition in its sequence, then P is called a ***simple path***. A ***circuit*** C is a path P from a vertex α to a vertex β of length greater than 1 such that $\alpha = \beta$. Also, a circuit C is called a ***cycle*** if it is a path containing no repetition except for the first and last vertex. A directed graph D is called ***connected*** if for any two vertices α and β there is an undirected path P from α to β, and is called ***strongly connected*** if the path P is directed. The ***out-degree*** (resp. ***in-degree***) of a vertex α is the number of vertices β that are adjacent to α (resp. the number of vertices β that α is adjacent to), where $\beta \in V$.

A ***graph*** Γ is a directed graph such that if (α, β) is a directed edge, then (β, α) is a directed edge (in this case, we replace the two arcs (α, β) and $(\alpha\beta)$ by an edge $\{\alpha, \beta\} = \alpha\beta$). A graph Γ is called ***simple*** if (α, α) is not an edge in Γ for all vertices α, and has no multiple edges. The ***degree*** of a vertex α in a graph Γ is the number of vertices adjacent to it and Γ is called ***regular*** if all vertices have the same degree.

A graph Γ is called ***complete*** if there is an edge between any two distinct vertices. It is denoted by K_m, where m is the number of vertices. A graph $\Gamma = (V, E)$ is called ***empty*** if $E = \varnothing$. It is called ***non-trivial*** if it is neither complete nor empty. A graph $\Gamma_1 = (V_1, E_1)$ is a ***subgraph*** of a graph $\Gamma_2 = (V_2, E_2)$ if V_1 is a subset of V_2 and E_1 is a subset of E_2. The graph Γ_1 is called an ***induced subgraph*** of Γ_2 if it is a subgraph and Γ_1 contains all edges between its vertices in Γ_2.

A ***clique*** in a graph Γ is a subset C of V such that any two vertices in C are adjacent in Γ. The size of a maximum clique is called the ***clique number*** of the graph Γ, it is denoted by $\omega(\Gamma)$. A ***co-clique (independent set)*** is a subset S of V such that no two vertices are adjacent. The size of a maximum co-clique is called the ***co-clique number*** of the graph Γ, it is denoted by $\alpha(\Gamma)$. A ***(proper) colouring*** of a graph Γ is an assignment of colours to the vertices so that adjacent vertices get different colours. The smallest number of colours needed for a proper colouring of Γ is called the ***chromatic number*** of the graph, it is denoted by $\chi(\Gamma)$.

2.3.2 Graph homomorphisms

Let Γ_1 and Γ_2 be finite graphs. A ***homomorphism*** from Γ_1 to Γ_2 is a map f from the vertex set $V(\Gamma_1)$ to the vertex set $V(\Gamma_2)$ such that f preserves the adjacency structure of the graph Γ_1 ,i.e. if $\alpha\beta$ is an edge in $E(\Gamma_1)$, then $(\alpha f)(\beta f)$ is an edge in $E(\Gamma_2)$. We say that Γ_1 is ***homomorphically equivalent*** to Γ_2 if there are two homomorphisms; one is from Γ_1 to Γ_2 and the other is from Γ_2 to Γ_1. An ***endomorphism*** is a homomorphism from Γ to itself. An ***automorphism*** is a bijective endomorphism which preserves adjacency and non-adjacency structure. The set of all automorphisms of a graph Γ defines a group on the vertex set with the composition operation, it is called the ***automorphism group*** of the graph Γ and denoted by $\mathrm{Aut}(\Gamma)$. A graph Γ is called ***vertex-transitive*** if its automorphism group is transitive.

An endomorphism which is not an automorphism is called ***proper***. A graph Γ is called ***core*** if it has no proper endomorphisms. We say that a graph Γ_2 is a core of a graph Γ_1, if it is core and there is a homomorphism from Γ_1 onto Γ_2.

Lemma 2.18. *[37, Lemma 6.2.1 or Lemma 6.2.2] Let Γ be a finite graph, then Γ has a core, which is an induced subgraph and unique up to isomorphism.*

Therefore, we can talk about the core of a graph Γ.

Theorem 2.19. *[21, Theorem 4, Lec 4] Let Γ be a finite graph, then the core of a graph is a complete graph K_m if and only if $\omega(\Gamma) = \chi(\Gamma) = m$.*

A homomorphism ϕ of a graph Γ is a ***colouring*** if the induced subgraph on $\phi(V(\Gamma))$ is a complete subgraph. A graph is called ***core-complete*** if it is core or its core is a complete graph. A stronger property than core-complete is ***pseudocore***, but it is weaker than core. A graph is called pseudocore if every proper endomorphism of Γ is a colouring[63].

2.3.3 Orbitals and orbital graphs

Let G be a transitive permutation group on a set Ω. The group G acts in a natural way on the set $\Omega \times \Omega$ and the orbits of this action are called ***orbitals***. The number of orbitals is called the **rank** of G. For each orbital R we can define a directed graph O_R, called an ***orbital graph***, such that its vertex set is Ω and there is a directed edge from a vertex α to a vertex β if (α, β) is in R. Since G is transitive the set $R_0 = \{(\alpha, \alpha) : \alpha \in \Omega\}$ is an orbital and is called the ***trivial*** or ***diagonal orbital***. An orbital R is called ***self-paired*** if $R = R^t$, where $R^t = \{(\beta, \alpha) : (\alpha, \beta) \in R\}$. The diagonal orbital is R_0 is self-paired.

Theorem 2.20. *[37, Lemma 2.4.2] Let G be a transitive group on a set Ω. There is a natural bijection between the orbitals of G and the orbits of a point stabilizer G_α.*

There are two notions of connectivity for directed graphs namely; connected and strongly connected directed graphs. However, since the orbital graphs of finite transitive permutation group are vertex-transitive, we have the following theorem.

Theorem 2.21. *[20, Theorem 1.10] A finite vertex transitive digraph which is connected is strongly connected.*

The following theorem is known as Higman's Theorem.

Theorem 2.22. *[20, Theorem 1.9] A transitive group G is primitive if and only if all non-trivial orbital graphs for G are connected.*

Higman's Theorem provides a combinatorial way to check if a finite permutation group is primitive or not. In an analogous way, Cameron states two results which help to apply graph theoretical techniques to the study of synchronisation and separation properties of finite permutation groups. They will be referred to as Cameron and Kazanidis techniques. In the following results by the trivial graph we mean a complete and null graph.

Theorem 2.23. *[21, Theorem 2.4] Let G be a permutation group on a set Ω. Then G is non-synchronising if and only if there is a non-trivial graph Γ on Ω with $G \leq \mathrm{Aut}(\Gamma)$ (G-invariant) having the property that $\omega(\Gamma) = \chi(\Gamma)$.*

Also, for separating groups we have the following.

Theorem 2.24. *[21, Theorem 5.4] Let G be a transitive permutation group on a set Ω. Then G is non-separating if and only if there is non-trivial graph Γ on the vertex set Ω with $G \leq \mathrm{Aut}(\Gamma)$ having the property that $\omega(\Gamma) \cdot \alpha(\Gamma) = |\Omega|$.*

Theorem 2.23 and Theorem 2.24 give an algorithm to check if a group is synchronising and separating using orbital graphs. Let G be a permutation group on a finite set Ω. There are $2^r - 2$ non-trivial G-invariant graphs (graphs whose automorphism group contains G), where r is the number of orbital graphs. Thus, there are $2^{r-1} - 1$ complementary pairs.

The first step is to check the clique and the co-clique numbers of one of each of the complementary pairs. If there is a graph Γ such that

$$\omega(\Gamma) \cdot \alpha(\Gamma) = |V(\Gamma)|,$$

then G is non-separating and we move to the next step. Otherwise, G is separating and synchronising.

The second step is to consider the complementary pair of graphs and check the chromatic numbers of both graphs. If there is a graph Γ such that the

$$\omega(\Gamma) = \chi(\Gamma),$$

then G is non-synchronising, otherwise G is synchronising [6].

In next subsection some background on the theory of association schemes will be given, which is a useful framework to conduct the algorithm.

2.3.4 Association schemes

Let d denote a positive integer, and let Ω be a non-empty finite set. A ***d-class homogenous association scheme*** (or for simplicity just an association scheme) $\mathcal{A}$ on Ω is a sequence $R_0, R_1, ..., R_d$ of non-empty subsets of the Cartesian product $\Omega \times \Omega$, satisfying

(a) $R_0 = \{(\alpha, \alpha) : \alpha \in \Omega\}$,

(b) $\Omega \times \Omega = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \varnothing$ for all $i \neq j$,

(c) For $i \in \{0, ..., d\}$, $R_i^t = \{(\beta, \alpha) : (\alpha, \beta) \in R_i\} = R_j$ for some $j \in \{0, 1, ..., d\}$,

(d) for all integers $i, j, k \in \{0, ..., d\}$, and for all $\alpha, \beta \in \Omega$ such that $(\alpha, \beta) \in R_k$, the number

$$p_{ij}^k = |\{\gamma \in \Omega : (\alpha, \gamma) \in R_i,\ (\gamma, \beta) \in R_j\}|$$

depends only on i, j, k and not on α or β. The numbers p_{ij}^k are the ***intersection numbers*** of the scheme.

The association scheme is ***commutative*** if:

- $p_{ij}^k = p_{ji}^k$ for all $i, j, k \in \{0, 1, ..., d\}$;

it is called ***symmetric*** if:

- $R_i^t = R_i$ for all $i \in \{0, 1, ..., d\}$.

Symmetric association schemes are commutative and commutative schemes are homogenous, but the converse not always true.

Remark: In the literature, the term coherent configuration is sometimes used instead of the term "association scheme". Actually, the term association scheme has been applied by some authors to each kind of coherent configurations: homogenous, commutative, symmetric. Here, we do not use the term coherent configuration, but we specify the kind of scheme.

Example 2.25. *Let G be a transitive permutation group on a finite set Ω, then the set of orbital graphs is an example of a homogeneous association scheme. Such a scheme will be called primitive if and only if G is primitive. It follows from Higman's Theorem that the association scheme is primitive if and only if all its non-diagonal orbital graphs are connected. Following the purpose of our study, we would like to investigate primitive homogeneous association schemes.*

Let $\mathcal{A}$ be a homogeneous association scheme, then every set R_i can be represented by an ***adjacency matrix*** A_i, that is, an $|\Omega| \times |\Omega|$ matrix whose entries can be defined by

$$A_i(\alpha, \beta) = \begin{cases} 1 & \text{if } (\alpha, \beta) \in R_i \\ 0 & \text{otherwise} \end{cases}$$

Association schemes can be defined using matrices.

Lemma 2.26. *[10] A d**-class commutative association scheme** $\mathcal{A}$ with vertex set Ω is a sequence of non-zero $\{0, 1\}$-matrices $A_0, ..., A_d$ with rows and columns indexed by Ω, such that* *(a)* $A_0 = I$*, where* I *is the identity matrix,*

(b) $\sum_{i=0}^{d} A_i = J$*, where* J *is the all-one matrix,*

(c) for all i *there exists* j *such that* $A_i^t = A_{j'}$*,*

(d) for all i, j *in* $\{0, ..., d\}$ *the product* $A_i A_j$ *is in the real span of* $A_0, ..., A_d$*.*

(e) $A_i A_j = A_j A_i$ *for all* $i, j \in \{0, 1, ..., d\}$*;*

it is called ***symmetric*** *if:*

- *the* A_i *are symmetric for all* $i \in \{0, 1, ..., d\}$ *.*

A homogenous association scheme $\{A_0, \ldots, A_d\}$ has the property that the linear span (over the real numbers) of the matrices is an algebra (closed under matrix multiplication), called the ***Bose–Mesner algebra*** of the scheme. See [10, 29] for further details.

Given an association scheme as above, each matrix A_i for $i > 0$ is the adjacency matrix of a graph, as indeed are the sums of some of these matrices. For $I \subseteq \{0, \ldots, d-1\}$, we denote by Γ_I the graph whose adjacency matrix is $\sum_{i \in I} A_i$. Such a graph will be called *non-trivial* if it is neither complete nor null, that is, if $I \neq \varnothing$ and $I \neq \{0, \ldots, d-1\}$. Note that the complement of the graph Γ_I is $\Gamma_{\{0,\ldots,d-1\} \setminus I}$.

Suppose that the matrices $A_0, \ldots, A_{d-1}$ (with $A_0 = I$) span the Bose–Mesner algebra of a commutative association scheme on n points. Since this algebra is a commutative algebra of real symmetric matrices, the matrices are simultaneously diagonalisable: that is, there are idempotent matrices $E_0, \ldots, E_{d-1}$ spanning the same algebra, with $E_0 = \frac{1}{n}J$, where J is the all-1 matrix. Thus, for some coefficients $P_j(i)$ and $Q_j(i)$, we have

$$\begin{aligned} A_j &= \sum_{i=0}^{d-1} P_j(i)E_i, \\ E_j &= n^{-1}\sum_{i=0}^{d-1} Q_j(i)A_i. \end{aligned}$$

Here the numbers $P_j(i)$ for $i = 0, \ldots, d-1$ are the eigenvalues of A_j. The matrices with (i, j) entry $P_j(i)$ and $Q_j(i)$ are called the ***matrix of eigenvalues*** and ***dual matrix of eigenvalues*** of the scheme.

Delsarte used these matrices to provide bounds on the clique and coclique numbers of graphs in an association scheme:

Theorem 2.27 ([29], Theorem 5.9; see also [36])**.** *Let $\mathcal{A}$ be a commutative association scheme on n vertices and let Γ be the union of some of the graphs in the scheme. If C is a clique and S is a coclique in Γ, then $|C|\cdot|S| \leq n$. If equality holds and x and y are the respective characteristic vectors of C and S, then $(xE_jx^\top)(yE_jy^\top) = 0$ for all $j > 0$.*

In the above notation, the inner distribution $a = (a_0, ..., a_{d-1})$ of a clique C is the vector where $a_i = xA_ix^\top/|C|$ for each $i \in \{0, \ldots, d-1\}$ (and $\mathcal{A}$ has d classes). Now if Q is the dual matrix of eigenvalues of $\mathcal{A}$, then

$$(aQ)_j = \frac{n}{|C|}xE_jx^\top$$

for all $j \geq 0$. This vector is sometimes known as the ***MacWilliams transform*** of C.

Corollary 2.28. *[36, Corollary 3.8.5] Let $\mathcal{A}$ be a commutative association scheme on n vertices and let Γ be the union of some of the graphs in the scheme. If C is a clique and S is a co-clique in Γ with $|C||S|= n$, then $|C \cap S|= 1$.*

The following theorem regarding the degree of a regular connected and will be used in next chapter.

Theorem 2.29. *Let Γ be a connected graph. The eigenvalue of Γ of largest absolute value is the maximum degree if and only if Γ is regular.*

The ***degree set*** of a subset X of the vertices of Γ is the set of nonzero indices i for which the i-th coordinate of its inner distribution is nonzero. The ***dual degree set*** of X is the set of nonzero indices j for which the j-th coordinate of its MacWilliams transform is nonzero. Two subsets X and Y of the vertices of Γ are ***design-orthogonal*** if their dual degree sets are disjoint. Similarly, X and Y are ***code-orthogonal*** if their degree sets are disjoint.

In [28], a generalisation of 2.27 is provided:

Theorem 2.30. *[28, Corollary 9] Assume C is a clique and S is a co-clique in a graph on n vertices which is in a homogeneous association scheme. Then,*

$$|C||S| \leq n.$$

An important property of graphs in an association scheme is that, in any such graph, the product of the clique number and the co-clique number is at most the number of vertices. (They share this property with vertex-transitive graphs).

Theorem 2.31. *[36, Corollary 2.12] Let Γ be a vertex transitive graph, then $\omega(\Gamma)\alpha(\Gamma) \leq |V(\Gamma)|$.*

The inequality in these two theorems is called **the clique–co-clique bound**.

2.4 Methods and results

2.4.1 O'Nan & Scott theorem

In the study of synchronising (separating) permutation group, it remains to determine which basic (not 2-transitive) permutation groups are synchronising or separating. Basic permutation groups fall in one of three classes of permutation groups. They are called almost simple, affine type or diagonal type. This fact follows from the celebrated O'Nan & Scott Theorem. We will state some definitions and results before we state the theorem.

Let G be a finite group. The ***socle*** of G is the subgroup generated by the set of all minimal normal subgroups of G. It turn out that finite primitive permutation groups have at most two minimal normal subgroups and if there are two, they must be isomorphic.

Theorem 2.32. *[6, Theorem 2.5.] A primitive permutation group has at most two minimal normal subgroups. If there are two, then they are isomorphic, non-abelian and regular. Moreover, each is the centraliser of the other in the symmetric group.*

A finite group G is called ***almost simple*** if there is a finite simple group T such that $T \leq G \leq \mathrm{Aut}(T)$. Its socle is simple [6]. The third chapter of this thesis considers examples of of almost simple groups.

Let $\mathbb{F}_q$ be a finite field and q be prime. Let $V = \mathbb{F}_q^n$ be an n-dimensional vector space over $\mathbb{F}_q$, then V has q^n elements. A group of symmetries of the vector space is given by the semidirect product of the set of translations (maps of the form $t_g : v \rightarrowtail v + g$, where $v, g \in V$) by the general linear group $GL(n, \mathbb{F}_q)$ (consisting of all invertible $n \times n$ matrices over $\mathbb{F}_q$). This group is called the ***affine general linear group*** and denoted $\mathrm{AGL}(n, \mathbb{F}_q)$.

A finite group G is called of ***affine type*** if $V \leq G \leq \mathrm{AGL}(n, \mathbb{F}_q)$. The group of translations forms a normal subgroup isomorphic to the additive group of the vector space V. It is isomorphic to the elementary abelian group of order q^n. The socle is abelian. Some examples of groups of affine type are considered in Chapter Four.

Let T be a finite simple group. A group G is called of ***diagonal type*** if its socle is a direct product of copies of a finite non-abelian simple groups acting on its diagonal subgroup. A more detailed definition will be given in Chapter Five, where we consider some diagonal groups. Here we state the O'Nan & Scott Theorem. It plays an important role in the study of synchronisation and separation properties beside the classification of finite simple groups. More information about it can be found in [20] and [31]. For the purpose of this work we present a modified version of the O'Nan & Scott Theorem, as it appears in [20].

Theorem 2.33. *[6, Theorem 4.6] Let G be a basic permutation group. Then G is one of three types; namely affine, diagonal, or almost simple.*

2.4.2 Results and outline

The goal is to consider some important examples of permutation groups and attempt to find out when they are synchronising or separating. Also, we want study the relationship between these two properties. In particular, when they are equivalent and when they are not. In addition, we would like to understand how these properties are related to properties in other branches of mathematics, for example, design theory and association schemes.

To achieve this goal we make use of known classifications of permutation groups such as the O'Nan & Scott Theorem, the classification of the affine distance-transitive groups and Aschbacher's Theorem. The results of Cameron and Kazanidis (Theorem 2.23 and Theorem 2.24) are the primary tools that are used in this thesis. To use these results, we move forwards and backwards between the context of permutation groups and the context of association schemes. This is because every permutation group gives an association scheme. The graphs in this association scheme are the G-invariant graphs which are needed to be considered in the theorems of Cameron and Kazanidis, this will be explained in detail in Chapter 3.

As we have seen above, synchronising and separating permutation groups are primitive. By the O'Nan & Scott Theorem, a basic group must be in one of the following families; almost simple, affine type or diagonal type. The classification of synchronising groups is quite difficult and we do not expect a full classification. In fact, we try to consider some important examples from each one of these families. Therefore, we divide the main part into three chapters each of which considers some examples of almost simple, affine and diagonal groups. The thesis makes up of three main chapters starting with Chapter 3.

In Chapter 3, we extend the definitions of synchronisation and separation to association schemes and showed that a finite permutation group G is separating (synchronising) if and only if the association scheme which is obtained from the orbital graphs of the group G, is separating (synchronising). This allow us to use association schemes to study groups. Then we considered two families of almost simple groups. First, we consider the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$ (we called this the first group). For large enough n and $k = 2$ and 3, we showed that the first group is non-synchronising if and only if it is non-separating if and only if there is a Steiner system $S(t,k,n)$ for some t. Also, for large enough n and $k = 4,5$, we showed that the first group is non-separating if and only if the divisibility conditions for $S(t,k,n)$ are satisfied for some t with $0 < t < k$. In addition, we provided an example of a non-separating, synchronising permutation group. These results are evidence for making a conjecture. This conjecture could be regarded as a significant extension of the Keevash's Theorem; that is, for large enough n in terms of k and t, a Steiner systems $S(t,k,n)$ exists if and only if the necessary divisibility conditions on the parameters are satisfied. Some of the previous results appeared as a joint paper with John Bamberg and Peter Cameron [1].

Second, we consider the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of uniform l-partitions of an n-set, $\{1,...,n\}$, into subsets of size k where $n = kl$ (we called this the second group). We proved that the second group is non-synchronising if $l > 2$. For the case $l = 2$, we showed that for $k = 2,3,4,5,6$, the second group is non-synchronising if and only if there is a resolvable Steiner system $S(k-1,k,2k)$. Then, for $k > 6$ we proved that if there is such a system, then the second group is non-synchronising, so non-separating and conjectured that the converse holds.

In Chapter 4, we investigate some examples of affine permutation groups, namely, the automorphism groups of some affine distance-transitive graphs. We showed that the synchronisation and separation properties are equivalent for affine groups. Then, we proved that the automorphism group is non-synchronising if the graph is one of the following; Hamming graphs $H(n,q)$, bilinear forms graphs $\mathrm{BF}(n_1,n_2,q)$, alternating forms graphs ($A\Gamma_4(3)$ or $A\Gamma_n(q)$ when both n and q are even), coset graph $Cos(C)$ of the extended ternary Golay code C, halved graphs $H\Gamma_n$ of $H(n,2)$ (when $n \geq 4$ and even or there is some positive integer m such that $n = 2^m - 1$, or $n = 23$), and folded halved graphs $FH\Gamma_n$ (when there is some positive integer m such that $n = 2^m$, or $n = 24$).

Moreover, we proved that the automorphism group is synchronising if the graph one of the following; halved graphs $H\Gamma_n$ of $H(n, 2)$, (where $n \leq 3$ or $n \geq 5$ and odd or there is no positive integer m such that $n = 2^m - 1$, or $n \neq 23$), folded halved graphs $FH\Gamma_n$, (when $n \leq 6$ or there is no positive integer m such that $n = 2^m$, or $n \neq 24$), alternating forms graph $A\Gamma_5(q)$, Hermitian graph $H\Gamma_2(\mathbb{F}_q)$, Hermitian graph $H\Gamma_3(\mathbb{F}_q)$, the coset graph $Cos(C)$ of the truncated binary Golay code C and the coset graph $Cos(C) = C_{23}$ of the binary Golay code C.

Finally, in Chapter 5, we started a study of the diagonal factorisation of finite non-abelian groups like the study of the factorisation of abelian groups by introducing the notion of diagonal factorisation and proving some basic results. Also, we considered the properties of diagonal permutation groups $D(T, d)$ and investigated the relationship between these groups and the diagonal factorization. In particular, we showed that a diagonal group $D(T, 2)$ is non-separating if and only the group T admits diagonal factorisation. In addition, we proved that $D(A_n, 2)$ is non-separating and $D(T, d)$ for $d \geq 3$, is non-synchronising. We ended this chapter by showing that the separating and synchronisation properties are equivalent for diagonal groups.

Chapter 3

Almost simple permutation groups

The purpose of this chapter is to investigate the synchronisation and separation properties of two important examples of primitive almost simple groups. Firstly, the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$ (we call this the first group). Secondly, the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of uniform l-partitions of an n-set, $\{1, ..., n\}$, into subsets of size k where $n = kl$ (we call this the second group).

The synchronisation and separation properties of the two groups are closely related to Steiner systems and intersecting systems. In 2014, Peter Keevash (see Theorem 3.11) answered an old open problem considering the existence of Steiner systems, that is, for large enough n in terms of k and t, a Steiner systems $S(t, k, n)$ exists if and only if the necessary divisibility conditions on the parameters are satisfied. In the first part of this chapter, we consider the first group and determine when it is synchronising and separating for small values of k. These results are evidence for making a conjecture. This conjecture could be regarded as a significant extension of the theorem of Keevash. In the second part of this chapter, the second group is studied. We show that it is non-synchronising for $l > 2$ and for $l = 2$ we give results and a conjecture similar to those of the first part.

3.0.1 Summary of the results

In the first part, we defined the concepts of separation and synchronisation for association schemes and showed in Theorem 3.1 and Theorem 3.2, that a finite permutation group is separating (synchronising) if and only if the association scheme which is obtained from the orbital graphs of the group, is separating (synchronising). Then, we proved some results which are important tools in our study of the separation and synchronisation properties. Corollary 3.6 shows that if a graph Γ in the scheme has the product of the clique and the co-clique numbers equals the number of the vertices, then the smallest eigenvalue τ divides the degree $deg(\Gamma)$ of the graph. Furthermore, we must have clique number equals to $1 - deg(\Gamma)/\tau$. Also, we proved that if there is a Steiner system $S(n, k, t)$, then the first group is non-separating, Theorem 3.17. Then, we showed that the vertex set of the graph in which two k-sets are joined if they intersect in fewer than t points, cannot be partitioned into co-cliques of EKR-type, by Theorem 3.18, and it can be partitioned into cliques if and only if there is a large set of Steiner system $S(t, k, n)$, Theorem 3.19.

For large enough n and $k = 2$ and 3, we showed that the first group is non-synchronising (non-separating) if and only if there is a Steiner system $S(t, k, n)$ for some t, Theorem 3.22 and Theorem 3.31. Also, for large enough n and $k = 4, 5$, we showed that the first group is non-separating if and only if the divisibility conditions (equation 3.3) for $S(t, k, n)$ are satisfied for some t with $0 < t < k$, Theorem 3.41 and Theorem 3.42. An interesting example of a non-separating, synchronising permutation group is stated in Theorem 3.42.

In view of the previous results, we conjectured that, for large n in terms of k and t, the first group is non-separating if and only if the divisibility conditions (equation 3.3) for $S(t, k, n)$ are satisfied for some t with $0 < t < k$, Conjecture 2. Moreover, Conjecture 7 suggests that for large n the first group is non-synchronising if and only if there is a large set of Steiner system $S(t, k, n)$ for some t. In Theorem 3.52 and Theorem 3.53, we proved that for large n some special graphs in Johnson association scheme cannot have the product of the clique and the co-clique numbers equals the number of vertices. In Conjecture 8, we suggests that all the co-cliques of the graph in which two k-sets ($k > 3$) are joined if they intersect in one point, are of the EKR-type. The previous results appeared as a joint paper with John Bamberg and Peter Cameron [1].

In the second part, we proved that the second group is non-synchronising if $l > 2$, Theorem 3.69. For the case $l = 2$, we showed that for $k = 2, 3, 4, 5, 6$, the second group is non-synchronising if and only if there is a resolvable Steiner system $S(k-1, k, 2k)$. Then, for $k > 6$ we showed that if there is such a system, then the second group is non-synchronising, so non-separating. Theorem 3.68. Also, we conjectured that the converse holds, Conjecture9.

3.1 First group and Johnson association schemes

Let Ω be the set of k-subsets of the n-set,$\{1 \ldots n\}$, and let G be the group induced by the action of $\mathrm{Sym}(n)$ on the set Ω. We will assume that $n \geq 2k$ as the actions of the symmetric group on k-subsets and $(n-k)$-subsets are equivalent. Since each action results in an association scheme, Cameron and Kazanidis techniques (see Theorem 2.23 and Theorem 2.24) will be used in our investigations as described in

Section 2.3.3. This requires checking the clique, co-clique and chromatic numbers of G-invariant graphs Γ, that is $G \leq \mathrm{Aut}(\Gamma)$. These are the unions of the orbital graphs of the action of $\mathrm{Sym}(n)$ on Ω. There are k orbital graphs and they are given by the following relations:

$$O_i = \{(A, B) : |A \cap B| = k - i,\ 1 \leq i \leq k\}.$$

The adjacency matrices of these relations (graphs) with the relation of equality define an association scheme known as the **Johnson association scheme** $\mathcal{J}(n, k)$. It is clear that the group G is transitive (the Johnson association scheme is transitive). It is imprimitive for $n = 2k$ (we leave this till Section 3.2) and primitive for $n > 2k$ [81]. This is because a transitive permutation group H on a set V is primitive if and only if the stabiliser of a point is a maximal subgroup in H. The stabiliser of a k-subset is the group $S_k \times S_{n-k}$ which is maximal when $n > 2k$. It is clear that when $k = 1$, the group G is 2-transitive and therefore, separating. For $k \geq 2$ we need to develop some tools.

The notions of synchronisation and separation can be extended to primitive association schemes. Adopting the definition from permutation group theory, we say that a primitive association scheme is **non-synchronising** if there is a non-trivial graph in the scheme with clique number equal to its chromatic number, and is **synchronising** otherwise. In the same manner, a primitive association scheme is **non-separating** if there is a non-trivial graph in the scheme such that the product of its clique number and its co-clique number is equal to the number of vertices, and is **separating** otherwise. Also, it is not difficult to prove the following theorems.

Theorem 3.1. *Let G be the group induced by the action of the symmetric group* $\mathrm{Sym}(n)$ *on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$ and $\mathcal{A}$ be the* *association scheme defined by orbital graphs of G. Then G is non-separating if and only if $\mathcal{A}$ is non-separating.*

Proof. First, assume that the group G is non-separating, then by Theorem 2.24 there is a non-trivial graph Γ such that the product of the clique number $\omega(\Gamma)$ and the co-clique number $\alpha(\Gamma)$ is equal to the number of vertices $|V(\Gamma)|$ such that $G \leq \mathrm{Aut}(\Gamma)$. By the definition of $\mathcal{A}$, Γ is a graph in the scheme. Also, by the definition of non-separating association schemes, $\mathcal{A}$ is non-separating.

Second, Assume that the association scheme $\mathcal{A}$ is non-separating, then there is a non-trivial graph Γ such that the product of the clique number $\omega(\Gamma)$ and the co-clique number $\alpha(\Gamma)$ is equal to the number of vertices $|V(\Gamma)|$. Note that $G \leq \mathrm{Aut}(\Gamma)$ and by Theorem 2.24, G is non-separating. $\square$

Theorem 3.2. *Let G be the group induced by the action of the symmetric group* $\mathrm{Sym}(n)$ *on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$ and $\mathcal{A}$ be the association scheme defined by the orbital graphs of G. Then G is non-separating if and only if $\mathcal{A}$ is non-synchronising.*

Proof. First, assume that the group G is non-synchronising, then by Theorem 2.23 there is a non-trivial graph Γ such that its clique number $\omega(\Gamma)$ is equal to its chromatic number $\chi(\Gamma)$ and $G \leq \mathrm{Aut}(\Gamma)$. By the definition of $\mathcal{A}$, the graph Γ is in the scheme. Also, by the definition of non-synchronising association schemes, $\mathcal{A}$ is non-synchronising.

Second, Assume that the association scheme $\mathcal{A}$ is non-synchronising, then there is a non-trivial graph Γ such that its clique number $\omega(\Gamma)$ is equal to its chromatic number. Note that $G \leq \mathrm{Aut}(\Gamma)$ and by Theorem 2.23, G is non-synchronising. $\square$

Assume that $\mathcal{A} = \mathcal{J}(n,k)$, a graph $\Gamma_I(n,k)$, $I \subset \{1,...,k\}$ in the scheme is defined to have the set of k-subsets as its vertex set and two k-subsets (vertices) A, B are adjacent if $|A \cap B| = k - i$, where $i \in I$. There are two particular cases of $\Gamma_I(n,k)$ that will be very important, for which we introduce a different notation:

- $\Delta_t(n,k) = \Gamma_{\{k-t+1,...,k\}}(n,k)$, the graph in which two k-sets are joined if they intersect in fewer than t points;
- $\Phi_t(n,k) = \Gamma_{\{1,...,k-t\}}(n,k)$, the complement of $\Delta_t(n,k)$, in which two k-sets are joined if they intersect in at least t points.

We mentioned in Section 2.3 that vertex-transitive graphs and graphs in commutative association schemes have the property that the product of the clique number and the co-clique number is at most the number of vertices, although no class is contained in the other. We called the bound in inequality

$$\omega(\Gamma) \cdot \alpha(\Gamma) \leq |V(\Gamma)|, \tag{3.1}$$

the ***clique–co-clique bound***.

Delsarte [29] uses the matrix of eigenvalues and the dual matrix of eigenvalues to prove bounds on the clique and co-clique numbers of graphs in Johnson association scheme.

Theorem 3.3. *Let Γ be a graph in a association scheme $\mathcal{A}$ on n vertices. If Γ has degree $deg(\Gamma)$ and its least eigenvalue is τ, then the clique number is bounded above by $1 - \frac{deg(\Gamma)}{\tau}$.*

The following results are consequences of the previous theorem and Theorem 2.27.

Corollary 3.4. *Suppose* Γ *is a graph from an association scheme* $\mathcal{A}$ *on* n *vertices, and suppose a clique* C *and coclique* S *meet the bound; that is* $|C|\cdot|S| = n$*. Then the Schur product* [1] *of the MacWilliams transforms of* C *and* S *equals* $(n, 0, \ldots, 0)$.

For a bound on the co-clique number we have a result by Lovász which can be stated as:

Theorem 3.5. *[55] Let* Γ *be a graph in an association scheme* $\mathcal{A}$ *on* n *vertices. If* Γ *has degree* $deg(\Gamma)$ *and its least eigenvalue is* τ*, then the co-clique number is bounded above by* $n(1 - \frac{deg(\Gamma)}{\tau})^{-1}$.

Corollary 3.6. *Suppose* Γ *is a graph from an association scheme* $\mathcal{A}$ *on* n *vertices, and suppose* $\alpha(\Gamma)\omega(\Gamma) = n$*. Then* $\omega(\Gamma) = 1 - \deg(\Gamma)/\tau$*, where* τ *is the smallest eigenvalue of* Γ*, and in particular,* τ *divides* $\deg(\Gamma)$.

Proof. Let τ be the smallest eigenvalue of Γ. By the result of Lovász [55], $\alpha(\Gamma) \leq \frac{n}{1-\deg(\Gamma)/\tau}$. So since $\alpha(\Gamma)\omega(\Gamma) = n$, we have $n \leq \omega(\Gamma)n/(1 - \deg(\Gamma)/\tau)$ and hence $1 - \deg(\Gamma)/\tau \leq \omega(\Gamma)$. On the other hand, by Theorem 3.3 we have $\omega(\Gamma) \leq 1 - \deg(\Gamma)/\tau$. Therefore, we obtain equality $\omega(\Gamma) = 1 - \deg(\Gamma)/\tau$. $\square$

In addition, Delsarte [29, Section 4.2.1] finds simple expressions for the eigenvalues of the Johnson scheme. These expressions are known as ***Eberlein polynomials***, or ***dual Hahn polynomials***. Given an integer $0 \leq j \leq k$, we define the Eberlein polynomial $E_j(x)$ in the indeterminate x, as follows:

$$E_j(x) := \sum_{t=0}^{j} (-1)^{j-t} \binom{k-t}{j-t} \binom{k-x}{t} \binom{n-k+t-x}{t}. \tag{3.2}$$

[1] Schur product of two matrices $A = [a_{i,j}]$ and $B = [b_{i,j}]$ is the matrix $A \circ B = [a_{i,j}b_{i,j}]$.

Now the entries of the dual matrix of eigenvalues are given by the following theorem.

Theorem 3.7. *[29, Theorem 4.6] The matrix P of eigenvalues and the dual matrix of eigenvalues Q of the Johnson scheme $\mathcal{J}(n,k)$ are given by*

$$P_j(i) = E_j(i), \quad Q_i(j) = \frac{\binom{n}{i} - \binom{n}{i-1}}{\binom{k}{j}\binom{n-k}{j}} E_j(i),$$

for $i, j = 0, 1, \ldots, k$.

These results will be used in our investigation but first we need some background on Steiner systems.

3.1.1 Intersecting systems and Steiner systems

Let n and k be positive integers such that $n \geq k$ and let $\binom{n}{[k]}$ denote the set of all k-subsets of $\{1, .., n\}$. If $T \subseteq \{0, \ldots, k-1\}$, then a T-**intersecting set** F is a subset of $\binom{n}{[k]}$ such that the size of the intersection of any two members of F is in T. An edge set of a graph Γ_I in a Johnson association scheme $\mathcal{J}(n,k)$ is determined by the set of intersection sizes $\{k - i : i \in I\}$ of the k-subsets. Therefore, a clique and a co-clique in such a graph are intersecting sets in the set of k-subsets. Some of these sets have special properties and special names.

A **Steiner system** $S(t,k,n)$, for $0 < t < k < n$, is a collection $\mathcal{B}$ of k-subsets of $\{1, \ldots, n\}$ with the property that any t-subset of $\{1, \ldots, n\}$ is contained in a unique member of $\mathcal{B}$. It is well-known that, for $0 \leq i \leq t-1$, the number of members of $\mathcal{B}$ containing an i-subset of $\{1, \ldots, n\}$ is $\binom{n-i}{t-i}/\binom{k-i}{t-i}$, independent of the choice of i-set. Thus, necessary conditions for the existence of $S(t,k,n)$ are that

$$\binom{k-i}{t-i} \text{ divides } \binom{n-i}{t-i} \text{ for } 0 \leq i \leq t-1. \tag{3.3}$$

We refer to these conditions as the ***divisibility conditions***.

A **resolution class** or **parallel class** in a Steiner system is a set of blocks that partition the point set. A **resolvable Steiner system** $S(t,k,n)$ is a system with the property that its block set admits a partition into parallel classes.

A ***projective plane*** of order q is a Steiner system $S(2, q+1, q^2+q+1)$ for some integer $q > 1$. Projective planes of all prime power orders exist, and none are known for other orders. A **large set** of of Steiner system $S(t,k,n)$ is a partition of the k-subsets of an n-set into Steiner systems $S(t,k,n)$.

An important result which provides a bound on the clique number of orbital graphs is known as the non-uniform Fisher's inequality:

Theorem 3.8. *[44, Theorem 1.11] Let X be a non-empty finite set and F a family of subsets of X such that the cardinality of the intersection of any two distinct members of F is the same positive integer. Then $|F| \leq |X|$.*

Another important result is Baranyai's Theorem [12]:

Theorem 3.9. *[76, Theorem 38.1] If k is an integer that divides n, and Ω is the set of k-subsets of an n-set, then Ω can be partitioned into parallel classes.*

Corollary 3.10. *[6, Theorem 6.2] If k divides n, then the Johnson association scheme $\mathfrak{J}(n,k)$ is non-synchronising*

In a remarkable recent result, Keevash showed:

Theorem 3.11. *[48, Theorem 1.4] There exists a function $F(t,k)$ such that, if $n \geq F(t,k)$ and the divisibility conditions are satisfied, then a Steiner system $S(t,k,n)$ exists.*

Theorem 3.12. *[76, Theorem 19.2] For $n > k$, the number of k-subsets in a Steiner system $S(t,k,n)$, is $\binom{n}{t}/\binom{k}{t}$.*

Now, consider the graph $\Delta_t(n,k)$, its clique number has an upper bound.

Lemma 3.13. *The graph $\Gamma_t(n,k)$ has clique number less bounded above by $\binom{n}{t}/\binom{k}{t}$. Moreover, the clique number is equal to $\binom{n}{t}/\binom{k}{t}$ if and only if there is a Steiner System $S(t,k,n)$.*

Proof. In the graph $\Delta_t(n,k)$ any two vertices are adjacent if the size of their interaction is less than t. Also, the size of a clique number in this graph is less than or equal to $\binom{n}{t}/\binom{k}{t}$, by double counting. If equality holds, the vertices in a clique of size $\binom{n}{t}/\binom{k}{t}$ define a Steiner system $S(t,k,n)$, by previous theorem. □

Moreover, there is a co-clique in this graph of size $\binom{n-t}{k-t}$, consisting of all the k-sets containing a fixed t-set. (We say that such a co-clique is of ***EKR type*** (Erdős–Ko–Rado type), since [32, Theorem 2] asserts that they are the largest co-cliques provided that n is sufficiently large). The exact bound in the Erdős–Ko–Rado theorem, proved by Wilson :

Theorem 3.14. *[82] Suppose that $n > (t+1)(k-t+1)$. Then a co-clique in the graph $\Delta_t(n,k)$ has size at most $\binom{n-t}{k-t}$, with equality if and only if it is of EKR type.*

The following result shows that if there is Steiner system $S(t,k,n)$, then the bound on n in Wilson's Theorem is satisfied.

Theorem 3.15. *In a non-trivial Steiner system $S(t, k, n)$ with $n > k$, we have $n \geq (t+1)(k-t+1)$.*

Proof. There are $\binom{n}{t+2}$ subsets of size $t+2$. Of these, $\binom{n}{t}\binom{k}{t+2}/\binom{k}{t}$ are subsets of blocks and $\binom{n}{t}\binom{k}{t+1(n-k)}/\binom{k}{t}$ have the property that some block contains $t+1$ of them. (There are no overlap among these blocks, since a $(t+2)$-set cannot have $t+1$ or more points in common with two different blocks.) Thus,

$$\binom{k}{t}\binom{n}{t+2} \geq \binom{n}{t}\left(\binom{k}{t+2} + \binom{k}{t+1}(n-k)\right),$$

which reduces to

$$(n-k)(n-(t+1)(k-t+1)) \geq 0,$$

implies

$$n \geq (t+1)(k-t+1).$$

□

Theorem 3.16. *If a non-trivial Steiner system $S(t, k, n)$ exists, then the product of the clique number and co-clique number in $\Delta_t(n, k)$ is equal to the number of vertices, and the Johnson scheme $\mathfrak{J}(n, k)$ is non-separating.*

Proof. Assume that there is non-trivial Steiner system $S(t, k, n)$, then by Theorem 3.12, it is a clique of size $\binom{n}{t}/\binom{k}{t}$ in the graph $\Delta_t(n, k)$. Also, by Theorem 3.15, $n \geq (t+1)(k-t+1)$ and by Theorem 3.14, there is a co-clique in this graph of size $\binom{n-t}{k-t}$, consisting of all the k-sets containing a fixed t-set. Moreover, it is easily checked that

$$\binom{n-t}{k-t} \cdot \binom{n}{t} \Big/ \binom{k}{t} = \binom{n}{k}.$$

Therefore, there is a graph in the Johnson scheme $\mathfrak{J}(n, k)$ such that the product of the clique and the co-clique numbers is equal to the number of vertices. Then, $\mathfrak{J}(n, k)$ is non-separating scheme. $\square$

Theorem 3.17. *If a non-trivial Steiner system $S(t, k, n)$ exists, then the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of k-element subsets of an n-set, is non-separating.*

What about synchronisation?

An association scheme is non-separating if there is a graph in the scheme for which the product of the clique and the co-clique numbers is equal to the number of vertices, by definition. Given such a situation, by the definition of non-synchronising association scheme there are two ways that synchronisation can fail: either there is a partition of the vertices into co-cliques of maximal size, so that the clique number and chromatic number are equal, or there is a partition into cliques of maximal size, so that this equality holds in the complementary graph.

We first observe that, the graph $\Delta_t(n, k)$ cannot have clique number equal to chromatic number.

Theorem 3.18. *For $t < k < n$, there is no partition of the set of k-subsets of an n-set into co-cliques of EKR type in the graph $\Delta_t(n, k)$.*

Proof. First we note that, if $k \geq 2t$, then any two t-sets are contained in some k-set; so any two sets of EKR type intersect. So we may assume that $k < 2t$.

A set S of EKR type consists of all the k-sets containing a fixed t-set T, which we call its *kernel*; we denote S by $S(T)$. Now, if T_1 and T_2 are t-sets with $|T_1 \cap T_2| \geq 2t - k$, then $|T_1 \cup T_2| \leq k$, and so $S(T_1) \cap S(T_2) \neq \varnothing$. So, in a family of pairwise disjoint sets of EKR type, the kernels are t-sets which intersect in at most $2t-k-1$ points.

The number of kernels in such a collection is at most $\binom{n}{2t-k}/\binom{t}{2t-k}$.

The size of a co-cliques of EKR type in the graph $\Delta_t(n,k)$ is $\binom{n-t}{k-t}$. Also, if there is a partition of the set of k-subsets of an n-set into co-cliques of EKR type in the graph, the number of the parts in the partition must be $\binom{n}{t}/\binom{k}{t}$; so we are done if we can show that

$$\binom{n}{t}\Big/\binom{k}{t} > \binom{n}{2t-k}\Big/\binom{t}{2t-k}.$$

For this, it is enough to show that the following claims are true:

(i) $\displaystyle\binom{n}{2t-k}\frac{t!\,(n-2t+k)!}{k!\,(n-t)!} = \binom{n}{t}\binom{t}{2t-k}\Big/\binom{k}{t}$;

(ii) $(t!\,(n-2t+k)!\,)/(k!\,(n-t)!\,) > 1$.

For (i), we have

$$\begin{aligned}\binom{n}{t}\binom{t}{2t-k}\Big/\binom{k}{t} &= \frac{n!}{(n-2t+k)!\,(2t-k)!}\,\frac{t!\,(n-2t+k)!}{k!\,(n-t)!}\\ &= \binom{n}{2t-k}\frac{t!\,(n-2t+k)!}{k!\,(n-t)!}.\end{aligned}$$

For (ii),

$$\frac{t!\,(n-2t+k)!}{k!\,(n-t)!} = \frac{(n-2t+k)(n-2t+k-1)\cdots(n-2t+k-(k-t)+1)}{k(k-1)\cdots(k-(k-t)+1)}$$

And since $n-2t+k > k$ for $n \geq 2k$ we have that

$$\frac{t!\,(n-2t+k)!}{k!\,(n-t)!} > 1. \qquad \square$$

The previous theorem shows that, if $n > (t+1)(k-t+1)$, then $\Delta_t(n,k)$ cannot have clique number equal to chromatic number, since the maximum-size co-cliques are of EKR type.

Theorem 3.19. *The graph $\Phi_t(n,k)$ has clique number equal to chromatic number if and only if there is a large set of Steiner systems $S(t,k,n)$.*

Proof. Assume that the graph $\Phi_t(n,k)$ has clique number equal to chromatic number, then there is a partition of the vertex-set into co-cliques. From Lemma 3.13 a co-clique in the graph $\Phi_t(n,k)$ is a Steiner system $S(t,k,n)$. Therefore, the vertex set of the graph admits a partition into Steiner systems. This is by definition, a large set of Steiner systems. The converse is done by similar way. □

For small n, non-synchronisation can also arise in one of two ways: either because there are other large co-cliques in $\Delta_t(n,k)$, or because one of the other graphs $\Gamma_I(n,k)$ in the association scheme has clique number equal to chromatic number.

3.1.2 $k = 2, 3, 4$ and 5

Here we investigate the synchronisation and separation properties of the first group G for small values of k. We do this by studying the two properties of the Johnson scheme $\mathcal{J}(n,k)$. Also, we illustrate with examples the discussion at the end of the previous subsection.

Remark 3.20. *In the following subsection, we will state our results in the language of association schemes. However, the main results will be restated in the language of group theory.*

3.1.2.1 The case $k = 2$

The group G is non-separating and non-synchronising is and only if n is even.

Theorem 3.21. *The Johnson scheme $\mathcal{J}(n,3)$ is non-synchronising and non-separating if and only if n is even.*

Proof. The association scheme $\mathcal{J}(n,2)$ has $\frac{n(n-1)}{2}$ vertices and two orbital graphs. One graph Γ is the graph with two vertices adjacent if and only if they intersect in one point and the other is its complement. The clique number of Γ is $n-1$. If $\mathcal{J}(n,2)$ is non-separating we must have the product of the clique and the co-clique numbers is equal to the number of vertices. Thus, $(n-1)$ dividing $\frac{n(n-1)}{2}$, by the definition of non-separating scheme, and this is possible if and only if n is even. Therefore, for n odd the scheme $\mathcal{J}(n,2)$ is separating and consequently synchronising.

What can we say if n is even? It is not difficult to see that the graph Γ has co-clique number equal to $\frac{n}{2}$, so $\mathcal{J}(n,2)$ is non-separating. If the scheme is non-synchronising, we must have the clique number equal to the chromatic number in the graph Γ or its complement $\bar{\Gamma}$. We have the first case, but not the other. This is because that Γ admits a partition into co-cliques, which follows from Baranyai's Theorem 3.9. $\square$

Theorem 3.22. *[6, Example 4.1] Let $n \geq 5$, and let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(n)$ *on the set of* 2*-element subsets of* $\{1,\ldots,n\}$. *Then the following are equivalent:*

(a) G is non-synchronising;

(b) G is non-separating;

(c) n is even.

3.1.2.2 The case $k = 3$

We start by the following results when $n = 7$ and 8:

The case $k = 3$, $n = 7$. The group G is non-separating and non-synchronising.

Lemma 3.23. *The Johnson scheme $\mathfrak{J}(7, 3)$ is non-separating and non-synchronising.*

Proof. Consider the graph $\Delta_2(7, 3)$, where two 3-subsets are adjacent if they are disjoint or intersect in one point. By Lemma 3.13 a maximum clique is the block set of a copy of $S(2, 3, 7)$. Therefore, the Fano plane is a clique in the graph with size 7. The graph $\Delta_2(7, 3)$, also, has a co-cliques of the EKR type and size 5 (all 3-sets containing a given two points). Since the graph $\Delta_2(7, 3)$ in the Johnson scheme $\mathfrak{J}(7, 3)$ and has the property that the product of the clique and the co-clique numbers equal to the number of vertices, this association scheme is non-separating. This graph cannot show non-synchronisation of the association scheme $\mathfrak{J}(7, 3)$ because Cayley [24] showed the non-existence of large set of Fano planes $S(2, 3, 7)$ and Theorem 3.18 shows the non-existence of partition of the vertex set of the graph into co-cliques of EKR type.

However, there are two graphs to check for non-synchronisation. One is the graph $\Gamma_{\{2\}}(7, 3)$, where two 3-subsets are adjacent if they intersect in one point. The Fano plane $S(2, 3, 7)$ is a clique of size 7 in the graph, by Fisher's Theorem 3.8. There are co-cliques of size 5 defined as follows: let L be a line of the Fano plane, and take L together with the four 3-sets disjoint from it. Furthermore, the seven such sets obtained by performing this construction for each line of the Fano plane partition the 35 sets of size 3 into seven co-cliques of size 5. So this graph has chromatic number equal to clique number. Therefore, the Johnson scheme $\mathfrak{J}(7, 3)$ is non-synchronising. □

Lemma 3.24. *Let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(7)$ *on the set of* 3*-element subsets of* $\{1, ..., 7\}$*. Then G is non-separating and non-synchronising.*

The case $k = 3$, $n = 8$. The group G is non-separating and non-synchronising.

Lemma 3.25. *The Johnson scheme* $\mathcal{J}(8, 3)$ *is non-separating and non-synchronising.*

Proof. Consider the graph $\Gamma_{\{2\}}(8, 3)$, the Fano plane gives us a 7-clique in this graph. Now the eight 3-sets consisting of a line L, three sets each comprising two points of L and the point outside the Fano plane, and the four sets consisting of three of the four points of the Fano plane outside L, form a co-clique; doing this for the seven lines we obtain a partition of the 56 sets of size 3 into seven co-cliques of size 8, so this graph has the clique number equal to the chromatic number. Therefore, The Johnson scheme $\mathcal{J}(8, 3)$ is non-synchronising and consequently, it is non-separating.

Another way of viewing this is to observe that the Fano plane has an extension to a $S(3, 4, 8)$ whose blocks fall into 7 parallel classes with two blocks in each; the eight 3-sets contained in a block of a parallel class form a co-clique, and we obtain seven such sets, one for each parallel class. $\square$

Lemma 3.26. *Let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(8)$ *on the set of* 3*-element subsets of* $\{1, ..., 8\}$*. Then G is non-separating and non-synchronising.*

The case $k = 3$, $n \geq 9$. Now we would like to consider the case $n \geq 9$ and $k = 3$ to show that the Johnson association scheme $\mathcal{J}(n, 3)$ is non-synchronising if and only if $\mathcal{J}(n,3)$ is non-separating if and only if there is a Steiner system $S(t,3,n)$ for some $1 \le t \le 2$. First we need the following technical lemma.

Lemma 3.27. *Let $n \ge 9$ and $\Delta := \Gamma_{\{2\}}(n,3)$. Then $\omega(\Delta)\alpha(\Delta) < |V(\Delta)| = \binom{n}{4}$.*

Proof. The matrix P of eigenvalues of the Johnson scheme $\mathcal{J}(n,3)$ can be calculated by using Eberlein polynomials (equation 3.2) and Theorem 3.7. The software Mathematica [83] was used to calculate and display the matrices P and Q.

$$P = \begin{pmatrix} 1 & 3(n-3) & \frac{3}{2}(n-4)(n-3) & \frac{1}{6}(n-5)(n-4)(n-3) \\ 1 & 2n-9 & \frac{1}{2}(n-9)(n-4) & -\frac{1}{2}(n-5)(n-4) \\ 1 & n-7 & 11-2n & n-5 \\ 1 & -3 & 3 & -1 \end{pmatrix}.$$

For the graph $\Gamma_{\{2\}}(n,3)$, the eigenvalues are the entries of the third column:

$$\frac{3}{2}(n-4)(n-3), \frac{1}{2}(n-9)(n-4), 11-2n, 3$$

The degree is the first eigenvalue, by Theorem 2.29, which is $\frac{3}{2}(n-4)(n-3)$, and the smallest eigenvalue is $11-2n$ as $n \ge 9$. By Corollary 3.6 if Γ_2 has the product of the clique and the co-clique numbers is equal to the number of vertices then the smallest eigenvalue divides the degree. Thus, by elementary number theory this is possible only if $n \in \{13, 28\}$. If $n = 13$, then $1 - \frac{deg(\Gamma_{\{2\}}(13,3))}{\tau}$ is 10 which does not divide the number of vertices (286), so $\omega(\Gamma_{\{2\}}(13,3))\alpha(\Gamma_{\{2\}}(13,3)) < \binom{13}{3}$. For $n = 28$, by GAP/GRAPE [68, 72][2] we can find the clique number $\omega(\Gamma_{\{2\}}(28,3))$ which is 13 and the co-clique number which is 28. Clearly, the product of these two numbers does not equal to the number of vertices which is $\binom{28}{3}$. $\square$

[2]The share package GRAPE for the computer algebra system GAP contains an efficient clique finder.

We need the following result regarding the existence of Steiner systems:

Theorem 3.28. *[49] A Steiner systems $S(2,3,n)$ exists if and only if n is congruent to* 1 *or* $3 \pmod 6$.

Lemma 3.29. *For $n \geq 9$, the Johnson association scheme $\mathcal{J}(n,3)$ is non-separating if and only if there is a Steiner system $S(t,3,n)$ for some $1 \leq t \leq 2$ (n is congruent to* 0, 1 *or* $3 \pmod 6$*).*

Proof. By the previous theorem a Steiner system $S(2,3,n)$ exists if and only if n is congruent to 1 or 3 $\pmod 6$. Also, by Baranyai's Theorem 3.9 a Steiner system $S(1,3,n)$ exists if and only if 3 divides n. Consequently, a Steiner system $S(t,3,n)$ exists if and only if n is congruent to 0, 1 or 3 $\pmod 6$.

If a Steiner system $S(t,3,n)$ exists, then the Johnson scheme $\mathcal{J}(n,3)$ is non-separating, by Theorem 3.16.

The other direction is that if the scheme $\mathcal{J}(n,3)$ is non-separating then there is a Steiner system. To show this we consider all graphs $\Gamma_I(n,3)$ and their intersections. When $k=3$, the possible values of I are $\{\}$ and its complement $\{1,2,3\}$, $\{2\}$ and its complement $\{1,3\}$, $\{1\}$ and its complement $\{2,3\}$ and $\{3\}$ and its complement $\{1,2\}$. In the first value of I, the graphs are trivial. If the scheme is non-separating, then at least one of the graphs $\Gamma_{\{2\}}(n,3)$, $\Gamma_{\{1\}}(n,3)$ and $\Gamma_{\{3\}}(n,3)$ has the product of the clique and the co-clique numbers equals the number of vertices. If this is true for graphs $\Gamma_{\{1\}}(n,3)$ or $\Gamma_{\{3\}}(n,3)$, then the co-clique in $\Gamma_{\{1\}}(n,3)$ is $S(2,3,n)$ or the clique in $\Gamma_{\{3\}}(n,3)$ is $S(1,3,n)$, by Lemma 3.13. It remains to study the clique number and the co-clique number of the graph $\Gamma_{\{2\}}(n,3)$ and prove that the product of the two numbers does not equal to the number of vertices. However, this graph can be neglected in the study of synchronization and separation of the scheme. This is because the graph does not satisfy the equality in the clique–co-clique bound, by lemma 3.27. $\square$

Theorem 3.30. *Let $n \geq 9$, the Johnson association scheme $\mathfrak{J}(n,3)$ is non-separating if and only if $\mathfrak{J}(n,3)$ is non-synchronising (there is a Steiner system $S(t,3,n)$ for some $0 \leq t \leq 2$).*

Proof. By the previous lemma the Johnson scheme $\mathfrak{J}(n,3)$ is non-separating if and only if there is a Steiner system $S(1,3,n)$ or $S(2,3,n)$. A Steiner system $S(1,3,n)$ exists if and only if 3 divides n and there a large set of the Steiner system, by Baranyai's Theorem 3.9. Therefore, the complement of the graph $\Gamma_{\{3\}(n,3)}$ has the clique number equal to the chromatic number, by Theorem 3.19 and the scheme $\mathfrak{J}(n,3)$ is non-synchronising. In similar way, a Steiner system $S(2,3,n)$ exists if and only if n is congruent to 1 or 3 (mod 6) by Kirkman's Theorem 3.28. Also, there is a large set of Steiner systems of $S(2,3,n)$ if and only if n is "admissible[3] " and grater than 7, by the result of Lu and Teirlinck [71]. This is the same as that the graph $\Gamma_{\{1\}(n,3)}$ has the clique number equal to the chromatic number, by Theorem 3.19 and thus the scheme $\mathfrak{J}(n,3)$ is non-synchronising. $\square$

Theorem 3.31. *[6, Theorem 6.3] Let $n \geq 9$, and let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(n)$ *on the set of* 3*-element subsets of* $\{1,\ldots,n\}$. *Then the following are equivalent:*

(a) G is non-synchronising;

(b) G is non-separating;

(c) n is congruent to 0, 1 *or* 3 (mod 6).

[3] An admissible n means an integer n, which satisfies the divisibility conditions (see condition 3.3) with respect to the integers k and t.

3.1.2.3 The case $k = 4$

The group G is non-separating and non-synchronising.

The case $k = 4$, $n = 9$.

Lemma 3.32. *The Johnson scheme $\mathcal{J}(9,4)$ is non-separating and non-synchronising.*

Proof. we consider the graph $\Gamma_{\{1,3\}}(9,4)$ in the association scheme $\mathcal{J}(9,4)$, the Steiner system $S(3,4,8)$ has 14 blocks, any two meeting in 0 or 2 points. Thus, a copy of the blocks of $S(3,4,8)$ form a co-clique of size 14. We can construct a clique of the graph $\Gamma_{\{1,3\}}(9,4)$ as a set of 9 subsets of $\{1,...,9\}$ each has size 4, any two meeting in 1 or 3 points, as follows: partition $\{1,\ldots,9\}$ into three sets of size 3, arranged around a circle; now take the 4-subsets consisting of one part and a single point of the next (in the cyclic order). Therefore, the product of the clique and co-cliques numbers equal to the number of vertices. This means that the scheme $\mathcal{J}(9,4)$ is non-separating.

For the non-synchronisation, Breach and Street [17] showed that the 126 4-subsets of a 9-set can be partitioned into a so-called *overlarge set* of nine Steiner systems $S(3,4,8)$ (each omitting a point); indeed, this can be done in just two non-isomorphic ways, each admitting a 2-transitive group. This gives a colouring of the graph $\Gamma_{\{1,3\}}(9,4)$ corresponding to intersections 1 and 3, so its clique and chromatic numbers are equal. This means that the scheme $\mathcal{J}(9,4)$ is non-synchronising. (Another proof was given by Cameron and Praeger [61].) □

From the previous lemma and Theorem 3.1 and Theorem 3.2 we have the following:

Lemma 3.33. *Let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(9)$ *on the set of* 4*-element subsets of* $\{1,...,9\}$. *Then G is non-separating and* *non-synchronising.*

The case $k = 4$, $n \geq 10$. Now we would like to consider the case $n \geq 10$ and $k = 4$ to show that the Johnson association scheme $\mathcal{J}(n, 4)$ is non-separating if and only if there is a Steiner system $S(t, 4, n)$ for some $1 \leq t \leq 3$. By Theorem 3.16, if there is there is a Steiner system $S(t, 4, n)$ for some $1 \leq t \leq 3$, then the scheme $\mathcal{J}(n, 4)$ is non-separating. It remains to show the other direction. First we need the following technical lemma.

Theorem 3.34. *Let $n \geq 10$ and $I \in \{\{1, 3, 4\}, \{1, 3\}, \{1, 4\}, \{1, 2, 4\}\}$, and let $\Delta := \Gamma_I(n, 4)$. Then $\omega(\Delta)\alpha(\Delta) < |V(\Delta)| = \binom{n}{4}$, with one exception for $\Delta := \Gamma_{\{1,2,4\}}(13, 4)$.*

Proof. The matrix P of eigenvalues, and the dual matrix Q, of the Johnson scheme $\mathcal{J}(n, 4)$ can be calculated by using Eberlein polynomials 3.2. The software Mathematica [83] was used to calculate and display the matrices P and Q.

$$P = \begin{pmatrix} 1 & 4(n-4) & 3(n-5)(n-4) & \frac{2}{3}(n-6)(n-5)(n-4) & \frac{1}{24}(n-7)(n-6)(n-5)(n-4) \\ 1 & 3n-16 & \frac{3}{2}(n-8)(n-5) & \frac{1}{6}(n-16)(n-6)(n-5) & -\frac{1}{6}(n-7)(n-6)(n-5) \\ 1 & 2(n-7) & \frac{1}{2}((n-21)n+92) & -(n-9)(n-6) & \frac{1}{2}(n-7)(n-6) \\ 1 & n-10 & -3(n-8) & 3n-22 & 7-n \\ 1 & -4 & 6 & -4 & 1 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & n-1 & \frac{1}{2}(n-3)n & \frac{1}{6}(n-5)(n-1)n & \frac{1}{24}(n-7)(n-2)(n-1)n \\ 1 & \frac{1}{4}(3n-7) - \frac{3}{n-4} & \frac{(n-7)(n-3)n}{4(n-4)} & \frac{(n-10)(n-5)(n-1)n}{24(n-4)} & -\frac{(n-7)(n-2)(n-1)n}{24(n-4)} \\ 1 & \frac{(n-8)(n-1)}{2(n-4)} & \frac{(n-3)n((n-21)n+92)}{12(n-5)(n-4)} & -\frac{(n-8)(n-1)n}{6(n-4)} & \frac{(n-7)(n-2)(n-1)n}{12(n-5)(n-4)} \\ 1 & \frac{(n-16)(n-1)}{4(n-4)} & -\frac{3(n-9)(n-3)n}{4(n-5)(n-4)} & \frac{(n-1)n(3n-22)}{4(n-6)(n-4)} & -\frac{(n-7)(n-2)(n-1)n}{4(n-6)(n-5)(n-4)} \\ 1 & -\frac{4(n-1)}{n-4} & \frac{6(n-3)n}{(n-5)(n-4)} & -\frac{4(n-1)n}{(n-6)(n-4)} & \frac{(n-2)(n-1)n}{(n-6)(n-5)(n-4)} \end{pmatrix}.$$

Remark: In all cases we assume for the contrary that the product of the clique and co-clique numbers is equal to the number of vertices. For the first two cases we use the matrix P of eigenvalues and Corollary 3.6 to get a contradiction. Given our assumption, we reach a contradiction if one of the following holds:

1. $1-\deg(\Gamma_I(n,k))/\tau < n$, where I is a singleton, by Fisher inequality 3.8.
2. $1-\deg(\Gamma_I(n,k))/\tau$ or $\omega(\Gamma_I(n,k))$ does not divide $\binom{n}{k}$, by Corollary 3.6.
3. $1-\deg(\Gamma_I(n,k))/\tau$ is not equal $\omega(\Gamma_I(n,k))$, by Corollary 3.6.
4. the product of $\omega(\Gamma_I(n,k))$ and $\alpha(\Gamma_I(n,k))$ is not equal $\omega(\Gamma_I(n,k))$, using GAP.

The dual matrix Q is used for the other cases by applying Theorem 2.27 and Corollary 3.4.

Case $I=\{1,3,4\}$**:** The complement $\overline{\Delta}$ of $\Delta := \Gamma_{\{1,3,4\}}(n,4)$ is a graph of an association scheme (because it is $\Gamma_{\{2\}}(n,4)$). Consider the third column of P. The eigenvalues of $\overline{\Delta}$ are

$$3(n-5)(n-4),\quad \frac{3}{2}(n-8)(n-5),\quad \frac{1}{2}(n^2-21n+92),\quad 24-3n, 6.$$

The degree of $\overline{\Delta}$ is the first eigenvalue $3(n-5)(n-4)$, by Theorem 2.29. For $n \geq 11$, the fourth eigenvalue $24-3n$ is the smallest eigenvalue, so let us assume that $n \geq 11$. By Corollary 3.6, $24-3n$ divides $3(n-5)(n-4)$, and hence $8-n$ divides $(n-5)(n-4)$. So by elementary number theory, we have $n \in \{11, 12, 14, 20\}$.

The cases $n = 10, 11, 12, 14, 20$ can be settled each in turn. We can calculate $\omega(\overline{\Delta})$ with GAP/GRAPE [68, 72] and compare it to $1-\deg(\overline{\Delta})/\tau$, where τ is the smallest eigenvalue $24-3n$.

n	$\omega(\overline{\Delta})$	$1 - \deg(\overline{\Delta})/\tau$
10	7	11
11	7	15
12	7	15
14	7	16
20	9	21

We find that $\omega(\overline{\Delta})$ is never equal to $1 - \deg(\overline{\Delta})/\tau$ and so by Corollary 3.6, $\omega(\Delta)\alpha(\Delta) < \binom{n}{4}$.

Case $I = \{1, 2, 4\}$**:** This time, the complement graph $\overline{\Delta}$ is $\Gamma_{\{3\}}(n, 4)$. The eigenvalues of $\overline{\Delta}$ are

$$\frac{2}{3}(n-6)(n-5)(n-4),\ \frac{1}{6}(n-16)(n-6)(n-5),\ -(n-9)(n-6), 3n-22,\ -4$$

For $n \geq 13$, the third eigenvalue of $\overline{\Delta}$ is the smallest τ in the spectrum of $\overline{\Delta}$. So by Corollary 3.6, $n - 9$ divides $\frac{2}{3}(n-5)(n-4)$ and hence $n \in \{13, 14, 17, 19, 29, 49\}$ (by basic elementary number theory). For $n = 11$, the smallest eigenvalue of $\overline{\Delta}$ does not divide the degree. Thus by Corollary 3.6, we are left with $n \in \{10, 12, 13, 14, 17, 19, 29, 49\}$ to check. For the case $n = 13$, we have equality $\omega(\overline{\Delta})\alpha(\overline{\Delta}) = \binom{n}{4}$, which is the case with the existence a projective plane of order 4 (Steiner System $S(2, 4, 13)$). The cases $n = 10, 12, 14, 17, 19, 29, 49$ can be settled each in turn with the computer algebra system GAP/GRAPE:

n	$\omega(\overline{\Delta})$	$1-\deg(\overline{\Delta})/\tau$	$\alpha(\overline{\Delta})$	Comments
10	5	5	28	$\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{10}{4}$
12	9	9	45	$\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{12}{4}$
14	13	13	66	$\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{14}{4}$
17	13	14	**	$1-\deg(\overline{\Delta})/\tau \neq \omega(\overline{\Delta})$
19	13	15	**	$1-\deg(\overline{\Delta})/\tau \neq \omega(\overline{\Delta})$
29	13	21	**	$1-\deg(\overline{\Delta})/\tau \neq \omega(\overline{\Delta})$
49	**	34	**	$1-\deg(\overline{\Delta})/\tau \nmid \binom{49}{4}$

We put ** in places where the information is not provided because we do not need it.

Case $I = \{1,3\}$**:** Let Q be the dual matrix of eigenvalues. The second column of Q is

$$c = \frac{n-1}{4(n-4)}\left(4(n-4), 3n-16, 2(n-8), n-16, -16\right).$$

Let $u = (1, a, 0, x-a-1, 0)$ and $v = (1, 0, b, 0, y-b-1)$ be such that $a, b \geq 0$, $x-a-1, y-b-1 \geq 0$ and $xy = \binom{n}{4}$. By Theorem 2.27 u and v are the inner distributions of an arbitrary clique and co-clique of $\Gamma_I(n,k)$, respectively, attaining the clique-co-clique bound. The second entries of uQ and vQ are

$$\begin{aligned}(uQ)_1 = uc^T &= \frac{n-1}{4(n-4)}((2a+x+3)n - 16x)\\ (vQ)_1 = vc^T &= \frac{n-1}{4(n-4)}2((b+2)n - 8y).\end{aligned}$$

By Corollary 3.4, the product of these quantities is zero, which gives us two scenarios: $x = n\frac{2a+3}{16-n}$ or $y = n\frac{1}{8}(b+2)$. We will consider the former, with the additional assumption that $xy = \binom{n}{4}$. This then yields an expression for y:

$$y = -\frac{(n-16)(n-3)(n-2)(n-1)}{48a+72}.$$

Now $a, y \geq 0$, which implies that $n \leq 16$. So we will assume for the moment that $n \geq 16$. Therefore,

$$x = \frac{(n-3)(n-2)(n-1)}{3(b+2)}, \quad y = \frac{1}{8}(b+2)n.$$

We now consider the two equations $(uQ)_2(vQ)_2 = 0$ and $(uQ)_4(vQ)_4 = 0$, with the above values of x and y substituted in:

$$(b(n-10)+6(n-4))(a(b+2)(n-8)+b(2n-13)-(n-4)((n-10)n+7)) = 0$$
$$a(b+2)(n-8)+18(n-4)-b(n^2-12n+38) = 0.$$

The second equation gives us a value for a, which we can substitute into the first equation. This results in the following equation:

$$(n-5)(b(n-10)+6(n-4))(b-n+4) = 0.$$

However, $n \neq 5$ and $b(n-10)+6(n-4) \neq 0$ (as $b \geq 0$ and $n > 10$), so it follows that $b = n-4$ and hence

$$x = \frac{(n-3)(n-1)}{3}, \quad y = \frac{1}{8}(n-2)n.$$

Now suppose we have a $\{1,3\}$-clique S of size $x = (n-1)(n-3)/3$. Consider the members of S containing a point p, with p removed from each. This is a family of 3-sets of an $(n-1)$-set, any two intersecting in 0 or 2 elements. By Corollary 3.54, we know that there are at most $n-1$ of them. Now the standard double count gives

$$|S| \leq n(n-1)/4.$$

But this is smaller than $(n-1)(n-3)/3$ so long as n is at least 16. This leaves the cases $10 \leq n \leq 16$ to be considered (since we have excluded $n = 9$).

n	$\omega(\Gamma_I)$	$\alpha(\Gamma_I)$
10	9	14
11	9	14
12	9	15
13	13	15
14	13	21
15	13	21
16	13	28

Case $I = \{1, 4\}$**:** In this case, Theorem 3.53 will show that the result holds for sufficiently large n; indeed, the proof there works for $n \geq 46$. However, the intervening values are far too large for computation, so we use the Q-matrix methods.

Let $u = (1, a, 0, 0, x - a - 1)$ and $v = (1, 0, b, y - b - 1, 0)$ such that $a, b \geq 0$, $x - a - 1, y - b - 1 \geq 0$ and $xy = \binom{n}{4}$. By Theorem 2.27 u and v are the inner distributions of an arbitrary clique and co-clique of $\Gamma_I(n, 5)$, respectively, attaining the clique- co-clique bound. The second coordinates of uQ and vQ are

$$
\begin{aligned}
(uQ)_1 = uc^T =& \frac{(n-1)}{4(n-4)}((3a+4)n - 16x), \\
(vQ)_1 = vc^T =& \frac{(n-1)}{4(n-4)}((b+y+3)n - 16y).
\end{aligned}
$$

By Corollary 3.4, the product of these quantities is zero, which gives us two scenarios:

(i) $x = n\frac{3a+4}{16}$, or

(ii) $y = n\frac{b+3}{16-n}$.

Since $y \geq 0$, Case (ii) does not arise if we assume $n \geq 17$, which we will for now. So suppose we have Case (i). If we now consider the equation $(uQ)_2(vQ)_2 = 0$, we have

$$((n-1)(a(n-11)+2(n-8))+24x)((n-1)(b(n-11)+6n-39)-9(n-9)y) = 0. \tag{3.4}$$

Assuming (i), that is $x = n(3a+4)/16$, Equation (3.4) becomes

$$(2(a+2)n - 11a - 16)\left((n-1)(b(n-11)+6n-39)-9(n-9)y\right) = 0. \tag{3.5}$$

However, if the first term is zero, then $a = (16-4n)/(2n-11)$ which is negative for $n \geq 6$; a contradiction. Therefore, the second term in Equation (3.5) is zero. In other words, we have an expression for b in terms of n and y:

$$b = \frac{-6n^2 + 9ny + 45n - 81y - 39}{(n-11)(n-1)}.$$

If we now consider the equation $(uQ)_3(vQ)_3 = 0$, upon substitution of our value for b, we obtain an equation relating a, y and n:

$$(a(n^2-18n+68)+4(n-8)(n-4))(2n^4-34n^3-9n^2y+181n^2+123ny-335n-426y+186) = 0. \tag{3.6}$$

Having the first term in Equation (3.6) equal to zero leads to a contradiction, since in this case we would have

$$a = -\frac{4\left(n^2-12n+32\right)}{n^2-18n+68}$$

which is negative for $n \geq 13$. So let us now assume $n \geq 13$. Then the second term in Equation (3.6) is zero, which gives us an expression for y in terms of n (and we also obtain an expression for x):

$$x = \frac{n(n-3)(3n^2 - 41n + 142)}{8(2n^2 - 28n + 93)},$$
$$y = \frac{(n-1)(n-2)(2n^2 - 28n + 93)}{9n^2 - 123n + 426}.$$

However, $x \leq n$ (Corollary 3.54), which implies that $n \leq 8$; a contradiction.

This leaves us now to consider by computer the cases where $10 \leq n \leq 16$.

n	$\omega(\Delta)$	$\alpha(\Delta)$	Comments
10	10	15	$\omega(\Delta)\alpha(\Delta) < \binom{10}{4}$
11	10	15	$\omega(\Delta)\alpha(\Delta) < \binom{11}{4}$
12	10	**	$\omega(\Delta) \nmid \binom{12}{4}$
13	10	**	$\omega(\Delta) \nmid \binom{13}{4}$
14	11	26	$\omega(\Delta)\alpha(\Delta) < \binom{14}{4}$
15	15	**	see below
16	15	**	$\omega(\Delta) \nmid \binom{16}{4}$

In the case $n = 15$, we do not know exactly the co-clique number, but to have the equality $\omega(\Delta)\alpha(\Delta) = \binom{15}{4}$ we must have $\alpha(\Delta) = 91$. Using GAP as follow we can see that this cannot happen.

gap> 1314graph:=Graph(SymmetricGroup(15), Combinations([1..15],4), OnSets, > function(x,y) return (x<>y) and (Size(Intersection(x,y))in [0,3]); end);;

This is a command in GAP to build the graph $\Delta = \Gamma_{\{1,4\}}(15, 4)$.

C:=ComplementGraph(1314graph);;

This to build the complement.

Then we ask GAP to find a clique in the complement (co-clique in $\Delta = \Gamma_{\{1,4\}}(15, 4)$) of size 91.

gap> LC:=CompleteSubgraphs(C,91,0);

[ ]

This means that there is no such clique.

□

The following well-known results of Hanani on the existence of Steiner systems $S(t, 4, n)$ [39, 40] are important for our study.

Theorem 3.35. *[39] A Steiner systems $S(3, 4, n)$ exists if and only if n is congruent to* 1 *or* $4 \pmod{12}$.

Theorem 3.36. *[40] A Steiner systems $S(2, 4, n)$ exists if and only if n is congruent to* 2 *or* $4 \pmod 6$.

Now we have enough results to prove the following theorem:

Theorem 3.37. *For $n \geq 10$, if the Johnson association scheme $\mathfrak{J}(n, 4)$ is non-separating, then there exists a Steiner system $S(t, k, n)$ for some t with $0 < t < k$ ($n \equiv 0, 1, 2, 4, 8, 10 \pmod{12}$).*

Proof. Form Theorem 3.34, we know that when $n \geq 10$, there is not equality in the clique– co-clique bound (inequality 3.1) for the graph $\Gamma_I(n, 4)$, where $I \in \{\{1, 3, 4\}, \{1, 3\}, \{1, 4\}, \{1, 2, 4\}\}$ except the graph $\Gamma_{1,2,4}(13, 4)$ (when there is a projective plane). Any other non-trivial graph in the scheme is $\Gamma_I(n, 4)$ or its complement, where $I \in \{\{4\},\{3,4\},\{2,3,4\}\}$. If the scheme is non-separating, then one of the last three graphs has equality in the clique–co-clique bound. If we have equality, a maximum co-cliques in the graphs $\Gamma_{\{4\}}(n,4)$,$\Gamma_{\{3,4\}}(n,4)$ and $\Gamma_{\{2,3,4\}}(n,4)$ form a Steiner systems $S(1,4,n)$, $S(2,4,n)$ and $S(3,4,n)$, respectively, by Lemma 3.13. $\square$

From The previous theorem and Theorem 3.16, we have:

Theorem 3.38. *For $n \geq 10$, the Johnson association scheme $\mathfrak{J}(n,4)$ is non-separating if and only if there exists a Steiner system $S(t,k,n)$ for some t with $0 < t < k$.*

From The previous theorem and Keevash's Theorem, we have:

Theorem 3.39. *For $k = 4$ and $n \geq 10$, the Johnson association scheme $\mathfrak{J}(n,k)$ is non-separating if and only if the divisibility conditions (equation 3.3) for $S(t,k,n)$ are satisfied for some t with $0 < t < k$.*

We can state the previous two theorems in the language of group theory using Theorem 3.1.

Theorem 3.40. *Let $n \geq 10$, the permutation group G induced by the symmetric group $\mathrm{Sym}(n)$ on the set of 4-element subsets of $\{1,\ldots,n\}$ is non-separating if and only if there exists a Steiner system $S(t,k,n)$ for some t with $0 < t < k$ ($n \equiv 0,1,2,4,8,10 \pmod{12}$).*

Theorem 3.41. *Let $n \geq 10$, the permutation group G induced by the symmetric group $\mathrm{Sym}(n)$ on the set of 4-element subsets of $\{1,\ldots,n\}$ is non-separating if and only if the divisibility conditions (equation 3.3) for $S(t,k,n)$ are satisfied for some t with $0 < t < k$.*

What about synchronisation? Wilson's Theorem 3.14 ensures that maximal co-cliques are of EKR type, so G is non-synchronising if and only if a large set of Steiner systems exists. Baranyai's Theorem 3.9 ensures that G is not synchronising if $n \equiv 0 \pmod 4$, but existence of large sets of Steiner systems in the other cases is unresolved (except for $t = 2$, $n = 13$, [50]).

In particular, the existence of a Steiner system $S(3, 4, 10)$ shows that the symmetric group S_{10} acting on 4-sets is non-separating. However, it is synchronising. Our above results show that synchronisation could only fail if there were a large set of seven pairwise disjoint $S(3, 4, 10)$ systems. However, Kramer and Mesner [51] showed that there cannot be more than five such systems. For $k = 4$, synchronisation and separation fail to be equivalent for $\mathrm{Sym}(n)$ on k-sets, unlike the cases $k = 2$ and $k = 3$ described earlier. We will state this fact as theorem.

Theorem 3.42. *Let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(10)$ *on the set of* 4*-element subsets of* $\{1, \ldots, 10\}$. *Then G is non-separating but synchronising.*

This example and the example in [6] are the only known examples for the non-equivalent of the two properties.

3.1.2.4 The case $k = 5$

The case $k = 5$, $n = 11$. The group G is non-separating and non-synchronising.

Lemma 3.43. *The Johnson scheme $\mathfrak{J}(11, 5)$ is non-separating and non-synchronising.*

Proof. Consider the graph $\Gamma_{\{2,3,4\}}(11, 5)$ in the scheme, the Steiner system $S(4, 5, 11)$, whose blocks intersect in 1, 2 or 3 points, forms a 66-clique in the graph. A block together with the six 5-sets disjoint from it form a co-clique of size 7. Therefore the product of the clique and the co-clique numbers is equal to the number of vertices and the scheme $\mathfrak{J}(11,5)$ is non-separating.

There are 66 co-cliques can be obtained in this way. These co-cliques form a colouring of the graph $\Gamma_{\{2,3,4\}}(11,5)$. Then, the scheme $\mathfrak{J}(11,5)$ is non-synchronising.

$\square$

Lemma 3.44. *Let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(11)$ *on the set of* 5*-element subsets of* $\{1,...,11\}$*. Then G is non-separating and non-synchronising.*

The case $k=5$, $n=12$. The group G is non-separating and non-synchronising.

Lemma 3.45. *The Johnson scheme* $\mathfrak{J}(12,5)$ *is non-separating and non-synchronising.*

Proof. Consider the graph $\Gamma_{\{2,3,4\}}(12,5)$ in the scheme, the blocks of the Steiner system $S(4,5,11)$ form a 66-clique in the graph. A co-clique can be given by the set of the 5-subsets of the set $\{1,2,3,4,5,6\}$ and 5-subsets of the set $\{7,8,9,10,11,12\}$. Thus, the product of the clique and the co-clique numbers is equal to the number of vertices in the graph and the scheme $\mathfrak{J}(12,5)$ is non-separating.

The Steiner system $S(4,5,11)$ has an extension to a $S(5,6,12)$ whose blocks come in 66 parallel classes with two disjoint blocks in each, and the twelve 5-sets contained in a block of a fixed parallel class form a co-clique. and we obtain 66 such sets, one for each parallel class. Thus, chromatic number of the graph equal to clique number and the scheme is non-synchronising.

$\square$

Lemma 3.46. *Let G be the permutation group induced by the symmetric group* $\mathrm{Sym}(12)$ *on the set of 5-element subsets of* $\{1, ..., 12\}$. *Then G is non-separating and non-synchronising.*

The case $k = 5$, $n \geq 13$. Now we would like to consider the case $n \geq 13$ and $k = 5$ to show that the Johnson association scheme $\mathfrak{J}(n, 5)$ is non-separating if and only if there is a Steiner system $S(t, 5, n)$ for some $1 \leq t \leq 4$. By Theorem 3.16, if there is there is a Steiner system $S(t, 5, n)$ for some $1 \leq t \leq 4$, then the scheme $\mathfrak{J}(n, 5)$ is non-separating. It remains to show the other direction. First we need the following technical lemma.

Theorem 3.47. *Let $n \geq 13$, and $I \in \{\{1,2,3,5\}, \{1,2,4,5\}, \{1,3,4,5\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}\}$ and let $\Delta = \Gamma_I(n, 5)$, then $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$, except the graph $\Delta = \Gamma_{\{1,2,3,5\}}(21, 5)$.*

The proof of this result appears in Appendix A.1.

Theorem 3.48. *For $n \geq 13$, if the Johnson association scheme $\mathfrak{J}(n, 5)$ is non-separating, then there exists a Steiner system $S(t, k, n)$ for some t with $0 < t < k$.*

Proof. Form the Theorem 3.47, for $n \geq 13$, there is not equality in the clique–co-clique bound (equation 3.1) for the graph $\Gamma_I(n, 5)$ where I as in the theorem, except the graph $\Gamma_{\{1,2,3,5\}}(21, 5)$; that when we have a projective plane. any other non-trivial graph in the scheme is the graph $\Gamma_I(n, 5)$ or its complement, where $I \in \{\{5\}, \{4,5\}, \{3,4,5\}, \{2,3,4,5\}\}$. If the scheme is non-separating, then one of the last four graphs has equality in the clique– co-clique bound. By Lemma

3.13, if we have equality, a maximum co-cliques in the graphs $\Gamma_{\{5\}}(n,5)$,$\Gamma_{\{4,5\}}(n,5)$, $\Gamma_{\{3,4,5\}}(n,5)$ and $\Gamma_{\{2,3,4,5\}}(n,5)$ form a Steiner systems $S(1,4,n)$, $S(2,4,n)$, $S(3,4,n)$ and $S(4,5,n)$ respectively. $\square$

From the previous theorem and Theorem 3.16, we have:

Theorem 3.49. *For $n \geq 13$, the Johnson association scheme $\mathfrak{J}(n,5)$ is non-separating if and only if there exists a Steiner system $S(t,k,n)$ for some t with $0 < t < 5$.*

Theorem 3.50. *Let $n \geq 13$, the permutation group G induced by the symmetric group* $\mathrm{Sym}(n)$ *on the set of* 5*-element subsets of* $\{1,\dots,n\}$ *is non-separating if and only if there exists a Steiner system $S(t,5,n)$ for some t with $0 < t < 5$.*

Theorem 3.51. *For large enough n in terms of k and t, the permutation group G induced by the symmetric group* $\mathrm{Sym}(n)$ *on the set of* 5*-element subsets of* $\{1,\dots,n\}$ *is non-separating if and only if the divisibility conditions (equation 3.3) for $S(t,k,n)$ are satisfied for some t with $0 < t < 5$.*

3.1.3 The main conjecture

We see that if a Steiner system $S(t,k,n)$ exists, then the Johnson association scheme $\mathfrak{J}(n,k)$ is non-synchronising. In view of previous results, we state the main conjecture which is that the converse holds, asymptotically:

Conjecture 2. *There is a function G such that, if $n \geq G(k)$ and the Johnson scheme $\mathfrak{J}(n,k)$ is non-separating, then there exists a Steiner system $S(t,k,n)$ for some t with $0 < t < k$.*

Putting this conjecture together with Keevash's theorem, we can re-formulate it as follows:

Conjecture 3. *There is a function H such that, if $n \geq H(k)$, then the Johnson scheme $\mathfrak{J}(n,k)$ is non-separating if and only if the divisibility conditions (equality 3.3) for $S(t,k,n)$ are satisfied for some t with $0 < t < k$.*

The two previous conjectures can be rephrased in the language of group theory as follow:

Conjecture 4. *There is a function G such that, if $n \geq G(k)$ and the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$, is non-separating, then there exists a Steiner system $S(t,k,n)$ for some t with $0 < t < k$.*

Conjecture 5. *There is a function H such that, if $n \geq H(k)$, then the group G induced by the action of the symmetric group $\mathrm{Sym}(n)$ on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$, is non-separating if and only if the divisibility conditions (equality 3.3) for $S(t,k,n)$ are satisfied for some t with $0 < t < k$.*

For the synchronisation we showed that for $n > (t+1)(k-t+1)$ the graph $\Delta_t(n,k)$ cannot have clique number equal to chromatic number, Theorem 3.18. We also have to consider the possibility that the complementary graph $\Phi_t(n,k)$ has clique number equal to chromatic number.

By the clique–co-clique bound (3.1) and Theorem 3.14 the existence of cliques of size $\binom{n-t}{k-t}$ in $\Phi_t(n,k)$ shows that the size of a co-clique in this graph is at most $\binom{n}{t}/\binom{k}{t}$, a fact that is easily proved directly (Lemma 3.13); equality holds if and only if the co-clique is a Steiner system. So the graph has clique number equal to the chromatic number if and only if the set of k-subsets of an n-set can be partitioned into block sets of Steiner systems $S(t,k,n)$ (the existence of large set) Theorem 3.19. In view of this, we further conjecture the following:

Conjecture 6. *There is a function L such that, if $n \geq L(k)$, then the Johnson scheme $\mathfrak{J}(n, k)$ is non-synchronising if and only if there exists a large set of Steiner systems $S(t, k, n)$ for some t with $0 < t < k$.*

again for groups we have:

Conjecture 7. *There is a function L such that, if $n \geq L(k)$, then the group G induced by the action of the symmetric group* $\mathrm{Sym}(n)$ *on the set Ω of k-element subsets of an n-set, say $\{1, ..., n\}$ is non-synchronising if and only if there exists a large set of Steiner systems $S(t, k, n)$ for some t with $0 < t < k$.*

Much less is known about the existence of large sets. The main results are the following:

(a) For $t = 1$, an $S(t, k, n)$ is simply a partition of $\{1, \ldots, n\}$ into sets of size k, which exists if and only if k divides n. A theorem of Baranyai [12] shows that a large set of such partitions exists whenever k divides n.

(b) For $t = 2$, $k = 3$, Kirkman [49] showed that a $S(2, 3, n)$ exists if and only if $n \equiv 1$ or $3 \pmod 6$. The smallest example is the *Fano plane* with $n = 7$. Cayley [24] showed that there does not exist a large set of Fano planes; indeed, there do not exist more than two pairwise disjoint Fano planes. However, Lu and Teirlinck [71] showed that, for all "admissible" n greater than 7, a large set of Steiner triple systems exists.

(c) Kolotoğlu and Magliveras [50] have constructed large sets of projective planes of order 3, (that is, $S(2, 4, 13)$).

It may be that large sets of $S(t, k, n)$ exist whenever the divisibility conditions are satisfied and n is sufficiently large. If so, then our conjecture above would imply that, for n sufficiently large in terms of k, the Johnson scheme $\mathfrak{J}(n,k)$ is synchronising if and only if it is separating. However, we are not sufficiently confident to conjecture this!

3.1.4 A way towards a proof of the main conjecture

Although we do not know how to prove the (separating conjecture) Conjecture 2 in general, we discuss a possible approach. This is related to the proofs of the cases of $k = 4$, and 5; that is, if n is large enough and $\Delta = \Gamma_I(n,k)$ is not $\Delta_t(n,k)$ or $\Phi_t(n,k)$ we have $\omega(\Delta)\alpha(\Delta) < \binom{n}{k}$. So we look for upper bounds on the sizes of the clique and co-clique numbers.

3.1.4.1 The case $\bar{I}$ is singleton

First we consider the case that I misses one size of intersection.

Theorem 3.52. *Let $\Delta = \Gamma_I(n,k)$ be a graph in the association scheme $\mathfrak{J}(n,k)$ such that I misses one size of intersection. Then for n, large enough the product of the clique and co-clique numbers of Δ is not equal to the number of vertices.*

Proof. Assume that Δ is as stated in the theorem, then clique number of the complement $\bar{\Delta}$ is bounded above by n, by Theorem 3.8. The equality holds if and only if the clique is a symmetric design. This show that, by using the clique–co-clique bound, the co-clique number is bounded above by:

$$\alpha(\bar{\Delta}) \leq \frac{1}{k}\binom{n-1}{k-1},$$

and it is enough to show that it cannot reach this bound.

The case Let $l = k$ be the missed one size of intersection in I, the clique number of $\bar{\Delta}$ is equal to n if and only if there is a projective plane of order k, by Fishes equality 3.8. It is clear for $n > k^2 - k + 1$ there is no projective plane of order k and $\omega(\bar{\Delta}) < n$. Frankl and FÃ¼redi show that for large enough n and $4 \leq k$ we have $\alpha(\Delta) \leq \binom{n-2}{n-2}$, with equality if and only if each k-set in the co-clique contains a fixed 2-set [33]. Since $\binom{n-2}{k-2} < \frac{1}{k}\binom{n-1}{k-1}$, we have $\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{n}{k}$ as desired.

The case $l \in \{2, ..., k-2\}$,

Step 1: By [18, Proposition 3.12] the smallest eigenvalue of graph $\bar{\Delta}$ (two of its vertices are adjacent if their intersection has size $k - l$) for large enough n and fixed k is $E_{k-l}(k - (k - l) + 1) = E_{k-l}(l + 1)$, where

$$E_{k-l}(i) = \sum_{h=0}^{k-l} (-1)^h \binom{i}{h} \binom{k-i}{k-l-h} \binom{n-k-i}{k-l-h}$$

Moreover, $E_{k-l}(i) \approx (-1)^{i-l}\binom{i}{i-l}\binom{n-k-i}{k-i}$ if $i - l > 1$.

Step 2: We show that for positive integers n, k such that $n \geq 2k$ and $l \in \{2, ..., k-2\}$, the following holds:

$$n - 1 < \frac{\binom{k}{l}\binom{n-k}{l}}{(k-l+1)\binom{n-2k+l+1}{l-1}}.$$

This can be proved by induction on k, so for $k = 4$, $l = 2$ and the right hand side will be:

$$\frac{(n-4)(n-5)}{(n-7)}$$

which is greater than $(n - 1)$. Next we assume that the satment is true for k and prove it for $k+1$.

$$\frac{\binom{k+1}{l}\binom{n-(k+1)}{l}}{n(k-l+2)\binom{n-2(k+1)+l-1}{l-1}} = \frac{\frac{(k+1)}{(k-l+1)}\binom{k}{j}\frac{(n-k-l)}{(n-k)}\binom{n-k}{l}}{n(k-l+2)\frac{(n-2k)(n-2k-1)}{(n-2k+l-1)()n-2k+l-2}\binom{n-2k+l-1}{l-1}}.$$

$$= \frac{(k+1)(n-k-l)(n-2k+l-1)(n-2k+l-2)}{(k-l+1)(n-k)(n-2k)(n-2k-1)} \frac{\binom{k}{l}\binom{n-k}{l}}{n(k+l-1)\binom{n-2k+l-1}{l-1}} > 1.$$

This follows from the assumption and the fact that

$$\frac{(k+1)(n-k-l)(n-2k+l-1)(n-2k+l-2)}{(k-l+1)(n-k)(n-2k)(n-2k-1)} \geq 1 \; for \; l \geq 2.$$

Step 3: Lovász in Theorem 3.5 shows that $\alpha(\Gamma) \leq \frac{\binom{n}{k}}{1-\frac{deg(\Gamma)}{\tau}}$ where τ is the smallest eigenvalue. $n < 1 - \frac{deg(\Gamma)}{\tau} \approx 1 - \frac{deg(\Gamma)}{E_l(k-l+1)}$, for large enough n, fixed k and $2 \leq l \leq k-2$. This follows from step 2.

Therefore, the product of the clique and co-clique numbers in Δ is not equal to the number of vertices as desired. □

3.1.4.2 The case $I = \{1, k\}$

In this section, we deal with the case $I = \{1, k\}$ (or the complement $I = \{2, \ldots, k-1\}$) of Conjecture 2, and show that these cannot occur if n is sufficiently large. In other words, taking account of the indexing used in the Johnson scheme, we show the following.

Theorem 3.53. *There is a function f such that, if $n \geq f(k)$, and S and T are families of k-subsets of $\{1, \ldots, n\}$ with the property that S is $\{0, k-1\}$-intersecting* *(that is, any two of its members intersect in* 0 *or* $k-1$ *points) and* T *is* $\{1,\ldots,k-2\}$*-intersecting, then* $|S|\cdot|T|< \binom{n}{k}$.

Proof. The proof proceeds in three steps.

Step 1 $|S|\leq n$.

To see this, consider first a $(k-1)$-intersecting family U of k-sets. It is easy to see that there are just two possibilities:

(a) all members of U contain a fixed $(k-1)$-set;

(b) all members of U are contained in a fixed $(k+1)$-set.

Next we claim that the relation $\sim$ on S defined by $A\sim B$ if $A=B$ or $|A\cap B|= k-1$ is an equivalence relation. It is clearly reflexive and symmetric, so suppose that $A\sim B$ and $B\sim C$. Then $|A\cup B|=|B\cup C|=k+1$, and so $|A\cap C|\geq k-2$, whence $|A\cap C|=k-1$ as required.

Now if two members of S belong to distinct equivalence classes, they are disjoint. So the support of S (the set of points lying in some element of S) is the union of the supports of the equivalence classes, which are pairwise disjoint. We have seen that the number of sets in each equivalence class does not exceed the cardinality of its support; so the same holds for S, and the claimed inequality follows.

For the next step, we note that T is an intersecting family. We split the proof into two subcases.

Step 2 If the intersection of the sets in T is non-empty, then $|T|\leq \binom{n-1}{k-2}/(k-1)$.

For let x be the unique point in the intersection. Then

$$T = \{\{x\} \cup B : B \in T'\},$$

where T' is a $\{0, \ldots, k-3\}$-intersecting family of $(k-1)$-subsets of $\{1, \ldots, n\} \setminus \{x\}$; in other words, a partial $S(k-2, k-1, n-1)$. So $|T| = |T'| \leq \binom{n-1}{k-2}/(k-1)$, the right-hand side being the number of blocks in a hypothetical Steiner system with these parameters.

Step 3 If the intersection of the sets in T is empty, then $|T| \leq \binom{n-1}{k-1} - \binom{n-k-1}{k-1} + 1$.

Since T is an intersecting family, this is just the conclusion of the Hilton–Milner Theorem [41, Theorem 3].

Conclusion of the proof We have

$$\binom{n}{k} = |S| \cdot |T| \leq \begin{cases} n\binom{n-1}{k-2}/(k-1) & \text{if } \bigcap T \neq \varnothing, \\ n(\binom{n-1}{k-1} - \binom{n-k-1}{k-1} + 1) & \text{if } \bigcap T = \varnothing. \end{cases}$$

But in each case, for fixed k, the left-hand side of the inequality is a polynomial of degree k in n, whereas the right-hand side is a polynomial of degree $k-1$; thus the inequality holds for only finitely many values of n. $\square$

We remark that, in fact, we know of no examples meeting the bound for this case with $n > 2k$. So as well as extending these techniques to other cases, the problem of deciding whether the bound is always strict remains.

Corollary 3.54. *For $k \geq 3$ and $n > 2k$, a $\{0, k-1\}$-intersecting family of k-subsets of $\{1, \ldots, n\}$ has size at most n.*

Babai and Frankl [9, Theorem 1] obtained a more general result:

Theorem 3.55. *Let n and k $(n \geq 2k)$ be two integers and S be an intersecting system of k-subsets such that the greatest common divisor of the sizes of their intersections does not divide k. Then $|S| \leq n$*

Corollary 3.56. *There is a function h such that, if $n \geq h(k)$, and S and T are families of k-subsets of $\{1, \ldots, n\}$ with the property that the common divisor of sizes of intersection of members of S does not divide k. Also T is $\{0, ..., k-1\} \setminus X$-intersecting, where X is th set of sizes of intersections in S. Then $|S| \cdot |T| < \binom{n}{k}$.*

The proof follows similar arguments in proof 3.1.4.2.

3.1.5 Projective planes

The constructions in Section 3.1.2 of the small examples involved the fact that, in certain Steiner systems, certain cardinalities of block intersection do not occur. There are relatively few examples of such systems: the only ones known are projective planes, $S(3, 4, 8)$, $S(4, 5, 11)$, $S(5, 6, 12)$, $S(3, 6, 22)$, $S(4, 7, 23)$ and $S(5, 8, 24)$.

A projective plane has the property that any two of its blocks meet in a point. Hence it is a clique in either of the graphs $\Gamma_{\{i>k-2\}}(n, k)$ or $\Gamma_{k-1}(n, k)$, with $k = q+1$ and $n = q^2 + q + 1$. In the first of these graphs, co-cliques of maximum cardinality are of EKR type, and we have

$$\binom{q^2+q-1}{q-1} \cdot (q^2 + q + 1) = \binom{q^2+q+1}{q+1},$$

so non-separation holds for this graph: these sets (all k-sets containing two given points) also show non-separation for $\Gamma_1(n, k)$. Also, by Theorem 3.18, we cannot partition the k-sets into subsets of EKR type.

In the case $q = 2$, in our example above, we observed that there were other co-cliques, so that the possibility of a colouring with $q^2 + q + 1$ colours cannot be ruled out; and indeed we saw that such a colouring exists.

Conjecture 8. *For $q > 2$, a co-clique of maximum size in the graph $\Gamma_q(q^2 + q + 1, q + 1)$ must consist of all the $(q + 1)$-sets containing two given points; so the chromatic number of this graph is strictly larger than $q^2 + q + 1$.*

A simple computation shows that the conjecture is true for $q = 3$ and for $q = 4$.

On the other hand, the truth of this conjecture would probably not give an infinite family of examples which are synchronising but not separating. Magliveras conjectured that large sets of projective planes of any order $q > 2$ exist; the existence is shown for $q = 3$[50].

3.2 The second group

Let $n = kl$ with $l \geq 2$, and let G be the symmetric group $\mathrm{Sym}(n)$ acting on the set Ω of uniform partitions of $\{1, ..., n\}$ into l parts of size k. The degree of the action is

$$\frac{1}{l!}\prod_{i=0}^{l-1}\binom{n-ik}{k}.$$

The group G is transitive. The stabiliser of a uniform partition of an n-set into l parts of size k is the wreath product $\mathrm{Sym}(l) \wr \mathrm{Sym}(k)$. Since it is a maximal subgroup of $\mathrm{Sym}(n)$ [81], the group G is primitive. The study here is divided into two cases; the case $l = 2$ and the case $l > 2$. In the first case $l = 2$, will investigate the separation and synchronisation properties for small values of $k = 2, 3, 4, 5, 6$. Then, we show that if there is a resolvable Steiner system $S(t, k, 2k)$, then the second group is non-separating and non-synchronising. Also, we provide a conjecture based proposing that the converse holds. In the second case $l > 2$, we show that the second group is non-synchronising, so non-separating.

3.2.1 The case $l = 2$ and folded Johnson schemes

In this case, the association scheme obtained from the action of the group is the same as that obtained from the distance graphs of the folded Johnson graph. We will call this scheme the folded Johnson association scheme and denote it by $\bar{J}(2k, k)$. The vertex set in each graph contains uniform partitions of $2k$-set into two sets each of size k. Thus, the number of vertices in this scheme is $\frac{1}{2}\binom{2k}{k} = \binom{2k-1}{k-1}$. The scheme has $\lfloor \frac{k}{2} \rfloor$ orbital graphs. Two vertices in each orbital graph Γ_i, $\lceil \frac{k}{2} \rceil \leq i \leq k-1$, are adjacent if and only if the sizes of the intersections of their parts belongs to $K_i = \{k-i, i\}$.

A graph Γ_I is defined to have vertex set as the folded Johnson scheme and two vertices (partitions) are adjacent if the sizes of the intersections of their parts belongs to $\bigcup_{i \in I} K_i$ where $I \subset \{\lceil \frac{k}{2} \rceil, ..., k-1\}$. Two cases are crucial and we introduce different notations for them:

- $\Delta_t(2k, k) = \Gamma_{\{\lceil \frac{k}{2} \rceil, ..., t-1\}\}}(2k, k)$, the graph in which two partitions are joined if their parts intersect in fewer than t points.
- $\Phi_t(2k, k) = \Gamma_{\{t, ..., k-1\}}(2k, k)$, the complement of $\Delta_t(2k, k)$, in which two partitions are joined if their parts intersect in $\geq t$ or $\leq k-t$ points.

We investigate the synchronisation and separation properties by looking at small examples first.

3.2.1.1 The case $k = 2$ or $k = 3$:

In this case, the second group G is 2-transitive and consequently separating.

3.2.1.2 The case $k = 4$:

The second group G is non-separating and non-synchronising.

Lemma 3.57. *The folded Johnson scheme $\bar{\mathfrak{J}}(8,4)$ is non-separating and non-synchronising.*

Proof. In this case the folded Johnson association scheme $\bar{\mathfrak{J}}(8,4)$ has exactly two orbital graphs, the folded Johnson graph and its complement. In the first graph two vertices $A = \{A_1, A_2\}$ and $B = \{B_1, B_2\}$ are adjacent if $|A_i \cap B_j| \in \{1, 3\}$ where $i, j \in \{1, 2\}$. In the second graph, two vertices are adjacent if the size of the intersection of their parts is 2. To see that the group G is non-separating, consider the complement of the folded Johnson graph Γ_2. The seven parallel classes of the Steiner system $S(3,4,8)$ form its maximum clique. The co-clique is constructed from a 3-intersecting set of EKR-type, which has size 5. This can be done by replacing each part in the 3-intersecting set by a partition containing this part and its complement. G, also, is non-synchronising. A 7-colouring can be constructed as follows: take a Fano plane $S(2,3,7)$ on $\{1, ..., 7\}$. Now, for each line L, we associate a colour c_L with L and give a partition the colour c_L if L is contained in a part of the partition. Since any two lines intersect and have five points between them, no partition gets more than one colour; and there are five partitions of each colour, so each partition gets a colour. Moreover, two partitions with the same colour have parts intersect in 1 or 3 points, and so are non-adjacent. □

Lemma 3.58. *Let $n = 8$ with $k = 4$, and let G be the symmetric group* $\mathrm{Sym}(8)$ *acting on the set Ω of uniform partitions of $\{1, ..., 8\}$ into 2 parts of size 4. Then G is non-separating and non-synchronising.*

3.2.1.3 The case $k = 5$:

The group G is separating. The association scheme $\bar{\mathcal{J}}(10, 5)$ has two orbital graphs the folded Johnson graph with sizes of intersections belong to $\{1, 4\}$ and its complement with sizes of intersections belong $\{2, 3\}$. Computational methods can be used to show that it is separating.

The following result states that the (dual) matrix of eigenvalues of orbital graphs of Johnson folded association scheme $\bar{\mathcal{J}}(2k, k)$ can be extracted from the (dual) matrix of eigenvalues the orbital graph in Johnson scheme $\mathcal{J}(2k, k)$.

Theorem 3.59. *[19, Proposition 4.2.3] Let Γ be distance regular graph with spectrum Φ, where $\theta \in \Phi$ has multiplicity $m(\theta)$. It Γ is antipodal of diameter $d \geq 3$, then the folded graph $\bar{\Gamma}$ has spectrum that is a subset $\bar{\Phi}$ of Φ and for $\theta \in \Phi$ the multiplicity of θ in the spectra of $\bar{\Phi}$ and Γ agree. Moreover, $\bar{\Phi}$ is obtained from Φ by taking every second eigenvalue.*

Lemma 3.60. *The folded Johnson scheme $\bar{\mathcal{J}}(10, 5)$ is separating, so synchronising.*

Proof. The eigenvalues matrix P of the folded Johnson scheme $\bar{\mathcal{J}}(10, 5)$ can be calculated by using Eberlein polynomials 3.2 and Theorem 3.59.

$$P = \begin{pmatrix} 1 & 25 & 100 \\ 1 & 7 & -8 \\ 1 & -3 & 2 \end{pmatrix}$$

Lemma 3.61. *Let $n = 10$ with $k = 5$, and let G be the symmetric group* $\mathrm{Sym}(10)$ *acting on the set Ω of uniform partitions of $\{1, ..., 10\}$ into 2 parts of size 5. Then G is separating, so synchronising.*

In this scheme there are two non-trivial orbital graphs Γ_1 with eigenvalues $25, 7, -3$ and its complement Γ_2 with the eigenvalues $100, -8, 2$. It is obvious that the smallest eigenvalue in each orbital graphs does not divide the degree. Therefore, by Corollary 3.6, there is no equality in the clique–co-clique bound (3.1) for both graphs. As a result, $\bar{\mathfrak{J}}(10, 5)$ is separating and synchronising. From the previous theorem, the group G is separating and synchronising. $\square$

3.2.1.4 The case $k = 6$:

The second group G is non-separating and non-synchronising.

Lemma 3.62. *The folded Johnson scheme* $\bar{\mathfrak{J}}(12, 6)$ *is non-separating and non-synchronising.*

Proof. The association scheme $\bar{\mathfrak{J}}(12, 6)$ has three orbital graphs. First is folded Johnson graph Γ_1 with sizes of intersections belong to $\{1, 5\}$. The other two graphs Γ_2 and Γ_3 with vertices have intersection sizes in $\{2, 4\}$ and $\{3\}$, respectively. Consider the graph Γ_1 , the 66 resolution classes of the Steiner system $S(5, 6, 12)$ form a clique in the complement of the graph. $\bar{\Gamma_1}$ can be coloured using the Steiner system $S(4, 5, 11)$ on $\{1, ..., 11\}$ there is a colour c_B for each block B, and a partition has colour c_B if and only if B is contained in a part. $\square$

Lemma 3.63. *Let* $n = 12$ *with* $k = 6$*, and let* G *be the symmetric group* $\mathrm{Sym}(12)$ *acting on the set* Ω *of uniform partitions of* $\{1, ..., 12\}$ *into* 2 *parts of size* 6*. Then* G *is non-separating and non-synchronising.*

Remark: In the previous examples, the existence of a non-trivial G-invariant graph in the scheme with the product of the clique number and the co-clique number equals the number of vertices requires a Steiner system $S(k - 1, k, 2k)$.

Such a system cannot exist unless $k+1$ is prime, and the only known examples are $S(3,4,8)$ and $S(5,6,12)$; it is known that $S(9,10,20)$ does not exist.

3.2.1.5 The conjecture

We can illustrate the connection between the non-synchronising property of this scheme and the existence of resolvable Steiner system by the following:

Let t be an integer such that $1 < t < k-1$, if there is a resolvable Steiner system $S(t,k,2k)$ then the set of its resolvable classes form a maximum clique in the graph $\Delta_t(2k,k)$. Moreover, there is a co-clique of size $\binom{2k-t}{k-t}$, constructed as follows: consider t-intersecting set F and let the co-clique S contains partitions each consists of one member of F and its complement in the $2k$-set. It is easy to check that

$$\frac{1}{2}\frac{\binom{2k}{t}}{\binom{k}{t}}\binom{2k-t}{k-t} = \binom{2k-1}{k-1}$$

So, if there is a resolvable Steiner system $S(t,k,2k)$ then the product of the clique number and co-clique number in the graph $\Delta_t(2k,k)$ equals to the number of vertices. Therefore, the folded Johnson scheme $\bar{\mathfrak{J}}(2k,k)$ is non-separating.

Theorem 3.64. *Let $k > 3$, and let Γ be a graph in the folded Johnson scheme $\bar{\mathfrak{J}}(2k,k)$, such that $\Gamma = \Delta_t(2k,k)$. Then the co-clique number of the graph has size $\binom{2k-t}{k-t}$. Moreover, there is a resolvable Steiner system $S(t,k,2k)$ if and only if there is a clique of size $\binom{2k-1}{k-1}/\binom{2k-t}{k-t}$.*

Interestingly, if a Steiner system $S(t,k,2k)$ exists, then there are only two possibilities; $t=1$ and $t=k-1$. The following result in a Corollary of Theorem 3.15.

Corollary 3.65. *If a Steiner system $S(t,k,2k)$ exists, then $t=1$ and $t=k-1$ are the only possibilities.*

Proof. From Theorem 3.15 we have $n \geq (t+1)(k-t+1)$. If $n = 2k$, this reduces to $(t-1)k \leq (t+1)(t-1)$. So, if $t > 1$, then $k \leq t+1$, or $t \geq k-1$. So $t = 1$ and $t = k-1$ are the only possibilities. $\square$

Theorem 3.66. *Let $k > 3$, and let Γ_1 be the graph whose vertex set is the set of partitions of $\{1, \ldots, 2k\}$ into two subsets of size k. Two partitions being adjacent if and only the intersecting size of their parts is 1 or $(k-1)$. Then $\omega(\Gamma_1) = k+1$. Moreover, the following are equivalent:*

(a) there exists a resolvable Steiner system $S(k-1, k, 2k)$;

(b) $\alpha(\Gamma_1) = \binom{2k-1}{k-1}/(k+1)$;

(c) there exists a Steiner system $S(k-2, k-1, 2k-1)$;

(d) $\chi(\bar{\Gamma}_1) = \omega(\bar{\Gamma}_1)$.

Proof. From (a) to (b) is true by Theorem 3.64. For the part from b to c, let S be a maximum co-clique in the graph Γ_1, choose a point x, and let $S(x) = \{A \setminus \{x\} : x \in A \in S\}$. Then $S(x)$ is an $\leq (k-3)$-intersecting family (means the size of intersection for any two members of S is equal or less than $(k-3)$) of $(k-1)$-subsets of a $(2k-1)$-set. So its cardinality is at most the number of blocks of a hypothetical $S(k-2, k-1, 2k-1)$, which is $\binom{2k-1}{k-1}/(k+1)$. To prove the case from (c) to (d), a $\binom{2k-1}{k-1}/(k+1)$-colouring of the graph $\bar{\Gamma}_1$ can be constructed as follows: take a Steiner system $S(k-2, k-1, 2k-1)$ on $\{1, ..., 2k-1\}$. Now, for each block B, we associate a colour c_B with B and colour a partition in the colour c_B if B is contained in a part of the partition. Since any two blocks intersect and have at most $2k-1$ points between them, no partition gets more than one colour; and there are $k+1$ partitions of each colour, so each partition gets a colour. Moreover, two partitions with the same colour have parts intersect in 1 or $k-1$ points, and so non-adjacent. The last part is true by the previous theorem. $\square$

Theorem 3.67. *If a Steiner system $S(k-1, k, 2k)$ exists, then the folded Johnson scheme $\bar{\mathfrak{J}}(2k, k)$ is non-separating and non-synchronising.*

In the language of group theory.

Theorem 3.68. *Let $n = 2k$, and let G be the symmetric group* $\mathrm{Sym}(n)$ *acting on the set Ω of uniform partitions of $\{1, ..., n\}$ into 2 parts of size k. If a Steiner system $S(k-1, k, 2k)$ exists, then the group G is non-separating and non-synchronising.*

Now, in view of the previous results and discussions we state the following conjecture.

Conjecture 9. *Let $n = 2k$, and let G be the symmetric group* $\mathrm{Sym}(n)$ *acting on the set Ω of uniform partitions of $\{1, ..., n\}$ into 2 parts of size k. Then the group G is non-separating (non-synchronising) if and only if there is a Steiner system $S(k-1, k, 2k)$.*

Using the P-matrix and Q-matrix of the folded association schemes and the algebra system GAP/GRAPE we can show that the folded Johnson schemes $\bar{\mathfrak{J}}(14, 7)$, $\bar{\mathfrak{J}}(16, 8)$, $\bar{\mathfrak{J}}(18, 9)$ and $\bar{\mathfrak{J}}(20, 10)$ are separating. (This can be done by a similar computational methods used in Section 1)

3.2.2 The case $l > 2$

In this subsection, we consider the case $l > 2$. It turned out that the group G is non-synchronizing.

Theorem 3.69. *Let $n = kl$ with $l > 2$, and let G be the group induced by the action of the symmetric group* $\mathrm{Sym}(n)$ *on the set Ω of uniform partitions of $\{1, ..., n\}$ into l parts of size k. Then the group G is non-synchronising, non-separating.*

Proof. Consider the graph Γ with vertex set Ω, in which two partitions are adjacent if they have no common part. $G \leq \mathrm{Aut}(\Gamma)$ and since $l > 2$, this is not the complete graph. We show that $\omega(\Gamma)\alpha(\Gamma) = |\Omega|$ and $\chi(\Gamma) = \omega(\Gamma)$.

The number of uniform l-partitions of n-set in a Baranyai's partition Theorem 3.9, is $\frac{1}{l}\binom{n}{k}$. Each of these is a partition into l parts of size k, and no two share a part, so they do form a clique in the graph. So, $\frac{1}{l}\binom{n}{k}$ is a lower bound on the clique number.

The set of all partitions having a fixed k-set as a part is a co-clique, and its size is the number of partitions of an $(n-k)$-set into k-sets, which (by the displayed formula in the introduction of this section with $l-1$ replacing l) is

$$\frac{1}{(l-1)!}\prod_{i=1}^{l-1}\binom{n-ik}{k}.$$

The product is the displayed formula. Therefore, the group G is non-separating.

We claim that $\chi(\Gamma) = \omega(\Gamma)$, to see this let $x \in \{1, ..., n\}$ and let A be a $(k-1)$-subsets of $\{1, ..., n\} \setminus \{x\}$. Give a partition P the colour c_A if $A \cup \{x\}$ is a part in P. Each partition will have exactly one colour as x is contained in one part. Two partitions have the same colour if they have a part in common. There number of $(k-1)$-subsets of $\{1, ..., n\} \setminus \{x\}$ is $\binom{n-1}{k-1}$. Also, the clique number is equal to $\frac{1}{l}\binom{n}{k} = \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$ Thus, we have the clique number is equal to the chromatic number and hence G is non-synchronising. $\square$

3.3 Conclusion and future work

In this chapter we consider two important almost simple permutation groups. The main goal is to investigate their synchronisation and separation properties. In the first group, when $k = 2, 3, 4$ and 5 we determine when these groups are separating. In general, we state a conjecture which if true, would be a crucial extension of the remarkable result regarding the existence of Steiner systems by Peter Keevash. For $k = 2$ and 3, these groups are separating if and only if synchronising. For $n = 4$ the statement fails for $n = 10$. In the second group we give a similar results to the first group when $l = 2$ and show that the group is non-synchronising if $l > 2$.

In the arguments for $k = 4$ and $I = \{1, 3\}$ and $I = \{1, 4\}$, we saw that the sizes of a clique and a co-clique whose product is equal to the number of vertices can be determined from the Q-matrix of the association scheme. Is this true in general?

Beside the attempt to solve the conjectures, future work from this chapter can be the study of q-analogues of Johnson association schemes. For $k = 2$ we have the same conclusion as Theorem 3.22 by the use of the eigenvalues technique and the existence of q analogue of Baranyai's theorem when $k = 2$ [13, 46]. For $k > 2$, the case seems to be difficult, for example, the first problem would be finding a proof for the q analogue of Baranyai's Theorem. Also, little is known about the existence of q-Steiner systems. However, it is still interesting to ask is it true that the q analogue of a Johnson scheme is non-separating if and only if there exists q-Steiner system, even for small values of k.

The computations with rational functions in Section 3, and Section 6 were performed with Mathematica [83]; computations of clique (co-clique) numbers in special cases were done with GAP and its package GRAPE.

Chapter 4

Affine permutation groups

This chapter addresses the synchronisation property for some of the permutation groups of affine type. In particular, affine distance-transitive groups are considered. We assume that V is an n-dimensional vector space over a finite field $\mathbb{F}_q$, where q is a prime power. Groups of affine type can be defined in general, as they preserve the structure of the affine geometry of the vector space V. A group G is said to be **distance transitive** if $G \leq \mathrm{Aut}(\Gamma)$ where Γ is a connected graph with diameter d such that for all pairs (x_1, y_1) , (x_2, y_2), $x_j, y_j \in V(\Gamma)$, with the property that $d(x_1, y_1) = d(x_2, y_2) = i$, $1 \leq i \leq d$, there is some $g \in G$ that satisfies $(x_1, y_1)g = (x_2, y_2)$. In this case, G is said to **act distance transitively** on the graph Γ, and Γ is said to be **distance transitive**.

The classification of the primitive affine distance-regular graphs which is given in [75, Theorem 1.1] is the road map for this chapter. The first section introduces affine-type permutation groups and some of their basic properties. Section 2 provides some background on coding theory. Section 3 deals with some results regarding imprimitive distance-regular graphs, and other sections follow the classification given for them in [75]. In Section 10 we provide a conjecture which extends the main conjecture in the previous chapter. The general references for this chapter are the books [20] and [62] for permutation groups, [27] for coding theory, and [19] for graph theory.

4.0.1 Summary of the results

We proved in Theorem 4.7 that the synchronisation and separation properties are equivalent for affine groups. Then we considered automorphism groups of some affine distance transitive graphs and obtained the following results; By Theorem 4.12, the automorphism group of the Hamming graph $H(n,q)$ is non-synchronising. By Theorem 4.18 the automorphism group of the halved graph $H\Gamma_n$ of $H(n,2)$ is synchronising if $n \leq 3$ and it is non-synchronising if $n \geq 4$ is even. Also, if $n \geq 5$ and odd the automorphism group is non-synchronising if and only if there is some positive integer m such that $n = 2^m - 1$, or $n = 23$, that is, there is a binary Hamming code or a binary Golay code. By Theorem 4.22, for n is even, the automorphism group of the halved folded graph $FH\Gamma_n$ of n-cube is synchronising if $n \leq 6$ and if $n > 6$ the automorphism group is non-synchronising if and only if there is some positive integer m such that $n = 2^m$, or $n = 24$.

By Theorem 4.29, the automorphism group of the bilinear forms graph $\mathrm{BF}(n_1, n_2, q)$ is non-synchronising. By Proposition 4.38, the automorphism group of the alternating forms graph $A\Gamma_5(q)$ is synchronising. By Proposition 4.39, the automorphism group of the alternating forms graph $A\Gamma_4(3)$ is non-synchronising. By Theorem 4.40, for both n and q even, the automorphism group of the alternating forms graph $A\Gamma_n(q)$ is non-synchronising.

By Proposition 4.44 the automorphism group G of the Hermitian graph $H\Gamma_2(\mathbb{F}_q)$ is synchronising. By Proposition 4.45 the automorphism group G of the Hermitian graph $H\Gamma_3(\mathbb{F}_q)$ is synchronising.

By Theorem 4.48, the automorphism group of the coset graph $Cos(C)$ of the extended ternary Golay code is non-synchronising. By Theorem 4.50, the automorphism group of the coset graph $Cos(C)$ of the truncated binary Golay code is synchronising. By Theorem 4.52, the automorphism group of the coset graph $Cos(C) = C_{23}$ of the binary Golay code is synchronising.

For a affine distance transitive graph Γ, if we state that its automorphism group G is synchronising (resp. non-synchronising), then any group H acts distance transitively on the graph Γ is synchronising (resp. non-synchronising). This is because the groups G and H have the same invariant graphs.

Also, we used the results in this chapter as evidences to propose Conjecture 10 which considers exceptional graphs. We say that a primitive distance-transitive graph Γ with diameter d, exceptional if $\mathrm{Aut}(\Gamma)$ is non-separating but there is no t with $0 < t < d$ such that for the distance at most t graph in Γ the product of the clique number and the co-clique number equals the number of vertices. The conjecture asserts that given a positive integer d, there are only finitely many exceptional graphs of diameter d.

4.1 Permutation groups of affine type

Let A be an abelian group with the property that every $a \in A$ defines a permutation t_a of A such that if $b \in A$, then $bt_a = b + a$. Such a permutation is called a ***right translation***, and the set of all right translations defines a group with composition as the group operation. This group is called the **group of translations** and denoted by T. Let G_0 be a group of automorphisms of A. Then a new group G can be generated by the two groups T and G_0, that is, $G = \langle T, G_0 \rangle$. The group

G acts naturally on A by applying the automorphism and then the translation, that is, if $g = (g_0, t_a) \in G$ and $b \in A$, then $bg = b(g_0, t_a) = bg_0 + a$.

The group G is a semi-direct product of T and G_0, where T is a regular normal subgroup of G. To see this, first observe that the only element of T with a fixed point is the identity, so it is semi-regular. Also, T acts transitively on A, since for all $a, b \in A$, there is some $t_{b-a} \in T$ such that $at_{b-a} = a + b - a = b$. Therefore, T is regular. Moreover, for all $g_0 \in G_0$, $t_a \in T$, and $b \in A$, we have

$$b(g_0^{-1} t_a g_0) = ((bg_0^{-1}) + a)g_0 = b + ag_0 = bt_{ag_0}.$$

Thus ${g_0}^{-1} T g_0 = T$, so G_0 normalizes T. Finally, the identity is the only element in the intersection of T and G_0. Consequently, $G = T \rtimes G_0$, which acts transitively on A since it contains T.

Let $A = V$ be a finite n-dimensional vector space over a finite field $\mathbb{F}_q$. The **general linear group** is the set of all invertible linear transformations of V, denoted by $GL(n, \mathbb{F}_q)$. The **affine general linear group** is the group $G = \langle T, G_0 \rangle$, where T is identified with the additive group of V and $G_0 = GL(n, \mathbb{F}_q)$. An **affine-type group** G is a subgroup of the affine general linear group which contains its abelian regular normal subgroup, that is, $G = V \rtimes G_0$, where G_0 is a subgroup of $GL(n, \mathbb{F}_q)$.

The study of the synchronisation property of permutation groups is reduced to the study of primitive groups—in particular, those that do not preserve Cartesian decompositions (basic groups). Whether a group G of affine type is primitive (basic) or not depends on the irreducibility (primitivity) of the associated linear group G_0. This will be discussed in the following subsection.

4.1.1 Primitive affine groups and irreducible linear groups

Let V be an n-dimensional vector space over a finite field $\mathbb{F}_q$, where q is prime power, and let $G_0 \leq GL(n, \mathbb{F}_q)$ be a linear group. Then a subspace W of V is said to be G_0**-invariant** if for all $w \in W$ and $g_0 \in G_0$ we have $wg_0 \in W$, in which case W is said to be a **trivial** subspace of V if either $W = \{0\}$ or $W = V$. A linear group $G_0 \leq GL(n, \mathbb{F}_q)$ is **irreducible** if there is no non-trivial G_0-invariant subspace of V; otherwise, G_0 is **reducible**. The results in this section are not new and can be found in [6],

Theorem 4.1. *[6, Theorem 2.9 (b)] [67, Theorem 6.2.1] Let $V = \mathbb{F}_q^n$ be an n-dimensional vector space over $\mathbb{F}_q$, and let G_0 be a subgroup of the general linear group $GL(n, \mathbb{F}_q)$. Then the affine group $G = V \rtimes G_0$ is imprimitive in its action on V if and only if G_0 is reducible.*

Example 4.2. *[67] Let $\mathbb{F}_2$ be the finite field with two elements and let V be a 2-dimensional vector space over $\mathbb{F}_2$, and let G_0 be the subgroup*

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

of the general linear group $GL(2, \mathbb{F}_2)$. Then G_0 is reducible, where $W = \{(0,0), (1,1)\}$ is the G_0-invariant subspace Also, $G = \mathbb{F}_2^2 \rtimes G_0$ is an imprimitive affine permutation group in its action on ${\mathbb{F}_2}^2$.

This group will be studied in detail in the coming sections.

4.1.2 Basic affine permutation groups and primitive linear groups

A linear group $G_0 \leq GL(n, \mathbb{F}_q)$ is said to be **imprimitive** if G_0 preserves a non-trivial direct sum decomposition of the vector space $V = \mathbb{F}_q^n$. If there is no such decomposition, we say that G_0 is **primitive**.

Theorem 4.3. *[6, Theorem 2.9 (c)] [67, Theorem 6.2.4] Let $V = \mathbb{F}_q^n$ be an n-dimensional vector space over $\mathbb{F}_q$, where q is prime power, and let G_0 be a subgroup of the general linear group $GL(n, \mathbb{F}_q)$. Then the affine group $G = V \rtimes G_0$ is basic if and only if the linear group G_0 is primitive.*

Example 4.4. *[67]*
Let $\mathbb{F}_q$ be the finite field where $q = p^k$, where is p a prime greater than 2. Assume that V is a 2-dimensional vector space over $\mathbb{F}_q$, and let G_0 be the subgroup

$$\left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} : x, y \in \mathbb{F}_q^* \right\}$$

of the general linear group $GL(2, \mathbb{F}_q)$. Then G_0 is irreducible and $G = \mathbb{F}_q 62 \rtimes G_0$ is a non-basic affine permutation group in its action on $\mathbb{F}_q^2$.

In this chapter I consider some of the types of groups that appear in the following theorem, detailed description of the graphs will appear later in the chapter.

Theorem 4.5. *[75, Theorem 1.1] Let p be a prime, let Γ be a graph with both the valency and the diameter are greater than or equal to 3 on $V \cong \mathbb{F}_q^n$, where q is a prime power of p. Let G_0 be a subgroup of $GL(V)$ such that $G = V \rtimes G_0$ acts primitively and distance transitively on V. Then up to isomorphism, Γ is in one of the following families of graphs, and $G \leq \mathrm{Aut}(\Gamma)$.*

(a) Γ *is a Hamming graph* $H(n,q)$.

(b) Γ *is a halved* $(n+1)$*-cube* $\mathrm{H}\Gamma_{(n+1)}$ *with* n *even.*

(c) Γ *is a folded* $(n+1)$*-cube* $\mathrm{F}\Gamma_{(\mathrm{n+1})}$ *with* n *even.*

(d) Γ *is a folded halved* $(n+2)$*-cube* $\mathrm{FH}\Gamma_{(n+2)}$ *with* n *even.*

(e) Γ *is a bilinear forms graph* $\mathrm{BF}(n_1,n_2,q)$.

(f) Γ *is an alternating forms graph* $\mathrm{A}\Gamma_n(q)$.

(g) Γ *is a Hermitian forms graph* $\mathrm{H}\Gamma_n(q)$.

(h) Γ *is an affine* E_6 *graph.*

(i) Γ *is the coset graph of the extended ternary Golay code.*

(j) Γ *is the coset graph of the truncated Golay code.*

(k) Γ *is the coset graph of the binary Golay code.*

(l) Γ *is the distance-2 graph of the coset graph of the binary Golay code.*

Proposition 4.6. *[35, Lemma 2.2] Let* Γ *be a distance-regular graph with vertex set* $V(\Gamma)$ *and diameter* d*. Then, the relations*

$$R_i = \{(x,y) \in V(\Gamma) \times V(\Gamma) : d(x,y) = i, 0 \leq i \leq d\}$$

define a symmetric association scheme $\mathcal{A}\Gamma$ *of class* d*.*

Interestingly, the synchronisation property in affine groups is equivalent to the separation property.

Theorem 4.7. *Synchronisation and separation properties are equivalent for groups of affine type.*

Proof. It follows from Theorem 2.24 and Theorem 2.23 that non-synchronising groups are non-separating. Now assume that G is affine group which is non-separating. Hence, there is a G-invariant graph Γ such that the product of the size of a maximum clique A and the size a maximum co-clique B equals the number of vertices. The group G contains an abelain subgroup H, and G is induced by the action of G on H by the right multiplication. Therefore, Γ is a Cayley graph $\mathrm{Cay}(H, S)$ (see discussion in Subsection 5.2.1 for Cayley graphs). Notice that, for distinct elements $a_1, a_2 \in A$ we have $a_1a_2^{-1} \in S$, but for distinct elements b_1, b_2 we have $b_1b_2^{-1} \notin S$.

We want to show that the graph Γ has the clique equals the chromatic numbers by showing that its vertex set can be partitioned into co-cliques aB where $a \in A$. First we show that for $a \in A$ the set aB is a co-clique, if not then there are distinct elements b_1 and b_2 in B such that $ab_1b_2^{-1}a^{-1} \in S$, but since H is abelian we have $b_1b_2^{-1} \in S$, contradiction. Now we show that a_1B and a_2B are disjoint for distinct element $a_1, a_2 \in A$. Assume for the contrary that we have $b_1, b_2 \in B$ such that $a_1b_1 = a_2b_2$ which implies $b_1b_2^{-1} = a_1a_2^{-1} \in S$, contradiction. Therefore, the chromatic number of the graph is $|V(\Gamma)|/|B| = |A|$. As a result, there is a G-invariant graph such that the chromatic number equals the clique nmber and by Theorem 2.23, G is non-synchronising. □

Using Theorem 2.24, Theorem 2.23 and Theorem 4.7, we will attempt to answer the following question: When is a group G from Theorem 4.5 non-synchronising? Sections 4–9 consider association schemes obtained from one or more families in Theorem 4.5. In particular, Section 4 deals with Hamming graphs (a), while

Section 5 considers families (b), (c), and (d). Family (e) is considered in Section 6. Sections 7 and 8 are devoted to study the families (f) and (g), respectively. I have not reached a conclusion for family (h). Finally, families (i), (j), (k), (l), and (m) are studied in Section 9.

4.2 Coding theory

This section contains some basic concepts and results from coding theory. Let Q be a finite set with q elements, where $q \geq 2$, and let Q^n be the set of all n-tuples of elements of Q, that is,

$$Q^n = \{(x_1, x_2, ..., x_n) : x_i \in Q, 1 \leq i \leq n\}.$$

A non-empty subset C of Q^n is called a (q-ary) **code** of length n. A code that contains either all elements of Q^n or only one element of Q is called a **trivial code**. We assume that a code C has at least two elements.

The set Q is usually called the **alphabet**, and the elements of Q^n are called **words** or **vectors**, even if Q is not a field. The elements of a code C are called **code words**. The set Q^n is known as the **Hamming space**. When Q is a field, the Hamming space is a vector space.

A metric d can be defined on the set of ordered pairs of elements of Q^n such that two codes $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ in Q^n are at distance i if they differ in i coordinate positions, that is,

$$d(x, y) = i \iff |\{j : x_j \neq y_j\}| = i$$

$d(x, y)$ is called the **Hamming distance**. Thus $0 \leq d(x, y) \leq n$.

A **(Hamming) weight** of a word $x \in Q^n$, denoted by $wt(x)$, is defined to be the number of non-zero coordinate positions in x. For $Q = \mathbb{F}_2$, the zero word is the one in which all the coordinates are 0; that is $\mathbf{0} = (0, ..., 0)$. A word in which all the coordinates are 1 is denoted by $\mathbf{1}$. A word is called an **odd word** if it has odd weight; otherwise, it is called an **even word**. For example, $\mathbf{0} = (0, ..., 0)$ is an even word.

The **(Hamming) sphere** $B(x, r)$ of radius r and centred at the word $x \in Q^n$ is the set of all words at distance less than or equal to r from x; that is,

$$B(x, r) = \{y \in Q^n : d(x, y) \leq r\}.$$

and its cardinality as shown in [27, p.16] is

$$V_q(n, r) = \sum_{i=1}^{r} \binom{n}{i} (q-1)^i.$$

For a code C in Q^n, **the minimum distance** $d(C)$ of C is the smallest distance between any two distinct code words in C, that is,

$$d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

The distance of $x \in Q^n$ from a code C is defined as

$$d(x, C) = \min\{d(x, c) : c \in C\},$$

and the **covering radius** $t(C)$ of a code C is defined as the smallest integer t such that for every word x be in Q^n there is at least one code word c in C such that $d(x, c) \leq t$:

$$t(C) = \max\{d(x, C) : x \in Q^n\}.$$

Equivalently, $t(C)$ is the smallest integer t such that the union of the Hamming spheres centred at the code words of C is Q^n. Also, if C is a code with minimum distance d, the integer $\lfloor \frac{d-1}{2} \rfloor$ is the error-correcting capability (packing radius) of C. It is the largest integer e such that the Hamming spheres of radius e are disjoint. This gives what is known as the **sphere-packing bound** or **Hamming bound** of C [27]:

$$|C| \leq \frac{|Q^n|}{|V_q(n,r)|}.$$

C is called a **perfect code** if equality in the sphere-packing bound holds.

A code $C \subset \mathbb{F}_q^n$ is said to be **linear** if it is a subspace of the Hamming space, that is, if it is closed under addition and scalar multiplication. Let $q = 2$, and let x be in a code C. Then the word $\bar{x}$ such that $\bar{x} + x = \mathbf{1}$, where $\mathbf{1}$ is the all-1 word, is called the complement of x. A code which contains the complements of all of its code words is said to be **self-complementary**. If $x, y \in \mathbb{F}_q^n$, then their inner product is defined as

$$\langle x, y \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

If a code C is linear and of dimension k and length n, it will be called an $[n, k, d]$ code. Also, we can find a basis $\{g_1, ..., g_k\}$ of C, and from this basis we define a matrix

$$G(C) = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}. \tag{4.1}$$

$G(C)$ is called the **generator matrix** of C. It can be transformed into one of the form $(I_k|P)$ by a combination of elementary row operations and column permutations. The elementary row operations put $G(C)$ into reduced echelon form, in which there is a set of k columns such that the i-th has 1 in position i and zero elsewhere; then a permutation of the columns moves these k columns to the front of the matrix.

The **dual code** $C^{\perp}$ of a linear code $C \subset \mathbb{F}_q$ is the set of all $x \in \mathbb{F}_q$ such that $\langle x, c \rangle = 0$ for all $c \in C$. The dimension of the dual code is $n - k$. The generator matrix of the dual code is $H(C) = (-P^t | I_{n-k})$ such that $G(C)H(C)^t = 0$ (the zero matrix). It is called the **parity-check matrix** of C. The code words of C satisfy $H(C)x^t = 0$.

For every code $C \subset \mathbb{F}_q^n$ in the Hamming space, the **extended code** is the subset of $\mathbb{F}_q^{n+1}$ which is obtained from C by adding an extra coordinate to each code word of C so that the sum of the coordinates is zero. A **truncation** of a code C is the code that is obtained from C by deleting one fixed coordinate position. Let C be an $[n, k, d]$ code, and let A_i be the number of code words of weight i . The numbers $A_0, A_1, \ldots, A_n$ are called the **weight distribution** of C.

We will define some important codes which are relevant to our study. These can be found in any standard book in coding theory, for instance [27] or [56]. The **binary**

Hamming code over $\mathbb{F}_2$ has the following parameters: length $n = 2^m - 1$, for positive integer $m \geq 3$, dimension $k = n - m$, and minimum distance $d = 3$. It has a parity check matrix $H(C)$ of size $m \times n$. The columns of $H(C)$ are all non-zero m-tuples of elements of $\mathbb{F}_2$. This is a perfect linear code.

The **Golay codes** can be defined by a generator matrix and can be constructed from the rows of that matrix. Consider the following matrices:

$$G_{11} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.2}$$

$$G_{12} = \left(\begin{array}{c|c} 0 & 1 \quad 1 \quad \ldots \quad 1 \\ \hline 1 & \\ \vdots & G_{11} \\ 1 & \end{array}\right) \tag{4.3}$$

$$G_{24} = (G_{12} | I_{12})$$

By [27, Corollary 11.1.4], the matrix G_{24} is a generator matrix of the **extended Golay code** C_{24}. This code has length $n = 24$, dimension 12, and minimum distance $d = 8$, by [27, Theorem 11.1.7]. The **binary Golay code** C_{23} can be obtained from the extended code C_{24} by deleting a fixed coordinate position. The code C_{23} is perfect with length $n = 23$, dimension 12, and minimum distance $d = 7$, by [27, Corollary 11.1.8, Corollary 11.1.9].

For ternary Golay codes, in the same way as before we provide the generator matrix of **the extended ternary Golay code** C_{12}, and **the perfect ternary code** C_{11} can be obtained from the extended code. Consider the following matrices:

$$G_5 = \begin{pmatrix} 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix} \tag{4.4}$$

$$G_6 = \left(\begin{array}{c|cccc} 0 & 1 & 1 & \dots & 1 \\ \hline 1 & & & & \\ \vdots & & G_5 & & \\ 1 & & & & \end{array}\right) \tag{4.5}$$

$$G_{12} = (G_6 | I_6) \tag{4.6}$$

By [56, Theorem 3] the extended ternary code C_{12} is spanned by the rows of G_{12} and has length $n = 12$, dimension $k = 6$, and minimum distance $d = 6$. The ternary code C_{11} is perfect and has length $n = 11$, dimension 6, and minimum distance $d = 5$ [27, Corollary 11.1.10].

A remarkable result in coding theory is the determination of the parameters of all perfect codes in the Hamming spaces over $\mathbb{F}_q$. It is due to Tietäväinen [73].

Theorem 4.8. *Let C be a non-trivial perfect code over a finite field $GF(q)$. Then C has the same parameters as either the Hamming code or the Golay code.*

The Hamming and binary Golay codes are e-error correcting codes. That concept was generalised by Karpovsky [47] to an L-code. For a subset L of $\{0, 1, \ldots, n\}$, the L-**sphere** around $x \in \mathbb{F}_q^n$ is the set

$$L(x) = \{y \in \mathbb{F}_q^n : d(x, y) \in L\}.$$

An L-**code** is a set $C \subset \mathbb{F}_q^n$ such that for any two code words $c_1, c_2 \in C$, we have $L(c_1) \cap L(c_2) = \phi$. The sphere-packing bound will be

$$|C| \leq \frac{q^n}{|L(c_1)|}$$

for some $c_1 \in C$. If equality holds, C will be called a perfect L-code. If code is linear, it will be denoted by $[n, k, L]$, where k is its dimension. For n odd, the following theorem by Cohen and Frankl [26] characterizes all self-complementary perfect L-codes in $\mathbb{F}_2^n$. It can be seen as an analogue of Theorem 4.8 in the binary case.

Theorem 4.9. *[26] For n odd, the only non-trivial self-complementary perfect*

L-codes in $\mathbb{F}_2^n$ are those with the same parameters as the Hamming binary code or the Golay binary code.

4.3 Imprimitive distance-regular graphs

A distance-regular graph Γ with diameter d is said to be ***imprimitive*** if there is a disconnected orbital graph Γ_i (a distance graph that has the same vertex set as Γ and where two vertices are adjacent if they are at distance i, where $\Gamma = \Gamma_1$). The set of connected components of the disconnected graph will be called **the system of imprimitivity**. When Γ is distance transitive, this set coincides with the system of imprimitivity of its automorphism group. Two important classes of imprimitive graphs are ***bipartite graphs*** and ***antipodal graphs***. A connected graph is said to be ***bipartite*** if its distance-2 graph is disconnected and it has exactly two connected components. An ***antipodal graph*** is defined as a connected graph Γ such that Γ_d is disconnected, d is the diameter of Γ. The following theorem is fundamental in the study of imprimitive graphs because it allows the reduction of the study of distance-regular graphs to only primitive graphs.

Theorem 4.10. *[19, Theorem 4.2.1] Let Γ be an imprimitive distance-regular graph with diameter d and degree at least 3. Then Γ is bipartite, antipodal, or both.*

If a distance-regular graph Γ with diameter $d \geq 2$ is bipartite, then Γ_2 has two connected components. A ***halved graph*** of Γ, denoted by $H\Gamma$, is defined as a graph with vertex set equal to the set of vertices in one of the components of Γ_2 and where two vertices in $H\Gamma$ are adjacent if their distance in Γ is 2. This graph has diameter $\left\lfloor \frac{d}{2} \right\rfloor$. If Γ is a distance-transitive graph, the two halved graphs are isomorphic.

For an antipodal distance-regular graph Γ with diameter d, we can define a new graph, called a **folded** graph $F\Gamma$, with the set of blocks as vertex set and where two blocks B_1, B_2 are adjacent if and only if there are $b_1 \in B_1$ and $b_2 \in B_2$ such that b_1, b_2 are adjacent in Γ. This graph has diameter $\lfloor \frac{d}{2} \rfloor$. We are interested in distance-regular graphs with diameter d, as we will make use of these graphs in the study of primitive graphs obtained from imprimitive Hamming graphs.

4.4 Hamming graphs

Let $Q^n = Q \times Q \times \cdots \times Q$, and let d be the Hamming distance on Q. We define the relations

$$R_i = \{(x, y) : d(x, y) = i\} \subseteq Q \times Q$$

where $1 \leq i \leq n$. The pair $(Q^n, R_{i\{0 \leq i \leq n\}})$ is the Hamming association scheme, and it is denoted by $\mathcal{A}H(n, q)$. Each relation R_i can be represented by an adjacency matrix, and hence by an orbital graph Γ_i. Thegraph. The graph that represents R_1 is the Hamming graph $H(n, q)$.

The automorphism group of the scheme is the wreath product $\mathrm{Sym}(q) \wr \mathrm{Sym}(n)$ that acts transitively on Q^n. Notice that $\mathrm{Sym}(q)$ is isomorphic to the symmetric group on Q, so if we assume that L is the direct product of n copies of $\mathrm{Sym}(q)$. Then the base group L acts as following; for every $y = (y_1, ..., y_n) \in L$ we have $xy = (x_1y_1, ..., x_ny_n)$, where $x \in Q^n$. Also, $\mathrm{Sym}(n)$ is the symmetric group on $\{1, \ldots, n\}$ that acts on Q^n by permuting the coordinates of its elements. The group $\mathrm{Sym}(q) \wr \mathrm{Sym}(n)$ is imprimitive when $q = 2$, and primitive and non-basic when $q > 2$. Thus the association scheme is non-synchronising, so non-separating. Nevertheless, we provide a maximum clique and maximum co-clique in $H(n, q)$ such that the product of their sizes is equal to the number of vertices in the scheme. This is to emphasize the approach we are going to take in this chapter.

Proposition 4.11. *The set $S = \{(x, 0, ..., 0) : x \in Q\}$ is a maximum clique in $\Gamma = H(n, q)$, and this graph has a co-clique of size q^{n-1}.*

Proof. Let $H(n, q)$ be the Hamming graph. The set S is a clique in Γ, hence it is sufficient to find a co-clique of size q^{n-1} to prove that S is maximum. Let C_1 be the set of all n-tuples of elements of $\mathbb{F}_q^n$ such that the first coordinate is 0. Then $|C_1| = q^{n-1}$. Define a new set as $C = \{c_1 A : c_1 \in C_1\}$, where A is the $n \times n$ matrix

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

The claim is that $|C| = q^{n-1}$, and that $d(c_1, c_2) > 1$ for every pair of distinct code words c_1, c_2 in C. Let $x = (0, x_1, ..., x_{n-1}), y = (0, y_2, ..., y_{n-1})$ be words in C_1, and assume that $xA = yA$. Then $(x_1, x_2, ..., x_1 + x_2 + \cdots + x_{n-1}) = (y_1, y_2, ..., y_1 + y_2 + y_{n-1})$, and this is true if and only if $x = y$, thus $|C_1| = |C| = q^{n-1}$. The distance between any pair of distinct code words x, y in C cannot be 1, because $x_n \neq y_n$ if and only if there is some i with $1 \leq i \leq n - 1$ such that $x_i \neq y_i$.

□

By Theorems 3.1, 3.2, we have:

Theorem 4.12. *The automorphism group G of the Hamming graph $H(n, q)$ is non-synchronising. Moreover, any subgroup H of G is non-synchronising*

Let Γ be an imprimitive distance-regular graph. Then from Section 3, it is possible to define a new distance-regular graph from Γ which might be primitive. The next section will address some of these graphs for which Γ is of type $H(n, 2)$.

4.5 Halved n-cube and folded halved n-cube

The vertex set of the n-cube (the Hamming graph $H(n, 2)$) defines a vector space known as the binary Hamming space and is denoted by $\mathbb{F}_2^n$. This graph is an imprimitive distance-regular graph with diameter n. It is bipartite and antipodal. It is bipartite because its distance-2 graph has two connected components: one that contains all the even words and one that contains all the odd words. It is antipodal because its distance-n graph has 2^{n-1} connected components each of which contains two vertices x and $\bar{x}$. In this section we use some results from coding theory over the field $\mathbb{F}_2$ to classify all non-synchronising association schemes obtained from the halved n-cube (the folded n-cube) and the folded halved n-cube. The halved graph, which is denoted by $H\Gamma_n$, will be defined on the set of even vertices. (It is isomorphic to the graph that is defined on the set of odd vertices.) The folded halved n-cube is denoted by $FH\Gamma_n$. This section is divided into two subsections. The first is for the case of halved n-cube, while the second is for the folded halved n-cube. Only the halved n-cube will be considered, as it produces the same association scheme as the folded n-cube. Let $H\Gamma_n$ be the halved graph of $H(n, 2)$, denote by $\mathcal{HA}_n$ the association scheme obtained from $H\Gamma_n$, and denote its orbital graphs by $H\Gamma = \Gamma_1, \Gamma_2, ..., \Gamma_{\lfloor \frac{n}{2} \rfloor}$.

4.5.1 Halved n-cube and folded n-cube

If $n \leq 3$, then $H\Gamma_n$ is a complete graph, so $\mathcal{HA}_n$ is synchronising. Therefore, from now on we assume that $n \geq 4$. Note that the halved n-cube is imprimitive when

$n \geq 4$ and even.

Lemma 4.13. *Let $n \geq 5$ be an odd integer and let ${\mathbb{F}_2}^{n^+}$ be the subspace of ${\mathbb{F}_2}^n$ that contains the even words. If there is a perfect L^+-code C^+ in $\mathbb{F}_2^{n^+}$ such that $L^+ \subset \{0, 2, ..., n-1\}$, then there is a self-complementary perfect L-code C in ${\mathbb{F}_2}^n$ such that $L \subset \{0, 1, ..., n\}$. Moreover, $C = \{\mathbf{0}, \mathbf{1}\} \oplus C^+$.*

Proof. Assume that $L^+ \subset \{0, 2, ..., n-1\}$. Let C^+ be a perfect L^+-code, and let S^+ be the L^+-sphere around $c \in C^+$. Both C^+ and S^+ consist only of even words, respectively. Since n is odd, $\mathbf{1}$ is an odd word. Set C to be $\{\mathbf{0}, \mathbf{1}\} \oplus C^+$, which is a self-complementary L-code in ${\mathbb{F}_2}^n$, where $L = L^+$.

For $x \in C^+$ and $S^+ = L^+(x) = \{z \in \mathbb{F}_2^{n^+} : d(x, z) \in L^+\}$, set

$$S = L(x \oplus \mathbf{1}) = \{z \oplus \mathbf{1} \in \mathbb{F}_2^n : d(x \oplus \mathbf{1}, z \oplus \mathbf{1}) = d(x, z) \in L\},$$

which contains only odd code words. Thus for all $x, y \in C^+$, $L(x) \cap L(y \oplus \mathbf{1}) = \phi$ and $L(x \oplus \mathbf{1}) \cap L(y \oplus \mathbf{1}) = \phi$ (otherwise, $L(x) \cap L(y) \neq \phi$). Thus, C is a self-complementary perfect L-code in $\mathbb{F}_2^n$. □

Lemma 4.14. *Let $n \geq 5$ be an odd integer and $L^+ \subset \{0, 2, ..., n-1\}$. Then the association scheme $\mathcal{HA}_n$ is non-synchronising if and only if there is a perfect L^+-code in the binary even space ${\mathbb{F}_2}^{n+}$.*

Proof. For the proof of $\Longrightarrow$, assume that $\mathcal{HA}$ is non-synchronising, so non-separating, by Theorem 4.7. Since it is primitive, there is a non-trivial connected graph Γ^* in the scheme such that its clique number is equal to the chromatic number and $|S||C| = |V(\Gamma^*)|$, where S and C are a maximum clique and a maximum co-clique, respectively. Thus, there is a partition of the vertex set to either cliques or co-cliques. Suppose that there is a partition of the vertex set of the graph into co-cliques. Denote each part in the partition by $S + c$, where $c \in C$. Each part intersects C in exactly one point, Corollary 2.28. Furthermore, Γ^* is a union of orbital graphs Γ_i, where $i \in L^+ \subset \{0, 2, ..., n-1\}$ and for every pair of code words s_1, s_2 in a coset of S we have $d(s_1, s_2) \in L$. Thus we can regard S as an L^+-sphere and C as the perfect L^+-code which satisfies the sphere-packing bound in $\mathbb{F}_2^{n^+}$.

For the converse, let $L^+ \subset \{0, 2, ..., n-1\}$, and let C be a perfect L^+-code in $\mathbb{F}_2^{n^+}$ such that for all $c \in C$, $L(c) = S$ is a sphere. Moreover, $|C||S| = |\mathbb{F}_2^{n^+}|$, and $L^+(c_1) \cap L^+(c_2) = \phi$ for all $c_1, c_2 \in C$. Define a graph Γ^- in the scheme $\mathcal{HA}_n$ as the union of the graphs Γ_i, where $i \in L^+$. This graph contains S, as it is a maximum clique, and we claim that C is a maximum co-clique. To prove this, we need to show that $d(c_1, c_2) \notin L^+$, so suppose not. Then $L^+(c_1) \cap L^+(c_2) \neq \phi$, which contradicts the fact that C is a perfect L^+-code. Finally, the product of the clique number and the co-clique number in Γ^- is equal to the number of vertices, which follows from the sphere-packing bound. □

Theorem 4.15. *Let $n \geq 5$ be an odd integer, and suppose that there is no self-complementary perfect L-code in $\mathbb{F}_2^n$. Then the association scheme $\mathcal{HA}_n$ is synchronising.*

Proof. This follows immediately from the previous two lemmas. □

Lemma 4.16. *Let $n \geq 5$ be an odd integer and $L^+ \subset \{0, 2, ..., n-1\}$, and let C be either a Hamming code or a binary Golay code in the binary Hamming space $\mathbb{F}_2^n$. Then there is a perfect linear L^+-code C^+ in the binary even space $\mathbb{F}_2^{n^+}$. Moreover, C^+ consists of all even code words of C.*

Proof. First, assume that C is a Hamming code which is linear, so either all code words are even or half of them are even. By Theorem 4.9, the code is self-complementary, so C contains $\mathbf{1}$ which is an odd code word. Thus, half of the code words in C are even. Denote the set of all even code words of C by C^+. Clearly, C^+ is a linear code in $\mathbb{F}_2^n$ and $\mathbb{F}_2^{n^+}$. It remains to show that C^+ is a perfect L^+-code in the even space. This can be done by finding an L^+-sphere S that satisfies the sphere-packing bound in $\mathbb{F}_2^{n^+}$. S can be constructed as the set of all words of weight $n-1$ in addition to the zero word, $\mathbf{0}$. Note that a word x with $wt(x) = n-1$ cannot be in C^+. Also, we have $L^+ = \{0, 2, n-1\}$.

Second, assume that C is a binary Golay code. By reasoning analogous to that in the proof for C a Hamming code, let C^+ be the set of all even code words in C. The sphere S and L can be found by looking at the weight distribution of the binary Golay code in [56, Theorem 27].

Table 4.1: Weight distribution of the binary Golay code

Weight	0	7	8	11	12	15	16	23
Number of code words	1	253	506	1288	1288	506	253	1

We can see that the code C^+ has size 2048 and that S must be of size $|\mathbb{F}_2^+|/|C^+| =$ 2048. Let S be the set of words of weight $0, 2, 20$, and 22. The numbers of words of those sizes are $1, 253, 1771$, and 23, respectively. Also, C is linear and the distance of any two code words cannot be $0, 2, 4, 10, 14, 18, 20$, or 22, by Table 4.1. Therefore, we choose L^+ to be $\{0, 2, 4, 10, 14, 18, 20, 22\}$. □

We have seen that the synchronisation property of $\mathcal{HA}_n$ is closely related to the notion of a perfect L-code in the binary Hamming space. This relation results in a complete determination for the cases where the association scheme is non-synchronising.

Theorem 4.17. *Let $\mathcal{HA}_n$ be the association scheme obtained from the halved graph $H\Gamma_n$ of $H(n,2)$. Then the following hold:*

(a) if $n \geq 4$ is even, $\mathcal{HA}_n$ is imprimitive and consequently non-synchronising.

(b) if $n \leq 3$, $H\Gamma_n$ is a complete graph and $\mathcal{HA}_n$ is synchronising.

(c) if $n \geq 5$ and odd, $\mathcal{HA}_n$ is non-synchronising if and only if there is some positive integer m such that $n = 2^m - 1$, or $n = 23$, that is, there is a binary Hamming code or a binary Golay code.

Proof. (a) If $n \geq 4$ and even, then the diameter of $\mathcal{HA}_n$ is $d = \frac{n}{2}$. The graph Γ_d with vertex set the same as $H\Gamma_n$ and two vertices x, y are adjacent if $d(x,y) = \frac{n}{2}$ in $H\Gamma_n$. The graph Γ_d is disconnected and each component contains an vector and its complement.

(b) If $n = 2$, then the graph $H\Gamma_n$ has two vertices; $(0,0)$ and $(1,1)$. The graph is complete, so the scheme is synchronising. If $n = 3$, then the graph $H\Gamma_n$ has four vertices and the distance between any two is 2, so the graph is complete. Therefore, the association scheme is synchronising.

(c) Assume that $\mathcal{HA}_n$ is non-synchronising. Then by Theorem 4.15 there is a self-complementary perfect L-code in $\mathbb{F}_2^n$, and by Theorem 4.9 this is true if and only if there is a Hamming code or a Golay code.

Conversely, if there is a binary Hamming code or a binary Golay code, then by Lemma 4.16 there is an even perfect L-code in $\mathbb{F}_2^{n^+}$. Therefore, by Lemma 4.14 the association scheme is non-synchronising.

□

By Theorems 3.1, 3.2, we have:

Theorem 4.18. *Let G be the automorphism group of the halved graph $H\Gamma_n$ of $H(n,2)$. Then the following hold:*

(a) if $n \geq 4$ is even, the group G is imprimitive and consequently non-synchronising.

(b) if $n \leq 3$, the group G is synchronising.

(c) if $n \geq 5$ and odd, the group G is non-synchronising if and only if there is some positive integer m such that $n = 2^m - 1$, or $n = 23$, that is, there is a binary Hamming code or a binary Golay code.

4.5.2 Folded halved n-cube

If $n \geq 4$ is even, the halved n-cube $H\Gamma_n$ is imprimitive and antipodal, whereas the folded n-cube $F\Gamma_n$ is imprimitive and bipartite. In this subsection the folded halved n-cube, which is isomorphic to the halved folded n-cube is considered. It is denoted by $FH\Gamma_n$, and its association scheme is denoted by $\mathcal{FHA}_n$. Let $\Delta_1, \Delta_2, ..., \Delta_{\frac{n}{4}}$ be the orbital graphs of $\mathcal{FHA}_n$.

Proposition 4.19. *Let $n \geq 8$ be an even integer. Then the orbital graphs of $\mathcal{FHA}_n$ are unions of the orbital graphs of $\mathcal{HA}_{n-1}$.*

Proof. Let $n \geq 8$ be even. Then the vertices (code words) of $\mathcal{FHA}_n$ are the 2-element subsets of the set of all even vertices in $\mathbb{F}_2^n$. Every 2-element subset contains an even vertex and its complement. Two vertices B_1, B_2 are adjacent if there are $x \in B_1$ and $y \in B_2$ such that $d(x,y) \in \{2, n-2\}$. Therefore, the intersection set of the association scheme is $\{I_1 = \{2, n-2\}, ..., I_{\frac{n}{4}} = \{\frac{n}{2}\}\}$, that is, for every orbital graph Δ_i in $\mathcal{FHA}_n$ there is a fixed I_i such that two vertices D_1, D_2 are adjacent if and only if there are $u \in D_1$ and $w \in D_2$ with $d(u, w) \in I_i$. On the other hand, the vertex set of $\mathcal{HA}_{n-1}$ contains all the even vertices in $\mathbb{F}_2^{n-1}$, and the orbital graphs of $\mathcal{HA}_{n-1}$ have intersection set $\{2, 4, ..., n-2\}$. Consider the vertices of $\mathcal{HA}_{n-1}$ by adding a zero component to each vertex. We can identify these vertices with the vertices in $\mathcal{FHA}_n$. Finally, by comparing the intersection sets of the two association schemes, we obtain the conclusion of the Proposition. $\square$

Corollary 4.20. *If $\mathcal{HA}_{n-1}$ is synchronising, then $\mathcal{FHA}_n$ is synchronising.*

Theorem 4.21. *Let $\mathcal{FHA}_n$ be the association scheme obtained from the halved folded graph $FH\Gamma_n$ of n-cube, where $n > 2$ and even. Then the following hold:*

(a) if $n \leq 6$, $FH\Gamma_n$ is a complete graph and $\mathcal{FHA}_n$ is synchronising.

(b) if $n \geq 8$, $\mathcal{FHA}_n$ is non-synchronising if and only if there is some positive integer m such that $n = 2^m$, or $n = 24$.

Proof. The proof of (a) is trivial. For (b), if there is no positive integer m such that $n = 2^m$, and if $n \neq 24$, then $\mathcal{HA}_{n-1}$ is synchronising and, by 4.20, $\mathcal{FHA}_n$ is synchronising. Conversely, if $n = 2^m$ for some positive integer m, then $\mathcal{HA}_{n-1}$ is non-synchronising and contains a graph Γ such that the product of the clique and co-clique numbers is equal to the number of vertices. In particular, by Theorem 4.16 this is a graph in which two vertices x, y are adjacent if and only if $d(x, y) \in \{2, n-2\}$. This graph is in $\mathcal{FHA}_n$. In the case where $n = 24$, by Lemma 4.16 there is a graph Γ that satisfies equality in the clique–co-clique bound. Two of its vertices x, y are adjacent if and only if $d(x, y) \in \{2, 4, 10, 14, 18, 20, 22\}$, and it is in $\mathcal{FHA}_n$. Therefore, $\mathcal{FHA}_n$ is non-synchronising. $\square$

By Theorems 3.1, 3.2, we have:

Theorem 4.22. *Let G be the automorphism group of the halved folded graph $FH\Gamma_n$ of n-cube, where n is even. Then the following hold:*

(a) if $n \leq 6$, the group G is synchronising.

(b) if $n \geq 8$, the group G is non-synchronising if and only if there is some positive integer m such that $n = 2^m$, or $n = 24$.

4.6 Bilinear forms graph

4.6.1 Basic definitions

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, and set $V_1 = \mathbb{F}^{n_1}$ and $V_2 = \mathbb{F}^{n_2}$. A ***bilinear form*** from $V_1 \times V_2$ to $\mathbb{F}$ is a function

$$B : V_1 \times V_2 \longrightarrow \mathbb{F}$$

such that for all $v \in V_1$ and $u \in V_2$, the maps

$$\begin{array}{ccc} B_u : V_1 \longrightarrow \mathbb{F} & & B_v : V_2 \longrightarrow \mathbb{F} \\ & \text{and} & \\ v \mapsto B(v,u) & & u \mapsto B(v,u) \end{array}$$

are linear.

Let V_1 and V_2 be as defined before. If $\{\beta_{11}, \beta_{12}, ..., \beta_{1n_1}\}$ is a basis for V_1 and $\{\beta_{21}, \beta_{22}, ..., \beta_{2n_2}\}$ is a basis for V_2, then every bilinear form B can be represented uniquely by an $n_1 \times n_2$ matrix A_B, where $A_B(i,j) = B(\beta_{1i}, \beta_{2j})$. The ***Segre outer product*** of $v_1 = (v_{11}, ..., v_{1n_1}) \in V_1$ and $v_2 = (v_{21}, ..., v_{n_2}) \in V_2$, denoted by $v_1 \otimes v_2$ is the array $[v_{1k_1} v_{2k_2}]_{k_1,k_2=1}^{n_1,n_2}$. The ***tensor product*** of V_1 and V_2, denoted by $V_1 \otimes V_2$, is the vector space that is spanned by all vectors of the form $v_1 \otimes v_2$ such that $v_1 \in V_1$ and $v_2 \in V_2$ over $\mathbb{F}$. The space $V = V_1 \otimes V_2$ has $\{\beta_{1k_1} \otimes \beta_{2k_2} : 1 \leq k_1 \leq n_1, 1 \leq k_2 \leq n_2\}$ as a basis. Therefore, any vector v in V can be written as

$$\sum_{k_1 k_2 = 1}^{n_1 n_2} a_{k_1 k_2} \beta_{1k_1} \otimes \beta_{2k_2},$$

and v can be represented by a matrix $A = (a_{k_1 k_2})$ and V can be regarded as the vector space of $n_1 \times n_2$ matrices (or bilinear forms) over the finite field $\mathbb{F}$.

Let $GL(n, \mathbb{F})$ be the general linear group which contains of all invertible $n \times n$ matrices over $\mathbb{F}$. The group $G_0 = GL(n_1, \mathbb{F}) \times GL(n_2, \mathbb{F})$ acts on the additive vector space V as following:

$$A \mapsto P^{-1} A Q, \ A \in V,$$

where $P \in GL(n_1, \mathbb{F})$ and $Q \in GL(n_2, \mathbb{F})$. Assume that G is the group generated by the following transformations:

$$A \mapsto P^{-1} A Q + R, \ A \in V,$$

where $P \in GL(n_1, \mathbb{F})$, $Q \in GL(n_2, \mathbb{F})$ and $R \in V$. Then, G acts transitively on V. To see this, let A_1 and A_2 be two $n_1 \times n_2$ matrices, then the map

$$A \mapsto A + (A_2 - A_1),$$

takes A_1 to A_2. Any graph Γ with the property that $G \leq \mathrm{Aut}(\Gamma)$ appears as union of orbital graphs obtained from the induced action of G on $V \times V$. Since G is transitive on V, by Lemma 2.4.1 in [37], there is a one to one correspondence between the orbits of G on $V \times V$ and the orbits of G_0 on V. Two matrices $A, B \in V$

are in the same orbit of G_0 if there are $P \in GL(n_1, \mathbb{F})$ and $Q \in GL(n_2, \mathbb{F})$ such that $P^{-1}AQ = B$. Then A and B have the same rank. Therefore, an orbital graph Γ_i is the graph with V as the vertex set and two vertices $A, B \in V$ are adjacent if $\text{rank}(A - B) = i, 1 \leq i \leq n_2 \leq n_1$ Furthermore, the group G acts irreducibly and we have the following:

Theorem 4.23. *[79, Theorems (2.2-2.3)] The group G acts primitively on the set V of all $n_1 \times n_2$ matrices over a finite field $\mathbb{F}$.*

The set of all orbital graphs together with the graph of the diagonal relation, provides an association scheme. Therefore, for a graph Γ in this association scheme we have $\omega(\Gamma)\alpha(\Gamma) \leq |V|$. The ***bilinear forms graph*** is the graph $\Gamma_1 = \text{BF}(n_1, n_2, q)$ with vertex set V and two vertices (matrices) $A, B \in V$ are adjacent if $\text{rank}(A - B) = 1$. In fact, any orbital graph Γ_i, for $2 \leq i \leq min\{n_1, n_2\}$ is distance i graph of the bilinear forms graph. Γ_1 is a connected regular graph which is distance transitive [79, Theorem 2.6]. Also it is not difficult to find its degree.

Lemma 4.24. *[79, Lemma 2.1] The degree of the bilinear forms graph equals* $\frac{(q^{n_1}-1)(q^{n_2}-1)}{q-1}$.

4.6.2 Maximal sets of rank 1

Let $V = V_1 \otimes V_2$ be the vector space, which is defined before. In [78, Corollary 3.9], the authors defined a maximal set of rank 1 to be a non-empty subset $\mathcal{M}$ of the vertex set of the graph Γ_1 with the property that any two points of $\mathcal{M}$ are adjacent and there is no other point outside $\mathcal{M}$, which is adjacent to each point of $\mathcal{M}$. Let $E_{k_1k_2}$ be the $n_1 \times n_2$ matrix with all entries equal 0 except the $(k_1, k_2)^{th}$ entry equals 1. Then, the set of all $E_{k_1k_2}$ matrices, where $1 \leq k_i \leq n_i$ for $i \in \{1, 2\}$, is a basis of the vector space V and we have the following.

Lemma 4.25. *[78, Corollary 3.9] A maximal set of rank* 1 *is either of the form*

$$\mathcal{M}_1 = \{P^{-1}A_{k_1}Q+R : 1 \leq k_1 \leq n_1,\ P \in GL(n_1,\mathbb{F}),\ Q \in GL(n_2,\mathbb{F}),\ \textit{and}\ R \in V\},$$

or of the form

$$\mathcal{M}_2 = \{P^{-1}A_{k_2}Q+R : 1 \leq k_2 \leq n_2,\ P \in GL(n_1,\mathbb{F}),\ Q \in GL(n_2,\mathbb{F}),\ \textit{and}\ R \in V\}.$$

4.6.3 Clique and co-cliuqe numbers

Every set $\mathcal{M}$ forms a clique in the bilinear forms graph Γ_1. Particularly, if $n_1 < n_2$, the set $\mathcal{M}_1$ is a maximum clique in the bilinear forms graph while the set $\mathcal{M}_2$ is a maximal but not maximum clique in the graph. Similarly, when n_2 is less than n_1. Therefore, the clique number of Γ_1 is equal to q^k, where $k = \max\{n_1, n_2\}$. If $n_1 < n_2$, then $\omega(\Gamma_1) = q^{n_2}$ and by the clique–co-clique bound we know that $\omega(\Gamma_1)\alpha(\Gamma_2) \leq q^{n_1 n_2}$, but the next theorem shows that the graph has co-clique number equal $q^{(n_1-1)n_2}$.

Theorem 4.26. *[43, Theorem 2.6] Let $2 \leq n_1 \leq n_2$, and Γ_1 be the bilinear forms graph. Then, its co-clique number is*

$$\alpha(\Gamma) = q^{(n_1-1)n_2}.$$

Corollary 4.27. *The association schemes that are obtained from bilinear forms graphs are non-separating.*

Also, by the equivalence of the separation and synchronisation properties of groups of affine type4.7, we have:

Corollary 4.28. *The association schemes that are obtained from bilinear forms graphs are non-synchronising.*

By Theorems 3.1, 3.2, we have:

Theorem 4.29. *The automorphism group of the bilinear forms graph* $\mathrm{BF}(n_1, n_2, q)$ *is non-synchronising.*

4.7 Alternating forms graph

Let V be an n-dimensional vector space over a finite field $\mathbb{F}_q$. A bilinear form B is said to be:

an **alternating form** if

$$B(x, x) = 0 \text{ } for \text{ } all \text{ } x \in V.$$

Consequently,

$$A_B(i, i) = 0 \text{ } and \text{ } A_B(i, j) = -A_B(j, i), 1 \leq i, j \leq n.$$

A_B is called an **alternating matrix**. The set of alternating $n \times n$ matrices over a finite field $\mathbb{F}_q$ is a vector space of dimension $\frac{1}{2}n(n-1)$, and denoted by $\mathrm{Alt}_n(\mathbb{F}_q)$. A basis of the vector space can be given by the set $\{E_{ij} - E_{ji} : 1 \leq i < j \leq n\}$, where E_{ij} is the $n \times n$ matrix in which the (i, j)th element is 1 and all the other elements are 0.

The rank of an alternating matrix A is always even.

Lemma 4.30. *[78, Proposition 1.34] Let A be an $n \times n$ alternating matrix over a finite field $\mathbb{F}_q$. Then A has even rank.*

Let $A\Gamma_n(q)$ be a graph defined on the set of alternating matrices over $\mathbb{F}_q$, where two matrices A, B are adjacent if and only if $\operatorname{rank}(A - B) = 2$. The graph $A\Gamma_n(q)$ is known as the **alternating forms graph**. This graph is primitive and distance transitive of diameter $\lfloor \frac{n}{2} \rfloor$ [19, Theorem 9.5.3]. The distance between any two matrices in $A\Gamma_n(q)$ is equal to $\frac{1}{2}\operatorname{rank}(A - B)$ [78, Proposition 4.5]. The clique number of the graph $A\Gamma_n(q)$ is the maximum number of matrices in $A\Gamma_n(q)$ such that for any two matrices A, B, we have $\operatorname{rank}(A - B) = 2$. In [78, Corollary 4.9], all maximal cliques in the graph $A\Gamma_n(q)$ are determined. They are called maximal sets of rank 2.

Lemma 4.31. *[78, Corollary 4.9] Let $A\Gamma_n(q)$ be the alternating forms graph. Then its clique number is $q^{(n-1)}$.*

Since the graph $A\Gamma_n(q)$ is distance transitive, it is distance regular, so the adjacency matrices of its distance graphs define an association scheme. This association scheme was first investigated by Cameron and Seidel [23] for the binary field. Then Delsarte and Goethals [30] studied the scheme for all q. In the study of synchronisation theory, it is clear that if $n = 2$ or 3 then the association scheme obtained from the alternating forms graph $A\Gamma_n(q)$ is obviously synchronising. This is because the graph $A\Gamma_n(q)$ is complete. For $n \geq 4$, we need more results.

Delsarte and Goethals consider the property of a set $Y \subset \operatorname{Alt}_n(\mathbb{F}_q)$ which is an analogue of the t-intersecting sets in the Johnson scheme. Such a set is called an (n, d)-set with the property that $\operatorname{rank}(A - B) \geq 2d$ for all $A, B \in Y$, where $1 \leq d \leq \lfloor \frac{n}{2} \rfloor$. In their study, they provide an upper bound on the size of Y.

Lemma 4.32. *[30, Theorem 4] Let Y be an (n, d)-subset of* $\mathrm{Alt}_n(\mathbb{F}_q)$ *. Then there is an upper bound on the size of Y, which is*

$$|Y| \leq c^{m-d+1},$$

where $c = q^{\frac{n(n-1)}{2m}}$ and $m = \lfloor \frac{n}{2} \rfloor$.

An $(n, 2)$-set is a co-clique in $A\Gamma_n(q)$. An (n, d)-set of size equal to this bound is said to be **maximal**. It has been shown that the bound is attained when n is odd or both n and q are even.

Lemma 4.33. *[30, Theorem 8] Let $n \geq 4$ be an odd integer . Then there exists a maximal (n, d)-set Y in* $\mathrm{Alt}_n(q)$.

Lemma 4.34. *[30, Theorem 9] Let $n \geq 4$ be an even integer, and let q be even. Then there exists a maximal (n, d)-set Y in* $\mathrm{Alt}_n(q)$.

Whether there exists an (n, d)-set of size equal to the bound when n is even and q is odd is stated as an open question in [30, p.26].

Theorem 4.35. *Let n and q be even. Then the association scheme that is obtained from the alternating forms graph $A\Gamma_n(q)$ is non-synchronising.*

Proof. Assume that n and q are even. Then, by Theorem 4.34, there exists a maximal $(n, 2)$-set Y in $\mathrm{Alt}_n(q)$. Its size is $q^{\frac{1}{2}(n-1)(n-2)}$, by Lemma 4.32. The set Y is a co-clique in the graph $A\Gamma_n(q)$. By Lemma 4.31, the clique number in this graph is $q^{(n-1)}$. The product of the clique number and the co-clique number is equal to the number of vertices in the graph which is $q^{\frac{1}{2}n(n-1)}$. Therefore, there is a graph in the scheme such that the product of the clique and co-clique numbers equals the number of vertices. Then, the scheme is non-separating, so non-synchronising by Theorem 4.7. $\square$

Proposition 4.36. *The association scheme obtained from the alternating forms graph $A\Gamma_5(q)$ is synchronising.*

Proof. The association scheme has two orbital graphs, $A\Gamma_n(q)$ and its complement. By Lemma 4.31, the clique number is q^4, while by Lemma 4.33 the co-clique number is q^5. However, the number of vertices is q^{10} , hence equality does not hold in the clique–co-clique bound. Therefore, the scheme is synchronising. $\square$

It is probably the case that the association scheme obtained from $A\Gamma_n(q)$ is synchronising whenever n is an odd integer.

A graph Γ is said to be **core** if every endomorphism is an automorphism, and **pseudo-core** if every endomorphism is an automorphism or a colouring. The authors of [42] studied the endomorphisms of the alternating forms graphs and showed the following:

Theorem 4.37. *[42, Theorem 1.1] Let $n \geq 4$ be an integer. Then the graph $A\Gamma_n(q)$ is a pseudo-core. Moreover, if n is odd, then $A\Gamma_n(q)$ is a core, but if both n and q are even, then $A\Gamma_n(q)$ is not a core.*

For the case where n is even and q is odd, it remains to be determined whether the graph $A\Gamma_n(q)$ is core or not. To the best of my knowledge, the only progress in this direction has been made by Patterson [59] showing that for $n = 4$ and $q = 3$, the co-clique number of the alternating form graph is $q^3 = 27$. In this case the corresponding association scheme is non-synchronising By Theorems 3.1, 3.2, we have:

Proposition 4.38. *The automorphism group G of the alternating forms graph $A\Gamma_5(q)$ is synchronising.*

Proposition 4.39. *The automorphism group G of the alternating forms graph $A\Gamma_4(3)$ is non-synchronising.*

Theorem 4.40. *Let n and q be even. Then the automorphism group G of the alternating forms graph $A\Gamma_n(q)$ is non-synchronising.*

4.8 Hermitian forms graph

Let $\mathbb{F}_{q^2}$ be a finite field of cardinality q^2 that is equipped with an involution $x \mapsto \overline{x}$ for every $x \in \mathbb{F}_{q^2}$, where $\overline{x} = x^q$ (An involution is an automorphism of order 2. Then $\mathbb{F}_q$ is the fixed field of $\mathbb{F}_{q^2}$.

Let $V = \mathbb{F}_{q^2}^n$, and let X be the set of all sesquilinear forms

$$f : V \times V \longrightarrow \mathbb{F}_{q^2}^n$$

such that $f(x, y)$ is linear in y and $f(y, x) = \overline{f(x, y)}$ for all $x, y \in V$. If $\{e_1, e_2, ..., e_n\}$ is a fixed basis of V, then for every form $f \in X$ there is a matrix $A = [f(e_i, e_j)]$. The form f is called a Hermitian form, and A is the corresponding Hermitian matrix. A satisfies $\bar{A}^t = A$, where the matrix A^t is the transpose of A and $\bar{A} = (\bar{a_{ij}})$ where $A = (a_{ij})$. Let $H_n(\mathbb{F}_{q^2}) = X$ be the space of all $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$. This is an n^2-dimensional vector space over $\mathbb{F}_{q^2}$ [19, p.285]. Define the Hermitian forms graph $H\Gamma_n(\mathbb{F}_q)$ as the graph that has $H_n(\mathbb{F}_{q^2})$ as its vertex set and where two vertices A, B are adjacent if their difference has rank 1. This graph is distance transitive of diameter n [19]. The association scheme of $H_n(\mathbb{F}_{q^2})$ will be denoted by $\mathcal{AH}\Gamma_n(\mathbb{F}_{q^2})$. Schmidt [65] studies the properties of a d-code in the space of Hermitian matrices through the association scheme of the Hermitian forms graph. The d-code is a subset of $H_n(\mathbb{F}_{q^2})$ such that the rank of the difference of any two of its matrices is at least d. Schmidt finds the eigenmatrix P of the association scheme $\mathcal{AH}\Gamma_n(\mathbb{F}_{q^2})$; the elements of P are given by the polynomial $P_{ij} = Q_j(i)$, where

$$Q_j(i) = (-1)^j \sum_{h=0}^{j} (-q)^{\binom{j-h}{2}+hd} \begin{bmatrix} d-h \\ d-j \end{bmatrix}_b \begin{bmatrix} d-i \\ h \end{bmatrix}_b \tag{4.7}$$

The base of the Gaussian coefficient is $b = -q$.

Let $\mathbb{F} = \mathbb{F}_{q^2}$, and let $GL(n, \mathbb{F})$ be the set of all $n \times n$ invertible matrices over $\mathbb{F}$. A maximal set of rank r in the space of Hermitian matrices is a set of Hermitian matrices such that the difference of any two matrices has rank at most r. The following result [78] gives a criterion for a maximal set of rank 2 in $H_n(\mathbb{F})$.

Lemma 4.41. *[78] Let $\Gamma_{1,2}$ be the graph with vertex set $H_n(\mathbb{F}_{q^2})$ and where two matrices are adjacent if the rank of their difference is* 1 *or* 2*. Then the maximum clique has size $q^{2(n-1)}$.*

The association scheme $\mathcal{AH}\Gamma_n(\mathbb{F}_{q^2})$ obtained from the Hermitian forms graph is expected to be synchronising; the cases where $n = 2$ and $n = 3$ are provided here. The eigenvalues of the graphs in $\mathcal{AH}\Gamma_2(\mathbb{F}_{q^2})$ and $\mathcal{AH}\Gamma_3(\mathbb{F}_{q^2})$ are used to prove that. (We use the result that if $\alpha(\Gamma)\omega(\Gamma) = V(\Gamma)$, then $\omega(\Gamma) = 1 - \frac{\deg(v)}{\tau}$, where τ is the smallest eigenvalue of Γ.)

Proposition 4.42. *The association scheme $\mathcal{AH}\Gamma_2(\mathbb{F}_{q^2})$ is synchronising.*

Proof. Since the graph $H\Gamma_2(\mathbb{F}_q)$ has diameter 2, this association scheme has only two orbital graphs. The Hermitian forms graph $H\Gamma_2(\mathbb{F}_q)$ and its complement.

The eigenvalues of $H\Gamma_2(\mathbb{F}_q)$ can be calculated by polynomial 4.7 and the software Mathematica [83]. The eigenvalues are

$$(q-1)(q^2+1),\ 1+q-q^2,\ (q-1).$$

The smallest eigenvalue is $\tau = 1+q-q^2$, and it does not divide the degree , because $\deg(v) = (q-1)(q^2+1)$, by Corollary 2.29. Furthermore, by Corollary 3.6 $\omega(\Gamma) < 1 - \frac{\deg(v)}{\tau}$. Therefore, the product of the clique and co-clique numbers is less than the number of vertices. The same holds for the complement, so the association scheme is synchronising. □

Theorem 4.43. *The association scheme $\mathcal{AH}\Gamma_3(\mathbb{F}_{q^2})$ is synchronising.*

Proof. The Hermitian graph has diameter 3, so the association scheme has three orbital graphs: $\Gamma_1 = H\Gamma_3(\mathbb{F}_q)$, Γ_2, and Γ_3. The other non-trivial graphs in the scheme are the complements of the orbital graphs. Therefore, we only need to check the product of the clique number and the co-clique number of orbital graphs.

We can use the polynomial 4.7 to obtain the eigenvalues of the first orbital graph $\Gamma_1 = H_3(\mathbb{F}_{q^2})$ are

$$(q^2+q+1)(q(q-1)-1)(q-1),\ -(q^2+1)q(q-1)-1,\ (q^2+1)(q-1),\ (-q^2+q-1).$$

The smallest eigenvalue is $\tau = -(q^2+1)q(q-1)-1$ and the degree is $\deg(v) = (q^2+q+1)(q(q-1)-1)(q-1)$, by Corollary 2.29. By Corollary 3.6, if the product of the clique and the co-clique numbers in the graph equals the number of vertices, then the smallest eigenvalue divides the degree. However, $deg(v) = (-q)\tau + (-2q^3+1)$, so $\omega(\Gamma_1)\alpha(\Gamma_1) < V(\Gamma_1)$.

By polynomial 4.7, the eigenvalues of the second orbital graph Γ_2 are

$$(q^2+q+1)(q^2+1)(q(q-1)-1)(q-1),\ (q^2+1)^2 q(q-1),\ (q(q-1)^2-1)q,\ q(-q^2+q-1)).$$

$\tau = q(-q^2+q-1)$ is the smallest eigenvalue, and the degree is $\deg(v) = (q^2+q+1)(q^2+1)(q(q-1)-1)(q-1)$, by Corollary 2.29. Assume that equality holds in the clique–co-clique bound. Then, by Corollary 3.6 the clique number must be

$$\omega(\Gamma_2) = 1 - \frac{\deg(v)}{\tau = 1-(q^2(q^3+q-1)}.$$

Also, the clique number must divide the number of vertices of Γ_2, that is,

$$\frac{V(\Gamma_2)}{\omega(\Gamma_2)} = \frac{q^7}{q^3+q-1},$$

must be an integer. This is not true for all q, which provides a contradiction to the assumption, and hence we have that $\omega(\Gamma_2)\alpha(\Gamma_2) < V(\Gamma_2)$.

By polynomial 4.7, the eigenvalue of the third orbital graph are

$$(q^2+q+1)(q^2+1)q^3(q-1)^2,\ -(q^2+1)q^3(q-1),\ -q^3(q-1),\ q^3.$$

In this case, the smallest eigenvalue is $\tau = -(q^2+1)q^3(q-1)$, the degree is $\deg(v) = (q^2+q+1)(q^2+1)q^3(q-1)^2$, by Corollary 2.29. The smallest eigenvalue divides the degree. If $\omega(\Gamma_3)\alpha(\Gamma_3) = V(\Gamma_3)$, the clique number, by Corollary 3.6, must be

$$\omega(\Gamma_3) = 1 - \frac{\deg(v)}{\tau} = 1-(1-q^3) = q^3.$$

As result, the co-clique number must be $\alpha(\Gamma_3) = q^6$. However, this is not true, as we can see from Theorem 4.41 that $\alpha(\Gamma_3) = q^5$, in contradiction to the assumption that $\omega(\Gamma_3)\alpha(\Gamma_3) = V(\Gamma_3)$. Therefore, the association scheme $\mathcal{AH}\Gamma_3(\mathbb{F}_{q^2})$ has no non-trivial graph with equality in the clique–co-clique bound, equation 3.1, which means it is separating, so synchronising by Theorem 4.7. $\square$

By Theorems 3.1, 3.2, we have:

Proposition 4.44. *The automorphism group G of the Hermitian graph $H\Gamma_2(\mathbb{F}_q)$ is synchronising.*

Proposition 4.45. *The automorphism group G of the Hermitian graph $H\Gamma_3(\mathbb{F}_q)$ is synchronising.*

4.9 Coset graphs of some Golay codes

Let Γ be a finite distance-regular graph, and let $\mathcal{P}$ be a partition of the vertex set of Γ into independent sets , $\mathcal{P} = \{P_1, ..., P_t\}$. Then the quotient graph can be defined as the graph $Q(\Gamma)$ with vertex set $\mathcal{P}$ and where two parts P_1, P_2 are adjacent if there are points $p_1 \in P_1$ and $p_2 \in P_2$ such that p_1 and p_2 are adjacent in Γ. If Γ is the Hamming graph $H(n, q)$ and C is a linear code, then the cosets of the code C provide a partition of the vertex set into independent sets, and the quotient graph of $H(n, q)$ is called the coset graph of C, which we denote by $Cos(C)$. In this section we will study the synchronisation property of the association schemes obtained from the coset graphs of some Golay codes.

4.9.1 The coset graph of the extended ternary Golay code

The graph $Cos(C)$ is distance transitive and has $3^6.2.M_{12}$ as its group of automorphisms. For more information, see [19, Theorem 11.3.1]. Now we will find a maximum clique and a maximum co-clique in $Cos(C)$.

Theorem 4.46. *[14, Theorem 3.2] The chromatic number of the graph $Cos(C)$, where $C = C_{24}$, is equal to* 3

Corollary 4.47. *Let C be the extended ternary Golay code, then the association scheme obtained from the graph $Cos(C)$ is non-synchronising.*

Proof. It is not difficult to show that 3 is a lower bound for the clique number of the graph $Cos(C)$. For example, for the representatives of the three cosets, consider the zero vector and the two vectors in which only the first coordinate is not zero. However, by Theorem 4.46, we have

$$3 \leq \omega(Cos(C)) \leq \chi(Cos(C)) = 3.$$

Therefore, there is a graph in the scheme such that the clique number is equal to the chromatic number, hence the association scheme is non-synchronising. □

By Theorems 3.1, 3.2, we have:

Theorem 4.48. *Let C be the extended ternary Golay code, then the automorphism group of the coset graph $Cos(C)$ is non-synchronising.*

4.9.2 The coset graph of the truncated binary Golay code

The truncated binary Golay code has length 22, dimension 12, and minimum distance 6. Its coset graph $Cos(C)$ is a distance-transitive graph with diameter 3. Its automorphism group is $2^{10}.M_{22}.2$ [19, Theorem 11.3.5].

Theorem 4.49. *The association scheme obtained from the coset graph $Cos(C)$ of the truncated binary Golay code is synchronising.*

Proof. The association scheme has three orbital graphs: Γ_1, Γ_2, and Γ_3, because the graph has diameter 3. There other graphs in the scheme are the complements of orbital graphs. If the scheme is non-synchronising (non-separating), then at lease for one of its graph the product of the clique number and the co-clique number is equal to the number of vertices.

The eigenvalues of Γ_1 are $(22, 6, -2, -10)$, [19, Theorem 11.3.5]. If the equality in the clique–co-clique bound (equation 3.1) is attained, then by Corollary 3.6, the smallest eigenvalue divides the degree of the graph. However, -10 does not divide 22, contradiction. Therefore, $\omega(\Gamma_1)\alpha(\Gamma_1) < |V(\Gamma_1)|$, so $\omega(\Gamma_1) \neq \chi(\Gamma_1)$.

In the second orbital graph, Γ_2, the degree is 231. If the clique number of the graph is equal to the chromatic number, then equality in the clique–co-clique bound is satisfied. This happens only if there exists a smallest eigenvalue (τ) such that $\omega(\Gamma) = 1 - \frac{\deg(v)}{\tau}$ is a positive integer greater than or equal to 1. All possible values are $\{\tau, \omega(\Gamma_2)\} \in \{\{-231, 2\}, \{-77, 4\}, \{-33, 8\}, \{-21, 12\}$, $\{-11, 22\}, \{-7, 34\}\{-3, 78\}, \{-1, 232\}\}$. Note that the only values of $\omega(\Gamma_2)$ that divide the number of vertices (1024) are 2, 4, and 8. However, it is not difficult to show that the clique number is at least 22. For example, consider cosets that are represented by vectors of weight 1. Therefore, $\omega(\Gamma_2) \neq \chi(\Gamma_2)$.

Finally, for the third orbital graph, Γ_3, the degree is 770. If we assume that the clique number is equal to the chromatic number, and consequently that equality of the clique–co-clique bound is attained, then there must be an integer τ such that $1 - \frac{\deg(\Gamma_3)}{\tau}$ is a positive integer greater than 1. Also, , $1 - \frac{\deg(\Gamma_3)}{\tau}$ must divide the number of vertices. The possible values of τ are -770, -110, and -77, and the possible clique numbers are 2, 8, and 11. However, the software GAP with the package GRAPE can be used to find a clique with size greater than 11. Thus equality in the clique–co-clique bound does not hold. Therefore, the third orbital graph does not have the clique number equal to the chromatic number, hence the association scheme is synchronising. $\square$

By Theorems 3.1, 3.2, we have:

Theorem 4.50. *The automorphism group of the coset graph $Cos(C)$ of the truncated binary Golay code is synchronising.*

4.9.3 The coset graph of the binary Golay code

The coset graph $Cos(C)$ of the binary Golay code $C = C_{23}$ is a distance-transitive graph with diameter 3. The automorphism group of this graph is $2^{11}.M_{23}$ [19]. The code has length 23, dimension 12, and minimum distance 7.

Theorem 4.51. *The association scheme obtained from the coset graph $Cos(C) = C_{23}$ of the binary Golay code is synchronising.*

Proof. Since the coset graph $Cos(C)$ has diameter 3, the association scheme which is obtained from $Cos(C)$ has three orbital graphs. The other graphs are the complements of the orbital graphs. If the scheme is non-synchronising (non-separating), then the product of the clique number and the co-clique number is equal to the number of vertices in at least one of the orbital graphs.

The eigenvalues of the graph $\Gamma_1 = Cos(C)$ are $(23, 7, -1, -9)$, [19, Theorem 3]. If we assume that there is equality in the clique–co-clique bound (equation 3.1), then by Corollary 3.6 the smallest eigenvalue must divide the degree of the graph. However, the smallest eigenvalues -9 does not divide the degree 23, contradiction. Therefore, $\omega(\Gamma_1)\alpha(\Gamma_1) < |V(\Gamma_1)|$, so $\omega(\Gamma_1) \neq \chi(\Gamma_1)$.

Second, Γ_2 has degree 253. Assume that τ is the smallest eigenvalue of Γ_2 . If $\omega(\Gamma_2) = \chi(\Gamma_2)$, equality holds in the clique–co-clique bound. Then τ must be a divisor of 253. The only possible values of τ are $-1, -11, -23$, and -253, so the size of the clique must be $1 - \frac{\deg(v)}{\tau}$; in particular, it must be one of the numbers $254, 24, 12$, and 2. However, the clique number is at least 22. Moreover, 254 and 24 do not divide the number of vertices (4096), in contradiction to the assumption. Thus $\omega(\Gamma_2) \neq \chi(\Gamma_2)$.

Finally, the graph Γ_3, has degree 1771. Assume that equality of the clique–co-clique bound holds. Then the smallest eigenvalue τ must be one of the numbers

$$-1, -7, -11, -23, -161, -253, -1771,$$

hence the possible clique numbers are

$$1772, 254, 162, 78, 24, 12, 8, 2.$$

The only ones that divide the number of vertices are 8 and 2. However, the clique number is greater than 8, which follows from the previous theorem.

Therefore, no graph in the association scheme satisfies equality in the clique–co-clique bound, so it is synchronising. $\square$

By Theorems 3.1, 3.2, we have:

Theorem 4.52. *The automorphism group of the coset graph $Cos(C) = C_{23}$ of the binary Golay code is synchronising.*

4.10 Conjecture

Let Γ be a primitive distance-transitive graph with diameter d. Let us say that Γ is ***exceptional*** if $\mathrm{Aut}(\Gamma)$ is non-separating but there is no t with $0 < t < d$ such that for the distance at most t graph in Γ the product of the clique number and the co-clique number equals the number of vertices.

Conjecture 10. *Given a positive integer d, there are only finitely many exceptional graphs of diameter d.*

This would extend Conjecture 2 about Johnson graphs.

4.11 Conclusion and future work

In this chapter, the synchronisation property of affine distance-transitive permutation groups was considered. The view of an association scheme was used. In most cases, it is possible to determine when these groups (association schemes) are synchronising. We gave a full classification of synchronising association schemes that are obtained from the halved n-cubes, for all n and the folded halved n-cubes, where n is even. Also, we show that the corresponding association schemes for the bilinear form graphs are non-synchronising. However, the case for alternating forms graphs $\mathrm{Alt}(n, q)$ is quite complicated, the association schemes are non-synchronising, when both n and q are even. The case that n is even and q is odd is undetermined. For the association schemes obtained from the Hermitian forms graphs and some alternating forms graphs, mainly when n is odd, a general result is desirable. Nevertheless, we show that they are synchronising for small n. For larger n, we expect these association schemes to be synchronising.

It is still not decided whether the association scheme obtained from the affine graph E_6 is synchronising or not. A full classification of synchronising association schemes from the coset graph of the binary Golay code was obtained in Section 9. We finished the chapter with a conjecture which extends the main conjecture in the previous chapter.

For future work, on one hand we will keep working on unsolved questions in this chapter. On the other hand we would like to investigate other affine permutation groups. A possible way to do this is by considering primitive permutation groups from Aschbacher's Theorem which is an analogue of O'Nan Scott Theorem for Linear groups. We already considered a class of these groups in Section 6.

Chapter 5

Diagonal permutation groups

This chapter discusses the synchronisation and separation properties of diagonal permutation groups. We know no of unified method that works for all diagonal groups. Thus, we divide diagonal groups into two classes. The first class contains diagonal groups with two factors in their socles. In this case, the problem is equivalent to the existence of a special factorisation of a finite simple group. The factors can be subgroups, subsets (not cosets) or one is a subgroup and the other is a subset (not a coset). This makes the study difficult because we do not know a lot of information if one of the factors is a subset. The second class contains diagonal groups with three or more factors in their socles. The authors of [16] have shown that such groups are non-synchronising. Also, we investigate the equivalence of separation and synchronisation properties.

This chapter includes five main sections. The first section introduces some basic notions and results on the factorisation of finite groups. Some of the results are known for abelian groups but not for non-abelian groups in general. The second and third sections investigate diagonal groups with two factors on their socles and some related problems. The fourth section is devoted to diagonal groups with at least three factors. The fifth section contains results regarding the equivalence between the synchronisation and separation properties.

5.0.1 Summary of the results

We introduced the notion of diagonal factorisation and started a study of the factorisation for finite non-abelian groups in Lemma 5.3, Proposition 5.4, lemma 5.5, Lemma 5.6 and Lemma 5.8 like the study of the factorisation for abelian groups. Also, we considered the properties of diagonal permutation groups $D(T, d)$ and investigated the relationship between these groups and the diagonal factorization od T. In particular, we showed that a diagonal group $D(T, 2)$ is non-separating if and only the group T admits diagonal factorisation, Theorem 5.16. In addition, we proved that $D(A_n, 2)$ is non-separating, Theorem 5.21 and $D(T, d)$ for $d \geq 3$, is non-synchronising in Theorem 5.30. We, also, studied the relationship between the group $D(A_n, 2)$ and inequivalent all-even Latin squares, Theorem 5.23. We ended this chapter by showing that the separating and synchronisation properties are equivalent for diagonal groups, Theorem 5.31.

5.1 Factorisation of finite groups

5.1.1 Basic definitions and results

A great deal of work has been done on the factorisation of the abelian finite groups into subsets. Two examples are the books [69] and [70]. In the factorisations of non-abelian groups some results are known. In particular, the factorisations are known when both factors are subgroups; see for instance, [54], [53]. However, little is known about the factorisation of finite non-abelian groups into subsets. This section contains definitions and basic results.

Let T be a finite group. We say that T admits a ***factorisation*** if there are two (non-trivial) subsets A and B of T such that $T = AB$ (a non-trivial subset means $|A| > 1$ and $AB = \{ab : a \in A \;\&\; b \in B\}$). An example of a factorisation is $A_6 = A_5 \cdot PSL(2,5)$, such a kind of factorisation is called a ***maximal factorisation into subgroups*** because each factor is a maximal subgroup of the group $T = A_6$.

A factorisation $T = AB$ is called ***exact*** if each $t \in T$ is expressed uniquely as the product ab where $a \in A$ and $b \in B$. An example of an exact factorisation is the representation of a group T as the product of a subgroup and the set of representatives of its right (left) cosets. Also, if both factors A and B are normal subgroups, then T is a direct product $A \times B$. In particular, this is true for abelian group, since all subgroups, are normal. In the literature, the notion of exact factorisation is used only for the exact factorisation of a finite non-abelian group into subgroups. When T is a finite abelian group written additively, an exact factorisation is called a ***direct factorisation***[70] (This is what we will consider from now on). A factorisation of a group $T = AB$ is called ***normalised*** if $A \cap B = \{e\}$.

The following result is for direct factorisation.

Lemma 5.1. *[70, Lemma 2.2]*
Let T be a finite abelian group and let A, B be non-trivial subsets of T. The following statements are all equivalent:

(a) $T = A + B$ *is a direct factorisation.*

(b) $T = A + B$ *and* $|T| = |A||B|$.

(c) $|T| = |A||B|$ *and* $|A \cap B| = 1$

(d) $|T| = |A||B|$ *and* $(A + (-A)) \cap (B + (-B)) = \{e\}$.

(e) $T = A + B$ *and* $(A + (-A)) \cap (B + (-B)) = \{e\}$.

(f) *The sets* $A + b, b \in B$ *form a partition of* T *and the sets* $a + B, a \in A$ *form a partition of* T.

Exact factorisations into subgroups and direct factorisations have similar features.

Proposition 5.2. *Let* $T = AB$ *be an exact factorisation into subgroups (direct factorisation). Then for distinct elements* $a_1, a_2 \in A$ *and distinct elements* $b_1, b_2 \in B$ *we have* $t^{-1}a_1^{-1}a_2t \neq b_1b_2^{-1}$, *for all* $t \in T$.

Proof. Let T be an abelian group and suppose that $T = AB$ is a direct factorisation. Assume for the contrary that for distinct $a_1, a_2 \in A$ and distinct $b_1, b_2 \in B$ we have $t^{-1}a_1^{-1}a_2t = b_1b_2^{-1}$, for some $t \in T$. Since T is abelian, we have $a_1a_2^{-1} = b_1b_2^{-1}$. Then by Lemma 5.1(d), we have $a_1 = a_2$ and $b_1 = b_2$, contradiction.

Let T be a non-abelian group and suppose that $T = AB$ is an exact factorisation into subgroups. Then, $|A \cap B| = 1$ and $|T| = |A||B|$. To show that for distinct elements $a_1, a_2 \in A$ and distinct elements $b_1, b_2 \in B$ we have $t^{-1}a_1^{-1}a_2t \neq b_1b_2^{-1}$, for all $t \in T$, it is enough to prove that $|t^{-1}A^{-1}At \cap BB^{-1}| = 1$ for all t (from this it will follow that $a_1 = a_2$ and $b_1 = b_2$). Assume for contradiction that $|t^{-1}A^{-1}At \cap BB^{-1}| > 1$, then for some $t \in T$, there are distinct $a_1, a_2 \in A$ and distinct $b_1b_2 \in B$ such that $t^{-1}a_1^{-1}a_2t = b_1b_2^{-1}$ if $a_1 = a_2$ then $b_1 = b_2$ and we are done. So, we assume that $a_1 \neq a_2$ then $h^{-1}atb$ are not all distinct for h and t range over T and $|h^{-1}atb| \leq |A||B|$. This is contradiction because $|A||B| = |T|$ and $|h^{-1}atb| = |T|$. The last follows because for all $h, t \in T$, we have $h^{-1}AtB = y^{-1}x^{-1}AxyB$ where $x \in A$ and $y \in B$. Then,

$$h^{-1}AtB = y^{-1}x^{-1}AxyB = y^{-1}AyB = y^{-1}ABy = T,$$

and $|h^{-1}AtB|=|T|$. $\square$

A generalisation of the exact factorisation into subgroups and the direct factorisation has to consider the property in the previous result. So, we say that a finite group T admits a ***diagonal factorisation into subsets*** $T = AB$ if there are non-trivial subsets A, B of T such that, for all $h, t \in T$, each element of T can be expressed uniquely as the product $h^{-1}atb$, where $a \in A$ and $b \in B$. By an argument similar to the one in the previous Lemma, we can prove that the diagonal factorisation implies that for distinct elements $a_1, a_2 \in A$ and distinct elements $b_1, b_2 \in B$ we have $t^{-1}a_1^{-1}a_2t \neq b_1b_2^{-1}$, for all $t \in T$.

The following result is a generalisation of Lemma 5.1 and some parts of it appear in [16] and in unpublished work by Sean Eberhard (2019, Personal communication, 24 July)

Lemma 5.3. *Let T be a finite group and let A, B be non-trivial subsets of T. The following statements are all equivalent:*

(a) T *admits a diagonal factorisation into* A *and* B.

(b) $|T|=|A||B|$ *and for all* $h, t \in T$, $(h^{-1}a_1t)b_1 = (h^{-1}a_2t)b_2$ *for* $a_1, a_2 \in A, b_1, b_2 \in B$ *implies* $a_1 = a_2, b_1 = b_2$.

(c) $|T|=|A||B|$ *and* $|t^{-1}At \cap B|=1$ *for all* $h, t \in T$.

(d) $T = A^{-1}B$ *is a diagonal factorisation.*

(e) $|T|=|A||B|$ *and* $t^{-1}(AA^{-1})t \cap BB^{-1} = \{e\}$ *for all* $t \in T$.

(f) $T = AB$ *and* $t^{-1}(AA^{-1})t \cap BB^{-1} = \{e\}$ *for all* $t \in T$.

Proof. To show that (a) implies (b) let $(h^{-1}a_1t)b_1 = (h^{-1}a_2t)b_2$ for $h, t \in T$ and $a_1, a_2 \in A$ and $b_1, b_2 \in B$. If $a_1 = a_2$ we are done and $b_1 = b_2$. Assume that $a_1 \neq a_2$, then the elements $h^{-1}atb$ for h and t range over T, are not all distinct and $|h^{-1}AtB| < |T|$. This contradicts the definition of the diagonal factorisation.

To show that (b) implies (c), we only need to show that $|t^{-1}At \cap B| = 1$ for some $t \in T$. Assume for the contrary that there are $g_1, g_2 \in t^{-1}At \cap B$. Then there are $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $g_1 = t^{-1}a_1t = b_1$ and $g_2 = t^{-1}a_2t = b_2$. From this we get

$$g_1g_2^{-1} = t^{-1}a_1a_2^{-1}t = b_1b_2^{-1},$$

so we have

$$t^{-1}a_1hh^{-1}a_2^{-1}t = b_1b_2^{-1}.$$

By (b) $a_1 = a_2$ and $b_1 = b_2$, Then $g_1 = g_2$ and $|h^{-1}At \cap B| = 1$.

We would like to show that $T = A^{-1}B$ is a diagonal factorisation. Assuming that (c) is true. It is clear that $|A||B| = |T|$. It remains to show that $T = h^{-1}A^{-1}tB$ for all h, t. Assume that $h^{-1}a_1^{-1}tb_1 = h^{-1}a_2^{-1}tb_2$. Thus,

$$b_1 = t^{-1}a_1\ (a_2^{-1}t)\ b_2 \in t^{-1}A\ (a_2^{-1}t) \cap B,$$

$$b_2 = t^{-1}a_2a_1^{-1}tb_1 = t^{-1}a_2\ (a_2^{-1}t)\ b_2 \in t^{-1}A(a_2^{-1}t) \cap B$$

and by (b) we have $a_1 = a_2$ and $b_1 = b_2$. Therefore, $T = A^{-1}B$ is diagonal.

Now, we prove that (d) implies (e). Since each element of $T = A^{-1}B$ is expressed uniquely as the product of an element from A^{-1} and an element from B, we have $= |A^{-1}||B|= |A||B|= |AB|$. Assume that $g \in t^{-1}AA^{-1}t \cap BB^{-1}$. We need to show that $g = e$. Since $g \in t^{-1}AA^{-1}t$, there are $a_1, a_2 \in A$ such that $g = t^{-1}a_1a_2^{-1}t$. Also, since $g \in BB^{-1}$, there are $b_1, b_2 \in B$ such that $g = b_1b_2^{-1}$. Thus $t^{-1}a_1hh^{-1}a_2^{-1}t = b_1b_2^{-1}$ for all $h \in T$. Thus,

$$h^{-1}a_2^{-1}tb_2 = h^{-1}a_1^{-1}tb_1.$$

But in this case, with the fact that $T = A^{-1}B$ is diagonal and by a similar argument to (b) we can show that $a_1^{-1} = a_2^{-1}$ and $b_1 = b_2$. Therefore, $g = e$.

To show that (e) implies (f), we need to prove that $T = AB$. Assume that there are $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $a_1b_1 = a_2b_2$. Then $a_1^{-1}a_2 = b_1b_2^{-1}$. By the fact that $a_2a_1^{-1}$ is conjugate to $a_1^{-1}a_2$, and (e) we have $a_1 = a_2$ and $b_1 = b_2$. Therefore, $T = AB$.

It remains to prove that (f) implies (a). Assume that $T = AB$ but the elements in $T = h^{-1}AtB$, for some $h, t \in T$, not all distinct. Therefore, there are distinct elements $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $h^{-1}a_1t\, b_1 = h^{-1}a_2t\, b_2$. So $t^{-1}a_1^{-1}a_2t = b_1b_2^{-1}$ by (f) we have $a_1 = a_2$ and $b_1 = b_2$, contradiction. Thus, $T = AB$ is diagonal. $\square$

Proposition 5.4. *Let $T = AB$ be a diagonal factorisation of T. Then the set $\{h^{-1}At\, b : b \in B\}$ forms a partition of T, for all $h, t \in T$.*

Proof. Assume that $T = AB$ is a diagonal factorisation of T, then $T = h^{-1}AtB$ for all $h, t \in T$. If there are two subset $h^{-1}At\, b_1$ and $h^{-1}At\, b_2$ such that b_1, b_2 are distinct elements in B and $|h^{-1}At\, b_1 \cap h^{-1}At\, b_2|\geq 1$, then for some $a_1, a_2 \in A$ we have $h^{-1}a_1tb_1 = h^{-1}a_2tb_2$. Thus, by the previous theorem $a_1 = a_2$ and $b_1 = b_2$ $\square$

In the following result we consider the construction of new factorisations from old ones.

Lemma 5.5. *Let $T = AB$ be a normalised diagonal factorisation of a finite group T, and let H be a subgroup of T such that $A \subset H$. Then*

$$H = AB \cap H = A(B \cap H).$$

is a normalised diagonal factorisation of H.

Proof. $T = AB$ is a diagonal factorisation if and only if for all distinct elements $a_1, a_2 \in A$ and distinct elements $b_1, b_2 \in B$ and all $t \in T$ we have $t^{-1}a_1a_2^{-1}t \neq b_1b_2^{-1}$.

First we show that $H = A(B \cap H)$. Let $h \in H \leq T$. Then $h = ab$ where $a \in A$ and $b \in B$. Since A is a subset of H we have $a \in H$ and thus $b \in H$. Therefore, $b \in (B \cap H)$. As a result, $h = ab \in A(B \cap H)$ and $H \subset A(B \cap H.)$ For the other direction assume that $t = ab \in A(B \cap H)$ where $a \in A$ and $b \in (B \cap H)$. So, $b \in B$ and $b \in H$. Since $A \subset H$, we have $a \in H$. Consequently, $t = ab \in H$ and $A(B \cap H) \subset H$ and $T = AB$ is diagonal, we have the factorisation, $H = A(B \cap H)$.

Finally, we show that this factorisation is diagonal. Let $h \in H$ and since $A \subset H$ it follows that $H = AB \cap H$, let a_1, a_2 be distinct elements from A and c_1, c_2 be distinct elements from $(B \cap H)$. Since $h \in T$ and $c_1, c_2 \in B$ we have $h^{-1}a_1a_2^{-1}h \neq c_1c_2^{-1}$.

□

This result will be referred to as the restriction of the factorisation $T = AB$ to the subgroup H of T. The identity $AB \cap H = A(B \cap H)$ is known as Dedekind's identity in the case of an exact factorisation. Also, it is true for abelian groups [70, Lemma 2.3]. A subset A of a finite group T will be called ***full-rank*** if $\langle A \rangle = T$ and a factorisation $T = AB$ is ***full-rank factorisation*** if both A and B are full-rank sets. The following result holds for direct products [70, Lemma 2.4].

Lemma 5.6. *Let $T = AB$ be a normalised diagonal factorisation of the finite group T. Assume that $K = \langle A \rangle \neq T$, that is the factorisation is not full-rank. Then, we can find subsets C_i, $1 \leq i \leq s$ of T and elements b_i, $1 \leq i \leq s$ in B such that the sets $C_i b_i$ for all $1 \leq i \leq s$ form a partition of B and $k = AC_i bi$ for all i are normalised factorisations of K.*

Proof. Let $T = AB$ be a normalised diagonal factorisation with $K = \langle A \rangle$ a proper subgroup of T. The union of the cosets Kt where $t \in T$ gives T. Let $t \in T$. We can write $t = ab$ for some $a \in A$ and $b \in B$, so $Kt = Kab = Kb$. The union of the cosets Kb form T as b range over B. Then, there are $b_1, b_2, ..., b_s$ in B such that the cosets $Kb_1, ..., Kb_s$ form a partition of T. Multiply both sides of $T = AB$ by b^{-1} gives the normal factorisation $T = ABb_i^{-1}$. Restricting this factorisation to K we have the factorisation $K = A(Bb_i^{-1} \cap K)$. Setting $C_i = Bb_i^{-1} \cap H$ we can see that $K = AC_i$ is a normal factorisation of T. Note that, $C_i b_i = B \cap Hb_i$ and so the sets

$$C_1 b_1, ..., C_s b_s$$

form a partition of B. $\square$

The result which is about to be stated, is correct for direct factorisations but it is not true even for exact factorisations.

Lemma 5.7. *[70, Lemma 2.5]*
Let H be a subgroup of a finite abelian group T and let $T = D + H$ be a normalised factorisation of T, where $D = \{b_1, ..., b_s\}$ with $b_1 = 0$. Suppose that

$$H = A + C_1,\ ...,\ H = A + C_s$$

are normalised factorisations of H. Set

$$B = (b_1 + C_1) \cup ... \cup (b_s + C_s).$$

Then $T = A + B$ is a normalised factorisations of T.

As we mentioned before this result is not correct for finite non-abelian groups in general. For example, $A_5 = A_4 \cdot C_5$ is a normalised exact factorisation and A_4 admits a normalised exact factorisation into the Klein four-group and a cyclic group C_3. But A_5 does not admit an exact factorisation with the Klein four-group or a cyclic group C_3 as factors.

A subset A of a finite group T is called ***right periodic*** (***left periodic***) if there is a $t \in T$ such that $t \neq e$ and $At = A$ ($tA = A$). The element t will be called a ***right*** (***left***) ***period*** of A. A subgroup of a group is right and left periodic set which equals its set of periods. Another example is the subset

$$A = \{(), (1,4,5)(2,6,3), (1,3,4,2)(5,6), (1,2,4,6)(3,5), (1,6,4,3)(2,5), (1,5,4)(2,3,6)\}$$

of the alternating group A_6. It is right periodic for

$$\{(), (1,4,5)(2,6,3), (1,5,4)(2,3,6)\}$$

being the set of right periods of A. It is not left periodic.

Lemma 5.8 (Lemma 2.8)**.** *[70] Let A be a non-empty subset of a finite group T. Let L be the periods of A.*

(a) If $t \in L$, then $At = A$.

(b) If $At = A$ for some $t \in T$, then $t \in L$.

(c) L is a subgroup of T.

The previous result is true for finite abelian groups and appear as a theorem in [70].

Let T be a finite group which admits an exact (diagonal) factorisation $T = AB$, we say that a factor A is ***replaceable*** by a subset C of T if $T = CB$ is an exact (diagonal) factorisation. It can be useful to know if a factor A in the factorisation can be replaced by a periodic set, subgroup or the inverse set A^{-1}.

5.2 Diagonal groups with two factors $D(T,2)$

Let T be a finite group, we can define an action of T on itself by right multiplication, that is $\mu_1(x,t) = xt$ for all x and t in T. This is known as the right regular representation. The left regular representation is given by the action $\mu_2(x,t) = t^{-1}x$ for x and t in T. Combining these two actions we obtain an action of the group $T \times T$ on T such that for all x, h, g in T we have the diagonal action:

$$\mu(x,(h,g)) = h^{-1}xg.$$

It is obvious this is an action as $\mu(x,(e,e)) = x$, where e is the identity element in T. Also, $\mu(\mu(x,(h_1,g_1)),(h_2,g_2)) = \mu(h_1^{-1}xg_1,(h_2,g_2))) = h_2^{-1}h_1^{-1}xg_1g_2 = (h_1h_2)^{-1}xg_1g_2 = \mu(x,(h_1h_2,g_1g_2))$. Moreover, for any x, y in T we can find $(h,g) = (x,y)$ in $G \times G$ such that $\mu(x,(h,g)) = x^{-1}xy = y$ which means that the action is transitive. The stabilizer of e is

$$\{(h,g) \in T \times T \ : \ h^{-1}eg = e\} = \{(h,h) \in T \times T\},$$

the diagonal subgroup. This action is faithful if and only if T has a trivial centre. The group induced by this action is called a diagonal group and denoted by $D(T, 2)$.

5.2.1 Conjugacy classes association scheme

The purpose of this section is to study the separation and synchronisation properties of $G = D(T, 2)$. Thus, we need to examine the non-trivial G-invariant graphs Γ with $G \leq Aut(\Gamma)$. Each such graph is a union of some orbital graphs of $D(T, 2)$.

A ***Cayley*** digraph, denoted by $\mathrm{Cay}(T, S)$ consists of a group T and a subset S of T, called the connection set. It has vertex set T and there is directed edge (arc) from t_1 to t_2 if $t_1t_2^{-1} \in S$. If S is closed under inverses and $t_1t_2^{-1} \in S$, then there are arcs in both ways i.e; $t_1t_2^{-1} \in S$ and $t_2t_1^{-1} \in S$. In this case, we replace the two arcs by an undirected edge and $\mathrm{Cay}(T, S)$ is an undirected graph. Furthermore, if the identity of T does not belong to S then $\mathrm{Cay}(T, S)$ is loopless. Therefore, if S is closed under inverses and does not contain the identity of T, $\mathrm{Cay}(T, S)$ is a simple graph. A Cayley digraph is called ***normal*** if its connection set is closed under conjugation. This implies that the connection set is a union of conjugacy classes. So, T acts regularly on the vertices of $\mathrm{Cay}(T, S)$ by left and right multiplication.

Remark 5.9. *The notion normal Cayley digraph is used sometimes to mean a graph of a group T such that T is normal subgroup of the automorphism group of the graph.*

The following results shows that the G-invariant graphs where $G = D(T, 2)$, are Cayley graphs.

Proposition 5.10. *Let T be a finite group and let $G = D(T, 2)$ be the group induced by the diagonal action of $T \times T$ on T. Then the G-invariant graphs are Cayley graphs.*

Proof. Assume that T is a finite group and G is the group induced by the action of $T \times T$ on T. If (x_1, y_1) and (x_2, y_2) are in $T \times T$, then they are in the same orbital relation if and only if there is (h, g) in $T \times T$ such that:

$$\Leftrightarrow h^{-1}(x_1, y_1)g = (x_2, y_2)$$

$$\Leftrightarrow (h^{-1}x_1g, h^{-1}y_1g) = (x_2, y_2)$$

$$\Leftrightarrow h^{-1}x_1y_1^{-1}h = x_2y_2^{-1}.$$

Therefore, (x_1, y_1) and (x_2, y_2) are in the same orbital relation if $x_1y_1^{-1}$ and $x_2y_2^{-1}$ are in the same conjugacy class. An orbital graph obtained from an orbital relation is a Cayley graph $Cay(T, S)$, where S is a conjugacy class. A G-invariant graph is a union of some orbital graphs. $\square$

Theorem 5.11. *Let T be a finite group. Then the orbital relations that are obtained from the group $G = D(T, 2)$ form an association scheme. Moreover, a Cayley graph $Cay(T, S)$, where S is a conjugacy class is a graph in the scheme.*

Proof. We have some claims to prove:

(a) There is a diagonal orbital relation $O_0 = \{(x, x) : x \in T\}$. This exists by the transitivity of G.

(b) The set of orbital relations is a partition of $T \times T$. This is ensured by the definition of orbits.

(c) If O is an orbital relation, then O^t is an orbital relation as well. This is for the same reason as the previous one.

(d) For each $i, j, k \in \{0, 1, ..., d\}$, and $(x, y) \in O_k$ the constant $|\{z \in T : (x, z) \in O_i, (z, y) \in O_j\}|= p_{ij}^k$ only depends on $i, j,\ k$. Assume $(x, y) \in O_k$ and

$t \in \{z \in T : (x,z) \in O_i, (z,y) \in O_j\}$. Then $tg \in \{z \in T : (xg,z) \in O_i, (z,yg) \in O_j\}$. Since $(x,y) \in O_k$, we have $(xg,yg) \in O_k$.

$$|\{z \in T : (xg,z) \in O_i, (z,yg) \in O_j\}| = |\{z \in T : (x,z) \in O_i, (z,y) \in O_j\}| = p_{ij}^k$$

So, p_{ij}^k depends only on i, j, k.

(e) If O_i and O_j are orbital relations represented by A_i and A_j respectively, then $A_iA_j = A_jA_i$.

Last statement follows from the previous result. □

This association scheme is called ***conjugacy classes association scheme*** and we will denote it by $\mathcal{AG}$(T) .

Theorem 5.12. *Let T be a finite group and let $G = D(T,2)$ be the group induced by the diagonal action of $T \times T$ on T. Then G is primitive if and only if T is a simple group.*

Proof. Let $\mathcal{AG}(T)$ be the conjugacy classes association scheme. It is clear that G is primitive if and only if $\mathcal{AG}(T)$ is primitive. The latter is primitive if and only if all digraphs in the scheme are connected, i.e., there is a directed path between any two vertices.

First, assume that T is not simple, then it contains a normal subgroup N. However, N is a union of conjugacy classes then $\mathrm{Cay}(T,N)$ is an orbital graph and it is disconnected since the connection set does not generate T. Therefore, $\mathcal{AG}$ is imprimitive.

Second, let $\mathcal{AG}(T)$ be imprimitive conjugacy classes association scheme. Then, there is a disconnected digraph $\mathrm{Cay}(T, S)$ in the scheme which means that $\langle S \rangle \neq T$. Thus, we have a graph $\Gamma = \mathrm{Cay}(T, \langle S \rangle \setminus \{e\})$ which is not connected and $G \leq \mathrm{Aut}(\Gamma)$, and $\langle S \rangle$ is closed under conjugation. Therefore, $\langle S \rangle$ is normal subgroup of T. $\square$

The most interesting situation happens when T is a non-abelian simple group because when T is not simple the group $G = D(T, 2)$ is non-separating and non-synchronising. For the reset of this chapter we assume that T is finite simple group. The following subsection discusses the relationship between the separation property of $D(T, 2)$ and diagonal factorisation of T.

5.2.2 The factorisation of finite groups and the separation property

The aim of this subsection is to show that for a finite non-abelian simple group T, the diagonal group $D(T, 2)$ is non-separating if and only if T admits a diagonal factorisation.

Lemma 5.13. *Let T be a finite non-abelian simple group which admits a diagonal factorisation $T = AB$ into two subsets $A, B \subset T$. Then we can define a normal Cayley graph $Cay(T, S)$, where S is a union of conjugacy classes C such that $C \cap \{a_1 a_2 : a_1, a_2^{-1} \in A, a_1 \neq a_2\} \neq \emptyset$. The two factors A and B are maximum clique and maximum Co-clique of $Cay(T, S)$, respectively.*

Proof. Assume that T is a finite non-abelian simple group admits a diagonal factorisation $T = AB$. We can define a graph Γ to have T as its vertex set and two vertices $t_1, t_2 \in T$ are adjacent if $t_1 t_2^{-1} \in S$, where S is the union of conjugacy classes C such that $C \cap \{a_1 a_2 : a_1, a_2^{-1} \in A, a_1 \neq a_2\} \neq \emptyset$. It is clear, Γ

is Cayley graph $Cay(T, S)$. It is normal because S is closed under conjugation. By the diagonal factorisation of T and the fact that $a_1a_2^{-1}$ and $a_1^{-1}a_2$ are conjugate for all $a_1, a_2 \in A$, the factor A is a clique in the graph. Also, for distinct elements $a_1, a_2 \in A$ and distinct elements $b_1, b_1 \in B$ we have that $a_1a_2^{-1}$ is not conjugate to $b_1b_2^{-1}$, so B is co-clique. Since $|A||B|= |T|$, the clique and co-clique are maximum. □

The following theorem follows from Theorem 5.11 and Lemma 5.13.

Theorem 5.14. *Let T be a finite non-abelian simple group which admits a diagonal factorisation $T = AB$ into two subsets $A, B \subset T$. Then the diagonal group $G = D(T, 2)$ is non-separating.*

Also, if $G = D(T, 2)$ is non-separating then there is a diagonal factorisation of T into subsets.

Theorem 5.15. *Let T be a finite non-abelian simple group. If the diagonal group $G = D(T, 2)$ is non-separating, then T admits a diagonal factorisation into two subsets $A, B \subset T$.*

Proof. Assume that $G = D(T, 2)$ is non-separating, then, by Theorem 2.24, there is a non-trivial G-graph Γ such that $\Gamma = \mathrm{Cay}(T, S)$ by Proposition 5.10, in the association scheme $\mathcal{AG}(\mathrm{T})$ such that $\alpha(\Gamma) \cdot \omega(\Gamma) = |T|$. Suppose that A and B represent the vertex sets of a maximum clique and a maximum co-clique, respectively. The connection set S is a union of conjugacy classes, so for all distinct a_1, a_2 in A and for all distinct b_1, b_2 in B, we have $a_1^{-1}a_2$ is not conjugate to $b_1b_2^{-1}$. The intersection of A and B contains exactly one point by Theorem 2.28. We can assume this point is the identity element of T. If not, $A \cap B = \{t \neq e\}$, we choose the vertex set of maximum clique to be At^{-1} and the vertex set of maximum co-clique to be Bt^{-1}. This can be done because the right multiplication by an element of T is an automorphism of Γ. $\square$

Now, there are three possibilities for the subsets A and B:

- if there is an exact factorisation of T into two subgroups A and B, then we have an exact factorisation into subgroups.

- if one of the factors is a subgroup, say A, while the other is a subset that is not a coset, say B. Then B is called a sharply transitive set.

  Let Ω be a set and H be a set of permutations on Ω, then H is called a ***sharply transitive set*** if for x and y in Ω, there is exactly one $h \in H$ such that $xh = y$. If Ω is finite then the number of elements in Ω equals the number of elements in H.

- if both of the subsets A and B are not cosets of subgroups. Little is known about the factorisation of groups into subsets. However, there are some examples of factorisation of finite groups into subsets. For abelian groups, consider the cyclic group generated by the element t of order 8 that is $T = \{e, t, t^2, t^3, t^4, t^5, t^6, t^7, t^8\}$. It can be expressed uniquely as a product of two subsets $A = \{e, t^2\}$ and $B = \{e, t, t^4, t^5\}$. For the non-abelian case, consider the group $T = \mathrm{Sym}(3) \times \langle(1, 2, 3)\rangle$. It can be factorised into the two subsets [15],

  $$A = \{(), (1, 2, 3), (1, 3, 2), (2, 3)(4, 5, 6), (1, 3)(4, 5, 6), (1, 2)(4, 5, 6)\}$$

  and

  $$B = \{(), (1, 3, 2)(4, 5, 6), (1, 3, 2)(4, 6, 5)\}.$$

The former generates T while the latter generates the subgroup

$$\langle B \rangle = \{(), (4,5,6), (4,6,5), (1,2,3), (1,2,3)(4,5,6), (1,2,3)(4,6,5),$$
$$(1,3,2), (1,3,2)(4,5,6), (1,3,2)(4,6,5)\}.$$

I do not know any such factorisation for finite simple groups!!

The main result in this subsection is:

Theorem 5.16. *Let T be a finite non-abelian simple group. The diagonal group $G = D(T,2)$ is non-separating if and only if T admits a diagonal factorisation into two subsets $A, B \subset T$.*

Proof. This can be seen from Theorem 5.14 and Theorem 5.15. $\square$

5.2.3 The diagonal groups $D(T,2)$ where $T = A_n$, and $n \geq 5$

All simple groups admitting exact factorisations into subgroups are known and appear in [53]. Not all finite simple groups admit exact factorisations into subgroups, for instance, in [80] it is shown that A_6 cannot be factorised into subgroups.

The alternating group A_n where $n \geq 5$, is the first candidate for T in the diagonal groups $D(T,2)$. The group A_n, for instance, can be factorised into two subgroups A_{n-1}, and C_n when n is odd. However, $T = A_6$, admits such no factorisation because $C6$ is not a subgroup in A_6. Nevertheless, it contains a sharply transitive set

$$B = \{e, (1,2,3,5)(4,6), (1,6,5,3)(2,4), (1,4)(2,5,6,3), (1,5,2,6)(3,4), (1,3,6,2)(4,5)\}$$

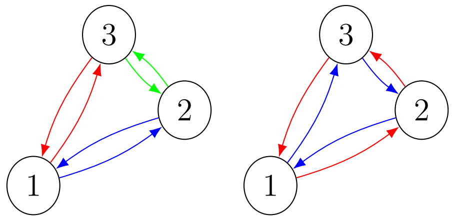

Figure 5.1: The decomposition of the complete digraph with three vertices into three directed cycles of length 2 and into two directed cycles of length 3.

which is system of coset representatives for A_5 in A_6. This provides a factorisation of A_6 into subgroup A_5 and B. This suggests a way of looking at the problem through the decomposition of complete directed graphs.

A **decomposition of a (di)graph** $\Gamma = (V(\Gamma), E(\Gamma))$ is a partition of the edge-set $E(\Gamma)$ into the edge-sets of the spanning sub-digraphs $K_1, \ldots, K_l$. If each of them is isomorphic to a particular subgraph (subdigraph) K, then Γ admits an ***K-decomposition***.

Let $\Omega = \{1...n\}$ and $T \leq Sym(\Omega)$, we say that t_1 and t_2 in T are ***intersecting*** if $it_1 = it_2$ for some $i \in \Omega$, and ***non-intersecting*** otherwise. If T is the alternating group A_n, then the subset of all pairwise non-intersecting permutations, is called the set of ***even derangements*** of size n. We will denote it by $ED(n)$. The ***even derangement graph*** Γ_n is a Cayley graph $\mathrm{Cay}(A_n, ED(n))$ which has A_n as its vertex set and $ED(n)$ its connection set. $ED(n)$ is a union of conjugacy classes in A_n, so Γ_n is a normal Cayley graph. Therefore, it is a graph in the conjugacy classes association scheme $\mathcal{AG}(A_n)$. It is not difficult to see that A_{n-1} is a co-clique in Γ_n with size $\frac{(n-1)!}{2}$. Thus, by the clique–co-clique bound, inequality 3.1, the maximum clique in Γ_n is bounded above by n.

The following result gives the necessary and sufficient conditions for the existence of a decomposition of a complete digraph K_n on n vertices into directed cycles of length m.

Theorem 5.17. *[2, Theorem 1.1] For positive integers m and n with $2 \leq m \leq n$ the digraph K_n can be decomposed into directed cycles of length m if and only if m divides the number of arcs in K_n and $(n,m) \neq (4,4)$, $(6,3)$, $(6,6)$.*

We illustrate what we mean by permutation of the shape $(2)(n-2)$, in the following result, by an example. For $n = 6$, an example of permutation of the shape $(2)(n-2)$ would be $(1,2)(3,4,5,6)$. Also, this permutation represents a set of two directed cycles in the complete digraph K_6.

Corollary 5.18. *There exists a decomposition of the complete directed graph K_n into $n-1$ cycles that are represented by permutations of shape $(2)(n-2)$.*

Proof. Assume that K_n is a complete digraph on the vertices $\{v_1, ..., v_n\}$. Consider the induced subgraph K_{n-1} on the vertices $\{v_2, .., v_n\}$. It is complete digraph as well. By the previous theorem, it can be decomposed into $n-1$ cycles of length $n-1$. Each cycle can be represented by a permutation of shape $(n-2)$. The permutations can be indexed such that C_i misses a vertex v_i from $\{v_2, .., v_n\}$. The remaining arcs in K_n can be decompose into $n-1$ transpositions $(v_1v_2), (v_1v_3), ..., (v_1v_n)$. Now, by joining each permutation C_i with (v_1v_i) we reach the desired conclusion. □

Lemma 5.19. *If n is odd, then there exists a clique of size n in the derangement graph Γ_n, which consists of $n-1$ permutations of shape (n) and the identity permutation.*

Proof. For n odd, showing that Γ_n has clique number $\omega(\Gamma_n) = n$ is the same as proving the existence of a non-intersecting set S contains $n-1$ permutations of shape (n) and identity. By the previous theorem, a complete directed graph K_n can be decomposed into $n-1$ cycles of length n. Each cycle represents a permutation. Let S be the set that consists of the permutations of these cycles together with the identity permutation. It is a clique in Γ with size n. □

Lemma 5.20. *If n is even, then there exists a clique in the derangement graph Γ which consists of $n-1$ permutations of shape $(2)(n-2)$ and the identity permutation.*

Proof. The permutations of shape $(2)(n-2)$ are even derangements. Let the clique S be the set of the $n-1$ even derangements that represent the cycles in Corollary 5.18 beside the identity permutation. It contains n elements and this proves the lemma. □

Theorem 5.21. *Let $n \geq 5$ and let T be the alternating group A_n. Then the diagonal group $G = D(A_n, 2)$ is non-separating.*

Proof. The even derangement graph Γ_n is a non-trivial G-invariant graph such that $\alpha(\Gamma_n) \cdot \omega(\Gamma_n) = |A_n|$. Therefore, by theorem 2.24, the group G is non-separating. □

For the case $T = PSL(2, q)$, Ito [45] proves that following

Theorem 5.22. *Let T be the projective special linear group $PSL(2, q)$. Then T admits a factorisation into two subgroups except $q \equiv 1 \mod 4$ and $q \neq 5, 9, 29$.*

For the case $PSL(2, 13)$, Sean Eberhard shows that it is separating and consequently synchronising (2019, Personal communication by email, 24 July). Also, in

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	1	2	3	5
5	1	2	3	4

Table 5.1: Example of Latin square of size 5.

1	2	3	4	5	6	$e = ()$
2	3	5	6	1	4	(1,2,3,5)(4,6)
6	4	1	2	3	5	(1,6,5,3)(2,4)
4	5	2	1	6	3	(1,4)(2,5,6,3)
5	6	4	3	2	1	(1,5,2,6)(3,4)
3	1	6	5	4	2	(1,3,6,2)(4,5)

Table 5.2: Example of all-even Latin square of size 6.

a recent paper [11] Bamberg, Giudici, Lansdown, and Royle have shown that the diagonal groups $T \times T$ where $T = PSL(2, 13)$ or $PSL(2, 17)$ are synchronising.

A ***Latin square*** L of size n is an $n \times n$ array in which each cell contains a single element from an n-set S, such that each element occurs exactly once in each row and exactly once in each column. The following Table is a Latin square of size 5. A Latin square L_n is called ***all-even Latin square*** if each row can be represent by an even permutation. The following is an example of all-even Latin square.

Remark : Let T be a finite group that admits a diagonal factorisation $T = AB$. If a factor is a subgroup, say A, then the other factor B can be considered as a set of permutations which is given by the rows of Latin square.

5.2.4 Related problems

The work in the previous section suggests the following question:

Let G be a primitive permutation group. Can we put any upper bound on the number of non-synchronising monoids containing G ?

Let T be a non-abelian simple group, and $G = T \times T$ acting on T by left and right multiplication. Suppose that A is a subgroup of T, and B a subset, providing a diagonal factorisation of T. Then the cosets of A form a partition of T such that Bg is a transversal (section) for all $g \in G$, and hence G is non-synchronizing.

Now take the case where T is an alternating group A_n, and A is the alternating group A_{n-1}. Then the elements of B are the rows of an all-even Latin square. Conversely any all-even Latin square gives a witness to non-synchronisation. If s denotes the map taking every element of T to the element of B in the same coset of A_{n-1}, then $\langle G, s\rangle$ is non-synchronising.

We showed the existence of all-even Latin squares in above section. The total number of Latin squares is very large, at least $(n/2e)^{n^2}$. If even an exponentially small proportion of them were all-even, then we would have many examples.
Here we study the two specific questions:

(a) Is it true that the proportion of Latin squares which are all-even is at least c^n of the total, for some $c > 0$?

(b) How many inequivalent Latin squares can give rise to the same non-synchronising monoid?

n	RL	AEL	The proportion	F
3	1	1	0.5	0.125
4	4	1	0.125	0.0625
5	56	3	0.0535714286	0.03125
6	9,408	312	0.0165816327	0.015625
7	16,942,080	254640	0.0075150159	0.0078125
8	535,281,401,856	4,266,190,848	0.0039849989	0.00390625
9	377,597,570,964,258,816	1,478,219,603,116,032	0.0019574008	0.001953125

Table 5.3: The proportion of all-even-Latin squares for $3 \leq n \leq 9$.

5.2.4.1 The proportion of all-even Latin squares

A Latin square L_n of of size n is ***reduced*** or in ***standard form*** if in the first row and column the elements occur in natural order. One should note that we have the number of all Latin squares of size n with n less than oe equal 11 and we have no confirmed number after that. I calculate the exact number of all-even Latin square for $3 \leq n \leq 7$. Ian Wanless provides the exact number for $n = 8, 9$ (2019, Personal communication, 30 January). As we can see in the following table this number lives in an interval around $\frac{1}{2}^n$ and it is getting closer to it when n increases. To understand the table we let:

- RL: be the number of all reduced Latin squares;
- AFL: be the number of all-even Latin squares;
- the proportion is given by $\frac{AFL}{2 \times L}$;
- F: be the fraction $\frac{1}{2}^n$.

R.Haggkvist and J. C.M. Janssen [38] show that the proportion of all $k \times n$ Latin rectangles with $k \leq n - 7$ is asymptotically equal to 2^{-k}. They use the lower

1	2	3	4		1	2	3	4
2	3	4	1		2	1	4	3
3	4	1	2		3	4	1	2
4	1	2	3		4	3	2	1

Table 5.4: Example of inequivalent Latin squares of size 4.

bound on the permanent of a doubly stochastic matrix and upper bound of the determinant of a Hadamard matrix. To use the same methods for proving the same result for Latin squares, one needs to improve the two bounds, which is a difficult problem!

5.2.4.2 Equivalent Latin squares and monoids

Two Latin squares L_1 and L_2 of size n are ***isotopic or equivalent*** if there are three bjiections from the rows, columns, and symbols of L_1 to the rows, columns, and symbols, respectively, of L_2, that map L_1 to L_2. In other words, we can obtain L_2 from L_1 by permuting the rows, columns, or symbols. The two tables above show an example of two inequivalent Latin squares of size 4. Let $G = D(T, 2)$ be the group induced by the diagonal action of $T \times T$ on T. The question is how many inequivalent Latin squares can give rise to the same non-synchronising monoid?

We consider the case where T is an alternating group A_n. Any all-even Latin square of size n gives a witness to non-synchronisation; that is, the set of cosets of A_{n-1} forms a partition of T and the set B which consists of the rows of all-even Latin square, is a section. If s denotes the map taking every element of T to the element of B in the same coset of A_{n-1}, then $\langle G, s\rangle$ is non-synchronising.

Theorem 5.23. *Let $G = D(A_n, 2)$ be a diagonal group, where $n \geq 5$ and let L_1 and L_2 be inequivalent Latin squares of size n. If s_1 and s_2 denote the maps taking* *every element of A_n to the elements of the sets of rows of L_1 and L_2, respectively, in the same coset of A_{n-1}. Then the non-synchronising monoids $\langle G, s_1 \rangle$ and $\langle G, s_2 \rangle$ are not the same.*

Proof. The group $T = A_n$ admits a factorisation $A_{n-1}B$ with one factor is the alternating group A_{n-1} and the other factor is a subset B. Also, the the set of cosets, $A_{n-1}b_i$, $b_i \in B, 1 \leq i \leq n$ is a section regular partition of A_n, that is, for all S such that $|S \cap Ab_i|= 1$ implies $|Sg \cap Ab_i|= 1$. Let B_1 and B_2 be two subsets of A_n which are sections of the partition of A_n into cosets of A_{n-1}, so $A_n = AB_1$ and $A_n = AB_2$.

Let s_1 and s_2 be the transformations that send every element of A_n to the elements of the sets B_1 and B_2, respectively, in the same coset of A_{n-1}. The sets B_1 and B_2 are sharply transitive subsets of A_n, so they can be represented by all-even Latin squares of size n namely L_1 and L_2, respectively.

The monoid $\langle G, s_1 \rangle$ consists of all possible compositions of s_1 and all $g \in G$. There are two ways to compose g and s_1 either gs_1 or s_1g. Let $\mathrm{Im}(gs_1) = B_1$ and $\mathrm{Im}(s_1g) = B^*$. Therefore, $A_n = AB^*$ and the permutations in B^* are rows in a Latin square L^*. Note that L_1 and L^* are equivalent because $G = T \times T$ acts by left and right multiplication on B_1 the left action corresponds to the column permutations on L_1 and right action corresponds to symbol permutation on L_2.

Let L_1 and L_2 be inequivalent all-even Latin squares which are in correspondence with the factorisations $A_n = AB_1$ and $A_n = AB_2$. If s_1 and s_2 are the two related transformations as explained above, then it is impossible to have $s_2 \in \langle G, s_1 \rangle$. $\square$

5.3 Diagonal groups $D(T,d)$ when $d \geq 3$

We recall the definition of diagonal groups as stated in [16]. A diagonal group $D(T,d)$, where T is a non-abelian simple group and d an integer greater than 1, is a permutation group on the set

$$\Omega = \{[t_2, ..., t_d] : t_i \in T,\ 2 \leq i \leq d\}.$$

and is generated by the following permutations of Ω:

- **(G1)** $(s_1, ..., s_d) : [t_2, ..., t_d] \mapsto [s_1^{-1}t_2s_2, ..., s_1^{-1}t_ds_d]$ (these form a group isomorphic to T^d, which is the socle of $D(T,d)$);
- **(G2)** $\alpha : [t_2, ..., t_d] \mapsto [t_2^\alpha, ..., t_d^\alpha]$, where $\alpha \in \mathrm{Aut}(T)$ (the inner automorphisms of T coincide with the diagonal permutations $(s, ..., s)$ of the preceding type);
- **(G3)** $\pi : [t_2, ..., t_d] \mapsto [t_{2\pi}, ..., t_{d\pi}]$, where $\pi \in \mathrm{Sym}(\{2, ..., d\})$;
- **(G4)** $\tau : [t_2, ..., t_d] \mapsto [t_2^{-1}, t_2^{-1}t_3, ..., t_2^{-1}t_d]$ (this corresponds to the transposition $(1,2)$ in $\mathrm{Sym}(\{1, ..., d\})$; together with the preceding type it generates $\mathrm{Sym}(\{1, ..., d\})$.

The construction simplifies if $d = 2$. Let $\Omega = T$, the mappings of equation (G1) take the form

$$t \mapsto s_1^{-1}ts_2$$

in other words, T acts on itself by left and right multiplication. The automorphism group of T acts in the natural way on T, with the inner automorphisms identified with the above action of the diagonal subgroup $\{(s,s) : s \in T\}$. The symmetric group $\mathrm{Sym}(n-1)$ in (G3) is trivial, while the action of τ in (G4) is simply $t \mapsto t^{-1}$.

5.3.1 The separation and synchronisation property for $D(T,d)$, when $d \geq 3$

In the case $G = D(T,d)$, when $d \geq 3$, we would like to show that the group is non-separating, so we need to find a non-trivial G-invariant graph Γ such that the product of the clique and co-clique numbers equals to the number of vertices, i.e., $\omega(\Gamma) \cdot \alpha(\Gamma) = |T|$. The authors of [16] define a G-invariant graph as follows:

The graph will have $\Omega = T^{n-1}$ as it is vertex set. Two vertices $[u_2, ..., u_d]$ and $[t_2, ..., t_d]$ are adjacent if and only if they satisfies one of the following conditions:

- **(A1)** there exists $i \in \{2, ..., d\}$ such that $u_i \neq t_i$ but $u_j = t_j$ for $j \neq i$;
- **(A2)** there exists $x \in T$ with $x \neq e$ such that $u_i = xt_i$ for $i = 2, ..., d$.

This graph will be called ***diagonal graph*** and it will be denoted by $D\Gamma(T,d)$.

Theorem 5.24. *[16, Theorem 1.5] Let T be a finite group, then the co-clique number of $D\Gamma(T,3)$ is $|T|$.*

Proposition 5.25. *Let T be a finite group, then the clique number of the diagonal graph $D\Gamma(T,3)$ is $|T|$.*

Proof. Let T be a finite group and $D\Gamma(T,3)$ be a diagonal graph. By the clique–co-clique bound (inequality 3.1) and the previous theorem, the clique number of the diagonal graph $D\Gamma(T,3)$ is bounded above by $|T|$. The set S of all vertices

$[x, t_3]$, where $x, t_3 \in T$, having a fixed entry in the first coordinate is a clique in the graph, by **(A1)** the definition of the diagonal graph. The size of S is $|T|$ and since it the upper bound, S is a maximum clique. $\square$

Lemma 5.26. *Let T be a finite group. There is a maximum clique C in the diagonal graph $D\Gamma(T, d \geq 3)$, in one of the following two types:*

*(a) non-diagonal clique, for fixed $i \in \{2, ..., d\}$ the maximum clique has $[u_2, ..., u_i, ..., u_d]$ where all entries are fixed except the position i. Vertices in this clique are adjacent by rule **(A1)**. Any maximum clique of this type can be transformed to the set $\{[e, ..., e, u_i, e, ..., e] : u_i \in T\}$.*

*(b) diagonal clique, for fixed vertex $[u_2, ..., u_i, ..., u_d]$ we have the set $C_* = \{x[u_2, ..., u_d] : x \in T\}$ as maximum clique. In particular, $C = \{x[e, ..., e, ..., e] : x \in T\}$ is a maximum clique. Vertices in this clique are adjacent by rule **(A2)**.*

Moreover, the vertex set of the graph can be partitioned by the disjoint cliques of the same type.

Proof. Let $|T|= n$ and consider the sets $C_i = \{[u_2, ..., u_i, ..., u_d] : u_i \in T\}$, where $u_2, .., u_{i-1}, u_{i+1}, ..., u_d$ are fixed entries for the positions $2, ..., i-1, i+1, ..., d$. C_i is a clique of size n. It can be transformed to $\{[e, ..., e, u_i, e, ..., e] : u_i \in T\}$ by $(e, u_2^{-1}, ..., u_{i-1}, e, u_{i+1}, ..., u_d)$ using **(G1)**. There are $|T|^{d-2}$ choices for the fixed entries for the positions $2, ..., i-1, i+1, ..., d$, so for each i there are $|T|^{d-2}$ cliques $C_{i1}, ..., C_{i|T|^{d-2}}$. Clearly, these cliques have pairwise disjoint vertex sets. Therefore, they provide a partition of the vertex set of $D\Gamma(T, d \geq 3)$ into disjoint cliques.

For the diagonal cliques, consider the action of T on the Cartesian product $T \times ... \times T$ with $d-1$ factors by left multiplication. By the regularity of the action of

T on itself, there are $|T|^{n-2}$ orbits of size $|T|$ each of which is a maximum clique in $D\Gamma(T, d \geq 3)$. Vertices in each orbit are adjacent by rule **(A2)** and the conclusion follow. $\square$

Lemma 5.27. *Any maximum clique in the graph* $D\Gamma(T, d \geq 3)$, *is either of diagonal or non-diagonal type.*

Proof. To prove the lemma, assume that x, y and z are vertices in the graph such that x and y are adjacent by rule $(A1)$ and x and z are adjacent by rule $(A2)$. It is enough to show that y and z can be adjacent in the diagonal graph. It is the same as if any two cliques of different type intersect. Then their intersection contains exactly one element. Let C_1 be a clique of non-diagonal type and C_2 be a clique of diagonal type, and assume for the contrary that $u, t \in C_1 \cap C_2$. Since $u, t \in C_1$ then u and t are different in exactly one position, say i, their entries in the other $d-2$ positions are fixed. However, in this case they cannot both belong to C_2 as the action of T by left multiplication on it self is regular. Therefore, the size of the intersection of C_1 and C_2 is at most 1. $\square$

Theorem 5.28. *Let T be a finite simple group, then the co-clique number of* $D\Gamma(T, d)$ *is* $|T|^{d-2}$, *for* $d \geq 3$.

Proof. Let $|T| = n$. This can be proved by induction on d. Theorem 5.24 provides the base case $d = 3$. Assume that the result is true for $D\Gamma(T, d)$, where $d \leq k$. Therefore, there is an independent set S with $|S| = |T|^{k-2}$. Also, the sets $t_iS = \{(t_iu_2, ..., t_iu_k) : (u_2, ..., u_k) \in S\}$ for all $t_i \in T$ are $|T|$ pairwise disjoint independent sets in $D\Gamma(T, k)$. Now consider the sets $(t_j, t_iS) = \{[t_j, t_iu_2, ..., t_iu_k] : (u_2, ..., u_k) \in S\}$ for all $t_j, t_i \in T$ independent sets in $D\Gamma(T, k)$ and partition its vertex set. Define a new graph Γ with these independent sets as vertices and two (t_j, t_iS) and (t_k, t_lS) are adjacent if:

(a) $(A1')$ if $t_j \neq t_k$, and $t_i = t_l$;

(b) $(A1')$ if $t_j = t_k$ and $t_iS = xt_lS$ for some $x \in T$;

(c) $(A3')$ there is $y \in T$ such that $(t_j, t_iS) = y(t_k, t_lS)$.

The graph Γ is the same as the graph $D\Gamma(T, 3)$ and its co-clique number equals $|T|$. The rules of adjacency in Γ ensure that the union of the sets (vertices) in a maximum independent set of Γ is an independent set in $D(T, k+1)$ of size $|T|^{k-1}$. This complete the proof. □

Theorem 5.29. *An association scheme $\mathcal{AG}$ that is obtained from a group $G = D(T, d)$, for $d \geq 3$ is non-synchronising. Hence non-separating.*

Proof. We have seen that the vertex set of $D\Gamma(T, d \geq 3)$ can be partition into either pairwise disjoint cliques or pairwise disjoint co-cliques. The partition into co-cliques provide a colouring of $D\Gamma(T, d \geq 3)$ by $|T|$ colours. Consequently, there is a G-invariant graph $D\Gamma(T, d \geq 3)$ with the clique number equals the chromatic number, so $\mathcal{AG}$ is non-synchronising. □

Theorem 5.30. *The permutation group $G = D(T, d)$ for $d \geq 3$ is non-synchronising and separating.*

5.4 The equivalence of separation and synchronisation properties

It is a fact that a separating group is synchronising which follows from Theorem 2.24 and Theorem 2.23. The converse is not always true. A counterexample is provided in Theorem3.42 when examples of almost simple groups are considered.

There are few such examples and it seems to be a rare phenomenon. Therefore, a good question to ask is:

When is a primitive permutation group non-separating but synchronising?

In the previous sections we see that the diagonal groups $D(T, d)$, when $d \geq 3$, are non-separating and non-synchronising. In this section, we will prove that the separation and synchronisation properties are equivalent for all diagonal groups.

Theorem 5.31. *Synchronisation and separation properties are equivalent for $D(T, 2)$.*

Proof. Assume that $G = D(T, 2)$ is a non-separating group. Then T admits a factorization into subsets A and B, Theorem 5.16. Also, there is a non-trivial Cayley graph $\Gamma = \mathrm{Cay}(T, S)$ (we can assume that S is closed under conjugation) in the conjugacy classes association scheme such that $|A||B| = |T|$, where A is a maximum clique and B is maximum co-clique in Γ.

Claim:

(a) The set $\{Ab : b \in B\}$ provides a partition of T (vertex set of Γ) into cliques.

(b) The set $\{aB : a \in A\}$ provides a partition of T into co-cliques.

We prove the first claim and the second one can be done by similar argument. Assume for the contrary that $|Ab_1 \cap Ab_2| \neq 0$ where $b_1, b_2 \in B$. Then, there are elements $a_1, a_2 \in A$ such that $a_1 b_1 = a_2 b_2$. Thus, we have $a_2^{-1} a_1 = b_2 b_1^{-1}$, from the definition of Cayley graph Γ, $b_2 b_1^{-1} \in T \setminus S$. Then, $\{b_1, b_2\}$ and $\{a_1^{-1}, a_2^{-1}\}$ are an edges in $\bar{\Gamma}$ (the complement of Γ). However, the fact that S is closed under conjugation $a_2^{-1}a_1 \in T \setminus S$ implies

$$a_1a_2^{-1}a_1a_1^{-1} = a_1a_2^{-1} \in T \setminus S.$$

Therefore, $\{a_1, a_2\}$ is an edge in $\bar{\Gamma}$, which contradicts the fact that $\{a_1, a_2\}$ is an edge in the clique A and this proves claim (a).

The partitions provide a colouring of the graph Γ such that the chromatic number equals the clique number. Consequently, we have a non-trivial G-invariant graph Γ with the property that the clique number equals the chromatic number. Thus, $G = D(T, 2)$ is non-synchronising. □

Observe that if a group is of diagonal or affine type then it contains a regular subgroup. Thus, is it true that a primitive almost simple group G with regular subgroup is synchronising if and only if it is separating? This is an open question in [16].

5.5 Conclusion and future work

In this chapter, we considered diagonal permutation groups and related topics. We initiate a study for the factorisation of finite non-abelian groups and indicate its relationship to the synchronisation property of diagonal groups $D(T, 2)$. We show that $D(A_n, 2)$, when $n \geq 5$ and $D(T, d)$, when $d \geq 3$ are non-synchronising.

The case $D(T, 2)$, when T is a finite simple group that does not admit a factorisation into maximal subgroups is still to be solved. I think it might be true that these groups are synchronising!! So the question is: It is true that the existence of diagonal factorisation implies the assistance of maximal factorisation.

Another problem which can be considered for a future work is the investigation of the equivalence of the synchronisation and separation properties for primitive almost simple groups with regular subgroups.

Appendix A

Appendix

A.1 The proof of Theorem 3.10

In this Section we will provide the proof of Theorem 3.10 from Chapter 3

Theorem A.1. *Let $n \geq 13$, and $I \in \{\{1,2,3,5\}\{1,2,4,5\},\{1,3,4,5\},$ $\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\}\}$ and let $\Delta = \Gamma_I(n,5)$, then $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$, except the graph $\Gamma_{\{1,2,3,5\}}(21,5)$.*

The proof starts in next page.

Corollary A.2. *For $k = 5$, Conjectures 2 and 3 hold for $n \geq 11$.*

Proof. We start by calculating the matrix of the eigenvalues P and the dual matrix Q the Johnson association scheme $\mathcal{J}(n,5)$:

$$P = \begin{pmatrix} 1 & 5(n-5) & 5(n-6)(n-5) & \frac{5}{3}(n-7)(n-6)(n-5) & \frac{5}{24}(n-8)(n-7)(n-6)(n-5) & \frac{1}{120}(n-9)(n-8)(n-7)(n-6)(n-5) \\ 1 & 4n-25 & (n-6)(3n-25) & \frac{1}{3}(n-7)(n-6)(2n-25) & \frac{1}{24}(n-25)(n-8)(n-7)(n-6) & -\frac{1}{24}(n-9)(n-8)(n-7)(n-6) \\ 1 & 3n-23 & \frac{3}{2}(n-19)n+127 & \frac{1}{6}(n-26)(n-9)(n-7) & -\frac{1}{6}(n-8)(n-7)(2n-27) & \frac{1}{6}(n-9)(n-8)(n-7) \\ 1 & 2n-19 & \frac{1}{2}(n-29)n+87 & -\frac{1}{2}3(n-21)n-157 & \frac{1}{2}(n-8)(3n-31) & -\frac{1}{2}(n-9)(n-8) \\ 1 & n-13 & 42-4n & 6n-58 & 37-4n & n-9 \\ 1 & -5 & 10 & -10 & 5 & -1 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & n-1 & \frac{1}{2}(n-3)n & \frac{1}{6}(n-5)(n-1)n & \frac{1}{24}(n-7)(n-2)(n-1)n & \frac{1}{120}(n-9)(n-3)(n-2)(n-1)n \\ 1 & \frac{4n}{5}-\frac{9}{5}-\frac{4}{n-5} & \frac{(n-3)n(3n-23)}{10(n-5)} & \frac{1}{30}(n-1)n(2n-19) & \frac{(n-13)(n-7)(n-2)(n-1)n}{120(n-5)} & -\frac{(n-9)(n-3)(n-2)(n-1)n}{120(n-5)} \\ 1 & \frac{3n}{5}-\frac{13}{5}-\frac{8}{n-5} & \frac{(n-3)n(3(n-19)n+254)}{20(n-6)(n-5)} & \frac{(n-1)n((n-29)n+174)}{60(n-6)} & -\frac{(n-7)(n-2)(n-1)n(2n-21)}{60(n-6)(n-5)} & \frac{(n-9)(n-3)(n-2)(n-1)n}{60(n-6)(n-5)} \\ 1 & \frac{(n-1)(2n-25)}{5(n-5)} & \frac{(n-26)(n-9)(n-3)n}{20(n-6)(n-5)} & -\frac{(n-1)n(3(n-21)n+314)}{20(n-7)(n-6)} & \frac{(n-2)(n-1)n(3n-29)}{20(n-6)(n-5)} & -\frac{(n-9)(n-3)(n-2)(n-1)n}{20(n-7)(n-6)(n-5)} \\ 1 & \frac{(n-25)(n-1)}{5(n-5)} & -\frac{2(n-3)n(2n-27)}{5(n-6)(n-5)} & \frac{2(n-1)n(3n-31)}{5(n-7)(n-6)} & -\frac{(n-2)(n-1)n(4n-37)}{5(n-8)(n-6)(n-5)} & \frac{(n-9)(n-3)(n-2)(n-1)n}{5(n-8)(n-7)(n-6)(n-5)} \\ 1 & -\frac{5(n-1)}{n-5} & \frac{10(n-3)n}{(n-6)(n-5)} & -\frac{10(n-1)n}{(n-7)(n-6)} & \frac{5(n-2)(n-1)n}{(n-8)(n-6)(n-5)} & -\frac{(n-3)(n-2)(n-1)n}{(n-8)(n-7)(n-6)(n-5)} \end{pmatrix}.$$

Remark: In all cases we assume for the contrary that the product of the clique and co-clique numbers equals the number of vertices. For the first two cases we use the matrix P of eigenvalues and corollary 3.6 to get a contradiction. Given our assumption, we reach a contradiction if one of the following holds:

1. $1 - \deg(\Gamma_I(n,k))/\tau < n$, where I is a singleton, by Fisher inequality 3.8.

2. $1 - \deg(\Gamma_I(n,k))/\tau$ or $omega(\Gamma_I(n,k))$ does not divide $\binom{n}{k}$, by Corollary 3.6.

3. $1 - \deg(\Gamma_I(n,k))/\tau$ is not equal $\omega(\Gamma_I(n,k))$, by Corollary 3.6.

4. the product of $\omega(\Gamma_I(n,k))$ and $\alpha(\Gamma_I(n,k))$ is not equal $\omega(\Gamma_I(n,k))$.

The dual matrix Q is used for the other cases by applying Theorem 2.27 and Corollary 3.4.

Case $I = \{1,2,3,5\}$: The complement $\bar{\Delta}$ of the graph Δ is $\Gamma_{\{4\}}(n,5)$ and its eigenvalues is given by the fifth column of P, so we have:

$$\frac{5}{24}(n-8)(n-7)(n-6)(n-5), \frac{1}{24}(n-25)(n-8)(n-7)(n-6), -\frac{1}{6}(n-8)(n-7)(2n-27), \frac{1}{2}(n-8)(3n-31), 37-4n, 5.$$

The degree is the first eigenvalue $\frac{5}{24}(n-8)(n-7)(n-6)(n-5)$ and for $n \geq 25$ the smallest eigenvalue is $-(1/6)(-8+n)(-7+n)(-27+2n)$. Because the graph attains the clique- co-clique bound, the smallest eigenvalue divides the degree. This can happen only if $n \in \{22, 26, 141, 226\}$. Additionally, we must have $\omega(\bar{\Delta}) = 1 - \frac{deg(\bar{\Delta})}{\tau}$ which cannot occur according to the following table and this contradict the assumption.

n	$1-\frac{deg(\bar{\Delta})}{\tau}$	
22	21	If the clique number is 21 then the co-clique number must be 1254. Using GAP (with package GRAPE) $\alpha(\bar{\Delta}) < 1254$.
26	22	Does not equal the clique number which is 21
141	91	Does not divide the number of vertices
226	144	This case will be treat later by using the matrix Q.

Therefore,$\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{n}{5}$.

When $n < 22$, the smallest eigenvalue is $1/24(-25+n)(-8+n)(-7+n)(-6+n)$ and if the clique-coclique bound is attained then the smallest eigenvalue divides the degree of the graph. This is possible for $n \in \{15, 20, 21\}$.

n	$1-\frac{deg(\bar{\Delta})}{\tau}$	
15	6	It is equal the clique number but it does not divide the number of vertices.
20	16	It is equal the clique number but $\alpha(\bar{\Delta})$.
21	21	There is Steiner system (Projective plane)

Therefore, $\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{n}{5}$.

Case $I = \{1, 3, 4, 5\}$**:** The complement $\bar{\Delta}$ of the graph Δ is $\Gamma\{2\}(n, 5)$ and its eigenvalues are provided by the fourth column of P, so we have:

$$\frac{5}{3}(n-7)(n-6)(n-5), \frac{1}{3}(n-7)(n-6)(2n-25), \frac{1}{6}(n-26)(n-9)(n-7), -\frac{1}{2}3(n-21)n-157, 6n-58, -10.$$

The degree is $\frac{5}{3}(n-7)(n-6)(n-5)$ and for $n \geq 21$ the smallest eigenvalue is $-\frac{1}{2}3(n-21)n-157$. By elementary number theory, we can see that the smallest eigenvalue does not divide the degree. This contradicts our assumption.

When $n < 21$, the smallest eigenvalue is $1/6(-26+n)(-9+n)(-7+n)$ and if the clique-coclique bound is attained then the smallest eigenvalue divides the degree of the graph. This is possible for $n \in \{14, 19\}$.

n	$1 - \frac{deg(\bar{\Delta})}{\tau}$	
14	13	But the clique number is 11.
19	27	But the clique number is 13.

Therefore, $\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{n}{5}$.

Case $I = \{1, 2, 4, 5\}$**:** The complement $\bar{\Delta}$ of the graph Δ is $\Gamma_{\{3\}}(n, 5)$ and its spectrum is provided by the third column of P, so we have:

$$5(n-6)(n-5), (n-6)(3n-25), \frac{3}{2}(n-19)n+127, \frac{1}{2}(n-29)n+87, 42-4n, 10$$

The degree is $5(n-6)(n-5), (n-6)(3n-25)$ and for $n \geq 15$ the smallest eigenvalue is $42-4n$. The smallest eigenvalue divides the degree if and only if $n \in \{15, 18, 27, 33, 38, 60, 93, 258\}$. We must have $n \geq \omega(\bar{\Delta}) = 1 - \frac{deg(\bar{\Delta})}{\tau}$ which cannot occur according to the following table.

n	$1 - \frac{deg(\bar{\Delta})}{\tau}$
15	26
18	27
27	36
33	43
38	49
60	76
93	117
258	323

Therefore, $\omega(\bar{\Delta})\alpha(\bar{\Delta}) < \binom{n}{5}$.

Case $I = \{1, 5\}$**:** Let $u = (1, a, 0, 0, 0, x - a - 1)$ and $v = (1, b, c, 0, y - b - c - 1, 0)$ such that $a, b, c \geq 0$, $x - a - 1, y - b - c - 1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$(uQ)_1 = \frac{(n-1)}{5(n-5)}((5+4a)n - 25x)$$
$$(vQ)_1 = \frac{(n-1)}{5(n-5)}(-25y + n(4+2b+c+y)).$$

Since the product of the clique and coclique numbers equals the number of vertices, the product of these quantities is zero. Therefore, at least one of the following scenarios occurs:

(i) $x = 1/25(5+4a)n$, or

(ii) $y = \frac{-2bn-cn-4n}{n-25}$.

Assume that

$$y = \frac{-2bn - cn - 4n}{n-25}$$

since $xy = \binom{n}{5}$, we have

$$y = -\frac{(n-25)(n-4)(n-3)(n-2)(n-1)}{120(2b+c+4)}.$$

If we now consider the system:

$$(uQ)_3(vQ)_3 = 0 \tag{A.1}$$

$$(uQ)_4(vQ)_4 = 0 \tag{A.2}$$

$$(uQ)_5(vQ)_5 = 0 \tag{A.3}$$

$$(uQ)_6(vQ)_6 = 0 \tag{A.4}$$

By substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = \frac{5(n-5)}{4}, b = -\frac{10\left(n^3 - 28n^2 + 277n - 810\right)}{n^3 - 28n^2 + 277n - 1050}, c = \frac{20\left(n^3 - 28n^2 + 237n - 610\right)}{n^3 - 28n^2 + 277n - 1050};$$

For all $n \geq 13$, $b < 0$ or b is not an integer which contradict our assumptions.

$$a = -\frac{5(n-5)}{n-11}, b = \frac{-n^4 + 41n^3 - 671n^2 + 4771n - 11580}{2\left(n^2 - 21n + 140\right)}, c = \frac{3n^4 - 123n^3 + 1793n^2 - 10893n + 23140}{2\left(n^2 - 21n + 140\right)};$$

For all $n \geq 13$, $b < 0$ or b is not an integer which contradict our assumptions.

$$a = -\frac{5(n-5)}{2(n-8)}, b = \frac{-3n^3 + 94n^2 - 821n + 2130}{2(n-15)}, c = \frac{-n^4 + 49n^3 - 725n^2 + 4247n - 8610}{3(n-15)};$$

For all $n \geq 13$, $a < 0$ or a is not an integer which contradict our assumptions.

$$a = \frac{5\left(n^2-15n+50\right)}{5n-46}, b = \frac{5\left(n^4-43n^3+709n^2-4917n+11610\right)}{4\left(n^3-29n^2+303n-1125\right)}, c = -\frac{5\left(3n^4-121n^3+1695n^2-9887n+20310\right)}{4\left(n^3-29n^2+303n-1125\right)};$$

For all $n \geq 13$, $c < 0$ or c is not an integer which contradict our assumptions.

$$a = -\frac{5\left(n^2-15n+50\right)}{n^2-23n+118}, b = \frac{-3n^4+123n^3-1808n^2+11028n-23440}{4\left(n^2-22n+120\right)},$$

$$c = \frac{-n^5+72n^4-1727n^3+18292n^2-88356n+158480}{12\left(n^2-22n+120\right)};$$

For all $n \geq 13$, $b < 0$ or b is not an integer which contradict our assumptions.

$$a = \frac{5\left(n^3-23n^2+173n-415\right)}{5n^2-90n+397}, b = \frac{5\left(3n^4-117n^3+1603n^2-9187n+18610\right)}{2\left(3n^3-90n^2+893n-2950\right)},$$

$$c = \frac{5\left(n^5-66n^4+1438n^3-14076n^2+63937n-109410\right)}{6\left(3n^3-90n^2+893n-2950\right)}.$$

For all $n \geq 13$, $b < 0$ or b is not an integer which contradict our assumptions.

Therefore, (ii) is not satisfied and we assume that (i) occurs, that is $x = 1/25(5+4a)n$. since $xy = \binom{n}{5}$, we have

$$y = \frac{5(n-4)(n-3)(n-2)(n-1)}{24(4a+5)}$$

. By substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = -\frac{5\left(n^2 - 15n + 50\right)}{2n^2 - 39n + 166}, b = \frac{-4n^3 + 87n^2 - 593n + 1290}{2n - 17}, c = -\frac{4\left(n^4 - 31n^3 + 341n^2 - 1601n + 2730\right)}{3(2n - 17)};$$

For all $n \geq 14$, $a < 0$ or a is not an integer. When $n = 13$, $a = 40$. However, b in this case is equal -56 which contradict our assumptions.

$$a = \frac{5\left(n^4 - 30n^3 + 335n^2 - 1650n + 3000\right)}{5n^3 - 125n^2 + 1050n - 2904}, b = \frac{5\left(3n^4 - 88n^3 + 953n^2 - 4488n + 7740\right)}{4n^3 - 99n^2 + 819n - 2274},$$

$$c = \frac{10\left(n^5 - 39n^4 + 599n^3 - 4509n^2 + 16608n - 23940\right)}{3\left(4n^3 - 99n^2 + 819n - 2274\right)};$$

For all $n \geq 13$, $a < 0$ or a is not an integer which contradict our assumptions. Thus, when $I = \{1, 5\}$, $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$.

Case $I = \{1, 4\}$**:** Let $u = (1, a, 0, 0, x - a - 1, 0)$ and $v = (1, 0, b, c, 0, y - b - c - 1)$ such that $a, b, c \geq 0$, $x - a - 1, y - b - c - 1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$(uQ)_1 = \frac{(n-1)}{5(n-5)} n(3a+x+4) - 25x$$
$$(vQ)_1 = \frac{(n-1)}{5(n-5)} (n(3b+2c+5) - 25y).$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x = \frac{-3an-4n}{n-25}$, or

(ii) $y = \frac{-2bn-cn-4n}{n-25}$.

It is clear that (i) does not arise when $n \geq 25$,for $n \leq 24$, by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$\left\{ a = -\frac{5\left(n^2-26n+105\right)}{3\left(n^2-26n+125\right)}, b = \frac{1}{2}(-5)\left(n^2-11n+30\right), c = \frac{1}{6}(-5)\left(n^3-18n^2+107n-210\right) \right\};$$

For all $n \geq 13$, $a < 0$ or a is not an integer, except $n = 20, 21$. However, b in these case is not integer which contradict our assumptions.

$$a = -\frac{5\left(n^3-40n^2+401n-1130\right)}{2n^3-89n^2+1045n-3550}, b = -\frac{5\left(5n^3-102n^2+667n-1410\right)}{2(7n-55)}, c = -\frac{5\left(4n^4-115n^3+1202n^2-5441n+9030\right)}{6(7n-55)};$$

For all $n \geq 13$, $a < 0$ or a is not an integer, which contradict our assumptions.

$$a = -\frac{5\left(n^4 - 47n^3 + 713n^2 - 4393n + 9390\right)}{n^4 - 55n^3 + 1049n^2 - 8129n + 21750}, b = -\frac{10\left(n^4 - 32n^3 + 368n^2 - 1807n + 3210\right)}{11n^2 - 177n + 718},$$

$$c = -\frac{5\left(n^5 - 45n^4 + 757n^3 - 6051n^2 + 23218n - 34440\right)}{3\left(11n^2 - 177n + 718\right)};$$

For all $n \geq 13$, $a < 0$ or a is not an integer, except $n = 16, 17$ and 23. However, b in these case is not integer which contradict our assumptions.

$$a = \frac{n^4 - 46n^3 + 671n^2 - 3986n + 8280}{n^3 - 41n^2 + 466n - 1560}, b = \frac{10\left(n^3 - 20n^2 + 129n - 270\right)}{3n^2 - 47n + 186}, c = \frac{5\left(n^4 - 30n^3 + 323n^2 - 1494n + 2520\right)}{3\left(3n^2 - 47n + 186\right)}$$

. For all $n \geq 13$, $a < 0$ or a is not an integer, except $n = 15$. However, b in these case is equal -225 which contradict our assumptions. Therefore, (i) is not satisfied and we assume that (ii) occurs, that is

$$y = \frac{-2bn - cn - 4n}{n - 25}$$

. since $xy = \binom{n}{5}$, we have

$$x = \frac{5(n-4)(n-3)(n-2)(n-1)}{24(3b + 2c + 5)}$$

. By substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = \frac{4(n-5)}{3}, b = -\frac{10\left(n^2-19n+70\right)}{n^2-19n+106}, c = \frac{20\left(n^2-13n+40\right)}{n^2-19n+106};$$

For all $n \geq 13$, $b < 0$ or b is not an integer, except $n = 14$, where $a = 9, b = 0, c = 30$ However, in this case $y = \frac{182}{5}$, so it is not an integer and contradict our assumptions.

$$a = -\frac{5\left(2n^3-57n^2+493n-1290\right)}{2n^3-73n^2+821n-2910}, b = -\frac{5\left(3n^3-77n^2+606n-1480\right)}{4(5n-44)}, c = -\frac{5\left(n^4-46n^3+659n^2-3782n+7560\right)}{12(5n-44)};$$

For all $n \geq 13$, $a < 0$ or a is not an integer,which contradict our assumptions.

$$a = \frac{2n^3-55n^2+472n-1235}{2n^2-45n+229}, b = \frac{5\left(3n^3-74n^2+569n-1370\right)}{2\left(3n^2-55n+254\right)}, c = \frac{5\left(n^4-41n^3+557n^2-3103n+6090\right)}{6\left(3n^2-55n+254\right)}$$

. For all $n \geq 13$, $b < 0$ or b is not an integer,which contradict our assumptions. Thus, when $I = \{1,4\}$, $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$.

Case $I = \{1,3\}$: Let $u = (1, a, 0, x-a-1, 0, 0)$ and $v = (1, 0, b, 0, c, y-b-c-1)$ such that $a, b, c \geq 0$, $x - a - 1, y - b - c - 1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively, attaining the clique-coclique bound. The second coordinates of uQ and vQ are

$$(uQ)_1 = \frac{(n-1)}{5(n-5)}(n(2a+2x+3)-25x)$$
$$(vQ)_1 = \frac{(n-1)}{5(n-5)}(n(2b-c+y+4)-25y).$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x = \frac{-2an-3n}{2n-25}$, or

(ii) $y = \frac{-2bn+cn-4n}{n-25}$.

It is clear that (i) does not arise when $n \geq 13$. Thus, we assume that (ii) occurs, that is

$$y = \frac{-2bn+cn-4n}{n-25}$$

since the clique-coclique bound is attained we get

$$x = -\frac{(n-25)(n-4)(n-3)(n-2)(n-1)}{120(2b-c+4)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a=-\frac{15\left(n^2-16n+55\right)}{3n^2-60n+313}, b=-\frac{5\left(n^3-24n^2+191n-480\right)}{2(5n-47)}, c=\frac{-3n^5+150n^4-2900n^3+27030n^2-121177n+208260}{80(5n-47)}$$

; For all $n \geq 13$, $a < 0$ or a is not an integer, which contradict our assumptions.

$$a=\frac{3(n-5)}{2}, b=-\frac{10(n-5)}{n-11}, c=\frac{-n^3+28n^2-237n+610}{10(n-11)}$$

; For all $n \geq 13$, $c < 0$ or c is not an integer, which contradict our assumptions.

$$a=\frac{3\left(n^2-19n+70\right)}{3n-34}, b=\frac{5\left(n^2-17n+60\right)}{4n-39}, c=\frac{-3n^4+121n^3-1695n^2+9887n-20310}{1560-160n};$$

For all $n \geq 13$, $c < 0$ or c is not an integer, which contradict our assumptions.

$$a=\frac{n^3-41n^2+443n-1315}{n^2-36n+227}, b=\frac{10\left(n^2-13n+40\right)}{5n-43}, c=\frac{-n^5+66n^4-1438n^3+14076n^2-63937n+109410}{120(5n-43)};$$

For all $n \geq 13$, $b < 0$ or b is not an integer, which contradict our assumptions.

$$a=-\frac{5\left(n^3-42n^2+443n-1290\right)}{n^3-50n^2+667n-2658}, b=-\frac{5\left(n^3-23n^2+170n-400\right)}{4(2n-17)},$$

$$c = \frac{n^6 - 81n^5 + 2375n^4 - 33835n^3 + 252984n^2 - 953684n + 1426320}{960(2n-17)};$$

For all $n \geq 13$, $c < 0$ or c is not an integer except $n = 82$. In this case $a = \frac{18095}{3181}$ which contradict our assumptions.

$$a = -\frac{5(n^3 - 34n^2 + 319n - 870)}{2(n^3 - 34n^2 + 355n - 1182)}, b = -\frac{5(3n^3 - 62n^2 + 421n - 930)}{2(7n-57)},$$

$$c = \frac{n^6 - 66n^5 + 1630n^4 - 20100n^3 + 133009n^2 - 452154n + 619920}{60(7n-57)}$$

. For all $n \geq 13$, $a < 0$ or a is not an integer except $n = 17$ and 27. In this case $b < 0$ which contradict our assumptions. Thus, when $I = \{1,3\}$, $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$.

Case $I = \{2,5\}$**:** Let $u = (1, 0, a, 0, 0, x - a - 1)$ and $v = (1, b, 0, c, y - b - c - 1, 0)$ such that $a, b, c \geq 0$, $x - a - 1, y - b - c - 1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$(uQ)_1 = \frac{(n-1)}{5(n-5)}((5+3a)n - 25x)$$
$$(vQ)_1 = \frac{(n-1)}{5(n-5)}(-25y + n(4 + 3b + c + y)).$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x = \frac{1}{25}(3a+5)n$, or

(ii) $y = \frac{-3bn-cn-4n}{n-25}$.

First we assume (i) that is $x = \frac{1}{25}(3a+5)n$ since the clique-coclique bound is attained we get

$$\frac{5(n-4)(n-3)(n-2)(n-1)}{24(3a+5)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = -\frac{10\left(n^2-15n+50\right)}{n^2-33n+206}, b = \frac{2\left(4n^2-63n+215\right)}{5n-47}, c = \frac{-2n^4+71n^3-844n^2+4165n-7350}{3(5n-47)};$$

But $a < 0$ unless $n \in \{14, 16, 19, 14\}$. In these cases b is not an integer except for $n = 16$. When $n = 16$, the value of a is 10 and we have $x = \frac{112}{5}$. This contradict the assumption that x is an integer.

Or we have

$$a = \frac{5\left(n^3-22n^2+163n-390\right)}{2\left(2n^2-43n+219\right)}, b = \frac{3n^3-80n^2+683n-1790}{3n^2-53n+244}, c = \frac{2\left(4n^4-119n^3+1274n^2-5869n+9870\right)}{3\left(3n^2-53n+244\right)}.$$

In this case for all $n \geq 13$ the value of b is not an integer. This contradict the assumption that b is an integer. Clearly (i) can not occur. We assume that (ii) is true, that is $y = \frac{-3bn-cn-4n}{n-25}$ by the equality in the clique–co-clique bound we have

$$x=-\frac{(n-25)(n-4)(n-3)(n-2)(n-1)}{120(3b+c+4)}$$

by substituting the values of x and y in the system A.1 and solving this system for a,b and c we have the following solutions:

$$a=\frac{5\left(n^2-11n+30\right)}{3(n-9)},b=\frac{n^4-41n^3+671n^2-4771n+11580}{n^3-36n^2+455n-1740},c=-\frac{2\left(3n^4-118n^3+1533n^2-8138n+15240\right)}{n^3-36n^2+455n-1740};$$

For all $n\geq 13$, the value of a is either negative or not an integer, which contradict the assumption that $a\geq 0$ and a is an integer. Or we have

$$a=\frac{1}{6}(-5)\left(n^2-11n+30\right),b=-\frac{5\left(n^3-28n^2+277n-810\right)}{2\left(n^3-28n^2+277n-900\right)},c=\frac{5\left(n^3-28n^2+217n-510\right)}{n^3-28n^2+277n-900}$$

For all $n\geq 13$, the value of b is not an integer, but b must be an integer according to our assumption, contradiction. Or we have

$$a=-\frac{10\left(n^2-11n+30\right)}{n^2-23n+114},b=\frac{3n^3-94n^2+821n-2130}{2\left(n^2-25n+120\right)},c=\frac{-n^5+55n^4-1091n^3+9893n^2-41796n+66780}{12\left(n^2-25n+120\right)};$$

For all $n\geq 13$, the value of b is not an integer except $n\in\{15,18,21,30\}$, and in each of the cases we reach a contradiction as we can

n	a	b	c
15	$a = 150$	$b = 14$	$c = -24$
18	$a = -65$	$b = 26$	
21	$a = -\frac{100}{3}$	$b = 20$	
30	$a = -\frac{500}{27}$	$b = 35$	

Or we have

$$a = -\frac{5\left(n^3 - 21n^2 + 140n - 300\right)}{3(3n - 26)}, b = -\frac{5\left(n^4 - 43n^3 + 709n^2 - 4917n + 11610\right)}{n^4 - 51n^3 + 941n^2 - 7341n + 20250}, c = \frac{20\left(n^4 - 39n^3 + 503n^2 - 2655n + 4950\right)}{n^4 - 51n^3 + 941n^2 - 7341n + 20250};$$

For all $n \geq 13$, the value of c either negative or not an integer which contradict the assumptions.

Or we have

$$a = \frac{5\left(n^3 - 21n^2 + 140n - 300\right)}{4n^2 - 73n + 318}, b = \frac{3n^4 - 123n^3 + 1808n^2 - 11028n + 23440}{3n^3 - 100n^2 + 1028n - 3280}, c = \frac{4\left(n^4 - 46n^3 + 611n^2 - 3206n + 5880\right)}{3\left(3n^2 - 70n + 328\right)};$$

For all $n \geq 13$, the value of a is not an integer, except when $n = 14$ we have $a = 18$. However, in this case $b = -\frac{9}{2}$, Contradiction.

Or we have

$$a = -\frac{5\left(n^4 - 29n^3 + 311n^2 - 1453n + 2490\right)}{10n^2 - 171n + 713}, b = -\frac{5\left(3n^4 - 117n^3 + 1603n^2 - 9187n + 18610\right)}{3n^4 - 129n^3 + 1963n^2 - 12759n + 30050},$$

$$c=-\frac{10\left(n^5-57n^4+1087n^3-9387n^2+37936n-58380\right)}{3\left(3n^4-129n^3+1963n^2-12759n+30050\right)}.$$

For all $n \geq 14$, the value of a is not an integer, and when $n=13$ we have $a=-28$ and we reach to a contradiction to the assumption and (ii) is not true. Therefore, $\omega(\Delta)\alpha(\Delta)<\binom{n}{5}$.

Case $I=\{2,4\}$**:** Let $u=(1,0,a,0,x-a-1,0)$ and $v=(1,b,0,c,0,y-b-c-1)$ such that $a,b,c\geq 0$, $x-a-1, y-b-c-1\geq 0$ and $xy=\binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and co-clique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$\begin{aligned}(uQ)_1&=\frac{(n-1)}{5(n-5)}n(2a+x+4)-25x\\(vQ)_1&=\frac{(n-1)}{5(n-5)}n(4b+2c+5)-25y.\end{aligned}$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x=-\frac{2(an+2n)}{n-25}$, or

(ii) $y=\frac{1}{25}n(4b+2c+5)$.

First we assume that (i) occurs, that is

$$x=-\frac{2(an+2n)}{n-25}$$

since the clique-coclique bound is attained we get

$$y = \frac{1}{25} n(4b + 2c + 5)$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = -\frac{10\left(n^2 - 26n + 105\right)}{3n^2 - 78n + 475}, b = \frac{15(n-5)}{8}, c = \frac{1}{24}(-5)\left(n^3 - 18n^2 + 107n - 210\right);$$

For all $n \geq 13$ the value of a is either negative or not an integer. This contradicts our assumptions.

Or we have

$$a = -\frac{10\left(n^3 - 40n^2 + 401n - 1130\right)}{n^3 - 58n^2 + 887n - 3950}, b = \frac{5\left(5n^2 - 72n + 235\right)}{8(2n-17)}, c = -\frac{5\left(n^4 - 31n^3 + 341n^2 - 1601n + 2730\right)}{24(2n-17)};$$

For all $n \geq 13$ the value of a is either negative or not an integer. This contradicts our assumptions.

Or we have

$$a = \frac{-n^4 + 46n^3 - 671n^2 + 3986n - 8280}{2\left(n^2 - 35n + 220\right)}, b = -\frac{5\left(n^2 - 14n + 45\right)}{n^2 - 17n + 74}, c = -\frac{5\left(n^3 - 18n^2 + 107n - 210\right)}{3\left(n^2 - 17n + 74\right)};$$

For all $n \geq 13$ the value of b is not an integer. This contradicts our assumptions.

Or we have

$$a = \frac{5\left(n^4 - 47n^3 + 713n^2 - 4393n + 9390\right)}{2\left(2n^3 - 93n^2 + 1186n - 4575\right)}, b = \frac{5\left(n^3 - 26n^2 + 212n - 535\right)}{5n^2 - 87n + 382}, c = \frac{5\left(2n^4 - 55n^3 + 556n^2 - 2453n + 3990\right)}{3\left(5n^2 - 87n + 382\right)};$$

For all $n \geq 13$ the value of b is not an integer. This contradicts our assumptions. This means that (i) cannot happen. Thus, we assume that (ii) occurs and

$$y = \frac{1}{25}n(4b + 2c + 5)$$

since the clique-coclique bound is attained we get

$$x = \frac{5(n-4)(n-3)(n-2)(n-1)}{24(4b + 2c + 5)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = \frac{5\left(3n^3 - 62n^2 + 409n - 870\right)}{8n^2 - 145n + 663}, b = \frac{5\left(n^4 - 41n^3 + 599n^2 - 3691n + 7980\right)}{5n^3 - 180n^2 + 1915n - 6252}, c = -\frac{10\left(3n^4 - 86n^3 + 909n^2 - 4186n + 7080\right)}{5n^3 - 180n^2 + 1915n - 6252};$$

For all $n \geq 13$ the value of c is either negative or not an integer. This contradicts our assumptions. Or we have

$$a = \frac{5\left(2n^4 - 69n^3 + 835n^2 - 4248n + 7740\right)}{8n^3 - 236n^2 + 2265n - 7062}, b = \frac{5\left(3n^4 - 107n^3 + 1376n^2 - 7540n + 14800\right)}{15n^3 - 420n^2 + 3764n - 10832},$$

$$c = \frac{20\left(n^5 - 40n^4 + 623n^3 - 4724n^2 + 17460n - 25200\right)}{3\left(15n^3 - 420n^2 + 3764n - 10832\right)}.$$

For all $n \geq 13$ the value of b is not an integer. This contradicts our assumptions. Therefore, (ii) cannot occur. Consequently, $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$.

Case $I = \{2, 3\}$**:** Let $u = (1, 0, a, x - a - 1, 0, 0)$ and $v = (1, b, 0, 0, c, y - b - c - 1)$ such that $a, b, c \geq 0$, $x - a - 1, y - b - c - 1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$\begin{aligned}
(uQ)_1 &= \frac{(n-1)}{5(n-5)} n(a + 2x + 3) - 25x \\
(vQ)_1 &= \frac{(n-1)}{5(n-5)} n(4b + c + 5) - 25y.
\end{aligned}$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x = \frac{-an-3n}{2n-25}$, or

(ii) $y = \frac{1}{25}n(4b + 2c + 5)$.

It is clear that (i) does not occur for $n \geq 13$, so we assume (ii), that is

$$y = \frac{1}{25}n(4b + c + 5)$$

since the clique-coclique bound is attained we get

$$x = \frac{5(n-4)(n-3)(n-2)(n-1)}{24(4b + c + 5)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = \frac{15\left(n^3 - 22n^2 + 151n - 330\right)}{2\left(3n^2 - 55n + 258\right)}, b = \frac{5\left(n^3 - 24n^2 + 191n - 480\right)}{5n^2 - 95n + 408}, c = \frac{5\left(3n^4 - 86n^3 + 909n^2 - 4186n + 7080\right)}{4\left(5n^2 - 95n + 408\right)}$$

For all $n \geq 14$, the value of b is not an integer. When $n = 13$, we have $b = 40$ but $a = \frac{84}{5}$, which is a contradiction to the assumptions.

Or we have

$$a = \frac{1}{2}(-3)\left(n^2 - 11n + 30\right), b = -\frac{5(n-5)}{2n-13}, c = -\frac{5\left(n^2 - 11n + 30\right)}{4(2n-13)}$$

For all $n \geq 14$, the value of c is either negative or not an integer. This is contradiction.

Or we have

$$a=-\frac{3\left(n^3-25n^2+184n-420\right)}{4(n-10)}, b=-\frac{5\left(n^2-17n+60\right)}{n^2-25n+120}, c=-\frac{5\left(n^3-20n^2+129n-270\right)}{2\left(n^2-25n+120\right)}$$

For all $n \geq 14$, the value of a is einter negative or not an integer. When $n=13$, we have $a=14$ but $b=\frac{10}{9}$, which is a contradiction to the assumptions. Therefore, (ii) cannot occur and $\omega(\Delta)\alpha(\Delta)<\binom{n}{5}$.

Case $I=\{2,3\}$: Let $u=(1,0,0,a,0,x-a-1)$ and $v=(1,b,c,0,y-b-c-1,0)$ such that $a,b,c\geq 0$, $x-a-1, y-b-c-1\geq 0$ and $xy=\binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$(uQ)_1=\frac{(n-1)}{5(n-5)}(2a+5)n-25x$$
$$(vQ)_1=\frac{(n-1)}{5(n-5)}n(3b+2c+y+4)-25y.$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x=\frac{1}{25}(2a+5)n$, or

(ii) $y=\frac{-3bn-2cn-4n}{n-25}$.

We start by assuming (ii), that is

$$x = \frac{1}{25}(2a+5)n$$

since the clique-coclique bound is attained we get

$$y = \frac{5(n-4)(n-3)(n-2)(n-1)}{24(2a+5)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = -\frac{10(n-5)}{n-17}, b = \frac{8(n-5)}{3}, c = n^2 - 11n + 30;$$

For all $n > 17$ the value of a is either negative or not an integer. For $n \in \{13, 14, 15, 16\}$ we reach a contradiction as we can see in the following table.

n	a	b	x
13	20	$\frac{64}{3}$	
14	30	24	$\frac{117}{5}$
15	50	$\frac{80}{3}$	
16	110	$\frac{88}{3}$	

Or we have

$$a = \frac{10\left(n^2 - 15n + 50\right)}{3(3n-38)}, b = \frac{8\left(n^2 - 18n + 65\right)}{4n-43}, c = \frac{2n^3 - 57n^2 + 445n - 1050}{4n-43};$$

For all $b \geq 13$ all value of b is either negative or not an integer except $n \in \{13, 28\}$ and we have contradiction as follows:

n	a	b	c	x
13	80	0	-56	
28	30	40	154	$\frac{364}{5}$

Or we have

$$a = \frac{5\left(n^4 - 30n^3 + 335n^2 - 1650n + 3000\right)}{6(5n-52)}, b = -\frac{5\left(n^3 - 26n^2 + 219n - 570\right)}{n^3 - 26n^2 + 231n - 711},$$

$$c = \frac{5\left(2n^3 - 43n^2 + 291n - 630\right)}{n^3 - 26n^2 + 231n - 711}$$

For all $n \geq 13$, the value of b is not integer. This contradicts our assumptions. Thus, (i) cannot occur and we assume (ii) that is

$$y = \frac{-3bn - 2cn - 4n}{n - 25}$$

since the clique-coclique bound is attained we get

$$x=-\frac{(n-25)(n-4)(n-3)(n-2)(n-1)}{120(3b+2c+4)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a=\frac{5\left(n^2-11n+30\right)}{3(n-10)}, b=\frac{2\left(n^3-42n^2+431n-1230\right)}{n^2-37n+210}, c=\frac{n^4-48n^3+755n^2-4608n+9540}{2\left(n^2-37n+210\right)};$$

For all $n \geq 13$ we have c is not an integer except $n=34$ where $c=812$, but $b=\frac{232}{3}$. This contradicts our assumptions.

Or we have

$$a=\frac{5}{12}\left(n^3-18n^2+107n-210\right), b=-\frac{10\left(n^3-28n^2+237n-610\right)}{3n^3-84n^2+731n-2050}, c=\frac{10\left(n^3-28n^2+217n-510\right)}{3n^3-84n^2+731n-2050};$$

For all $n \geq 13$, the value of b is not an integer which is a contradiction to our assumption.

Or we have

$$a=-\frac{5\left(n^3-21n^2+140n-300\right)}{3(5n-46)}, b=\frac{n^4-65n^3+1272n^2-9388n+22640}{n^3-52n^2+668n-2480}, c=-\frac{4\left(n^3-39n^2+338n-840\right)}{n^2-42n+248};$$

For all $n \geq 13$, the value of b is either negative or not an integer except $n \in \{14, 20\}$ where we have contradictions as the following:

n	a	b	c	x
14	$-\frac{20}{3}$	10		
20	$\frac{20650}{417}$	250		

Or we have

$$a = \frac{5\left(n^4 - 29n^3 + 311n^2 - 1453n + 2490\right)}{27(n-9)}, b = -\frac{5\left(n^4 - 59n^3 + 1025n^2 - 6901n + 15630\right)}{n^4 - 59n^3 + 1061n^2 - 7729n + 19950},$$

$$c = \frac{10\left(n^4 - 50n^3 + 737n^2 - 4228n + 8340\right)}{n^4 - 59n^3 + 1061n^2 - 7729n + 19950};$$

For all $n \geq 13$, the value of b is not an integer which is a contradiction to our assumption.

Or we have

$$a = -\frac{5\left(n^3 - 18n^2 + 107n - 210\right)}{3(3n-25)}, b = \frac{3n^4 - 123n^3 + 1793n^2 - 10893n + 23140}{3n^3 - 96n^2 + 913n - 2740},$$

$$c = -\frac{2\left(3n^4 - 118n^3 + 1533n^2 - 8138n + 15240\right)}{3n^3 - 96n^2 + 913n - 2740};$$

For all $n \geq 13$, the value of c is either negative or not an integer which is a contradiction to our assumption.

Or we have

$$a = \frac{5\left(n^4 - 28n^3 + 287n^2 - 1280n + 2100\right)}{3(7n-58)}, b = -\frac{5\left(3n^4 - 121n^3 + 1695n^2 - 9887n + 20310\right)}{3n^4 - 129n^3 + 1927n^2 - 12151n + 27750},$$

$$c = \frac{20\left(n^4 - 39n^3 + 503n^2 - 2655n + 4950\right)}{3n^4 - 129n^3 + 1927n^2 - 12151n + 27750}$$

For all $n \geq 13$, the value of b is not an integer which is a contradiction to our assumption. Therefore, (ii) cannot be true and $\omega(\Delta)\alpha(\Delta) < \binom{n}{5}$.

Case $I = \{3,4\}$**:** Let $u = (1,0,0,a,x-a-1,0)$ and $v = (1,b,c,0,0,y-b-c-1)$ such that $a,b,c \geq 0$, $x-a-1, y-b-c-1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and coclique of Γ_I, respectively,attaining the clique-coclique bound.

The second coordinates of uQ and vQ are

$$(uQ)_1 = \frac{(n-1)}{5(n-5)}n(a+x+4) - 25x$$
$$(vQ)_1 = \frac{(n-1)}{5(n-5)}n(4b+3c+5) - 25y.$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x = \frac{-an-4n}{n-25}$, or

(ii) $y = \frac{1}{25}n(4b + 3c + 5)$.

If we assume (i),

$$x = \frac{-an - 4n}{n - 25}$$

and since the clique-coclique bound is attained we get

$$y = -\frac{(n-25)(n-4)(n-3)(n-2)(n-1)}{120(a+4)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a = -\frac{10\left(n^2 - 26n + 105\right)}{n^2 - 26n + 225}, b = \frac{5(n-5)}{2}, c = \frac{5}{6}\left(n^2 - 11n + 30\right);$$

For all $n \geq 13$ the value of a is either negative or not an integer except for $n \in \{15, 21\}$ where we do not have contradiction according to the following table. However, we use GAP with the package $GRAPE$ to show that the equality does not hold in the clique-coclique bound.

n	a	b	c	x	$\alpha(\Delta)$
15	10	25	75	< 143	
21	0	40	200	< 969	

Or we have

$$a = \frac{10\left(n^3 - 40n^2 + 401n - 1130\right)}{3\left(3n^2 - 81n + 550\right)}, b = \frac{5\left(4n^2 - 63n + 215\right)}{2(5n - 47)}, c = \frac{5\left(n^3 - 24n^2 + 173n - 390\right)}{2(5n - 47)}$$

For all $n \geq 13$ all value of a is either negative or not an integer, which is a contradiction.

Or we have

$$a = -\frac{5\left(n^4 - 47n^3 + 713n^2 - 4393n + 9390\right)}{18\left(n^2 - 28n + 175\right)}, b = \frac{5\left(n^3 - 32n^2 + 299n - 820\right)}{5n^2 - 95n + 458}, c = -\frac{10\left(2n^3 - 41n^2 + 269n - 570\right)}{5n^2 - 95n + 458}$$

For all $n \geq 13$ the value of b is not an integer, which is a contradiction.

Or we have

$$a = \frac{n^4 - 46n^3 + 671n^2 - 3986n + 8280}{6(n - 20)}, b = -\frac{5\left(n^2 - 17n + 60\right)}{n^2 - 17n + 78}, c = \frac{10\left(n^2 - 11n + 30\right)}{n^2 - 17n + 78}$$

For all $n \geq 13$ the value of b is not an integer, which is a contradiction. This means our assumption that (i) cannot be true. Then, we assume (ii) that is

$$y = \frac{1}{25}n(4b + 3c + 5)$$

since the clique-coclique bound is attained we get

$$x=\frac{5(n-4)(n-3)(n-2)(n-1)}{24(4b+3c+5)}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$$a=\frac{2n^4-67n^3+802n^2-4067n+7410}{9(n-11)}, b=-\frac{5\left(n^3-34n^2+319n-870\right)}{n^3-34n^2+355n-1158}, c=\frac{10\left(n^3-25n^2+184n-420\right)}{n^3-34n^2+355n-1158}$$

For all $n \geq 13$ the value of a is not integer, which is contradiction. Or we have

$$a=\frac{20\left(n^3-23n^2+162n-360\right)}{3\left(3n^2-59n+306\right)}, b=\frac{10\left(n^3-26n^2+213n-540\right)}{5n^2-105n+486}, c=\frac{5\left(n^4-32n^3+387n^2-2016n+3780\right)}{2\left(5n^2-105n+486\right)}$$

For all $n \geq 13$ the value of a is not an integer except $n = 26$, but in this case $b = \frac{12495}{284}$, and we reach a contradiction.

Or we have

$$a=-\frac{5\left(2n^4-69n^3+835n^2-4248n+7740\right)}{3\left(8n^2-157n+774\right)}, b=\frac{5\left(n^4-49n^3+776n^2-4940n+10800\right)}{5n^3-180n^2+1900n-6192},$$

$$c=-\frac{20\left(n^4-33n^3+392n^2-1980n+3600\right)}{5n^3-180n^2+1900n-6192}.$$

For all $n \geq 13$ the value of b is not an integer except $n \in \{14, 20\}$, but according to the following table we have contradictions.

n	a	b
14	$\frac{20}{3}$	10
20	$-\frac{20650}{417}$	250

Therefore, (ii) does not occur and $\omega(\Delta)\alpha(\Delta) < \binom{n}{5})$.

Finally, we have one possibility remain from the case $I = \{1, 2, 4, 5\}$ which we need to check. Assume that $n = 226$.

Case $I = \{1, 2, 4, 5\}$**:** Let $u = (1, a, b, 0, c, x - a - b - c - 1)$ and $v = (1, 0, 0, y - 1, 0, 0)$ such that $a, b, c \geq 0$, $x - a - 1, y - b - c - 1 \geq 0$ and $xy = \binom{n}{5}$. So u and v are the inner distributions of an arbitrary clique and co-clique of Γ_I, respectively,attaining the clique–co-clique bound.

The second coordinates of uQ and vQ are

$$(uQ)_1 = \frac{(n-1)}{5(n-5)} n226(4a + 3b + 2c + 5) - 25x$$

$$(vQ)_1 = \frac{(n-1)}{5(n-5)} n((678 + 427y).$$

We will follow the same steps as in previous case. Therefore, we have at least one of the following scenarios:

(i) $x = \frac{226}{25}(4a + 3b + 2c + 5)$, or

(ii) $y = -\frac{678}{427}$.

It is clear that (ii) can not occur, so we assume that

$$x = \frac{226}{25}(4a + 3b + 2c + 5)$$

since the clique–co-clique bound is attained we get

$$y = \frac{519813000}{4a + 3b + 2c + 5}$$

by substituting the values of x and y in the system A.1 and solving this system for a, b and c we have the following solutions:

$\square$

Bibliography

[1] Aljohani, M., Bamberg, J. and Cameron, P. (2018) 'Synchronization and separation in the Johnson schemes', *Portugaliae Mathematica* **74**(3), 213–232.

[2] Alspach, B., Gavlas, H., Šajna, M. and Verrall, H. (2003) 'Cycle decompositions IV: complete directed graphs and fixed length directed cycles', *Journal of Combinatorial Theory, Series A* **103**(1), 165–208.

[3] Araújo, J. (2006) 'A group theoretical approach to synchronizing automata and the Černý problem'. Unpublished.

[4] Araújo, J., Bentz, W. and Cameron, P. (2013) 'Groups synchronizing a transformation of non-uniform kernel', *Theoretical Computer Science* **498**, 1–9.

[5] Araújo, J. and Cameron, P. (2014) 'Primitive groups synchronize non-uniform maps of extreme ranks', *Journal of Combinatorial Theory, Series B* **106**(1), 98–114.

[6] Araújo, J., Cameron, P. and Steinberg, B. (2017) 'Between primitive and 2-transitive: synchronization and its friends', *EMS Surveys in Mathematical Sciences* **4**(2), 101–184.

[7] Araújo, J., Mitchell, J. and Schneider, C. (2011) 'Groups that together with

any transformation generate regular semigroups or idempotent generated semigroups', *Journal of Algebra* **343**(1), 93–106.

[8] Arnold, F. and Steinberg, B. (2006) 'Synchronizing groups and automata', *Theoretical Computer Science* **359**(1-3), 101–110.

[9] Babai, L. and Frankl, P. (1980) 'On set intersections', *Journal of Combinatorial Theory, Series A* **28**(1), 103–105.

[10] Bailey, R. A. (2004) *Association schemes: designed experiments, algebra and combinatorics*, Cambridge Studies in Advanced Mathematics (84), Cambridge, Cambridge University Press.

[11] Bamberg, J., Giudici, M., Lansdown, J. and Royle, G. (2021) 'Synchronising primitive groups of diagonal type exist', *arXiv preprint arXiv:2104.13355* .

[12] Baranyai, Z. (1975) 'On the factorization of the complete uniform hypergraphs', *Infinite and finite sets* **10**, 91–107.

[13] Beutelspacher, A. (1974) 'On parallelisms in finite projective spaces', *Geometriae Dedicata* **3**(1), 35–40.

[14] Blokhuis, A., Brouwer, A. E. and Haemers, W. H. (2006) 'On 3-chromatic distance-regular graphs', *SSRN Electronic Journal* **44**(1), 293–305.

[15] Božović, V. and Pace, N. (2008) 'On group factorizations using free mappings', *Journal of Algebra and Its Applications* **07**(05), 647–662.

[16] Bray, J. N., Cai, Q., Cameron, P., Spiga, P. and Zhang, H. (2020) 'The Hall–Paige conjecture, and synchronization for affine and diagonal groups', *Journal of Algebra* **545**, 27–42.

[17] Breach, D. and Street, A. (1988) 'Partitioning sets of quadruples into designs II', *J. Combin. Math. Combin. Comput* **3**, 41–48.

[18] Brouwer, A. E., Cioabă, S. M., Ihringer, F. and McGinnis, M. (2018) 'The smallest eigenvalues of Hamming graphs, Johnson graphs and other distance-regular graphs with classical parameters', *Journal of Combinatorial Theory. Series B* **133**, 88–121.

[19] Brouwer, A. E., Cohen, A. M. and Neumaier, A. (1989) *Distance-regular graphs*, Vol. 18 of *A Series of Modern Surveys in Mathematics*, Berlin, Heidelberg: Springer.

[20] Cameron, P. (1999) *Permutation groups*, London Mathematical Society Student Texts (45), Cambridge, Cambridge University Press.

[21] Cameron, P. (2010) *Synchronization*, LTCC intensive course, [Lecture Notes] Unpublished.

[22] Cameron, P. and Kazanidis, P. A. (2008) 'Cores of symmetric graphs', *Journal of the Australian Mathematical Society* **85**(2), 145–154.

[23] Cameron, P. and Seidel, J. (1991) Quadratic forms over GF(2), *in* D. Corneil and R. Mathon, eds, 'Geometry and Combinatorics', Academic Press, pp. 290–297.

[24] Cayley, A. (1850) 'IV. On the triadic arrangements of seven and fifteen things', *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* **37**(247), 50–53.

[25] Černỳ, J. (1964) 'Poznámka k homogénnym experimentom s konečnỳmi automatmi', *Matematicko-Fyzikálny Časopis* **14**(3), 208–216.

[26] Cohen, G. and Frankl, P. (1980) 'On tilings of the binary vector space', *Discrete Mathematics* **31**(3), 271–277.

[27] Cohen, G., Honkala, I., Litsyn, S. and Lobstein, A. (1997) *Covering codes*, Vol. 54 of *North-Holland Mathematical Library*, Oxford: Elsevier.

[28] de Carli Silva, M. K., Coutinho, G., Godsil, C. and Roberson, D. E. (2019) 'Algebras, Graphs and Thetas', *Electronic Notes in Theoretical Computer Science* **346**, 275–283.

[29] Delsarte, P. (2016) An algebraic approach to the association schemes of coding theory, PhD thesis, Catholic University of Louvain, Louvain.

[30] Delsarte, P. and Goethals, J. (1975) 'Alternating bilinear forms over GF(q)', *Journal of Combinatorial Theory, Series A* **19**(1), 26–50.

[31] Dixon, J. D. and Mortimer, B. (1996) *Permutation groups*, Vol. 163 of *Graduate Texts in Mathematics*, New York: Springer.

[32] Erdós, P., Ko, C. and Rado, R. (1961) 'Intersection theorems for systems of finite sets', *The Quarterly Journal of Mathematics* **12**(1), 313–320.

[33] Frankl, P. and Füredi, Z. (1985) 'Forbidding just one intersection', *Journal of Combinatorial Theory, Series A* **39**(2), 160–176.

[34] Ganyushkin, O. and Mazorchuk, V. (2009) *Classical finite transformation semigroups: an introduction*, Vol. 9 of *Algebra and Applications*, London: Springer.

[35] Godsil, C. (1993) *Algebraic combinatorics*, Chapman and Hall Mathematical Series, London: Chapman and Hall/CRC.

[36] Godsil, C. and Meagher, K. (2015) *Erdős–Ko–Rado theorems: algebraic approaches*, Cambridge Studies in Advanced Mathematics (149), Cambridge: Cambridge University Press.

[37] Godsil, C. and Royle, G. (2001) *Algebraic Graph Theory*, Vol. 207 of *Graduate Texts in Mathematics*, New York: Springer.

[38] Häggkvist, R. and Janssen, J.C. (1996) 'All-even Latin squares', *Discrete Mathematics* **157**(1-3), 199–206.

[39] Hanani, H. (1960) 'On quadruple systems', *Canadian Journal of Mathematics* **12**, 145–157.

[40] Hanani, H. (1961) 'The existence and construction of balanced incomplete block designs', *The Annals of Mathematical Statistics* **32**(2), 361–386.

[41] Hilton, A. and Milner, E. (1967) 'Some intersection theorems for systems of finite sets', *The Quarterly Journal of Mathematics* **18**(1), 369–384.

[42] Huang, L. P., Huang, J. Q. and Zhao, K. (2015) 'On endomorphisms of alternating forms graph', *Discrete Mathematics* **338**(3), 110–121.

[43] Huang, L. P., Huang, Z., Li, C. K. and Sze, N. S. (2014) 'Graphs associated with matrices over finite fields and their endomorphisms', *Linear Algebra and its Applications* **447**, 2–25.

[44] Ionin, Y. J. and Shrikhande, M. S. (2006) *Combinatorics of symmetric designs*, Vol. 5 of *New Mathematical Monographs (5)*, Cambridge: Cambridge University Press.

[45] Ito, N. (1953) 'On the factorizations of the linear fractional group $\mathrm{LF}(2, p^n)$', *Acta Sci. Math* **15**(1), 79–84.

[46] Johnson, N. L. and Montinaro, A. (2012) 'The transitive t-parallelisms of a finite projective space', *Advances in Geometry* **12**(3), 401–429.

[47] Karpovsky, M. (1981) 'Weight distribution of translates, covering radius, and perfect codes correcting errors of given weights', *IEEE Transactions on Information Theory* **27**(4), 462–472.

[48] Keevash, P. (2014) 'The existence of designs', *arXiv preprint arXiv:1401.3665.* .

[49] Kirkman, T. (1847) 'On a problem in combinations', *Cambridge and Dublin Mathematical Journal* **2**, 191–204.

[50] Kolotoğlu, E. and Magliveras, S. S. (2013) 'On large sets of projective planes of orders 3 and 4', *Discrete Mathematics* **313**(20), 2247–2252.

[51] Kramer, E. S. and Mesner, D. M. (1974) 'Intersections among Steiner systems', *Journal of Combinatorial Theory, Series A* **16**(3), 273–285.

[52] Li, W. and Li, X. (2018) 'On two problems of almost synchronizing groups', *Theoretical Computer Science* **707**, 94–95.

[53] Liebeck, M., Praeger, C. and Saxl, J. (2010) *Regular subgroups of primitive permutation groups*, Vol. 203 of *Memoirs of the American Mathematical Society (952)*, Providence: American Mathematical Society.

[54] Liebeck, M. W., Praeger, C. E. and Saxl, J. (1990) *The maximal factorizations of the finite simple groups and their automorphism groups*, Vol. 86 of *Memoirs of the American Mathematical Society (432)*, Providence: American Mathematical Society.

[55] Lovasz, L. (1979) 'On the Shannon capacity of a graph', *IEEE Transactions on Information Theory* **25**(1), 1–7.

[56] MacWilliams, F. J. and Sloane, N. J. A. (1977) *The theory of error-correcting codes*, Vol. 16 of *North-Holland Mathematical Library*, Amsterdam: Elsevier.

[57] Neumann, P. M. (1975) 'The lawlessness of groups of finitary permutations', *Archiv der Mathematik* **26**(1), 561–566.

[58] Neumann, P. M. (2009) 'Primitive permutation groups and their section-regular partitions', *Michigan Mathematical Journal* **58**(1), 309–322.

[59] Patterson, N. (1976) 'A four-dimensional Kerdock set over GF(3)', *Journal of Combinatorial Theory, Series A* **20**(3), 365–366.

[60] Pin, J. E. (1978) Sur un cas particulier de la conjecture de Černý, *in* G. Ausiello and C. Böhm, eds, 'Automata, Languages and Programming', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 345–352.

[61] Praeger, C. and Cameron, P. (1992) 'Partitioning into Steiner systems', *Combinatorics' 88* **2**, 61–71.

[62] Praeger, C. E. and Schneider, C. (2018) *Permutation groups and Cartesian decompositions*, Vol. 449 of *London Mathematical Society Lecture Note Series (449)*, Cambridge: Cambridge University Press.

[63] Roberson, D. E. (2019) 'Homomorphisms of strongly regular graphs', *Algebraic Combinatorics* **2**(4), 486.

[64] Schaefer, A. (2016) Synchronizing permutation groups and graph endomorphisms, PhD thesis, University of St Andrews, St Andrews.

[65] Schmidt, K.-U. (2018) 'Hermitian rank distance codes', *Designs, Codes and Cryptography* **86**(7), 1469–1481.

[66] Schneider, C. and Silva, A. C. (2015) ‘Cliques and colorings in generalized Paley graphs and an approach to synchronization’, *Journal of Algebra and Its Applications* **14**(06), 1550088.

[67] Silva, A. (2012) Low-dimensional affine synchronizing groups, Master’s thesis, University of Lisbon, Lisbon.

[68] Soicher, L. H. (2017) ‘GRAPE Package for GAP’. Version 4.7.
URL: *http://www.maths.qmul.ac.uk/ leonard/grape/*

[69] Szabó, S. (2004) *Topics in factorization of abelian groups*, Texts and Readings in Mathematics (29), Gurgaon: Hindustan Book Agency.

[70] Szabo, S. and Sands, A. D. (2009) *Factoring groups into subsets*, Vol. 257 of *Lecture Notes in Pure and Applied Mathematics*, New York: Chapman and Hall/CRC.

[71] Teirlinck, L. (1991) ‘A completion of Lu’s determination of the spectrum for large sets of disjoint Steiner triple systems’, *Journal of Combinatorial Theory, Series A* **57**(2), 302–305.

[72] The GAP Group (2017) ‘GAP - Groups, Algorithms, and Programming’. Version 4.8.7.
URL: *http://www.gap-system.org*

[73] Tietäväinen, A. (1973) ‘On the nonexistence of perfect codes over finite fields’, *SIAM Journal on Applied Mathematics* **24**(1), 88–96.

[74] Trahtman, A. N. (2007) ‘The Černý conjecture for aperiodic automata’, *Discrete Mathematics and Theoretical Computer Science* **9**(2), 3–10.

[75] Van Bon, J. (2007) ‘Finite primitive distance-transitive graphs’, *European Journal of Combinatorics* **28**, 517–532.

[76] Van Lint, J. H. and Wilson, R. M. (1994) *A course in combinatorics*, Subjects:Mathematics, Discrete Mathematics Information Theory and Coding, second edn, Cambridge: Cambridge university press.

[77] Volkov, M. V. (2008) Synchronizing automata and the černý conjecture, *in* C. Martín-Vide, F. Otto and H. Fernau, eds, 'Language and Automata Theory and Applications', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 11–27.

[78] Wan, Z. X. (1996) *Geometry of matrices*, London: World Scientific.

[79] Wang, Y., Huo, Y., Ma, C. and Ma, J. (2011) *Association schemes of matrices*, International Series of Numerical Mathematics, Sudbury: Jones & Bartlett.

[80] Wiegold, J. and Williamson, A. G. (1980) 'The factorisation of the alternating and symmetric groups', *Mathematische Zeitschrift* **175**(2), 171–179.

[81] Wilson, R. A. (2009) *The finite simple groups*, Vol. 251 of *Graduate Texts in Mathematics*, London: Springer-Verlag.

[82] Wilson, R. M. (1984) 'The exact bound in the Erdös-Ko-Rado theorem', *Combinatorica* **4**(2-3), 247–257.

[83] Wolfram Research, Inc. (2017) 'Mathematica'. Version 11.2.
URL: *https://www.wolfram.com/mathematica/online/*