Super Catalan Numbers and Fourier Summations over Finite Fields

Author:
Limanta, Kevin

Publication Date:
2022

DOI:
https://doi.org/10.26190/unsworks/24053

License:
https://creativecommons.org/licenses/by/4.0/
Link to license to see what you are allowed to do with this resource.

Downloaded from http://hdl.handle.net/1959.4/100346 in https://unsworks.unsw.edu.au on 2024-04-19

Super Catalan Numbers and Fourier Summations over Finite Fields

Kevin Mandira Limanta

A thesis submitted in fulfilment of the requirements
for the degree of Doctor of Philosophy

School of Mathematics and Statistics
Faculty of Science
May 2022

ORIGINALITY STATEMENT

☑ I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

COPYRIGHT STATEMENT

☑ I hereby grant the University of New South Wales or its agents a non-exclusive licence to archive and to make available (including to members of the public) my thesis or dissertation in whole or part in the University libraries in all forms of media, now or here after known. I acknowledge that I retain all intellectual property rights which subsist in my thesis or dissertation, such as copyright and patent rights, subject to applicable law. I also retain the right to use all or part of my thesis or dissertation in future works (such as articles or books).

For any substantial portions of copyright material used in this thesis, written permission for use has been obtained, or the copyright material is removed from the final public version of the thesis.

AUTHENTICITY STATEMENT

☑ I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis.

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in the candidate's thesis in lieu of a Chapter provided:

- The candidate contributed **greater than 50%** of the content in the publication and are the "primary author", i.e. they were responsible primarily for the planning, execution and preparation of the work for publication.
- The candidate has obtained approval to include the publication in their thesis in lieu of a Chapter from their Supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis.

☑ The candidate has declared that **their thesis contains no publications, either published or submitted for publication**.

Candidate's Declaration

I declare that I have complied with the Thesis Examination Procedure.

Abstract

We find an algebraic interpretation of the super Catalan numbers through polynomial summation formulas over unit circles over finite fields of odd characteristic. While traditional Fourier analysis involves Riemann integration over the unit circle in the real number plane, we will develop a purely algebraic integration theory without recourse to infinite procedures, and develop an algorithm for explicitly computing such Fourier sums for general monomials.

We consider three unit circles that arise from the Euclidean geometry and two relativistic geometries, and demonstrate the strong relationship between the integration theory in each geometry. The algebraic integrals in the three geometries are called the Fourier summation functionals and take values in the same finite field.

The key results in this thesis are the existence and uniqueness of the Fourier summation functionals, as well as the explicit formulas for them in terms of the super Catalan numbers and their rational variants which we call the circular super Catalan numbers.

This investigation not only opens up new avenues in developing finite field harmonic analysis from a completely algebraic point of view, but also highlights many similarities to the traditional integration theory over the unit circle.

Acknowledgements

The past four years have been one of the most rewarding periods in my life. I am thankful for the love and support from my family members, academic supervisors, and friends. I met amazing people along the way, some of them have become a second family to me. I have had the pleasure to share my research, travel to exciting places, and live in one of the most beautiful cities on earth.

Foremost, I am eternally grateful to my supervisor Norman Wildberger. I have been under his continued guidance since 2015 and I could not have asked for a better supervisor. Norman has been constantly supporting me, providing valuable insight, and pushed me to achieve a lot of things. From suggesting the topic of this thesis to the final stages of proof-reading, Norman has truly made me more confident in pursuing a career in mathematics.

I am also thankful for the insight and constructive comments from my co-supervisor Daniel Chan. A major part of this thesis is established due to Daniel's feedback during the final stage of my PhD studies.

I am blessed to have a supportive and understanding family – my mom and late dad for whom my sincerest gratitude cannot be overstated, and also my two little brothers. Also instrumental in keeping me sane during my study is a group of people I am happy to call my second family in Sydney. They are my two housemates Eka Putra and Edward Santoso, as well as Intan Rahayu, Ellys Yapit, Raymond Mak, Yuriko Tjung, Nicholas Aliwarga, William Raharjo, Evan Buntoro, Mandy Chung, and Tania Cahyono.

I would like to also thank these wonderful people at the School of Mathematics and Statistics, which on top of my mind include my desk and house neighbour Meiram Akhymbek, my fellow Indonesian and combinatorialist-in-the-making Yudhi Bunjamin, my now-graduated late-nighter partner Dr. Wai Hong Tan, also to Fiona Kim, Alan Stoneham, Joshua Ho, Harry Crimmins, Thomas Scheckter, Susannah Waters, Gemayne Magbanua, Markie Lugton. There are of course many others who I cannot mention one by one, but you know who you are!

At some point during my PhD studies I developed quite an affiliation to a combinatorial object known as Dyck paths. The Dyck paths themselves are maybe

not as important as the subsequent encounter with Hopein Christofen Tang, who has helped me a lot more than he wants to admit. On the off chance that he is reading this, I want to thank him, in the most cryptic way possible, for existing.

I also want to acknowledge many helps offered by Yohanes Tjandrawidjaja, who is kind enough to answer every single query I have, although I admit most of my queries were unimportant (*la vache...*). *Merci de m'avoir prêté tes oreilles et donné ta perspicacité précieuse.*

I would also like to express my gratitude to Yozef Tjandra and Davin Wangsa for the constant support from afar. More specifically, I would like to thank Yozef for his helpful comments. The timing of my thesis submission is also perfect to dedicate this thesis as a wedding gift to Davin. You don't usually hand out your thesis as a wedding gift, do you?

Last but certainly not least, I would like to thank the Indonesian government for allowing me the opportunity to study at the University of New South Wales. The following excerpt from a traditional Indonesian song, which depicts one's pride and longing of their homeland, has certainly become more personal over time.

```
Walaupun banyak negri kujalani
Yang masyhur permai dikata orang
Tetapi kampung dan rumahku
Di sanalah kurasa senang
```

Sydney, May 2022

Kevin Limanta

To every aspiring mathematician out there.

Contents

Abstract iii

Acknowledgements iv

List of Figures ix

I Introduction and Preliminaries 1

1 Introduction 2

1.1 Summing polynomials over unit circles over finite fields 5

1.2 Connection to traditional integration theory over the unit circle . . . 14

1.3 Outline of the thesis 16

2 Preliminary Theory 18

2.1 Polynumbers and polynomials over finite fields 19

2.2 Polynumbers and functions over finite fields 24

2.2.1 Group actions on $\mathbb{F}_q^{\mathbb{A}}$ and G-invariant functions 27

2.2.2 The dual space and G-invariant linear functionals 30

2.3 Prior developments on the super Catalan numbers 31

2.3.1 Circular super Catalan numbers 34

2.4 Krawtchouk polynumbers and matrices 37

2.5 The circular polynumbers 41

II Fourier Summations over Finite Fields 45

3 Chromogeometry and Dihedrons 46

3.1 Blue, red, and green complex numbers over a general field 46

3.2 Geometry over complex numbers 49

3.3 Unit circles in chromogeometry 52

3.3.1 Unit circle parametrisations 54

3.3.2 The Legendre and Jacobi symbols 56

3.3.3 Sizes of unit circles in chromogeometry over $\mathbb{F}_q$ 58
3.3.4 The cyclic group structure on the unit circles 59
3.4 Special orthogonal groups in chromogeometry 61

4 Circular Integral Functionals **68**
4.1 Circular integral functionals on $\mathbb{F}_q^{\mathbb{A}}$ 69
4.2 Circular integral functionals on $\mathrm{Pol}_2(\mathbb{F}_q)$ 71
4.3 Some examples of Fourier summation functional evaluation 74

5 Circular Super Catalan Numbers and Explicit Formulas for $\psi_{c,q}$ **81**
5.1 Explicit formulas for $\psi_{c,q}$ via chromogeometry 82
5.1.1 The green Fourier summation functional 82
5.1.2 The red Fourier summation functional 83
5.1.3 The blue Fourier summation functional when $\left(\frac{-1}{q}\right) = 1$ 86
5.2 An explicit formula for $\psi_{b,q}$ when $\left(\frac{-1}{q}\right) = -1$ via complex summations 87
5.2.1 A combined formula for $\psi_{b,q}$ 92
5.3 Some examples of the computation of $\psi_{c,q}$ 94

III Secondary Analysis and Conclusion **97**

6 Further Properties **98**
6.1 The Periodicity property 98
6.2 Symmetric difference table 105
6.3 Forward difference table 109

7 Afterword **113**

Bibliography **115**

List of Figures

1.1 The blue unit circle $S_{b,13}$ in two different configurations. 10

4.1 The green unit circle $S_{g,17}$. 75
4.2 The red unit circle $S_{r,17}$. 75
4.3 The blue unit circle $S_{b,17}$. 76
4.4 The three unit circles $S_{g,17}$, $S_{r,17}$, and $S_{b,17}$ in $\mathbb{A}(\mathbb{F}_{17})$. 76
4.5 Three unit circles $S_{c,17}$ in a different configuration. 77

Part I

Introduction and Preliminaries

Chapter 1

Introduction

This thesis will elucidate the crucial and perhaps surprising role that super Catalan numbers, and closely associated rational numbers which we will call circular super Catalan numbers, play in both algebra and analysis. We first observe that these numbers arise in classical Fourier summation formulas for polynomials over the unit circle in the rational Euclidean plane, and that correspondingly they can also be shown to be at the heart of similar summation formulas over finite fields in both Euclidean and relativistic geometries.

The relation between the Euclidean case and two particular relativistic geometries, introduced by Wildberger and called chromogeometry, will play an important role in relating the corresponding orthogonal groups and allowing pleasant relations between the Euclidean and relativistic formulas.

Super Catalan numbers are natural numbers of the form

$$S(m,n) \equiv \frac{(2m)!\,(2n)!}{m!n!\,(m+n)!} \tag{1.1}$$

parametrised by two natural numbers m and n, and were first introduced by Catalan [8] in 1874. The first modern study of these numbers term was initiated by Gessel in his 1992 paper [19].

These numbers are generalisations of the well-known **Catalan numbers**

$$C_n \equiv \frac{1}{n+1}\binom{2n}{n}$$

since $S\,(1,n) = 2C_n$. The table below lists the super Catalan numbers $S\,(m,n)$ for small values of m and n listed in row m and column n, with indexing starting at 0. A bigger table is given in Chapter 2.

$m\backslash n$	0	1	2	3	4	5
0	1	2	6	20	70	252
1	2	2	4	10	28	84
2	6	4	6	12	28	72
3	20	10	12	20	40	90
4	70	28	28	40	70	140
5	252	84	72	90	140	252

Table 1: $S(m,n)$ for $0 \leq m,n \leq 5$

The fact that $S(m,n)$ is always an integer is a consequence of the recurrence relation

$$4S(m,n) = S(m+1,n) + S(m,n+1) \tag{1.2}$$

and from the definition it is clear that $S(n,m) = S(m,n)$. A further inspection of the formula shows that the entries of the zeroth row and zeroth column of the table agree with the diagonal entries, and these are the central binomial coefficients

$$S(k,0) = S(0,k) = S(k,k) = \binom{2k}{k}.$$

Somewhat surprisingly, there is no known general combinatorial understanding for $S\,(m,n)$ to date. This is in marked contrast to the situation with the Catalan numbers, which have hundreds of combinatorial interpretations, compiled for example in [43]; see also sequence A000108 in the Online Encyclopedia of Integer Sequences (OEIS) [42]. There are, however, some combinatorial or weighted interpretations of $S\,(m,n)$ for some particular values of m and n which we will describe in the next chapter.

In this thesis we introduce also a closely related family of rational numbers, called the **circular super Catalan numbers** given by

$$\Omega(m,n) \equiv \frac{S(m,n)}{4^{m+n}}. \tag{1.3}$$

The table of numbers $\Omega(m,n)$ for $0 \leq m,n \leq 5$ is given in Table 2 in the next page, associated with the values of $S\,(m,n)$ in Table 1 above.

Table 2 below is still symmetric, namely $\Omega(n,m) = \Omega(m,n)$, but now the relation between the entries of the zeroth row, or the zeroth column, and the diagonal entries is

$$\Omega(k,k) = \frac{1}{4^k}\Omega(k,0) = \frac{1}{4^k}\Omega(0,k) = \frac{1}{4^{2k}}\binom{2k}{k}.$$

$m\backslash n$	0	1	2	3	4	5
0	1	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{5}{16}$	$\frac{35}{128}$	$\frac{63}{256}$
1	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{5}{128}$	$\frac{7}{256}$	$\frac{21}{1024}$
2	$\frac{3}{8}$	$\frac{1}{16}$	$\frac{3}{128}$	$\frac{3}{256}$	$\frac{7}{1024}$	$\frac{9}{2048}$
3	$\frac{5}{16}$	$\frac{5}{128}$	$\frac{3}{256}$	$\frac{5}{1024}$	$\frac{5}{2048}$	$\frac{45}{32\,768}$
4	$\frac{35}{128}$	$\frac{7}{256}$	$\frac{7}{1024}$	$\frac{5}{2048}$	$\frac{35}{32\,768}$	$\frac{35}{65\,536}$
5	$\frac{63}{256}$	$\frac{21}{1024}$	$\frac{9}{2048}$	$\frac{45}{32\,768}$	$\frac{35}{65\,536}$	$\frac{63}{262\,144}$

Table 2: $\Omega(m,n)$ for $0 \leq m,n \leq 5$

More importantly, the recurrence property of the super Catalan numbers becomes what we might call the **Pascal property** of the circular super Catalan numbers:

$$\Omega(m,n) = \Omega(m+1,n) + \Omega(m,n+1)$$

so that each entry is the sum of the entry directly below it and to the right. It is not hard to see that these three conditions, together with the normalisation condition that $\Omega(0,0) = 1$, completely determine the table.

We will see that the circular super Catalan numbers actually have a central algebraic and analytic interpretation in the context of *integration* or *summation theory of polynomials over unit circles over finite fields of odd characteristic* in a remarkable manner.

Their role extends even to summations over suitably defined unit circles in relativistic geometries, and the curious relations between the Euclidean and relativistic formulas are an aspect of the three-fold symmetry of *chromogeometry* [49] which is an outgrowth of rational trigonometry [50]. This theory brings together Euclidean planar geometry with quadratic form $x^2 + y^2$ (blue) with two different forms of relativistic Einstein-Minkowski geometries with quadratic forms $x^2 - y^2$ (red) and xy (green). The relations and indeed symmetries between these three geometries play a crucial role in our derivations, as summations over unit circles in both Euclidean and relativistic geometries are closely related, and connections between them provide a powerful tool for explicit evaluations.

In the rest of this introduction we will explain the remarkable formulas in which the circular super Catalan numbers play the primary role and illustrate them with examples. We will also observe that the classical results for polynomial integration over the circle in the Euclidean plane, for example as laid out by Folland [17], can also be restated in terms of the super Catalan numbers.

This correspondence suggests that there is a bridge between characteristic zero and odd characteristic harmonic analysis. We will see that additionally these formulas suggest also the study of a wide variety of further (rational) numbers that occur as coefficients of an important family of polynomials which we call the *circular polynumbers*.

1.1 Summing polynomials over unit circles over finite fields

The problem of summing polynomials over a finite field has many profound implications to number theory, Fourier analysis, and more generally harmonic analysis. In 2015, Thakur gave an expository survey on sums of integral powers of monic polynomials of certain degrees over finite fields [46], in which relations to the zeta function also appear.

Much of traditional harmonic analysis involving objects defined over finite fields assumes that the functions take values in the usual complex number field $\mathbb{C}$. This approach has many applications, for example in the sum-product estimate in finite fields (see Bourgain [4]) which is an emerging topic in additive combinatorics (see Tao and Vu [44]). Carbery gives a summary of recent discoveries on harmonic analysis theory over finite fields in [6]. Most recently, an exposition on harmonic analysis on $\mathrm{GL}(n)$ over finite fields can be found in Gurevich [22].

One of the aims of this thesis is to investigate polynomial summation over the unit circles over finite fields of odd characteristic in which the functions involved take values in the same finite field. This gives an alternate direction for finite field Fourier analysis, with an interplay between number theoretical and combinatorial aspects.

To start with, we consider a finite field $\mathbb{F} = \mathbb{F}_q$ where $q = p^r$ is a power of an odd prime p, so that $\mathbb{F}_p \subseteq \mathbb{F}_q$. The algebra of 2×2 matrices with entries in $\mathbb{F}_q$ will be called the **dihedron** algebra $\mathbb{D}$, introduced by Wildberger in [53]. We can define a natural symmetric bilinear form on $\mathbb{D}$ and also three special commutative subalgebras of $\mathbb{D}$, namely the algebras of blue complex numbers, red complex numbers, and green complex numbers. The restriction of the symmetric bilinear form on each subalgebra then gives rise to three different geometries which we call the blue, red, and green geometries. There is also a quadratic form that corresponds to the symmetric bilinear form in each geometry which we call quadrance, and we define the unit circle in each geometry as the collection of all complex numbers with quadrance 1.

The associated affine plane $\mathbb{A}$ of $\mathbb{F}_q$ consists of points $[x, y]$ where x, y are in $\mathbb{F}_q$, and in each algebra of complex numbers we can identify a complex number z with an affine point $[x, y]$. With this identification, the unit circles in each geometry are

then defined by

$$S_b(\mathbb{F}_q) = S_{b,q} \equiv \left\{[x,y] \in \mathbb{A} : \ x^2 + y^2 = 1\right\}$$
$$S_r(\mathbb{F}_q) = S_{r,q} \equiv \left\{[x,y] \in \mathbb{A} : \ x^2 - y^2 = 1\right\}$$
$$S_g(\mathbb{F}_q) = S_{g,q} \equiv \{[x,y] \in \mathbb{A} : \ xy = 1\}$$

where the subscripts b, r, and g naturally refer to blue, red, and green respectively; for brevity, we use the subscript c when we wish to refer to an undetermined one of these colours. We will also use $S_{c,q}$ as a shorthand for $S_c(\mathbb{F}_q)$ when the underlying field is clear from the context.

The dichotomy of whether -1 is a square or not in $\mathbb{F}_q$ plays a role in the blue geometry and is noted through the Jacobi symbol, a generalisation of the Legendre symbol defined in Chapter 3. For any odd prime p, the Legendre symbol specialises to

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } -1 \text{ is a square in } \mathbb{F}_p \\ -1 & \text{if } -1 \text{ is not a square in } \mathbb{F}_p \end{cases}$$

and for any prime power $q = p^r$ the **Jacobi symbol** is defined as

$$\left(\frac{-1}{q}\right) \equiv \left(\frac{-1}{p}\right)^r.$$

This symbol comes into play in the following elementary count of the sizes of the unit circles.

Lemma 1. *Let $S_{b,q}$, $S_{r,q}$, and $S_{g,q}$ be the unit circles in the blue, red, and green geometries respectively over the field $\mathbb{F}_q$. Then*

$$|S_{g,q}| = q - 1 \qquad |S_{r,q}| = q - 1 \quad \text{and} \quad |S_{b,q}| = q - \left(\frac{-1}{q}\right).$$

In particular the natural numbers $|S_{g,q}|$, $|S_{r,q}|$, and $|S_{b,q}|$ when regarded as elements of the field $\mathbb{F}_q$ are never zero.

Note that while we naturally consider the blue Euclidean geometry to be primary, we list the results in the order green, red, and blue which we will see generally aligns with the natural increasing complexity of formulas.

Now consider the linear space $\mathrm{Pol}_2(\mathbb{F}_q)$ of polynomials in two variables α and β with coefficients in $\mathbb{F}_q$, which we will introduce in terms of variants called *polynumbers* which have been used by Wildberger [51] and allow us more clearly to distinguish between polynomials as algebraic objects and as functions.

Polynumbers can be evaluated as functions, but their definition is solely in terms

of an array of coefficients, and so in the context of polynumbers, the monomials $\alpha^k\beta^l$ as k and l range over all natural numbers (including 0) are independent. We will adopt the convention that $\alpha^0\beta^0 = \mathbf{1}$ represents the constant polynumber whose value as a function is identically $1 = 1_q$ in $\mathbb{F}_q$.

For c one of b, r, or g, define the $\mathbb{F}_q$-valued **Fourier summation functional**

$$\psi_{c,q} : \mathrm{Pol}_2(\mathbb{F}_q) \to \mathbb{F}_q$$

to be the linear functional whose value on a monomial $\alpha^k\beta^l$ for natural numbers k and l is given by

$$\psi_{c,q}\left(\alpha^k\beta^l\right) \equiv \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} x^k y^l$$

where we treat the integer $|S_{b,q}|$ as being an element of $\mathbb{F}_q$. By Lemma 1 above, $|S_{c,q}| \neq 0$ in $\mathbb{F}_q$ and thus the expression is well-defined. We then may more specifically write down the individual formulas for the green, red, and blue Fourier summation functionals as

$$\begin{aligned}
\psi_{g,q}\left(\alpha^k\beta^l\right) &= -\sum_{[x,y]\in S_{g,q}} x^k y^l \\
\psi_{r,q}\left(\alpha^k\beta^l\right) &= -\sum_{[x,y]\in S_{r,q}} x^k y^l \\
\psi_{b,q}\left(\alpha^k\beta^l\right) &= -\left(\frac{-1}{q}\right) \sum_{[x,y]\in S_{b,q}} x^k y^l.
\end{aligned} \tag{1.4}$$

We will show that $\psi_{c,q}$ satisfies the following three conditions which we state loosely here to avoid getting too technical, namely:

(Normalisation) For the polynumber $\mathbf{1}$ in $\mathrm{Pol}_2(\mathbb{F}_q)$ we have that $\psi_{c,q}(\mathbf{1}) = 1_q$

(Locality) For any polynumber f that as a polynomial function restricts to zero on the circle $S_{c,q}$ we have that $\psi_{c,q}(f) = 0$

(Invariance) $\psi_{c,q}$ is invariant under any linear transformation that preserves the bilinear form of the associated geometry c.

These conditions will be presented in a more precise manner in Chapter 4 after a prior discussion of the associated isometry groups. We call any linear functional satisfying the three conditions above a **circular integral functional** on $\mathrm{Pol}_2(\mathbb{F}_q)$ with respect to $S_{c,q}$. A first main theorem is the following.

Theorem 1. *The linear functional $\psi_{c,q}$ is the unique circular integral functional on $\mathrm{Pol}_2(\mathbb{F}_q)$ with respect to the unit circle $S_{c,q}$ in the green, red, and blue geometries over $\mathbb{F}_q$.*

We prove this by first considering a linear functional on the space $\mathbb{F}_q^{\mathbb{A}}$ of functions from the affine plane $\mathbb{A}$ to $\mathbb{F}_q$ that satisfies similar Normalisation, Locality, and Invariance conditions as prescribed above. We establish that this linear functional exists and is unique, and then use that to establish uniqueness of $\psi_{c,q}$ as the circular integral functional on $\mathrm{Pol}_2(\mathbb{F}_q)$ with respect to the unit circle $S_{c,q}$.

Moreover, we also determine an explicit formula of $\psi_{c,q}$ in each geometry. The derivation of the formula for $\psi_{c,q}$ in the blue geometry when -1 is a square can be established from that in the red geometry, which stems from that in the green geometry.

In the blue geometry where -1 is not a square, things run a bit differently and we utilise another approach, involving the quadratic extension field of $\mathbb{F}_q$ coming from the blue complex numbers in this case. This argument is more akin to classical Fourier analysis arguments in the characteristic zero case, but curiously the obtained formula is similar to that in the blue geometry when -1 is a square and the red geometry.

More precisely, we will show that we can describe the circular integral functionals $\psi_{r,q}$ and $\psi_{b,q}$ in terms of the circular super Catalan numbers reduced modulo p, namely

$$\begin{aligned}\Omega(m,n) \bmod p &= \frac{S(m,n)}{4^{m+n}} \bmod p \\ &= \frac{(2m)!\,(2n)!}{4^{m+n} m!n!\,(m+n)!} \bmod p\end{aligned}$$

where p is the characteristic of the underlying field. These are elements of $\mathbb{F}_p$ which we can think of as being embedded in $\mathbb{F}_q$. They are well-defined since $S(m,n)$ is always an integer and the term 4^{m+n} in the denominator is never a multiple of p.

Here is a simplified and restricted version of the formulas for $\psi_{c,q}$ in the red and blue geometries. This is the heart of our understanding of the true significance of the super Catalan numbers, and their rational cousins the circular super Catalan numbers. Note the similarity between the two formulas, with the only difference being the occurrence of an extra factor $(-1)^n$ in the formula for $\psi_{r,q}$.

Theorem 2. *Consider the finite field $\mathbb{F}_q$ of size $q = p^r$ for some prime $p > 2$ and positive integer r.*

1. *In the red geometry, for $0 \leq k + l < q - 1$,*

$$\psi_{r,q}\left(\alpha^k \beta^l\right) = \begin{cases} (-1)^n \Omega(m,n) \bmod p & \text{if } k = 2m \text{ and } l = 2n \\ 0 & \text{otherwise.} \end{cases}$$

2. In the blue geometry, for $0 \leq k+l < q-1$,

$$\psi_{b,q}\left(\alpha^k\beta^l\right) = \begin{cases} \Omega(m,n) \bmod p & \text{if } k=2m \text{ and } l=2n \\ 0 & \text{otherwise.} \end{cases}$$

Here are some immediate consequences.

Corollary 2.1. *Consider the finite field* $\mathbb{F}_q$ *of size* $q=p^r$ *for some prime* $p>2$ *and positive integer* r. *Let* k *and* l *be two natural numbers satisfying* $k+l<q-1$.

1. *The normalised sums* $\psi_{r,q}\left(\alpha^k\beta^l\right)$ *and* $\psi_{b,q}\left(\alpha^k\beta^l\right)$ *lie in the prime field* $\mathbb{F}_p$ *and are independent of the power* r *of* p.

2. *Suppose* $l=2n$. *We then have* $\psi_{r,q}\left(\alpha^k\beta^l\right) = (-1)^n \psi_{b,q}\left(\alpha^k\beta^l\right)$.

3. *If* k *and* l *are both even, then* $\psi_{r,q}\left(\alpha^k\beta^l\right)$ *and* $\psi_{b,q}\left(\alpha^k\beta^l\right)$ *are never* 0.

However to us it is even more remarkable that the single rational number $\Omega(m,n)$ determines the values $\psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right)$ and $\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right)$ for all prime powers $q > 2(m+n)+1$ in such a direct and uniform fashion. Here is an example to illustrate these formulas.

Example 1. *Consider the Euclidean (blue) geometry in the case* $q=p=13$, *so that we can identify* $\mathbb{F}_{13}$ *as* $\{0,1,2,\ldots,12\}$. *Here,* $-1=12=5^2$ *is a square, so* $\left(\frac{-1}{q}\right)=1$. *From Theorem 2, if* $0 \leq 2(m+n) < q-1=12$ *then*

$$\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right) = \Omega(m,n) \bmod 13.$$

The (blue) unit circle is, in this case,

$$S_{b,13} = \left\{ \begin{array}{cccccc} [1,0] & [12,0] & [0,1] & [0,12] & [2,6] & [2,7] \\ [11,6] & [11,7] & [6,2] & [7,2] & [6,11] & [7,11] \end{array} \right\}$$

where there is no need for commas as the points are not naturally ordered.

Here are two pictures of $S_{b,13}$ *in the affine plane, where by the affine plane we mean a square array of boxes with horizontal and vertical positions labeled using elements in* $\mathbb{F}_{13}$, *and a point is represented by a single box in the affine plane. The left configuration below assumes a labelling from* 0 *to* 12, *while the right one uses the numbers* $-6,-5,\ldots,5,6$, *where we identify* -1 *by* 12 *and so on. This follows from Wildberger's approach in [50].*

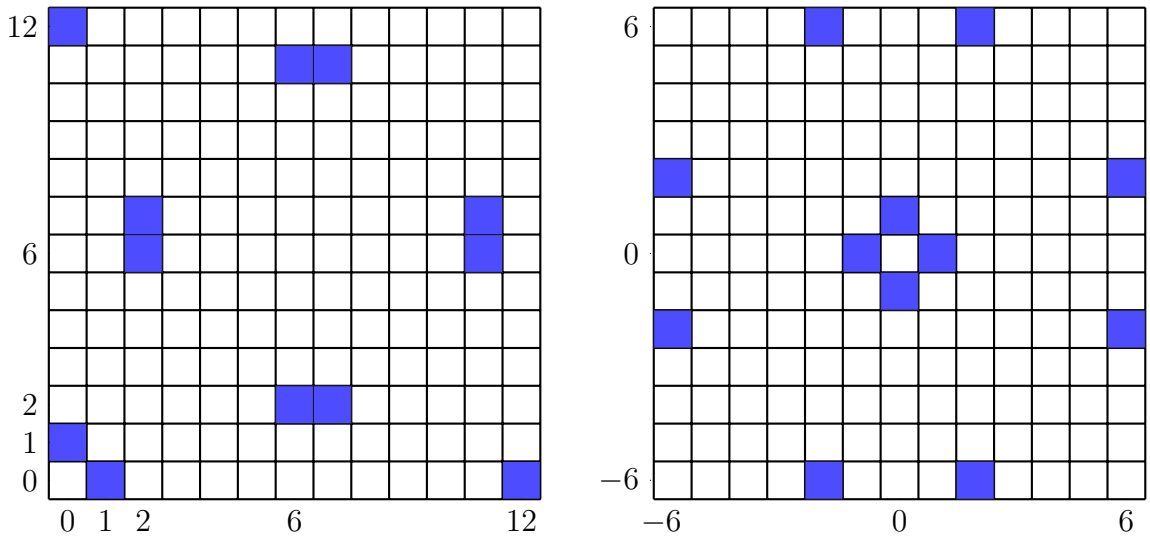

Figure 1.1: The blue unit circle $S_{b,13}$ in two different configurations.

By manual inspection, working over $\mathbb{F}_{13}$ *and omitting the zero terms,*

$$\psi_{b,13}\left(\alpha^4\right) = -\left(\frac{-1}{q}\right)\sum_{[x,y]\in S_{b,13}} x^4 = -\sum_{[x,y]\in S_{b,13}} x^4$$

which evaluates to $-\left(1^4+12^4+2^4+2^4+11^4+11^4+6^4+7^4+6^4+7^4\right)=2$. *Using the formula of Theorem 2, we may verify that*

$$\psi_{b,11}\left(\alpha^4\right) = \Omega(2,0) \bmod 13 = \frac{3}{8} \bmod 13 = 2.$$

Similarly

$$\begin{aligned}
\psi_{b,13}\left(\alpha^2\beta^6\right) &= -\left(\frac{-1}{q}\right)\sum_{[x,y]\in S_{b,13}} x^2y^6 \\
&= -\sum_{[x,y]\in S_{b,13}} x^2y^6 \\
&= -\left(2^26^6+2^27^6+11^26^6+11^27^6+6^22^6+7^22^6+6^211^6+7^211^6\right) \\
&= 4
\end{aligned}$$

and again using the formula we verify that

$$\psi_{b,13}\left(\alpha^2\beta^6\right) = \Omega(1,3) \bmod 13 = \frac{5}{128} \bmod 13 = 4.$$

For the example above, the values $\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right)$ are recorded for $0 \le m,n < 10$ in the following table. Note that they are indeed all non-zero, at least when $m+n < \frac{1}{2}(q-1) = 6$, in accordance with Corollary 2.1.

$\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right) : m\backslash n$	0	1	2	3	4	5	6	7	8
0	1	7	2	6	2	7	3	7	2
1	7	5	9	4	8	4	9	5	9
2	2	9	5	9	4	8	4	9	5
3	6	4	9	5	9	4	8	4	9
4	2	8	4	9	5	9	4	8	4
5	7	4	8	4	9	5	9	4	8
6	3	9	4	8	4	9	5	9	4
7	7	5	9	4	8	4	9	5	9
8	2	9	5	9	4	8	4	9	5

Table 3: The values of $\psi_{b,11}\left(\alpha^{2m}\beta^{2n}\right)$ for $0 \leq m, n < 9$.

Correspondingly, here are the values of the circular super Catalan numbers in the same range, reduced mod 13.

$\Omega(m,n) \bmod 13 : m\backslash n$	0	1	2	3	4	5	6	7	8
0	1	7	2	6	2	7	1	0	0
1	7	5	9	4	8	6	1	0	0
2	2	9	5	9	2	5	1	0	0
3	6	4	9	7	10	4	1	0	0
4	2	8	2	10	6	3	1	0	0
5	7	6	5	4	3	2	1	0	6
6	1	1	1	1	1	1	1	7	7
7	0	0	0	0	0	0	7	0	0
8	0	0	0	0	0	6	7	0	0

Table 4: The values of $\Omega(m,n) \bmod 13$ for $0 \leq m, n < 9$.

So while we see that there is indeed agreement between the circular super Catalan numbers and the summations $\psi_{b,11}\left(\alpha^{2m}\beta^{2n}\right)$, this generally holds in the range we

have stipulated, namely $m+n<\frac{q-1}{2}=6$, which we may call the upper triangular range. In fact we cannot in general expect the circular super Catalan numbers beyond the upper triangular range to determine the summation values, as the numerators of the super Catalan numbers generally contain large factorials which will become 0 modulo any finite prime p beyond some point. However for fixed m and n all but finitely many prime powers q will satisfy the upper triangular range condition.

The complete formulas for the red and blue geometries which go beyond this constraint are more involved but still quite attractive, and they point towards an additional family of integers that extend the super Catalan numbers. These formulas are given in terms of sums of particular coefficients of the rational polynumbers

$$\pi_{k,l}=\pi_{k,l}(\alpha)\equiv\left(\frac{1+\alpha}{2}\right)^{k}\left(\frac{1-\alpha}{2}\right)^{l}$$

which we will call the **circular polynumbers**, suitably reduced mod p. We use the convention that for a polynumber π in α, the expression $[\alpha^{m}]\,\pi$ denotes the coefficient of α^{m} in π, and allow ourselves to write

$$[\alpha^{m_1}]\,\pi+[\alpha^{m_2}]\,\pi+\cdots+[\alpha^{m_l}]\,\pi=\left(\sum_{i=1}^{l}[\alpha^{m_i}]\right)\pi.$$

The key point that connects these circular polynumbers and the super Catalan numbers is the result of Georgiadis, Munemasa, and Tanaka in [18]. In their paper, the super Catalan numbers are presented as the evaluation of a family of polynomials (or polynumbers, as we call them) called the Krawtchouk polynumbers at some integers. We present the following restatement of their theorem, in terms of the circular super Catalan numbers and the polynumbers $\pi_{k,l}$ rather than Krawtchouk polynumbers, and also offer an independent proof.

Theorem 3 (Georgiadis, Munemasa, and Tanaka)**.** *For any natural numbers m and n, we have that*

$$\Omega(m,n)=(-1)^{n}\left[\alpha^{m+n}\right]\pi_{2m,2n}.$$

We now give the complete summation formulas for $\psi_{c,q}$ in each geometry; these will make separate appearances in Theorems 18, 19, and 24 respectively. The formulas involve a constant w that depends on the size of the unit circle in each geometry, along with associated constants $R_{k,l}$ which depend also on natural numbers k and l. Recall that if x is a rational number, then the symbol $\lfloor x\rfloor$ represents the usual floor function, namely the greatest integer less than or equal to x.

Theorem 4. *Consider the finite field $\mathbb{F}_q$ where $q=p^r$ for some prime $p>2$ and positive integer r.*

1. In the green geometry,

$$\psi_{g,q}\left(\alpha^k\beta^l\right) = \begin{cases} 1_q & \text{if } |S_{g,q}| \mid (k-l) \\ 0 & \text{otherwise.} \end{cases}$$

2. In the red geometry, with $w \equiv \frac{1}{2}|S_{r,q}|$ *and* $R = R_{k,l} \equiv \left\lfloor \frac{k+l}{|S_{r,q}|} \right\rfloor$,

$$\psi_{r,q}(\alpha^k\beta^l) = \begin{cases} \left(\sum_{|d|\leq R} \left[\alpha^{m+n+dw}\right]\right) \pi_{k,l} \bmod p & \text{if } k = 2m,\ l = 2n \\ 0 & \text{otherwise.} \end{cases}$$

3. In the blue geometry, with $w \equiv \frac{1}{2}|S_{b,q}|$ *and* $R = R_{k,l} \equiv \left\lfloor \frac{k+l}{|S_{b,q}|} \right\rfloor$,

$$\psi_{b,q}(\alpha^k\beta^l) = \begin{cases} \left(\sum_{|d|\leq R} \left[\alpha^{m+n+dw}\right]\right) (-1)^n \pi_{k,l} \bmod p & \text{if } k = 2m,\ l = 2n \\ 0 & \text{otherwise.} \end{cases}$$

We see that our main formulas to evaluate $\psi_{r,q}(\alpha^k\beta^l)$ and $\psi_{b,q}(\alpha^k\beta^l)$ involve an equally-spaced ladder of coefficients of $\pi_{k,l}$ or $-\pi_{k,l}$ symmetrically placed around the central coefficient, which is the circular super Catalan number $\Omega(m,n)$ when $k = 2m$ and $l = 2n$, and is zero otherwise. In the following examples, we will evaluate $\psi_{b,q}$ at $\alpha^8\beta^2$ over two different fields $\mathbb{F}_{13}$ and $\mathbb{F}_7$. Here $k = 8$ and $l = 2$ are both even, so $m = 4$ and $n = 1$. Both computations require us to find certain coefficients of the (rational) polynumber

$$(-1)^n \pi_{k,l} = -\pi_{8,2} = -\left(\frac{1+\alpha}{2}\right)^8 \left(\frac{1-\alpha}{2}\right)^2$$

which, upon expansion, is equal to

$$-\frac{1}{1024}\left(1 + 6\alpha + 13\alpha^2 + 8\alpha^3 - 14\alpha^4 - 28\alpha^5 - 14\alpha^6 + 8\alpha^7 + 13\alpha^8 + 6\alpha^9 + \alpha^{10}\right).$$

Note that the expression is palindromic around the central term involving α^5, and that the coefficient of that term is, in agreement with Georgiadis, Munemasa, and Tanaka, the circular super Catalan number $\frac{7}{256} = \Omega(4,1)$.

Example 2. *Continuing our previous example where* $q = p = 13$*, we deduce that*

$|S_{b,13}| = 12$ *so that* $w = \frac{1}{2}|S_{b,13}| = 6$ *and* $R = \left\lfloor \frac{k+l}{|S_{b,13}|} \right\rfloor = \left\lfloor \frac{10}{12} \right\rfloor = 0$. *The formula for* $\psi_{b,q}$ *in Theorem 4 above then reads*

$$\psi_{b,13}(\alpha^8\beta^2) = \left(\sum_{|d|\leq 0} \left[\alpha^{5+6d}\right] \right) (-\pi_{8,2}) \bmod 13 = \left[\alpha^5\right] (-\pi_{8,2}) \bmod 13$$
$$= \frac{7}{256} \bmod 13 = 8.$$

Note that the condition $0 \leq k + l < q - 1$ *reduces the sum to just the central term.*

Example 3. *Now consider the corresponding formula when* $q = p = 7$. *In this case,* -1 *is not a square so according to Lemma 1,* $w = \frac{1}{2}|S_{b,7}| = 4$ *and* $R = \left\lfloor \frac{k+l}{|S_{b,7}|} \right\rfloor = \left\lfloor \frac{2+8}{8} \right\rfloor = 1$. *It follows that*

$$\begin{aligned}\psi_{b,7}(\alpha^8\beta^2) &= \left(\sum_{|d|\leq 1} \left[\alpha^{5+4d}\right] \right) (-\pi_{8,2}) \bmod 7 \\ &= \left(\left[\alpha^1\right] + \left[\alpha^5\right] + \left[\alpha^9\right] \right) (-\pi_{8,2}) \bmod 7 \\ &= \left(-\frac{3}{512} + \frac{7}{256} - \frac{3}{512} \right) \bmod 7 = \frac{1}{64} \bmod 7 = 1.\end{aligned}$$

It can be verified that

$$S_{b,7} = \Big\{ [1,0] \;\; [6,0] \;\; [0,1] \;\; [0,1] \;\; [2,2] \;\; [5,5] \;\; [2,5] \;\; [5,2] \Big\}$$

and we can check directly by working modulo 7 *that*

$$\psi_{b,7}(\alpha^2\beta^8) = 2^2 2^8 + 5^2 5^8 + 2^2 5^8 + 5^2 2^8 = 1.$$

1.2 Connection to traditional integration theory over the unit circle

The theory of integrating polynomials on a sphere, even in higher dimensions, dates back at least to the paper of Baker [2]. Later, Folland [17] offered a shorter way of computing the integral of a polynomial over a sphere, and both Baker's and Folland's formulas utilise the gamma function Γ. Here we restate the main theorem in Folland's paper, without proof, involving the usual rotationally invariant measure $d\mu$ on the $(d-1)$-dimensional unit sphere in $\mathbb{R}^d$ coming from the usual Riemannian structure on $\mathbb{R}^d$.

Theorem 5. *Let* $S^{d-1} = \left\{[x_1, x_2, \ldots, x_d] \in \mathbb{R}^d \ : \ x_1^2 + x_2^2 + \cdots + x_d^2 = 1\right\}$. *We have that*

$$\int_{S^{d-1}} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d} \ d\mu = \frac{2\Gamma\left(b_1\right)\Gamma\left(b_2\right)\cdots\Gamma\left(b_d\right)}{\Gamma\left(b_1 + b_2 + \cdots + b_d\right)}$$

if all the natural numbers a_i *are even with* $b_i = \frac{1}{2}\left(a_i + 1\right)$, *and is zero otherwise.*

In a paper separate from this thesis, we will show that algebraic reformulations of the classical formulas of Baker and Folland for integrating polynomials over spheres can be obtained without reference to the transcendental function Γ and the irrational number π. We do this by initiating a new algebraic theory of integration on spheres which avoids classical measure theory entirely, does not rely on limit processes or real numbers, and allows us to realise the circular super Catalan numbers and additional variants and generalisations as encoding fundamental integral formulas for polynomials over circles and spheres in general characteristic zero fields.

In the two-dimensional case we will see that the integrals we obtain over the Euclidean circle can be algebraically expressed using the circular super Catalan numbers. Moreover, such integrals yield formulas which are essentially identical to the ones obtained in this thesis in the finite field case.

To see how Folland's classical formula might be restated without reference to irrationalities, we may make the following manipulations in the case $d = 2$ and $a_1 = 2m$, $a_2 = 2n$ in Theorem 5:

$$\begin{aligned}
\frac{2\Gamma\left(b_1\right)\Gamma\left(b_2\right)}{\Gamma\left(b_1 + b_2\right)} &= \frac{2\Gamma\left(m + \frac{1}{2}\right)\Gamma\left(n + \frac{1}{2}\right)}{\Gamma\left(m + n + 1\right)} \\
&= \frac{2\left(m - \frac{1}{2}\right)\left(m - \frac{3}{2}\right)\cdots\left(\frac{3}{2}\right)\left(\frac{1}{2}\sqrt{\pi}\right)\left(n - \frac{1}{2}\right)\left(n - \frac{3}{2}\right)\cdots\left(\frac{3}{2}\right)\left(\frac{1}{2}\sqrt{\pi}\right)}{(m+n)!} \\
&= \frac{2\pi\left((2m-1)\times(2m-3)\times\cdots\times 1\right)\left((2n-1)\times(2n-3)\times\cdots\times 1\right)}{2^{m+n}\,(m+n)!} \\
&= \frac{2\pi\,(2m)!\,(2n)!}{4^{m+n} m!n!\,(m+n)!} \\
&= 2\pi\Omega(m,n).
\end{aligned}$$

Then a renormalisation of the invariant measure allows us to summarise the above calculation as the following restatement of the classical result:

Theorem 6. *If the rotationally invariant measure* $d\mu$ *on the (Euclidean) unit circle* S^1 *is normalised, so that*

$$\int_{S^1} d\mu = 1,$$

then we have that

$$\int_{S^1} x_1^{a_1} x_2^{a_2} \, d\mu = \begin{cases} \Omega(m,n) & \text{if } a_1 = 2m,\ a_2 = 2n \\ 0 & \text{otherwise.} \end{cases} \tag{1.5}$$

This formula is strikingly similar to the formula of $\psi_{b,q}$ presented in Theorem 2. Note that the values of the integral sit in the prime subfield $\mathbb{Q}$ of $\mathbb{R}$. One may compare this to the result from Corollary 2.1 and subsequently Theorem 4 that we established earlier: the values of the Fourier summation functional always sit in the prime subfield $\mathbb{F}_p$ of $\mathbb{F}_q$. While our derivation of the formula (1.5) above utilises the classical formula of Folland, the analysis presented in this thesis will highlight the key idea in establishing a completely algebraic approach for the theory of polynumber integration over the unit circle in fields of characteristic zero. In a paper separate from this thesis, we will carry out such a program to obtain an integration theory for polynumbers over the unit circle in the rational plane purely algebraically, without a prior theory of real numbers or transcendental functions.

Finally, we wish to emphasise that while there is something combinatorial about the connection between the super Catalan numbers (and their circular variants) with summations over the unit circles over finite fields of odd characteristic, the broader picture that we obtain shows that their real significance is *algebraic* and *analytic* at the same time. We are obtaining here formulas which ought to be at the heart of *modular Fourier analysis* over general fields, where we study not complex-number-valued functions on a circle or a sphere, but rather functions taking values in the field over which the circle or sphere is defined, or possibly finite extensions of it.

1.3 Outline of the thesis

We conclude our introduction by giving the organisation of the thesis. In Chapter 2, we will carefully define an alternative notion of polynomials which we call polynumbers and separate them from polynomial functions. We then consider various group actions on the relevant spaces in this thesis, followed by a more comprehensive literature review on the super Catalan numbers. We will also introduce the Krawtchouk polynumbers and matrices, establish several key properties for them, and define a family of rational numbers which we call the circular super Catalan numbers, as well as a family of polynumbers called the circular polynumbers.

We proceed by introducing the key idea of chromogeometry in Chapter 3. We do this by first defining the ambient space in which we carry our analysis, called the dihedron algebra, and introduce three subalgebras of complex numbers as well as the three geometries of which chromogeometry is an aspect. The three geometries

consist of the Euclidean geometry and two relativistic geometries. We will set up the notion of unit circle in each geometry and the rotation groups which then act on various spaces established in Chapter 2. We conclude Chapter 3 by giving the connection between the unit circle and the rotation group in each geometry.

In Chapter 4, we will introduce our notion of algebraic integral over the unit circle, which is motivated by the traditional Riemann integral. In this key chapter we establish the existence and uniqueness of such a circular integral functional with respect to a unit circle in all three geometries.

This is followed by an explicit formula for the circular integral functional in each geometry in Chapter 5. Here chromogeometry will be the key to linking the various formulas in the different geometries. However one of the cases of the blue geometry will require a distinctly different treatment which utilises the blue complex numbers as a field extension of our finite field and some cyclic symmetry occurring in the associated unit circle.

Finally, in Chapter 6 we will offer a more efficient and practical way of computing the circular integral functional, which we call the Fourier Summation Procedure. This is then followed by establishing several identities for the circular super Catalan numbers coming from finite difference calculus and observations that go back to Leibniz. Some potential future research directions are given in Chapter 7.

Chapter 2

Preliminary Theory

We begin this chapter by quickly summarising basic results in finite field theory, which we assume to be familiar to the reader. A field $\mathbb{F}$ is a set equipped with two binary operations $+$ and $\times$ such that $(\mathbb{F}, +)$ is an abelian group with identity 0, $(\mathbb{F} - \{0\}, \times)$ is an abelian group with identity $1_{\mathbb{F}}$, and the distributive property holds.

A set $K \subseteq \mathbb{F}$ is called a **subfield** of K if K itself is a field under the operations $+$ and $\times$ inherited from $\mathbb{F}$. We denote the multiplicative group $\mathbb{F} - \{0\}$ of $\mathbb{F}$ by $\mathbb{F}^{\times}$. For $a, b \in \mathbb{F}$, we shall write $a \times b$ more succinctly as ab and the notation $\frac{a}{b}$ shall mean ab^{-1} provided that b is not zero.

The characteristic of a field $\mathbb{F}$ is the least positive integer p such that

$$p1_{\mathbb{F}} = \underbrace{1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{p \text{ times}} = 0$$

and if no such p exists we set $p = 0$. The characteristic of a field is either zero or a prime number. A finite field is necessarily of prime characteristic $p > 0$, and the cardinality of such a field is p^r for some positive integer r. Any field of prime characteristic p has a subfield K consisting of p elements, and we call any field consisting of p elements a prime field.

An example of a field of characteristic zero is the field of rational numbers $\mathbb{Q}$, while an example of a field of characteristic $p > 0$ is obtained from the integers modulo p denoted by $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. A fundamental result in finite field theory is that up to isomorphism, there is one and only one finite field of size p^r for each prime p and positive integer r. We will henceforth write $\mathbb{F} = \mathbb{F}_q$ when referring to *the* finite field of size $q = p^r$. Note that this means we will be identifying $\mathbb{Z}/p\mathbb{Z}$ with $\mathbb{F}_p$.

Here are some further properties of finite fields that will be used in this thesis.

Proposition 1. *Let $q = p^r$ for some prime p and positive integer r.*

1. *$\mathbb{F}_{p^r}$ is (isomorphic to) a subfield of $\mathbb{F}_{p^s}$ precisely when $r \mid s$.*

2. *The group $\mathbb{F}_q^\times$ is cyclic of order $q-1$. As a result, for any $x \in \mathbb{F}_q$ we have $x^q = x$. This will be referred as the* ***Fermat property****.*

3. *$(x+y)^p = x^p + y^p$ for any $x, y \in \mathbb{F}_q$.*

Since we are dealing here with finite mathematics and finite arithmetic, we propose to dispense with the usual reliance on "infinite sets". Throughout this thesis, $\mathbb{N}$ denotes the type of natural numbers which for us includes the number 0, $\mathbb{Z}$ denotes the type of integers, $\mathbb{Q}$ denotes the type of rational numbers, and $\mathbb{F}_q$ denotes the finite field of size q where q is a power of an odd prime p.

We aim for this to be in line with what a computer would do: recognising when an expression that it meets is of a given type, without having to rely on prior databases. In some places, we will indicate the multiplicative identity in $\mathbb{F}_q$ by 1_q instead of just 1 if there is a possibility of confusion. Any integer m then can be regarded as an element of $\mathbb{F}_q$ via the embedding $m \mapsto m1_q$. We also use the convention that $0^0 = 1$.

2.1 Polynumbers and polynomials over finite fields

It will be useful to clarify the subtle difference between polynomials, over a general field $\mathbb{F}$, as formal expressions and as functions. In characteristic zero this distinction can often be finessed, but when working with finite fields it pays to be rather precise and keep the notions carefully separate, as we shall see.

To make this distinction explicit we will introduce a more fundamental computational object called a polynumber, which takes the coefficient list of a classical polynomial as primary. This terminology and approach has been promoted by Wildberger in his *MathFoundations* playlist on YouTube [51], although it will be close to the way computer scientists have traditionally worked with polynomials by using linked lists, see for example [24] and [40].

Evaluation associates to a polynumber a polynomial function, but over a finite field $\mathbb{F}_q$ different polynumbers may give rise to the same function. Specifically we will see that if two polynumbers π_1 and π_2 satisfy the equality $\pi_1(t) = \pi_2(t)$ for all $t \in \mathbb{F}_q$, then they are not necessarily equal as polynumbers.

At a glance this might seem like polynumbers are just polynomials as formal expressions, but we shall see that the construction of polynumbers does not require us to have a notion of formal symbols or variables to adjoin to the underlying field, and in fact the variable is suppressed when dealing with polynumbers.

Here is the definition: a **polynumber** π over a field $\mathbb{F}$ is a (finite) list of numbers in $\mathbb{F}$ written vertically with a bar above it and another one to the left, as in

$$\pi = \left|\overline{\begin{array}{l} u_0 \\ u_1 \\ \vdots \\ u_k \end{array}}\right. .$$

We call the numbers u_i the **entries** of π. Two polynumbers π_1 and π_2 are equal precisely when one can be obtained from the other by adding or removing zeroes from the bottom. For example,

$$\left|\overline{\begin{array}{l} 3 \\ 0 \\ -1 \\ 2 \end{array}}\right. = \left|\overline{\begin{array}{l} 3 \\ 0 \\ -1 \\ 2 \\ 0 \end{array}}\right. .$$

The **zero polynumber** and the **identity polynumber** are respectively

$$\mathbf{0} \equiv \left|\overline{0}\right. \qquad \text{and} \qquad \mathbf{1} \equiv \left|\overline{1}\right. .$$

If k is the largest natural number such that $u_k \neq 0$ then $k \equiv \deg(\pi)$ is called the **degree** of the polynumber π. Addition of polynumbers is defined entry-wise, adding zeroes at the bottom to make two polynumbers have the same number of entries if necessary. The scalar product of a polynumber π by a number $\lambda \in \mathbb{F}$ is also entry-wise.

Given two polynumbers

$$\pi_1 = \left|\overline{\begin{array}{l} u_{10} \\ u_{11} \\ \vdots \\ u_{1k} \end{array}}\right. \qquad \text{and} \qquad \pi_2 = \left|\overline{\begin{array}{l} u_{20} \\ u_{21} \\ \vdots \\ u_{2l} \end{array}}\right.$$

of degree k and l respectively, the product of π_1 and π_2 is another polynumber π (of degree $k + l$) given by

$$\pi = \pi_1\pi_2 \equiv \left|\overline{\begin{array}{c} u_0 \\ u_1 \\ \vdots \\ u_{k+l} \end{array}}\right.$$

so that for $0 \leq m \leq k+l$,

$$u_m = \sum_{i+j=m} u_{1i}u_{2j}.$$

This is the familiar Cauchy product of sequences. We denote the algebra of polynumbers over $\mathbb{F}$ by $\mathrm{Pol}(\mathbb{F})$.

We now proceed by defining the special polynumber

$$\alpha \equiv \left|\overline{\begin{array}{c} 0 \\ \\ 1 \end{array}}\right. .$$

A **polynomial** in α is a polynumber written as a linear combination of powers of the polynumber α, where for $k \in \mathbb{N}$, α^k will be a list of k zeroes followed by a single 1, with $\alpha^0 = \mathbf{1}$. For example, if

$$\pi = \left|\overline{\begin{array}{c} 2 \\ \frac{1}{2} \\ 0 \\ \frac{1}{3} \\ -3 \end{array}}\right.$$

is a polynumber over $\mathbb{Q}$, then

$$\pi = 2\left|\overline{\begin{array}{c} 1 \end{array}}\right. + \frac{1}{2}\left|\overline{\begin{array}{c} 0 \\ \\ 1 \end{array}}\right. + 0\left|\overline{\begin{array}{c} 0 \\ 0 \\ 1 \end{array}}\right. + \frac{1}{3}\left|\overline{\begin{array}{c} 0 \\ 0 \\ 0 \\ 1 \end{array}}\right. - 3\left|\overline{\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{array}}\right. = 2\alpha^0 + \frac{1}{2}\alpha^1 + 0\alpha^2 + \frac{1}{3}\alpha^3 - 3\alpha^4$$

which we will write more informally as

$$\pi = 2 + \frac{1}{2}\alpha + \frac{1}{3}\alpha^3 - 3\alpha^4.$$

If $\pi = u_0\alpha^0 + u_1\alpha + \cdots + u_k\alpha^k \in \mathrm{Pol}(\mathbb{F})$ is a general polynomial in α, then u_k is called the **coefficient** of α^k in π and the extraction of such a coefficient is denoted by

$$u_k = \left[\alpha^k\right]\pi.$$

When we are interested in taking the sum of multiple coefficients of π, say corresponding to positions $k_1, k_2, \ldots, k_l$, then we will write

$$\left(\sum_{i=1}^{l}\left[\alpha^{k_i}\right]\right)\pi \equiv \left[\alpha^{k_1}\right]\pi + \cdots + \left[\alpha^{k_l}\right]\pi.$$

We also define the **evaluation** of $\pi \equiv u_0 + u_1\alpha + \cdots + u_k\alpha^k$ at $t \in \mathbb{F}$ to be

$$\pi(t) \equiv u_0 + u_1 t + \cdots + u_k t^k \in \mathbb{F}$$

and call $\pi(t)$ a **polynomial function**. From this point henceforth, we will refer to polynomials in α as simply polynumbers so that they are not confused with polynomial functions. We will introduce a more formal way of defining evaluation also in the next section.

A polynumber $\pi \in \mathrm{Pol}(\mathbb{F})$ is **irreducible** over $\mathbb{F}$ precisely when π cannot be written as a product of two polynumbers whose degrees are strictly less than that of π. Recall that for a given $q = p^r$, we can construct a finite field of size q as follows, using an irreducible polynumber with leading coefficient 1 of degree r, say $\pi = u_0 + u_1\alpha + \cdots + u_{r-1}\alpha^{r-1} + \alpha^r \in \mathrm{Pol}(\mathbb{F}_p)$.

Consider the set

$$\left\{ c_0 + c_1\alpha + \cdots + c_{r-1}\alpha^{r-1} \in \mathrm{Pol}(\mathbb{F}_p) \right\}$$

with addition defined as usual, and multiplication defined modulo π; that is, we replace every occurrence of α^r by $-(u_0\alpha^0 + u_1\alpha^1 + \cdots + u_{r-1}\alpha^{r-1})$. It can be verified that this yields a field of size p^r, and since there is only one finite field of size p^r up to isomorphism, the choice of π does not matter.

In a similar fashion we can define a 2-**polynumber** over $\mathbb{F}$ (or a bi-polynumber, also introduced by Wildberger in [52]) to be a two-dimensional array of numbers in $\mathbb{F}$ of the form

$$\pi \equiv \left|\overline{\begin{array}{cccc} u_{00} & u_{01} & \cdots & u_{0n} \\ u_{10} & u_{11} & \cdots & u_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m0} & u_{m1} & \cdots & u_{mn} \end{array}}\right| .$$

Again we adopt the convention that adding further zeroes to the right and/or down leaves the 2-polynumber unchanged.

Addition, subtraction, and scalar multiplication of such 2-polynumbers are pointwise, forming a vector space over $\mathbb{F}$. Multiplication of 2-polynumbers is defined by the two-dimensional version of the Cauchy product, so that for example

$$\left|\overline{\begin{array}{cc} 1 & 2 \\ 3 & -1 \end{array}}\right| \times \left|\overline{\begin{array}{cc} 5 & -1 \\ 2 & 4 \end{array}}\right| = \left|\overline{\begin{array}{ccc} 5 & 9 & -2 \\ 17 & 0 & 9 \\ 6 & 10 & -4 \end{array}}\right| . \tag{2.1}$$

Let $\mathrm{Pol}_2(\mathbb{F})$ be the algebra of 2-polynumbers over $\mathbb{F}$ with multiplicative identity $\mathbf{1} = \alpha^0\beta^0$. After we define another special polynumber

$$\beta \equiv \left|\overline{\begin{array}{cc} 0 & 1 \end{array}}\right|$$

any 2-polynumber can be written as a linear combination of powers of α and β. For example, the 2-polynumber

$$\pi \equiv \left|\overline{\begin{array}{cccc} 2 & 1 & -1 & 0 \\ 3 & 0 & 0 & 4 \\ -1 & 7 & 0 & 0 \\ 0 & 0 & 5 & 0 \end{array}}\right|$$

can be written as

$$2\alpha^0\beta^0 + 3\alpha^1\beta^0 - \alpha^2\beta^0 + \alpha^0\beta^1 + 7\alpha^2\beta^1 - \alpha^0\beta^2 + 5\alpha^3\beta^2 + 4\alpha\beta^3$$

which we may write more simply as $2 + 3\alpha - \alpha^2 + \beta + 7\alpha^2\beta - \beta^2 + 5\alpha^3\beta^2 + 4\alpha\beta^3$.

With this in mind, the algebra operations then agree with the familiar operations

on polynomials. For example, the 2-polynumber multiplication in (2.1) above corresponds to the more usual computation

$$\begin{aligned}&(1+3\alpha+2\beta-\alpha\beta)\,(5+2\alpha-\beta+4\alpha\beta)\\&=5+17\alpha+6\alpha^2+9\beta-2\beta^2+10\alpha^2\beta+9\alpha\beta^2-4\alpha^2\beta^2.\end{aligned}$$

It is important to emphasise that here and throughout α and β are *not* variables; they are just *particular polynumbers*. Clearly we may choose to regard $\mathrm{Pol}(\mathbb{F})$ as a subalgebra of $\mathrm{Pol}_2(\mathbb{F})$.

2.2 Polynumbers and functions over finite fields

Denote by $\mathbb{A} = \mathbb{A}(\mathbb{F})$ the two-dimensional affine space with entries in $\mathbb{F}$. In other words,

$$\mathbb{A} = \left\{ [x,y] \ : \ x,y \in \mathbb{F} \right\}$$

and we call $\mathbb{A}$ the **affine plane** over $\mathbb{F}$.

Moreover, denote by $\mathbb{F}^{\mathbb{A}}$ the space of functions from $\mathbb{A}$ to $\mathbb{F}$. This is a vector space over $\mathbb{F}$ with addition and scalar multiplication defined point-wise by

$$\begin{aligned}(f_1+f_2)\,([x,y]) &\equiv f_1\,([x,y]) + f_2\,([x,y])\\(\lambda f_1)\,([x,y]) &\equiv \lambda f_1\,([x,y])\end{aligned}$$

for any $f_1, f_2 \in \mathbb{F}^{\mathbb{A}}$ and $\lambda \in \mathbb{F}$. Then $\mathbb{F}^{\mathbb{A}}$ becomes an $\mathbb{F}$-algebra under the pointwise multiplication

$$(f_1 f_2)\,([x,y]) = f_1\,([x,y])\, f_2\,([x,y])\,.$$

For brevity, we shall usually write $f\,([x,y])$ simply as $f\,(x,y)$.

If $\mathbb{F} = \mathbb{F}_q$ is a finite field with $q = p^r$ elements for some odd prime p and positive integer r, then the associated affine plane $\mathbb{A}$ has q^2 elements, and the space of functions $\mathbb{F}_q^{\mathbb{A}}$ from $\mathbb{A}$ to $\mathbb{F}_q$ is a vector space over $\mathbb{F}_q$ with $\dim\left(\mathbb{F}_q^{\mathbb{A}}\right) = q^2$. A basis for $\mathbb{F}_q^{\mathbb{A}}$ is

$$\left\{ \delta_{[a,b]} \ : \ \ [a,b] \in \mathbb{A} \right\}$$

where $\delta_{[a,b]}$ is the delta function

$$\delta_{[a,b]}\,(x,y) = \begin{cases} 1_q & \text{if } [x,y] = [a,b] \\ 0 & \text{if } [x,y] \neq [a,b]\,. \end{cases}$$

The multiplicative identity in $\mathbb{F}_q^{\mathbb{A}}$ is the constant function that takes any $[x,y] \in \mathbb{A}$ to 1_q. We denote this multiplicative identity by $1_{\mathbb{F}^{\mathbb{A}}}$ and express it as

$$1_{\mathbb{F}^{\mathbb{A}}} = \sum_{[a,b]\in\mathbb{A}} \delta_{[a,b]} \tag{2.2}$$

since $\delta_{[a,b]}(x,y)$ vanishes at every point in $\mathbb{A}$ except $[a,b]$.

Evaluation of a 2-polynumber in $\mathrm{Pol}_2(\mathbb{F}_q)$ then gives a linear map

$$\varepsilon \,:\, \mathrm{Pol}_2(\mathbb{F}_q) \to \mathbb{F}_q^{\mathbb{A}}$$

that converts any polynumber to a polynomial function. For example if

$$\pi = 2 + 3\alpha - \alpha^2 + \beta + 7\alpha^2\beta - \beta^2 + 5\alpha^3\beta^2 + 4\alpha\beta^3 \in \mathrm{Pol}_2(\mathbb{F}_q)$$

then $\varepsilon(\pi)$ is a function from $\mathbb{A}$ to $\mathbb{F}_q$ defined by

$$\varepsilon(\pi)(x,y) = 2 + 3x - x^2 + y + 7x^2y - y^2 + 5x^3y^2 + 4xy^3$$

for any $[x,y] \in \mathbb{A}$.

In the finite field case, this map is not injective since two different polynumbers may evaluate to the same function. For example, the polynumbers $\pi_1 = \alpha + \beta$ and $\pi_2 = \alpha + \beta + \alpha\beta - \alpha^q\beta$ evaluate to the same function $f(x,y) = x + y$ since

$$\varepsilon(\pi_2)(x,y) = x + y + xy - x^q y = x + y + (x - x^q)\, y = x + y = \varepsilon(\pi_1)(x,y)$$

by the Fermat property $x^q - x = 0$.

Viewed as a map between two $\mathbb{F}_q$-algebras, ε is an algebra homomorphism. We list below some further properties of the evaluation map ε.

Proposition 2. *Suppose ε is the evaluation map $\varepsilon : \mathrm{Pol}_2(\mathbb{F}_q) \to \mathbb{F}_q^{\mathbb{A}}$. Then*

1. *The map ε is onto*
2. *The kernel of ε, denoted by $\ker(\varepsilon)$, is an ideal of $\mathrm{Pol}_2(\mathbb{F}_q)$ generated by $\alpha^q - \alpha$ and $\beta^q - \beta$. More precisely,*

$$\ker(\varepsilon) = \langle \alpha^q - \alpha, \beta^q - \beta \rangle .$$

Proof. For any $[a,b] \in \mathbb{A}$, define the 2-polynumber

$$\pi_{[a,b]} = \frac{1}{d_{[a,b]}} \prod_{\substack{t\in\mathbb{F}_q \\ t\neq a}} (t - \alpha) \prod_{\substack{u\in\mathbb{F}_q \\ u\neq b}} (u - \beta) \tag{2.3}$$

in $\mathrm{Pol}_2(\mathbb{F}_q)$ where $d_{[a,b]}$ is the non-zero element of $\mathbb{F}_q$ given by

$$d_{[a,b]} \equiv \prod_{\substack{t\in\mathbb{F}_q \\ t\neq a}} (t-a) \prod_{\substack{u\in\mathbb{F}_q \\ u\neq b}} (u-b)\,.$$

Then $\pi_{[a,b]}$ evaluates to the delta function $\delta_{[a,b]}$ since

$$\varepsilon\left(\pi_{[a,b]}\right)(x,y) = \begin{cases} 1 & \text{if } [x,y]=[a,b] \\ 0 & \text{if } [x,y]\neq[a,b]\,. \end{cases} \tag{2.4}$$

Now if

$$f = \sum_{[a,b]\in\mathbb{A}} \lambda_{[a,b]}\delta_{[a,b]}$$

for some scalars $\lambda_{[a,b]} \in \mathbb{F}_q$, then the 2-polynumber

$$\pi = \sum_{[a,b]\in\mathbb{A}} \lambda_{[a,b]}\pi_{[a,b]}$$

satisfies $\varepsilon(\pi) = f$. This proves the first statement.

Since ε is a surjective algebra homomorphism and $\ker(\varepsilon)$ is an ideal of $\mathrm{Pol}_2(\mathbb{F}_q)$, it follows that

$$\mathrm{Pol}_2(\mathbb{F}_q)/\ker(\varepsilon) \simeq \varepsilon\left(\mathrm{Pol}_2(\mathbb{F}_q)\right) = \mathbb{F}_q^{\mathbb{A}}$$

and viewed as vector spaces, we have that $\dim\left(\mathrm{Pol}_2(\mathbb{F}_q)/\ker(\varepsilon)\right) = \dim\left(\mathbb{F}_q^{\mathbb{A}}\right) = q^2$.

Moreover, $\langle \alpha^q-\alpha, \beta^q-\beta\rangle$ is an ideal of $\ker(\varepsilon)$ since both $\alpha^q-\alpha$ and $\beta^q-\beta$ belong in $\ker(\varepsilon)$ by the Fermat condition. Consequently, $\langle \alpha^q-\alpha, \beta^q-\beta\rangle$ is an ideal of $\mathrm{Pol}_2(\mathbb{F}_q)$ too and as a vector space, $\dim\left(\mathrm{Pol}_2(\mathbb{F}_q)/\langle \alpha^q-\alpha, \beta^q-\beta\rangle\right) = q^2$ since a basis for $\mathrm{Pol}_2(\mathbb{F}_q)/\langle \alpha^q-\alpha, \beta^q-\beta\rangle$ is

$$\left\{\alpha^k\beta^l + \langle \alpha^q-\alpha, \beta^q-\beta\rangle \;:\; 0\leq k,l\leq q-1\right\}.$$

By the Third Isomorphism Theorem and the fact that $\mathrm{Pol}_2(\mathbb{F}_q)/\langle \alpha^q-\alpha, \beta^q-\beta\rangle$ and $\mathrm{Pol}_2(\mathbb{F}_q)/\ker(\varepsilon)$ are both finite-dimensional vector spaces of the same dimension, we have that

$$\left(\mathrm{Pol}_2(\mathbb{F}_q)/\langle \alpha^q-\alpha, \beta^q-\beta\rangle\right) \Big/ \left(\ker(\varepsilon)/\langle \alpha^q-\alpha, \beta^q-\beta\rangle\right) \simeq \mathrm{Pol}_2(\mathbb{F}_q)/\ker(\varepsilon)$$

and

$$\mathrm{Pol}_2(\mathbb{F}_q)/\ker(\varepsilon) \simeq \mathrm{Pol}_2(\mathbb{F}_q)/\langle \alpha^q-\alpha, \beta^q-\beta\rangle\,.$$

We therefore conclude that $\ker(\varepsilon)/\langle \alpha^q - \alpha, \beta^q - \beta \rangle$ is trivial and hence $\ker(\varepsilon) = \langle \alpha^q - \alpha, \beta^q - \beta \rangle$. ■

Define $\mathcal{P}_q$ to be the subspace of $\mathrm{Pol}_2(\mathbb{F}_q)$ consisting of polynumbers in α and β with degree at most $q-1$ in α and with degree at most $q-1$ in β. Then $\dim(\mathcal{P}_q) = q^2$ since a basis for $\mathcal{P}_q$ is $\left\{\alpha^k \beta^l \ : \ 0 \leq k, l \leq q-1\right\}$. We call $\mathcal{P}_q$ the **principal subspace** of $\mathrm{Pol}_2(\mathbb{F}_q)$. The second part of Proposition 2 above gives the following result.

Proposition 3. *The restriction of ε to $\mathcal{P}_q$ is a vector space isomorphism to $\mathbb{F}_q^{\mathbb{A}}$.*

Proof. Since $\dim(\mathcal{P}_q) = \dim\left(\mathbb{F}_q^{\mathbb{A}}\right) = q^2$ and ε is linear, it suffices to show that the map $\varepsilon|_{\mathcal{P}_q}$ is onto. The 2-polynumber $\pi_{[a,b]}$ defined above in (2.3) is clearly in $\mathcal{P}_q$, proving that $\varepsilon|_{\mathcal{P}_q}$ is onto. Then $\varepsilon|_{\mathcal{P}_q}$ is necessarily injective and thus is a vector space isomorphism. ■

Corollary 6.1. *The set $\left\{\pi_{[a,b]} \ : \ [a,b] \in \mathbb{A}\right\}$ is a basis for $\mathcal{P}_q$.*

Proof. Since $\left\{\delta_{[a,b]} \ : \ [a,b] \in \mathbb{A}\right\}$ is a basis for $\mathbb{F}_q^{\mathbb{A}}$ and $\varepsilon|_{\mathcal{P}_q}$ is an isomorphism between $\mathcal{P}_q$ and $\mathbb{F}_q^{\mathbb{A}}$ from Proposition 3, it follows that $\left\{\varepsilon|_{\mathcal{P}_q}^{-1}\left(\delta_{[a,b]}\right) = \pi_{[a,b]} \ : \ [a,b] \in \mathbb{A}\right\}$ is a basis for $\mathcal{P}_q$. ■

The difference between polynumbers and polynomial functions is essentially captured by the evaluation map ε. Analysis on the whole 2-polynumber space $\mathrm{Pol}_2(\mathbb{F}_q)$ is more subtle than that on the function space $\mathbb{F}_q^{\mathbb{A}}$, which we may soon see when we have defined our notion of algebraic integral on $\mathrm{Pol}_2(\mathbb{F}_q)$. It is therefore useful to gain a better understanding of the algebraic structure of $\mathrm{Pol}_2(\mathbb{F}_q)$. The following result gives a decomposition of $\mathrm{Pol}_2(\mathbb{F}_q)$ as a vector space.

Proposition 4. *Any 2-polynumber in $\mathrm{Pol}_2(\mathbb{F}_q)$ can be written uniquely as a sum of a 2-polynumber in $\mathcal{P}_q$ with a 2-polynumber in $\ker()$. Equivalently,*

$$\mathrm{Pol}_2(\mathbb{F}_q) = \mathcal{P}_q \oplus \ker(\varepsilon).$$

Proof. Take any $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$. Then by Proposition 3 above, there is a unique $\pi_1 \in \mathcal{P}_q$ for which

$$\varepsilon(\pi_1) = \varepsilon(\pi)$$

namely $\pi_1 = \left(\varepsilon|_{\mathcal{P}_q}^{-1} \circ \varepsilon\right)(\pi)$. By the linearity of ε, we have that $\varepsilon(\pi - \pi_1) = 0$ and so $\pi - \pi_1 \in \ker(\varepsilon)$.Thus any 2-polynumber in $\mathrm{Pol}_2(\mathbb{F}_q)$ can be uniquely written as the sum of elements in $\mathcal{P}_q$ and $\ker(\varepsilon)$. ■

2.2.1 Group actions on $\mathbb{F}_q^{\mathbb{A}}$ and G-invariant functions

We now want to define some group actions on the relevant space that will be useful later in our analysis. The traditional treatment to specifying a group action is by

fixing a direction the group acts from, that is, agreeing that every action will be a left action or a right action.

We will instead be more flexible and specify explicitly whether a given action is a left or a right action. From our point of view, this has at least two benefits. First, any potential notion of duality can generally be appreciated better. Moreover, this avoids the need for inverses since they are expensive to calculate and should be avoided theoretically whenever possible.

Let G be a group with identity element e and X be a set. We say that G **left acts** on X if there exists a map $A_l : G \times X \to X$ satisfying the following two properties: $A_l(e, x) = x$ and $A_l(h_1, A_l(h_2, x)) = A_l(h_1 h_2, x)$ for any $h_1, h_2 \in G$ and $x \in X$. Similarly, we say that G **right acts** on X if there exists a map $A_r : X \times G \to X$ satisfying $A_r(x, e) = x$ and $A_r(A_r(x, h_1), h_2) = A_r(x, h_1 h_2)$ for all $h_1, h_2 \in G$ and $x \in X$.

We will sometimes indicate $A_l(h, x)$ or $A_r(x, h)$ by $h \cdot x$ or $x \cdot h$ respectively if the action and the direction which the group acts from is clear. We can think of elements of G as being a transformation on X, with $e \in G$ represents the identity transformation.

Now suppose that G is a group with identity element e that right acts on the affine plane $\mathbb{A}$. Then there is a natural left action of G on the space of functions $\mathbb{F}_q^{\mathbb{A}}$ defined for $h \in G$ and $f \in \mathbb{F}_q^{\mathbb{A}}$ by

$$(h \cdot f)(x, y) \equiv f([x, y] \cdot h).$$

Indeed, if $h_1, h_2 \in G$ and $f \in \mathbb{F}_q^{\mathbb{A}}$ then for any $[x, y] \in \mathbb{A}$, we may check that

$$(e \cdot f)(x, y) = f([x, y] \cdot e) = f(x, y)$$

so $e \cdot f = f$ and

$$\begin{aligned}
(h_2 \cdot (h_1 \cdot f))(x, y) &= (h_1 \cdot f)([x, y] \cdot h_2) \\
&= f(([x, y] \cdot h_2) \cdot h_1) \\
&= f([x, y] \cdot h_2 h_1) \ \text{(since } G \text{ right acts on } \mathbb{A}) \\
&= ((h_2 h_1) \cdot f)(x, y)
\end{aligned}$$

so $h_2 \cdot (h_1 \cdot f) = (h_2 h_1) \cdot f$. We can quickly verify that the set $\left\{\delta_{[a,b]} : [a, b] \in \mathbb{A}\right\}$ is invariant under this left action of G. To see this, observe that for any $h \in G$,

$$\left(h \cdot \delta_{[a,b]}\right)(x, y) = \delta_{[a,b]}([x, y] \cdot h) = \begin{cases} 1_q & \text{if } [x, y] = [a, b] \cdot h^{-1} \\ 0 & \text{if } [x, y] \neq [a, b] \cdot h^{-1} \end{cases}$$

and consequently

$$h \cdot \delta_{[a,b]} = \delta_{[a,b]\cdot h^{-1}}. \tag{2.5}$$

That is, the (left) action of G on a delta function gives another delta function.

We say that a function $f \in \mathbb{F}_q^{\mathbb{A}}$ is G-**invariant** precisely when $h \cdot f = f$ for any $h \in G$, and let $\mathcal{I}_G$ be the space of G-invariant functions in $\mathbb{F}_q^{\mathbb{A}}$; this is clearly a subalgebra of $\mathbb{F}_q^{\mathbb{A}}$. We see below that we can always construct a projection onto the space of G-invariant functions, provided that G satisfies a number-theoretical condition on its order.

Theorem 7. *Let G be a finite group that right acts on $\mathbb{A} = \mathbb{A}(\mathbb{F}_q)$ and suppose that $|G|$ is not zero in the prime field $\mathbb{F}_p$ of $\mathbb{F}_q$. Then the operator ρ_G on $\mathbb{F}_q^{\mathbb{A}}$ defined by the rule*

$$\rho_G(f) \equiv \frac{1}{|G|} \sum_{h \in G} (h \cdot f)$$

is a projection onto $\mathcal{I}_G$.

Proof. The condition $|G| \neq 0$ in $\mathbb{F}_q$ makes the division by $|G|$ in the definition of $\rho_G(f)$ above well-defined. It is also clear that ρ_G is a linear operator on $\mathbb{F}_q^{\mathbb{A}}$ since for any $f_1, f_2 \in \mathbb{F}_q^{\mathbb{A}}$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q$, we have that

$$\begin{aligned}
\rho_G(\lambda_1 f_1 + \lambda_2 f_2)(x,y) &= \frac{1}{|G|} \sum_{h \in G} (h \cdot (\lambda_1 f_1 + \lambda_2 f_2))(x,y) \\
&= \frac{1}{|G|} \sum_{h \in G} (\lambda_1 f_1 + \lambda_2 f_2)([x,y] \cdot h) \\
&= \frac{\lambda_1}{|G|} \sum_{h \in G} f_1([x,y] \cdot h) + \frac{\lambda_2}{|G|} \sum_{h \in G} f_2([x,y] \cdot h) \\
&= \frac{\lambda_1}{|G|} \sum_{h \in G} (h \cdot f_1)(x,y) + \frac{\lambda_2}{|G|} \sum_{h \in G} (h \cdot f_2)(x,y) \\
&= \lambda_1 \rho_G(f_1)(x,y) + \lambda_2 \rho_G(f_2)(x,y) \\
&= (\lambda_1 \rho_G(f_1) + \lambda_2 \rho_G(f_2))(x,y)
\end{aligned}$$

for any $[x,y] \in \mathbb{A}$, concluding that $\rho_G(\lambda_1 f_1 + \lambda_2 f_2) = \lambda_1 \rho_G(f_1) + \lambda_2 \rho_G(f_2)$.

Now we show that $g \cdot \rho_G(f) = \rho_G(f)$ for any $g \in G$. Indeed, for any $[x,y] \in \mathbb{A}$,

$$\begin{aligned}
(g \cdot \rho_G(f))(x,y) &= \rho_G(f)([x,y] \cdot g) \\
&= \frac{1}{|G|} \sum_{h \in G} (h \cdot f)([x,y] \cdot g) \\
&= \frac{1}{|G|} \sum_{h \in G} (gh \cdot f)(x,y) \\
&= \frac{1}{|G|} \sum_{h \in G} (h \cdot f)(x,y) \ \text{(via a change of index } h \mapsto g^{-1}h)
\end{aligned}$$

$$= \rho_G(f)(x,y).$$

Since this is true for any $[x,y] \in \mathbb{A}$, $g \cdot \rho_G(f) = \rho_G(f)$ as required. Furthermore if $f \in \mathcal{I}_G$ then

$$\rho_G(f) = \frac{1}{|G|}\sum_{h\in G}(h\cdot f) = \frac{1}{|G|}\sum_{h\in G} f = \frac{|G|}{|G|}f = f.$$

Thus ρ_G is indeed a projection onto $\mathcal{I}_G$. ■

We call the function $\rho_G(f)$ the **G-average of the function** f. Note that even if $|G|$ is zero in $\mathbb{F}_q$, we can still define a linear G-summation operator Σ_G on $\mathbb{F}_q^{\mathbb{A}}$ by the rule

$$\Sigma_G(f) \equiv \sum_{h\in G}(h\cdot f).$$

This will still map into the space of G-invariant functions $\mathcal{I}_G$, although it might not necessarily be onto.

2.2.2 The dual space and G-invariant linear functionals

Now we consider the dual space $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ of $\mathbb{F}_q^{\mathbb{A}}$, by which we mean the space of $\mathbb{F}_q$-linear functionals $\phi : \mathbb{F}_q^{\mathbb{A}} \to \mathbb{F}_q$. We continue to suppose rather generally that the group G right acts on $\mathbb{A}$ as in the previous section. Since G left acts on $\mathbb{F}_q^{\mathbb{A}}$, we can define a right action of G on $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ by

$$(\phi\cdot h)(f) \equiv \phi(h\cdot f)$$

for any $\phi \in \left(\mathbb{F}_q^{\mathbb{A}}\right)^*$, $h \in G$, and $f \in \mathbb{F}_q^{\mathbb{A}}$. We can verify that this is indeed a right action since for any $\phi \in \left(\mathbb{F}_q^{\mathbb{A}}\right)^*$, $h_1, h_2 \in G$, and $f \in \mathbb{F}_q^{\mathbb{A}}$ we have

$$\begin{aligned}((\phi\cdot h_1)\cdot h_2)(f) &= (\phi\cdot h_1)(h_2\cdot f)\\ &= \phi(h_1\cdot(h_2\cdot f))\\ &= \phi((h_1h_2)\cdot f) \ \text{ (since } G \text{ left acts on } \mathbb{F}_q^{\mathbb{A}})\\ &= (\phi\cdot(h_1h_2))(f)\end{aligned}$$

so that indeed $(\phi\cdot h_1)\cdot h_2 = \phi\cdot(h_1h_2)$. Note that here the duality between $\mathbb{F}_q^{\mathbb{A}}$ and $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ is also reflected in the left and right action of G on $\mathbb{F}_q^{\mathbb{A}}$ and $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ respectively.

A linear functional $\phi \in \left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ is **G-invariant** precisely when $\phi\cdot h = \phi$ for any $h \in G$ and let $\mathcal{I}_G^*$ be the space of G-invariant functionals in $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$; this is clearly a subspace of $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$. We can also employ a G-averaging method to project onto the space of G-invariant linear functionals.

Theorem 8. *Let G be a finite group that right acts on $\mathbb{A} = \mathbb{A}(\mathbb{F}_q)$ and suppose that $|G|$ is not zero in the prime field of $\mathbb{F}_q$. Then the operator $\widehat{\rho}_G$ on $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ defined by*

the rule

$$\widehat{\rho}_G(\phi) \equiv \frac{1}{|G|}\sum_{h\in G}(\phi \cdot h)$$

is a projection onto $\mathcal{I}_G^*$.

Proof. The proof is similar to that of Theorem 7. The expression $\widehat{\rho}_G(\phi)$ is well-defined since there is no division by zero and $\widehat{\rho}_G$ is a linear operator on $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$. Now, for any $g \in G$ and $f \in \mathbb{F}_q^{\mathbb{A}}$,

$$\begin{aligned}
\left(\widehat{\rho}_G(\phi)\cdot g\right)(f) &= \left(\left(\frac{1}{|G|}\sum_{h\in G}(\phi\cdot h)\right)\cdot g\right)(f)\\
&= \frac{1}{|G|}\sum_{h\in G}\left((\phi\cdot h)\cdot g\right)(f)\\
&= \frac{1}{|G|}\sum_{h\in G}\phi(hg\cdot f)\\
&= \frac{1}{|G|}\sum_{h\in G}\phi(h\cdot f)\ \text{ (via a change of index } h\mapsto hg^{-1})\\
&= \frac{1}{|G|}\sum_{h\in G}(\phi\cdot h)(f)\\
&= \widehat{\rho}_G(\phi)(f).
\end{aligned}$$

Therefore we conclude that $\widehat{\rho}_G(\phi)\cdot g = \widehat{\rho}_G(\phi)$, which shows that $\widehat{\rho}_G(\phi) \in \mathcal{I}_G^*$.

Finally, if $\phi \in \mathcal{I}_G^*$, then

$$\widehat{\rho}_G(\phi) = \frac{1}{|G|}\sum_{h\in G}(\phi\cdot h) = \frac{1}{|G|}\sum_{h\in G}\phi = \frac{|G|}{|G|}\phi = \phi$$

and this shows that $\widehat{\rho}_G$ is onto. ■

Analogous to the G-average function $\rho_G(f)$ above, we shall call $\widehat{\rho}_G(\phi)$ the G-**average of the linear functional** ϕ.

2.3 Prior developments on the super Catalan numbers

This section is dedicated to the main developments on the super Catalan numbers since their introduction by Catalan in his 1874 paper [8], in which he claimed that for any two natural numbers a and b, the expression

$$\frac{(a+1)\times(a+2)\times\cdots\times(2a)\times(b+1)\times(b+2)\times\cdots\times(2b)}{1\times 2\times\cdots\times(a+b)}$$

always evaluates to a natural number.

These numbers were then re-introduced by Gessel more than a century later, in his paper [19] as a special case of the super ballot numbers using the factorial notation

$$S(m,n)=\frac{(2m)!\,(2n)!}{m!n!\,(m+n)!}$$

parametrised by two natural numbers m and n. We list below the values of $S(m,n)$ for $0\leq m,n\leq 9$.

$m\backslash n$	0	1	2	3	4	5	6	7	8	9
0	1	2	6	20	70	252	924	3432	12 870	48 620
1	2	2	4	10	28	84	264	858	2860	9724
2	6	4	6	12	28	72	198	572	1716	5304
3	20	10	12	20	40	90	220	572	1560	4420
4	70	28	28	40	70	140	308	728	1820	4760
5	252	84	72	90	140	252	504	1092	2520	6120
6	924	264	198	220	308	504	924	1848	3960	8976
7	3432	858	572	572	728	1092	1848	3432	6864	14 586
8	12 870	2860	1716	1560	1820	2520	3960	6864	12 870	25 740
9	48 620	9724	5304	4420	4760	6120	8976	14 586	25 740	48 620

Table 5: $S(m,n)$ for $0\leq m,n\leq 9$.

Here are some basic properties of the super Catalan numbers.

Proposition 5. *For any given natural numbers m and n,*

1. $S(m,n)=S(n,m)$
2. $4S(m,n)=S(m+1,n)+S(m,n+1)$
3. $S(1,n)=2C_n$ *where C_n is the n-th Catalan number*

$$C_n=\frac{1}{n+1}\binom{2n}{n}$$

4. $S(m,n)$ *is always an even integer with the exception of* $S(0,0)=1$.

Proof. The first one is trivial:

$$S(m,n)=\frac{(2m)!\,(2n)!}{m!n!\,(m+n)!}=S(n,m).$$

The recurrence relation $4S(m,n) = S(m+1,n) + S(m,n+1)$ can be derived from the definition directly. Observe that

$$\begin{aligned} S(m+1,n) + S(m,n+1) &= \frac{(2m+2)!\,(2n)!}{(m+1)!n!\,(m+n+1)!} + \frac{(2m)!\,(2n+2)!}{m!\,(n+1)!\,(m+n+1)!} \\ &= S(m,n)\left(\frac{(2m+2)\,(2m+1)}{(m+1)\,(m+n+1)} + \frac{(2n+2)\,(2n+1)}{(n+1)\,(m+n+1)}\right) \\ &= S(m,n)\left(\frac{2\,(2m+1)}{m+n+1} + \frac{2\,(2n+1)}{m+n+1}\right) \\ &= \frac{2\,(2m+2n+2)}{m+n+1} S(m,n) \\ &= 4S(m,n)\,. \end{aligned}$$

To prove the third identity, we note that

$$S(1,n) = \frac{2!\,(2n)!}{n!\,(n+1)!} = \frac{2}{n+1}\binom{2n}{n} = 2C_n.$$

Finally, to show that $S(m,n)$ is always even except when $m = n = 0$, we first show that for any $n \geq 0$, $S(m,n)$ is even for any $m \geq 1$. We note that for $m \geq 1$,

$$\begin{aligned} S(m,0) = \binom{2m}{m} &= \frac{(2m)\,(2m-1)\,(2m-2)!}{m\,(m-1)!m!} \\ &= \frac{2\,(2m-1)}{m}\binom{2m-2}{m-1} = 2\,(2m-1)\,C_{m-1} \end{aligned}$$

where C_{m-1} is the $(m-1)$-th Catalan number. Since C_{m-1} is an integer, this shows that $S(m,0)$ is even for $m \geq 1$, proving the base step. Suppose for a fixed n, $S(m,n)$ is even for any $m \geq 1$. Using the recurrence relation in part 2 of this proposition,

$$S(m,n+1) = 4S(m,n) - S(m+1,n)\,.$$

The right-hand side is even from the inductive hypothesis, showing that $S(m,n+1)$ is also even. Since the choice of m is arbitrary, $S(m,n+1)$ is even for any $m \geq 1$, finishing the induction. We complete the proof by observing that $S(m,0) = S(0,m)$ by the first part of this proposition, showing that $S(m,n)$ is even for any natural numbers m and n except when $m = n = 0$. ■

The fact that the super Catalan numbers are always natural numbers suggests that they ought to have a combinatorial interpretation, meaning that we can find a set of objects that depends on m and n whose cardinality is $S(m,n)$. Since the super Catalan numbers generalise the Catalan numbers C_n, it might seem rather surprising that to date there is no general combinatorial interpretation of the super Catalan numbers.

The sequence of Catalan numbers is certainly one of the most well-studied sequences in mathematics, with more than two hundred interpretations (see for example Stanley [43] and the OEIS entry A000108 [42]). They were first introduced by Euler to count triangulations of polygons in the plane, but of the many other interpretations we mention that for example the Catalan numbers C_n enumerate the number of lattice paths from $(0,0)$ to (n,n) consisting of unit right- and up-steps that never cross the line $y = x$, otherwise known as Dyck paths.

The super Catalan numbers, on the other hand, so far only have some particular interpretations, often in terms of the closely related numbers $T(m,n) \equiv \frac{1}{2}S(m,n)$ since $S(m,n)$ is even except when $m = n = 0$. A description of $T(2,n)$ in terms of blossom trees was discovered by Schaeffer [37], and another in terms of cubic trees by Pippenger and Schleich [34]. Gessel [20] gave an explanation of $T(2,n)$ in terms of pairs of Dyck paths with restricted heights, in which an interpretation of $T(3,n)$ also appeared. A meaning for $T(m,m+s)$ for $0 \leq s \leq 3$ in terms of restricted lattice paths was found by Chen and Wang [9]. Most recently, a combinatorial interpretation for $T(3,n)$ and $T(4,n)$ was given by Gheorghiciuc and Orelowitz [21] as the numbers of 3-tuples and 4-tuples of Dyck paths satisfying certain conditions.

There is also a weighted interpretation of $S(m,n)$ in terms of 2-Motzkin paths, discovered by Allen and Gheorghiciuc [1]. The term weighted interpretation here means assigning a weight to each element in a certain set such that the sum of the weights corresponds to the object of study. In this case, their description of $S(m,n)$ involved a notion of positive and negative 2-Motzkin paths.

Another weighted interpretation of the super Catalan numbers, which will play a prominent role in this thesis, is as certain values of Krawtchouk polynomials which was found by Georgiadis, Munemasa, and Tanaka in [18]. We will discuss this in more detail later.

Finally, there are some other established identities involving the super Catalan numbers. Some identities related to the reciprocal super Catalan matrix were discovered by Prodinger [35]. There is also some obtained identity on the congruences of the super Catalan numbers by Liu [29]. Most recently, the paper by Mikić [33] gives an identity of convolution of the super Catalan numbers.

2.3.1 Circular super Catalan numbers

In this thesis, we will be dealing with closely connected variants of the super Catalan numbers. These are rational numbers which we call the **circular super Catalan numbers**, defined for two natural numbers m and n by

$$\Omega(m,n) \equiv \frac{(2m)!\,(2n)!}{4^{m+n}m!n!\,(m+n)!} = \frac{S(m,n)}{4^{m+n}}.$$

The term circular here is used to suggest a connection between this family of rational numbers with the integration theory over a circle. Here is a table of values of $\Omega(m,n)$ for $0 \leq m,n \leq 8$.

$m\backslash n$	0	1	2	3	4	5	6	7	8
0	1	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{5}{16}$	$\frac{35}{128}$	$\frac{63}{256}$	$\frac{231}{1024}$	$\frac{429}{2048}$	$\frac{6435}{32\,768}$
1	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{5}{128}$	$\frac{7}{256}$	$\frac{21}{1024}$	$\frac{33}{2048}$	$\frac{429}{32\,768}$	$\frac{715}{65\,536}$
2	$\frac{3}{8}$	$\frac{1}{16}$	$\frac{3}{128}$	$\frac{3}{256}$	$\frac{7}{1024}$	$\frac{9}{2048}$	$\frac{99}{32\,768}$	$\frac{143}{65\,536}$	$\frac{429}{262\,144}$
3	$\frac{5}{16}$	$\frac{5}{128}$	$\frac{3}{256}$	$\frac{5}{1024}$	$\frac{5}{2048}$	$\frac{45}{32\,768}$	$\frac{55}{65\,536}$	$\frac{143}{262\,144}$	$\frac{195}{524\,288}$
4	$\frac{35}{128}$	$\frac{7}{256}$	$\frac{7}{1024}$	$\frac{5}{2048}$	$\frac{35}{32\,768}$	$\frac{35}{65\,536}$	$\frac{77}{262\,144}$	$\frac{91}{524\,288}$	$\frac{455}{4194\,304}$
5	$\frac{63}{256}$	$\frac{21}{1024}$	$\frac{9}{2048}$	$\frac{45}{32\,768}$	$\frac{35}{65\,536}$	$\frac{63}{262\,144}$	$\frac{63}{524\,288}$	$\frac{273}{4194\,304}$	$\frac{315}{8388\,608}$
6	$\frac{231}{1024}$	$\frac{33}{2048}$	$\frac{99}{32\,768}$	$\frac{55}{65\,536}$	$\frac{77}{262\,144}$	$\frac{63}{524\,288}$	$\frac{231}{4194\,304}$	$\frac{231}{8388\,608}$	$\frac{495}{33\,554\,432}$
7	$\frac{429}{2048}$	$\frac{429}{32\,768}$	$\frac{143}{65\,536}$	$\frac{143}{262\,144}$	$\frac{91}{524\,288}$	$\frac{273}{4194\,304}$	$\frac{231}{8388\,608}$	$\frac{429}{33\,554\,432}$	$\frac{429}{67\,108\,864}$
8	$\frac{6435}{32\,768}$	$\frac{715}{65\,536}$	$\frac{429}{262\,144}$	$\frac{195}{524\,288}$	$\frac{455}{4194\,304}$	$\frac{315}{8388\,608}$	$\frac{495}{33\,554\,432}$	$\frac{429}{67\,108\,864}$	$\frac{6435}{2147\,483\,648}$

Table 6: $\Omega(m,n)$ for $0 \leq m,n \leq 8$.

We immediately note the symmetry in the parameters is clearly maintained so that $\Omega(m,n) = \Omega(n,m)$ for any m and n. The recurrence relation $4S(m,n) = S(m+1,n) + S(m,n+1)$ of the super Catalan numbers becomes the relation

$$\Omega(m,n) = \Omega(m+1,n) + \Omega(m,n+1) \tag{2.6}$$

for any m and n, which we call the **Pascal property**. It tells us that any entry in the table of the circular super Catalan numbers is the sum of the entry on its right and the entry below it.

Moreover, it can also be checked that the entries in the top row and the left-most column of the table of the circular super Catalan numbers are given by

$$\Omega(m,0) = \Omega(0,m) = \frac{1}{4^m}\binom{2m}{m}$$

and the diagonal entries are given by

$$\Omega(m,m) = \frac{1}{4^{2m}}\binom{2m}{m} = \frac{1}{4^m}\Omega(m,0). \tag{2.7}$$

In particular, the top-left entry will be $\Omega(0,0) = 1$.

In fact, the uniqueness of the circular super Catalan numbers can be deduced by the above properties by a simple mathematical induction.

Theorem 9. *If a table of rational numbers $c(m,n)$ for natural numbers m and n has the following properties:*

1. $c(0,0) = 1$
2. $c(m,n) = c(n,m)$
3. $c(m,m) = \frac{1}{4^m} c(m,0)$ *and*
4. $c(m,n) = c(m+1,n) + c(m,n+1)$

then it must be that $c(m,n) = \Omega(m,n)$ for any m and n.

Proof. Define $d(m,n) = c(m,n) - \Omega(m,n)$ for any natural numbers m and n. Since $\Omega(0,0) = 1$, $\Omega(m,n) = \Omega(n,m)$, $\Omega(m,m) = \frac{1}{4^m}\Omega(m,0)$, and $\Omega(m,n) = \Omega(m+1,n) + \Omega(m,n+1)$, it follows that

$$d(0,0) = 0 \tag{2.8}$$
$$d(m,n) = d(n,m) \tag{2.9}$$
$$d(m,m) = \frac{1}{4^m} d(m,0) \tag{2.10}$$
$$d(m,n) = d(m+1,n) + d(m,n+1). \tag{2.11}$$

We now assert that $d(m,n) = 0$ for any m and n such that $m+n \leq 2N$ for any $N \geq 0$ by mathematical induction. The base case $N = 0$ is obviously true from (2.8). Now assume that the statement is true for a fixed $N \geq 1$. As a consequence $d(N,N) = 0$ and thus

$$\begin{aligned} 0 &= d(N,N) \\ &= d(N+1,N) + d(N,N+1) \quad \text{(by equation (2.11))} \\ &= d(N+1,N) + d(N+1,N) \quad \text{(by equation (2.9))} \\ &= 2d(N+1,N). \end{aligned}$$

Therefore we conclude that $d(N+1,N) = 0$.

By repeated use of equation (2.11), we have that $d(m,n) = 0$ for any m and n such that $m+n = 2N+1$. Now again from the inductive hypothesis, $d(N+1,0) = 0$ since $N+1 \leq 2N$. From equation (2.10), it follows that

$$d(N+1,N+1) = \frac{1}{4^{N+1}} d(N+1,0) = 0.$$

It follows again by repeated applications of equation (2.11) that $d(m,n) = 0$ for any m and n such that $m + n = 2(N+1)$, proving the inductive step. Since the statement $d(m,n) = 0$ for any m and n such that $m + n \leq 2N$ is true for any $N \geq 0$, we conclude that $d(m,n) = 0$ for any natural numbers m and n, showing that $c(m,n) = \Omega(m,n)$. ■

For a given prime $p > 2$, we can reduce any circular super Catalan number modulo p. Note that the reduction

$$\Omega(m,n) \bmod p \equiv \frac{S(m,n)}{4^{m+n}} \bmod p$$

is well-defined since the numerator is always an integer and the denominator is never a multiple of p, therefore avoiding the possibility of dividing by zero if we treat this as an element in the prime field $\mathbb{F}_p$ of $\mathbb{F}_q$.

2.4 Krawtchouk polynumbers and matrices

For a natural number l, we define the rational polynumber

$$\binom{\alpha}{l} \equiv \begin{cases} \dfrac{\alpha(\alpha-1)(\alpha-2)\ldots(\alpha-l+1)}{l!} & \text{if } l \geq 1 \\ \mathbf{1} & \text{if } l = 0. \end{cases}$$

These polynumbers generalise the binomial coefficients when evaluated at the non-negative integers. With this notation, composition of $\binom{\alpha}{l}$ for $l \geq 1$ with another polynumber π in α can be written as

$$\binom{\pi}{l} = \frac{\pi(\pi-1)(\pi-2)\ldots(\pi-l+1)}{l!}.$$

In the late 1920s, Mikhail Krawtchouk introduced a family of polynomials which serves as a generalisation of the Hermite polynumbers, later called the Krawtchouk polynomials [25], [26]. Since we prefer to restate polynomial arithmetic in terms of polynumbers, we define the n-th **Krawtchouk polynumber** of order d, for $0 \leq n \leq d$ and denoted by $k_n^{(d)}$, as

$$k_n^{(d)}(\alpha) \equiv \sum_{l=0}^{n} (-1)^l \binom{\alpha}{l}\binom{d-\alpha}{n-l}.$$

For example, if $d = 3$ and $n = 2$ then

$$k_2^{(3)}(\alpha) = \binom{\alpha}{0}\binom{3-\alpha}{2} - \binom{\alpha}{1}\binom{3-\alpha}{1} + \binom{\alpha}{2}\binom{3-\alpha}{0}$$

$$
\begin{aligned}
&= \frac{(3-\alpha)(3-\alpha-1)}{2!} - \frac{\alpha(3-\alpha)}{1!1!} + \frac{\alpha(\alpha-1)}{2!} \\
&= \frac{1}{2}\left(6-5\alpha+\alpha^2\right) - \left(3\alpha-\alpha^2\right) + \frac{1}{2}\left(-\alpha+\alpha^2\right) \\
&= 3-6\alpha+2\alpha^2.
\end{aligned}
$$

Krawtchouk polynumbers play an important role in many areas of mathematics, such as harmonic analysis in the context of orthogonal polynumbers [13], [14], coding theory in the context of bounds of codes [27], [28], [30], and probability theory in the context of symmetric random walk [16].

In 2011, Georgiadis, Munemasa, and Tanaka in their paper [18] gave an interpretation of the super Catalan numbers in terms of specific values of some Krawtchouk polynumbers. We state their main result below without proof.

Theorem 10 (Georgiadis, Munemasa, Tanaka)**.** *For any natural numbers m and n,*

$$
k_{m+n}^{(2m+2n)}(2m) = (-1)^m S(m,n). \tag{2.12}
$$

One main property of the Krawtchouk polynumbers of order d is in terms of their generating function.

Proposition 6. *If $k_n^{(d)}(m)$ is the evaluation of $k_n^{(d)}$ at $m \in \mathbb{Z}$, then for $0 \le m \le d$, we have that*

$$
\sum_{n=0}^{d} k_n^{(d)}(m)\alpha^n = (1-\alpha)^m (1+\alpha)^{d-m}.
$$

Proof. Observe that

$$
\begin{aligned}
\sum_{n=0}^{d} k_n^{(d)}(m)\alpha^n &= \sum_{n=0}^{d}\sum_{l=0}^{n} (-1)^l \binom{m}{l}\binom{d-m}{n-l}\alpha^n \\
&= \sum_{l\ge 0}\sum_{n=l}^{d} (-1)^l \binom{m}{l}\binom{d-m}{n-l}\alpha^n
\end{aligned} \tag{2.13}
$$

where in the second equality we perform a change of summation order. The last double-summation in (2.13) can be written as a product of two single-summations since

$$
\begin{aligned}
\sum_{l\ge 0}\sum_{n=l}^{d} (-1)^l \binom{m}{l}\binom{d-m}{n-l}\alpha^n &= \sum_{l\ge 0}\sum_{n=0}^{d-l} (-1)^l \binom{m}{l}\binom{d-m}{n}\alpha^{l+n} \\
&= \left(\sum_{l\ge 0} (-1)^l \binom{m}{l}\alpha^l\right)\left(\sum_{n=0}^{d-l}\binom{d-m}{n}\alpha^n\right).
\end{aligned}
$$

We now note that for a given integer m, the expression $\binom{m}{l}$ is zero precisely when $l < 0$ or $l > m$. Hence for $n > d - m$, the expression $\binom{d-m}{n}$ will vanish. Therefore,

$$\sum_{l \geq 0} (-1)^l \binom{m}{l} \alpha^l = \sum_{l=0}^{m} (-1)^l \binom{m}{l} \alpha^l = (1-\alpha)^m$$

and

$$\sum_{n=0}^{d-l} \binom{d-m}{n} \alpha^n = \sum_{n=0}^{d-m} \binom{d-m}{n} \alpha^n = (1+\alpha)^{d-m}$$

by the Binomial Theorem expansion.

It follows that

$$\sum_{n=0}^{d} k_n^{(d)}(m) \alpha^n = \left(\sum_{l=0}^{d} (-1)^l \binom{m}{l} \alpha^l \right) \left(\sum_{n=0}^{d-l} \binom{d-m}{n} \alpha^n \right) = (1-\alpha)^m (1+\alpha)^{d-m}$$

for $0 \leq m \leq d$ as claimed. ■

The result in Proposition 6 above enables us to encode the evaluations of the Krawtchouk polynumbers at integer values in matrix form. Given a natural number d, there are precisely $d+1$ Krawtchouk polynumbers of order d, which are $k_n^{(d)}$ for $0 \leq n \leq d$.

Define a $(d+1) \times (d+1)$ matrix whose entries in column m are the integer coefficients of $(1-\alpha)^m (1+\alpha)^{d-m}$, in ascending powers of α. It follows that all entries in row n of this matrix correspond to the values of $k_n^{(d)}(m)$ for $0 \leq m \leq d$. Such a matrix is called the **Krawtchouk matrix** of order d, and such terminology was first introduced by Bose in his book [3].

More precisely, for a given natural number d, define the $(d+1) \times (d+1)$ matrix $K^{(d)}$ whose (n,m)-entry is

$$\left(K^{(d)}\right)_{n,m} = [\alpha^n] (1-\alpha)^m (1+\alpha)^{d-m}$$

for any m and n. It is easy to verify that that $K^{(0)} = (1)$. The Krawtchouk matrices of order one up to five are given below:

$$K^{(1)} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad K^{(2)} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & -2 \\ 1 & -1 & 1 \end{pmatrix} \quad K^{(3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 1 & -1 & -3 \\ 3 & -1 & -1 & 3 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

$$K^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix} \quad K^{(5)} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 3 & 1 & -1 & -3 & -5 \\ 10 & 2 & -2 & -2 & 2 & 10 \\ 10 & -2 & -2 & 2 & 2 & -10 \\ 5 & -3 & 1 & 1 & -3 & 5 \\ 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}.$$

The earliest appearance of these matrices is arguably in terms of eigenmatrices of the binary Hamming scheme, where the terminology eigenmatrix itself dates back to Delsarte [12]. For a more detailed account, we refer the reader to Chapter 21 of [30], although we remark that the eigenmatrices differ to $K^{(d)}$ by a transpose sign.

In [15], it is shown that Krawtchouk matrices can be defined through the perhaps more well-known Sylvester-Hadamard matrices. We will revisit Krawtchouk matrices in a later chapter and connect this with the Fourier summation functional formulas established in Part II.

We can now use Proposition 6 to restate the result of Georgiadis, Munemasa, and Tanaka in Theorem 10 as follows:

Corollary 10.1. *For any natural numbers m and n,*

$$(-1)^m S(m,n) = \left[\alpha^{m+n}\right](1-\alpha)^{2m}(1+\alpha)^{2n}. \tag{2.14}$$

One elementary reformulation of Corollary 10.1 is the following, where we have interchanged the roles of the powers m and n.

Proposition 7. *For any natural numbers m and n,*

$$S(m,n) = (-1)^n \left[\alpha^{m+n}\right](1+\alpha)^{2m}(1-\alpha)^{2n}.$$

Proof. Multiply both sides of equation (2.14) in Corollary 10.1 by $(-1)^{m+n}$ to get

$$\begin{aligned}(-1)^n S(m,n) &= (-1)^{m+n}\left[\alpha^{m+n}\right](1-\alpha)^{2m}(1+\alpha)^{2n} \\ &= \left[(-\alpha)^{m+n}\right](1-\alpha)^{2m}(1+\alpha)^{2n}.\end{aligned}$$

We can therefore regard the right-hand side above as the composition of the polynumber $(1+\alpha)^{2m}(1-\alpha)^{2n}$ with the polynumber $-\alpha$.

We thus have that

$$(-1)^n S(m,n) = \left[\alpha^{m+n}\right](1+\alpha)^{2m}(1-\alpha)^{2n}$$

and the desired result is found by multiplying both sides by $(-1)^n$. ■

2.5 The circular polynumbers

We now introduce, for natural numbers k and l, polynumbers which will play a central role in this thesis, the rational **circular polynumbers**

$$\pi_{k,l} \equiv \left(\frac{1+\alpha}{2}\right)^k \left(\frac{1-\alpha}{2}\right)^l. \tag{2.15}$$

It is clear that $\pi_{0,0} = \mathbf{1}$. Here is a table of the polynumbers $\pi_{k,l}$ for the next few values of k and l, organised by the sum $k+l$:

$\pi_{k,l}$	$k+l=1$
$\pi_{0,1}$	$\frac{1}{2}(1-\alpha)$
$\pi_{1,0}$	$\frac{1}{2}(1+\alpha)$

$\pi_{k,l}$	$k+l=2$
$\pi_{0,2}$	$\frac{1}{4}(1-2\alpha+\alpha^2)$
$\pi_{1,1}$	$\frac{1}{4}(1-\alpha^2)$
$\pi_{2,0}$	$\frac{1}{4}(1+2\alpha+\alpha^2)$

$\pi_{k,l}$	$k+l=3$
$\pi_{0,3}$	$\frac{1}{8}(1-3\alpha+3\alpha^2-\alpha^3)$
$\pi_{1,2}$	$\frac{1}{8}(1-\alpha-\alpha^2+\alpha^3)$
$\pi_{2,1}$	$\frac{1}{8}(1+\alpha-\alpha^2-\alpha^3)$
$\pi_{3,0}$	$\frac{1}{8}(1+3\alpha+3\alpha^2+\alpha^3)$

$\pi_{k,l}$	$k+l=4$
$\pi_{0,4}$	$\frac{1}{16}(1-4\alpha+6\alpha^2-4\alpha^3+\alpha^4)$
$\pi_{1,3}$	$\frac{1}{16}(1-2\alpha+2\alpha^3-\alpha^4)$
$\pi_{2,2}$	$\frac{1}{16}(1-2\alpha^2+\alpha^4)$
$\pi_{3,1}$	$\frac{1}{16}(1+2\alpha-2\alpha^3-\alpha^4)$
$\pi_{4,0}$	$\frac{1}{16}(1+4\alpha+6\alpha^2+4\alpha^3+\alpha^4)$

$\pi_{k,l}$	$k+l=5$
$\pi_{0,5}$	$\frac{1}{32}(1-5\alpha+10\alpha^2-10\alpha^3+5\alpha^4-\alpha^5)$
$\pi_{1,4}$	$\frac{1}{32}(1-3\alpha+2\alpha^2+2\alpha^3-3\alpha^4+\alpha^5)$
$\pi_{2,3}$	$\frac{1}{32}(1-\alpha-2\alpha^2+2\alpha^3+\alpha^4-\alpha^5)$
$\pi_{3,2}$	$\frac{1}{32}(1+\alpha-2\alpha^2-2\alpha^3+\alpha^4+\alpha^5)$
$\pi_{4,1}$	$\frac{1}{32}(1+3\alpha+2\alpha^2-2\alpha^3-3\alpha^3-\alpha^5)$
$\pi_{5,0}$	$\frac{1}{32}(1+5\alpha+10\alpha^2+10\alpha^3+5\alpha^4+\alpha^5)$

Table 7: The circular polynumbers $\pi_{k,l}$ for $0 \leq k+l \leq 5$.

We will connect these circular polynumbers to the circular super Catalan numbers via Proposition 7, which itself was derived from the key formula of Georgiadis,

Munemasa, and Tanaka in Theorem 10. These polynumbers will be crucial in describing the Fourier summation functional formulas in both the Euclidean and relativistic geometries.

From the first few Krawtchouk matrices defined earlier and Table 7 above we can immediately observe two symmetry/anti-symmetry phenomena in the coefficients of $(1+\alpha)^k (1-\alpha)^l$ and thus the circular polynumbers. Listed in ascending order of powers of α, the coefficients are symmetrical up to a sign. We will see that this is true in general and we will use this to give an algebraic proof of the identity (2.12) in Theorem 10 above in terms of the circular super Catalan numbers and the circular polynumbers.

We say that a polynumber

$$\pi = u_0\alpha^0 + u_1\alpha^1 + \cdots + u_{d-1}\alpha^{d-1} + u_d\alpha^d$$

of degree d is **palindromic** (sometimes called self-reciprocal) precisely when $u_k = u_{d-k}$ for all $0 \leq k \leq d$, and define it to be **anti-palindromic** precisely when $u_k = -u_{d-k}$ for all $0 \leq k \leq d$. It is easy to verify that the product of two palindromic polynumbers or two anti-palindromic polynumbers is palindromic, while the product of a palindromic and an anti-palindromic polynumber is anti-palindromic.

Lemma 2 (Palindromic property of $\pi_{k,l}$)**.** *If $0 \leq i, j \leq k+l$ and $i+j = k+l$ then*

$$\left[\alpha^i\right] \pi_{k,l} = (-1)^l \left[\alpha^j\right] \pi_{k,l}.$$

Proof. Clearly $\pi_{k,0}$ is a palindromic polynumber for any k, while $\pi_{0,l}$ is palindromic if l is even and anti-palindromic if l is odd. Since $\pi_{k,l} = \pi_{k,0}\pi_{0,l}$, the result then follows. ■

Lemma 3 (Symmetry property of $\pi_{k,l}$)**.** *If $0 \leq i \leq k+l$ then*

$$\left[\alpha^i\right] \pi_{k,l} = (-1)^i \left[\alpha^i\right] \pi_{l,k}.$$

Proof. We observe that

$$\pi_{l,k}(-\alpha) = \left(\frac{1-\alpha}{2}\right)^l \left(\frac{1+\alpha}{2}\right)^k = \pi_{k,l}(\alpha).$$

Thus, extracting the coefficient of α^i from both sides,

$$\left[\alpha^i\right] \pi_{k,l} = \left[\alpha^i\right] \pi_{l,k}(-\alpha) = \left[(-\alpha)^i\right] \pi_{l,k} = \left[(-1)^i \alpha^i\right] \pi_{l,k} = (-1)^i \left[\alpha^i\right] \pi_{l,k}$$

as claimed. ■

Now, if the degree of a palindromic or an anti-palindromic polynumber π is an even number, say $2d$, then the term involving α^d will be called the **central term**. In particular, Proposition 7 states that up to a sign, the super Catalan number $S(m,n)$ appears as the coefficient of the central term of the polynumber $(1+\alpha)^{2m}(1-\alpha)^{2n}$.

We now restate the result of Georgiadis, Munemasa, and Tanaka of Theorem 10 in terms of the circular super Catalan numbers $\Omega(m,n)$ and the central coefficient of the circular polynumbers $\pi_{2m,2n}$ and give an independent algebraic proof. This allows us to naturally identify the remaining coefficients around the central one as secondary but still important variants of the circular super Catalan numbers.

Theorem 11. *For any natural numbers m and n,*

$$\Omega(m,n) = (-1)^n \left[\alpha^{m+n}\right] \pi_{2m,2n} = (-1)^n \left[\alpha^{m+n}\right] \left(\left(\frac{1+\alpha}{2}\right)^{2m} \left(\frac{1-\alpha}{2}\right)^{2n} \right).$$

Before we get into the proof, we briefly note that throughout the rest of this thesis, we will drop the parentheses in writing the expansion $[\alpha^{m+n}]\,\pi_{2m,2n}$. That is, we will instead write

$$\left[\alpha^{m+n}\right] \pi_{2m,2n} = \left[\alpha^{m+n}\right] \left(\frac{1+\alpha}{2}\right)^{2m} \left(\frac{1-\alpha}{2}\right)^{2n}.$$

Proof. We calculate that

$$\begin{aligned}
(-1)^n \left[\alpha^{m+n}\right] \pi_{2m,2n} &= (-1)^n \left[\alpha^{m+n}\right] \left(\frac{1+\alpha}{2}\right)^{2m} \left(\frac{1-\alpha}{2}\right)^{2n} \\
&= \frac{(-1)^n}{4^{m+n}} \left[\alpha^{m+n}\right] (1+\alpha)^{2m} (1-\alpha)^{2n} \\
&= \frac{(-1)^n}{4^{m+n}} \sum_{\substack{0\le s\le 2m \\ 0\le t\le 2n \\ s+t=m+n}} (-1)^t \binom{2m}{s}\binom{2n}{t}.
\end{aligned}$$

By using the convention that $\binom{k}{s} = 0$ if $s<0$ or $s>k$, we may rearrange this sum as

$$\begin{aligned}
(-1)^n \left[\alpha^{m+n}\right] \pi_{2m,2n} &= \frac{(-1)^n}{4^{m+n}} \sum_{s=0}^{m+n} (-1)^{m+n-s} \binom{2m}{s}\binom{2n}{m+n-s} \\
&= \frac{(-1)^m}{4^{m+n}} \sum_{s=0}^{m+n} (-1)^s \frac{(2m)!}{s!\,(2m-s)!} \frac{(2n)!}{(m+n-s)!\,(n-m+s)!} \\
&= \frac{(-1)^m\,(2m)!\,(2n)!}{4^{m+n}\,(m+n)!\,(m+n)!} \sum_{s=0}^{m+n} \frac{(-1)^s\,(m+n)!\,(m+n)!}{s!\,(m+n-s)!\,(2m-s)!\,(n-m+s)!}
\end{aligned}$$

$$= \frac{(-1)^m (2m)! (2n)!}{4^{m+n} (m+n)!^2} \sum_{s=0}^{m+n} (-1)^s \binom{m+n}{s} \binom{m+n}{2m-s}. \qquad (2.16)$$

The summation on the right-hand side of (2.16) can be realised as

$$\left[\alpha^{2m}\right] (1+\alpha)^{m+n} (1-\alpha)^{m+n} = \left[\alpha^{2m}\right] \left(1-\alpha^2\right)^{m+n}$$

so we get

$$\begin{aligned}
(-1)^n \left[\alpha^{m+n}\right] \pi_{2m,2n} &= \frac{(-1)^m (2m)! (2n)!}{4^{m+n} (m+n)! (m+n)!} \left[\alpha^{2m}\right] \left(1-\alpha^2\right)^{m+n} \\
&= \frac{(-1)^m (2m)! (2n)!}{4^{m+n} (m+n)! (m+n)!} \left[\alpha^{2m}\right] \left(\sum_{r=0}^{m+n} (-1)^r \binom{m+n}{r} \alpha^{2r} \right) \\
&= \frac{(2m)! (2n)!}{4^{m+n} (m+n)! (m+n)!} \binom{m+n}{m} \\
&= \frac{(2m)! (2n)!}{4^{m+n} m! n! (m+n)!} \\
&= \Omega (m,n) .
\end{aligned}$$

This finishes the proof. ■

Part II

Fourier Summations over Finite Fields

Chapter 3

Chromogeometry and Dihedrons

3.1 Blue, red, and green complex numbers over a general field

In this chapter, we will introduce chromogeometry as a foundation for studying different geometrical cases of Fourier summation over finite fields. There are two main objects that we will consider here: the unit circle over which the Fourier summation takes place and the group of rotation matrices which acts on the space of 2-polynumbers. The unit circle will be defined through a symmetric bilinear form induced by a symmetric matrix, so this allows us to avoid notions of distance involving square roots, which do not generally apply to finite fields.

Let $\mathbb{F}$ be a field of characteristic not two. The ambient space in which our discussion of chromogeometry takes place is the algebra of 2×2 matrices over $\mathbb{F}$, which we shall call the **dihedron algebra** over $\mathbb{F}$, denoted by $\mathbb{D} = \mathbb{D}(\mathbb{F})$. This terminology was introduced by Wildberger in his online *Linear Algebra* lectures series on YouTube [53].

The vector space operations are the usual matrix addition and scalar multiplication (entry-wise), and the multiplication in this dihedron algebra is the usual matrix multiplication. We define four special matrices in $\mathbb{D}$, which are

$$1_{\mathbb{D}} \equiv \begin{pmatrix} 1_{\mathbb{F}} & 0 \\ 0 & 1_{\mathbb{F}} \end{pmatrix} \quad i \equiv \begin{pmatrix} 0 & 1_{\mathbb{F}} \\ -1_{\mathbb{F}} & 0 \end{pmatrix} \quad j \equiv \begin{pmatrix} 0 & 1_{\mathbb{F}} \\ 1_{\mathbb{F}} & 0 \end{pmatrix} \quad k \equiv \begin{pmatrix} 1_{\mathbb{F}} & 0 \\ 0 & -1_{\mathbb{F}} \end{pmatrix}.$$

As a vector space, a basis for $\mathbb{D}$ is $\{1_{\mathbb{D}}, i, j, k\}$ and thus $\mathbb{D}$ is a 4-dimensional algebra over $\mathbb{F}$. These four elements and their negatives form a finite group of order 8 which is the dihedral group D_4, hence the name of the associated algebra. The situation is analogous to and shares many parallels with the quaternion group Q also of order 8 and the associated four dimensional algebra $\mathbb{H}$ of quaternions.

By simple computations we observe that

$$\begin{aligned} i^2 = -1_{\mathbb{D}} \quad j^2 = 1_{\mathbb{D}} \quad k^2 = 1_{\mathbb{D}} \\ ij = k \quad ji = -k \quad jk = -i \\ kj = i \quad ik = -j \quad ki = j. \end{aligned} \tag{3.1}$$

The difference between the dihedron algebra and the quaternion algebra $\mathbb{H}$ then amounts to small alterations in signs for the structure constants when comparing the basis elements $1_{\mathbb{D}}$, i, j, and k and the usual corresponding elements in Q.

We can think of $\mathbb{F}$ as being embedded in $\mathbb{D}$ by making the identification

$$t \mapsto t1_{\mathbb{D}} \tag{3.2}$$

which is clearly an injective map.

For $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{D}$, the **adjugate** of h is defined to be $h^* \equiv \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, and the product of the matrix h and its adjugate h^*, in either order, is

$$hh^* = h^*h = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \det(h)1_{\mathbb{D}}. \tag{3.3}$$

It follows that $h \in \mathbb{D}$ is invertible precisely when $\det(h) \neq 0$ and in that case,

$$h^{-1} = \frac{1}{\det(h)} h^*. \tag{3.4}$$

The adjugate is a linear map on $\mathbb{D}$ so that for $h_1, h_2 \in \mathbb{D}$ and $\lambda \in \mathbb{F}$,

$$\begin{aligned} (h_1 + h_2)^* &= h_1^* + h_2^* \\ (\lambda h_1)^* &= \lambda h_1^*. \end{aligned}$$

Note that we are not assuming any underlying involution on $\mathbb{F}$ here. The adjugate is also an involution on $\mathbb{D}$ in that for $h \in \mathbb{D}$,

$$(h^*)^* = h$$

and it further satisfies the property that

$$(h_1 h_2)^* = h_2^* h_1^*.$$

Putting these together, $\mathbb{D}$ becomes a $*$-**algebra** over $\mathbb{F}$.

We will be considering three special subalgebras of $\mathbb{D}$, namely

$$\mathbb{C}_b(\mathbb{F}) \equiv \operatorname{span}\{1_{\mathbb{D}}, i\} = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \ : \ x, y \in \mathbb{F} \right\}$$

$$\mathbb{C}_r(\mathbb{F}) \equiv \operatorname{span}\{1_{\mathbb{D}}, j\} = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} \ : \ x, y \in \mathbb{F} \right\}$$

$$\mathbb{C}_g(\mathbb{F}) \equiv \operatorname{span}\{1_{\mathbb{D}}, k\} = \left\{ \begin{pmatrix} x+y & 0 \\ 0 & x-y \end{pmatrix} \ : \ x, y \in \mathbb{F} \right\}.$$

We will call these subalgabras the **blue complex numbers**, **red complex numbers**, and **green complex numbers** respectively. As usual the subscripts b, r, and g above are shorthand for blue, red, and green respectively. If we are referring to an algebra of complex numbers of an arbitrary one of these colours, we will write $\mathbb{C}_c$ where c is one of b, r, or g. Any element of $\mathbb{C}_b$ is called a **blue complex number**, and similarly we have a notion of **red** and **green complex numbers**. A generic complex number will often be denoted by z.

This attempt to extend the notion of complex numbers is of course not new. A red complex number is also sometimes called a **split-complex number** or a **hyperbolic number** in some of the literatures. The first known reference to split-complex numbers is probably in the introduction of *tessarines* by Cockle [11]. These numbers also appear in the definition of quarternion algebra or split-biquarternions introduced by Clifford [10].

Traditionally, a red complex number is an element of the vector space

$$\mathbb{F}_q(j) = \{z = x1_q + yj \ : \ x, y \in \mathbb{F}_q\}$$

over $\mathbb{F}_q$ with ordered basis $\{1_q, j\}$ which can be made into a commutative associative $\mathbb{F}_q$-algebra by declaring that the formal symbol j satisfies $j^2 = 1_q$. With our approach, the role of the formal symbol j is replaced by the specific 2×2 matrix

$$j \equiv \begin{pmatrix} 0 & 1_q \\ 1_q & 0 \end{pmatrix}.$$

One benefit of adopting this point of view is that computations are generally more explicit since we are after all working in the dihedron algebra $\mathbb{D}$ which is just the

algebra of 2×2 matrices over $\mathbb{F}$, and this may make them easier to implement using standing computational algebra packages. It also has the theoretical advantage that the usual properties of matrix arithmetic restrict naturally to the complex numbers of the various colours.

Since each of the subalgebras $\mathbb{C}_c(\mathbb{F})$ are generated by $1_{\mathbb{D}}$ and either one of i, j, or k, they are commutative. Moreover, since

$$i^* = -i \qquad j^* = -j \qquad k^* = -k \tag{3.5}$$

each of these algebras is also closed under the adjugate operations. Thus each of $\mathbb{C}_b(\mathbb{F})$, $\mathbb{C}_r(\mathbb{F})$, and $\mathbb{C}_g(\mathbb{F})$ are commutative $*$-algebras over $\mathbb{F}$.

Note that the relations (3.5) imply that the adjugation operation in these algebras of complex numbers corresponds to conjugation in the traditional sense. Indeed, if $z = x1_{\mathbb{D}} + yi \in \mathbb{C}_b(\mathbb{F})$, then

$$z^* = (x1_{\mathbb{D}} + yi)^* = x1_{\mathbb{D}}^* + yi^* = x1_{\mathbb{D}} - yi.$$

Adjugation applied to red and green complex numbers is similar. Thus we have an analogue of real and imaginary part extraction of a given complex number: if $z = x1_{\mathbb{D}} + yi$ is a blue complex number then $z^* = x1_{\mathbb{D}} - yi$ and so

$$x1_{\mathbb{D}} = \frac{1}{2}(z + z^*) \quad \text{and} \quad y1_{\mathbb{D}} = -\frac{1}{2}(z - z^*)\, i \tag{3.6}$$

where the second identity follows from multiplying both sides of the equation $yi = \frac{1}{2}(z - z^*)$ by $-i$. If $z = x1_{\mathbb{D}} + yj$ is a red complex number then $z^* = x1_{\mathbb{D}} - yj$ and so

$$x1_{\mathbb{D}} = \frac{1}{2}(z + z^*) \quad \text{and} \quad y1_{\mathbb{D}} = \frac{1}{2}(z - z^*)\, j. \tag{3.7}$$

Finally, if $z = x1_{\mathbb{D}} + yk$ is a green complex number then $z^* = x1_{\mathbb{D}} - yk$ and so

$$x1_{\mathbb{D}} = \frac{1}{2}(z + z^*) \quad \text{and} \quad y1_{\mathbb{D}} = \frac{1}{2}(z - z^*)\, k. \tag{3.8}$$

In both situations, we use the relation $j^2 = k^2 = 1_{\mathbb{D}}$ to get the formula for $y1_{\mathbb{D}}$. These elements $x1_{\mathbb{D}}$ and $y1_{\mathbb{D}}$ then correspond to elements x and y in the base field $\mathbb{F}$ via the identification (3.2).

3.2 Geometry over complex numbers

Now we introduce some geometry into the algebra of dihedrons, and then restrict this to each of the coloured complex numbers following the approach of Wildberger

in [53]. Define a symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $\mathbb{D}$ by the rule that for h_1, h_2 in $\mathbb{D}$ the element $\langle h_1, h_2 \rangle$ in $\mathbb{F}$ is

$$\langle h_1, h_2 \rangle \equiv \frac{1}{2} \operatorname{tr}(h_1 h_2^*). \tag{3.9}$$

This is well-defined since $2 \neq 0$ in $\mathbb{F}$.

This symmetric bilinear form then relates to the embedding map (3.2) in the following way: if $x \mapsto x1_{\mathbb{D}}$ then $x = \langle x1_{\mathbb{D}}, 1_{\mathbb{D}} \rangle$. Moreover, if $z = x1_{\mathbb{D}} + yi \in \mathbb{C}_b(\mathbb{F})$ then

$$x = \left\langle \frac{1}{2}(z + z^*), 1_{\mathbb{D}} \right\rangle \quad \text{and} \quad y = \left\langle -\frac{1}{2}(z - z^*), i \right\rangle.$$

If $z = x1_{\mathbb{D}} + yj \in \mathbb{C}_r(\mathbb{F})$ then

$$x = \left\langle \frac{1}{2}(z + z^*), 1_{\mathbb{D}} \right\rangle \quad \text{and} \quad y = \left\langle \frac{1}{2}(z - z^*), j \right\rangle$$

and if $z = x1_{\mathbb{D}} + yk \in \mathbb{C}_k(\mathbb{F})$ then

$$x = \left\langle \frac{1}{2}(z + z^*), 1_{\mathbb{D}} \right\rangle \quad \text{and} \quad y = \left\langle \frac{1}{2}(z - z^*), k \right\rangle.$$

The symmetric bilinear form (3.9) is then associated to a quadratic form on $\mathbb{D}$ given by

$$Q(h) \equiv \langle h, h \rangle = \frac{1}{2} \operatorname{tr}(hh^*) = \frac{1}{2} \operatorname{tr}(\det(h) 1_{\mathbb{D}}) = \det(h). \tag{3.10}$$

The element $Q(h)$ of $\mathbb{F}$ will be called the **quadrance** of h. This symmetric bilinear form and quadratic form allow us to consider a variety of geometrical notations that are parallel to familiar facts for complex numbers, but we are able to study all three geometries at once under the umbrella of the dihedron geometry.

Specifically the blue, red, and green geometries are obtained by restricting the symmetric bilinear form $\langle \cdot, \cdot \rangle$ and associated quadratic form Q on the algebra $\mathbb{D}$ to the respective subalgebras of blue, red, and green complex numbers. If we want to emphasise this restriction, we will write $\langle \cdot, \cdot \rangle_b$, $\langle \cdot, \cdot \rangle_r$, and $\langle \cdot, \cdot \rangle_g$ for the respective symmetric bilinear forms and Q_b, Q_r, and Q_g for the respective blue, red and green quadratic forms on the corresponding geometries.

Over the blue geometry, if $z_1 = x_1 1_{\mathbb{D}} + y_1 i$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 i$, then

$$\begin{aligned} \langle z_1, z_2 \rangle_b &= \frac{1}{2} \operatorname{tr}(z_1 z_2^*) \\ &= \frac{1}{2} \operatorname{tr}((x_1 x_2 + y_1 y_2) 1_{\mathbb{D}} + (x_2 y_1 - x_1 y_2) i) \\ &= x_1 x_2 + y_1 y_2. \end{aligned}$$

The symmetric bilinear form in the red and green geometries are similar, in the sense that if $z_1 = x_1 1_{\mathbb{D}} + y_1 j$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 j$ are two red complex numbers then

$$\langle z_1, z_2 \rangle_r = \frac{1}{2} \operatorname{tr}(z_1 z_2^*) = x_1 x_2 - y_1 y_2$$

while if $z_1 = x_1 1_{\mathbb{D}} + y_1 k$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 k$ are two green complex numbers, then

$$\langle z_1, z_2 \rangle_g = \frac{1}{2} \operatorname{tr}(z_1 z_2^*) = x_1 x_2 - y_1 y_2.$$

These follow from the relations $j^2 = k^2 = 1_{\mathbb{D}}$.

With the above explicit formulas for the symmetric bilinear form in each geometry, we can see that in $\mathbb{C}_b(\mathbb{F})$,

$$Q_b(x1_{\mathbb{D}} + yi) = Q\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\right) = x^2 + y^2$$

and in $\mathbb{C}_r(\mathbb{F})$,

$$Q_r(x1_{\mathbb{D}} + yj) = Q\left(\begin{pmatrix} x & y \\ y & x \end{pmatrix}\right) = x^2 - y^2$$

and finally in $\mathbb{C}_g(\mathbb{F})$,

$$Q_g(x1_{\mathbb{D}} + yk) = Q\left(\begin{pmatrix} x+y & 0 \\ 0 & x-y \end{pmatrix}\right) = x^2 - y^2.$$

However in the green geometry in $\mathbb{C}_g(\mathbb{F})$ we can also write the quadrance perhaps more simply as

$$Q_g\left(\begin{pmatrix} t & 0 \\ 0 & u \end{pmatrix}\right) = tu.$$

These formulas make it clear that the blue geometry can be identified with the familiar Euclidean geometry, while the red and green geometries correspond to two Einstein-Minkowski (relativistic) geometries which are intimately connected. Physicists often refer to the green geometry in terms of null coordinates or light-cone coordinates in special relativity theory, by making a change of coordinate from the xy-coordinate to the tu-coordinate where $t = x + y$ and $u = x - y$ (see [36], [38], or [39] for more references in special relativity). This colour assignment is in line with the approach of Wildberger to *chromogeometry* [49] as an outgrowth of rational

trigonometry [50].

Each geometry has its own notion of the unit circle, which we call the blue, red, and green unit circles. We shall define these circles more carefully in the next section, along with the orthogonal groups of isometries that preserve the respective symmetric bilinear form in (3.9) and act on the unit circles in each geometry.

3.3 Unit circles in chromogeometry

From this point henceforth, we will be dealing with finite fields of odd characteristic $\mathbb{F}_q$ of size $q = p^r$ for some odd prime p and positive integer r. Recall from Proposition 1 that the group $\mathbb{F}_q^\times$ is cyclic of order $q-1$, and so for any $x \in \mathbb{F}_q$, we have the Fermat property or Fermat relation $x^q - x = 0$ which in some literature is called the *Frobenius property* since Frobenius introduced the endomorphism $x \mapsto x^p$ of commutative rings with prime characteristic p. Recall also that our treatment of the various complex number algebras over $\mathbb{F}_q$ imbeds them in the dihedron algebra $\mathbb{D} = \mathbb{D}_q$ of 2×2 matrices over $\mathbb{F}_q$.

For c one of the blue, red, or green geometries, the unit circle $S_c(\mathbb{F}_q)$ is then defined to be the set of complex numbers in $\mathbb{C}_{c,q}$ of quadrance 1_q, that is,

$$S_c(\mathbb{F}_q) \equiv \Big\{ z \in \mathbb{C}_{c,q} \ : \ Q(z) = 1_q \Big\}.$$

Since the quadrance of a complex number z is the determinant of z as a 2×2 matrix, it is a multiplicative function: for any complex numbers z_1 and z_2 in $\mathbb{C}_c(\mathbb{F}_q)$ we have

$$Q(z_1 z_2) = Q(z_1)\, Q(z_2).$$

Theorem 12. *The unit circle $S_c(\mathbb{F}_q)$ forms an abelian group under multiplication.*

Proof. Since the determinant is multiplicative, it follows that if z_1 and z_2 are in $S_c(\mathbb{F}_q)$, then

$$Q(z_1 z_2) = Q(z_1)\, Q(z_2) = 1_q \times 1_q = 1_q$$

so $z_1 z_2 \in S_{c,q}$. The associativity of $S_c(\mathbb{F}_q)$ is inherited from the associativity of $\mathbb{D}_q$. The identity element in $S_c(\mathbb{F}_q)$ is $1_{\mathbb{D}}$, and the inverse of $z \in S_c(\mathbb{F}_q)$ is its adjugate z^* since $zz^* = \det(z)\, 1_{\mathbb{D}} = 1_{\mathbb{D}}$ by (3.3). The commutativity is clear since we have seen that each complex number subalgebra $\mathbb{C}_c(\mathbb{F}_q)$ is indeed commutative. ∎

We have also seen that there is a natural identification of complex numbers of any particular colour as affine points in the affine plane $\mathbb{A}$ over the field $\mathbb{F}_q$. Note that the green parametrisation is a bit different here from the blue and red parametrisations.

Proposition 8. *The maps between $\mathbb{C}_{c,q}$ and $\mathbb{A} = \mathbb{A}(\mathbb{F}_q)$ defined by*

$$\begin{aligned} z = x1_{\mathbb{D}} + yi &\mapsto [x, y] \\ z = x1_{\mathbb{D}} + yj &\mapsto [x, y] \\ z = x1_{\mathbb{D}} + yk &\mapsto [x + y, x - y] \end{aligned}$$

over the algebras of blue, red, and green complex numbers respectively are each a bijection.

Proof. Over the blue complex numbers, if $[x_1, y_1] = [x_2, y_2]$ then $x_1 = x_2$ and $y_1 = y_2$, so $x_1 1_{\mathbb{D}} + y_1 i = x_2 1_{\mathbb{D}} + y_2 i$ and the map is injective. Moreover, any $[x, y] \in \mathbb{A}$ corresponds to $z = x1_{\mathbb{D}} + yi$ by construction so it is also onto. The association over the red complex numbers is proved similarly. Over the green complex numbers, if $[x_1 + y_1, x_1 - y_1] = [x_2 + y_2, x_2 - y_2]$ then we have a system of equations

$$\begin{cases} x_1 + y_1 = x_2 + y_2 \\ x_1 - y_1 = x_2 - y_2 \end{cases} \tag{3.11}$$

where $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$. Adding the two equations gives $2x_1 = 2x_2$ and since $\mathbb{F}_q$ is of odd characteristic, this implies that $x_1 = x_2$ and thus $y_1 = y_2$. It thus follows that $x_1 1_{\mathbb{D}} + y_1 k = x_2 1_{\mathbb{D}} + y_2 k$, proving the injectivity. Moreover, for any $[x, y] \in \mathbb{A}$, we have that

$$z = \left(\frac{x + y}{2}\right) 1_{\mathbb{D}} + \left(\frac{x - y}{2}\right) k \mapsto [x, y]$$

and the division by 2 above is well-defined since $2 \neq 0$ in $\mathbb{F}_q$. This proves the surjectivity. ■

We thus can identify the unit circles $S_c(\mathbb{F}_q)$ as subsets of $\mathbb{A}$ in the following way:

$$\begin{aligned} S_b(\mathbb{F}_q) = S_{b,q} &= \left\{[x, y] \in \mathbb{A} : \ x^2 + y^2 = 1\right\} \\ S_r(\mathbb{F}_q) = S_{r,q} &= \left\{[x, y] \in \mathbb{A} : \ x^2 - y^2 = 1\right\} \\ S_g(\mathbb{F}_q) = S_{g,q} &= \left\{[x, y] \in \mathbb{A} : \ xy = 1\right\}. \end{aligned} \tag{3.12}$$

For brevity, we shall use the notations $S_{b,q}$, $S_{r,q}$, and $S_{g,q}$ to indicate the blue, red, and green unit circles respectively when the underlying field is clear from context, and $S_{c,q}$ to indicate an arbitrary unit circle in the three geometries where c is one of b, r, or g. We use the notation $S_c(\mathbb{F}_q)$ only if we need to emphasise the underlying field over which the unit circle is defined.

We also note that from this identification, the blue unit circle is the unit circle in what is the finite field version of Euclidean geometry. The red and green unit circles can be regarded as two unit circles in finite field versions of the Minkowski-Einstein

(relativistic) geometry.

From the group structure of $S_{c,q}$ in Theorem 12, we then can define a multiplication structure in $S_{c,q}$ when viewed as a set of affine points in $\mathbb{A}$. Over the blue, red, and green geometries respectively, we have that

$$\begin{aligned}
[x_1, y_1] \times_b [x_2, y_2] &= [x_1x_2 - y_1y_2, x_1y_2 + x_2y_1] \\
[x_1, y_1] \times_r [x_2, y_2] &= [x_1x_2 + y_1y_2, x_1y_2 + x_2y_1] \\
[x_1, y_1] \times_g [x_2, y_2] &= [x_1x_2, y_1y_2] \,.
\end{aligned} \tag{3.13}$$

Also with the identification of the unit circles as set of affine points in $\mathbb{A}$, it becomes clear that over a finite field the three unit circles are also finite since $\mathbb{A}$ is a finite set with q^2 elements. The size of each unit circle will be given in the next subsection.

3.3.1 Unit circle parametrisations

While the green unit circle $S_{g,q}$ is easily parametrised algebraically, the traditional parametrisations for the blue and red unit circles over the real numbers are often presented via trigonometric functions and hyperbolic trigonometric functions respectively. However, since our discussion is purely algebraic, we prefer to utilise the respective rational parametrisations

$$\left[\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right] \quad \text{and} \quad \left[\frac{1+t^2}{1-t^2}, \frac{2t}{1-t^2}\right]$$

for the blue and red unit circles.

These parametrisations conveniently extend also to the finite field case, as we see in the following lemma, where we state the situation for all three geometries. This is of course a classical argument, going back to at least Fermat in the Euclidean case, and arguably to Euclid from his classification of Pythagorean triples.

Lemma 4. *Every point on the green unit circle $S_{g,q}$ can be written as $[x, y] = [t, t^{-1}]$ for a unique element $t \in \mathbb{F}_q^\times$. Every point on the red unit circle $S_{r,q}$ except for $[-1, 0]$ can be written as*

$$[x, y] = \left[\frac{1+t^2}{1-t^2}, \frac{2t}{1-t^2}\right]$$

for a unique element $t \in \mathbb{F}_q$. Every point on the blue unit circle $S_{b,q}$ except for $[-1, 0]$ can be written as

$$[x, y] = \left[\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right]$$

for a unique element $t \in \mathbb{F}_q$.

Proof. Since every point $[x, y]$ on the green unit circle satisfies $xy = 1$, the conclusion follows by letting $x = t$ and observing that t cannot be zero. On the red unit circle, one may verify that

$$\left(\frac{1+t^2}{1-t^2}\right)^2 - \left(\frac{2t}{1-t^2}\right)^2 = 1$$

for all $t \in \mathbb{F}_q$ for which $1 - t^2 \neq 0$. Similarly, on the blue unit circle one may also verify that

$$\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1$$

for all $t \in \mathbb{F}_q$ such that $1 + t^2 \neq 0$.

Now consider the line through the points $[-1, 0]$ and $[0, t]$ given by $y = tx + t$. This line intersects the red unit circle $x^2 - y^2 = 1$ in exactly two points, one of which is $[-1, 0]$. To see this, we solve $x^2 - (tx + t)^2 = 1$ for x, which amounts to solving the quadratic equation

$$\left(1 - t^2\right) x^2 - 2t^2 x - \left(1 + t^2\right) = 0.$$

We can factor the left-hand side into $(x + 1)\left(\left(1 - t^2\right) x - \left(1 + t^2\right)\right) = 0$ which gives two values of x, namely $x = -1$ which corresponds to the point $[-1, 0]$ and $x = \frac{1+t^2}{1-t^2}$ which corresponds to the point $\left[\frac{1+t^2}{1-t^2}, \frac{2t}{1-t^2}\right]$. This implies that every point on the red unit circle except $[-1, 0]$ corresponds to exactly one $t \in \mathbb{F}_q$ except for $t = 1$ and $t = -1$.

The same line $y = tx + t$ intersects the blue unit circle $x^2 + y^2 = 1$ in exactly two points too, one of which is $[-1, 0]$. To find the other point of intersection, similar to the red unit circle situation we solve $x^2 + (tx + t)^2 = 1$ for x, which is equivalent to

$$\left(1 + t^2\right) x^2 + 2t^2 x - \left(1 - t^2\right) = 0.$$

The left-hand side above can be written as $(x + 1)\left(\left(1 + t^2\right) x - \left(1 - t^2\right)\right) = 0$, which gives $x = -1$ that corresponds to our known point of intersection $[-1, 0]$ and $x = \frac{1-t^2}{1+t^2}$ which corresponds to the point $\left[\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right]$. We conclude that every point on the blue unit circle except $[-1, 0]$ corresponds to exactly one $t \in \mathbb{F}_q$ except for those t that satisfy $t^2 = -1$, if any. ∎

Remark 12.1. *These parametrisations rely on the existence of a known point on the unit circle. While we can also consider intersecting the line through* $[0, 1]$ *and* $[t, 0]$ *with the blue unit circle to get the parametrisation*

$$\left[\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right]$$

this will not work in the red geometry since the point $[0, 1]$ *does not lie on the red unit circle* $x^2 - y^2 = 1$.

3.3.2 The Legendre and Jacobi symbols

Since we are working in a finite field, we have to take into account the possibility of division by zero. In the parametrisation of the red unit circle, the denominator $1 - t^2$ is zero precisely when $t = 1$ or $t = -1$. In the parametrisation of the blue unit circle, $1 + t^2 = 0$ has solutions precisely when -1 is a square in $\mathbb{F}_q$. This is a number-theoretic condition, suggesting that the analysis for the two cases should be done separately.

In particular, the case where -1 is not a square number gives an additional algebraic structure to the algebra of blue complex numbers $\mathbb{C}_{b,q}$. Before we show that, we make a simple observation.

Proposition 9. *Let* $\mathbb{F}_q$ *be a field in which* -1 *is not a square. Then the equation* $x^2 + y^2 = 0$ *for* $x, y \in \mathbb{F}_q$ *implies that* $x = y = 0$.

Proof. Suppose on the contrary that either x or y is non-zero. Without loss of generalisation, assume $y \neq 0$. Then $y^2 \neq 0$ and we can divide both sides of the equation $x^2 + y^2 = 0$ by y^2 to get

$$\left(\frac{x}{y}\right)^2 + 1 = 0.$$

But this means that $\frac{x}{y}$ is an element of $\mathbb{F}_q$ whose square is -1, which contradicts our assumption. Therefore the assumption that either x or y is non-zero must be false and thus both are zero. ■

Proposition 9 above is used to prove that under the assumption that -1 is not a square number in $\mathbb{F}_q$, $\mathbb{C}_{b,q}$ is actually a field; this will become important later in this thesis.

Theorem 13. *Let* $\mathbb{F}_q$ *be a field in which* -1 *is not a square. Then the algebra of blue complex numbers* $\mathbb{C}_{b,q}$ *is a field of size* q^2.

Proof. Since $\mathbb{C}_{b,q}$ is already an algebra, it remains to show that the only non-invertible element of $\mathbb{C}_{b,q}$ is the zero complex number $01_{\mathbb{D}} + 0i$. Let $z = x1_{\mathbb{D}} + yi$ be any blue complex number, then z^{-1} exists precisely when $\det(z) \neq 0$ by (3.4). Now if z has no inverse, consequently $0 = \det(z) = x^2 + y^2$. By Proposition 9 above, we must have that $x = y = 0$, and thus z is the zero complex number.

Since the association $z = x1_{\mathbb{D}} + yi \mapsto [x, y]$ between $\mathbb{C}_{b,q}$ and $\mathbb{A}$ is a bijection by Proposition 8, and $\mathbb{A}$ has q^2 elements, the size of $\mathbb{C}_{b,q}$ is also q^2. ■

For an odd prime p and an integer a, define a to be a **quadratic residue modulo** p precisely when there exists some integer x such that $x^2 \equiv a \bmod p$. Recall the **Legendre symbol**

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } p \text{ does not divide } a \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p \\ 0 & \text{if } p \text{ divides } a. \end{cases}$$

In particular, if $a = -1$ then p never divides a, so $\left(\frac{-1}{p}\right)$ is either 1 if there exists some x such that $x^2 \equiv -1 \bmod p$ or -1 otherwise. In other words,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } -1 \text{ is a square in } \mathbb{F}_p \\ -1 & \text{if } -1 \text{ is not a square in } \mathbb{F}_p. \end{cases}$$

For a more general prime power $q = p^r$, we utilise a generalisation of the Legendre symbol known as the **Jacobi symbol**, which is defined as

$$\left(\frac{-1}{q}\right) \equiv \left(\frac{-1}{p}\right)^r.$$

Note that both the Legendre and Jacobi symbols are integer-valued. This is consistent with the following well-known characterisation of finite fields $\mathbb{F}_q$ in which -1 is a square number; we give a proof for completeness.

Proposition 10. *Let $q = p^r$ for some odd prime p and positive integer r. We have that -1 is not a square in $\mathbb{F}_q$ precisely when $p \equiv -1 \bmod 4$ and r is odd.*

Proof. Suppose $p \equiv 1 \bmod 4$, then $\frac{p-1}{2}$ is even. By Wilson's theorem, $(p-1)! \equiv -1 \bmod p$. Since

$$\begin{aligned}(p-1)! &= 1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \cdots \times (p-2) \times (p-1) \\ &\equiv 1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(-\frac{p-1}{2}\right) \times \cdots \times (-2) \times (-1) \bmod p \\ &\equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \bmod p \\ &\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \bmod p\end{aligned}$$

it follows that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = -1$$

regarded as an equation over $\mathbb{F}_p$. Thus -1 is a square in $\mathbb{F}_p$ which implies that it is also a square in $\mathbb{F}_q$ since $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$.

If $p \equiv -1 \bmod 4$, then -1_p is not a square in $\mathbb{F}_p$ and hence we can extend $\mathbb{F}_p$ quadratically by Proposition 9 to the field

$$\mathbb{C}_b(\mathbb{F}_p) = \left\{ x1_{\mathbb{D}} + yi \,:\, x, y \in \mathbb{F}_p \right\}$$

of size p^2. In this field, we may regard -1_p by $-1_{\mathbb{D}(\mathbb{F}_p)}$ which is a square since $i^2 = -1_{\mathbb{D}(\mathbb{F}_p)}$. Any field of size p^2 is isomorphic to $\mathbb{C}_b(\mathbb{F}_p)$ and from Proposition 1 $\mathbb{C}_b(\mathbb{F}_p)$ is a subfield of $\mathbb{F}_{p^r}$ precisely when $2 \mid r$. If r is even, we may then identify $-1_{\mathbb{D}(\mathbb{F}_p)}$ by -1_q and this element will be a square in $\mathbb{F}_q$.

Now for the sake of contradiction assume that -1_q is a square in $\mathbb{F}_q = \mathbb{F}_{p^r}$ where $p \equiv -1 \bmod 4$ and r is odd. Then there exists an element $\imath \in \mathbb{F}_{p^r}$ such that $\imath^2 = -1_q$. Consider $K = \{a1_q + b\imath \,:\, a, b \in \mathbb{F}_p\}$. Then K is a subfield of $\mathbb{F}_{p^r}$ with p^2 elements but this implies that 2 divides r which is impossible. Hence our assumption is false and thus -1_q is not a square in $\mathbb{F}_q$ if $p \equiv -1 \bmod 4$ and r is odd. ■

With that in mind, we can also restate the definition of the Jacobi symbol in terms of whether or not -1 is a square in the finite field $\mathbb{F}_q$ as

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 & \text{if } -1 \text{ is a square in } \mathbb{F}_q \\ -1 & \text{if } -1 \text{ is not a square in } \mathbb{F}_q. \end{cases}$$

Remark 13.1. *Proposition 10 above is equivalent to the following:* $\left(\frac{-1}{q}\right) = -1$ *precisely when* $q \equiv -1 \bmod 4$.

3.3.3 Sizes of unit circles in chromogeometry over $\mathbb{F}_q$

Although it is natural to consider the blue (Euclidean) unit circle to be primary, we shall see that it is more beneficial to list the unit circles in ascending complexity: green, red, and blue. This will be the default colour ordering in the presentation of the results in this thesis. We first establish a simple but crucial formula for the sizes of the unit circles in each of the geometries, using a basic counting argument.

Proposition 11. *Let* $S_{b,q}$, $S_{r,q}$, *and* $S_{g,q}$ *be the blue, red, and green unit circles respectively over the field* $\mathbb{F}_q$. *Then*

$$|S_{g,q}| = q - 1 \quad |S_{r,q}| = q - 1 \quad \textit{and} \quad |S_{b,q}| = q - \left(\frac{-1}{q}\right).$$

Proof. Since we can parametrise any element in $S_{g,q}$ as $[t, t^{-1}]$ where $t \in \mathbb{F}_q^\times$, it follows that $|S_{g,q}| = \left|\mathbb{F}_q^\times\right| = q - 1$. By Lemma 4, every element in $S_{r,q}$ except $[-1, 0]$

can be expressed as

$$\left[\frac{1+t^2}{1-t^2}, \frac{2t}{1-t^2}\right]$$

for some $t \in \mathbb{F}_q$, $t \neq \pm 1$. It is then obvious that $|S_{r,q}| = 1 + (q-2) = q-1$.

Finally, from the same lemma, any point on blue unit circle $S_{b,q}$ except $[-1, 0]$ can be written as

$$\left[\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right]$$

for some $t \in \mathbb{F}_q$ such that $1 + t^2 \neq 0$. It thus follows that if -1 is not a square, then the number of such points is $q+1$. Otherwise, there are exactly two solutions to the equation $t^2 = -1$, so the number of points on $S_{b,q}$ is $1 + (q-2) = q-1$. ■

3.3.4 The cyclic group structure on the unit circles

We close this section by establishing a richer algebraic structure in each unit circle. More precisely, we will show that each unit circle is a cyclic group, where the group structure is established in Theorem 12. We shall start from the green unit circle $S_{g,q}$ whose parametrisation is the simplest among all three unit circles.

Proposition 12. *The green unit circle $S_{g,q}$ is a cyclic group of order $q-1$.*

Proof. By Lemma 4, we can write any point on $S_{g,q}$ as $[t, t^{-1}]$. The map $t \mapsto [t, t^{-1}]$ from $\mathbb{F}_q^\times$ to $S_{g,q}$ is an isomorphism and since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, so is $S_{g,q}$. ■

The main key that connects the red to the green unit circle is that a generic red complex number shares the same quadrance with a generic green complex number. More precisely, if $z_1 = x1_{\mathbb{D}} + yj$ is a red complex number and $z_2 = x1_{\mathbb{D}} + yk$ is a green complex number, then

$$Q_r(z_1) = x^2 - y^2 = Q_g(z_2).$$

To capture the connection between the two unit circles more rigorously, observe that there are two non-trivial idempotent elements in $\mathbb{C}_{r,q}$, namely

$$e = \frac{1}{2}(1_{\mathbb{D}} + j) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \text{and} \qquad e^* = \frac{1}{2}(1_{\mathbb{D}} - j) = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

that satisfy

$$e^2 = e \qquad (e^*)^2 = e^* \qquad \text{and} \qquad ee^* = e^*e = 0.$$

Clearly $\{e, e^*\}$ also forms an ordered basis for $\mathbb{C}_{r,q}$ and

$$z = x1_{\mathbb{D}} + yj = (x+y)\,e + (x-y)\,e^*.$$

In addition

$$(x_1 e + y_1 e^*)(x_2 e + y_2 e^*) = x_1 x_2 e + y_1 y_2 e^*$$

so that the multiplication becomes pointwise in this basis.

The above observation implies that there is a pointwise multiplication structure embedded in the red unit circle, similar to that in the green unit circle. This motivates the following important result.

Proposition 13. *The red unit circle $S_{r,q}$ and the green unit circle $S_{g,q}$ are isomorphic as groups. In particular, the red unit circle $S_{r,q}$ is a cyclic group of order $q-1$.*

Proof. Consider the map

$$\begin{aligned} \theta \;:\; & S_r(\mathbb{F}_q) \longrightarrow S_g(\mathbb{F}_q) \\ & x1_{\mathbb{D}} + yj \mapsto x1_{\mathbb{D}} + yk. \end{aligned}$$

Let $z_1 = x_1 1_{\mathbb{D}} + y_1 j$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 j$ be any two red complex numbers. Since $z_1 z_2 = (x_1 x_2 + y_1 y_2) 1_{\mathbb{D}} + (x_1 y_2 + x_2 y_1) j$ it follows that

$$\begin{aligned} \theta(z_1 z_2) &= \theta\left((x_1 x_2 + y_1 y_2) 1_{\mathbb{D}} + (x_1 y_2 + x_2 y_1) j\right) \\ &= (x_1 x_2 + y_1 y_2) 1_{\mathbb{D}} + (x_1 y_2 + x_2 y_1) k \\ &= (x_1 1_{\mathbb{D}} + y_1 k)(x_2 1_{\mathbb{D}} + y_2 k) \\ &= \theta(z_1)\,\theta(z_2). \end{aligned}$$

This shows that θ is a group homomorphism.

Now, if $\theta(z_1) = \theta(z_2)$ then $x_1 1_{\mathbb{D}} + y_1 k = x_2 1_{\mathbb{D}} + y_2 k$. This gives the system of equations (3.11) which we established earlier: $x_1 = x_2$ and $y_1 = y_2$. It follows that $z_1 = z_2$ and therefore θ is one-to-one. Moreover, both unit circles are finite hence θ is also onto, proving the assertion that θ is an isomorphism.

The cyclicity of $S_{r,q}$ then follows from the cyclicity of $S_{g,q}$ established in Proposition 12. ■

Over the blue unit circle, Proposition 11 suggests that we have to discriminate the cases whether -1 is a square in $\mathbb{F}_q$ or not, since the size of the unit circle depends on this distinction. We first assume that -1 is a square in the field, so that $\left(\frac{-1}{q}\right) = 1$. We shall see that the red and the blue unit circles are strongly related.

Proposition 14. *Let $\mathbb{F}_q$ be a field in which $-1 = \imath^2$ is a square. Then the map $\varrho\colon\ S_b(\mathbb{F}_q) \longrightarrow S_r(\mathbb{F}_q)$ defined by*

$$\varrho(x1_{\mathbb{D}} + y\imath) \equiv x1_{\mathbb{D}} + y\imath j$$

is a group isomorphism between $S_b(\mathbb{F}_q)$ and $S_r(\mathbb{F}_q)$. In particular, the blue unit circle $S_{b,q}$ is a cyclic group of order $q-1$.

Proof. If $z_1 = x_1 1_{\mathbb{D}} + y_1 i$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 i$ are two blue complex numbers on $S_{b,q}$, then

$$\begin{aligned}\varrho(z_1 z_2) &= \varrho\left((x_1x_2 - y_1y_2)\,1_{\mathbb{D}} + (x_1y_2 + x_2y_1)\,i\right)\\ &= (x_1x_2 - y_1y_2)\,1_{\mathbb{D}} + (x_1y_2 + x_2y_1)\,\imath j\end{aligned}$$

while

$$\begin{aligned}\varrho(z_1)\,\varrho(z_2) &= (x_1 1_{\mathbb{D}} + y_1\imath j)\,(x_2 1_{\mathbb{D}} + y_2\imath j)\\ &= \left(x_1x_2 + y_1y_2\imath^2\right)1_{\mathbb{D}} + (x_1y_2\imath + x_2y_1\imath)\,j\\ &= (x_1x_2 - y_1y_2)\,1_{\mathbb{D}} + (x_1y_2 + x_2y_1)\,\imath j.\end{aligned}$$

So $\varrho(z_1 z_2) = \varrho(z_1)\,\varrho(z_2)$ and therefore ϱ is a group homomorphism.

Now if $\varrho(z_1) = \varrho(z_2)$ then it follows that $x_1 1_{\mathbb{D}} + y_1\imath j = x_2 1_{\mathbb{D}} + y_2\imath j$. By comparing the entries of the two matrices directly we get that $x_1 = x_2$ and $y_1\imath = y_2\imath$. Since $\imath \neq 0$, it follows that $y_1 = y_2$ and therefore $z_1 = z_2$, showing that ϱ is an injection. Again, ϱ is immediately onto because $S_b(\mathbb{F}_q)$ and $S_r(\mathbb{F}_q)$ are finite sets, so ϱ is a group isomorphism.

The cyclicity of $S_{b,q}$ thus follows from the cyclicity of $S_{r,q}$ established in Proposition 13. ∎

Now we assume that -1 is not a square in $\mathbb{F}_q$, so $\left(\frac{-1}{q}\right) = -1$. Then the map ϱ defined above is not directly defined, but we may then extend our field to the quadratic extension $\mathbb{C}_{b,q}$ of $\mathbb{F}_q$. Observe that $\mathbb{C}_{b,q} \simeq \mathbb{F}_{q^2}$ by the uniqueness of finite fields of a given size. Since $S_{b,q}$ naturally lives in $\mathbb{C}_{b,q}$ and $S_{b,q}$ itself is a group by Theorem 12, we can think of $S_{b,q}$ as a subgroup of the multiplicative group $\mathbb{C}_{b,q}^{\times}$ of $\mathbb{C}_{b,q}$.

Proposition 15. *Over a field $\mathbb{F}_q$ in which -1 is not a square, the blue unit circle $S_{b,q}$ is a cyclic group of order $q+1$.*

Proof. Since $\mathbb{C}_{b,q}$ is a field, its multiplicative group $\mathbb{C}_{b,q}^{\times}$ is cyclic. It follows that $S_{b,q}$ is also cyclic since $S_{b,q}$ is a subgroup of $\mathbb{C}_{b,q}^{\times}$. The order of $S_{b,q}$ is $q+1$ which follows from Proposition 11. ∎

3.4 Special orthogonal groups in chromogeometry

Previously, we have defined three unit circles that correspond to three different commutative $*$-subalgebras of the dihedron algebra $\mathbb{D}$. Recall that we defined the

symmetric bilinear form on $\mathbb{D}$ to be

$$\langle h_1, h_2 \rangle = \frac{1}{2} \operatorname{tr} (h_1 h_2^*)$$

for all $h_1, h_2 \in \mathbb{D}$. This symmetric bilinear form gives rise to the blue, red, and green geometries once we restrict it to the algebras of blue, red, and green complex numbers respectively. We shall investigate these three geometries here in ascending order of complexity stipulated earlier: the green, red, and blue geometry.

If $z_1 = x_1 1_{\mathbb{D}} + y_1 k$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 k$ are two green complex numbers, then

$$\begin{aligned}
\langle z_1, z_2 \rangle &= \frac{1}{2} \operatorname{tr} (z_1 z_2^*) \\
&= \frac{1}{2} \operatorname{tr} \begin{pmatrix} (x_1 + y_1)(x_2 - y_2) & 0 \\ 0 & (x_1 - y_1)(x_2 + y_2) \end{pmatrix} \\
&= \frac{1}{2} \left((x_1 + y_1)(x_2 - y_2) + (x_1 - y_1)(x_2 + y_2) \right).
\end{aligned}$$

With the association $x 1_{\mathbb{D}} + yk \mapsto [x + y, x - y]$ from Proposition 8, the symmetric bilinear form on $\mathbb{C}_{g,q}$ above corresponds to the symmetric bilinear form on $\mathbb{A}$ defined by

$$[x_1, y_1] \cdot_g [x_2, y_2] \equiv \frac{1}{2} (x_1 y_2 + x_2 y_1).$$

We call the geometry induced by $\cdot_g$ the **green geometry** on $\mathbb{A}$.

If $z_1 = z_1 = x_1 1_{\mathbb{D}} + y_1 j$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 j$ are two red complex numbers, then

$$\begin{aligned}
\langle z_1, z_2 \rangle &= \frac{1}{2} \operatorname{tr} (z_1 z_2^*) \\
&= \frac{1}{2} \operatorname{tr} \begin{pmatrix} x_1 x_2 - y_1 y_2 & x_2 y_1 - x_1 y_2 \\ x_2 y_1 - x_1 y_2 & x_1 x_2 - y_1 y_2 \end{pmatrix} \\
&= x_1 x_2 - y_1 y_2.
\end{aligned}$$

With the association $x 1_{\mathbb{D}} + yj \mapsto [x, y]$ from Proposition 8, the symmetric bilinear form on $\mathbb{C}_{r,q}$ above corresponds to the symmetric bilinear form on $\mathbb{A}$ defined by

$$[x_1, y_1] \cdot_r [x_2, y_2] \equiv x_1 x_2 - y_1 y_2.$$

We call the geometry induced by $\cdot_r$ the **red geometry** on $\mathbb{A}$.

Finally, if $z_1 = z_1 = x_1 1_{\mathbb{D}} + y_1 i$ and $z_2 = x_2 1_{\mathbb{D}} + y_2 i$ are two blue complex numbers,

then

$$\begin{aligned}\langle z_1, z_2\rangle &= \frac{1}{2}\operatorname{tr}\left(z_1 z_2^*\right)\\ &= \frac{1}{2}\operatorname{tr}\begin{pmatrix} x_1x_2 + y_1y_2 & x_2y_1 - x_1y_2 \\ x_1y_2 - x_2y_1 & x_1x_2 + y_1y_2 \end{pmatrix}\\ &= x_1x_2 + y_1y_2.\end{aligned}$$

With the association $x1_{\mathbb{D}} + yi \mapsto [x, y]$ from Proposition 8, the symmetric bilinear form on $\mathbb{C}_{b,q}$ above corresponds to the symmetric bilinear form on $\mathbb{A}$ defined by

$$[x_1, y_1] \cdot_b [x_2, y_2] \equiv x_1x_2 + y_1y_2.$$

We call the geometry induced by $\cdot_b$ the **blue geometry** on $\mathbb{A}$.

Denote by $\mathrm{GL}(2, \mathbb{F}_q)$ the group of 2×2 invertible matrices with entries in $\mathbb{F}_q$. Since every matrix in $\mathrm{GL}(2, \mathbb{F}_q)$ can be regarded as an invertible linear transformation, we see that there is a natural right action of $\mathrm{GL}(2, \mathbb{F}_q)$ on the affine plane $\mathbb{A}$ by identifying it with the associated vector space $\mathbb{V}$ of row vectors (x, y). More precisely, given $h = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_q)$ and $[x, y] \in \mathbb{A}$, we define a right action of $\mathrm{GL}(2, \mathbb{F}_q)$ on $\mathbb{A}$ by the rule $[x, y] \cdot h = [h_{11}x + h_{21}y, h_{12}x + h_{22}y]$.

Now we are interested in finding the group of isometries $O_c(\mathbb{F}_q) = O_{c,q}$ in each geometry, that is, those invertible matrices h that preserve that bilinear form $\cdot_c$ in each geometry on $\mathbb{A}$ in the sense that

$$([x_1, y_1] \cdot h) \cdot_c ([x_2, y_2] \cdot h) = [x_1, y_1] \cdot_c [x_2, y_2]$$

for all $[x_1, y_1], [x_2, y_2] \in \mathbb{A}$. The collection of such h must be a subgroup of $\mathrm{GL}(2, \mathbb{F}_q)$. To see this, let h_1 and h_2 be two invertible matrices that preserve the bilinear form $\cdot_c$ on $\mathbb{A}$. We have that

$$\begin{aligned}([x_1, y_1] \cdot h_1h_2) \cdot_c ([x_2, y_2] \cdot h_1h_2) &= (([x_1, y_1] \cdot h_1) \cdot h_2) \cdot_c (([x_2, y_2] \cdot h_1) \cdot h_2)\\ &= ([x_1, y_1] \cdot h_1) \cdot_c ([x_2, y_2] \cdot h_1)\\ &= [x_1, y_1] \cdot_c [x_2, y_2]\end{aligned}$$

where the first equality follows from the $\mathrm{GL}(2, \mathbb{F}_q)$-action on $\mathbb{A}$. Hence h_1h_2 also preserves the bilinear form $\cdot_c$ on $\mathbb{A}$.

The following proposition gives a simple determinant condition satisfied by such matrices.

Proposition 16. *If $h \in O_{c,q}$, then* $\det(h)^2 = 1$.

Proof. By identifying the affine plane $\mathbb{A}$ with the associated vector space $\mathbb{V}$ of row vectors (x, y) via $[x, y] \mapsto (x, y)$, we have that

$$[x_1, y_1] \cdot_g [x_2, y_2] = \frac{1}{2}(x_1 y_2 + x_2 y_1) = (x_1, y_1) \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} (x_1, y_1)^T$$

$$[x_1, y_1] \cdot_r [x_2, y_2] = x_1 x_2 - y_1 y_2 = (x_1, y_1) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} (x_1, y_1)^T$$

$$[x_1, y_1] \cdot_b [x_2, y_2] = x_1 x_2 + y_1 y_2 = (x_1, y_1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (x_1, y_1)^T.$$

Now the affine point $[x, y] \cdot h$ can be identified with the vector $(x, y)\, h$, so by writing $\mathbf{u} = (x_1, y_1)$ and $\mathbf{v} = (x_2, y_2)$ we have that

$$[x_1, y_1] \cdot_c [x_2, y_2] = \mathbf{u} M \mathbf{v}^T$$

where in the green, red, and blue geometries, the value of M is $\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ respectively. In all cases, $\det(M) \neq 0$.

The condition that h preserves the bilinear form $\cdot_c$ on $\mathbb{A}$ is equivalent to the condition $(\mathbf{u}h)\, M\, (\mathbf{v}h)^T = \mathbf{u} M \mathbf{v}^T$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{V}$ which is equivalent to

$$hMh^T = M. \tag{3.14}$$

By taking the determinant of both sides, we get

$$\det(h)^2 \det(M) = \det\left(hMh^T\right) = \det(M).$$

The conclusion follows since $\det(M) \neq 0$. ∎

We will call $O_{c,q}$ the **orthogonal group**, or more precisely the blue, red, and green orthogonal group, whose name is motivated by the orthogonality condition $hMh^T = M$ in (3.14). We call any element of $O_{c,q}$ an **orthogonal matrix**.

The collection of orthogonal matrices of determinant 1 itself is a subgroup of $O_{c,q}$ since the determinant is multiplicative, and this subgroup is the **special**

orthogonal group $SO_c(\mathbb{F}_q) = SO_{c,q}$ and we refer to it as the blue, red, or green special orthogonal group, depending on the context. We call any element of $SO_{c,q}$ a **special orthogonal matrix**, or sometimes just a **rotation matrix**. We will be particularly interested in the analysis pertaining to the special orthogonal group $SO_{c,q}$ in this thesis by considering how $SO_{c,q}$ acts on various spaces.

The special orthogonal group naturally right acts on $\mathbb{A}$ via the restriction of the right action of $\mathrm{GL}(2,\mathbb{F}_q)$ on $\mathbb{A}$. There is then naturally an associated left action of $SO_{c,q}$ on $\mathbb{F}_q^{\mathbb{A}}$, and an associated right action of $SO_{c,q}$ on $\left(\mathbb{F}_q^{\mathbb{A}}\right)^*$ defined as in Chapter 2.

Define a left action of $\mathrm{GL}(2,\mathbb{F}_q)$ on $\mathrm{Pol}_2(\mathbb{F}_q)$ as follows: for a polynumber $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$ and

$$h = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_q)$$

let $h \cdot \pi$ be the polynumber defined by

$$(h \cdot \pi)(\alpha,\beta) \equiv \pi(h_{11}\alpha + h_{21}\beta, h_{12}\alpha + h_{22}\beta). \tag{3.15}$$

This action respects evaluation, that is

$$\varepsilon(h \cdot \pi) = h \cdot \varepsilon(\pi).$$

Note that the $\mathrm{GL}(2,\mathbb{F}_q)$-action on the left-hand side is the action on $\mathrm{Pol}_2(\mathbb{F}_q)$, while the $\mathrm{GL}(2,\mathbb{F}_q)$-action on the right-hand side is the action on $\mathbb{F}_q^{\mathbb{A}}$.

Similarly, the left action of $SO_{c,q}$ on $\mathrm{Pol}_2(\mathbb{F}_q)$ is induced as the restriction of the action of $\mathrm{GL}(2,\mathbb{F}_q)$ on $\mathrm{Pol}_2(\mathbb{F}_q)$ defined in equation (3.15) and so this still respects evaluation, in the sense that for each $h \in SO_{c,q}$,

$$\varepsilon(h \cdot \pi) = h \cdot \varepsilon(\pi). \tag{3.16}$$

Our setup now makes it easy and pleasant to explicitly describe the matrices in each special orthogonal group for the general finite field $\mathbb{F}_q$.

Theorem 14. *The special orthogonal group $SO_{c,q}$ is precisely the unit circle group $S_{c,q}$ consisting of complex numbers with quadrance* 1. *The order of each special orthogonal group is*

$$|SO_{g,q}| = q-1 \quad |SO_{r,q}| = q-1 \quad \textit{and} \quad |SO_{b,q}| = q - \left(\frac{-1}{q}\right).$$

Proof. Take any $h \in SO_{c,q}$ so that $\det(h) = 1$ by the definition of $SO_{c,q}$. Since

over any geometry with colour c, h must be in $\mathbb{C}_{c,q}$, it follows that the condition $\det(h) = 1$ is equivalent to the condition $h \in S_{c,q}$, which implies that $SO_{c,q} \subseteq S_{c,q}$.

Now if $z \in S_{c,q}$ then $Q(z) = \det(z) = 1$ by the definition of $S_{c,q}$. Specifically, z is invertible. To show that z preserves the bilinear form $\cdot_c$ on $\mathbb{A}$, we just need to show that $zMz^T = M$ where M is one of $\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, depending on the geometry.

Over the green geometry, $M = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$ and z has the form $\begin{pmatrix} x+y & 0 \\ 0 & x-y \end{pmatrix}$ where $x^2 - y^2 = 1$. We can indeed verify that

$$zMz^T = \begin{pmatrix} 0 & \frac{1}{2}(x^2-y^2) \\ \frac{1}{2}(x^2-y^2) & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} = M.$$

Over the red geometry, $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and z has the form $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ where $x^2 - y^2 = 1$. By a simple computation,

$$zMz^T = \begin{pmatrix} x^2-y^2 & 0 \\ 0 & -(x^2-y^2) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = M.$$

Finally, over the blue geometry, $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and z has the form $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ where $x^2 + y^2 = 1$, so

$$zMz^T = \begin{pmatrix} x^2+y^2 & 0 \\ 0 & x^2+y^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M.$$

In all three cases, $zMz^T = M$ and thus z preserves the bilinear form $\cdot_c$ on $\mathbb{A}$. Since $\det(z) = 1$, then by definition $z \in SO_{c,q}$ and this proves that $S_{c,q} \subseteq SO_{c,q}$.

We conclude that the two groups are indeed equal and therefore have the same size, and this follows from the size of each unit circle given in Proposition 11. ■

The result above allows us to present the following observation about the action of $SO_{c,q}$ on the affine plane $\mathbb{A}$.

Theorem 15. *The unit circle $S_{c,q}$ is an orbit of the group $SO_{c,q}$ in $\mathbb{A}$. Moreover, the action of $SO_{c,q}$ in $S_{c,q}$ is faithful.*

Proof. From Theorem 14 above, the two groups $S_{c,q}$ and $SO_{c,q}$ are the same. Now if we identify $S_{c,q}$ as the set of affine points, then $[x,y]\cdot h$ can be identified as zh where $z\in\mathbb{C}_{c,q}$ is the complex number associated to $[x,y]$. Since $S_{c,q}$ is closed under group multiplication, it follows that if $[x,y]\in S_{c,q}$, then $[x,y]\cdot h\in S_{c,q}$ for any $h\in SO_{c,q}$.

To see that the action of $SO_{c,q}$ in $S_{c,q}$ is indeed faithful, we need to show that the only solution for h to the equation $[x,y]\cdot h=[x,y]$ for any $[x,y]\in S_{c,q}$ is the identity matrix. The equation $[x,y]\cdot h=[x,y]$ for all $[x,y]\in S_{c,q}$ may then be identified as the equation $zh=z$ for all $z\in S_{c,q}$. Multiplying by z^{-1} to both sides from the left yields $h=1_{\mathbb{D}}$, finishing our claim. ∎

As a final remark, the theory of orthogonal matrices over finite fields over a general geometry has been intensively studied (see [7], [31], [45]). More specifically, the explicit formula for the size of the group $SO_b(n,\mathbb{F}_q)$ consisting of all $n\times n$ orthogonal matrices over $\mathbb{F}_q$ with determinant 1 is known and depends on the parity of n. The case where n is even is more complicated and there is again a distinction whether -1 is a square number or not, which aligns with our obtained formula earlier. The size of the group $SO_b(n,\mathbb{F}_q)$ is given by, for odd n,

$$|SO_b(2m+1,\mathbb{F}_q)|=q^{m^2}\prod_{k=1}^{m}\left(q^{2k}-1\right)$$

and for even n,

$$|SO_b(2m,\mathbb{F}_q)|=\begin{cases}\dfrac{1}{q^m+1}\displaystyle\prod_{k=0}^{m-1}\left(q^{2m}-q^{2k}\right) & \text{if } -1 \text{ is a square in } \mathbb{F}_q\\ \dfrac{1}{q^m+(-1)^m}\displaystyle\prod_{k=0}^{m-1}\left(q^{2m}-q^{2k}\right) & \text{if } -1 \text{ is not a square in } \mathbb{F}_q.\end{cases}$$

It is clear that when $n=2m=2$, the formula above matches with the result established in Theorem 14.

Chapter 4

Circular Integral Functionals

We now introduce the central object of this thesis: a notion of an algebraic integral on the unit circle valid for a general finite field $\mathbb{F}_q$ of odd characteristic, which works in each of the three geometries. This will be a linear functional that takes a 2-polynumber over a finite field $\mathbb{F}_q$ to some element in the same field. Over fields of characteristic zero, polynumbers and polynomial functions are often considered as the same, but their difference becomes more apparent in the finite characteristic situation. We first introduce a linear functional on the function space $\mathbb{F}_q^{\mathbb{A}}$, and then use the evaluation map as a bridge to our algebraic integral on the space of polynumbers.

We identify two defining properties that the classical Riemann integral over the unit circle satisfies: what we call the Locality and Invariance conditions. The Locality condition is that the integral of any polynumber that evaluates to zero on the unit circle is zero. The Invariance condition is that the integral should be invariant under any rotation action on the unit circle.

We will also require that our integral in the finite field case is normalised to have value 1_q on the constant function $1_{\mathbb{F}^{\mathbb{A}}}$, which we will call the Normalisation condition. It is therefore reasonable to require also our proposed algebraic integral in the finite field situation to satisfy these three conditions.

We shall see that the Normalisation, Locality, and Invariance conditions are sufficient to assert the existence and uniqueness of such a *circular algebraic integral* in the green, red, and blue geometries. However as a preliminary we first study the simpler case of a corresponding functional on the space $\mathbb{F}_q^{\mathbb{A}}$ of functions on $\mathbb{A}$. This will be presented in the first two sections in this chapter. We dedicate the last section of this chapter to numerous examples of the computation of our established circular integral functional, which entails summing polynomial functions over the unit circle in each geometry over some finite fields.

The algebraic approach to the integral adopted in this thesis opens up the possibility to investigate harmonic analysis from a new angle, where the functions of interest assume values in the finite field that determines the underlying geometry, or

perhaps a suitable field extension.

The appearance of the group of rotation matrices $SO_{c,q}$ as acting on various spaces indicates a possible connection to modular representation theory, where one studies linear representations of finite groups over a field of positive characteristic. This is also a fairly recent field of study in mathematics which was prominently developed by Richard Brauer [5]. A possible starting point to the subject can be found in Serre [41], while Thevenaz [47] gives some recent developments in modular representation theory.

4.1 Circular integral functionals on $\mathbb{F}_q^{\mathbb{A}}$

We assume that we have chosen one of the blue (b), red (r) or green (g) geometries on the affine space $\mathbb{A}$ over $\mathbb{F}_q$ and we refer to this colour as c. There is then the unit circle $S_{c,q}$ and the group $SO_{c,q}$ of orthogonal matrices of determinant 1 which preserve the bilinear form $\cdot_c$ on $\mathbb{A}$.

Recall that $\mathbb{F}_q^{\mathbb{A}}$ is the vector space of all functions from $\mathbb{A}$ to $\mathbb{F}_q$ of dimension q^2. The multiplicative identity of $\mathbb{F}_q^{\mathbb{A}}$ is the constant function $1_{\mathbb{F}^{\mathbb{A}}}$ defined by $1_{\mathbb{F}^{\mathbb{A}}}(x,y) = 1_q$ for all $[x,y] \in \mathbb{A}$. A linear functional ϕ on $\mathbb{F}_q^{\mathbb{A}}$ will be called a **circular integral functional with respect to** $S_{c,q}$ precisely when the following three conditions are satisfied:

(Normalisation) The functional ϕ maps the constant function $1_{\mathbb{F}^{\mathbb{A}}}$ to 1_q

(Locality) If $f \in \mathbb{F}_q^{\mathbb{A}}$ restricts to the zero function on $S_{c,q}$, then $\phi(f) = 0$

(Invariance) The functional ϕ is $SO_{c,q}$-invariant, that is $\phi \cdot h = \phi$ for all $h \in SO_{c,q}$.

The following result shows that there is a unique circular integral functional with respect to $S_{c,q}$ on the function space $\mathbb{F}_q^{\mathbb{A}}$.

Theorem 16. *There is one and only one circular integral functional with respect to $S_{c,q}$ on $\mathbb{F}_q^{\mathbb{A}}$, namely*

$$\phi(f) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} f(x,y).$$

Proof. First, we note that the definition of ϕ above is well-defined since $|S_{c,q}| \not\equiv 0 \mod p$ by Proposition 11. This functional is normalised, since

$$\phi(1_{\mathbb{F}^{\mathbb{A}}}) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} 1_{\mathbb{F}^{\mathbb{A}}}(x,y) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} 1_q = \frac{|S_{c,q}|}{|S_{c,q}|} = 1_q.$$

Moreover, if f restricts to the zero function on $S_{c,q}$, then $f(x,y) = 0$ for all $[x,y] \in S_{c,q}$, so that clearly $\phi(f) = 0$ and therefore the Locality property holds.

Finally, for any $h \in SO_{c,q}$ and $f \in \mathbb{F}_q^{\mathbb{A}}$, we have that

$$(\phi \cdot h)(f) = \phi(h \cdot f) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} (h \cdot f)(x,y) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} f([x,y] \cdot h).$$

By Theorem 15, $S_{c,q}$ is an $SO_{c,q}$-orbit in $\mathbb{A}$ and so for all $h \in SO_{c,q}$ and $[x,y] \in S_{c,q}$, the point $[x,y] \cdot h$ also lies on $S_{c,q}$. Since $SO_{c,q}$ acts as a group of bijections on $S_{c,q}$,

$$(\phi \cdot h)(f) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} f([x,y] \cdot h) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} f(x,y) = \phi(f).$$

We have that $(\phi \cdot h)(f) = \phi(f)$ for all $f \in \mathbb{F}_q^{\mathbb{A}}$ and so $\phi \cdot h = \phi$ for all $h \in SO_{c,q}$, proving the Invariance property.

Now suppose that η is any circular integral functional on $\mathbb{F}_q^{\mathbb{A}}$ with respect to $S_{c,q}$. We wish to show that $\eta(f) = \phi(f)$ for all $f \in \mathbb{F}_q^{\mathbb{A}}$. Since $\left\{\delta_{[a,b]} : [a,b] \in \mathbb{A}\right\}$ is a basis for $\mathbb{F}_q^{\mathbb{A}}$, it suffices to show that $\eta\left(\delta_{[a,b]}\right) = \phi\left(\delta_{[a,b]}\right)$ for all $[a,b] \in \mathbb{A}$. Now,

$$\phi\left(\delta_{[a,b]}\right) = \frac{1}{|S_{c,q}|} \sum_{[x,y] \in S_{c,q}} \delta_{[a,b]}(x,y) = \begin{cases} \dfrac{1}{|S_{c,q}|} & \text{if } [a,b] \in S_{c,q} \\ 0 & \text{if } [a,b] \notin S_{c,q}. \end{cases} \tag{4.1}$$

If $[a,b] \notin S_{c,q}$, then $\delta_{[a,b]} = 0$ on $S_{c,q}$ and therefore by the Locality property,

$$\eta\left(\delta_{[a,b]}\right) = 0 = \phi\left(\delta_{[a,b]}\right).$$

On the other hand if $[a,b] \in S_{c,q}$, then by the Invariance property, for any $h \in SO_{c,q}$ it follows that

$$\eta\left(\delta_{[a,b]}\right) = \eta\left(h \cdot \delta_{[a,b]}\right) = \eta\left(\delta_{[a,b] \cdot h^{-1}}\right). \tag{4.2}$$

Since $SO_{c,q}$ acts transitively on $S_{c,q}$, η is constant on the set $\left\{\delta_{[a,b]} : [a,b] \in S_{c,q}\right\}$. As a consequence,

$$1_q = \eta(1_{\mathbb{F}^{\mathbb{A}}}) = \eta\left(\sum_{[x,y] \in \mathbb{A}} \delta_{[x,y]}\right) = \eta\left(\sum_{[x,y] \in S_{c,q}} \delta_{[x,y]}\right)$$

where the first equation follows from the Normalisation property, the second equation follows from equation (2.2), and the last equation follows from applying Locality property to the function

$$\sum_{[x,y] \in \mathbb{A}} \delta_{[x,y]} - \sum_{[x,y] \in S_{c,q}} \delta_{[x,y]} = \sum_{[x,y] \in \mathbb{A} \setminus S_{c,q}} \delta_{[x,y]}$$

which restricts to zero on $S_{c,q}$.

By the linearity of η, we have that

$$1_q = \sum_{[x,y]\in S_{c,q}} \eta\left(\delta_{[x,y]}\right) = |S_{c,q}|\,\eta\left(\delta_{[a,b]}\right)$$

where we have used the fact that η is constant on the set $\left\{\delta_{[a,b]} : \ [a,b] \in S_{c,q}\right\}$ from (4.2). Hence if $[a,b] \in S_{c,q}$, then

$$\eta\left(\delta_{[a,b]}\right) = \frac{1}{|S_{c,q}|} = \phi\left(\delta_{[a,b]}\right)$$

and this proves the assertion. ■

4.2 Circular integral functionals on $\mathrm{Pol}_2(\mathbb{F}_q)$

A linear functional ψ on $\mathrm{Pol}_2(\mathbb{F}_q)$ is called a **circular integral functional with respect to** $S_{c,q}$ precisely when the following three conditions are satisfied:

(Normalisation) The functional ψ maps the polynumber $\mathbf{1}$ to 1_q.

(Locality) If $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$ evaluates to the zero function on $S_{c,q}$ then $\psi(\pi) = 0$.

(Invariance) The functional ψ is $SO_{c,q}$-invariant, that is $\psi(h \cdot \pi) = \psi(\pi)$ for any $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$ and $h \in SO_{c,q}$.

Of course these three conditions are virtually identical to the corresponding conditions discussed above for a circular integral functional on $\mathbb{F}_q^{\mathbb{A}}$. However, as we shall see in the proof of existence and uniqueness below, there is quite a subtle difference between the analysis on the function space and on the polynumber space.

Theorem 17. *There is one and only one circular integral functional on* $\mathrm{Pol}_2(\mathbb{F}_q)$ *with respect to* $S_{c,q}$*, namely*

$$\psi_{c,q}(\pi) = \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} \varepsilon(\pi)(x,y)\,. \tag{4.3}$$

Proof. We first note that $\psi_{c,q} = \phi \circ \varepsilon$ where ϕ is the unique circular integral functional on $\mathbb{F}_q^{\mathbb{A}}$ with respect to $S_{c,q}$ established in Theorem 16. Moreover, the division by $|S_{c,q}|$ in the definition of $\psi_{c,q}$ is well-defined since $|S_{c,q}| \neq 0$ as an element of $\mathbb{F}_q$.

We now show that $\psi_{c,q}$ satisfies the Normalisation, Locality, and Invariance properties. The evaluation of the polynumber $\mathbf{1}$ is $\varepsilon(\mathbf{1}) = 1_{\mathbb{F}^{\mathbb{A}}}$ which is the constant

function 1_q. It is therefore easy to verify that the Normalisation condition holds:

$$\psi_{c,q}(\mathbf{1}) = \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} \varepsilon(\mathbf{1})(x,y) = \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} 1_{\mathbb{F}^{\mathbb{A}}}(x,y) = \frac{|S_{c,q}|}{|S_{c,q}|} = 1_q.$$

Now, if a polynumber $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$ evaluates to the zero function on $S_{c,q}$, then that implies $\varepsilon(\pi)(x,y) = 0$ for all $[x,y] \in S_{c,q}$, so

$$\psi_{c,q}(\pi) = \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} \varepsilon(\pi)(x,y) = \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} 0 = 0$$

which establishes the Locality property.

To prove the Invariance property, we note from (3.16) that the $SO_{c,q}$-left-action on $\mathrm{Pol}_2(\mathbb{F}_q)$ respects evaluation, so that

$$\varepsilon(h\cdot\pi) = h\cdot\varepsilon(\pi)$$

for all $h \in SO_{c,q}$ and $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$. Consequently,

$$\begin{aligned}
\psi_{c,q}(h\cdot\pi) &= \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} \varepsilon(h\cdot\pi)(x,y) \\
&= \frac{1}{|S_{c,q}|} \sum_{[x,y]\in S_{c,q}} (h\cdot\varepsilon(\pi))(x,y) \\
&= \phi(h\cdot\varepsilon(\pi)) = \phi(\varepsilon(\pi)) = \psi_{c,q}(\pi)
\end{aligned}$$

where we used the definition of ϕ in the third equation and the Invariance property of ϕ in the following equation. We deduce that $\psi_{c,q}$ is a circular integral functional on $\mathrm{Pol}_2(\mathbb{F}_q)$ with respect to $S_{c,q}$.

Now suppose χ is any circular integral functional on $\mathrm{Pol}_2(\mathbb{F}_q)$ with respect to $S_{c,q}$. We want to show that

$$\chi(\pi) = \psi_{c,q}(\pi)$$

for any $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$. By Theorem 4, any $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$ can be written uniquely as $\pi_1 + \pi_2$ where $\pi_1 \in \mathcal{P}_q$ and $\pi_2 \in \ker(\varepsilon)$. Since $\varepsilon(\pi_2) = 0$, it follows that π_2 also evaluates to the zero function on $S_{c,q}$ and thus by Locality we have that $\chi(\pi_2) = 0$. Hence

$$\chi(\pi) = \chi(\pi_1+\pi_2) = \chi(\pi_1) + \chi(\pi_2) = \chi(\pi_1)$$

which means that we only need to consider the possible values of χ on $\mathcal{P}_q$.

Since $\left\{\pi_{[a,b]} : [a,b] \in \mathbb{A}\right\}$ is a basis for $\mathcal{P}_q$, it therefore suffices to show that

$$\chi\left(\pi_{[a,b]}\right) = \psi_{c,q}\left(\pi_{[a,b]}\right)$$

for all $[a,b] \in \mathbb{A}$. Because $\psi_{c,q} = \phi \circ \varepsilon$, we have that

$$\psi_{c,q}\left(\pi_{[a,b]}\right) = \phi\left(\delta_{[a,b]}\right) = \begin{cases} \dfrac{1}{|S_{c,q}|} & \text{if } [a,b] \in S_{c,q} \\ 0 & \text{if } [a,b] \notin S_{c,q} \end{cases}$$

where the second equality follows from (4.1).

Recall that $\varepsilon\left(\pi_{[a,b]}\right) = \delta_{[a,b]}$ for any $[a,b] \in \mathbb{A}$ from (2.4). If $[a,b] \notin S_{c,q}$, then $\varepsilon\left(\pi_{[a,b]}\right) = \delta_{[a,b]} = 0$ on $S_{c,q}$ which implies that $\chi\left(\pi_{[a,b]}\right) = 0 = \psi_{c,q}\left(\pi_{[a,b]}\right)$ by Locality. Now suppose $[a,b] \in S_{c,q}$. In this case,

$$\varepsilon\left(h \cdot \pi_{[a,b]}\right) = h \cdot \varepsilon\left(\pi_{[a,b]}\right) = h \cdot \delta_{[a,b]} = \delta_{[a,b]\cdot h^{-1}} = \varepsilon\left(\pi_{[a,b]\cdot h^{-1}}\right)$$

where the third equality above follows from (2.5). It follows that

$$h \cdot \pi_{[a,b]} - \pi_{[a,b]\cdot h^{-1}} \in \ker(\varepsilon)$$

and therefore $h \cdot \pi_{[a,b]} - \pi_{[a,b]\cdot h^{-1}}$ evaluates to the zero function on $S_{c,q}$. By the Invariance and Locality of χ,

$$\chi\left(\pi_{[a,b]\cdot h^{-1}}\right) = \chi\left(h \cdot \pi_{[a,b]}\right) = \chi\left(\pi_{[a,b]}\right).$$

This implies that χ is constant on the set $\left\{\pi_{[a,b]} \ : \ [a,b] \in S_{c,q}\right\}$.

Finally,

$$1_q = \chi\left(\mathbf{1}\right) = \chi\left(\sum_{[a,b]\in\mathbb{A}} \pi_{[a,b]}\right) = \chi\left(\sum_{[a,b]\in S_{c,q}} \pi_{[a,b]}\right) = \sum_{[a,b]\in S_{c,q}} \chi\left(\pi_{[a,b]}\right) = |S_{c,q}|\,\chi\left(\pi_{[a,b]}\right)$$

which implies that if $[a,b] \in S_{c,q}$, then

$$\chi\left(\pi_{[a,b]}\right) = \frac{1}{|S_{c,q}|} = \psi_{c,q}\left(\pi_{[a,b]}\right).$$

This concludes the proof. ■

Having established the existence and uniqueness of $\psi_{c,q}$ introduced in Theorem 17 above, we shall call it the **Fourier summation functional**. The next quest is to find explicit formulas for $\psi_{c,q}$ that are effective for computations in each of the three geometries.

By the linearity of $\psi_{c,q}$, it suffices to find a formula for $\psi_{c,q}$ evaluated at basis elements $\alpha^k\beta^l$ of $\mathrm{Pol}_2\left(\mathbb{F}_q\right)$. Moreover, since we know the size of each unit circle by Proposition 11, we only need to find a formula for the following three functionals, which we shall call the green, red, and blue Fourier summation functionals respec-

tively:

$$\psi_{g,q}\left(\alpha^k\beta^l\right) \equiv -\sum_{[x,y]\in S_{g,q}} x^k y^l \tag{4.4}$$

$$\psi_{r,q}\left(\alpha^k\beta^l\right) \equiv -\sum_{[x,y]\in S_{r,q}} x^k y^l \tag{4.5}$$

$$\psi_{b,q}\left(\alpha^k\beta^l\right) \equiv -\left(\frac{-1}{q}\right)\sum_{[x,y]\in S_{b,q}} x^k y^l. \tag{4.6}$$

We also note that while $\psi_{c,q}$ is basically a finite sum, there will be more terms involved if the size of the field increases. We illustrate this by giving some examples of the computation of the Fourier summation functionals $\psi_{c,q}$ on some polynumber $\alpha^k\beta^l$ in three different fields in ascending size and also order of complexity.

4.3 Some examples of Fourier summation functional evaluation

The various calculations presented here were obtained with the help of a computer.

Example 4. *Let $q = 17$. Then $\mathbb{F}_{17} = \{0, 1, 2, \ldots, 15, 16\}$ and the unit circles are*

$$S_{g,17} = \left\{ \begin{array}{cccccccc} [1,1] & [2,9] & [3,6] & [4,13] & [5,7] & [6,3] & [7,5] & [8,15] \\ [9,2] & [10,12] & [11,14] & [12,10] & [13,4] & [14,11] & [15,8] & [16,16] \end{array} \right\}$$

$$S_{r,17} = \left\{ \begin{array}{cccccccc} [1,0] & [16,0] & [6,1] & [6,16] & [11,1] & [11,16] & [3,5] & [3,12] \\ [14,5] & [14,12] & [4,7] & [4,10] & [13,7] & [13,10] & [0,4] & [0,13] \end{array} \right\}$$

$$S_{b,17} = \left\{ \begin{array}{cccccccc} [1,0] & [16,0] & [0,1] & [0,16] & [4,6] & [4,11] & [13,6] & [13,11] \\ [6,4] & [6,13] & [11,4] & [11,13] & [3,3] & [3,14] & [14,3] & [14,14] \end{array} \right\}$$

so that $|S_{g,17}| = |S_{r,17}| = |S_{b,17}| = 16$. Note that $\left(\frac{-1}{17}\right) = 1$ since $-1 = 16 = 4^2$.

As an illustration, here are the three unit circles in the affine plane $\mathbb{A} = \mathbb{A}(\mathbb{F}_{17})$. We first give the pictures of each unit circle in $\mathbb{A}$, then the three unit circles at the same time where we label the horizontal and vertical positions by numbers 0 up to 16.

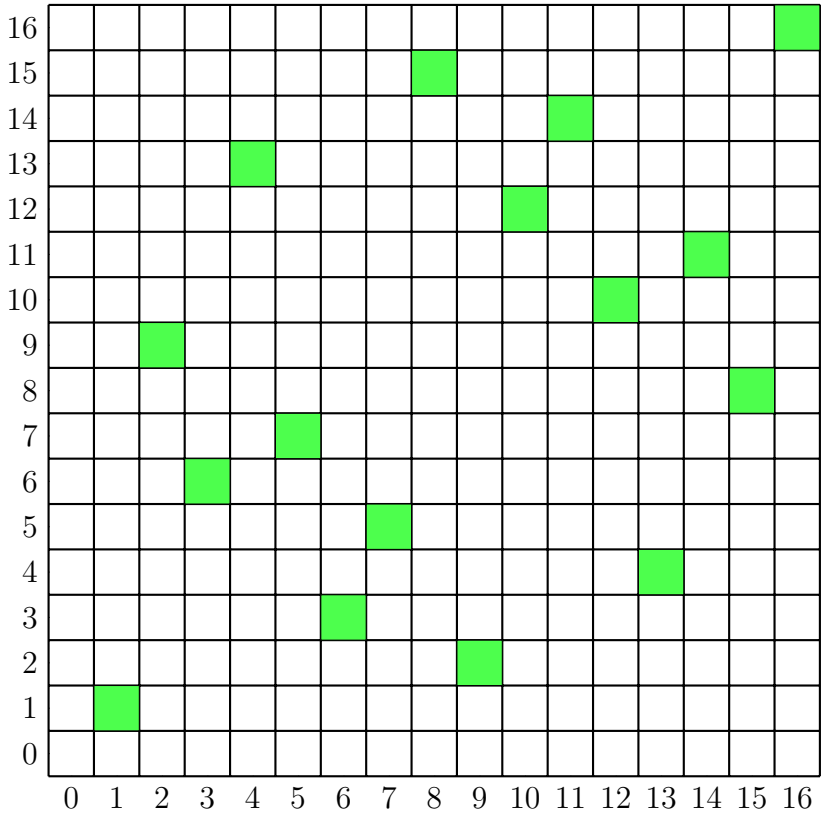

Figure 4.1: The green unit circle $S_{g,17}$.

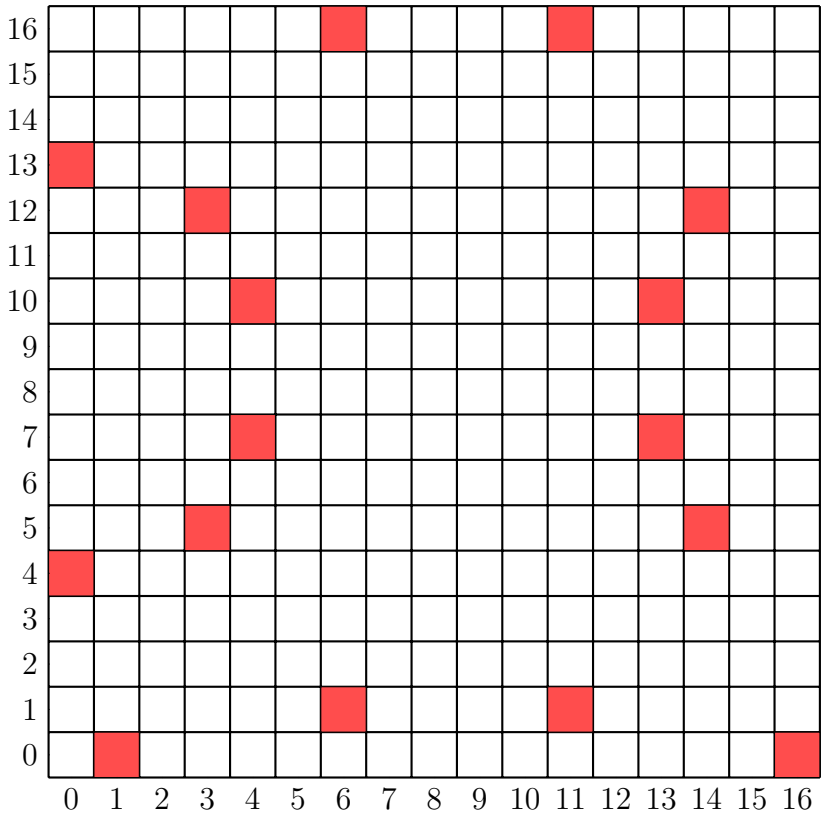

Figure 4.2: The red unit circle $S_{r,17}$.

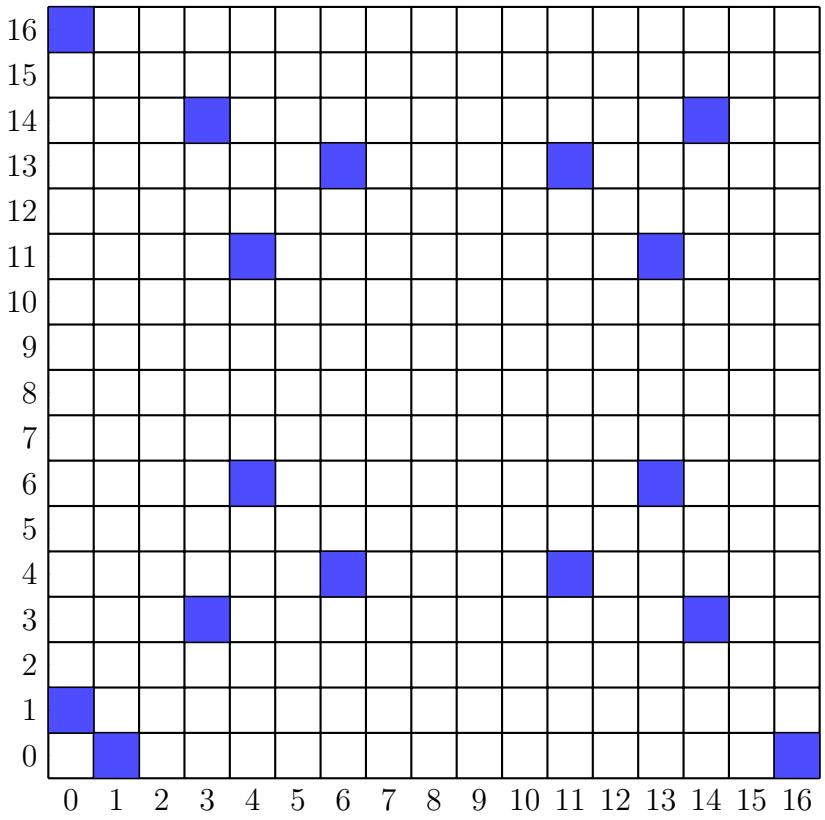

Figure 4.3: The blue unit circle $S_{b,17}$.

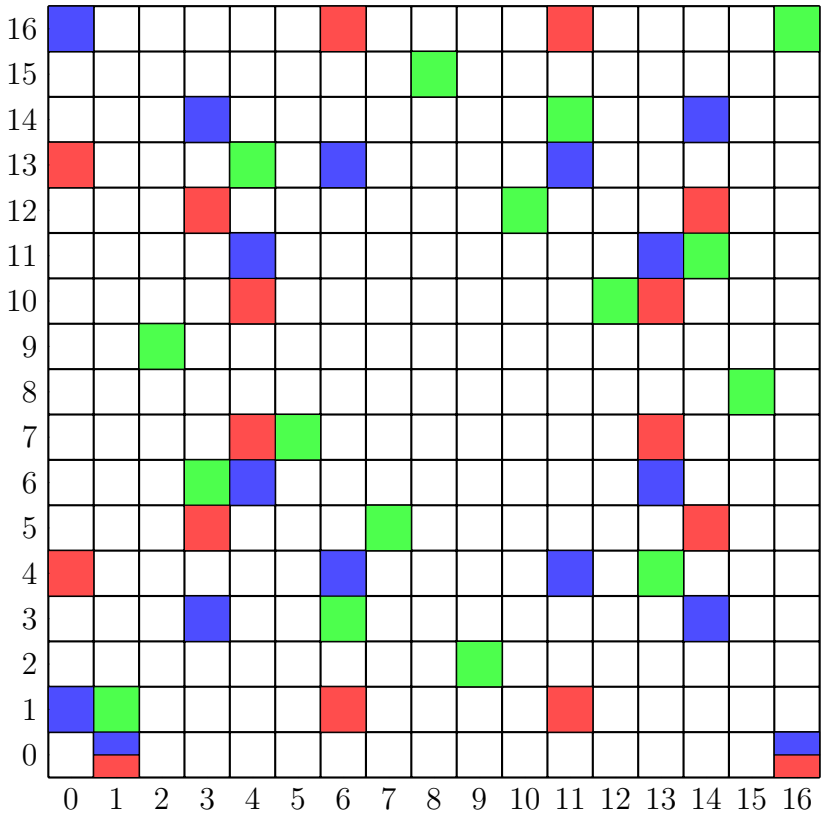

Figure 4.4: The three unit circles $S_{g,17}$, $S_{r,17}$, and $S_{b,17}$ in $\mathbb{A}(\mathbb{F}_{17})$.

This is of course not the only labelling of the horizontal and vertical positions. In fact, since finite fields are not ordered, we can use any permutation of elements of $\mathbb{F}_{17}$ *to label the horizontal and vertical positions.*

There is however one benefit if we relabel the horizontal and vertical positions with the numbers $-8, -7, \ldots, 7, 8$*, since there is symmetry in the three unit circles that we can observe. We illustrate it in Figure 4.5 below.*

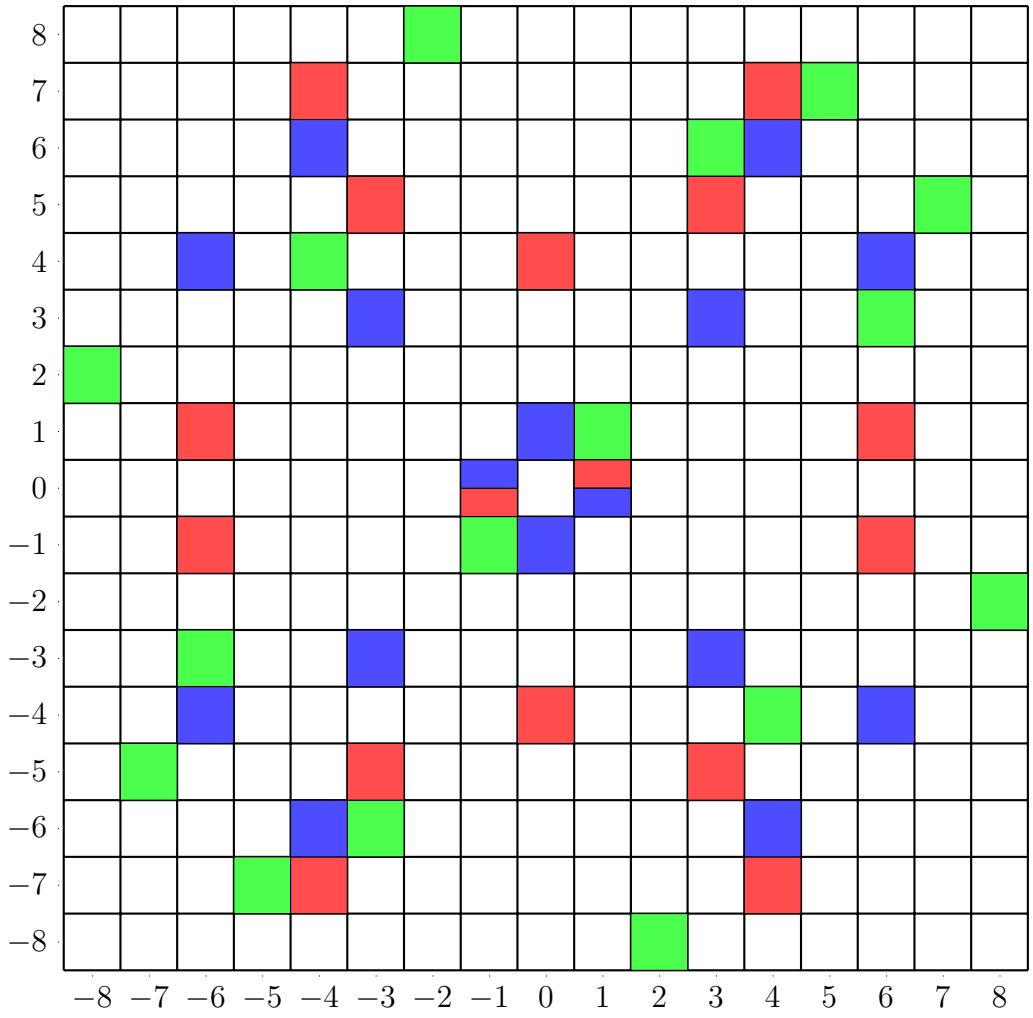

Figure 4.5: Three unit circles $S_{c,17}$ in a different configuration.

Note that in both Figure 4.4 and Figure 4.5, the points $[1, 0]$ *and* $[16, 0] = [-1, 0]$ *are both red and blue since they belong to both* $S_{r,17}$ *and* $S_{b,17}$*.*

It can be verified that, working in all the three geometries over $\mathbb{F}_{17}$*, we have in the green geometry*

$$\psi_{g,17}\left(\alpha^6\beta^4\right) = -\sum_{[x,y]\in S_{g,17}} x^6y^4$$

$$= - \left(\begin{array}{c} 1^6 1^4 + 2^6 9^4 + 3^6 6^4 + 4^6 13^4 + 5^6 7^4 + \\ 6^6 3^4 + 7^6 5^4 + 8^6 15^4 + 9^6 2^4 + 10^6 12^4 + \\ 11^6 14^4 + 12^6 10^4 + 13^6 4^4 + 14^6 11^4 + 15^6 8^4 + 16^6 16^4 \end{array} \right) = 0,$$

which computes to 0. *In the red geometry,*

$$\begin{aligned} \psi_{r,17}\left(\alpha^6\beta^4\right) &= - \sum_{[x,y]\in S_{r,17}} x^6 y^4 \\ &= - \left(\begin{array}{c} 1^6 0^4 + 16^6 0^4 + 0^6 1^4 + 0^6 16^4 + 4^6 6^4 + 4^6 11^4 + 13^6 6^4 + 13^6 11^4 + \\ 6^6 4^4 + 6^6 13^4 + 11^6 4^4 + 11^6 13^4 + 3^6 3^4 + 3^6 14^4 + 14^6 3^4 + 14^6 14^4 \end{array} \right) \end{aligned}$$

which evaluates to 3. *In the blue geometry,*

$$\begin{aligned} \psi_{b,17}\left(\alpha^6\beta^4\right) &= - \left(\frac{-1}{17}\right) \sum_{[x,y]\in S_{b,17}} x^6 y^4 \\ &= - \left(\begin{array}{c} 1^6 0^4 + 16^6 0^4 + 0^6 1^4 + 0^6 16^4 + 11^6 1^4 + 11^6 16^4 + 3^6 5^4 + 3^6 12^4 + \\ 14^6 5^4 + 14^6 12^4 + 4^6 7^4 + 4^6 10^4 + 13^6 7^4 + 13^6 10^4 + 0^6 4^4 + 0^6 13^4 \end{array} \right) \end{aligned}$$

and this again evaluates to 3.

Example 5. *Let* $q = 25 = 5^2$. *We may identify* $\mathbb{F}_{25}$ *as* $\{a + b\omega \,:\, a, b \in \mathbb{F}_5\}$ *where the addition of polynumbers is done in the usual way, but for the multiplication we stipulate that every occurrence of* ω^2 *is replaced by* 2 *since the polynumber* $2 - \alpha^2 \in \mathrm{Pol}\left(\mathbb{F}_5\right)$ *is irreducible over* $\mathbb{F}_5$. *With this identification and the fact that*

$$\left(\frac{-1}{25}\right) = \left(\frac{-1}{5}\right)^2 = 1^2 = 1$$

one may find that the green, red, and blue unit circles respectively are

$$S_{g,25} = \left\{ \begin{array}{c} [1,1] \;\; [2,3] \;\; [3,2] \;\; [4,4] \;\; [\omega, 3\omega] \;\; [2\omega, 4\omega] \;\; [3\omega, \omega] \;\; [4\omega, 2\omega] \\ [1+\omega, 4+\omega] \;\; [1+2\omega, 2+\omega] \;\; [1+3\omega, 2+4\omega] \;\; [1+4\omega, 4+4\omega] \\ [2+\omega, 1+2\omega] \;\; [2+2\omega, 2+3\omega] \;\; [2+3\omega, 2+2\omega] \;\; [2+4\omega, 1+3\omega] \\ [3+\omega, 4+2\omega] \;\; [3+2\omega, 3+3\omega] \;\; [3+3\omega, 3+2\omega] \;\; [3+4\omega, 4+3\omega] \\ [4+\omega, 1+\omega] \;\; [4+2\omega, 3+\omega] \;\; [4+3\omega, 3+4\omega] \;\; [4+4\omega, 1+4\omega] \end{array} \right\}$$

$$S_{r,25} = \left\{ \begin{array}{c} [1,0]\ \ [4,0]\ \ [0,2]\ \ [0,3]\ \ [\omega,1]\ \ [\omega,4]\ \ [4\omega,1]\ \ [4\omega,4] \\ [2,2\omega]\ \ [2,3\omega]\ \ [3,2\omega]\ \ [3,3\omega]\ \ [2\omega,\omega]\ \ [2\omega,4\omega]\ \ [3\omega,\omega]\ \ [3\omega,4\omega] \\ [1+\omega,2+3\omega]\ \ [1+\omega,3+2\omega]\ \ [4+4\omega,2+3\omega]\ \ [4+4\omega,3+2\omega] \\ [1+4\omega,2+2\omega]\ \ [1+4\omega,3+3\omega]\ \ [4+\omega,2+2\omega]\ \ [4+\omega,3+3\omega] \end{array} \right\}$$

$$S_{b,25} = \left\{ \begin{array}{c} [1,0]\ \ [0,1]\ \ [4,0]\ \ [0,4]\ \ [\omega,2]\ \ [\omega,3]\ \ [4\omega,2]\ \ [4\omega,3] \\ [2,\omega]\ \ [3,\omega]\ \ [2,4\omega]\ \ [3,4\omega]\ \ [2\omega,2\omega]\ \ [2\omega,3\omega]\ \ [3\omega,2\omega]\ \ [3\omega,3\omega] \\ [1+\omega,1+4\omega]\ \ [1+\omega,4+\omega]\ \ [4+4\omega,1+4\omega]\ \ [4+4\omega,4+\omega] \\ [1+4\omega,1+\omega]\ \ [4+\omega,1+\omega]\ \ [1+4\omega,4+4\omega]\ \ [4+\omega,4+4\omega] \end{array} \right\}$$

and all of them are of size 24.

With this, one may verify by direct computation that for example

$$\psi_{r,25}\left(\alpha^2\beta^2\right) = -\sum_{[x,y]\in S_{r,25}} x^2y^2 = 3$$
$$\psi_{b,25}\left(\alpha^2\beta^2\right) = -\left(\frac{-1}{25}\right)\sum_{[x,y]\in S_{b,25}} x^2y^2 = -\sum_{[x,y]\in S_{b,25}} x^2y^2 = 2.$$

Example 6. *Let* $q = 27 = 3^3$. *We can identify* $\mathbb{F}_{27}$ *as* $\{a+b\omega+c\omega^2 \ : \ a,b,c\in\mathbb{F}_3\}$ *where again the addition of polynumbers is done in the usual way, and the multiplication is performed by stipulating that whenever* ω^3 *occurs, we replace it with* $1+\omega$, *since the polynumber* $1+\alpha-\alpha^3 \in \mathrm{Pol}\left(\mathbb{F}_3\right)$ *is irreducible over* $\mathbb{F}_3$. *Now the blue unit circle is*

$$S_{b,27} = \left\{ \begin{array}{c} [1,0]\ \ [2,0]\ \ [0,1]\ \ [0,2]\ \ [\omega^2,2\omega+\omega^2]\ \ [\omega^2,\omega+2\omega^2]\ \ [2\omega^2,2\omega+\omega^2] \\ [2\omega^2,\omega+2\omega^2]\ \ [2\omega+\omega^2,\omega^2]\ \ [\omega+2\omega^2,\omega^2]\ \ [2\omega+\omega^2,2\omega^2] \\ [\omega+2\omega^2,2\omega^2]\ \ [2+\omega^2,1+\omega+\omega^2]\ \ [2+\omega^2,2+2\omega+2\omega^2] \\ [2\omega+2\omega^2,1+2\omega+\omega^2]\ \ \ [1+2\omega^2,2+2\omega+2\omega^2] \\ [1+2\omega^2,1+\omega+\omega^2]\ \ [1+\omega+\omega^2,2+\omega^2]\ \ [2+2\omega+2\omega^2,2+\omega^2] \\ [1+\omega+\omega^2,1+2\omega^2]\ \ [\omega+\omega^2,1+2\omega+\omega^2]\ \ [\omega+\omega^2,2+\omega+2\omega^2] \\ [2\omega+2\omega^2,2+\omega+2\omega^2]\ \ [1+2\omega+\omega^2,\omega+\omega^2]\ \ [2+\omega+2\omega^2,\omega+\omega^2] \\ [2+2\omega+2\omega^2,1+2\omega^2]\ \ [1+2\omega+\omega^2,2\omega+2\omega^2]\ \ [2+\omega+2\omega^2,2\omega+2\omega^2] \end{array} \right\}.$$

Using this we may directly compute that

$$\begin{aligned}\psi_{b,27}\left(\alpha^4\beta^6\right) &= -\left(\frac{-1}{27}\right)\sum_{[x,y]\in S_{b,27}} x^4y^6\\ &= -\left(\frac{-1}{3}\right)^3\sum_{[x,y]\in S_{b,27}} x^4y^6\\ &= -\sum_{[x,y]\in S_{b,27}} x^4y^6\\ &= 0.\end{aligned}$$

Obviously such direct calculations can become seriously imposing, especially when working over large prime power fields $\mathbb{F}_q$. So the problem now is: can we find relatively simple and effective alternate formulas for these functionals that avoid having to evaluate the summations directly?

This is where the circular super Catalan numbers, and various associated constants involved in the circular polynumbers, become involved — as we now explore.

Chapter 5

Circular Super Catalan Numbers and Explicit Formulas for $\psi_{c,q}$

In the previous chapter, we have shown that the Fourier summation functional $\psi_{c,q}$ is the unique circular integral functional on $\mathrm{Pol}_2(\mathbb{F}_q)$ with respect to the unit circle $S_{c,q}$ in each geometry. We now aim to give explicit formulas for these functionals evaluated at the monomial $\alpha^k\beta^l$ for natural numbers k and l, and these turn out to involve the circular super Catalan numbers in the red and blue geometries. Somewhat remarkably, the explicit formula for the Fourier summation functional $\psi_{g,q}$ in the green geometry is relatively easy to find, and this is the key to obtaining the formula in the red geometry, which then gives us the formula in the blue geometry in the case when -1 is a square in $\mathbb{F}_q$.

This is perhaps a rather surprising reasoning, since we are accustomed to thinking that the Euclidean geometry is the natural one, while the relativistic geometry is the exotic one. This chain of connection between the three geometries suggests that the relativistic geometry might be more natural than the Euclidean geometry, at least in the narrative of this thesis. We shall see that the derivation of the formula for $\psi_{c,q}$ except in the blue geometry where -1 is not a square rests strongly on the three-fold symmetry of chromogeometry.

The case when -1 is not a square in $\mathbb{F}_q$ over the blue geometry warrants a special treatment, and we shall employ Fourier analysis style arguments to derive a formula for $\psi_{b,q}$. This different approach is reflected not only from the size of the unit circle, which is $q+1$ in this case instead of $q-1$ like the rest, but also from its similarity to the field of real numbers, in which -1 is also not a square.

The Fourier analysis motivated reasoning involved in deriving a formula for $\psi_{b,q}$ in this case suggests there may well be further interesting aspects to the study of finite field Fourier analysis — in the context of function spaces taking values in the finite field, rather than the more traditional context of complex-valued functions. To build such a theory from a purely algebraic point of view is a big quest and is beyond

the scope of this thesis, but our formula for the Fourier summation functionals $\psi_{c,q}$ will likely be an important tool in developing it.

5.1 Explicit formulas for $\psi_{c,q}$ via chromogeometry

5.1.1 The green Fourier summation functional

The explicit formula for $\psi_{g,q}$ rests on the group structure of $\mathbb{F}_q^\times$, which we know to be cyclic of order $q-1$. This involves summing over powers of all elements of $\mathbb{F}_q^\times$ which can easily be found by employing the cyclicity of $\mathbb{F}_q^\times$. We present the result below by rewriting $q-1$ as $|S_{g,q}|$, the size of the green unit circle.

Theorem 18. *For any natural numbers k and l,*

$$\psi_{g,q}\left(\alpha^k\beta^l\right) = \begin{cases} 1_q & \text{if } |S_{g,q}| \mid (k-l), \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

Proof. We first observe, from the parametrisation of $S_{g,q}$, that

$$\psi_{g,q}\left(\alpha^k\beta^l\right) = -\sum_{[x,y]\in S_{g,q}} x^k y^l = -\sum_{t\in\mathbb{F}_q^\times} t^k \left(t^{-1}\right)^l = -\sum_{t\in\mathbb{F}_q^\times} t^{k-l}.$$

Now, since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, let ξ be a generator of $\mathbb{F}_q^\times$. That is, $\mathbb{F}_q^\times = \{\xi^n : 0 \le n \le q-2\}$ where ξ satisfies $\xi^{q-1} = 1_q$ and $\xi \neq 1_q$.

If $k-l$ is divisible by $q-1$, then $k-l = m(q-1)$ for some integer m and thus in this case,

$$\begin{aligned}\psi_{g,q}\left(\alpha^k\beta^l\right) &= -\sum_{t\in\mathbb{F}_q^\times} t^{k-l} = -\sum_{n=0}^{q-2} (\xi^n)^{m(q-1)} = -\sum_{n=0}^{q-2} (\xi^{mn})^{q-1} \\ &= -\sum_{n=0}^{q-2} 1_q = -(q-1)\,1_q = 1_q.\end{aligned}$$

Here we have used the Fermat condition in the fourth equality.

If $k-l$ is not divisible by $q-1$, then

$$\psi_{g,q}\left(\alpha^k\beta^l\right) = -\sum_{t\in\mathbb{F}_q^\times} t^{k-l} = -\sum_{n=0}^{q-2} \left(\xi^n\right)^{k-l} = -\sum_{n=0}^{q-2} \left(\xi^{k-l}\right)^n = -\frac{\left(\xi^{k-l}\right)^{q-1} - 1_q}{\xi^{k-l} - 1_q}$$

where we use a basic geometric series manipulation in the last equation. Since $k-l$ is not divisible by $q-1$, it follows that $\xi^{k-l} \neq 1_q$ and thus the division is well-defined. The numerator simplifies to 0 from the Fermat condition, proving the result. ∎

5.1.2 The red Fourier summation functional

We have seen in Proposition 13 that the red and green unit circles are isomorphic as groups. We shall see the same observation being employed again here, giving a key to deriving an explicit formula for $\psi_{r,q}$.

We begin by introducing some numerical invariants for the red geometry over $\mathbb{F}_q$. The first is the purely geometric invariant $w \equiv \frac{1}{2}|S_{r,q}| = \frac{1}{2}(q-1)$ which is a natural number since q is an odd prime. The second depends also on natural numbers k and l, and is $R_{k,l} \equiv \left\lfloor \frac{k+l}{|S_{r,q}|} \right\rfloor$.

Theorem 19. *For any natural numbers k and l, if q is a power of the odd prime p then*

$$\psi_{r,q}(\alpha^k\beta^l) = \begin{cases} \left(\sum_{|d|\leq R_{k,l}} \left[\alpha^{m+n+dw}\right] \right) \pi_{k,l} \bmod p & \text{if } k=2m,\ l=2n \\ 0 & \text{otherwise.} \end{cases} \tag{5.2}$$

Proof. For any $[x,y] \in S_{r,q}$, let $u = x+y$ and $v = x-y$ so that $[u,v]$ is then in the green unit circle $S_{g,q}$. Inversely the expressions $x = \frac{u+v}{2}$ and $y = \frac{u-v}{2}$ are both well-defined, since in the field $\mathbb{F}_q$ the assumption on q implies that $2 \neq 0$. Thus

$$\begin{aligned} \psi_{r,q}\left(\alpha^k\beta^l\right) &= -\sum_{[x,y]\in S_{r,q}} x^k y^l \\ &= -\sum_{[u,v]\in S_{g,q}} \left(\frac{u+v}{2}\right)^k \left(\frac{u-v}{2}\right)^l \\ &= -\frac{1}{2^{k+l}} \sum_{[u,v]\in S_{g,q}} (u+v)^k (u-v)^l . \end{aligned}$$

This means we can express $\psi_{r,q}\left(\alpha^k\beta^l\right)$ in terms of values of $\psi_{g,q}\left(\alpha^m\beta^n\right)$ for some integers m and n.

Reverting back from u and v to x and y,

$$\begin{aligned} \psi_{r,q}\left(\alpha^k\beta^l\right) &= -\frac{1}{2^{k+l}} \sum_{[x,y]\in S_{g,q}} (x+y)^k (x-y)^l \\ &= -\frac{1}{2^{k+l}} \sum_{[x,y]\in S_{g,q}} \left(\sum_{s=0}^{k} \binom{k}{s} x^s y^{k-s}\right) \left(\sum_{t=0}^{l} (-1)^{l-t} \binom{l}{t} x^t y^{l-t}\right) \\ &= -\frac{1}{2^{k+l}} \sum_{s=0}^{k}\sum_{t=0}^{l} (-1)^{l-t} \binom{k}{s}\binom{l}{t} \sum_{[x,y]\in S_{g,q}} x^{s+t} y^{k+l-(s+t)} \\ &= \frac{(-1)^l}{2^{k+l}} \sum_{s=0}^{k}\sum_{t=0}^{l} (-1)^t \binom{k}{s}\binom{l}{t} \psi_{g,q}\left(\alpha^{s+t}\beta^{k+l-(s+t)}\right) \end{aligned} \tag{5.3}$$

where in the last equality we have used the definition of $\psi_{g,q}$. Note that the minus sign originally in front of the expression has been absorbed.

Now that we have established the connection between the formulas for $\psi_{r,q}$ and $\psi_{g,q}$, we are ready to simplify equation (5.3). By Theorem 18,

$$\psi_{g,q}\left(\alpha^{s+t}\beta^{k+l-(s+t)}\right) = 1_q$$

precisely when $(s+t)-(k+l-(s+t)) = 2(s+t)-(k+l)$ is divisible by $|S_{g,q}| = q-1$, which is equivalent to the equation

$$2(s+t) = k+l+d(q-1) \tag{5.4}$$

for some $d \in \mathbb{Z}$. Note that here s and t are indices in the ranges $0 \leq s \leq k$ and $0 \leq t \leq l$.

If k and l have different parity, then equation (5.4) has no solution for s and t since the left-hand side is even but the right-hand side is odd, so we conclude that $\psi_{g,q}\left(\alpha^{s+t}\beta^{k+l-(s+t)}\right) = 0$ which leads to $\psi_{r,q}\left(\alpha^k\beta^l\right) = 0$. Let us therefore assume that $k+l = 2N$ for some integer N.

Write $R_{k,l} \equiv \left\lfloor \frac{k+l}{|S_{r,q}|} \right\rfloor = \left\lfloor \frac{k+l}{q-1} \right\rfloor$ and therefore by the definition of the floor function,

$$R_{k,l}(q-1) \leq k+l < (R_{k,l}+1)(q-1).$$

If $d \geq R_{k,l}+1$ then

$$k+l+d(q-1) \geq k+l+(R_{k,l}+1)(q-1) > 2(k+l) \geq 2(s+t)$$

while if $d \leq -(R_{k,l}+1)$ then

$$2(s+t) = k+l+d(q-1) \leq k+l-(R_{k,l}+1)(q-1) < 0.$$

In both cases, the equality $2(s+t) = k+l+d(q-1)$ is never achieved.

Next, we write $w \equiv \frac{1}{2}|S_{r,q}| = \frac{1}{2}(q-1)$ and observe that for each d such that $|d| \leq R_{k,l}$, the equation $2(s+t) = k+l+d(q-1)$ gives

$$s+t = N + \frac{q-1}{2}d = N+dw.$$

Since

$$0 \leq N+dw \leq N+R_{k,l}w \leq \frac{1}{2}(k+l) + \frac{1}{2}\left(\frac{k+l}{q-1}\right)(q-1) = k+l$$

and $0 \leq s \leq k$, $0 \leq t \leq l$, the equation $s+t = N+dw$ has solutions for s and t. We

therefore conclude that the equation $2(s+t) = k + l + d(q-1)$ has solutions for s and t precisely when $|d| \leq R_{k,l}$.

Consequently, we can simplify the right-hand side of equation (5.3) to

$$\psi_{r,q}\left(\alpha^k \beta^l\right) = \frac{(-1)^l}{2^{2N}} \sum_{|d| \leq R_{k,l}} \sum_{s=0}^{k} (-1)^{N+dw-s} \binom{k}{s} \binom{l}{N+dw-s} 1_q. \tag{5.5}$$

For each d,

$$\sum_{s=0}^{k} (-1)^{N+dw-s} \binom{k}{s} \binom{l}{N+dw-s} = \left[\alpha^{N+dw}\right] (1+\alpha)^k (1-\alpha)^l$$

so equation (5.5) reduces to

$$\psi_{r,q}\left(\alpha^k \beta^l\right) = \frac{(-1)^l}{2^{2N}} \sum_{|d| \leq R_{k,l}} \left[\alpha^{N+dw}\right] (1+\alpha)^k (1-\alpha)^l 1_q. \tag{5.6}$$

Using Lemma 2,

$$\left[\alpha^{N+dw}\right] (1+\alpha)^k (1-\alpha)^l = (-1)^l \left[\alpha^{N-dw}\right] (1+\alpha)^k (1-\alpha)^l$$

for all $|d| \leq R_{k,l}$ so if l is odd, (5.6) simplifies to

$$\psi_{r,q}\left(\alpha^k \beta^l\right) = 0.$$

We may therefore write $k = 2m$ and $l = 2n$. In this case, $N = m + n$ and equation (5.6) becomes

$$\begin{aligned} \psi_{r,q}\left(\alpha^k \beta^l\right) &= \frac{1}{2^{2m+2n}} \sum_{|d| \leq R_{k,l}} \left[\alpha^{m+n+dw}\right] (1+\alpha)^{2m} (1-\alpha)^{2n} 1_q \\ &= \left(\sum_{|d| \leq R_{k,l}} \left[\alpha^{m+n+dw}\right] \right) \pi_{2m,2n} \bmod p \end{aligned}$$

as desired. ■

The above theorem gives us an exact formula for the unique circular integral functional $\psi_{r,q}$ in terms of a sum of coefficients of the circular polynumber $\pi_{k,l}$. In a special case, the formula restricts to just involve the rational super Catalan numbers $\Omega(m,n)$ suitably reduced modulo p.

Theorem 20. *In the red geometry over $\mathbb{F}_q$, where $q = p^r$ for some prime p, and for any natural numbers k and l such that $0 \leq k + l < q - 1$, the Fourier summation*

functional $\psi_{r,q}$ has the form

$$\psi_{r,q}\left(\alpha^k\beta^l\right) = (-1)^n\,\Omega(m,n) \bmod p.$$

Proof. From Theorem 19 we deduce that if $0 \leq k+l < q-1$ then $R_{k,l} = 0$ and so

$$\begin{aligned}\psi_{r,q}\left(\alpha^k\beta^l\right) &= \left[\alpha^{m+n}\right]\pi_{2m,2n} \bmod p \\ &= (-1)^n\left[\alpha^{m+n}\right](-1)^n\,\pi_{2m,2n} \bmod p \\ &= (-1)^n\,\Omega\left(m,n\right) \bmod p\end{aligned}$$

where the last equation follows from Theorem 11, which is a restatement of the identity given by Georgiadis, Munemasa, and Tanaka [18] given in Theorem 10. ∎

5.1.3 The blue Fourier summation functional when $\left(\frac{-1}{q}\right) = 1$

If -1 is a square in $\mathbb{F}_q$, then $\left(\frac{-1}{q}\right) = 1$ and there exists some element $\imath \in \mathbb{F}_q$ such that $\imath^2 = -1$. From Proposition 14, the red and blue unit circles are isomorphic through the map ϱ defined by

$$\begin{aligned}\varrho\ :\ S_b\left(\mathbb{F}_q\right) &\to S_r\left(\mathbb{F}_q\right) \\ x1_{\mathbb{D}} + yi &\mapsto x1_{\mathbb{D}} + y\imath j.\end{aligned}$$

We may then regard ϱ as a map that sends the point $[x,y]$ on the blue unit circle to the point $[x,y\imath]$ on the red unit circle.

An explicit formula for $\psi_{b,q}$ can now be found from the previous formula for $\psi_{r,q}$, by utilising the bijectivity of ϱ.

Theorem 21. *In the blue geometry over $\mathbb{F}_q$ when -1 is a square, define a geometric constant $w \equiv \frac{1}{2}\left|S_{b,q}\right| = \frac{1}{2}\left(q-1\right)$. For any natural numbers k and l, let $R_{k,l} \equiv \left\lfloor \frac{k+l}{\left|S_{b,q}\right|} \right\rfloor$. We have that*

$$\psi_{b,q}\left(\alpha^k\beta^l\right) = \begin{cases} \left(\sum_{|d|\leq R_{k,l}} \left[\alpha^{m+n+dw}\right]\right)(-1)^n\,\pi_{k,l} \bmod p & \text{if } k=2m,\ l=2n \\ 0 & \text{otherwise.}\end{cases}$$

Proof. Using the bijection ϱ above we compute that

$$\psi_{b,q}\left(\alpha^k\beta^l\right) = -\sum_{[x,y]\in S_{b,q}} x^k y^l = -\left(-\imath\right)^l \sum_{[x,y\imath]\in S_{r,q}} x^k\left(y\imath\right)^l.$$

By renaming the point $[x, y\imath] \in S_r(\mathbb{F}_q)$ to $[x, y]$, we obtain a bridge from the blue Fourier summation functional $\psi_{b,q}$ to the red Fourier summation functional $\psi_{r,q}$ as follows:

$$\begin{aligned}\psi_{b,q}\left(\alpha^k\beta^l\right) &= -(-\imath)^l \sum_{[x,y\imath]\in S_{r,q}} x^k (y\imath)^l \\ &= -(-\imath)^l \sum_{[x,y]\in S_{r,q}} x^k y^l \\ &= (-\imath)^l \psi_{r,q}\left(\alpha^k\beta^l\right). \end{aligned} \tag{5.7}$$

The result then follows from the formula of $\psi_{r,q}\left(\alpha^k\beta^l\right)$ given in Theorem 19 above. If either k or l is odd, then $\psi_{b,q}\left(\alpha^k\beta^l\right) = 0$, and if $k = 2m$ and $l = 2n$, then

$$\begin{aligned}\psi_{b,q}\left(\alpha^k\beta^l\right) &= (-\imath)^{2n} \psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right) \\ &= \left(\sum_{|d|\leq R_{k,l}} \left[\alpha^{m+n+dw}\right]\right)(-1)^n \pi_{k,l} \bmod p.\end{aligned}$$

This concludes the proof. ■

Corollary 21.1. *If -1 is a square in $\mathbb{F}_q$, then the blue and red Fourier summation functional $\psi_{b,q}$ and $\psi_{r,q}$ are related in the following manner: for all natural numbers k and l,*

$$\psi_{b,q}\left(\alpha^k\beta^l\right) = \begin{cases} \psi_{r,q}\left(\alpha^k\beta^l\right) & \text{if } l \not\equiv 2 \bmod 4 \\ -\psi_{r,q}\left(\alpha^k\beta^l\right) & \text{if } l \equiv 2 \bmod 4. \end{cases}$$

5.2 An explicit formula for $\psi_{b,q}$ when $\left(\frac{-1}{q}\right) = -1$ via complex summations

Up until now, we have established an explicit formula for $\psi_{c,q}$ in the green, red, and blue geometries where we assumed -1 is a square in $\mathbb{F}_q$ when working in the blue geometry. The key idea of this derivation rests on the isomorphism of all the unit circles in each geometry, which is a phenomenon of chromogeometry.

We conclude our analysis by giving an explicit formula for $\psi_{b,q}$ when -1 is not a square in $\mathbb{F}_q$, that is, $\left(\frac{-1}{q}\right) = -1$. While there is no element $\imath \in \mathbb{F}_q$ such that $\imath^2 = -1$, we may think of $\mathbb{F}_q$ as being embedded in the algebra of blue complex numbers $\mathbb{C}_{b,q} = \mathbb{C}_b(\mathbb{F}_q)$ via the identification $t \mapsto t1_{\mathbb{D}}$ and carry our analysis in $\mathbb{C}_{b,q}$ which by Theorem 13 is a field of size q^2. We therefore can think of $\mathbb{C}_{b,q}$ as a quadratic field

extension of $\mathbb{F}_q$ and identify $\psi_{b,q}\left(\alpha^k\beta^l\right)$ as

$$\psi_{b,q}\left(\alpha^k\beta^l\right)1_{\mathbb{D}} = \sum_{[x,y]\in S_{b,q}} x^k y^l 1_{\mathbb{D}}. \tag{5.8}$$

Now every blue complex number $z = x1_{\mathbb{D}} + yi$ that lies on the blue unit circle $S_{b,q}$ is determined from the special property $z^{-1} = z^*$, so if $z = x1_{\mathbb{D}} + yi \in S_{b,q}$ then identity (3.6) can be written as

$$x1_{\mathbb{D}} = \frac{1}{2}\left(z + z^{-1}\right) \qquad \text{and} \qquad y1_{\mathbb{D}} = -\frac{1}{2}\left(z - z^{-1}\right)i.$$

This allows us to find a formula for $\psi_{b,q}\left(\alpha^k\beta^l\right)1_{\mathbb{D}}$ in (5.8) as an (algebraic) function in z instead of a function in x and y given by

$$\begin{aligned}
\psi_{b,q}\left(\alpha^k\beta^l\right)1_{\mathbb{D}} &= \sum_{[x,y]\in S_{b,q}} x^k y^l 1_{\mathbb{D}} \\
&= \sum_{[x,y]\in S_{b,q}} \left(x1_{\mathbb{D}}\right)^k \left(y1_{\mathbb{D}}\right)^l \\
&= \sum_{z\in S_{b,q}} \left(\frac{1}{2}\left(z + z^{-1}\right)\right)^k \left(-\frac{1}{2}\left(z - z^{-1}\right)i\right)^l.
\end{aligned} \tag{5.9}$$

The last summation in (5.9) in particular tells us that a formula for $\psi_{b,q}\left(\alpha^k\beta^l\right)$ can be found in reference to summations of integer powers of complex numbers over the blue unit circle.

More precisely, we want to find a formula for $\sum_{z\in S_{b,q}} z^k$ where k is any integer. We shall see below that an explicit formula for the above summation can be found by utilising the cyclic group structure of the blue unit circle. Since the green and red unit circles are also cyclic groups, we present the following theorem in its full generality.

Theorem 22. *Let $\mathbb{F}_q$ be a finite field with size $q = p^r$ for some odd prime p and positive integer r. Over the green, red, and blue geometries, we have that*

$$\sum_{z\in S_{c,q}} z^k = \begin{cases} |S_{c,q}|\,1_{\mathbb{D}} & \text{if } |S_{c,q}| \text{ divides } k \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Over the green geometry, red geometry, and blue geometry where -1 is a square in $\mathbb{F}_q$, the three unit circles are cyclic of order $q-1$ by Proposition 12, Proposition 13, and Proposition 14. Thus there is a generator $\zeta \in S_{c,q}$ such that

$S_{c,q} = \{\xi^m \,:\, 0 \leq m \leq q-2\}$ and $\xi^{q-1} = 1_{\mathbb{D}}$. It follows that

$$\sum_{z \in S_{c,q}} z^k = 1^k + \xi^k + \left(\xi^2\right)^k + \cdots + \left(\xi^{q-2}\right)^k = \sum_{m=0}^{q-2} \left(\xi^m\right)^k = \sum_{m=0}^{q-2} \xi^{km}$$

which we may realise as a simple geometric series.

If $q-1 = |S_{c,q}|$ divides k, then $k = l\,(q-1)$ for some integer l and therefore

$$\sum_{z \in S_{c,q}} z^k = \sum_{m=0}^{q-2} \xi^{km} = \sum_{m=0}^{q-2} \xi^{l(q-1)m} = \sum_{m=0}^{q-2} \left(\xi^{q-1}\right)^{lm} = \sum_{m=0}^{q-2} 1_{\mathbb{D}} = (q-1)\, 1_{\mathbb{D}} = |S_{c,q}|\, 1_{\mathbb{D}}.$$

If $|S_{r,q}|$ does not divide k, then $\xi^k \neq 1_{\mathbb{D}}$ and consequently

$$\begin{aligned} \sum_{z \in S_{c,q}} z^k = \sum_{m=0}^{q-2} \xi^{km} &= \left(\left(\xi^k\right)^{q-1} - 1_{\mathbb{D}}\right)\left(\xi^k - 1_{\mathbb{D}}\right)^{-1} \\ &= \left(\left(\xi^{q-1}\right)^k - 1_{\mathbb{D}}\right)\left(\xi^k - 1_{\mathbb{D}}\right)^{-1} = 0. \end{aligned}$$

Now over the blue geometry where -1 is not a square in $\mathbb{F}_q$, the blue unit circle $S_{b,q}$ is cyclic of order $q+1$ by Proposition 15 so there exists a generator $\xi \in S_{b,q}$ such that $S_{b,q} = \{\xi^m \,:\, 0 \leq m \leq q\}$ and $\xi^{q+1} = 1_{\mathbb{D}}$. The claim is proved in a similar manner. Since

$$\sum_{z \in S_{b,q}} z^k = \sum_{m=0}^{q} \xi^{km}$$

it follows that if $q+1 = |S_{b,q}|$ divides k, then $k = l\,(q+1)$ for some integer l and

$$\sum_{z \in S_{b,q}} z^k = \sum_{m=0}^{q} \xi^{km} = \sum_{m=0}^{q} \xi^{l(q+1)m} = \sum_{m=0}^{q} 1_{\mathbb{D}} = |S_{b,q}|\, 1_{\mathbb{D}}.$$

If $|S_{b,q}|$ does not divide k then $\xi^k \neq 1_{\mathbb{D}}$ and therefore

$$\sum_{z \in S_{b,q}} z^k = \sum_{m=0}^{q} \xi^{km} = \left(\left(\xi^{q+1}\right)^k - 1_{\mathbb{D}}\right)\left(\xi^k - 1_{\mathbb{D}}\right)^{-1} = 0$$

as required. ■

We note that summation of integer powers of complex numbers is akin to an integration of the form

$$\int_{S^1} e^{in\theta}\, d\mu$$

which is fundamental for classical Fourier analysis. Here μ denotes a normalised measure on the unit circle S^1. Furthermore, notice a similarity between the result of

Theorem 22 and the integral above since

$$\int_{S^1} e^{in\theta}\, d\mu = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n \neq 0 \end{cases}$$

by choosing $d\mu = \dfrac{1}{2\pi}$.

With Theorem 22 in mind, we are now ready to present a formula for $\psi_{b,q}\left(\alpha^k \beta^l\right)$ which is parallel to the other Fourier summation formulas that we have already obtained.

Theorem 23. *In the blue geometry over $\mathbb{F}_q$ when -1 is not a square, define a geometric constant $w \equiv \frac{1}{2}\left|S_{b,q}\right| = \frac{1}{2}(q+1)$, and for any natural numbers k and l, let $R_{k,l} \equiv \left\lfloor \frac{k+l}{\left|S_{b,q}\right|} \right\rfloor$. We have that*

$$\psi_{b,q}\left(\alpha^k \beta^l\right) = \begin{cases} \left(\displaystyle\sum_{|d| \leq R_{k,l}} \left[\alpha^{m+n+dw}\right] \right) (-1)^n \pi_{k,l} \bmod p & \text{if } k = 2m,\ l = 2n \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By identifying $\psi_{b,q}\left(\alpha^k \beta^l\right) \in \mathbb{F}_q$ with $\psi_{b,q}\left(\alpha^k \beta^l\right) 1_{\mathbb{D}} \in \mathbb{C}_{b,q}$, from equation (5.9) we have that

$$\begin{aligned} \psi_{b,q}\left(\alpha^k \beta^l\right) 1_{\mathbb{D}} &= \sum_{z \in S_{b,q}} \left(\frac{1}{2}\left(z + z^{-1}\right)\right)^k \left(-\frac{1}{2}\left(z - z^{-1}\right) i\right)^l \\ &= \frac{(-1)^l}{2^{k+l}} i^l \sum_{z \in S_{b,q}} \left(z + z^{-1}\right)^k \left(z - z^{-1}\right)^l \\ &= \frac{(-1)^l}{2^{k+l}} i^l \sum_{z \in S_{b,q}} \left(\sum_{s=0}^{k} \binom{k}{s} z^{2s-k} \right) \left(\sum_{t=0}^{l} (-1)^{l-t} \binom{l}{t} z^{2t-l} \right). \end{aligned} \tag{5.10}$$

Since all of the summations in the right-hand side of equation (5.10) contain finitely many terms, we can rearrange the triple summations above to get

$$\psi_{b,q}\left(\alpha^k \beta^l\right) 1_{\mathbb{D}} = \frac{1}{2^{k+l}} i^l \sum_{s=0}^{k} \sum_{t=0}^{l} (-1)^t \binom{k}{s} \binom{l}{t} \sum_{z \in S_{b,q}} z^{2(s+t)-(k+l)}. \tag{5.11}$$

Here, we have implicitly written $(-1)^{l-t} = (-1)^{l+t}$ and moved the factor $(-1)^l$ to the front of the summations.

By Theorem 22, it follows that

$$\sum_{z\in S_{b,q}} z^{2(s+t)-(k+l)} = \begin{cases} (q+1)\,1_{\mathbb{D}} & \text{if } q+1 \text{ divides } 2\,(s+t)-(k+l) \\ 0 & \text{otherwise} \end{cases}$$

and so the right-hand side of equation (5.11) will vanish except for those s and t for which the equation

$$2\,(s+t) = k+l+d\,(q+1) \tag{5.12}$$

has solutions. This allows us to argue as in the proof of Theorem 19.

If k and l have different parity then there is no integer solution d to the equation (5.12) since the left-hand side is even but the right-hand side is odd. We can therefore assume that $k+l=2N$ for some integer N. Next, by letting $R_{k,l} \equiv \left\lfloor \frac{k+l}{|S_{b,q}|} \right\rfloor = \left\lfloor \frac{k+l}{q+1} \right\rfloor$ we claim that $2\,(s+t) = (k+l)+d\,(q+1)$ has solutions for s and t precisely when $|d| \leq R_{k,l}$.

Indeed, if $d \geq R_{k,l}+1$, then

$$k+l+d\,(q+1) \geq k+l+(R_{k,l}+1)\,(q+1) > 2\,(k+l) \geq 2\,(s+t)$$

and if $d \leq -\,(R_{k,l}+1)$ then

$$k+l+d\,(q+1) \leq k+l-(R_{k,l}+1)\,(q+1) < 0 \leq 2\,(s+t)\,.$$

In both cases, equality is never attained.

Moreover, if $|d| \leq R_{k,l}$ then

$$0 \leq 2\,(s+t) = 2N+d\,(q+1) \leq k+l+R_{k,l}\,(q+1) \leq 2\,(k+l)$$

where in the last inequality we used the fact that

$$k+l+R_{k,l}\,(q+1) \leq k+l+\frac{k+l}{q+1}\,(q+1) = 2\,(k+l)\,.$$

Since $0 \leq s \leq k$ and $0 \leq t \leq l$, we have that $0 \leq s+t \leq k+l$ and therefore the equation (5.12) has solutions for s and t.

Each d where $|d| \leq R_{k,l}$ then contributes to the specific equation

$$s+t = \frac{1}{2}\,(k+l)+\frac{1}{2}\,(q+1)\,d = N+dw$$

so by letting $w = \frac{1}{2}|S_{b,q}|$, we can simplify equation (5.11) to

$$\psi_{b,q}\left(\alpha^k\beta^l\right)1_{\mathbb{D}} = \frac{1}{2^{2N}}i^l \sum_{|d|\leq R_{k,l}} \sum_{s=0}^{k} (-1)^{N+dw-s} \binom{k}{s}\binom{l}{N+dw-s}1_{\mathbb{D}}. \tag{5.13}$$

The same analysis pertains as in the red geometry: we have that

$$\sum_{s=0}^{k} (-1)^{N+dw-s} \binom{k}{s}\binom{l}{N+dw-s} = \left[\alpha^{N+dw}\right](1+\alpha)^k(1-\alpha)^l$$

so if k and l are both odd, then the right-hand side of (5.13) vanishes since

$$\left[\alpha^{N+dw}\right](1+\alpha)^k(1-\alpha)^l = (-1)^l\left[\alpha^{N-dw}\right](1+\alpha)^k(1-\alpha)^l$$

by Lemma 2, and if $k = 2m$ and $l = 2n$, then we may rewrite equation (5.13) as

$$\begin{aligned}
\psi_{b,q}\left(\alpha^k\beta^l\right)1_{\mathbb{D}} &= \frac{1}{2^{2N}}i^l \sum_{|d|\leq R_{k,l}} \left(\left[\alpha^{N+dw}\right](1+\alpha)^k(1-\alpha)^l\right)1_{\mathbb{D}} \\
&= \frac{1}{2^{2(m+n)}}i^{2n} \sum_{|d|\leq R_{k,l}} \left(\left[\alpha^{m+n+dw}\right](1+\alpha)^{2m}(1-\alpha)^{2n}\right)1_{\mathbb{D}} \\
&= \frac{(-1)^n}{2^{2(m+n)}} \sum_{|d|\leq R_{k,l}} \left[\alpha^{m+n+dw}\right](1+\alpha)^{2m}(1-\alpha)^{2n}1_{\mathbb{D}} \\
&= \left(\sum_{d\leq R_{k,l}} \left[\alpha^{m+n+dw}\right](-1)^n\left(\frac{1+\alpha}{2}\right)^{2m}\left(\frac{1-\alpha}{2}\right)^{2n}\right)1_{\mathbb{D}}.
\end{aligned}$$

It then follows that

$$\begin{aligned}
\psi_{b,q}\left(\alpha^k\beta^l\right) &= \sum_{d\leq R_{k,l}} \left[\alpha^{m+n+dw}\right](-1)^n\left(\frac{1+\alpha}{2}\right)^{2m}\left(\frac{1-\alpha}{2}\right)^{2n}1_q \\
&= \left(\sum_{|d|\leq R_{k,l}} \left[\alpha^{m+n+dw}\right]\right)(-1)^n\,\pi_{2m,2n} \bmod p.
\end{aligned}$$

This completes the proof. ■

5.2.1 A combined formula for $\psi_{b,q}$

The established formulas for $\psi_{b,q}$ in both settings show that they are exactly the same with the exception of the geometric constant w and consequently the quantities $R_{k,l}$. When -1 is a square, $w = \frac{1}{2}(q-1)$ while when -1 is not a square, $w = \frac{1}{2}(q+1)$.

Since the value of $R_{k,l}$ depends on that of w, a factor of $q-1$ or $q+1$ will be present in the computation of $R_{k,l}$. However, we can combine both formulas into a

single formula by recalling from Proposition 11 that

$$|S_{b,q}| = q - \left(\frac{-1}{q}\right) = \begin{cases} q-1 & \text{if } -1 \text{ is a square in } \mathbb{F}_q \\ q+1 & \text{if } -1 \text{ is not a square in } \mathbb{F}_q. \end{cases}$$

Such a unified formula may then be expressed involving $|S_{b,q}|$ in a fashion which makes it similar to the formula for $\psi_{g,q}$ and $\psi_{r,q}$ established in Theorem 18 and 19 respectively.

Theorem 24 (A unified formula for $\psi_{b,q}$)**.** *In the blue geometry over a general finite field $\mathbb{F}_q$ of size $q = p^r$ for some prime $p > 2$ and positive integer r, define a geometric constant*

$$w \equiv \frac{1}{2}|S_{b,q}| = \frac{1}{2}\left(q - \left(\frac{-1}{q}\right)\right).$$

For any natural numbers k and l, let $R_{k,l} \equiv \left\lfloor \frac{k+l}{|S_{b,q}|} \right\rfloor$. We have that

$$\psi_{b,q}(\alpha^k \beta^l) = \begin{cases} \left(\sum_{|d| \leq R_{k,l}} \left[\alpha^{m+n+dw}\right] \right) (-1)^n \pi_{k,l} \bmod p & \text{if } k = 2m,\ l = 2n \\ 0 & \text{otherwise.} \end{cases} \tag{5.14}$$

Not only does the above formula capture the number-theoretic aspect of the size of the finite field $\mathbb{F}_q$, it is also strikingly similar to the formula of the red Fourier summation functional $\psi_{r,q}$. The only notable difference is the presence of the factor $(-1)^n$ in front of the circular polynumber $\pi_{k,l}$. Moreover, if the degree of the input monomial $\alpha^k \beta^l$ is restricted, then the values of the circular integral functional $\psi_{b,q}$ can be described solely in terms of the circular super Catalan numbers $\Omega(m,n)$.

Theorem 25. *In the blue geometry over a field $\mathbb{F}_q$, for any natural numbers k and l such that $0 \leq k + l < q - 1$, the Fourier summation functional $\psi_{b,q}$ has the form*

$$\psi_{b,q}(\alpha^k \beta^l) = \begin{cases} \Omega(m,n) \bmod p & \text{if } k = 2m \text{ and } l = 2n \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If either k or l is odd, then $\psi_{b,q}\left(\alpha^k \beta^l\right) = 0$ regardless of whether -1 is a square or not in $\mathbb{F}_q$. Moreover, if $0 \leq k + l < q - 1$ then by Theorem 24, $R_{k,l} = \left\lfloor \frac{k+l}{|S_{b,q}|} \right\rfloor = 0$ and thus if $k = 2m$ and $l = 2n$, we consequently have

$$\psi_{b,q}(\alpha^k \beta^l) = \left[\alpha^{m+n}\right] (-1)^n \pi_{2m,2n} = \Omega(m,n) \bmod p$$

by Theorem 11. ■

We conclude our analysis of the derivation of the formula for the Fourier summation functional $\psi_{b,q}$ by highlighting the similarity of the formula for $\psi_{b,q}\left(\alpha^k\beta^l\right)$ when $0 \leq k+l < q-1$ above with the characteristic 0 integration formula (1.5) presented in Theorem 6. We restate the result below for convenience, by renaming the polynumber $x_1^k x_2^l$ in equation (1.5) to $\alpha^k\beta^l$ to match with our notation and recalling that $d\mu$ is a normalised rotationally invariant measure on S^1:

$$\int_{S^1} \alpha^k\beta^l \, d\mu = \begin{cases} \Omega(m,n) & \text{if } k=2m \text{ and } l=2n \\ 0 & \text{otherwise.} \end{cases}$$

A pleasant feature of the analysis that we have presented here lies in its flexibility to extend to general fields of characteristic zero. In a further paper, we will show that the traditional unit circle integration theory over the field of real numbers, that utilises transcendental functions and infinite processes and limits, can be replaced with a purely algebraic approach in terms of a circular integral functional, and the pleasant connection to the super Catalan numbers suggests that there is something combinatorial about this theory of integration.

With this algebraic approach, the connection between algebraic combinatorics and harmonic analysis could be better appreciated, and the characteristic zero and finite field situations can be viewed more uniformly.

5.3 Some examples of the computation of $\psi_{c,q}$

We exhibit some examples of computing $\psi_{c,q}$ via the various formulas involving the super Catalan numbers and their extensions that have now been established. We will use the same examples as in the end of Chapter 4 to better appreciate the simplicity of the formulas for $\psi_{c,q}$ as a sum of particular coefficients of circular polynumbers.

Example 7. *Let $q=17$. From Example 4, we know that $\psi_{r,17}\left(\alpha^6\beta^4\right)=3$. Now, using the result in Theorem 19,*

$$\psi_{r,17}\left(\alpha^6\beta^4\right) = (-1)^2\,\Omega(3,2) \bmod 17 = \frac{3}{256} \bmod 17 = 3.$$

Moreover, if $k=40$ and $l=24$, then

$$R_{k,l} = \left\lfloor \frac{k+l}{q-1} \right\rfloor = \left\lfloor \frac{64}{16} \right\rfloor = 4$$

and therefore

$$\begin{aligned}\psi_{r,17}\left(\alpha^{40}\beta^{24}\right) &= \sum_{|d|\leq 4}[\alpha^{32+8d}]\pi_{40,24} \bmod 17 \\ &= \left(\left[\alpha^{0}\right] + \left[\alpha^{8}\right] + \cdots + \left[\alpha^{56}\right] + \left[\alpha^{64}\right]\right)\pi_{40,24}.\end{aligned}$$

Through inspection,

$$\begin{aligned}[\alpha^{0}]\pi_{40,24} = [\alpha^{64}]\pi_{40,24} &= \frac{1}{2^{64}} \\ [\alpha^{8}]\pi_{40,24} = [\alpha^{56}]\pi_{40,24} &= \frac{90744}{2^{64}} \\ [\alpha^{16}]\pi_{40,24} = [\alpha^{48}]\pi_{40,24} &= -\frac{15\,156\,452}{2^{64}} \\ [\alpha^{24}]\pi_{40,24} = [\alpha^{40}]\pi_{40,24} &= -\frac{264\,053\,432}{2^{64}} \\ [\alpha^{32}]\pi_{40,24} &= \frac{1650\,887\,238}{2^{64}}\end{aligned}$$

and thus

$$\begin{aligned}\psi_{r,17}\left(\alpha^{40}\beta^{24}\right) &= \left(\frac{2\left(1 + 90744 - 15\,156\,452 - 264\,053\,432\right) + 1650\,887\,238}{2^{64}}\right) \bmod 17 \\ &= 4.\end{aligned}$$

Example 8. *Let $q = 25 = 5^2$. It has been computed in Example 5 that $\psi_{r,25}\left(\alpha^2\beta^2\right) = 3$. Now, with our formula,*

$$\psi_{r,25}\left(\alpha^2\beta^2\right) = (-1)^1\,\Omega(1,1) \bmod 5 = -\frac{1}{8} \bmod 5 = 3.$$

Moreover, if $k = 30$ and $l = 24$ then

$$R_{k,l} = \left\lfloor \frac{k+l}{q-1} \right\rfloor = \left\lfloor \frac{54}{24} \right\rfloor = 2$$

and therefore

$$\begin{aligned}\psi_{r,25}\left(\alpha^{30}\beta^{24}\right) &= \sum_{|d|\leq 2}[\alpha^{27+12d}]\pi_{30,24} \bmod 5 \\ &= \left(\left[\alpha^{3}\right] + \left[\alpha^{15}\right] + \left[\alpha^{27}\right] + \left[\alpha^{39}\right] + \left[\alpha^{51}\right]\right)\pi_{30,24} \bmod 5.\end{aligned}$$

It can be computed that

$$[\alpha^{3}]\pi_{30,24} = [\alpha^{51}]\pi_{30,24} = -\frac{124}{2^{54}}$$

$$[\alpha^{15}]\pi_{30,24} = [\alpha^{39}]\pi_{30,24} = \frac{360\,272}{2^{54}}$$
$$[\alpha^{27}]\pi_{30,24} = \frac{24\,129\,392}{2^{54}}$$

thus it follows that

$$\begin{aligned}\psi_{r,25}\left(\alpha^{30}\beta^{24}\right) &= -2\left(\frac{124}{2^{54}} - \frac{360\,272}{2^{54}}\right) + \frac{24\,129\,392}{2^{54}} \bmod 5 \\ &= \frac{3106\,211}{2^{51}} \bmod 5 \\ &= 2.\end{aligned}$$

Example 9. *Let* $q = 27 = 3^3$. *From Example 6,* $\left(\frac{-1}{3}\right) = -1$ *and* $\psi_{b,27}(\alpha^2) = 2$ *which agrees with Theorem 23. Moreover, if* $k = l = 26$, *then* $w = \frac{1}{2}(q+1) = 14$ *and*

$$R_{k,l} = \left\lfloor \frac{k+l}{q+1} \right\rfloor = \left\lfloor \frac{52}{28} \right\rfloor = 1.$$

Therefore

$$\begin{aligned}\psi_{b,27}\left(\alpha^{26}\beta^{26}\right) &= \sum_{|d|\leq 1} [\alpha^{26+14d}]\,(-1)^{13}\,\pi_{26,26} \bmod 3 \\ &= -\left([\alpha^{12}] + [\alpha^{26}] + [\alpha^{40}]\right)\pi_{26,26} \bmod 3.\end{aligned}$$

Since

$$[\alpha^{12}]\pi_{26,26} = [\alpha^{40}]\pi_{26,26} = \frac{230\,230}{2^{52}}$$
$$[\alpha^{26}]\pi_{26,26} = -\frac{10\,400\,600}{2^{52}}$$

we have that

$$\begin{aligned}\psi_{b,27}\left(\alpha^{26}\beta^{26}\right) &= \left(\frac{10\,400\,600}{2^{52}} - \frac{460\,460}{2^{52}}\right) \bmod 3 \\ &= \frac{9940140}{2^{52}} \bmod 3 \\ &= 0.\end{aligned}$$

Part III

Secondary Analysis and Conclusion

Chapter 6

Further Properties

Up until this point, we have established that the Fourier summation functional $\psi_{c,q}$ is the unique functional on $\mathrm{Pol}_2(\mathbb{F}_q)$ that satisfies the Normalisation, Locality, and Invariance properties. We have also given an explicit formula for $\psi_{c,q}$ in each geometry. With the exception of the green geometry, the formula for $\psi_{c,q}$ that we obtained involves summing particular coefficients of the circular polynumbers $\pi_{k,l}$.

In this chapter, we aim to give some additional identities relating to the formula for $\psi_{c,q}$ and the super Catalan numbers themselves. First, we offer a simplification of the formulas for $\psi_{r,q}$ and $\psi_{b,q}$ which allows us to compute their values at $\alpha^k\beta^l$ fairly quickly especially when the powers k and l are big.

Moreover, we also employ the Locality property of $\psi_{c,q}$ to derive a Pascal-like property in the red and blue geometries which connects with symmetric forward difference tables. We may then use ideas from the finite difference calculus to obtain new identities for the super Catalan numbers and their rational variants, the circular super Catalan numbers which relate to classical formulas of Leibniz, Gregory, and Newton from the 17th century.

6.1 The Periodicity property

Recall from Theorem 4 that any polynumber $\pi \in \mathrm{Pol}_2(\mathbb{F}_q)$ can be uniquely written as $\pi_1 + \pi_2$ where $\pi_1 \in \mathcal{P}_q$, the principal subspace of $\mathrm{Pol}_2(\mathbb{F}_q)$, and $\pi_2 \in \ker(\varepsilon)$ where ε is the evaluation map that takes any polynumber to its associated polynomial function on the corresponding affine space. More specifically, the map $\pi \mapsto \pi_1$ is a projection from $\mathrm{Pol}_2(\mathbb{F}_q)$ onto $\mathcal{P}_q$ and $\psi_{c,q}(\pi) = \psi_{c,q}(\pi_1)$ from the proof of Theorem 17. This suggests that there ought to be a simplification of the formulas for $\psi_{c,q}$ especially if the degree of the input polynumber π is large.

In this section, we shall see a further simplification of the formulas for the Fourier summation functionals $\psi_{r,q}$ and $\psi_{b,q}$ by employing a property which we will call the

Periodicity property. This condition enables us to reduce the degree of the input polynumber π so that we are able to work purely in the principal subspace $\mathcal{P}_q$.

Theorem 26 (Periodicity property)**.** *Let $\psi_{c,q}$ be the Fourier summation functional in any geometry. For all natural numbers k, l, r, and s, we have that*

$$\psi_{c,q}\left(\alpha^{k+rq}\beta^{l+sq}\right) = \psi_{c,q}\left(\alpha^{k+r}\beta^{l+s}\right). \tag{6.1}$$

Proof. Let four natural numbers k, l, r, and s be given. The polynumber $\pi = \alpha^{k+rq}\beta^{l+sq} - \alpha^{k+r}\beta^{l+s}$ evaluates to the zero function since

$$\varepsilon(\pi)(x,y) = x^{k+rq}y^{l+sq} - x^{k+r}y^{l+s} = x^k y^l\left((x^r y^s)^q - x^r y^s\right) = 0$$

by the Fermat condition. Hence by the Locality property and the linearity of $\psi_{c,q}$, we must have that $\psi_{c,q}\left(\alpha^{k+rq}\beta^{l+sq}\right) = \psi_{c,q}\left(\alpha^{k+r}\beta^{l+s}\right)$ as asserted. ■

To illustrate the Periodicity property, we consider again the case $q = 13$ in the blue geometry and gather a table of values of $\psi_{b,13}\left(\alpha^k\beta^l\right)$ for various values of k and l. Since $\psi_{b,13}\left(\alpha^k\beta^l\right) = 0$ if either k or l is odd, it is sufficient to list just the values of $\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right)$ in such a table, a portion of which was given in Table 3. Now, according to Theorem 26,

$$\psi_{b,13}\left(\alpha^{2m+13r}\beta^{2n+13s}\right) = \psi_{b,13}\left(\alpha^{2m+r}\beta^{2n+s}\right)$$

so all the information required to determine the values $\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right)$ is contained in the following finite list of values of $\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right)$ for $0 \leq m, n \leq 6$.

$\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right) : m\backslash n$	0	1	2	3	4	5	6
0	1	7	2	6	2	7	3
1	7	5	9	4	8	4	9
2	2	9	5	9	4	8	4
3	6	4	9	5	9	4	8
4	2	8	4	9	5	9	4
5	7	4	8	4	9	5	9
6	3	9	4	8	4	9	5

Table 8: All the information to determine $\psi_{b,13}\left(\alpha^{2m}\beta^{2n}\right)$.

For example, if we need to determine $\psi_{b,13}\left(\alpha^{100}\beta^{200}\right)$ then we may write

$$\psi_{b,13}\left(\alpha^{100}\beta^{200}\right) = \psi_{b,13}\left(\alpha^{9+7\times 13}\beta^{5+15\times 13}\right)$$

and therefore by Theorem 26, it follows that

$$\psi_{b,13}\left(\alpha^{100}\beta^{200}\right) = \psi_{b,13}\left(\alpha^{9+7}\beta^{5+15}\right) = \psi_{b,13}\left(\alpha^{16}\beta^{20}\right).$$

We have reduced the powers of α and β significantly, but we can still reduce them further by noting that

$$\psi_{b,13}\left(\alpha^{16}\beta^{20}\right) = \psi_{b,13}\left(\alpha^{3+1\times 13}\beta^{7+1\times 13}\right) = \psi_{b,13}\left(\alpha^{3+1}\beta^{7+1}\right) = \psi_{b,13}\left(\alpha^{4}\beta^{8}\right)$$

where we again use Theorem 26 in the second equality above. We therefore conclude that $\psi_{b,13}\left(\alpha^{100}\beta^{200}\right) = \psi_{b,13}\left(\alpha^{4}\beta^{8}\right)$ whose value is given in Table 8 above to be 4.

The Periodicity property is in particular useful in the red and blue geometries. First, since $\psi_{c,q}\left(\alpha^{k}\beta^{l}\right) = 0$ if either k or l is odd over the red and blue geometries by Theorem 19 and 24, we may assume that both powers k and l are even. Now the Periodicity condition asserts that it is sufficient to find all the values of $\psi_{c,q}\left(\alpha^{2m}\beta^{2n}\right)$ where $\alpha^{2m}\beta^{2n} \in \mathcal{P}_q$, that is when $0 \leq m, n \leq \frac{1}{2}(q-1)$.

In line with the term principal subspace, we shall call the list of values of $\psi_{c,q}\left(\alpha^{2m}\beta^{2n}\right)$ where $0 \leq m, n \leq \frac{1}{2}(q-1)$ the **principal block**. Equivalently, the Periodicity condition guarantees that for any natural numbers m and n, the value of $\psi_{c,q}\left(\alpha^{2m}\beta^{2n}\right)$ can always be found in the principal block. Table 8 above is an example of a principal block in the blue geometry over $\mathbb{F}_{13}$.

We first consider an explicit formula for $\psi_{r,q}$ and $\psi_{b,q}$ evaluated at $\alpha^{2m}\beta^{2n} \in \mathcal{P}_q$ in the following two propositions.

Proposition 17. *Suppose $\mathbb{F}_q$ is a finite field with $q = p^r$ elements for some prime $p > 2$ and positive integer r. Let $w \equiv \frac{1}{2}(q-1)$. If $0 \leq m, n \leq w$, then*

$$\psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right) = \left((-1)^n \Omega(m,n) + 2[\alpha^{m+n+w}]\pi_{2m,2n} + \frac{2}{4^{m+n}}\delta_{m+n,2w}\right) \bmod p$$

and if -1 is a square in $\mathbb{F}_q$,

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \left(\Omega(m,n) + 2[\alpha^{m+n+w}](-1)^n \pi_{2m,2n} + \frac{2}{4^{m+n}}(-1)^n \delta_{m+n,2w}\right) \bmod p.$$

Proof. We will only prove the first required identity since, by Theorem 21, if -1 is a square in $\mathbb{F}_q$ then

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = (-1)^n \psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right).$$

If $0 \leq m+n < w$, it follows from Theorem 19 that $R_{k,l} = \left\lfloor \frac{k+l}{q-1} \right\rfloor = 0$, so only the central term $(-1)^n \Omega(m,n) \bmod p$ will appear in the formula.

Now suppose $w \leq m+n < 2w$. Then $R_{k,l} = 1$ which gives us two additional terms in the formula of $\psi_{r,q}$; they are $\left[\alpha^{m+n+w}\right] \pi_{2m,2n} \bmod p$ and $\left[\alpha^{m+n-w}\right] \pi_{2m,2n} \bmod p$. By Lemma 2,

$$\left[\alpha^{m+n+w}\right] \pi_{2m,2n} = (-1)^{2n} \left[\alpha^{m+n-w}\right] \pi_{2m,2n} = \left[\alpha^{m+n-w}\right] \pi_{2m,2n}$$

so

$$\begin{aligned}
\psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right) &= \left(\sum_{|d|\leq 1} \left[\alpha^{m+n+dw}\right]\right) \pi_{2m,2n} \bmod p \\
&= \left(\left[\alpha^{m+n-w}\right] \pi_{2m,2n} + \left[\alpha^{m+n}\right] \pi_{2m,2n} + \left[\alpha^{m+n+w}\right] \pi_{2m,2n}\right) \bmod p \\
&= \left(\left[\alpha^{m+n}\right] \pi_{2m,2n} + 2\left[\alpha^{m+n+w}\right] \pi_{2m,2n}\right) \bmod p \\
&= \left((-1)^n \Omega(m,n) + 2\left[\alpha^{m+n+w}\right] \pi_{2m,2n}\right) \bmod p.
\end{aligned}$$

Finally, if $m+n = 2w$, we have two further additional terms, namely

$$\left[\alpha^{m+n+2w}\right] \pi_{2m,2n} \bmod p \qquad \text{and} \qquad \left[\alpha^{m+n-2w}\right] \pi_{2m,2n} \bmod p$$

which again by Lemma 2 are both equal and evaluate to

$$\begin{aligned}
\left[\alpha^{m+n+2w}\right] \pi_{2m,2n} \bmod p &= \left[\alpha^{m+n+2w}\right] \left(\frac{1+\alpha}{2}\right)^{2m} \left(\frac{1-\alpha}{2}\right)^{2n} \bmod p \\
&= \left[\alpha^{2m+2n}\right] \left(\frac{1+\alpha}{2}\right)^{2m} \left(\frac{1-\alpha}{2}\right)^{2n} \bmod p \\
&= \frac{1}{4^{m+n}} \bmod p \\
&= \frac{1}{4^{m+n}} \delta_{m+n,2w} \bmod p.
\end{aligned}$$

The third equality above follows by observing that $\pi_{2m,2n}$ is a polynumber of degree $2m+2n$ and the coefficient of the highest power of α can only be found by multiplying the coefficient of the highest powers of α in $\left(\frac{1+\alpha}{2}\right)^{2m}$ and $\left(\frac{1-\alpha}{2}\right)^{2n}$, which are $\frac{1}{2^{2m}}$ and $\frac{1}{2^{2n}}$ respectively. Consequently,

$$\begin{aligned}
\psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right) &= \left(\sum_{|d|\leq 2} \left[\alpha^{m+n+dw}\right]\right) \pi_{2m,2n} \bmod p \\
&= \left(\left[\alpha^{m+n}\right] \pi_{2m,2n} + 2\left[\alpha^{m+n+w}\right] \pi_{2m,2n} + 2\left[\alpha^{m+n+2w}\right] \pi_{2m,2n}\right) \bmod p
\end{aligned}$$

$$= \left((-1)^n \Omega(m,n) + 2\left[\alpha^{m+n+w}\right] \pi_{2m,2n} + \frac{2}{4^{m+n}} \delta_{m+n,2w} \right) \bmod p$$

as claimed. ■

Proposition 18. *Suppose $\mathbb{F}_q$ is a finite field with $q = p^r$ elements for some prime $p > 2$ and positive integer r. Suppose further that -1 is not a square in $\mathbb{F}_q$ and let $w \equiv \frac{1}{2}(q+1)$. If $0 \leq m, n \leq \frac{q-1}{2}$, then*

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \left(\Omega(m,n) + 2[\alpha^{m+n+w}] (-1)^n \pi_{2m,2n}\right) \bmod p.$$

Proof. The proof is similar to that of Proposition 17 above. We divide into two cases: the case $0 \leq m+n < w$ corresponds to $R_{k,l} = 0$ by Theorem 23, and the case $w \leq m+n \leq q-1$ corresponds to $R_{k,l} = 1$. If $0 \leq m+n < w$ then

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \left[\alpha^{m+n}\right] (-1)^n \pi_{2m,2n} \bmod p = \Omega(m,n) \bmod p$$

and if $w \leq m+n \leq q-1$ then

$$\begin{aligned}
\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) &= \left(\left[\alpha^{m+n-w}\right] + \left[\alpha^{m+n}\right] + \left[\alpha^{m+n+w}\right]\right) (-1)^n \pi_{2m,2n} \bmod p \\
&= \left(\left[\alpha^{m+n}\right] \pi_{2m,2n} + \left[\alpha^{m+n-w}\right] \pi_{2m,2n} + \left[\alpha^{m+n+w}\right] \pi_{2m,2n}\right) \bmod p \\
&= \left(\Omega(m,n) + 2\left[\alpha^{m+n+w}\right] (-1)^n \pi_{2m,2n}\right) \bmod p.
\end{aligned}$$

In the last equation above, we again used the result from Lemma 2. ■

Now we are ready to present a simplified procedure for calculating $\psi_{r,q}(\alpha^{2m}\beta^{2n})$ and $\psi_{b,q}(\alpha^{2m}\beta^{2n})$ for any natural numbers m and n.

Theorem 27 (Fourier Summation Procedure)**.** *Suppose $\mathbb{F}_q$ is a finite field with $q = p^r$ elements for some prime $p > 2$ and positive integer r. Given any natural numbers m and n, perform the following procedure:*

1. *Set $m_0 = 2m$ and $n_0 = 2n$*
2. *For each $k \in \mathbb{N}$, identify four integers Q_k, R_k, S_k, and T_k such that Q_k and S_k are the largest integers such that*

   $$m_k = Q_k q + R_k \text{ and } n_k = S_k q + T_k$$

   for some natural numbers R_k and T_k.
3. *Set $m_{k+1} = Q_k + R_k$ and $n_{k+1} = S_k + T_k$. If either $m_{k+1} \geq q$ or $n_{k+1} \geq q$, then repeat step 2. If not, then set $M = m_{k+1}$ and $N = n_{k+1}$ and stop the procedure.*

We have that

1. *The procedure will halt, that is, M and N exist*

2. *M and N are necessarily even, say $M = 2m^*$ and $N = 2n^*$ for some natural numbers m^* and n^**

3. *In the red geometry,*

$$\psi_{r,q}\left(\alpha^{2m}\beta^{2n}\right) = \left((-1)^{n^*}\,\Omega\left(m^*, n^*\right) + 2[\alpha^{m^*+n^*+\frac{q-1}{2}}]\pi_{2m^*,2n^*} + \frac{2}{4^{m^*+n^*}}\delta_{m^*+n^*,q-1}\right) \bmod p$$

and in the blue geometry, if -1 is a square in $\mathbb{F}_q$ then

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \left(\Omega\left(m^*, n^*\right) + 2\left(-1\right)^{n^*}\,[\alpha^{m^*+n^*+\frac{q-1}{2}}]\pi_{2m^*,2n^*} + \frac{2\left(-1\right)^{n^*}}{4^{m^*+n^*}}\delta_{m^*+n^*,q-1}\right) \bmod p$$

and if -1 is not a square in $\mathbb{F}_q$ then

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \left(\Omega\left(m^*, n^*\right) + 2[\alpha^{m^*+n^*+\frac{q+1}{2}}]\left(-1\right)^{n^*}\pi_{2m^*,2n^*}\right) \bmod p.$$

Proof. Suppose the procedure does not halt. Consider the sequence (m_k) where $k \in \mathbb{N}$. From the construction of this sequence, we have that

$$m_k = Q_k q + R_k > Q_k + R_k = m_{k+1}$$

for all $k \in \mathbb{N}$, which implies that (m_k) is a strictly decreasing sequence. But (m_k) is a sequence of non-negative integers. Such a sequence cannot be strictly decreasing from the well-ordering property. Therefore the procedure must halt. This proves the first assertion.

Now, since $m_0 = Q_0 q + R_0$ is even and q is odd, it follows that if Q_0 is odd then R_0 is necessarily odd; if Q_0 is even then R_0 is necessarily even. In both cases, $m_1 = Q_0 + R_0$ is always even. By a similar argument, $n_1 = S_0 + T_0$ is also even. We can proceed by induction to show that m_k and n_k are even. Since the procedure halts, there exists some integers k, M, and N, such that $m_{k+1} = M$ and $n_{k+1} = N$, showing that M and N must be themselves even. This proves the second assertion.

Finally, we observe that for any k,

$$\begin{aligned}
\psi_{c,q}\left(\alpha^{m_k}\beta^{n_k}\right) &= \psi_{c,q}\left(\alpha^{Q_k q + R_k}\beta^{S_k q + T_k}\right) \\
&= \psi_{c,q}\left(\alpha^{Q_k + R_k}\beta^{S_k + T_k}\right) \quad \text{(by equation (6.1))} \\
&= \psi_{c,q}\left(\alpha^{m_{k+1}}\beta^{n_{k+1}}\right).
\end{aligned}$$

Since the procedure halts, by writing $M = 2m^*$ and $N = 2n^*$, we have that

$$\psi_{c,q}\left(\alpha^{2m}\beta^{2n}\right) = \psi_{c,q}\left(\alpha^{m_0}\beta^{n_0}\right) = \psi_{c,q}\left(\alpha^{M}\beta^{N}\right) = \psi_{c,q}\left(\alpha^{2m^*}\beta^{2n^*}\right).$$

Since $0 \leq M, N \leq q-1$ it follows that $0 \leq m^*, n^* \leq \frac{1}{2}(q-1)$. Thus we can apply Proposition 17 and Proposition 18, proving the last assertion. ■

We close this section by revisiting Example 7 and Example 8 which we now compute using the simplified procedure encoded in Theorem 27.

Example 10. *From Example 7, to compute $\psi_r\left(\alpha^{40}\beta^{24}\right)$ using the periodicity condition, we do the procedure established in Theorem 27 with $m_0 = 40$, $n_0 = 24$, and $q = 17$ to get $M = N = 8$. Therefore,*

$$\begin{aligned}
\psi_{r,17}\left(\alpha^{40}\beta^{24}\right) &= \psi_{r,17}\left(\alpha^{8}\beta^{8}\right) \\
&= \left((-1)^4\,\Omega(4,4) + 2\left[\alpha^0\right]\pi_{8,8}\right) \bmod 17 \\
&= \left(\frac{35}{2^{15}} + \frac{1}{2^{15}}\right) \bmod 17 \\
&= 4.
\end{aligned}$$

Example 11. *From Example 8, to compute $\psi_r\left(\alpha^{30}\beta^{24}\right)$ here we use $m_0 = 30$, $n_0 = 24$, and $q = 25$ to get $M = 6$ and $N = 24$, so that*

$$\begin{aligned}
\psi_{r,25}\left(\alpha^{30}\beta^{24}\right) &= \psi_{r,25}\left(\alpha^{6}\beta^{24}\right) \\
&= \left((-1)^{12}\,\Omega(3,12) + 2\left[\alpha^3\right]\pi_{6,24}\right) \bmod 5 \\
&= \left(\frac{7429}{67\,108\,864} - \frac{177}{2^{27}}\right) \bmod 5 \\
&= \frac{14\,681}{134\,217\,728} \bmod 5 \\
&= 2.
\end{aligned}$$

Example 12. *Suppose $q = 13$ and we wish to compute $\psi_{b,13}\left(\alpha^{1000}\beta^{600}\right)$. If we were to use the formula for $\psi_{b,q}$ in Theorem 24, we need to find particular coefficients of the circular polynumber $\pi_{1000,600}$ of degree 1600. This is of course computationally expensive. However, with the aid of Theorem 27, we can perform the procedure applied to $m_0 = 1000$, $n_0 = 600$, and $q = 13$ to get*

$$m_1 = 76 + 12 = 88 \text{ and } n_1 = 46 + 2 = 48$$

since $1000 = 76 \times 13 + 12$ and $600 = 46 \times 13 + 2$,

$$m_2 = 6 + 10 = 16 \text{ and } n_2 = 3 + 9 = 12$$

since $88 = 6 \times 13 + 10$ *and* $48 = 3 \times 13 + 9$,

$$m_3 = 1 + 3 = 4 \text{ and } n_3 = 0 + 12 = 12$$

since $16 = 1 \times 13 + 3$ *and* $12 = 0 \times 13 + 12$.

Since now both $m_3, n_3 < q$, *the procedure halts and thus* $M = 4$ *and* $N = 12$. *It follows that* $m^* = 2$ *and* $n^* = 6$ *so*

$$\psi_{b,13}\left(\alpha^{1000}\beta^{600}\right) = \psi_{b,13}\left(\alpha^4\beta^{12}\right)$$

which can be computed to be

$$\left(\Omega(2,6) + 2(-1)^6\left[\alpha^{14}\right]\left(\frac{1+\alpha}{2}\right)^4\left(\frac{1-\alpha}{2}\right)^{12}\right) \bmod 13 = \left(\frac{9}{2^{15}} + \frac{3}{2^{12}}\right) \bmod 13$$
$$= 9.$$

6.2 Symmetric difference table

In this section, we shall establish an identity on the circular super Catalan numbers $\Omega(m,n)$ motivated by some additional properties of the blue Fourier summation functional $\psi_{b,q}$, and connect with the remarkable harmonic triangle of Leibniz.

Proposition 19. *Let* m *and* n *be two natural numbers. By writing* $I_b(m,n) \equiv \psi_{b,q}(\alpha^{2m}\beta^{2n})$, *we have that*

$$I_b(m,n) = I_b(n,m) \tag{6.2}$$

and

$$I_b(m,n) = I_b(m+1,n) + I_b(m,n+1). \tag{6.3}$$

Proof. We first observe that $h = \begin{pmatrix} 0 & 1_q \\ -1_q & 0 \end{pmatrix} \in SO_{b,q}$ since $\det(h) = 1_q$ and it satisfies the orthogonality condition

$$\begin{pmatrix} 0 & 1_q \\ -1_q & 0 \end{pmatrix}\begin{pmatrix} 0 & 1_q \\ -1_q & 0 \end{pmatrix}^T = \begin{pmatrix} 1_q & 0 \\ 0 & 1_q \end{pmatrix}$$

so by the Invariance property of $\psi_{b,q}$,

$$I_b(m,n) = \psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \psi_{b,q}\left(h \cdot \alpha^{2m}\beta^{2n}\right) = \psi_{b,q}\left(\alpha^{2n}\beta^{2m}\right) = I_b(n,m).$$

To prove the second identity, we first see that the polynumber

$$\pi = \alpha^{2m+2}\beta^{2n} + \alpha^{2m}\beta^{2n+2} - \alpha^{2m}\beta^{2n}$$

evaluates to the zero function on $S_{b,q}$ since

$$\varepsilon(\pi)(x,y) = x^{2m+2}y^{2n} + x^{2m}y^{2n+2} - x^{2m}y^{2n} = x^{2m}y^{2n}\left(x^2+y^2-1\right) = 0$$

where we have used the defining property $x^2+y^2=1$ for all $[x,y] \in S_{b,q}$. Consequently, the Locality property of the Fourier summation functional $\psi_{b,q}$ applies, and we have that

$$\psi_{b,q}\left(\alpha^{2m}\beta^{2n}\right) = \psi_{b,q}\left(\alpha^{2m+2}\beta^{2n}\right) + \psi_{b,q}\left(\alpha^{2m}\beta^{2n+2}\right). \tag{6.4}$$

By letting $I_b(m,n) = \psi_{b,q}(\alpha^{2m}\beta^{2n})$ we may now see the identity (6.4) more clearly as

$$I_b(m,n) = I_b(m+1,n) + I_b(m,n+1)$$

as required. ■

We call the property (6.2) and (6.3) above the **symmetry property** and the **blue Pascal-like property** respectively. We can interpret the symmetry property as follows: the entries of the table of numbers $I_b(m,n)$ are symmetric along the diagonal entries, while the blue Pascal-like property suggests that in a table of values of $I_b(m,n)$, each entry is the sum of the entry to its right and the entry below it.

The symmetry and blue Pascal-like properties above motivate us to define a more general table of numbers which we shall call a **symmetric difference table**. More precisely, a two-dimensional array of numbers indexed by natural numbers where the entry of P at row m and column n is $P(m,n)$ is called a symmetric difference table precisely when P satisfies the symmetry property, that is $P(m,n) = P(n,m)$ and P satisfies the blue Pascal-like property, that is

$$P(m,n) = P(m+1,n) + P(m,n+1)$$

for all natural numbers m and n.

From Theorem 9, the circular super Catalan numbers $\Omega(m,n)$ satisfy the symmetry and the blue Pascal-like properties. It thus follows that the table of rational numbers with entries $\Omega(m,n)$ is a symmetric difference table. The identity that we will derive below is motivated by the work of 17th century mathematician Gottfried Wilhelm Leibniz.

The earliest observation of a symmetric difference table arguably dates back to the year 1673 by Leibniz in his work *De Triangulo Harmonico* [23]. He first considered what he called a harmonic triangle which is a triangular arrangement of

rational numbers, similar to that of Pascal's triangle of binomial coefficients, with the property that the first and last entry in row n is $\frac{1}{n+1}$ where $n \in \mathbb{N}$ and every entry in the middle is the sum of the two entries diagonally below it, one on the left and one on the right. The top part of Leibniz's harmonic triangle is given below.

									1											
								$\frac{1}{2}$				$\frac{1}{2}$								
							$\frac{1}{3}$				$\frac{1}{6}$				$\frac{1}{3}$					
						$\frac{1}{4}$			$\frac{1}{12}$				$\frac{1}{12}$				$\frac{1}{4}$			
					$\frac{1}{5}$			$\frac{1}{20}$				$\frac{1}{30}$				$\frac{1}{20}$				$\frac{1}{5}$	
				$\frac{1}{6}$			$\frac{1}{30}$			$\frac{1}{60}$				$\frac{1}{60}$			$\frac{1}{30}$			$\frac{1}{6}$
			$\frac{1}{7}$			$\frac{1}{42}$			$\frac{1}{105}$			$\frac{1}{140}$			$\frac{1}{105}$			$\frac{1}{42}$			$\frac{1}{7}$
		$\frac{1}{8}$			$\frac{1}{56}$			$\frac{1}{168}$			$\frac{1}{280}$			$\frac{1}{280}$			$\frac{1}{168}$			$\frac{1}{56}$			$\frac{1}{8}$
	$\frac{1}{9}$			$\frac{1}{72}$			$\frac{1}{252}$			$\frac{1}{504}$			$\frac{1}{630}$			$\frac{1}{504}$			$\frac{1}{252}$			$\frac{1}{72}$			$\frac{1}{9}$
$\frac{1}{10}$			$\frac{1}{90}$			$\frac{1}{360}$			$\frac{1}{840}$			$\frac{1}{1260}$			$\frac{1}{1260}$			$\frac{1}{840}$			$\frac{1}{360}$			$\frac{1}{90}$			$\frac{1}{10}$

Table 9: Leibniz's harmonic triangle.

We can rearrange Leibniz's harmonic triangle into a symmetric difference table P by the convention that the m-th entry in row n of the harmonic triangle is $P(m, n-m)$, where we agree to start the indexing from 0. We give the rearrangement of Leibniz's harmonic triangle into a bigger symmetric difference table in the next page.

Leibniz's motivation in the construction of the harmonic triangle largely was to study infinite series that are similar to the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

which in his previous work was demonstrated to diverge. Leibniz deduced that by rearranging the entries of his harmonic triangle into a symmetric difference table, the unending sum

$$\frac{1}{2} + \frac{1}{6} + \frac{1}{12} + \frac{1}{20} + \frac{1}{30} + \frac{1}{42} + \cdots$$

whose entries are precisely all the numbers in the second column, can be found by a simple argument. Since each number in the series is a difference between the number

to its immediate left and the number below it, the sum is precisely the first number in the first column.

$m\backslash n$	0	1	2	3	4	5	6	7	8	9
0	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{8}$	$\frac{1}{9}$	$\frac{1}{10}$
1	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{1}{20}$	$\frac{1}{30}$	$\frac{1}{42}$	$\frac{1}{56}$	$\frac{1}{72}$	$\frac{1}{90}$	$\frac{1}{110}$
2	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{30}$	$\frac{1}{60}$	$\frac{1}{105}$	$\frac{1}{168}$	$\frac{1}{252}$	$\frac{1}{360}$	$\frac{1}{495}$	$\frac{1}{660}$
3	$\frac{1}{4}$	$\frac{1}{20}$	$\frac{1}{60}$	$\frac{1}{140}$	$\frac{1}{280}$	$\frac{1}{504}$	$\frac{1}{840}$	$\frac{1}{1320}$	$\frac{1}{1980}$	$\frac{1}{2860}$
4	$\frac{1}{5}$	$\frac{1}{30}$	$\frac{1}{105}$	$\frac{1}{280}$	$\frac{1}{630}$	$\frac{1}{1260}$	$\frac{1}{2310}$	$\frac{1}{3960}$	$\frac{1}{6435}$	$\frac{1}{10010}$
5	$\frac{1}{6}$	$\frac{1}{42}$	$\frac{1}{168}$	$\frac{1}{504}$	$\frac{1}{1260}$	$\frac{1}{2772}$	$\frac{1}{5544}$	$\frac{1}{10296}$	$\frac{1}{18018}$	$\frac{1}{30030}$
6	$\frac{1}{7}$	$\frac{1}{56}$	$\frac{1}{252}$	$\frac{1}{840}$	$\frac{1}{2310}$	$\frac{1}{5544}$	$\frac{1}{12012}$	$\frac{1}{24024}$	$\frac{1}{45045}$	$\frac{1}{80080}$
7	$\frac{1}{8}$	$\frac{1}{72}$	$\frac{1}{360}$	$\frac{1}{1320}$	$\frac{1}{3960}$	$\frac{1}{10296}$	$\frac{1}{24024}$	$\frac{1}{51480}$	$\frac{1}{102960}$	$\frac{1}{194480}$
8	$\frac{1}{9}$	$\frac{1}{90}$	$\frac{1}{495}$	$\frac{1}{1980}$	$\frac{1}{6435}$	$\frac{1}{18018}$	$\frac{1}{45045}$	$\frac{1}{102960}$	$\frac{1}{218790}$	$\frac{1}{437580}$
9	$\frac{1}{10}$	$\frac{1}{110}$	$\frac{1}{660}$	$\frac{1}{2860}$	$\frac{1}{10010}$	$\frac{1}{30030}$	$\frac{1}{80080}$	$\frac{1}{194480}$	$\frac{1}{437580}$	$\frac{1}{923780}$

Table 10: Leibniz's symmetric difference table.

More precisely, Leibniz argued that the above series simplifies to

$$\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+\cdots$$

and that the sum must be 1, since every term other than 1 will cancel with the number following it. Similarly, the unending sum

$$\frac{1}{72}+\frac{1}{360}+\frac{1}{1320}+\frac{1}{3960}+\frac{1}{10296}+\cdots$$

by Leibniz's argument can be rewritten as

$$\left(\frac{1}{56}-\frac{1}{252}\right)+\left(\frac{1}{252}-\frac{1}{840}\right)+\left(\frac{1}{840}-\frac{1}{2310}\right)+\cdots$$

which evaluates to $\frac{1}{56}$, the left-most entry. A comprehensive exposition of Leibniz's works on the harmonic triangle can be found in [32].

Nowadays, we realise this type of series as a telescoping series and that there is a limiting process involved in the computation. Nevertheless, adopting Leibniz's point of view, we can come up with an interesting identity for the circular super Catalan numbers.

Theorem 28. *For any natural numbers m and n,*

$$\sum_{k\geq m}\frac{(2k)!\,(2n+2)!}{4^{k+n+1}k!\,(n+1)!\,(k+n+1)!}=\frac{(2m)!\,(2n)!}{4^{m+n}m!n!\,(m+n)!}.$$

Proof. Since the table of circular super Catalan numbers $\Omega(m,n)$ is a symmetric difference table, by Leibniz's argument

$$\sum_{k\geq m}\frac{(2k)!\,(2n+2)!}{4^{k+n+1}k!\,(n+1)!\,(k+n+1)!}=\ \Omega(m,n+1)+\Omega(m+1,n+1)+\cdots$$

can be rewritten as

$$(\Omega(m,n)-\Omega(m+1,n))+(\Omega(m+1,n)-\Omega(m+2,n))+\cdots$$

and this evaluates to $\Omega(m,n)$ which is the right-hand side of the above identity. ■

As an example, considering the numbers in the second column of Table 6 of the circular super Catalan numbers, the sum

$$\frac{3}{8}+\frac{1}{16}+\frac{3}{128}+\frac{3}{256}+\frac{7}{1024}+\frac{9}{2048}+\cdots$$

evaluates to $\frac{1}{2}$ which is the entry in the first column and zeroth row of the table.

6.3 Forward difference table

We shall now introduce a slight variant of the symmetric difference table. This is motivated by an analogous property satisfied by the red Fourier summation functional $\psi_{r,q}$ which we establish below.

Proposition 20. *Let m and n be any natural numbers. By writing $I_r(m,n)\equiv\psi_{r,q}(\alpha^{2m}\beta^{2n})$, we have that*

$$I_r(m,n)=I_r(m+1,n)-I_r(m,n+1). \tag{6.5}$$

Proof. The polynumber $\pi=\alpha^{2m+2}\beta^{2n}-\alpha^{2m}\beta^{2n+2}-\alpha^{2m}\beta^{2n}$ evaluates to the zero function on $S_{r,q}$ since

$$\varepsilon(\pi)(x,y)=x^{2m+2}y^{2n}-x^{2m}y^{2n+2}-x^{2m}y^{2n}=x^{2m}y^{2n}\left(x^2-y^2-1\right)=0$$

by the defining property of the red unit circle $S_{r,q}$ that $x^2-y^2=1$ for all $[x,y]\in S_{r,q}$. It thus follows by the Locality property that $\psi_{r,q}(\pi)=0$, which simplifies to $I_r(m,n)=I_r(m+1,n)-I_r(m,n+1)$ as required. ■

We shall call the property (6.5) above the **red Pascal-like property**. As with the previous case, we call any table of numbers that satisfies the red Pascal-like property a **forward difference table**.

More precisely, a two-dimensional array of numbers Q indexed by natural numbers where the entry of Q at row m and column n is $Q(m,n)$ is called a forward difference table precisely when $Q(m,n) = Q(m+1,n) - Q(m,n+1)$ for all natural numbers m and n. Note that we no longer require Q to be symmetric, unlike in the definition of the symmetric difference table.

Suppose then that $Q(m,n)$ is a forward difference table and let $a_m = Q(m,0)$ for all natural numbers m. Then the entire table may be recursively described in terms of the entries a_m, and suitable binomial coefficients, as indicated below.

$m\backslash n$	0	1	2	3	
0	a_0	$a_1 - a_0$	$a_2 - 2a_1 + a_0$	$a_3 - 3a_2 + 3a_1 - a_0$	$\cdots$
1	a_1	$a_2 - a_1$	$a_3 - 2a_2 + a_1$	$a_4 - 3a_3 + 3a_2 - a_1$	
2	a_2	$a_3 - a_2$	$a_4 - 2a_3 + a_2$	$a_5 - 3a_4 + 3a_3 - a_2$	
3	a_3	$a_4 - a_3$	$a_5 - 2a_4 + a_3$	$a_6 - 3a_5 + 3a_4 - a_3$	
	$\vdots$				$\ddots$

Table 11: A forward difference table associated to a_m.

For any $k \in \mathbb{N}$, define $\Delta^k a$ to be the k-th column of Q and $\Delta^k a(0)$ to be its entry in the zeroth row. The following result is sometimes called Newton's formula of interpolation, although it was James Gregory who discovered it in 1670, according to a letter sent by him to Collins, who then notified Newton of Gregory's discovery [48].

The formula allows us to recover the initial (column) sequence a in terms of the successive first entries of repeated differences. Since the binomial coefficients $\binom{m}{k}$ which appear on the right hand side are polynumbers in m, this can then be used to interpolate, or extrapolate the original sequence a.

Proposition 21 (Gregory-Newton Interpolation)**.** *For any $m \in \mathbb{N}$,*

$$a_m = \sum_{k=0}^{m} \binom{m}{k} \Delta^k a(0).$$

It can be observed that if $a_m = \frac{1}{m+1}$, we would get Leibniz's rearrangement of the harmonic triangle into the symmetric difference table, but with a negative sign

at every entry in the odd columns as illustrated below:

$m\backslash n$	0	1	2	3	4	
0	1	$-\frac{1}{2}$	$\frac{1}{3}$	$-\frac{1}{4}$	$\frac{1}{5}$	$\cdots$
1	$\frac{1}{2}$	$-\frac{1}{6}$	$\frac{1}{12}$	$-\frac{1}{20}$	$\frac{1}{30}$	
2	$\frac{1}{3}$	$-\frac{1}{12}$	$\frac{1}{30}$	$-\frac{1}{60}$	$\frac{1}{105}$	
3	$\frac{1}{4}$	$-\frac{1}{20}$	$\frac{1}{60}$	$-\frac{1}{140}$	$\frac{1}{280}$	
4	$\frac{1}{5}$	$-\frac{1}{30}$	$\frac{1}{105}$	$-\frac{1}{280}$	$\frac{1}{630}$	
	$\vdots$					$\ddots$

With relation to the circular super Catalan numbers, if we choose $a_m = \frac{1}{4^m}\binom{2m}{m}$ then we get the table of circular super Catalan numbers $\Omega(m,n)$ but with a negative sign at every odd column entry as shown below.

$m\backslash n$	0	1	2	3	4	
0	1	$-\frac{1}{2}$	$\frac{3}{8}$	$-\frac{5}{16}$	$\frac{35}{128}$	$\cdots$
1	$\frac{1}{2}$	$-\frac{1}{8}$	$\frac{1}{16}$	$-\frac{5}{128}$	$\frac{7}{256}$	
2	$\frac{3}{8}$	$-\frac{1}{16}$	$\frac{3}{128}$	$-\frac{3}{256}$	$\frac{7}{1024}$	
3	$\frac{5}{16}$	$-\frac{5}{128}$	$\frac{3}{256}$	$-\frac{5}{1024}$	$\frac{5}{2048}$	
4	$\frac{35}{128}$	$-\frac{7}{256}$	$\frac{7}{1024}$	$-\frac{5}{2048}$	$\frac{35}{32768}$	
	$\vdots$					$\ddots$

In this case,

$$Q(m,n) = (-1)^n \Omega(m,n)$$

which is precisely the central term that appears in the formula for $\psi_{r,q}$.

Applying the Gregory-Newton interpolation formula to our circular super Catalan numbers, we get the following identity.

Theorem 29. *For any natural numbers m and n,*

$$\Omega(m,n) = \sum_{k=0}^{m} (-1)^k \frac{1}{4^{n+k}} \binom{m}{k} \binom{2n+2k}{n+k}.$$

Proof. Fix a natural number n and define a forward difference table Q whose entries

in the zeroth column are $a_m = Q(m,0) = \Omega(m,n)$ for all natural numbers m. Then the entries in column k, denoted by $\Delta^k a$, are precisely $(-1)^k \Omega(m, n+k)$ and so

$$\Delta^k a(0) = (-1)^k \Omega(0, n+k).$$

By Proposition 21, we have that

$$\begin{aligned}\Omega(m,n) = a_m = \sum_{k=0}^{m} \binom{m}{k} \Delta^k a(0) &= \sum_{k=0}^{m} \binom{m}{k} (-1)^k \Omega(0, n+k) \\ &= \sum_{k=0}^{m} (-1)^k \frac{1}{4^{n+k}} \binom{m}{k} \binom{2n+2k}{n+k}\end{aligned}$$

finishing the claim. ■

Chapter 7

Afterword

We briefly summarise the results discussed in this thesis and pose some open problems for future works. We first introduced a variant of polynomials which we call polynumbers whose construction does not need a prior understanding of *variables* or *unknowns*. We carefully distinguished polynomials as formal objects and as functions by defining an evaluation map ε to give us a cleaner and more precise framework to do our analysis. We defined the three metrical geometries and consequently three unit circles and three rotation groups which act on the unit circle.

We then introduced a notion of algebraic integral over the unit circle that is analogous to the traditional Riemann integral called the circular integral functional and showed that there is one and only one circular integral functional in each geometry. The explicit formula for the circular integral functional in each geometry was given and in the more complicated geometries, the formula is given in terms of sums of particular coefficients of the circular polynumbers $\pi_{k,l}$ given by

$$\pi_{k,l} = \left(\frac{1+\alpha}{2}\right)^k \left(\frac{1-\alpha}{2}\right)^l.$$

By introducing two relativistic geometries and thus working in three metrical geometries at the same time, as opposed to working in just the Euclidean geometry, we are able to show that the three geometries have an intricate connection, which is what *chromogeometry* asserts. Perhaps surprisingly, the result in the Euclidean (blue) geometry when -1 is a square number in the field is derived from the relativistic geometries.

While we are used into thinking that the Euclidean geometry is the primary framework of doing geometry, this three-fold symmetry suggests that the three geometries should co-exist together. The result in the blue geometry when -1 is not a square number is treated differently and this difference in approaching the polynumber summation problem is reflected in the size of the unit circle in this

setting. The argument we employed in this case is motivated by the approach of traditional Fourier analysis and we then show that the result in the blue geometry, regardless of whether -1 is a square number or not, is similar.

We then show a curious connection between the problem of summing polynumbers over the unit circles and a family of integers as well as its rational intermediaries called the super Catalan numbers and the circular super Catalan numbers. The circular super Catalan numbers arise naturally as the coefficient of the central terms of the circular polynumbers. This warrants further studies of the coefficients of the circular polynumbers which we may think of as a generalisation of the circular super Catalan numbers and we believe that their explicit formulas are not trivial.

We also offer a reduction of the main formulas for the Fourier summation functionals that utilises the Periodicity condition which is the distinguishing aspect of working with finite fields as opposed to fields of characteristic zero. This reduction of formula gives us a computationally more efficient procedure to evaluate the Fourier summation functionals $\psi_{c,q}$, especially if the characteristic of the underlying field is a large prime number. We also utilise the recurrence relation satisfied by the super Catalan numbers and therefore by the circular super Catalan numbers to derive some identities using finite differential calculus.

The results in this thesis certainly open up a new direction to finite field Fourier analysis. We now have the basic technology to set up a proper theory of Fourier analysis over finite fields of odd characteristic from a purely algebraic point of view. The main feature of the algebraic Fourier analysis is that the functions of interest are defined on the unit circle that depends on the choice of geometry and take complex number values over which the field is defined, without reference to the field of real numbers $\mathbb{R}$ or (traditional) complex numbers $\mathbb{C}$.

For example, we might consider functions f from the red unit circle $S_{r,q}$ to the algebra of red complex numbers $\mathbb{C}_r\left(\mathbb{F}_q\right)$ or functions f from the blue unit circle $S_{b,q}$ to the field extension $\mathbb{C}_b\left(\mathbb{F}_q\right)$ of $\mathbb{F}_q$ when -1 is not a square.

The integration theory that we set up is completely specifiable without appealing to infinite procedures. This established theory also connects Fourier analysis to combinatorics from its connection to the super Catalan numbers, which have no general combinatorial interpretation at the time this thesis is submitted.

Finally, we could set up an analogous theory over fields of characteristic zero. One could develop a polynumber integration theory over general spheres which would be a generalisation of the current result in integrating polynomials over spheres, which assumed the underlying field to be $\mathbb{R}$. The occurrence of the super Catalan numbers and circular super Catalan numbers also warrants further studies of the coefficients of the circular polynumbers which we may think of as a generalisation of the circular super Catalan numbers.

Bibliography

[1] E. Allen and I. Gheorghiciuc. A weighted interpretation for the super Catalan numbers. *arXiv preprint arXiv:1403.5246*, 2014.

[2] J. A. Baker. Integration over spheres and the divergence theorem for balls. *The American mathematical monthly*, 104(1):36–47, 1997.

[3] N. K. Bose. *Digital Filters: Theory and Applications*. Krieger publishing company, 1993.

[4] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geometric & Functional Analysis GAFA*, 14(1):27–57, 2004.

[5] R. Brauer. Collected Papers, Vols. I-III, 1980.

[6] A. Carbery. Harmonic analysis on vector spaces over finite fields. *Lecture notes, November*, 2006.

[7] L. Carlitz. Representations by quadratic forms in a finite field. *Duke Mathematical Journal*, 21(1):123–137, 1954.

[8] E. Catalan. Question 1135. *Nouvelles Annales de Mathématiques: Journal des Candidats aux Écoles Polytechnic et Normale*. 2nd series, 13:207, 1874.

[9] X. Chen and J. Wang. The super Catalan numbers $s(m, m+s)$ for $s \leq 4$. *arXiv preprint arXiv:1208.4196*, 2012.

[10] W. Clifford. Preliminary sketch of biquaternions. *Proceedings of the London Mathematical Society*, 1(1):381–395, 1871.

[11] J. Cockle. III. On a new imaginary in algebra. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 34(226):37–47, 1849.

[12] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplement*, 10:vi+–97, 1973.

[13] C. F. Dunkl. A Krawtchouk polynomial addition theorem and wreath products of symmetric groups. *Indiana University Mathematics Journal*, 25(4):335–358, 1976.

[14] C. F. Dunkl and D. E. Ramirez. Krawtchouk polynomials and the symmetrization of hypergroups. *SIAM Journal on Mathematical Analysis*, 5(3):351–366, 1974.

[15] P. Feinsilver and J. Kocik. Krawtchouk polynomials and Krawtchouk matrices. In *Recent advances in applied probability*, pages 115–141. Springer, 2005.

[16] P. Feinsilver and R. Schott. Krawtchouk polynomials and finite probability theory. In *Probability Measures on Groups X*, pages 129–135. Springer, 1991.

[17] G. B. Folland. How to integrate a polynomial over a sphere. *The American Mathematical Monthly*, 108(5):446–448, 2001.

[18] E. Georgiadis, A. Munemasa, and H. Tanaka. A note on super Catalan numbers. *Interdisciplinary Information Sciences*, 18(1):23–24, 2012.

[19] I. M. Gessel. Super ballot numbers. *Journal of symbolic computation*, 14(2-3):179–194, 1992.

[20] I. M. Gessel and G. Xin. A Combinatorial Interpretation of the Numbers $6(2n)!/n!(n+2)!$. *Journal of Integer Sequences*, 8(2):3, 2005.

[21] I. Gheorghiciuc and G. Orelowitz. Super-Catalan Numbers of the Third and Fourth Kind. *arXiv preprint arXiv:2008.00133*, 2020.

[22] S. Gurevich and R. Howe. Harmonic analysis on GL_n over finite fields. *Pure and Applied Mathematics Quarterly*, 17(4):1387–1463, 2021.

[23] E. Knobloch. Die mathematischen Studien von GW Leibniz zur Kombinatorik. *Janus Leiden*, 63(1-2-3):1–25, 1976.

[24] D. E. Knuth. *The art of computer programming*, volume 3. Pearson Education, 1997.

[25] M. Krawtchouk. Sur la distribution des racines des polynomes orthogonaux. *Comptes Rendus*, 196:739–741, 1933.

[26] M. Krawtchouk. Sur une généralisation des polynomes d'Hermite. *Comptes Rendus*, 189(620-622):5–3, 1929.

[27] V. I. Levenshtein. Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces. *IEEE Transactions on Information Theory*, 41(5):1303–1321, 1995.

[28] S. Ling and C. Xing. *Coding theory: a first course*. Cambridge University Press, 2004.

[29] J. Liu. Congruences on Sums of Super Catalan Numbers. *Results in Mathematics*, 73(4):1–8, 2018.

[30] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[31] J. MacWilliams. Orthogonal matrices over finite fields. *The American Mathematical Monthly*, 76(2):152–164, 1969.

[32] M. R. Massa Esteve. The harmonic triangle in Mengoli's and Leibniz's works. *Quaderns d'història de l'enginyeria*, 16:233–258, 2018.

[33] J. Mikić. On a New Alternating Convolution Formula for the Super Catalan Numbers. *arXiv preprint arXiv:2110.04805*, 2021.

[34] N. Pippenger and K. Schleich. Topological characteristics of random triangulated surfaces. *Random Structures & Algorithms*, 28(3):247–288, 2006.

[35] H. Prodinger. The reciprocal super Catalan matrix. *Special Matrices*, 3(1), 2015.

[36] W. Rindler. Introduction to special relativity. 2, 1991.

[37] G. Schaeffer. A combinatorial interpretation of super-Catalan numbers of order two. *unpublished note*, 2003.

[38] H. M. Schwartz. *Introduction to Special Relativity*. McGraw-Hill, 1968.

[39] P. M. Schwarz and J. H. Schwarz. *Special Relativity: From Einstein to Strings*. Cambridge University Press, 2004.

[40] R. Sedgewick. Algorithms. *Addison Wesley Series in Computer Science*, 1983.

[41] J. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate texts in mathematics*. Springer, 1977, pages I–X, 1–170.

[42] N. J. A. Sloane and T. O. F. Inc. The Online Encyclopedia of Integer Sequences, 2022. URL: `https://oeis.org/A000108`.

[43] R. P. Stanley. *Catalan numbers*. Cambridge University Press, 2015.

[44] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

[45] D. E. Taylor. *The geometry of the classical groups*, volume 9. Heldermann Verlag, 1992.

[46] D. S. Thakur. Power sums of polynomials over finite fields and applications: a survey. *Finite Fields and Their Applications*, 32:171–191, 2015.

[47] J. Thévenaz. *G*-algebras and modular representation theory. Technical report, Clarendon Press, 1995.

[48] E. T. Whittaker and G. Robinson. *Calculus of observations: Treatise on Numerical Mathematics 3rd Edition*. Blackie and Sons Limited, London, 1940.

[49] N. J. Wildberger. Chromogeometry. *The Mathematical Intelligencer*, 32(1):26–32, 2010.

[50] N. J. Wildberger. *Divine Proportions: Rational Trigonometry to Universal Geometry*. Wild Egg Sydney, 2005.

[51] N. J. Wildberger. Polynomials and Polynumbers — Arithmetic and Geometry Math Foundations 57 — NJ Wildberger. YouTube. 2010. URL: https://www.youtube.com/watch?v=-Ad6pYjCAmg.

[52] N. J. Wildberger. Row and column polynumbers — Arithmetic and Geometry Math Foundations 65 — NJ Wildberger. YouTube. 2010. URL: https://www.youtube.com/watch?v=_9FvrO1JTTI.

[53] N. J. Wildberger. The chromatic algebra of 2×2 matrices II — Wild Linear Algebra b 42 — NJ Wildberger. YouTube. 2020. URL: https://www.youtube.com/watch?v=QDIcznHyWT.