Group Realizations of Configurations

by

Jeffrey Lanyon

A thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

in partial fulfillment of the requirements of the degree of

Master of Science

Department of Mathematics

University of Manitoba

Winnipeg

Abstract

An (n_k) configuration is a family of n points and n (straight) lines in the real plane such that each point is on precisely k of the lines; each line contains precisely k of the points, and any two points are on at most one line. The study of configurations goes back more than a century and it was popularized by Hilbert and Cohn-Vossen by introducing an attractive chapter on geometric configurations in their now classical book called "Geometry and Imagination." Recently, this topic has been revived by Branko Grünbaum in his wonderful book entitled "Configurations of Points and Lines" It presents in detail the history of the topic, with its surges and declines since its beginning in 1876. It covers all the advances in the field since the revival of interest in geometric configurations some 25 years ago. Here we refer to this fundamental publication as "the Book".

In this thesis, we address several open problems mentioned in the Book. One of the basic and profound questions frequently asked in this topic is about the "existence" of configurations. Given an abstract combinatorially defined point-block configuration, the basic questions are "what do we mean

by exist" and how do we "realize" the configuration. The Book deals with two kinds of realizations: points are points in the real Euclidean (or projective) plane and the blocks are straight lines or (topological) pseudo-lines.

Motivated by the fascinating fact that a non-singular cubic curve in the projective plane over a field admits a natural group law "+" such that three points $\{P, Q, R\}$ are collinear if and only if the the sum $P + Q + R = 0$ under the group law, we define the concept of a group realization of a given configuration: an (n_k) configuration C is group-realizable if there is an embedding f of C into a group G such that $\{P_1, P_2, \ldots, P_k\}$ is a block in $C \implies f(P_1) + f(P_2) + \cdots + f(P_k) = 0$ in G. The group realizations are, in turn, pressed into service to construct geometric realizations (of $(n_3)'s$ and $(n_4)'s$) in the real or the complex plane using the well-known group structures on cubic curves. Using a variety of techniques from algebra and number theory like: the resultant of polynomials, Hensel's Lemma on lifting primitive roots, companion matrices and Bunyakovski's conjecture, the following new realization theorems are proved in this thesis.

1. Group realizations of several cyclic (n_3)-configurations.

2. Geometric realizations of (n_3)-configurations using the group structure on cubic curves.

3. Group realizations of several cyclic (n_4)-configurations.

4. Group law on non-circular ellipses using points and circles.

5. A new geometric representation of (n_4)'s using point-circle models.

6. Hensel's Lemma and infinitude of (n_3)'s and (n_4)'s with group realizations.

7. Properties forced by group realizations

8. Group realizations of some designs (e.g. finite projective planes, biplanes etc.).

9. Miscellaneous examples.

   (a) The Desargues configuration (10_3).

   (b) Group realizable cyclic (n_5)-configurations.

   (c) Group realizations of some well-known orchards.

   (d) Examples of configurations having no group realization.

   (e) The Cremona-Richmond (15_3)-configuration.

Acknowledgements

Thank you to my supervisor, Dr. R. Padmanabhan, for: sharing with me the problems he and the late Dr. N.S. Mendelsohn began together; his infectious enthusiasm for his work; and, for his much appreciated encouragement over the last two years. Thank you to my thesis committee, Dr. S. Kirkland, Dr. W. Kocay, and Dr. Y. Zhang for their constructive comments. Finally, thank you to the University of Manitoba Department of Mathematics and its wonderful faculty and staff.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this thesis we study the representation of abstract configurations, with particular emphasis on cyclic configurations, by abelian groups. Finite configurations share analogous properties with plane geometry, the most general being an underlying set of points and a distinguished subset of those points which we will call lines, or blocks. We further require that each point be incident with the same number of lines, and that each line contain the same number of points. To clarify, in a given configuration C, the points $P_1, P_2, \ldots, P_n$ of C being collinear simply means that $\{P_1, P_2, \ldots, P_n\}$ is a block (line) of C.

Definition 1.0.1. *An (n_k) configuration is a set of n points and n lines in which each point is contained in exactly k lines; each line contains exactly k points; and, any two lines intersect in at most one point.*

We use the notation of Grünbaum ([18] page 68) to represent cyclic (n_k)

configurations.

Definition 1.0.2. *A general cyclic configuration* $C_k(n, a_1, a_2, \ldots, a_{k-1})$ *consists of* $k-$*tuples* $j, a_1+j, a_2+j, \ldots, a_{k-1}+j$, *for given* $a_1, \ldots, a_{k-1}$ *with* $0 < a_1 < \ldots < a_{k-1} < n$ *and for* $1 \leq j \leq n$, *all entries taken modulo* n.

For example the well-known seven point Fano configuration can be represented as the cyclic configuration $C_3(7, 1, 3)$. Here the points are given by the set $\{0, 1, 2, 3, 4, 5, 6\}$ and the blocks by the triples $\{j, j+1, j+3\} \pmod 7$ where $0 \leq j \leq 6$. The configuration table thus obtained for the $C_3(7, 1, 3)$ is depicted in the following table.

0	1	2	3	4	5	6
1	2	3	4	5	6	0
3	4	5	6	0	1	2

Table 1.1: Blocks defining the configuration (7_3)

Classically, realizability simply meant drawing a reasonably exact drawing of the configuration in the real plane. The problems with this definition became clear early in the study of configurations. A suitable remedy followed: a realization in the real plane would be a coordinatization of the points where the lines are given by linear equations.

It is a folklore result in the field that the Fano configuration cannot be represented in the real plane. In addition to the Fano configuration, the reader is no doubt familiar with the famous Möbius-Kantor configuration, as well as the configurations associated with the famous Desargues and Pappus Theorems. The impetus behind this thesis is to embed such configurations

into abelian groups by drawing an analogy with the theory of cubic curves. Namely, as a guide, we adapt the geometric definition of the group law on cubic curves, and in chapter 4 introduce a new notion of realizability that is natural for cyclic (n_4) configurations.

Definition 1.0.3. *A group embedding is an injective mapping, f, from an (n_k) configuration, C, into an abelian group G, such that if a set of k points $\{P_1, \ldots, P_k\}$ is a line C, then $f(P_1) + \cdots + f(P_k) = 0$ in G. (Extra collinearities may occur in the group image without being true in the original C.)*

As a simple example, the Möbius-Kantor configuration, with point set $\{0, 1, 2, 3, 4, 5, 6, 7\}$ can be embedded into $\mathbb{Z}_3 \times \mathbb{Z}_3$ according to the rule:

$$i \to \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^i \begin{pmatrix} 0 \\ 1 \end{pmatrix} \pmod 3.$$

This generates the following embedding:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 2 \\ 1 \end{pmatrix} & \begin{pmatrix} 2 \\ 2 \end{pmatrix} & \begin{pmatrix} 0 \\ 2 \end{pmatrix} & \begin{pmatrix} 2 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 2 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array}$$

The verification that the sum of the images of the points on each line(*line sums*) is $(0, 0)$ in the group $\mathbb{Z}_3 \times \mathbb{Z}_3$ is easily verified by inspecting the following

graphical depiction of the embedding.

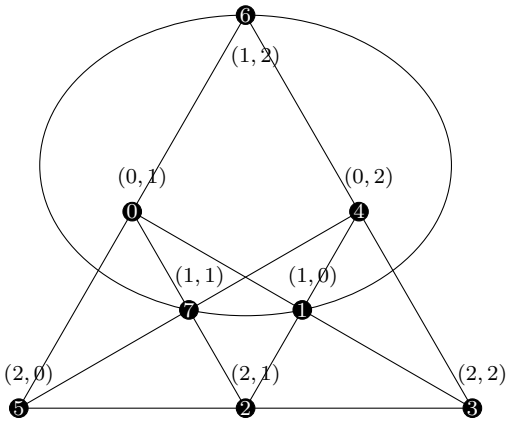

Figure 1.1: (8_3) in $\mathbb{Z}_3 \times \mathbb{Z}_3$

Indeed, the majority of the body of this thesis is dedicated to finding the sort of exponential map illustrated in the previous embedding, and developing general techniques for their construction. Three of the four major techniques we use, and develop for embedding cyclic configurations all hinge upon the resultant of two polynomials.

Definition 1.0.4. *The Sylvester matrix of two univariate polynomials* $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, *and* $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ *of degrees* m *and* n *respectively, is the* $(m+n) \times (m+n)$ *matrix formed by filling the matrix beginning with the upper left corner with the coefficients of* $f(x)$*; appending the remainder of the entries of the row with zeroes; then, shifting down one row and one column to the right and filling in the coefficients starting there until they hit the right side. The process is then repeated for the coefficients of g(x). We denote this by* $Syl(f, g; x)$.

Definition 1.0.5. *The Resultant of two univariate polynomials* $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, *and* $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ *of degrees* m *and* n *respectively, is defined to be the determinant of the Sylvester matrix* $Syl(f, g; x)$.

Definition 1.0.6. *The Singer polynomial of the general cyclic configuration* $C_k(n, a_1, a_2, \ldots, a_{k-1})$ *is denoted by* $\sigma(x)$, *and given by* $\sigma(x) = 1 + x^{a_1} + x^{a_2} + \cdots + x^{a_{k-1}}$.

The resultant of two polynomials is zero if and only if the two polynomials have a common root (see [11]). By examining the prime factorizations of the resultants of the associated Singer polynomial of a cyclic (n_k) configuration, and either the n^{th} cyclotomic polynomial $(c_n(x))$ or the polynomial $x^n - 1$, we can gain insight into potential group candidates with which to construct our embeddings.

Example 1.0.7. *Given the the polynomials* $f(x) = 3x^3 + x^2 + 2x + 1$, *and* $g(x) = 5x^2 + 7x + 9$ *their Sylvester matrix* $Syl(f, g; x)$ *is given by the following:*

$$Syl(f, g; x) = \begin{pmatrix} 3 & 1 & 2 & 1 & 0 \\ 0 & 3 & 1 & 2 & 1 \\ 5 & 7 & 9 & 0 & 0 \\ 0 & 5 & 7 & 9 & 0 \\ 0 & 0 & 5 & 7 & 9 \end{pmatrix}.$$

The resultant of $Syl(f, g; x)$ is given by the following:

$$\begin{aligned} resultant(f, g; x) &= det(Syl(f, g; x)) \\ &= \begin{vmatrix} 3 & 1 & 2 & 1 & 0 \\ 0 & 3 & 1 & 2 & 1 \\ 5 & 7 & 9 & 0 & 0 \\ 0 & 5 & 7 & 9 & 0 \\ 0 & 0 & 5 & 7 & 9 \end{vmatrix} \\ &= 4697 \\ &= 7 \cdot 11 \cdot 61. \end{aligned}$$

So the two polynomials have no common solution over the reals; however, it can be shown that they share a common solution of 8 modulo 11.

The four basic techniques we develop are influenced heavily by the work of J.Singer [32], and Mendelsohn, Padmanabhan, and Wolk [31]. They are briefly described as follows:

- *Type 1 Embedding* This embedding maps a cyclic (n_k) configuration into a single copy of a cyclic group.

- *Type 2 Embedding* This embedding maps a cyclic configuration into a direct product of cyclic groups by considering field extensions.

- *Type 3 Embedding* This embedding maps a cyclic configuration into a single copy of a cyclic group, but differs from the first type by using the Carmichael Lambda function to identify an appropriate group.

- *Type 4 Embedding* Cyclic embedding matrices, analogous to the canonical concept of a "companion matrix" (in fact, elementarily equivalent to the standard form, see [13]. We thank Dr. S. Kirkland for this reference). Here we associate a square matrix with a Singer polynomial or one of its factors.

Definition 1.0.8. *For a positive integer $n \geq 2$, the Carmichael Lambda function is defined to be the smallest positive integer $\lambda(n)$ such that for all integers m where $gcd(m, n) = 1$, $m^{\lambda(n)} \equiv 1 \mod n$.*

So, for a given positive $n \geq 2$, the Carmichael Lambda function calculates the exponent of the group of units modulo n. In other words it calculates the *lcm* of the orders of the elements of the group of units. We can calculate it with the following formulas:

$$\lambda\left(p^{\alpha}\right) = \begin{cases} \phi\left(p^{\alpha}\right), \text{ if } \alpha \leq 2 \text{ or } p \geq 3 \\ \frac{1}{2}\phi\left(p^{\alpha}\right), \text{ if } \alpha \geq 3 \text{ and } p = 2 \end{cases}$$

$$\lambda\left({p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}\right) = lcm\left(\lambda\left({p_1}^{\alpha_1}\right), \cdots, \lambda\left({p_k}^{\alpha_k}\right)\right),$$

where the p_i are distinct positive prime numbers.

In this thesis we describe group embeddings for hundreds of cyclic (n_k) configurations. Of particular note we give a partial answer to a question of Grünbaum [18] page 68, in establishing the existence of infinitely many geometrically realizable $C_3(n, 1, 4)$ configurations. We also describe a new notion of geometric realizability for cyclic $C_4(n, 1, 4, 6)$ configurations which employs the group law on a non-circular conic and has a natural correspondence with Type 1 Embeddings.

Chapter 2

Point-Line Configurations, Groups and Cubic Curves

The importance of cubic curves for the problem of geometric realizations of configurations comes from two facts:

1. Non-singular cubic curves give a natural geometrically defined group law such that three points $\{P, Q, R\}$ on the cubic curve are collinear if and only if $P + Q + R = 0$ under the group law.

2. The group of points on a non-singular cubic curve over the complex field is $S^1 \times S^1$, and the group over the reals is S^1, or $S^1 \times \mathbb{Z}_2$, where S^1 is the circle group. [33]

In particular, every finite cyclic group is a subgroup of S^1 (parameter values viewed as 'degrees'), and a product of two finite cyclic groups is a

subgroup of $S^1 \times S^1$(see page 247 of [18]). Hence a configuration embedded in a single cyclic group exists in the real plane and similarly a configuration embedded in the product of two cyclic groups exists in the complex projective plane. The most well-known example of the latter type is $AG(2,3)$ which is embeddable in $\mathbb{Z}_3 \times \mathbb{Z}_3$ and hence is realizable in the complex projective plane as the set of inflection points of a complex cubic (the 19th century famous Wendespunkte). It was this design that prompted J.J. Sylvester to make the now famous Sylvester-Gallai Theorem.

Theorem 2.0.1. *(Sylvester Gallai Theorem [21]) Given a finite number of points in the Euclidean plane, either all the points lie on a single line; or there is a line which contains exactly two of the points.*

Using the language of the group law on cubics, we describe some of the geometric properties of (n_3) configurations in the language of groups and vice-versa.

2.1 The Group Law on a Cubic Curve

The starting point is the binary $* -$ *operation* defined by the chord tangent process. In particular, we need the following well-known facts about the group law on non-singular cubic curves which we state in the form of theorems (for proofs and more details see [27], and [31]).

Theorem 2.1.1. *The following properties are well-known for the chord-tangent process in a non-singular cubic curve(see Lemma 1.3 in [27]).*

1. *$e * e = e$ if and only if e is an inflection point(i.e., the tangent at e meets the curve again at e).*

2. *$P * Q = Q * P$.*

3. *$P * (Q * P) = Q$*

4. *$(P * Q) * (R * S) = (P * R) * (Q * S)$*

5. *$((P * Q) * R) * S = ((S * Q) * R) * P$*

In fact, modulo (2.) and (3.), the identities (4.), and (5.) are equivalent. Knapp has given a detailed proof of (4.) (see Lemma 3.9 of [22]).

Theorem 2.1.2. *For a point P on the curve E, the following statements are equivalent.*

1. *P is an inflection point i.e. the tangent at P meets the curve again at P.*

2. *$P * P = P$.*

3. *$P + P + P = e$, the zero of the group law $+$: $P + Q = (P * Q) * e$.*

Proof. (1.) $\implies$ (2.) by the very definition of the $*$ operation. (2.) $\implies$ (3.). $P+P+P = ((P*P)*e)+P = (P*e)+P = ((P*e)*P)*e = e*e = e$.

(3.) $\Longrightarrow$ (1.) Let $P + P + P = e$. Then,

$$\begin{aligned}
(e * P) * P &= e && ((3.) \text{ of Theorem 2.2.1}) \\
&= P + P + P && (\text{assumption}) \\
&= ((P * P) * e) * P) * e, && (\text{definition of } +) \\
&= ((e * e) * P) * (P * P) && ((5.) \text{ of Theorem 2.2.1}) \\
&= (e * P) * (P * P)
\end{aligned}$$

and hence $P = P * P$, meaning that P is an inflection point. In view of this, we can choose any inflection point as the identity element of the group law.

□

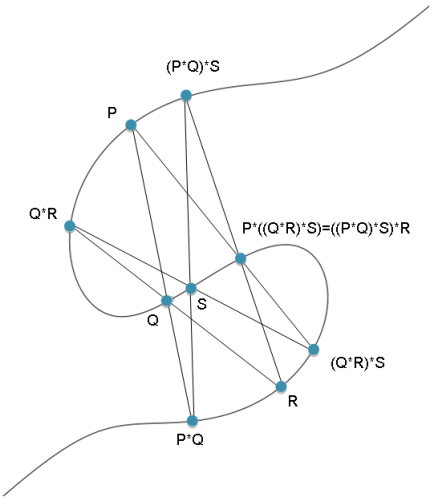

Figure 2.1: Validity of the identity $P * ((Q * R) * S) = ((P * Q) * S) * R$ for the chord-tangent operation $(*)$ on non-singular cubic curve.

Theorem 2.1.3. *Let e be an inflection point on a non-singular cubic curve C. Let the binary operation $+$ be defined by the familiar rule $P+Q = (P*Q)*e$. Then the algebra $(C; +, -, e)$ is an abelian group such that three points P, Q, R are collinear if and only if $P + Q + R = e$.*

Proof. It is obvious that the group law $+$ is commutative since the $*$-operation is commutative. The non-trivial associativity is just a reformulation of (5) of Theorem 2.2.1:

$$\begin{aligned}(P+Q)+R &= (((P*Q)*e)*R)*e \\ &= (((R*Q)*e)*P)*e \\ &= (R+Q)+P \\ &= P+(Q+R).\end{aligned}$$

Finally, let three points P, Q, R be collinear. Then

$$\begin{aligned}P+Q+R &= (P+Q)+(P*Q) \\ &= ((P*Q)*e+(P*Q) \\ &= (((P*Q)*e)*(P*Q))*e \\ &= e*e \\ &= e.\end{aligned}$$

The converse is equally easy to see.

□

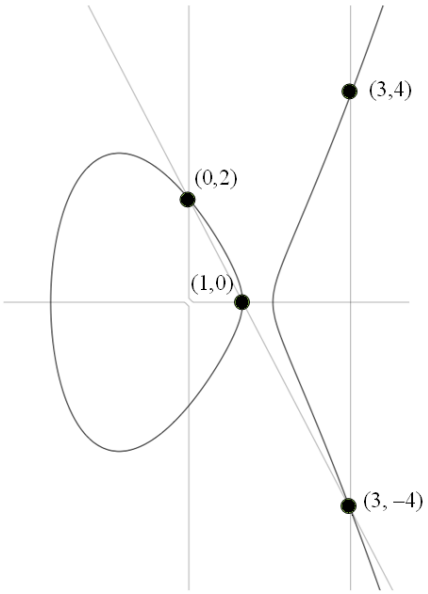

Figure 2.2: Group law on the cubic curve $y^2 = x^3 - 5x + 4$.

Referring to Figure 2.2 here: $(0,2) * (1,0) = (3,-4)$ and hence $(0,2) + (1,0) = (3,4)$. The group law calculation is as follows: the line joining $(0,2)$ and $(1,0)$ is $y = 2 - 2x$. Eliminating y from the equations of this line and the given cubic, we have $(2-2x)^2 = x^3 - 5x + 4$. This cubic in x has three solutions and already we know two of them: $x = 0$ and $x = 1$. The remaining third root r is where the line meets the curve again. The sum of the three roots is 4 i.e. $0 + 1 + r = 4$ and hence $r = 3$. So $y = 2 - 6- = -4$. This proves that $(0,2) * (1,0) = (3,-4)$ and one vertical reflection shows that $(0,2) + (1,0) = (3,4)$.

In Problem 2 (of Section 2.11, page 151, the Book) asks: Are there any obstructions to the geometric realizability of (n_3) configurations? In this the-

sis, we suggest that the minimal group rank may force an (n_3) configuration to be non-realizable over the real plane. More specifically,

Conjecture 2.1.4. *If the minimal group realization of a cyclic (n_3)-configuration contains two or more copies of a cyclic group $\mathbb{Z}_m$ where $m \geq 3$, then it has no geometric realization.*

Here are a few examples proved in this thesis which support this claim.

Table 2.1: Support for Conjecture 2.1.4

Configuration	(n_3)	Minimal Group	Realizable over reals?
$C_3(7,1,3)$	Fano (7_3)	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	No; (realizable over $GF(k)$ iff k satisfies $2 = 0$)
$C_3(8,1,3)$	M-K (8_3)	$\mathbb{Z}_3 \times \mathbb{Z}_3$	No;(realizable over $\mathbb{F}$ iff k has a cube root of unity)
$C_3(15,1,3)$	(15_3)	$\mathbb{Z}_{31}$	Realizable over the real plane (via cubic curves)
$C_3(20,1,4)$	(20_3)	$\mathbb{Z}_{25}$	Yes, Realizable over the Real plane (via cubic curves)
Pappus	(9_3)	$\mathbb{Z}_9$	Yes, realizable over the real plane
Desargues	(10_3)	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Yes, realizable over the real plane
Cremona-Richmond	(15_3)	$\mathbb{Z}_{30}$	Yes, realizable over the real plane
$PG(2,3)$	(13_4)	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	No

Chapter 3

Cyclic (n_3) Configurations

The cyclic (n_3) configurations $C_3(n, a, b)$ are perhaps the best studied of all configurations; early studies of $C_3(n, a, b)$ go back to 1895[6] done by Brunel. They hold an important position in our study of configurations for several reasons. The (n_3) configurations represent the most fundamental configurations. Indeed among the (n_3)'s are the Fano configuration, the Möbius-Kantor configuration, the Pappus configuration, and the Desargues configuration. They provide a canonical underlying structure for the notion of an *Extension of a Configuration* which we introduce in Chapter 5

The motivation for the study of cyclic (n_3)'s comes from a problem of Grünbaum [18] page 68 problem 4. It asks: *Is* $C_3(n, 1, 4)$ *geometrically realizable for some* n*? Generalize.* In section 3.1 we provide some 120 group embeddings of $C_3(n, 1, 3)$'s most of which are embeddings into single cyclic groups (implying classical geometric realizability). In section 3.3 we give

group embeddings for almost 40 $C_3(n, 1, 4)$'s almost all of which are embeddings into single cyclic groups, and give a partial answer to Grünbaums problem. In Chapter 6, using Hensel's lifting lemma 6.1.1, we show that there are infinitely many realizations of $C_3(n, 1, 4)$'s. The basis for our study of cyclic (n_3)'s is the paper of Mendelsohn, Padmanabhan, and Wolk [27]. Indeed, much of the work of this chapter focuses on expanding upon and extending the ideas presented in [27].

3.1 $C_3(n, 1, 3)$

In this section we provide several examples of the embedding types described in the introduction.

The first example is of Type 1 embedding of an n_3 configuration: there is a prime p dividing the resultant and also $n|p-1$.Consider the cyclic configuration $C_3(19, 1, 3)$. Since the resultant $Res(x^3 + x + 1, c_{19}(x)) = 457$, a prime, and $19|456$ we have a candidate for an embedding. Note also that 16 has order 19 in the multiplicative group modulo 457. We have the following result:

Theorem 3.1.1. *The cyclic configuration $C_3(19, 1, 3)$ has a group realization in $\mathbf{Z}_{457}$.*

Proof. Let $f : C_3(19, 1, 3) \to \mathbb{Z}_{457}$ be given by the following:

$$f : i \to 16^i \mod 457.$$

With respect to multiplication, the order of 16 modulo 457 is 19, thus f is injective. Since $16^3 + 16 + 1 \equiv 0 \mod 457$, we have that for any j

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= 16^j + 16^{j+1} + 16^{j+3} \mod 457 \\ &= 16^j(1 + 16 + 16^3) \mod 457 \\ &\equiv 0 \mod 457. \end{aligned}$$

Thus f is a group embedding.

□

Corollary 3.1.1.1. *$C_3(19, 1, 3)$ is geometrically realizable.*

The second example is a Type 4 embedding(matrix) of an (n_3) configuration: there is a prime power p^k dividing the resultant and also $n|p^k - 1$. The first example in Table 3.1 is $C_3(7, 1, 3)$. The resultant of $x^3 + x + 1$, and $c_7(x)$ is 8, and $7|2^3 - 1$. Therefore, our target group for embedding $C_3(7, 1, 3)$ is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; however, this isn't as simple as the Type 1 embedding. For a Type 4 embedding we embed into a group of units of a factor ring, in this particular case the group of units of $\mathbb{Z}_2[x]/(x^3 + x + 1)$, (i.e., $GF(8)$).

Theorem 3.1.2. *The cyclic configuration $C_3(7, 1, 3)$ has a group realization in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, and $v = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Define the mapping $f : C_3(7, 1, 3) \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ to be given by the following

$$f : i \to \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^i \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mod 2.$$

That f is injective can be shown by computation (i.e, order of A modulo 2 is 7). Notice that

$$\begin{aligned} f(0) + f(1) + f(3) &= Iv + Av + A^3v \mod 2 \\ &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \mod 2 \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \mod 2 \end{aligned}$$

More generally, we have

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= A^j(I + A + A^3)v \mod 2 \\ &\equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \mod 2 \end{aligned}$$

Thus, f is a group embedding.

□

The third example is a Type 3 embedding which uses the Carmichael lambda function to identify a target group for an embedding. The resultant of

the ninth cyclotomic polynomial,$c_9(x)$ and the Singer polynomial x^3+x+1 is 3. The situation is not amenable to a Type 1 or a Type 2 embedding. To deal with this situation we use the Type 3 embedding. Notice that $\lambda(27) = 18$, and that the order of 7 modulo 27 is 9, and also that $7^3+7+1 \equiv 0 \mod 27$, therefore our target group for an embedding of $C_3(9,1,3)$ is $\mathbb{Z}_{27}$. Thus we have the following result.

Theorem 3.1.3. *The cyclic configuration $C_3(9,1,3)$ is group embeddable in $\mathbb{Z}_{27}$.*

Proof. Define the map $f : C_3(9,1,3) \to \mathbb{Z}_{27}$ by

$$f : i \to 7^i \mod 27.$$

Since the order of 7 modulo 27 is 9, f is injective. Since $7^3 + 7 + 1 \equiv 0 \mod 27$, we have that for any j

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= 7^j + 7^{j+1} + 7^{j+3} \mod 27 \\ &= 7^j(1 + 7 + 7^3) \mod 27 \\ &\equiv 0 \mod 27. \end{aligned}$$

Thus f is a group embedding.

□

The following table gives over 100 group embeddings for cyclic configurations: including many not found in appendix II of [27]. Note: a $*$ in

the *base* column of a table indicates that the base is a matrix (i.e., Type 4 embedding).

Table 3.1: $\mathcal{C}_3(n, 1, 3)$ embeddings

$configuration$	$Type$	$Resultant$	$Group$	$base$
$\mathcal{C}_3(7,1,3)$	2	8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$*$
$\mathcal{C}_3(8,1,3)$	2	9	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$*$
$\mathcal{C}_3(9,1,3)$	3	3	$\mathbb{Z}_{27}$	7
$\mathcal{C}_3(10,1,3)$	1	11	$\mathbb{Z}_{11}$	2
$\mathcal{C}_3(10,1,3)$	3	11	$\mathbb{Z}_{33}$	13
$\mathcal{C}_3(11,1,3)$	1	23	$\mathbb{Z}_{23}$	4
$\mathcal{C}_3(12,1,3)$	1	13	$\mathbb{Z}_{13}$	7
$\mathcal{C}_3(13,1,3)$	1	53	$\mathbb{Z}_{53}$	36
$\mathcal{C}_3(14,1,3)$	2	8	$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$	$*$
$\mathcal{C}_3(15,1,3)$	1	31	$\mathbb{Z}_{31}$	14
$\mathcal{C}_3(15,1,3)$	3	31	$\mathbb{Z}_{93}$	76
$\mathcal{C}_3(16,1,3)$	1	17	$\mathbb{Z}_{17}$	11
$\mathcal{C}_3(16,1,3)$	3	17	$\mathbb{Z}_{51}$	28
$\mathcal{C}_3(17,1,3)$	1	239	$\mathbb{Z}_{239}$	216
$\mathcal{C}_3(18,1,3)$	1	37	$\mathbb{Z}_{37}$	25
$\mathcal{C}_3(19,1,3)$	1	457	$\mathbb{Z}_{457}$	16
$\mathcal{C}_3(20,1,3)$	1	61	$\mathbb{Z}_{61}$	37
$\mathcal{C}_3(21,1,3)$	1	43	$\mathbb{Z}_{43}$	38
$\mathcal{C}_3(22,1,3)$	1	67	$\mathbb{Z}_{67}$	58
$\mathcal{C}_3(23,1,3)$	1	47	$\mathbb{Z}_{47}$	34
$\mathcal{C}_3(23,1,3)$	1	47	$\mathbb{Z}_{47}$	25
$\mathcal{C}_3(24,1,3)$	2	9	$\mathbb{Z}_9 \times \mathbb{Z}_9$	$*$
$\mathcal{C}_3(25,1,3)$	1	4651	$\mathbb{Z}_{4651}$	3978
$\mathcal{C}_3(26,1,3)$	1	131	$\mathbb{Z}_{131}$	51
$\mathcal{C}_3(27,1,3)$	1	379	$\mathbb{Z}_{379}$	193
$\mathcal{C}_3(27,1,3)$	3	379	$\mathbb{Z}_{81}$	61
$\mathcal{C}_3(28,1,3)$	1	$29 \cdot 2^3$	$\mathbb{Z}_{29}$	26
$\mathcal{C}_3(28,1,3)$	3	$29 \cdot 2^3$	$\mathbb{Z}_{87}$	55
$\mathcal{C}_3(29,1,3)$	1	21577	$\mathbb{Z}_{21577}$	10907

$\mathcal{C}_3(30,1,3)$	3	31	$\mathbb{Z}_{93}$	34
$\mathcal{C}_3(30,1,3)$	1	31	$\mathbb{Z}_{31}$	3
$\mathcal{C}_3(30,1,3)$	3	31	$\mathbb{Z}_{99}$	79
$\mathcal{C}_3(31,1,3)$	1	46811	$\mathbb{Z}_{46811}$	13318
$\mathcal{C}_3(32,1,3)$	1	449	$\mathbb{Z}_{449}$	321
$\mathcal{C}_3(33,1,3)$	1	1453	$\mathbb{Z}_{1453}$	1321
$\mathcal{C}_3(33,1,3)$	3	1453	$\mathbb{Z}_{207}$	142
$\mathcal{C}_3(34,1,3)$	1	613	$\mathbb{Z}_{613}$	226
$\mathcal{C}_3(35,1,3)$	1	26881	$\mathbb{Z}_{26881}$	11358
$\mathcal{C}_3(36,1,3)$	1	73	$\mathbb{Z}_{73}$	23
$\mathcal{C}_3(36,1,3)$	3	73	$\mathbb{Z}_{351}$	7
$\mathcal{C}_3(37,1,3)$	1	$149 \cdot 3109$	$\mathbb{Z}_{149}$	67
$\mathcal{C}_3(37,1,3)$	1	$149 \cdot 3109$	$\mathbb{Z}_{3109}$	2186
$\mathcal{C}_3(38,1,3)$	1	1483	$\mathbb{Z}_{1483}$	724
$\mathcal{C}_3(39,1,3)$	1	79^2	$\mathbb{Z}_{79}$	11
$\mathcal{C}_3(39,1,3)$	3	79^2	$\mathbb{Z}_{477}$	142
$\mathcal{C}_3(40,1,3)$	1	241	$\mathbb{Z}_{241}$	47
$\mathcal{C}_3(41,1,3)$	1	2135117	$\mathbb{Z}_{2135117}$	1650854
$\mathcal{C}_3(42,1,3)$	1	379	$\mathbb{Z}_{379}$	124
$\mathcal{C}_3(43,1,3)$	1	$173 \cdot 26489$	$\mathbb{Z}_{173}$	136
$\mathcal{C}_3(43,1,3)$	1	$173 \cdot 26489$	$\mathbb{Z}_{26489}$	21428
$\mathcal{C}_3(44,1,3)$	1	4357	$\mathbb{Z}_{4357}$	252
$\mathcal{C}_3(45,1,3)$	1	35281	$\mathbb{Z}_{35281}$	34376
$\mathcal{C}_3(46,1,3)$	1	$47 \cdot 139$	$\mathbb{Z}_{47}$	35
$\mathcal{C}_3(46,1,3)$	1	$47 \cdot 139$	$\mathbb{Z}_{139}$	105
$\mathcal{C}_3(47,1,3)$	1	$283 \cdot 74731$	$\mathbb{Z}_{283}$	216
$\mathcal{C}_3(47,1,3)$	1	$283 \cdot 74731$	$\mathbb{Z}_{74731}$	50412
$\mathcal{C}_3(48,1,3)$	1	577	$\mathbb{Z}_{577}$	505
$\mathcal{C}_3(48,1,3)$	3	577	$\mathbb{Z}_{153}$	79
$\mathcal{C}_3(49,1,3)$	1	$197 \cdot 28813$	$\mathbb{Z}_{197}$	133
$\mathcal{C}_3(49,1,3)$	1	$197 \cdot 28813$	$\mathbb{Z}_{28813}$	7969
$\mathcal{C}_3(50,1,3)$	1	1301	$\mathbb{Z}_{1301}$	666
$\mathcal{C}_3(51,1,3)$	1	136069	$\mathbb{Z}_{136069}$	90067
$\mathcal{C}_3(52,1,3)$	1	20593	$\mathbb{Z}_{20593}$	1862
$\mathcal{C}_3(53,1,3)$	1	209520979	$\mathbb{Z}_{209520979}$	20125211
$\mathcal{C}_3(54,1,3)$	1	811	$\mathbb{Z}_{811}$	224
$\mathcal{C}_3(55,1,3)$	1	19567351	$\mathbb{Z}_{19567351}$	16525916

$\mathcal{C}_3(56,1,3)$	1	$617 \cdot 2^3$	$\mathbb{Z}_{617}$	20
$\mathcal{C}_3(57,1,3)$	1	$229 \cdot 3079$	$\mathbb{Z}_{229}$	167
$\mathcal{C}_3(57,1,3)$	1	$229 \cdot 3079$	$\mathbb{Z}_{3079}$	843
$\mathcal{C}_3(57,1,3)$	3	$229 \cdot 3079$	$\mathbb{Z}_{4113}$	16
$\mathcal{C}_3(58,1,3)$	1	65657	$\mathbb{Z}_{65657}$	58953
$\mathcal{C}_3(59,1,3)$	1	$3541 \cdot 709 \cdot 827$	$\mathbb{Z}_{709}$	681
$\mathcal{C}_3(59,1,3)$	1	$3541 \cdot 709 \cdot 827$	$\mathbb{Z}_{827}$	235
$\mathcal{C}_3(59,1,3)$	1	$3541 \cdot 709 \cdot 827$	$\mathbb{Z}_{3541}$	3100
$\mathcal{C}_3(60,1,3)$	2	121	$\mathbb{Z}_{11} \times \mathbb{Z}_{11}$	$*$
$\mathcal{C}_3(60,1,3)$	3	121	$\mathbb{Z}_{793}$	98
$\mathcal{C}_3(60,1,3)$	3	121	$\mathbb{Z}_{143}$	46
$\mathcal{C}_3(61,1,3)$	1	4459734401	$\mathbb{Z}_{4459734401}$	2051096448
$\mathcal{C}_3(62,1,3)$	1	$1117 \cdot 5^3$	$\mathbb{Z}_{1117}$	865
$\mathcal{C}_3(63,1,3)$	1	3093931	$\mathbb{Z}_{3093931}$	263384
$\mathcal{C}_3(64,1,3)$	1	204353	$\mathbb{Z}_{204353}$	183585
$\mathcal{C}_3(65,1,3)$	1	$22621 \cdot 131^2$	$\mathbb{Z}_{131}$	5
$\mathcal{C}_3(65,1,3)$	1	$22621 \cdot 131^2$	$\mathbb{Z}_{131}$	75
$\mathcal{C}_3(65,1,3)$	1	$22621 \cdot 131^2$	$\mathbb{Z}_{22621}$	11766
$\mathcal{C}_3(65,1,3)$	3	67^2	$\mathbb{Z}_{393}$	136
$\mathcal{C}_3(66,1,3)$	1	67^2	$\mathbb{Z}_{67}$	13
$\mathcal{C}_3(66,1,3)$	1	67^2	$\mathbb{Z}_{67}$	63
$\mathcal{C}_3(66,1,3)$	3	67^2	$\mathbb{Z}_{201}$	130
$\mathcal{C}_3(67,1,3)$	1	$3330973 \cdot 13267$	$\mathbb{Z}_{13267}$	9395
$\mathcal{C}_3(68,1,3)$	1	442069	$\mathbb{Z}_{442069}$	256885
$\mathcal{C}_3(69,1,3)$	1	14323159	$\mathbb{Z}_{14323159}$	2469685
$\mathcal{C}_3(69,1,3)$	3	14323159	$\mathbb{Z}_{423}$	25
$\mathcal{C}_3(70,1,3)$	1	7351	$\mathbb{Z}_{7351}$	3929
$\mathcal{C}_3(71,1,3)$	1	203878759789	$\mathbb{Z}_{203878759789}$	112633599223
$\mathcal{C}_3(72,1,3)$	1	$1297 \cdot 3^2$	$\mathbb{Z}_{1297}$	397
$\mathcal{C}_3(73,1,3)$	1	$293 \cdot 1494570611$	$\mathbb{Z}_{293}$	256
$\mathcal{C}_3(74,1,3)$	1	1385429	$\mathbb{Z}_{1385429}$	675378
$\mathcal{C}_3(75,1,3)$	1	$151 \cdot 14401$	$\mathbb{Z}_{151}$	121
$\mathcal{C}_3(75,1,3)$	1	$151 \cdot 14401$	$\mathbb{Z}_{14401}$	13801
$\mathcal{C}_3(76,1,3)$	1	2033989	$\mathbb{Z}_{2033989}$	1105489
$\mathcal{C}_3(77,1,3)$	1	$4621 \cdot 617 \cdot 3851$	$\mathbb{Z}_{617}$	170
$\mathcal{C}_3(77,1,3)$	1	$4621 \cdot 617 \cdot 3851$	$\mathbb{Z}_{3851}$	3005

$\mathcal{C}_3(77,1,3)$	1	$4621 \cdot 617 \cdot 3851$	$\mathbb{Z}_{4621}$	3700
$\mathcal{C}_3(78,1,3)$	1	22777	$\mathbb{Z}_{22777}$	4561
$\mathcal{C}_3(79,1,3)$	1	$8383481 \cdot 517609$	$\mathbb{Z}_{8383481}$	521602
$\mathcal{C}_3(80,1,3)$	1	$401 \cdot 641$	$\mathbb{Z}_{401}$	157
$\mathcal{C}_3(80,1,3)$	1	$401 \cdot 641$	$\mathbb{Z}_{641}$	584
$\mathcal{C}_3(80,1,3)$	3	$401 \cdot 641$	$\mathbb{Z}_{187}$	79
$\mathcal{C}_3(81,1,3)$	1	$3 \cdot 303610033$	$\mathbb{Z}_{303610033}$	234749658
$\mathcal{C}_3(82,1,3)$	1	$83 \cdot 77081$	$\mathbb{Z}_{83}$	35
$\mathcal{C}_3(82,1,3)$	1	$83 \cdot 77081$	$\mathbb{Z}_{77081}$	54333
$\mathcal{C}_3(82,1,3)$	3	$83 \cdot 77081$	$\mathbb{Z}_{249}$	118
$\mathcal{C}_3(83,1,3)$	1	20019533360297	$\mathbb{Z}_{20019533360297}$	2085399523672
$\mathcal{C}_3(84,1,3)$	1	3109	$\mathbb{Z}_{3109}$	1989
$\mathcal{C}_3(84,1,3)$	3	3109	$\mathbb{Z}_{261}$	142
$\mathcal{C}_3(85,1,3)$	1	179916121591	$\mathbb{Z}_{179916121591}$	50541620165
$\mathcal{C}_3(86,1,3)$	1	$431 \cdot 31907$	$\mathbb{Z}_{431}$	47
$\mathcal{C}_3(86,1,3)$	1	$431 \cdot 31907$	$\mathbb{Z}_{31907}$	17963
$\mathcal{C}_3(87,1,3)$	1	$1741 \cdot 523 \cdot 1567$	$\mathbb{Z}_{523}$	114
$\mathcal{C}_3(87,1,3)$	1	$1741 \cdot 523 \cdot 1567$	$\mathbb{Z}_{1567}$	141
$\mathcal{C}_3(87,1,3)$	1	$1741 \cdot 523 \cdot 1567$	$\mathbb{Z}_{1741}$	12
$\mathcal{C}_3(88,1,3)$	1	$89 \cdot 25169$	$\mathbb{Z}_{89}$	14
$\mathcal{C}_3(88,1,3)$	1	$89 \cdot 25169$	$\mathbb{Z}_{25169}$	11940
$\mathcal{C}_3(89,1,3)$	1	$159311 \cdot 179 \cdot 6956597$	$\mathbb{Z}_{179}$	149
$\mathcal{C}_3(89,1,3)$	1	$159311 \cdot 179 \cdot 6956597$	$\mathbb{Z}_{159311}$	43670
$\mathcal{C}_3(90,1,3)$	1	2341	$\mathbb{Z}_{2341}$	582
$\mathcal{C}_3(90,1,3)$	3	2341	$\mathbb{Z}_{837}$	34
$\mathcal{C}_3(91,1,3)$	1	1004948196253	$\mathbb{Z}_{1004948196253}$	738933342073
$\mathcal{C}_3(92,1,3)$	1	$277 \cdot 156217$	$\mathbb{Z}_{277}$	37
$\mathcal{C}_3(92,1,3)$	1	$277 \cdot 156217$	$\mathbb{Z}_{156217}$	37494
$\mathcal{C}_3(93,1,3)$	1	6517097017	$\mathbb{Z}_{6517097017}$	5190225171
$\mathcal{C}_3(94,1,3)$	1	$941 \cdot 67399$	$\mathbb{Z}_{941}$	513
$\mathcal{C}_3(94,1,3)$	1	$941 \cdot 67399$	$\mathbb{Z}_{67399}$	32105
$\mathcal{C}_3(95,1,3)$	1	$571 \cdot 7533294421$	$\mathbb{Z}_{571}$	521
$\mathcal{C}_3(96,1,3)$	1	207073	$\mathbb{Z}_{207073}$	51222
$\mathcal{C}_3(97,1,3)$	1	$43457 \cdot 971 \cdot 100062679$	$\mathbb{Z}_{971}$	223
$\mathcal{C}_3(97,1,3)$	1	$43457 \cdot 971 \cdot 100062679$	$\mathbb{Z}_{43457}$	10308
$\mathcal{C}_3(98,1,3)$	1	$491 \cdot 34693$	$\mathbb{Z}_{491}$	394
$\mathcal{C}_3(98,1,3)$	1	$491 \cdot 34693$	$\mathbb{Z}_{34693}$	28606
$\mathcal{C}_3(99,1,3)$	1	30152894311	$\mathbb{Z}_{30152894311}$	8264954137
$\mathcal{C}_3(99,1,3)$	3	30152894311_{24}	$\mathbb{Z}_{621}$	142
$\mathcal{C}_3(100,1,3)$	1	3273601	$\mathbb{Z}_{3273601}$	1582139

The data obtained from Table 3.1 was generated using either the Resultant Method 3.4.3 (embeddings into single cyclic groups), or by using the companion matrix technique illustrated in Figure 9.2. The data also provides the basis for the following two theorems relating to Type 1 and Type 3 group embeddings of cyclic configurations $C_3(n, 1, 3)$.

Theorem 3.1.4. *The cyclic configuration $C_3(n, 1, 3)$ has a group realization in $\mathbb{Z}_k$, provided there exists an r which is a common solution to both $c_n(x) = 0$ and $x^3 + x + 1 = 0 \mod k$ and the order of r modulo k is n.*

Proof Let $f : C_3(n, 1, 3) \to \mathbb{Z}_k$ be the mapping given by

$$f : i \to r^i \mod k.$$

Then since $r^3 + r + 1 \equiv 0 \mod k$ we have that for any j

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= r^j + r^{j+1} + r^{j+3} \mod k \\ &= r^j(1 + r + r^3) \mod k \\ &\equiv 0 \mod k \end{aligned}$$

Since the order of r modulo k is n, f is injective. Thus f is a group embedding.

□

3.2 An Algorithm for Type 1 Embeddings

In this section we describe Type 1 embeddings of $C_3(n, 1, 3)$ in simple algebraic terms, and give a simple algorithm for their determination. Instead of using cyclotomic polynomials, the polynomial $x^n - 1$ is used to find appropriately sized groups.

Example 3.2.1. *An algebraic technique to embed* $C_3(11, 1, 3)$ *into* $\mathbb{Z}_{23}$.

From Table 3.1 we have that $C_3(11, 1, 3)$ can be embedded into $\mathbb{Z}_{23}$ according to the rule $f(i) = 4^i \mod 23$. Our goal here is to reproduce the Type 1 embedding found in the previous section by analyzing the algebra associated with the problem. To this end, we want a finite field in which $x^{11} - 1 = 0$, and $x^3 + x + 1 = 0$ are both soluble. Since $x^3 = -x - 1$, we have the following two equations:

$$x^6 = x^2 + 2x + 1; \tag{3.1}$$

$$\begin{aligned} x^5 &= -x^3 - x^2 \\ &= -(-x - 1) - x^2 \\ &= -x^2 + x + 1. \end{aligned} \tag{3.2}$$

Therefore,

$$\begin{aligned} x^{11} &= x^6 \cdot x^5 \\ &= (x^2 + 2x + 1)(-x^2 + x + 1) \\ &= -x^4 - x^3 + 2x^2 + 3x + 1 \\ &= 3x^2 + 5x + 2 \end{aligned}$$

This gives

$$3x^2 + 5x + 1 = 0. \tag{3.3}$$

Multiplying equation 3.3 by x and reducing modulo x^3 gives

$$5x^2 - 2x - 3 = 0. \tag{3.4}$$

Solving equations 3.3 and 3.4 gives $x = \frac{-14}{31}$ in some field where 31 is invertible. Substituting $x = \frac{-14}{31}$ into $x^3 + x + 1 = 0$ gives $\frac{13593}{31^3} = 0$. As $13593 = 3 \cdot 23 \cdot 197$, we choose the prime 23 (our target group is thus $\mathbb{Z}_{23}$) and reducing $x = \frac{-14}{31}$ modulo 23 gives $x = 4$. Thus we have reproduced the Type 1 embedding from the previous section.

Example 3.2.2. *An algebraic technique to embed $C_3(13, 1, 3)$ into $\mathbb{Z}_{53}$.*

As a second example we will reproduce the Type 1 embedding of $C_3(13, 1, 3)$ from Table 3.1. Once again we assume that $x^3 + x + 1 = 0$, and $x^{13} - 1 = 0$.

With a similar series of calculations as in Example 3.2.1 it can be shown that $x^{13} = -x^2 - 8x - 5$, giving

$$x^2 + 8x + 6 = 0. \tag{3.5}$$

Multiplying equation 3.5 by x and reducing modulo $x^3 = -x - 1$ gives

$$8x^2 + 5x + 1 = 0. \tag{3.6}$$

Solving equation 3.5 and 3.6 for x gives $x = -\frac{49}{59}$, and substituting this into $x^3 + x + 1 = 0$ and solving gives $-\frac{82839}{59^3} = 0$ in some field. Since $82839 = 3 \cdot 53 \cdot 521$ we select 53 and $\mathbb{Z}_{53}$ is our target embedding group. Since $x = -\frac{49}{53} \equiv 36 \mod 53$, the base for the embedding is 36. Note that the order of 36 modulo 53 is 13, thus we have reproduced the Type 1 embedding from Table 3.1.

We can generalize the procedure illustrated in the previous two examples. Given the equations $x^n - 1 = 0$ and $x^3 + x + 1 = 0$, we can represent the equation $x^n - 1 = 0$ as the quadratic $ax^2 + bx + c = 0$. We get the auxiliary polynomial $bx^2 + (c - a)x - a = 0$, by multiplying $ax^2 + bx + c = 0$ by x and reducing modulo $x^3 + x + 1 = 0$. Solving the two quadratics gives $x = -\frac{a^2+bc}{a^2+b^2-ac}$, from which we can find our embedding. For example when $n = 11$, we have $a = 3, b = 5, c = 1$.

Algorithm 3.2.3. *QETM1(n) A list of bases and their associated groups are determined for an embedding of* $C_3(n, 1, 3)$. *A single integer input for the value of* n *outputs a list of pairs of integers.*

$\sigma(x) := x^3 + x + 1$

$c_n(x) \leftarrow x^n - 1$

1. $p \leftarrow c_n(x) \mod \sigma(x)$

2. $q \leftarrow x \cdot p \mod \sigma(x)$

3. $t \leftarrow$ solve p and q for x

4. $b \leftarrow \sigma(t)$

5. $d \leftarrow |numerator(b)|$

For each element k in the factor set of d if

(i) $n|k - 1$; and,

(ii) order of $t \mod k$ is n

$return(t \mod k, k)$

```
QEMT1 := proc(n::integer)
     local s,c,p,q,P,Q,R,t,b,d,T,k,i,a;
     s := x^3+x+1;
     c := x^n-1;
     p := rem(c, s, x);
     q := rem(x*p, s, x);
     P := coeff(q, x, 2)*p;
     Q := coeff(p, x, 2)*q;
     R := P-Q;
     t := solve(R, x);
     b := -value(Eval(s, x = t));
     d := numer(b);
     T := factorset(d);
     k := numelems(T);
for i from 1 to k do
     if ((T[i]-1 mod n)=0) then
          a:=t mod T[i];
          if order(a,T[i])=n then
               print(a,T[i]);
          end if
     end if
end do
end proc;
```

Figure 3.1: The MAPLE code for Algorithm 3.2.3.

3.3 $C_3(n, 1, 4)$

This section has its motivation in addressing a problem of Grünbaum [18] page 68, problem 4: *Is $C_3(n, 1, 4)$ geometrically realizable for some n? Generalize.* The techniques and types of embeddings of the previous section are applicable to $C_3(n, 1, 4)$ in an analogous manner, the chief difference being that the Singer polynomial in the case of $C_3(n, 1, 4)$ is $x^4 + x + 1$.

Example 3.3.1. *A Type 1 embedding of $C_3(18, 1, 4)$ into $\mathbb{Z}_{19}$.*

The resultant of $x^4 + x + 1$, and $c_{18}(x)$ is 19, and 18 divides $19 - 1 = 18$; also, since 2 satisfies the congruence $x^4 + x + 1 \equiv 0 \mod 19$ and the order of 2 modulo 19 is 18. We have the following result.

Theorem 3.3.2. *$C_3(18, 1, 4)$ has a group realization in $\mathbb{Z}_{19}$.*

Proof. Define the map $f : C_3(18, 1, 4) \to \mathbb{Z}_{19}$ by

$$f : i \to 2^i \mod 19.$$

Since the order of 2 modulo 19 is 18, f is injective. Since $2^4 + 2 + 1 \equiv 0 \mod 19$, we have that for any j

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= 2^j + 2^{j+1} + 2^{j+4} \mod 19 \\ &= 2^j(1 + 2 + 2^4) \mod 19 \\ &\equiv 0 \mod 19. \end{aligned}$$

Thus f is a group embedding.

□

Example 3.3.3. *A Type 3 embedding of* $C_3(20, 1, 4)$ *into* $\mathbb{Z}_{25}$.

The resultant of x^4+x+1 and $c_{20}(x)$ is 5, thus $C_3(20, 1, 4)$ is not amenable to Type 1 methods. So, we look for integers n such that $\lambda(n) = 20$. The resultant of $x^4 + x + 1$, and $x^{20} - 1$ is $825 = 3 \cdot 5^2 \cdot 11$. Notice that $\lambda(25) = 20$, $\lambda(55) = 20$, $\lambda(165) = 20$, $\lambda(275) = 20$, $\lambda(825) = 20$: any of these give an embedding. Since the order of 13 modulo 25 is 20, and $13^4 + 13 + 1 \equiv 0 \mod 25$ we have the following.

Theorem 3.3.4. $C_3(20, 1, 4)$ *is group embeddable.*

Proof. Define the map $f : C_3(20, 1, 4) \to \mathbb{Z}_{25}$ by

$$f : i \to 13^i \mod 25.$$

Since the order of 13 modulo 25 is 20 (i.e. 13 is a primitive root of 25), f is injective. Since $13^4 + 13 + 1 \equiv 0 \mod 25$, we have that for any j

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= 13^j + 13^{j+1} + 13^{j+4} \mod 25 \\ &= 13^j(1 + 13 + 13^4) \mod 25 \\ &\equiv 0 \mod 25. \end{aligned}$$

Thus f is a group embedding.

□

See Theorem 6.2.2 from the chapter on Infinitude of Geometric Realizations for a sweeping generalization: $C_3(4 \times 5^{n-1}, 1, 4)$ is group realizable for all $n \geq 2$.

Example 3.3.5. *A Type 4 embedding of* $C_3(15, 1, 4)$ *into* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

The resultant of $x^4 + x + 1$ and $c_{15}(x)$ is 16, and as 15 divides $2^4 - 1$ a candidate group for an embedding is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. To find the embedding matrix let $x^n = a_n x^3 + b_n x^2 + c_n x + d_n$, and $x^4 + x + 1 = 0$. Then upon reduction modulo $x^4 + x + 1$ we have that $x^{n+1} = b_n x^3 + c_n x^2 + (d_n - a_n)x - a_n$, from whence comes

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \\ d_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \\ c_n \\ d_n \end{pmatrix}.$$

Letting $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$, routine calculations establish that : the order of A modulo 2 is 15, and $A^0 + A + A^4 \equiv 0 \mod 2$.

The matrix A is a form for a companion matrix, and thus has $\lambda^4 + \lambda + 1$ as its characteristic polynomial. Hence by Cayley's theorem, the matrix A satisfies $A^4 + A + I = 0$.

Theorem 3.3.6. *$C_3(15, 1, 4)$ is group embeddable in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Let $\mathbf{x} = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^T$. Define the map $f : C_3(15, 1, 4) \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$f : i \to A^i \mathbf{x} \mod 2.$$

Since the order of A modulo 2 is 15, f is injective. Now we have that for any j

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= A^j + A^{j+1} + A^{j+4} \mod 2 \\ &= A^j(I + A + A^4) \mod 2 \\ &\equiv 0 \mod 2. \end{aligned}$$

Thus f is a group embedding.

□

The following table gives 68 group embeddings of cyclic configurations $C_3(n, 1, 4)$. Each Type 1 and Type 3 embedding is geometrically realizable in the real plane, since they are embeddings into a single cyclic group.

Table 3.2: $C_3(n, 1, 4)$ embeddings

$configuration$	$Type$	$Resultant$	$Group$	$base$
$\mathcal{C}_3(9, 1, 4)$	2	3^3	$\mathbb{Z}_{27}$	22
$\mathcal{C}_3(10, 1, 4)$	1	$3 \cdot 11$	$\mathbb{Z}_{11}$	7
$\mathcal{C}_3(11, 1, 4)$	1	$3 \cdot 23$	$\mathbb{Z}_{23}$	18
$\mathcal{C}_3(12, 1, 4)$	3	$3^2 \cdot 5$	$\mathbb{Z}_{45}$	13
$\mathcal{C}_3(13, 1, 4)$	2	3^4	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$*$
$\mathcal{C}_3(14, 1, 4)$	1	$3 \cdot 29$	$\mathbb{Z}_{29}$	4
$\mathcal{C}_3(15, 1, 4)$	2	$2^4 \cdot 3^2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$*$
$\mathcal{C}_3(16, 1, 4)$	1	$3 \cdot 5 \cdot 17$	$\mathbb{Z}_{17}$	3
$\mathcal{C}_3(17, 1, 4)$	1	$3 \cdot 103$	$\mathbb{Z}_{103}$	93
$\mathcal{C}_3(18, 1, 4)$	1	$3^3 \cdot 19$	$\mathbb{Z}_{19}$	2
$\mathcal{C}_3(19, 1, 4)$	3	$3 \cdot 191$	$\mathbb{Z}_{191}$	30
$\mathcal{C}_3(20, 1, 4)$	3	$3 \cdot 5^2 \cdot 11$	$\mathbb{Z}_{25}$	13
$\mathcal{C}_3(20, 1, 4)$	3	$3 \cdot 5^2 \cdot 11$	$\mathbb{Z}_{55}$	18
$\mathcal{C}_3(20, 1, 4)$	3	$3 \cdot 5^2 \cdot 11$	$\mathbb{Z}_{165}$	73
$\mathcal{C}_3(20, 1, 4)$	3	$3 \cdot 5^2 \cdot 11$	$\mathbb{Z}_{275}$	238
$\mathcal{C}_3(20, 1, 4)$	3	$3 \cdot 5^2 \cdot 11$	$\mathbb{Z}_{825}$	238
$\mathcal{C}_3(21, 1, 4)$	1	$3^2 \cdot 127$	$\mathbb{Z}_{127}$	50
$\mathcal{C}_3(22, 1, 4)$	1	$3 \cdot 23^2$	$\mathbb{Z}_{23}$	19
$\mathcal{C}_3(23, 1, 4)$	1	$3 \cdot 829$	$\mathbb{Z}_{829}$	817
$\mathcal{C}_3(24, 1, 4)$	1	$3^2 \cdot 5 \cdot 73$	$\mathbb{Z}_{73}$	7
$\mathcal{C}_3(25, 1, 4)$	1	$3 \cdot 1601$	$\mathbb{Z}_{1601}$	1104
$\mathcal{C}_3(26, 1, 4)$	1	$3^4 \cdot 79$	$\mathbb{Z}_{79}$	57
$\mathcal{C}_3(27, 1, 4)$	1	$3^4 \cdot 109$	$\mathbb{Z}_{109}$	73
$\mathcal{C}_3(28, 1, 4)$	1	$3 \cdot 5 \cdot 29^2$	$\mathbb{Z}_{29}$	21
$\mathcal{C}_3(29, 1, 4)$	1	$3 \cdot 5801$	$\mathbb{Z}_{5801}$	1125
$\mathcal{C}_3(30, 1, 4)$	3	$2^8 \cdot 3^2 \cdot 11$	$\mathbb{Z}_{99}$	40

$\mathcal{C}_3(31,1,4)$	1	$3 \cdot 11657$	$\mathbb{Z}_{11657}$	8788
$\mathcal{C}_3(32,1,4)$	1	$3 \cdot 5 \cdot 17 \cdot 193$	$\mathbb{Z}_{193}$	42
$\mathcal{C}_3(33,1,4)$	1	$3^2 \cdot 23 \cdot 331$	$\mathbb{Z}_{331}$	198
$\mathcal{C}_3(34,1,4)$	1	$3 \cdot 103 \cdot 307$	$\mathbb{Z}_{307}$	34
$\mathcal{C}_3(35,1,4)$	1	$3 \cdot 71 \cdot 631$	$\mathbb{Z}_{71}$	10
$\mathcal{C}_3(35,1,4)$	1	$3 \cdot 71 \cdot 631$	$\mathbb{Z}_{631}$	5
$\mathcal{C}_3(36,1,4)$	1	$3^3 \cdot 5 \cdot 19 \cdot 73$	$\mathbb{Z}_{73}$	35
$\mathcal{C}_3(37,1,4)$	1	$3 \cdot 149 \cdot 593$	$\mathbb{Z}_{149}$	63
$\mathcal{C}_3(37,1,4)$	1	$3 \cdot 149 \cdot 593$	$\mathbb{Z}_{593}$	225
$\mathcal{C}_3(38,1,4)$	1	$3 \cdot 191 \cdot 647$	$\mathbb{Z}_{647}$	446
$\mathcal{C}_3(39,1,4)$	1	$3^8 \cdot 79$	$\mathbb{Z}_{79}$	76
$\mathcal{C}_3(40,1,4)$	1	$3 \cdot 5^2 \cdot 11 \cdot 881$	$\mathbb{Z}_{881}$	462
$\mathcal{C}_3(41,1,4)$	1	$3 \cdot 337759$	$\mathbb{Z}_{337759}$	84193
$\mathcal{C}_3(42,1,4)$	1	$3^2 \cdot 29 \cdot 43 \cdot 127$	$\mathbb{Z}_{43}$	28
$\mathcal{C}_3(43,1,4)$	1	$3 \cdot 665039$	$\mathbb{Z}_{665039}$	198638
$\mathcal{C}_3(44,1,4)$	1	$3 \cdot 5 \cdot 23^2 \cdot 353$	$\mathbb{Z}_{353}$	135
$\mathcal{C}_3(45,1,4)$	1	$2^4 \cdot 3^3 \cdot 9091$	$\mathbb{Z}_{9091}$	4919
$\mathcal{C}_3(46,1,4)$	1	$3 \cdot 47^2 \cdot 829$	$\mathbb{Z}_{47}$	10
$\mathcal{C}_3(46,1,4)$	1	$3 \cdot 47^2 \cdot 829$	$\mathbb{Z}_{47}$	39
$\mathcal{C}_3(47,1,4)$	1	$3 \cdot 2567987$	$\mathbb{Z}_{2567987}$	1145617
$\mathcal{C}_3(48,1,4)$	1	$3^2 \cdot 5 \cdot 17 \cdot 73 \cdot 193$	$\mathbb{Z}_{193}$	48
$\mathcal{C}_3(49,1,4)$	1	$3 \cdot 197 \cdot 25579$	$\mathbb{Z}_{197}$	54
$\mathcal{C}_3(49,1,4)$	1	$3 \cdot 197 \cdot 25579$	$\mathbb{Z}_{25579}$	6251
$\mathcal{C}_3(50,1,4)$	1	$3 \cdot 11 \cdot 401 \cdot 1601$	$\mathbb{Z}_{401}$	145
$\mathcal{C}_3(51,1,4)$	1	$3^2 \cdot 103 \cdot 32029$	$\mathbb{Z}_{32029}$	612
$\mathcal{C}_3(52,1,4)$	1	$3^4 \cdot 5 \cdot 79 \cdot 1301$	$\mathbb{Z}_{1301}$	646
$\mathcal{C}_3(53,1,4)$	1	$3 \cdot 107^2 \cdot 1697$	$\mathbb{Z}_{107}$	27
$\mathcal{C}_3(53,1,4)$	1	$3 \cdot 107^2 \cdot 1697$	$\mathbb{Z}_{107}$	92
$\mathcal{C}_3(53,1,4)$	1	$3 \cdot 107^2 \cdot 1697$	$\mathbb{Z}_{1697}$	50
$\mathcal{C}_3(54,1,4)$	1	$3^4 \cdot 19 \cdot 109 \cdot 487$	$\mathbb{Z}_{487}$	343
$\mathcal{C}_3(55,1,4)$	1	$3 \cdot 23 \cdot 1658471$	$\mathbb{Z}_{1658471}$	454790
$\mathcal{C}_3(56,1,4)$	1	$3 \cdot 5 \cdot 29^2 \cdot 12713$	$\mathbb{Z}_{12713}$	12428
$\mathcal{C}_3(57,1,4)$	1	$3^2 \cdot 191 \cdot 229 \cdot 571$	$\mathbb{Z}_{571}$	339
$\mathcal{C}_3(58,1,4)$	1	$3 \cdot 5801 \cdot 18097$	$\mathbb{Z}_{18097}$	4438
$\mathcal{C}_3(59,1,4)$	1	$3 \cdot 147135617$	$\mathbb{Z}_{147135617}$	37283910

$\mathcal{C}_3(60,1,4)$	1	$2^{12}\cdot 3^2\cdot 5^2\cdot 11\cdot 61$	$\mathbb{Z}_{61}$	35
$\mathcal{C}_3(61,1,4)$	1	$3\cdot 35869\cdot 8053$	$\mathbb{Z}_{8053}$	5133
$\mathcal{C}_3(61,1,4)$	1	$3\cdot 35869\cdot 8053$	$\mathbb{Z}_{35869}$	35566
$\mathcal{C}_3(62,1,4)$	1	$3\cdot 11657\cdot 34721$	$\mathbb{Z}_{34721}$	28184
$\mathcal{C}_3(63,1,4)$	1	$3^3\cdot 127^2\cdot 3907$	$\mathbb{Z}_{127}$	13
$\mathcal{C}_3(63,1,4)$	1	$3^3\cdot 127^2\cdot 3907$	$\mathbb{Z}_{3907}$	1097
$\mathcal{C}_3(64,1,4)$	1	$3\cdot 5\cdot 17\cdot 193\cdot 48449$	$\mathbb{Z}_{48449}$	13276

In an analogous manner Algorithm 3.2.3 can be adapted to work for $C_3(n,1,4)$. Since the Singer polynomial in this case has degree 4, we generate three degree 3 polynomials, and solve the associated 3×3 system.

```
QEMT1s4 := proc(n::integer,s::polynom(integer,x))
     local c,p,q,r,M1,M2,M3,M,M_sol,t,b,d,T,k,i,a;
     c := x^n-1;
     p := rem(c, s, x);
     q := rem(x*p, s, x);
     r := rem((x^2)*p,s,x);
     M1 := Transpose(CoefficientVector(p, x, termorder = reverse));
     M2 := Transpose(CoefficientVector(q, x, termorder = reverse));
     M3 := Transpose(CoefficientVector(r, x, termorder = reverse));
     if degree(p) < 3 then
          p := x^3+p;
          M1 := Transpose(CoefficientVector(p, x, termorder = reverse));
          M1[1] := 0;
     end if;

     if degree(q) < 3 then
          q := x^3+q;
          M2 := Transpose(CoefficientVector(q, x, termorder = reverse));
          M2[1] := 0;
     end if;

     if degree(r) < 3 then
          r := x^3+r;
          M3 := Transpose(CoefficientVector(r, x, termorder = reverse));
          M3[1] := 0;
     end if;

     M := Matrix([[M1], [M2], [M3]]);
     M_sol := LinearSolve(M);
     t := -M_sol[3];
     b := -value(Eval(s, x = t));
     d := numer(b);
     T := factorset(d);
     k := numelems(T);
for i from 1 to k do
     if ((T[i]-1 mod n)=0) then
          a:=t mod T[i];
          if order(a,T[i])=n then
               print(n);
               print(a,T[i]);
          end if
     end if
end do
end proc;
```

Figure 3.2: The MAPLE code for Algorithm 2

3.4 An Infinite Class of $C_3(n, 1, 3)$'s

In this section we take a slightly different approach to finding group embeddings of cyclic configurations $C_3(n, 1, 3)$. Essentially, we work backwards from the Singer polynomial $\sigma(x) = x^3 + x + 1$, evaluate $\sigma(k)$, and look for primes p dividing $\sigma(k)$ from which we can construct group embeddings.

As an example, consider $\sigma(4) = 4^3 + 4 + 1 = 69$. A prime dividing 69 is 23, and the order of 4 modulo 23 is 11. Thus we can embed $C_3(11, 1, 3)$ into $\mathbb{Z}_{23}$.

Theorem 3.4.1. *$C_3(11, 1, 3)$ has a group realization in $\mathbb{Z}_{23}$.*

Proof.

Let $f : C_3(11, 1, 3) \to \mathbb{Z}_{23}$ be given by $f(i) = 4^i \mod 23$. Thus for any j we have

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= 4^j + 4^{j+1} + 4^{j+3} \mod 23 \\ &= 4^j(1 + 4 + 4^3) \mod 23 \\ &\equiv 0 \mod 23. \end{aligned}$$

That f is injective is obvious. Thus f is a group embedding.

□

The following table gives several examples of group embeddings using this new procedure.

Table 3.3: $C_3(n, 1, 3)$ embeddings supporting Theorem 3.4.2

k	$s(k)$	$Prime$	Order of p mod k	$Embedding$
2	11	11	10	$C_3(10, 1, 3) \to \mathbb{Z}_{11}$
3	31	31	30	$C_3(30, 1, 3) \to \mathbb{Z}_{31}$
4	69	23	11	$C_3(11, 1, 3) \to \mathbb{Z}_{23}$
5	131	131	65	$C_3(65, 1, 3) \to \mathbb{Z}_{131}$
6	223	223	222	$C_3(222, 1, 3 \to \mathbb{Z}_{223}$
7	351	13	12	$C_3(12, 1, 3) \to \mathbb{Z}_{13}$
8	521	521	260	$C_3(260, 1, 3) \to \mathbb{Z}_{521}$
9	739	739	369	$C_3(369, 1, 3) \to \mathbb{Z}_{739}$
10	1011	337	336	$C_3(336, 1, 3) \to \mathbb{Z}_{337}$
11	1343	17	16	$C_3(16, 1, 3) \to \mathbb{Z}_{17}$
11	1343	79	39	$C_3(39, 1, 3) \to \mathbb{Z}_{79}$
12	1741	1741	67	$C_3(67, 1, 3) \to \mathbb{Z}_{1741}$
13	2211	67	66	$C_3(66, 1, 3) \to \mathbb{Z}_{67}$
14	2759	31	15	$C_3(15, 1, 3) \to \mathbb{Z}_{31}$
14	2759	89	88	$C_3(88, 1, 3) \to \mathbb{Z}_{89}$
15	3391	3391	226	$C_3(226, 1, 3) \to \mathbb{Z}_{3391}$
16	4113	457	19	$C_3(19, 1, 3) \to \mathbb{Z}_{457}$
17	4931	4931	145	$C_3(145, 1, 3) \to \mathbb{Z}_{4931}$
18	5851	5851	5850	$C_3(5850, 1, 3) \to \mathbb{Z}_{5851}$
19	6879	2293	764	$C_3(764, 1, 3) \to \mathbb{Z}_{2293}$
20	8021	617	56	$C_3(56, 1, 3) \to \mathbb{Z}_{617}$
21	9283	9283	663	$C_3(663, 1, 3) \to \mathbb{Z}_{9283}$
22	10671	3557	508	$C_3(508, 1, 3) \to \mathbb{Z}_{3557}$
23	12191	73	36	$C_3(36, 1, 3) \to \mathbb{Z}_{73}$
23	12191	167	166	$C_3(166, 1, 3) \to \mathbb{Z}_{167}$
24	13849	1259	1258	$C_3(1258, 1, 3) \to \mathbb{Z}_{1259}$
25	15651	37	18	$C_3(18, 1, 3) \to \mathbb{Z}_{37}$
25	15651	47	23	$C_3(23, 1, 3) \to \mathbb{Z}_{47}$

The technique illustrated in the previous table provides the basis for the following result.

Theorem 3.4.2. *Let k be a positive integer and let p be a prime factor of the Singer polynomial $\sigma(x)$ evaluated at k. Let n be the order of k modulo p. Then the cyclic point line configuration $C_3(n, 1, 3)$ can be embedded in the group $\mathbb{Z}_p$ such that whenever $[P, Q, R]$ is a line in $C_3(n, 1, 3)$, then the sum of the images of P, Q, and R is zero in the group.*

Proof. Let the map $f : C_3(n, 1, 3) \to \mathbb{Z}_p$ be given by $f(i) = k^i \pmod p$. Then for any j we have

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= k^j + k^{j+1} + k^{j+3} \mod p \\ &= k^j(1 + k + k^3) \mod p \\ &\equiv 0 \mod p. \end{aligned}$$

Since the order of k modulo p is n, the mapping is injective. Hence f is a group embedding.

□

Corollary 3.4.2.1. *Since the groups realizing these cyclic configurations are all cyclic groups, these $C_3(n, 1, 3)$ configurations exist in the real plane as subgroups of the group of a non-singular cubic curve over the reals.*

Algorithm 3.4.3. *The Resultant Method Algorithm(n, σ) builds a cyclotomic polynomial of input degree n (or the polynomial $x^n - 1$) and takes the resultant of that with the input Singer polynomial $\sigma(x) = 1 + x^{d_1} + \cdots + x^{d_k}$. It outputs a list of pairs of integers, each pair consists of a group and a base for an embedding of $C_k(n, d_1, \ldots, d_k)$.*

$c_n(x) \leftarrow cyclotomic(n)$ (or $x^n - 1$)

1. $R \leftarrow |resultant(c_n(x), \sigma(x))|$

2. $T \leftarrow primefactorset(R)$

For every prime p in T

check for common roots r of $c_n(x)$ and $\sigma(x)$ mod p then if

(i) $\sigma(r) \equiv 0 \mod p$; and,

(ii) order of $r \mod p$ is n

return(group p and base r)

The following Figure 3.3 is the actual MAPLE code for Algorithm 3.4.3

```
ResultantMethod := proc(n::integer,s::polynom(integer,x))
     local c,R,T,k,i,j,a,b, prT;

#change c to cyclotomic if using cyclotomic polynomial.
c := cyclotomic(n, x);
#c := x^n -1 ;

R := abs(resultant(c, s, x));
T := factorset(R);
prT := ifactor(R);
k := numelems(T);
print();
print("n =",n);
print("Resultant =", R);
print("Resultant Factors =" , prT);
for i from 1 to k do
     a := Roots(c) mod T[i];
     b := Roots(s) mod T[i];
     for j from 1 to numelems(b) do
          if member(b[j],a) then
               if  ((value(Eval(s, x = b[j,1]))) mod T[i] = 0) then
                    if (order(b[j,1], T[i])=n) then
                         print("group, base: ",T[i], b[j,1]);
                    end if
               end if
          end if
     end do
end do
end proc;
```

Figure 3.3: The MAPLE code for Algorithm 3.4.3.

Chapter 4

Group Realizations of (n_4) Configurations

Thanks to the recent publication of Grünbaum's book [18], there has been a surge in the research on point-line configurations, especially those realizable over the real plane. While the number of configurations (n_4) is exponentially large, not all of them are realizable over the field of real numbers. See Grünbaum's paper entitled "Which (n_4)'s exist?" [17] for an interesting historical survey on this topic.

Given an abstract combinatorially defined point-block configuration, the basic questions are what do we mean by "exist" and how do we "realize" it. *The Book* deals with two kinds of realization: points are points in the real Euclidean (or projective) plane and the blocks are straight lines i.e. given by linear equations over the real field. This makes lot of sense because, after all

we live in this "real-world ($\mathbb{R} \times \mathbb{R} \times \mathbb{R}$)," and since geometric pictures drawn over the real plane provide valuable insight in solving problems, especially in guessing solutions. But there are many beautiful configurations which are not realizable in this sense. The second kind of realization arises by weakening the demand that the blocks may be represented by the so-called pseudolines (see *The Book*, page 21). These are the so-called topological realizations. Here again, there are some nice configurations which are not even topological. In a recent paper [2], Bokowski and Schewe have shown that there are no topologically realizable (15_4) or (16_4)-configurations. More recently, the same authors have proved that there is no geometric configuration (17_4) [3].

Now let us consider the cyclic (15_4) configuration defined by the cyclic base $(0, 1, 4, 6)$ i.e. the configuration $C_4(15, 1, 4, 6)$ in the notation of the Book (see page 60). Since this does not even have a topological realization, how do we perceive its existence? Can we draw it in the real plane in some *geometrically meaningful* way? In this chapter, we answer this question in the affirmative. After straight lines, we have conics and circles as perhaps the simplest examples of blocks. In section 4.2 we describe a new procedure to realize the cyclic $C_4(15, 1, 4, 6)$ as a configuration of points and circles in the real plane so that each block of 4 points lie on a circle in the Euclidean plane. It will be very clear that this technique will apply to many cyclic (n_4) configurations (see the Table 4.1 for a list of about 60 realizable (n_4)'s).

4.1 Cyclic (n_4)'s

Recall the definition of a *general cyclic configuration* given in [18]. A general cyclic configuration $\mathcal{C}_k(n, a_1, a_2, \ldots, a_{k-1})$ consists of $k-tuples$ $\{j, a_1 + j, a_2 + j, \ldots, a_{k-1} + j\}$, for given $a_1, a_2, \ldots, a_{k-1}$ with $0 < a_i < a_{i+1} < n$ and for all $1 \leq j \leq n$, all entries taken modulo n.

Theorem 4.1.1. *The cyclic configuration $\mathcal{C}_4(15, 1, 4, 6)$ has a group realization.*

Proof. The cyclic configuration $\mathcal{C}_4(15, 1, 4, 6)$ is given by the following fifteen quadruples.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
4	5	6	7	8	9	10	11	12	13	14	0	1	2	3
6	7	8	9	10	11	12	13	14	0	1	2	3	4	5

Since 10 is a root of $x^6 + x^4 + x + 1 \equiv 0 \mod 31$ and the order of 10 modulo 31 is 15, we define the mapping $f : \mathcal{C}_4(15, 1, 4, 6) \to \mathbb{Z}_{31}$ given by $f(i) = 10^i \mod 31$. The mapping is injective as can be seen from the following.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
10	7	8	18	25	2	20	14	16	5	19	4	9	28	1

To verify that f is indeed a group embedding, consider that $f(0) + f(1) + f(4) + f(6) = 1 + 10 + 18 + 2 \equiv 0 \mod 31$. More generally,

$$\begin{aligned} f(j) + f(j+1) + f(j+4) + f(j+6) &= 10^j + 10^{j+1} + 10^{j+4} + 10^{j+6} \\ &= 10^j(1 + 10 + 10^4 + 10^6) \\ &\equiv 10^j(1 + 10 + 18 + 2) \mod 31 \\ &\equiv 0 \mod 31. \end{aligned}$$

□

Using the same resultant technique appropriate groups and exponential maps are found to give the group realizations listed in Table 4.1.

Table 4.1: Cyclic (n_4) embeddings

$configuration$	$Group$	$base$
$\mathcal{C}_4(14,1,3,9)$	$\mathbb{Z}_{43}$	32
$\mathcal{C}_4(15,1,4,6)$	$\mathbb{Z}_{31}$	10
$\mathcal{C}_4(16,1,4,6)$	$\mathbb{Z}_{97}$	85
$\mathcal{C}_4(17,1,4,6)$	$\mathbb{Z}_{1327}$	1147
$\mathcal{C}_4(18,1,4,6)$	$\mathbb{Z}_{37}$	3
$\mathcal{C}_4(19,1,4,6)$	$\mathbb{Z}_{2927}$	1527
$\mathcal{C}_4(20,1,4,6)$	$\mathbb{Z}_{241}$	6
$\mathcal{C}_4(21,1,4,6)$	$\mathbb{Z}_{883}$	838
$\mathcal{C}_4(22,1,4,6)$	$\mathbb{Z}_{331}$	257
$\mathcal{C}_4(23,1,4,6)$	$\mathbb{Z}_{102397}$	41349
$\mathcal{C}_4(24,1,4,6)$	$\mathbb{Z}_{73}$	17
$\mathcal{C}_4(25,1,4,6)$	$\mathbb{Z}_{16451}$	7166
$\mathcal{C}_4(26,1,4,6)$	$\mathbb{Z}_{131}$	86
$\mathcal{C}_4(27,1,4,6)$	$\mathbb{Z}_{109}$	88
$\mathcal{C}_4(27,1,4,6)$	$\mathbb{Z}_{541}$	449
$\mathcal{C}_4(28,1,4,6)$	$\mathbb{Z}_{29}$	8
$\mathcal{C}_4(29,1,4,6)$	$\mathbb{Z}_{233}$	38
$\mathcal{C}_4(29,1,4,6)$	$\mathbb{Z}_{5279}$	1922
$\mathcal{C}_4(30,1,4,6)$	$\mathbb{Z}_{271}$	19
$\mathcal{C}_4(31,1,4,6)$	$\mathbb{Z}_{683}$	646
$\mathcal{C}_4(31,1,4,6)$	$\mathbb{Z}_{8929}$	6290
$\mathcal{C}_4(32,1,4,6)$	$\mathbb{Z}_{3457}$	1784
$\mathcal{C}_4(33,1,4,6)$	$\mathbb{Z}_{45541}$	28105
$\mathcal{C}_4(34,1,4,6)$	$\mathbb{Z}_{8161}$	8078
$\mathcal{C}_4(35,1,4,6)$	$\mathbb{Z}_{211}$	25
$\mathcal{C}_4(35,1,4,6)$	$\mathbb{Z}_{1471}$	128
$\mathcal{C}_4(36,1,4,6)$	$\mathbb{Z}_{37}$	18
$\mathcal{C}_4(36,1,4,6)$	$\mathbb{Z}_{109}$	17
$\mathcal{C}_4(37,1,4,6)$	$\mathbb{Z}_{149}$	127
$\mathcal{C}_4(37,1,4,6)$	$\mathbb{Z}_{467977}$	420663
$\mathcal{C}_4(38,1,4,6)$	$\mathbb{Z}_{26107}$	894
$\mathcal{C}_4(39,1,4,6)$	$\mathbb{Z}_{157}$	37

$\mathcal{C}_4(40,1,4,6)$	$\mathbb{Z}_{41}$	13
$\mathcal{C}_4(40,1,4,6)$	$\mathbb{Z}_{761}$	208
$\mathcal{C}_4(41,1,4,6)$	$\mathbb{Z}_{22469}$	2328
$\mathcal{C}_4(41,1,4,6)$	$\mathbb{Z}_{51907}$	2056
$\mathcal{C}_4(42,1,4,6)$	$\mathbb{Z}_{127}$	5
$\mathcal{C}_4(43,1,4,6)$	$\mathbb{Z}_{32423}$	3357
$\mathcal{C}_4(43,1,4,6)$	$\mathbb{Z}_{81701}$	1770
$\mathcal{C}_4(44,1,4,6)$	$\mathbb{Z}_{89}$	36
$\mathcal{C}_4(44,1,4,6)$	$\mathbb{Z}_{353}$	232
$\mathcal{C}_4(45,1,4,6)$	$\mathbb{Z}_{271}$	72
$\mathcal{C}_4(45,1,4,6)$	$\mathbb{Z}_{15031}$	621
$\mathcal{C}_4(46,1,4,6)$	$\mathbb{Z}_{47}$	30
$\mathcal{C}_4(46,1,4,6)$	$\mathbb{Z}_{1013}$	757
$\mathcal{C}_4(47,1,4,6)$	$\mathbb{Z}_{19343925737}$	16337885332
$\mathcal{C}_4(48,1,4,6)$	$\mathbb{Z}_{337}$	153
$\mathcal{C}_4(49,1,4,6)$	$\mathbb{Z}_{491}$	164
$\mathcal{C}_4(49,1,4,6)$	$\mathbb{Z}_{19047673}$	11939844
$\mathcal{C}_4(50,1,4,6)$	$\mathbb{Z}_{251}$	151
$\mathcal{C}_4(50,1,4,6)$	$\mathbb{Z}_{1451}$	626
$\mathcal{C}_4(51,1,4,6)$	$\mathbb{Z}_{40258483}$	28276203
$\mathcal{C}_4(52,1,4,6)$	$\mathbb{Z}_{53}$	31
$\mathcal{C}_4(52,1,4,6)$	$\mathbb{Z}_{16069}$	12813
$\mathcal{C}_4(53,1,4,6)$	$\mathbb{Z}_{1697}$	304
$\mathcal{C}_4(53,1,4,6)$	$\mathbb{Z}_{286559447}$	174921346
$\mathcal{C}_4(54,1,4,6)$	$\mathbb{Z}_{10909}$	2209
$\mathcal{C}_4(55,1,4,6)$	$\mathbb{Z}_{121868891}$	110366746
$\mathcal{C}_4(56,1,4,6)$	$\mathbb{Z}_{113}$	13
$\mathcal{C}_4(56,1,4,6)$	$\mathbb{Z}_{2857}$	2573
$\mathcal{C}_4(57,1,4,6)$	$\mathbb{Z}_{571}$	464
$\mathcal{C}_4(57,1,4,6)$	$\mathbb{Z}_{702469}$	310740
$\mathcal{C}_4(58,1,4,6)$	$\mathbb{Z}_{59}$	32
$\mathcal{C}_4(58,1,4,6)$	$\mathbb{Z}_{60089}$	12688
$\mathcal{C}_4(59,1,4,6)$	$\mathbb{Z}_{1092209}$	1046041
$\mathcal{C}_4(59,1,4,6)$	$\mathbb{Z}_{14017693}$	5835262
$\mathcal{C}_4(60,1,4,6)$	$\mathbb{Z}_{4441}$	3516

$\mathcal{C}_4(61,1,4,6)$	$\mathbb{Z}_{40047602642833}$	2814268316620
$\mathcal{C}_4(62,1,4,6)$	$\mathbb{Z}_{311}$	87
$\mathcal{C}_4(62,1,4,6)$	$\mathbb{Z}_{16493}$	4978
$\mathcal{C}_4(63,1,4,6)$	$\mathbb{Z}_{631}$	143
$\mathcal{C}_4(63,1,4,6)$	$\mathbb{Z}_{5647951}$	3145909
$\mathcal{C}_4(64,1,4,6)$	$\mathbb{Z}_{8019073}$	1449474
$\mathcal{C}_4(65,1,4,6)$	$\mathbb{Z}_{131}$	13
$\mathcal{C}_4(65,1,4,6)$	$\mathbb{Z}_{10531}$	7596
$\mathcal{C}_4(65,1,4,6)$	$\mathbb{Z}_{28081}$	5850

4.2 Geometric Realizations of (n_4) Configurations

Now that we have group realizations of several (n_4) configurations, it is natural to ask whether they can be used to represent the configurations in the real plane where the points are still the usual points and the blocks are algebraic curves of some constant degree. In the case of (n_3) configurations, the blocks of size three are straight lines. The group embeddings of (n_3) configurations are motivated by the group law on a cubic. For (n_4) configurations we take our inspiration from the geometrically defined group law on a non-circular conic, see [14], [25]. With the embeddings given in Table 4.1 to guide us, here we show that the $C_4(n,1,4,6)$ having an embedding into a single cyclic group can be realized over the real plane where the points lie on a non-circular conic, and the blocks of size four are circles. In [14], R.R. Fletcher provides a natural way to realize our group embeddings in the real plane: it is demonstrated that every cyclic group $\mathbb{Z}_n$ can be found on

non-circular conics such that four points are concyclic if and only if their group-sum is zero in $\mathbb{Z}_n$.

Figure 4.1 illustrates the group law on a non-circular ellipse. The group law on a non-circular ellipse $\mathcal{C}$ defined over a field $\mathbb{F}$ is quite simple: fix any point O on $\mathcal{C}$; to find the sum of two rational points P, Q, draw the line through O parallel to PQ , and denote its second point of intersection with $\mathcal{C}$ by $P + Q$. Four points P, Q, R, and S are "collinear" if and only if $P + Q + R + S = 0$ under the group law on the conic.

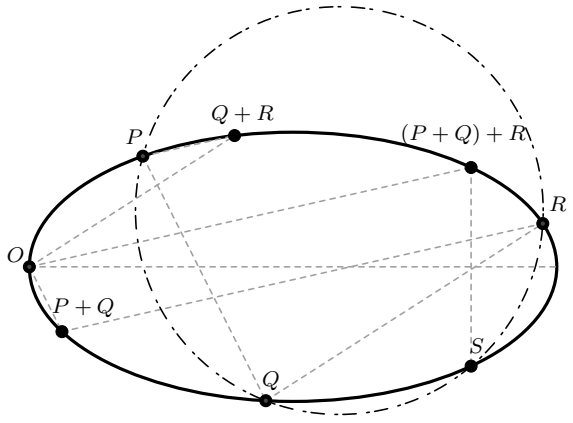

Figure 4.1: Group Law on a non-circular ellipse.

In light of the previous notions, we offer the following new concept of realizability. An (n_4) configuration shall be called *circle-realizable* over the real plane if the points of the configuration are the usual real coordinates, and the blocks of four points have corresponding coordinates which lie on a real circle.

4.2.1 A Circle Realization of $C_4(28, 1, 4, 6)$

Since the resultant of $x^6 + x^4 + x + 1$ and the 28^{th} cyclotomic polynomial is $232 = 2^3 \cdot 29$; $8^6 + 8^4 + 8 + 1 \equiv 0 \mod 29$, and 8 is a primitive root of 29 we get the following embedding. $f : C_4(28, 1, 4, 6) \to \mathbb{Z}_{29}$ where

$$f : i \to 8^i \mod 29.$$

The embedding is given explicitly in Table 4.2: the images are the nonzero elements of the copy of $\mathbb{Z}_{29}$ on the conic in Figure 4.2.

Table 4.2: A group embedding of $C_4(28, 1, 4, 6)$

$f(0) = 1$	$f(6) = 13$	$f(12) = 24$	$f(18) = 22$	$f(24) = 25$
$f(1) = 8$	$f(7) = 17$	$f(13) = 18$	$f(19) = 2$	$f(25) = 26$
$f(2) = 6$	$f(8) = 20$	$f(14) = 28$	$f(20) = 16$	$f(26) = 5$
$f(3) = 19$	$f(9) = 15$	$f(15) = 21$	$f(21) = 12$	$f(27) = 11$
$f(4) = 7$	$f(10) = 4$	$f(16) = 23$	$f(22) = 9$	$f(28) = 1$
$f(5) = 27$	$f(11) = 3$	$f(17) = 10$	$f(23) = 14$	

Indeed, $f(i) + f(i + 1) + f(i + 4) + f(i + 6) = 8^i(1 + 8 + 7 + 13) \equiv 0 \mod 29$, thus we have a group embedding of $C_4(28, 1, 4, 6)$ into $\mathbb{Z}_{29}$. The results of [14] give that the images of our blocks are concyclic, hence we have a geometric realization of $C_4(28, 1, 4, 6)$ in the real plane.

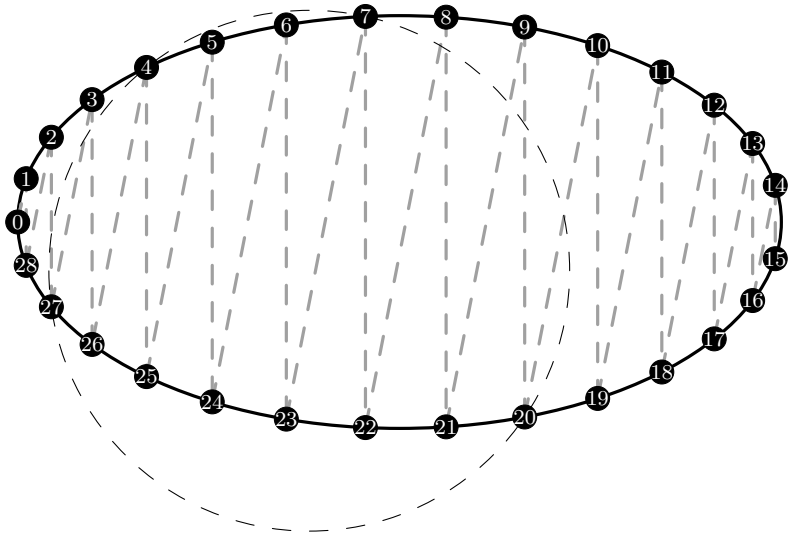

Figure 4.2: The circle through the points $4, 7, 20$, and 27 of the conic correspond to the block$\{4, 5, 8, 10\}$ of the cyclic configuration. Notice that $4 + 7 + 20 + 27 \equiv 0 \mod 29$

4.2.2 A Circle Realization of $C_4(15, 1, 4, 6)$

As promised in the introduction, the following is a group embedding of $C_4(15, 1, 4, 6)$ which implies the circle realizability of the (n_4) configuration.

Theorem 4.2.1. *The cyclic configuration $C_4(15, 1, 4, 6)$ has a group realization in $\mathbb{Z}_{31}$.*

Proof. *Let* $f : C_4(15, 1, 4, 6) \to \mathbb{Z}_{31}$ be given by $f(i) = 10^i \mod 31$. Consider that $f(0) + f(1) + f(4) + f(6) = 1 + 10 + 18 + 2 \equiv 0 \mod 31$. In general, we have

$$\begin{aligned} f(j) + f(j+1) + f(j+4) + f(j+6) &= 10^j + 10^{j+1} + 10^{j+4} + 10^{j+6} \\ &= 10^j(1 + 10 + 10^4 + 10^6) \\ &\equiv 10^j(1 + 10 + 18 + 2) \mod 31 \\ &\equiv 0 \mod 31. \end{aligned}$$

□

Corollary 4.2.1.1. *$C_4(15, 1, 4, 6)$ is circle realizable.*

The following figure illustrates the mapping from $C_4(15, 1, 4, 6)$ to the real plane and the associated circle realization.

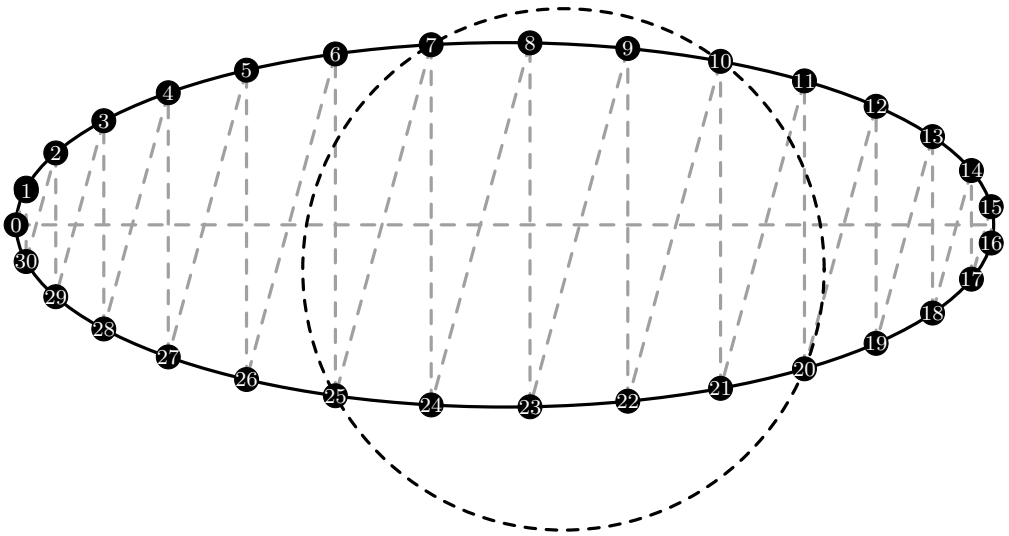

Figure 4.3: A circular realization of $C_4(15, 1, 4, 6)$ in the group $\mathbb{Z}_{31}$, where [1,2,5,7] are concyclic.

4.3 The Status of $(n_4)'s$ with $13 \leq n \leq 19$

The following table summarizes the status of the realizability of (n_4) configurations with $13 \leq n \leq 19$.

Table 4.3: The status of $(n_4)'s$ with $13 \leq n \leq 19$

n	Geometric(lines)	Topological	Group	Geometric(circles)
13	No	No	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$PG(2,3)$
14	No	No	$\mathbb{Z}_{43}$	$\mathbb{Z}_{43}$
15	No	No	$\mathbb{Z}_{31}$	$\mathbb{Z}_{31}$
16	No	No	$\mathbb{Z}_{97}$	$\mathbb{Z}_{97}$
17	No	Yes	$\mathbb{Z}_{1327}$	$\mathbb{Z}_{1327}$
18	Yes	Yes	$\mathbb{Z}_{37}$	$\mathbb{Z}_{37}$
19	?	Yes	$\mathbb{Z}_{2927}$	$\mathbb{Z}_{2927}$

In [28] Merlin shows that there exist no geometric (lines) (n_4) configurations for $n \leq 15$. In [3], and [2] Bokoski, and Schewe show that there are no geometric realizations of (n_4) configurations for $n \leq 17$, and that there are no topological realizations of (n_4) configurations for $n \leq 16$.

From our point of view, the first four cases (i.e, $n = 14, 15, 16$, and 17) are interesting. While none of these have geometric realizations in the classical sense, we show that they are all geometric in the new sense. That is to say, that blocks of four points in the configuration are concyclic in the real plane with respect to the group law on the non-circular ellipse. (We have shown the case where $n = 15$ in the previous section 4.2.2.)

Since $C_4(14, 1, 4, 6)$ is not amenable to our technique of embedding, as the resultant fails to give useful primes, we give instead a group embedding

of $C_4(14, 1, 3, 9)$. The embedding of $C_4(14, 1, 3, 9)$ in turn implies the circle realization of an (n_4).

Theorem 4.3.1. *The cyclic configuration $C_4(14, 1, 3, 9)$ has a group realization in $\mathbb{Z}_{43}$.*

Proof. Let $f : C_4(14, 1, 3, 9) \to \mathbb{Z}_{43}$ be given by $f(i) = 32^i \mod 43$. Consider that $f(0) + f(1) + f(3) + f(9) = 1 + 32 + 2 + 8 \equiv 0 \mod 43$. In general, we have

$$\begin{aligned} f(j) + f(j+1) + f(j+3) + f(j+9) &= 32^j + 32^{j+1} + 32^{j+3} + 32^{j+9} \\ &= 32^j(1 + 32 + 32^3 + 32^9) \\ &\equiv 32^j(1 + 32 + 2 + 8) \mod 43 \\ &\equiv 0 \mod 43. \end{aligned}$$

□

Corollary 4.3.1.1. *$C_4(14, 1, 3, 9)$ is circle-realizable.*

The paper of Bokowski and Schewe [3] establishes the existence of geometric (lines) realizations of (n_4) configurations for all $n \geq 18$, except possibly for $n = 19, 22, 23, 26, 37$, and 43. The results of this section demonstrate the existence of circle realizations for all unknown values in [3] (see Table 5.1). We conclude this section with the following conjecture.

Conjecture 4.3.2. *For $n \geq 15$, $C_4(n, 1, 4, 6)$ is group realizable in a single cyclic group, and hence is circle realizable.*

4.4 PG(2,3)

The $PG(2,3)$-the projective plane of order 3 is perhaps the most well-known (n_4) configuration. It is folklore that if $PG(2,2)$ exists in $PG(2,k)$ for some field $GF(k)$, then $2 = 0$ in $GF(k)$, see [26] or [34]. In this section we prove an analogous result for $PG(2,3)$. In addition we provide a group realization of $PG(2,3)$ into $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ that is minimal with respect to group size and exponent.

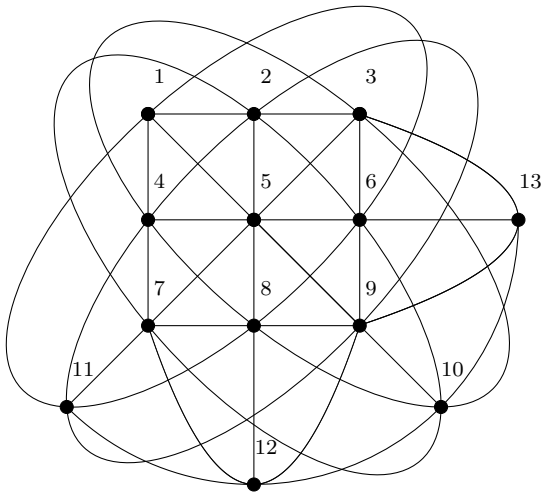

Figure 4.4: $PG(2,3)$

Theorem 4.4.1. *If $PG(2,3)$ exists in $PG(2,k)$ for some field $GF(k)$, then $3 = 0$ in $GF(k)$.*

Proof. The proof is analytical and uses homogeneous coordinates in the projective plane. Without loss of generality, assign homogeneous coordinates

to the frame formed by the points 1, 3, 7, and 9 of figure 4.4: $1 \to (1,0,0)$, $3 \to (0,1,0)$, $7 \to (1,1,1)$,and $9 \to (0,0,1)$.

The line formed by points 1 and 9 is given by $1 \vee 9$ and is simply the cross product of of the coordinates assigned to the points 1 and 9. $1 \vee 9 = (1,0,0) \times (0,0,1) = [0,1,0]$. Similarly, $3 \vee 7 = [1,0,-1]$, and point 5 is defined as the intersection of the lines $1 \vee 9$ and $3 \vee 7$ which is again computed using a simple cross product. We get that $5 \to (1,0,1)$. To assign a coordinate to point 11 on line $\{3,5,7,11\}$ we assign it the general coordinates (a,b,c) and observe that the following equation must be satisfied.

$$\begin{aligned} 0 &= \begin{vmatrix} a & b & c \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} \\ &= a - c \end{aligned}$$

Therefore we can assign $11 \to (1,a,1)$.

Through a similar series of calculations it is found that $1 \vee 3 = [0,0,1]$, and $7 \vee 9 = [1,-1,0]$, and since $13 = (1 \vee 3) \wedge (7 \vee 9)$, we assign $13 \to (1,1,0)$. Similarly, $12 \to (0,1,1)$. The line $\{10,11,12,13\}$ must satisfy the following equation.

$$0 = \begin{vmatrix} 1 & a & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{vmatrix}$$
$$= a - 2$$

This allows us to assign $11 \to (1, 2, 1)$.

Through more of the same calculations we see that $10 = (11 \vee 12) \wedge (1 \vee 9)$ so we assign $10 \to (1, 0, -1)$. Also $4 = (1 \vee 7) \wedge (5 \vee 13)$, so that $4 \to (2, 1, 1)$. Now, the line $\{2, 4, 9, 11\}$ must satisfy the following the equation.

$$0 = \begin{vmatrix} 0 & 0 & 1 \\ 2 & 1 & 1 \\ 1 & 2 & 1 \end{vmatrix}$$
$$= 3$$

□

We conclude this section with another parallel folklore result on the group realizability of $PG(2, 3)$. See [12] for a Prover 9 procedure for embedding $PG(2, 3)$ into a group. The projective plane $PG(2, 3)$ can be described as the cyclic difference set $\{0, 1, 4, 6\} \mod 13$ or $C_4(13, 1, 4, 6)$ in the notation of Grünbaum. Conspicuously absent from Table 4.1 is an embedding of $C_4(13, 1, 4, 6)$ into a single cyclic group. Since the resultant of the Singer polynomial $\sigma(x) = x^6 + x^4 + x + 1$, and the thirteenth cyclotomic polynomial $c_{13}(x)$ is $729 = 3^6$, embedding into a single cyclic group is not possible with

our basic Type resultant technique. However, provided that $\sigma(x)$ has an irreducible cubic $\mod 3$, it may be possible to embed $C_4(13,1,4,6)$ into the multiplicative group of $GF(27)$ (i.e. a Type 2 or 4 embedding). To this end, notice that

$$x^6 + x^4 + x + 1 = (x^3 + x^2 + 1)(x^3 + 2x^2 + 2x + 2) \mod 3$$

We will use $x^3 = x^2 + x + 1$ to describe $x^n = a_n x^2 + b_n x + c_n$, and derive an embedding matrix. We have that

$$\begin{aligned} x^{n+1} &= a_n x^3 + b_n x^2 + c_n x \\ &= a_n(x^2 + x + 1) + b_n x^2 + c_n x \\ &= (a_n + b_n)x^2 + (a_n + c_n)x + a_n \\ &= a_{n+1}x^2 + b_{n+1}x + c_{n+1} \end{aligned}$$

from which comes,

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}$$

Define the map $f : C_3(13,1,4,6) \to \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ by $f(i) = A^i \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

mod 3, where $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Then,

$$\begin{aligned} f(0)+f(1)+f(4)+f(6) &= (I+A+A^4+A^6)\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 7 & 4 & 2 \\ 6 & 3 & 2 \\ 4 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 24 & 13 & 7 \\ 20 & 11 & 6 \\ 13 & 7 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 33 & 18 & 9 \\ 27 & 15 & 9 \\ 18 & 9 & 6 \end{pmatrix} \\ &\equiv 0 \mod 3. \end{aligned}$$

More generally,

$$\begin{aligned} f(j)+f(j+1)+f(j+4)+f(j+6) &= A^j(I+A+A^4+A^6)\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \\ &\equiv 0 \mod 3. \end{aligned}$$

Showing that f is injective is routine (the order of A modulo 3 is 13), hence f is a group embedding of $C_3(13, 1, 4, 6)$ into $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

With Lemma 4.4.2 we have have established Theorem 4.4.3.

Lemma 4.4.2. *Any group embedding of $PG(2, 3)$ has at least 13 elements of order 3.*

Theorem 4.4.3. *$PG(2, 3)$ is minimally group realizable in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.*

4.5 Applications to Some Exercises of Grünbaum

In this section we use several of the algebraic techniques we have already developed to address a few miscellaneous questions relating to (n_4) configurations.

Problem 3 on page 161 of [18] asks the reader to show that the cyclic configurations $C_4(15, 1, 4, 6)$, and $C_4(15, 2, 8, 12)$ are isomorphic; $C_4(15, 1, 5, 7)$ and $C_4(15, 1, 9, 11)$ are isomorphic, and $C_4(15, 1, 3, 7)$ and $C_4(15, 1, 9, 13)$ are isomorphic.

To establish the first isomorphism, consider that $C_4(15, 1, 4, 6)$ can be embedded in $\mathbb{Z}_{31}$ according to $f(i) = 10^i \mod 31$. Now, as with $C_4(15, 1, 4, 6)$ the resultant of the fifteenth cyclotomic polynomial,$c_{15}(x)$ and $\sigma(x) = x^{12} + x^8 + x^2 + 1$ is 31. A common solution to $c_{15}(x)$ and $\sigma(x)$ is 14. Thus $C_4(15, 2, 8, 12)$ can be embedded in $\mathbb{Z}_{31}$ according to $f(i) = 14^i \mod 31$.

Table 4.4: Isomorphism calculations

$C_4(15,1,4,6)$	$10^i \mod 31$	$C_4(15,2,8,12)$	$14^i \mod 31$
0	1	0	1
1	10	2	10
2	7	4	7
3	8	6	8
4	18	8	18
5	25	10	25
6	2	12	2
7	20	14	20
8	14	1	14
9	16	3	16
10	5	5	5
11	19	7	19
12	4	9	4
13	9	11	9
14	28	13	28

With the aid of Table 4.4 we can construct the explicit isomorphism $f : C_4(15,1,4,6) \to C_4(15,2,8,12)$ it is given by $f : i \to 2i \mod 15$.

To establish that $C_4(15,1,5,7)$ and $C_4(15,1,9,11)$ are isomorphic, compare the block $[0,1,5,7]$ in $C_4(15,1,5,7)$ to the four blocks in $C_4(15,1,9,11)$ which contain the point 0. We see that $(0,1,5,7)$ is a multiple of $(0,4,5,13)$ mod 15. In particular $4(0,1,5,7) = (0,4,5,13) \mod 15$, from which we obtain the isomorphism $f : C_4(15,1,4,6) \to C_4(15,1,5,7)$ given by $f : i \to 4i$ mod 15. Similarly, we can show that the mapping $f : i \to 7i \mod 15$ induces an isomorphism from $C_4(15,1,3,7)$ to $C_4(15,1,9,13)$.

Chapter 5

The Möbius-Kantor Configuration

5.1 Introduction

The Möbius-Kantor configuration is the unique (8_3) configuration. Combinatorially, one can view the (8_3) as the deletion of the $AG(2,3)$ i.e., the (8_3) is obtained from the $AG(2,3)$ by deleting a single point and the four lines incident with that point, see [20]. Like the $AG(2,3)$, the Möbius-Kantor configuration violates the Sylvester-Gallai Theorem and hence is not realizable in the real plane.

From the point of view of group realization the (8_3) is a more fundamental structure than the $AG(2,3)$. Indeed the (8_3) proves to be an "extendable" structure in $\mathbb{Z}_3^n \times \mathbb{Z}_3^n$(see 5.4 and 5.5).

5.2 Field Embedding Through Parameterization

In this section we will demonstrate a coordinatization of (8_3) in $PG(2,k)$, and describe the fields $\mathbb{F}_k$ in which this is possible. The technique used is well-known, and colloquially referred to as "coordinate chasing."

To begin select a frame, that is to say four points no three of which are collinear; and, WLOG assign them the homogeneous coordinates $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, and $(1,1,1)$. With respect to Figure 5.1, $7 \to (1,0,0)$, $6 \to (0,1,0)$, $4 \to (0,0,1)$, and $5 \to (1,1,1)$. We get the updated diagram:

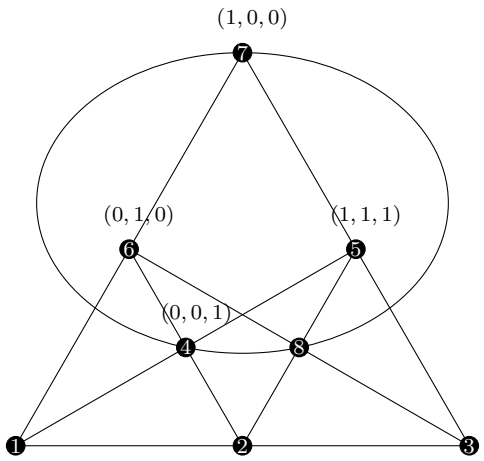

Figure 5.1: Coordinate chase STEP 1

Point 3 is assigned a homogeneous coordinate by observing that $5 \vee 7$ can be described by the homogeneous line given by the cross product $(1,0,0) \times (1,1,1)$, giving $5 \vee 7 \to [0,-1,1]$. Any point on $[0,-1,1]$ satisfies $0 =$

$[0, -1, 1] \cdot (a, b, c)$, implying $b = c$, giving $(a, 1, 1)$ as the coordinate to assign to 3. We get the updated diagram:

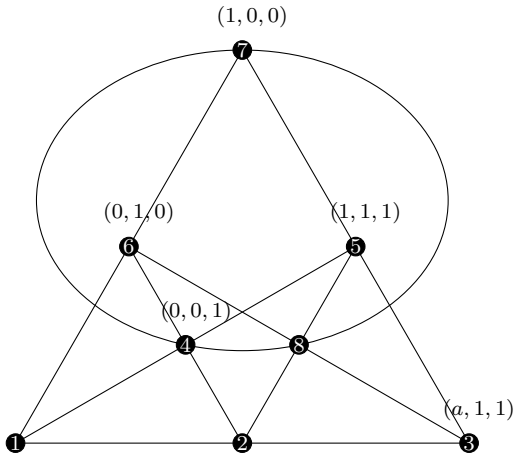

Figure 5.2: Coordinate chase STEP 2

To give the point 8 a coordinate, define it as $(6 \vee 3) \wedge (7 \vee 4)$. The line $7 \vee 4$ is described by the homogeneous line $(1, 0, 0) \times (0, 0, 1) = [0, 1, 0]$, and $6 \vee 3$ by $(0, 1, 0) \times (a, 1, 1) = [1, 0, -a]$.

Now, $[0,1,0]\times[a,1,1] = (a,0,1)$, giving $8 \to (a,0,1)$. We get the updated diagram:

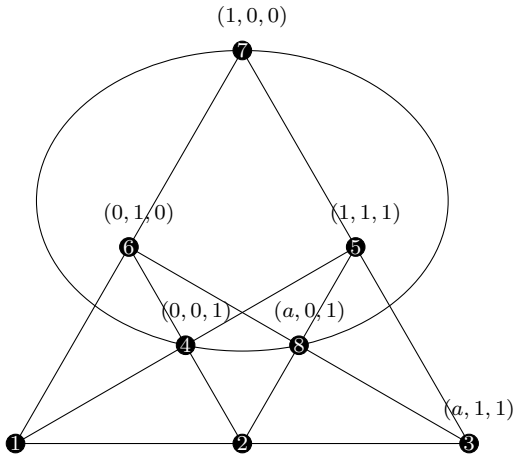

Figure 5.3: Coordinate chase STEP 3

Next we assign 2 a coordinate by defining $2 = (6 \vee 4) \wedge (5 \vee 8)$. The line $6 \vee 4$ is given by the homogeneous line $(0,1,0) \times (0,0,1) = [1,0,0]$, and the line $5 \vee 8$ by the homogeneous line $(1,1,1) \times (a,0,1) = [1, a-1, a]$. Now, $[1,0,0] \times [1, a-1, a] = (0, a, a-1)$, and so $2 \to (0, a, a-1)$. We get the updated diagram:

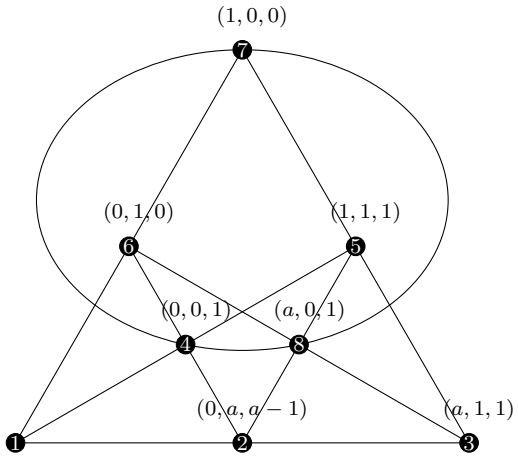

Figure 5.4: Coordinate chase STEP 4

Next, define the point $1 = (6 \vee 7) \wedge (4 \vee 5)$. Describe $4 \vee 5$ by the homogeneous line $(0,0,1) \times (1,1,1) = [1,-1,0]$, and $6 \vee 7$ by the homogeneous line $(1,0,0) \times (0,1,0) = [0,0,1]$. This gives $[1,-1,0] \times [0,0,1] = (1,1,0)$, and we map $1 \to (1,1,0)$. We get the updated diagram:

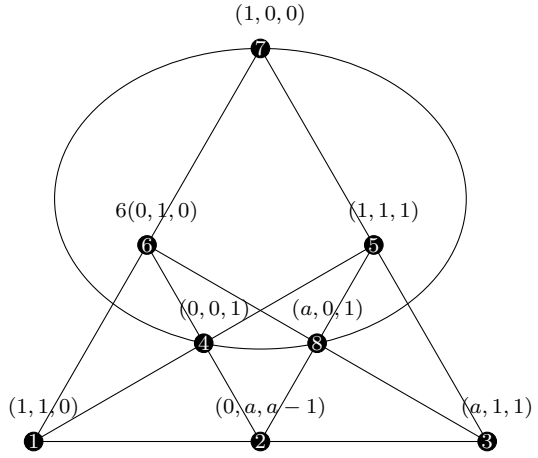

Figure 5.5: Coordinate chase STEP 5

Now for the points on the line $\{1, 2, 3\}$ to be collinear we must have $det((1, 1, 0), (0, a, a-1)(a, 1, 1)) = 0$. This implies that $a^2 - a + 1 = 0$, giving $a = \frac{1}{2}(1 \pm \sqrt{-3})$. So provided that $\sqrt{-3}$ exists in the coordinatizing field, a will exist. The finite fields $GF(7)$, $GF(13)$, and $GF(19)$ all provide examples of fields which give a coordinatization. In the next section we provide group realizations for the Möbius-Kantor configuration in both $GF(7)$, and $GF(13)$.

5.3 Group Realizations Using Cubic Curves

5.3.1 The Möbius-Kantor Configuration in the Affine Plane $AG(2, 7)$

The group realization provided in what follows isn't direct like the field plane coordinatization provided in section 5.1. Instead, we appeal to a result of Jungnickel et. al [20], after we have provided a group realization of $AG(2, 3)$ as the nine inflection points of a cubic curve over a finite field.

A suitable cubic curve is found by examining solutions to the cubic equation $y^2 = x^3 + c$ over the finite field $GF(7)$. Since the field has only seven elements, the calculations are still manageable by hand.

By inspecting the fourth row of Table 5.1. and observing the squares modulo 7, it is found that $(0, 3), (0, 4), (3, 1), (3, 6), (5, 1), (5, 6), (6, 1)$, and $(6, 6)$ are all solutions to the cubic $y = x^3 + 2$ over $GF(7)$. By append-

Table 5.1: Solutions to $y = x^3 + 2$ in $GF(7)$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
$x^3 + 2$	2	3	3	1	3	1	1

ing an additional 'point at infinity' denoted $\mathcal{O}$, a set of nine points given by $C(GF(7)) = \{\mathcal{O}, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$ is obtained. The set $C(GF(7))$, together with the addition law on cubic curves, forms an abelian group of order 9. Thus there are two possible groups, namely $\mathbb{Z}_9$, and $\mathbb{Z}_3 \times \mathbb{Z}_3$. To distinguish these, we construct a group table. We will use the following equations found in [31] pages 31, and 107-108 for the cubic in normal form $y^2 = x^3 + ax^2 + bx + c$.

The x-coordinate of $2(x, y)$ is given by the following, called the duplication formula:

$$x\text{-coordinate of } 2(x,y) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

The formula above is particularly useful. For a curve in normal form along with the points P, and Q, one obtains $P + Q$ from $P * Q$ by reflecting in the x-axis.

The slope of the line between the two points $P_1 = (x_2, y_1)$, and $P_2 = (x_2, y_2)$ is denoted λ, and given by

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2ax_1 + b}{2y_1} & \text{if } P_1 = P_2. \end{cases}$$

Then, $P_1 * P_2 = (x_3, y_3)$, and $P_1 + P_2 = (x_3, -y_3)$ where $x_3 = \lambda^2 - a - x_1 - x_2$, and $y_3 = \lambda x_3 + \nu$, where $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

In particular for $y^2 = x^3 + 2$, the duplication formula reduces to: x-coordinate of $2(x, y) = \frac{x^4+5x}{4x^3+1}$. A few sample calculations follow.

The x-coordinate of $(3, 1) * (3, 1) = \frac{81+15)}{108+1} = \frac{5}{4} = 3$; using the formulas above, the y coordinate is found to be $y = 1$, so that $(3, 1) * (3, 1) = (3, 1)$. This implies that $(3, 1)$ is an inflection point. With the formulas provided, it is easy to see that $(0, 3) * (0, 3) = (0, 3)$, and $(0, 6) * (0, 6) = (0, 6)$. With similar calculations it can be shown that each point is an inflection point, implying each non identity point has order three. This implies the group is in fact $\mathbb{Z}_3 \times \mathbb{Z}_3$.The following table can be generated with the formulas above. This provides a group embedding of $AG(2, 3)$ into $\mathbb{Z}_3 \times \mathbb{Z}_3$

Table 5.2: Group table

+	$\mathcal{O}$	(0, 3)	(0, 4)	(3, 1)	(3, 6)	(5, 1)	(5, 6)	(6, 1)	(6, 6)
$\mathcal{O}$	$\mathcal{O}$	(0,3)	(0,4)	(3,1)	(3,6)	(5,1)	(5,6)	(6,1)	(6,6)
(0, 3)	(0, 3)	(0,4)	$\mathcal{O}$	(6,1)	(5,6)	(3,1)	(6,6)	(5,1)	(3,6)
(0, 4)	(0,4)	$\mathcal{O}$	(0,3)	(5,1)	(6,6)	(6,1)	(3,6)	(3,1)	(5,6)
(3, 1)	(3,1)	(6,1)	(5,1)	(3,6)	$\mathcal{O}$	(6,6)	(0,3)	(5,6)	(0,4)
(3, 6)	(3,6)	(5,6)	(6,6)	$\mathcal{O}$	(3,1)	(0,4)	(6,1)	(0,3)	(5,1)
(5, 1)	(5,1)	(3,1)	(6,1)	(6,6)	(0,4)	(5,6)	$\mathcal{O}$	(3,6)	(0,3)
(5, 6)	(5,6)	(6,6)	(3,6)	(0,3)	(6,1)	$\mathcal{O}$	(5,1)	(0,4)	(3,1)
(6, 1)	(6,1)	(5,1)	(3,1)	(5,6)	(0,3)	(3,6)	(0,4)	(6,6)	$\mathcal{O}$
(6, 6)	(6,6)	(3,6)	(5,6)	(0,4)	(5,1)	(0,3)	(3,1)	$\mathcal{O}$	(6,1)

With some routine calculations, and a few observations, the following group embedding is obtained.

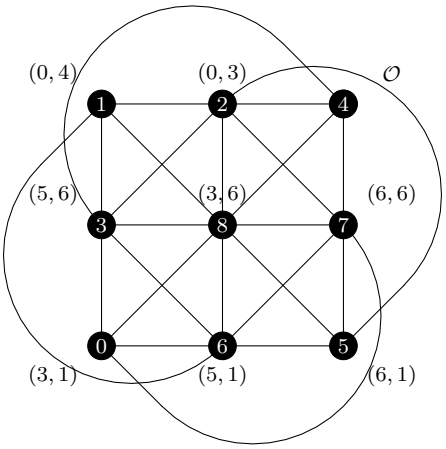

Figure 5.6: Group embedding of $AG(2,3)$ into $\mathbb{Z}_3 \times \mathbb{Z}_3$

The verifications of the twelve collinearities is obtained from the group table, and are as follows.

1. $((0,3) * (0,4)) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$

2. $((3,6) * (3,1)) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$

3. $((6,1) * (6,6)) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$

4. $((0,3) * (3,6)) * (5,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

5. $((0,3) * (6,6)) * (3,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

6. $((0,3) * (5,6)) * (6,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

7. $((3,6) * (0,4)) * (6,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

8. $((5,6) * (0,4)) * (3,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

9. $((6,6) * (0,4)) * (5,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

10. $((6,1) * (5,1)) * (3,1) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

11. $((5,6) * (6,6)) * (3,6) = \mathcal{O} * \mathcal{O} = \mathcal{O}$

12. $((5,1) * (5,6)) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$

Now with the result of Jungnickel et al. [20], by removing any point from the $AG(2,3)$ and the lines incident with it, an (8_3) is obtained. For example, by removing the point labeled '8' from the group realization of $AG(2,3)$ in Figure 5.7 leaves a group representation of the (8_3). The collinearities of the remaining lines still hold.

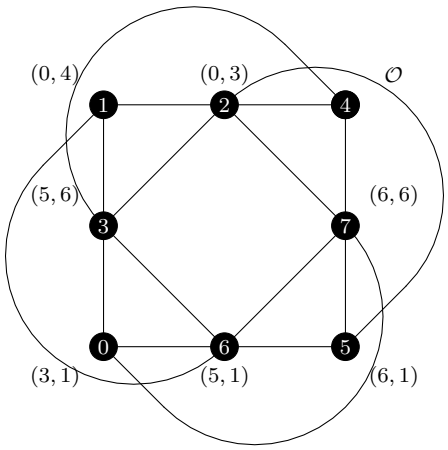

Figure 5.7: Group embedding of (8_3) into $\mathbb{Z}_3 \times \mathbb{Z}_3$

5.3.2 The Möbius-Kantor configuration in the Affine Plane $AG(2, 13)$

Using the the cubic curve $y^2 = x^3 + 3 \mod 13$, in this section we give an embedding of the Möbius-Kantor configuration into the affine plane $AG(2, 13)$. The curve has nine points over $GF(13)$, they are as follows: $(1, 2)$, $(3, 2)$, $(9, 2)$, $(0, 4)$, $(0, 9)$, $(1, 11)$, $(3, 11)$, $(9, 11)$, and $\mathcal{O}$ (the point at infinity). All of the nine points are inflexion points i.e., $P * P = P$. The algebra of incidence is given in the following $*$-table ($P * Q = R$ if and only if P, Q ,and R are collinear).

Table 5.3: Group table

$*$	$\mathcal{O}$	$(1,2)$	$(3,2)$	$(9,2)$	$(0,4)$	$(0,9)$	$(1,11)$	$(3,11)$	$(9,11)$
$\mathcal{O}$	$\mathcal{O}$	(1,11)	(3,11)	(9,11)	(0,9)	(0,4)	(1,2)	(3,2)	(9,2)
$(1,2)$	$(1,11)$	(1,2)	(9,2)	(3,2)	(3,11)	(9,11)	$\mathcal{O}$	(0,4)	(0,9)
$(3,2)$	(3,11)	(9,2)	(3,2)	(1,2)	(9,11)	(1,11)	(0,9)	$\mathcal{O}$	(0,4)
$(9,2)$	(9,11)	(3,2)	(1,2)	(9,2)	(1,11)	(3,11)	(0,4)	(0,9)	$\mathcal{O}$
$(0,4)$	(0,9)	(3,11)	(9,11)	(1,11)	(0,4)	$\mathcal{O}$	(9,2)	(1,2)	(3,2)
$(0,9)$	(0,4)	(9,11)	(1,11)	(3,11)	$\mathcal{O}$	(0,9)	(3,2)	(9,2)	(1,2)
$(1,11)$	(1,2)	$\mathcal{O}$	(0,9)	(0,4)	(9,2)	(3,2)	(1,11)	(9,11)	(3,11)
$(3,11)$	(3,2)	(0,4)	$\mathcal{O}$	(0,9)	(1,2)	(9,2)	(9,11)	(3,11)	(1,11)
$(9,11)$	(9,2)	(0,9)	(0,4)	$\mathcal{O}$	(3,2)	(1,2)	(3,11)	(1,11)	(9,11)

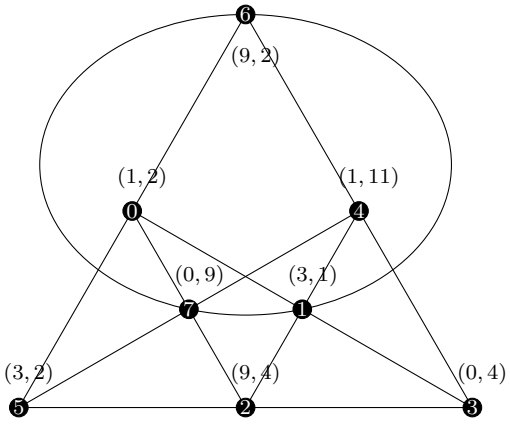

Figure 5.8: (8_3) in $AG(2, 13)$

5.4 Extensions of Möbius-Kantor Configurations

In this section, we define new configurations $\mathcal{C}_3(8 \times 3^n, 1, 3)$ that are higher analogues of the basic Möbius-Kantor configuration and prove that they are embedabble in the group $\mathbb{Z}_{3^{n+1}} \times \mathbb{Z}_{3^{n+1}}$. Since the direct product of two cyclic groups is always a subgroup of a non-singular cubic curve over the complex field, it follows that these new extended Möbius-Kantor configurations all have geometric realizations over the complex projective plane. The classical Möbius-Kantor configuration $\mathcal{C}_3(8, 1, 3)$ is a special case with $n = 0$. To construct higher analogs of the Möbius-Kantor Configuration, we employ an algebraic technique which uses analogues of the Singer polynomial associated

with the cyclic difference set $\{(0,1,3) \pmod 8\}$. The algebraic technique allows for the construction of the matrices which define our embeddings. Theorem 5.4.1 gives an alternative group embedding of the Möbius-Kantor configuration as a cyclic $C_3(8,1,3)$ which forms the basis for the subsequent extensions.

Theorem 5.4.1. *The cyclic configuration $\mathcal{C}_3(8,1,3)$ has a group realization.*

Proof. The cyclic configuration $\mathcal{C}_3(8,1,3)$ is given by the following eight triples.

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ 3 & 4 & 5 & 6 & 7 & 0 & 1 & 2 \end{array}$$

Let the mapping $f : \mathcal{C}_3(8,1,3) \to \mathbb{Z}_3 \times \mathbb{Z}_3$ be given by:

$$f : i \to A^i \mathbf{v} \mod 3$$

where $A = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$, and $\mathbf{v} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. The mapping is injective as can be seen from the following.

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 2 \\ 1 \end{pmatrix} & \begin{pmatrix} 2 \\ 2 \end{pmatrix} & \begin{pmatrix} 0 \\ 2 \end{pmatrix} & \begin{pmatrix} 2 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 2 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array}$$

To verify that f is indeed a group embedding, consider that

$$\begin{aligned} f(0) + f(1) + f(3) &= I\mathbf{v} + A\mathbf{v} + A^3\mathbf{v} \\ &\equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 2 \\ 2 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 3. \end{aligned}$$

More generally,

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= A^j\mathbf{v} + A^{j+1}\mathbf{v} + A^{j+3}\mathbf{v} \\ &= A^j(I\mathbf{v} + A\mathbf{v} + A^3\mathbf{v}) \\ &\equiv A^j \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 3 \\ &\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 3. \end{aligned}$$

□

Figure 5.9 gives a pictorial representation of the Möbius-Kantor configuration (solid lines and black nodes) along with the group coordinates obtained from Theorem 5.4.1. Additionally, the natural completion of the Möbius-Kantor to the $AG(2,3)$ is depicted as the four additional dashed lines and the white node in the middle labeled with '8'. Since the Möbius-Kantor configuration violates the Sylvester-Gallai theorem, as a super structure, so does the $AG(2,3)$. Hence neither are realizable in the real plane.

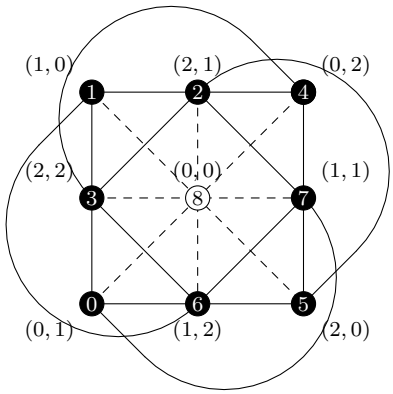

Figure 5.9: Group embedding of the (8_3) and its completion

It should be noted that the choice to embed the Möbius-Kantor configuration into direct products of $\mathbb{Z}_3$ is not without justification.

Lemma 5.4.2. *For any group embedding of the Möbius-Kantor configuration, the image of each point has order three in the group.*

Proof. Let f be a group embedding of the Möbius-Kantor configuration

into an abelian group. Using the cyclic $\{0, 1, 3\}$ description of the Möbius-Kantor configuration we have that for any point i, the blocks containing i are given by $\{i, i+1, i+3\}$, $\{i, i+5, i+6\}$, $\{i, i+2, i+7\} \mod 8$. The sum of the images of the blocks is 0; letting $j = i+1$ and $k = i+2$ we have the following.

$$\begin{aligned} -3f(i) &= f(i+1) + f(i+6) + f(i+7) + f(i+2) + f(i+3) + f(i+5) \\ &= f(j) + f(j+5) + f(j+6) + f(k) + f(k+1) + f(k+3) \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

□

5.4.1 A New Example

In this section we give an explicit construction of the first extension of the $\mathcal{C}_3(8, 1, 3)$, the $\mathcal{C}_3(24, 1, 3)$, and show that it has a group realization in the abelian group $\mathbb{Z}_9 \times \mathbb{Z}_9$. Analogous to the previous section we construct an exponential map obtained from the associated Singer polynomial.

Theorem 5.4.3. *The cyclic configuration $\mathcal{C}_3(24, 1, 3)$ has a group realization.*

Proof. Let the map $f : \mathcal{C}_3(24, 1, 3) \to \mathbb{Z}_9 \times \mathbb{Z}_9$ be given by:

$$f : i \to A^i \mathbf{v} \mod 9$$

where $A = \begin{pmatrix} 2 & 1 \\ 4 & 0 \end{pmatrix}$, and $\mathbf{v} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. It is straightforward to establish that f is injective. To verify that f is indeed a group embedding, consider that

$$\begin{aligned} f(0) + f(1) + f(3) &= I\mathbf{v} + A\mathbf{v} + A^3\mathbf{v} \\ &\equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 8 \\ 8 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 9. \end{aligned}$$

More generally,

$$\begin{aligned} f(j) + f(j+1) + f(j+3) &= A^j\mathbf{v} + A^{j+1}\mathbf{v} + A^{j+3}\mathbf{v} \\ &= A^j(I\mathbf{v} + A\mathbf{v} + A^3\mathbf{v}) \\ &\equiv A^j \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 9 \\ &\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 9. \end{aligned}$$

□

5.5 Generalized Möbius-Kantor Configurations

In this section we provide some technical lemmas necessary to establish the main result, and provide the motivation and an explicit construction for the matrices found in Theorem 5.4.1 and Theorem 5.4.3.

The aim is to show that we can "linearize" the value of x^2 in our coordinate generating calculations. The calculations to generate our coordinates are linked to the Singer polynomial x^3+x+1, so we assume that $x^3+x+1 = 0$. We want to show that $C_3(3^n, 1, 3)$ is realizable in a group of rank 2. Assuming that we can linearize x^2, we have that $x^2 = ax + b$ (where a and b are to be determined). We generate x^3 from the linearized form of x^2 to get $x^3 = ax^2 + bx = (a^2 + b)x + ab$ (after substitution). Since $x^3 = -x - 1$ it follows that $a^2 + b = -1$ and $ab = -1$. So, $b = -a^{-1}$, $a^2 - a^{-1} = -1$, or $a^3 + a - 1 = 0$. Table 5.4 gives sample calculations of a and b, and provides the motivation and basis for establishing Lemma 5.5.1.

Table 5.4: Sample calculations

3^n	$x^3 + x + 1$	$a^3 + a - 1$	b	$x^2 = ax + b$
3	1	2	1	$2x + 1$
9	7	2	4	$2x + 4$
27	7	20	4	$20x + 4$
81	61	20	4	$20x + 4$
243	223	20	85	$20x + 85$
729	709	20	328	$20x + 328$
2187	1438	749	1057	$749x + 1057$
6561	3625	2936	1057	$2936x + 1057$
3^n	$s(n)$	$3^n - s(n)$	$-(3^n - s(n))^{-1}$	$(3^n - s(n))x - (3^n - s(n))^{-1}$

Lemma 5.5.1. *The congruence* $x^3 + x - 1 \equiv 0 \mod 3^n$ *has a solution for all non-negative integers* n.

Proof. The proof is by induction on n. Notice that for $n = 1$, we have that $2^3 + 2 - 1 \equiv 0 \mod 3$. Let x_0 be a solution to the congruence $x^3 + x - 1 \equiv 0 \mod 3^n$, i.e $x_0^3 + x_0 - 1 = 3^n u$ for some integer u. Define $y_0 = x_0 - 3^n u$, then

$$\begin{aligned} y_0^3 + y_0 - 1 &= (x_0 - 3^n u)^3 + x_0 - 3^n u - 1 \\ &= x_0^3 - \binom{3}{1} 3^n u x_0^2 + \binom{3}{2} 3^{2n} u^2 x_0 - 3^{3n} u^3 + x_0 - 3^n u - 1 \\ &\equiv (x_0^3 + x_0 - 1) - 3^n u + 0 \mod 3^{n+1} \\ &\equiv 3^n u - 3^n u \mod 3^{n+1} \\ &\equiv 0 \mod 3^{n+1}. \end{aligned}$$

□

With Lemma 5.5.1 in hand we define the matrices used to give our embeddings. For a given positive integer n, let a be a solution to the congruence $x^3 + x - 1 \equiv 0 \mod 3^n$, the n^{th} *cyclic embedding matrix* A_n is given by

$$A_n = \begin{pmatrix} a & 1 \\ -a^{-1} & 0 \end{pmatrix}$$

Lemma 5.5.2. *The* n^{th} *cyclic embedding matrix* A_n *satisfies* $A_n^3 + A_n + I \equiv 0 \mod 3^n$.

Proof. Since $a^3 + a - 1 \equiv 0 \mod 3^n$, and $A_n^3 = \begin{pmatrix} a^3 - 2 & a^2 - a \\ -a + a^2 & -1 \end{pmatrix}$, it follows that

$$A_n^3 + A_n + I = \begin{pmatrix} a^3 + a - 1 & a^2 - a^{-1} + 1 \\ -a + a^{-2} - a^{-1} & 0 \end{pmatrix}$$
$$\equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \mod 3^n.$$

□

Lemma 5.5.3. *The n^{th} cyclic embedding matrix satisfies $A_n^8 \equiv -3A_n - 2I \mod 3^n$.*

Proof. The proof is a straight forward application of the previous lemma.

□

Lemma 5.5.4 is a variant of a result due to Kummer: it is used to demonstrate the vanishing binomial coefficients in Lemma 5.5.1

Lemma 5.5.4. *(Kummer, 1852,[24]) For integers n and k where $n \geq k \geq 0$, $\frac{n}{gcd(n,k)}$ divides $\binom{n}{k}$.*

Lemma 5.5.5. $A_n^{8 \times 3^{n-1}} \equiv I \mod 3^n$

Proof. By virtue of the previous lemma we have that

$$\begin{aligned} A_n^{8\times 3^{n-1}} &= (-(3A_n + 2I))^{3^{n-1}} \\ &= -\sum_{j=0}^{3^{n-1}} \binom{3^{n-1}}{j} (3A_n)^{3^{n-1}-j}(2I)^j \\ &\equiv -2^{3^{n-1}} I \mod 3^n. \end{aligned}$$

Now, the result follows provided that $2^{3^{n-1}} \equiv -1 \mod 3^n$. Since $2^{\phi(3^n)} = (2^{3^{n-1}})^2 \equiv 1 \mod 3^n$, and 2 is a generator for the entire cyclic group modulo any positive power of 3 (see [8], page 161) it follows that $2^{3^{n-1}} \equiv -1 \mod 3^n$.

□

The goal is to actually show that each of the binomial coefficients in the expansion(save the last, of course) is divisible by 3^n. It is enough to show that 3^n divides $\binom{3^{n-1}}{j} 3^{3^{n-1}-j}$. Notice that provided $j \leq 3^{n-1} - n$, then 3^n divides $3^{3^{n-1}-j}$. For $j \geq 3^{n-1} - n$, we must make up the required $3's$ from the binomial coefficient. To simplify the problem we will rewrite the bounds on j that we are interested in. These values of $j \geq 3^{n-1} - 1$ are $j = 3^{n-1} - (n-1), 3^{n-1} - (n-2), \ldots, 3^{n-1} - 1$. With respect to $3^{3^{n-1}-j}$ these correspond to the values $3^{n-1}, 3^{n-2}, \ldots, 3^1$. Now because of the symmetry of the binomial coefficients we have that $\binom{3^{n-1}}{j} = \binom{3^{n-1}}{3^{n-1}-j}$. Letting $k = 3^{n-1} - j$, the values $j = 3^{n-1} - (n-1), 3^{n-1} - (n-2), \ldots, 3^{n-1} - 1$ give $k = 1, 2, \ldots, n-1$, respectively. We can now rephrase the problem. We want to show that 3^n divides $\binom{3^{n-1}}{k} 3^k$ for $k = 1, 2, \ldots, n-1$.

Lemma 5.5.5 applied to our particular problem says that $\frac{3^{n-1}}{gcd(3^{n-1},k)}$ divides $\binom{3^{n-1}}{k}$.

Notice that

$$gcd(3^{n-1}, k) \leq k \Longrightarrow \frac{3^{n-1}}{3^{\log_3 gcd(3^{n-1},k)}} \geq \frac{3^{n-1}}{3^{\log_3 k}}.$$

Now, $3^{n-1-\log_3 k}3^k = 3^{n-1-\log_3 k+k}$, so provided that $k \geq \log_3 k + 1$, the result holds. Equivalently, the result holds if $3^k \geq 3k$, which is easily established by induction. Thus we have established the following:

Lemma 5.5.6. *3^n divides $\binom{3^{n-1}}{k}3^k$, for $k = 1, 2, \ldots, n-1$.*

Theorem 5.5.7. *Every n_3 configuration $C_3(8 \times 3^n, 1, 3)$ has a group realization in the rank 2 group $\mathbb{Z}_{3^{n+1}} \times \mathbb{Z}_{3^{n+1}}$.*

Proof.

Let A_n be the n^{th} cyclic embedding matrix, $\mathbf{v} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and let $f : \mathcal{C}_3(8 \times 3^n, 1, 3) \to \mathbb{Z}_{3^{n+1}} \times \mathbb{Z}_{3^{n+1}}$ be given by $f(i) = A_{n+1}^i \mathbf{v} \mod 3^{n+1}$. Then

$$\begin{aligned} f(i) + f(i+1) + f(i+3) &= (A_n^i + A_n^{i+1} + A_n^{i+3})\mathbf{v} \\ &= (A_n^i(I + A_n + A_n^3))\mathbf{v} \\ &\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 3^{n+1}. \end{aligned}$$

□

Corollary 5.5.7.1. *The configuration $\mathcal{C}_3(8 \times 3^n, 13)$ exists in the complex projective plane where the blocks are straight lines in the geometric sense as well.*

Proof. The underlying group structure of a non-singular cubic curve over the complex field is the torus group $S^1 \times S^1$ and this contains $\mathbb{Z}_{3^{n+1}} \times \mathbb{Z}_{3^{n+1}}$ as a subgroup.

□

Chapter 6

Infinitude of Geometric Realizations

In this chapter we prove that there are infinitely many (n_3) and (n_4) configurations having group realizations. In the case of the $(n_3)'s$, we show that these group realizations do yield actual geometric realizations over the real plane. In the case of the $(n_4)'s$ we get circle-realizations, again, over the real plane. In constructing these geometric models, we employ Hensel's Lemma to the corresponding Singer polynomials which define the cyclic configurations. Thus we have a synergy of techniques drawn from polynomial algebra, number theory, and geometry to arrive at the realizations.

6.1 Hensel's Lemma

The version of Hensel's Lemma we use comes in three parts, only the first of which is relevant to our work. It is stated without proof for reference only.

Theorem 6.1.1. *(Hensel's Lemma [30, 19]) Let $f(x)$ be a polynomial with integer coefficients, where p is prime and k is a positive integer. Let x_0 be a solution to the polynomial congruence $f(x) \equiv 0 \mod p^k$. Then exactly one of the following holds:*

1. *If $f'(x) \not\equiv 0 \mod p$ then x_0 lifts to exactly one solution x_1 to $f(x) \equiv 0 \mod p^{k+1}$. This solution is given by $x_1 = x_0 + tp^k$, where*

$$t = -\frac{f(x_0)}{p^k}(f'(x_0))^{-1}.$$

   Here t is understood to be reduced modulo p if necessary, and $(f'(x_0))^{-1}$ represents the multiplicative inverse of $f'(x_0)$ modulo p.

2. *If $f'(x) \equiv 0 \mod p$ and x_0 is a solution to $f(x) \equiv 0 \mod p^{k+1}$ then x_0 lifts to $x_1 = x_0 + tp^k$ for all integers $0 \leq t \leq p-1$. Thus x_0 lifts to p distinct solutions of $f(x) \equiv 0 \mod p^{k+1}$.*

3. *Finally, if $f'(x) \equiv 0 \mod p$ but x_0 is not a solution of $f(x) \equiv 0 \mod p^{k+1}$, then x_0 does not lift to any solutions of $f(x) \equiv 0 \mod p^{k+1}$.*

In addition to Hensel's Lemma we use a result of N. Jolly [19] which ensures our lifted primitive root solutions are primitive root solutions for the

new lifted prime powered modulus. It is stated without proof for reference.

Theorem 6.1.2. *(N. Jolly [19]) If p is an odd prime, $k \geq 2$, and g is a primitive root of p^k, then $g + tp^k$ is a primitive root of p^{k+1} for all $0 \leq t \leq p-1$.*

6.2 Infinite Embeddings via Hensel Lifting

We will proceed with a simple illustrative example.

Theorem 6.2.1. *The cyclic (n_3) configuration $C_3(20, 1, 4)$ is geometrically realizable.*

Proof. The proof is a simple application of Hensel's Lemma. For $f(x) = x^4 + x + 1$ it is routine to show that $f(3) \equiv 0 \mod 5$, and that 3 is a primitive root modulo 5. With Hensel's Lemma we lift the solution modulo 5 to a solution modulo 25. $f'(x) = 4x^3 + 1$, given that $f'(3) = 109$, and $(f'(3))^{-1} = 4 \mod 5$, therefore

$$\begin{aligned} t &= -\frac{f(3)}{5}((f'(3))^{-1}) \\ &= -\frac{85}{5}(4) \\ &= -68 \mod 5 \\ &= 2. \end{aligned}$$

With the required value of t, we can construct the lifted solution $x_1 = 3+2\cdot 5 = 13$. Thus 13 is a solution to the congruence $x^4+x+1 \equiv 0 \mod 25$,

moreover 13 is a primitive root modulo 25.

Define the mapping $\alpha : C_3(20, 1, 4) \to \mathbb{Z}_{25}$ by $\alpha : i \to 13^i \mod 25$. Then, as $13^4 + 13 + 1 \equiv 0 \mod 25$, it follows that for any j that

$$\begin{aligned}\alpha(j+4) + \alpha(j+1) + \alpha(j) &= 13^{j+4} + 13^{j+1} + 13^j \\ &= 13^j(13^4 + 13 + 1) \\ &\equiv 0 \mod 25.\end{aligned}$$

Since 13 is a primitive modulo 25 and $\phi(25) = 25 - 5 = 20$, the order of 13 modulo 25 is 20. Therefore α is a group embedding.

□

With Hensel's Lemma, and Jolly's Theorem we can produce the following lifted group embeddings.

Table 6.1: Ten Hensel-lifted embeddings of $C_3(4 \cdot 5^n, 1, 4)$

$configuration$	$Group$	$base$
$\mathcal{C}_3(100, 1, 4)$	$\mathbb{Z}_{125}$	88
$\mathcal{C}_3(500, 1, 4)$	$\mathbb{Z}_{625}$	338
$\mathcal{C}_3(2500, 1, 4)$	$\mathbb{Z}_{3125}$	1588
$\mathcal{C}_3(12500, 1, 4)$	$\mathbb{Z}_{15625}$	7838
$\mathcal{C}_3(62500, 1, 4)$	$\mathbb{Z}_{7838}$	7838
$\mathcal{C}_3(312500, 1, 4)$	$\mathbb{Z}_{390625}$	320338
$\mathcal{C}_3(1562500, 1, 4)$	$\mathbb{Z}_{1953125}$	710963
$\mathcal{C}_3(7812500, 1, 4)$	$\mathbb{Z}_{9765625}$	8523463
$\mathcal{C}_3(1562500, 1, 4)$	$\mathbb{Z}_{1953125}$	710963
$\mathcal{C}_3(7812500, 1, 4)$	$\mathbb{Z}_{9765625}$	8523463

Hensel's Lemma together with the result of Jolly provide the means by

which to demonstrate the existence of the group embeddability of the cyclic configurations $C_3(4 \cdot 5^n, 1, 4)$ into $\mathbb{Z}_{5^n}$.

Theorem 6.2.2. *$C_3(4 \cdot 5^{n-1}, 1, 4)$ has a group embedding into $\mathbb{Z}_{5^n}$ for all $n \geq 2$.*

Proof. Since 13 is a primitive solution to $x^4 + x + 1 \equiv 0 \mod 25$, we can lift to a solution, r, modulo 5^n, where $n \geq 2$. Moreover, by Jolly's result, this lifted solution is also a primitive root modulo 5^n. Define the map $\alpha : C_3(4 \cdot 5^{n-1}, 1, 4) \to \mathbb{Z}_{5^n}$ by $\alpha(i) = r^i \mod 5^n$. Then, we have that $r^4 + r + 1 \equiv 0 \mod 5^n$, and in general

$$\begin{aligned} \alpha(j+4) + \alpha(j+1) + \alpha(j) &= r^{j+4} + r^{j+1} + r^j \\ &= r^j(r^4 + r + 1) \\ &\equiv 0 \mod 5^n. \end{aligned}$$

Since $\phi(5^n) = 5^n - 5^{n-1} = 4 \cdot 5^{n-1}$, the order of r modulo 5^n is $4 \cdot 5^{n-1}$, as required for injectivity. Thus α is a group embedding, and the result follows.

□

With the previous result in hand, natural questions about the ability to generalize the technique presented arise.

Theorem 6.2.3. *Let $\sigma(x) = x^4 + x + 1$ satisfy the following three conditions:*

1. *$\sigma(r) = p$ for some prime p, and $r \in \mathbb{Z}^+$;*
2. *r is a primitive root modulo p;*
3. *The first Hensel lifted value of r has order $\phi(p^2)$ modulo p^2 (i.e., r generates the multiplicative group of units modulo p^2).*

Then $C_3((p-1)\cdot p^{n-1}, 1, 4)$ is embeddable in $\mathbb{Z}_{p^n}$ for all $n \geq 1$.

Proof. Let r be a primitive root modulo p where $\sigma(r) \equiv 0 \mod p$. Then applying Hensel's Lemma we can lift r to a solution r_1 of $\sigma(x) \equiv 0 \mod p^2$, and by assumption the order of r_1 modulo p^2 is $\phi(p^2)$. By Hensel's Lemma and Jolly's result r_1 can be lifted to a primitive solution r_{n-1} modulo p^n for all $n \geq 3$. Define the map $\alpha : C_3((p-1)\cdot p^{n-1}, 1, 4) \to \mathbb{Z}_{p^n}$ by $\alpha : i \to r^i \mod p^n$. Then by assumption we have that $r_{n-1}^4 + r_{n-1} + 1 \equiv 0 \mod p^n$, and in general we have that

$$\begin{aligned}\alpha(j+4) + \alpha(j+1) + \alpha(j) &= r_{n-1}^{j+4} + r_{n-1}^{j+1} + r_{n-1}^{j} \\ &= r_1^j(r_{n-1}^4 + r_{n-1} + 1) \\ &\equiv 0 \mod p^n.\end{aligned}$$

Since the order of r_{n-1} modulo p^n is $(p-1)p^{n-1}$, the map is for injective. Thus α is a group embedding, and the result follows.

□

Table 6.2: The first nine Hensel-lifted embeddings of the cyclic configuration $C_3(18 \cdot 19^i, 1, 4)$.

$configuration$	$Group$	$base$
$\mathcal{C}_3(18, 1, 4)$	$\mathbb{Z}_{19}$	2
$\mathcal{C}_3(342, 1, 4)$	$\mathbb{Z}_{361}$	78
$\mathcal{C}_3(6498, 1, 4)$	$\mathbb{Z}_{6856}$	2244
$\mathcal{C}_4(123462, 1, 4)$	$\mathbb{Z}_{130321}$	111988
$\mathcal{C}_3(2345778, 1, 4)$	$\mathbb{Z}_{2476099}$	633272
$\mathcal{C}_3(44569782, 1, 4)$	$\mathbb{Z}_{47045881}$	45203054
$\mathcal{C}_3(846825858, 1, 4)$	$\mathbb{Z}_{893871739}$	515661864
$\mathcal{C}_4(16089691302, 1, 4)$	$\mathbb{Z}_{16983563041}$	7666635776
$\mathcal{C}_3(305704134738, 1, 4)$	$\mathbb{Z}_{32268767779}$	143535140104

The previous technique is not limited to the Singer polynomial x^4+x+1. Indeed, it applies equally well to any cyclically described (n_3) configuration , or any general cyclic configuration $C_k(n, a_1, \ldots, a_k - 1)$ with Singer polynomial $x^{a_{k-1}} + \cdots + x^{a_1} + 1$. The results thus obtained for cyclic $(n_3)'s$ provide an additional partial answer to the question posed by Grünbaum in [18], page 68, on the existence of cyclic $(n_3)'s$ which are geometrically realizable.

Theorem 6.2.4. *Let $\sigma(x) = x^{a_{k-1}} + \cdots + x^{a_1} + 1$ satisfy the following three conditions:*

1. *$\sigma(r) = p$ for some prime p, and $r \in \mathbb{Z}^+$;*

2. *r is a primitive root modulo p;*

3. *The first Hensel lifted value, r_1, has order $\phi(p^2)$ modulo p^2.*

Then $C_k(n, a_1, \ldots, a_{k-1})$ is embeddable in $\mathbb{Z}_{p^n}$ for all $n \geq 1$.

Proof. Let r be a primitive root modulo p where $\sigma(r) \equiv 0 \mod p$. Then applying Hensel's Lemma we can lift r to a solution r_1 of $\sigma(x) \equiv 0 \mod p^2$, and by assumption the order of r_1 modulo p^2 is $\phi(p^2)$. By Hensel's Lemma and Jolly's result r_1 can be lifted to a primitive solution r_{n-1} modulo p^n for all $n \geq 3$. Define the map $\alpha : C_k(n, a_1, \ldots, a_{k-1}) \to \mathbb{Z}_{p^n}$ by $\alpha : i \to r^i \mod p^n$. Then in general we have

$$\begin{aligned}\alpha(j + a_{k-1}) + \cdots + \alpha(j + a_1) + \alpha(j) &= r_{n-1}^{j+a_{k-1}} + \cdots + r_{n-1}^{j+a_1} + r_{n-1}^{j} \\ &= r_1^j(r_{n-1}^{a_{k-1}} + \cdots + r_{n-1}^{a_1} + 1) \\ &\equiv 0 \mod p^n.\end{aligned}$$

Since the order of r_{n-1} modulo p^n is $(p-1)p^{n-1}$, the map is injective. Thus α is a group embedding, and the result follows.

□

Table 6.3: The first five Hensel-lifted embeddings of the cyclic configuration $C_4(522 \cdot 523^i, 1, 3, 9)$.

$configuration$	$Group$	$base$
$\mathcal{C}_4(522, 1, 3, 9)$	$\mathbb{Z}_{523}$	2
$\mathcal{C}_4(273006, 1, 3, 9)$	$\mathbb{Z}_{273529}$	44980
$\mathcal{C}_4(142782138, 1, 3, 9)$	$\mathbb{Z}_{143055667}$	318509
$\mathcal{C}_4(7465058174, 1, 3, 9)$	$\mathbb{Z}_{74818113841}$	69525372671
$\mathcal{C}_4(39055055425002, 1, 3, 9)$	$\mathbb{Z}_{39129873538843}$	6653519390679

Table 6.4: The first ten Hensel-lifted embeddings of the cyclic configuration $C_3(10 \cdot 11^i, 1, 3)$.

$configuration$	$Group$	$base$
$\mathcal{C}_3(10, 1, 3)$	$\mathbb{Z}_{11}$	2
$\mathcal{C}_3(110, 1, 3)$	$\mathbb{Z}_{121}$	57
$\mathcal{C}_3(1210, 1, 3)$	$\mathbb{Z}_{1331}$	1267
$\mathcal{C}_3(13310, 1, 3)$	$\mathbb{Z}_{14641}$	6591
$\mathcal{C}_3(146410, 1, 3)$	$\mathbb{Z}_{161051}$	153001
$\mathcal{C}_3(161051, 1, 3)$	$\mathbb{Z}_{1771561}$	475103
$\mathcal{C}_3(17715610, 1, 3)$	$\mathbb{Z}_{19487171}$	7561347
$\mathcal{C}_3(194871710, 1, 3)$	$\mathbb{Z}_{214358881}$	182945886
$\mathcal{C}_3(2143588810, 1, 3)$	$\mathbb{Z}_{2357947691}$	611663648
$\mathcal{C}_3(23579476910, 1, 3)$	$\mathbb{Z}_{25937424601}$	5327559030

Table 6.5: The first ten Hensel-lifted embeddings of the cyclic configuration $C_4(82 \cdot 83^i, 1, 4, 6)$.

$configuration$	$Group$	$base$
$\mathcal{C}_4(82, 1, 4, 6)$	$\mathbb{Z}_{83}$	2
$\mathcal{C}_4(6806, 1, 4, 6)$	$\mathbb{Z}_{6889}$	3737
$\mathcal{C}_4(564898, 1, 4, 6)$	$\mathbb{Z}_{571787}$	299964
$\mathcal{C}_4(46886534, 1, 4, 6)$	$\mathbb{Z}_{47458321}$	10592130
$\mathcal{C}_4(3891582322, 1, 4, 6)$	$\mathbb{Z}_{3939040643}$	1149591834
$\mathcal{C}_4(323001332726, 1, 4, 6)$	$\mathbb{Z}_{326940373369}$	52357120193
$\mathcal{C}_4(26809110616258, 1, 4, 6)$	$\mathbb{Z}_{27136050989627}$	18034077655488
$\mathcal{C}_4(2225156181149414, 1, 4, 6)$	$\mathbb{Z}_{2252292232139041}$	343666689531012
$\mathcal{C}_4(184687963035401362, 1, 4, 6)$	$\mathbb{Z}_{186940255267540403}$	56650972493007037
$\mathcal{C}_4(15329100931938313046, 1, 4, 6)$	$\mathbb{Z}_{15516041187205853449}$	3982396333111355500

The existence of primitive roots modulo a prime power is a well-known result. However, in light of the previous results we can ask whether the Singer polynomial, $\sigma(x)$, actually takes on prime values with any sort of regularity, or at all. The Bunyakovsky conjecture is a well-known conjecture in number

theory. It conjectures the existence of infinitely many primes of the form $\sigma(r)$, as r runs over the positive integers, and is generally believed to be true. However, the only known case is the famous Dirichlet Theorem on primes in arithmetic progression. No counter-example is known either. Coupled with the assumed truth of the Bunyakovsky conjecture, Theorems 6.2.3 and 6.2.4 and the examples given in this chapter suggests that our technique may be valid infinitely often, and each instance in turn giving infinitely many group embeddings via lifting.

Chapter 7

Group Embeddings of Designs

In this chapter we describe several cyclic symmetric (v, k, λ) designs as groups. In describing these cyclic designs as group we finally employ the field extension method described in the introduction.

Definition 7.0.1. *A* Balanced Incomplete Block Design*(BIBD) is a pair* $(V, \mathcal{B})$ *where the set* V *has* v *elements and* $\mathcal{B}$ *is a collection of* b *subsets of* V *called blocks, each with size* k*. Each element of* V *is contained in exactly* r *blocks and any pair of elements of* V *is contained in exactly* λ*. The numbers* v, b, k, λ, r *are the parameters of the* $BIBD$*. A* $BIBD$ *with* $v = b$ *is a symmetric* (v, k, λ) *design, or* $SBIBD$*.*

Definition 7.0.2. *Let* G *be a cyclic abelian group of order* v*. A* k *element subset* D *of* G *is a* $(v, k, \lambda; n)$ *is a difference set of order* $n = k - \lambda$ *if every non-zero element of* G *occurs exactly* λ *times among the differences* $d_i - d_j$*, where* d_i *and* d_j *are elements of* D*.* D *is called a* cyclic difference set*.*

We have already seen examples of $(v, k, \lambda; n)$ difference sets. The Fano configuration is the $(7, 3, 1)$ $SBIBD$ with cyclic difference set $\{0, 1, 3\}$. See page 16 of chapter 1. Similarly, $\{0, 1, 3, 9\}$ is a $(13, 4, 1; 3)$ difference set of order 3.

In the terminology of design theory the analogue of the Singer polynomial is often referred to as the Hall polynomial. The Hall polynomial of a difference set $D = \{d_1, \ldots, d_k\}$ is given by $h(x) = x^{d_k} + \cdots + x^{d_1}$. We will use the two names interchangeably in what follows.

Definition 7.0.3. *Let D be a $(v, k, \lambda; n)$ difference set over a group G. The set of all distinct sets $g + D$, where $g \in G$ is called the development of D. The development of D is denoted $Dev(D)$.*

7.1 Finite Projective Planes as Groups

Perhaps the best known of the $(v, k, 1)$ $SBIBD's$ are the finite projective planes. Here $v = p^2 + p + 1$, $k = p + 1$, and as already stated $\lambda = 1$. In this section we present a table of group embeddings of several finite projective planes. We leave the explanation of the Type 2 embeddings used to generate the embeddings in this section until the next section on biplanes. All embeddings in this chapter were generated as Type 2 embeddings using a crude method in MAPLE.

Table 7.1: The first nine finite projective planes as groups given by the design parameters $(p^{2k} + p^k + 1, p^k + 1, 1)$.

Design	Singer Exponents	Resultant	Group
$(7, 3, 1)$	$0, 1, 3$	8	$(\mathbb{Z}_2)^3$
$(13, 4, 1)$	$0, 1, 3, 9$	3^6	$(\mathbb{Z}_3)^3$
$(21, 5, 1)$	$3, 6, 7, 12, 14$	2^{12}	$(\mathbb{Z}_2)^6$
$(31, 6, 1)$	$0, 1, 3, 8, 12, 18$	5^{15}	$(\mathbb{Z}_5)^3$
$(57, 8, 1)$	$1, 5, 6, 8, 18, 37, 41, 48$	7^8	$(\mathbb{Z}_7)^3$
$(73, 9, 1)$	$1, 2, 4, 6, 16, 32, 37, 55, 64$	2^{108}	$(\mathbb{Z}_2)^9$
$(91, 10, 1)$	$0, 1, 3, 9, 27, 49, 56, 61, 77, 81$	3^{72}	$(\mathbb{Z}_3)^6$
$(133, 12, 1)$	$0, 10, 15, 39, 40, 42, 51,$ $59, 73, 77, 120, 127$	11^{54}	$(\mathbb{Z}_{11})^3$
$(183, 14, 1)$	$0, 1, 3, 16, 23, 28, 42, 76,$ $82, 86, 119, 137, 154, 175$	13^{60}	$(\mathbb{Z}_{13})^3$

7.2 Group Realizations of some Biplanes

Interpreted as a design, a biplane is a $(v, k, 2)$ design. Although trivial, it is worth noting that the $(4, 3, 2)$ biplane cannot be represented as a group. Consider the following representation of the $(4, 3, 2)$ biplane given in Figure 7.1.

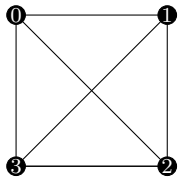

Figure 7.1: $(4, 3, 2)$ Biplane

To embed the $(4, 3, 2)$ biplane in a group, the sum of the images of the points on any line must be the group identity. In particular, we must have that $f(0) + f(1) + (2) = e = f(0) + f(1) + f(3)$. But then by cancellation we must have $f(2) = f(3)$.

It is also worth noting that the $(4, 3, 2)$ biplane can be represented by a cyclic difference set modulo 4. It is routine to verify that $Dev\{0, 1, 2\}$ modulo 4 describes the $(4, 3, 2)$ biplane. Thus we have an example of a biplane realizable as a cyclic difference set, but not realizable as a group.

7.3 The (7,4,2) Biplane (The Fano Biplane)

The classical construction for the (7,4,2) biplane is by complementing the Fano plane. The point set for the (7,4,2) biplane remains the same as that of the Fano plane, but the lines are the complements of the lines of the Fano plane with respect to the point set. A few observations about embedding the Fano biplane into a group follow.

Lemma 7.3.1. *If f is a group embedding of the Fano biplane into an abelian group G, then $4\sum_{i\in P} f(i) = e$.*

Proof. The proof is simple: sum over the group images of each line. The sum of images over any line is e, and each element appears four times amongst the lines. Thus,

$$4\sum_{i\in P} f(i) = e.$$

□

Theorem 7.3.2. *Let f be a group embedding of the Fano biplane into an abelian group G. Then for all $i \in P$, $4f(i) = e$.*

Proof. Fix some i in the configuration, and sum over the images of only the lines containing i, and we have

$$2f(i) = -2\sum_{i\in P} f(i) = e.$$

Coupled with the previous lemma, it follows that $4f(i) = e$.

□

Corollary 7.3.2.1. *In any group embedding of the Fano biplane, the group order of each embedded element is 2 or 4.*

Without the aid of the resultant the previous results suggest that the smallest possible group embedding of the Fano biplane is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. It's well known that the quadratic non-residues of $GF(7)$ form a cyclic difference set for the (7,4,2) biplane with points $P = \{0, 1, 2, 3, 4, 5, 6\}$ whose blocks are given by $Dev\{0, 3, 5, 6\}$. We employ the Field Extension technique: a factorization of the Hall polynomial $p(x) = x^6 + x^5 + x^3 + 1$ modulo 2 gives: $p(x) = (x+1)(x^3+x+1)$. Calculating the powers of x^i in $\mathbb{Z}_2[x]/(x^3+x+1)$

gives a natural association, ϕ, between the Fano biplane and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The results of these calculations and the explicit mapping for ϕ are given in Table 7.2.

Table 7.2: Group embedding of the Fano biplane.

Point	*Power*	*Polynomial*	$3-tuple$
0	x^0	1	$\phi(0) = (0,0,1)$
1	x^1	x	$\phi(1) = (0,1,0)$
2	x^2	x^2	$\phi(2) = (1,0,0)$
3	x^3	$x+1$	$\phi(3) = (0,1,1)$
4	x^4	x^2+x	$\phi(4) = (1,1,0)$
5	x^5	x^2+x+1	$\phi(5) = (1,1,1)$
6	x^6	x^2+1	$\phi(6) = (1,0,1)$

The calculations verifying that ϕ is indeed a group embedding of the Fano biplane into $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are given in Table 7.3. The calculations for the Fano biplane are simple enough to complete by hand, and are included only to be illustrative of the basic technique. The complete verifications for the (11,5,2), and (37,9,2) biplanes are omitted, but were carried out by a simple routine in MAPLE.

Figure 7.2 gives a classical depiction of the Fano plane with a depiction of the Fano biplane beside it. The seven lines of the Fano biplane are given by six circles, and one tetrahedral star (the line $\{0,3,5,6\}$).

Table 7.3: Line-sum calculations for the Fano plane embedding.

Line	*Sum of the images of the points*
$\{0,3,5,6\}$	$\phi(0)+\phi(3)+\phi(5)+\phi(6) = (0,0,1)+(0,1,1)+(1,1,1)+(1,0,1)$ $= (0,0,0)$
$\{1,4,6,0\}$	$\phi(1)+\phi(4)+\phi(6)+\phi(0) = (0,1,0)+(1,1,0)+(1,0,1)+(0,0,1)$ $= (0,0,0)$
$\{2,5,0,1\}$	$\phi(2)+\phi(5)+\phi(0)+\phi(1) = (1,0,0)+(1,1,1)+(0,0,1)+(0,1,0)$ $= (0,0,0)$
$\{3,6,1,2\}$	$\phi(3)+\phi(6)+\phi(1)+\phi(2) = (0,1,1)+(1,0,1)+(0,1,0)+(1,0,0)$ $= (0,0,0)$
$\{4,0,2,3\}$	$\phi(4)+\phi(0)+\phi(2)+\phi(3) = (1,1,0)+(0,0,1)+(1,0,0)+(0,1,1)$ $= (0,0,0)$
$\{5,1,3,4\}$	$\phi(5)+\phi(1)+\phi(3)+\phi(4) = (1,1,1)+(0,1,0)+(0,1,1)+(1,1,0)$ $= (0,0,0)$
$\{6,2,4,5\}$	$\phi(6)+\phi(2)+\phi(4)+\phi(5) = (1,0,1)+(0,1,0)+(1,1,0)+(1,1,1)$ $= (0,0,0)$

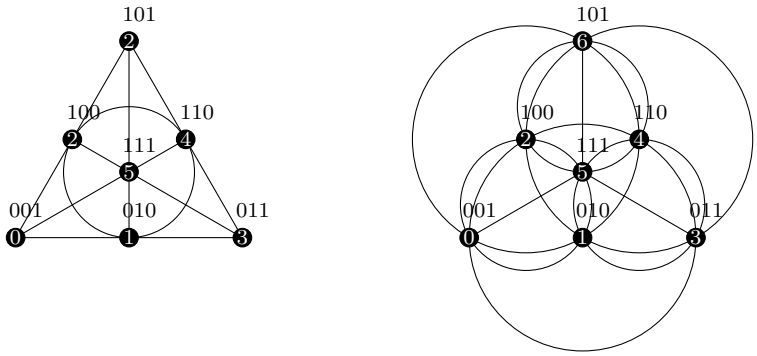

Figure 7.2: The Fano plane and the Fano biplane

7.4 The $(11, 5, 2)$ Biplane

In this section we will exhibit a group embedding of the $(11, 5, 2)$ biplane into $\mathbb{Z}_3^5$ using the field extension technique. To this end we generalize Theorem 7.3.2, and use it as a guide to find minimal embeddings.

Theorem 7.4.1. *If D is a (v, k, λ) $SBIBD$, and f is a group embedding of D into an abelian group G, then there exists an element $g \in G$ such that for all elements d in the design D $(k - \lambda)f(d) = g$.*

Proof. Fix some i in D, and sum over the images of only the lines containing i, and we have

$$(k - \lambda)f(i) = -\lambda \sum_{d \in D} f(d),$$

where $g = -\lambda \sum_{d \in D} f(d)$.

□

Without the aid of the resultant, Theorem 7.4.1 is a powerful tool in identifying potential minimal embeddings. To find embeddings that minimize the order of the embedded elements, and the size of the group we set $g = e$ in Theorem 7.4.1. Applied to the $(11, 5, 2)$ biplane it suggests that we should try to embed into direct products of $\mathbb{Z}_3$. To generate the embedding of the (11,5,2) biplane into $\mathbb{Z}_3^5$ we argue analogously to the embedding of the (7,4,2). It is well known that $\{8, 4, 3, 2, 0\}$ is a cyclic difference set modulo 11 for the

(11,5,2) biplane. Factoring the Singer polynomial $s(x) = x^8+x^4+x^3+x^2+1$ over $GF(3)$ gives: $s(x) = x^8 + x^4 + x^3 + x^2 + 1 = (x + 1)(x^2 + 2x + 2)(x^5 + 2x^3 + x^2 + 2x + 2)$. Reducing the powers x^i for $i = 0, \ldots, 11$ modulo $x^5 + 2x^3 + x^2 + 2x + 2$ gives the embedding. The embedding is given in Table 7.4.

Table 7.4: Group embedding of the $(11, 5, 2)$ biplane.

Point	*Power*	*Polynomial*	$5 - tuple$
0	x^0	1	$\phi(0) = (0, 0, 0, 0, 1)$
1	x^1	x	$\phi(1) = (0, 0, 0, 1, 0)$
2	x^2	x^2	$\phi(2) = (0, 0, 1, 0, 0)$
3	x^3	x^3	$\phi(3) = (0, 1, 0, 0, 0)$
4	x^4	x^4	$\phi(4) = (1, 0, 0, 0, 0)$
5	x^5	$1x^3 + 2x^2 + 1x + 1$	$\phi(5) = (0, 1, 2, 1, 1)$
6	x^6	$x^4 + 2x^3 + x^2 + x$	$\phi(6) = (1, 2, 1, 1, 0)$
7	x^7	$2x^4 + 2x^3 + x + 1$	$\phi(7) = (2, 2, 0, 1, 1)$
8	x^8	$2x^4 + 2x^3 + 2x^2 + 2$	$\phi(8) = (2, 2, 2, 0, 2)$
9	x^9	$2x^4 + x^3 + x^2 + x + 2$	$\phi(9) = (2, 1, 1, 1, 2)$
X	x^{10}	$x^4 + 2x^2 + x + 2$	$\phi(X) = (1, 0, 2, 1, 2)$

Now, $Dev\{0, 2, 3, 4, 8\}$ describes the lines of the $(11, 5, 2)$ biplane. As a sample calculation that the given embedding is indeed a group embedding consider the line $\{2, 4, 5, 6, X\}$: $\phi(2) + \phi(4) + \phi(5) + \phi(6) + \phi(X) = (0, 0, 1, 0, 0)+(1, 0, 0, 0, 0)+(0, 1, 2, 1, 1)+(1, 2, 1, 1, 0)+(1, 0, 2, 1, 2) = (0, 0, 0, 0, 0)$.

7.5 The (37,9,2) Biplanes

In this section we exhibit two different group embeddings of the (37,9,2) biplane into $\mathbb{Z}_7^9$.

To generate the group embeddings we begin with the cyclic difference set $\{33, 32,\ 25, 15, 11, 9, 8, 6, 1\}$ and form the Singer polynomial $\sigma(x) = x^{33} + x^{32} + x^{25} + x^{15} + x^{11} + x^9 + x^8 + x^6 + 1$, and factor it over $GF(7)$. This gives $\sigma(x) = x^{33} + x^{32} + x^{25} + x^{15} + x^{11} + x^9 + x^8 + x^6 + 1 = (x^3 + x^2 + 6x + 5)(x^4 + x^3 + 6x^2 + 2)(x^8 + 6x^7 + 2x^6 + x^4 + 6x^3 + 5x^2 + 3x + 5)(x^9 + 3x^6 + 4x^5 + 4x^4 + 2x^3 + 2x^2 + 5x + 6)(x^9 + x^7 + 2x^6 + 2x^5 + 2x^4 + 6x^3 + 3x^2 + x + 6)$.

In the factorization we get two irreducibles of degree nine, and each gives an embedding into $\mathbb{Z}_7^9$. Table 7.5 is the embedding corresponding to the polynomial $x^9+3x^6+4x^5+4x^4+2x^3+2x^2+5x+6$, and Table 7.6 corresponds to the polynomial $x^9+x^7+2x^6+2x^5+2x^4+6x^3+3x^2+x+6$. Analogously the lines of both of the $(37, 9, 2)$ biplanes are given by $Dev\{33, 32, 25, 15, 11, 9, 8, 6, 1\}$.

Table 7.5: Group embedding of the $(37, 9, 2)$ biplane.

Point	*Power*	$9-tuple$
0	x^0	$(0,0,0,0,0,0,0,0,1)$
1	x^1	$(0,0,0,0,0,0,0,1,0)$
2	x^2	$(0,0,0,0,0,0,1,0,0)$
3	x^3	$(0,0,0,0,0,1,0,0,0)$
4	x^4	$(0,0,0,0,1,0,0,0,0)$
5	x^5	$(0,0,0,1,0,0,0,0,0)$
6	x^6	$(0,0,1,0,0,0,0,0,0)$
7	x^7	$(0,1,0,0,0,0,0,0,0)$
8	x^8	$(1,0,0,0,0,0,0,0,0)$
9	x^9	$(0,0,4,3,3,5,5,2,1)$
10	x^{10}	$(0,4,3,3,5,5,2,1,0)$
11	x^{11}	$(4,3,3,5,5,2,1,0,0)$
12	x^{12}	$(3,3,0,3,0,0,6,1,4)$
13	x^{13}	$(3,0,1,2,2,0,2,3,3)$
14	x^{14}	$(0,1,0,4,2,3,4,2,3)$
15	x^{15}	$(1,0,4,2,3,4,2,3,0)$
16	x^{16}	$(0,4,6,6,0,0,1,2,1)$
17	x^{17}	$(4,6,6,0,0,1,2,1,0)$
18	x^{18}	$(1,6,2,5,6,1,0,1,4)$
19	x^{19}	$(6,2,1,3,5,2,3,2,6)$
20	x^{20}	$(1,1,6,2,6,5,4,4,6)$
21	x^{21}	$(1,6,3,5,4,0,0,3,2)$
22	x^{22}	$(6,3,2,0,3,5,2,4,1)$
23	x^{23}	$(3,2,3,0,2,3,6,6,6)$
24	x^{24}	$(2,3,5,4,5,0,0,5,3)$
25	x^{25}	$(3,5,5,4,6,3,1,0,1)$
26	x^{26}	$(5,5,2,1,5,2,1,1,3)$
27	x^{27}	$(5,2,0,6,3,5,5,6,5)$
28	x^{28}	$(2,0,5,4,6,2,3,1,5)$
29	x^{29}	$(0,5,5,5,1,6,4,2,2)$
30	x^{30}	$(5,5,5,1,6,4,2,2,0)$
31	x^{31}	$(5,5,0,0,5,6,6,3,5)$
32	x^{32}	$(5,0,6,6,0,3,0,1,5)$
33	x^{33}	$(0,6,5,1,4,4,5,1,5)$
34	x^{34}	$(6,5,1,4,5,4,1,5,0)$
35	x^{35}	$(5,1,0,1,2,3,0,5,6)$
36	x^{36}	$(1,0,0,3,4,4,2,2,5)$

Table 7.6: Group embedding of the $(37, 9, 2)$ biplane.

$Point$	$Power$	$9-tuple$
0	x^0	$(0,0,0,0,0,0,0,0,1)$
1	x^1	$(0,0,0,0,0,0,0,1,0)$
2	x^2	$(0,0,0,0,0,0,1,0,0)$
3	x^3	$(0,0,0,0,0,1,0,0,0)$
4	x^4	$(0,0,0,0,1,0,0,0,0)$
5	x^5	$(0,0,0,1,0,0,0,0,0)$
6	x^6	$(0,0,1,0,0,0,0,0,0)$
7	x^7	$(0,1,0,0,0,0,0,0,0)$
8	x^8	$(1,0,0,0,0,0,0,0,0)$
9	x^9	$(0,6,5,5,5,1,4,6,1)$
10	x^{10}	$(6,5,5,5,1,4,6,1,0)$
11	x^{11}	$(5,6,0,3,6,5,4,1,6)$
12	x^{12}	$(6,2,0,3,2,2,0,1,5)$
13	x^{13}	$(2,1,5,4,6,0,4,6,6)$
14	x^{14}	$(1,3,0,0,2,6,0,4,2)$
15	x^{15}	$(3,6,5,0,4,1,1,1,1)$
16	x^{16}	$(6,2,1,5,2,4,6,5,3)$
17	x^{17}	$(2,2,0,4,6,5,1,4,6)$
18	x^{18}	$(2,5,0,2,1,3,5,4,2)$
19	x^{19}	$(5,5,5,4,6,0,5,0,2)$
20	x^{20}	$(5,0,1,3,4,3,6,4,5)$
21	x^{21}	$(0,3,0,1,0,4,3,0,5)$
22	x^{22}	$(3,0,1,0,4,3,0,5,0)$
23	x^{23}	$(0,5,1,5,4,3,3,4,3)$
24	x^{24}	$(5,1,5,4,3,3,4,3,0)$
25	x^{25}	$(1,0,1,0,0,2,2,2,5)$
26	x^{26}	$(0,0,5,5,0,3,6,4,1)$
27	x^{27}	$(0,5,5,0,3,6,4,1,0)$
28	x^{28}	$(5,5,0,3,6,4,1,0,0)$
29	x^{29}	$(5,2,0,3,1,6,6,2,5)$
30	x^{30}	$(2,2,0,5,3,4,1,0,5)$
31	x^{31}	$(2,5,1,6,0,3,1,3,2)$
32	x^{32}	$(5,6,2,3,6,3,4,0,2)$
33	x^{33}	$(6,4,0,3,0,2,6,4,5)$
34	x^{34}	$(4,1,5,2,4,5,0,6,6)$
35	x^{35}	$(1,1,1,3,4,4,1,2,4)$
36	x^{36}	$(1,0,1,2,2,2,6,3,1)$

Table 7.7: The first four Biplanes as groups.

Design	Singer Exponents	Resultant	Group
$(7, 4, 2)$	$2, 4, 5, 6$	8	$(\mathbb{Z}_2)^3$
$(11, 5, 2)$	$0, 2, 3, 4, 8$	3^5	$(\mathbb{Z}_3)^5$
$(16, 6, 2)$	$0, 2, 3, 5, 15, 17$	$2^2 \cdot 17$	$\mathbb{Z}_{17}$
$(37, 9, 2)$	$0, 6, 8, 9, 11, 15, 25, 32, 33$	7^{12}	$(\mathbb{Z}_7)^9$

7.6 Miscellaneous Cyclic Designs as Groups

This section tabulates some embeddings of cyclic designs. All embeddings were derived using the field extension technique (Type 2 embedding) in MAPLE.

Table 7.8: Miscellaneous Cyclic Designs taken from Handbook of Combinatorial Designs. [10]

Design	Singer Exponents	Resultant	Group
$(11, 6, 3)$	$0, 2, 6, 7, 8, 10$	3^5	$(\mathbb{Z}_3)^5$
$(15, 7, 3)$	$0, 1, 2, 4, 5, 8, 10$	2^8	$(\mathbb{Z}_2)^4$
$(19, 9, 4)$	$1, 3, 4, 5, 6, 8, 10, 15, 16$	5^9	$(\mathbb{Z}_5)^9$
$(23, 11, 5)$	$0, 1, 2, 3, 5, 7, 8, 11, 12, 15, 17$	$2^{11} \cdot 3^1 1$	$(\mathbb{Z}_2)^{12}$
$(23, 11, 5)$	$0, 1, 2, 3, 5, 7, 8, 11, 12, 15, 17$	$2^{11} \cdot 3^1 1$	$(\mathbb{Z}_3)^{11}$
$(35, 17, 8)$	$0, 1, 3, 4, 7, 9, 11, 12, 13,$ $14, 16, 17, 21, 27, 28, 29, 33$	3^{24}	$(\mathbb{Z}_3)^{12}$
$(40, 13, 4)$	$1, 2, 3, 9, 17, 19, 24, 26, 30, 35, 39$	3^{16}	$(\mathbb{Z}_3)^4$
$(47, 23, 11)$	$1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17,$ $18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42$	$2^{46} \cdot 3^{23}$	$(\mathbb{Z}_2)^{23}$

Chapter 8

Properties Forced by Group Embeddings

A group structure imposed on a configuration $\mathcal{C}$ influences its geometric structure in a profound way. For example as early as 1985 Metelka [29] discovered the appearance of extra collinearities when he tried to inscribe a given configuration on an elliptic curve. The additional collinearities, troublesome as they were for Metelka, are in fact a natural consequence of the group law present in every non-singular cubic curve. This group structure is what adds the additional properties to the combinatorially defined configuration. In principle, this is similar to the concept of *almost a theorem* of Kocay [23].

Let us make this phenomenon a little bit more precise. Suppose $\mathcal{C}$ is a point-line configuration and let P be a property expressible in the language of concurrency, collinearity, and equality of points. We will say $\mathcal{C} \models_G P$ (in

words, $\mathcal{C}$ implies P in groups) if whenever $\mathcal{C}$ is realized in a group, then the property P is valid for the embedded image of $\mathcal{C}$, even though P may not be valid in the original configuration $\mathcal{C}$. This gives a sort of constraint that must be valid for group realizable configurations. In this chapter we give some examples of this phenomenon. In fact, such properties enable us to find actual group realizations of point-line configurations.

Theorem 8.0.1. $\{C_3(10,1,3) \mod 10\} \vDash_G [i, i+5]$ *concurrent for all* i.

Proof. Recall the incidence relations defining the configuration $C_3(10,1,3)$, they are given as follows.

0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	0
3	4	5	6	7	8	9	0	1	2

Assuming f is a group embedding, we have

$$\begin{aligned}
f(0)+f(5) &= -f(1)-f(3)-f(4)-f(7) && \text{(lines: } \{0,1,3\} \text{ \& } \{4,5,7\}) \\
&= -f(1)-f(4)-f(3)-f(7) && \text{(commutativity)} \\
&= f(2)-f(3)-f(7) && (\{1,2,4\} \text{ is a line}) \\
&= -f(9)-f(0)-f(3)-f(7) && (\{0,2,9\} \text{ is a line}) \\
&= -(f(9)+f(7))-(f(0)+f(3)) && \text{(commutativity)} \\
&= f(6)+f(1) && \text{(lines: } \{6,7,9\} \text{ \& } \{0,1,3\}).
\end{aligned}$$

Since adding 1 modulo 10 preserves incidence, we have that

$$\begin{aligned} f(0) + f(5) &= f(1) + f(6) \\ &= f(2) + f(7) \\ &= f(3) + f(8) \\ &= f(4) + f(9). \end{aligned}$$

Therefore, all five lines $[0, 5]$, $[1, 6]$, $[2, 7]$, $[3, 8]$, and $[4, 9]$ are concurrent.

□

Note: the additional lines are not concurrent in C, but only in the group image. The following illustration from [27] is a depiction of the previous result.

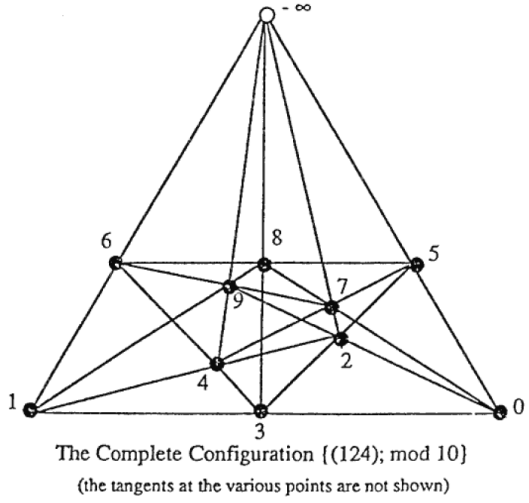

Figure 8.1: By letting $f(\infty) = 0$ in the group we have a depiction of the forced collinearities of the configuration.

Lemma 5.4.2 establishes that in any group embedding of the Möbius-Kantor configuration each element has order 3 in the group, thus we have the following corollary.

Corollary 8.0.1.1. $C_3(8,1,3) \vDash_G 3g = 0$ *for all* g *in* G.

Figure 5.9 suggests that the inverse pairs in the group embedding of the Möbius-Kantor configuration must also be collinear. We demonstrate this fact in the following theorem.

Theorem 8.0.2. $\{C_3(8,1,3) \mod 8\} \vDash_G AG(2,3)$.

Proof. Recall the incidence relations for $C_3(8,1,3)$.

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ 3 & 4 & 5 & 6 & 7 & 0 & 1 & 2 \end{array}$$

Assuming that f is a group embedding of $C_3(8,1,3)$, we have the following:

$$\begin{aligned} f(0) + f(4) &= -f(1) - f(3) - f(5) - f(7) \\ &= f(2) + f(6). \end{aligned}$$

We also have,

$$\begin{aligned} f(0) + f(4) &= -f(5) - f(6) - f(1) - f(2) \\ &= f(3) + f(7) \end{aligned}$$

and also,

$$\begin{aligned} f(0) + f(4) &= -f(2) - f(7) - f(3) - f(6) \\ &= f(5) + f(1). \end{aligned}$$

Therefore, the lines $[0, 4]$, $[1, 5]$, $[2, 6]$, and $[3, 7]$ are all concurrent.

□

Lemma 8.0.3. *$C_3(13, 1, 4) \vDash_G 3f(x) = e$ for all x in $C_3(13, 1, 4)$.*

Proof. Let f be a group embedding of $C_3(13, 1, 4)$, then

$$\begin{aligned} e &= e + e \\ &= (f(0) + f(1) + f(4)) + (f(1) + f(2) + f(5)) \\ &= (f(1) + f(1)) + (f(2) + f(0)) + (f(4) + f(5)) \\ &= (f(1) + f(1)) + (f(2) + f(0)) + (f(9) + f(12)) \\ &= (f(1) + f(1)) + (f(2) + f(12)) + (f(0) + f(9)) \\ &= (f(1) + f(1)) - f(11) - f(10) \\ &= f(1) + f(1) + f(1). \end{aligned}$$

Thus $3f(1) = e$, and since adding 1 modulo 13 is an automorphism $3f(x) = e$ for all x in $C_3(13, 1, 4)$.

□

As all of the elements of any embedding must be of order 3 in the target group, and as there are 13 elements to embed, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ would represent

a minimal group for our purposes. This suggests that $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ is the most natural embedding for $C_3(13, 1, 4)$. Indeed we have the following.

Theorem 8.0.4. *$C_3(13, 1, 4)$ group embeddable in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.*

8.1 Fano-Like Configurations

Definition 8.1.1. *A configuration C is called* Fano-like *if $C \vDash_G C_3(7, 1, 3)$, the Fano configuration. That is to say, there exists a Fano plane as a sub-configuration in every group image of C.*

Theorem 8.1.2. *The (14_3) configuration $C_3(14, 1, 3)$ is Fano-like.*

Proof. The $C_3(14, 1, 3)$ configuration is given by the following 14 triples.

0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2	3	4	5	6	7	8	9	10	11	12	13	0
3	4	5	6	7	8	9	10	11	12	13	0	1	2

Let f be a group embedding of the configuration into an abelian group G. Let S be the subset of G given by

$$S = \{f(i) + f(i + 7) : i \in \mathbb{Z}_{14}\}.$$

We claim that this subset S of G forms an image of the Fano plane as shown in the following figure. Let $f(i) = \mathbf{i}$, for each $i \in C_3(14, 1, 3)$.

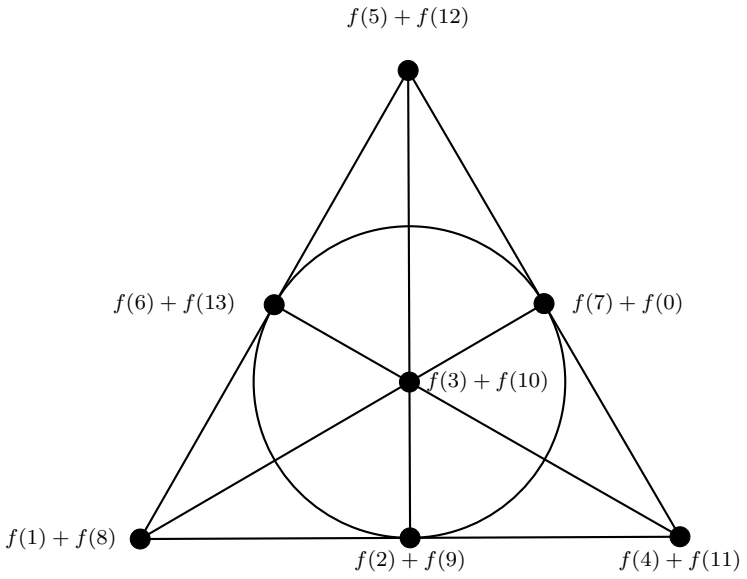

Figure 8.2: An image of the Fano plane

Now let us formally verify that the group sum over each line in the configuration is indeed zero in the group G.

$$\begin{aligned}\mathbf{1} + \mathbf{8} + \mathbf{2} + \mathbf{9} + \mathbf{4} + \mathbf{11} &= \mathbf{1} + \mathbf{2} + \mathbf{4} + \mathbf{8} + \mathbf{9} + \mathbf{11} \\ &= e + e \\ &= e.\end{aligned}$$

$$\begin{aligned}\mathbf{1}+\mathbf{8}+\mathbf{3}+\mathbf{10}+\mathbf{7}+0 &= 0+\mathbf{1}+\mathbf{3}+\mathbf{7}+\mathbf{8}+\mathbf{10}\\ &= e+e\\ &= e.\end{aligned}$$

$$\begin{aligned}\mathbf{1}+\mathbf{8}+\mathbf{6}+\mathbf{13}+\mathbf{5}+\mathbf{12} &= \mathbf{5}+\mathbf{6}+\mathbf{8}+\mathbf{12}+\mathbf{3}+\mathbf{1}\\ &= e+e\\ &= e.\end{aligned}$$

$$\begin{aligned}\mathbf{2}+\mathbf{9}+\mathbf{3}+\mathbf{10}+\mathbf{5}+\mathbf{12} &= \mathbf{2}+\mathbf{3}+\mathbf{5}+\mathbf{9}+\mathbf{10}+\mathbf{12}\\ &= e+e\\ &= e.\end{aligned}$$

$$\begin{aligned}\mathbf{4}+\mathbf{11}+\mathbf{7}+0+\mathbf{5}+\mathbf{12} &= \mathbf{4}+\mathbf{5}+\mathbf{7}+\mathbf{11}+\mathbf{12}+0\\ &= e+e\\ &= e.\end{aligned}$$

$$\begin{aligned}\mathbf{4}+\mathbf{11}+\mathbf{3}+\mathbf{10}+\mathbf{6}+\mathbf{13} &= \mathbf{3}+\mathbf{4}+\mathbf{6}+\mathbf{10}+\mathbf{11}+\mathbf{13}\\ &= e+e\\ &= e.\end{aligned}$$

$$\begin{aligned}\mathbf{2}+\mathbf{9}+\mathbf{7}+0+\mathbf{6}+\mathbf{13} &= \mathbf{6}+\mathbf{7}+\mathbf{9}+\mathbf{13}+0+\mathbf{2}\\ &= e+e\\ &= e.\end{aligned}$$

Thus we have an image of the $7-$*point* Fano plane in G. That is to say, $C_3(14,1,3) \vDash_G C_3(7,1,3)$. Thus the configuration $C_3(14,1,3)$ is Fano-like.

□

This "group consequence" suggests that the minimal group rank for any group embedding of $C_3(14,1,3)$ is three. Here we show that this configuration can be realized in $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$. Indeed, this 64 element group is packed with four copies of $C_3(14,1,3)$, and along with one copy of the Fano plane, as well as the identity element. This was first observed by N.S. Mendelsohn in 1987, and is implicit in Theorem 2.2 of [27]. Note that the induced Fano plane *occurs only in the group* in which the $C_3(14,1,3)$ is embedded. We thank Dr. W. Kocay for pointing this out.

Theorem 8.1.3. *The non-zero elements of* $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ *can be packed with four copies of* $C_3(14,1,3)$ *and one copy of* $C_3(7,1,3)$

Proof. We exhibit the explicit mappings in Table 8.1 and Table 8.2.

Table 8.1: Mappings of $(0,1,3) \mod 14$.

$Point$	$Map1$	$Map2$	$Map3$	$Map4$
0	$(1,0,0)$	$(3,0,0)$	$(1,1,1)$	$(3,3,3)$
1	$(0,1,0)$	$(0,3,0)$	$(3,0,1)$	$(1,0,3)$
2	$(0,0,1)$	$(0,0,3)$	$(3,2,0)$	$(1,2,0)$
3	$(3,3,0)$	$(1,1,0)$	$(0,3,2)$	$(0,1,2)$
4	$(0,3,3)$	$(0,1,1)$	$(2,2,3)$	$(2,2,1)$
5	$(1,1,3)$	$(3,3,1)$	$(1,3,2)$	$(3,1,2)$
6	$(1,2,1)$	$(3,2,3)$	$(2,3,3)$	$(2,1,1)$
7	$(3,0,2)$	$(1,0,2)$	$(1,3,3)$	$(3,1,1)$
8	$(2,1,0)$	$(2,3,0)$	$(1,2,3)$	$(3,2,1)$
9	$(0,2,1)$	$(0,2,3)$	$(1,2,2)$	$(3,2,2)$
10	$(3,3,2)$	$(1,1,2)$	$(2,3,2)$	$(2,1,2)$
11	$(2,1,3)$	$(2,3,1)$	$(2,0,3)$	$(2,0,1)$
12	$(1,3,1)$	$(3,1,3)$	$(1,3,0)$	$(3,1,0)$
13	$(3,0,3)$	$(1,0,1)$	$(0,1,3)$	$(0,3,1)$

Table 8.2: Mappings of $(0,1,3) \mod 7$.

$Point$	Map
0	$(2,0,0)$
1	$(0,2,0)$
2	$(0,0,2)$
3	$(2,2,0)$
4	$(0,2,2)$
5	$(2,2,2)$
6	$(2,0,2)$

□

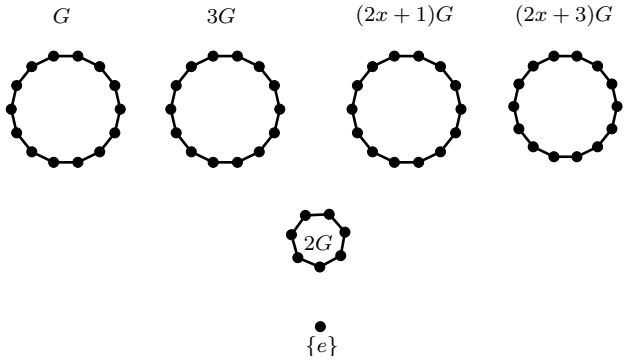

Figure 8.3: A coset partition of the factor ring $\mathbb{Z}_4[x]/(x^3+x+1)$ by the group $G =< x >$. The group G is easily verified to be the triples of $Map1$ in table 8.1 where the polynomial x is naturally the triple $(0,1,0)$. The group G is isomorphic to the cyclic group $\mathbb{Z}_{14}$.

8.2 Metelka's Observation

In 1985 V. Metelka [29] was able to construct a geometric realization of the $(12_4, 16_3)$(12 points each contained in 4 lines, and 16 lines each containing 3 points) given in figure 8.4 taken from [18].

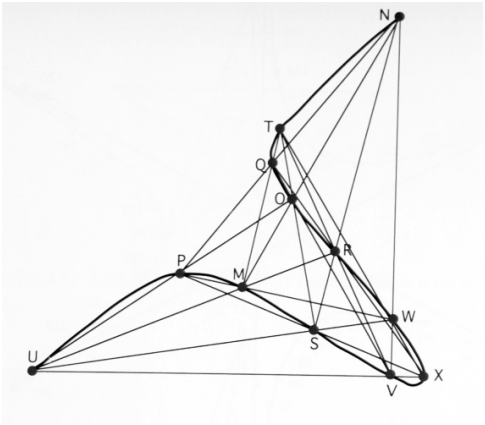

Figure 8.4: Metelka's configuration.

Metelka used a cubic curve to construct his realization, and to his dismay he discovered that his realization had 3 extra collinearities. In this section we show that these extra three collinearities are a group consequence. Metelka observed that in addition to the collinearities observed in Figure 8.4, that $\{N, T, U\}$, $\{O, R, W\}$, and $\{M, S, V\}$ were all collinear in his construction. Assuming that the labeling given in Figure 8.4 are the group elements of a group embedding, we have the following.

$$\begin{aligned} N &= -Q - P \\ &= (V + X) + (O + S) \\ &= (V + O) + (X + S) \\ &= -U - T. \end{aligned}$$

Thus, N, U, and T are collinear. The two other demonstrations are as follows.

$$\begin{aligned} O &= -S - T \\ &= (P + X) + (Q + M) \\ &= (X + Q) + (P + M) \\ &= -R - W. \end{aligned}$$

$$\begin{aligned} M &= -R - U \\ &= (Q + X) + (O + P) \\ &= (Q + O) + (X + P) \\ &= -V - S. \end{aligned}$$

This implies that O, R, and W are collinear, and also that M, V, and S are collinear, thus we have the following.

Theorem 8.2.1. *The* 16 *collinearities of Metelka's configuration(as defined in figure)* $\vDash_G$ *each set* $\{N, U, T\}$, $\{O, R, W\}$, $\{M, V, S\}$ *is a line.*

Chapter 9

Miscellaneous Examples

A geometric realization of the triangle-free configuration (17_3), taken from [1].

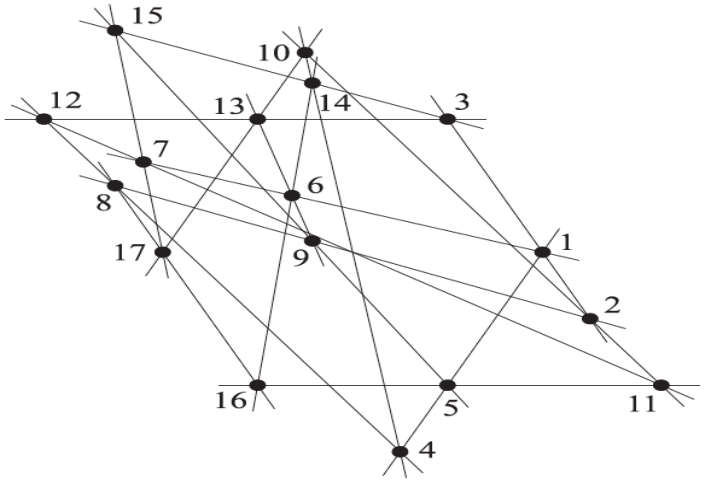

Figure 9.1: Non group realizable (17_3).

The triangle-free configuration (17_3) has lines given by the following triples:

1	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	10
2	4	6	8	10	12	14	8	10	9	11	9	14	11	15	16	13
3	5	7	9	11	13	15	12	14	15	16	13	16	12	17	17	17

Theorem 9.0.1. *The* (17_3) *above has no group realization.*

Proof. Let f be a group embedding of the (17_3) into an abelian group G. We have

$$\begin{aligned} f(1) &= -f(2) - f(3) \\ &= -f(2) + (f(12) + f(13)) \\ &= -f(2) + (f(12) - (f(17) + f(10))) \\ &= -f(17) + (f(12) - (f(2) + f(10))) \\ &= -f(17) + (f(12) + f(11)) \\ &= -f(12) - f(7) \\ &= f(15). \end{aligned}$$

Therefore in any group embedding of this (17_3), the two points 1, and 15 will be mapped onto the same group element and hence will not be an embedding.

□

9.1 Group Realizable $(n_5)'s$

The body of literature on (n_5) configurations is sparse. It has been shown by Gropp [16] that $\{0, 1, 4, 9, 11\}$ is a basis for a cyclic configuration for all $n \geq 23$. Additionally, Gropp [15] has noted that $\{0, 3, 4, 9, 11\}$ is a cyclic basis for all $n \geq 23$, and for $n = 21$. We begin by finding a group embedding of the cyclic configuration $C_5(24, 1, 4, 9, 11)$.

The resultant of $x^{11} + x^9 + x^4 + x + 1$ and the 24^{th} cyclotomic polynomial is $625 = 5^4$. This suggests that an embedding into the group of units of $\mathbb{Z}_5 \times \mathbb{Z}_5$ may be possible, provided a suitable irreducible quadratic exists. An examination of the factorizations of the Singer polynomial and the cyclotomic polynomial modulo 5 gives that $x^2 + 2x + 3$ is an irreducible factor of both polynomials modulo 5.

Then, letting $x^2 + 2x + 3 \equiv 0 \mod 5$, we have that $x^2 = 3x + 2$. So, letting $x^n = a_n x + b_n$ we have

$$\begin{aligned} x^{n+1} &= a_n x^2 + b_n x \\ &= a_n(3x + 2) + b_n x \\ &= (3a_n + b_n)x + 2a_n. \end{aligned}$$

Therefore,

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}.$$

Let $A = \begin{pmatrix} 3 & 1 \\ 2 & 0 \end{pmatrix}$, which is invertible modulo 5. Then it is straightforward to verify that

$$\begin{aligned} A^{12} &= \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \\ &= -I \mod 5 \end{aligned}$$

and,

$$\begin{aligned} A^{24} &= \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} \\ &= I \mod 5. \end{aligned}$$

Note also that both $A^2+2A+3I \equiv 0 \mod 5$, and $A^{11}+A^9+A^4+A+I \equiv 0 \mod 5$. It follows that the mapping $f : C_5(24, 1, 4, 9, 11) \to \mathbb{Z}_5 \times \mathbb{Z}_5$ given by $f : i \to A^i \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is a group embedding, and we have the following result.

Theorem 9.1.1. *The cyclic* (n_5) *configuration* $C_5(24, 1, 4, 9, 11)$ *is group realizable in* $\mathbb{Z}_5 \times \mathbb{Z}_5$.

With an analogous set of arguments the following results are established. Notice that $Resultant(x^{11} + x^9 + x^4 + x^3 + 1, c_{24}(x)) = 2^2 \cdot 11^2$. Since 24 divides 120, $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$ is a possible group for an embedding. Factoring $x^{11} + x^9+x^4+x^3+1$ modulo 11 furnishes us with a suitable irreducible polynomial

to construct the embedding. The companion matrix of $x^{11}+x^9+x^4+x^3+1$ is given by:

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

The matrix A defines the group embedding we seek, and we have the following result.

Theorem 9.1.2. *The cyclic* (n_5) *configuration* $C_5(24, 3, 4, 9, 11)$ *is group realizable in* $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$.

Applying the algorithm 3.4.3 to the Singer polynomial $x^{11}+x^9+x^4+x+1$ and $n = 23$ gives a group $\mathbb{Z}_{47}$ and base 17 for an embedding, and establishes the following result.

Theorem 9.1.3. *The cyclic* (n_6) *configuration* $C_6(23, 1, 4, 9, 11)$ *is group realizable in* $\mathbb{Z}_{47}$.

Theorem 9.1.4. *The cyclic* (n_5) *configuration* $C_5(21, 1, 4, 9, 11)$ *is group realizable in* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. The embedding matrix, A, is found by computing the companion matrix of $x^6+x^4+x^2+x+1$ modulo 2 (an irreducible factor of the associated Singer polynomial modulo 2).

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

□

$with(Student[LinearAlgebra])$:

$s := x^{11} + x^9 + x^4 + x^3 + 1$

$$s := x^{11} + x^9 + x^4 + x^3 + 1$$

$resultant(x^{11} + x^9 + x^4 + x^3 + 1,\ cyclotomic(21, x), x)$

$$4096$$

$Factor(s)\ \mathbf{mod}\ 2$

$$(x^3 + x^2 + 1)\ (x^2 + x + 1)\ (x^6 + x^4 + x^2 + x + 1)$$

$C := CompanionMatrix(x^6 + x^4 + x^2 + x + 1)\ \mathbf{mod}\ 2$

$$C := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$C^{21}\ \mathbf{mod}\ 2$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Figure 9.2: MAPLE calculations for the previous result.

9.2 Orchards as Groups

A $(p,t) - arrangement$ consists of p points and t (straight) lines in the euclidean (or in the real projective) plane chosen so that each line has exactly 3 points on it. The orchard problem is to find an arrangement with the greatest t for each given value of p. See [7].

9.2.1 The Orchard$(7,6)$ as a Group

In this section we give a group representation of the Orchard$(7,6)$ using cubic curves.

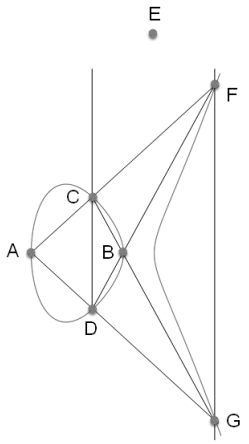

Figure 9.3: The cubic curve $y^2 = x^3 + 5x^2 + 4x$. The coordinates in the real plane are given by: $A = (-4,0), B = (-1,0), C = (-2,2), D = (-2,-2), F = (2,6), G = (2,-6)$, and $E = (0,1,0)$ being the point at infinity.

With the coordinatization in Figure 9.3 and testing the group order of each point we determine that the group formed by the points on the cubic is $\mathbb{Z}_2 \times \mathbb{Z}_4$. One representation of Orchard$(7,6)$ as $\mathbb{Z}_2 \times \mathbb{Z}_4$ is given in the following figure.

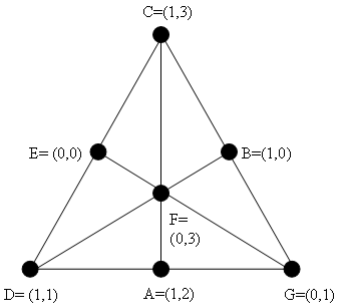

Figure 9.4: The Orchard $(7,6)$ embedded in the group $\mathbb{Z}_2 \times \mathbb{Z}_4$. The coordinates shown are group labels.

- $A + C + F = (1,2) + (0,3) + (1,3) = (0,0)$
- $A + D + G = (1,2) + (1,1) + (0,1) = (0,0)$
- $B + C + G = (1,0) + (1,3) + (0,1) = (0,0)$
- $B + D + F = (1,0) + (1,1) + (0,3) = (0,0)$
- $C + D + E = (1,3) + (1,1) + (0,0) = (0,0)$
- $E + F + G = (0,0) + (0,3) + (0,1) = (0,0)$

9.2.2 The Pappus Orchard as a Group

Figure 9.5 gives a realization of the Pappus $Orchard(9, 10)$ with 9 points and 10 lines realized in the cyclic group $\mathbb{Z}_9$. Three points P, Q, and R are collinear then $P + Q + R = 0$ in the group $\mathbb{Z}_9$.

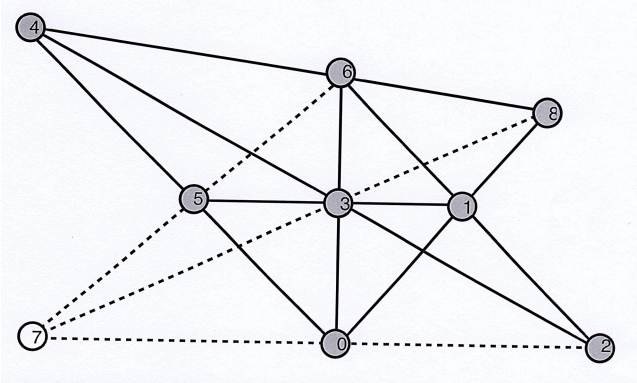

Figure 9.5: Orchard$(8, 7) \vDash$ Orchard$(9, 10)$ (the Pappus Orchard)

From the figure above (taken from [12]), it can be seen that the Orchard$(8, 7)$ is a subconfiguration of the Pappus Orchard$(9, 10)$. The deletion of the point labeled 7, and the dotted lines gives the Orchard$(8, 7)$.

Theorem 9.2.1. *Orchard*$(8, 7) \vDash_G$ *Orchard*$(9, 10)$.

Proof. Using the binary star operation we see that,

$$\begin{aligned} 6 * 5 &= (4 * 8) * (3 * 1) \\ &= (4 * 3) * (8 * 1) \\ &= 2 * 0 \end{aligned}$$

and also,

$$\begin{aligned} 3 * 8 &= (1 * 5) * (6 * 4) \\ &= (1 * 6) * (5 * 4) \\ &= 2 * 0. \end{aligned}$$

Therefore, the the three lines $[6, 5]$, $[3, 8]$, and $[2, 0]$ are concurrent in any group realization of Orchard$(8, 7)$. Alternatively, the Pappus Orchard$(9, 10)$ is the minimal group completion of the Orchard$(8, 7)$. Hence both the Pappus Orchard$(9, 10)$ and Orchard$(8, 7)$ are group realizable in $\mathbb{Z}_9$. See [7] page 398, figure 1, images (f) and (g).

□

9.2.3 A non-Group-Realizable Orchard

The Orchard$(11, 16)$ provides an example of a non-group-realizable orchard. Figure 9.6 is taken from [7].

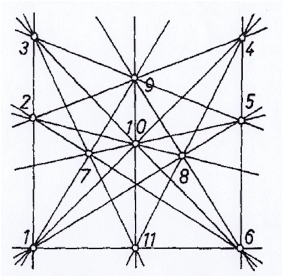

Figure 9.6: The non-group-realizable Orchard$(11, 16)$.

Theorem 9.2.2. *The Orchard*$(11, 16)$ *is not group realizable.*

Proof. Using Figure 9.6 as a guide, and employing the binary star operation we have the following.

$$\begin{aligned} 4 &= 1 * 10 \\ &= (2 * 3) * (7 * 5) \\ &= (2 * 7) * (3 * 5) \\ &= 6 * 9 \\ &= 8. \end{aligned}$$

Therefore $4 = 8$ in any group embedding of Orchard$(11, 16)$, and thus cannot be embedded in any group.

□

9.3 The Desargues configuration as a Group

The Desargues configuration($D(10_3)$) is one of the ten (10_3) configurations. It is non-cyclic, and as such the techniques from the previous chapters are not applicable. Instead we employ some basic algebra to derive an identity(similar to Theorem 7.4.1) which will point us in the right direction to find an appropriate group.

Theorem 9.3.1. *In any group embedding,* f*, of* $D(10_3)$*,* $2f(X) = 2f(Y)$ *for any two images* $f(X)$*, and* $f(Y)$*.*

Proof. Let triangle ABC, and triangle PQR be centrally perspective from a point O(as shown in figure 9.7). Then,

$$\begin{aligned} f(A) + f(A) &= -f(B) - f(W) - f(C) - f(V) \\ &= -f(B) - f(C) - f(W) - f(V) \\ &= f(U) + f(U). \end{aligned}$$

Similarly,

$$\begin{aligned} f(A) + f(A) &= -f(O) - f(P) - f(B) - f(W) \\ &= -f(O) - f(B) - f(P) - f(W) \\ &= f(Q) + f(Q). \end{aligned}$$

Also,

$$\begin{aligned} f(O) + f(O) &= -f(A) - f(P) - f(B) - f(Q) \\ &= -f(A) - f(B) - f(P) - f(Q) \\ &= f(W) + f(W). \end{aligned}$$

Thus by symmetry, we have $2f(X) = 2f(Y)$ for all ten points. To minimize the order of the embedded elements, set $2f(X) = e$, so that an abelian group with ten elements of order 2 would be a possible group to embed in. The labeling in Figure 9.7 (taken from [12]) provides an example of an embedding of $D(10_3)$ into $\mathbb{Z}_2^4$.

□

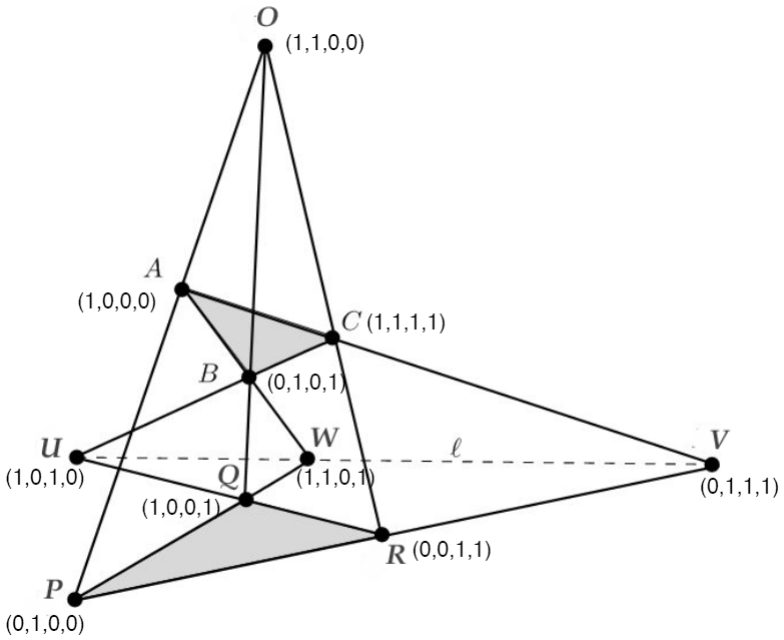

Figure 9.7: A group embedding of the Desargues configuration into $\mathbb{Z}_2^4$

9.4 The Cremona-Richmond Configuration

The Cremona-Richmond configuration($CRC(15_3)$) is a (15_3) configuration (see e.g. p. 329, the Book for a geometric realization in $\mathbb{R}^2$). Since $15 = \binom{6}{2}$, one fixes a 6-element set of labels, say $\{a, b, c, d, e, f\}$ and name the 15 points as ab, ac, bd etc. Here we show that this purely combinatorial description of the Cremona-Richmond configuration leads naturally to a group realization.

Let us take a typical line labelled by, say $(ab), (cd), (ef)$ where the six labels are to be chosen as natural numbers. Rename the three points on a typical line $\{ab, cd, ef\}$ as $\{a+b, c+d, e+f\}$. Now the sum of the three points is $a + b + c + d + e + f = k$, say. Another line with labels $\{(ad), (be), (cf)\}$ gets the label $\{a + d, b + e, c + f\}$ and the line-sum $a + d + b + e + c + f$ is still the same k. This is the idea. Now we need to choose proper values for the six elements (so that no name gets repeated) and convert this into an abelian group, and there are several ways. In what follows, we present one such group realization in the cyclic group $\mathbb{Z}_{30}$. Consistent with our theme, we use the group law on the cubic curve $y^2z = x^3 + 17z^3 \mod 29$ to get a group realization of this configuration.

The homogenous coordinates of the 15 points show that all these points lie on the cubic curve $y^2z = x^3 + 17z^3 \mod 29$. For example, $2^3 + 17 = 25 = 5^2$

Table 9.1: Group embedding of the $CRC(15_3)$.

Points in CRC	Homog. Coord. in $PG(2,29)$	Blocks in CRC	Homog Linear equns. of the Blocks
1	$(2,5,1)$	$[1,8,21]$	$3x+4y+3z=0$
6	$(4,20,1)$	$[1,9,20]$	$22x+13y+7z=0$
8	$(18,22,1)$	$[1,11,18]$	$x+26y+13z=0$
9	$(15,12,1)$	$[6,18,16]$	$27x+14y+18z=0$
11	$(28,4,1)$	$[6,9,15]$	$8x+11y+9z=0$
13	$(20,19,1)$	$[6,11,13]$	$16x+24y+7z=0$
15	$(17,0,1)$	$[8,25,27]$	$19x+9y+11z=0$
16	$(23,2,1)$	$[9,25,26]$	$9x+12y+11z=0$
18	$(12,18,1)$	$[11,24,25]$	$24x+5y+4z=0$
20	$(8,6,1)$	$[13,20,27]$	$13x+17y+26z=0$
21	$(15,17,1)$	$[13,21,26]$	$2x+24y+26z=0$
24	$(4,9,1)$	$[15,18,27]$	$11x+24y+16z=0$
25	$(27,3,1)$	$[15,21,24]$	$12x+27y+28z=0$
26	$(22,14,1)$	$[16,8,26]$	$13x+18y+13z=0$
27	$(6,28,1)$	$(16,20,24)$	$25x+14y+6z=0$

and hence the point 1 lies on the curve. Also the three points $1, 8, 21$ are collinear since they satisfy the homogenous linear equation $3x + 4y + 3z = 0$ mod 29. Since the three points lying on the cubic curve are collinear, their sum is zero under the group law i.e. $1+8+21 = 0 \mod 30$. Notice that this "+" is not the usual addition of integers, it is the group law on the cubic. However, we have chosen the notation in such a way that it agrees with the natural addition. That explains the non-standard naming of the points in the first column of the table. In fact, if we want just a group realization, then we can ignore the cubic curve aspect and the notation already gives the desired group embedding into the cyclic group $\mathbb{Z}_{30}$.

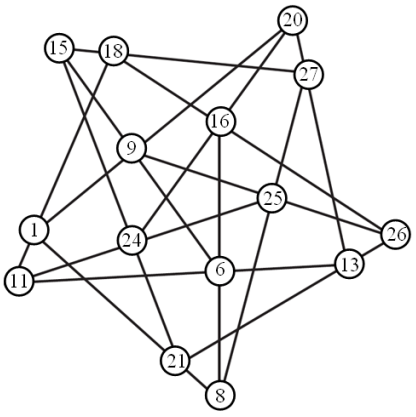

Figure 9.8: A group embedding of the Cremona-Richmond configuration $CRC(15_3)$ (taken from [18]), where $\{P, Q, R\}$ is a block in $CRC(15_3) \implies P + Q + R \equiv 0 \mod 30$.

Chapter 10

Further Works

Several additional unanswered questions naturally arose from the work done in this thesis. One such question(which was also pointed out by W. Kocay) is that of generating the geometric embedding of the group realizations of (n_3) configurations we obtained. Presently, we are not sure how to proceed from a group realization to a geometric realization, except that their existence in the plane is well-known.

The Sylvester-Gallai theorem states that given a finite number of points in the Euclidean plane, either all the points lie on a single line; or there is a line which contains exactly two of the points. The Möbius-Kantor configuration is an example of a configuration which violates the Sylvester-Gallai theorem. Indeed, the line joining any two points of the Möbius-Kantor configuration contain a third point of the configuration. The Sylvester-Gallai theorem can be seen as an obstruction to geometric realizability. In this thesis we

conjecture that if the minimal group realizing a cyclic (n_3) configuration is a direct product of more that two copies of $\mathbb{Z}_p$, for some prime $p \geq 2$, then the configuration cannot be realized over the real plane.

Based upon the results from chapter 4, we conjecture that for $n \geq 15$, the cyclic configuration $C(n, 1, 4, 6)$ is group realizable in a single cyclic group, and hence is geometrically realizable as ellipse-circle models. The proof may depend upon the validity of the Bunyakovski conjecture, which is widely believed to be true.

Additionally, in chapter 4 we show prove that if $PG(2, 3)$ exists in $PG(2, k)$ for some field $GF(k)$, then $3 = 0$ in $GF(k)$. This is of course a parallel of the folklore result for the Fano plane. We conjecture that if $PG(2, n)$ exists in $PG(2, k)$ for some field $GF(k)$, then $n = 0$ in $GF(k)$. Notice this is not true in affine planes: in this thesis we have shown that $AG(2, 3)$ exists in both $PG(2, 7)$, and in $PG(2, 13)$.

In chapter 6 we proved theorems 6.2.3, and 6.2.4 which establish conditions for the embeddability of cyclic configurations into single cyclic groups of prime power order. Interestingly, it appears that the third assumption that the first Hensel lifted value, r_1, have order $\phi(p^2)$ modulo p^2 is redundant. In each example we have generated the first Hensel lifted root turns out to be a primitive root modulo p^2.

Bibliography

[1] M. Boben, B. Grünbaum, T. Pisanski, A. Zitnik, *Small Triangle-Free Configurations of Points and Lines*, Discrete Comp. Geom. 35 (2006), no. 3, 405-427. 123

[2] J. Bokowski, Lars Schewe *There are no realizable* 15_4 *and* 16_4*-configurations* Rev. Roumaine Math. Pures Appl., 50 (56) (2005), pp. 483-493 45, 55

[3] J.Bokoski, L.Schewe, *On the finite set of missing geometric configurations* n_4, Comput. Geom. 46(2013), no. 5, 532-540. 45, 55, 56

[4] E. Brown, *The Many Names of (7,3,1)*, Mathematics Magazine 75 (April 2002), 83-94.

[5] E. Brown, *The Fabulous (11,5,2) Biplane*, Mathematics Magazine 77 (April 2004), 87-100.

[6] G. Brunel, Polygones autoinscrits. Proc. Verb. Sánces Soc. Sci. Phys. Nat. Bordeau, 1895/96, pp. 35-39. 16

[7] S.A Burr, B. Grunbaum, N.J. Sloan, The Orchard Problem, Geometriae Dedicata 2 (1974), 397-424. 129, 132

[8] David M. Burton, *Elementary Number Theory* 6th edition, McGraw Hill co. inc., Toronto, 2007. 84

[9] P.J. Cameron, *Combinatorics Topics Techniques Algorithms*, Cambridge University Press, 1994.

[10] C.J. Colbourn, J.H. Dinitz editors, *The CRC Handbook of Combinatorial Designs*, CRC Press Inc. 1996. ix, 109

[11] D. Cox, J. Little and D O'Shea, *Understanding Algebraic Geometry*, Springer-Verlag, 1998, page 72 5

[12] E.Ens, R.Padmanabhan, *Group Embeddings of the Projective Plane* $PG(2,3)$, Automated Reasoning and Mathematics, LNAI 7788, Springer Heidelberg, 2013. 59, 131, 134

[13] M. Fiedler, *A note on companion matrices*, Linear Algebra and its Applications, 372(2003), 325-331 7

[14] R.R. Fletcher, *Group Circle Systems on Conics*, Springer Proceedings in Mathematics and Statistics 90, Springer International (2014) 50, 52

[15] H. Gropp, *On the existence and nonexistence of configurations* n_k. J. Combinatorics, Information and System Science 15(1990), 34-38. 125

[16] H. Gropp, *Nonisomorphic configurations* n_k, Electronic Notes in Discrete Math. 27(2006), 43-44. 125

[17] B. Grünbaum, *Which* n_4 *Configurations Exist?*, Geombinatorics 9 (2000), no. 4, 164-169. 44

[18] B. Grünbaum, *Configurations of Points and Lines*, AMS Graduate Studies in Mathematics vol. 103, 2009.bg09 xii, 1, 8, 10, 16, 31, 44, 46, 62, 93, 120, 138

[19] N. Jolly *Constructing the primitive roots of prime powers*, arXiv:0809.2139v1 [math.HO],12 Sep 2008 88, 89

[20] D. Jungnickel, M.S. Abdul-Elah, M.W. Al-Dhahir, 8_3 *in* $PG(2, q)$, Arch. Math., Vol. 49, 141-150, 1987.dj.87 64, 69, 73

[21] Kelly, L. M. (1986), "A resolution of the SylvesterGallai problem of J. P. Serre", Discrete and Computational Geometry, 1 (1): 101104 10

[22] A.W. Knapp, *Elliptic Curves*,(MN-40), Volume 40, Princeton University Press (Oct. 25 1992). 11

[23] W. Kocay, *A* 10_3 *Configuration that is almost a Theorem* Bull. Inst. Comb. Appl. 68 (2013) 33-39 110

[24] E.E. Kummer *Über die Ergänzungssätze zu den allgemeinen Reciprocitäsgesetzen,* Journal für die reine und angewandte Mathematik 44(1852), 93-146. 83

[25] F. Lemmermeyer, *Conics, a poor man's elliptic curve*, arXiv:math/0311306. 50

[26] R.Lidl, H.Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1994 116-118. 57

[27] N.S. Mendelsohn, R. Padmanabhan, B.Wolk, *Designs Embeddable in Planar Cubic Curves*, Note di Matematica Vol. VII, 113-148,1987. nsm.87 10, 17, 20, 112, 118

[28] E. Merlin, *Sur les configurations planes* n_4. Bull. Cl. Sci. Acad. Roy. Belg. 1913, 647-660 55

[29] V. Metelka, *On Two Special Configurations* $(12_4, 16_3)$, [In Czech, with German and Russian summaries.] Časopis pro Pestovani Matematiky 110(1985), 351-355. [245+] 110, 120

[30] I. Niven, S. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, 5thEd., John Wiley and sons, New York, 1991. 88

[31] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag Undergraduate Texts in Mathematics, 1992. jhs.92 6, 10, 70

[32] J. Singer, *A Theorem in Finite Projective Geometry and Some Applications to Number Theory* Trans. Amer. Math. Soc., 43 (1938), 377385. 6

[33] L.C. Washington, *Elliptic Curves Number Theory and Cryptography*, 2ndEd., Chapman and Hall/CRC, Boca Raton, London, New York, 2008. 9

[34] R. Wilson, H. van Lint, *A Course in Combinatorics*, Cambridge university Press, 2001 57