PROPERTY D CYCLIC NEOFIELDS

by

SCOTT LACY

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

May 2015

Dedication

To my father, Jack Lacy, and to my grandmother, Irene Lacy. I miss you both more than I would otherwise dream possible.

Acknowledgements

I would like to thank my adviser, Minerva Cordero-Epperson, and my dissertation committee members Ruth Gornet, Dimitar Grantcharov, Guojun Liao, and Michaela Vancliff. I would also like to thank those who often served as mentors during my graduate studies: Theresa Jorgensen, Hristo Kojouharav, and Cecilia Levings. And I would especially like to thank Donald Keedwell for his encouragement and inspiration.

A special thanks to my family: my mother Patricia Ferguson, my brother Mark Lacy, my sister Heather Thompson and my nephew Gage Evans, who are forced by family ties to tolerate my antics for my entire life. My most sincere gratitude to those who tolerate my antics willingly, my friends: Dave and Penelope Brickell, Chris Kraft, Jeremy and Sharan Lambert, Amy Ottesen, Aaron and Kristal Potts, Andrea Russel, Ashley Russel, Thomas Seaquist, James Smith, Clancy Soehren, Garrison and Julie Sutton, and Eric Tausch.

Most of all, in loving memory, I would like to thank my father, Jack Lacy, who for me clearly defined being a man; my grandmother, Irene Lacy; who for me clearly defined being human; and my grandfather, Henry Ferguson, who served as a beacon for the many times my certainty wavered, to set me back on my course.

April 20, 2015

Abstract

PROPERTY D CYCLIC NEOFIELDS

Scott Lacy, PhD

The University of Texas at Arlington, 2015

Supervising Professor: Minerva Cordero-Epperson

In 1948 L. J. Paige introduced the notion of a neofield $(N,\oplus,\cdot)$ as a set N with two binary operations, generally referred to as addition ($\oplus$) and multiplication ($\cdot$) such that $(N,\oplus)$ is a loop with identity 0 and $(N-\{0\},\cdot)$ is a group, with both left and right distribution of multiplication over addition. The neofield was considered a generalization of a field and its application was for the coordinatizing of projective planes and related geometry problems. In 1967 A.D. Keedwell introduced the notion of property D cyclic neofields in relation to his study of latin squares and their application to projective geometry. In particular, the existence of a property D cyclic neofield guarantees the existence of a pair of orthogonal latin squares. Keedwell provides a theorem for the existence of property D cyclic neofields with a set of conditions on a sequence of integers.

We provide an alternate condition for Keedwell's existence theorem that requires only one criteria for each condition in contrast to Keedwell's two criteria.

We then establish a set of conditions for the existence of commutative property D cyclic neofields that require a sequence half as long as for Keedwell's existence theorem. We also examine subneofields of property D cyclic neofields and consider their application to extending known neofields to higher order property D cyclic neofields.

Table of Contents

List of Tables

Chapter 1

Introduction

In Chapter 2 we provide all the background material needed to introduce Keedwells existence theorem, which provides us with a powerful tool to determine the existence of a property D cyclic neofield by a set of conditions on a sequence of integers. In Chapter 3 we discuss commutative property D neofields. And in chapter 4 we examine subneofields.

Chapter 2

Background

Our goal in this chapter is to provide a foundation for introducing Keedwell's existence theorem which provides us a set of conditions for a sequence of integers to generate a property D cyclic neofield. We begin in section 1 by defining necessary structures with a single operation; namely a quasigroup, a loop, and a group, then finish the section by defining a neofield. In section 2 we discuss special mappings that determine if a group is what L. J. Paige refers to in [5] as an admissible group; meaning a group that may the multiplicative structure of a neofield. Then in section 3 we define what it means for a cyclic neofield to have property D and close with Keedwell's existence theorem.

2.1 Foundational Structures

In this section we introduce the basic algebraic structures necessary to define a property D cyclic neofield. Most mathematicians are familiar with the structure of a group. Typically a group is defined as a set with a closed binary operation on the set with the associative, identity and inverse properties. An early theorem in most abstract algebra texts is that equations in a group operation can be solved uniquely. By this we mean that if x plus y equals z, and we know any two of x, y or z, then we are able to solve for the third. In this dissertation we will define algebraic structures slightly differently.

Our most basic structure is a quasigroup. A quasigroup is a set with an operation such that it satisfies this "solvability" property. A finite quasigroup may be

commonly thought of as a latin square, or a square array with a set of elements represented distinctly on every row and every column. To find the result of an operation using the table (say $x \oplus y = z$), cross-reference the row of the first element x with the column of the second element y to find z. Furthermore, if say x and z are known, but not y, then use the row of x to find z, and it will be in the y column.

Quasigroups with additional properties define other algebraic structures. We introduce two of these in this section - loops and groups. We conclude the section by introducing the neofield. A neofield is an algebraic structure very similar to a field, except that the addition need not be associative, and the multiplication need not be commutative. Aside from the structural difference between them, the most notable difference between finite fields and finite neofields is their orders. Finite fields exist only for orders that are prime or a power of a prime, and a finite field of a given order is isomorphically unique for that order. Finite neofields exist for all orders and with the exception of very small orders, there are a great many for any particular order.

Definition 2.1. A *quasigroup* $(Q, \circ)$ is a nonempty set Q together with a binary operation $(\circ)$ on Q such that for all $a, b \in Q$ there exist unique $x, y \in Q$ such that

$$x \circ a = b \text{ and } a \circ y = b \text{ (\textit{unique solubility of equations})}$$

A finite quasigroup may be thought of as an $n \times n$ array with each element from a set of n elements represented uniquely on every row and every column of the array and where the entry in row a and column b corresponds to $a \circ b$. An array such as this is commonly called a *latin square*. A familiar example is the popular

Sudoku puzzle game with the numbers 1 through 9 represented on each row and each column. (Sudoku has a further restriction of numbers within boxes, not so with latin squares in general). Every completed Sudoku puzzle could be defined as the operation table for a quasigroup of nine elements. Example 2.2 is of a quasigroup of order three, while example 2.3 contrasts with a structure that is not a quasigroup.

Example 2.2. Table 2.1 below is an example operation $(\oplus)$ table on a quasigroup of three elements. In this example, a is a right-identity but there is no left-identity. The operation $(\oplus)$ is neither commutative (e.g. $a \oplus b = c$ yet $b \oplus a = b$) nor associative (e.g. $(b \oplus b) \oplus b = c$ yet $b \oplus (b \oplus b) = b$).

Table 2.1: Cayley table of a quasigroup with three elements

$\oplus$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Example 2.3. Table 2.2 below is an example operation $(*)$ table on a structure of three elements that is not a quasigroup. In this example, 1 is a two-sided identity. The operation $(*)$ is commutative but not associative (e.g. $(2*3)*3 = 1$, yet $2*(3*3) = 2$). More importantly, it does not have the property of unique solubility of equations (e.g. for $3*x = 3$, x could be either 1 or 2).

Table 2.2: Cayley table of a structure with three elements that is not a quasigroup

$*$	1	2	3
1	1	2	3
2	2	1	3
3	3	3	1

Definition 2.4. A *loop* $(Q, \circ)$ is a quasigroup with an element $e \in Q$ such that,

$$\text{for all } a \in Q,\ a \circ e = a = e \circ a \text{ (existence of a two-sided identity)}$$

Example 2.5. Table 2.3 below is an example operation $(\oplus)$ table on a loop of five elements. In this example, 1 is a two-sided identity. The operation $\oplus$ is neither commutative (e.g. $2 \oplus 3 = 5$ yet $3 \oplus 2 = 4$) nor associative (e.g. $(2 \oplus 3) \oplus 4 = 2$ yet $2 \oplus (3 \oplus 4) = 4$).

Table 2.3: Cayley table of a loop with five elements

$\oplus$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

Definition 2.6. A *group* $(G, \circ)$ is a quasigroup such that, for all $a, b, c \in G$,

$$a \circ (b \circ c) = (a \circ b) \circ c \text{ (associative property)}$$

Groups are typically defined by the properties of associativity, identity and inverses. We define a group differently, but these properties still hold for our definition.

Recall that a group $(G, \circ)$ has the following properties:

1. there exists an element $e \in G$ such that, for all $a \in G$,
   $a \circ e = a = e \circ a$ (existence of a two-sided identity)

2. for all $a \in G$ there exists an element $a^{-1} \in G$ such that
   $a^{-1} \circ a = e = a \circ a^{-1}$ (existence of a two-sided inverse)

Verifying this is straightforward, and since it quite nicely demonstrates use of the unique solubility of equations property, it is included here for illustration purposes.

Proof. (1) Let $a, b \in G$. By unique solubility of equations in G, there exists $e, c \in G$ such that $e \circ a = a$ and $a \circ c = b$. Then $e \circ b = e \circ (a \circ c) = (e \circ a) \circ c = a \circ c = b$. Since b is arbitrary, e is a left identity for all elements in G. Similarly, by unique solubility of equations in G, there exists $e_r, d \in G$ such that $a \circ e_r = a$ and $d \circ a = b$. Then $b \circ e_r = (d \circ a) \circ e_r = d \circ (a \circ e_r) = d \circ a = b$. So e_r is a right identity for all elements in G. Also, because e is a left identity and e_r is a right identity, $e = e \circ e_r = e_r$. Thus, e is a two-sided identity for all elements of G.

(2) Let $a \in G$. By unique solubility of equations in G, there exists an element $a^{-1} \in G$ such that $a^{-1} \circ a = e$. Then $(a \circ a^{-1}) \circ a = a \circ (a^{-1} \circ a) = a \circ e = a$, which implies $a \circ a^{-1} = e$ and therefore $a^{-1}$is a two-sided inverse.

Modern cryptography is often based on finite fields. A field is usually defined as a set with two binary operations and a distribution relation between them. A corresponding structure for non-associative algebra is the neofield. There are potentially

many advantages to neofields over fields, not least of which is the vastly numerous neofields for any particular order, compared to the unique field for order p^k where p is prime.

Definition 2.7. A *left neofield* $(N, \oplus, \cdot)$ is a set N together with two binary operations $(\oplus)$ and $(\cdot)$ on N such that $(N, \oplus)$ is a loop, $(N - \{0\}, \cdot)$ (where 0 is the identity of $(N, \oplus)$) is a group, and for all $a, b, c \in N$, $a \cdot (b \oplus c) = (a \cdot b) \oplus (a \cdot c)$ (left distribution). If $(\cdot)$ also distributes from the right, then N is a *neofield*.

Often we will require the multiplicative group for the neofield to be cyclic. These neofields have special properties and so we distinguish them.

Remark 2.8. A *cyclic neofield* is a neofield such that the multiplicative group is cyclic.

Example 2.9. Table 2.4 below is an example of a cyclic neofield of order 6. The operation $(\oplus)$ defines a proper loop; It has an identity (x^0), has unique solubility of equations, and is neither commutative nor associative. The operation $(\cdot)$ with the non-zero elements defines a group isomorphic to $\mathbb{Z}_5$.

Table 2.4: Cayley tables of a cyclic neofield with six elements

$\oplus$	0	x^0	x^1	x^2	x^3	x^4
0	0	x^0	x^1	x^2	x^3	x^4
x^0	x^0	0	x^4	x^3	x^2	x^1
x^1	x^1	x^2	0	x^0	x^4	x^3
x^2	x^2	x^4	x^3	0	x^1	x^0
x^3	x^3	x^1	x^0	x^4	0	x^2
x^4	x^4	x^3	x^2	x^1	x^0	0

$\cdot$	0	x^0	x^1	x^2	x^3	x^4
0	0	0	0	0	0	0
x^0	0	x^0	x^1	x^2	x^3	x^4
x^1	0	x^1	x^2	x^3	x^4	x^0
x^2	0	x^2	x^3	x^4	x^0	x^1
x^3	0	x^3	x^4	x^0	x^1	x^2
x^4	0	x^4	x^0	x^1	x^2	x^3

Remark. A neofield without associativity will be said to be a *proper neofield*.

2.2 Orthomorphisms and Near-Orthomorphisms

Groups are well known structures and less numerous than loops, so it may be natural to wonder if there is a process by which one may examine a group to determine if it forms the multiplicative structure of a neofield. In [5] L. J. Paige named any such group an *admissible group* and proved that any finite abelian group and any finite group of odd order are admissible, as well as several less general results.

Definition 2.10. Let $(G,\cdot)$ be a group. If the mapping $\theta : G \to G$ is a bijection and the mapping $\phi : G \to G$ given by $\phi(g) = g \cdot \theta(g)$ is also a bijection, then ϕ is called an *orthomorphism* and θ is called the *complete mapping* associated with ϕ. If $\phi(1) = 1$ where 1 is the identity in G, then ϕ is said to be in *canonical form*.

Example 2.11. Let $G = \langle x \rangle, x^5 = x^0$ and $\theta = (x^0)(x^1x^3x^4x^2)$. Then $\phi = g \cdot \theta(g) = (x^0)(x^1x^4)(x^2x^3)$. Both θ and ϕ are bijections of G, and so ϕ is an orthomorphism of G (in canonical form because $\phi(x^0) = x^0$) and θ is the complete mapping associated with ϕ.

Definition 2.12. Let $(G,\cdot)$ be a group and $\eta, \iota \in G, \eta \neq \iota$. If the mapping $\theta : G - \{\eta\} \to G - \{\iota\}$ is a bijection and the mapping $\phi : G - \{\eta\} \to G - \{\iota\}$ given by $\phi(g) = g \cdot \theta(g)$ is also a bijection, then ϕ is called a *near-orthomorphism* and θ is called the *near-complete mapping* associated with ϕ. If $\iota = 1$ where 1 is the identity in G, then ϕ is said to be in *canonical form*. The element η with no image under these mappings is called the *ex-domain element.*

Example 2.13. Let $G = \langle x \rangle, x^6 = x^0$and $\theta = [x^0x^4x^1x^2x^5x^3]$ (meaning x^0 maps to x^4, etc, while $\theta(x^3)$ has no image and x^0 has no pre-image). Then $\phi = [x^0x^4x^5x^2x^1x^3]$.

Both θ and ϕ are bijections of $G - \{x^3\} \to G - \{x^0\}$, and so ϕ is a near-orthomorphism of G (in canonical form because x^0 has no pre-image) with ex-domain element x^3, and θ is the near-complete mapping associated with ϕ.

Before we draw the connection between orthomorphisms/near-orthomorphisms and neofields, it's beneficial for us to make an observation using the properties of a neofield. If we think of a neofield in terms of its operation tables, we may notice a peculiar pattern emerge in the additive loop. In particular, it is apparent that there is an "order" to the diagonals for all non-zero elements. In the additive loop table from example 2.9 we see that the diagonal directly above the main diagonal has the values x^4, x^0, x^1, x^2. If we then "wrap around" back to the left side of the table, the next value is x^3. Examining the next diagonal above that, we have x^3, x^4, x^0 followed by x^1, x^2 after "wrapping around" back to the left hand side. The ascending order of exponents (modulo n) in the diagonals of an addition table of a cyclic neofield is no coincidence. In fact, for any left neofield, by applying the left distributive property we have that $x \oplus y = x \cdot (1 \oplus x^{-1} \cdot y)$ for all $x \neq 0$. For example, in the neofield from example 2.9 we have that $x^2 \oplus x^4 = x^2 \cdot (x^0 \oplus x^2) = x^2 \cdot x^3 = x^0$.

At first this may seem like an extra step over simply referencing the table, what it ultimately means is that we may exploit this phenomenon to store the entire additive loop table in single row. Using this fact, for any calculation we may "factor out" an appropriate element then reference our chosen row. This could be almost any row, but it is most convenient to choose the row of the multiplicative identity and "factor out" the first element of the equation.

Definition 2.14. Let $(N, \oplus, \cdot)$ be a left neofield. A *presentation function* is a mapping $\psi : N \to N$ given by $\psi(g) = 1 \oplus g$.

In short, the presentation function (along with defining $0 \oplus a = a$ for all $a \in N$) determines the complete addition table.

Theorem 2.15. (A.D. Keedwell) *Let $(N, \oplus, \cdot)$ be a finite left neofield. If $1 \oplus 1 = 0$ in N, then N defines an orthomorphism of $(N - \{0\}, \cdot)$ in canonical form. If for $\eta \neq 1$, $1 \oplus \eta = 0$, then N defines a near orthomorphism of $(N - \{0\}, \cdot)$ in canonical form with η as ex-domain element. Conversely, let $(N - \{0\}, \cdot)$ be a finite group with identity 1 and $N - \{0\}$ possess an orthomorphism ϕ in canonical form. Then $(N, \oplus, \cdot)$ is a left neofield with presentation function ψ defined by $\psi(0) = 1$, $\psi(1) = 0$ and $\psi(g) = \phi(g)$ for all $g \neq 0, 1$. Alternately, let $N - \{0\}$ possess a near orthomorphism in canonical form. Then $(N, \oplus, \cdot)$ is a left neofield with presentation function ψ defined by $\psi(0) = 1$, $\psi(\eta) = 0$ and $\psi(g) = \phi(g)$ for all $g \neq 0, \eta$ where η is the ex-domain element of ϕ.*

Example 2.16. The neofield presented in example 2.9 has presentation function $\psi = (x^0 0)(x^1 x^4)(x^2 x^3)$ in disjoint cycle form. Using theorem 2.15 we have $\phi = (x^0)(x^1 x^4)(x^2 x^3)$ and $\theta = (x^0)(x^1 x^3 x^4 x^2)$ which we see in example 2.11 as an orthomorphism and complete mapping. Conversely, the orthomorphism from example 2.11 can be used to define the presentation function for the neofield in example 2.9.

Example 2.17. The near-orthomorphism from example 2.13 can be used to define the presentation function $\psi = (x^0 x^4 x^5 x^2 x^1 x^3 0)$ of a cyclic neofield of order 7.

For the remainder of this dissertation, we will be almost exclusively concerned with cyclic neofields. It is therefore beneficial for us to establish that when the multiplicative group is cyclic (more generally, commutative), then the neofield has

both left and right distribution.

Remark 2.18. Let $(N, \oplus, \cdot)$ be a left neofield with $a \cdot b = b \cdot a$ for all $a, b \in N$. Then N is a neofield.

Searching through potential candidates for orthomorphisms and near-orthomorphisms quickly becomes a large computational problem. The following two observations eliminate certain combinations from these searches.

Remark 2.19. Let $(G, \cdot)$ be a group with $a \cdot b = b \cdot a$ for all $a, b \in G$ and $\theta : G \to G$ be a bijective mapping with a 2-length cycle. Then $\phi : G \to G$ given by $\phi(g) = g \cdot \theta(g)$ is not a bijective mapping.

Proof. Let $(g_1 g_2)$ be a 2-length cycle in θ. Then $\phi(g_1) = g_1 \cdot \theta(g_1) = g_1 \cdot g_2 = g_2 \cdot g_1 = g_2 \cdot \theta(g_2) = \phi(g_2)$. Therefore ϕ is not a bijective mapping.

Remark 2.20. Let $(G, \cdot)$ be a group and $\theta : G \to G$ be a bijective mapping. If $\theta(a) = a^{-1}$ for some $a \neq 1 \in G$ then $\phi : G \to G$ given by $\phi(g) = g \cdot \theta(g)$ is not an orthomorphism in canonical form.

Proof. $\phi(a) = a \cdot \theta(a) = a \cdot a^{-1} = 1$. If ϕ is in canonical form, then $\phi(1) = 1$ and so ϕ is not a bijection.

2.3 Property D Cyclic Neofields

A primary goal for Paige in studying neofields was in the hope of providing another structure for coordinatizing projective planes. He was partially successful in this endeavor, but not to the extent that he had hoped. Given that neofields exist for all orders and the vast number that exist for any order, he hoped to find at least one example of a coordinatizing structure that was not an order of a prime power. Keedwell had similar ambitions, but approached the subject from the study of orthogonal latin squares.

It is proven that a projective plane of order n exists if and only if there exists n mutually orthogonal latin squares of order n. Thus if one shows that no pair of orthogonal latin squares exist for an order (as is the case for order 6), then no projective plane of that order exists. It is an open question whether there exists a pair of orthogonal latin squares for every order beyond 6. However, Keedwell defines a special type of neofield (named property D) and establishes [2] that the existence of a property D cyclic neofield of some order guarantees the existence of a pair of orthogonal latin squares of that order.

Definition 2.21. A cyclic neofield (of order $m = n+1$) based on the multiplicative cyclic group $\langle x \rangle$ where $x^0 = 1$ is the multiplicative identity, is said to have *property D* if

$$(1 \oplus x^{r+1})/(1 \oplus x^r) = (1 \oplus x^{s+1})/(1 \oplus x^s) \iff r \equiv s \text{ modulo } n,$$

where r, s are any positive integers.

In terms of a presentation function as a row of the addition table of a cyclic neofield, this means that the differences in exponents between consecutive elements in the row are unique. The following example from our familiar example 2.9 shows a case where they are not.

Table 2.5: Presentation function in row form for a cyclic neofield with six elements

$\oplus$	0	x^0	x^1	x^2	x^3	x^4
x^0	x^0	0	x^4	x^3	x^2	x^1

Example 2.22. Table 2.5 is a presentation function in row form for the cyclic neofield in example 2.9 above. Notice that the differences in the exponents of each

consecutive element are all the same (i.e.-1), so this cyclic neofield does not have property D. (More specifically, let us choose r and s, say $r = 1, s = 3$, then $(x^0 \oplus x^{r+1})/(x^0 \oplus x^r) = (x^0 \oplus x^2)/(x^0 \oplus x^1) = (x^0 \oplus x^2) \cdot (x^0 \oplus x^1)^{-1} = x^3 \cdot x^{-4} = x^4$ and $(x^0 \oplus x^{s+1})/(x^0 \oplus x^s) = (x^0 \oplus x^4)/(x^0 \oplus x^3) = (x^0 \oplus x^4) \cdot (x^0 \oplus x^3)^{-1} = x^1 \cdot x^{-2} = x^4$ are equal, while r and s are not.)

Table 2.6: Presentation function in row form for a cyclic neofield with seven elements

$\oplus$	0	x^0	x^1	x^2	x^3	x^4	x^5
x^0	x^0	x^4	x^3	x^1	0	x^5	x^2

Example 2.23. Table 2.6 is a presentation function in row form for the cyclic neofield in example 2.17 above. This cyclic neofield has property D.

Theorem 2.24. *(Keedwell's Existence Theorem) A necessary and sufficient set of conditions for a cyclic neofield of order $m = n+1$ to exist is that $n-2$ (not necessarily distinct) residues modulo n from the set $\{2,3,...,n-1\}$ can be arranged in a sequence P such that:*

(i) *the partial sums of the first one, two, ... , $n-2$ terms are all distinct and non-zero modulo n; and*

(ii) *when each term of the sequence is reduced by one, the new sequence, P' say, also satisfies (i).*

Furthermore, the cyclic neofield has property D if and only if the terms of P are all distinct.

Definition 2.25. An *acceptable sequence* is a sequence as described above that meets criteria (i) and (ii), *and* such that all terms are distinct.

Below are two applications of Keedwell's existence theorem. The first example is a sequence that generates a cyclic neofield that does not have property D; notice that the terms of the sequence P in this example are not distinct. The second example is a sequence that generates a cyclic neofield that does have property D, and all the terms in this sequence are distinct.

Example 2.26. Let $n = 7$ and $P = \{2,2,2,2,2\}$. Let S be the sequence of partial sums (modulo n) of P and S' be the sequence of partial sums (modulo n) of P'. Then $S = \{2,4,6,1,3\}$. All elements of S are distinct and non-zero, thus condition (i) is met. $P' = \{1,1,1,1,1\}$ and so $S' = \{1,2,3,4,5\}$. All elements of S' are distinct and non-zero, thus condition (ii) is met. So the sequence P generates a cyclic neofield of order 8. More generally, for any odd-valued n, a sequence of 2's will generate a cyclic neofield. Similarly, for an even-valued n, a sequence of 2's with a 3 in the $\frac{n}{2}$th position will achieve the same result. In this way, a cyclic neofield of any order may be generated.

Example 2.27. Let $n = 7$ and $P = \{3,2,4,6,5\}$. Then:

$$P = \{3,2,4,6,5\}, \qquad S = \{3,5,2,1,6\}$$

$$P' = \{2,1,3,5,4\}, \qquad S' = \{2,3,6,4,1\}$$

All elements of S and S' are distinct and non-zero, thus conditions (i) and (ii) are met respectively. All elements of P are distinct, so the neofield generated by P is a property D cyclic neofield of order 8. Notice that the neofield generated by P is the finite field $GF(8)$.

Chapter 3

Commutative Property D Cyclic Neofields

Keedwell's existence theorem provides an incredibly useful tool for classifying property D cyclic neofields by correlating the additive structure of the neofield to a sequence of integers and applying conditions on the sequence. In the first part of this chapter we provide an alternate condition to this theorem and in the second we provide a set of conditions for an abbreviated sequence to classify commutative property D cyclic neofields.

3.1 An Alternate Condition to Keedwell's Existence Theorem

The existence of a property D cyclic neofield guarantees the existence of a pair of mutually orthogonal latin squares. Much of Keedwell's work is based on latin squares and many of his proofs involve the use of arrays. In contrast, working with sequences to generate property D cyclic neofields, the following fact becomes apparent. Condition (i) of Keedwell's Existence Theorem requires that all values in the sequence of partial sums (S) be non-zero and *distinct* modulo n. If two values in the sequence are identical, then the sum of the values *between* them must then be equal to 0 modulo n. It is therefore possible to alter condition (i) in Keedwell's Existence Theorem with the following lemma.

Lemma 3.1. *An alternate condition to condition* (i) *of Keedwell's existence theorem is*

(iii) *the sum of every subsequence of consecutive elements (hereafter simply referred to as a subsequence) of P is non-zero modulo n.*

Proof. Let $P = \{p_1, p_2, ..., p_{n-2}\}$ be a sequence, $S = \{s_1, s_2, ..., s_{n-2}\}$ be the sequence of partial sums, $P_{\iota,\kappa} = \{p_{\iota+1}, p_{\iota+2}, ..., p_{\iota+\kappa}\}$ be a subsequence of κ consecutive elements of P and $\sum_{P_{\iota,\kappa}}$ be the sum of all elements in $P_{\iota,\kappa}$ modulo n.

(i) implies (iii) : Let P satisfy condition (i). If $\iota = 0$, then $\sum_{P_{\iota,\kappa}} = s_\kappa$ is non-zero. Otherwise, $s_{\iota+\kappa} = s_\iota + \sum_{P_{\iota,\kappa}}$ and since $s_{\iota+\kappa} \neq s_\iota$ by condition (i), $\sum_{P_{i,k}}$ is non-zero. Therefore, every subsequence of P is non-zero satisfying condition (iii).

(iii) implies (i): Let P satisfy condition (iii). Then $s_k = \sum_{P_{0,k}}$ is non-zero and so all elements of S are non-zero. Also, for $s_i, s_j \in S$ with $i < j$, let $k = j - i$ so $s_j = s_i + \sum_{P_{i,k}}$ and since $\sum_{P_{i,k}}$ is non-zero, $s_i \neq s_j$. So all elements of S are distinct. Therefore, all elements of S are distinct and non-zero satisfying condition (i).

Remark 3.2. A sequence of distinct elements as described in Keedwell's existence theorem that meets condition (ii) of the theorem and condition (iii) of lemma 3.1 is an acceptable sequence.

Example 3.3. In light of this lemma, it is easy to see that no property D cyclic neofield of order 6 exists. Let $n = 5$, then the sequence P must be an arrangement from the set $\{2,3,4\}$. The subsequence $\{2,3\}$ has a sum of zero, and there is no arrangement where this subsequence does not occur in either P or P'. This is a direct corollary to Euler's famous thirty-six officer problem.

Many of Keedwell's results may now be proven using this lemma, in some cases elegantly and with surprisingly short proofs. Of special importance to us are two acceptable sequences derived directly from an acceptable sequence.

Definition 3.4. Given a sequence $P = \{p_1, p_2, ..., p_{n-2}\}$, the *mirror sequence* is the sequence $P^M = \{p_{n-2}, p_{n-3}, ..., p_1\}$.

The mirror sequence is simply the sequence P in reverse.

Definition 3.5. Given a sequence $P = \{p_1, p_2, ..., p_{n-2}\}$, the *dual sequence* is the sequence $P^D = \{n+1-p_1, n+1-p_2, ..., n+1-p_{n-2}\}$.

In Keedwell's existence theorem we define a sequence P of terms from the set $\{2, 3, ..., n-1\}$ and an alteration P' by subtracting one from the value of each term in the sequence P. Keedwell could just as easily have defined P from the set $\{1, 2, ..., n-2\}$ and P' by adding one to each value. The theorem itself would be functionally identical. (In practice, this would then require using P' to build the neofield, illustrating a probable reason for Keedwell choosing the method he did). Also note that modular arithmetic applies just as readily to negative values as it does to positive, especially when considering that we are mostly concerned with whether the sum of a subsequence is zero or not. With these two ideas, if we consider the dual sequence of P to be the negative of P', then we get a very good idea of why the dual sequence of an acceptable sequence is also acceptable. The following two propositions originally proved by Keedwell in [2], here use lemma 3.1 to prove our claim that these two sequences are acceptable.

Proposition 3.6. *If a sequence is acceptable, then the mirror sequence is acceptable.*

Proof. Let P be an acceptable sequence. Then the sum of every subsequence of P (and P') is non-zero. Since the sum of every subsequence of P^M and P'^M is equal to the sum of a subsequence of P and P' respectively, then the sum of every subsequence of P^M and P'^M is also non-zero. Therefore, P^M is an acceptable sequence.

Example 3.7. Let $n = 11$ and $P = \{3,5,4,6,2,7,10,9,8\}$. Then:

$$P = \{3,5,4,6,2,7,10,9,8\}, \qquad S = \{3,8,1,7,9,5,4,2,10\}$$

$$P' = \{2,4,3,5,1,6,9,8,7\}, \qquad S' = \{2,6,9,3,4,10,8,5,1\}$$

P generates a property D neofield of order 12.

The sequence $P^M = \{8,9,10,7,2,6,4,5,3\}$ with:

$$P^M = \{8,9,10,7,2,6,4,5,3\}, \qquad S^M = \{8,6,5,1,3,9,2,7,10\}$$

$$P'^M = \{7,8,9,6,1,5,3,4,2\}, \qquad S'^M = \{7,4,2,8,9,3,6,10,1\}$$

also generates a property D neofield of order 12.

The property D cyclic neofields generated by P and P^M are isomorphic [3] by mapping an element to its multiplicative inverse.

Proposition 3.8. *If a sequence is acceptable, then the dual sequence is acceptable.*

Proof. Let P be an acceptable sequence. Then the sum of every subsequence $P_{\iota,\kappa} = \{p_{\iota+1}, p_{\iota+2}, ..., p_{\iota+\kappa}\}$ of P and $P'_{\iota,\kappa} = \{p_{\iota+1} - 1, p_{\iota+2} - 1, ..., p_{\iota+\kappa} - 1\}$ of P' is non-zero. Assume by contradiction that the sum of a subsequence $P^D_{\iota,\kappa} = \{n + 1 - p_{\iota+1}, n + 1 - p_{\iota+2}, ..., n + 1 - p_{\iota+\kappa}\}$ of P^D or $P'^D_{\iota,\kappa} = \{n - p_{\iota+1}, n - p_{\iota+2}, ..., n - p_{\iota+\kappa}\}$ of P'^D is zero. Then $\sum_{P^D_{\iota,\kappa}} = (n + 1 - p_{\iota+1}) + (n + 1 - p_{\iota+2}) + ... + (n + 1 - p_{\iota+\kappa}) = \kappa n + \kappa - (p_{\iota+1} + p_{\iota+2} + ... + p_{\iota+\kappa}) \equiv \kappa - \sum_{P_{\iota,\kappa}} = 0$ or $\sum_{P'^D_{\iota,\kappa}} = (n - p_{\iota+1}) + (n - p_{\iota+2}) + ... + (n - p_{\iota+\kappa}) = \kappa n - (p_{\iota+1} + p_{\iota+2} + ... + p_{\iota+\kappa}) \equiv \sum_{P_{\iota,\kappa}} = 0$. Clearly $\sum_{P_{\iota,\kappa}} \neq 0$ and so $\sum_{P_{\iota,\kappa}} = \kappa$. However, $\sum_{P'_{\iota,\kappa}} = (p_{\iota+1} - 1) + (p_{\iota+2} - 1) + ... + (p_{\iota+\kappa} - 1) = (p_{\iota+1} + p_{\iota+2} + ... + p_{\iota+\kappa}) - \kappa = \sum_{P_{\iota,\kappa}} - \kappa \neq 0$ implies that $\sum_{P_{\iota,\kappa}} \neq \kappa$

which leads to our contradiction. Therefore, every subsequence of P^D and P'^D is non-zero and P^D is an acceptable sequence.

Example 3.9. Using the same sequence as in example 3.7, let $n = 11$ and $P = \{3,5,4,6,2,7,10,9,8\}$. Then the sequence $P^D = \{9,7,8,6,10,5,2,3,4\}$ with:

$$P^D = \{9,7,8,6,10,5,2,3,4\}, \qquad S^D = \{9,5,2,8,7,1,3,6,10\}$$

$$P'^D = \{8,6,7,5,9,4,1,2,3\}, \qquad S'^D = \{8,3,10,4,2,6,7,9,1\}$$

also generates a property D cyclic neofield of order 12.

The property D cyclic neofields generated by P and P^D are isomorphic if they are commutative and anti-isomorphic if they are not commutative [3]. The following result gives an important relationship between the dual and mirror sequences and commutativity. It was first proven by Keedwell in [2]; below we provide a proof using lemma 3.1.

Theorem 3.10. *If $P = \{p_1, p_2, ...p_{n-2}\}$ is an acceptable sequence generating a property D cyclic neofield N, then $P^M = P^D$ if and only if N is commutative.*

Proof. Note that $P^M = P^D \Leftrightarrow p_i = n+1-p_{n-i-1} \Leftrightarrow p_i + p_{n-i-1} = n+1$.

Let $S = \{s_1, s_2, ..., s_{n-2}\}$ be the sequence of partial sums of P. By definition, $0 \oplus \alpha = \alpha = \alpha \oplus 0$ and so 0 commutes with all elements of N for any neofield N. By construction of a cyclic neofield [**?**] $x^0 \oplus x^h = 0$, $x^0 \oplus x^{h+1} = x^{a_{01}}$ and $x^0 \oplus x^{h+i+1} = x^{a_{01}+s_i}$. Then $x^{h+i+1} \oplus x^0 = x^{h+i+1}(x^0 \oplus x^{h+(n-i-2)+1}) = x^{a_{01}+s_{n-i-2}+h+i+1}$.

Let P be an acceptable sequence generating N where $P^M = P^D$. For non-zero $x^a, x^b \in N$, $x^a \oplus x^b = x^a(x^0 \oplus x^{b-a})$ and $x^b \oplus x^a = x^a(x^{b-a} \oplus x^0)$, so we need only show that x^0 commutes with all non-zero elements of N. Observe that for any acceptable sequence, $s_{n-2} = n-h-1$. Also, when $P^M = P^D$, $\sum_{k=1}^{i} p_k + \sum_{k=n-i-1}^{n-2} p_k =$

$i(n+1)$. Then we have $s_{n-i-2} = s_{n-2} - \sum_{k=n-i-1}^{n-2} p_k = s_{n-2} + \sum_{k=1}^{i} p_k - i(n+1) = n-h-1+s_i-i$. Thus, $s_i = s_{n-i-2} + h + i + 1$. Therefore, $x^0 \oplus x^{h+i+1} = x^{a_{01}+s_i} = x^{a_{01}+s_{n-i-2}+h+i+1} = x^{h+i+1} \oplus x^0$ and so x^0 commutes with all non-zero elements of N.

Conversely, let N be commutative. Then for non-zero $x^a, x^b \in N$, $x^a \oplus x^b = x^b \oplus x^a \Rightarrow x^a(x^0 \oplus x^{b-a}) = x^a(x^{b-a} \oplus x^0) \Rightarrow x^0 \oplus x^{b-a} = x^{b-a} \oplus x^0$. Thus $s_i = s_{n-i-2} + h + i + 1$. And since $p_i = s_i - s_{i-1}$, we have $p_i + p_{n-i-1} = s_i - s_{i-1} + s_{n-i-1} - s_{n-i-2} = (s_{n-i-2} + h + i + 1) - (s_{n-i-1} + h + i) + s_{n-i-1} - s_{n-i-2} = 1 \equiv n+1$. Therefore $P^M = P^D$.

Example 3.11. Let $n = 9$ and $P = \{3,4,8,5,2,6,7\}$. Then:

$$P = \{3,4,8,5,2,6,7\}, \qquad S = \{3,7,6,2,4,1,8\}$$

$$P' = \{2,3,7,4,1,5,6\}, \qquad S' = \{2,5,3,7,8,4,1\}$$

Since $P^M = \{7,6,2,5,8,4,3\} = P^D$, the order 10 property D cyclic neofield generated by P is commutative under addition.

In early research of this subject a particular pattern emerged in acceptable sequences. The sequences $\{2,3,4,5,6,7\}$ and $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$ are both acceptable. Attempts to verify this pattern revealed that $\{2,3,4,...,23\}$ is not acceptable while $\{2,3,4,...,31\}$ and $\{2,3,4,...,63\}$ both are acceptable. Keedwell [2] reached the same conclusion and verified the existence of this family of property D cyclic neofields by a proof using row arrays. The proof given here once again uses lemma 3.1.

Theorem 3.12. *If $n = 2^k$ and $P = \{2,3,4,...,2^k-1\}$ then P is an acceptable sequence generating a property D cyclic neofield of order $m = 2^k + 1$.*

Proof. Let $P_{\iota,\kappa}$ be a subsequence of P. If κ is odd, say $\kappa = 2\beta + 1$, then $P_{\iota,\kappa} = \{\iota + 1, \iota + 2, ..., \iota + 2\beta + 1\} = \{\gamma - \beta, ..., \gamma - 1, \gamma, \gamma + 1, ..., \gamma + \beta\}$ where $\gamma = \iota + \beta + 1$ is the middle term of $P_{\iota,\kappa}$. Thus $\sum_{P_{\iota,\kappa}} = \kappa\iota + \kappa\frac{\kappa+1}{2} = \gamma(2\beta + 1)$. Because γ is strictly less than 2^k and $2\beta + 1$ is odd, the product is non-zero mod 2^k. If κ is even, say 2β, then $P_{\iota,\kappa} = \{\iota + 1, \iota + 2, ..., \iota + 2\beta\} = \{\gamma - (\beta - 1), ..., \gamma - 1, \gamma, \gamma + 1, \gamma + 2, ..., \gamma + \beta\}$ where $\gamma = \iota + \beta$ is the first of the middle two terms of $P_{\iota,\kappa}$. So $\sum_{P_{\iota,\kappa}} = \kappa\iota + \frac{\kappa}{2}(\kappa + 1) = \beta(2\gamma + 1)$. Similar to the above, since β is strictly less than 2^k and $2\gamma + 1$ is odd, their product is non-zero mod 2^k.

Since the argument rests on the fact that all values of each subsequence are consecutive, condition (ii) of the theorem is satisfied identically.

Example 3.13. Let $n = 2^3 = 8$ and $P = \{2, 3, 4, 5, 6, 7\}$. Then:

$$P = \{2, 3, 4, 5, 6, 7\}, \qquad S = \{2, 5, 1, 6, 4, 3\}$$

$$P' = \{1, 2, 3, 4, 5, 6\}, \qquad S' = \{1, 3, 6, 2, 7, 5\}$$

So P generates a property D cyclic neofield of order 9. This is the lowest order property D cyclic neofield that is not a field.

Example 3.14. Let $n = 2^4 = 16$ and $P = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$. Then:

$$P = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$$

$$S = \{2, 5, 9, 14, 4, 11, 3, 12, 6, 1, 13, 10, 8, 7\}$$

$$P' = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$

$$S' = \{1, 3, 6, 10, 15, 5, 12, 4, 13, 7, 2, 14, 11, 9\}$$

P generates a property D neofield of order 17. As in example 3.13, this neofield is also not a field. In fact, Keedwell [2] proved that the additive loops of the corresponding neofields are associative only for the values $k = 1$ and $k = 2$.

3.2 Commutative Property D Cyclic Neofield Existence Theorem

Keedwell [3] classified all property D cyclic neofields of order up to 18 and provided examples up to order 20. He further conjectured that property D cyclic neofields exist for all orders beyond 20. Searching for examples of property D cyclic neofields can be cumbersome to say the least. Presently the time for a computer program to find all examples of property D cyclic neofields of an order in the low twenties is measured in months. The main issue is that each additional term in the sequence doesn't simply add to the number of algorithms involved. Since the mechanical check is examining each subsequence, adding terms to the sequence adds a corresponding number of algorithms plus lengthens the time it takes to do each of them.

There are several unique features of commutative property D cyclic neofields that should give us an advantage in searches. Remembering that there is a correlation of P' to P^D,the mere fact that $P^M = P^D$ tells us a great deal when considering conditions (i) and (ii) of Keedwell's existence theorem.

Lemma 3.15. *If $P^M = P^D$ for a sequence P, then condition (i) (equivalently (iii) of lemma 3.1) in Keedwell's existence theorem is sufficient for an acceptable sequence.*

Proof. Let P be a sequence with $n-2$ distinct terms such that $P^M = P^D$ and satisfying condition (i) of Keedwell's existence theorem. By contradiction assume

the sequence P' fails to meet condition (ii). Then by lemma 3.1 there exists a subsequence $P'_{\iota,\kappa}$ of P' such that $\sum_{P'_{\iota,\kappa}} \equiv 0$. Since each element in $P'_{\iota,\kappa}$ is one less than the corresponding term in the subsequence $P_{\iota,\kappa}$ of P, $\sum_{P_{\iota,\kappa}} \equiv 0 + \kappa = \kappa$. However, since $P^M = P^D$, then there also exists a subsequence $P_{(n-2-\iota-\kappa),\kappa}$ of P such that for each $p \in P_{\iota,\kappa}$ there exists an $r \in P_{(n-2-\iota-\kappa),\kappa}$ such that $p + r = n + 1$. Then $\sum_{P_{\iota,\kappa}} + \sum_{P_{(n-2-\iota-\kappa),\kappa}} = \kappa(n+1) = \kappa n + \kappa \equiv \kappa = \sum_{P_{\iota,\kappa}}$, which implies$\sum_{P_{(n-2-\iota-\kappa),\kappa}} \equiv 0$ contradicting the hypothesis that P satisfies condition (i).

In a sequence that generates a commutative property D cyclic neofield, it is easy to see that the first term of the sequence determines the last term of the sequence. Similarly, the second term of the sequence determines the second to last term of the sequence, and so on. It should therefore be possible to determine whether a sequence that meets the criteria for a commutative property D cyclic neofield (i.e. $P^M = P^D$) is acceptable or not by examining only the first half of the sequence. Thus it seems reasonable that searching through potential candidate sequences for commutative property D cyclic neofields should take a significantly shorter length of time. Theorem 3.16 below provides the condition for such sequences to be acceptable.

As we have seen previously, there is a major structural difference in the construction of a property D cyclic neofield depending on whether the order is odd or even. If the sequence P has an odd number of terms, then we must decide how to proceed when examining the first "half" of the sequence. By the very nature of sequences where $P^M = P^D$ with an odd n, the middle term of the sequence is a fixed number $\frac{n+1}{2}$. Using the criteria that for a sequence to be acceptable, the sum of all subsequences must be non-zero, it is very easy for us to determine by the first

"half" of a sequence whether a subsequence that falls entirely in the first half or the second half is non-zero or not. For a subsequence that straddles the two halves, we must consider the presence of this middle term when there are an odd number of terms. Although it is possible to prove the conditions for a commutative property D cyclic neofield regardless of whether there are an even or odd number of terms in the sequence, for clarity they are proven here as separate cases.

Theorem 3.16. *Commutative Property D Cyclic Neofield Existence Theorem*

(Part I)

Let n be odd, $O = \{o_1, o_2, ..., o_{\frac{n-3}{2}}\}$ *be a sequence of terms from the set* $\{2, 3, ..., n-1\} - \{\frac{n+1}{2}\}$ *and* $O_{\sigma,\lambda} = \{o_{\sigma+1}, o_{\sigma+2}, ..., o_{\sigma+\lambda}\}$ *be a subsequence of O with* λ *terms.*

(a) For all $i \neq j, o_i \neq o_j$ *and* $o_i + o_j \neq n+1$.

(b) $\sum_{O_{\sigma,\lambda}} \not\equiv 0, \lambda, \sigma+\lambda+1$ *or* $n-\sigma-1$ *modulo n.*

Let $P = \{p_1, p_2, ..., p_{n-2}\}$, *where* $p_{\frac{n-1}{2}} = \frac{n+1}{2}$, $p_i = o_i$ *for* $i < \frac{n-1}{2}$ *and* $p_i = n+1-o_{n-i-1}$ *for* $i > \frac{n-1}{2}$.

Then P is an acceptable sequence generating a commutative property D cyclic neofield.

(Part II)

Let n be even, $E = \{e_1, e_2, ..., e_{\frac{n-2}{2}}\}$ *be a sequence of terms from the set* $\{2, 3, ..., n-1\}$ *and* $E_{\sigma,\lambda} = \{e_{\sigma+1}, e_{\sigma+2}, ..., e_{\sigma+\lambda}\}$ *be a subsequence of E with* λ *terms.*

(a) For all $i \neq j, e_i \neq e_j$ *and* $e_i + e_j \neq n+1$.

(b) $\sum_{E_{\sigma,\lambda}} \not\equiv 0, \lambda, \frac{n-2}{2} - \sigma$ *or* $\sigma+\lambda+\frac{n+2}{2}$ *modulo n.*

Let $P = \{p_1, p_2, ..., p_{n-2}\}$, *where* $p_i = e_i$ *for* $i < \frac{n}{2}$ *and* $p_i = n+1-e_{n-i-1}$ *for* $i \geq \frac{n}{2}$.

Then P is an acceptable sequence generating a commutative property D cyclic neofield.

Proof. (Part I)

By the way we have defined P, $p_i + p_{n-i-1} = n+1$, so $P^M = P^D$; thus we need only verify condition (iii).

Let $P_{\iota,\kappa} = \{p_{\iota+1}, p_{\iota+2}, ..., p_{\iota+\kappa}\}$ be a subsequence of P with κ terms.

Case 1, $\iota + \kappa < \frac{n-1}{2}$ (that is, every term in $P_{\iota,\kappa}$ is before the middle term of P). Then $P_{\iota,\kappa} = O_{\iota,\kappa}$and therefore $\sum_{P_{\iota.\kappa}} \neq 0$.

Case 2, $\iota + 1 > \frac{n-1}{2}$ (that is, every term in $P_{\iota,\kappa}$ is after the middle term of P). Then $\sum_{P_{\iota,\kappa}} = \kappa(n+1) - \sum_{O_{j,\kappa}} = \kappa - \sum_{O_{j,\kappa}}$ for some j. And since $\sum_{O_{j,\kappa}} \neq \kappa$ for all j, $\sum_{P_{\iota,\kappa}} \neq 0$.

Case 3, $\iota + 1 \leq \frac{n-1}{2} \leq \iota + \kappa$ (that is, the middle term of P is a term of $P_{\iota,\kappa}$). Let $p_\gamma = p_{\frac{n-1}{2}}$ be the middle term of P and $0 \leq \beta < \frac{\kappa}{2}$ such that $p_{\gamma-\beta}, p_{\gamma+\beta} \in P_{\iota,\kappa}$. Then $\sum_{j=\gamma-\beta}^{\gamma+\beta} p_j = \beta(n+1) + \frac{n+1}{2} \equiv \beta + \frac{n+1}{2}$ modulo n.

Sub-case a, $n-2 = 2\iota + \kappa$ (that is, the middle term of P is the middle term of $P_{\iota,\kappa}$). Then $\beta = \frac{n-1}{2} - (\iota+1) = \iota + \kappa - \frac{n-1}{2}$ and $\sum_{P_{\iota,\kappa}} = \beta + \frac{n+1}{2} = \iota + \kappa + 1 \neq 0$ modulo n.

Sub-case b, $n-2 < 2\iota + \kappa$ (that is, the middle term of P is in the first half terms of $P_{\iota,\kappa}$). Then $\beta = \frac{n-1}{2} - (\iota+1)$ and $\sum_{P_{\iota,\kappa}} = \sum_{j=\iota+1}^{\gamma+\beta} p_j + \sum_{j=\gamma+\beta+1}^{\iota+\kappa} p_j$. As shown previously, $\sum_{j=\iota+1}^{\gamma+\beta} p_j = \beta + \frac{n+1}{2} = n - \iota - 1$ and since $\sum_{j=\gamma+\beta+1}^{\iota+\kappa} p_j$ is in the last half of P, $\sum_{j=\gamma+\beta+1}^{\iota+\kappa} p_j = \alpha - \sum_{j=\iota-\alpha+1}^{\iota} p_j$ where $\alpha = (2\iota+\kappa) - (n-2)$. Then $\sum_{P_{i,k}} = n - i - 1 + 2i + k - (n-2) - \sum_{O_{\iota-\alpha,\alpha}} = \iota + \kappa + 1 - \sum_{O_{(n-\iota-\kappa-2),(2\iota+\kappa-n+2)}}$ and since $\sum_{O_{(n-\iota-\kappa-2),(2\iota+\kappa-n+2)}} \neq \iota + \kappa + 1 (= n - \sigma - 1)$, $\sum_{P_{\iota,\kappa}} \neq 0$.

Sub-case c, $n-2 > 2\iota + \kappa$ (that is, the middle term of P is in the last half

terms of $P_{\iota,\kappa}$). Then $\beta = \iota + \kappa - \frac{n-1}{2}$ and $\sum_{P_{\iota,\kappa}} = \sum_{j=\iota+1}^{\gamma-\beta-1} p_j + \sum_{j=\gamma-\beta}^{\iota+\kappa} p_j$. As shown previously, $\sum_{j=\gamma-\beta}^{\iota+\kappa} p_j = \beta + \frac{n+1}{2} = \iota + \kappa + 1$ and since $\sum_{j=\iota+1}^{\gamma-\beta-1} p_j$ is in the first half of P, $\sum_{j=\iota+1}^{\gamma-\beta-1} p_j = \sum_{O_{\iota,\alpha}}$ where $\alpha = \gamma - \beta - 1 - \iota = n - 2\iota - \kappa - 2$. Then $\sum_{P_{i,k}} = \iota + \kappa + 1 + \sum_{O_{i,(n-2\iota-\kappa-2)}}$ and since $\sum_{O_{\iota,(n-2\iota-\kappa-2)}} \neq n - \iota - \kappa - 1 (= \sigma + \lambda + 1)$, $\sum_{P_{\iota,\kappa}} \neq 0$.

(Part II)

By the way we have defined P, $p_i + p_{n-i-1} = n+1$, so $P^M = P^D$; thus we need only verify condition (iii).

Let $P_{\iota,\kappa} = \{p_{\iota+1}, p_{\iota+2}, ..., p_{\iota+\kappa}\}$ be a subsequence of P with κ terms.

Case 1, $\iota + \kappa < \frac{n}{2}$ (that is, every term in $P_{\iota,\kappa}$ is before the middle of P). Then $P_{\iota,\kappa} = E_{\iota,\kappa}$and therefore $\sum_{P_{\iota.\kappa}} \neq 0$.

Case 2, $\iota + 1 \geq \frac{n}{2}$ (that is, every term in $P_{\iota,\kappa}$ is after the middle of P). Then $\sum_{P_{\iota,\kappa}} = \kappa(n+1) - \sum_{E_{j,\kappa}} = \kappa - \sum_{E_{j,\kappa}}$ for some j. And since $\sum_{E_{j,\kappa}} \neq \kappa$ for all j, $\sum_{P_{\iota,\kappa}} \neq 0$.

Case 3, $\iota + 1 < \frac{n}{2} \leq \iota + \kappa$ (that is, the middle of P is in $P_{\iota,\kappa}$). Let $p_\gamma = p_{\frac{n}{2}}$ be the second of the middle two terms of P and $0 < \beta \leq \frac{\kappa}{2}$ such that $p_{\gamma-\beta}, p_{\gamma+\beta-1} \in P_{\iota,\kappa}$. Then $\sum_{j=\gamma-\beta}^{\gamma+\beta-1} p_j = \beta(n+1) \equiv \beta$ modulo n.

Sub-case a, $n - 2 = 2\iota + \kappa$ (that is, the middle of P is the middle of $P_{\iota,\kappa}$). Then $\beta = \frac{n}{2} - (\iota + 1) = \iota + \kappa - \frac{n-2}{2}$ and $\sum_{P_{\iota,\kappa}} = \beta \neq 0$ modulo n.

Sub-case b, $n - 2 < 2\iota + \kappa$ (that is, the middle of P is in the first half of $P_{\iota,\kappa}$). Then $\beta = \frac{n}{2} - (\iota + 1)$ and $\sum_{P_{\iota,\kappa}} = \sum_{j=\iota+1}^{\gamma+\beta-1} p_j + \sum_{j=\gamma+\beta}^{\iota+\kappa} p_j$. As shown previously, $\sum_{j=\iota+1}^{\gamma+\beta-1} p_j = \beta = \frac{n}{2} - (\iota + 1)$ and since $\sum_{j=\gamma+\beta}^{\iota+\kappa} p_j$ is in the last half of P, $\sum_{j=\gamma+\beta}^{\iota+\kappa} p_j = \alpha - \sum_{j=\iota-\alpha+1}^{\iota} p_j$ where $\alpha = (2\iota + \kappa) - (n-2)$. Then $\sum_{P_{i,k}} = \beta + \alpha - \sum_{j=\iota-\alpha+1}^{\iota} p_j = \frac{n}{2} - (i+1) + (2i+k) - (n-2) - \sum_{E_{\iota-\alpha,\alpha}} = \iota + \kappa - \frac{n-2}{2} -$

$\sum_{E_{(n-2-\iota-\kappa),(2\iota+\kappa-n+2)}}$ and since $\sum_{E_{(n-\iota-\kappa-2),(2\iota+\kappa-n+2)}} \neq \iota+\kappa-\frac{n-2}{2}(=\frac{n-2}{2}-\sigma)$, $\sum_{P_{\iota,\kappa}} \neq 0$.

Sub-case c, $n-2 > 2\iota+\kappa$ (that is, the middle of P is in the last half of $P_{\iota,\kappa}$). Then $\beta = \iota+\kappa-\frac{n-2}{2}$ and $\sum_{P_{\iota,\kappa}} = \sum_{j=\iota+1}^{\gamma-\beta-1} p_j + \sum_{j=\gamma-\beta}^{\iota+\kappa} p_j$. As shown previously, $\sum_{j=\gamma-\beta}^{\iota+\kappa} p_j = \beta = \iota+\kappa-\frac{n-2}{2}$ and since $\sum_{j=\iota+1}^{\gamma-\beta-1} p_j$ is in the first half of P, $\sum_{j=\iota+1}^{\gamma-\beta-1} p_j = \sum_{E_{\iota,\alpha}}$ where $\alpha = (n-2)-(2\iota+\kappa)$. Then $\sum_{P_{i,k}} = \beta + \sum_{E_{\iota,\alpha}} = \iota+\kappa-\frac{n-2}{2} + \sum_{E_{i,(n-2\iota-\kappa-2)}}$ and since $\sum_{E_{\iota,(n-2\iota-\kappa-2)}} \neq -\iota-\kappa+\frac{n-2}{2}(=\sigma+\lambda+\frac{n+2}{2})$, $\sum_{P_{\iota,\kappa}} \neq 0$.

Using the conditions of this theorem with the aid of a computer we have found numerous examples (perhaps all examples) of commutative property D cyclic neofields of orders greater than 2 and less than 33, with the exceptions of orders 6, 12 and 14. As shown in example 3.3, no order 6 property D cyclic neofield exists, the nonexistence of a commutative property D cyclic neofields of order 12 or 14 is proven here.

Proposition 3.17. *There exists no commutative property D cyclic neofield of order* 12.

Proof. Let $n = 11$ and $O = \{o_1, o_2,, o_3, o_4\}$ with $o_i \in \{2,3,4,5,7,8,9,10\}$.

We may immediately eliminate some values from certain positions. If we consider the case of $\lambda = 1$ then we are examining a subsequence of length 1 with the position determined by σ. For example, $O_{2,1}$ is the subsequence $\{o_3\}$. In this way, we may show using (c) and (d) that $0_i \neq i+1$ and $o_i \neq 11-i$. Thus $o_1 \neq 2,10$, $o_2 \neq 3,9$, $o_3 \neq 4,8$ and $o_4 \neq 5,7$. We will use the fact that the mirror of any acceptable sequence is also acceptable, so we need only examine cases where $o_1 \in \{3,4,5\}$.

- Case $O = \{3, o_2, o_3, o_4\}$. By (a),$o_2 \in \{2,4,5,7,8,10\}$.

- $O = \{3,2,o_3,o_4\}$. By (a), $o_3 \in \{5,7\}$.
  - $O = \{3,2,5,o_4\} \Rightarrow O_{0,3} = \{3,2,5\} \Rightarrow \sum_{O_{0,3}} = 10 = n - \sigma - 1$ (e).
  - $O = \{3,2,7,o_4\} \Rightarrow O_{1,2} = \{2,7\} \Rightarrow \sum_{O_{1,2}} = 9 = n - \sigma - 1$ (e).
- $O = \{3,4,o_3,o_4\}$. By (a), $o_3 \in \{2,5,7,10\}$.
  - $O = \{3,4,2,o_4\}$. By (a), $o_4 \in \{5,7\}$ but as shown $o_4 \neq 5,7$.
  - $O = \{3,4,5,o_4\} \Rightarrow O_{1,2} = \{4,5\} \Rightarrow \sum_{O_{1,2}} = 9 = n - \sigma - 1$ (e).
  - $O = \{3,4,7,o_4\} \Rightarrow O_{1,2} = \{4,7\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).
  - $O = \{3,4,10,o_4\}$. By (a), $o_4 \in \{5,7\}$ but as shown $o_4 \neq 5,7$.
- $O = \{3,5,o_3,o_4\}$. By (a), $o_3 \in \{2,10\}$.
  - $O = \{3,5,2,o_4\} \Rightarrow O_{0,3} = \{3,5,2\} \Rightarrow \sum_{O_{0,3}} = 10 = n - \sigma - 1$ (e).
  - $O = \{3,5,10,o_4\} \Rightarrow O_{1,2} = \{5,10\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).
- $O = \{3,7,o_3,o_4\} \Rightarrow O_{0,2} = \{3,7\} \Rightarrow \sum_{O_{0,2}} = 10 = n - \sigma - 1$ (e).
- $O = \{3,8,o_3,o_4\} \Rightarrow O_{0,2} = \{3,8\} \Rightarrow \sum_{O_{0,2}} = 0$ (b)
- $O = \{3,10,o_3,o_4\} \Rightarrow O_{0,2} = \{3,10\} \Rightarrow \sum_{O_{0,2}} = 2 = \lambda$ (c).

- Case $O = \{4,o_2,o_3,o_4\}$. By (a),$o_2 \in \{2,5,7,10\}$.
  - $O = \{4,2,o_3,o_4\}$. By (a),$o_3 \in \{3,5,7,9\}$.
    - $O = \{4,2,3,o_4\}$. By (a),$o_4 \in \{5,7\}$ but as shown $o_4 \neq 5,7$.
    - $O = \{4,2,5,o_4\} \Rightarrow O_{0,3} = \{4,2,5\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
    - $O = \{4,2,7,o_4\} \Rightarrow O_{1,2} = \{2,7\} \Rightarrow \sum_{O_{1,2}} = 9 = n - \sigma - 1$ (e).
    - $O = \{4,2,9,o_4\} \Rightarrow O_{1,2} = \{2,9\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).

- $O = \{4,5,o_3,o_4\}$. By (a),$o_3 \in \{2,3,9,10\}$.
  - $O = \{4,5,2,o_4\} \Rightarrow O_{0,3} = \{4,5,2\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
  - $O = \{4,5,3,o_4\}$. By (a),$o_4 \in \{2,10\}$.
    - $O = \{4,5,3,2\} \Rightarrow O_{2,2} = \{3,2\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
    - $O = \{4,5,3,10\} \Rightarrow O_{0,4} = \{4,5,3,10\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
  - $O = \{4,5,9,o_4\}$. By (a),$o_4 \in \{2,10\}$.
    - $O = \{4,5,9,2\} \Rightarrow O_{2,2} = \{9,2\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
    - $O = \{4,5,9,10\} \Rightarrow O_{2,2} = \{9,10\} \Rightarrow \sum_{O_{2,2}} = 8 = n - \sigma - 1$ (e).
  - $O = \{4,5,10,o_4\} \Rightarrow O_{1,2} = \{5,10\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).
- $O = \{4,7,o_3,o_4\} \Rightarrow O_{0,2} = \{4,7\} \Rightarrow \sum_{O_{0,2}} = 0$ (b).
- $O = \{4,10,o_3,o_4\} \Rightarrow O_{0,2} = \{4,10\} \Rightarrow \sum_{O_{0,2}} = 3 = \sigma + \lambda + 1$ (d).

- Case $O = \{5,o_2,o_3,o_4\}$. By (a),$o_2 \in \{2,4,8,10\}$.
  - $O = \{5,2,o_3,o_4\}$. By (a),$o_3 \in \{3,9\}$.
    - $O = \{5,2,3o_4\} \Rightarrow O_{0,3} = \{5,2,3\} \Rightarrow \sum_{O_{0,3}} = 10 = n - \sigma - 1$ (e).
    - $O = \{5,2,9,o_4\} \Rightarrow O_{1,2} = \{2,9\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).
  - $O = \{5,4,o_3,o_4\}$. By (a),$o_3 \in \{2,3,9,10\}$.
    - $O = \{5,4,2,o_4\} \Rightarrow O_{0,3} = \{5,4,2\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
    - $O = \{5,4,3,o_4\}$. By (a),$o_3 \in \{2,10\}$.
      - $O = \{5,4,3,2\} \Rightarrow O_{2,2} = \{3,2\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
      - $O = \{5,4,3,10\} \Rightarrow O_{0,4} = \{5,4,3,10\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).

* $O = \{5,4,9,o_4\} \Rightarrow O_{1,2} = \{4,9\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).
* $O = \{5,4,10,o_4\}$. By (a),$o_4 \in \{3,9\}$.
  - $O = \{5,4,10,3\} \Rightarrow O_{0,4} = \{5,4,10,3\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
  - $O = \{5,2,10,9\} \Rightarrow O_{2,2} = \{10,9\} \Rightarrow \sum_{O_{2,2}} = 8 = n - \sigma - 1$ (e).

– $O = \{5,8,o_3,o_4\} \Rightarrow O_{0,2} = \{5,8\} \Rightarrow \sum_{O_{0,2}} = 2 = \lambda$ (c).

– $O = \{5,10,o_3,o_4\}$. By (a),$o_3 \in \{3,9\}$.
* $O = \{5,10,3,o_4\} \Rightarrow O_{1,2} = \{10,3\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).
* $O = \{5,10,9,o_4\}$. By (a),$o_4 \in \{4,8\}$.
  - $O = \{5,10,9,4\} \Rightarrow O_{2,2} = \{9,4\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).
  - $O = \{5,10,9,8\} \Rightarrow O_{1,3} = \{10,9,8\} \Rightarrow \sum_{O_{1,3}} = 5 = \sigma + \lambda + 1$ (d).

Proposition 3.18. *There exists no commutative property D cyclic neofield of order* 14.

Proof. Let $n = 13$, $O = \{o_1, o_2, , o_3, o_4, o_5\}$ with $o_i \in \{2,3,4,5,6,8,9,10,11,12\}$.

We may immediately eliminate certain values from certain positions. If we consider the case of $\lambda = 1$ then we are examining a subsequence of length 1 with the position determined by σ. For example, $O_{2,1}$ is the subsequence $\{o_3\}$. In this way, we may show using (c) and (d) that $0_i \neq i+1$ and $o_i \neq 11-i$. Thus $o_1 \neq 2,12$, $o_2 \neq 3,11$, $o_3 \neq 4,10$, $o_4 \neq 5,9$ and $o_5 \neq 6,8$. We may also use the fact that the mirror of any acceptable sequence is also acceptable, so we need only examine cases where $o_1 \in \{3,4,5,6\}$.

Case $O = \{3,o_2,o_3,o_4,o_5\}$. By (a),$o_2 \in \{2,4,5,6,8,9,10,12\}$.

- $O = \{3,2,o_3,o_4,o_5\}$. By (a),$o_3 \in \{5,6,8,9\}$.
  - $O = \{3,2,5,o_4,o_5\}$. By (a),$o_4 \in \{4,6,8,10\}$.
    - $O = \{3,2,5,4,o_5\} \Rightarrow O_{1,3} = \{2,5,4\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).
    - $O = \{3,2,5,6,o_5\} \Rightarrow O_{1,3} = \{2,5,6\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
    - $O = \{3,2,5,8,o_5\} \Rightarrow O_{2,2} = \{5,8\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
    - $O = \{3,2,5,10,o_5\} \Rightarrow O_{2,2} = \{5,10\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).
  - $O = \{3,2,6,o_4,o_5\}$. By (a),$o_4 \in \{4,10\}$.
    - $O = \{3,2,6,4,o_5\} \Rightarrow O_{2,2} = \{6,4\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).
    - $O = \{3,2,6,10,o_5\} \Rightarrow O_{1,3} = \{2,6,10\} \Rightarrow \sum_{O_{1,3}} = 5 = \sigma + \lambda + 1$ (d).
  - $O = \{3,2,8,o_4,o_5\} \Rightarrow O_{0,3} = \{3,2,8\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
  - $O = \{3,2,9,o_4,o_5\} \Rightarrow O_{1,2} = \{2,9\} \Rightarrow \sum_{O_{1,2}} = 11 = n - \sigma - 1$ (e).
- $O = \{3,4,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,5,6,8,9,12\}$.
  - $O = \{3,4,2,o_4,o_5\}$. By (a),$o_4 \in \{6,8\}$.
    - $O = \{3,4,2,6,o_5\}$. By (a),$o_5 \in \{5,9\}$.
      - $O = \{3,4,2,6,5\} \Rightarrow O_{2,3} = \{2,6,5\} \Rightarrow \sum_{O_{2,3}} = 0$ (b).
      - $O = \{3,4,2,6,9\} \Rightarrow O_{3,2} = \{6,9\} \Rightarrow \sum_{O_{3,2}} = 2 = \lambda$ (c).
    - $O = \{3,4,2,8,o_5\} \Rightarrow O_{0,4} = \{3,4,2,8\} \Rightarrow \sum_{O_{0,4}} = 4 = \lambda$ (c).
  - $O = \{3,4,5,o_4,o_5\} \Rightarrow O_{0,3} = \{3,4,5\} \Rightarrow \sum_{O_{0,3}} = 12 = n - \sigma - 1$ (e).

- $O = \{3,4,6,o_4,o_5\} \Rightarrow O_{0,3} = \{3,4,6\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
- $O = \{3,4,8,o_4,o_5\}$. By (a),$o_4 \in \{2,12\}$.
  - $O = \{3,4,8,2,o_5\} \Rightarrow O_{0,4} = \{3,4,8,2\} \Rightarrow \sum_{O_{0,4}} = 4 = \lambda$ (c).
  - $O = \{3,4,8,12,o_5\} \Rightarrow O_{1,3} = \{4,8,12\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).
- $O = \{3,4,9,o_4,o_5\} \Rightarrow O_{1,2} = \{4,9\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).
- $O = \{3,4,12,o_4,o_5\}$. By (a),$o_4 \in \{6,8\}$.
  - $O = \{3,4,12,6,o_5\} \Rightarrow O_{2,2} = \{12,6\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
  - $O = \{3,4,12,8,o_5\} \Rightarrow O_{1,3} = \{4,12,8\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).

- $O = \{3,5,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,6,8,12\}$.
  - $O = \{3,5,2,o_4,o_5\}$. By (a),$o_4 \in \{4,6,8,10\}$.
    - $O = \{3,5,2,4,o_5\} \Rightarrow O_{1,3} = \{5,2,4\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).
    - $O = \{3,5,2,6,o_5\} \Rightarrow O_{1,3} = \{5,2,6\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
    - $O = \{3,5,2,8,o_5\} \Rightarrow O_{0,4} = \{3,5,2,8\} \Rightarrow \sum_{O_{0,4}} = 5 = \sigma + \lambda + 1$ (d).
    - $O = \{3,5,2,10,o_5\}$. By (a),$o_5 \in \{6,8\}$ but as shown $o_5 \neq 6,8$.
  - $O = \{3,5,6,o_4,o_5\} \Rightarrow O_{1,2} = \{5,6\} \Rightarrow \sum_{O_{1,2}} = 11 = n - \sigma - 1$ (e).
  - $O = \{3,5,8,o_4,o_5\} \Rightarrow O_{1,2} = \{5,8\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).
  - $O = \{3,5,12,o_4,o_5\} \Rightarrow O_{1,2} = \{5,12\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).

- $O = \{3,6,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,5,9,12\}$.
  - $O = \{3,6,2,o_4,o_5\}$. By (a),$o_4 \in \{4,10\}$.
    - $O = \{3,6,2,4,o_5\}$. By (a),$o_5 \in \{5,9\}$.
      - $O = \{3,6,2,4,5\} \Rightarrow O_{1,4} = \{6,2,4,5\} \Rightarrow \sum_{O_{1,4}} = 4 = \lambda$ (c).
      - $O = \{3,6,2,4,9\} \Rightarrow O_{3,2} = \{4,9\} \Rightarrow \sum_{O_{3,2}} = 0$ (b).
    - $O = \{3,6,2,10,o_5\} \Rightarrow O_{1,3} = \{6,2,10\} \Rightarrow \sum_{O_{1,3}} = 5 = \sigma + \lambda + 1$ (d).
  - $O = \{3,6,5,o_4,o_5\} \Rightarrow O_{1,2} = \{6,5\} \Rightarrow \sum_{O_{1,2}} = 11 = n - \sigma - 1$ (e).
  - $O = \{3,6,9,o_4,o_5\} \Rightarrow O_{1,2} = \{6,9\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).
  - $O = \{3,6,12,o_4,o_5\}$. By (a),$o_4 \in \{4,10\}$.
    - $O = \{3,6,12,4,o_5\}$. By (a),$o_5 \in \{5,9\}$.
      - $O = \{3,6,12,4,5\} \Rightarrow O_{3,2} = \{4,5\} \Rightarrow \sum_{O_{3,2}} = 9 = n - \sigma - 1$ (e).
      - $O = \{3,6,12,4,9\} \Rightarrow O_{3,2} = \{4,9\} \Rightarrow \sum_{O_{3,2}} = 0$ (b).
    - $O = \{3,6,12,10,o_5\} \Rightarrow O_{0,4} = \{3,6,12,10\} \Rightarrow \sum_{O_{0,4}} = 5 = \sigma + \lambda + 1$ (d).
- $O = \{3,8,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,5,9,12\}$.
  - $O = \{3,8,2,o_4,o_5\} \Rightarrow O_{0,3} = \{3,8,2\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
  - $O = \{3,8,5,o_4,o_5\} \Rightarrow O_{1,2} = \{8,5\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).
  - $O = \{3,8,9,o_4,o_5\} \Rightarrow O_{1,2} = \{8,9\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).

- $O = \{3,8,12,o_4,o_5\}$. By (a),$o_4 \in \{4,10\}$.
  - $O = \{3,8,12,4,o_5\} \Rightarrow O_{1,3} = \{8,12,4\} \Rightarrow \sum_{O_{1,3}} = 11 = n-\sigma-1$ (e).
  - $O = \{3,8,12,10,o_5\}$. By (a),$o_5 \in \{5,9\}$.
    - $O = \{3,8,12,10,5\} \Rightarrow O_{3,2} = \{10,5\} \Rightarrow \sum_{O_{3,2}} = 2 = \lambda$ (c).
    - $O = \{3,8,12,10,9\} \Rightarrow O_{1,4} = \{8,12,10,9\} \Rightarrow \sum_{O_{1,4}} = 0$ (b).

- $O = \{3,9,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{3,9\} \Rightarrow \sum_{O_{0,2}} = 12 = n-\sigma-1$ (e).
- $O = \{3,10,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{3,10\} \Rightarrow \sum_{O_{0,2}} = 0$ (b).
- $O = \{3,12,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{3,12\} \Rightarrow \sum_{O_{0,2}} = 2 = \lambda$ (c).

Case $O = \{4,o_2,o_3,o_4,o_5\}$. By (a),$o_2 \in \{2,5,6,8,9,12\}$.

- $O = \{4,2,o_3,o_4,o_5\}$. By (a),$o_3 \in \{3,5,6,8,9,11\}$.
  - $O = \{4,2,3,o_4,o_5\}$. By (a),$o_4 \in \{6,8\}$.
    - $O = \{4,2,3,6,o_5\} \Rightarrow O_{1,3} = \{2,3,6\} \Rightarrow \sum_{O_{1,3}} = 11 = n-\sigma-1$ (e).
    - $O = \{4,2,3,8,o_5\} \Rightarrow O_{1,3} = \{2,3,8\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
  - $O = \{4,2,5,o_4,o_5\}$. By (a),$o_4 \in \{3,6,8,11\}$.
    - $O = \{4,2,5,3,o_5\}$. By (a),$o_5 \in \{6,8\}$ but as shown $o_5 \neq 6,8$.
    - $O = \{4,2,5,6,o_5\} \Rightarrow O_{1,3} = \{2,5,6\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
    - $O = \{4,2,5,8,o_5\} \Rightarrow O_{2,2} = \{5,8\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
    - $O = \{4,2,5,11,o_5\} \Rightarrow O_{1,3} = \{2,5,11\} \Rightarrow \sum_{O_{1,3}} = 5 = \sigma+\lambda+1$ (d).

- $O = \{4,2,6,o_4,o_5\} \Rightarrow O_{0,3} = \{4,2,6\} \Rightarrow \sum_{O_{0,3}} = 12 = n - \sigma - 1$ (e).
- $O = \{4,2,8,o_4,o_5\}$. By (a),$o_4 \in \{3,11\}$.
  - $O = \{4,2,8,3,o_5\} \Rightarrow O_{1,3} = \{2,8,3\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
  - $O = \{4,2,8,11,o_5\} \Rightarrow O_{0,4} = \{4,2,8,11\} \Rightarrow \sum_{O_{0,4}} = 12 = n - \sigma - 1$ (e).
- $O = \{4,2,9,o_4,o_5\} \Rightarrow O_{1,2} = \{2,9\} \Rightarrow \sum_{O_{1,2}} = 11 = n - \sigma - 1$ (e).
- $O = \{4,2,11,o_4,o_5\} \Rightarrow O_{1,2} = \{2,11\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).

- $O = \{4,5,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,3,6,8,11,12\}$.
  - $O = \{4,5,2,o_4,o_5\}$. By (a),$o_4 \in \{3,6,8,11\}$.
    - $O = \{4,5,2,3,o_5\} \Rightarrow O_{2,2} = \{2,3\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
    - $O = \{4,5,2,6,o_5\} \Rightarrow O_{1,3} = \{5,2,6\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
    - $O = \{4,5,2,8,o_5\} \Rightarrow O_{2,2} = \{2,8\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).
    - $O = \{4,5,2,11,o_5\} \Rightarrow O_{2,2} = \{2,11\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
  - $O = \{4,5,3,o_4,o_5\} \Rightarrow O_{0,3} = \{4,5,3\} \Rightarrow \sum_{O_{0,3}} = 12 = n - \sigma - 1$ (e).
  - $O = \{4,5,6,o_4,o_5\} \Rightarrow O_{1,2} = \{5,6\} \Rightarrow \sum_{O_{1,2}} = 11 = n - \sigma - 1$ (e).
  - $O = \{4,5,8,o_4,o_5\} \Rightarrow O_{0,3} = \{4,5,8\} \Rightarrow \sum_{O_{0,3}} = 4 = \sigma + \lambda + 1$ (d).
  - $O = \{4,5,11,o_4,o_5\}$. By (a),$o_4 \in \{2,6,8,12\}$.
    - $O = \{4,5,11,2,o_5\} \Rightarrow O_{2,2} = \{11,2\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
    - $O = \{4,5,11,6,o_5\} \Rightarrow O_{0,4} = \{4,5,11,6\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
    - $O = \{4,5,11,8,o_5\} \Rightarrow O_{1,3} = \{5,11,8\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).

* $O = \{4,5,11,12,o_5\} \Rightarrow O_{2,2} = \{11,12\} \Rightarrow \sum_{O_{2,2}} = 10 = n-\sigma-1$ (e).

– $O = \{4,5,12,o_4,o_5\} \Rightarrow O_{1,2} = \{5,12\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma+\lambda+1$ (d).

- $O = \{4,6,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,3,5,9,11,12\}$.

– $O = \{4,6,2,o_4,o_5\} \Rightarrow O_{0,3} = \{4,6,2\} \Rightarrow \sum_{O_{0,3}} = 12 = n-\sigma-1$ (e).

– $O = \{4,6,3,o_4,o_5\} \Rightarrow O_{0,3} = \{4,6,3\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).

– $O = \{4,6,5,o_4,o_5\} \Rightarrow O_{1,2} = \{6,5\} \Rightarrow \sum_{O_{1,2}} = 11 = n-\sigma-1$ (e).

– $O = \{4,6,9,o_4,o_5\} \Rightarrow O_{1,2} = \{6,9\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).

– $O = \{4,6,11,o_4,o_5\} \Rightarrow O_{1,2} = \{6,11\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma+\lambda+1$ (d).

– $O = \{4,6,12,o_4,o_5\}$. By (a),$o_4 \in \{3,11\}$.

* $O = \{4,6,12,3,o_5\} \Rightarrow O_{2,2} = \{12,3\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).

* $O = \{4,6,12,11,o_5\} \Rightarrow O_{1,3} = \{6,12,11\} \Rightarrow \sum_{O_{1,3}} = 3 = \lambda$ (c).

- $O = \{4,8,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{4,8\} \Rightarrow \sum_{O_{0,2}} = 12 = n-\sigma-1$ (e).

- $O = \{4,9,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{4,9\} \Rightarrow \sum_{O_{0,2}} = 0$ (b).

- $O = \{4,12,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{4,12\} \Rightarrow \sum_{O_{0,2}} = 3 = \sigma+\lambda+1$ (d).

Case $O = \{5,o_2,o_3,o_4,o_5\}$. By (a),$o_2 \in \{2,4,6,8,10,12\}$.

- $O = \{5,2,o_3,o_4,o_5\}$. By (a),$o_3 \in \{3,6,8,11\}$.

– $O = \{5,2,3,o_4,o_5\}$. By (a),$o_4 \in \{4,6,8,10\}$.

* $O = \{5,2,3,4,o_5\}$. By (a),$o_5 \in \{6,8\}$ but as shown $o_5 \neq 6,8$.

* $O = \{5,2,3,6,o_5\} \Rightarrow O_{1,3} = \{2,3,6\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).
* $O = \{5,2,3,8,o_5\} \Rightarrow O_{1,3} = \{2,3,8\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
* $O = \{5,2,3,10,o_5\} \Rightarrow O_{2,2} = \{3,10\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).

– $O = \{5,2,6,o_4,o_5\} \Rightarrow O_{0,3} = \{5,2,6\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).

– $O = \{5,2,8,o_4,o_5\}$. By (a),$o_4 \in \{3,4,10,11\}$.

* $O = \{5,2,8,3,o_5\} \Rightarrow O_{1,3} = \{2,8,3\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
* $O = \{5,2,8,4,o_5\}$. By (a),$o_5 \in \{3,11\}$.
  · $O = \{5,2,8,4,3\} \Rightarrow O_{1,4} = \{2,8,4,3\} \Rightarrow \sum_{O_{1,4}} = 4 = \lambda$ (c).
  · $O = \{5,2,8,4,11\} \Rightarrow O_{3,2} = \{4,11\} \Rightarrow \sum_{O_{3,2}} = 2 = \lambda$ (c).
* $O = \{5,2,8,10,o_5\} \Rightarrow O_{2,2} = \{8,10\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
* $O = \{5,2,8,11,o_5\} \Rightarrow O_{0,4} = \{5,2,8,11\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).

– $O = \{5,2,11,o_4,o_5\} \Rightarrow O_{1,2} = \{2,11\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).

• $O = \{5,4,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,3,6,8,11,12\}$.

– $O = \{5,4,2,o_4,o_5\}$. By (a),$o_4 \in \{3,6,8,11\}$.

* $O = \{5,4,2,3,o_5\} \Rightarrow O_{2,2} = \{2,3\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
* $O = \{5,4,2,6,o_5\} \Rightarrow O_{0,4} = \{5,4,2,6\} \Rightarrow \sum_{O_{0,4}} = 4 = \lambda$ (c).
* $O = \{5,4,2,8,o_5\} \Rightarrow O_{2,2} = \{2,8\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).
* $O = \{5,4,2,11,o_5\} \Rightarrow O_{2,2} = \{2,11\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).

– $O = \{5,4,3,o_4,o_5\} \Rightarrow O_{0,3} = \{5,4,3\} \Rightarrow \sum_{O_{0,3}} = 12 = n - \sigma - 1$ (e).

– $O = \{5,4,6,o_4,o_5\}$. By (a),$o_4 \in \{2,3,11,12\}$.

* $O = \{5,4,6,2,o_5\} \Rightarrow O_{0,4} = \{5,4,6,2\} \Rightarrow \sum_{O_{0,4}} = 4 = \lambda$ (c).
* $O = \{5,4,6,3,o_5\} \Rightarrow O_{1,3} = \{4,6,3\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
* $O = \{5,4,6,11,o_5\} \Rightarrow O_{0,4} = \{5,4,6,11\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
* $O = \{5,4,6,12,o_5\} \Rightarrow O_{2,2} = \{6,12\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).

– $O = \{5,4,8,o_4,o_5\} \Rightarrow O_{0,3} = \{5,4,8\} \Rightarrow \sum_{O_{0,3}} = 4 = \sigma + \lambda + 1$ (d).

– $O = \{5,4,11,o_4,o_5\} \Rightarrow O_{1,2} = \{4,11\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).

– $O = \{5,4,12,o_4,o_5\}$. By (a),$o_4 \in \{3,6,8,11\}$.

* $O = \{5,4,12,3,o_5\} \Rightarrow O_{2,2} = \{12,3\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).
* $O = \{5,4,12,6,o_5\} \Rightarrow O_{2,2} = \{12,6\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
* $O = \{5,4,12,8,o_5\} \Rightarrow O_{1,3} = \{4,12,8\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).
* $O = \{5,4,12,11,o_5\} \Rightarrow O_{2,2} = \{12,11\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).

- $O = \{5,6,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,3,11,12\}$.

– $O = \{5,6,2,o_4,o_5\} \Rightarrow O_{0,3} = \{5,6,2\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).

– $O = \{5,6,3,o_4,o_5\}$. By (a),$o_4 \in \{2,4,10,12\}$.

* $O = \{5,6,3,2,o_5\} \Rightarrow O_{2,2} = \{3,2\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
* $O = \{5,6,3,4,o_5\} \Rightarrow O_{1,3} = \{6,3,4\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
* $O = \{5,6,3,10,o_5\} \Rightarrow O_{2,2} = \{3,10\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
* $O = \{5,6,3,12,o_5\} \Rightarrow O_{0,4} = \{5,6,3,12\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).

– $O = \{5,6,11,o_4,o_5\} \Rightarrow O_{1,2} = \{6,11\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).

- $O = \{5,6,12,o_4,o_5\}$. By (a),$o_4 \in \{3,4,10,11\}$.
  - $O = \{5,6,12,3,o_5\} \Rightarrow O_{0,4} = \{5,6,12,3\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
  - $O = \{5,6,12,4,o_5\}$. By (a),$o_5 \in \{3,11\}$.
    - $O = \{5,6,12,4,3\} \Rightarrow O_{2,3} = \{12,4,3\} \Rightarrow \sum_{O_{2,3}} = 6 = \sigma + \lambda + 1$ (d).
    - $O = \{5,6,12,4,11\} \Rightarrow O_{3,2} = \{4,11\} \Rightarrow \sum_{O_{3,2}} = 2 = \lambda$ (c).
  - $O = \{5,6,12,10,o_5\}$. By (a),$o_5 \in \{3,11\}$.
    - $O = \{5,6,12,10,3\} \Rightarrow O_{3,2} = \{10,3\} \Rightarrow \sum_{O_{3,2}} = 0$ (b).
    - $O = \{5,6,12,10,11\} \Rightarrow O_{1,4} = \{6,12,10,11\} \Rightarrow \sum_{O_{1,4}} = 0$ (b).
  - $O = \{5,6,12,11,o_5\} \Rightarrow O_{1,3} = \{6,12,11\} \Rightarrow \sum_{O_{1,3}} = 3 = \lambda$ (c).
- $O = \{5,8,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{5,8\} \Rightarrow \sum_{O_{0,2}} = 0$ (b).
- $O = \{5,10,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{5,10\} \Rightarrow \sum_{O_{0,2}} = 2 = \lambda$ (c).
- $O = \{5,12,o_3,o_4,o_5\}$. By (a),$o_3 \in \{3,6,8,11\}$.
  - $O = \{5,12,3,o_4,o_5\} \Rightarrow O_{1,2} = \{12,3\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).
  - $O = \{5,12,6,o_4,o_5\}$. By (a),$o_4 \in \{3,4,10,11\}$.
    - $O = \{5,12,6,3,o_5\} \Rightarrow O_{0,4} = \{5,12,6,3\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
    - $O = \{5,12,6,4,o_5\} \Rightarrow O_{2,2} = \{6,4\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).
    - $O = \{5,12,6,10,o_5\}$. By (a),$o_5 \in \{3,11\}$.
      - $O = \{5,12,6,10,3\} \Rightarrow O_{3,2} = \{10,3\} \Rightarrow \sum_{O_{3,2}} = 0$ (b).
      - $O = \{5,12,6,10,11\} \Rightarrow O_{1,4} = \{12,6,10,11\} \Rightarrow \sum_{O_{1,4}} = 0$ (b).

* $O = \{5,12,6,11,o_5\} \Rightarrow O_{1,3} = \{12,6,11\} \Rightarrow \sum_{O_{1,3}} = 3 = \lambda$ (c).

– $O = \{5,12,8,o_4,o_5\} \Rightarrow O_{0,3} = \{5,12,8\} \Rightarrow \sum_{O_{0,3}} = 12 = n - \sigma - 1$ (e).

– $O = \{5,12,11,o_4,o_5\}$. By (a),$o_4 \in \{4,6,8,10\}$.

* $O = \{5,12,11,4,o_5\} \Rightarrow O_{2,2} = \{11,4\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).

* $O = \{5,12,11,6,o_5\} \Rightarrow O_{1,3} = \{12,11,6\} \Rightarrow \sum_{O_{1,3}} = 3 = \lambda$ (c).

* $O = \{5,12,11,8,o_5\} \Rightarrow O_{1,3} = \{12,11,8\} \Rightarrow \sum_{O_{1,3}} = 5 = \sigma + \lambda + 1$ (d).

* $O = \{5,12,11,10,o_5\} \Rightarrow O_{0,4} = \{5,12,11,10\} \Rightarrow \sum_{O_{0,4}} = 12 = n - \sigma - 1$ (e).

Case $O = \{6,o_2,o_3,o_4,o_5\}$. By (a),$o_2 \in \{2,4,5,9,10,12\}$.

- $O = \{6,2,o_3,o_4,o_5\}$. By (a),$o_3 \in \{3,5,9,11\}$.

– $O = \{6,2,3,o_4,o_5\}$. By (a),$o_4 \in \{4,10\}$.

* $O = \{6,2,3,4,o_5\}$. By (a),$o_5 \in \{5,9\}$.

· $O = \{6,2,3,4,5\} \Rightarrow O_{3,2} = \{4,5\} \Rightarrow \sum_{O_{3,2}} = 9 = n - \sigma - 1$ (e).

· $O = \{6,2,3,4,9,o_5\} \Rightarrow O_{3,2} = \{4,9\} \Rightarrow \sum_{O_{3,2}} = 0$ (b).

* $O = \{6,2,3,10,o_5\} \Rightarrow O_{2,2} = \{3,10\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).

– $O = \{6,2,5,o_4,o_5\} \Rightarrow O_{0,3} = \{6,2,5\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).

– $O = \{6,2,9,o_4,o_5\} \Rightarrow O_{1,2} = \{2,9\} \Rightarrow \sum_{O_{1,2}} = 11 = n - \sigma - 1$ (e).

– $O = \{6,2,11,o_4,o_5\} \Rightarrow O_{1,2} = \{2,11\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).

- $O = \{6,4,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,3,5,9,11,12\}$.
  - $O = \{6,4,2,o_4,o_5\} \Rightarrow O_{0,3} = \{6,4,2\} \Rightarrow \sum_{O_{0,3}} = 12 = n - \sigma - 1$ (e).
  - $O = \{6,4,3,o_4,o_5\} \Rightarrow O_{0,3} = \{6,4,3\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).
  - $O = \{6,4,5,o_4,o_5\}$. By (a),$o_4 \in \{2,3,11,12\}$.
    - $O = \{6,4,5,2,o_5\} \Rightarrow O_{1,3} = \{4,5,2\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).
    - $O = \{6,4,5,3,o_5\} \Rightarrow O_{0,4} = \{6,4,5,3\} \Rightarrow \sum_{O_{0,4}} = 5 = \sigma + \lambda + 1$ (d).
    - $O = \{6,4,5,11,o_5\} \Rightarrow O_{0,4} = \{6,4,5,11\} \Rightarrow \sum_{O_{0,4}} = 0$ (b).
    - $O = \{6,4,5,12,o_5\}$. By (a),$o_5 \in \{3,11\}$.
      - $O = \{6,4,5,12,3\} \Rightarrow O_{3,2} = \{12,3\} \Rightarrow \sum_{O_{3,2}} = 2 = \lambda$ (c).
      - $O = \{6,4,5,12,11\} \Rightarrow O_{1,4} = \{4,5,12,11\} \Rightarrow \sum_{O_{1,4}} = 6 = \sigma + \lambda + 1$ (d).
  - $O = \{6,4,9,o_4,o_5\} \Rightarrow O_{1,2} = \{4,9\} \Rightarrow \sum_{O_{1,2}} = 0$ (b).
  - $O = \{6,4,11,o_4,o_5\} \Rightarrow O_{1,2} = \{4,11\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).
  - $O = \{6,4,12,o_4,o_5\}$. By (a),$o_4 \in \{3,11\}$.
    - $O = \{6,4,12,3,o_5\} \Rightarrow O_{2,2} = \{12,3\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).
    - $O = \{6,4,12,11,o_5\} \Rightarrow O_{2,2} = \{12,11\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).
- $O = \{6,5,o_3,o_4,o_5\}$. By (a),$o_3 \in \{2,3,11,12\}$.
  - $O = \{6,5,2,o_4,o_5\} \Rightarrow O_{0,3} = \{6,5,2\} \Rightarrow \sum_{O_{0,3}} = 0$ (b).

- $O = \{6,5,3,o_4,o_5\}$. By (a),$o_4 \in \{2,4,10,12\}$.
  - $O = \{6,5,3,2,o_5\} \Rightarrow O_{2,2} = \{3,2\} \Rightarrow \sum_{O_{2,2}} = 5 = \sigma + \lambda + 1$ (d).
  - $O = \{6,5,3,4,o_5\} \Rightarrow O_{0,4} = \{6,5,3,4\} \Rightarrow \sum_{O_{0,4}} = 5 = \sigma + \lambda + 1$ (d).
  - $O = \{6,5,3,10,o_5\} \Rightarrow O_{2,2} = \{3,10\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
  - $O = \{6,5,3,12,o_5\} \Rightarrow O_{2,2} = \{3,12\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).
- $O = \{6,5,11,o_4,o_5\}$. By (a),$o_4 \in \{2,4,10,12\}$.
  - $O = \{6,5,11,2,o_5\} \Rightarrow O_{2,2} = \{11,2\} \Rightarrow \sum_{O_{2,2}} = 0$ (b).
  - $O = \{6,5,11,4,o_5\} \Rightarrow O_{2,2} = \{11,4\} \Rightarrow \sum_{O_{2,2}} = 2 = \lambda$ (c).
  - $O = \{6,5,11,10,o_5\} \Rightarrow O_{1,3} = \{5,11,10\} \Rightarrow \sum_{O_{1,3}} = 0$ (b).
  - $O = \{6,5,11,12,o_5\} \Rightarrow O_{2,2} = \{11,12\} \Rightarrow \sum_{O_{2,2}} = 10 = n - \sigma - 1$ (e).
- $O = \{6,5,12,o_4,o_5\} \Rightarrow O_{1,2} = \{5,12\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).

- $O = \{6,9,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{6,9\} \Rightarrow \sum_{O_{0,2}} = 2 = \lambda$ (c).
- $O = \{6,10,o_3,o_4,o_5\} \Rightarrow O_{0,2} = \{6,10\} \Rightarrow \sum_{O_{0,2}} = 3 = \sigma + \lambda + 1$ (d).
- $O = \{6,12,o_3,o_4,o_5\}$. By (a),$o_3 \in \{3,5,9,11\}$.
  - $O = \{6,12,3,o_4,o_5\} \Rightarrow O_{1,2} = \{12,3\} \Rightarrow \sum_{O_{1,2}} = 2 = \lambda$ (c).
  - $O = \{6,12,5,o_4,o_5\} \Rightarrow O_{1,2} = \{12,5\} \Rightarrow \sum_{O_{1,2}} = 4 = \sigma + \lambda + 1$ (d).
  - $O = \{6,12,9,o_4,o_5\}$. By (a),$o_4 \in \{3,4,10,11\}$.
    - $O = \{6,12,9,3,o_5\} \Rightarrow O_{1,3} = \{12,9,3\} \Rightarrow \sum_{O_{1,3}} = 11 = n - \sigma - 1$ (e).

* $O = \{6,12,9,4,o_5\} \Rightarrow O_{2,2} = \{9,4\} \Rightarrow \sum O_{2,2} = 0$ (b).
* $O = \{6,12,9,10,o_5\} \Rightarrow O_{1,3} = \{12,9,10\} \Rightarrow \sum O_{1,3} = 5 = \sigma + \lambda + 1$ (d).
* $O = \{6,12,9,11,o_5\} \Rightarrow O_{0,4} = \{6,12,9,11\} \Rightarrow \sum O_{0,4} = 12 = n - \sigma - 1$ (e).

– $O = \{6,12,11,o_4,o_5\} \Rightarrow O_{0,3} = \{6,12,11\} \Rightarrow \sum O_{0,3} = 3 = \lambda$ (c).

As mentioned above, we prove theorem 3.16 for odd and even values of n separately for clarity, but the statement of the theorem need not be segregated. In theorem 3.16, value conditions appear different for odd and even cases. However, in [1] Keedwell defines a value h by whether n is odd or even. In light of this, the conditions for odd or even n may be combined into the following statement.

Corollary 3.19. *Let A be as either E or O in theorem 3.16, depending on whether n is odd or even. Define* $h = 0$ *if n is odd or* $h = \frac{n}{2}$ *if n is even. Then,*

(a) For all $i \neq j, a_i \neq a_j$ *and* $a_i + a_j \neq n + 1$.

(b) $\sum A_{\sigma,\lambda} \not\equiv 0, \lambda, \sigma + \lambda + h + 1, n - \sigma - h - 1$. *modulo n.*

Construct P as described in 3.16 replacing E or O with A, depending on whether n is odd or even. Then P is an acceptable sequence generating a commutative property D cyclic neofield.

Proof. Case n is odd. Then $h = 0$, $\sigma + \lambda + h + 1 = \sigma + \lambda + 1$ and $n - \sigma - h - 1 = n - \sigma - 1$.

Case n is even. Then $h = \frac{n}{2}$, $\sigma + \lambda + h + 1 = \sigma + \lambda + \frac{n}{2} + 1 = \sigma + \lambda + \frac{n+2}{2}$ and $n - \sigma - h - 1 = n - \frac{n}{2} - \sigma - 1 = \frac{n-2}{2} - \sigma$.

This corollary is especially helpful when conducting searches with the aid of a

computer, as we may now define h in our program and use one set of criteria rather than program two different sets of criteria for odd or even cases.

Chapter 4

Subneofields of Property D Cyclic Neofields

Keedwell conjectured that property D cyclic neofields exist for all orders greater than 20. A program to find all commutative property D cyclic neofields generates 92 examples for order 21 (this accounts for mirrors/duals, but not other possible isomorphisms) and 34 examples of order 22. These numbers climb rapidly to over 50,000 examples for order 31 and over 20,000 examples for order 32. This still does not prove Keedwell's conjecture, but it does a great deal to support it. But even with modern computer processors, the extremely high volume of numbers involved in checking each possible combination make thorough examination and brute force computing of higher order examples prohibitive. It may therefore be beneficial to search for alternative ways to find high order property D cyclic neofields. It may be even more beneficial to find ways to construct them. For finite fields there is an intimate connection between the ideas of subfields and field extensions. If a field has a subfield, then it is always possible to extend the subfield to reconstruct the field. It is therefore worth examining subneofields for ideas in extending known (property D cyclic) neofields to even larger property D cyclic neofields.

Definition 4.1. Given a neofield $(N, \oplus, \cdot)$, a subset $N' \subseteq N$ is a *subneofield* if $(N', \oplus, \cdot)$ is a neofield.

Certain basic facts must be established to properly talk about subneofields. For fields, since each structure (additive and multiplicative) is a group and groups are very well studied, certain notions may seem obvious or trivial. Since the additive structure of a neofield is a proper loop, these particular trivialities are not quite so

trivial. For example, are the identities of each structure included in the substructure? Is it conceivable for a substructure to be constructed in such a way that some other element (other than the identity) is carrying out duties to form a loop? The answer is no.

Proposition 4.2. *A subneofield of a neofield contains the multiplicative and additive identities.*

Proof. Let $(N, \oplus, \cdot)$ be a neofield with additive identity of $(N, \oplus)$ as 0 and multiplicative identity of $(N - \{0\}, \cdot)$ as 1. Let N' be a subneofield of N. Then $(N', \oplus)$ is a loop with identity, say $0'$. Since the identity element of a loop is unique and since $0' \in N$, then $0' = 0$ and so $0 \in N'$. Similarly $(N' - \{0\}, \cdot)$ is a group and since the identity element of a group is unique, $1 \in H - \{0\}$.

4.1 Cycle Representation

Recall from chapter 2 that the entire additive loop structure may be stored in a single row of its Cayley table by use of the fact that for all (left) neofields $x \oplus y = x \cdot (1 \oplus x^{-1} \cdot y)$. We choose the row with the multiplicative identity and defined a presentation function $\psi : N \to N$ by this row, giving us $\psi(g) = 1 \oplus g$. As an automorphism from N to N, it is acceptable (and often very useful) to display ψ in disjoint cycle form. In particular, by closure of the operations $(\oplus)$ and $(\cdot)$, it should be clear that a subneofield that contains any element of a cycle will contain every element of the cycle. Being already aware of at least two elements that must be present in a subneofield provides an excellent foundation for examining presentation functions of a neofield for the existence or non-existence of subneofields.

Definition 4.3. The *lead cycle* of a presentation function of a neofield in disjoint cycle form is the cycle containing the multiplicative identity of the neofield.

Example 4.4. Let $\psi = (x^0 0)(x^1 x^4)(x^2 x^3)$ be the presentation function of a neofield N. Then the cycle $(x^0 0)$ is the lead cycle.

It will also be beneficial to identify the cycle that contains the additive identity, but as we show next, it is the lead cycle. (In fact it would be identically useful for us to define the lead cycle by the inclusion of the additive identity and prove the inclusion of the multiplicative).

Proposition 4.5. *A lead cycle contains the additive identity of the neofield.*

Proof. By definition, $x^0 \oplus 0 = x^0$ and therefore 0 is in the same cycle as x^0. Furthermore, if x^0 is listed first in the cycle, then 0 is listed last.

Example 4.6. The sequence $P = \{2,4,3,6,5,7\}$ generates a property D neofield of order 9 (in this case $GF(9)$) with presentation function

$$\psi = (x^0 x^4 0)(x^1 x^2 x^7)(x^3 x^6 x^5)$$

in disjoint cycle form. The cycle $(x^0 x^4 0)$ is the lead cycle with multiplicative identity listed first, and consequently the additive identity listed last.

4.2 Examples of Subfields of Small Order

On the subject of subneofields, a most natural first question is if there exists *any* subneofields for proper property D cyclic neofields. The following theorem provides an entire family of property D cyclic neofields with substructures.

Proposition 4.7. *A property D cyclic neofield of even order contains a subfield isomorphic to* $GF(2)$.

Proof. Let $(N, \oplus, \cdot)$ be a property D cyclic neofield of even order $m = n+1$. Then n is odd. By construction, $1 \oplus x^h = 0$ where $h = 0$ if n is odd.

So for the set $N' = \{0, x^0\}$ we have $0 \oplus 0 = x^0 \oplus x^0 = 0$ and $x^0 \oplus 0 = 0 \oplus x^0 = x^0$ for $(N', \oplus)$, and $0 \cdot 0 = 0 \cdot x^0 = x^0 \cdot 0 = 0$ and $x^0 \cdot x^0 = x^0$ for $(N', \cdot)$. Therefore $(N', \oplus, \cdot)$ is isomorphic to $GF(2)$.

Example 4.8. The sequence $P = \{3,4,8,5,2,6,7\}$ generates a commutative property D cyclic neofield of order 10 with presentation function

$$\psi = (x^0 0)(x^1 x^4)(x^2 x^7 x^5 x^6 x^8 x^3)$$

in disjoint cycle form. The elements in the cycle $(x^0 0)$ form a subfield isomorphic to $GF(2)$.

Thus every even order property D neofield includes a subneofield. But this is identically true for fields as every even order field contains $GF(2)$ as a subfield. So this result may not be very enlightening. However, we see a much more surprising result for many odd order property D cyclic neofields.

Proposition 4.9. *A property D cyclic neofield of odd order with a lead cycle of length* 3 *contains a subfield isomorphic to* $GF(3)$.

Proof. Let N be a property D cyclic neofield of odd order $m = n + 1$ and lead cycle $(x^0 a\ b)$. Then n is even. By construction, $x^0 \oplus x^h = 0$ where $h = \frac{n}{2}$ if n is even. As shown previously, the lead cycle contains 0 and it is listed last if x^0 is listed first, so $b = 0$ implying that $a = x^h$.

Then $x^h \oplus x^0 = x^h \cdot (x^0 \oplus x^h) = 0$ and $x^h \oplus x^h = x^h \cdot (x^0 \oplus x^0) = x^0$. So for the set $N' = \{0, x^0, x^h\}$ we have $0 \oplus 0 = x^0 \oplus x^h = x^h \oplus x^0 = 0$, $x^0 \oplus 0 = 0 \oplus x^0 = x^h \oplus x^h = x^0$ and $0 \oplus x^h = x^h \oplus 0 = x^0 \oplus x^0 = x^h$ for $(N', \oplus)$. And we have $0 \cdot g = g \cdot 0 = 0$ for all $g \in N'$, $x^0 \cdot x^h = x^h \cdot x^0 = x^h$ and $x^0 \cdot x^0 = x^h \cdot x^h = x^0$ for $(N', \cdot)$. Therefore $(N', \oplus, \cdot)$ is isomorphic to $GF(3)$.

Example 4.10. The (non-commutative) property D cyclic neofield of order 17 with presentation function (in disjoint cycle form)

$$\psi = (x^0x^80)(x^1x^2x^9x^{13}x^{12}x^6)(x^3x^5)(x^4x^{10}x^{15}x^{11}x^{14}x^7)$$

has a subfield isomorphic to $GF(3)$.

Example 4.11. The (commutative) property D cyclic neofield of order 25 with presentation function

$$\psi = (x^0x^{12}0)(x^1x^8x^{14}x^{17}x^{21}x^{19}x^{13}x^{15}x^{11}x^2)(x^3x^{22}x^{23}x^7x^4x^9x^{20}x^5x^{18}x^{10})(x^6x^{16})$$

has a subfield isomorphic to $GF(3)$.

Both of these examples illustrate that the order of a subneofield does not necessarily divide the order of the neofield, in contrast to the theorem of Lagrange for groups.

4.3 Subneofields

For a finite field of order, say p^k, the possible order of a subfield is restricted not just by p but also by k. For example, $GF(16)$ has both $GF(2)$ and $GF(4)$ as subfields, but not $GF(8)$. Examples 4.10 and 4.11 above illustrate that for neofields we should not take restrictions such as these for granted. Fortunately, the multiplicative structure of a neofield is a group so we have an established basis for studying subneofields. For example, Paige [5] proved that the center of any admissible group is admissible. For any group, the order of a subgroup must divide the order of the group, and this leads us to some foundational results.

Proposition 4.12. *A subneofield of a neofield of even order is of even order.*

Proof. Let N be a neofield of even order $m = n+1$ and subneofield N'. Then $N - \{0\}$ is a group of order n with $N' - \{0\}$ a subgroup of order, say k. By Theorem of Lagrange for groups, k must divide n, and since n is odd, so is k. Therefore, the order of N' is $k+1$ which is even.

Proposition 4.13. *A subneofield of a cyclic neofield of odd order is of odd order.*

Proof. Let N be a cyclic neofield of odd order $m = n+1$ and subneofield N' with order $m' = n'+1$. Then n is even and n' divides n (by Lagrange). Let x^r be a generator of $N' - \{0\}$ where r is the lowest value such that $n'r \equiv 0 \bmod n$, so $n'r = n$. By construction of a cyclic neofield, $1 \oplus x^h = 0$ where $h = \frac{n}{2}$ if n is even. By unique solubility of equations in the additive loop, and since $0 \in N'$, we have $x^{\frac{n}{2}} \in N'$. Then there must be some k such that $kr = \frac{n}{2} \Rightarrow 2kr = n = n'r \Rightarrow 2k = n' \Rightarrow n'$ is even. Since n' is even, $m' = |N'|$ is odd.

Example 4.14. For a cyclic neofield of order 25, any subneofield must be of orders $3, 5, 7, 9$ or 13. There is no subneofield of order 4, even though 3 divides 24.

We have established that examining cycles is important in determining the presence of a subneofield. By necessity, if a subneofield exists, then every element in the lead cycle is an element in the subneofield. But there exists the possibility of more interesting cases where the subneofield may be composed of more than one cycle.

Proposition 4.15. *A cyclic neofield of order* $4k+1$ *does not contain a subneofield of order* 5 *with presentation function disjoint cycles of length 3 and 2.*

Proof. Let N be a cyclic neofield of order $4k+1$. Suppose by contradiction that N has a subneofield of order 5 with disjoint cycles of length 3 and 2, say $(x^0\ x^{\frac{n}{2}}\ 0)(a\ b)$. Because $(N - \{0\}, \cdot)$ is a cyclic group, $a, b \in \{x^{\frac{n}{4}}, x^{\frac{3n}{4}}\}$. Regardless

of which is which, by the presentation function we have that $x^0 \oplus x^{\frac{n}{4}} = x^{\frac{3n}{4}}$. But then we have $x^{\frac{n}{4}} \oplus x^{\frac{n}{4}} = x^{\frac{n}{4}} \cdot (x^0 \oplus x^0) = x^{\frac{n}{4}} \cdot x^{\frac{n}{2}} = x^{\frac{3n}{4}}$. This indicates that $(N, \oplus)$ does not have unique solubility of equations and so is not a loop.

Example 4.16. The (commutative) property D cyclic neofield of order 21 with presentation function

$$\psi = (x^0 x^{10} 0)(x^1 x^6)(x^2 x^{15} x^{11} x^{18} x^{19} x^3 x^{17} x^8 x^{14} x^{13} x^{16} x^5)(x^4 x^{12})(x^7 x^9)$$

has no subneofield of order 5. Aside from the more obvious lack of an $(x^5 x^{15})$ or $(x^{15} x^5)$ cycle, proposition 4.15 ensures that no such example exists.

There are also other indicators in the presentation function that a subneofield is not present.

Proposition 4.17. *For any cyclic neofield, a subneofield that contains x^1 (the generator of the cyclic group) as an element is the entire cyclic neofield.*

Proof. Let N be a cyclic neofield with subneofield N' and $x^1 \in N'$. Because $N' - \{0\}$ is a group, any nonzero element $x^k \in N$ is $(x^1)^k$ which is also in N' by closure..

Example 4.18. The (commutative) property D cyclic neofield of order 25 with presentation function

$$\psi = (x^0 x^{12} 0)(x^1 x^4 x^{22} x^{15})(x^2 x^{17} x^6 x^8 x^7 x^{13} x^9 x^{10} x^5 x^{21} x^{11} x^{20} x^{18})(x^3 x^{14} x^{19} x^{16} x^{23})$$

has no subneofield of order 7. The presence of x^1 in the cycle $(x^1 x^4 x^{22} x^{15})$ indicates that if this cycle is part of a subneofield, then the subneofield is the entire neofield.

Proposition 4.19. *For any cyclic neofield, a subneofield that contains consecutive elements of the multiplicative group is the entire cyclic neofield.*

Proof. Let N be a cyclic neofield with subneofield N' and $x^k, x^{k+1} \in N'$. By closure of the group $(N' - \{0\}, \cdot)$, $x^{k+1} \cdot x^{-k} = x^1$ is also in N'. As shown previously, this implies that $N' = N$.

Example 4.20. The (commutative) property D cyclic neofield of order 25 with presentation function

$$\psi = (x^0x^6x^7x^9x^{12}0)(x^1x^{21}x^{11}x^{15}x^3x^{14}x^{13}x^4x^{22}x^{17}x^2x^{19}x^5x^{10}x^{23}x^{20}x^{18})(x^8x^{16})$$

has no proper subneofield. The presence of x^6 and x^7 in the lead cycle indicates that if this cycle is part of a subneofield, then the subneofield is the entire neofield.

Proposition 4.21. *For any cyclic neofield of order $m = n+1$, a subneofield that contains x^p as an element, where p is relatively prime to n, is the entire cyclic neofield.*

Proof. Let N be a cyclic neofield with subneofield N' and $x^p \in N'$. Because $N - \{0\}$ is a cyclic group of order n, and p is relatively prime to n, any nonzero element $x^q \in N$ can be expressed as $(x^p)^k$ for some integer k. And since $x^p \in N'$ and $N' - \{0\}$ is a cyclic group, $x^q = (x^p)^k \in N'$ by closure. Therefore $N \subseteq N'$ and so $N = N'$.

Example 4.22. The (commutative) property D cyclic neofield of order 21 with presentation function

$$\psi = (x^0x^7x^{12}x^{18}x^{10}0)(x^1x^2x^{16}x^9x^{17})(x^3x^{19}x^{14}x^5x^4x^6x^{15}x^{13})(x^8x^{11})$$

has no proper subneofield. Because 7 is relatively prime to 20, the presence of x^7 in the lead cycle prohibits the possibility of a proper subneofield.

Often while searching for examples of subneofields of property D cyclic neofields of order 25, there were lead cycles of length 5 that were different in appearance - specifically $(x^0x^6x^{18}x^{12}0)$ and $(x^0x^{18}x^6x^{12}0)$. Both generate subneofields of order 5, and as we show below, they are in fact both subfields isomorphic to $GF(5)$.

Proposition 4.23. *If $(N,\oplus,\cdot)$ is a cyclic neofield of order $4k+1$ with a length 5 lead cycle that generates a subneofield N', then N' is isomorphic to $GF(5)$.*

Proof. Let N be a cyclic neofield of order $4k+1$ $(n=4k)$ with lead cycle $(1\ a\ b\ c\ 0)$ that generates a subneofield N'. Then the Cayley table for $(N',\oplus)$ is as follows

$\oplus$	0	1	a	b	c
0	0	1	a	b	c
1	1	a	b	c	0
a	a	$a\cdot(1\oplus 1/a)$	$a\cdot(1\oplus 1)$	$a\cdot(1\oplus b/a)$	$a\cdot(1\oplus c/a)$
b	b	$b\cdot(1\oplus 1/b)$	$b\cdot(1\oplus a/b)$	$b\cdot(1\oplus 1)$	$b\cdot(1\oplus c/b)$
c	c	$c\cdot(1\oplus 1/c)$	$c\cdot(1\oplus a/c)$	$c\cdot(1\oplus b/c)$	$c\cdot(1\oplus 1)$

Since $1\oplus x^{\frac{n}{2}}=0$, we have that $c=x^{\frac{n}{2}}$ and since $N'-\{0\}$ is a cyclic group of four elements we have that $a,b\in\{x^{\frac{n}{4}},x^{\frac{3n}{4}}\}$. Reducing these expressions (for example $a\cdot(1\oplus c/a)=a\cdot(1\oplus a)=a\cdot b=1$), then the Cayley table simplifies as follows

$\oplus$	0	1	a	b	c
0	0	1	a	b	c
1	1	a	b	c	0
a	a	b	c	0	1
b	b	c	0	1	a
c	c	0	1	a	b

This is clearly isomorphic of $\mathbb{Z}_5$. Since $(N', \oplus)$ is a cyclic group of order 5 and $(N' - \{0\}, \cdot)$ is a cyclic group of order 4 with distribution inherited from N, N' is a field of order 5 isomorphic to $GF(5)$.

4.4 The Goal of Embedding Property D Cyclic Neofields into Larger Property D Cyclic Neofields.

In searching for substructures of property D cyclic neofields, no examples of subneofields of order greater than 5 emerged. The search of commutative property D cyclic neofields of order 25 was exhaustive, but the search through non-commutative was far from it. (Roughly estimated to take multiple years on a single computer). It therefore might be more beneficial to attempt to construct one rather than searching through thousands of examples. However, in attempting to construct an order 25 property D cyclic neofield with an order 13 subneofield an impossibility surfaces. More generally, we have this result.

Proposition 4.24. *A property D cyclic neofield of order* $2k+1$ *has no subneofield of order* $k+1$.

Proof. By contradiction, let $(N, \oplus, \cdot)$ be a property D cyclic neofield of order $2k+1$with a subneofield N' of order $k+1$. Let x be the generator of $(N, \cdot)$; so the

elements of N' are precisely the k elements of N of the form x^{2h} for $0 \leq h \leq k-1$. By closure of N' we have $x^0 \oplus x^{2h} = x^{2i}$ for some $0 \leq i \leq k-1$. This means that every even value exponent from x^0 through x^{2k-2} is mapped to an even value exponent by the presentation function. Consequently, the odd value exponents map to odd value exponents, so $x^0 \oplus x^{2h+1} = x^{2j+1}$. Thus, for every $0 \leq r,s \leq 2k$, the difference $\frac{x^0 \oplus x^{r+1}}{x^0 \oplus x^r}$ is an odd valued exponent and the difference $\frac{x^0 \oplus x^{s+1}}{x^0 \oplus x^s}$ is also an odd valued exponent. Then there are $2k$ odd differences, yet only k possible odd values, so there must exist some $r \neq s$ such that $\frac{x^0 \oplus x^{r+1}}{x^0 \oplus x^r} = \frac{x^0 \oplus x^{s+1}}{x^0 \oplus x^s}$ and therefore N does not have property D.

Example 4.25. Suppose there exists a property D cyclic neofield $(N, \oplus, \cdot)$ of order 17 with a subneofield $(N', \oplus, \cdot)$ of order 9 generated by the sequence $P = \{2,3,4,5,6,7\}$(example 3.13). Then the presentation function of N' is $\psi'(y) = (y^0 y^2 y^5 y^1 y^7 y^6 y^3 y^4 0)$. The multiplicative group of N' is a cyclic subgroup of the cyclic multiplicative group of N, so the corresponding $(y = x^2)$ exponents in the lead cycle of N will be even valued exponents $(x^0 x^4 x^{10} x^2 x^{14} x^{12} x^6 x^8 0)$. This accounts for all even exponents, indicating that evens map to evens, and so odds must map to odds. Looking at the difference in exponents, we have that $\psi(x^1)$ has an odd exponent and $\psi(x^0)$ has an even exponent, thus $\frac{\psi(x^1)}{\psi(x^0)}$ must have an odd exponent. Similarly, $\psi(x^2)$ has an even exponent, thus $\frac{\psi(x^2)}{\psi(x^1)}$ has an odd exponent, and so on. This illustrates that all differences (16 in total) must have an odd exponent, but there are only eight odd values available. So the difference in exponents between some consecutive elements must be duplicates, and this contradicts the requirement for a property D cyclic neofield.

Bibliography

[1] A.D. Keedwell: *Construction, properties and applications of finite neofields*, Commentationes Mathematicae Universitatis Carolinae 41,2 (2000), 283-297

[2] A.D. Keedwell: *On orthogonal latin squares and a class of neofields*, Rendiconti di Matematica (5) Vol 25 (1966), 519-561

[3] A.D. Keedwell: *On property D neofields*, Rendiconti di Matematica (3-4) Vol 26 (1967), 383-402

[4] A.D. Keedwell: *On property D neofields and some problems concerning orthogonal latin squares,* Computational Problems in Abstract Algebra (1969), 315-319

[5] L.J. Paige, *Neofields*, Duke Mathematical Journal, 16 (1949), 39-60

Biographical Information

Scott Lacy's academic career spanned 25 years from 1990 to 2015, attending Houston Community College, Texas A&M University, Mesa Community College and Tarrent County College at various times and for various lengths of time. In 2007 he enrolled at University of Texas at Arlington and in 2009 earned his Bachelor of Science in Mathematics. As a graduate student in mathematics at University of Texas at Arlington he studied non-associative algebra. In 2011 he was selected for two-year participation in the NSF MAVS GK-12 program, spending ten hours each week in a Title I middle or high school as a mathematician in residence, supplementing mathematical instruction for predominantly under-represented populations. He is also a proud veteran of the U.S. Army and Texas National Guard.