

ON THE NUMBER OF CONJUGATES

OF TERNARY QUASIGROUPS

ON THE NUMBER OF CONJUGATES
OF TERNARY QUASIGROUPS

By

MARY ELIZABETH (DEUTSCH) McLEISH, B.Sc, M.Sc.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements

for the Degree

Doctor of Philosophy

McMaster University

1976

DOCTOR OF PHILOSOPHY (1976)
(Mathematics)

McMASTER UNIVERSITY
Hamilton, Ontario

TITLE: On the Number of Conjugates of Ternary
Quasigroups

AUTHOR: Mary Elizabeth (Deutsch) McLeish,
B.Sc. (Hon.) (Queen's University)
M.Sc. (McMaster University)

SUPERVISOR: Professor A. Rosa

NUMBER OF PAGES: vii, 106

Abstract

An n -ary quasigroup is a set together with an n -ary operation which is cancellative in every variable. To every permutation on $n + 1$ elements there is associated a conjugate quasigroup of the original quasigroup. The elements of both quasigroups are the same, but the conjugate n -ary operation is defined as follows. It acts on a permuted set of elements to produce a permutation of the result of the original operation on the unpermuted elements.

These conjugate quasigroups need not be distinct. The number of distinct such conjugates is called the conjugacy class number of the quasigroup. It has been shown that this number must always be a divisor of $(n+1)!$

In the case of ordinary quasigroups, it is known that for any order greater than or equal to four, there exists a quasigroup of that order having a specified number of distinct conjugates. An investigation of the conjugacy class number leads to a study of quasigroup identities. The existence of quasigroups satisfying certain identities has been widely investigated for ordinary quasigroups, but for higher dimensional quasigroups, much less is known.

We investigate the existence of ternary quasigroups having a given class number. In all but two cases, the question is completely answered. Ternary quasigroups, having six of the possible eight class numbers, are shown to exist of every order, except for a small, finite number of low orders. In the remaining two cases, infinitely many quasigroups have been constructed with these

conjugacy class numbers.

An investigation is begun of the existence of n -ary quasigroups with prescribed conjugacy class numbers. The problem is solved for two sets of classes and for n -ary quasigroups having sufficiently large orders.

A combination of methods is used throughout, varying from exact constructions, to "ad hoc" constructions for low orders and adaptations of block designs.

Acknowledgments

The author wishes to thank her supervisor, Dr. A. Rosa, for his advice and patience in the preparation of this thesis. The author would also like to thank McMaster University for financial assistance and Ms. Olwyn Buckland for her prompt and efficient typing of the manuscript.

Table of Contents

| | | |
|--------------|---|----|
| Introduction | | 1 |
| Chapter 1 | Basic Concepts | 7 |
| | §1.1 Quasigroups and n-ary Quasigroups | 7 |
| | §1.2 Conjugates | 12 |
| | §1.3 Block Designs and Steiner Systems | 18 |
| Chapter 2 | The Classification of Identities for Ternary Quasigroups | 27 |
| | §2.1 Permutation Classification | 27 |
| | §2.2 A Breakdown of Class Numbers by Subgroups | 29 |
| Chapter 3 | The Existence of Ternary Quasigroups with 1, 3, 4, 6, 12, or 24 Conjugacy Classes | 33 |
| | §3.1 Twenty-Four Classes | 33 |
| | §3.2 Twelve Classes | 43 |
| | §3.3 Six Classes | 52 |
| | §3.4 Four Classes | 57 |
| | §3.5 Three Classes | 62 |
| | §3.6 One Class | 63 |
| | §3.7 Conclusion | 63 |
| Chapter 4 | The Existence of Ternary Quasigroups with 2 or 8 Conjugacy Classes | 66 |
| | §4.1 The Structure of Ternary Quasigroups having 2 or 8 Conjugacy Classes | 66 |
| | §4.2 The Case of 2 or 8 Conjugacy Classes for Orders ≤ 5 | 69 |
| | §4.3 The Case of 2 or 8 Conjugacy Classes for Orders 8 and 10 | 74 |
| | §4.4 Conclusion | 86 |
| Chapter 5 | The Existence of an n-ary Quasigroup with a Specified Number of Conjugacy Classes | 88 |
| | §5.1 Conjugacy Classes of Size $\frac{(n+1)!}{q!}$, where $q = 1, 2, \dots, n + 1$ | 88 |

| | | |
|------|--|-----|
| §5.2 | The Cases of $\frac{n(n+1)}{2}$ and $\frac{(n+1)!}{[(\frac{n}{2})!]^2 (\frac{n+2}{2})}$, n even, Conjugacy Classes | 96 |
| §5.3 | Conclusion | 102 |
| | Bibliography | 103 |

INTRODUCTION

This thesis studies certain algebraic identities for ternary and n -ary quasigroups, which in turn provide information about the conjugates of the quasigroups. The central question is: Given any divisor q of $4!$, does there exist a ternary quasigroup with exactly q distinct conjugates?

Briefly, a quasigroup (Q, \circ) is a set Q together with a binary, cancellative operation \circ ; an n -ary quasigroup $(Q, \langle \rangle)$ is a set Q together with an n -ary operation, $\langle \rangle$, which is cancellative in every position. To every permutation $\pi \in S_{n+1}$, there is associated a conjugate quasigroup $(Q, \langle \rangle_{\pi})$, defined by $\langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle_{\pi} = a_{\pi(n+1)}$ if and only if $\langle a_1, \dots, a_n \rangle = a_{n+1}$ in $(Q, \langle \rangle)$, for every a_1, \dots, a_n, a_{n+1} in Q . If $(Q, \langle \rangle_{\pi_1}) = (Q, \langle \rangle_{\pi_2})$ for two different permutations π_1 and π_2 , the conjugates (and correspondingly the permutations) are said to be in the same (equivalence) class and the number of distinct conjugates of $(Q, \langle \rangle)$ (or non-equivalent members of S_{n+1}) is called the conjugacy class number.

Conjugates have been studied by S.K. Stein [43] and more recently by C.C. Lindner and D. Steedley [33]. Lindner and Steedley completely answer the question of the existence of ordinary quasigroups with a prescribed conjugacy class number in [33], and there pose the same questions for ternary

quasigroups.

Lindner and Steedley made significant use of the singular direct product of quasigroups (see [27], [40]; see also [34]). However, many attempts were made by the author to extend this product in a natural way to three dimensions. Some parts of the definition do extend in a straightforward fashion, but it was discovered that a complete extension was impossible. If a $7 \times 7 \times 7$ cube (the Cayley representation of a ternary quasigroup) was filled in, in all the positions covered by an obvious extension of the definition, then it was impossible, in any way, to complete the cube to represent a ternary quasigroup. (The impossibility of an extension of the singular direct product to the ternary case can be deduced, essentially, also from [12].)

This necessitated an entirely different approach to the ternary case. A combination of algebraic and basic construction methods are used. In particular, in the case of 2 and 8 conjugacy classes, an adaptation of Steiner quadruple systems (a 3-design with $\lambda = 1$, $k = 4$) is used.

The thesis consists of an introduction and five chapters. Chapter 1 contains the basic definitions and background information. Chapters 2, 3 and 4 discuss ternary quasigroups exclusively and Chapter 5 deals with the general n -ary quasigroup case.

Chapter 2 sets out explicitly the relationship between quasigroup identities, permutations in S_4 , and conjugacy classes. Table 2.1.1 lists the identities and §2.2 arranges these identities into the necessary subsets, corresponding to the different conjugacy class numbers.

In Chapter 3, it is proven that ternary quasigroups of order n with 6, 12 or 24 conjugacy classes exist if and only if $n \geq 4$. For 3 or 4 conjugacy classes, it is shown that the order n must be ≥ 3 . And finally, there always ($n \geq 1$) exists a ternary quasigroup with 1 conjugacy class. The existence problem for the class numbers of Chapter 3 is thus completely solved.

Chapter 4 deals with the remaining cases of 2 and 8 conjugacy classes. It is here that ad hoc constructions and quadruple systems are used. A ternary quasigroup of order n having exactly 2 or 8 conjugacy classes is shown to exist if $n \equiv 0 \pmod{8}$, $n \equiv 0$ or $5 \pmod{10}$ or $n \equiv 4, 8$ or $10 \pmod{12}$, provided $n \geq 5$. If $n < 5$, there does not exist any ternary quasigroup with 2 or 8 conjugacy classes.

In the process of obtaining these results, occasionally alternate methods are given, depending on a different choice of quasigroup identities. However, an attempt was not made to construct quasigroups satisfying all the possible combinations of identities arising from the subgroups of S_4 ,

as this is not part of the basic existence problem.

In passing, the generalized idempotent law, $\langle x, x, y \rangle = y$, whose spectrum is not yet known, is discussed and a construction made. (See §3.2.3 and references [30] and [31].) The generalized idempotent and commutative ternary quasigroup ($\langle x, y, z \rangle = \langle x, z, y \rangle = \langle y, x, z \rangle$) is shown to exist for all orders $n \equiv 2$ or $4 \pmod{6}$ and only those n (§3.4). In §3.1.9, a simpler method to that given in [33], is used to construct ordinary quasigroups having six conjugacy classes.

Concluding remarks follow Chapters 3 and 4 and containing the main Theorems of these Chapters, namely Theorems 3.7.3 and 4.4.5 respectively.

In Chapter 5, n -ary quasigroups are discussed. This is intended only as an introduction to the problem, as this thesis' primary purpose is to solve the problem of conjugacy classes for 3-quasigroups. Remark 5.1.2 further explains the problems encountered here and why the general case is discussed at the end of this thesis, rather than being considered initially, allowing 3-quasigroups as a special case.

The first result obtained in Chapter 5, Section 5.1, is that for sufficiently large orders m (that is, for every order $m \geq m_j(n)$, where $m_j(n)$ is a certain constant) there exists an n -ary quasigroup of order m with exactly $(n+1)!/j!$ distinct conjugates (where $j = 1, 2, \dots, n+1$).

In particular, if $j = 1$, the constant $m_{j(1)}$ does not exceed $4(n-1)^2$. It is also shown in §5.2 that for sufficiently large $m_{(n)}$, there exist n -ary quasigroups of every order $m \geq m_{(n)}$ with exactly $n(n+1)/2$ or $[(n+1)!] / [(\frac{n+2}{2})(\frac{n}{2}!)^2]$, n even, conjugacy classes. Concluding remarks are made following the completion of Chapter 5.

This thesis was made more difficult by the fact that there did not already exist a wide variety of construction methods for ternary quasigroups, as is the case for ordinary quasigroups. Algebraic identities satisfied by ordinary quasigroups have been very well investigated. (See [8].)

Some work has been done on special types of latin cubes by J. Arkin [1], [2]; J. Arkin and Hoggatt, Jr. [3], [4]; and J. Arkin and E.G. Straus [5]. Similar work has been done by J. Hendricks [17], [18], [19], [20]; J. Meeus [37], and P.D. Warrington [44]. However, any constructions used by these authors were of little help to the particular problem of this thesis. Still looking at the representation as a cube, one may consult A. Heppes and P. Révész in [21], K. Brownlee and P. Loraine in [6], and A. Cruse in [7]. More closely resembling the approach of this thesis are the papers by T. Evans [10], [11]; L. Humbolt [22], C.C. Lindner [29], [30], and F. Radó and M. Hosszú [39]. Some of these will be mentioned more explicitly in the ensuing text.

In summary, this thesis solves the conjugacy problem in the ternary case for all classes and orders, with two exceptions. In the case of quasigroups having 2 or 8 distinct conjugates, some infinite sets of such quasigroups have been obtained. It also brings an investigation of the conjugacy classes of n -ary quasigroups. In some cases, the results obtained show that an n -quasigroup with a given number of conjugacy classes exists for every sufficiently large order.

CHAPTER 1

Basic Concepts

This chapter contains known results and information deduced from them, as well as definitions and explanations to be used later in the thesis. It is arranged in three main parts, discussing quasigroups, conjugacy classes and block designs respectively.

§1.1 Quasigroups and n-ary quasigroups.

Definition 1.1.1. A quasigroup (Q, \circ) is a set Q , together with a binary operation \circ such that $a \circ b = a \circ c$ implies $b = c$ and $b \circ a = c \circ a$ implies $b = c$ for all $a, b, c \in Q$.

The cardinality of Q is called the order of the quasigroup. We will consider finite sets Q only.

One would often like to consider quasigroups satisfying a given set of algebraic identities. Such quasigroups are given special names accordingly.

A Steiner quasigroup ([8]) is a quasigroup (Q, \circ) in which the following identities hold:

- (1) $x \circ x = x, \forall x \in Q$; idempotent law
- (2) $x \circ (x \circ y) = y, \forall x, y \in Q$; Sade's left "keys" law
- (3) $x \circ y = y \circ x, \forall x, y \in Q$; commutative law.

Definition 1.1.2. An n -ary quasigroup $(Q, \langle \rangle)$ is a set Q together with an n -ary operation $\langle \rangle$, such that if $\langle a_1, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_n \rangle = d$ and $\langle a_1, \dots, a_{j-1}, a_j', a_{j+1}, \dots, a_n \rangle = d$, then one must have $a_j = a_j'$, where all the a_i, a_j' and d belong to Q . In other words, the operation must be cancellative in every position.

If $n = 3$, $(Q, \langle \rangle)$ is called a ternary quasigroup, 3-quasigroup or 3-skein ([10]).

A Steiner 3-skein ([29]) is a ternary quasigroup $(Q, \langle \rangle)$ satisfying:

- (1) $\langle x, x, y \rangle = y$, $\forall x, y \in Q$; generalized idempotent law.
- (2) $\langle x, y, \langle x, y, z \rangle \rangle = z$, $\forall x, y, z \in Q$; Steiner's law.
- (3) $\langle x, y, z \rangle = \langle x, z, y \rangle = \langle y, x, z \rangle$, $\forall x, y, z \in Q$; generalized commutative law.

Definition 1.1.3. Latin cubes, k -cubes, permutation cubes and variational cubes:

A 3-dimensional latin cube of order m is an $m \times m \times m$ matrix [an n -dimensional latin cube is an $\underbrace{[m \times m \times m \dots m]}_{n \text{ times}}$ matrix, respectively], the elements of which are the integers $0, 1, 2, \dots, m-1$ and such that every line of the matrix contains a permutation of $0, 1, 2, \dots, m-1$.

Remark. There is some lack of consistency in the terminology

used. Dénes and Keedwell ([8]) would call a cube as defined above a "permutation cube" and would define a latin cube as follows: An $m \times m \times m$ three dimensional matrix comprising m layers each having m rows and m columns, such that it has m distinct elements each repeated m^2 times and so arranged that in each layer parallel to each of the three pairs of opposite faces of the cube all the m distinct elements appear and each is repeated exactly m times in that layer. A 3-regular latin cube becomes a permutation cube and the terms 2,1, 0-regular are reserved for the possibilities of repeating elements within a column in 1, 2 or 3 directions.

Our definition of latin cube corresponds to the Cayley table of n -ary quasigroups (although the set of elements in the table may not be $\{0,1,\dots,m-1\}$, but any set of m distinct elements) and hence corresponds to the usual terminology when $n = 2$. It is this definition that will be used throughout.

§1.1.4. Representations of an n -ary quasigroup or latin k -cube by diagrams.

Diagrams 1 and 2 are the more usual methods of representing a ternary quasigroup ([8]). Diagram 3 is a more compact version.

"A ternary quasigroup of order three"

$$(Q, \langle \cdot, \cdot, \cdot \rangle), Q = \{1, 2, 3\}$$

Diagram 1

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |
| 3 | 1 | 2 |

FACE 1

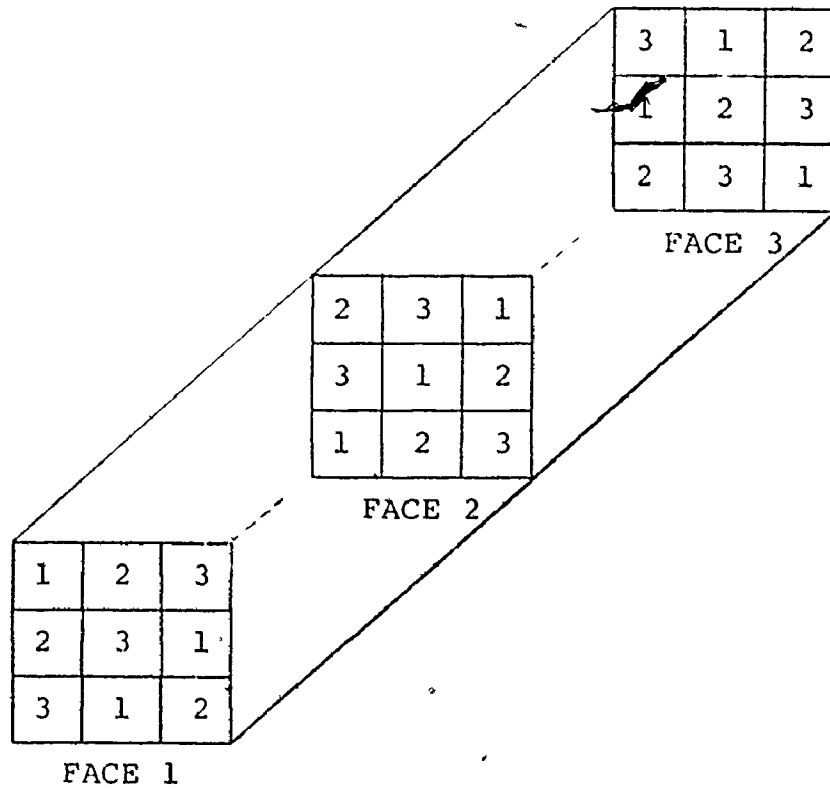
| | | |
|---|---|---|
| 2 | 3 | 1 |
| 3 | 1 | 2 |
| 1 | 2 | 3 |

FACE 2

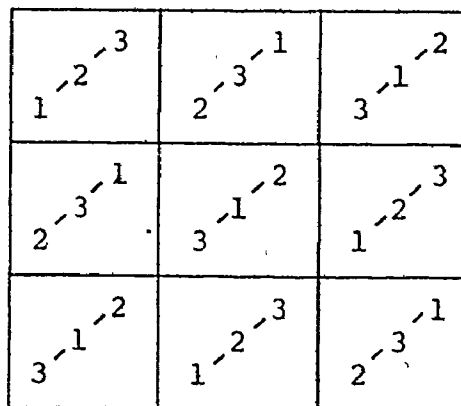
| | | |
|---|---|---|
| 3 | 1 | 2 |
| 1 | 2 | 3 |
| 2 | 3 | 1 |

FACE 3

Here the faces are determined by fixing the third element. That is, face 1 is really the Cayley table of the ordinary quasigroup defined by $x \circ y = z$ if and only if $\langle x, y, 1 \rangle = z$ in the ternary quasigroup, and similarly for faces 2 and 3. For example, $\langle 2, 3, 3 \rangle = 3$, $\langle 1, 3, 2 \rangle = 1$ and $\langle 3, 2, 1 \rangle = 1$.

Diagram 2Diagram 3

Here, face 1 appears in the lower left-hand corner, followed diagonally back, by faces 2 and 3.



Definition 1.1.5. An n -ary quasigroup $(P, \langle \rangle_P)$ is called a subquasigroup of an n -ary quasigroup $(Q, \langle \rangle_Q)$ if $P \subseteq Q$ and $\langle a_1, a_2, \dots, a_n \rangle_P = \langle a_1, a_2, \dots, a_n \rangle_Q$ for all $a_1, \dots, a_n \in P$.

If a quasigroup $(P, \langle \rangle_P)$ is a subquasigroup of $(Q, \langle \rangle_Q)$, we say that $(P, \langle \rangle_P)$ is contained in $(Q, \langle \rangle_Q)$ or that $(P, \langle \rangle_P)$ has been embedded in $(Q, \langle \rangle_Q)$.

Definition 1.1.6. Two quasigroups (Q_1, \circ) and (Q_2, \times) are said to be isotopic if there exists an ordered triple of one-to-one maps (θ, ϕ, ψ) of Q_1 onto Q_2 such that $(\theta(x)) \times (\phi(y)) = \psi(x \circ y)$ for all $x, y \in Q_1$. If $\theta = \phi = \psi$, the quasigroups are said to be isomorphic (cf. [8], p. 23).

If $(Q_1, \langle \rangle_1)$ and $(Q_2, \langle \rangle_2)$ are two n -ary quasigroups, they are said to be isomorphic if there exists a one-to-one map θ of Q_1 onto Q_2 such that $\langle \theta(a_1), \dots, \theta(a_n) \rangle_2 = \theta \langle a_1, \dots, a_n \rangle_1$ for all $a_1, \dots, a_n \in Q_1$.

§1.2 Conjugatès.

Definition 1.2.1. Let (Q, \circ) be a finite quasigroup. On the set Q define the six binary operations $\circ(1,2,3)$, $\circ(1,3,2)$, $\circ(2,1,3)$, $\circ(2,3,1)$, $\circ(3,1,2)$ and $\circ(3,2,1)$ as follows:

$$a \circ b = c \text{ if and only if:}$$

$$a \circ (1, 2, 3) b = c ,$$

$$a \circ (1, 3, 2) c = b ,$$

$$b \circ (2, 1, 3) a = c ,$$

$$b \circ (2, 3, 1) c = a ,$$

$$c \circ (3, 1, 2) a = b ,$$

$$c \circ (3, 2, 1) b = a .$$

The six, not necessarily distinct, quasigroups $(Q, \circ(i, j, k))$ are called conjugates or parastrophes of (Q, \circ) (see, e.g. [33], [8]). The set of conjugates of (Q, \circ) is denoted by $C(Q, \circ)$.

To illustrate that the six conjugates of a given quasigroup (Q, \circ) need not be distinct, consider the following example:

| | | | |
|---------|---|---|---|
| \circ | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 3 | 1 | 2 |
| 3 | 2 | 3 | 1 |

 (Q, \circ)

| | | | |
|------------------|---|---|---|
| $\circ(2, 1, 3)$ | 1 | 2 | 3 |
| 1 | 1 | 3 | 2 |
| 2 | 2 | 1 | 3 |
| 3 | 3 | 2 | 1 |

 $(Q, \circ(2, 1, 3))$

| | | | |
|------------------|---|---|---|
| $\circ(1, 3, 2)$ | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 1 |
| 3 | 3 | 1 | 2 |

 $(Q, \circ(1, 3, 2))$

| | | | |
|------------------|---|---|---|
| $\circ(2, 3, 1)$ | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 1 |
| 3 | 3 | 1 | 2 |

 $(Q, \circ(2, 3, 1))$

$$\circ(3,1,2)$$

| | | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 1 |
| 3 | 3 | 1 | 2 |

$(Q, \circ(3,1,2))$

$$\circ(3,2,1)$$

| | | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 3 | 1 | 2 |
| 3 | 2 | 3 | 1 |

$(Q, \circ(3,2,1))$

$C(Q, \circ)$ has only three distinct members. $C(Q, \circ)$ may also be thought of as a set of conjugacy classes of (Q, \circ) , where here $\{(Q, \circ(2,1,3))\}$, $\{(Q, \circ), (Q, \circ(3,2,1))\}$, and $\{(Q, \circ(1,3,2)), (Q, \circ(3,1,2)), (Q, \circ(3,1,2))\}$ are the three classes. The permutations, π , may also be arranged into (equivalence) classes according to $\pi_1 = \pi_2$ if and only if $(Q, \circ_{\pi(1)}) = (Q, \circ_{\pi(2)})$.

$|C(Q, \circ)|$ is called the conjugacy class number of (Q, \circ) .

Definition 1.2.2. Let $(Q, \langle \rangle)$ be an n -ary quasigroup where $\langle a_1, a_2, \dots, a_n \rangle = a_{n+1}$ (or d), $a_i, d \in Q$, $i = 1, 2, \dots, n+1$. Let π be any member of S_{n+1} . Then $(Q, \langle \rangle_{\pi})$ is defined by $\langle a_1, \dots, a_n \rangle = a_{n+1}$ if and only if $\langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle_{\pi} = a_{\pi(n+1)}$.

The following theorem (and its proof) is an extension of a result in [33], where the statement has been proven for $n = 2$.

Theorem 1.2.3. The conjugacy class number $|C(Q, \langle \rangle)|$ is always a divisor of $(n+1)!$ (that is $\frac{(n+1)!}{|C(Q, \langle \rangle)|}$ is an integer for all $n \geq 2$).

Proof: Let S_{n+1} denote the symmetric group on $\{1, 2, \dots, n, n+1\}$. Let F be the set of all $\alpha \in S_{n+1}$ such that $\langle \rangle_\alpha = \langle \rangle$. In other words, the new operation $\langle \rangle_\alpha$ results in the same quasigroup as the original operation $\langle \rangle$. Then F is a subgroup of S_{n+1} .

For let $\alpha, \beta \in F$. Then $\langle \rangle_{\alpha\beta} = (\langle \rangle_\alpha)_\beta = (\langle \rangle_\beta) = \langle \rangle$. Now $\langle \rangle_\alpha = \langle \rangle_\beta$ if and only if α and β belong to the same (right) coset of F in S_{n+1} . For if $\langle \rangle_\alpha = \langle \rangle_\beta$, then $\langle \rangle_{\alpha\beta^{-1}} = \langle \rangle$ implies $\alpha\beta^{-1} \in F$ or $F_\alpha = F_\beta$. Therefore, the number of distinct quasigroups in $C(Q, \langle \rangle)$ is precisely the index of F in S_{n+1} , which must be a divisor of $(n+1)!$.

One may also obtain this result from the following considerations. If Q is a finite set, let E be the set of all n -ary quasigroup operations $\langle \rangle$ on Q . Then S_{n+1} may be considered to act on E according to $\pi(\langle \rangle) = \langle \rangle_\pi$. Then $S = \{\pi(\langle \rangle) \mid \pi \in S_{n+1}\}$ for some fixed element $\langle \rangle$ of E , forms a set of transitivity of E ([14], p. 55). Clearly $|S| = |C(Q, \langle \rangle)|$. Now the permutations of S_{n+1} which fix $\langle \rangle$ form a subgroup of S_{n+1} , which is of index $|S|$ in S_{n+1} , by Corollary 5.2.1 of [14].

Theorem 1.2.4. If $n = 3$, the coincidence of the conjugates of (Q, \circ) with (Q, \circ) itself is determined as follows:

- (i) $(Q, \circ(1,3,2)) = (Q, \circ)$ if and only if (Q, \circ) satisfies $x \circ (x \circ y) = y$,
- (ii) $(Q, \circ(2,1,3)) = (Q, \circ)$ if and only if (Q, \circ) satisfies $x \circ y = y \circ x$,
- (iii) $(Q, \circ(2,3,1)) = (Q, \circ)$ if and only if (Q, \circ) satisfies $x \circ (y \circ x) = y$,
- (iv) $(Q, \circ(3,1,2)) = (Q, \circ)$ if and only if (Q, \circ) satisfies $(x \circ y) \circ x = y$,
- (v) $(Q, \circ(3,2,1)) = (Q, \circ)$ if and only if (Q, \circ) satisfies $(y \circ x) \circ x = y$.

Proof: For (i), suppose $(Q, \circ) = (Q, \circ(1,3,2))$. Then, for any $a, b \in Q$, we have $a \circ b = c$ and $a \circ(1,3,2)b = c$. But $a \circ(1,3,2)b = c$ if and only if $a \circ c = b$. Therefore $a \circ b = c$ and $a \circ c = b$, or $a \circ(a \circ b) = b$, and the identity holds. Conversely, if $x \circ(x \circ y) = y$ for all $x, y \in Q$, $a \circ(a \circ b) = b$ for any a, b and if $a \circ b = c$, $a \circ c = b$. But $a \circ c = b$ if and only if $a \circ(1,3,2)b = c$. Therefore $(Q, \circ) = (Q, \circ(1,3,2))$. The proofs for (ii), (iii), (iv) and (v) are similar. (For a proof of (v), see also [33], Theorem 3.)

In [33], Lindner and Steedley have constructed quasi-groups satisfying subsets of these five identity classes and

were thus able to find quasigroups with varying specified conjugacy class numbers. Their results are summarized by the following theorem:

Theorem 1.2.5. For every $m \geq 4$ and every $x \in \{1, 2, 3, 6\}$, there exists a quasigroup (Q, \circ) of order m such that $|C(Q, \circ)| = x$.

One can see that if (Q, \circ) is a Steiner quasigroup, then all of the identities (i) to (v) are satisfied and hence (Q, \circ) has only one conjugacy class. This would not be a complete answer to this case however, as Steiner quasigroups do not exist for all orders. (The requirement of idempotency for Steiner quasigroups is too restrictive.)

From Theorem 1.2.4 and reference [33], it can be seen that the conjugacy class number of a given quasigroup is a direct result of the particular set of algebraic identities satisfied by the quasigroup. This will also be seen to be the case for ternary and n-ary quasigroups in Chapters 2, and 5 respectively.

The identities of Theorem 1.2.4 remain unchanged by an isomorphism of the quasigroup and thus isomorphic quasigroups have the same conjugacy class number. (Clearly this applies to ternary and n-ary quasigroups as well.) Therefore, if one wishes to show that no 3-quasigroup of order 3, for example, exists with conjugacy class number 6, it is only

necessary to investigate the class numbers of all possible non-isomorphic 3-quasigroups of order 3.

§1.3 Block Designs and Steiner Systems.

Definition 1.3.1. A balanced incomplete block design is a pair (S, B) , where S is a v -set and B is a collection of k -subsets of S , called blocks, such that every 2-subset of S occurs in exactly λ blocks.

Such a design is denoted by $BIBD(b, v, r, k, \lambda)$, where each element occurs in exactly r different blocks and B has a total of b different blocks. It is well known that $bk = rv$ and $r(k-1) = \lambda(v-1)$ are necessary conditions for the existence of such a design ([13]). A design (S, B) is therefore completely determined by the parameters v, k, λ .

A triple system is a BIBD with $k = 3$. The conditions for existence then become $3b = rv$, $2r = \lambda(v-1)$, and if one also requires $\lambda = 1$, one obtains $v \equiv 1$ or $3 \pmod{6}$.

In this latter case, a $BIBD(v, b, r, 3, 1)$ is called a Steiner triple system. Again, it is well-known, (see, e.g. [13]) that the necessary conditions for existence are also sufficient. And thus a Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod{6}$.

Although the following theorem is well-known, we include its proof for later convenience.

Theorem 1.3.2. Every Steiner triple system of order v uniquely determines a Steiner quasigroup of order v and conversely.

Proof: If (S, B) denotes a Steiner triple system, then we define an operation \circ on S by $x \circ y = z$ if and only if $\{x, y, z\}$ occur together in a block of B . We also define $x \circ x = x$, for all x .

Suppose $x \circ y = x \circ t = z$, where $y, t \neq x$. Then we must have $\{x, y, z\}$ and $\{x, t, z\}$ as two distinct blocks of B . But then the pair (x, z) occurs in more than one block, a contradiction. If $x \circ x = x \circ y = z$, we have $x = z$ or $\{x, y, x\}$ forms a block of B , which is impossible. Thus (Q, \circ) is a quasigroup.

(Q, \circ) is clearly idempotent and commutative. Consider $x \circ (x \circ y)$, where $x \neq y$. Now $x \circ y = z$, where $\{x, y, z\}$ form a block of B . Therefore $x \circ z = y$. If $x = y$, $x \circ (x \circ x) = x \circ x = x$. Thus (Q, \circ) is a Steiner quasigroup.

Conversely, given a Steiner quasigroup (S, \circ) , if we define $\{x, y, z\}$ to be a block of B , whenever $x \circ y = z$, x, y, z distinct, then we clearly obtain a Steiner triple system (S, B) . For consider any pair of elements (x, y) .

Could, (x,y) belong to more than one block? Suppose $x \circ y = z$ and thus $\{x,y,z\}$ is one block containing the pair. If $\{x,y,t\}$ is also a triple, either $x \circ t = y$ or $y \circ t = x$. But $x \circ (x \circ y) = y$ and so $t = z$ or $y \circ (y \circ x) = x$, where again $z = t$.

We now consider a more general type of design.

Definition 1.3.3. A Steiner system $S(t,k,v)$ is a pair (S,B) , where S is a v -set and B is a collection of k -subsets of S called blocks, such that a t -subset of S occurs in exactly one block of B .

Thus a Steiner triple system of order v is also a Steiner system $S(2,3,v)$. An $S(3,4,v)$ is called a Steiner quadruple system or simply a quadruple system.

One may also speak of isomorphic Steiner systems.

Definition 1.3.3a. Let (S_1, B_1) and (S_2, B_2) be two Steiner systems $S(t,k,v)$. The system (S_1, B_1) is said to be isomorphic to (S_2, B_2) if there is a bijection $\alpha : S_1 \rightarrow S_2$, which maps the blocks of B_1 onto the blocks of B_2 .

Theorem 1.3.4. A quadruple system of order v exists only if $v \equiv 2$ or $4 \pmod{6}$.

Proof: (cf. also [36].) If an $S(3,4,v)$ contains b blocks, each element appears in r blocks and every pair of

elements (unordered) occurs in λ blocks, then the relations for the existence of a balanced incomplete block design imply that $4b = rv$ and $3r = \lambda(v-1)$.

In addition, every unordered pair of elements $\{x, y\}$, form part of $v-2$ triples. That is, there are $v-2$ remaining elements, that joined with $\{x, y\}$, produce a triple. Now every block containing $\{x, y\}$, contains 2 triples made up of $\{x, y\}$ and a third element. Every triple occurs in exactly one block. Therefore, every pair of elements $\{x, y\}$ occurs in $\frac{v-2}{2}$ blocks. From this we obtain:

$$r = \frac{(v-1)(v-2)}{6} \quad \text{and}$$

$$b = \frac{v(v-1)(v-2)}{24} \quad \text{and}$$

$$\lambda = \frac{v-2}{2} .$$

These three equations readily imply $v \equiv 2$ or $4 \pmod{6}$.

Remark 1.3.5. The more general necessary relations for the existence of any Steiner system $S(t, k, v)$ are:

$$(1) \quad \binom{v}{\ell} / \binom{k}{\ell} = b \quad , \quad \text{the number of blocks of } S(t, k, v)$$

$$(2) \quad \binom{v-h}{\ell-h} / \binom{k-h}{\ell-h} = \text{the number of blocks of } S(t, k, v)$$

which contain a fixed subset of size
 $h = 0, 1, \dots, t-1$.

(cf. also [15].) If $k = 4$, $t = 3$, $h = 1$, (2) becomes

equal to r and if $k = 4$, $t = 3$, $h = 2$, (2) becomes λ .
The expressions thus reduce to those given in Theorem 1.3.4.

Theorem 1.3.6. A quadruple system of order v exists if and only if $v \equiv 2$ or $4 \pmod{6}$.

Proof: See Hanani [15].

Theorem 1.3.7. Every quadruple system of order v determines a Steiner ternary quasigroup of order v and conversely.

Proof: Let (S, B) be a quadruple system $S(3,4,v)$ and let $\{x, y, z, t\}$ denote any block of B . On S define an operation \langle, \rangle as follows: $\langle x, y, z \rangle = t$ if and only if x, y, z and t belong to the same block of B . Let \langle, \rangle also satisfy the generalized idempotent law. It is clear that (Q, \langle, \rangle) will be a ternary quasigroup which satisfies the generalized commutative law. Let $\{x, y, z\} = t$, where x, y, z, t are all distinct. Then $\{x, y, z, t\}$ is a block of B and $\langle x, y, \langle x, y, z \rangle \rangle = \langle x, y, t \rangle = z$. If one or more elements are equal, $\langle x, x, y \rangle = y$ and $\langle x, x, \langle x, x, y \rangle \rangle = \langle x, x, y \rangle = y$.

Conversely, if we define a set of quadruples from a Steiner 3-quasigroup (Q, \langle, \rangle) by forming a block by $\{x, y, z, t\}$ if and only if $\langle x, y, z \rangle = t$, we obtain a Steiner quadruple system, in a similar fashion to that of a Steiner triple system.

Remark 1.3.8. We will see in Chapter 2 that the identities given for a Steiner 3-quasigroup imply such a quasigroup has only one conjugacy class. Again, the generalized idempotent law is actually unnecessary. Thus the Steiner 3-quasigroups and ordinary Steiner quasigroups play identical roles concerning conjugacy classes.

Definition 1.3.9. Derived quasigroups from quadruple systems are defined as follows (cf. [31]).

If (S, B) is any $S(3, 4, v)$ and we fix an element $z \in S$, define a quasigroup operation " \circ " on $S \setminus \{z\}$ by $x \circ y = t$ if and only if $\{x, y, t, z\} \in B$. Also define $x \circ x = x$, $\forall x$. Then $(S \setminus \{z\}, \circ)$ will in fact be a Steiner quasigroup.

For consider $x \circ (x \circ y)$, where $x \neq y$. If $x \circ y = t$, then $\{x, y, z, t\} \in B$. Therefore $x \circ t = y$. (S, \circ) is clearly commutative and idempotent.

In a similar fashion, ordinary quasigroups may be derived from ternary quasigroups. If (Q, \langle, \rangle) is a ternary quasigroup and z is any fixed element of Q , define $x \circ y = t$, $x, y, t \in Q$ if $\langle x, y, z \rangle = t$. One may obtain other quasigroups via $\langle z, x, y \rangle = t$, $\langle x, z, y \rangle = t$ and $\langle x, y, t \rangle = z$. We will see further uses of these quasigroups in Chapter 2, 3, and 4. In every case, if (Q, \langle, \rangle) is a Steiner 3-quasigroup, (Q, \circ) will be a Steiner quasigroup. For, if we

consider $x \circ (x \circ y)$, where $x \circ y = t$, we have $\langle x, y, z \rangle = t$, say. Then $x \circ t$ is defined by $\langle x, t, z \rangle = \langle x, \langle x, y, z \rangle, z \rangle = \langle x, z, \langle x, y, z \rangle \rangle = \langle x, z, \langle x, z, y \rangle \rangle = y$. One obtains similar results, if the other definitions are used.

A reverse process is sometimes possible. That is, from a collection of n quasigroups of order $n-1$, one can construct a 3-quasigroup of order n provided certain conditions are met.

Theorem 1.3.10. Suppose a set of idempotent quasigroups $(Q_1, \circ_1) \dots (Q_n, \circ_n)$ are defined on the sets $\{2, \dots, n\}$, $\{3, \dots, n, 1\}$, \dots , $\{1, 2, \dots, n-1\}$ respectively, such that the following condition holds. If for each (Q_i, \circ_i) , we derive a set of ordered triples $\{(x, y, z)_i\}$ where $x \circ_i y = z$, $x, y, z \in Q_i$ are all distinct, then $(x, y, z)_i \neq (\ell, m, n)_j$ for any $i \neq j$, $x, y, z \in Q_i$, $\ell, m, n \in Q_j$. (That is, all the triples of $\{(x, y, z)_i, i = 1, \dots, n\}$ are distinct.) Then there exists a ternary quasigroup (Q, \langle, \rangle) having the (Q_i, \circ_i) as derived quasigroups.

Proof: Define (Q, \langle, \rangle) as follows on the set $\{1, 2, \dots, n\}$. Let $\langle x, y, z \rangle = t$ if and only if $(x, y, z)_t$ is a triple derived from (Q_t, \circ_t) . Further, require (Q, \langle, \rangle) to satisfy the generalized idempotent law.

Now suppose $\langle x, y, z \rangle = \langle x, y, \ell \rangle = t$, where $z \neq \ell$ and (x, y, z) and (x, y, ℓ) are triples having all three

elements different. Then $(x, y, z)_t$ and $(x, y, \ell)_t$ are formed from Q_t , or $x \circ_t y = z$ and $x \circ_t y = \ell$, a contradiction. Suppose $\langle x, z, y \rangle = \langle x, \ell, y \rangle = t$. Then $x \circ_t z = y$ and $x \circ_t \ell = y$ implies $z = \ell$ also.

If $\langle x, y, y \rangle = \langle x, y, \ell \rangle = t$, then $x = t$ or $\langle x, y, \ell \rangle = x$. Then $x \circ_x y = \ell$. But $x \notin Q_x$ and so this is impossible, unless $\ell = y$. If we have $\langle x, y, y \rangle = \langle x, \ell, y \rangle$, again $x = \langle x, \ell, y \rangle$ gives $x \circ_x \ell = y$ and $x \notin Q_x$. If $\langle x, y, x \rangle = \langle x, y, \ell \rangle$, a similar contradiction is obtained. Thus $\langle x, y, \ell \rangle$ will have a unique value in every case and the operation is defined for every possible set of triples. Therefore (Q, \langle, \rangle) is a ternary quasigroup.

It is interesting to note that even if all of the quasigroups (Q_i, \circ_i) are Steiner quasigroups, the ternary quasigroup (Q, \langle, \rangle) constructed from them need not be a Steiner 3-quasigroup. (An example of this will be seen in §2.3.) For consider $\langle x, y, \langle x, y, z \rangle \rangle$. If $\langle x, y, z \rangle = t$, where $x \circ_t y = z$ and $\langle x, y, t \rangle = r$, where $x \circ_r y = t$, there is no guarantee that $r = z$. The operations \circ_r and \circ_t do not have to bear any relation to one another. If the (Q_i, \circ_i) are defined in such a way that these connecting relations are satisfied, then it is possible to make (Q, \langle, \rangle) Steiner.

There remain two theorems about subsystems of quadruple systems, which will be needed later in Chapter 4.

Theorem 1.3.11. A quadruple system of order 8 may be embedded in a quadruple system of order $v \equiv 4$ or $8 \pmod{12}$.

Proof: See Rosa and Lindner in [38].

Theorem 1.3.12. A quadruple system of order v may be embedded in a quadruple system of order $3v-2$.

Proof: See Hanani [15].

CHAPTER 2

The Classification of Identities for Ternary Quasigroups

§2.1 Permutation Classification.

As shown in [33] for ordinary quasigroups, each conjugate quasigroup is identical to the original quasigroup, if and only if a certain identity is satisfied by the original quasigroup. The following list gives, for each $\pi_i \in S_{n+1}$, an identity L_i such that $\langle \rangle = \langle \rangle_{\pi_i}$ if and only if L_i holds in $(Q, \langle \rangle)$. These identities correspond to Theorem 1.2.4 of Chapter 1.

Actually the choice of L_i is not unique. In the case of L_3 , one has $\langle a, b, c \rangle = d$ and $\langle b, a, d \rangle = c$ in Q . These become $\langle b, a, \langle a, b, c \rangle \rangle = c$ or $\langle a, b, \langle b, a, d \rangle \rangle = d$, depending on whether a substitution is made for d or c . These two equalities are clearly identical. However, for L_2 , one has either $\langle \langle b, d, c \rangle, b, c \rangle = d$ or $\langle b, \langle a, b, c \rangle, c \rangle = a$, under similar substitutions. These two seemingly different identities may be transformed from one into the other as follows. Replace b by $\langle b, a, c \rangle$ in $\langle b, \langle a, b, c \rangle, c \rangle$ to obtain $\langle \langle b, a, c \rangle, \langle a, \langle b, a, c \rangle, c \rangle, c \rangle = \langle \langle b, a, c \rangle, b, c \rangle = a$. Similarly replace b by $\langle d, b, c \rangle$ in $\langle \langle b, d, c \rangle, b, c \rangle$ to obtain $\langle b, \langle d, b, c \rangle, c \rangle = d$.

Table 2.1.1

| | <u>Permutation</u> π_i | <u>Type</u> | <u>Corresponding Identity</u> L_i |
|-----|----------------------------|--|---|
| 1. | 1243 | (\cdot) (\cdot) ($\cdot\cdot$) | $\langle a, b, \langle a, b, d \rangle \rangle = d$ |
| 2. | 2134 | ($\cdot\cdot$) (\cdot) (\cdot) | $\langle a, b, c \rangle = \langle b, a, c \rangle$ |
| 3. | 2143 | ($\cdot\cdot$) ($\cdot\cdot$) | $\langle a, b, \langle b, a, d \rangle \rangle = d$ |
| 4. | 1324 | (\cdot) ($\cdot\cdot$) (\cdot) | $\langle a, b, c \rangle = \langle a, c, b \rangle$ |
| 5. | 4231 | (\cdot) (\cdot) ($\cdot\cdot$) | $\langle \langle d, b, c \rangle, b, c \rangle = d$ |
| 6. | 4321 | ($\cdot\cdot$) ($\cdot\cdot$) | $\langle \langle d, c, b \rangle, b, c \rangle = d$ |
| 7. | 3214 | ($\cdot\cdot$) (\cdot) (\cdot) | $\langle c, b, a \rangle = \langle a, b, c \rangle$ |
| 8. | 3412 | ($\cdot\cdot$) ($\cdot\cdot$) | $\langle a, \langle c, d, a \rangle, c \rangle = d$ |
| 9. | 1432 | (\cdot) (\cdot) ($\cdot\cdot$) | $\langle a, \langle a, d, c \rangle, c \rangle = d$ |
| 10. | 2314 | (\cdot) ($\cdot\cdot\cdot$) | $\langle c, a, b \rangle = \langle a, b, c \rangle$ |
| 11. | 3124 | ($\cdot\cdot\cdot$) (\cdot) | $\langle b, c, a \rangle = \langle a, b, c \rangle$ |
| 12. | 2431 | (\cdot) ($\cdot\cdot\cdot$) | $\langle a, \langle d, a, c \rangle, c \rangle = d$ |
| 13. | 4132 | (\cdot) ($\cdot\cdot\cdot$) | $\langle \langle b, d, c \rangle, b, c \rangle = d$ |
| 14. | 3241 | (\cdot) ($\cdot\cdot\cdot$) | $\langle a, b, \langle d, b, a \rangle \rangle = d$ |
| 15. | 4213 | (\cdot) ($\cdot\cdot\cdot$) | $\langle c, b, \langle d, b, c \rangle \rangle = d$ |
| 16. | 1423 | (\cdot) ($\cdot\cdot\cdot$) | $\langle a, \langle a, c, d \rangle, c \rangle = d$ |
| 17. | 1342 | (\cdot) ($\cdot\cdot\cdot$) | $\langle a, b, \langle a, d, b \rangle \rangle = d$ |
| 18. | 4123 | ($\cdot\cdot\cdot\cdot$) | $\langle \langle b, c, d \rangle, b, c \rangle = d$ |
| 19. | 4312 | ($\cdot\cdot\cdot\cdot$) | $\langle \langle c, d, b \rangle, b, c \rangle = d$ |
| 20. | 2341 | ($\cdot\cdot\cdot\cdot$) | $\langle a, b, \langle d, a, b \rangle \rangle = d$ |
| 21. | 2413 | ($\cdot\cdot\cdot\cdot$) | $\langle a, \langle c, a, d \rangle, c \rangle = d$ |
| 22. | 3142 | ($\cdot\cdot\cdot\cdot$) | $\langle a, b, \langle b, d, a \rangle \rangle = d$ |
| 23. | 3421 | ($\cdot\cdot\cdot\cdot$) | $\langle a, \langle d, c, a \rangle, c \rangle = d$ |
| 24. | 1234 | the identity permutation | $\langle a, b, c \rangle = d$ |

Again, as in the case of ordinary quasigroups, it is the subgroups of S_4 which determine the conjugacy class number. However, now the number of subgroups of a given order is larger than in the case of S_3 , and any subgroup of a given order n is sufficient to determine a ternary quasigroup with $\frac{24}{n}$ conjugacy classes. This work is primarily concerned with existence and hence the particular subgroup used is picked for expediency only. However, a broader problem would be to construct quasigroups satisfying the sets of identities corresponding to all the subgroups of S_4 . In some cases, an alternate construction is suggested, depending on a different subgroup choice. But the complete problem has not been considered.

§2.2. A Breakdown of Class Numbers by Subgroups.

(See [24] and [14] for a confirmation of some of these results.)

Case 1. Twenty-Four Classes.

This is the trivial case when no identities are satisfied.

Case 2. Twelve Classes.

A ternary quasigroup $(Q, <, >)$ will have $|C(Q, <, >)| = 12$ if and only if exactly one of the identities L_i with $i = 1, 2, 3, 4, 5, 6, 7, 8$ or 9 are satisfied and no other identities hold (except L_{24} of course).

Case 3. Eight Classes.

One has $|C(Q, <, >)| = 8$ if and only if exactly one of the following sets of identities are satisfied and no other identity is: $\{L_{10}, L_{11}, L_{24}\}$, $\{L_{12}, L_{13}, L_{24}\}$, $\{L_{14}, L_{15}, L_{24}\}$ or $\{L_{16}, L_{17}, L_{24}\}$. These correspond to precisely all the permutations of order three.

Case 4. Six Classes.

One has $|C(Q, <, >)| = 6$ if and only if exactly one of the following sets of identities are satisfied and no other identity is: $\{L_3, L_6, L_8, L_{24}\}$, $\{L_{18}, L_{20}, L_8, L_{24}\}$, $\{L_{19}, L_{23}, L_3, L_{24}\}$, $\{L_{21}, L_{22}, L_6, L_{24}\}$, $\{L_1, L_2, L_3, L_{24}\}$, $\{L_4, L_5, L_6, L_{24}\}$ or $\{L_7, L_8, L_9, L_{24}\}$. These correspond to precisely all the subgroups of order 4.

Case 5. Four Classes.

One has $|C(Q, <, >)| = 4$ if and only if exactly one of the following sets of identities are satisfied and no other identity is: $\{L_2, L_4, L_7, L_{10}, L_{11}, L_{24}\}$, $\{L_2, L_5, L_9, L_{12}, L_{13}, L_{24}\}$, $\{L_1, L_5, L_7, L_{14}, L_{15}, L_{24}\}$, $\{L_1, L_4, L_9, L_{16}, L_{17}, L_{24}\}$.

These correspond to all the subgroups of order 6.

Case 6. Three Classes.

One has $|C(Q, <, >)| = 3$ if and only if exactly one of the following sets of identities are satisfied and no other identity is. These correspond to all the subgroups of order 8, which are in fact all isomorphic to the dihedral group of order $2n = 8$, where $n = 4$: $\{L_1, L_2, L_3, L_6, L_8, L_{19}, L_{23}, L_{24}\}$ corresponds to the dihedral group where $A = \pi_{19}$, $B = \pi_2$, $A^4 = 1$, $B^2 = 1$, and $BA = A^3B$; $\{L_3, L_4, L_5, L_6, L_8, L_{21}, L_{22}, L_{24}\}$ corresponds to $A = \pi_{21}$, $B = \pi_4$; $\{L_3, L_6, L_8, L_9, L_{18}, L_{20}, L_{24}\}$ corresponds to $A = \pi_{18}$, $B = \pi_7$.

Case 7. Two Classes.

Only one set of identities will give $|C(Q, <, >)| = 2$, if they are satisfied and no other identities hold. They come from the alternating subgroup A_4 , whose members are the permutations: $\{\pi_3, \pi_6, \pi_8, \pi_{10}, \pi_{11}, \pi_{12}, \pi_{13}, \pi_{14}, \pi_{15}, \pi_{16}, \pi_{17}, \pi_{24}\}$.

Case 8. One Class.

One has $|C(Q, <, >)| = 1$ if and only if all the identities are satisfied. Actually, identities L_{18} and L_{10} are sufficient to generate all the rest. In fact, one can see that permutation π_{10} is an even permutation of order three and π_{18} is odd of order 4. As the only sub-

group of order 12 is the alternating subgroup, any such pair would generate all of S_4 .

In conclusion, these eight cases give all theoretically possible classes of quasigroup identities and have been obtained by considering all subgroups of S_4 . In Chapter 3 and 4, it is shown, in most cases, that different quasigroups exist, satisfying sufficiently many identities (corresponding to sufficiently many subgroups of S_4) to cover all possible numbers of conjugates.

CHAPTER 3

The Existence of Ternary Quasigroups with 1, 3, 4, 6, 12 or 24 Conjugacy Classes

§3.1 Twenty-Four Classes

Lemma 3.1.1. Let $Q = \{0, 1, 2, \dots, n-1\}$. Suppose $q, r \in Q$, $q \neq r$ and q and r are relatively prime to n . Suppose furthermore that $q+r \not\equiv 0 \pmod{n}$; and $q, r \neq n-1$ or 1 . Define $\langle a, b, c \rangle = a + bq + cr$ for all $a, b, c \in Q$, where addition is modulo n . Then $|C|(Q, \langle \cdot, \cdot, \cdot \rangle) = 24$ for the 3-quasigroup $(Q, \langle \cdot, \cdot, \cdot \rangle)$.

Proof: (1) To check that $(Q, \langle \cdot, \cdot, \cdot \rangle)$ is a quasigroup, consider $\langle a, b, c \rangle = \langle a', b, c \rangle$. Clearly $a = a'$. If $\langle a, b', c \rangle = \langle a, b, c \rangle$, then $b'q \equiv bq \pmod{n}$, which implies $q(b'-b) \equiv 0 \pmod{n}$. Therefore $n/(b'-b)$, as no prime factor of n can divide q . Therefore $b \equiv b' \pmod{n}$ or $b = b'$ as $b, b' \in Q$. Similarly $c = c'$ if $\langle a, b, c' \rangle = \langle a, b, c \rangle$.

(2) Consider any single transposition among the first three positions of $\langle a, b, c \rangle = d$. For example, $\langle a, b, c \rangle = \langle a, c, b \rangle$ implies $cq + br \equiv bq + cr \pmod{n}$. If $c = 0$ and $b = 1$, then $q = r$, which is a contradiction. Similar contradictions are obtained in the other two cases. Hence identities L_2 , L_4 , and L_7 are not satisfied.

(3) A cyclic permutation of a, b and c may be handled as follows. If $\langle a, b, c \rangle = \langle b, c, a \rangle \forall a, b, c$, choose $b = c$. Then $\langle a, b, b \rangle = \langle b, b, a \rangle$, which implies, for $b = 0$, $a = 1$, that $1 = r$. Hence identities L_{10} and L_{11} are not satisfied.

(4) Suppose d is interchanged with either b or c . In particular if $\langle a, b, c \rangle \equiv d$ and $\langle a, b, d \rangle \equiv c$, we have $ap + bq + r(ap + bq + rd) \equiv d$. If $a = b = 0$, $r^2 d \equiv d$. By a suitable choice of c, d can be made $= 1$. Hence $r^2 \equiv 1$. Therefore $a + bq + rap + rbq \equiv 0$, or $(r+1)(ap + bq) \equiv 0$. If $a = 1, b = 0$, we must have $r+1 \equiv 0$, which contradicts $r \neq n-1$. Hence identities L_1 and L_9 are not satisfied.

(5) Suppose d is interchanged with a . Then $(d + bq + cr) + bq + cr \equiv d$. Therefore $2(bq + cr) \equiv 0$. If $c = 1, b = 0$, then $2r \equiv 0$, which contradicts r relatively prime to n . (If $n = 2$, then $r = 1$, which is impossible. If $n = 2m$, any prime factor of m must divide r .) Thus identity L_5 is not satisfied.

(6) Suppose d is interchanged with b or c and the remaining two letters are permuted, as in (2143). Thus $\langle a, b, c \rangle \equiv d$ and $\langle b, a, d \rangle \equiv c$. If we let $a = 0, b = 1$, we obtain $q + r \equiv 0 \pmod{n}$, a contradiction. Hence identities L_3 and L_8 do not hold.

(7) If d is interchanged with a , and b and c are permuted (4321) , we obtain $d + cq + br + bq + cr \equiv d$. Therefore $cq + br + bq + cr \equiv 0 \pmod{n}$ and $(q+r)(b+c) \equiv 0 \pmod{n}$, from which $q+r \equiv 0 \pmod{n}$, by a suitable choice of b and c . Identity L_6 is therefore not satisfied.

(8) Now one may show by a consideration of subgroups that identities 18-23 do not hold. If L_{18} holds, π_{18} will generate a subgroup of order 4 containing π_8 , but L_8 does not hold. Similarly π_3 is in the subgroup $\{\pi_3, \pi_{19}, \pi_{23}, \pi_{24}\}$ and π_6 belongs to $\{\pi_6, \pi_{21}, \pi_{22}, \pi_{24}\}$.

(9) The only remaining identities are $L_{12}-L_{17}$, which correspond to permutations with a fixed point and a cyclic permutation of the remaining letters, with d never fixed. Each of these cases may be reduced to case (4) as follows: Identity L_{12} comes from $\pi_{12} = (2431)$. Let $a = b$ and we have $\langle a, a, c \rangle \equiv d$ and $\langle a, d, c \rangle \equiv d$. Thus $a + (a + dq + cr)q + cr \equiv d$. As before $q^2 d \equiv d$ ($a=0$) gives $q^2 \equiv 1 \pmod{n}$, if c is chosen to make $d = 1$. As in (4), $(a + cr)(q + 1) \equiv 0 \pmod{n}$ means $q + 1 \equiv 0 \pmod{n}$, contradicting the assumptions. Hence L_{12} and L_{13} do not hold. ($\{\pi_{12}, \pi_{13}, \pi_{24}\}$ is a subgroup). For (3241) , let $a = c$, and for (1423) , let $b = c$. Contradictions are obtained identical to case (4). Therefore $L_{12}-L_{17}$ do not hold.

The proof is now complete.

Lemma 3.1.2. If

(i) $n \geq 7$, n odd, or if

(ii) $n \geq 14$, n even,

then there exist integers $q, r \in \{0, 1, 2, \dots, n-1\}$ such that $q \neq r$, q, r are relatively prime to n , $q+r \not\equiv 0 \pmod{n}$, and $q, r \neq n-1$ or 1 . Moreover, q, r may be given explicitly.

Proof: Case (1). Suppose n is odd, $n \geq 7$. Then $q = 2$, $r = \lfloor \frac{n}{2} \rfloor$ may be chosen.

Case (2). Let $n = 2^s m \geq 14$ where $s \geq 1$ and m is odd. Then we may take $q = m+2$ and $r = m+4$. Now any prime different from 2 which divides $2^s m$, must divide m and thus will not divide r . If the prime is 2 and it divides $(2+m)$ or $(4+m)$, then it divides m , which contradicts m odd.

If $m+2 = n-1 = 2^s m-1$, then $m(2^s-1) = 3$. The only possibilities are $s = 1$, $m = 3$, $n = 6$, or $s = 2$, $m = 1$, $n = 4$.

If $m+4 = n-1$, then $5 = m(2^s-1)$, whose only solution is $m = 5$, $s = 1$, $n = 10$.

Could we have $(m+4) + (m+2) = 2^s m$? Then $(2^{s-1}-1)m =$

3, with solutions $s = 2$, $m = 3$, $n = 12$ and $s = 3$, $m = 1$, $n = 8$. In all other cases, $(m+4) + (m+2)$ are relatively prime to n , do not sum to n , and are different from $n-1$.

Lemma 3.1.3. There do not exist any 3-quasigroups with 24 conjugacy classes of order 1, 2 or 3.

Proof: Recall the discussion following Definition 1.3.9.

In the case $n = 3$, the only possible candidates for 24 conjugacy classes would arise from a permutation of the following three faces:

| | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 1 | 2 | 3 |
| 2 | 3 | 1 | 2 |
| 3 | 2 | 3 | 1 |

FACE 1

| | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 2 | 3 | 1 |
| 2 | 1 | 2 | 3 |
| 3 | 3 | 1 | 2 |

FACE 2

| | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 3 | 1 | 2 |
| 2 | 2 | 3 | 1 |
| 3 | 1 | 2 | 3 |

FACE 3

However, no matter how they are permuted, one complete set of derived quasigroups will be commutative. For example, if (Q_i, \circ) is defined by $b \circ c = d$ if and only if $\langle i, b, c \rangle = d$ for $i = 1, 2, 3$, then all the (Q_i, \circ) are commutative. Therefore the ternary quasigroup, whose faces are shown above, satisfies L_4 .

Lemma 3.1.4. There exists a 3-quasigroup of order 4 with 24 conjugacy classes.

Proof: Consider the 3-quasigroup defined by the following faces:

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 3 | 4 | 1 | 2 |
| 3 | 4 | 3 | 2 | 1 |
| 4 | 2 | 1 | 4 | 3 |

FACE 1

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 4 | 3 | 1 | 2 |
| 2 | 1 | 2 | 4 | 3 |
| 3 | 2 | 1 | 3 | 4 |
| 4 | 3 | 4 | 2 | 1 |

FACE 2

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 3 | 4 | 2 | 1 |
| 2 | 2 | 1 | 3 | 4 |
| 3 | 1 | 2 | 4 | 3 |
| 4 | 4 | 3 | 1 | 2 |

FACE 3

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 1 | 4 | 3 |
| 2 | 4 | 3 | 2 | 1 |
| 3 | 3 | 4 | 1 | 2 |
| 4 | 1 | 2 | 3 | 4 |

FACE 4

Law 2 is clearly not satisfied. L_1 is contradicted by $\langle 2, 2, 3 \rangle = 1$, and $\langle 2, 2, 1 \rangle = 4$. If L_1 is not satisfied with the first two positions equal (2), then L_3 is not satisfied. L_6 is contradicted by $\langle 3, 2, 1 \rangle = 3$, $\langle 1, 2, 3 \rangle = 4$. This also means L_4 does not hold. L_9 is contradicted by $\langle 1, 3, 2 \rangle = 1$, $\langle 1, 1, 2 \rangle = 4$. L_8 is contradicted by $\langle 2, 3, 1 \rangle = 1$, $\langle 1, 1, 2 \rangle = 4$, while for L_7 ,

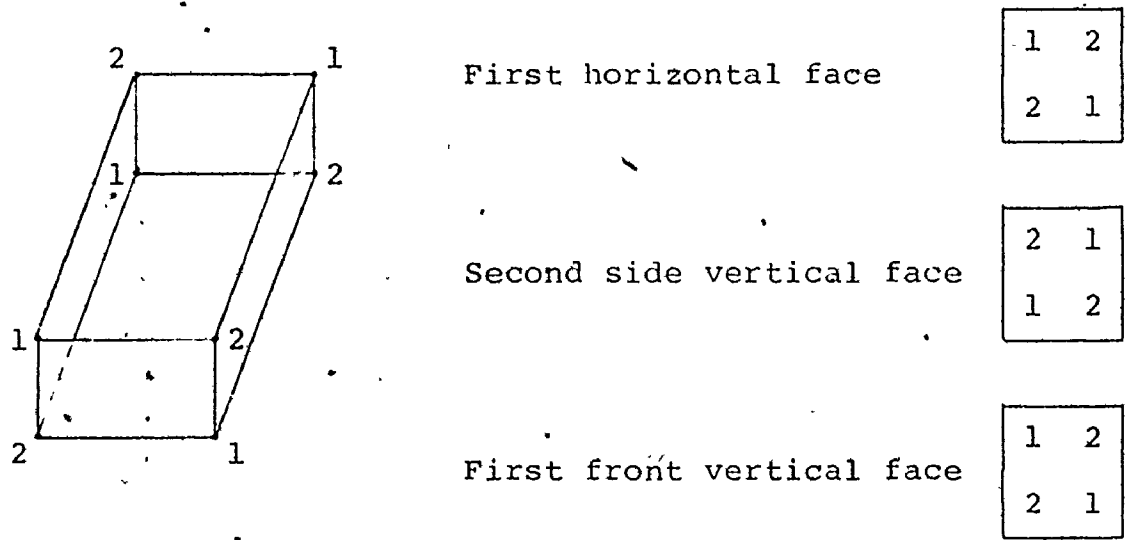
consider. $\langle 3,2,1 \rangle = 3$, $\langle 1,2,3 \rangle = 4$. Now L_{10} does not hold because $\langle 1,2,3 \rangle = 4$, $\langle 2,3,1 \rangle = 1$ and therefore L_{11} does not hold either. For L_{12} - L_{17} , we need only consider L_{12} , L_{14} and L_{16} . L_{12} is violated by $\langle 2,1,3 \rangle = 2$, $\langle 1,2,3 \rangle = 4$; L_{14} by $\langle 3,2,1 \rangle = 3$, $\langle 1,2,3 \rangle = 4$; and L_{16} by $\langle 2,1,3 \rangle = 2$, $\langle 2,2,1 \rangle = 4$. As in Lemma 3.1.1, L_{18} - L_{23} cannot hold. Therefore the faces represent a 3-quasigroup with 24 conjugacy classes.

Remark 3.1.5. At this point, one would normally try to give examples for the remaining missing orders. However, the example for $n = 5$ was found to generalize to produce an alternate method for constructing quasigroups of higher orders with 24 conjugacy classes. As this method arises from studying the three dimensional cube, rather than from algebraic considerations, it is included here to indicate the range of possibilities in solving the general problem.

Definition 3.1.6. Define the front vertical faces of a ternary quasigroup (Q, \langle, \rangle) to be the faces of the cubic representation obtained by fixing the third coordinate in the operation \langle, \rangle . That is, the faces are the Cayley tables of the quasigroups (Q_{F_i}, \circ) derived from (Q, \langle, \rangle) by setting $a \circ b = c$ if and only if $\langle a, b, i \rangle = c$, $\forall a, b, c \in Q$, $\forall i = 1, \dots, n$ where n is the order of (Q, \langle, \rangle) .

The side vertical faces are obtained by fixing the second coordinate in $\langle , , \rangle$. The faces are the Cayley tables of the quasigroups (Q_{S_i}, \circ) derived from $(Q, \langle , , \rangle)$ by setting $a \circ b = c$ if and only if $\langle a, i, b \rangle = c$.

Finally, the horizontal faces are obtained by fixing the first coordinate in $\langle , , \rangle$. The faces are the Cayley tables of the quasigroups (Q_{H_i}, \circ) derived from $(Q, \langle , , \rangle)$ by setting $a \circ b = c$ if and only if $\langle i, a, b \rangle = c$. The illustration below shows the faces on a cube of order 2.



Lemma 3.1.7. There exists a ternary quasigroup of order n with 24 conjugacy classes for all $n \geq 5$.

Proof: Consider the following construction of a 3-quasigroup. Let the first front vertical face (or (Q_{F_1}, \circ)) be defined

by $a \circ b \equiv (a+b-1) \pmod n \forall a, b \in Q$. Here $Q = \{1, 2, \dots, n\}$, $n \geq 5$. Interchange the first two rows of (Q_{F_1}, \circ) . Construct the remaining front vertical faces $2, \dots, n$ by adding 1 (mod n) successively to each of the corresponding elements of face 1. Clearly the resulting cube will be latin. Call the corresponding 3-quasigroup $(Q, <, , >)$.

Perform the following operations, which will not destroy the quasigroup nature of $(Q, <, , >)$. Interchange the first and second front vertical faces. Interchange the second and third side vertical faces (the first and second cannot be chosen as commutativity is then restored to the original faces).

These manipulations result in the following entries in the first, second and third front vertical faces:

| | | | | | | | | | | | |
|--------|---|---|-----|--------|---|---|-----|--------|---|---|-----|
| 2 | 4 | 3 | ... | 3 | 5 | 4 | ... | 4 | 0 | 5 | ... |
| 1 | 3 | 2 | ... | 2 | 4 | 3 | ... | 3 | 5 | 4 | ... |
| 3 | 5 | 4 | ... | 4 | 0 | 5 | ... | 5 | 0 | 0 | ... |
| 4 | . | . | . | . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . | . | . | . | . |
| FACE 1 | | | | FACE 2 | | | | FACE 3 | | | |

The zeroed entries have values greater than 5 if $n > 6$, 1 or 2 if $n = 5$, and 1 and 6 if $n = 5$.

Now face 1 is non-commutative, so $(Q, <, , >)$ does not satisfy L_2 . Further, L_1 is violated by $\langle 2, 2, 1 \rangle = 3$,

and $\langle 2,2,3 \rangle = 5$. This also violates L_3 . L_4 is violated by $\langle 2,3,1 \rangle = 2$, $\langle 2,1,3 \rangle = 3$. L_5 doesn't hold because $\langle 2,1,3 \rangle = 3$, while $\langle 3,1,3 \rangle = 5$. L_6 is contradicted by the example for L_4 . L_7 does not hold because $\langle 2,1,3 \rangle = 3$, but $\langle 3,1,2 \rangle = 4$. L_8 is contradicted by $\langle 1,1,1 \rangle = 2$ and $\langle 1,2,1 \rangle = 4$, which also contradicts L_9 . It remains only to discuss L_{10} , L_{12} , L_{14} and L_{16} . The fact that $\langle 1,2,1 \rangle = 4$, $\langle 2,1,1 \rangle = 1$ contradicts L_{10} . For L_{12} , $\langle 1,1,1 \rangle = 2$ should imply $\langle 1,2,1 \rangle = 1$, but $\langle 1,2,1 \rangle = 4$. For L_{14} , $\langle 1,1,1 \rangle = 2$ implies $\langle 1,1,2 \rangle = 1$, while we have $\langle 1,1,2 \rangle = 3$.

For L_{16} , $\langle 1,1,1 \rangle = 2$ implies $\langle 1,2,1 \rangle = 1$, whereas here $\langle 1,2,1 \rangle = 4$.

The lemmas of §3.1 prove the following theorem.

Theorem 3.1.8. Ternary quasigroups with 24 conjugacy classes exist for all orders $n \geq 4$ and do not exist for any $n < 4$.

Remark 3.1.9. One may prove a similar theorem to Lemma 3.1.1 in the case of ordinary quasigroups; namely, if $x \circ y$ on $Q = \{1, \dots, n-1\}$ is defined to be $x + py \pmod{n}$, where $p \neq 1$ or $n-1$ and p is relatively prime to n , then the multiplication defines a quasigroup with exactly 6 conjugacy classes. If $n \geq 5$ and odd, one may choose $p = \frac{n+1}{2}$. If $n \geq 8$ and even, $n = 2^s m$ (m odd) , then one may choose $p = m+2$. This then

provides a simple alternate construction to that given in [33], where embedding theorems are needed.

§3.2 Twelve Classes.

Lemma 3.2.1. There exists a ternary quasigroup of order n with 12 conjugacy classes if

- (i) $n \geq 5$, if n odd, or
- (ii) $n \geq 8$, if n even.

Proof: (1) Let $Q = \{0, 1, 2, \dots, n-1\}$. Define a ternary operation $\langle \cdot, \cdot, \cdot \rangle$ on Q by $\langle a, b, c \rangle = d \equiv (a+b+pc) \pmod{n}$ where $p \neq n-1$ or 1 , $p \in Q$, and p is relatively prime to n . Then $(Q, \langle \cdot, \cdot, \cdot \rangle)$ is a 3-quasigroup as in Lemma 3.1.1. Clearly L_2 holds and if we can show no other identities hold, $|C(Q, \langle \cdot, \cdot, \cdot \rangle)|$ will be equal to 12.

(2) One sees that L_4 and L_7 do not hold, as in Lemma 3.1.1. If d and c are interchanged, whether or not a and b are also interchanged, one obtains $a+b+p(a+b+pc) \equiv c \pmod{n}$. If $a = b = 0$, $p^2c \equiv c \pmod{n}$. If $d = 1$, $\langle 0, 0, d \rangle \equiv pd \equiv c$ or $c = p$ gives $p^3 \equiv p \pmod{n}$. Thus $p(p^2-1) \equiv 0 \pmod{n}$. This leads to $p^2 \equiv 1 \pmod{n}$ and $(p+1)(a+b) \equiv 0 \pmod{n} \forall a, b \in Q$. This contradicts $p \neq n-1$. Thus L_1 and L_3 are not satisfied.

(3) If d is interchanged with a or b , one obtains $\langle a, b, c \rangle = d$ or $\langle d, b, c \rangle = a$, say. Therefore $(a+b+c) + b + pc \equiv a \pmod{n}$. Then $2b + c(p+1) \equiv 0 \pmod{n}$. If $b = 0$, $c = 1$, we obtain $p \equiv n-1$, a contradiction. If $b = c$ a similar contradiction can be found. Therefore L_5 , L_6 , L_8 and L_9 are violated.

(4) If identity L_{10} holds, $a + b + pc \equiv b + c + pa$, implying $a + pc \equiv c + pa$, or $p \equiv 1$ if $a = 0$, $c = 1$. Identity L_{12} implies $b+(a+b+pc) + pc \equiv a$, or $2 \equiv 0$ if $b = 1$, $c = 0$. Identity L_{14} implies $c + b + p(a+b+cp) \equiv a$. If $b = c = 0$, $a = d$ and $pa \equiv a$. If $a = d = 1$, this gives $p \equiv 1$. Identity L_{16} implies $a+(a+b+pc) + pb \equiv c$. If $a = b = 0$, again we obtain $c = d$ and $pc \equiv c$, which means $p \equiv 1$, if $d = 1$.

(5) As in the earlier proofs, this is all that needs to be shown. (Note that π_2 does not belong to any of the subgroups of order 4 containing π_{18} to π_{23} .)

(6) Now if $n \geq 5$, n odd, let $p = 2$. If $n \geq 18$, n even, let $p = m+2$, where $n = 2^s m$ (m odd). As before, $m+2$ is relatively prime to n and if $m+2 = 2^{s-1}$, or $3 = m(2^s - 1)$, this has a solution only for $n = 4$ or 6 .

Lemma 3.2.2. There exists a 3-quasigroup of order 6 with 12 conjugacy classes, and with the further property that it satisfies the generalized idempotent law.

Proof: Let $Q = \{1,2,3,4,5,6\}$. Define $\langle a,b,c \rangle$ so that $\langle a,b,c \rangle \neq a, b$ or c , where a, b, c are distinct, by the table below. Then the remaining products may be defined by the generalized idempotent law. One may check that these products do indeed define a 3-quasigroup.

Definition of triples with 3 distinct elements

| | | |
|-----------------------------|-----------------------------|-----------------------------|
| $\langle 1,2,3 \rangle = 4$ | $\langle 1,3,4 \rangle = 6$ | $\langle 1,4,6 \rangle = 2$ |
| $\langle 2,3,1 \rangle = 5$ | $\langle 3,4,1 \rangle = 5$ | $\langle 4,6,1 \rangle = 5$ |
| $\langle 3,1,2 \rangle = 6$ | $\langle 4,1,3 \rangle = 2$ | $\langle 6,1,4 \rangle = 3$ |
| $\langle 2,1,3 \rangle = 6$ | $\langle 3,1,4 \rangle = 2$ | $\langle 4,1,6 \rangle = 3$ |
| $\langle 1,3,2 \rangle = 5$ | $\langle 1,4,3 \rangle = 5$ | $\langle 1,6,4 \rangle = 5$ |
| $\langle 3,2,1 \rangle = 4$ | $\langle 4,3,1 \rangle = 6$ | $\langle 6,4,1 \rangle = 2$ |
| $\langle 1,2,4 \rangle = 3$ | $\langle 1,3,5 \rangle = 2$ | $\langle 1,5,6 \rangle = 3$ |
| $\langle 2,4,1 \rangle = 6$ | $\langle 3,5,1 \rangle = 6$ | $\langle 5,6,1 \rangle = 4$ |
| $\langle 4,1,2 \rangle = 5$ | $\langle 5,1,3 \rangle = 4$ | $\langle 6,1,5 \rangle = 2$ |
| $\langle 2,1,4 \rangle = 5$ | $\langle 3,1,5 \rangle = 4$ | $\langle 5,1,6 \rangle = 2$ |
| $\langle 1,4,2 \rangle = 6$ | $\langle 1,5,3 \rangle = 6$ | $\langle 1,6,5 \rangle = 4$ |
| $\langle 4,2,1 \rangle = 3$ | $\langle 5,3,1 \rangle = 2$ | $\langle 6,5,1 \rangle = 3$ |
| $\langle 1,2,5 \rangle = 6$ | $\langle 1,3,6 \rangle = 4$ | $\langle 2,3,4 \rangle = 1$ |
| $\langle 2,5,1 \rangle = 4$ | $\langle 3,6,1 \rangle = 2$ | $\langle 3,4,2 \rangle = 6$ |
| $\langle 5,1,2 \rangle = 3$ | $\langle 6,1,3 \rangle = 5$ | $\langle 4,2,3 \rangle = 5$ |
| $\langle 2,1,5 \rangle = 3$ | $\langle 3,1,6 \rangle = 5$ | $\langle 3,2,4 \rangle = 5$ |
| $\langle 1,5,2 \rangle = 4$ | $\langle 1,6,3 \rangle = 2$ | $\langle 2,4,3 \rangle = 6$ |
| $\langle 5,2,1 \rangle = 6$ | $\langle 6,3,1 \rangle = 4$ | $\langle 4,3,2 \rangle = 1$ |

$$\langle 1, 2, 6 \rangle = 5 \quad \langle 1, 4, 5 \rangle = 3 \quad \langle 2, 3, 5 \rangle = 6$$

$$\langle 2, 6, 1 \rangle = 3 \quad \langle 4, 5, 1 \rangle = 2 \quad \langle 3, 5, 2 \rangle = 4$$

$$\langle 6, 1, 2 \rangle = 4 \quad \langle 5, 1, 4 \rangle = 6 \quad \langle 5, 2, 3 \rangle = 1$$

$$\langle 2, 1, 6 \rangle = 4 \quad \langle 4, 1, 5 \rangle = 6 \quad \langle 3, 2, 5 \rangle = 1$$

$$\langle 1, 6, 2 \rangle = 3 \quad \langle 1, 5, 4 \rangle = 2 \quad \langle 2, 5, 3 \rangle = 4$$

$$\langle 6, 2, 1 \rangle = 5 \quad \langle 5, 4, 1 \rangle = 3 \quad \langle 5, 3, 2 \rangle = 6$$

$$\langle 2, 3, 6 \rangle = 5 \quad \langle 2, 4, 5 \rangle = 1 \quad \langle 2, 4, 6 \rangle = 3$$

$$\langle 3, 6, 2 \rangle = 1 \quad \langle 4, 5, 2 \rangle = 6 \quad \langle 4, 6, 2 \rangle = 5$$

$$\langle 6, 2, 3 \rangle = 4 \quad \langle 5, 2, 4 \rangle = 3 \quad \langle 6, 2, 4 \rangle = 1$$

$$\langle 3, 2, 6 \rangle = 4 \quad \langle 4, 2, 5 \rangle = 3 \quad \langle 4, 2, 6 \rangle = 1$$

$$\langle 2, 6, 3 \rangle = 1 \quad \langle 2, 5, 4 \rangle = 6 \quad \langle 2, 6, 4 \rangle = 5$$

$$\langle 6, 3, 2 \rangle = 5 \quad \langle 5, 4, 2 \rangle = 1 \quad \langle 6, 4, 2 \rangle = 3$$

$$\langle 2, 5, 6 \rangle = 1 \quad \langle 3, 4, 5 \rangle = 2 \quad \langle 3, 4, 6 \rangle = 1$$

$$\langle 5, 6, 2 \rangle = 3 \quad \langle 4, 5, 3 \rangle = 1 \quad \langle 4, 6, 3 \rangle = 2$$

$$\langle 6, 2, 5 \rangle = 4 \quad \langle 5, 3, 4 \rangle = 6 \quad \langle 6, 3, 4 \rangle = 5$$

$$\langle 5, 2, 6 \rangle = 4 \quad \langle 4, 3, 5 \rangle = 6 \quad \langle 4, 3, 6 \rangle = 5$$

$$\langle 2, 6, 5 \rangle = 3 \quad \langle 3, 5, 4 \rangle = 1 \quad \langle 3, 6, 4 \rangle = 2$$

$$\langle 6, 5, 2 \rangle = 1 \quad \langle 5, 4, 3 \rangle = 2 \quad \langle 6, 4, 3 \rangle = 1$$

$$\langle 3, 5, 6 \rangle = 2 \quad \langle 5, 3, 6 \rangle = 4 \quad \langle 4, 5, 6 \rangle = 3 \quad \langle 5, 4, 6 \rangle = 2$$

$$\langle 5, 6, 3 \rangle = 1 \quad \langle 3, 6, 5 \rangle = 1 \quad \langle 5, 6, 4 \rangle = 1 \quad \langle 4, 6, 5 \rangle = 1$$

$$\langle 6, 3, 5 \rangle = 4 \quad \langle 6, 5, 3 \rangle = 2 \quad \langle 6, 4, 5 \rangle = 2 \quad \langle 6, 5, 4 \rangle = 3$$

From the definition of (Q, \langle, \rangle) , one sees that L_7 is satisfied. Suppose (Q, \langle, \rangle) had only 3 conjugacy classes. Then there would be a subgroup of order 8 of S_4 such that all the corresponding identities were satisfied. However, π_7 is in the subgroup $\{\pi_{18}, \pi_{20}, \pi_8, \pi_7, \pi_6, \pi_3, \pi_9, \pi_{24}\}$ and no other subgroup of order 8. We have $\langle 1, \langle 3, 6, 1 \rangle, 3 \rangle = \langle 1, 2, 3 \rangle = 4 \neq 6$, contradicting L_8 . Therefore (Q, \langle, \rangle) cannot have only 3 conjugacy classes. π_7 is an odd permutation and thus cannot belong to the alternating subgroup A_4 . But then (Q, \langle, \rangle) cannot have 2 conjugacy classes.

The only subgroups of order 6 containing π_7 are $\{\pi_1, \pi_2, \pi_4, \pi_7, \pi_{10}, \pi_{11}, \pi_{24}\}$ and $\{\pi_5, \pi_1, \pi_7, \pi_{14}, \pi_{15}, \pi_{24}\}$. As (Q, \langle, \rangle) is clearly not commutative in the first 2 positions, L_2 is not satisfied. Also $\langle 2, 1, 3 \rangle = 6$, but $\langle 2, 1, 6 \rangle = 4 \neq 3$, contradicting L_1 . Therefore we do not have a subgroup of order 6 of S_4 with all the corresponding identities satisfied.

Finally, the only subgroup of order 4 containing π_7 is $\{\pi_{24}, \pi_7, \pi_8, \pi_9\}$. But this is itself a subgroup of the subgroup of order 8 above. Therefore $|C(Q, \langle, \rangle)| = 12$.

Remark 3.2.3. L. Humbolt in [22] constructs idempotent 3-quasigroups. In his paper, however, idempotent means only $\langle x, x, x \rangle = x$. The existence of 3-quasigroups satisfying the generalized idempotent law has not been settled. It is known

from Chapter 1, that the 3-quasigroup derived from any quadruple system will satisfy this law. Therefore there exist generalized idempotent 3-quasigroups of every order congruent to 2 or 4 mod 6. If one uses the ordinary direct product of 3-quasigroups, then one may construct other generalized idempotent 3-quasigroups from the example of order 6 given here and the ternary quasigroups derived from quadruple systems. (Clearly the ordinary direct product preserves this law. If $(Q_1, \langle, \rangle_1)$ and $(Q_2, \langle, \rangle_2)$ are generalized idempotent quasigroups, then $\langle (a_1, a_2), (a_1, a_2), (b_1, b_2) \rangle = (\langle a_1, a_1, b_1 \rangle_1, \langle a_2, a_2, b_2 \rangle_2) = (b_1, b_2)$.) Therefore, there exist generalized idempotent quasigroups having orders of the form 6^n , $6(2+6n)$ or $6(4+6n)$, $n \in \mathbb{N}$.

Further results concerning the generalized idempotent law may be found in [30].

Theorem 3.2.4. There exists a ternary quasigroup of order n with exactly 12 conjugacy classes if and only if $n \geq 4$.

Proof: In view of Lemmas 3.2.1 and 3.2.2, it remains only to consider the cases $n = 2, 3$ and 4 .

If $n = 2$, any ternary quasigroup of order 2 may be seen to have fewer than 12 conjugacy classes.

If $n = 3$, without loss of generality (i.e. up to isomorphism), the front vertical faces of a ternary quasigroup are either:

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |
| 3 | 1 | 2 |


| | | |
|---|---|---|
| 2 | 3 | 1 |
| 3 | 1 | 2 |
| 1 | 2 | 3 |

| | | |
|---|---|---|
| 3 | 1 | 2 |
| 1 | 2 | 3 |
| 2 | 3 | 1 |

1A

2A

3A


 order possibly reversed

or:

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 3 | 1 | 2 |
| 2 | 3 | 1 |


| | | |
|---|---|---|
| 2 | 3 | 1 |
| 1 | 2 | 3 |
| 3 | 1 | 2 |

| | | |
|---|---|---|
| 3 | 1 | 2 |
| 2 | 3 | 1 |
| 1 | 2 | 3 |

1B

2B

3B


 order possibly reversed

In the case we take 1A , 2A , 3A , the front vertical faces and the horizontal faces are all commutative as quasigroups, implying that at least 2 identities are satisfied. (The first horizontal face is

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |
| 3 | 1 | 2 |

.)

In the case 1A , 3A and 2A , the front vertical faces are commutative as quasigroups and L_3 can be seen to hold. In the case 1B , 2B , 3B , the horizontal faces are commutative as quasigroups, and again L_3 is satisfied. In the case 1B , 3B , 2B , the side vertical faces are commutative as quasigroups and L_1 is satisfied. Therefore, no ternary quasigroup of order 3 with 12 conjugacy classes exists.

If $n = 4$, consider the following example:

| | | | |
|------------------|------------------|------------------|------------------|
| 4 3 2 ① | 1 4 3 ② | 2 1 4 ③ | 3 2 1 ④ |
| 1 4 3 ② | 3 2 1 ④ | 4 3 2 ① | 2 1 4 ③ |
| 2 1 4 ③ | 4 3 2 ① | 3 2 1 ④ | 1 4 3 ② |
| 3 2 1 ④ | 2 1 4 ③ | 1 4 3 ② | 4 3 2 ① |

The elements of Face 1 of the front vertical faces are circled and those of Face 3 are squared to be seen more easily. Now the front vertical faces are all commutative as quasigroups, implying L_2 holds. L_1 does not hold because $\langle 1, 2, \langle 1, 2, 3 \rangle \rangle = 1 \neq 3$. L_3 does not hold because $\langle 1, 2, \langle 2, 1, 3 \rangle \rangle = 1 \neq 3$. For L_4 and L_7 , one notes that the second horizontal face:

| | | | |
|---|---|---|---|
| 2 | 4 | 1 | 3 |
| 3 | 1 | 2 | 4 |
| 4 | 2 | 3 | 1 |
| 1 | 3 | 4 | 2 |

is not commutative as a quasigroup, nor is the second side vertical face:

| | | | |
|---|---|---|---|
| 2 | 3 | 4 | 1 |
| 4 | 1 | 2 | 3 |
| 1 | 2 | 3 | 4 |
| 3 | 4 | 1 | 2 |

L_5 is violated by $\langle\langle 3,1,2\rangle,1,2\rangle = \langle 4,1,2\rangle = 1 \neq 3$; L_6 is violated by $\langle\langle 3,1,2\rangle,1,2\rangle = 1 \neq 3$; L_8 by $\langle 1,\langle 3,2,1\rangle,3\rangle = \langle 1,1,3\rangle = 3 \neq 2$ and, finally, L_9 by $\langle 2,\langle 2,4,1\rangle,1\rangle = \langle 2,3,1\rangle = 1 \neq 4$. Now π_2 cannot belong to a subgroup of S_4 of order 12 (A_4) as it is an odd permutation. It cannot be part of a subgroup of order 8, as the only one containing π_2 also contains π_1, π_3, π_6 and π_8 , whose corresponding identities do not hold. The two subgroups of order 6 containing π_2 are $\{\pi_2, \pi_4, \pi_7, \pi_{10}, \pi_{11}, \pi_{24}\}$ and $\{\pi_2, \pi_9, \pi_5, \pi_{12}, \pi_{13}, \pi_{24}\}$, each of which contains at least one subscript corresponding to an identity which does not hold. Finally, the only subgroup of order 4 containing π_2 is $\{\pi_1, \pi_2, \pi_3, \pi_{24}\}$. Therefore, L_2 must hold alone and the ternary quasigroup represented by the tables here has 12 conjugacy classes.

§3.3 Six Classes.

Lemma 3.3.1. If $n > 3$ and odd, there exists a ternary quasigroup of order n with 6 conjugacy classes.

Proof: Let $Q = \{0, 1, \dots, n-1\}$. Define \langle, \rangle on Q by $\langle a, b, c \rangle \equiv (2a+2b-c) \pmod{n} \quad \forall a, b, c \in Q$. It can be easily shown that L_1, L_2 and L_3 are satisfied.

Now the only subgroup larger than $\{\pi_1, \pi_2, \pi_3, \pi_{24}\}$ and containing it is the subgroup of order 8 = $\{\pi_1, \pi_2, \pi_3, \pi_6, \pi_8, \pi_9, \pi_{23}, \pi_{24}\}$. However, consider $L_6 : \langle \langle d, c, b \rangle, b, c \rangle \equiv (2d+2c-b)^2 + 2b - c \equiv d$. If $b = 0, c = 1, d = 1, 4 \equiv 1 \pmod{n}$, which is false.

Lemma 3.3.2. If $n > 6$, n is even and $n \neq 8, 12, \text{ or } 24$, there exists a ternary quasigroup of order n .

Proof: Let $Q = \{0, 1, \dots, n-1\}$. Define \langle, \rangle on Q by $\langle a, b, c \rangle \equiv (a(m+2) + b(m+2) - c) \pmod{n}$ where $n = 2^s m$, m odd. We need only show that L_6 does not hold. Now $\langle \langle d, c, b \rangle, b, c \rangle \equiv (d(m+2) + c(m+2) - b)(m+2) + b(m+2) - c \equiv c((m+2)^2 - 1) + d(m+2)^2 \equiv d \pmod{n}$. This implies $(m+2)^2 \equiv 1 \pmod{n}$, or $m^2 + 4m + 4 \equiv 1 \pmod{n}$, which gives $m^2 + 4m + 3 \equiv 0 \pmod{n}$. As $m/n, m/3$. Therefore $m = 1$ or 3 . If $m = 1, 9 \equiv 1 \pmod{n}$ or $n = 4$ or 8 . If $m = 3, 25 \equiv 1 \pmod{n}$ and $n = 6, 12$ or 24 . In every other case $(m+2)^2 \not\equiv 1 \pmod{n}$.

Lemma 3.3.3. There exists a ternary quasigroup of order 4 and of order 6 with 6 conjugacy classes.

There does not exist any 3-quasigroup of order n with 6 conjugacy classes for $n \leq 3$.

Proof: (1) For $n = 3$, consider the quasigroups given in Theorem 3.2.4. In the case of choosing $1A, 2A, 3A, L_2$ and L_4 are satisfied. These identities have corresponding permutations which do not belong together to any subgroup of order 4. In the case $1A, 3A, 2A, L_1$ and L_2 and L_3 are satisfied. However, so is L_6 . In the case $1B, 2B, 3B, L_3$ and L_4 hold, but π_3 and π_4 do not appear together in any subgroup of order 4. Finally, in the case $1B, 3B, 2B$, laws L_7 and L_1 hold, which again makes it impossible to obtain 6 conjugacy classes.

(2) If $n = 4$, consider the following example:

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 2 | 4 | 1 | 3 |
| 3 | 1 | 4 | 2 |
| 4 | 3 | 2 | 1 |

FACE 1

| | | | |
|---|---|---|---|
| 4 | 1 | 2 | 3 |
| 1 | 3 | 4 | 2 |
| 2 | 4 | 3 | 1 |
| 3 | 2 | 1 | 4 |

FACE 2

| | | | |
|---|---|---|---|
| 3 | 4 | 1 | 2 |
| 4 | 2 | 3 | 1 |
| 1 | 3 | 2 | 4 |
| 2 | 1 | 4 | 3 |

FACE 3 .

| | | | |
|---|---|---|---|
| 2 | 3 | 4 | 1 |
| 3 | 1 | 2 | 4 |
| 4 | 2 | 1 | 3 |
| 1 | 4 | 3 | 2 |

FACE 4

L_2 is satisfied. L_1 corresponds to $\pi_1 = (1243)$. Now this means that everywhere there is a 1 in the second front vertical face, there should be a 2 in the first front vertical face and similarly for the pairs (1 and 3) and (1 and 4) in the third and fourth front vertical faces. Everytime there is a 3 or 4 in the second front vertical face, there should be a 2 in the corresponding place in faces 3 and 4 above. Finally, every position containing a 4 in face 3 above, should contain a 3 in the fourth front vertical face. One can check that these conditions do indeed hold and that they are enough to guarantee L_1 . Therefore L_1 , L_2 and L_3 are satisfied. However $\langle\langle 1,3,2 \rangle, 2,3 \rangle = \langle 2,2,3 \rangle = 2 \neq 1$. Hence L_6 does not hold. Therefore, the 3-quasigroup defined by the four faces above has 6 conjugacy classes.

(3) If $n = 6$, choose face 1 as follows:

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 3 | 1 | 6 | 4 | 5 |
| 3 | 1 | 2 | 5 | 6 | 4 |
| 4 | 6 | 5 | 1 | 2 | 3 |
| 5 | 4 | 6 | 2 | 3 | 1 |
| 6 | 5 | 4 | 3 | 1 | 2 |

The remaining faces are chosen all isotopic to Face 1 as follows. Let $\theta = \phi =$ identity mapping. For each face let ψ be defined as below:

| | | |
|-----------------|-----------------|-----------------|
| $\psi_2(1) = 2$ | $\psi_3(1) = 3$ | $\psi_4(1) = 4$ |
| $\psi_2(2) = 1$ | $\psi_3(2) = 5$ | $\psi_4(2) = 6$ |
| $\psi_2(3) = 4$ | $\psi_3(3) = 1$ | $\psi_4(3) = 2$ |
| $\psi_2(4) = 5$ | $\psi_3(4) = 6$ | $\psi_4(4) = 1$ |
| $\psi_2(5) = 6$ | $\psi_3(5) = 4$ | $\psi_4(5) = 3$ |
| $\psi_2(6) = 3$ | $\psi_3(6) = 2$ | $\psi_4(6) = 5$ |
| FACE 2 | FACE 3 | FACE 4 |

| | |
|---------------|---------------|
| $\psi(1) = 5$ | $\psi(1) = 6$ |
| $\psi(2) = 3$ | $\psi(2) = 4$ |
| $\psi(3) = 6$ | $\psi(3) = 5$ |
| $\psi(4) = 2$ | $\psi(4) = 3$ |
| $\psi(5) = 1$ | $\psi(4) = 2$ |
| $\psi(6) = 4$ | $\psi(4) = 1$ |
| FACE 5 | FACE 6 |

For example, Face 2 becomes:

| | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 4 | 5 | 6 | 3 |
| 1 | 4 | 2 | 3 | 5 | 6 |
| 4 | 2 | 1 | 6 | 3 | 5 |
| 5 | 3 | 6 | 2 | 1 | 4 |
| 6 | 5 | 3 | 1 | 4 | 2 |
| 3 | 6 | 5 | 4 | 2 | 1 |

As in Lemma 3.3.3, (2), where there is a 1 in the first vertical face, there is a 2 in the second, a 3 in the third, etc. In fact, the faces have been constructed so that L_1 holds. The faces 1-6 are commutative as quasigroups. Therefore L_1 , L_2 and L_3 hold. However L_6 would imply $\langle 2,4,5 \rangle = 4$ if and only if $\langle 4,5,4 \rangle = 2$. But $\langle 4,5,4 \rangle = 6$. Therefore the ternary quasigroup resulting from these faces has exactly 6 conjugacy classes.

Thus we have:

Theorem 3.3.4. If $n > 3$ and $n \neq 8, 12$ or 24 , there exists a 3-quasigroup of order n with 6 conjugacy classes.

If $n \leq 3$, there does not exist any 3-quasigroup of order n with 6 conjugacy classes.

Remark 3.3.5. Ternary quasigroups with 6 conjugacy classes of orders $n = 8, 12, 24$ will be constructed as a consequence

of Theorem 3.7.1 where a general theorem, providing many alternate constructions methods, is given.

§3.4 Four Classes.

Theorem 3.4.1. There exists a ternary quasigroup of order n with 4 conjugacy classes if and only if $n \geq 3$.

Proof: Let $Q = \{0, 1, 2, \dots, n-1\}$. Define $\langle a, b, c \rangle \equiv (a+b+c) \pmod{n} \forall a, b, c \in Q$. Then (Q, \langle, \rangle) is a 3-quasigroup satisfying $L_2, L_4, L_7, L_{10}, L_{11}$. Along with π_{24} , the corresponding permutations form a subgroup of order 6. However this subgroup is not itself a subgroup of the alternating subgroup A_4 . Furthermore, for $n > 2$, not all the identities hold. If $\langle a, b, d \rangle = c$, then $(a+b+(a+b+c)) \equiv c$ or $2(a+b) \equiv 0 \pmod{n}$ for all n , which is false. Therefore L_1 does not hold.

Remark 3.4.2. In this case, it is easy to provide constructions for 3-quasigroups satisfying the sets of laws corresponding to the remaining subgroups of order 6 of S_4 .

For the subgroup $\{\pi_2, \pi_5, \pi_9, \pi_{12}, \pi_{13}, \pi_{24}\}$, define $\langle a, b, c \rangle \equiv -a-b+c \pmod{n}$ on $Q = \{0, 1, 2, \dots, n-1\}$. Clearly L_2 is satisfied. For L_5 , $\langle d, b, c \rangle \equiv -(-a-b+c)-b+c \equiv a$; for L_9 , $\langle a, d, c \rangle \equiv -a-(-a-b+c) \equiv b$; and for L_{12} , $\langle b, d, c \rangle \equiv -b-(-a-b+c)+c \equiv a$. Similarly the subgroup $\{\pi_1, \pi_5, \pi_7, \pi_{14},$

π_{15}, π_{24} is obtained by defining $\langle a, b, c \rangle \equiv (-a+b-c) \pmod{n}$ and the subgroup $\{\pi_1, \pi_4, \pi_9, \pi_{16}, \pi_{17}, \pi_{24}\}$ by defining $\langle a, b, c \rangle \equiv (a-b-c) \pmod{n}$.

Definition 3.4.3. Let (Q, \langle, \rangle) be a 3-quasigroup which satisfies the generalized idempotent and commutative laws, but does not satisfy Steiner's law: $\langle x, y, \langle x, y, z \rangle \rangle = z$. Such a 3-quasigroup will be called a generalized idempotent and commutative non-Steiner ternary quasigroup.

Such quasigroups have been considered by C.C. Lindner [25], who observed that they will exist only if $n \equiv 2$ or $4 \pmod{6}$. For, as observed in Chapter 1, given such a 3-quasigroup (Q, \langle, \rangle) , we may define an ordinary quasigroup as follows: on $Q_i = Q \setminus \langle i \rangle$ define an operation \circ_i by $a \circ_i b = c$ if and only if $\langle a, b, c \rangle = i$. Then all these (Q_i, \circ_i) will be Steiner quasigroups.

The generalized idempotent and commutative non-Steiner 3-quasigroup has 4 conjugacy classes. It satisfies the identities corresponding to the subgroup $\{\pi_2, \pi_4, \pi_7, \pi_{10}, \pi_{11}, \pi_{24}\}$. The following theorem then provides yet another construction of a 3-quasigroup with 4 conjugacy classes.

Theorem 3.4.4. A generalized idempotent and commutative non-Steiner 3-quasigroup of order n exists if and only if $n \equiv 2$ or $4 \pmod{6}$, $n > 2$.

Proof: Necessity follows from the above comments.

To show the sufficiency, we make the following construction:

(1) Suppose (Q, \langle, \rangle) is a ternary quasigroup derived from a Steiner quadruple system of order n as described in Chapter 1. Furthermore, let (Q_1, \circ) and (Q_2, \circ) be defined as above and consider the triples (of 3 distinct elements) of (Q_1, \circ) which contain the element 1. Interchange these sets of triples. Redefine all the remaining triples (of three distinct elements) of (Q_1, \circ) to have value 2, and the remaining triples of (Q_2, \circ) to have value 1. If we call the resulting idempotent systems (Q_1, x) and (Q_2, x) , in (Q_1, x) we will have the triples of (Q_1, \circ) , which contained the element 2 and all the triples of (Q_2, \circ) , which did not contain the element 1. Similarly, in (Q_2, x) , we will have all the triples of (Q_2, \circ) which contained 1. The remaining (Q_1, \circ) will be left unchanged. Call the resulting system (Q, \langle, \rangle') .

(2) Proof that (Q, \langle, \rangle') is a ternary quasigroup:

Clearly all the triples of (Q, \langle, \rangle) are contained in (Q, \langle, \rangle') and no new ones have been added. There is no conflict between (Q_1, x) and (Q_2, x) , because, if a triple $\langle 1, e, f \rangle$ belonged to (Q_2, \circ) , then $\langle 2, e, f \rangle$ must have been in (Q_1, \circ) . For if $\langle 1, e, f \rangle = 2$, then $\langle \langle 1, e, f \rangle, e, f \rangle =$

$$\langle 2, e, f \rangle = 1 .$$

One then obtains $(Q, \langle \cdot, \cdot, \cdot \rangle')$ by requiring the generalized idempotent law to hold and defining $\langle \cdot, \cdot, \cdot \rangle'$ in terms of the (Q_1, x) , (Q_2, x) and (Q_i, \circ) , $i = 2, \dots, n$ as described in Chapter 1.

(3) Proof that $(Q, \langle \cdot, \cdot, \cdot \rangle')$ is non-Steiner:

Suppose $\langle x, y, z \rangle' = 2$ in $(Q, \langle \cdot, \cdot, \cdot \rangle')$, where $x \times y = z$ in (Q_2, x) and x, y, z are all different from 1 or 2. Now $\langle \langle x, y, z \rangle', y, z \rangle' = \langle 2, y, z \rangle' = \langle 2, y, z \rangle$. But $\langle \langle x, y, z \rangle', y, z \rangle = \langle 1, y, z \rangle = x$. Therefore $\langle 2, y, z \rangle \neq x$ and $(Q, \langle \cdot, \cdot, \cdot \rangle')$ is non-Steiner.

Remark 3.4.5. As an example, consider the Steiner Quadruple System described below of order 8 and the derived system $(Q, \langle \cdot, \cdot, \cdot \rangle')$. (For the sake of brevity, braces and commas are omitted.)

Quadruple System of Order 8

| | |
|---------|---------|
| 1 2 3 4 | 2 3 6 8 |
| 1 2 5 6 | 2 3 5 7 |
| 1 2 7 8 | 2 4 5 8 |
| 1 3 5 8 | 2 4 6 7 |
| 1 3 6 7 | 3 4 5 6 |
| 1 4 5 7 | 3 4 7 8 |
| 1 4 6 8 | 5 6 7 8 |

The Quasigroups (Q_i, \circ)

Here $a \circ b = c$ if and only if $\langle a, b, c \rangle$ form a triple in any order.

| | | | |
|---|---|---|---|
| $\langle 2, 3, 4 \rangle$ | $\langle 1, 3, 4 \rangle$ | $\langle 1, 2, 4 \rangle$ | $\langle 1, 2, 3 \rangle$ |
| $\langle 2, 5, 6 \rangle$ | $\langle 1, 5, 6 \rangle$ | $\langle 1, 5, 8 \rangle$ | $\langle 1, 5, 7 \rangle$ |
| $\langle 2, 7, 8 \rangle$ | $\langle 1, 7, 8 \rangle$ | $\langle 1, 6, 7 \rangle$ | $\langle 1, 6, 8 \rangle$ |
| $\langle 3, 5, 8 \rangle$ | $\langle 3, 6, 8 \rangle$ | $\langle 2, 6, 8 \rangle$ | $\langle 3, 5, 6 \rangle$ |
| $\langle 3, 6, 7 \rangle$ | $\langle 3, 5, 7 \rangle$ | $\langle 2, 5, 7 \rangle$ | $\langle 3, 7, 8 \rangle$ |
| $\langle 4, 5, 7 \rangle$ | $\langle 4, 5, 8 \rangle$ | $\langle 4, 5, 6 \rangle$ | $\langle 2, 5, 8 \rangle$ |
| $\langle 4, 6, 8 \rangle$ | $\langle 4, 6, 7 \rangle$ | $\langle 4, 7, 8 \rangle$ | $\langle 2, 6, 7 \rangle$ |
| <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> |
| (Q_1, \circ) | (Q_2, \circ) | (Q_3, \circ) | (Q_4, \circ) |
| $\langle 1, 2, 6 \rangle$ | $\langle 1, 4, 8 \rangle$ | $\langle 1, 3, 6 \rangle$ | $\langle 1, 3, 5 \rangle$ |
| $\langle 1, 3, 8 \rangle$ | $\langle 1, 3, 7 \rangle$ | $\langle 1, 4, 5 \rangle$ | $\langle 1, 2, 7 \rangle$ |
| $\langle 1, 4, 7 \rangle$ | $\langle 1, 2, 5 \rangle$ | $\langle 1, 2, 8 \rangle$ | $\langle 1, 4, 6 \rangle$ |
| $\langle 2, 4, 8 \rangle$ | $\langle 2, 3, 8 \rangle$ | $\langle 2, 3, 5 \rangle$ | $\langle 2, 3, 6 \rangle$ |
| $\langle 2, 3, 7 \rangle$ | $\langle 2, 4, 7 \rangle$ | $\langle 2, 4, 6 \rangle$ | $\langle 2, 4, 5 \rangle$ |
| $\langle 3, 4, 6 \rangle$ | $\langle 3, 4, 5 \rangle$ | $\langle 3, 4, 8 \rangle$ | $\langle 3, 4, 7 \rangle$ |
| $\langle 6, 7, 8 \rangle$ | $\langle 5, 7, 8 \rangle$ | $\langle 5, 6, 8 \rangle$ | $\langle 5, 6, 7 \rangle$ |
| <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> |
| (Q_5, \circ) | (Q_6, \circ) | (Q_7, \circ) | (Q_8, \circ) |

| <u>The Derived Quasigroups</u> | (Q_i, x) for $i = 1, 2$ |
|---|---|
| $\langle 2, 3, 4 \rangle$ | $\langle 1, 3, 4 \rangle$ |
| $\langle 2, 5, 6 \rangle$ | $\langle 1, 5, 6 \rangle$ |
| $\langle 2, 7, 8 \rangle$ | $\langle 1, 7, 8 \rangle$ |
| $\langle 3, 6, 8 \rangle$ | $\langle 3, 5, 8 \rangle$ |
| $\langle 3, 5, 7 \rangle$ | $\langle 3, 6, 7 \rangle$ |
| $\langle 4, 5, 8 \rangle$ | $\langle 4, 5, 7 \rangle$ |
| $\langle 4, 6, 7 \rangle$ | $\langle 4, 6, 8 \rangle$ |
| <hr style="width: 50%; margin: 0 auto;"/> | <hr style="width: 50%; margin: 0 auto;"/> |
| (Q_1, x) | (Q_2, x) |

§3.5 Three Classes.

Theorem 3.5.1. A ternary quasigroup of order n with exactly 3 conjugacy classes exists if and only if $n \geq 3$.

Proof: On $Q = \{0, 1, 2, \dots, n-1\}$, define $\langle a, b, c \rangle = a - b + c$, with addition (mod n). Consider L_{18} , $\langle d, a, b \rangle \equiv c$ implies $(a - b + c) - a + b \equiv c$. Therefore L_{18} , L_{20} and L_8 all hold. Clearly L_7 holds and so does L_9 as L_8 and L_7 imply L_9 . L_3 states that $\langle b, a, d \rangle \equiv c$ or $b - a + (a - b + c) \equiv c$. L_6 gives $\langle d, c, b \rangle \equiv a$ or $(a - b + c) - c + b \equiv a$. Therefore all the identities corresponding to the elements of the subgroup $\{\pi_3, \pi_6, \pi_7, \pi_8, \pi_9, \pi_{18}, \pi_{20}, \pi_{24}\}$ are satisfied. However, L_1 would require $a - b + (a - b + c) \equiv c$. This implies

$2(a-b) \equiv 0 \pmod{n}$ for all $a, b \in Q$, which is false. Therefore, $|C(Q, \circ)| = 3$.

Remark 3.5.2. Again it is possible to construct 3-quasigroups which satisfy sets of identities corresponding to the other permutation subgroups of order 8. For the subgroup $\{\pi_1, \pi_2, \pi_3, \pi_6, \pi_8, \pi_{19}, \pi_{23}, \pi_{24}\}$, define a ternary operation on Q by $\langle a, b, c \rangle \equiv (a+b-c) \pmod{n}$ and for the subgroup $\{\pi_3, \pi_4, \pi_5, \pi_6, \pi_8, \pi_{21}, \pi_{22}, \pi_{24}\}$ take $\langle a, b, c \rangle \equiv (-a+b+c) \pmod{n}$.

§3.6 One Class.

Theorem 3.6.1. For all $n \geq 1$, there exists a ternary quasigroup of order n with exactly one conjugacy class.

Proof: On $Q = \{0, 1, 2, \dots, n-1\}$ define a ternary operation $\langle \cdot, \cdot, \cdot \rangle$ by $\langle a, b, c \rangle = -(a+b+c) \pmod{n}$ $\forall a, b, c \in Q$ where addition is modulo n . Then clearly L_{11} is satisfied. L_{18} requires that $\langle \langle b, c, d \rangle, b, c \rangle \equiv d$ and here $\langle \langle b, c, d \rangle, b, c \rangle = -(-(b+c+d)+b+c) \equiv d$. From §2.2, $|C(Q, \langle \cdot, \cdot, \cdot \rangle)| = 1$.

§3.7 Conclusion.

The following general theorem provides many useful alternate constructions to those given throughout Chapter 3

and completes the construction of ternary quasigroups of all orders greater than 3 with 6 conjugacy classes.

Theorem 3.7.1. If q/n is any factor of n and if there exists a ternary quasigroup of order q with a specified number of conjugacy classes, then there exists a ternary quasigroup of order n with the same specified number of conjugates.

Proof: Let (Q, \langle, \rangle) be the 3-quasigroup defined in Theorem 3:6.1. Suppose $n = pq$; $q > 1$, $p > 1$. Consider the q elements $\{0, p, 2p, \dots, (q-1)p\}$. We can denote them by $\{mp\}$, $m = 0, \dots, q-1$. Then $\langle m_1 p, m_2 p, m_3 p \rangle = -(m_1 + m_2 + m_3)p \equiv \ell p \pmod{n}$ where $m_i \in \{mp\}$, $\ell = rq - (m_1 + m_2 + m_3)$, $\ell p \in \{0, \dots, n-1\}$ and $\ell p = -(m_1 + m_2 + m_3) + rn$. Therefore (P, \langle, \rangle) where $P = \{mp\}$, $m = 0, \dots, q-1$, forms a subquasigroup of (Q, \langle, \rangle) of order q .

On P define a new ternary quasigroup (P, \langle, \rangle') of order q with a specified number c of conjugacy classes. Replace (P, \langle, \rangle) by (P, \langle, \rangle') within the larger quasigroup (Q, \langle, \rangle) . Call the resulting quasigroup of order n (Q, \langle, \rangle') . On P , only $24/c$ identities will be satisfied and therefore (Q, \langle, \rangle') can have no fewer than c conjugacy classes. However, all those $\frac{24}{c}$ identities are satisfied by (Q, \langle, \rangle') and therefore (Q, \langle, \rangle') must have no more than c conjugacy classes.

Corollary 3.7.2. There exists a ternary quasigroup of order $n = 8, 12$ and 24 with exactly 6 conjugacy classes.

Proof: This follows from Lemma 3.3.3, which gives the existence of a ternary quasigroup of order 4 with 6 conjugacy classes.

In conclusion, we summarize the results obtained in this chapter:

Theorem 3.7.3.

- (1) There exist 3-quasigroups of order n with 6, 12 or 24 conjugacy classes if and only if $n \geq 4$.
- (2) There exist 3-quasigroups of order n with 3 or 4 conjugacy classes if and only if $n \geq 3$.
- (3) There exists a ternary quasigroup with one conjugacy class for all orders ≥ 1 .

CHAPTER 4

The Existence of Ternary Quasigroups with 2 or 8 Conjugacy Classes

§4.1. The Structure of Ternary Quasigroups having 2 or 8 Conjugacy Classes.

Recall from §2.2 that the sets of identities which must be satisfied by a 3-quasigroup (and no others) to enable that quasigroup to have 8 conjugacy classes are:

(1) Identities 10 and 11; represented by L_{10} :

$$\langle a, b, c \rangle = \langle c, a, b \rangle .$$

(2) Identities 12 and 13; represented by L_{12} :

$$\langle a, \langle d, a, c \rangle, c \rangle = d .$$

(3) Identities 14 and 15; represented by L_{14} :

$$\langle a, b, \langle d, b, a \rangle \rangle = d .$$

(4) Identities 16 and 17; represented by L_{16} :

$$\langle a, \langle a, c, d \rangle, c \rangle = d .$$

Definition 4.1.1. If (Q, \circ) is an ordinary quasigroup and $a \circ b = c$ implies $b \circ c = a$ and $c \circ a = b$ for all $a, b, c \in Q$, then (Q, \circ) is called a cyclic quasigroup. This corresponds to requiring that $a \circ (b \circ a) = (a \circ b) \circ a = b$ for all $a, b \in Q$. (See [23], [26], [28], [32].)

Theorem 4.1.2. Let $(Q, <, , >)$ be a ternary quasigroup which satisfies the identities in identity set (i), $1 \leq i \leq 4$. Then one may derive a set of cyclic quasigroups (Q_{ij}, \circ) , $j = 1, 2, \dots, |Q|$, from $(Q, <, , >)$.

Proof: If $i = 1$, define (Q_{1j}, \circ) as follows: $a \circ b = c$ if and only if $\langle a, b, c \rangle = j$ and $a, b, c \in Q$. For $i = 2$, (Q_{ij}, \circ) is defined to be (Q_{F_j}, \circ) ; for $i = 3$, (Q_{ij}, \circ) is defined to be (Q_{S_j}, \circ) ; for $i = 4$, (Q_{ij}, \circ) is defined to be (Q_{H_j}, \circ) .

Remark 4.1.3. The following Theorems 4.1.4 and 4.1.5 are a result of §2.2 and an investigation of the generators of A_4 , the alternating subgroup.

Theorem 4.1.4. $C|(Q, <, , >)| = 2$ if and only if at least two of the identity sets (1) to (4) are satisfied by $(Q, <, , >)$ and at least one (Q_{ij}, \circ) , $i = 1, 2, \dots, 4$, $j = 1, 2, \dots, |Q|$, is non-commutative.

Theorem 4.1.5. $C|(Q, <, , >)| = 8$ if and only if:

- (1) $(Q, <, , >)$ satisfies at least one identity set (i),
- (2) $(Q, <, , >)$ does not satisfy at least one identity set (k),
- (3) at least one (Q_{ij}, \circ) , $j = 1, 2, \dots, |Q|$ is non-commutative.

Proof: Here this follows from the fact that the identities in sets (1) through (4) and the identities which are equivalent to commutativity in the derived cyclic quasigroups correspond to permutations, in each case, which belong to the same subgroup of order 6.

Remark 4.1.6. The literature quoted in Definition 4.1.1 has been investigated with the following conclusions. If one tries to undertake a construction similar to that described in Theorem 1.3.10 of Chapter 1, whereby a set of n cyclic quasigroups of order n are used to form the n faces of the graphical representation of a ternary quasigroup, then, if the quasigroups are isomorphic, they can contain at most one idempotent. As only isomorphism, and not weaker isotopism preserves the cyclic structure of a quasigroup, the possibility of a construction, based on generating a set of n cyclic quasigroups from a single one by isomorphism, necessitates the restriction on the number of idempotents. This, however, eliminates the use of papers [35] and [32].

Another possible construction would be to make use of the section of [33] discussing the case of exactly two conjugacy classes and its generalization in [28]. Many examples were tried for use as the above faces, not necessarily all isomorphic, but no ternary examples could be constructed.

However, in the next section, some constructions were found using quadruple systems and building infinite classes

from lower order examples.

§4.2. The Case of 2 or 8 Conjugacy Classes for Orders ≤ 5 .

Theorem 4.2.1. There does not exist any ternary quasigroup of order 3 with 2 or 8 conjugacy classes.

Proof: By Theorem 3.2.4, every ternary quasigroup of order 3 satisfies at least one of L_2 , L_4 and L_7 and thus cannot have 2 or 8 conjugacy classes.

Theorem 4.2.2. There does not exist any ternary quasigroup of order 4 with 2 or 8 conjugacy classes.

Proof: (1) At least one of identity sets (1) through (4) of §4.1 must be satisfied, by Theorem 4.1.4 and 4.1.5. As any two of the four identity sets imply the rest, $(Q, <, >)$ will have 2 or 8 conjugacy classes only if there exists a (Q_{ij}, \circ) which is cyclic and non-commutative. Without loss of generality, suppose (Q_{ij}, \circ) , $(i = 2, \dots, 4, j = 1, \dots, 4)$ is one such quasigroup. Furthermore, suppose $2 \circ 1 \neq 1 \circ 2$, where $Q = \{1, 2, 3, 4\}$. Then $2 \circ 1$ cannot equal 1 or 2 and similarly for $1 \circ 2$. For suppose $1 \circ 2 = 1$. Then $2 \circ (1 \circ 2) = 2 \circ 1 = 1$ also. We obtain a similar contradiction in the other cases. Therefore the only possibility for (Q_{ij}, \circ) is:

| | | | | |
|---|---|---|---|---|
| ◦ | 1 | 2 | 3 | 4 |
| 1 | 1 | 3 | 4 | 2 |
| 2 | 4 | 2 | 1 | 3 |
| 3 | 2 | 4 | 3 | 1 |
| 4 | 3 | 1 | 2 | 4 |

and its transpose.

As these quasigroups are idempotent, not all the $\{(Q_{ij}, \circ), j = 1, 2, 3, 4\}$ can be non-commutative.

Suppose then that some of the (Q_{ik}, \circ) are commutative and (Q_{ij}, \circ) , as before, is not. Clearly if (Q_{ik}, \circ) is commutative it cannot be idempotent, as it is not Steiner, if the order is 4. In fact, none of the (Q_{ik}, \circ) , except (Q_{ij}, \circ) , can have any idempotents at all. If $1 \circ 1 = 2$ in (Q_{ik}, \circ) , then it follows that $1 \circ 2 = 1 = 2 \circ 1$ and the only possible quasigroups, when trying to minimize the number of idempotents are:

| | | | | |
|---|---|---|---|---|
| ◦ | 1 | 2 | 3 | 4 |
| 1 | 2 | 1 | 4 | 3 |
| 2 | 1 | 3 | 2 | 4 |
| 3 | 4 | 2 | 3 | 1 |
| 4 | 3 | 4 | 1 | 2 |

and

| | | | | |
|---|---|---|---|---|
| ◦ | 1 | 2 | 3 | 4 |
| 1 | 2 | 1 | 4 | 3 |
| 2 | 1 | 4 | 3 | 2 |
| 3 | 4 | 3 | 2 | 1 |
| 4 | 3 | 2 | 1 | 4 |

As both of these contain at least one idempotent element, we

have a contradiction if identity sets (2) to (4) are the ones involved.

(2) If identity set (1) is involved, then the (Q_{1j}, \circ) , $j = 1, 2, 3, 4$ are all cyclic. If some (Q_{1j}, \circ) is idempotent, the remaining quasigroups (Q_{1j}, \circ) cannot have any idempotents. For if $\langle a, a, a \rangle = j_1$, for all $a \in Q$, $\langle a, a, a \rangle$ cannot be j_i for another $j_i \in \{1, 2, 3, 4\}$. As at least one (Q_{1j}, \circ) must be non-commutative, our arguments in part (1) of the proof show that identity set (1) cannot be satisfied.

Therefore (Q, \langle, \rangle) cannot have 2 or 8 conjugacy classes.

Theorem 4.2.3. There exists a ternary quasigroup of order 5 with 8 conjugacy classes.

Proof: Let (Q, \langle, \rangle) be a ternary quasigroup defined on $Q = \{1, 2, 3, 4, 5\}$ as follows:

$$\begin{array}{ll} \langle 1, 2, 3 \rangle = 1 & \langle 2, 1, 3 \rangle = 2 \\ \langle 1, 2, 4 \rangle = 2 & \langle 2, 1, 4 \rangle = 3 \\ \langle 1, 2, 5 \rangle = 3 & \langle 2, 1, 5 \rangle = 1 \end{array}$$

$$\begin{array}{ll}
\langle 1,3,4 \rangle = 5 & \langle 3,1,4 \rangle = 2 \\
\langle 1,3,5 \rangle = 1 & \langle 3,1,5 \rangle = 5 \\
\langle 2,3,4 \rangle = 2 & \langle 3,2,4 \rangle = 4 \\
\langle 2,3,5 \rangle = 4 & \langle 3,2,5 \rangle = 1 \\
\langle 1,4,5 \rangle = 5 & \langle 4,1,5 \rangle = 3 \\
\langle 2,4,5 \rangle = 3 & \langle 4,2,5 \rangle = 4 \\
\langle 3,4,5 \rangle = 4 & \langle 4,3,5 \rangle = 5
\end{array}$$

$$\begin{array}{llllll}
\langle 1,1,1 \rangle = 4 & \langle 2,1,1 \rangle = 5 & \langle 3,1,1 \rangle = 3 & \langle 4,1,1 \rangle = 1 & \langle 5,1,1 \rangle = 2 \\
\langle 1,2,2 \rangle = 4 & \langle 2,2,2 \rangle = 5 & \langle 3,2,2 \rangle = 3 & \langle 2,2,4 \rangle = 1 & \langle 2,2,5 \rangle = 2 \\
\langle 1,3,3 \rangle = 4 & \langle 2,3,3 \rangle = 5 & \langle 3,3,3 \rangle = 3 & \langle 4,3,3 \rangle = 1 & \langle 5,3,3 \rangle = 2 \\
\langle 1,4,4 \rangle = 4 & \langle 2,4,4 \rangle = 5 & \langle 3,4,4 \rangle = 3 & \langle 4,4,4 \rangle = 1 & \langle 5,4,4 \rangle = 2 \\
\langle 1,5,5 \rangle = 4 & \langle 2,5,5 \rangle = 5 & \langle 3,5,5 \rangle = 3 & \langle 4,5,5 \rangle = 1 & \langle 5,5,5 \rangle = 2
\end{array}$$

The definition is completed to make the cyclic laws 10 and 11 satisfied. Clearly (Q, \langle, \rangle) is not totally commutative.

One sees that $\langle 1,2, \langle 3,1,2 \rangle \rangle = 5$ and not 3. Therefore, this quasigroup has exactly 8 conjugacy classes.

Theorem 4.2.4. There exists a ternary quasigroup of order 5 with exactly 2 conjugacy classes.

Proof: Consider the following definition of a ternary quasigroup (Q, \langle, \rangle) of order 5, which satisfies the generalized idempotent law. The cyclic laws L_{10} and L_{11} are also satisfied.

| | |
|-------------------------------|-------------------------------|
| $\langle 1, 2, 3 \rangle = 4$ | $\langle 1, 4, 5 \rangle = 2$ |
| $\langle 2, 1, 3 \rangle = 5$ | $\langle 4, 1, 5 \rangle = 3$ |
| $\langle 1, 2, 4 \rangle = 5$ | $\langle 2, 3, 4 \rangle = 5$ |
| $\langle 2, 1, 4 \rangle = 3$ | $\langle 3, 2, 4 \rangle = 1$ |
| $\langle 1, 2, 5 \rangle = 3$ | $\langle 2, 3, 5 \rangle = 1$ |
| $\langle 2, 1, 5 \rangle = 4$ | $\langle 3, 2, 5 \rangle = 4$ |
| $\langle 1, 3, 4 \rangle = 2$ | $\langle 2, 4, 5 \rangle = 3$ |
| $\langle 3, 1, 4 \rangle = 5$ | $\langle 4, 2, 5 \rangle = 1$ |
| $\langle 1, 3, 5 \rangle = 4$ | $\langle 3, 4, 5 \rangle = 1$ |
| $\langle 3, 1, 5 \rangle = 2$ | $\langle 4, 3, 5 \rangle = 2$ |

Clearly L_2 is not satisfied. However L_{12} is. For suppose $a = b$. Then $\langle a, a, c \rangle = d = c$ implies $\langle a, c, c \rangle = a$, by idempotency. If $a \neq b$, but $c = a$ or b , $\langle a, b, a \rangle = b$ implies $\langle b, b, a \rangle = a$. If $c = b$, $\langle a, b, b \rangle = a$ implies $\langle b, a, b \rangle = a$. Therefore, if any 2 elements are equal, law 12 is satisfied. Now suppose the 5 elements in Q are a, b, c, d and e and that $\langle c, a, b \rangle = d$ or e . Suppose in fact it is d . Then $\langle a, \langle c, a, b \rangle, b \rangle = \langle a, d, b \rangle$. Suppose this equals e and not c . Then $\langle a, d, b \rangle = c$. However $\langle a, b, c \rangle = d$ by the cyclic law, and so $\langle a, c, b \rangle$ must be e . But $\langle a, d, b \rangle = e$ then gives $c = d$ and therefore $\langle a, \langle c, a, b \rangle, b \rangle = c$. A similar contradiction is obtained if we had supposed $\langle c, a, b \rangle = e$. Therefore by Theorem 4.1.4 of §4.1, $(Q, \langle \cdot, \cdot, \cdot \rangle)$ has exactly 2 conjugacy classes.

§4.3 The Case of 2 or 8 Conjugacy Classes for Orders 8 and 10.

Theorem 4.3.1. There exists a ternary quasigroup of order 8 with exactly 8 conjugacy classes.

Proof: Consider the Steiner quadruple system given following Remark 3.4.5. Again let the derived quasigroup by (Q_i, \circ) , $i = 1, 2, \dots, 8$, where $a \circ b = c$ if and only if $\langle a, b, c \rangle = i$, $i = 1, 2, \dots, 8$, where (Q, \langle, \rangle) is the ternary quasigroup corresponding to the quadruple system.

We will construct a set of replacements for the (Q_i, \circ) which will be used to reconstruct a new ternary quasigroup with 8 conjugacy classes. The new quasigroups will be denoted by (Q_i, \times) and will be idempotent and cyclic, but not necessarily commutative.

The eight quasigroups (Q_i, \times) are defined as follows: (where it is assumed that $\langle a, b, c \rangle = \langle b, c, a \rangle = \langle c, a, b \rangle = \langle b, a, c \rangle = \langle a, c, b \rangle = \langle c, b, a \rangle$, if only one triple appears containing a , b and c .)

| | |
|-----------------------------|-----------------------------|
| $\langle 2 \ 3 \ 4 \rangle$ | $\langle 1 \ 3 \ 4 \rangle$ |
| $\langle 2 \ 5 \ 6 \rangle$ | $\langle 1 \ 5 \ 6 \rangle$ |
| $\langle 2 \ 7 \ 8 \rangle$ | $\langle 1 \ 7 \ 8 \rangle$ |
| $\langle 3 \ 5 \ 8 \rangle$ | $\langle 5 \ 3 \ 8 \rangle$ |
| $\langle 3 \ 6 \ 7 \rangle$ | $\langle 6 \ 3 \ 7 \rangle$ |
| $\langle 5 \ 3 \ 7 \rangle$ | $\langle 3 \ 5 \ 7 \rangle$ |

$$\begin{array}{cc}
 \langle 6 \ 3 \ 8 \rangle & \langle 3 \ 6 \ 8 \rangle \\
 \langle 4 \ 5 \ 7 \rangle & \langle 5 \ 4 \ 7 \rangle \\
 \langle 5 \ 4 \ 8 \rangle & \langle 4 \ 5 \ 8 \rangle \\
 \langle 6 \ 4 \ 7 \rangle & \langle 4 \ 6 \ 7 \rangle \\
 \langle 4 \ 6 \ 8 \rangle & \langle 6 \ 4 \ 8 \rangle \\
 \hline
 (Q_1, x) & (Q_2, x)
 \end{array}$$

The remaining (Q_i, x) , $i = 3, \dots, 8$ remain as obtained from the quadruple system originally. Thus $(Q_i, x) = (Q_i, \circ)$, for $i = 3, \dots, 8$.

One may verify by inspection that (Q_1, x) and (Q_2, x) are indeed quasigroups and can see that one may form a new ternary quasigroup (Q, \langle, \rangle') by replacing the (Q_i, \circ) by (Q_i, x) and requiring the generalized idempotent law to hold.

Clearly (Q_1, x) and (Q_2, x) are not commutative. To see that L_{12} is not satisfied, note that $\langle 3, \langle 6, 3, 8 \rangle', 8 \rangle' = \langle 3, 1, 8 \rangle' = 5$ and not 6. Therefore by Theorem 4.1.5, (Q, \langle, \rangle') has exactly 8 conjugacy classes.

Theorem 4.3.2. There exists a ternary quasigroup of order 8 with exactly 2 conjugacy classes.

Proof: Beginning with the same quadruple system used in Theorem 4.3.1, the derived quasigroups (Q_i, \circ) , $i = 1, \dots, 8$, are now replaced by the new quasigroups (Q_i, x) , $i = 1, \dots, 8$, as follows:

| | | | |
|----------------------|----------------------|----------------------|----------------------|
| <2 3 4> | <1 3 4> | <1 2 4> | <1 2 3> |
| <2 5 6> | <1 5 6> | <4 5 6> | <3 5 6> |
| <2 7 8> | <1 7 8> | <4 7 8> | <3 7 8> |
| <3 5 8> | <5 3 8> | <2 5 8> | <5 2 8> |
| <4 5 7> | <5 4 7> | <5 2 7> | <2 5 7> |
| <3 6 7> | <6 3 7> | <5 1 8> | <1 5 8> |
| <4 6 8> | <6 4 8> | <6 2 8> | <2 6 8> |
| <5 3 7> | <3 5 7> | <1 6 8> | <6 1 8> |
| <3 8 6> | <3 6 8> | <1 5 7> | <5 1 7> |
| <6 4 7> | <4 6 7> | <6 1 7> | <1 6 7> |
| <5 4 8> | <4 5 8> | <2 6 7> | <6 2 7> |
| _____ | _____ | _____ | _____ |
| (Q ₁ , x) | (Q ₂ , x) | (Q ₃ , x) | (Q ₄ , x) |
| <1 2 6> | <1 2 5> | <1 2 8> | <1 2 7> |
| <3 4 6> | <3 4 5> | <3 4 8> | <3 4 7> |
| <6 7 8> | <5 7 8> | <5 6 8> | <5 6 7> |
| <1 3 8> | <3 1 8> | <1 3 5> | <3 1 5> |
| <3 2 8> | <2 3 8> | <5 3 2> | <3 5 2> |
| <2 4 8> | <4 2 8> | <3 1 6> | <1 3 6> |
| <4 1 8> | <1 4 8> | <4 1 5> | <1 4 5> |
| <1 4 7> | <4 1 7> | <1 4 6> | <4 1 6> |
| <3 1 7> | <1 3 7> | <4 2 6> | <2 4 6> |
| <2 3 7> | <3 2 7> | <2 3 6> | <3 2 6> |
| <4 2 7> | <2 4 7> | <2 4 5> | <4 2 5> |
| _____ | _____ | _____ | _____ |
| (Q ₅ , x) | (Q ₆ , x) | (Q ₇ , x) | (Q ₈ , x) |

The basic method of construction is the same as that used in Theorem 4.3.1, however, here the triples belonging to (Q_3, \circ) have been split in pairs with those of (Q_4, \circ) to form (Q_3, x) and (Q_4, x) . The same type of splitting is done between (Q_5, \circ) and (Q_6, \circ) and also between (Q_7, \circ) , (Q_8, x) to form (Q_5, x) , (Q_6, x) and (Q_7, x) , (Q_8, x) respectively. This splitting has been done precisely to ensure that L_{12} is satisfied by the new ternary quasigroup (Q, \langle, \rangle) constructed from (Q_i, x) , $i = 1, \dots, 8$ as described in Chapter 1.

For example, $\langle 5, \langle 3, 5, 8 \rangle, 8 \rangle = \langle 5, 1, 8 \rangle = 3$,
 $\langle 8, \langle 5, 8, 3 \rangle, 3 \rangle = \langle 8, 1, 3 \rangle = 5$ and $\langle 3, \langle 8, 3, 5 \rangle, 5 \rangle =$
 $\langle 3, 1, 5 \rangle = 8$. One may verify that L_{12} is satisfied in all instances by inspection and therefore (Q, \langle, \rangle) , constructed from these eight quasigroups, has 2 conjugacy classes by Theorem 4.1.4.

Theorem 4.3.3. There exists a ternary quasigroup of order 10 with exactly 8 conjugacy classes.

Proof: Consider the following Steiner quadruple system of order 10:

| | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 4 | 5 | 1 | 2 | 3 | 7 | 1 | 3 | 5 | 8 |
| 2 | 3 | 5 | 6 | 2 | 3 | 4 | 8 | 2 | 4 | 6 | 9 |
| 3 | 4 | 6 | 7 | 3 | 4 | 5 | 9 | 3 | 5 | 7 | 10 |
| 4 | 5 | 7 | 8 | 4 | 5 | 6 | 10 | 4 | 6 | 8 | 1 |
| 5 | 6 | 8 | 9 | 5 | 6 | 7 | 1 | 5 | 7 | 9 | 2 |
| 6 | 7 | 9 | 10 | 6 | 7 | 8 | 2 | 6 | 8 | 10 | 3 |
| 7 | 8 | 10 | 1 | 7 | 8 | 9 | 3 | 7 | 9 | 1 | 4 |
| 8 | 9 | 1 | 2 | 8 | 9 | 10 | 4 | 8 | 10 | 2 | 5 |
| 9 | 10 | 2 | 3 | 9 | 10 | 1 | 5 | 9 | 1 | 3 | 6 |
| 10 | 1 | 3 | 4 | 10 | 1 | 2 | 6 | 10 | 2 | 4 | 7 |

As in Theorem 4.3.1, consider the derived quasigroups (Q_i, \circ) , where now $i = 1, \dots, 10$. For $i = 1$ and 2 we have:

| (Q_1, \circ) | (Q_2, \circ) |
|--|--|
| $\langle 4 \ 7 \ 9 \rangle$ | $\langle \underline{1} \ \underline{4} \ \underline{5} \rangle$ |
| $\langle \underline{2} \ \underline{4} \ \underline{5} \rangle$ | $\langle 3 \ 5 \ 6 \rangle$ |
| $\langle 7 \ 8 \ 10 \rangle$ | $\langle \underline{1} \ \underline{8} \ \underline{9} \rangle$ |
| $\langle \underline{2} \ \underline{8} \ \underline{9} \rangle$ | $\langle 3 \ 9 \ 10 \rangle$ |
| $\langle 3 \ 4 \ 10 \rangle$ | $\langle \underline{1} \ \underline{3} \ \underline{7} \rangle$ |
| $\langle \underline{2} \ \underline{3} \ \underline{7} \rangle$ | $\langle 3 \ 4 \ 8 \rangle$ |
| $\langle 5 \ 6 \ 7 \rangle$ | $\langle 6 \ 7 \ 8 \rangle$ |
| $\langle 9 \cdot 10 \ 5 \rangle$ | $\langle \underline{1} \ \underline{6} \ \underline{10} \rangle$ |
| $\langle \underline{10} \ \underline{2} \ \underline{6} \rangle$ | $\langle 4 \ 6 \ 9 \rangle$ |
| $\langle 3 \ 5 \ 8 \rangle$ | $\langle 5 \ 7 \ 9 \rangle$ |
| $\langle 4 \ 6 \ 8 \rangle$ | $\langle 5 \ 8 \ 10 \rangle$ |
| $\langle 3 \ 6 \ 9 \rangle$ | $\langle 4 \ 7 \ 10 \rangle$ |

As in Theorem 4.3.1, we split all the triples, except the circled ones, to obtain (Q_1, x) and (Q_2, x) , leaving (Q_i, \circ) , $i = 3, \dots, 10$ unchanged.

| | |
|------------|------------|
| <2 4 5> | <1 4 5> |
| <2 8 9> | <1 8 9> |
| <2 3 7> | <1 3 7> |
| <2 6 10> | <1 6 10> |
| <3 6 9> | <6 3 9> |
| <4 7 9> | <7 4 9> |
| <7 5 9> | <5 7 9> |
| <6 4 9> | <4 6 9> |
| <7 4 10> | <4 7 10> |
| <6 5 7> | <5 6 7> |
| <3 5 6> | <3 6 5> |
| <6 7 8> | <7 6 8> |
| <8 7 10> | <7 8 10> |
| <4 6 8> | <6 4 8> |
| <3 4 8> | <4 3 8> |
| <4 3 10> | <3 4 10> |
| <10 3 9> | <3 10 9> |
| <10 9 5> | <9 10 5> |
| <5 8 10> | <8 5 10> |
| <5 3 8> | <3 5 8> |
| <hr/> | <hr/> |
| (Q_1, x) | (Q_2, x) |

It is clear that (Q_1, x) and (Q_2, x) are quasigroups and that L_{12} is not satisfied, if these replace (Q_1, \circ) and (Q_2, \circ) . For $\langle 3, \langle 6, 3, 9 \rangle', 9 \rangle' = \langle 3, 2, 9 \rangle' = 10$ and not 6. Therefore $(Q, \langle, \circ \rangle')$ has exactly 8 conjugacy classes.

Theorem 4.3.4. There exists a ternary quasigroup of order 10 with exactly 2 conjugacy classes.

Proof: (1) The Construction:

Let (Q_1, x) and (Q_2, x) be defined as in Theorem 4.3.3. For any $m > 2$, m occurs in 6 of the split triples listed in the definition of (Q_1, x) and in 6 listed for (Q_2, x) . (For example, if $m = 3$, m occurs in $\langle 3, 6, 9 \rangle$, $\langle 3, 5, 6 \rangle$, $\langle 3, 4, 8 \rangle$, $\langle 4, 3, 10 \rangle$, $\langle 10, 3, 9 \rangle$ and $\langle 5, 3, 8 \rangle$ of Q_1 and $\langle 6, 3, 9 \rangle$, $\langle 5, 3, 6 \rangle$, $\langle 4, 3, 8 \rangle$, $\langle 3, 4, 10 \rangle$ and $\langle 3, 10, 9 \rangle$ of Q_2 .) This then defines 12 triples (a, b, c) such that $\langle a, b, c \rangle = m$ by forcing L_{12} to be satisfied. That is, we require $\langle x, \langle m, x, y \rangle', y \rangle' = m$, where $\langle m, x, y \rangle' = 1$ or 2 .

Now of the 6 triples coming from (Q_1, x) , exactly 3 were in the original list for (Q_1, \circ) and similarly for (Q_2, x) . (For $n = 3$, $\langle 3, 6, 9 \rangle$, $\langle 3, 5, 8 \rangle$, and $\langle 3, 4, 10 \rangle$ were originally in (Q_1, \circ) .) Thus exactly 6 of the 12 triples now defined to be m occurred originally in the definition of (Q_m, \circ) . We will define (Q_m, x) to consist of the remaining 6 triples of (Q_m, \circ) , taken in all 6 permutations, along with the 12 new triples as defined by $\langle x, \langle m, x, y \rangle', y \rangle' = m$.

The construction is given below, where the circled triples are taken in all 6 orders and the *'d triples were in the original (Q_i, \circ) . The remaining 6 triples come from the split triples of (Q_i, x) , $i = 1, 2$ which were not originally in (Q_1, \circ) .

| | | | |
|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| $(\langle 1 \ 2 \ 7 \rangle)$ | $(\langle 1 \ 2 \ 5 \rangle)$ | $(\langle 1 \ 2 \ 4 \rangle)$ | $(\langle 1 \ 2 \ 10 \rangle)$ |
| $(\langle 7 \ 8 \ 9 \rangle)$ | $(\langle 9 \ 8 \ 10 \rangle)$ | $(\langle 7 \ 8 \ 4 \rangle)$ | $(\langle 5 \ 8 \ 9 \rangle)$ |
| $(\langle 6 \ 8 \ 10 \rangle)$ | $(\langle 5 \ 8 \ 7 \rangle)$ | $(\langle 6 \ 8 \ 9 \rangle)$ | $(\langle 7 \ 9 \ 10 \rangle)$ |
| $(\langle 4 \ 6 \ 7 \rangle)$ | $(\langle 5 \ 6 \ 10 \rangle)$ | $(\langle 3 \ 4 \ 9 \rangle)$ | $(\langle 4 \ 5 \ 10 \rangle)$ |
| $(\langle 4 \ 5 \ 9 \rangle)$ | $(\langle 3 \ 5 \ 9 \rangle)$ | $(\langle 4 \ 6 \ 10 \rangle)$ | $(\langle 3 \ 8 \ 10 \rangle)$ |
| $(\langle 5 \ 7 \ 10 \rangle)$ | $(\langle 3 \ 6 \ 7 \rangle)$ | $(\langle 3 \ 7 \ 10 \rangle)$ | $(\langle 1 \ 2 \ 10 \rangle)$ |
| * $\langle 6 \ 1 \ 9 \rangle$ | * $\langle 6 \ 1 \ 8 \rangle$ | * $\langle 6 \ 7 \ 1 \rangle$ | * $\langle 8 \ 1 \ 4 \rangle$ |
| * $\langle 8 \ 1 \ 5 \rangle$ | * $\langle 7 \ 1 \ 9 \rangle$ | * $\langle 10 \ 1 \ 9 \rangle$ | * $\langle 9 \ 1 \ 3 \rangle$ |
| * $\langle 10 \ 2 \ 9 \rangle$ | * $\langle 7 \ 2 \ 10 \rangle$ | * $\langle 10 \ 2 \ 8 \rangle$ | * $\langle 9 \ 2 \ 4 \rangle$ |
| * $\langle 10 \ 1 \ 4 \rangle$ | * $\langle 3 \ 1 \ 10 \rangle$ | * $\langle 3 \ 1 \ 8 \rangle$ | * $\langle 5 \ 1 \ 7 \rangle$ |
| * $\langle 8 \ 2 \ 4 \rangle$ | * $\langle 3 \ 2 \ 8 \rangle$ | * $\langle 3 \ 2 \ 6 \rangle$ | * $\langle 5 \ 2 \ 3 \rangle$ |
| * $\langle 2 \ 5 \ 6 \rangle$ | * $\langle 6 \ 2 \ 9 \rangle$ | * $\langle 7 \ 2 \ 9 \rangle$ | * $\langle 8 \ 2 \ 7 \rangle$ |
| $\langle 9 \ 1 \ 10 \rangle$ | $\langle 9 \ 1 \ 6 \rangle$ | $\langle 9 \ 1 \ 7 \rangle$ | $\langle 4 \ 1 \ 9 \rangle$ |
| $\langle 4 \ 1 \ 8 \rangle$ | $\langle 1 \ 7 \ 10 \rangle$ | $\langle 6 \ 1 \ 3 \rangle$ | $\langle 7 \ 1 \ 8 \rangle$ |
| $\langle 5 \ 1 \ 6 \rangle$ | $\langle 8 \ 1 \ 3 \rangle$ | $\langle 8 \ 1 \ 10 \rangle$ | $\langle 3 \ 1 \ 5 \rangle$ |
| $\langle 4 \ 2 \ 10 \rangle$ | $\langle 9 \ 2 \ 7 \rangle$ | $\langle 8 \ 2 \ 3 \rangle$ | $\langle 3 \ 2 \ 9 \rangle$ |
| $\langle 5 \ 2 \ 8 \rangle$ | $\langle 8 \ 2 \ 6 \rangle$ | $\langle 9 \ 2 \ 10 \rangle$ | $\langle 7 \ 2 \ 5 \rangle$ |
| $\langle 2 \ 6 \ 9 \rangle$ | $\langle 10 \ 2 \ 3 \rangle$ | $\langle 6 \ 2 \ 7 \rangle$ | $\langle 4 \ 2 \ 8 \rangle$ |
| <hr/> | <hr/> | <hr/> | <hr/> |
| (Q_3, x) | (Q_4, x) | (Q_5, x) | (Q_6, x) |

| | | | |
|--------------------------------|--------------------------------|--------------------------------|-------------------------------|
| $\langle 1 \ 2 \ 3 \rangle$ | $\langle 1 \ 2 \ 9 \rangle$ | $\langle 1 \ 2 \ 8 \rangle$ | $\langle 1 \ 2 \ 6 \rangle$ |
| $\langle 4 \ 5 \ 8 \rangle$ | $\langle 3 \ 7 \ 9 \rangle$ | $\langle 4 \ 8 \ 10 \rangle$ | $\langle 3 \ 6 \ 8 \rangle$ |
| $\langle 3 \ 4 \ 6 \rangle$ | $\langle 3 \ 6 \ 10 \rangle$ | $\langle 6 \ 7 \ 10 \rangle$ | $\langle 4 \ 5 \ 6 \rangle$ |
| $\langle 6 \ 9 \ 10 \rangle$ | $\langle 4 \ 9 \ 10 \rangle$ | $\langle 5 \ 6 \ 8 \rangle$ | $\langle 4 \ 8 \ 9 \rangle$ |
| $\langle 8 \ 9 \ 3 \rangle$ | $\langle 5 \ 6 \ 9 \rangle$ | $\langle 3 \ 4 \ 5 \rangle$ | $\langle 6 \ 7 \ 9 \rangle$ |
| $\langle 3 \ 5 \ 10 \rangle$ | $\langle 4 \ 5 \ 7 \rangle$ | $\langle 7 \ 8 \ 3 \rangle$ | $\langle 3 \ 5 \ 7 \rangle$ |
| * $\langle 9 \ 1 \ 4 \rangle$ | * $\langle 7 \ 1 \ 10 \rangle$ | * $\langle 3 \ 1 \ 6 \rangle$ | * $\langle 8 \ 1 \ 7 \rangle$ |
| * $\langle 6 \ 1 \ 5 \rangle$ | * $\langle 4 \ 1 \ 6 \rangle$ | * $\langle 4 \ 1 \ 7 \rangle$ | * $\langle 4 \ 1 \ 3 \rangle$ |
| * $\langle 10 \ 1 \ 8 \rangle$ | * $\langle 5 \ 1 \ 3 \rangle$ | * $\langle 5 \ 1 \ 10 \rangle$ | * $\langle 9 \ 1 \ 5 \rangle$ |
| * $\langle 9 \ 2 \ 5 \rangle$ | * $\langle 7 \ 2 \ 6 \rangle$ | * $\langle 5 \ 2 \ 7 \rangle$ | * $\langle 4 \ 2 \ 7 \rangle$ |
| * $\langle 10 \ 2 \ 4 \rangle$ | * $\langle 4 \ 2 \ 3 \rangle$ | * $\langle 4 \ 2 \ 6 \rangle$ | * $\langle 9 \ 2 \ 3 \rangle$ |
| * $\langle 6 \ 2 \ 8 \rangle$ | * $\langle 5 \ 2 \ 10 \rangle$ | * $\langle 3 \ 2 \ 10 \rangle$ | * $\langle 8 \ 2 \ 5 \rangle$ |
| $\langle 4 \ 1 \ 10 \rangle$ | $\langle 6 \ 1 \ 7 \rangle$ | $\langle 6 \ 1 \ 4 \rangle$ | $\langle 7 \ 1 \ 4 \rangle$ |
| $\langle 8 \ 1 \ 6 \rangle$ | $\langle 3 \ 1 \ 4 \rangle$ | $\langle 10 \ 1 \ 3 \rangle$ | $\langle 3 \ 1 \ 9 \rangle$ |
| $\langle 5 \ 1 \ 9 \rangle$ | $\langle 10 \ 1 \ 5 \rangle$ | $\langle 7 \ 1 \ 5 \rangle$ | $\langle 5 \ 1 \ 8 \rangle$ |
| $\langle 4 \ 2 \ 9 \rangle$ | $\langle 10 \ 2 \ 7 \rangle$ | $\langle 6 \ 2 \ 3 \rangle$ | $\langle 7 \ 2 \ 8 \rangle$ |
| $\langle 5 \ 2 \ 6 \rangle$ | $\langle 6 \ 2 \ 4 \rangle$ | $\langle 7 \ 2 \ 4 \rangle$ | $\langle 3 \ 2 \ 4 \rangle$ |
| $\langle 8 \ 2 \ 10 \rangle$ | $\langle 3 \ 2 \ 5 \rangle$ | $\langle 10 \ 2 \ 5 \rangle$ | $\langle 5 \ 2 \ 9 \rangle$ |
| <hr/> | <hr/> | <hr/> | <hr/> |
| (Q_7, x) | (Q_8, x) | (Q_9, x) | (Q_{10}, x) |

(2) Proof that (Q, \langle, \rangle) is a Quasigroup:

(a) One can see that (Q_1, x) and (Q_2, x) are quasi-groups by inspection and that no triple appears in both Q_1 and Q_2 . Also among the 6 triples of (Q_i, x) , $i \geq 3$ which

were in the original definition of (Q_i, \circ) , there is clearly no conflict. (These are the circled triples.)

(b) Among the 6 triples of (Q_i, x) coming from applying law 12 to (Q_1, x) , there could not be any conflict, as there was none in (Q_1, x) . More precisely, if $\langle 1, y, z \rangle' = \langle 1, y, t \rangle' = m$, we had $\langle z, \langle m, z, y \rangle', y \rangle' = m = \langle t, \langle m, t, y \rangle', y \rangle'$, where $\langle m, z, y \rangle' = \langle m, t, y \rangle' = 1$ in (Q_1, x) and so $z = t$. Similarly, among the six triples containing 2 and coming from (Q_2, x) , there will be no conflict.

(c) Could there be any conflict between the 2 groups discussed in (b)? That is, could $\langle 2, y, z \rangle' = \langle 1, y, z \rangle' = m$, where y and z are different from 1 and 2? But then, $\langle m, z, y \rangle' = 1$ and $\langle m, z, y \rangle' = 2$, which is impossible.

(d) Now the 6 circled triples of (Q_i, x) , which were originally in the definition of (Q_i, \circ) , did not conflict in any cyclic order with the other 6 triples of (Q_i, \circ) . However, 6 of the 12 triples considered in (b) (the *'d triples), are exactly those other 6 triples of (Q_i, \circ) , restricted to cyclic orders. Therefore, there can be no conflict between these sets of triples.

(e) Suppose, however, that a conflict occurred between the 6 triples which were not obtained from triples originally in (Q_1, \circ) or (Q_2, \circ) (the unmarked triples) and the circled triples. That is, suppose $\langle m, x, y \rangle' \in (Q_1, x)$,

where $\langle m, x, y \rangle \in (Q_2, \circ)$. Now we would have $\langle m, x, y \rangle' = 1$ and $\langle m, y, x \rangle = 2$, only in the 3 cyclic orders. Could $\langle x, 1, y \rangle' = \langle x, r, y \rangle' = m$, where x and y are different from 1 and 2? But $\langle m, y, x \rangle = 2$ implies $\langle y, 2, x \rangle = m$ in (Q_m, \circ) originally. Therefore $\langle x, r, y \rangle$ and $\langle x, 2, y \rangle$ were both triples of (Q_m, \circ) and so $r = 2$. But then $\langle x, 2, y \rangle' = \langle x, 1, y \rangle' = m$, which was ruled out in part (c).

Could $\langle x, 1, y \rangle' = \langle x, 1, z \rangle' = m$? If $\langle x, 1, z \rangle'$ is a circled triple and $\langle x, 1, y \rangle'$ is unmarked, then z must be 2. Thus $\langle x, 1, y \rangle' = \langle x, 1, 2 \rangle' = m$. But then in the original quadruple system, $\langle m, y, x \rangle = 2$ and so $\langle y, 2, x \rangle = m$ and $\langle 1, 2, x \rangle = m$ in (Q_m, \circ) . Therefore $y = 1$, a contradiction.

(f) Thus each (Q_i, x) is a quasigroup, $i = 1, 2, \dots, 10$. No triples of (Q, \langle, \rangle) have been omitted in (Q, \langle, \rangle') and no one triple appears in two different quasigroups (Q_i, x) . For suppose an unmarked triple $\langle x, y, z \rangle'$ appeared in (Q_i, x) and (Q_j, x) , where $i \neq j$, $i, j \geq 3$. Without loss of generality, suppose $y=1$, $x \neq z \neq 2$. Then (Q_2, \circ) must have contained the triples $\langle i, z, y \rangle$ and $\langle j, z, y \rangle$ and so $i = j$. Therefore (Q, \langle, \rangle') is a quasigroup.

(3) Proof that L_{12} is satisfied:

Clearly L_{12} is satisfied when triples involving elements from Q_1 to Q_i , $i \geq 2$, or Q_2 to Q_i , $i \geq 2$ are

considered. Also, if only triples which were in the original definition of (Q, \langle, \rangle) are involved, L_{12} must be satisfied.

Now the only interaction between Q_1 and Q_2 involving L_{12} concerns the triples of Q_1 and Q_2 containing a 1 or 2, which remain unchanged from their original definition.

Consider then Q_x and Q_r and an unmarked triple $\langle x, 1, z \rangle' = r$ where $x, z, r \geq 3$ where $\langle r, x, z \rangle' = 1$, and originally $\langle r, x, z \rangle = 2$ in (Q_2, \circ) . Then $\langle 1, \langle x, 1, z \rangle', z \rangle' = \langle 1, r, z \rangle'$. Now $\langle r, x, z \rangle' = 1$. Therefore $\langle x, z, r \rangle' = 1$ and $\langle z, \langle x, z, r \rangle', r \rangle' = \langle z, 1, r \rangle' = x$. But $\langle z, 1, r \rangle' = \langle 1, r, z \rangle'$ and so $\langle 1, \langle x, 1, z \rangle', z \rangle' = x$.

Finally suppose $\langle 1, 2, q \rangle' = r$ in (Q_r, x) , where $r, q \geq 3$. Then we must show $\langle 2, \langle 1, 2, q \rangle', q \rangle' = 1$ or $\langle 2, r, q \rangle' = 1$. Suppose to the contrary that $\langle 2, r, q \rangle' = p$. Then $\langle p, q, r \rangle' = 2$ in (Q_2, x) . But if $\langle 1, 2, q \rangle' = r$, then $\langle 1, 2, q \rangle$ was an original triple of Q_r and so $\langle q, r, 1 \rangle' = 2$ in all cyclic orders. But (Q_2, x) is a quasigroup. Therefore $p = 1$.

L_{12} is therefore satisfied and (Q, \langle, \rangle') has exactly 2 conjugacy classes.

§4.4 Conclusion.

From the proof of Theorems 4.3.3 and 4.3.4, one can see that as long as the triples of some (Q_i, \circ) and (Q_j, \circ) , $i \neq j$, can be split to form (Q_i, x) and (Q_j, x) as disjoint quasigroups, then ternary quasigroups with 2 or 8 conjugacy classes may be constructed. However, many attempts were made to carry out a similar splitting process on quadruple systems of order 14, with no success. For $n = 8, 10$, there is only one isomorphism class of quadruple systems, but for $n = 14$, there are 4 and every type was tried. At present, no further attempt has been made to generalize this construction.

However, from the examples given so far, certain infinite classes of 3-quasigroups with 2 or 8 conjugacy classes may be obtained.

4.4.5 Main Theorem. There exists a ternary quasigroup of order n having exactly 2 or 8 conjugacy classes for every $n \geq 5$ such that one of the following holds:

- (1) $n \equiv 0$ or $5 \pmod{10}$
- (2) $n \equiv 0 \pmod{8}$
- (3) $n \equiv 4, 8$ or $10 \pmod{12}$.

If $n < 5$, there does not exist any ternary quasigroup of order n with 2 or 8 conjugacy classes.

Proof: From Theorem 3.7.1, one obtains (1) and (2). Using a similar method of replacing a subsystem with one having the required number of conjugates, one obtains $n \equiv 4$ or $8 \pmod{12}$ from Theorem 1.3.11. Using $n \equiv 4 \pmod{12}$ in Theorem 1.3.12, one obtains the case $n \equiv 10 \pmod{12}$. We remark in conclusion that no further results can be obtained from Theorem 1.3.12.

CHAPTER 5

The Existence of an n-ary Quasigroup with a Specified Number of Conjugacy Classes

§5.1 Conjugacy Classes of size $\frac{(n+1)!}{q!}$
where $q = 1, 2, \dots, n+1$

Theorem 5.1.1. There exists an n-ary quasigroup with exactly one conjugacy class for all orders $m \geq 1$.

Proof: Let $Q = \{0, \dots, m-1\}$ and define an n-ary operation $\langle \rangle$ on Q by $\langle a_1, \dots, a_n \rangle = -(a_1 + a_2 + \dots + a_n) \equiv d = a_{n+1} \pmod{m}$ where $a_i, i = 1, \dots, n \in Q$ and $d \in Q$. Then clearly $(Q, \langle \rangle)$ is an n-ary quasigroup. Clearly $\langle \rangle_\pi = \langle \rangle$, if $\pi(n+1) = n+1$, where $\pi \in S_{n+1}$. However if we consider some permutation π where $\pi(n+1) \neq n+1$ and π acts on $\{1, \dots, n+1\}$, then $\langle a_{\pi(1)}, \dots, a_{\pi(j-1)}, d, a_{\pi(j+1)}, \dots, a_{\pi(n)} \rangle = -(a_{\pi(1)} + a_{\pi(2)} + \dots + a_{\pi(j-1)} + (a_1 + a_2 + \dots + a_n) + a_{\pi(j+1)} + \dots + \pi(a_n)) = a_{\pi(j)}$.

Remark 5.1.2. In the following cases, it is very difficult to determine for which small orders the quasigroups exist and, for the most part, no attempt has been made to do this. For an arbitrary n , an exact enumeration of the members of all the subgroups of S_{n+1} is not feasible, and so the types of proofs used in Chapter 2 are no longer possible.

Although some of these theorems seems to include the ternary case, at least for large enough orders, in fact $n=3$ proves to be an exception in Theorem 5.2.1.

For these reasons, this Chapter is given at the end, rather than at the beginning of this thesis. An attempt to obtain "complete" results concerning these cases has not been made as the thesis emphasis is on the ternary case. Instead, a number of "straightforward conjugacy classes" are discussed in this section and a couple of variations in the next, in order to indicate the possibilities for a more detailed investigation.

Lemma 5.1.3. Let $\phi(n)$ be the Euler function, i.e. $\phi(n)$ is the number of integers relatively prime to n and not exceeding n . Then $\phi(n) \geq \sqrt{n}$, except when $n = 2$ or 6 .

Proof: From [16], we have the relationship

$$\phi(n) = \prod_{p^\alpha/n} p^{\alpha-1} (p-1). \text{ Now } p^{\alpha-1} (p-1) \geq p^{\alpha/2}, \text{ if}$$

$(\alpha-1) \geq \alpha/2$, i.e. $\alpha \geq 2$. Therefore consider the case when $\alpha = 1$. Then we need $p-1 \geq p^{1/2}$ or $\sqrt{p}(\sqrt{p}-1) \geq 1$, which is true if $p \geq 3$. Thus the only difficulty occurs if n has a unique factor of 2. That is $n = 2p_1 p_2 \dots p_r$ and $\phi(n) = (p_1-1)(p_2-1)\dots(p_r-1)$. But $p-1 \geq \sqrt{2p}$, or $p^2+1 \geq 4p$ if $p \geq 5$. Thus only if $n=2$ or $n=6$ is $\phi(n) \leq \sqrt{n}$.

Theorem 5.1.4. If $m > 4(n-1)^2$ then there exists an n -ary

quasigroup of order m with $(n+1)!$ conjugacy classes.

Proof: Let (Q, \langle, \rangle) be an n -ary quasigroup of order m with $Q = \{0, 1, \dots, m-1\}$; where $\langle a_1, a_2, \dots, a_n \rangle = d \equiv a_1 + a_2 p_2 + \dots + a_n p_n \pmod{m}$; where all the p_i are relatively prime to m ; and where $p_i + p_j \not\equiv 0 \pmod{m}$, $(i \neq j)$, $p_i \neq p_j$, and $p_i \neq n-1, \forall i$. Then (Q, \langle, \rangle) has $(n+1)!$ conjugacy classes.

To show this consider the following cases:

(1) Clearly any single transposition among the integers 1 to n alters the value of $\langle a_1, \dots, a_n \rangle$. (See Chapter 3.)

(2) Consider any permutation of $\{1, 2, \dots, n+1\}$, which leaves $n+1$ fixed. Then suppose $\pi = (i_1, j_1) (i_2, j_2) \dots$

(i_{n-1}, j_{n-1}) , when written as a product of transposition.

Suppose that $i_1 \neq j_1$. Let $a_{i_1} \neq a_{j_1} \neq 0$ and the remaining a_{i_k}, a_{j_k} all be 0. Then we have a contradiction from case 1 again.

(3) Suppose $\pi(n+1) = s$, $s \neq 1$ and $\pi(s) = n+1$, where every other element is left unchanged by π . Then we have

$\langle a_1, \dots, a_n \rangle = d$ and suppose $\langle a_1, \dots, a_{s-1}, d, a_{s+1}, \dots, a_n \rangle \equiv$

$$a_1 + \sum_{\substack{i \neq s \\ i > 2}}^n p_i a_i + p_s (a_1 + \sum_2^n a_i p_i) = a_s. \quad \text{If } a_i = 0, \forall i,$$

$i \neq s$, then $p_s^2 a_s \equiv a_s \Rightarrow p_s^2 \equiv 1 \pmod{m}$. But then

$$a_1 (1+p_s) + \sum_{i=2}^n a_i (1+p_s) \equiv 0 \pmod{m}. \quad \text{If } a_i = 0 \forall i \geq 2,$$

then $1+p_s$ must be $\equiv 0 \pmod{m}$, which is false.

(4) Suppose $\pi(n+1) = 1$ and $\pi(1) = n+1$, and every other element is left fixed by π . Suppose $\langle a_1, \dots, a_n \rangle = d$ and $\langle d, a_2, \dots, a_n \rangle = a_1$. Then $(a_1 + \sum_{i=2}^n p_i a_i) + \sum_{i=2}^n p_i a_i = a_1$ and $2 \sum_{i=2}^n a_i p_i \equiv 0 \pmod{m}$. Letting $a_2 = 1$ and all other $a_i = 0$, one obtains $2p_2 \equiv 0 \pmod{m}$, a contradiction.

(5) Suppose $n+1$ and 1 are interchanged under π and the remaining a_i are permuted by at least one transposition. Then $\langle a_1, \dots, a_n \rangle = d$ and $\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_1$. Thus $a_1 + \sum_{i=2}^n p_i a_i + \sum_{i=2}^n p_i a_{\pi(i)} \equiv a_1 \pmod{m}$, where at least one $a_{\pi(i)} \neq a_i$. Suppose in fact $\pi(i) \neq i$ for some fixed i . Then there exists a j such that $\pi(j) = i$. Let $a_k = 0$ for all $k \neq 1$ or i . We have $(p_i + p_j) \equiv 0 \pmod{m}$, a contradiction.

(6) Suppose $n+1$ and 2 (or any $i, i \neq 1$) are interchanged under π and the remaining elements are permuted by at least one transposition. Then $\langle a_1, \dots, a_n \rangle = d$ and, say, $\langle a_{\pi(1)}, d, \dots, a_{\pi(n)} \rangle = a_2$. Thus $a_{\pi(1)} + p_2(a_1 + \sum_{i=2}^n a_i p_i) + \sum_{i=3}^n a_{\pi(i)} p_i \equiv a_2 \pmod{m}$. From this, we may conclude that $p_2^2 \equiv 1 \pmod{m}$, and $a_1(p_2 + p_s) + a_{\pi(1)}(1 + p_2 p_{\pi(1)}) + \sum_{i=3}^n a_{\pi(i)}(p_2 p_{\pi(i)} + p_i) \equiv 0 \pmod{m}$ where $\pi(s) = 1$ for some $s \neq 1$. Choose $a_i = 0$, $\forall a_i$ except a_1 and a_2 ;

let $a_1 = 1$. Then $p_2 + p_s \equiv 0 \pmod{m}$, a contradiction.

If, however, $\pi(1) = 1$, $a_1(1+p_2) + \sum_3^n a_{\pi(i)}(p_2 p_{\pi(i)} + p_i) \equiv 0 \pmod{m}$. If all $a_i \equiv 0$, $i \geq 3$, then $1 + p_2 \equiv 0$, a contradiction.

(7) Suppose $a_{\pi(1)} = d$, but $\pi(n+1) \neq 1$. Say $\langle a_1, \dots, a_n \rangle = d$, but $\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_{\pi(n+1)}$ where $a_{\pi(n+1)} \neq a_1$. Then $a_1 + \sum_{i=2}^n a_i p_i + \sum_{i=2}^n a_{\pi(i)} p_i = a_{\pi(n+1)}$. If $a_1 = 1$ and all the other $a_i = 0$, then $a_1(1+p_{\pi(j)}) \equiv 0 \pmod{m}$, where $\pi(j) = 1$, and this is impossible.

(8) Finally, suppose $\pi(i) = n+1$ for some $i \neq 1$ (w.l.g. $i = 2$) and $\pi(n+1) \neq 2$. Then we make the following three considerations.

Suppose $\pi(n+1) = 1$. Then $\langle a_1 \dots a_n \rangle = d$ and $\langle a_{\pi(1)}, d, \dots, a_{\pi(n)} \rangle = a_1$ or $a_{\pi(1)} + p_2 a_1 + p_2 \sum_{i=2}^n a_i p_i + \sum_{i=3}^n a_{\pi(i)} p_i \equiv a_1 \pmod{m}$. But this implies $p_2 = 1$, a contradiction.

Suppose $\pi(1) = 1$. Then $a_1 + (a_1 + \sum_2^n a_i p_i) p_2 + \sum_3^n a_{\pi(i)} p_i \equiv a_{\pi(n+1)} \pmod{m}$, which implies $1 + p_2 \equiv 0 \pmod{m}$, a contradiction.

Suppose $\pi(j) = 1$, $j \neq 1$. Then $a_{\pi(1)} + p_2(a_1 + \sum_2^n a_i p_i) + p_j a_j + \sum_{\substack{i=3 \\ i \neq j}}^n a_{\pi(i)} p_i \equiv a_{\pi(n+1)}$. But this

leads to $p_2 + p_j \equiv 0 \pmod{m}$, a contradiction.

To complete the proof of the theorem, we need only show that one can choose $n-1$ numbers p_i , which are relatively prime to m and not pairwise summable to m or equal to $m-1$. Now if each p_i is less than $\frac{m}{2}$ and is relatively prime to m , this will be the case. Thus if we can make $\frac{\phi(m)}{2} > n-1$, $n-1$ such numbers can be found. By Lemma 5.1.3, if $m \neq 2$ or 6 , $\phi(m) \geq \sqrt{m}$. So if $\frac{\sqrt{m}}{2} > n-1$, which is true if $m > 4(n-1)^2$, we are done. (As $m \geq 16$, if $n \geq 3$, we are not considering $m = 2$ or 6 .)

Theorem 5.1.5. There exists an integer $m_j(n)$ such that for every order $m \geq m_j(n)$ there exists an n -ary quasigroup of order m with $\frac{(n+1)!}{j!}$ conjugacy classes, $j = 1, \dots, n$.

Proof: (1) We have just seen the case $j = 1$. Consider every case other than $j = 1$ or n . Define (Q, \langle, \rangle) , where $Q = \{0, 1, \dots, m-1\}$ by $\langle a_1, \dots, a_n \rangle = a_1 + a_2 + \dots + a_j + p_{j+1}a_{j+1} + \dots + p_n a_n$ where addition is taken \pmod{m} . Here p_{j+1}, \dots, p_n are integers relatively prime to m , are not pairwise summable to m , and are all different from $m-1$ or 1 . Then every permutation π on $\{1, \dots, n+1\}$, which fixes the elements $1, \dots, j$, $j \leq n$, will leave the product $\langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle$ unchanged and thus not introduce a new conjugacy class. We must show that any other type of permutation π on $\{1, \dots, n+1\}$ results in $\langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle \neq a_{\pi(n+1)}$.

Consider the case where π fixes $n+1$ and $a_{\pi(i)} = a_\ell$ for some $i > j$ and $\ell \leq j$. Then we have $\sum_{i=1}^j a_{\pi(i)} + \sum_{i=j+1}^n p_i a_{\pi(i)} = \sum_{i=1}^j a_i + \sum_{i=j+1}^n p_i a_i$. Let $a_\ell = 1$ and the rest of the a_i be $=0$. Then $p_i = 1$. Suppose $\pi(i) = \pi(\ell)$, where i and $\ell > j$. Let $a_\ell = 1$ and the remaining a_i 's all be zero. Then $p_i a_\ell = p_\ell a_\ell$ implies $p_i = p_\ell$, a contradiction.

If $a_{\pi(i)} = d$ and $a_{\pi(n+1)} = a_i$ for any $i \leq j$, and π fixes all the other i , we have:

$$a_1 + a_2 + \dots + a_{i-1} + \left(\sum_{i=1}^j a_i + \sum_{i=j+1}^n p_i a_i \right) + a_{i+1} + \dots + a_j + \sum_{i=j+1}^n p_i a_i$$

$= a_i$. If all $a_k = 0$ except $a_{j+1} = 1$, we have $2p_{j+2} \equiv 0 \pmod{m}$, a contradiction.

If $a_{\pi(n+1)} = a_i$ and $a_{\pi(i)} = d$, where $i > j$, and π fixes every other element, we obtain a contradiction similar to that in (3) of Theorem 5.1.4.

If $a_{\pi(n+1)} = a_i$, $i \leq j$, $a_{\pi(i)} = d$, we obtain a contradiction similar to Theorem 5.1.4, (5).

If $a_{\pi(n+1)} = a_j$ and $a_{\pi(j)} = d$, where $i > j$, we obtain a contradiction similar to Theorem 5.1.4, (6).

Now if $a_{\pi(i)} = d$, where $i \leq j$, but $a_{\pi(n+1)} \neq a_i$, we obtain: $\langle a_{\pi(1)}, \dots, d, \dots, a_{\pi(n)} \rangle = a_{\pi(n+1)}$, and so

$$a_{\pi(1)} + \dots + a_{\pi(i-1)} + \left(\sum_{i=1}^j a_i + \sum_{i=j+1}^n p_i a_i \right) + a_{\pi(i+1)} + \dots + a_{\pi(j)} + \sum_{i=j+1}^n p_i a_{\pi(i)} = a_{\pi(n+1)}.$$

If $a_{\pi(n+1)} = a_k$, where $k \leq j$, let all the a_ℓ 's be zero except one a_t and possibly a_k , where $t \leq j$, $t \neq i$. Then either $a_t(1+p_s) \equiv 0 \pmod{m}$ for some s or $2a_t \equiv 0 \pmod{m}$; in either case we get a contradiction for $m > 2$.

If $a_{\pi(n+1)} \neq a_i$, $i > j$, but $a_{\pi(i)} = d$, then

$$\sum_{i=1}^j a_{\pi(i)} + p_i \left(\sum_{i=1}^j a_i + \sum_{i=j+1}^n p_i a_i \right) + \sum_{\substack{s=j+1 \\ s \neq i}} p_s a_{\pi(s)} \equiv a_{\pi(n+1)},$$

if $\langle \rangle_\pi = \langle \rangle$.

Then if $a_\ell \neq 0$, $\forall \ell$ except k , where $a_k = a_{\pi(n+1)}$, we obtain either $p_k^2 a_k \equiv a_k \pmod{m}$ or $p_i a_k \equiv a_k \pmod{m}$.

The latter case is impossible, and in the former, we cancel $p_k^2 a_k$ and a_k from the equation. In the resulting equation, let $a_1 = 1$ and the remaining a_ℓ 's be all zero. Then if $1 = \pi(k)$, where $k \leq j$, $a_1 + p_i a_1 \equiv 0$ or $(1+p_i) \equiv 0 \pmod{m}$. If $\pi(k) > j$, $p_i a_1 + p_k(a_1) \equiv 0 \pmod{m}$ implies $(p_i + p_k) \equiv 0 \pmod{m}$. Both these are impossible, and so the theorem is proven for $j < n$.

(2) If $j = n$, we define $\langle a_1, \dots, a_n \rangle = a_1 + a_2 + \dots + a_n$. Clearly there are $n!$ members of one class. Consider the two following possibilities: $\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_1$ or

$\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_{\pi(n+1)} \neq a_1$, say $a_{\pi(n+1)} = a_k$. In the first case $\sum_{i=1}^n a_i + \sum_{i=2}^n a_{\pi(i)} \equiv a_1$ and so $2(\sum_{i=2}^n a_i) \equiv 0$, a contradiction. In the second case, $\sum_{i=1}^n a_i + \sum_{i=2}^n a_{\pi(i)} \equiv a_k$, or $(\sum_{i=1, i \neq k}^n a_i + \sum_{i=2}^n a_{\pi(i)}) \equiv 0$ and hence $2(\sum_{i=1, i \neq k}^n a_i) \equiv 0$, a contradiction. Therefore, there are exactly $n+1$ classes.

(3) As in Theorem 5.1.4, Lemma 5.1.3 may be used to determine $m_j(n)$, depending on the number of relatively prime numbers required.

§5.2 The Cases of $\frac{n(n+1)}{2}$ and $\frac{(n+1)!}{(\frac{n}{2})! (\frac{n+2}{2})!}$, n even, Conjugacy Classes.

Theorem 5.2.1. There exists an integer $m(n) \geq 3$ such that for every $m \geq m(n)$, there exists an n -ary quasigroup ($n > 3$) of order m with exactly $\frac{n(n+1)}{2}$ conjugacy classes.

Proof: Define (Q, \langle, \rangle) , where $Q = \{0, 1, \dots, m-1\}$, by $\langle a_1, \dots, a_n \rangle = d = -a_1 + a_2 + \dots + a_n$ and addition is taken (mod m), $a_i, i = 1, \dots, n, d \in Q$. If π is any permutation on $\{1, 2, \dots, n+1\}$ which fixes 1 and $n+1$, then $\langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle = a_{\pi(n+1)}$. Therefore, the conjugate 3-quasigroup $(Q, \langle, \rangle_{\pi})$ defined by $\langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle_{\pi} = a_{\pi(n+1)}$ if and only if $\langle a_1, \dots, a_n \rangle = d = a_{n+1}$ is identical with (Q, \langle, \rangle) . There are $(n-1)!$ such permutations and

therefore at least $(n-1)!$ members of one conjugacy class.

Suppose π is a permutation on $\{1, 2, \dots, n+1\}$ such that $a_{\pi(1)} = d$ and $a_{\pi(n+1)} = a_1$. Then $\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_1$ only if
$$-(-a_1 + \sum_{i=2}^n a_i) + \sum_{i=2}^n a_{\pi(i)} \equiv a_1 \pmod{m}.$$

Therefore the 3-quasigroup $(Q, \langle \cdot, \cdot, \cdot \rangle_{\pi}) = (Q, \langle \cdot, \cdot, \cdot \rangle)$. There are another $(n-1)!$ permutations of this type. Therefore, there are at least $2(n-1)!$ members of the conjugacy class identical with Q .

However, if $\langle a_1, d, a_{\pi(3)}, \dots, a_{\pi(n)} \rangle = a_2$, that is $\pi(2) = n+1$, $\pi(n+1) = 2$, $\pi(1) = 1$, then

$$-a_1 - a_1 + \sum_{i=2}^n a_i + \sum_{i=3}^n a_{\pi(i)} \equiv a_2 \pmod{m}.$$

This becomes

$$-2a_1 + 2 \sum_{i=3}^n a_i \equiv 0 \pmod{m},$$

a contradiction if $m \geq 3$.

Consider the case where $\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_{\pi(n+1)} = a_k$, $k \neq 1$. Then
$$a_1 - \sum_{i=2}^n a_i + \sum_{i=2}^n a_{\pi(i)} \equiv a_k \pmod{m}$$
 and $2(a_1 - a_k) \equiv 0 \pmod{m}$, again a contradiction.

If $\langle a_{\pi(1)}, d, a_{\pi(3)}, \dots, a_{\pi(n)} \rangle = a_{\pi(n+1)} = a_k$, $k \neq 2$, then
$$-a_{\pi(1)} - a_1 + \sum_{i=2}^n a_i + \sum_{i=3}^n a_{\pi(i)} \equiv a_k \pmod{m}.$$
 If $n=3$, there is one case in which this is indeed true. Namely, if $\langle a_2, d, a_1 \rangle = a_3$, $-a_2 - a_1 + a_2 + a_3 + a_1$ equals a_3 . However, if $n > 3$ and $m(n) > 3$, then
$$-a_{\pi(1)} - a_1 + \sum_{i=2}^n a_i + \sum_{i=3}^n a_{\pi(i)} \equiv 0 \pmod{m},$$
 and there remains at least one variable, with a

coefficient ≤ 2 , that will not cancel out on the left hand side. Hence the congruence will not always be identically zero.

Therefore, there are $2(n-1)!$ members of one conjugacy class and every other class contains exactly one conjugate 3-quasigroup. Therefore (Q, \langle, \rangle) has $\frac{(n+1)!}{2(n-1)!} = \frac{n(n+1)}{2}$ conjugacy classes.

Values of m which are close to n must be considered separately to find the exact value of $m(n)$ in every case.

Theorem 5.2.2. There exists an integer $m(n)$ such that for every $m \geq m(n)$, there exists an n -ary quasigroup (n even) of order m with exactly $\frac{(n+1)!}{[(\frac{n}{2})!]^2 (\frac{n+2}{2})}$ conjugacy classes.

Proof: On the set $\{0, 1, \dots, m-1\}$ define (Q, \langle, \rangle) so that $\langle a_1, a_2, \dots, a_n \rangle = d + (a_1 - a_2 + a_3 - a_4 + \dots - a_n) \pmod{m}$. Clearly any positive positions may be permuted among themselves (and similarly for the negative ones) without altering d . This gives rise to $[(\frac{n}{2})!]^2$ members of one conjugacy class.

Suppose $a_{\pi(n+1)} = a_t$, where t is even and $a_{\pi(r)} = d$, where r is even. Also suppose the remaining elements are permuted according to $\pi(2i) = 2j$ and $\pi(2i-1) = 2k-1$, that is, like signs are retained. Then $a_{\pi(1)} - a_{\pi(2)} + \dots + a_{\pi(r-1)} - d + a_{\pi(r+1)} + \dots - a_{\pi(n)} \equiv a_t \pmod{m}$, or $a_{\pi(1)} - a_{\pi(2)} + \dots + a_{\pi(r-1)} - (a_1 - a_2 + \dots + a_{t-1} - a_t + a_{t+1} \dots - a_n) + a_{\pi(r+1)} + \dots - a_{\pi(n)} = a_t$, as all the other

terms cancel out in pairs. In other words, if d is in any negative position, with any element from a negative position replacing d , and provided the other elements are permuted in a sign preserving way, the identity arising from the permutation holds.

Now d can appear in $\frac{n}{2}$ places, and the elements in odd positions may be arranged among themselves in $(\frac{n}{2})!$ ways. There are $\frac{n}{2}$ choices for $\pi(d)$ and the remaining elements in even positions may be arranged in $(\frac{n}{2} - 1)!$ ways. Thus we have a total of $[(\frac{n}{2})!]^2 (\frac{n}{2})$ possibilities. Adding the $[(\frac{n}{2})!]^2$ possibilities with $n+1$ fixed, gives $[(\frac{n}{2})!]^2 (\frac{n+2}{2})$ members of the same conjugacy class.

We wish to show that no other identities can hold. The remaining cases are as follows: $\langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_1, \langle d, a_{\pi(2)}, \dots, a_{\pi(n)} \rangle = a_k, k \neq 1, \langle a_{\pi(1)}, \dots, a_{\pi(s-1)}, d, a_{\pi(s+1)}, \dots, a_{\pi(n)} \rangle = a_t, t \text{ odd, } s \text{ even}$ and $\langle a_{\pi(1)}, \dots, a_{\pi(s-1)}, d, a_{\pi(s+1)}, \dots, a_{\pi(n)} \rangle = a_t, t \text{ even, } s \text{ even}$, where some $a_{\pi(1)}$ has the opposite sign under the operation from a_i (that is $a_{\pi(i)} = a_\ell$, where i and ℓ have a different parity). A careful investigation will show that the terms no longer cancel each other out in pairs, and hence the identities do not hold in general.

For example, in the second case we must consider a number of possibilities. We have $(a_1 - a_2 + a_3 + \dots - a_n) - \pi(a_2) +$

... $\pi(a_n) = a_k \pmod{m}$. If $a_{\pi(j)} = a_1$, where j is

odd and k is odd, we have $2a_k + \sum_{\substack{i=2 \\ i \neq k}}^n (-1)^{i-1} a_i +$

$$\sum_{\substack{i=2 \\ i \neq j}}^n (-1)^{i-1} a_{\pi(i)} \equiv 0 \pmod{m}, \text{ a contradiction, if only } a_i$$

is non-zero and $m(n) > 2$.

If $a_{\pi(j)} = a_1$, where j is odd and k is even,

$$\text{we have } -2a_k + 2a_1 + \sum_{\substack{i=2 \\ i \neq k}}^n (-1)^{i-1} a_i + \sum_{\substack{i=2 \\ i \neq j}}^n (-1)^{i-1} a_{\pi(i)} \equiv 0$$

\pmod{m} , a contradiction.

If $a_{\pi(j)} = a_1$, where j is even, k is odd,

$$\sum_{\substack{i=2 \\ i \neq k}}^n (-1)^{i-1} a_1 + \sum_{\substack{i=2 \\ i \neq j}}^n (-1)^{i-1} a_{\pi(j)} \equiv 0 \pmod{m}. \text{ However, the}$$

first sum contains $(\frac{n}{2} - 1)$ minus signs and $(\frac{n}{2} - 1)$ plus signs. The second sum has $(\frac{n}{2} - 2)$ plus signs and $\frac{n}{2}$ minus signs. Therefore, the terms cancel out in pairs.

Finally, if $a_{\pi(j)} = a_i$, where j is even, k is

$$\text{even, } -2a_k + \sum_{\substack{i=2 \\ i \neq k}}^n (-1)^{i-1} a_1 + \sum_{\substack{i=2 \\ i \neq j}}^n (-1)^{i-1} a_{\pi(i)} \equiv 0 \pmod{m},$$

a contradiction, choosing only a_k non-zero.

Again $m(n)$ must be chosen by checking the individual structures when $m < n$. Here we also need $m(n) > 2$. If $m(n) \geq n$ as well, the theorem will clearly hold.

Remark 5.2.3. For a given n , the number of conjugacy classes discussed in Theorem 5.2.2 is actually relatively small. If $n = 4$, $\frac{(n+1)!}{[(\frac{n}{2})!]^2 (\frac{n+2}{2})} = 10$, while $(4+1)! = 120$ is the total number of conjugacy classes. If $n = 6$, the number of conjugacy classes given is 35, compared with a possible 5040, and if $n = 10$, there are 462 classes compared to 1,628,800 possible classes.

§5.3 Conclusion.

There is still a great deal of work to be done to answer the general question, "Given an order m , does there exist an n -ary quasigroup Q of order m with a specified number $|C(Q)|$ of conjugacy classes?". One can generate more examples by variations of the techniques used in this Chapter. In particular, arranging negative signs and numbers relatively prime to the order m in various orders in front of the a_i 's, in the definition of the n -ary operation, will produce alternate conjugacy class numbers. However, if (Q, \langle, \rangle) must satisfy an identity corresponding to a permutation containing a cycle (abc) , and yet simultaneously not satisfy an identity corresponding to the transpositions (ab) , (bc) or (ac) , the algebraic techniques used here are fruitless. In Chapter 4, some success was obtained in constructing ternary quasigroups which satisfied such identity requirements (as the cases of 2 and 8 conjugacy classes do),

but the constructions were "ad hoc" or adaptations of quadruple systems. Unfortunately for larger n , any similar attempt becomes extremely cumbersome, and instead one would hope to be able to find a general technique, applying simultaneously to many values of n .

BIBLIOGRAPHY

- [1] Arkin, J., The first solution of the classical Eulerian magic cube problem of order ten, *Fibonacci Quarterly* 11 (1973), 174-178.
- [2] Arkin, J., A solution to the classical problem of finding systems of three mutually orthogonal numbers in a cube formed by three superimposed $10 \times 10 \times 10$ latin cubes, *Sugaku Seminar* 13 (1974), 90-94.
- [3] Arkin, J., Hoggatt, Jr., Exploded myths, *J. Recreat. Math.* 7 (1974), 90-93.
- [4] Arkin, J., Hoggatt, Jr., Magic latin k-cubes of order n, *Fibonacci Quarterly*, to appear.
- [5] Arkin, J., Straus, E.G., Latin k-cubes, *Fibonacci Quarterly* 12 (1974), 288-292.
- [6] Brownlee, K., Loraine, P., The relationship between finite groups and completely orthogonal squares, cubes and hyper-cubes, *Biometrika* 35 (1948), 277-281.
- [7] Cruse, A., On the finite completion of partial latin cubes, *J. Combinatorial Theory (A)* 17 (1974), 112-119.
- [8] Dénes, J., Keedwell, A.D., *Latin Squares and their Applications*, Academic Press, New York, 1974.
- [9] Doyen, J., Rosa, A., A bibliography and survey of Steiner systems, *Bollettino U.M.I.* (4), 7 (1973), 392-419.
- [10] Evans, T., The construction of orthogonal k-skeins and latin k-cubes, *Aequationes Math.* 14 (1976), 485-491.

- [11] Evans, T., Latin cubes orthogonal to their transposes - a ternary analogue of Stein quasigroups, *Aequationes Math.* 9 (1973), 296-297.
- [12] Ganter, B., *Combinatorial Designs and Algebras*, Preprint Nr. 270, Mai 1976, Technische Hochschule, Darmstadt.
- [13] Hall, M. Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass. 1967.
- [14] Hall, M. Jr., *The Theory of Groups*, MacMillan, New York, 1959.
- [15] Hanani, H., On quadruple systems, *Canad. J. Math.* 12 (1960), 147-157.
- [16] Hardy, G.H., Wright, E.M., *An Introduction to the Theory of Numbers*, Oxford University Press, 1968.
- [17] Hendricks, J., Magic cubes of odd order, *J. Recreat. Math.* 6 (1973), 268-273.
- [18] Hendricks, J., Species of third order magic squares and cubes, *J. Recreat. Math.* 6 (1973), 190-192.
- [19] Hendricks, J., The Pan-3-agonal magic cube of order 5, *J. Recreat. Math.* 5 (1972), 205-206.
- [20] Hendricks, J., The third order magic cube complete, *J. Recreat. Math.* 5 (1972), 43-50
- [21] Heppes, A., Révész, P., A new generalization of the method of latin squares and orthogonal latin squares and its application to the design of experiments, *Magyar Tud. Akad. Math. Int. Közl* 1 (1956), 379-390 (In Hungarian).

- [22] Humbolt, L., Sur une extension de la notion de carrés latins. C.R. Acad. Sc. Paris, Ser. A. 273 (1971), 795-798.
- [23] Johnson, D.M., Mendelsohn, N.S., Extended Triple Systems, Aequationes Math. 8 (1972), 291-298.
- [24] Lederman, W., Introduction to the Theory of Finite Groups, Oliver and Boyd, Edinburgh, 1967.
- [25] Lindner, C.C., Private communication.
- [26] Lindner, C.C., Finite partial cyclic triple systems can be finitely embedded, Alg. Universalis 1 (1971), 93-96.
- [27] Lindner, C.C., Identities preserved by the singular direct product, Alg. Universalis 1 (1971), 86-89.
- [28] Lindner, C.C., On the construction of cyclic quasigroups, Discrete Math. 6 (1973), 149-158.
- [29] Lindner, C.C., Two finite embedding theorems for partial 3-quasigroups, to appear.
- [30] Lindner, C.C., A finite partial idempotent latin cube can be embedded in a finite idempotent latin cube, J. Combinatorial Theory (A), 21 (1976), 104-109.
- [31] Lindner, C.C., Some remarks on the Steiner triple systems associated with Steiner quadruple systems. Colloquium Math. 32 (1975), 301-306.
- [32] Lindner, C.C., Mendelsohn, N.S., Construction of n -cyclic quasigroups and applications, Aequationes Math. 14 (1976), 111-121.
- [33] Lindner, C.C., Steedley, D., On the number of conjugates of a quasigroup, Alg. Universalis 5 (1975), 191-196.

- [34] McLeish, M., On the existence of latin squares with no subsquares of order two, *Utilitas Math.* 8 (1975), 41-53.
- [35] Mendelsohn, N.S., A natural generalization of Steiner triple systems, in *Computers in Number Theory*, Academic Press, New York 1971, pp. 323-338.
- [36] Mendelsohn, N.S., Hung, S.H.Y., On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$, *Utilitas Math.* 1 (1972), 5-95.
- [37] Meeus, J., Tetracubes, *J. Recreat. Math.* 6 (1973), 266-267.
- [38] Rosa, A., Lindner, C.C., A survey of Steiner quadruple systems, *Discrete Math.*, to appear.
- [39] Radó, F., Hosszú, M., Über eine Klasse von ternären Quasigruppen, *Acta Math. Acad. Sci., Hungar.* 15 (1964), 29-36.
- [40] Sade, A., Produit direct-singulier de quasigroups, orthogonaux et anti-abéliens, *Ann. Soc. Sci. Bruxelles, Sér. I*, 74 (1960), 91-99.
- [41] Steedley, D., Separable quasigroups, *Aequationes Math.* 0 (1973), 1-7.
- [42] Steedley, D., Separable quasigroups, *Aequationes Math.* 10 (1974), 116-117.
- [43] Stein, S.K., On the foundations of quasigroups, *Trans. Amer. Math. Soc.* 85 (1957), 228-256.
- [44] Warrington, P.D., Graeco-latin cubes, *J. Recreat. Math.* 6 (1973), 47-53.