Nilpotent Algebras with Maximal Class in Congruence Modular Varieties

by

Xuebin Zhang

A thesis submitted to the FACULTY OF GRADUATE STUDIES of the UNIVERSITY OF MANITOBA in partial fulfillment of the requirements of the degree of

Doctor of Philosophy

Department of Mathematics and Astronomy
University of Manitoba
Winnipeg, Manitoba

THE UNIVERSITY OF MANITOBA

FACULTY OF GRADUATE STUDIES

*****

COPYRIGHT PERMISSION PAGE

NILPOTENT ALGEBRAS WITH MAXIMAL CLASS IN CONGRUENCE MODULAR VARIETIES

BY

XUEBIN ZHANG

A Thesis/Practicum submitted to the Faculty of Graduate Studies of The University of Manitoba in partial fulfillment of the requirements of the degree of

DOCTOR OF PHILOSOPHY

Acknowledgments

I am deeply grateful to my supervisor Professor Robert Quackenbush. He awakened in me an interest in Universal Algebra; He suggested to me to investigate quaternary Mendelsohn quasigroups, and this investigation has finally led to this thesis. He patiently discussed with me my ideas, and provided me with his experience.

I would like to thank the Department of Mathematics and Astronomy, especially Professor Lynn Batten and Professor Nathan Mendelsohn for their support and encouragement.

I appreciate the financial support given to me by the Faculty of Graduate Studies of the University of Manitoba, by the Department of Mathematics and Astronomy and by Professor Robert Quackenbush.

Abstract

General representation theory by polynomials for nilpotent algebras in modular congruence varieties has been established and studied by several authors. An interesting open question is how to recursively construct nilpotent algebras with maximal class. In this thesis, several algebras are investigated: quaternary Mendelsohn quasigroups, Steiner quasigroups, Steiner loops, Steiner skeins, and p-groups.

First, we obtain the structure theorem of finite nilpotent quaternary Mendelsohn quasigroups.

By recursive construction we prove that for any natural number n, (i) there exist a nilpotent quaternary Mendelsohn quasigroup of order 4^{n+1} with maximal class n, and a solvable quaternary Mendelsohn quasigroup of order 4^n with maximal class n; (ii) there exist a nilpotent Steiner quasigroup of order 3^{n+1} with maximal class n, and a nilpotent Steiner loop of order 2^{n+2} with maximal class n; (iii) any subdirectly irreducible quaternary Mendelsohn quasigroup (Steiner quasigroup) of class n+1 with some conditions can be expanded to a subdirectly irreducible quaternary Mendelsohn quasigroup (Steiner quasigroup) of class n+2.

We also give a new and simple recursive construction for a nilpotent Steiner skeins of order 2^{n+2} with maximal class n such that all its derived Steiner loops are of nilpotence class n; and we represent by polynomials the dihedral group and the generalized quaternion group of order 2^{n+1} which are nilpotent p-groups with maximal class n.

Table of Contents

Acknowledgments ----------i

Abstract ----------ii

Table of Contents ----------iii

Chapter 1. Introduction ----------1

Chapter 2. Preliminaries ----------4

1. Groups ----------4
2. The commutator and the center ----------6
3. Abelian and affine algebras ----------10
4. Nilpotence and solvability ----------11
5. Representing nilpotent algebras ----------12
6. Subdirectly irreducible algebras ----------13

Chapter 3. Quaternary Mendelsohn Quasigroups ----------15

7. Quaternary Mendelsohn quasigroups ----------15
8. Quaternary Mendelsohn quasigroups of order 4 and 4^2 ----------20
9. Representing nilpotent quaternary Mendelsohn quasigroups ----------24
10. Recursive construction for nilpotent quaternary Mendelsohn quasigroups with maximal class ----------28
11. Recursive construction for solvable quaternary Mendelsohn quasigroups with maximal class ----------33

Chapter 4. Co-ordinatizations of Steiner Triple Systems ----------37

12. Steiner quasigroups ----------37

13. Steiner loops ----------46

Chapter 5. Co-ordinatizations of Steiner Quadruple Systems ----------50

14. Steiner skeins ----------50

15. Representation of finite nilpotent Steiner skeins ----------52

16. Recursive construction for Steiner skeins of nilpotence class n
with all derived Steiner loops of nilpotence class n ----------53

Chapter 6. *p*-Groups ----------59

17. Definitions and basic results ----------59

18. Finite nilpotent groups with maximal class ----------62

19. Recursive representation for the dihedral group D_{2^n} ----------63

My Publications ----------72

Bibliography ----------74

Chapter 1. Introduction

A general representation theory for nilpotent algebras in modular congruence varieties was established by Freese and McKenzie [7]. By applying this representation theory to some special algebras based on vector spaces, Guelzow [2] obtained some general representation theories by polynomials. Guelzow also posed an interesting question, that is, are there any recursive constructions for finite nilpotent algebras with maximal class? In this thesis, several algebras are investigated: quaternary Mendelsohn quasigroups, Steiner quasigroups, Steiner loops, Steiner skeins and p-groups.

In Chapter 2, we introduce basic concepts from group theory to universal algebra, and the general representation theory of Freese and McKenzie.

In Chapter 3, we study quaternary Mendelsohn quasigroups. In 1971, Mendelsohn generalized Steiner triple systems to cyclic triple systems; later such cyclic triple systems were called Mendelsohn triple systems. Similar to Steiner quasigroups which are obtained from the co-ordinatization of Steiner triple systems, Mendelsohn quasigroups are obtained from the co-ordinatization of Mendelsohn triple systems. Recently, Quackenbush introduced quaternary Mendelsohn triple systems and their corresponding quaternary Mendelsohn quasigroups. We study some algebraic properties with universal algebra as a tool; we obtain the structure theorem of finite nilpotent quaternary Mendelsohn quasigroups ; and by recursive construction we prove that for any natural number n:

(i) there exists a nilpotent quaternary Mendelsohn quasigroup of order 4^{n+1} with maximal class n;

(ii) there exists a solvable quaternary Mendelsohn quasigroup of order 4^n with maximal class n;

(iii) any subdirectly irreducible nilpotent quaternary Mendelsohn quasigroup of class n+1 with some conditions can be expanded to a subdirectly irreducible nilpotent quaternary Mendelsohn quasigroup of class n+2.

In Chapter 4, we investigate recursive constructions of nilpotent Steiner quasigroups and nilpotent Steiner loops. Guelzow presented a strengthened version of the representation theorem given by Klossek [15] for finite distributive Steiner quasigroups, and generalized the theorem to the class of all finite nilpotent Steiner quasigroups and posed the following open questions:

(i) Are there any recursive constructions for nilpotent Steiner quasigroups that raise the nilpotence class?

(ii) Are there any such constructions for distributive Steiner quasigroups?

For the first question we give a recursive construction; the second question is still open. A similar result is given for Steiner loops. That is,

(i) There exists a nilpotent Steiner quasigroup of order 3^{n+1} with maximal class n.

(ii) There exists a nilpotent Steiner loop of order 2^{n+2} with maximal class n.

(iii) Any subdirectly irreducible nilpotent Steiner quasigroup of class n+1 can expanded to a subdirectly irreducible nilpotent Steiner quasigroup of class n+2.

In Chapter 5, we give a recursive construction for a nilpotent Steiner skein of order 2^{n+2} with maximal class n such that all its derived Steiner loops are of nilpotence class n. Armanious and Guelzow [1, 3] obtained the structure theorem of finite nilpotent Steiner skeins. Guelzow [3] gave a construction of a Steiner skein of nilpotence class n with all

derived Steiner loops of nilpotence class 1. Armanious [1] gave a construction for Steiner skeins of nilpotence class n with all its derived Steiner loops of nilpotence class n. In this chapter we survey the main results on nilpotent Steiner skeins and give a new and simple construction, in the form of polynomials, for Steiner skeins of nilpotence class n with all its derived Steiner loops of nilpotence class n.

In Chapter 6, we investigate recursive constructions of finite p-groups. Some general representation theorems for finite nilpotent groups and some examples for p-groups with small order have been given by Guelzow. By recursive construction we shall represent the dihedral group and the generalized quaternion group of order 2^{n+1} which are nilpotent p-groups with maximal class n. At the same time, we see that the representation theories by polynomials provide a powerful tool for isomorphism classification of finite p-groups.

Chapter 2. Preliminaries

1. Groups

In the theory of groups, the important concepts of Abelian (commutative) group, the center of a group, the centralizer of a normal subgroup, solvable group, and nilpotent group can all be defined in terms of the commutator operation, that is, $[x, y] = x^{-1}y^{-1}xy$. Alternatively, these concepts can be defined in terms of the operation $[M, N] = Sg(\{[x, y] : x \in M, y \in N\})$, on normal subgroups, also called the commutator ($Sg(X)$ is the subgroup generated by X). Analogous concepts, based on the multiplication of ideals, are important in ring theory. An extension of these concepts to algebras other than groups and rings is behind one of the most exciting new directions of research in general algebra. The following definitions and results can be found in [21, 22].

Definition 1.1. An algebra $G = \langle G; \bullet, ^{-1}, e \rangle$ is a *group* if it satisfies the following identities:

(i) $(x \bullet y) \bullet z = x \bullet (y \bullet z)$;

(ii) $x \bullet e = e \bullet x = x$;

(iii) $x \bullet x^{-1} = x^{-1} \bullet x = e$.

A group G is called *abelian* if the commutative identity holds:

(iv) $x \bullet y = y \bullet x$

A group G is called *cyclic* if G is generated by one element.

Definition 1.2. A subgroup N of a group G is *normal*, if $gNg^{-1} = N$ for every $g \in G$.

Definition 1.3. If $a, b \in G$, the *commutator* of a and b, denoted by [a, b], is

$$[a, b] = a^{-1}b^{-1}ab.$$

Definition 1.4. The *commutator subgroup* (or derived subgroup) of G, denoted by G', is the subgroup of G generated by all the commutators. The higher commutator subgroups of G are defined inductively:

$$G^{(0)} = G, \quad G^{(i+1)} = G^{(i)'};$$

that is, $G^{(i+1)}$ is the commutator subgroup of $G^{(i)}$.

Definition 1.5. A group G is *solvable* if $G^{(n)} = \{e\}$ for some n, and the least such n is called the *class* of the solvable group G. Let H, K be normal subgroups of G; define

$[H, K] = Sg(\{ [h, k] : h \in H \text{ and } k \in K \})$, which is a normal subgroup of G.

Definition 1.6. Define the subgroups $\psi_i(G)$ of G by induction:

$$\psi_0(G) = G, \qquad \psi_{i+1}(G) = [\psi_i(G), G].$$

The *lower central series* of G is the series

$$G = \psi_0(G) \geq \psi_1(G) \geq \ldots .$$

Definition 1.7. The *center* of a group, $Z(G) = \{ a \in G : a \cdot x = x \cdot a \text{ for all } x \in G \}$, and note that it is a normal subgroup of G. The upper central series $\{\zeta_i(G)\}$ is the series of subgroups of G defined by induction:

$$\zeta_0(G) = \{e\}, \quad \zeta_{i+1}(G)/\zeta_i(G) = Z(G/\zeta_i(G));$$

that is, if ν_i: $G \to G/\zeta_i(G)$ is the natural map, then $\zeta_{i+1}(G)$ is the inverse image of the center of $G/\zeta_i(G)$.

The *upper central series* of G is the series

$$\{e\} = \zeta_0(G) \leq \zeta_1(G) \leq \zeta_2(G) \leq \ldots \quad .$$

Definition 1.8. A group G is *nilpotent* if $\psi_n(G) = \{e\}$ for some n, and the least such n is called the *class* of the nilpotent group G.

Theorem 1.9. If G is a group, then there is an integer n with $\zeta_n(G) = G$ if and only if $\psi_n(G) = \{e\}$. Moreover, in this case, $\psi_i(G) \leq \zeta_{n-i}(G)$ for all i.

Theorem 1.10. G is nilpotent of class $n > 1$ if and only if G/Z(G) is nilpotent of class n-1.

2. The commutator and the center

General commutator theory has to do with a binary operation, the commutator, that can be defined on the lattice of congruences of an algebra. The operation is very well behaved in congruence modular varieties, but much less so in most other varieties.

In 1976, Smith in his book on Mal'cev varieties [24] generalized the group theoretic concept of the commutator to the theory of Mal'cev varieties. With this concept he also generalized such notions as the 'center' and 'nilpotence'. In 1979, Hagemann and Herrmann [13] extended the theory of the commutator to modular varieties. In 1980 and 1983 Gumm [9, 10] presented an introduction to commutator theory which motivates the commutator geometrically. In 1987, Freese and McKenzie [7] published a book on commutator theory for congruence modular varieties, a more complete introduction to commutator theory.

The following definitions and results can be found in [7, 9, 10, 16].

Definition 2.1. Let A be any algebra. The *center* of A is the binary relation $\zeta(A)$ defined by :

$$< a, b > \in \zeta(A)$$

if and only if for every $n \geq 1$, and for every term operation $t \in Clo_{n+1}A$,

and for all $(c_1, c_2, \ldots , c_n)$ and $(d_1, d_2, \ldots , d_n) \in A^n$,

$$t(a, c_1, \ldots , c_n) = t(a, d_1, \ldots , d_n) \leftrightarrow t(b, c_1, \ldots , c_n) = t(b, d_1, \ldots , d_n).$$

A is called *abelian* if and only if $\zeta(A) = A \times A$.

Definition 2.2. Let α, β, η be congruences of an algebra A. We say that α *centralizes* β *modulo* η , written

$$C(\alpha, \beta, \eta),$$

if and only if for every $n \geq 1$, and for every term operation $t \in Clo_{n+1}A$,

and $< a, b > \in \alpha$ and $< c_1, d_1>, \ldots , < c_n, d_n> \in \beta$ we have

$$t(a, c_1, \ldots , c_n) \equiv_\eta t(a, d_1, \ldots , d_n) \leftrightarrow t(b, c_1, \ldots , c_n) \equiv_\eta t(b, d_1, \ldots , d_n).$$

Definition 2.3. For congruences α and β of A, we define their *commutator*, denoted $[\alpha, \beta]$, to be the smallest congruence η of A for which α centralizes β modulo η. The *centralizer* of β modulo α denoted $(\alpha : \beta)$, is the largest congruence γ of A such that γ centralizes β modulo α.

Lemma 2.4. Let 0_A and 1_A be the least and largest congruences of A. Then

(i) $\zeta(A) = (0_A : 1_A)$, that is, the largest congruence α such that $[\alpha, 1_A] = 0_A$;

(ii) $[1_A, 1_A]$ is the smallest congruence on A such that $A/[1_A, 1_A]$ is abelian;

in particular, $[1_A, 1_A] = 0_A$ iff $\zeta(A) = 1_A$ iff A is abelian;

(iii) $[\alpha, \beta] \leq \alpha \cap \beta$.

The commutator has proved to be a powerful tool for investigating congruence modular varieties. This is largely due to the fact that for any algebra in a congruence modular variety, the commutator is a commutative and completely join-preserving operation on congruences. We refer the reader to [7] for an extensive discussion on modular varieties and the commutator in these varieties.

Theorem 2.5. (Mal'cev [7]). A variety V has *permuting congruences* iff there is a 3-ary term p such that the equations $p(x, y, y) = x$, $p(x, x, y) = y$ are valid in V.

Theorem 2.6. (Jónsson [7]). A variety V has *distributive congruences* iff there exists an n and 3-ary terms $d_0, \ldots, d_n$ such that the following equations hold in V.

(i) $d_0(x, y, z) = x$;

(ii) $d_i(x, y, x) = x$ for $0 \leq i \leq n$;

(iii) $d_i(x, y, y) = d_{i+1}(x, y, y)$ for all even $i < n$;

(iv) $d_i(x, x, y) = d_{i+1}(x, x, y)$ for all odd $i < n$;

(v) $d_n(x, y, z) = z$.

Theorem 2.7. (Gumm [7]). A variety V has *modular congruences* iff there exists an n and 3-ary terms p and $d_0, \ldots, d_n$ such that the following equations hold in V.

(i) $d_0(x, y, z) = x$;

(ii) $d_i(x, y, x) = x$ for $0 \leq i \leq n$;

(iii) $d_i(x, y, y) = d_{i+1}(x, y, y)$ for all even $i < n$;

(iv) $d_i(x, x, y) = d_{i+1}(x, x, y)$ for all odd $i < n$;

(v) $d_n(x, y, y) = p(x, y, y)$;

(vi) $p(x, x, y) = y$.

Lemma 2.8. If A is an algebra in a congruence modular variety, then

(i) $[\alpha, \beta] = [\beta, \alpha]$;

(ii) $[\vee \alpha_i, \beta] = \vee [\alpha_i, \beta]$.

Definition 2.9. Let α and β be congruences on an algebra A. $\Delta_\alpha{}^\beta$ is the congruence generated by $\{ ((x, x), (y, y)) : x \beta y \}$ in α, where α is taken as a subalgebra of $A \times A$.

Lemma 2.10. (Gumm [9]). If A is an algebra in a congruence modular variety then the commutator $[\alpha, \beta] = \{ (d, c) : (b, b) \Delta_\alpha{}^\beta (d, c) \}$.

Definition 2.11. Let V be any variety. A ternary term $d(x, y, z)$ is called a *Gumm difference term* if it satisfies the following two conditions:

(i) $d(x, x, y) = y$ is an identity in V.

(ii) If $(x, y) \in \theta \in \mathrm{Con}\, A$, for some $A \in V$, then $d(x, y, y)\ [\theta, \theta]\ x$.

It is well known that every modular variety has a Gumm difference term and that in a permutable variety the Mal'cev term is a Gumm difference term.

Theorem 2.12. Let $< A, \Gamma >$ be an algebra of a modular variety. Let $d(x, y, z)$ be a Gumm difference term. Then $a\ \zeta(A)\ b$ if and only if

(i) $f(d(r_1(a,b), r_1(b,b), c_1), \ldots , d(r_n(a,b), r_n(b,b), c_n))$

$= d(f(r_1(a,b), \ldots , r_n(a,b)), f(r_1(b,b), \ldots, r_n(b,b)), f(c_1, \ldots , c_n))$, and

(ii) $d(r(a,b), r(b,b), r(b,b)) = r(a,b)$,

for all $f \in \Gamma$, all $(c_1, \ldots , c_n) \in A^n$ (n being the arity of f) and for all binary term functions $r_1(x, y), \ldots , r_n(x, y)$.

Corollary 2.13. Let $< A, \Gamma >$ be an algebra in a permutable variety and let $p(x, y, z)$ be a Mal'cev term. Then $a \zeta(A) b$ if and only if

$f(p(r_1(a,b), r_1(b,b), c_1), \ldots , p(r_n(a,b), r_n(b,b), c_n))$

$= p(f(r_1(a,b), \ldots , r_n(a,b)), f(r_1(b,b), \ldots, r_n(b,b)), f(c_1, \ldots , c_n))$,

for all $f \in \Gamma$, all $(c_1, \ldots , c_n) \in A^n$ (n being the arity of f) and for all binary term functions $r_1(x, y), \ldots , r_n(x, y)$.

3. Abelian and affine algebras

Definition 3.1. Let $< A ; F >$ be any algebra. A is called *affine* if there exists an abelian group $< A ; +, -, 0 >$ and a ternary term function $\tau(x, y, z)$ of A such that

(i) $\tau(x, y, z) = x - y + z$ for all $x, y, z \in A$,

and for each n-ary operation $f \in F$ there are endomorphisms $\alpha_1, \ldots , \alpha_n$ of the abelian group $< A ; +, -, 0 >$ and $c \in A$ such that

(ii) $f(x_1, \ldots , x_n) = \alpha_1(x_1) + \ldots + \alpha_n(x_n) + c$.

If this abelian group exists it is called the *group associated with A* and the term function

τ is called a *difference function* for A.

Theorem 3.2. (Herrmann [12]). The following are equivalent for an algebra A in a modular variety :

(i) A is abelian; (ii) A is affine.

4. Nilpotence and solvability

The following definition can be found in [2, 7].

Definition 4.1. Let A be an algebra. Define

$[1_A]^0 = 1_A$, $[1_A]^1 = [1_A, 1_A]$, $[1_A]^{k+1} = [[1_A]^k, [1_A]^k]$ for $k \geq 1$.

Definition 4.2. An algebra A is *solvable* if $[1_A]^n = 0_A$ for some n, and the least such n is called the *class* of the solvable algebra A.

Definition 4.3. Define

$$\psi_0(A) = 1_A, \quad \psi_{i+1}(A) = [\psi_i(A), 1_A] \quad \text{for } i \geq 0.$$

The *lower central series* of A is the series

$$G = \psi_0(A) \geq \psi_1(A) \geq \ldots .$$

Definition 4.4. An algebra A is *nilpotent* if $\psi_n(A) = 0_A$ for some n, and the least such n is called the *class* of the nilpotent algebra A.

A nilpotent algebra A of class 1 is *abelian*.

Definition 4.5. Define

$$\zeta_0(A) = 0_A\ ,\quad \zeta_{i+1}(A)/\zeta_i(A) = \zeta(A/\zeta_i(A)) \text{ for } i \geq 0.$$

The *upper central series* of A is the series

$$0_A = \zeta_0(A) \leq \zeta_1(A) \leq \zeta_2(A) \leq \ldots \quad .$$

Theorem 4.6. Let A be an algebra in a modular variety. Then A is nilpotent of class k if and only if $\zeta_k = 1_A$ and $\zeta_{k-1} \neq 1_A$.

Theorem 4.7. Let A be an algebra in a modular variety. Then A is nilpotent of class $k > 1$ if and only if $A/\zeta(A)$ is nilpotent of class k-1.

5. Representing nilpotent algebras

The main tool in the proof of some representation theorems is the description of the structure of the non-affine algebras in a congruence modular variety given by Freese and McKenzie in [7]. This description uses the following concept of a product of two algebras:

Definition 5.1. (Freese and McKenzie [7]). Let $< M; \{F^i\}_{i \in I} >$ and $< N; \{F^i\}_{i \in I} >$ be algebras in a congruence modular variety. Let M be affine with associated group $< M; +, -, 0 >$. Let T be a system of maps T_i: $N^{t_i} \rightarrow M$, (for $i \in I$) where t_i is the arity of F^i. Then $A = N \otimes^T M = < N \times M; \{F^i\}_{i \in I} >$ is defined to be the algebra with :

$F^i((n_1, m_1), \ldots, (n_{t_i}, m_{t_i})) = (F^i(n_1, \ldots, n_{t_i}),\ F^i(m_1, \ldots, m_{t_i}) + T_i(n_1, \ldots, n_{t_i}))$

where $(n_1, m_1), \ldots, (n_{t_i}, m_{t_i}) \in N \times M$.

Theorem 5.2. (Freese and McKenzie [7]). Let A be an algebra in a congruence modular variety V. Let $N = A/\zeta(A)$. Then there exists an abelian algebra M in V and a system T of maps as described above such that $A \cong N \otimes^T M$ and the center of $N \otimes^T M$ is the kernel of the projection onto N.

Corollary 5.3. An algebra in a congruence modular variety V is nilpotent of class 2 or less if and only if it can be represented as (that is, is isomorphic to) $N_1 \otimes^T N_2$ where N_1 and N_2 are abelian algebras in V.

Corollary 5.4. If an algebra in a congruence modular variety V is nilpotent of class n, then it can be represented as (that is, is isomorphic to)

$$((\ldots ((N_1 \otimes^{T_1} N_2) \otimes^{T_2} N_3) \ldots) \otimes^{T_{n-1}} N_n),$$

where $N_1, \ldots N_n$ are abelian algebras in V and $T_1, \ldots, T_{n-1}$ are some systems of maps as described above.

6. Subdirectly irreducible algebras

The following definitions and results can be found in [8].

Definition 6.1. An algebra is called *subdirectly irreducible* if for any subset $C \subset Con(A)$, the relation

$$\cap (\alpha \in C) = 0_A$$

implies the existence of $\beta \in C$ such that $\beta = 0_A$.

Corollary 6.2. An algebra A is *subdirectly irreducible* if and only if it has only one

element or Con(A) has one and only one atom, which is contained in every congruence relation other than 0_A.

Theorem 6.3. (Birkhoff [8]). Every algebra is isomorpic to a subdirect product of subdirectly irreducible algebras.

The following lemma is an exercise in [7].

Lemma 6.4. Let A be a nilpotent algebra in a congruence modular variety. Let $\alpha \in$ Con(A). Then $\alpha \neq 0_A$ if and only if $\alpha \cap \zeta(A) \neq 0_A$.

Lemma 6.5. A nilpotent algebra in a congruence modular variety is subdirectly irreducible if and only if for any subset $C \subset \{ \alpha \in \text{Con}(A) : \alpha \leq \zeta(A) \}$ the relation

$$\cap (\alpha \in C) = 0_A$$

implies the existence of $\beta \in C$ such that $\beta = 0_A$.

Chapter 3. Quaternary Mendelsohn Quasigroups

7. Quaternary Mendelsohn quasigroups

Definition 7.1. A *combinatorial quasigroup* is an ordered pair $(A, \circ)$, where A is set and "$\circ$" is a binary operation on A such that for all not necessarily distinct $a, b \in A$, the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions.

Definition 7.2. An *algebraic quasigroup* is an algebra $\langle A; \circ, \backslash, / \rangle$, such that "$\circ$", "$\backslash$", "$/$" are three binary operations on A satisfying the four identities:

(i) $x \circ (x \backslash y) = y$;

(ii) $x \backslash (x \circ y) = y$;

(iii) $(x / y) \circ y = x$;

(iv) $(x \circ y) / y = x$.

Suppose $(A, \circ)$ is a combinatorial quasigroup. We can define two binary operations "$\backslash$", "$/$" on A by $a \circ b = c$ iff $a \backslash c = b$ iff $c / b = a$. It is not difficult to see that $\langle A; \circ, \backslash, / \rangle$ is an algebraic quasigroup. On the other hand, if $\langle A; \circ, \backslash, / \rangle$ is an algebraic quasigroup then each of $(A, \circ)$, $(A, \backslash)$ and $(A, /)$ is a combinatorial quasigroup.

In 1971, N. S. Mendelsohn [17] generalized Steiner triple systems to cyclic triple systems; later such cyclic triple systems were called Mendelsohn triple systems [27, 28].

Similar to Steiner quasigroups which are obtained from the co-ordinatization of Steiner triple systems, Mendelsohn quasigroups are obtained from the co-ordinatization of Mendelsohn triple systems.

Definition 7.3. A *Mendelsohn triple system* is a pair (X, B), where X is a set of elements (called points) and B is a collection of cycles with size three such that each ordered pair of distinct points of X appears in exactly one cycle of B. (The ordered pairs (a, b), (b, c), (c, a) appear in the cycle (a, b, c) and the cycles (a, b, c), (b, c, a), (c, a, b) are all equal.)

Definition 7.4. A *Mendelsohn quasigroup* is a combinatorial quasigroup $(A, \circ)$ satisfying the following identities:

(i) $x \circ x = x$;

(ii) $(x \circ y) \circ x = y$.

Lemma 7.5. If (X, B) is a Mendelsohn triple system, define $A = X$, $a \circ a = a$ for all $a \in A$ and otherwise $a \circ b = c$ if and only if $(a, b, c) \in B$. Then $(A, \circ)$ is a Mendelsohn quasigroup. If $(A, \circ)$ is a Mendelsohn quasigroup, define $X = A$ and $B = \{ (a, b, c) \mid a \neq b$ and $a \circ b = c \}$. Then (X, B) is a Mendelsohn triple system.

Lemma 7.6. An algebra $\langle A, \circ \rangle$ is a Mendelsohn quasigroup if and only if $\langle A, \circ \rangle$ satisfies the following identities:

(i) $x \circ x = x$;

(ii) $(x \circ y) \circ x = y$.

Recently, R. W. Quackenbush introduced quaternary Mendelsohn triple systems corresponding quaternary Mendelsohn quasigroups.

Definition 7.7. (Quackenbush). A Mendelsohn triple system is *quaternary* if for any cycle (a, b, c) there is a unique fourth point d such that (b, a, d), (c, b, d) and (a, c, d) are cycles.

Definition 7.8. (Quackenbush). A Mendelsohn quasigroup $(A, \circ)$ is *quaternary* if it satisfies the identity :

(iii) $(x \circ y) \circ y = y \circ x$.

Lemma 7.9. An algebra $\langle A, \circ \rangle$ is a quaternary Mendelsohn quasigroup if and only if $\langle A, \circ \rangle$ satisfies the following identities:

(i) $x \circ x = x$;

(ii) $(x \circ y) \circ x = y$;

(iii) $(x \circ y) \circ y = y \circ x$.

Lemma 7.10. A quaternary Mendelsohn quasigroup satisfies the following identities :

(iv) $x \circ (y \circ x) = y$;

(v) $x \circ (x \circ y) = y \circ x$;

(vi) $(x \circ y) \circ (y \circ x) = x$.

From the fact that quaternary Mendelsohn quasigroups are algebraic, we have that the variety of quaternary Mendelsohn quasigroups is a congruence uniform, regular, coherent, permutable and modular variety. That is,

Lemma 7.11. The variety of quaternary Mendelsohn quasigroups is a modular variety.

Proof. Since there is a Mal'cev term $p(x, y, z) = (x \circ y) \circ (z \circ x)$ with $p(x, x, y) = y$ and $p(x, y, y) = x$, it is congruence-permutable and so is congruence-modular.

Lemma 7.12. Let $< A; \circ >$ be a quaternary Mendelsohn quasigroup, and α a congruence of A. Then

(i) all congruence classes of α are of same size;

(ii) each congruence class of α generates the congruence α;

(iii) each congruence class of α is a subalgebra;

(iv) each subalgebra that contains a class of α is the union of congruence classes of α.

Lemma 7.13. If an idempotent combinatorial quasigroup satisfies the medial law, that is, $(x \circ y) \circ (z \circ t) = (x \circ z) \circ (y \circ t)$, then

(i) $s \circ (x \circ z) = v \circ (x \circ t)$ implies $s \circ (y \circ z) = v \circ (y \circ t)$;

(ii) $(x \circ z) \circ n = (x \circ t) \circ m$ implies $(y \circ z) \circ n = (y \circ t) \circ m$.

Proof. Let $x = y \circ u$. Since

$\{s \circ (x \circ z)\} \circ \{v \circ (x \circ t)\} = (s \circ v) \circ \{x \circ (z \circ t)\} = (s \circ v) \circ \{(y \circ u) \circ (z \circ t)\}$

$= \{s \circ (y \circ z)\} \circ \{v \circ (u \circ t)\}$ and $v \circ (x \circ t) = v \circ \{(y \circ u) \circ t\} = \{v \circ (y \circ t)\} \circ \{v \circ (u \circ t)\}$.

So $s \circ (y \circ z) = v \circ (y \circ t)$ and we have (i). Similarly, we have (ii).

Lemma 7.14. The following are equivalent for a quaternary Mendelsohn quasigroup $< A; \circ >$:

(i) $< A; \circ >$ is affine;

(ii) $< A; \circ >$ is abelian;

(iii) $< A; \circ >$ satisfies the medial law, that is, $(x \circ y) \circ (z \circ t) = (x \circ z) \circ (y \circ t)$.

Proof. From Lemma 7.11 we have the variety of quaternary Mendelsohn quasigroups is a modular variety, and then from Theorem 3.2, (i) and (ii) are equivalent. Assume it is abelian; since $(z \circ y) \circ (z \circ z) = (z \circ z) \circ (y \circ z)$, we have $(z \circ y) \circ (z \circ t) = (z \circ z) \circ (y \circ t)$, and then $(x \circ y) \circ (z \circ t) = (x \circ z) \circ (y \circ t)$. Assume it satisfies the medial law; then it is abelian from Lemma 7.13.

Definition 7.15. Let $< B; \circ >$ be a subalgebra of $< A; \circ >$. $< B; \circ >$ is *normal* if B is a coset of a congruence on $< A; \circ >$.

Lemma 7.16. Let $< A; \circ >$ be a finite quaternary Mendelsohn quasigroup. If it satisfies the medial law, then $|A| = 4^n$ for some $n \geq 0$.

Proof. Since it satisfies the medial law, we have $\{x, y, x \circ y, y \circ x\}$ is a normal subalgebra for any $x, y \in A$.

Lemma 7.17. Let $< A; \circ >$ be a quaternary Mendelsohn quasigroup. Then each class of the center is a subalgebra which satisfies the medial law.

Proof. This follows from Definition 2.1 of the center.

Theorem 7.18. Let $< A; \circ >$ be a finite quaternary Mendelsohn quasigroup. If it is

nilpotent, then $|A| = 4^n$ for some $n \geq 0$.

Proof. This follows from Lemma 7.14, Lemma 7.16 and Theorem 4.7.

Lemma 7.19. Let $< A; \circ >$ be a quaternary Mendelsohn quasigroup. Then $a\ \zeta(A)\ b$ if and only if for all $x, y \in A$,

$$x \circ y = (r_1 \circ r_2) \circ \{ \{ ((r_1 \circ b) \circ (x \circ r_1)) \circ ((r_2 \circ b) \circ (y \circ r_2)) \} \circ ((r_1 \circ r_2) \circ b) \}$$

for $r_1, r_2 \in \{ a, b, a \circ b, b \circ a \}$.

Proof. Apply Corollary 2.13 with Mal'cev term $p(x, y, z) = (x \circ y) \circ (z \circ x)$ and note that the only binary term functions are $x, y, x \circ y, y \circ x$.

8. Quaternary Mendelsohn quasigroups of order 4 and 4^2

Let α be a congruence with class size 4 on a quaternary Mendelsohn quasigroup $< A, \circ >$. First we ask whether it is true that $\alpha \leq \zeta(A)$; we shall show the answer is negative. In this section and the Sections 9 and 10 we always let $GF(4) = \{0, 1, \theta, 1+\theta\}$ with $\theta^2 = 1 + \theta$.

From Lemma 6.5 we have

Lemma 8.1. A nilpotent quaternary Mendelsohn quasigroup with the size of its center classes being 4 is subdirectly irreducible.

Lemma 8.2. Define $a \bullet b = \theta a + (1+\theta) b$ for $a, b \in GF(4)$. Then $< GF(4), \bullet >$ is

an abelian quaternary Mendelsohn quasigroup which is simple and hence subdirectly irreducible.

Lemma 8.3. Let A be a quaternary Mendelsohn quasigroup with 4 elements. Then A is isomorphic to $< GF(4), \bullet >$.

Notice that if we define $a \bullet b = (1+\theta)a + \theta b$ for $a, b \in GF(4)$, then $< GF(4), \bullet >$ is a 4-element quaternary Mendelsohn quasigroup, and hence isomorphic to $< GF(4), \bullet >$. It is the *opposite* of $< GF(4), \bullet >$ since $x \bullet y = y \bullet x$. Clearly, on any 4-element set there are exactly two ways of defining a quaternary Mendelsohn quasigroup and these are opposites of each other. Call any 4-element subquasigroup of a quaternary Mendelsohn quasigroup a *quartet.* If A is any quaternary Mendelsohn quasigroup containing the quartet Q and we replace Q with its opposite, then the modified algebra is again a quaternary Mendelsohn quasigroup.

Theorem 8.4. Let $< B, \bullet >$ and $< H, \bullet >$ be two quaternary Mendelsohn quasigroups of size 4 where $B = \{ a, b, a \bullet b, b \bullet a \}$ and $H = \{ c, d, c \bullet d, d \bullet c \}$.

Let $A = \{ (u, f) : u \in B, f \in H \}$. Define "$\circ$" on A as follows.

$$(u, f) \circ (v, g) = (u \bullet v, g \bullet f) \qquad \text{if } u = v = b \bullet a ;$$

$$(u, f) \circ (v, g) = (u \bullet v, f \bullet g) \qquad \text{otherwise.}$$

Then

(i) $< A, \circ >$ is obtained from $< B, \bullet > \times < H, \bullet >$ by replacing the quartet $\{(b \bullet a, h) \mid h \in H\}$ with its opposite and consequently is a quaternary Mendelsohn quasigroup;

(ii) $\eta = \{ < (u, f), (u, g) > : u \in B, f, g \in H \}$ is the unique atomic congruence, which

is contained in every congruence relation other than 0_A making $< A, \circ >$ subdirectly irreducible;

(iii) $< A, \circ >$ is not nilpotent;

(iv) $< A, \circ >$ is solvable of class 2;

(v) $\zeta(A) = 0_A$.

Proof. (ii). First it is readily checked that η is a congruence. To see this, note that if α is a congruence of the quaternary Mendelsohn quasigroup M and M' is a subquasigroup contained in some block of α, and M" is a quaternary Mendelsohn quasigroup on the same set as M', then $M^* = (M - M') \cup M''$ is a quaternary Mendelsohn quasigroup and α is a congruence of M*. Since its class size is 4, it is an atom. In the following we show that it is the only atom.

Let θ be a congruence other than 0_A and η; then there are two elements, say, (u, f) and (v, g), with $u \neq v$, $u \neq b \bullet a$ and (u, f) θ (v, g).

If $f \neq g$, then $x \theta y$ for $x, y \in E_1 = \{$ (u, f), (v, g), (u•v, f•g), (v•u, g•f) $\}$. By multiplying E_1 on the left by (u, g), (u, f•g), (u, g•f), respectively, we have

$E_2 = \{$ (u, g•f), (v, f•g), (u•v, g), (v•u, f) $\}$,

$E_3 = \{$ (u, g), (v, f), (u•v, g•f), (v•u, f•g) $\}$,

$E_4 = \{$ (u, f•g), (v, g•f), (u•v, f), (v•u, g) $\}$;

and we see that $x \theta y$ for $x, y \in E_i$ where i = 2, 3, 4. We let $v = b \bullet a$ without loss generality; then (u, f)∘(u, g•f) θ (v, g)∘(v, f•g), that is, (u, g) θ (v, g•f), and so (u, g) θ (u, f•g), implying $\eta < \theta$.

If $f = g$, then taking $h \neq f$, then we see that $x \theta y$ for $x, y \in F_i$,

where $1 \leq i \leq 4$ and

$$F_1 = \{ (u, f), \quad (v, f), \quad (u \bullet v, f), \quad (v \bullet u, f) \},$$

$$F_2 = \{ (u, h \bullet f), \quad (v, h \bullet f), \quad (u \bullet v, h \bullet f), \quad (v \bullet u, h \bullet f) \},$$

$$F_3 = \{ (u, h), \quad (v, h), \quad (u \bullet v, h), \quad (v \bullet u, h) \},$$

$$F_4 = \{ (u, f \bullet h), \quad (v, f \bullet h), \quad (u \bullet v, f \bullet h), \quad (v \bullet u, f \bullet h) \}.$$

We let $v = b \bullet a$ without loss generality, than $(u, f) \circ (u, h \bullet f) \; \theta \; (v, f) \circ (v, h \bullet f)$, that is, $(u, h) \; \theta \; (v, f \bullet h)$, and then $(u, h) \; \theta \; (u, f \bullet h)$, so that $\eta < \theta$.

(iii) and (iv). In the following we apply Definition 2.9 and Lemma 2.10 to show that $[1_A, [1_A, 1_A]] = [1_A, 1_A]$ and $[[1_A, 1_A], [1_A, 1_A]] = 0_A$. We take

$$\alpha = 1_A = A \times A, \quad \beta = 1_A = A \times A, \quad x = (a, c), \quad y = (b \bullet a, d),$$

$$s_1 = (a, d), \quad t_1 = (b \bullet a, c), \quad s_2 = (b, c \bullet d), \quad t_2 = (a \bullet b, d \bullet c)$$

We have

$$(s_2, t_2) \circ \{(x, x) \circ (s_1, t_1)\} = ((b \bullet a, c \bullet d), (b \bullet a, c \bullet d)), \text{ and}$$

$$(s_2, t_2) \circ \{(y, y) \circ (s_1, t_1)\} = ((a, d \bullet c), (a, d)), \quad \text{so}$$

$$((b \bullet a, c \bullet d), (b \bullet a, c \bullet d)) \; \Delta_\alpha^\beta \; ((a, d \bullet c), (a, d)), \quad \text{so}$$

$$(a, d \bullet c) \; [\alpha, \beta] \; (a, d); \quad \text{that is,}$$

$$(a, d \bullet c) \; [1_A, 1_A] \; (a, d).$$

From this, we have $[1_A, 1_A] = \{ < (u, f), (u, g) > : u \in B, f, g \in H \}$.

We take $\alpha = 1_A = A \times A$, $\beta = [1_A, 1_A]$, $x = (a, c)$, $y = (a, d)$,

$$s_1 = (a, d), \quad t_1 = (b, c), \quad s_2 = (b, d \bullet c), \quad t_2 = (b \bullet a, c \bullet d).$$

We have

$$(s_2, t_2)\circ\{(s_1, t_1)\circ(x, x)\} = ((b\bullet a, d\bullet c), (b\bullet a, d\bullet c)), \quad \text{and}$$

$$(s_2, t_2)\circ\{(s_1, t_1)\circ(y, y)\} = ((b\bullet a, c), (b\bullet a, c\bullet d)), \qquad \text{so}$$

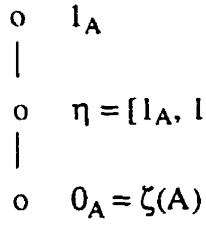
$$((b\bullet a, d\bullet c), (b\bullet a, d\bullet c)) \ \Delta_\alpha{}^\beta \ ((b\bullet a, c), (b\bullet a, c\bullet d)), \ \text{so}$$

$$(b\bullet a, c) \ [\alpha, \beta] \ (b\bullet a, c\bullet d); \quad \text{that is,}$$

$$(b\bullet a, c) \ [1_A, \ [1_A, 1_A]] \ (b\bullet a, c\bullet d),$$

and then $[1_A, [1_A, 1_A]] = [1_A, 1_A]$. Therefore, it is not nilpotent by the definition, and it is easy to see that $[[1_A, 1_A], [1_A, 1_A]] = 0_A$, so it is solvable of class 2.

(v). This follows from (iii).



The lattice of all congruences on $< A, \circ >$

9. Representing nilpotent quaternary Mendelsohn quasigroups

Applied to quaternary Mendelsohn quasigroups the descriptions in Definition 5.1, Theorem 5.2, Corollary 5.3 and Corollary 5.4 therefore become :

Definition 9.1. Let $< M; \circ >$ and $< N; \circ >$ be quaternary Mendelsohn quasigroups.

Let M be affine with associated group $< M; +, -, 0 >$. Let p be a map from $N \times N \to M$. Then $A = N \otimes^p M$ is defined to be the algebra on $N \times M$ with :

$$(n_1 , m_1) \circ (n_2 , m_2) = (n_1 \circ n_2 , m_1 \circ m_2 + p(n_1, n_2)).$$

Theorem 9.2. Let $< A ; \circ >$ be a quaternary Mendelsohn quasigroup. Let $N = A/\zeta(A)$. Then there exists an abelian quaternary Mendelsohn quasigroup M and a map p as described above such that $A = N \otimes^p M$ and the center of $N \otimes^p M$ is the kernel of the projection onto N.

Corollary 9.3. A quaternary Mendelsohn quasigroup is nilpotent of class 2 or less if and only if it can be represented as (that is, is isomorphic to) $N_1 \otimes^p N_2$ where N_1 and N_2 are abelian quaternary Mendelsohn quasigroups.

Corollary 9.4. If a quaternary Mendelsohn quasigroup is nilpotent of class n, then it can be represented as (that is, is isomorphic to)

$$((\ldots ((N_1 \otimes^{p_1} N_2) \otimes^{p_2} N_3) \ldots) \otimes^{p_{n-1}} N_n),$$

where $N_1, \ldots N_n$ are abelian quaternary Mendelsohn quasigroups, and $p_1, \ldots, p_{n-1}$ are some systems of maps as described above.

Since every abelian (that is, medial) quaternary Mendelsohn quasigroup is isomorphic to $< (GF(4))^n; \bullet >$ with $x \bullet y = \theta x + (1+\theta)y$, Theorem 9.2 can be used to prove the following representation theorem by induction over the class of nilpotence :

Theorem 9.5. Let $A = < A; \circ >$ be a finite quaternary Mendelsohn quasigroup of nilpotence class k. Then there exists an m-dimensional vector space Ω, a polynomial p:

$\Omega^2 \to \Omega$ over GF(4), and a sequence $1 \le n_1 < \ldots < n_k = m$ of integers such that

(i) if $1 \le s < k$ and $n_s < i \le n_{s+1}$, then $p_i(x, y)$ does not depend on the variables $x_{n_s+1}, \ldots, x_m$ and $y_{n_s+1}, \ldots, y_m$;

(ii) $p_i(x, y) = 0$ for all $x, y \in \Omega$ and $1 \le i \le n_1$;

(iii) $\Omega = <\Omega; \circ>$ is isomorphic to A where $x \circ y = \theta x + (\theta+1)y + p(x, y)$;

(iv) the center of A corresponds to the kernel of the projection onto the first n_{k-1} components of Ω. This projection is a homomorphism.

From Theorem 9.5. we have the following theorem.

Theorem 9.6. Let $<A; \circ>$ be a finite quaternary Mendelsohn quasigroup of order 4^m. Then $<A; \circ>$ is nilpotent if and only if it is isomorphic to $<\Omega; \circ>$, where Ω is an m-dimensional vector space over GF(4), $x \circ y = \theta x + (\theta+1)y + p(x, y)$, such that

(i) $p_1(x, y) = 0$;

(ii) $p_i(x, y) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1})$ for $2 \le i \le m$;

(iii) $p(x, x) = 0$, $\theta p(x, y) = p(x \circ y, x)$ and $\theta p(x, y) = p(x \circ y, y) + p(y, x)$

for all $x, y \in A$.

Proof. We only need to show (iii). Since $x \circ x = x$ if and only if $p(x, x) = 0$, $(x \circ y) \circ x = y$ if and only if $\theta p(x, y) = p(x \circ y, x)$, and $(x \circ y) \circ y = y \circ x$ if and only if $\theta p(x, y) = p(x \circ y, y) + p(y, x)$.

Lemma 9.7. Let A be an m-dimensional vector space over GF(4). Define

$$x \circ y = \theta x + (1+\theta)y + p(x, y), \quad \text{such that}$$

$< A ; \circ >$ is a quaternary Mendelsohn quasigroup. Then we have

(i) $p(x, x) = 0$ for all x;

(ii) $\theta p(x, y) = p(x \circ y, x)$ for all $x, y \in A$;

(iii) $\theta p(x, y) = p(x \circ y, y) + p(y, x)$ for all $x, y \in A$.

From (ii) and (iii) we have, for all $x, y \in A$,

$p(x, y) = p(x, y)$, $\quad p(x \circ y, x) = \theta p(x, y)$, $\quad p(y, x \circ y) = \theta^2 p(x, y)$;

$p(y, x) = p(y, x)$, $\quad p(y \circ x, y) = \theta p(y, x)$, $\quad p(x, y \circ x) = \theta^2 p(y, x)$;

$p(x \circ y, y) = \theta p(x, y) + p(y, x)$, $\quad p(y \circ x, x \circ y) = \theta^2 p(x, y) + \theta p(y, x)$,

$p(y, y \circ x) = p(x, y) + \theta^2 p(y, x)$; $\quad p(y \circ x, x) = \theta p(y, x) + p(x, y)$,

$p(x \circ y, y \circ x) = \theta^2 p(y, x) + \theta p(x, y)$, $\quad p(x, x \circ y) = p(y, x) + \theta^2 p(x, y)$.

From Theorem 9.6 and Lemma 9.7 we have

Theorem 9.8. (Nilpotent Quaternary Mendelsohn Quasigroup Construction)

Let $< A ; \circ >$ be a nilpotent quaternary Mendelsohn quasigroup of order 4^m. Define

$$\Omega = A \times GF(4) \text{ and } (x, i) \circ (y, j) = (x \circ y, \ \theta i + (1+\theta)j + p_{m+1}(x, y)).$$

Then $< \Omega ; \circ >$ is a nilpotent quaternary Mendelsohn quasigroup

if and only if the following identities hold:

(i) $p_{m+1}(x, x) = 0$ for all $x \in A$,

(ii) $\theta p_{m+1}(x, y) = p_{m+1}(x \circ y, x)$ for all $x, y \in A$,

(iii) $\theta p_{m+1}(x, y) = p_{m+1}(x \circ y, y) + p_{m+1}(y, x)$ for all $x, y \in A$.

Moreover, this is true if and only if for any 4-subalgebra $B = \{x, y, x \circ y, y \circ x\}$ of A, $< B \times GF(4) ; \circ >$ is an abelian.

Theorem 9.9. A finite quaternary Mendelsohn quasigroup is nilpotent if and only if it is isomorphic to a quaternary Mendelsohn quasigroup obtained from the 4-element quaternary Mendelsohn quasigroup by repeated application of Nilpotent Quaternary Mendelsohn Quasigroup Construction.

10. Recursive construction for nilpotent quaternary Mendelsohn quasigroups with maximal class

In this section we define $a \bullet b = \theta a + (1+\theta)b$ for $a, b \in GF(4)$ and $(x \bullet y)_i = x_i \bullet y_i = \theta x_i + (1+\theta)y_i$ for $x, y \in GF(4)^n$.

Lemma 10.1. Let $< A ; \circ >$ be a quaternary Mendelsohn quasigroup and $a,b \in A$ with $a \neq b$. Let $H = \{a, b, a \circ b, b \circ a\}$, $x \in A$ with $x \notin H$ and $B = \{a \circ x, a, x, x \circ a\}$. If $<a, b> \in \zeta(A)$, then $E = \{m \circ u : m \in B \text{ and } u \in H\}$ is a sub-quaternary Mendelsohn quasigroup which is isomorphic to the direct product of two 4-element quaternary Mendelsohn quasigroups B and H.

Proof. It is easily checked that

$$(m \circ a) \circ (n \circ a) = [(m \circ n) \circ a] \circ [(m \circ n) \circ a] \quad \text{for } m, n \in B.$$

Since $\langle u, a\rangle \in \zeta(A)$, we have

$$(m \circ u) \circ (n \circ u) = [(m \circ n) \circ u] \circ [(m \circ n) \circ u] \quad \text{for } m, n \in B \text{ and } u \in H.$$

That is,

$$(m \circ u) \circ (n \circ u) = (m \circ n) \circ (u \circ u) \quad \text{for } m, n \in B \text{ and } u \in H.$$

Since $\langle u, v\rangle \in \zeta(A)$, we have

$$(m \circ u) \circ (n \circ v) = (m \circ n) \circ (u \circ v) \quad \text{for } m, n \in B \text{ and } u, v \in H.$$

Lemma 10.2. Let $A = GF(4)^2$. Define $x \circ y = (x_1 \cdot y_1,\ x_2 \cdot y_2 + p(x_1, y_1))$ so that it is a quaternary Mendelsohn quasigroup. Then

$$p(x_1, y_1) = (x_1^2 + y_1^2) \{ (1+\theta)(a+b)x_1 + \theta(a+b)y_1 + \theta(a+b) + a \},$$

where $p(0, 1) = a$ and $p(1, 0) = b$; moreover, $x \circ y$ satisfies the medial law. That is, a nilpotent quaternary Mendelsohn quasigroup of order 16 is abelian.

Proof. From Lemma 10.1, we see that $< A ; \circ >$ is abelian, that is, a nilpotent quaternary Mendelsohn quasigroup of order 16 is abelian. In the following we show that

$$p(x_1, y_1) = (x_1^2 + y_1^2) \{ (1+\theta)(a+b)x_1 + \theta(a+b)y_1 + \theta(a+b) + a \}.$$

Let $u(s) = (1, s, s^2, s^3)$, $w(i) = (c_{i0}, c_{i1}, c_{i2}, c_{i3})$,

$$v(x) = (p(x, 0),\ p(x, 1),\ p(x, 1+\theta),\ p(x, \theta),$$

$$Y = (w(0),\ w(1), w(2), w(3))^T, \quad A = (u(0),\ u(1), u(1+\theta), u(\theta))^T,$$

$$Q = (v(0), v(1), v((1+\theta), v(\theta))^T.$$

From Lemma 9.7, we have

$$v(0) = (0,\ a,\ a(1+\theta)+b,\ b(1+\theta)), \quad v(1) = (b,\ 0,\ a(1+\theta),\ a+b(1+\theta)),$$

$$v(1+\theta) = (a\theta,\ a\theta+b,\ 0,\ a\theta+b(1+\theta)), \quad v(\theta) = (a+\theta b,\ b\theta,\ a(1+\theta)+b\theta,\ 0).$$

Since

$$p(x_1, y_1) = u(x_1)\, Y\, u(y_1)^T,$$

we have

$$A\, Y\, A^T = Q;$$

and then,

$$Y = A^{-1} Q (A^{-1})^T;$$

that is,

$$p(x_1, y_1) = (x_1^2 + y_1^2)\ \{\ (1+\theta\ )(a+b)x_1 + \theta(a+b)y_1 + \theta(a+b) + a\ \}.$$

Lemma 10.3. Let A be a 3-dimensional vector space over GF(4). Let

$x \circ y = \theta x + (1+\theta)y + p(x, y)$ and $p_1(x, y) = p_2(x, y) = 0$. If

(1) $p_3(x, y) = (x_1 + y_1)(x_2 + y_2)$, or

(2) $p_3(x, y) = (x_1y_2 + x_2y_1)^2$, or

(3) $p_3(x, y) = (x_2 + y_2)(x_1y_2 + x_2y_1)$,

then we have that

(a) $< A; \circ >$ is quaternary Mendelsohn quasigroup for cases (1), (2) and (3);

(b) $< A; \circ >$ is abelian in cases (1) and (2);

(c) $< A; \circ >$ is nilpotent of class 2 in case (3);

(d) $< A; \circ >$ is subdirectly irreducible in case (3).

Proof. It is readily checked for cases (1), (2) and (3) that

(i) $p_3(x_1, x_2; x_1, x_2) = 0$;

(ii) $p_3(x_1 \bullet y_1, x_2 \bullet y_2;\ x_1, x_2) = \theta p_3(x_1, x_2;\ y_1, y_2)$;

(iii) $p_3(x_1 \bullet y_1, x_2 \bullet y_2;\ y_1, y_2) = \theta p_3(x_1, x_2;\ y_1, y_2) + p_3(y_1, y_2;\ x_1, x_2)$,

so (a) holds.

It is also readily checked that for cases (1) and (2) the medial law holds, so (b) holds.

For case (3), first note that it is not abelian since $x\circ(y\circ z) \neq (x\circ y)\circ(x\circ z)$ for $x = (0, 0, 1)$, $y = (1, 0, 0)$ and $z = (0, 1, 0)$. By the results of the section 5, we know that A is nilpotent of class k with $2 \leq k \leq 3$ and that $A/\zeta(A)$ is nilpotent of class k-1. Since $|A/\zeta(A)| \leq 16$, it is of class 1, and so $k = 2$ and (c) holds. But $\alpha = \{ < x, y > : x_1 = y_1, x_2 = y_2 \} \leq \zeta(A)$ and A/α is of class 1 as $|A/\alpha| = 16$. This forces $\alpha = \zeta(A)$ and (d) holds.

Theorem 10.4. Let A be an (m+1)-dimensional vector space over GF(4) with $x\circ y = \theta x + (1+\theta)y + p(x, y)$. If we define $p(x, y)$ as follows:

(i) $p_1(x, y) = p_2(x, y) = 0$;

(ii) $p_k(x, y) = (x_{k-1} + y_{k-1} + p_{k-1}(x, y))(x_1y_2 + x_2y_1)$ for $3 \leq k \leq m+1$,

then $< A; \circ >$ is a nilpotent subdirectly irreducible quaternary Mendelsohn quasigroup of class m.

Proof. By induction, it is readily checked that for $1 \leq i \leq m+1$,

(i) $p_i(x, x) = 0$ for all x;

(ii) $\theta p_i(x, y) = p_i(x\circ y, x)$ for all $x, y \in A$;

(iii) $\theta p_i(x, y) = p_i(x\circ y, y) + p_i(y, x)$ for all $x, y \in A$.

Then we have,

(i) $p(x, x) = 0$ for all x;

(ii) $\theta p(x, y) = p(x\circ y, x)$ for all $x, y \in A$;

(iii) $\theta p(x, y) = p(x \circ y, y) + p(y, x)$ for all $x, y \in A$.

Thus, $< A; \circ >$ is a quaternary Mendelsohn quasigroup.

To prove $< A; \circ >$ is nilpotent of class m, it is sufficient to show that $\zeta(A) = \alpha := \{ < x, y > : x_i = y_i, \text{for } 1 \le i \le m \}$. For this it is enough to show that $b\ \zeta(A)\ 0$ iff $b_i = 0$ for $1 \le i \le m$.

By induction, A/α is nilpotent of class m-1 and $b_i = 0$ for $1 \le i \le m - 1$. Thus, we assume that $b = (0, \ldots, 0, b_m, b_{m+1})$ and let $b\ \zeta(A)\ 0$. By applying Lemma 7.19 with $r_1 = 0$ and $r_2 = b$ we have

$$x \circ y = (0 \circ b) \circ \{ \{ ((0 \circ b) \circ (x \circ 0)) \circ y \} \circ (b \circ 0) \}.$$

From the definition of $x \circ y$, we see that $x \circ y = \theta x + (1+\theta) y$ if either $x_1 = x_2 = 0$ or $y_1 = y_2 = 0$. Thus,

$$(0 \circ b) \circ \{ \{ ((0 \circ b) \circ (x \circ 0)) \circ y \} \circ (b \circ 0) \} = (b+x) \circ y + \theta b,$$

and so we must have

$$x \circ y = (b+x) \circ y + \theta b.$$

But,

$$(x \circ y)_{m+1} = \theta x_{m+1} + (1+\theta) y_{m+1} + (x_m + y_m + p_m(x, y))(x_1 y_2 + x_2 y_1),$$

while

$((b+x) \circ y + \theta b)_{m+1}$

$= \theta (b+x)_{m+1} + (1+\theta) y_{m+1} + ((b+x)_m + y_m + p_m(b+x, y)) ((b+x)_1 y_2 + (b+x)_2 y_1) + \theta b_{m+1}$

$= \theta x_{m+1} + (1+\theta) y_{m+1} + ((b_m + x_m + y_m + p_m(b+x, y))(x_1 y_2 + x_2 y_1).$

Note that since $(b+x)_i = b_i$ for $1 \le i \le m - 1$, $p_m(b+x, y) = p_m(x, y)$. Hence,

$(x \circ y)_{m+1} = ((b+x) \circ y + \theta b)_{m+1}$ iff $b_m (x_1 y_2 + x_2 y_1) = 0$. If we take $x_1 = y_2 = 1$ and $x_2 = y_1 = 0$, this then forces $b_m = 0$, as was to be proved.

Theorem 10.5. Let A be an m-dimensional vector space over GF(4) and $\Omega = A \times GF(4)$. Let $\langle A; \circ \rangle$ is subdirectly irreducible quaternary Mendelsohn quasigroup of class n with

$$x \circ y = \theta x + (1+\theta) y + p(x, y), \quad \text{where}$$

(i) $p_1(x, y) = p_2(x, y) = 0$;

(ii) $p_i(x, y) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1})$ for $2 \le i \le m$;

(iii) $p(x, y) = p(y, x)$;

(iv) $p(x, y) = 0$ if $x = 0$ or $y = 0$.

Define

$$(x, i) \circ (y, j) = (x \circ y, \theta i + (1+\theta) j + p_{m+1}(x, y)), \quad \text{where}$$

(v) $p_{m+1}(x, y) = (x_m + y_m + p_m(x, y))(x_1 y_2 + x_2 y_1)$.

Then $< \Omega; \circ >$ is a subdirectly irreducible quaternary Mendelsohn quasigroup of class n+1.

Proof. First it is readily checked that

(i) $p_{m+1}(x, x) = 0$;

(ii) $\theta p_{m+1}(x, y) = p_{m+1}(x \circ y, x)$;

(iii) $\theta p_{m+1}(x, y) = p_{m+1}(x \circ y, y) + p_{m+1}(y, x)$,

so $< \Omega; \circ >$ is a quaternary Mendelsohn quasigroup.

To prove $< \Omega; \circ >$ is subdirectly irreducible of class n+1, we only need to show

that if $b = (0, \ldots, 0, b_m, b_{m+1})$ and $b \zeta(\Omega) 0$ then $b_m = 0$.

By applying Lemma 7.19 with $r_1 = 0$ and $r_2 = b$ we have

$$x \circ y = (0 \circ b) \circ \{ \{ ((0 \circ b) \circ (x \circ 0)) \circ y \} \circ (b \circ 0) \}, \text{ and we have}$$

$$(b \circ 0) \circ \{(x \circ y) \circ (0 \circ b)\} = \{(0 \circ b) \circ (x \circ 0)\} \circ y.$$

Since

$$\{(0 \circ b) \circ (x \circ 0)\} \circ y$$

$$= \theta(b + x + p((1+\theta)b, \theta x) + (1+\theta)y + p(b + x + p((1+\theta)b, \theta x), y);$$

$$(b \circ 0) \circ \{(x \circ y) \circ (0 \circ b)\}$$

$$= \theta(\theta b) + (1+\theta)\{\theta(x \circ y) + (1+\theta)(1+\theta)b + p(x \circ y, (1+\theta)b) \};$$

and

$$p_{m+1}(x, y) = p_{m+1}(y, x) = 0 \text{ if } x_1 = x_2 = 0.$$

We have

$$p_{m+1}(x, y) = p_{m+1}(b + x + p((1+\theta)b, \theta x), y),$$

and then

$$b_m(x_1 y_2 + x_2 y_1) = 0,$$

and then

$$b_m = 0.$$

11. Recursive construction for solvable quaternary Mendelsohn quasigroups with maximal class

Theorem 11.1. Let $A = (GF(4))^m$ with $x \circ y = \theta x + (1+\theta)y + p(x, y)$. If

(i) $p_1(x, y) = 0$, and

(ii) for $k \geq 2$, $p_k(x, y) = (x_k + y_k)$ for $x_i = y_i = \theta$ and $i = 1, 2, \ldots, k-1$, and

$p_k(x, y) = 0$ otherwise,

then $\langle A; \circ \rangle$ is a solvable subdirectly irreducible quaternary Mendelsohn quasigroup of class m.

Proof. First it is readily checked that $\langle A; \circ \rangle$ is a solvable quaternary Mendelsohn quasigroup. We take $\alpha = 1_A$, $\beta = 1_A$,

$$x = (0, 0, 0, 0, \dots, 0), \qquad y = (\theta, 1, 0, 0, \dots, 0),$$

$$u = (0, 1, 0, 0, \dots, 0), \qquad s = (\theta, 0, 0, 0, \dots, 0),$$

$$v = (1, 1+\theta, 0, 0, \dots, 0), \qquad t = (1+\theta, \theta, 0, 0, \dots, 0).$$

We have,

$$(v, t)\circ\{(x, x)\circ(u, s)\} = ((\theta, 1+\theta, 0, 0, \dots, 0), (\theta, 1+\theta, 0, 0, \dots, 0)),$$

$$(v, t)\circ\{(y, y)\circ(u, s)\} = ((0, \theta, 0, 0, \dots, 0), (0, 1, 0, 0, \dots, 0)),$$

and then,

$$((\theta, 1+\theta, 0, 0, \dots, 0), (\theta, 1+\theta, 0, 0, \dots, 0))$$

$$\equiv ((0, \theta, 0, 0, \dots, 0), (0, 1, 0, 0, \dots, 0)) \quad (\Delta_\alpha^\beta),$$

and then,

$$(0, \theta, 0, 0, \dots, 0) [\alpha, \beta] (0, 1, 0, 0, \dots, 0), \text{ so}$$

$$(0, 0, 0, 0, \dots, 0) [\alpha, \beta] (0, a_2, 0, 0, \dots, 0) \text{ for } a_2 \in \{ 0, 1, 1+\theta, \theta \}.$$

We take

$$x = (0, 0, 0, 0, \dots, 0), \qquad y = (\theta, \theta, 1, 0, \dots, 0),$$

$$u = (0, 1, 0, 0, \dots, 0), \qquad s = (\theta, \theta, 0, 0, \dots, 0),$$

$$v = (1, 1+\theta, 0, 0, \dots, 0), \qquad t = (1+\theta, 0, 0, 0, \dots, 0).$$

We have

$$(v, t)\circ\{(x, x)\circ(u, s)\} = (\ (\theta, 1+\theta, 0, 0, \ldots, 0), (\theta, 1+\theta, 0, 0, \ldots, 0)\ ),$$

$$(v, t)\circ\{(y, y)\circ(u, s)\} = (\ (0, 1, \theta, 0, \ldots, 0), (0, 1, 1, 0, \ldots, 0)\ ),$$

and then,

$$(0, 1, \theta, 0, \ldots, 0)\ [\ \alpha,\ \beta\ ]\ (0, 1, 1, 0, \ldots, 0),$$

and then,

$$(0, a_2, 0, 0, \ldots, 0)\ [\ \alpha,\ \beta\ ]\ (0, a_2, a_3, 0, \ldots, 0)$$

for $a_2, a_3 \in \{ 0, 1, 1+\theta, \theta \}$;

.....

$$(0, a_2, a_3, a_4, \ldots, a_{m-1}, 0)\ [\ \alpha,\ \beta\ ]\ (0, a_2, a_3, a_4, \ldots, a_{m-1}, a_m)$$

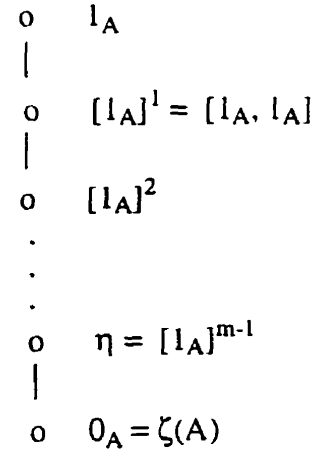
for $a_2, a_3, \ldots, a_m \in \{ 0, 1, 1+\theta, \theta \}$.

Hence

$$(0, 0, 0, 0, \ldots, 0)\ [\ \alpha,\ \beta\ ]\ (0, a_2, a_3, a_4, \ldots, a_{m-1}, a_m)$$

for $a_2, a_3, \ldots, a_m \in \{ 0, 1, 1+\theta, \theta \}$.

Therefore $\langle A; \circ \rangle$ is a solvable quaternary Mendelsohn quasigroup of class m. Similar to the proof of Theorem 8.4 we can show that it is subdirectly irreducible.



The lattice of all congruences on $< A, \circ >$

Chapter 4. Co-ordinatizations of Steiner Triple Systems

A Steiner triple system is a pair (X, B), where X is a set of elements (called points) and B is a collection of subsets of size three (called blocks) such that each pair of distinct points of X appears in exactly one block of B.

Steiner quasigroups and Steiner loops arise from the co-ordinatization of Steiner triple systems (see [2, 4, 11, 18, 19]). Guelzow [2, 4] presented a strenghtened version of the representation theorem given by Klossek [15] for finite distributive Steiner quasigroups and generalized this theorem to the class of all finite nilpotent Steiner quasigroups. He posed the following open questions:

(i) Are there any recursive constructions for nilpotent Steiner quasigroups that raise the nilpotence class ?

(ii) Are there any such constructions for distributive Steiner quasigroups ?

For the first question we will give a recursive constuction; the second question remains open. Similar results will be given for Steiner loops.

12. Steiner quasigroups

Definition 12.1. A *Steiner quasigroup* is an algebra which has a binary operation satisfying the following identities:

(i) $x \circ x = x$;

(ii) $x \circ y = y \circ x$;

(iii) $(x \circ y) \circ x = y$.

A Steiner quasigroup is called *distributive* if it satisfies the distributive law :

(iv) $(x \circ y) \circ z = (x \circ z) \circ (y \circ z)$.

A Steiner quasigroup is called *medial* if it satisfies the medial law :

(v) $(x \circ y) \circ (z \circ t) = (x \circ z) \circ (y \circ t)$.

Lemma 12.2. A Steiner quasigroup is a combinatorial quasigroup.

Lemma 12.3. Let A be an m-dimensional vector space over GF(3), and p a polynomial: $A^2 \rightarrow A$ over GF(3). Define $x \circ y = - x - y + p(x, y)$.

Then $A = < A ; \circ >$ is a Steiner quasigroup iff p(x, y) satisfies:

(i) $p(x, x) = 0$ for all x;

(ii) $p(x, y) = p(y, x)$ for all $x, y \in A$;

(iii) $p(x, y) = p(x \circ y, x)$ for all $x, y \in A$.

Proof. $x \circ x = x$ iff $p(x, x) = 0$;

$x \circ y = y \circ x$ iff $p(x, y) = p(y, x)$;

$(x \circ y) \circ x = y$ iff $p(x, y) = p(x \circ y, x)$.

Lemma 12.4. Let $< A, \circ >$ be a Steiner quasigroup. Then $a \, \zeta(A) \, b$ if and only if for all $x, y \in A$ the following equalities hold :

$$x \circ y = \{ b \circ \{ ((r_1 \circ x) \circ b) \circ ((r_2 \circ y) \circ b) \} \} \circ (r_1 \circ r_2)$$

for $r_1, r_2 \in \{a, b, a \circ b\}$. That is,

(i) $x \circ y = \{ b \circ \{ ((a \circ x) \circ b) \circ ((a \circ y) \circ b) \} \} \circ a$;

(ii) $x \circ y = \{ b \circ \{ ((a \circ x) \circ b) \circ y \} \} \circ (a \circ b)$;

(iii) $x \circ y = ((a \circ x) \circ b) \circ (((a \circ b) \circ y) \circ b)$;

(iv) $x \circ y = \{ b \circ \{ x \circ (((a \circ b) \circ y) \circ b) \} \} \circ a$;

(v) $x \circ y = \{ b \circ \{ (((a \circ b) \circ x) \circ b) \circ (((a \circ b) \circ y) \circ b) \} \} \circ (a \circ b)$.

Proof. Apply Corollary 2.13 with $p(x, y, z) = (x \circ y) \circ (z \circ x)$ and note that the only binary term functions are x, y, $x \circ y$. Notice that the equation with $(r_1, r_2) = (b, b)$ is always true and that for (b, a), $(a \circ b, a)$, $(a \circ b, b)$ are equivalent to these for (a, b), $(a, a \circ b)$, $(b, a \circ b)$, respectively.

Applying Theorem 5.2, Corollary 5.3 and Corollary 5.4 to Steiner quasigroups, Guelzow [2, 4] obtained the following theorem.

Theorem 12.5. Let $A = < A; \circ >$ be a finite Steiner quasigroup of nilpotence class k. Then there exists an m-dimensional vector space W, a polynomial $p: \Omega^2 \rightarrow \Omega$ over GF(3), and a sequence $1 \leq n_1 < \ldots < n_k = m$ of integers such that

(i) if $1 \leq s < k$ and $n_s < i \leq n_{s+1}$, then $p_i(x, y)$ does not depend on the variables $x_{n_s+1}, \ldots, x_m$ and $y_{n_s+1}, \ldots, y_m$;

(ii) $p_i(x, y) = 0$ for all $x, y \in \Omega$ and $1 \leq i \leq n_1$;

(iii) $\Omega = < \Omega; \circ >$ is isomorphic to A where $x \circ y = -x - y + p(x, y)$;

(iv) the center of A corresponds to the kernel of the projection onto the first n_{k-1} components of Ω. This projection is a homomorphism.

From Theorem 12.5 we have the following theorem.

Theorem 12.6. Let $A = \langle A; \circ \rangle$ be a finite Steiner quasigroup with order 3^m. Then $\langle A; \circ \rangle$ is nilpotent if and only if it is isomorphic to $\langle \Omega; \circ \rangle$, where Ω is an m-dimensional vector space over GF(3), $x \circ y = -x - y + p(x, y)$, such that

(i) $p_1(x, y) = 0$;

(ii) $p_i(x, y) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1})$ for $2 \le i \le m$;

(iii) $p(x, x) = 0$, $p(x, y) = p(y, x)$ and $p(x, y) = p(x \circ y, x)$ for all $x, y \in \Omega$.

Theorem 12.6 is equivalent to the following Generalized Tripling Construction:

Theorem 12.7. (Generalized Tripling Construction). Let $\langle A; \circ \rangle$ be a nilpotent Steiner quasigroup of class n with order 3^m. Let B_0, B_1, B_2 be a partition of the set of all 3-element subalgebras of A, $\Omega = A \times GF(3)$. Define

$$(x, i) \circ (y, j) = (x \circ y, \; i + j + \lambda(x, y)),$$

where $\lambda(x,y) = 0$ if $x = y$ or $Sg\{x, y\} \in B_0$;

$\lambda(x,y) = 1$ if $Sg\{x, y\} \in B_1$;

$\lambda(x,y) = 2$ if $Sg\{x, y\} \in B_2$.

Then $\langle \Omega; \circ \rangle$ is a nilpotent Steiner quasigroup of class $n+1$ or n.

Theorem 12.8. A finite Steiner quasigroup is nilpotent if and only if it is isomorphic to a Steiner quasigroup obtained from the 3-element Steiner quasigroup by repeated application of Generalized Tripling Construction.

The following lemma can be easily proved from Theorem 12.7.

Lemma 12.9. Let $A = (GF(3))^2$. Define

$$x \circ y = (- x_1 - y_1, \ - x_2 - y_2 + p_2(x_1, y_1))$$

such that $< A, \circ >$ is a Steiner quasigroup. Then $p_2(x_1, y_1) = c\,(x_1 - y_1)^2$ where $c \in$ GF(3), and then $< A, \circ >$ is medial. In fact, it is well known and easy to show that there is up to isomorphism only one Steiner quasigroup of size 9, namely the affine plane over GF(3).

Let $A = (GF(3))^3$. Define $x \circ y = (- x_1 - y_1, \ - x_2 - y_2, \ - x_3 - y_3 + p_3(x_1, x_2; y_1, y_2))$. In the following we give some special polynomials $p_3(x_1, x_2; y_1, y_2)$ such that $< A, \circ >$ is a Steiner quasigroup.

Example 12.10. $p_3(x_1, x_2; y_1, y_2) = x_2\, y_2(1 + x_2\, y_2)(x_1 - y_1)^2$ for which the distributive law does not hold.

Proof. Since $z \circ (x \circ y) \neq (z \circ x) \circ (z \circ y)$ for $z = (0, 1, 0)$, $x = (1, 0, 0)$, $y = (1, 1, 0)$.

Example 12.11. $p_3(x_1, x_2; y_1, y_2) = x_2\, y_2(x_2 + y_2)(x_1 - y_1)^2$ for which the distributive law does not hold.

Proof. Since $z \circ (x \circ y) \neq (z \circ x) \circ (z \circ y)$ for $z = (0, 1, 0)$, $x = (1, 0, 0)$, $y = (1, 1, 0)$.

Example 12.12. (Guelzow [2]). $p_3(x_1, x_2; y_1, y_2) = x_2\, y_2(1 + x_2)(1 + y_2)(x_1 - y_1)^2$ for which the distributive law does not hold.

Proof. Since $z \circ (x \circ y) \neq (z \circ x) \circ (z \circ y)$ for $z = (0, 1, 0)$, $x = (1, 0, 0)$, $y = (1, 1, 0)$.

Example 12.13. $p_3(x_1,x_2; y_1,y_2) = (x_1 - y_1)(x_2 - y_2)$ for which the distributive law holds.

Example 12.14. $p_3(x_1,x_2; y_1,y_2) = (x_1 - y_1)(x_1y_2 - x_2y_1)$ for which the distributive law holds.

It is known that the only distributive Steiner quasigroups of size 27 are also medial and so isomorphic to the 3-dimensional affine geometry over GF(3).

Example 12.15. $p_3(x_1,x_2; y_1,y_2) = (x_2 - y_2)^2 (x_1 - y_1)^2$ for which the distributive law does not hold.

Proof. Since $z \circ (x \circ y) \neq (z \circ x) \circ (z \circ y)$ for $z = (0, 1, 0)$, $x = (1, 0, 0)$, $y = (1, 1, 0)$.

Lemma 12.16. Let A be a 3-dimensional vector space over GF(3).
Let $x \circ y = -x - y + p(x, y)$ and $p_1(x, y) = p_2(x, y) = 0$.

If $p_3(x, y) = [\alpha (x_2 - y_2)^2 + \beta x_2 y_2(1 + x_2 y_2) + \kappa x_2 y_2(x_2 + y_2)] (x_1 - y_1)^2$.

where $\alpha \neq 0$ or $\beta \neq 0$ or $\kappa \neq 0$, then $A = \langle A; \circ \rangle$ is a subdirectly irreducible nilpotent Steiner quasigroup of class 2.

Proof. From Example 12.10, Example 12.11 and Example 12.15, we have $\langle A; \circ \rangle$ is a nilpotent Steiner quasigroup.

To prove $\langle A; \circ \rangle$ is subdirectly irreducible nilpotent of class 2, it is sufficient to show that $\zeta(A) = \alpha = \{ \langle x, y \rangle : x_i = y_i \text{ for } 1 \leq i \leq 2 \}$. For this we only need to show that the distributive law holds iff $\alpha = \beta = \kappa = 0$.

We take $x = (1, 0, 0)$, $y = (-1, 1, 0)$ and $z = (0, 1, 0)$. From $(x \circ z) \circ y = (x \circ y) \circ (z \circ y)$, we have $\alpha + \beta + \kappa = 0$; From $(y \circ z) \circ x = (y \circ x) \circ (z \circ x)$, we have $\alpha + \beta = 0$.

We take $x = (1, 0, 0)$, $y = (1, 1, 0)$ and $z = (0, -1, 0)$. From $(y \circ z) \circ x = (y \circ x) \circ (z \circ x)$, we have $\alpha = 0$. Hence $\alpha = \beta = \kappa = 0$.

Theorem 12.17. Let A be an $(m+1)$-dimensional vector space over GF(3) with

$$x \circ y = -x - y + p(x, y).$$

Let $\alpha \neq 0$ or $\beta \neq 0$ or $\kappa \neq 0$ and define

$$r(x_1, y_1) = \alpha (x_1 - y_1)^2 + \beta x_1 y_1 (1 + x_1 y_1) + \kappa x_1 y_1 (x_1 + y_1);$$

$$p_1(x, y) = p_2(x, y) = 0;$$

$$p_k(x, y) = r(x_1, y_1)(x_{k-1} - y_{k-1})^2 [1 - p_{k-1}(x, y)^2] \quad \text{for} \quad 3 \leq k \leq m+1.$$

Then $< A; \circ >$ is a subdirectly irreducible nilpotent Steiner quasigroup of class m.

Proof. By induction, it is readily checked that for $1 \leq i \leq m+1$, for all $x, y \in A$,

(i) $p_i(x, x) = 0$;

(ii) $p_i(x, y) = p_i(y, x)$;

(iii) $p_i(x, y) = p_i(x \circ y, x)$.

Then we have, for all $x, y \in A$,

(i) $p(x, x) = 0$;

(ii) $p(x, y) = p(y, x)$;

(iii) $p(x, y) = p(x \circ y, x)$;

Thus, $< A; \circ >$ is a nilpotent Steiner quasigroup.

To prove $< A; \circ >$ is subdirectly irreducible nilpotent of class m, it is sufficient to show that $\zeta(A) = \{ < x, y > : x_i = y_i \text{ for } 1 \le i \le m \}$. For this we only need to show that $< 0, b > \in \zeta(A)$ iff $b_i = 0$ for $1 \le i \le m$. By induction, we may assume that $b_i = 0$ for $1 \le i \le m - 1$.

Let $b = (0, \ldots, 0, b_m, b_{m+1})$ and $< 0, b > \in \zeta(A)$. From (iii) of Lemma 12.4 we have

$$x \circ y = [(0 \circ x) \circ b] \circ [((0 \circ b) \circ y) \circ b] \quad \text{for all } x, y \in A, \text{ that is,}$$

$$(*) \qquad (x \circ y) \circ \{ (0 \circ x) \circ b \} = ((0 \circ b) \circ y) \circ b \qquad \text{for all } x, y \in A$$

Taking $x = 0$, $y = (1, 0, \ldots, 0)$ we have

$$(x \circ y) \circ \{ (0 \circ x) \circ b \} = (0 \circ y) \circ \{ (0 \circ 0) \circ b \} = (0 \circ y) \circ \{ 0 \circ b \} = \{-y + p(0, y)\} \circ \{-b+p(0, b)\}$$

$$= (-y) \circ \{-b \} = y + b + p(-y, -b)$$

$$[((0 \circ b) \circ y) \circ b] = (-b + p(0, b)) \circ y) \circ b = (-b) \circ y) \circ b = (b -y + p(-b, y)) \circ b$$

$$= (-b +y - p(-b, y) \ -b \ + p(b -y + p(-b, y), b)$$

$$= y \ + b - p(-b, y) + p(b -y, b)$$

$$= y \ + b - p(-b, y)$$

From the equation (*), we have

$$p_{m+1}(-y, -b) + p_{m+1}(-b, y) = 0;$$

that is,

$$\alpha \, b_m^{\,2} = 0.$$

If $\alpha \neq 0$ then $b_m = 0$.

If $\alpha = 0$, taking $x = y$ we have

$$(x \circ y) \circ \{ (0 \circ x) \circ b \} = x \circ \{ (0 \circ x) \circ b \} = x \circ \{ (- x + p(0, y)) \circ b \}$$

$$= x \circ \{ (- x) \circ b \} \quad \text{since } \alpha = 0,\ r(0, y_1) = 0$$

$$= x \circ \{ (x - b + p(-x, b)) \}$$

$$= x \circ (x - b) \qquad \text{since } \alpha = 0,\ r(-x_1, 0) = 0$$

$$= - x - x + b + p(x, x-b)$$

$$= x + b + p(x, x-b)$$

$$[((0 \circ b) \circ y) \circ b] = (-b + p(0, b)) \circ y) \circ b = (-b) \circ y) \circ b = (b - y + p(-b, y)) \circ b$$

$$= (b - y) \circ b \quad \text{since } \alpha = 0,\ r(0, y_1) = 0$$

$$= -b + y - b + p(b - y, b)$$

$$= y + b \qquad \text{since } \alpha = 0,\ r(-y_1, 0) = 0$$

$$= x + b$$

From the equation (*), we have

$$p_{m+1}(x, x-b) = 0$$

that is,

$$r(x_1, x_1)\, b_m^2 = 0$$

that is

$$[\, \beta\, x_1^2\, (1 + x_1^2) - \kappa\, x_1 \,]\, b_m^2 = 0.$$

By taking $x_1 = 1$ or -1, we have

$$\beta b_m^2 = \kappa\, b_m^2 = 0;$$

since $\alpha \neq 0$ or $\beta \neq 0$ or $\kappa \neq 0$, we have $b_m = 0$.

On the other hand it is readily checked that $< 0, b > \in \zeta(A)$ for $b = (0, \ldots, 0, 1)$ by Lemma 12.4. Therefore we have completed the proof.

Theorem 12.18. Let A be an m-dimensional vector space over GF(3) and Ω = $A \times GF(3)$. Let $\langle A; \circ \rangle$ be a subdirectly irreducible Steiner quasigroup of class n with

$$x \circ y = - x - y + p(x, y),$$

where

(i) $p_1(x, y) = 0$;

(ii) $p_i(x, y) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1})$ for $2 \le i \le m$;

(iii) $p(x, y) = 0$ if $x_i = 0$ for $2 \le i \le m$.

Define

$$(x, i) \circ (y, j) = (x \circ y, -i -j + p_{m+1}(x, y)),$$

where

(iv) $p_{m+1}(x, y) = x_1 y_1 (x_1 + y_1)(x_m - y_m)^2 [1 - p_m(x, y)^2]$.

Then $\langle \Omega; \circ \rangle$ is a subdirectly irreducible nilpotent Steiner quasigroup of class n+1.

Proof. The proof is similar to that of Theorem 12.17.

13. Steiner loops

Definition 13.1. An *algebraic loop* is an algebraic quasigroup with identity.

A *combinatorial loop* is a combinatorial quasigroup with identity.

Definition 13.2. A *Steiner loop* is an algebra that has a binary operation " $\oplus$ " with identity 0 satisfying the following identities:

(i) $x \oplus x = 0$;

(ii) $x \oplus 0 = 0 \oplus x = x$;

(iii) $x \oplus y = y \oplus x$;

(iv) $x \oplus (x \oplus y) = y$.

Lemma 13.3. A Steiner loop is a combinatorial loop.

Lemma 13.4. (Quackenbush [19]). Let $< A, \oplus, 0 >$ be a Steiner loop. Then a $\zeta(A)$ 0 if and only if for all $x, y \in A$, $\{a, x, y\}$ generates an associative subloop of A.

Proof. Apply Corollary 2.1.10 with $p(x, y, z) = (x \oplus y) \oplus z$ and the only binary term functions are $x, y, x \oplus y$.

Lemma 13.5. Let $< A, \oplus, 0 >$ be a Steiner loop. The following are equivalent :

(i) $< A, \oplus, 0 >$ is abelian;

(ii) $< A, \oplus, 0 >$ satisfies the medial law;

(iii) $< A, \oplus, 0 >$ satisfies $(x \oplus y) \oplus (x \oplus z) = y \oplus z$;

(iv) $< A, \oplus, 0 >$ satisfies $x \oplus (y \oplus z) = (x \oplus y) \oplus z$.

Similar to finite nilpotent Steiner quasigroups, we have

Theorem 13.6. Let $A = < A, \oplus, 0 >$ be a finite Steiner loop with order 2^m. Then $< A, \oplus, 0 >$ is nilpotent if and only if it is isomorphic to $< \Omega, \circ, 0 >$, where Ω is an m-dimensional vector space over GF(2), $x \circ y = x + y + p(x, y)$, such that

(i) $p_1(x, y) = 0$;

(ii) $p_i(x, y) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1})$ for $2 \leq i \leq m$;

(iii) $p(x, 0) = p(x, x) = 0$, $p(x, y) = p(y, x)$ and $p(x, y) = p(x \circ y, x)$ for all $x, y \in \Omega$.

The following Generalized Doubling Construction is classical.

Theorem 13.7. (Generalized Doubling Construction). Let $\langle A;\ \oplus, 0\rangle$ be a Steiner loop and B a set of 4-element subalgebras of A . Let λ be the characteristic function of B, $\Omega = A \times GF(2)$, and $(x, i)\circ(y, j) = (\ x\oplus y,\ \ i + j + \lambda(Sg\{x, y\})\ )$. Then $\langle\Omega;\ \circ, 0\rangle$ is a sloop. Moreover, if $\langle A;\ \oplus, 0\rangle$ is nilpotent of class n, then $\langle\Omega;\ \circ, 0\rangle$ is nilpotent of class n or n+1; and ker (π) is a congruence on Ω and contained in its center, where π is the projection of Ω onto A.

From Theorem 13.6 and Theorem 13.7, we have

Theorem 13.8. A finite Steiner loop is nilpotent if and only if it is isomorphic to a Steiner loop obtained from the 2-element Steiner loop by repeated application of the Generalized Doubling Construction.

Lemma 13.9. Let A be a 2-dimensional vector space over GF(2). Let

$$x\oplus y = x + y + p(x, y) \text{ and } p_1(x, y) = 0.$$

If $< A, \oplus, 0 >$ is a Steiner loop, then $p_2(x, y) = 0$; that is, $< A, \oplus, 0 >$ is abelian.

Lemma 13.10. Let A be a 3-dimensional vector space over GF(2). Let

$$x\oplus y = x + y + p(x, y) \text{ and } p_1(x, y) = p_2(x, y) = 0.$$

If $< A, \oplus, 0 >$ is a Steiner loop. Then $p_3(x, y) = 0$, or $p_3(x, y) = x_1y_2 + x_2y_1$; that is, $< A, \oplus, 0 >$ is abelian.

It is well known that all Steiner loops of size ≤ 8 are abelian.

Theorem 13.11. Let A be an (m+2)-dimensional vector space over GF(2) with $x \oplus y = x + y + p(x, y)$. Let $p(x, y)$ be as follows:

(i) $p_1(x, y) = p_2(x, y) = 0$;

(ii) $p_3(x, y) = r(x, y) = x_1y_2 + x_2 y_1$;

(iii) $p_{k+2}(x, y) = (x_{k+1}y_{k+1})\,(x_ky_k) \ldots (x_3y_3)\, r(x, y)$ for $2 \le k \le m$.

Then $< A, \oplus, 0 >$ is a subdirectly irreducible nilpotent Steiner loop of class m.

Proof. See the proof of Theorem 16.4.

Note the construction in Thereom 13.11 can be viewed as a special case of the Generalized Doubling Construction. To see this, let A_0 be a 2-dimensional vector space over GF(2) with $x \circ_0 y = x + y$, and

$$B_0 = \{ (0, 0), (0, 1), (1, 0), (1, 1) \},$$

$$B_1 = \{ (0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 1) \}, \quad \text{for } 2 \le k \le m,$$

$$B_k = \{ (0, 0, \ldots 0), (0, 1, \ldots, 1), (1, 0, 1, \ldots, 1), (1, 1, \ldots 1) \}.$$

Chapter 5. Co-ordinatizations of Steiner Quadruple Systems

Armanious and Guelzow [1, 3] obtained structure theorems for finite nilpotent Steiner skeins. Guelzow [3] gave a construction of a Steiner skein of nilpotence class n with all derived Steiner loops of nilpotence class 1. Armanious [1] gave a construction for Steiner skeins of nilpotence class n with all its derived Steiner loops of nilpotence class n. In this chapter we survey the main results on nilpotent Steiner skeins and give a new and simple construction, in polynomial form, for Steiner skeins of nilpotence class n with all its derived Steiner loops of nilpotence class n.

14. Steiner skeins

Definition 14.1. A *Steiner quadruple system* is a pair (X, B), where X is a set of elements (called points) and B is a collection of subsets of size four (called blocks) such that each 3-subset of X appears in exactly one block of B.

Definition 14.2. A *Steiner skein* is an algebra which has a ternary operation ρ satisfying the following identities:

(i) $\rho(x, x, y) = y$;

(ii) $\rho(x, y, z) = \rho(x, z, y)$, $\rho(x, y, z) = \rho(y, z, x)$;

(iii) $\rho(x, y, \rho(x, y, z)) = z$.

It is well known that there is a one-to-one correspondence between Steiner quadruple systems and Steiner skeins (see [20]).

Definition 14.3. (Quackenbush). A Steiner skein is called *semi-boolean* if it satisfies the additional equation:

(iv) $\rho(x, u, \rho(y, u, z)) = \rho(\rho(x, u, y), u, z)$.

Definition 14.4. A Steiner skein is called *boolean* if it satisfies the additional equation:

(v) $\rho(x, u, \rho(y, u, z)) = \rho(x, y, z)$.

A Steiner skein is boolean iff it is nilpotent of class 1, and is semi-boolean. A Steiner skein is semi-boolean iff every derived Steiner loop is boolean (see [2, 3]).

Since the ternary operation ρ of Steiner skeins itself is a Mal'cev term, the variety of all Steiner skeins is permutable and then modular. From Corollary 2.13 we have the following lemma.

Lemma 14.5. Let $< A, \rho >$ be a Steiner skein. Then $a\ \zeta(A)\ b$ if and only if for all $x, y, z \in A$, the following equality holds :

$$\rho(\rho(a, b, x), y, z) = \rho(a, b, \rho(x, y, z)).$$

It is easy to see that the congruences of a finite Steiner skein are regular and uniform, that is, any congruence is uniquely determined by any of its congruence classes, and any two congruence classes of the same congruence have the same size. Hence by Lemma 6.5, we have

Lemma 14.6. Let $< A, \rho >$ be a finite nilpotent Steiner skein of order. Then $< A, \rho >$ is subdirectly irreducible if and only if $\zeta(A)$ is a congruence with class size 2.

15. Representation of finite nilpotent Steiner skeins

Applying Definition 5.1, Theorem 5.2, Corollary 5.3 and Corollary 5.4 to Steiner skeins, Guelzow [2, 3] stated the following theorem.

Theorem 15.1. Let $A = < A; \rho >$ be a finite Steiner skein of nilpotence class k with order 2^m. Then there exists an m-dimensional vector space W, a polynomial $p: \Omega^3 \rightarrow \Omega$ over GF(2), and a sequence $1 \leq n_1 < \ldots < n_k = m$ of integers such that

(i) if $1 \leq s < k$ and $n_s < i \leq n_{s+1}$, then $p_i(x, y)$ does not depend on the variables $x_{n_s+1}, \ldots, x_m$ and $y_{n_s+1}, \ldots, y_m$;

(ii) $p_i(x, y, z) = 0$ for all $x, y, z \in \Omega$ and $1 \leq i \leq n_1$;

(iii) $\Omega = < \Omega; \tau >$ is isomorphic to A where $\tau(x, y, z) = x + y + z + p(x, y, z)$;

(iv) the center of A corresponds to the kernel of the projection onto the first n_{k-1} components of Ω. This projection is a homomorphism.

(v) A is subdirectly irreducible if and only if $n_{k-1} = m - 1$.

From Theorem 15.1 we have

Theorem 15.2. Let $< A; \rho >$ be a finite Steiner skein with order 2^m. Then $< A; \rho >$ is nilpotent if and only if it is isomorphic to $< \Omega; \tau >$, where Ω is an m-dimensional vector space over GF(2) and $\tau(x, y, z) = x + y + z + p(x, y, z)$. such that

(i) $p_1(x, y, z) = 0$;

(ii) $p_i(x, y, z) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1}, z_1, \ldots, z_{i-1})$ for $2 \le i \le m$;

(iii) $p(x, x, y) = 0$, $p(x, y, z) = p(x, z, y) = p(y, z, x)$, $p(x, y, z) = p(x, y, \rho(x,y, z))$.

Theorem 15.3. (Generalized Doubling Construction). Let $\langle A; \rho \rangle$ be a Steiner skein and B a set of 4-element subalgebras of A. Let λ be the characteristic function of B, $\Omega = A \times GF(2)$, and $\tau((x, i), (y, j), (z, k)) = (\rho(x, y, z), \ i + j + k + \lambda(Sg\{x, y, z\}))$. Then $\langle \Omega; \tau \rangle$ is a Steiner skein. Moreover, if $\langle A; \rho \rangle$ is nilpotent of class n, then $\langle \Omega; \tau \rangle$ is nilpotent of class n or n +1; and ker (π) is a congruence on Ω and contained in its center, where π is the projection of Ω onto A.

Theorem 15.4. A finite Steiner skein is nilpotent if and only if it is isomorphic to a Steiner skein obtained from the 2-element Steiner skein by repeated application of the generalized doubling construction.

16. Recursive construction for Steiner skeins of nilpotence class n with all derived Steiner loops of nilpotence class n

The following is a construction of a Steiner skein of nilpotence class n with all derived Steiner loops of nilpotence class 1 given by Guelzow [3].

Theorem 16.1. Let $\langle A; \rho \rangle$ be a Steiner skein and B a set of all 4-element subalgebras of A. Let λ be the characteristic function of B, and $\Omega = A \times GF(2)$, Define

$$\tau((x, i), (y, j), (z, k)) = (\rho(x, y, z), \quad i + j + k + \lambda(Sg\{x, y, z\})).$$

Then $\langle \Omega; \tau \rangle$ is a Steiner skein. If $\langle A; \rho \rangle$ is semi-boolean then $\langle \Omega; \tau \rangle$ is semi-boolean. Moreover, if $\langle \Omega; \tau \rangle$ is subdirectly irreducible and nilpotent of class n+1 if and only if $\langle A; \rho \rangle$ nilpotent of class n.

The following is an example of a Steiner skein of nilpotence class 2 with all its derived Steiner loops of nilpotence class 2 given by Armanious [1].

Lemma 16.2. Let A be a 4-dimensional vector space over GF(2). Define

$$\rho(x, y, z) = x + y + z + p(x, y, z);$$

$$r(x, y, z) = x_1y_2 + y_1z_2 + z_1x_2 + x_1z_2 + y_1x_2 + z_1y_2;$$

$$p_1(x, y, z) = p_2(x, y, z) = p_3(x, y, z) = 0;$$

$$p_4(x, y, z) = r(x, y, z)(x_3 + y_3 + z_3 + x_3y_3 + y_3z_3 + z_3x_3).$$

Then $< A; \rho >$ is a subdirectly irreducible nilpotent Steiner skein of class 2 with all its derived Steiner loops of nilpotence class 2.

Theorem 16.3. (Armanious [1]). Let $\langle A; \rho \rangle$ be a finite subdirectly irreducible nilpotent Steiner skein of class n with all its derived Steiner loops of nilpotence class n. Let

$$A = \{ z_i : 0 \le i \le 2^{m-1} - 1 \}, \quad \Omega = A \times GF(2),$$

$$[z_{2i}]\ \zeta(A) = \{z_{2i}, z_{2i+1}\}, \quad B = \{ \{z_{4i}, z_{4i+1}, z_{4i+2}, z_{4i+3}\} : 0 \le i \le 2^{m-2} - 1 \},$$

λ be the characteristic function of B,

$$\tau((x, i), (y, j), (z, k)) = (\rho(x, y, z), \quad i + j + k + \lambda(Sg\{x, y, z\})).$$

Then $\langle \Omega; \tau \rangle$ is subdirectly irreducible and nilpotent of class n+1 with all its derived Steiner loops of nilpotence class n+1.

In the following we give a new and simple construction in the form of polynomials.

Theorem 16.4. Let A be an (m+2)-dimensional vector space over GF(2) with $\rho(x, y, z) = x + y + z + p(x, y, z)$. Define

$r(x, y, z) = x_1y_2 + y_1z_2 + z_1x_2 + x_1z_2 + y_1x_2 + z_1y_2$;

$p_1(x, y, z) = p_2(x, y, z) = 0$;

$p_3(x, y, z) = r(x, y, z)$;

$p_{k+1}(x, y, z) = p_k(x, y, z)(x_ky_k + y_kz_k + z_kx_k)$ for $3 \le k \le m+1$.

Then $< A; \rho >$ is a subdirectly irreducible nilpotent Steiner skein of class m with all its derived Steiner loops of nilpotence class m.

Proof. First we show that $< A; \rho >$ is a Steiner skein. It is easy to see that $r(x, x, y) = 0$; so we have $\rho(x, x, y) = y$. Clearly, $\rho(x, y, z) = \rho(x, z, y) = \rho(y, z, x)$. To show $\rho(x, y, \rho(x, y, z)) = z$, we only need to show $p_i(x, y, z) = p_i(x, y, \rho(x, y, z))$ for $1 \le i \le m+2$.

Clearly it is true for i = 1, 2. Since $\rho_1(x, y, z) = x_1 + y_1 + z_1$ and $\rho_2(x, y, z) = x_2 + y_2 + z_2$, we have $p_3(x, y, z) = p_3(x, y, \rho(x, y, z))$; that is, it is true for i = 3.

Assume that it is true for $i = k (\ge 3)$, then

$$\begin{aligned} p_{k+1}(x, y, \rho(x, y, z)) &= p_k(x, y, \rho(x, y, z))(x_ky_k + y_k\rho_k(x, y, z) + \rho_k(x, y, z)x_k) \\ &= p_k(x, y, z)(x_ky_k + (y_k + x_k)(x_k + y_k + z_k + p_k(x, y, z)) \\ &= p_k(x, y, z)(x_ky_k + y_kz_k + z_kx_k) = p_{k+1}(x, y, z). \end{aligned}$$

Hence $< A; \rho >$ is a nilpotent Steiner skein.

To prove $A = \langle A; \rho \rangle$ is nilpotent of class m, it is sufficient to show that $\zeta(A) = \{\langle x, y \rangle : x_i = y_i, \text{ for } 1 \le i \le m+1 \}$. For this we only need to show that if $b\ \zeta(A)\ 0$ then $b_i = 0$ for $1 \le i \le m+1$.

Let $b = (b_1, b_2, \ldots, b_{m+2})$ and $0\ \zeta(A)\ b$. From Lemma 14.5, we have

$$(*) \qquad \rho(\rho(0, b, x), y, z) = \rho(0, b, \rho(x, y, z)) \quad \text{for all } x, y, z \in A.$$

Taking $x_1 = x_2 = x_3 = 0$, $y_1 = y_2 = 0$ and $y_3 = z_3 = 1$, we have $b_1z_2 + b_2z_1 = 0$ since $\rho_4(\rho(0, b, x), y, z) = \rho_4(0, b, \rho(x, y, z))$, and then $b_1 = b_2 = 0$.

Assume $b = (0, \ldots, 0, b_{m+1}, b_{m+2})$ and $0\ \zeta(A)\ b$. We have

$$\begin{aligned}
\rho(\rho(0, b, x), y, z) &= \rho(0, b, x) + y + z + p(\rho(0, b, x), y, z) \\
&= b + x + p(0, b, x) + y + z + p(\rho(0, b, x), y, z) \\
&= b + x + y + z + p(b+x, y, z) \quad (\text{since } b_1 = b_2 = 0, \ r(0, b, y) = 0); \\
\rho(0, b, \rho(x, y, z)) &= b + \rho(x, y, z) + p(0, b, \rho(x, y, z)) \\
&= b + \rho(x, y, z) \quad (\text{since } b_1 = b_2 = 0, \ r(0, b, \rho(x, y, z)) = 0) \\
&= b + x + y + z + p(x, y, z).
\end{aligned}$$

From the equation $(*)$, we have

$$p_{m+2}(b+x, y, z) = p_{m+2}(x, y, z)$$

and then,

$$b_{m+1} = 0.$$

Finally, we show that all its derived Steiner loops are of nilpotence class m. Let $c \in A$, we define $x \oplus y = \rho(x, y, c)$ for all $x, y \in A$, and we show that $\langle A; \oplus, c \rangle$ is nilpotent of class m. It is sufficient to show that

$$\zeta(A) = \{ < x, y > : x_i = y_i \text{ for } 1 \le i \le m+1 \}.$$

For this we only need to show that if $b\ \zeta(A)\ 0$ then $b_i = 0$ for $1 \le i \le m+1$.

Let $b = (b_1, b_2, \ldots, b_{m+2})$ and $c\ \zeta(A)\ b$. From Lemma 13.4, we have

$$(x \oplus y) \oplus b = x \oplus (y \oplus b) \quad \text{for all } x, y \in A.$$

that is,

$$(**) \qquad \rho(\rho(x, y, c), b, c) = \rho(x, c, \rho(y, b, c)) \quad \text{for all } x, y \in A.$$

Taking $x_1 = y_1$, $x_2 = y_2$ and $x_3 = y_3 = 1 + c_3$, we have $r(y, b, c) = 0$ since $\rho_4(\rho(x, y, c), b, c) = \rho_4(x, c, \rho(y, b, c))$, and then $b_1 = c_1$ and $b_2 = c_2$.

Assume $b = (c_1, \ldots, c_m, b_{m+1}, b_{m+2})$ and $0\ \zeta(A)\ b$. We have

$$\begin{aligned}\rho(\rho(x, y, c), b, c) &= \rho(x, y, c) + b + c + p(\rho(x, y, c), b, c) \\ &= x + y + c + p(x, y, c) + b + c + p(\rho(x, y, c), b, c) \\ &= x + y + b + p(x, y, c) \qquad \text{since} \quad (b_1, b_2) = (c_1, c_2),\end{aligned}$$

and then $r(\rho(x, y, c), b, c) = 0$;

$$\begin{aligned}\rho(x, c, \rho(y, b, c)) &= \rho(y, b, c) + x + c + p(\rho(y, b, c), x, c) \\ &= x + y + c + p(y, b, c) + b + c + p(\rho(y, b, c), x, c) \\ &= x + y + b + p(\rho(y, b, c), x, c) \qquad \text{since} \quad (b_1, b_2) = (c_1, c_2),\end{aligned}$$

and then $r(\rho(x, y, c), b, c) = 0$;

From the equation (**), we have

$$p_{m+2}(x, y, c) = p_{m+2}(\rho(y, b, c), x, c) \quad \text{for all } x, y \in A.$$

that is,

$$p_{m+1}(x, y, c)((b_{m+1} + c_{m+1})(c_{m+1} + x_{m+1}) = 0 \quad \text{for all } x, y \in A.$$

this forces $b_{m+1} = c_{m+1}$.

Theorem 16.5. Let A be an (m+1)-dimensional vector space over GF(2) and $\Omega = A \times GF(2)$. Let $\langle A; \rho \rangle$ be a nilpotent Steiner skein with

$\rho(x, y, z) = x + y + z + p(x, y, z)$ and

(i) $p_1(x, y, z) = 0$ and

(ii) $p_i(x, y, z) = p_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{i-1}, z_1, \ldots, z_{i-1})$ for $2 \leq i \leq m+1$.

Then $< \Omega; \tau >$ is a nilpotent Steiner skein, where

$\tau((x, i), (y, j), (z, k)) = (\rho(x, y, z), i + j + k + p_{m+2}(x, y, z))$ and

(iii) $p_{m+2}(x, y, z) = p_{m+1}(x, y, z)(x_{m+1}y_{m+1} + y_{m+1}z_{m+1} + z_{m+1}x_{m+1})$.

Furthermore, if $\langle A; \rho \rangle$ is subdirectly irreducible Steiner skein of class n with all its derived Steiner loops subdirectly irreducible and of nilpotence class n, then $\langle \Omega; \tau \rangle$ is subdirectly irreducible and nilpotent of class n+1 with all its derived Steiner loops subdirectly irreducible and of nilpotence class n+1.

Proof. The proof is similar to that of Theorem 16.4.

Chapter 6. *p*-Groups

General representation theorem for finite nilpotent groups and some examples of representations of finite *p*-groups for $p = 2$ with small order have been given by Guelzow in [2]. In this chapter, we will represent the dihedral group D_{2n} and the generalized quaternion group Q_{2n} which have maximal class, by recursive construction.

17. Definitions and basic results

The following definitions and results can be found in [21].

Definition 17.1. If p is a prime, then a *p-group* is a group in which every element has order a power of p.

Lemma 17.2. A finite group is a *p*-group if and only if the order of G is a power of p.

Lemma 17.3. If $G \neq \{e\}$ is a finite *p*-group, then its center $Z(G) \neq \{e\}$.

Lemma 17.4. If p is a prime, then every group G of order p^2 is abelian.

Lemma 17.5. If p is a prime and G is a non abelian group G of order p^3, then $|Z(G)| = p$, $G/Z(G) \cong Z_p \times Z_p$.

Theorem 17.6. Every finite *p*-group is nilpotent.

Definition 17.7. A group G is said to be a *torsion* group if every $g \in G$ has a finite order.

Definition 17.8. The *quaternions* is a group Q of order 2^3 generated by elements a and b such that $a^4 = e$, $b^2 = a^2$ and $ba = a^3b$.

Definition 17.9. If $n \geq 3$, a *generalized quaternion* group Q_{2^n} is a group of order 2^n generated by elements a and b such that $a^{2^{n-1}} = e$, $b^2 = a^{2^{n-2}}$ and $ba = a^{-1}b$.

Definition 17.10. If $n \geq 1$, a *dihedral* group D_{2^n} is a group of order 2^n generated by elements a and b such that $a^{2^{n-1}} = e$, $b^2 = e$ and $ba = a^{-1}b$.

Lemma 17.11. $Q_{2^n}/Z(Q_{2^n}) \equiv D_{2^{n-1}}$.

Lemma 17.12. Let G be a non empty finite set with an associative binary operation such that for all $a, b, c \in G$, $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$ (called the cancellation law). Then G is a group.

Theorem 17.13. A group of order p^n has a cyclic maximal subgroup if and only if it is of one of the following type :

(i) a cyclic group of order p^n;

(ii) the direct product of a cyclic group of order p^{n-1} and one of order p;

(iii) $< x, a \mid x^p = e = a^{p^{n-1}}, xax^{-1} = a^{1+p^{n-2}} >$, $n \geq 3$;

(iv) the dihedral group D_{2^n}, $n \geq 3$;

(v) the generalized quaternion group Q_{2^n}, $n \geq 3$;

(vi) the semidihedral group $< x, a \mid x^2 = e = a^{2^{n-1}}, xax^{-1} = a^{2^{n-2}-1} >$, $n \geq 3$.

Let G be a finitely generated torsion group. If G is abelian, it is easy to show

that G must be finite. In 1902, Burnside raised the following provocative question:

General Burnside Problem : Let G be a finitely generated torsion group. Is G necessarily finite?

Restricted Burnside Problem : Let G be a finitely generated torsion group of bounded exponent. Is G necessarily finite?

The answer to the General Burnside Problem is "no" in general. In 1964, Golod showed that, for any prime p, there exists an infinite p-group G generated by two elements. As for the Restricted Burnside Problem, the full answer is not completely known. If we let n be the exponent of G, the answer to the Restricted Burnside Problem turns out to depend on n. For $n = 2$, the answer is clearly " yes " as G must be abelian. For $n = 3, 4, 6$, the answers are still " yes ", by results of Burnside (1902), Sanov (1940), and M. Hall (1950). For n odd and ≥ 4381, the negative answer to the Restricted Burnside Problem appeared in the work of Novikov and Adjan in 1968. Subsequent work of Adjan showed that there is a negative answer to it for n odd and ≥ 655. Very recently, Ivanov (see [22]) has proved that there is a negative answer to it for all sufficiently large exponents n whether even or odd. For small values of n, apparently not much is known. In particular, the case for $n = 5$ is still open.

Theorem 17.14. Let G be a finitely generated torsion group. If G is nilpotent then G is finite (see [22]).

Corollary 17.15. No finitely generated infinite torsion group is nilpotent.

18. Finite nilpotent groups with maximal class

Theorem 18.1. The dihedral group $D_{2^{n+1}}$ is a nilpotent group of class n for $n \geq 1$.

Proof. This is a standard exercise in group theory. Let $m = 2^{n-1}$. Let α and τ generate D_{4m} and satisfy the following relation:

$$\text{(i)}\ \alpha^2 = e, \qquad \text{(ii)}\ \tau^{2m} = e, \qquad \text{(iii)}\ \alpha\tau = \tau^{-1}\alpha.$$

First it is true for $n = 1$.

For $n \geq 2$, we let $\omega = \alpha^i\tau^j \in Z(G)$, where $0 \leq i \leq 1$, $0 \leq j \leq 2m - 1$; then $\omega\tau = \tau\omega$, and then $\alpha^i\tau^j\tau = \tau\alpha^i\tau^j$, and then $\alpha^i\tau = \tau\alpha^i$. Since $\alpha\tau = \tau^{-1}\alpha$ and $\tau \neq \tau^{-1}$ we have $i = 0$. That is, $\omega = \tau^j$. From $\omega\alpha = \alpha\omega$, we have $\tau^j\alpha = \alpha\tau^j$, and then $\tau^j\alpha = \tau^{-j}\alpha$, so that $\tau^{2j} = e$. Hence $Z(G) = \{e, \tau^m\}$, and then $G/Z(G)$ is a group of order $2m$ generated by $[\alpha]$ and $[\tau]$ satisfy the following relation :

$$\text{(i)}\ [\alpha]^2 = [e], \qquad \text{(ii)}\ [\tau]^m = [e], \qquad \text{(iii)}\ [\alpha][\tau] = [\tau]^{-1}[\alpha].$$

Therefore by mathematical induction, we have completed the proof.

Corollary 18.2. For $n \geq 2$, the generalized quaternion group Q_n is a nilpotent group of class n-1.

Lemma 18.3. For each $n \geq 2$, let G_n be a finite *p*-group of class n, Define H to be the group of all sequences $(g_1, g_2, \ldots)$, with $g_n \in G_n$ for all n and with $g_n = 1$ for all large n; that is, $g_n \neq 1$ for only a finite number of g_n. Then H is an infinite p-group which is not nilpotent.

19. Recursive representation for D_{2^n} and Q_{2^n}

Let $p_k(x, y) = p_k(x_1, x_2, \dots, x_{k-1}; y_1, y_2, \dots, y_{k-1})$ and $q_k(x) = q_k(x_1, x_2, \dots, x_{k-1})$.

Lemma 19.1. Let $A = (GF(p))^n$. Define

$$\begin{aligned} x \circ y = (\ & x_1 + y_1, \\ & x_2 + y_2 + p_2(x_1; y_1), \\ & x_3 + y_3 + p_3(x_1, x_2; y_1, y_2), \\ & x_4 + y_4 + p_4(x_1, x_2, x_3; y_1, y_2, y_3), \\ & \cdots\cdots \\ & x_n + y_n + p_n(x_1, x_2, \dots, x_{n-1}; y_1, y_2, \dots, y_{n-1})\ ). \end{aligned}$$

Then this binary operation satisfies the cancellation law.

Lemma 19.2. Let $A = (GF(2))^2$. Define

$$x \circ y = (\ x_1 + y_1,\ x_2 + y_2 + p_2(x_1, y_1)\ );$$

$$x^{-1} = (\ x_1,\ x_2 + q_2(x_1)\ );\quad e = (0,\ 0),$$

such that it is a group. Then $p_2(x_1, y_1) = cx_1y_1$, $q_2(x_1) = cx_1$, where $c = 0, 1$.

It is easy to see that when $c = 0$ the group is $Z_2 \times Z_2$ and when $c = 1$ it is Z_4, as listed in table 1.

$p_2(x_1, y_1)$	$\langle A; \circ, ^{-1}, e \rangle$
0	$Z_2 \times Z_2$
x_1y_1	Z_4.

Table 1

Lemma 19.3. Let $A = (GF(2))^3$. Define

$$x \circ y = (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3 + p_3(x_1, x_2; y_1, y_2));$$

$$x^{-1} = (x_1,\ x_2,\ x_3 + q_3(x_1, x_2)); \quad e = (0,\ 0,\ 0),$$

such that it is a group. Then $p_3(x, y) = \alpha x_1y_1 + \beta x_2y_2 + \lambda x_1y_2 + \mu x_2y_1$, $q_3(x) = \alpha x_1 + \beta x_2 + (\lambda + \mu)x_1x_2$, where $\alpha, \beta, \lambda, \mu \in \{0, 1\}$ (see the table 2).

$p_3(x, y)$	$\langle A; \circ, ^{-1}, e \rangle$
0	$Z_2 \times Z_2 \times Z_2$
$x_1y_2 + x_2y_1$	$Z_2 \times Z_2 \times Z_2$
x_1y_1	$Z_4 \times Z_2$
x_2y_2	$Z_4 \times Z_2$
$x_1y_1 + x_2y_2$	$Z_4 \times Z_2$
$x_1y_1 + x_1y_2 + x_2y_1$	$Z_4 \times Z_2$
$x_2y_2 + x_1y_2 + x_2y_1$	$Z_4 \times Z_2$
$x_1y_1 + x_2y_2 + x_1y_2 + x_2y_1$	$Z_4 \times Z_2$
x_1y_2	D_8
x_2y_1	D_8
$x_1y_1 + x_1y_2$	D_8
$x_1y_1 + x_2y_1$	D_8
$x_2y_2 + x_1y_2$	D_8
$x_2y_2 + x_2y_1$	D_8
$x_1y_1 + x_2y_2 + x_1y_2$	Q_8
$x_1y_1 + x_2y_2 + x_2y_1$	Q_8

Table 2

Proof. Let $A = (GF(2))^3$. Let

$$x \circ y = (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3 + \alpha x_1y_1 + \beta x_2y_2 + \lambda x_1y_2 + \mu x_2y_1);$$

$$x^{-1} = (x_1,\ x_2,\ x_3 + \alpha x_1 + \beta x_2 + (\lambda + \mu)x_1x_2); \quad e = (0,\ 0,\ 0);$$

$$x \bullet y = (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3 + \alpha' x_1y_1 + \beta' x_2y_2 + \lambda' x_1y_2 + \mu' x_2y_1);$$

$$x^{-1} = (x_1,\ x_2,\ x_3 + \alpha' x_1 + \beta' x_2 + (\lambda' + \mu')x_1x_2); \quad e = (0,\ 0,\ 0).$$

Consider the following mappings f_1, f_2, f_3 :

$$f_1(x_1,\ x_2,\ x_3) = (x_1 + x_2,\ x_2,\ x_3),$$

$$f_2(x_1,\ x_2,\ x_3) = (x_1,\ x_2,\ x_3 + x_1x_2),$$

$$f_3(x_1,\ x_2,\ x_3) = (x_2,\ x_1,\ x_3),$$

we have that $\langle A; \bullet, ^{-1}, e \rangle$ is isomorphic to $\langle A; \circ, ^{-1}, e \rangle$ if

(i) $(\alpha', \beta', \lambda', \mu') = (\alpha,\ \alpha + \beta + \lambda + \mu,\ \alpha + \lambda,\ \alpha + \mu)$ or

(ii) $(\alpha', \beta', \lambda', \mu') = (\alpha,\ \beta,\ \lambda + 1,\ \mu + 1)$ or

(iii) $(\alpha', \beta', \lambda', \mu') = (\beta,\ \alpha,\ \mu,\ \lambda)$ or

(iv) finite composition of (i), (ii) and (iii).

Theorem 19.4. Let $A = (GF(2))^n$. Let $p_1(x, y) = 0$, $p_2(x, y) = x_1y_1$,

$p_k(x, y) = x_{k-1}y_{k-1} + (x_{k-1} + y_{k-1})\, p_{k-1}(x, y)$ for $2 \le k \le n$,

$q_1(x) = 0$, $q_2(x) = x_1$, $q_k(x) = x_{k-1}[\, x_{k-1} + q_{k-1}(x)\,] + q_{k-1}(x)$ for $2 \le k \le n$.

Define $x \circ y = x + y + p(x, y)$, $e = (0, \ldots, 0)$.

Then $\langle A; \circ, ^{-1}, e \rangle$ is a cyclic group of order 2^n with $x^{-1} = x + q(x)$ and

$u = (1, 0, \ldots, 0)$ a generator.

Proof. It is easily checked that $p_k(x, y)$ for $1 \le k \le n$ are the carry functions for addition modulo 2^n based on addition modulo 2.

Lemma 19.5. Let $A = (GF(2))^3$. Define a group operation

$x \circ y = (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3 + p_3(x_1, x_2; y_1, y_2) + x_2y_2)$ such that

$\tau^4 = \alpha^2 = (0, 0, 0)$ and $\alpha \circ \tau = \tau^3 \circ \alpha$ for $\tau = (0, 1, 0)$, $\alpha = (1, 0, 0)$.

Then $p_3(x_1, x_2; y_1, y_2) = x_1y_2$ or $p_3(x_1, x_2; y_1, y_2) = x_2y_1$.

Lemma 19.6. Let $A = (GF(2))^3$. Define

$x \circ y = (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3 + x_1y_2 + x_2y_2)$.

Then $\langle A; \circ \rangle$ is a dihedral group such that for $\tau = (0, 1, 0)$ and $\alpha = (1, 0, 0)$,

(i) $\tau^4 = \alpha^2 = (0, 0, 0)$ and $\alpha \circ \tau = \tau^3 \circ \alpha$; (ii) $\tau^i\alpha = \tau^i + \alpha$ for $0 \le i \le 3$.

Lemma 19.7. Let $A = (GF(2))^4$. Define

$x \circ y = (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3 + x_1y_2 + x_2y_2,$

$x_4 + y_4 + x_3y_3 + x_2y_2(x_3 + y_3) + x_1y_2 (x_2 + x_3 + y_2 + y_3) + x_1y_3)$.

Then $\langle A; \circ \rangle$ is a dihedral group such that for $\tau = (0, 1, 0, 0)$ and $\alpha = (1, 0, 0, 0)$,

(i) $\tau^8 = \alpha^2 = (0, 0, 0, 0)$ and $\alpha \circ \tau = \tau^7 \circ \alpha$; (ii) $\tau^i \circ \alpha = \tau^i + \alpha$ for $0 \le i \le 7$.

In the following we let

$H(x, y) = (h_1(x, y),\ h_2(x, y), \ldots, h_n(x, y))$;

$P(x, y) = (p_1(x, y),\ p_2(x, y), \ldots, p_n(x, y))$;

$h_1(x, y) = h_2(x, y) = 0$; $p_1(x, y) = p_2(x, y) = 0$;

$h_{k+1}(x, y) = x_k y_k + h_k(x, y)(x_k + y_k)$ for $2 \le k \le n-1$.

Lemma 19.8. Let $A = (GF(2))^n$. Suppose $x \circ y = x + y + P(x, y)$ define a group operation such that for $e = (0, \ldots, 0)$, $\tau = (0, 1, 0, \ldots, 0)$ and $\alpha = (1, 0, 0, \ldots, 0)$,

(i) $\tau^{2^{n-1}} = \alpha^2 = e$ and $\alpha \circ \tau = \tau^{-1} \circ \alpha$;

(ii) $\tau^i \circ \alpha = \tau^i + \alpha$;

(iii) $\tau^{i+j} = \tau^i \circ \tau^j = \tau^i + \tau^j + H(\tau^i, \tau^j)$.

Then $P(x, y) = H(x, y) + \{ H(x, y) + H(x \circ y, y) \} x_1$.

Proof. It is easy to see that

(a) $H(x, y) = H(y, x)$;

(b) $H(\tau^i, \tau^j) = H(\tau^i \circ \alpha, \tau^j) = H(\tau^i, \tau^j \circ \alpha) = H(\tau^i \circ \alpha, \tau^j \circ \alpha)$;

(c) $\tau^i = \tau^j \circ \tau^{i-j} = \tau^j + \tau^{i-j} + H(\tau^j, \tau^{i-j})$;

and then we have

(d) $P(\tau^i, \tau^j) = H(\tau^i, \tau^j)$ by (iii);

(e) $P(\tau^i, \tau^j \circ \alpha) = H(\tau^i, \tau^j) = H(\tau^i, \tau^j \circ \alpha)$ from $\tau^i \circ (\tau^j \circ \alpha) = \tau^{i+j} + \alpha$ and (b);

(f) $P(\tau^i \circ \alpha, \tau^j) = H(\tau^{i-j}, \tau^j) = H(\tau^{i-j} \circ \alpha, \tau^j) = H(\tau^i \circ \alpha \circ \tau^j, \tau^j)$

from $(\tau^i \circ \alpha) \circ \tau^j = \tau^{i-j} + \alpha$ and (c), and (b);

(g) $P(\tau^i \circ \alpha, \tau^j \circ \alpha) = H(\tau^{i-j}, \tau^j) = H(\tau^{i-j}, \tau^j \circ \alpha) = H(\tau^i \circ \alpha \circ \tau^j \circ \alpha, \tau^j \circ \alpha)$

from $(\tau^i \circ \alpha) \circ (\tau^j \circ \alpha) = \tau^{i-j}$ and (c), and (b).

Therefore, we have $P(x, y) = H(x, y) + \{ H(x, y) + H(x \circ y, y) \} x_1$.

Theorem 19.9. Let $A = (GF(2))^n$. Define $x \circ y = x + y + P(x, y)$ where

$P(x, y) = H(x, y) + \{ H(x, y) + H(x \circ y, y) \} x_1$.

Then for $e = (0, \ldots, 0)$, $\tau = (0, 1, 0, \ldots, 0)$, $\alpha = (1, 0, 0, \ldots, 0)$,

(i) $\tau^{2^{n-1}} = \alpha^2 = e$ and $\alpha \circ \tau = \tau^{-1} \circ \alpha$;

(ii) $\tau^i \circ \alpha = \tau^i + \alpha$;

(iii) $\tau^{i+j} = \tau^i \circ \tau^j = \tau^i + \tau^j + H(\tau^i, \tau^j)$;

(iv) $\langle A; \circ \rangle$ is the dihedral group D_{2^n};

(v) $p_{k+1}(x, y) = (x_k + x_1)y_k + p_k(x, y)(x_k + y_k + x_1)$;

(vi) $q_{k+1}(x) = (x_k + x_1)(x_k + q_k(x)) + q_k(x)(1 + x_1)$

$= (x_1 + 1)x_k + (1 + x_k)q_k(x)$.

Proof. We only show that the associative law holds by mathematical induction. For this, we show by induction that

(i) $p_k(x, y) + p_k(x \circ y, z) = p_k(y, z) + p_k(x, y \circ z)$;

(ii) $p_k(x, y)\, p_k(x \circ y, z) + y_1 p_k(x \circ y, z) = p_k(y, z)\, p_k(x, y \circ z) + y_1 p_k(y, z)$.

First, since $p_1(x, y) = p_2(x, y) = h_1(x, y) = h_2(x, y) = 0$,

we have (i) and (ii) for $k = 1, 2$.

Second, since $h_3(x, y) = x_2 y_2$, and $h_3(x \circ y, y) = (x_2 + y_2)y_2$, and then

$p_3(x, y) = (x_2 + x_1)y_2$; $p_3(x \circ y, z) = (x_2 + x_1 + y_2 + y_1)z_2$;

$p_3(y, z) = (y_2 + y_1)z_2$; $p_3(x, y \circ z) = (x_2 + x_1)(y_2 + z_2)$.

Thus, we have (i) and (ii) for $k = 3$.

Finally, we assume that (i) and (ii) hold for $k = m$ and we show that (i) and (ii) hold for $k = m + 1$.

Since $x_1p_k(x, y) = x_1h_k(x \circ y, y)$ and

$[h_k(x, y) + p_k(x, y)](x_k + y_k)\, x_1 = [h_k(x, y) + p_k(x, y)](x_k + y_k)$,

we have

$$p_{k+1}(x, y) = h_{k+1}(x, y) + (h_{k+1}(x, y) + h_{k+1}(x \circ y, y))\, x_1$$

$$= x_k y_k + h_k(x, y)(x_k + y_k) + \{ (x_k + y_k + p_k(x,y))\, y_k +$$

$$h_k(x \circ y, y)(x_k + y_k + p_k(x, y) + y_k) + x_k y_k + h_k(x, y)(x_k + y_k) \}\, x_1$$

$$= x_k y_k + h_k(x, y)(x_k + y_k) + \{ (x_k + y_k + p_k(x,y))\, y_k +$$

$$p_k(x, y)(x_k + y_k + p_k(x, y) + y_k) + x_k y_k + h_k(x, y)(x_k + y_k) \}\, x_1$$

$$= x_k y_k + h_k(x, y)(x_k + y_k) + x_1 p_k(x, y) + x_1 y_k + [h_k(x, y) + p_k(x, y)](x_k + y_k)\, x_1$$

$$= x_k y_k + h_k(x, y)(x_k + y_k) + x_1 p_k(x, y) + x_1 y_k + [h_k(x, y) + p_k(x, y)](x_k + y_k)$$

$$= (x_k + x_1)y_k + p_k(x, y)(x_k + y_k + x_1).$$

Hence, we have

$$p_{k+1}(x, y) = (x_k + x_1)y_k + p_k(x, y)(x_k + y_k + x_1);$$

$$p_{k+1}(y, z) = (y_k + y_1)z_k + p_k(y, z)(y_k + z_k + y_1);$$

$$p_{k+1}(x \circ y, z) = [x_k + y_k + p_k(x, y) + x_1 + y_1]\, z_k +$$

$$p_k(x \circ y, z)[x_k + y_k + p_k(x, y) + x_1 + y_1 + z_k];$$

$$p_{k+1}(x, y \circ z) = (x_k + x_1) [y_k + z_k + p_k(y, z)] +$$

$$p_k(x, y \circ z) [x_k + y_k + z_k + p_k(y, z) + x_1].$$

It is easily checked that

$$p_{k+1}(x, y) + p_{k+1}(y, z) + p_{k+1}(x \circ y, z) + p_{k+1}(x, y \circ z)$$

$$= (x_k + x_1)y_k + p_k(x, y)(x_k + y_k + x_1) + (y_k + y_1)z_k + p_k(y, z)(y_k + z_k + y_1) +$$

$$[x_k + y_k + p_k(x, y) + x_1 + y_1]\, z_k + p_k(x \circ y, z)[x_k + y_k + p_k(x, y) + x_1 + y_1 + z_k] +$$

$(x_k + x_l)\,[\,y_k + z_k + p_k(y, z)] \;+\; p_k(x, y \circ z)\,[\,x_k + y_k + z_k + p_k(y, z) + x_l\,]$

$= \; p_k(x, y)(x_k + y_k + x_l) + p_k(y, z)(y_k + z_k + y_l) +$

$p_k(x, y)\, z_k + p_k(x \circ y, z)[\,x_k + y_k + p_k(x, y) + x_l + y_l + z_k\,] +$

$(x_k + x_l)p_k(y, z) \;+\; p_k(x, y \circ z)\,[\,x_k + y_k + z_k + p_k(y, z) + x_l]$

$= \; p_k(x, y)(x_k + y_k + z_k + x_l) + p_k(y, z)(y_k + z_k + x_k + x_l + y_l) +$

$p_k(x \circ y, z)[\,x_k + y_k + p_k(x, y) + x_l + y_l + z_k\,] +$

$p_k(x, y \circ z)\,[\,x_k + y_k + z_k + p_k(y, z) + x_l\,]$

$= \; [\,p_k(x, y) + p_k(y, z) + p_k(x \circ y, z) + p_k(x, y \circ z)\,]\,(x_k + y_k + z_k + x_l) +$

$p_k(y, z)\, y_l \;+\; p_k(x \circ y, z)\, y_l \;+\; p_k(x \circ y, z)\, p_k(x, y) \;+\; p_k(x, y \circ z)\, p_k(y, z)$

$= 0.$

Similarly,

$p_{k+1}(y, z)\, y_l + p_{k+1}(x \circ y, z)\, y_l + p_{k+1}(x \circ y, z)\, p_{k+1}(x, y) + p_{k+1}(x, y \circ z)\, p_{k+1}(y, z)$

$= \; (y_k + y_l)z_k y_l \;+\; p_k(y, z)(y_k + z_k + y_l)y_l \;+\; [\,x_k + y_k + p_k(x, y) + x_l + y_l]\, z_k y_l +$

$p_k(x \circ y, z)[\,x_k + y_k + p_k(x, y) + x_l + y_l + z_k\,]y_l +$

$\{\,[\,x_k + y_k + p_k(x, y) + x_l + y_l]\, z_k + p_k(x \circ y, z)[\,x_k + y_k + p_k(x, y) + x_l + y_l + z_k\,]\,\}$

$\{\,(x_k + x_l)y_k \;+\; p_k(x, y)(x_k + y_k + x_l)\,\} \;+$

$\{\,(x_k + x_l)\,[\,y_k + z_k + p_k(y, z)] \;+\; p_k(x, y \circ z)\,[\,x_k + y_k + z_k + p_k(y, z) + x_l\,]\,\}$

$\{\,(y_k + y_l)z_k + \; p_k(y, z)(y_k + z_k + y_l)\,\}$

$= \; p_k(y, z)\, c(x, y) + p_k(x, y)\, b(x, y) \;+\; p_k(x \circ y, z)\, c(x, y) + p_k(x, y \circ z)\, b(x, y) \;+$

$p_k(x \circ y, z)\, p_k(x, y)\, a(x, y) \;+\; p_k(x, y \circ z)\, p_k(y, z)\, a(x, y)$

$= \; b(x, y)\{\,p_k(x, y) + p_k(x \circ y, z) + p_k(y, z) + p_k(x, y \circ z)\,\} +$

$[\,b(x, y) + c(x, y)\,]\{\,p_k(y, z) + p_k(x \circ y, z)\,\} +$

$a(x, y)\,\{\,p_k(x \circ y, z)\, p_k(x, y) + p_k(x, y \circ z)\, p_k(y, z)\,\}$

$= b(x, y)\ \{\ p_k(x, y) + p_k(x \circ y, z) + p_k(y, z) + p_k(x, y \circ z)\ \} +$

$a(x, y)\ \{\ p_k(y, z)y_l + p_k(x \circ y, z)y_l + p_k(x \circ y, z)\ p_k(x, y) + p_k(x, y \circ z)\ p_k(y, z)\ \}$

$= 0,$

where

$a(x, y) = \{\ y_l + x_k y_k + x_l y_k + y_l x_k + y_l y_k + y_l x_l + x_k z_k + y_k z_k + x_l z_k\ \},$

$b(x, y) = \{\ x_k z_k y_k + x_l z_k y_k + x_k z_k y_l + y_k z_k y_l + z_k y_l + x_l z_k y_l\ \},$ and

$c(x, y) = \{\ (x_k y_l + y_k y_l + x_l y_l + y_l + z_k y_l + y_l x_k y_k + y_l x_l y_k + z_k x_k y_k + x_l y_k z_k\ \}.$

We have completed the proof.

Theorem 19.10. Let $A = (GF(2))^n$, $n \geq 3$ and $L(x, y) = (0, \ldots, 0, x_l y_l)$.

Define $x \circ y = x + y + P(x, y)$ and

$$P(x, y) = H(x, y) + \{\ H(x, y) + H(x \circ y, y)\ \}x_l + L(x, y).$$

Then for $\tau = (0, 1, 0, \ldots, 0)$, $\alpha = (1, 0, 0, \ldots, 0)$,

(i) $\tau^{2^n} = e$, $\tau^{2^{n-1}} = \alpha^2$ and $\alpha \circ \tau = \tau^{-1} \circ \alpha$;

(ii) $\tau^i \circ \alpha = \tau^i + \alpha$;

(iii) $\tau^{i+j} = \tau^i \circ \tau^j = \tau^i + \tau^j + H(\tau^i, \tau^j)$;

(iv) $\langle A; \circ \rangle$ is the generalized quaternion group Q_{2^n}.

My Publications

[1] Zhang Xuebin,

On the existence of (v,4,1)-PMD, Ars Combinatoria 29 (1990), 3-12.

[2] F. E. Bennett, Zhang Xuebin and Zhu Lie,

Perfect Mendelsohn designs with block size four, Ars Combinatoria 29 (1990), 65-72.

[3] F. E. Bennett and Zhang Xuebin,

Resolvable Mendelsohn designs with block size four, Aequationes Mathematicae 40 (1990), 248-260.

[4] Zhu Lie, Du Beiliang and Zhang Xuebin,

A few more RBIBDs with k=5 and $\lambda = 1$, Discrete Mathematics 97 (1991), 409-417.

[5] Zhang Xuebin,

Constructions of resolvable Mendelsohn designs, Ars Combinatoria 34 (1992), 225-250.

[6] Zhang Xuebin,

Constructions for perfect threshold schemes, Combinatorics and Graph Theory, (Hefei,1992), 87-90, World Science Publishing, River Edge, NJ, 1993.

[7] Zhang Xuebin,

Indecomposable triple systems with $\lambda = 5$, Journal of Combinatorial Mathematics and Combinatorial Computing 16 (1994), 153-162.

[8] Zhang Xuebin,

Construction for indecomposable simple (v,4, λ)-BIBDs, Discrete Mathematics 156 (1996), 317-322.

[9] Zhang Xuebin,

On the existence of (v,4,1)-RPMD, Ars Combinatoria 42 (1996), 3-31.

[10] Zhang Xuebin,

Construction of orthogonal group divisible designs, Journal of Combinatorial Mathematics and Combinatorial Computing 20 (1996), 121-128.

[11] Zhang Xuebin,

Direct construction methods for incomplete perfect Mendelsohn designs with block size four, Journal of Combinatorial Designs, 4(1996), 117-134.

[12] F. E. Bennett and Zhang Xuebin,

Holey Perfect Mendelsohn designs of type m^h with block size four, Journal of Combinatorial Designs, 5 (1997), 203-213.

[13] Kong Gaohua and Zhang Xuebin,

On the existence of (v, n, 4, λ)-IPMD for even λ, Ars Combinatoria, to appear.

Note that my work of the last three papers above was done at Department of Mathematics and Astronomy of University of Manitoba.

Bibliography

1. M. H. Armanious,

Nilpotent SQS-Skeins with nilpotent derived sloops, preprint.

2. A. J. Guelzow,

Some classes of E-Minimal Algebras of Affine Type: Nilpotent squags, p-group and Nilpotent SQS-Skeins. Ph.D. Thesis, University of Manitoba, 1991.

3. A. J. Guelzow,

The structure of Nilpotent Steiner Quadruple systems , Journal of Combinatorial Designs, 1 (1993), 301-321.

4. A. J. Guelzow,

Representation of finite nilpotent squags , Discrete Math. 154 (1996), 63-76.

5. J. H. Dinitz and D. R. Stinson,

Contemporary Design Theory : A Collection of Surveys , New York, NY : Wiley, 1992.

6. C. J. Colbourn and D. R. Stinson,

The CRC Handbook of Combinatorial Designs. Boca Raton, FL : CRC Press, 1996.

7. R. S. Freese and R. N. McKenzie,

Commutator theory for congruence modular varieties. Cambridge University Press, 1987.

8. G. Grätzer,

Universal Algebra, New York : Springer-Verlag, 1979.

9. H. P. Gumm,

An easy way to the commutator in modular varieties, Arch. Math. 34 (1980), 220-228.

10. H. P. Gumm,

Geometrical methods in congruence modular algebras, Memoirs of the American Math. Society, Vol.45, no. 286, (1983).

11. B. Ganter and H. Werner,

Equational classes of Steiner systems, Algebra Universalis 5 (1975), 125-140.

12. C. Herrmann,

Affine algebras in congruence modular varieties, Acta Sci. Math. 41(1979), 119-125.

13. J. Hagemann and C. Herrmann,

A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity, Arch. Math. 32 (1979), 234-245.

14. C. C. Lindner and A. Rosa,

Steiner quadruple systems: a survey, Discrete Mathematics 21 (1979), 147-181.

15. S. Klossek,

Kommutative spiegelungsräume, Mitt. Math. Sem. Gießen 117(1975).

16. R. N. McKenzie, G. F. McNulty and W. F. Taylor,

Algebras, Lattices, Varieties, Wadsworth & Brooks, 1987.

17 N. S. Mendelsohn,

A natural generalization of Steiner triple systems, in Computers in Number Theory, Academic Press, New York, 1971, 323-338.

18. R. W. Quackenbush,

Varieties of Steiner loops and Steiner quasigroups, Canada J. Math. 28 (1976), 1187-1198.

19. R. W. Quackenbush,

Algebraic speculations about Steiner systems, Annals of Discrete Mathematics 7 (1980), 25-36.

20. R. W. Quackenbush,

Nilpotent block designs I: Basic concepts for Steiner triple and quadruple systems, preprint.

21. J. J. Rotman,

An introduction to the theory of groups, Springer-Verlag, 1995.

22. D. J. S. Robinson,

A course in the theory of groups, Springer-Verlag, 1996.

23. S. Sidki,

On a 2-generated infinite 3-group, Journal of Algebra 110 (1987), 13-25.

24. J. D. H. Smith,

Mal'cev varieties. Lecture Notes in Mathematics. Vol. 554, Springer-Verlag.

25. W. Taylor,

Some applications of the term condition, Algebra Universalis 14 (1982), 11-24.

26. M. R. Vaughan-Lee,

Nilpotentce in permutable varieties, Lecture Notes in Mathematics, Vol.1004, Springer-Verlag.

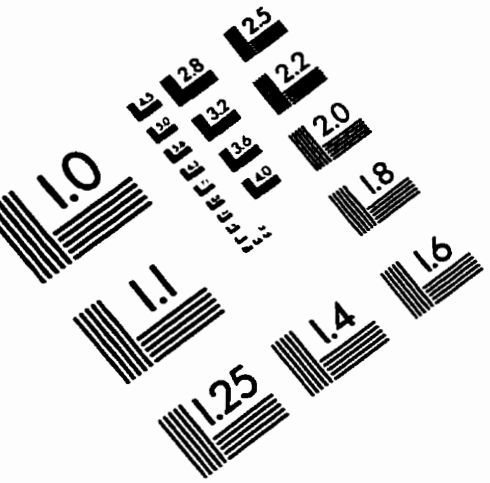
27. R. Mathon and Rosa,

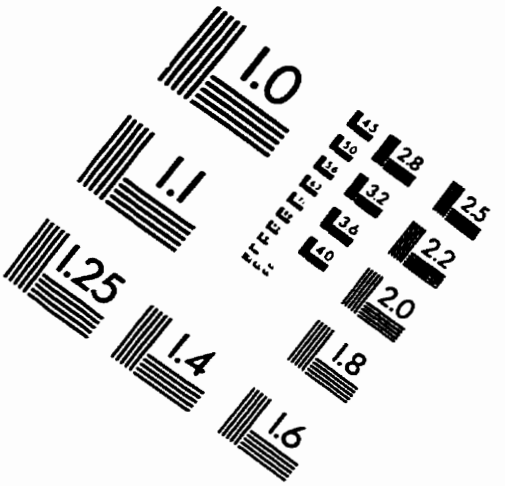
A census of Mendelsohn triple systems of order nine, Ars Combinatioria, 4 (1977), 309-315.

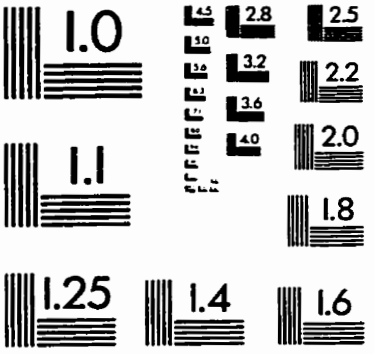
28. F. E. Bennett,

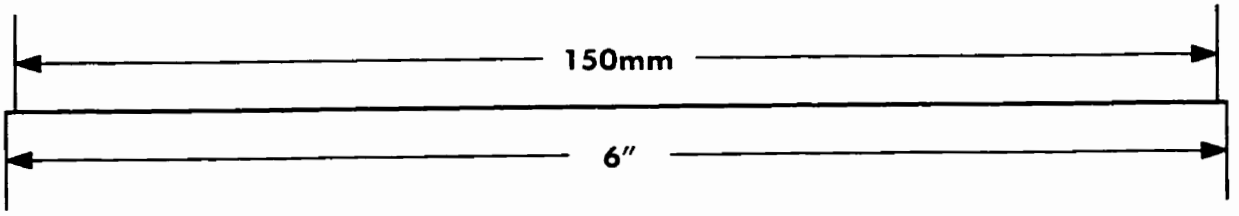
Mendelsohn triple systems without repeated blocks, Congr. Number, 20 (1977), 383-398.

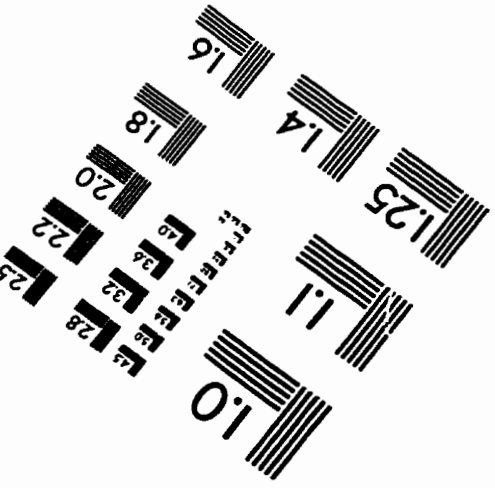
IMAGE EVALUATION
TEST TARGET (QA-3)

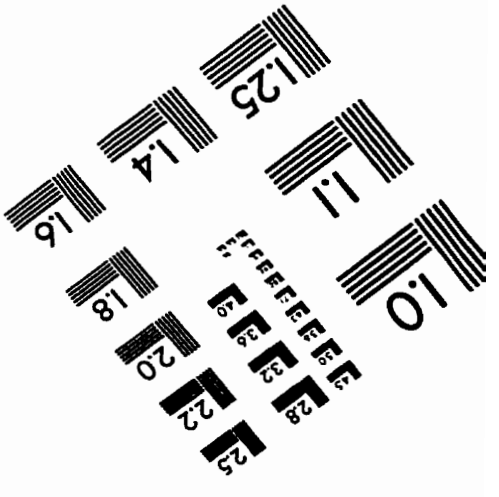












APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989