Introduction

Although Galois realized the importance of fields in the early 19th century when he completely determined the finite fields, generalization of the concept took some time. In their 1907 paper *Non-Desarguesian and non-Pascalian geometries*, Veblen and Wedderburn give examples of field-like structures displaying weakened or no distributive properties. These structures arose from their study of projective geometry as a means of coordinatizing finite plane geòmetries in which Desargues' Theorem (a condition on triangles which holds in all projective spaces of dimension three or higher) fails.

As the relationship between finite projective geometries and the algebraic structures which coordinatize them was better understood, progress was made in the classification of finite projective planes. In 1949, Bruck and Ryser produced the classical result omitting an infinite class of integers, those numbers which are not the sum of two squares and are congruent to 1 or 2 mod 4, as possible orders of projective planes.

A few years later, Lenz and Barlotti divided projective planes into 53 subclasses which are often arranged into seven major groups based on the algebraic properties of their coordinatizing structure. Of the 53 classes, 38 are known to be empty, 14 are nonempty, and one is uncertain. Of the 14 nonempty classes, only seven contain planes with finitely many points and lines. (source: Quasigroups and Loops: Theory and Application) Yet this classification is rather crude, and we prefer the more natural approach of determining the number of planes of a given order.

The only known projective planes have prime power order. Conversely, every finite field coordinatizes a projective plane. Bruck-Ryser's result eliminates many possible orders and a computer search has eliminated 10 as a possible order, but the remaining possible orders, of which 12 is the smallest, are unknown. [GK]

Congruence lattices have been used to discover properties of general algebras for many years, but the theory that illustrates just how deeply revealing congruence lattices can be sprung into existence around 1980 with a paper by P.P. Palfy and P. Pudlak. By 1984, several authors had hammered out the basic details of tame congruence theory and their work was compiled by Hobby and McKenzie in *The Structure of Finite Algebras*. The theory reveals that locally finite varieties of algebras are sharply divided into six families, each characterized by the behavior of its congruences. One particular aspect of the theory is that each covering pair in the congruence lattice of a finite algebra is associated with one of five types of algebras: a unary, or permutational, algebra, a vector space over a finite field, the two-element Boolean algebra, the two-element lattice, or the two-element semilattice. Knowing which types occur (or do not occur) in the congruence lattice can reveal important properties of the algebra. [HM]

The goal of this paper is to apply tame congruence analysis to ternary rings, the generalized field-like algebras which coordinatize projective planes, and objects strongly connected to ternary rings, to better understand their structures and properties.

1. Basic Definitions, Concepts, and Notations

Universal Algebras. By an *(indexed) algebra* we mean a nonempty set A and some *basic operations* on the set requiring only finitely many variables. The underlying set A will sometimes be called the *universe* of the algebra. We will be working primarily with algebras with only one or two basic operations, and we will generally write such algebras $\mathbf{A} = \langle A, \{f_i : i \in I\}\rangle$ where f_i denotes the basic operation indexed by i. Some simple examples of this notation are the ring of integers $\langle \mathbb{Z}, \{f_i : i \in \{+, -, \times\}\}\rangle$, and any group $\left\langle G, *, ^{-1}, e\right\rangle$ (note that we often write only the symbol indexing the operation to prevent the notation from becoming too cumbersome). We say an algebra is *finite* if its universe has finite cardinality. In this paper we shall be concerned exclusively with finite algebras.

The *similarity type* of an algebra is a function $\rho : I \to \mathbb{Z}^+ \cup \{0\}$, where I is the index set for the basic operations, such that $\rho(i)$ is the arity of the basic operation f_i. For the ring of integers mentioned above, $\rho(+) = \rho(-) = \rho(\times) = 2$, and for the group, $\rho(*) = 2$, $\rho(^{-1}) = 1$, and $\rho(e) = 0$. Two algebras are said to be *similar* if they have the same similarity type. Similarity is easily seen to be an equivalence relation, and the equivalence classes will be called *similarity classes*.

When considering similar algebras, the concepts of homomorphism and Cartesian product are defined in the obvious way. If $\mathbf{A}$ is an algebra, then a subset B of the universe of $\mathbf{A}$ is called a *subuniverse* of $\mathbf{A}$ if it is closed under each basic operation. If $\mathbf{B}$ is an algebra similar to $\mathbf{A}$, the universe of $\mathbf{B}$ is a subuniverse of $\mathbf{A}$, and the basic operations of $\mathbf{B}$ are the restrictions to B of the basic operations of $\mathbf{A}$, then $\mathbf{B}$ is called a *subalgebra* of $\mathbf{A}$. Let X be a subset of the universe A of an algebra $\mathbf{A}$. The *subuniverse of* $\mathbf{A}$ *generated by* X is the smallest subset of A containing X which is closed under the basic operations of $\mathbf{A}$. The *subalgebra of* $\mathbf{A}$ *generated by* X is defined similarly. If the subalgebra of $\mathbf{A}$ generated by X is again $\mathbf{A}$, we will say that X *generates* $\mathbf{A}$ or $\mathbf{A}$ *is generated by* X.

By an n-ary operation on a set A, we mean a function $f : A^n \to A$. In this paper we will commonly use "unary", "binary", and "ternary" instead of 1-ary, 2-ary, and 3-ary. Let $f_1, \ldots, f_k$ be n-ary operations and let g be a k-ary operation. We will commonly use the notation $\bar{x}$ to represent an n-tuple $(x_1, \ldots, x_n)$. Then the *composition* of g with the f_i's is the n-ary operation $h(\bar{x}) = g(f_1(\bar{x}), \ldots, f_n(\bar{x}))$. The n-ary *projection operations* are the functions $p_i^n(x_1, \ldots, x_n) = x_i$. A *clone* on a nonempty set A is a set of operations on A which is closed under compositions and contains the projections p_i^n for all n and all $1 \leq i \leq n$.

There are two examples of clones on an algebra which we will find useful.

Definition 1.1. *The* **clone of term operations** *of an algebra* $\mathbf{A}$*, denoted* $\mathrm{Clo}(\mathbf{A},$ *is the smallest clone on the universe* A *that contains the basic operations of* $\mathbf{A}$*. The elements of* $\mathrm{Clo}(\mathbf{A})$ *will be called* **term operations***, or, simply,* **terms***.*

The **clone of polynomial operations** *of an algebra* $\mathbf{A}$*, denoted* $\mathrm{Pol}(\mathbf{A})$*, is the smallest clone on the universe* A *that contains the basic operations of* $\mathbf{A}$ *and the constant 0-ary operations. The elements of* $\mathrm{Pol}(\mathbf{A})$ *will be called* **polynomial operations** *or just* **polynomials***.*

If we wish to refer only to the n-ary term or polynomial operations, we may use the notation $\mathrm{Clo}_n(\mathbf{A})$ *and* $\mathrm{Pol}_n(\mathbf{A})$ *to refer to those sets.*

If t is an $m+n$-ary term operation on $\mathbf{A}$, and $\bar{a} = \langle a_1, \ldots, a_m \rangle$, where $a_i \in A$ for each $i = 1, \ldots, m$, then $g(\bar{x}) = f(\bar{a}, \bar{x})$ is a polynomial operation on $\mathbf{A}$. Indeed, every polynomial operation arises via the substitution of constants for some of the variables in a term operation.

We will encounter algebras for which $\mathrm{Pol}_n(\mathbf{A}) = \mathrm{Pol}_n(A)$ for all $n \geq 1$. That is, algebras in which every function $f : A^n \to A$ is expressed by an n-ary polynomial operation. Such algebras will be called *functionally complete.* If every n-ary function on the universe of an algebra is expressed by an n-ary term operation, we will call the algebra *primal.*

A relation α on a set A is said to be *compatible* with a function $f : A^n \to A$ if $f(a_1, \ldots, a_n)\ \alpha\ f(b_1, \ldots, b_n)$ whenever $a_i\ \alpha\ b_i$ for $i = 1, \ldots, n$. By an *n-ary admissible relation* of an algebra $\mathbf{A}$ we mean a subset of A^n which is compatible with all the basic operations of $\mathbf{A}$. A *congruence* of $\mathbf{A}$ is an admissible equivalence relation. The set $x/\alpha = \{y \in A : x\ \alpha\ y\}$ is called the *α-congruence class* of x, or just the α-class of x. Congruences are extremely important in universal algebra in much the same way that normal subgroups play a vital role in group theory. (In fact, the normal subgroups of a group are in 1-1 correspondence with the congruences on the group).

Lemma 1.2. *Let θ be an equivalence relation on an algebra $\mathbf{A}$. Then θ is a congruence if and only if θ is compatible with all the unary polynomials of $\mathbf{A}$.*

Proof. ($\Longrightarrow$) is by definition. Suppose θ is compatible with all the unary polynomials of $\mathbf{A}$. Let f be an n-ary basic operation of $\mathbf{A}$. Then $g(x) = f(x, a_1, \ldots, a_{n-1})$ is a unary polynomial, and for all choices of the constants $a_1, \ldots, a_{n-1} \in A$, θ is compatible with $g(x)$. Interchanging the x and a_i arguments to f for each $i = 1, \ldots, n-1$ shows θ is compatible with f. Since f was an arbitrary basic operation, the result follows. □

As the analogy to group theory might suggest, we will need the concept of a quotient algebra. Let α be a congruence on $\mathbf{A}$ and let f be an n-ary operation on $\mathbf{A}$. If $A/\alpha = \{x/\alpha : x \in A\}$ is the set of congruence classes, then

$$f_\alpha(x_1/\alpha, \ldots, x_n/\alpha) = f(x_1, \ldots, x_n)/\alpha$$

defines an n-ary operation f_α on A/α. So if $\mathbf{A} = \langle A, f_1, \ldots, f_k \rangle$ is an algebra and α is a congruence on $\mathbf{A}$, we define the *quotient* algebra

$$\mathbf{A}/\alpha = \langle A/\alpha, f_{1\alpha}, \ldots, f_{k\alpha} \rangle .$$

Two algebras $\mathbf{A}$ and $\mathbf{B}$ are said to be *polynomially equivalent* if they have the same universe and $\mathrm{Pol}(\mathbf{A}) = \mathrm{Pol}(\mathbf{B})$.

Lemma 1.3. *Let $\mathbf{A}$ and $\mathbf{B}$ be polynomially equivalent algebras. Then the algebras have precisely the same congruences.*

Proof. Let α be a congruence on $\mathbf{A}$. α is clearly an equivalence relation on $\mathbf{B}$, since the algebras have the same universe. It remains to show that α is an admissible relation on $\mathbf{B}$. Every basic operation of $\mathbf{B}$ is in $\mathrm{Pol}(\mathbf{B}) = \mathrm{Pol}(\mathbf{A})$. α is closed under members of $\mathrm{Clo}(\mathbf{A})$ since it is closed under the basic operations (and hence compositions of basic operations). Since the diagonal terms $\langle x, x \rangle$ are in α for all $x \in A$, α is closed under all the constant operations, and hence it is closed under polynomials. So α is a congruence on $\mathbf{B}$. Interchanging the roles of $\mathbf{A}$ and $\mathbf{B}$, the result follows. □

Definition 1.4. $\mathbf{A}|_X = \langle X, (\mathrm{Pol}(\mathbf{A}))|_X\rangle$ *where* X *is a subset of* A *and*

$$(\mathrm{Pol}(\mathbf{A}))|_X = \{h|_X : h \in \mathrm{Pol}_n(\mathbf{A}) \text{ for some } n, \text{ and } h(X^n) \subseteq X\}$$

is called the **algebra induced on X by A**.

Definition 1.5. *Let* **A** *be an algebra and let* X *and* Y *be nonempty subsets of* A. *If there are polynomials* $f, g \in \mathrm{Pol}_1(\mathbf{A})$ *such that* $f(X) = Y$, $g(Y) = X$, $fg|_Y = id_Y$ *and* $gf|_X = id_X$, *then* X *and* Y *are said to be* **polynomially isomorphic**, *denoted* $X \simeq Y$.

Note that polynomial isomorphism is an equivalence relation on nonempty subsets of **A**. It is also important to note that the map $\pi = f|_X$ is an algebra isomorphism from $\mathbf{A}|_X$ to $\mathbf{A}|_Y$.

Lattices. A *lattice* is an algebra $\langle A, \wedge, \vee\rangle$ such that the following properties hold for all $a, b, c \in A$:

$$\begin{array}{cc}
a \wedge (b \wedge c) = (a \wedge b) \wedge c & a \vee (b \vee c) = (a \vee b) \vee c \\
a \wedge b = b \wedge a & a \vee b = b \vee a \\
a \wedge a = a & a \vee a = a \\
a \wedge (a \vee b) = a & a \vee (a \wedge b) = a
\end{array}$$

The collection of all equivalence relations becomes a lattice by taking $\wedge$ to be set intersection and $\vee$ to be the transitive closure of the union of two equivalence relations (the transitive closure of a relation α is the smallest transitive relation containing α). Another example of a lattice is the set of natural numbers with $\wedge$ representing the highest common factor and $\vee$ representing the least common multiple. In a lattice, the operation $\wedge$ is referred to as the *meet* operation, and $\vee$ is called the *join* operation.

For any algebra **A**, Con **A** denotes the set of all congruences on **A**. It is a subset of the collection of all equivalence relations on A, and hence it forms a lattice **Con A**= $\langle \mathrm{Con}\,\mathbf{A}, \vee, \wedge\rangle$ called the *congruence lattice* of **A**. It is important to note that **Con A** is a *complete* lattice. That is, **Con A** is closed under infinite meets and joins.

An algebra **A** is called *simple* if **Con A** is a two element lattice. An equivalent condition to **A** having a two element congruence lattice is for **A** to have at least two elements and every homomorphism $f : \mathbf{A} \to \mathbf{B}$ is either one-to-one or constant.

Varieties and Free Algebras. Varieties are a central theme in the study of general algebras, as they offer a method of grouping algebras into classes based on some model. A class $\mathcal{K}$ of similar algebras is called a **variety** if and only if $\mathcal{K}$ is closed under the formation of homomorphic images (**H**), subalgebras (**S**), and direct products (**P**). The notation $\mathbf{V}(\mathcal{K})$ denotes the smallest variety containing $\mathcal{K}$, called the **variety generated by** $\mathcal{K}$. According to the HSP Theorem of G. Birkhoff, $\mathbf{V}(\mathcal{K}) = \mathbf{HSP}(\mathcal{K})$. There are numerous volumes on the theory of varieties; we will only mention here some fact we will need.

Let $\mathcal{K}$ be a class of similar algebras. Let an algebra **U** be similar to the elements of $\mathcal{K}$ (though **U** need not be in $\mathcal{K}$ itself). Let X be a subset of **U**. If **U** is generated by X, and if **U** has the property that for every $\mathbf{A} \in \mathcal{K}$ and for every mapping $\phi : X \to A$, there is an algebra homomorphism $\bar{\phi} : \mathbf{U} \to \mathbf{A}$ with $\bar{\phi}(x) = \phi(x)$ for every $x \in X$, we will say that $\mathbf{U}$ is a **free algebra in $\mathcal{K}$, freely generated by X**. Note that a free algebra $\mathbf{U}$ in $\mathcal{K}$ is determined up to an isomorphism which is the identity on the generating set X. If $|X|$ is finite, we will say $\mathbf{U}$ is *finitely generated.*

An important example of a free algebra is the so-called term algebra. Let σ denote the similarity type of a set I of operation symbols, and let $\mathcal{K}_\sigma$ be the class of all algebras with similarity type σ. Let X be a set disjoint from I. Let T be the smallest set of finite sequences from $X \cup I$ such that one-element sequences are in T, and if $Q \in I$, $\sigma(Q) = n$, and $w_1, \dots, w_n$ are in T, then $Qw_1w_2 \dots w_n \in T$. T becomes an algebra by taking the basic operations to be $Q(x_1, \dots, x_n) = Qx_1 \dots x_n$ where $Q \in I$ and $\sigma(Q) = n$. The algebra $\mathbf{T}$ is called the *term algebra of type σ over X*. The term algebra can be shown to be free in $\mathcal{K}_\sigma$ (see Section 4.11 of [MMT] for details).

We will often write an element t of the term algebra $t(x_1, \dots, x_n)$ where $x_1, \dots, x_n$ are those distinct elements of the generating set which appear in the sequence. Every element of the term algebra gives rise to a term operation $t^{\mathbf{A}}(a_1, \dots, a_n)$ on an algebra $\mathbf{A} \in \mathcal{K}_\sigma$ $(a_1, \dots, a_n \in \mathbf{A})$ via the algebra homomorphism $\phi : \mathbf{T} \to \mathbf{A}$ such that $\phi(x_1) = a_1, \dots, \phi(x_n) = a_n$ (such a homomorphism exists by our definition of free algebra). $t^{\mathbf{A}}$ is called the *interpretation* of t in $\mathbf{A}$.

When working with free algebras, we will be especially interested in the case where $\mathcal{K}$ is a variety, and we will write $\mathbf{F}_{\mathcal{K}}(X)$ to denote a free algebra in the variety $\mathbf{V}(\mathcal{K})$ with generating set X. An important theorem is the following:

Theorem 1.6. *Let $\mathcal{K}$ be a class of similar algebras such that $\mathbf{V}(\mathcal{K})$ contains a nontrivial member and let $\mathbf{T}$ be the term algebra of the same type over a finite generating set X. Let $p, q \in T$. Then $p^{\mathbf{A}} = q^{\mathbf{A}}$ for all $\mathbf{A} \in \mathcal{K}$ if and only if $p^{\mathbf{F}_{\mathcal{K}}(X)} = q^{\mathbf{F}_{\mathcal{K}}(X)}$*

Proof. [MMT] Theorem 4.127. □

2. Classification of Minimal Algebras

One of the driving results of tame congruence theory is the theorem of Palfy presented in this section. When considering a single algebra, a goal of the theory is to describe the structure of the algebra via a localization process. In a way, we try to describe the whole by its parts. Palfy's Theorem completely classifies algebras which are "small" in the following sense:

Definition 2.1. *Let* **A** *be a finite algebra. If f is either constant or a permutation for all $f \in \mathrm{Pol}_1(A)$, then* **A** *is called a* **minimal** *algebra.*

Examples.

- Any two element algebra is minimal.
- Since the unary polynomials in a vector space are of the form $ax + b$, where a is a scalar and b is a vector, any finite vector space is minimal.
- A set of permutations acting on a finite set, sometimes called a *unary permutational algebra* is minimal.

Indeed, P.P. Palfy proved that these are the *only* minimal algebras. It is common to further distinguish the two element algebras, as we will see at the end of this section. First, we introduce some terminology, notation, and an elementary result, stated without proof.

The reader is no doubt familiar with the concept of idempotence (e.g of an element, of a function of one variable, etc.), though perhaps not in exactly our framework. Nevertheless, our definition should not be too startling.

Definition 2.2. *An n-ary operation f on an algebra* **A** *is called* **idempotent in the i-th variable** *if the equation*

$$f(x_1, \ldots, x_{i-1}, f(x_1, \ldots, x_n), x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_n)$$

holds for all $x_1, \ldots, x_n \in A$.

In the general setting, we will refer to successive compositions in the same variable, so it will be useful to have the following notation:

Definition 2.3. *If $f(x_1, x_2, \ldots, x_n)$ is an n-ary operation in an algebra* **A**, *$i \leq n$ and $k \geq 0$, then we define $f^k_{(i)}(x_1, x_2, \ldots, x_n)$ inductively by*

$$\begin{aligned} f^0_{(i)}(x_1, \ldots, x_n) &= x_i \\ f^{k+1}_{(i)}(x_1, \ldots, x_n) &= f(x_1, \ldots, x_{i-1}, f^k_{(i)}(x_1, \ldots, x_n), x_{i+1}, \ldots, x_n). \end{aligned}$$

In the next lemma, we see an important consequence of finiteness: that given any operation, we may iterate it in one variable until it is idempotent in that variable. Idempotent operations are central to the study of tame congruence theory.

Lemma 2.4. *Let* **A** *be a finite algebra, let f be an n-ary operation on A, and let $1 \leq i \leq n$ be an integer. Then there exists an integer $k > 0$ such that $f^k_{(i)}(x_1, \ldots, x_n)$ is idempotent in the i-th variable.*

Proof. Lemma 4.4 in [HM]. □

Definition 2.5. *A ternary operation $t(x, y, z)$ on a set A is said to be a* **Mal'cev operation** *if it satisfies $t(x, x, y) = y = t(y, x, x)$ for all $x, y \in A$. An algebra* **A** *is said to be* **Mal'cev** *if it has a term operation which is a Mal'cev operation.*

Examples.

- $xy^{-1}z$ is a Mal'cev term operation on any group.
- $((x \wedge z) \vee y') \wedge (x \vee z)$ is a Mal'cev term operation on the two element Boolean algebra $(\{0,1\}, \wedge, \vee, ')$.

Definition 2.6. *An algebra $(G, \cdot)$, where $\cdot$ is a binary operation, is a* **quasigroup** *if the equations $a \cdot x = c$ and $y \cdot b = c$ have unique solutions in G for all $a, b, c \in G$.*

Note that this definition is equivalent to saying that $x{\cdot}a$ and $a{\cdot}x$ are permutations of G for all $a \in G$. The following lemma will be extremely useful, not only for classifying minimal algebras, but in later sections as well. Quasigroups are discussed in more detail in Chapter 4.

Lemma 2.7. *Every finite quasigroup is Mal'cev.*

Proof. [CV] Let $\mathbf{A} = (A, f)$ be finite quasigroup. By Lemma 2.4, we may choose $k \geq 0$ such that $f^k_{(1)}(x,y) = f^k_{(1)}(f^k_{(1)}(x,y), y)$ holds in $\mathbf{A}$. For all $a \in A$, the operation $f^k_{(1)}(x, a)$ is idempotent and a permutation of A by the note above. Since the only idempotent permutation is the identity, $f^k_{(1)}(x,a) = x$. Thus $f^k_{(1)}(x,y) = x$ holds for all $x, y \in A$, and if we define $d_1(x,y) = f^{k-1}_{(1)}(x,y)$, then $f(d_1(x,y), y) = x$. Note that $d_1(x,y)$ is a term operation. We may repeat this construction, iterating in the second variable this time, and get a term operation $d_2(x,y)$ such that $f(x, d_2(x,y)) = y$. Define

$$t(x,y,z) = f(d_1(x, d_2(y,y)), d_2(y,z)).$$

From our definition of $d_1(x,y)$, we have that $f(d_1(y, d_2(y,y)), d_2(y,y)) = y$ (by taking $y = d_2(y,y)$) and from our definiton of $d_2(x,y)$, we have $f(y, d_2(y,y)) = y$ (taking $x = y$). Since $\mathbf{A}$ is a quasigroup, there is a unique solution to $f(x, d_2(y,y)) = y$ for all $y \in A$, so we may conclude that $d_1(y, d_2(y,y)) = y$. Hence,

$$t(y,y,x) = f(y, d_2(y,x)) = x.$$

Again taking $y = d_2(y,y)$ in the definition of $d_1(x,y)$, we have

$$t(x,y,y) = f(d_1(x, d_2(y,y)), d_2(y,y)) = x.$$

□

The next few results will be stated without proof to ease the presentation of Palfy's Theorem. For a one-shot version of Palfy's Theorem, see [HM]. For proofs of these results, see [CV].

Theorem 2.8 (due to Smith and Gumm). *If $\mathbf{A}$ has a Mal'cev polynomial $t(x,y,z)$ and satisfies*

$$\forall \bar{u}\ \forall \bar{v}\ \forall y, z, \quad t(\bar{u}, y) = t(\bar{u}, z) \implies t(\bar{v}, y) = t(\bar{v}, z)$$

for all term operations $t(\bar{x}, y)$, then if $0 \in A$,

1. *$\mathbf{M} = (A, +, -, 0)$ is an abelian group with $a + b = t(a, 0, b)$ and $-a = t(0, a, 0)$,*
2. *$\mathbf{R} = \{p(x) \in \mathrm{Pol}_1(\mathbf{A}) : p(0) = 0\}$ is a subring of $\mathrm{End}(\mathbf{M})$, the ring of all endomorphisms of $\mathbf{M}$, and*
3. *$\mathbf{M}$ is an $\mathbf{R}$-module polynomially equivalent to $\mathbf{A}$.*

Lemma 2.9 (Twin Lemma I). *Let* $\mathbf{A}$ *be a minimal algebra with at least three elements and* $f(\bar{x}, y) \in \mathrm{Pol}(\mathbf{A})$. *If* $\bar{c}, \bar{d} \in A$, *then* $f(\bar{c}, y)$ *is a permutation of* A *iff* $f(\bar{d}, y)$ *is.*

Definition 2.10. *An* n*-ary polynomial* $f(x_1, \ldots, x_n)$ *is said to* **depend on** *the variable* x_i *if the unary polynomial* $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ *is nonconstant for some choice of the* a_j, $j \in \{1, \ldots, n\} - \{i\}$.

Lemma 2.11. *Let* $\mathbf{A}$ *be an algebra and suppose that* $f \in \mathrm{Pol}(\mathbf{A})$ *depends on at least* n *variables. Then for each* k, $1 \leq k \leq n$, $\mathbf{A}$ *has a* k*-ary polynomial operation that depends on all* k *variables.*

Theorem 2.12 (Palfy's Theorem). *If* $\mathbf{A}$ *is a finite minimal algebra with at least three elements, then either*

(1) *every basic operation of* $\mathbf{A}$ *depends on at most one variable, or*
(2) $\mathbf{A}$ *is polynomially equivalent to a vector space over a finite field.*

Proof. [CV] Assume that $f \in \mathrm{Pol}(\mathbf{A})$ depends on more than one variable. By Lemma 2.11, we may assume f is binary. Since $f(x, y)$ depends on x, there exists a $c \in A$ such that $f(x, c)$ is nonconstant. Since $\mathbf{A}$ is minimal, $f(x, c)$ must be a permutation. By the Twin Lemma (2.9), $f(x, c)$ is a permutation for *all* $c \in A$. Similarly, $f(c, y)$ is a permutation for all $c \in A$. As we noted above, this is sufficient to prove that (A, f) is a quasigroup. By Lemma 2.7, $\mathbf{A}$ has a Mal'cev term operation.

Now let $g(\bar{x}, y) \in \mathrm{Pol}(\mathbf{A})$ be any polynomial. Let $\bar{a}, \bar{b}, c, d \in A$, and suppose $g(\bar{a}, c) = g(\bar{a}, d)$. If $c = d$, then $g(\bar{b}, c) = g(\bar{b}, d)$, so assume $c \neq d$. Since c and d were arbitrary, $g(\bar{a}, y)$ must be constant. By the Twin Lemma, $g(\bar{b}, y)$ is also constant, so $g(\bar{b}, c) = g(\bar{b}, d)$. We have shown

$$\forall \bar{a}\ \forall \bar{b}\ \forall c, d\ \ g(\bar{a}, c) = g(\bar{a}, d) \implies g(\bar{b}, c) = g(\bar{b}, d)$$

for every polynomial $g(\bar{x}, y) \in \mathrm{Pol}(\mathbf{A})$. Hence we may apply Theorem 2.8 and conclude that $\mathbf{A}$ is polynomially equivalent to a module M over a ring R as defined in the theorem. Since $\mathbf{A}$ is minimal, every nonzero element p of R is a permutation, so it has an inverse which is in R because $p(0) = 0$. Thus, R is a finite division ring, that is, a field, so M is a vector space over a finite field. □

Corollary 2.13. *Let* $\mathbf{A}$ *be a finite minimal algebra. Then* $\mathbf{A}$ *is polynomially equivalent to one of the following (of which none are polynomially equivalent):*

(1) *a unary permutational algebra*
(2) *a vector space over a finite field*
(3) *the two-element boolean algebra*
(4) *the two-element lattice*
(5) *the two-element semilattice.*

We define the **type** *of a finite minimal algebra* $\mathbf{A}$, *denoted* $\mathrm{typ}(\mathbf{A})$, *to be the number in the enumeration of the algebra to which* $\mathbf{A}$ *is polynomially equivalent.*

We will prove the Corollary shortly, but first we present a lemma due to Werner, which can be found in [W].

Lemma 2.14 (The Composition Theorem for Operations). *Let A be a finite set and $0, 1 \in A$ with $0 \neq 1$. Let $\wedge$ and $\vee$ be binary operations on A satisfying $a \wedge 1 = a$, $a \wedge 0 = 0$, $a \vee 0 = a = 0 \vee a$ and for every $a \in A$, let*

$$g_a(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

be a unary operation on A. Let $\bar{x}$ be an n-tuple of indeterminants and $\bar{a}$ be an n-tuple of elements of A. Let

$$g_{\bar{a}}(\bar{x}) = (\ldots((g_{a_1}(x_1) \wedge g_{a_2}(x_2)) \wedge g_{a_3}(x_3)) \wedge \ldots) \wedge g_{a_n}(x_n).$$

Then every operation $f : A^n \to A$ can be written

$$f(\bar{x}) = \bigvee_{\bar{a} \in A^n} \{c^n_{f(\bar{a})}(\bar{x}) \wedge g_{\bar{a}}(\bar{x})\}$$

where $c^n_{f(\bar{a})}(\bar{x})$ is the n-ary constant operation which evaluates to $f(\bar{a})$.

Proof. This is essentially obvious from the definitions in the lemma. Note that all terms in the join are 0 except possibly one, so the fact that we did not assume commutativity or associativity is not a problem. □

Definition 2.15. *Let $\leq$ be a partial order on a set A. A function $f : A^n \to A$ is said to* **preserve** *$\leq$ if $f(a_1, \ldots, a_n) \leq f(b_1, \ldots, b_n)$ whenever $a_i \leq b_i$ for each $i = 1, \ldots, n$. f is said to be* **order-preserving** *if f preserves $\leq$ for every partial order $\leq$ on A.*

Lemma 2.16. *Let $\mathbf{A}$ be an algebra and $\leq \subset A^2$ a partial order on A. Suppose that*

$$\mathrm{Pol}(\mathbf{A}) \not\subseteq \bigcup_{n=1}^{\infty} \{g : A^n \to A \mid g \text{ is order-preserving}\}.$$

Then there exists $f \in \mathrm{Pol}_1(\mathbf{A})$ which does not preserve $\leq$.

Proof. Let $g \in \mathrm{Pol}_n(\mathbf{A})$ fail to preserve $\leq$. Then there exist n-tuples $\bar{a} = (a_1, \ldots, a_n)$ and $\bar{b} = (b_1, \ldots, b_n)$ such that $a_i \leq b_i$ for $i = 1, \ldots, n$ and $g(\bar{a}) \not\leq g(\bar{b})$. Starting at $i = 1$, we set each $a_i = b_i$ and observe the resulting change in $g(\bar{a})$. There exists a largest $j \in \{1, \ldots, n\}$ such that $g(b_1, \ldots, b_{j-1}, a_j, a_{j+1}, \ldots, a_n) \not\leq g(\bar{b})$. Thus, the unary polynomial $\bar{g}(x) = g(b_1, \ldots, b_{j-1}, x, a_{j+1}, \ldots, a_n)$ is not $\leq$-order-preserving. □

The proof of Corollary 2.13 will involve a systematic elimination of cases based on a few properties:

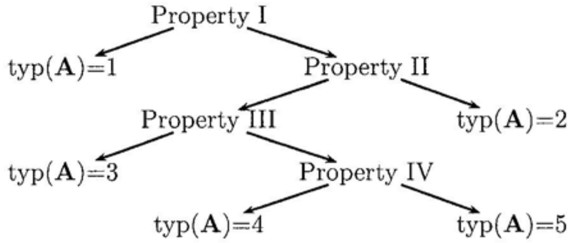
Property I: $\mathbf{A}$ has a binary polynomial f which depends on both variables.

Property II: For $f \in \mathrm{Pol}_2(\mathbf{A})$, $\forall a, b, c, d \in A$, $f(a, c) = f(a, d) \Rightarrow f(b, c) = f(b, d)$. (Compare to the condition in Theorem 2.8).

Property III: All polynomials on $\mathbf{A}$ are order-preserving.

Property IV: $\mathbf{A}$ is polynomially equivalent to a semilattice.

The following flowchart outlines the proof. If a Property holds, the proof progresses along the rightmost path.



A partial proof of the Corollary is given in [HM], with several things left as exercises. We present a complete proof, along the lines of [HM], with the details included.

Proof. One element algebras are trivially type 1, and the finite minimal algebras with at least three elements are handled by Palfy's Theorem, so suppose $\mathbf{A}$ is a two element minimal algebra.

If every basic operation of $\mathbf{A}$ depends on at most one variable, then every polynomial is either a constant or a permutation, so $\mathbf{A}$ is type 1. So assume $\mathbf{A}$ has a basic operation which depends on more than one variable. By Lemma 2.11, $\mathbf{A}$ has a binary polynomial operation f that depends on both variables. Suppose

$$(*) \qquad \forall a, b, c, d \in \{0,1\}, f(a,c) = f(a,d) \implies f(b,c) = f(b,d).$$

If $f(0,0) = 0$, then $f(0,1) = 1$ since, otherwise, $(*)$ implies that $f(1,0) = f(1,1)$ and f depends on only one variable. Now $f(1,0) = 1$ since $f(1,0) = 0$ will contradict either $(*)$ or the fact that f depends on both variables. Finally, by $(*)$, $f(1,1) = 0$. If $f(0,0) = 1$, then we may go through a similar argument and determine that the Cayley table for f is either

f	0	1
0	1	0
1	0	1

or

f	0	1
0	0	1
1	1	0

.

In the former case, $f(f(x,y),z)$ is a Mal'cev term, and in the latter case, $f(f(x,z),y)$ is a Mal'cev term. By Theorem 2.8, $\mathbf{A}$ is polynomially equivalent to a module. This module is a vector space over a finite field by the same argument as in the proof of Palfy's Theorem, so $\mathbf{A}$ is type 2.

Now suppose $(*)$ fails. Then there are $a, b, c, d \in \{0,1\}$ such that $f(a,c) = f(a,d)$ and $f(b,c) \neq f(b,d)$. This obviously requires that $a \neq b$ and $c \neq d$, so the Cayley table of f must contain exactly three zeros or three ones.

If $\mathbf{A}$ has a polynomial which is not order-preserving, then by Lemma 2.16, there is an operation $' \in \mathrm{Pol}_1(\mathbf{A})$ which is not order-preserving. There are only three partial orders on $\{0,1\}$, and the trivial one $\{(0,0),(1,1)\}$ is necessarily preserved by all polynomials. The other two are $\{(0,0),(1,1),(0,1)\}$ and $\{(0,0),(1,1),(1,0)\}$. Clearly, there is but one unary operation which fails to preserve one (and hence both) of these partial orders, so $'$ is the "negation" operation which swaps 0 and 1.

Recall that, by assumption, the Cayley table of $f(x,y)$ contains either three 0s or three 1s. If the table contains three 0s, it is straightforward to observe that one of $f(x,y)$, $f(x',y)$, $f(x,y')$ and $f(x',y')$ is a meet operation $\wedge$. Similarly, if the table contains three 1s, one of these four is a join operation $\vee$. Finally, $x \wedge y = (x' \vee y')'$ and $x \vee y = (x' \wedge y')'$, so $\mathrm{Pol}(\mathbf{A})$ contains the polynomial clone of the two-element Boolean algebra. The reverse inclusion is given by Lemma 2.14, so $\mathbf{A}$ is type 3.

Next, assume all polynomials on **A** are order-preserving.

It can be easily seen by examining cases that the join and meet operations

$$\begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \text{and} \qquad \begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

are the only two order-preserving binary operations on $\{0, 1\}$ which depend on both variables, so $\mathrm{Pol}(\mathbf{A})$ must contain at least one of these. Lattices contain both as basic operations, so the polynomial clone on the two-element lattice is the set of all order-preserving operations on $\{0, 1\}$. Without loss of generality, suppose $\wedge \in \mathrm{Pol}(\mathbf{A})$. A (meet) semilattice is an algebra which satisfies this criterion. If **A** is a semilattice, it is type 5.

Suppose there is $g \in \mathrm{Pol}_n(\mathbf{A})$ which is not a semilattice polynomial. We must show $\mathrm{Pol}(\mathbf{A})$ contains a join operation. Note that g is not constant, so both 0 and 1 are in the range of g.

For a set $I \subseteq \{1, \ldots, n\}$, let $x_I = (x_1, \ldots, x_n)$ be the n-tuple such that $x_i = 1$ if $i \in I$ and $x_i = 0$ otherwise. Since g is order-preserving, for $I \subseteq J \subseteq \{1, \ldots, n\}$ we have $g(x_I) \leq g(x_J)$. Since 1 is in the range of g, the set $\{I : g(x_I) = 1\}$ has at least one minimal member. If there is only one such set I_0, then $g(x_I) = 1$ if and only if $I_0 \subseteq I$, so

$$g(x_1, \ldots, x_n) = \bigwedge_{i \in I_0} x_i,$$

which contradicts the assumption that g is not a meet semilattice polynomial.

Thus, there are two distinct sets $I_1, I_2 \subseteq \{1, \ldots, n\}$ such that $g(x_{I_1}) = g(x_{I_2}) = 1$ and $g(x_J) = 0$ whenever $J \subsetneq I_1$ or $J \subsetneq I_2$. We create a binary operation $b(x, y)$ as follows: If $i \in I_1 - I_2$, replace x_i by x in g. If $i \in I_2 - I_1$, replace x_i by y in g. If $i \notin I_1 \cup I_2$, replace x_i by 0 in g. If $i \in I_1 \cap I_2$, replace x_i by 1 in g.

The resulting polynomial is $b(x, y)$. Observe that $b(1, 0) = g(x_{I_1}) = 1$ and $b(0, 1) = g(x_{I_2}) = 1$, while $b(0, 0) = g(x_{I_1 \cap I_2}) = 0$, so b is a join operation. Thus $\mathrm{Pol}(\mathbf{A})$ contains the polynomial clone of a lattice. It remains to show that the polynomial clone of a lattice contains the set of all order-preserving operations on $\{0, 1\}$.

Let $h : \{0, 1\}^n \to \{0, 1\}$ be order preserving. Then we claim

$$h(x_1, \ldots, x_n) = \bigvee \bigwedge_{i \in S} x_i.$$

where the join is taken over all sets $S \subseteq \{1, \ldots, n\}$ such that $h(x_S) = 1$.

If S is any subset of $\{1, \ldots, n\}$ such that $h(x_S) = 1$, then the expression

$$\bigwedge_{i \in S} x_i$$

will evaluate to 1. By joining over all such S, our expression for h is clearly 1 if $h(x_S) = 1$. Conversely, if our expression evaluates to 1, then the x_i are coordinates of an n-tuple x_T which is 1 in each coordinate x_S is 1 for each S such that $h(x_S) = 1$. That is, $S \subseteq T$ for every S such that $h(x_S) = 1$. Since h is order-preserving, $h(x_T)$ must be 1. Hence, our expression is 1 if and only if $h(x_1, \ldots, x_n) = 1$, so every order-preserving operation on $\{0, 1\}$ may be expressed as a polynomial on the two-element lattice.

So **A** is a lattice, and it is type 4.

It is obvious that a unary algebra is not polynomially equivalent to an algebra with operations which depend on two or more variables. We have seen that the two-element Boolean algebra is not polynomially equivalent to the lattice or semilattice because it has a polynomial which is not order-preserving. Putting a 0 into a polynomial which is a composition of meet operations must evaluate to 0, and dually, a 1 in a polynomial of joins must evaluate to 1, so semilattices are polynomially inequivalent to lattices. Finally, lattices, semilattices, and Boolean algebras all contain a non-Abelian operation, and hence are polynomially inequivalent to a vector space. Thus the five types are indeed distinct. □

3. Tame Quotients in Finite Algebras

Following [CV], we define a neighborhood of an algebra:

Definition 3.1. *A* **neighborhood** *of an algebra* $\mathbf{A}$ *is a subset* $U \subseteq A$ *such that* $U = e(A)$ *for some idempotent* $e \in \mathrm{Pol}_1(\mathbf{A})$.

Recall that a congruence on an algebra is an equivalence relation which is "compatible" with the basic operations, and hence the polynomials, of the algebra. The idea of tame congruence theory is to use the congruences of a finite algebra to reveal as much as possible about the algebra's polynomials. This is accomplished by looking at certain neighborhoods of the algebra, an idea we begin to develop now.

Definition 3.2. *Let* $\mathbf{A}$ *be an algebra and let* $U \subseteq A$. *Then the* **induced algebra** $\mathbf{A}|_U$ *is the algebra*

$$\langle U, \{f(\bar{x})|_U : f \in \mathrm{Pol}_n(\mathbf{A}), f(U^n) \subseteq U, n \text{ finite}\}\rangle$$

The following important theorem is due to Palfy and Pudlak.

Theorem 3.3. *Let* U *be a neighborhood of an algebra* $\mathbf{A}$. *Then the restriction map* $\theta \mapsto \theta|_U$ *from* $\mathrm{Con}(\mathbf{A})$ *to* $\mathrm{Con}(\mathbf{A}|_U)$ *is a surjective lattice homomorphism.*

Proof. [CV] Let e be an idempotent unary polynomial on $\mathbf{A}$ such that $e(A) = U$. Clearly, the mapping $\theta \mapsto \theta|_U$ sends θ to an equivalence relation on U. By Lemma 1.2, θ is compatible with all unary polynomials on $\mathbf{A}$, so its restriction is compatible with all restrictions of unary polynomials on $\mathbf{A}$. Thus $\theta|_U$ is a congruence.

That restriction preserves the meet of two congruences is straightforward, and hence restriction preserves the lattice order (which is defined as $a \leq b \Leftrightarrow a = a \wedge b$).

Claim: For $\alpha \in \mathrm{Con}(\mathbf{A}|_U)$,

$$\hat{\alpha} = \{\langle x, y\rangle \in A^2 : \langle ef(x), ef(y)\rangle \in \alpha \text{ for all polynomials } f\}$$

is the largest congruence on bf A whose restriction to U is α. In particular, the restriction map is surjective.

Proof of Claim: $\hat{\alpha}$ is obviously an equivalence relation on A. Let $\langle a, b\rangle \in \hat{\alpha}$ and $f \in \mathrm{Pol}_1(\mathbf{A})$. If g is another unary polynomial, $\langle egf(a), egf(b)\rangle \in \alpha$ by definition of $\hat{\alpha}$. So $\langle f(a), f(b)\rangle \in \hat{\alpha}$, and $\hat{\alpha}$ is a congruence by Lemma 1.2. $\alpha \leq \hat{\alpha}|_U$ is clear, and if $\langle a, b\rangle \in \hat{\alpha}|_U$, then $\langle e^2(a), e^2(b)\rangle = \langle a, b\rangle \in \alpha$, so $\hat{\alpha}|_U = \alpha$.

To finish the proof of the claim, let θ be another congruence such that $\theta|_U = \alpha$. Let $\langle a, b\rangle \in \theta$. Let f be an aribitrary unary polynomial. Then $\langle ef(a), ef(b)\rangle \in \theta$, and $\langle ef(a), ef(b)\rangle \in U^2$, so $\langle ef(a), ef(b)\rangle \in \theta|_U = \alpha$. By definition, $\langle a, b\rangle \in \hat{\alpha}$, $\theta \subseteq \hat{\alpha}$, and the claim is proven.

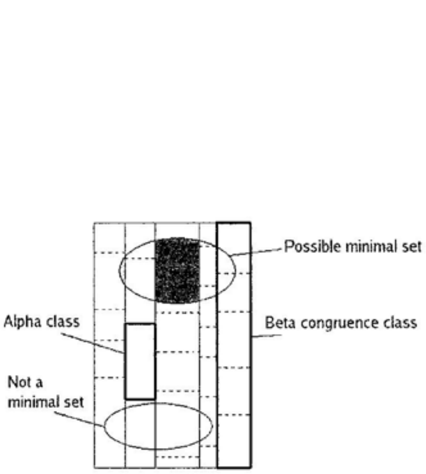
Finally, we show that restriction preserves joins. Let θ_1 and θ_2 be two congruences of $\mathbf{A}$. Let $\beta = \theta_1 \vee \theta_2$ and $\alpha = \theta_1|_U \vee \theta_2|_U$. Since $\theta_1, \theta_2 \leq \beta$, $\theta_1|_U, \theta_2|_U \leq \beta|_U$ because restriction preserves lattice order, and thus $\alpha \leq \beta|_U$. Conversely, $\theta_1|_U, \theta_2|_U \leq \alpha$, so $\theta_1, \theta_2 \leq \hat{\alpha}$ by the Claim. Thus $\beta \leq \hat{\alpha}$ and $\beta|_U \leq \hat{\alpha}|_U = \alpha$. □

Definition 3.4. *A pair* $\langle \alpha, \beta\rangle$ *with* $\alpha < \beta \in \mathrm{Con}(\mathbf{A})$ *in finite algebra* $\mathbf{A}$ *is called a* **congruence quotient** *of* $\mathbf{A}$.

The set of (α, β)**-separating** *polynomials of* $\mathbf{A}$ *is*

$$\mathrm{Sep}(\alpha, \beta) = \{f \in \mathrm{Pol}_1(\mathbf{a}) : f(\beta) \nsubseteq \alpha\}.$$

Let $U_{\mathbf{A}}(\alpha, \beta) = \{f(A) : f \in \mathrm{Sep}(\alpha, \beta)\}$. *The* (α, β)**-minimal sets** *are the elements of* $U_{\mathbf{A}}(\alpha, \beta)$ *which are minimal with respect to set inclusion. The set of* (α, β)*-minimal sets is denoted* $M_{\mathbf{A}}(\alpha, \beta)$.



The (α, β)-minimal sets for which $\alpha \prec \beta$ are the "certain neighborhoods" referred to above. We now prove that they are indeed neighborhoods.

Lemma 3.5. *Let $\alpha \prec \beta$ be congruences of a finite algebra $\mathbf{A}$. The (α, β)-minimal sets are neighborhoods of $\mathbf{A}$.*

Proof. [CV] Let $U \in M_{\mathbf{A}}(\alpha, \beta)$. Let $K = \{f \in \mathrm{Pol}_1(\mathbf{A}) : f(A) \subseteq U\}$. Observe that

$$\mu = \{\langle x, y\rangle \in \beta : \langle f(x), f(y)\rangle \in \alpha \text{ for all } f \in K\}$$

is an equivalence relation on $\mathbf{A}$. By Lemma 1.2, it suffices to show that μ is compatible with the unary polynomials. If $\langle a, b\rangle \in \mu$ and $g \in \mathrm{Pol}_1(\mathbf{A})$, then $fg \in K$, so $\langle fg(a), fg(b)\rangle \in \alpha$ for all $f \in K$. By definition of μ, $\langle g(a), g(b)\rangle \in \mu$. Thus μ is a congruence on $\mathbf{A}$.

Let $\langle x, y\rangle \in \alpha \prec \beta$. Then $\langle f(x), f(y)\rangle \in \alpha$ for all $f \in K$ because α is a congruence. Hence, by definition, $\alpha \leq \mu \leq \beta$, so μ is either α or β.

Since $U \in M_{\mathbf{A}}(\alpha, \beta)$, there is $h \in \mathrm{Sep}(\alpha, \beta)$ with $h(A) = U$. Since h separates β, let $\langle a, b\rangle \in \beta$ such that $\langle h(a), h(b)\rangle \notin \alpha$, and hence $\langle a, b\rangle \notin \mu$. Therefore, $\mu = \alpha$. By definition of μ, there is a $k \in K$ such that $\langle kh(a), kh(b)\rangle \notin \alpha$.

So $k(A), kh(A) \subseteq U$ and $kh(\beta) \nsubseteq \alpha$. By the minimality of U, $kh(A) = U$. Since $h(A) = U$, $k(U) = U$ and $k|_U$ is a permutation. Iterating k, we get an idempotent unary polynomial $e(x)$ with $e(A) = U$. □

Tame congruence theory takes its name from the next definition.

Definition 3.6. *A congruence quotient $\langle \alpha, \beta\rangle$ is called* **tame** *if there exist a set $V \in M_{\mathbf{A}}(\alpha, \beta)$ and an idempotent $e \in \mathrm{Pol}_1(\mathbf{A})$ such that $e(A) = V$ and $|_V$ is a lattice homomorphism such that the preimages of $\alpha|_V$ and $\beta|_B$ are α and β, respectively.*

A crucial result in the development of the theory was McKenzie's characterization of (α, β)-minimal sets through tame quotients. In particular, $M_{\mathbf{A}}(\alpha, \beta)$ is an equivalence class under polynomial isomorphism when $\langle \alpha, \beta\rangle$ is a tame quotient.

Theorem 3.7. *Let $\langle \alpha, \beta\rangle$ be a tame quotient of a finite algebra $\mathbf{A}$. Then,*

1. *Any two (α, β)-minimal sets are polynomially isomorphic.*
2. *Every (α, β)-minimal set U is a neighborhood; moreover, the map $|_U$ is (α, β)-separating.*
3. *For all $U \in M_{\mathbf{A}}(\alpha, \beta)$ and $f \in \mathrm{Pol}_1(\mathbf{A})$, if $f(\beta|_U) \nsubseteq \alpha$, then $f(U) \in M_{\mathbf{A}}(\alpha, \beta)$ and f is a polynomial isomorphism between U and $f(U)$.*

(4) *If* $\langle a,b\rangle \in \beta - \alpha$ *and* $U \in M_{\mathbf{A}}(\alpha,\beta)$*, then there exists a polynomial* $f \in \mathrm{Pol}_1(\mathbf{A})$ *such that* $f(A) = U$ *and* $\langle f(a), f(b)\rangle \notin \alpha$*.*

(5) *If* $U \in M_{\mathbf{A}}(\alpha,\beta)$*,* β *is the transitive closure of*

$$\alpha \cup \{\langle g(x), g(y)\rangle : \langle x,y\rangle \in \beta|_U \text{ and } g \in \mathrm{Pol}_1(\mathbf{A})\}.$$

(6) *If* $f \in \mathrm{Sep}(\alpha,\beta)$*, then there is a* $U \in M_{\mathbf{A}}(\alpha,\beta)$ *with* $U \simeq f(U)$*.*

Proof. The proof is rather long, although we have already proved (2), so it will be omitted here. See [HM] or [CV] complete proofs. □

Examples.

- If $\mathbf{A}$ is a simple algebra, then Sep(0,1) is the set of all nonconstant unary polynomials and $M_{\mathbf{A}}(0,1)$ is the set of all minimal ranges of such polynomials.
- If $\mathbf{A}$ is assumed to be minimal, then Sep(0,1) is the set of permutations on A, and $M_{\mathbf{A}}(0,1) = \{A\}$. Conversely, if $M_{\mathbf{A}}(0,1) = \{A\}$, then every element of Sep(0,1) maps A onto itself, that is, permutes the elements of A. But only constant maps can collapse the 1-congruence to 0, so $\mathbf{A}$ is minimal.
- If $\mathbf{A}$ is a finite, simple, nonabelian group (or even *loop*, which will be defined later), then the minimal sets are two-element boolean algebras. Moreover, $M_{\mathbf{A}}(0,1)$ contains *all* two-elements subsets of A. This result is highly nontrivial, particularly in the case of loops, and depends on the fact that every n-ary function on A is a polynomial.

Definition 3.8. *Let* $\mathbf{L}$ *be a lattice with a unique smallest element 0 and a unique largest element 1 relative to the lattice order. A lattice homomorphism* $f : L \longrightarrow L'$ *is called* $(0,1)$**-separating** *if* $f^{-1}\{f(0)\} = 0$ *and* $f^{-1}\{f(1)\} = 1$*.*

If $1 < |L| < \infty$*, every nonconstant lattice homomorphism is* $(0,1)$*-separating, and if, for every function* $\mu : L \to L$ *such that* $\mu(x) > x$ *and* $\mu(x \wedge y) = \mu(x) \wedge \mu(y)$*,* μ *is constant, then* $\mathbf{L}$ *is said to be a* **tight** *lattice.*

Example. The two-element lattice is tight. More generally, for any covering pair $\alpha \prec \beta$ in a finite lattice $\mathbf{L}$, the interval sublattice $I[\alpha,\beta] = \{\gamma \in \mathbf{L} : \alpha \leq \gamma \leq \beta\}$ is tight.

Theorem 3.9. *If* $\langle \alpha,\beta\rangle$ *is a congruence quotient of a finite algebra* $\mathbf{A}$ *such that* $I[\alpha,\beta]$ *is tight, then* $\langle \alpha,\beta\rangle$ *is tame.*

Proof. [HM] Let $U \in M_{\mathbf{A}}(\alpha,\beta)$. A rather technical argument, found in [HM], shows that since the interval lattice is tight, there is an idempotent unary polynomial e with $e(A) = U$ and $e(\beta) \nsubseteq \alpha$. Then the restriction $|_U$ considered as a map on $I[\alpha,\beta]$ is a non-constant, surjective lattice homomorphism by Theorem 3.3. Since $I[\alpha,\beta]$ is tight, $|_U$ is $(0,1)$-separating. □

Corollary 3.10. *Every congruence quotient* $\langle\alpha,\beta\rangle$ *of a finite algebra* $\mathbf{A}$ *such that* $\alpha \prec \beta$ *is tame.*

Due to this corollary, our analysis of finite algebras will be primarily concerned with covering pairs in the congruence lattice.

Definition 3.11. *Let* $\mathbf{A}$ *be a finite algebra,* $\alpha \prec \beta$ *congruences on* $\mathbf{A}$*, and* U *a set in* $M_{\mathbf{A}}(\alpha,\beta)$*. The* $\beta|_U$ *congruence classes which contain more than one* $\alpha|_U$ *congruence class are called* (α,β)**-traces**.

The union of all (α, β)-traces of U is called the **body** *of U. The remainder, $U - body(U)$ is called the* **tail** *of U.*

Note that every (α, β)-minimal set contains at least one (α, β)-trace by definition, and if $\beta = 1$, then the minimal set *is* the trace.

Proposition 3.12. *Any two (α, β)-traces of a finite algebra $\mathbf{A}$ are polynomially isomorphic.*

Proof. [CV] Proposition 2.12. □

Lemma 3.13. *Let $\alpha \prec \beta$ be congruences of a finite algebra $\mathbf{A}$.*

(1) $\mathrm{Pol}(\mathbf{A}/\alpha) = \{f_\alpha : f \in \mathrm{Pol}(\mathbf{A})\}$
(2) *If $M_{\mathbf{A}}(\alpha, \beta) = \{A\}$, then $M_{\mathbf{A}/\alpha}(0, \beta/\alpha) = \{A/\alpha\}$.*
(3) *If U is an (α, β)-minimal set of $\mathbf{A}$, then U/α is a $(0, \beta/\alpha)$-minimal set of $\mathbf{A}/\alpha$.*

Proof. [HM] (1): The set of all operations f on $\mathbf{A}$ such that f preserves α and $f_\alpha \in \mathrm{Pol}(\mathbf{A}/\alpha)$ is easily seen to be closed under compositions and to contain the constant operations, the trivial projection operations and the basic operations of $\mathbf{A}$ by our definition of quotient algebra. Thus $f \in \mathrm{Pol}(\mathbf{A}) \implies f_\alpha \in \mathrm{Pol}(\mathbf{A}/\alpha)$. The reverse inclusion follows similarly.

(2): Suppose $M_{\mathbf{A}}(\alpha, \beta) = \{A\}$ and that $f \in \mathrm{Pol}_1(\mathbf{A}/\alpha)$ and $f(\beta/\alpha) \nsubseteq 0$. By (1), we have that $f = g_\alpha$ for some $g \in \mathrm{Pol}_1(\mathbf{A})$, so there are $x/\alpha, y/\alpha \in \mathbf{A}/\alpha$ such that $\langle x/\alpha, y/\alpha\rangle \in \beta/\alpha$ but $\langle g_\alpha(x/\alpha), g_\alpha(y/\alpha)\rangle \notin 0$. That is, $\langle x, y\rangle \in \beta$ but $\langle g(x), g(y)\rangle \notin \alpha$. Since $M_{\mathbf{A}}(\alpha, \beta) = \{A\}$, g is a permutation of A. Thus $f(\mathbf{A}/\alpha) = \mathbf{A}/\alpha$, and by finiteness, f is a permutation. Thus every unary polynomial that does not collapse β/α to 0 is a permutation, so $M_{\mathbf{A}/\alpha}(0, \beta/\alpha) = \{A/\alpha\}$.

(3): Let $\alpha \prec \beta$ and $U \in M_{\mathbf{A}}(\alpha, \beta)$. By Theorem 3.7, there is an idempotent unary polynomial e such that $e(A) = U$ and $e(\beta) \nsubseteq \alpha$.

Claim: For any $f \in \mathrm{Pol}_1(\mathbf{A})$, $f(\beta) \nsubseteq \alpha \Leftrightarrow f_\alpha(\beta/\alpha) \nsubseteq 0$

Proof of Claim: Let $f \in \mathrm{Pol}_1(\mathbf{A})$.

$$\begin{aligned} f(\beta) \nsubseteq \alpha \quad &\Leftrightarrow \quad \exists \langle a, b\rangle \in \beta - \alpha \text{ such that } \langle f(a), f(b)\rangle \notin \alpha \\ &\Leftrightarrow \quad \exists \langle a/\alpha, b/\alpha\rangle \in \beta/\alpha - 0 \text{ such that } \langle f(a)/\alpha, f(b)/\alpha\rangle \notin 0 \\ &\Leftrightarrow \quad f_\alpha(\beta/\alpha) \nsubseteq 0 \end{aligned}$$

By the Claim, $e_\alpha(\beta/\alpha) \nsubseteq 0$. Since e is idempotent,

$$e_\alpha(e_\alpha(x/\alpha)) = e_\alpha(e(x)/\alpha) = e(e(x))/\alpha = e(x)/\alpha = e_\alpha(x/\alpha),$$

and $e_\alpha(A/\alpha) = e(A)/\alpha = U/\alpha$. So U/α is the image of a $(0, \beta/\alpha)$-separating polynomial. It remains to show U/α is minimal.

Let $f_\alpha \in \mathrm{Pol}_1(\mathbf{A}/\alpha)$ such that $f_\alpha(A/\alpha) \subseteq U/\alpha$ and $f_\alpha(\beta/\alpha) \nsubseteq 0$. It follows from part (1) that f_α corresponds to a unary polynomial f on $\mathbf{A}$ which is (α, β)-separating by the Claim. Let $y \in f(A)$. Since $f_\alpha(A/\alpha) \subseteq U/\alpha$, $y/\alpha \in U/\alpha$, that is, $\exists x \in U$ such that $x/\alpha = y/\alpha$. In particular, $y \in x/\alpha$, so $y \in U$. Therefore, $f(A) \subseteq U$, and $f(A) = U$ by the minimality of U. So $f_\alpha(A/\alpha) = U/\alpha$ and the result follows. □

Proposition 3.14. *If $\alpha \prec \beta$ are congruences in a finite algebra $\mathbf{A}$ and N is an (α, β)-trace, then $\alpha|_N$ is a congruence on $\mathbf{A}|_N$ and $\mathbf{A}|_N/\alpha|_N$ is a minimal simple algebra.*

Proof. [CV] By Lemma 3.13 (3), we can assume that $\alpha = 0$. We must show that every unary polynomial on $\mathbf{A}|_N$ is either constant or a permutation. Let $p(x) \in \text{Pol}_1(\mathbf{A}|_N)$, and let $q(x) \in \text{Pol}_1(\mathbf{A})$ such that $p(x) = q(x)|_N$ and $q(N) \subseteq N$. Let $U \in M_{\mathbf{A}}(0, \beta)$ minimal set containing N. Since there is an idempotent unary polynomial e on $\mathbf{A}$ with $e(A) = U$, we may assume $q(A) \subseteq U$ by replacing q by eq.

If p is not constant, then $q(\beta|_N) \nsubseteq 0$. By the minimality of U, $q(U) = U$. Since U is finite, q, and hence p, is a permutation of N.

Finally, since $0 \prec \beta$, $0|_N \prec \beta|_N$, and since N is a β-congruence class, the largest congruence on $\mathbf{A}|_N$ is $N \times N = \beta|_N$. So $\mathbf{A}|_N$ is simple. □

Thanks to Palfy's Theorem, we know all the minimal algebras. We called the type of a minimal algebra to be the number associated with its polynomial equivalent in the listing of Palfy's Theorem. We can now extend this defintion.

Definition 3.15. *Let $\alpha \prec \beta$ be congruences in a finite algebra $\mathbf{A}$. The* **type** *of the quotient $\langle \alpha, \beta \rangle$, written* $\text{typ}(\alpha, \beta)$, *is the type of the minimal algebra $\mathbf{A}|_N/\alpha|_N$ for any (α, β)-trace N.*

The **type set** *of a finite algebra $\mathbf{A}$ is the set*

$$\text{typ}\{\mathbf{A}\} = \{\text{typ}(\alpha, \beta) : \alpha \prec \beta \textit{ in } Con(\mathbf{A})\}.$$

Note that the type of a congruence quotient is well-defined by Proposition 3.12 and the fact that algebras induced by restriction to polynomially isomorphic subsets are isomorphic. Giving a type to each covering pair turns $\text{Con}(\mathbf{A})$ into a labelled lattice, so the definition of type set seems natural. Freese and Kiss [preprint] have shown that the type set actually depends only on the types of the join irreducibles with their unique lower cover, which considerably reduces the amount of computation needed to find an algebra's type set.

Lemma 3.16. *Isomorphic algebras have the same type set.*

Proof. Let $\pi : \mathbf{A} \to \mathbf{B}$ be an algebra isomorphism. Then, as a map of sets, $\pi : A \to B$ is a bijection, and h is an n-ary operation of $\mathbf{A}$ if and only if there exists a unique n-ary operation h' of $\mathbf{B}$ such that $\pi h(x_1, \ldots, x_n) = h'(\pi x_1, \ldots, \pi x_n)$. Hence the polynomial clones of $\mathbf{A}$ and $\mathbf{B}$ have the same cardinality, and corresponding polynomials "behave the same" when viewed as functions. As a result, θ is a congruence on $\mathbf{A}$ if and only if $\pi(\theta)$ is a congruence on $\mathbf{B}$. Moreover, given congruences α and β on $\mathbf{A}$, $f \in \text{Sep}(\alpha, \beta)$ if and only if there is a corresponding $f' \in \text{Sep}(\pi(\alpha), \pi(\beta))$ subject to the condition above. Since pairs of congruences and the polynomials which separate them determine the type of a congruence quotient, and hence the type set of an algebra, the type sets of $\mathbf{A}$ and $\mathbf{B}$ are identical. □

Lemma 3.17. *Let $\mathbf{A}$ be either unary or polynomially equivalent to a lattice or semilattice. Then $\mathbf{A}$ is not Mal'cev.*

Proof. To be a Mal'cev algebra, $\mathbf{A}$ must have a ternary term operation $t(x, y, z)$ such that $t(x, x, y) = y = t(y, x, x)$ for all $x, y \in A$. This obviously eliminates the possibility that a Mal'cev algebra is unary. If $\mathbf{A}$ is a lattice with at least two elements (we may make this assumption, since a one-element algebra is necessarily unary) and a Mal'cev term operation t, let $a < b \in \mathbf{A}$, $a \neq b$. Then $t(a, a, b) = b$ and $t(a, b, b) = a$. But t is a composition of join and meet operations, which are lattice order preserving, so t must preserve the lattice order as well, a contradiction. Hence

A cannot have a Mal'cev term. The polynomial clone of a semilattice is properly contained in the polynomial clone of a lattice, so a semilattice is not Mal'cev. □

Lemma 3.18. *If* **A** *is Mal'cev, then* typ$\{\mathbf{A}\} \subseteq \{2,3\}$.

Proof. [CV] If $\alpha \prec \beta$ are congruences on **A**, we must determine typ(α, β), that is, the type of the algebra $\mathbf{A}|_N/\alpha|_N$ for any (α, β)-trace N. Homomorphic images of Mal'cev algebras are easily seen to be Mal'cev, so we can replace **A** by $\mathbf{A}/\alpha$ and assume $\alpha = 0$. Let $p(x,y,z)$ be a Mal'cev polynomial, U be a $(0,\beta)$-minimal set, and N a $(0,\beta)$-trace in U. Let e be an idempotent unary polynomial whose range is U.

$e(p(x,y,x))|_N$ clearly satisfies the equations defining a Mal'cev operation, so we need only show that it is a polynomial of $\mathbf{A}|_N$. Let $a,b,c \in N$. Then $a \;\beta\; b$, so $e(p(a,b,c)) \;\beta\; e(p(b,b,c)) = c$ and N is the class of everything β-related to c, $e(p(a,b,c)) \in N$ for all $a,b,c \in N$. So $\mathbf{A}|_N$ is a minimal simple algebra with a Mal'cev polynomial, hence by the previous lemma, it has type 2 or 3. □

We conclude with our second "Twin Lemma". This one is due to Kiss, and will be of use to us later.

Definition 3.19. *Two n-ary polynomials $f(\bar{x})$ and $g(\bar{x})$ are called* **twins** *if there is a k-ary polynomial $p(\bar{x},\bar{y})$, $k > n$ and two tuples $\bar{a}$ and $\bar{b}$ such that $f(\bar{x}) = p(\bar{x},\bar{a})$ and $g(\bar{x},\bar{b})$. If the tuples come from the body of a minimal set, f and g are called* **body twins***.*

Theorem 3.20 (Twin Lemma II)**.** *Let $\alpha \prec \beta$ be congruences on a finite algebra* **A***. Suppose $M_{\mathbf{A}}(\alpha,\beta) = \{A\}$. If* **A** *has two unary body twins of which one is a permutation and the other is not, then the body B of* **A** *consists of a single (α,β)-trace which is a union of two α congruence classes. Furthermore,* **A** *has a polynomial which induces a semilattice operation on B/α, so* typ$(\alpha,\beta) \in \{3,4,5\}$.

Proof. [CV] Lemma 3.15. □

4. Ternary Rings and Projective Planes

Definition 4.1. *A* **ternary ring** *is an algebra* $\mathbf{R} = (R, T)$*, where* R *is a nonempty set containing (at least) the elements 0 and 1 and* $T : R \times R \times R \to R$ *satisfying:*

(i) For all a, b, c *in* R,

$$T(0, b, c) = T(a, 0, c) = c$$

$$T(1, a, 0) = T(a, 1, 0) = a$$

(ii) For a, b, c *in* R*, there exists a unique element* $z \in R$ *such that* $T(a, b, z) = c$.

(iii) If a,b,c,d are in R *with* $a \neq c$*, there exists a unique element* $z \in R$ *such that* $T(z, a, b) = T(z, c, d)$.

(iv) If a,b,c,d are in R *with* $a \neq c$*, there exists a unique ordered pair* $x, y \in R$ *such that* $T(a, x, y) = b$ *and* $T(c, x, y) = d$.

(v) If a,b,c are in R *with* $a \neq 0$*, there exist unique elements* $x, y \in R$ *such that* $T(x, a, b) = c$ *and* $T(a, y, b) = c$.

Since all ternary rings contain 0 and 1, we will, when necessary, consider these among the basic operations of the algebra.

Example. There are many examples of ternary rings in the literature. A large class of ternary rings comes from division rings. If $(D, +, \cdot, 0, 1)$ is a division ring, then (D, T) is a ternary ring where $T(a, b, c) = (a \cdot b) + c$. So in a sense, a ternary ring is a generalization of a division ring.

Given a ternary ring (R, T), we associate a geometry Π defined as follows. The set of points of the geometry is $P = \{(a, b) : a, b \in R\} \cup \{(m) : m \in R\} \cup \{\infty\}$, where ∞ is not in R. The lines L of the geometry are:

$$[m, k] \equiv \{(x, y) : y = T(x, m, k)\} \cup \{(m)\} \quad \text{for all } m, k \in R$$

$$[\infty, k] \equiv \{(k, y) : y \in R\} \cup \{\infty\} \quad \text{for all } k \in R$$

$$l_\infty \equiv \{(m) : m \in R\} \cup \{\infty\}.$$

Observe the following facts about Π.

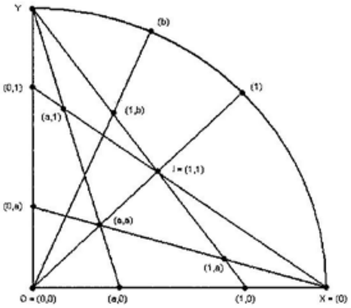
(1) Two points lie together on exactly one line.
(2) Two lines intersect in exactly one point.
(3) There exist four points, three of which are not on a line.

These three items axiomatize a class of geometric structures called **projective planes**. Conversely, from a given set of points and lines which satisfy the axioms of a projective plane, we may construct a ternary ring. The method we use is due to M. Hall and is outlined in [H]:

(1) In the projective plane, choose four points X, Y, O, I, no three on a line. We will refer to a line by naming two points, which is sufficient by Axiom 1.
(2) We will assign coordinates to each point in the plane, except those on the line XY, which we think of as the "line at infinity". To the point O assign the coordinates $(0, 0)$. To the point I assign the coordinates $(1, 1)$. Let $C = XY \cap OI$ and represent C by (1). Represent the point Y by (∞).
(3) For the remaining point of OI, assign the coordinates (a, a). Do not assign distinct points the same coordinates.

(4) Take any point P not on XY. Suppose YP intersects OI in a point with coordinates (a, a) and suppose XP intersects OI in a point with coordinates (c, c). Then assign P the coordinates (a, c).
(5) Designate the intersection of XY and $(0, 0)(1, b)$ by (b). The plane is now sufficiently coordinatized.
(6) If (x, y) is on the line $(0, c)(b)$, then we define $T(x, b, c) = y$.

Here is a diagram of what we're doing:



A Partial Coordinatization of a Projective Plane

Theorem 4.2. *Let* Π *be a projective plane. The ternary operation* $T(x, b, c)$ *defined above together with the set* $\{a : (a, a)$ *are the coordinates of a point on* $OI\}$ *forms a ternary ring.*

Proof. Observe that the points with coordinates $(0, a)$ lie on the line OY, points with coordinates $(a, 0)$ lie on OX, and the points represented by (b) lie on XY.

(i) $T(0, b, c) = c$ and $T(a, 0, c) = c$, $T(1, a, 0) = a$ and $T(a, 1, 0) = a$.

The line through $(0, c)$ and (b) intersects the line OY in exactly one point: $(0, c)$. Thus the second coordinate of a point $(0, y)$ on the line through $(0, c)$ and (b) is c, so $T(0, b, c) = c$. The line through $(0, 0)$ and $(1, 0)$ is OX, so X is represented by (0). The line through $(0, c)$ and $(0) = X$ intersects OI at (c, c), and hence any point on this line has second coordinate c, so $T(a, 0, c) = c$.

The point (a) lies on the line through $(0, 0)$ and $(1, a)$ by definition. Any point $P = (1, y)$ lies on the line through Y and $(1, 0)$. This line intersects the line through $(0, 0)$ and $(1, a)$ in exactly one point: $(1, a)$. So if P lies on $(0, 0)(1, a)$, $P = (1, a)$. Thus $T(1, a, 0) = a$. If $P = (a, y)$, then YP intersects OI in (a, a). If P also lies on $(0, 0)(1) = OI$, then P is the unique intersection of OI and YP, so $P = (a, a)$ and $T(a, 1, 0) = a$.

(ii) There is a unique element z such that $T(a, b, z) = c$.

z exists because the lines $(b)(a, c)$ and $(0, 0)Y$ intersect. The intersection is not on the line XY since $(b) \neq Y$, so it has some coordinates $(0, z)$. This intersection point is unique by Axiom 2.

(iii) If $a \neq c$, there is a unique z such that $T(z, a, b) = T(z, c, d)$.

Since $a \neq c$, the lines $(0, b)(a)$ and $(0, d)(c)$ do not intersect at a point on XY. Rather, they intersect at a unique point with coordinates (z, y).

(iv) If $a \neq c$, there is a unique ordered pair (x, y) such that $T(a, x, y) = b$ and $T(c, x, y) = d$.

The two points (a,b) and (c,d) determine a unique line. Since $a \neq c$, this line is not the line through $(a,0)$ and Y. Hence the line through (a,b) and (c,d) intersects XY in a unique point $(x) \neq Y$ and OY in a unique point $(0,y)$.

(v) If $a \neq 0$, there exist unique elements x and y such that $T(x,a,b) = c$ and $T(a,y,b) = c$.

We handle $T(x,a,b) = c$ first. In this case, the line $(a)(0,b)$ does not contain the point X since $a \neq 0$. The line through Y and (c,c) intersects $(a)(0,b)$, so there is a point $P = (x,c)$ on the line for some x, which is uniquely determined by the intersection of XP with OI.

Now we consider the case $T(a,y,b) = c$. Since $a \neq 0$, the line $(a,c)(0,b)$ does not contain Y, so it intersects XY in a unique point (y). □

So it is clear that every ternary ring determines a projective plane and vice versa. The process of constructing a ternary ring from a given projective plane does not, in general, yield a unique ternary ring. We will see that the induced ternary ring is unique up to a useful equivalence relation, however.

Definition 4.3. *Let $\mathbf{R}_1 = (R_1, T_1)$ and $\mathbf{R}_2 = (R_2, T_2)$ be ternary rings. An* **isotopism** *from $\mathbf{R}_1$ onto $\mathbf{R}_2$ is a set of three 1-1 functions $\{f,g,h\}$ from R_1 to R_2 such that $h(0) = 0$ and $h(T_1(a,b,c)) = T_2(f(a),g(b),h(c))$ for all $a,b,c \in R_1$. An isotopism in which h is the identity map is called a* **principal isotopism**.

One easily observes that ternary ring isotopy is an equivalence relation.

In his dissertation [K], Knuth proves several important facts about ternary ring isotopy. We state some of his results here without proof.

Theorem 4.4. *Let $\mathbf{R}$ be a ternary ring and let $y,z \in R$ be nonzero. Let $\phi = L_y$ be left multiplication by y (i.e. $L_y(x) = T(y,x,0)$) and let $\psi = R_z$ be right multiplication by z. If $f = \psi^{-1}$ and $g = \phi^{-1}$ and we define $T_1(a,b,c) = T(f(a),g(b),c)$, then $\mathbf{R}_1 = (R,T_1)$ is a ternary ring isotopic to $\mathbf{R}$ with $1_{R_1} = T(y,z,0)$. Furthermore, all ternary rings isotopic to $\mathbf{R}$ can be constructed this way, up to isomorphism.*

Theorem 4.5. *Isotopic ternary rings coordinatize isomorphic projective planes. Conversely, if an isomorphism of projective planes fixes the points with coordinates $(0,0)$, (0), and (∞) (defined above) then the ternary rings of the planes are isotopic.*

Corollary 4.6. *All isotopic ternary rings coordinatize the same projective plane. The automorphisms of a projective plane which fix the points with coordinates $(0,0)$, (0), and (∞) form a group isomorphic to the group of autotopisms of one of the plane's ternary rings.*

Theorem 4.7. *Let $\mathbf{R}$ be a ternary ring with n elements. The number of non-isomorphic ternary rings isotopic to $\mathbf{R}$ is at most $(n-1)^2$.*

Knuth observes that this estimate is best possible, as there is a ternary ring of order 32 with 31^2 non-isomorphic isotopes. Furthermore, if the ternary ring is a finite field, all isotopes of $\mathbf{R}$ are isomorphic to $\mathbf{R}$. We will come back to the notion of isotopy in the next chapter.

The connection between ternary rings and projective planes has been very useful in working towards the solution of a long outstanding problem related to *finite* projective planes; that is, planes whose set of points has finite cardinality. Here are three important, but elementary, facts about projective planes.

Lemma 4.8. *Let Π be a projective plane. If p is a point not on a line l in Π, then there is a one-to-one correspondence between the lines through p and the points on l.*

Theorem 4.9. *In a projective plane, the number of points on every line is the same, and that is the same as the number of lines through any point.*

Corollary 4.10. *If Π is a finite projective plane with $n+1$ points on every line, (and hence $n+1$ lines through every point) then Π has n^2+n+1 points and lines. Furthermore, by construction, the induced ternary ring contains n elements.*

Definition 4.11. *The number n in Corollary 4.10 is called the* **order** *of Π (or the order of the ternary ring $\mathbf{R}$).*

The open problem relating to finite projective planes is: For what values of n is there a projective plane of order n. The only known projective planes of finite order are those of prime power order (e.g. those coordinatized by finite fields).

The main (and only) result which eliminates an infinite class of possible orders is due to Bruck and Ryser.

Theorem 4.12. *If $n \equiv 1 (mod\ 4)$ or $n \equiv 2(mod\ 4)$, and n is not the sum of two squares, then there is no projective plane (or ternary ring) of order n.*

The only other result on this problem is that 10 is not the order of a projective plane or ternary ring, which was determined by an exhaustive computer search.

It is not the goal of this paper to produce a result on the possible orders of projective planes, but to use tame congruence analysis to see if any interesting or useful structure is shared among finite ternary rings which may lead to future results.

5. Quasigroups and Loops

The theory of binary systems figures prominently in the study of ternary rings. We will see how in a moment. Recall,

Definition 5.1. *An algebra $(G, \cdot)$, where $\cdot$ is a binary operation, is a* **quasigroup** *if the equations $a \cdot x = c$ and $y \cdot b = c$ have unique solutions in G for all $a, b, c \in G$. A quasigroup which has an identity element is called a* **loop**.

Examples.

- Any group is a loop.
- Any algebra $(G, \cdot)$, where $\cdot$ is a binary operation whose Cayley table is a latin square is a quasigroup.

Lemma 5.2. *Let $\mathbf{R} = (R, T)$ be a ternary ring. Then $(R, +)$ and $(R - \{0\}, \cdot)$, where $a + b = T(a, 1, b)$ and $a \cdot b = T(a, b, 0)$, are loops (called the addition and multiplication loops respectively).*

Proof. The fact that $(R, +)$ is a loop with identity 0_R follows immediately from properties (i), (ii), and (v) of ternary rings. Properties (i) and (v) show that $(R - \{0_R\}, \times)$ is a loop. □

Corollary 5.3. *The addition and multiplication loops of finite ternary rings are Mal'cev algebras, and their type sets are subsets of $\{2, 3\}$.*

Proof. This follows from Lemma 2.7 and Lemma 3.18. □

Observe that we could define $a + b = T(1, a, b)$ without affecting the conclusion of the lemma. Since loops are essentially just groups without associativity, many of the basic theorems of groups also hold in loops.

Lemma 5.4. *Let L be a finite set and let f be a binary operation on L such that (L, f) is a loop. Then for each $a \in L$, there is a least element $k \in \mathbb{Z}^+$ for which $f^{k-1}_{(1)}(a, a) = e$, where e is the identity element in (L, f).*

Proof. Since the positive integers are well-ordered, we need only show the existence of one such k.

Suppose $|L| = m$ for some $m \in \mathbb{Z}^+$. Then for $a \in L$, there are distinct $i, j \in \{1, 2, \ldots, m + 1\}$ with $i > j$ for which $f^{i}_{(1)}(a, a) = f^{j}_{(1)}(a, a)$. By definition, $f(f^{i-1}_{(1)}(a, a), a) = b = f(f^{j-1}_{(1)}(a, a), a)$ for some $b \in L$, and by property (iii) of loops, $f^{i-1}_{(1)}(a, a) = f^{j-1}_{(1)}(a, a)$. Repeating this argument $j - 1$ times, $f^{i-j}_{(1)}(a, a) = f^{0}_{(1)}(a, a) = a$.

So $f^{i-j}_{(1)}(a, a) = f(f^{i-j-1}_{(1)}(a, a), a) = a = f(e, a)$ by property (i) of loops, and so by the uniqueness in property (iii), $f^{i-j-1}_{(1)}(a, a) = e$. Since $i > j$, $k = i - j \in \mathbb{Z}^+$. □

Note: If the loop operation is addition or multiplication, we will write ka or a^k instead of $f^{k-1}_{(1)}(a, a)$. Keep in mind that this value is different, in general, than $f^{k-1}_{(2)}(a, a)$ or any other way of multiplying a by itself k times, since the loop need not be associative.

Definition 5.5. *Let (L, f) be a loop. If $a \in L$, then the* **order** *of a is the smallest integer $k \in \mathbb{Z}^+$ for which $f^{k-1}_{(1)}(a, a) = e$.*

Lemma 5.6. *Let (L, f) be a loop. If $a \in L$, $f_{(1)}^{l-1}(a,a) = e$ if and only if $k|l$ where k is the order of a.*

Proof. Suppose $f_{(1)}^{l-1}(a,a) = e$. If $l = k$, then $k|l$, so assume $l \neq k$. Since k is the smallest positive integer for which $f_{(1)}^{k-1}(a,a) = e$, $l > k$ and hence $l = kq + r$ for some $q, r \in \mathbb{Z}^+$, $0 \leq r < k$. Then $f_{(1)}^{l-1}(a,a) = f_{(1)}^{k-1}(a,a)$. As in the proof of the previous lemma, this means $f_{(1)}^{l-k}(a,a) = f_{(1)}^{0}(a,a) = a$, so $f_{(1)}^{l-k-1}(a,a) = e$. k is the smallest positive integer for which $f_{(1)}^{k-1}(a,a) = e$, so $l - k \geq k$. If $l - k = k$, then $l = 2k$ and $k|l$. Otherwise, $l - k > k$. Repeating this process $q - 1$ more times, we get $f_{(1)}^{l-kq}(a,a) = f_{(1)}^{0}(a,a) = a$. Now, $l = kq + r$, so we have $f_{(1)}^{r}(a,a) = f_{(1)}^{0}(a,a) = a = f_{(1)}^{k}(a,a)$. But $0 \leq r < k$, so $r = 0$, $l = kq$, and $k|l$.

Suppose $k|l$. Then for some $q \in \mathbb{Z}^+$, $l = kq$. If $q = 1$, then $f_{(1)}^{l-1}(a,a) = f_{(1)}^{k-1}(a,a) = e$. Assume inductively that the result holds for each integer n, $1 \leq n < q$. Then

$$\begin{aligned}
f_{(1)}^{k(q-1)-1}(a,a) &= e \\
f_{(1)}^{k(q-1)}(a,a) &= a = f_{(1)}^{0}(a,a) \\
f_{(1)}^{k(q-1)+1}(a,a) &= f_{(1)}^{1}(a,a) \\
&\dots \\
f_{(1)}^{k(q-1)+k-1}(a,a) &= f_{(1)}^{k-1}(a,a) = e
\end{aligned}$$

So $f_{(1)}^{l-1}(a,a) = f_{(1)}^{kq-1}(a,a) = e$. □

Definition 5.7. *Let $\mathbf{R} = (R, T)$ be a finite ternary ring. For all $x, y \in R$, define $\obslash : R \times R \to R$ to be the unique element $z \in R$ for which $T(x, 1_R, z) = y$. By condition (ii), this operation is well-defined. We will call the operation $\obslash$* **left subtraction**, *and instead of $\obslash(x, y)$, we will use the more conventional notation $x \obslash y$.*

Similarly, we define **right subtraction** *$\oslash : R \times R \to R$ to be the unique element $z \in R$ for which $T(z, 1_R, y) = x$.*

Lemma 5.8. *$\obslash$ is a term operation on* $\mathbf{R}$.

Proof. Let $\mathcal{V}(R)$ be the variety generated by the loop $(R, +)$ and let $\mathbf{F}$ be the free algebra in $\mathcal{V}(R)$ on two generators $F_{\mathcal{V}(R)}(x, y)$. Let B be the smallest subset of F containing y with the additional property that $b \in B \implies x + b \in B$. $\mathbf{F}$ is cancellative, since $(R, +)$ is a loop, so $b \mapsto x + b$ is a 1-1 map of B into B. The map is onto by the minimality of B. Thus $y = x + b$ for some $b \in B$. But $b \in \mathbf{F}$, so b is some term $t(x, y)$. By the definition of $\obslash$, and by Theorem 1.6, $\obslash = t(x, y)$ is a term operation on $\mathbf{R}$. □

The notion of isotopy in ternary rings we encountered earlier is a generalization of a similar notion used in the theory of binary systems.

Definition 5.9. *Let $(G,*)$ and $(H,\circ)$ be two quasigroups and let $\alpha,\beta,\gamma : G \to H$ be bijections. If $\alpha(x)\circ\beta(y) = \gamma(x*y)$ for all $x,y \in G$, then the triple (α,β,γ) is said to be a* **quasigroup isotopism** *of G onto H and G is said to be* **isotopic to** *or* **an isotope of** *H.*

Isotopy is easily seen to be an equivalence relation, and it is easily seen that our notion of isotopy in ternary rings reduces to isotopy in the multiplication loop by taking $c = 0$ in the definition of ternary ring isotopy. It is also clear that ternary ring principal isotopy reduces to isotopy in the addition loop.

Definition 5.10. *An isotopism (α,β,I_G) of $(G,*)$ onto $(G,\circ)$, where I_G denotes the identity map on G, is called a* **principal isotopism.**

Principal isotopism is also seen to be an equivalence relation. Now, given an isotopy (α,β,γ) of $(G,*)$ onto $(H,\circ)$, define $(G,\times)$ by

$$x \times y = \alpha^{-1}(\gamma(x)) * \beta^{-1}(\gamma(y))$$

so $(G,\times)$ is a principal isotope of $(G,*)$. Also,

$$\alpha(\alpha^{-1}(\gamma(x))) \circ \beta(\beta^{-1}(\gamma(y))) = \gamma(x)\circ\gamma(y) = \gamma(x \times y).$$

So we have proved:

Lemma 5.11. *Every isotope of a quasigroup is isomorphic to a principal isotope of the quasigroup.*

When we work with quasigroups it is useful to define two maps $L_x, R_x : Q \to Q$ from the quasigroup Q to itself for all $x,y \in Q$ by

$$L_x(y) = xy \qquad \text{and} \qquad R_x(y) = yx.$$

Since Q is a quasigroup, L_x and R_x are permutations of Q and hence have inverse maps L_x^{-1} and R_x^{-1}.

We now present part of a stronger theorem of Albert as published in his paper *Quasigroups I*.

Theorem 5.12. *If a loop (a quasigroup with a unique two-sided identity element) Q^0 is a principal isotope of a quasigroup Q with left and right multiplication as above, then*

1. *the principal isotopism is $(R_h^{-1}, L_g^{-1}, I_Q)$, and*
2. *right and left multiplication on Q^0 are given by $R_x^0 = R_{L_g^{-1}(x)}R_h^{-1}$ and $L_x^0 = L_{R_h^{-1}(x)}L_g^{-1}$*

for elements $g,h \in Q$ such that $f = gh$ is the identity element of Q^0.

Proof. [A] Suppose loop Q^0 is a principal isotope of Q and let L_x and R_x be left and right multiplication by x in Q. Let (α,β,I_Q) be the principal isotopism. Then $L_x^0 = L_{\alpha(x)}\beta$ and $R_x^0 = R_{\beta(x)}\alpha$. Let f be the identity element of Q^0. Then

$$R_f^0 = R_{\beta(f)}\alpha = I_Q^0 = L_f^0 = L_{\alpha(f)}\beta.$$

Put $g = \alpha(f)$ and $h = \beta(f)$. Then $f = \alpha^{-1}(g) = R_h(g) = gh$ and we have (1) and (2). □

Let's consider R_h^{-1} for a moment. This is the mapping from quasigroup Q to itself such that $R_h^{-1}(y)$ is the unique element $x \in Q$ for which $xh = y$. In other words, R_h^{-1} is right division by h and L_g^{-1} is left division by g.

In Lemma 5.8, we saw that left and right subtraction were term operations on the loop $(R, +)$. By changing the operation from addition to multiplication we have an analagous situation here, and hence R_h^{-1} and L_g^{-1} are in $\mathrm{Pol}_1(Q)$. But then the loop multiplication defined by

$$x *_{Q^0} y = R_h^{-1}(x) *_Q L_g^{-1}(y)$$

is a polynomial in Q, so $\mathrm{Pol}(Q^0) \subseteq \mathrm{Pol}(Q)$. If we let Q be a loop, and keep in mind that principal isotopy is an equivalence relation, we have the reverse inclusion as well, so

Lemma 5.13. *Principally isotopic loops are polynomially equivalent.*

Corollary 5.14. *Principally isotopic ternary rings are polynomially equivalent.*

Corollary 5.15. *Principally isotopic loops and ternary rings have the same congruences and the same congruence lattice.*

Corollary 5.16. *Principally isotopic loops and ternary rings have the same type set.*

Proof. By Lemma 5.13 and Corollary 5.15, the (α, β)-separating polynomials are the same and hence the (α, β)-minimal sets are the same. □

Corollary 5.17. *Isotopic loops and ternary rings have the same type set.*

Proof. By Lemma 5.11, Corollary 5.16, and the fact that isomorphic algebras have the same type set (Lemma 3.16). □

Consider the two quasigroups below.

$$Q_1 = \begin{array}{c|cccccc} * & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 2 & 4 & 6 & 3 & 1 & 5 \\ 3 & 3 & 6 & 1 & 5 & 4 & 2 \\ 4 & 4 & 1 & 5 & 2 & 6 & 3 \\ 5 & 5 & 3 & 4 & 6 & 2 & 1 \\ 6 & 6 & 5 & 2 & 1 & 3 & 4 \end{array} \qquad Q_2 = \begin{array}{c|cccccc} \circ & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 6 & 4 & 2 & 5 & 3 & 1 \\ 2 & 5 & 3 & 4 & 1 & 6 & 2 \\ 3 & 1 & 6 & 3 & 2 & 4 & 5 \\ 4 & 3 & 2 & 1 & 6 & 5 & 4 \\ 5 & 2 & 5 & 6 & 4 & 1 & 3 \\ 6 & 4 & 1 & 5 & 3 & 2 & 6 \end{array}$$

Q_1 is isotopic to Q_2, as $(Q_2, \circ)$ was defined by

$$x \circ y = \alpha(x) * \beta(y)$$

where $\alpha = (1345)(26)$ and $\beta = (125)(36)$ as permutations.

Using Ralph Freese's computer program, we compute the type set of each of these quasigroups and determine that $\mathrm{typ}(Q_1) = \{2\}$ and $\mathrm{typ}(Q_2) = \{3\}$. So isotopy, and in particular principal isotopy, does not preserve type sets in quasigroups.

6. The Type of a Finite Algebra with a Ternary Discriminator Term

Definition 6.1. *A* **ternary discriminator** *for an algebra* $\mathbf{A}$ *is a ternary operation* $d : A \times A \times A \to A$ *defined by*

$$d(x,y,z) = \begin{cases} x & \textit{if } x \neq y \\ z & \textit{if } x = y \end{cases}$$

Examples.

- Let $(A, +, -, \cdot, 0, 1, g)$ be a ring with the additional unary operation
$$g(x) = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$
A special case of such a ring is a finite field of characteristic $p > 0$ with $g(x) = x^{p-1}$. Then $t(x,y,z) = z + (x-z)g(y-x)$ is a ternary discriminator.
- $((x \wedge z) \vee y') \wedge (x \vee z)$ is a ternary discriminator on the two element Boolean algebra $(\{0,1\}, \wedge, \vee, ')$. Note that this was also given as an example of a Mal'cev term in Chapter 1. Indeed, we may observe that a ternary discriminator *is* a Mal'cev operation.

Corollary 6.2. *A finite algebra with a ternary discriminator term operation is a Mal'cev algebra.*

Lemma 6.3. *A finite algebra* $\mathbf{A}$ *with a ternary discriminator term operation is functionally complete.*

Proof. [W] Let $d(x,y,z)$ be the ternary discriminator term operation. Define $x \wedge y = d(y,1,x)$, $x \vee y = d(x,0,y)$, $\chi_0(x) = d(0,x,1)$, and for $a \neq 0$, $\chi_a(x) = d(0, d(a,x,0), 1)$. Then, by the Composition Theorem for Operations, every function $f : A^n \to A$ can be written as a composition of these and the n-ary constant operations. □

Corollary 6.4. *If* $\mathbf{A}$ *is a finite algebra with a ternary discriminator term operation, then* $\operatorname{typ}\{\mathbf{A}\} \subseteq \{2,3\}$.

Proof. By Lemma 3.18. □

Lemma 6.5. *A finite algebra* $\mathbf{A}$ *with a ternary discriminator term and all its subalgebras are simple, and hence tame.*

Proof. Let $\mathbf{S}$ be a subalgebra of $\mathbf{A}$ and let $0 \neq \theta \in \operatorname{Con}(\mathbf{S})$. Let $x, y \in S$, $x\theta y$, and $x \neq y$. Let $d(x,y,z)$ be the ternary discriminator term on $\mathbf{A}$. Then for each $z \in S$, we have $x = d(x,y,z)\theta d(x,x,z) = z$, so $\theta = 1$ and $\mathbf{S}$ is simple. Since $0 \prec 1$ in $\operatorname{Con}(\mathbf{S})$, the quotient $\langle 0, 1 \rangle$ is tame, so $\mathbf{S}$ is tame. □

Simple is bad from the point of view of trying to understand an algebra as a product of algebras. Nontrivial simple algebras are subdirectly irreducible, which means that if $\mathbf{A}$ is a simple algebra, $|A| > 1$, and

$$f : A \to \prod_{i \in I} A_i$$

is a one to one homomorphism and the projection of f onto each coordinate $f_i : A \to A_i$ is onto for all $i \in I$, then $\mathbf{A} \cong \mathbf{A}_i$ for some i.

Next, we prove that for any finite algebra $\mathbf{A}$ with a ternary discriminator as a term operation (a finite simple algebra), $\text{typ}\{\mathbf{A}\} = \{3\}$. In particular, we show all minimal subalgebras with more than one element are type 3.

Recall that the type set of a Mal'cev algebra is contained in $\{2, 3\}$. The type of a finite simple algebra, an algebra we have shown to be Mal'cev, is the type of the congruence quotient $\langle 0, 1\rangle$, which is given by the type of the minimal algebra formed by restricting to a (0,1)-trace. Note that, by definition, the (0,1)-traces (and hence (0,1)-minimal sets) of finite simple algebras must contain at least two elements.

Proposition 6.6. *If $\mathbf{A}$ is a finite simple algebra with more than one element and a ternary discriminator term operation $d(x, y, z)$, then all two-element subsets of A are $(0, 1)$-minimal. Moreover, if U is a $(0, 1)$-minimal set, then $|U| = 2$.*

Proof. Let $a, b \in A$, $a \neq b$. A has a ternary discriminator $d(x, y, z)$ as a term operation, and $d(a, d(a, x, b), b)$ is a unary polynomial on $\mathbf{A}$ which is nonconstant, and whose range is a two-element set. Moreover, $d(a, d(a, x, b), b)$ is idempotent. Thus, all two-element subsets of A arise as ranges of $(0, 1)$-separating idempotent polynomials, and since there are no one-element $(0, 1)$-minimal sets, all two-element subsets of A are $(0, 1)$-minimal.

By the discussion preceeding the proposition, $|U| \geq 2$. $U \in M_{\mathbf{A}}(0, 1)$, and since all two-element sets are in $M_{\mathbf{A}}(0, 1)$, there is a $V \in M_{\mathbf{A}}(0, 1)$ such that $V \subseteq U$ and $|V| = 2$. By definition of $M_{\mathbf{A}}(0, 1)$, $V = U$, so $|U| = 2$. □

Note: If $\mathbf{M}$ is any minimal subalgebra of $\mathbf{A}$ and $a, b \in A$ are distinct, then $d|_M(a, y, b)$ is a nonconstant unary polynomial on M with a two-element range. Since M is minimal, $d|_M(a, y, b)$ must be a permutation, so $|M| = 2$ and all minimal subalgebras of A with at least two elements are $(0, 1)$-minimal subalgebras.

Theorem 6.7. *If $\mathbf{A}$ is a finite algebra with a ternary discriminator term operation, then* $\text{typ}\{\mathbf{A}\} = \{3\}$.

Proof. To determine $\text{typ}\{A\}$, we need only determine $\text{typ}(0, 1)$, since A is simple. Consider a $(0, 1)$-minimal set U of A. Note that U is its own unique $(0, 1)$-trace. By Proposition 6.6, $\mathbf{A}|_U$ is a two-element algebra. Let $a, b \in U$ be distinct elements. Since A is functionally complete by Corollary 6.3, the function

$$n(x, y, u, v) = \begin{cases} u & \text{if } x = y \\ v & \text{if } x \neq y \end{cases}$$

is a polynomial on A. Observe that $n|_U(x, a, a, a)$ and $n|_U(x, a, b, a)$ are body twins. The former is clearly constant, while the latter is a permutation. By Lemma 3.20, $\text{typ}(0, 1) \in \{3, 4, 5\}$. But by Lemma 3.18, $\text{typ}(0, 1) \in \{2, 3\}$, so $\text{typ}\{\mathbf{A}\} = \{3\}$. □

Corollary 6.8. *In a finite algebra $\mathbf{A}$ with a ternary discriminator term, all minimal subalgebras of $\mathbf{A}$ with more than one element have type 3.*

The next theorem is an unpublished result of Ralph Freese.

Theorem 6.9. *A finite ternary ring has a ternary discriminator as a term operation.*

Proof. Let $(R, T, 0_R, 1_R)$ be a finite ternary ring. Recall the left subtraction operation $\oslash$ defined in Chapter 4. Observe that $x \oslash y = 0_R$ if and only if $x = y$. Hence, for any integer $n > 0$, $(x \oslash y)^n = 0_R$ if and only if $x = y$.

Suppose $x \neq y$. By Lemma 5.4, there exists a least element $k_{x,y} \in \mathbb{Z}^+$ for which $(x \oslash y)^{k_{x,y}} = 1_R$. Since R is finite, let

$$n = \text{lcm}\{k_{x,y} : x, y \in R, x \neq 0_R \neq y\}.$$

By Lemma 5.6, $(x \oslash y)^n = 1_R$ for all nonzero $x, y \in R$.

Define $d : R \times R \times R \to R$ by

$$d(x,y,z) = T(T((x \oslash y)^n, x, 0_R), 1_R, T(1_R \oslash (x \oslash y)^n, z, 0_R))$$

.

If $x = y$, then

$$\begin{aligned} d(x,y,z) &= T(T(0_R, x, 0_R), 1_R, T(1_R \oslash 0_R, z, 0_R)) \\ &= T(0_R, 1_R, T(1_R, z, 0_R)) \\ &= T(0_R, 1_R, z) \\ &= z \end{aligned}$$

If $x \neq y$, then

$$\begin{aligned} d(x,y,z) &= T(T(1_R, x, 0_R), 1_R, T(1_R \oslash 1_R, z, 0_R)) \\ &= T(x, 1_R, T(0_R, z, 0_R)) \\ &= T(x, 1_R, 0_R) \\ &= x \end{aligned}$$

So $d(x,y,z)$ is a ternary discriminator.

By Lemma 5.8, we have expressed $d(x,y,z)$ as a composition of term operations, so it is also a term operation. □

Corollary 6.10. *A finite ternary ring* $\mathbf{R}$ *is a simple, functionally complete Mal'cev algebra, and* typ$\{\mathbf{R}\} = \{3\}$.

The fact that finite ternary rings are all type 3 is a disappointment. There are representation theorems of tame congruence theory for tame algebras of types 1 and 2, and those of types 4 and 5 at least have some interesting properties. There are no representation theorems for type 3 akin to those for types 1 and 2, other than that such an algebra is isomorphic to a subreduct of a $[k]$-th matrix power of the two-element Boolean algebra, which is meaningless, since *every* algebra has this property [HM].

We thus proceed to analyze common algebraic structures associated with ternary rings.

Recall that we defined a multiplication operation on a ternary ring (R, T) by $a * b = T(a, b, 0)$. Throughout, let $\mathbf{A} = (R - \{0\}, *)$ and $\mathbf{B} = (R, *)$. We have already seen that $\mathbf{A}$ is a loop.

NOTE: $0 * a = a * 0 = 0$ for all $a \in R$, and by the uniqueness in part (v) of the definition of ternary ring, $x * y = 0$ if and only if x or y is 0. Thus A, the universe of $\mathbf{A}$, is also a subuniverse of $\mathbf{B}$. Subuniverses are closed under term operations, so $\text{Clo}(\mathbf{A}) = \{f|_A ; f \in \text{Clo}(\mathbf{B})\}$. All polynomial operations arise by substituting constants for variables in term operations, and, by the above, we see that substituting the constant 0 into a term operation results in the constant zero operation, so if $h \in \text{Pol}_n(\mathbf{B})$, $h(A^n) \subseteq A$. Thus $\text{Pol}(\mathbf{A}) = \{h|_A : h \in \text{Pol}(\mathbf{B}), h \neq 0\}$.

Lemma 6.11. *Let $\beta \in \mathrm{Con}(\mathbf{B})$. Then $|\,[0]_\beta\,| = 1$ if and only if $\beta \neq 1_{\mathrm{Con}(\mathbf{B})}$.*

Proof. ($\Rightarrow$) is obvious. Let $\beta \in \mathrm{Con}(\mathbf{B})$ and $0 \neq x \in R$. Let n be the multiplicative order of x. Suppose $0 \;\beta\; x$. Then

$(0{*}x^{n-1}) \;\beta\; (x{*}x^{n-1}) \Rightarrow 0 \;\beta\; 1_R \Rightarrow (0{*}y) \;\beta\; (1_R{*}y)$ for all $y \in R \Rightarrow 0 \;\beta\; y$ for all $y \in R \Rightarrow$ $y \;\beta\; z$ for all $y, z \in R \Rightarrow \beta = 1_{\mathrm{Con}(\mathbf{B})}$. □

Corollary 6.12. *There is a 1-1 correspondence between elements of* $\mathrm{Con}(\mathbf{A})$ *and* $\mathrm{Con}(\mathbf{B}) - \{1\}$ *which preserves the lattice order.*

Corollary 6.13. *Let $\alpha \prec \beta \in \mathrm{Con}(\mathbf{A})$. Let $\bar{\alpha}, \bar{\beta} \in \mathrm{Con}(\mathbf{B})$ be the corresponding congruences $\bar{\alpha} = \alpha \cup (0,0)$, $\bar{\beta} = \beta \cup (0,0)$. Then $\mathrm{typ}(\bar{\alpha}, \bar{\beta}) = \mathrm{typ}(\alpha, \beta)$.*

Proof. By the note above regarding the polynomials on each algebra, and with the observation that 0_R is in every $(\bar{\alpha}, \bar{\beta})$-minimal set, every (α, β)-minimal set U becomes $(\bar{\alpha}, \bar{\beta})$-minimal by $U' = U \cup 0_R$, and conversely every $(\bar{\alpha}, \bar{\beta})$-minimal set V becomes (α, β)-minimal by $V' = V \cap A$. But by Lemma 6.11, 0_R is in the tail of every $(\bar{\alpha}, \bar{\beta})$-minimal set, so $(\bar{\alpha}, \bar{\beta})$-traces N' are identical to (α, β)-traces N and the resulting minimal algebras $\mathbf{B}|_{N'}/\bar{\alpha}|_{N'}$ and $\mathbf{A}|_N/\alpha|_N$ are identical. □

So in $\mathrm{Con}(\mathbf{B})$ there is only one quotient whose type cannot be determined using elements from $\mathrm{Con}(\mathbf{A})$ - the quotient of $1_{\mathrm{Con}(\mathbf{B})}$ and its unique lower cover β (i.e. $1_{\mathrm{Con}(\mathbf{A})} \cup (0,0)$). Let U be a $(\beta, 1)$-minimal set. Then the tail is empty and the body consists of two β-classes, one of which is $\{0_R\}$. The restriction of the basic operation $*$ to U is obviously a semilattice operation on the minimal algebra $\mathbf{B}|_U/\beta|_U$. The algebra is clearly semilattice type since for every $h \in \mathrm{Pol}_2(\mathbf{B})$, $h(0,0) = h(0,1) = h(1,0) = 0$.

Recall that every finite quasigroup is a Mal'cev algebra, and that every such algebra has a type set contained in $\{2,3\}$. So $\mathrm{typ}\{\mathbf{A}\} \subseteq \{2,3\}$ and $\mathrm{typ}\{\mathbf{B}\} \subseteq \{2,3,5\}$. Whenever $\mathbf{R}$ is a finite field, $\mathbf{A}$ is an abelian group and every congruence quotient has type 2, so $\mathrm{typ}\{\mathbf{A}\} = \{2\}$. The following is a multiplication loop table derived from the Hall plane of order 9. Note that it is non-abelian.

·	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	6	8	7	3	5	4
3	3	6	4	7	1	8	2	5
4	4	8	1	5	6	2	3	7
5	5	7	8	1	3	4	6	2
6	6	3	5	2	8	7	4	1
7	7	5	2	6	4	1	8	3
8	8	4	7	3	2	5	1	6

Moreover, this loop is simple. (Since loops are so closely related to groups, many group theoretic concepts are generalized in loop theory. Moreover, many of the same theorems hold. In particular, we have a concept of normal subloop and a version of Lagrange's Theorem. For more on the theory of loops, see [B]). The possible orders of proper normal subloops are 2 and 4. There is no element of order

4 and only one of order 2, so a 4-subloop is impossible. There is only one 2-subloop, namely $\{1,2\}$. Computing,

$$(\{1,2\}3)4 = \{2,7\} \qquad \text{and} \qquad \{1,2\}(3 \cdot 4) = \{5,7\}$$

so $\{1,2\}$ is not normal. Thus this loop is simple and non-abelian. Such loops are functionally complete by a result of Lemieux in [L], and as a result, the type set is $\{3\}$. It is worth remarking that the addition loop of this ternary ring is $\mathbb{Z}_3 \times \mathbb{Z}_3$, an abelian group whose type set is $\{2\}$. There is absolutely no type correspondence between addition and multiplation loops of a given ternary ring.

The following is a multiplication loop table derived from the Andre plane of order 27. Its type set, computed by Ralph Freese's program, is $\{2,3\}$.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	2	6	18	16	9	5	25	19	4	1	17	13	23	8	11	7	10	20	24	14	26	21	22	12	15	3
3	3	23	16	24	18	19	21	4	22	8	26	2	9	6	14	20	13	15	25	10	1	11	7	17	12	5
4	4	16	20	11	25	7	10	24	15	9	6	23	22	19	2	17	5	14	12	8	3	26	21	13	1	18
5	5	9	14	25	16	4	11	12	7	6	1	22	21	24	10	15	2	8	13	19	18	3	26	23	17	20
6	6	5	24	7	4	9	15	22	16	2	10	3	18	23	17	25	1	12	21	13	8	14	20	26	11	19
7	7	25	12	10	11	15	2	21	17	16	9	18	20	22	5	1	4	13	26	23	19	8	14	3	6	24
8	8	3	6	22	19	23	20	2	18	13	14	11	1	17	12	24	26	4	9	25	15	16	5	7	21	10
9	9	4	26	15	7	16	17	14	25	5	2	24	12	20	1	11	6	3	8	18	22	23	13	19	10	21
10	10	1	22	9	6	2	16	18	5	17	15	8	19	3	25	4	11	21	20	26	13	12	24	14	7	23
11	11	17	8	6	1	10	9	13	2	15	7	21	26	12	16	5	25	19	23	24	20	18	3	22	4	14
12	12	14	1	3	13	26	19	10	8	21	24	25	17	15	22	23	20	5	6	16	7	9	2	4	18	11
13	13	8	10	18	23	3	24	17	19	26	12	7	11	25	21	22	14	6	2	4	16	5	1	9	20	15
14	14	26	15	23	8	13	18	25	3	12	20	9	7	4	24	19	21	10	17	6	5	1	11	2	22	16
15	15	11	23	2	10	17	5	3	1	25	16	14	8	26	4	6	7	22	18	21	12	24	19	20	9	13
16	16	7	19	17	15	25	1	23	11	4	5	26	3	13	6	10	9	24	22	12	14	20	18	21	2	8
17	17	10	21	5	2	1	4	20	6	11	25	19	24	18	7	9	15	26	14	3	23	13	12	8	16	22
18	18	22	2	12	20	24	26	1	21	19	3	15	10	11	8	14	23	9	5	7	25	4	6	16	13	17
19	19	18	17	21	24	22	14	11	20	23	8	16	15	7	13	12	3	2	1	9	4	6	10	5	26	25
20	20	21	11	13	14	12	3	15	26	24	18	4	25	16	19	8	22	1	10	5	9	2	17	6	23	7
21	21	12	9	8	26	14	23	5	13	20	22	10	6	1	18	3	24	7	16	11	17	25	4	15	19	2
22	22	24	5	14	21	20	13	6	12	18	23	17	2	10	3	26	19	16	4	15	11	7	9	25	8	1
23	23	19	25	20	22	18	12	7	24	3	13	5	16	9	26	21	8	17	11	2	6	10	15	1	14	4
24	24	20	7	26	12	21	8	16	14	22	19	6	4	5	23	13	18	11	15	1	2	17	25	10	3	9
25	25	15	13	1	17	11	6	26	10	7	4	20	14	21	9	2	16	23	3	22	24	19	8	18	5	12
26	26	13	4	19	3	8	22	9	23	14	21	1	5	2	20	18	12	25	7	17	10	15	16	11	24	6

This completes a set of examples showing that we cannot restrict type sets of multiplication loops in any way beyond what is done by the Mal'cev term. Similar examples can be given for the addition loops.

Concluding Remarks. We have seen that a tame congruence analysis of finite ternary rings in general leads essentially nowhere. The most encouraging results came from examining isotopy. We saw a definition of isotopy in ternary rings which reduced to the usual notion of isotopy in the multiplication and addition loops of the ternary ring. The key theorem with regard to isotopy is that isotopic ternary rings coordinatize isomorphic projective planes, and a partial converse. The full converse can be easily demonstrated to be false by generating two ternary rings from the same projective plane whose addition loops have different type sets. I have done this with a semifield plane of order 16. One wonders if loop isotopy is enough to force ternary ring isotopy. That is, are ternary rings with isotopic multiplication or addition loops isotopic?

References

[A] A. Albert
[B] R. H. Bruck
[CV] M. Clasen and M. Valeriote
[GK] E. G. Goodaire and M.J. Kallaher
[H] M. Hall
[HM] D. Hobby and R. McKenzie
[K] D. Knuth
[L] C. Lemieux
[MMT] R. McKenzie, G. McNulty, W. Taylor
[W] H. Werner