FINITE EQUATIONAL BASES
FOR UNIVERSAL ALGEBRAS

A Thesis Abstract
Presented to
the Faculty of Graduate Studies
University of Manitoba

In Partial Fulfillment
of the Requirements for the Degree
Master of Arts

---

by
Theodore Alexander Galay
April 1968

THESIS ABSTRACT

This thesis is concerned with the problem of determining under what conditions the identities holding in a universal algebra can be formally deduced from a finite subset (a finite equational basis) of these identities. After a preliminary review of the basic results of Universal Algebra, the problem is considered in its most general form, and some results about the concept of deducibility are obtained. Then the effect of the number of elements in a finite algebra upon its possession of a finite equational basis is investigated. Finally, further results in the field are stated and discussed, to provide a review of the research to date.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Prof. G. Gratzer, for his kind assistance, and for making available to me various unpublished results.

I would also like to thank the administrative staff of Brandon University for their assistance in preparing the final copies of this thesis.

CHAPTER I

PRELIMINARIES

The purpose of this chapter is to introduce the basic concepts and theorems of Universal Algebra which will be required in the remainder of the discussion. The results are presented without proof, and the reader is referred to G. Gratzer's Universal Algebra [3] for full details.

1. Universal Algebras

Definition 1.1: A type τ is a sequence of non-negative integers, $\langle n_0, n_1, \ldots n_\gamma, \ldots \rangle$, $\gamma < o(\tau)$, where $o(\tau)$ is an ordinal number called the order of the type.

For each $\gamma < o(\tau)$, we introduce a symbol $\underline{f}_\gamma$, called an operation symbol.

Definition 1.2: An algebra $\mathfrak{A} = \langle A; F \rangle$ of type τ is an ordered pair, where A is a non-void set, and $F = \langle f_0, f_1, \ldots f_\gamma, \ldots \rangle$, $\gamma < o(\tau)$, is a sequence of operations on A.

f_γ is an n_γ- ary operation, called the realization of $\underline{f}_\gamma$ in $\mathfrak{A}$. If $n_\gamma = 0$, f_γ is a nullary operation; that is, a mapping f_γ: $A^\circ = \{\emptyset\} \longrightarrow A$, and so effectively picks out an element $a = f_\gamma(\emptyset)$ from A. We will often denote f_γ by a in this case.

If $\mathfrak{A}$ and $\mathfrak{B}$ are algebras of the same type, we denote the realizations of $\underline{f}_\gamma$ in both algebras by f_γ. If there is danger of confusion, we will use the notation $(f_\gamma)_{\mathfrak{A}}$ and $(f_\gamma)_{\mathfrak{B}}$. Thus, in general, we will write $\mathfrak{A} = \langle A;F\rangle$ and $\mathfrak{B} = \langle B;F\rangle$.

<u>Definition 1.3</u>: An algebra will be said to be <u>A-finite</u> if the set of elements upon which it is defined is finite, and <u>F-finite</u> if the set of operations is finite. An algebra is <u>finite</u> if it is both A-finite and F-finite. When an algebra is F-finite, so that the set of operations has the form $\langle f_0, f_1, \ldots f_{n-1}\rangle$, we will write $\mathfrak{A} = \langle A; f_0, f_1, \ldots f_{n-1}\rangle$.

We denote by $K(\tau)$ the class of all algebras of type τ.

Definition 1.4: Let $\mathfrak{A}$ and $\mathfrak{B}$ $\in K(\tau)$. Then a mapping δ: $A \longrightarrow B$ is a homomorphism if

$$f_\gamma(a_0, a_1, \ldots a_{n_\gamma -1})\delta = f_\gamma(a_0\delta, a_1\delta, \ldots a_{n_\gamma -1}\delta)$$

for all $f_\gamma \in F$, and all $a_i \in A$. The concepts of endomorphism, isomorphism, and automorphism are then defined in the usual manner.

Definition 1.5: An equivalence relation Θ on A is a congruence relation on $\mathfrak{A} = \langle A;F \rangle$ if $a_i \equiv b_i(\Theta)$ implies

$$f_\gamma(a_0, a_1, \ldots a_{n_\gamma -1}) \equiv f_\gamma(b_0, b_1, \ldots b_{n_\gamma -1})\ (\Theta)$$

for all $f_\gamma \in F$.

If Θ is a congruence relation on $\mathfrak{A}$, we can define a factor algebra $\mathfrak{A}/\Theta = \langle A/\Theta; F \rangle$ in the usual manner. If δ: $\mathfrak{A} \longrightarrow \mathfrak{B}$ is a homomorphism, then the relation Θ on A defined by: $a \equiv b(\Theta)$ if and only if $a\delta = b\delta$, is a congruence on $\mathfrak{A}$. Furthermore, $\mathfrak{A}/\Theta$ is isomorphic to $\langle A\delta; F \rangle$. There are two trivial congruence relations on any algebra: the relation of equality, and the total relation, where any two elements are congruent.

2. Polynomials and Polynomial Symbols

Definition 1.6: The n-ary polynomials of an algebra $\mathfrak{A}$ are functions from $A^n \longrightarrow A$, defined as follows:

(i) The projections $e_i^n(x_0, x_1, \ldots x_{n-1}) = x_i$, for $i = 0, 1, \ldots n-1$, are n-ary polynomials. In practice, the function e_i^n is identified with the variable x_i.

(ii) If $p_0(x_0, \ldots x_{n-1}), p_1(x_0, \ldots x_{n-1}), \ldots p_{n_\gamma -1}(x_0, \ldots x_{n-1})$ are n-ary polynomials, then so is $f_\gamma(p_0, p_1, \ldots p_{n_\gamma -1})(x_0, \ldots x_{n-1}) = f_\gamma(p_0(x_0, \ldots x_{n-1}), \ldots p_{n_\gamma -1}(x_0, \ldots x_{n-1}))$.

(iii) The n-ary polynomials of the algebra are those, and only those, which can be obtained from (i) and (ii) in a finite number of steps.

Equality of n-ary polynomials is equality of functions.

We can extend this definition to α-ary polynomials, where α is an arbitrary ordinal number, by considering functions from A^α into A. We need only replace $e_i^n(x_0, \ldots x_{n-1})$ by $e_i^\alpha(x_0, \ldots x_\gamma, \ldots)$, $\gamma < \alpha$. Then every α-ary polynomial depends upon only a finite number of its variables, and every n-ary polynomial can be extended to an α-ary polynomial by the introduction of dummy variables. Since every α-ary polynomial is essentially finite, it is usually most convenient to consider

ω-ary polynomials, where ω is the order type of the natural numbers. We obtain essentially the same operations on A as we would from the n-ary polynomials, n = 0, 1, 2,..., with the advantage that we can discuss the equality of functions without considering their arities.

A nullary operation is an α-ary polynomial for every α, and nullary polynomials exist if and only if there are nullary operations.

We will write $p(x_0, x_1, \ldots x_{n-1})$ to mean that the set of variables upon which the function p depends is contained within the set $\{x_0, x_1, \ldots x_{n-1}\}$.

Definition 1.7: The n-ary polynomial symbols of type τ are defined as follows:

(i) $\underline{x}_0, \underline{x}_1, \ldots \underline{x}_{n-1}$ are n-ary polynomial symbols.

(ii) If $\underline{p}_0, \underline{p}_1, \ldots \underline{p}_{n_\gamma -1}$ are n-ary polynomial symbols, then so is $\underline{f}_\gamma(\underline{p}_0, \underline{p}_1, \ldots \underline{p}_{n_\gamma -1})$.

(iii) The n-ary polynomial symbols are those, and only those, which can be obtained from (i) and (ii) in a finite number of steps.

Again, we can extend the above definition for an arbitrary ordinal α by modifying clause (i) to admit $\underline{x}_0, \underline{x}_1, \ldots \underline{x}_\gamma, \ldots, \gamma < \alpha$, as α-ary polynomial symbols.

Nullary polynomial symbols exist if and only if nullary operation symbols exist in the type τ. If a is a nullary operation, then $\underline{a}$ will denote the corresponding symbol.

We will write $\underline{p}(\underline{x}_0, \underline{x}_1, \ldots \underline{x}_{n-1})$ to indicate that the set of variable symbols occurring in $\underline{p}$ is contained within the set $\{\underline{x}_0, \underline{x}_1, \ldots \underline{x}_{n-1}\}$. The expression $\underline{p}(\underline{r}_0, \underline{r}_1, \ldots \underline{r}_{n-1})$ will denote the polynomial symbol which results from replacing each occurrence of $\underline{x}_i$ by the polynomial symbol $\underline{r}_i$ in $\underline{p}$.

If infix notation is used for operations, the same notation will be used for the corresponding operation symbol, as, for example, in $\underline{x}_0 + \underline{x}_1$. The context will make clear whether the operation + or the operation symbol + is intended. When only several variable symbols are involved in a polynomial symbol, we will use the more usual $\underline{x}, \underline{y}, \underline{z}, \underline{u}, \underline{v}, \underline{w}, \ldots$, instead of $\underline{x}_0, \underline{x}_1, \underline{x}_2, \ldots$.

As with polynomials, we will henceforth consider all polynomial symbols to be ω-ary, unless otherwise stated.

Definition 1.8: Let $\underline{p}$ by a polynomial symbol of type τ and $\mathfrak{A}$ an algebra of type τ. Then the polynomial induced in $\mathfrak{A}$ by $\underline{p}$ is defined as follows:

(i) $\underline{x}_i$ induces $e_i^{\omega}(x_0, x_1, \dots x_\gamma, \dots)$.

(ii) If $\underline{p}$ is $\underline{f}_\gamma(\underline{p}_0, \underline{p}_1, \dots \underline{p}_{n_\gamma - 1})$, and if $\underline{p}_i$ induces $p_i(x_0, \dots x_\gamma, \dots)$, then $\underline{p}$ induces $f_\gamma(p_0, \dots p_{n_\gamma - 1})(x_0, \dots x_\gamma, \dots)$.

Definition 1.9: Let $\underline{P}(\tau)$ denote the ω-ary polynomial symbols of type τ. Then for $f_\gamma \in F$, and $\underline{p}_0, \dots \underline{p}_{n_\gamma - 1} \in \underline{P}(\tau)$, we define:

$$f_\gamma(\underline{p}_0, \dots \underline{p}_{n_\gamma - 1}) = \underline{f}_\gamma(\underline{p}_0, \dots \underline{p}_{n_\gamma - 1}).$$

Then we get an algebra of type τ :

$$\mathfrak{P}(\tau) = \langle \underline{P}(\tau); F \rangle$$

called the polynomial algebra of type τ.

Similarly, we can define the α-ary polynomial algebra $\mathfrak{P}^{(\alpha)}(\tau)$, using α-ary polynomial symbols.

3. Subterms

Definition 1.10: For each polynomial symbol $\underline{p}$ of type τ, we define a set $s(\underline{p}) \subseteq \underline{P}(\tau)$ called the set of subterms of $\underline{p}$:

(i) $s(\underline{x}_i) = \{\underline{x}_i\}$

(ii) If $\underline{p}$ is $\underline{f}_\gamma(\underline{p}_0, \underline{p}_1, \ldots \underline{p}_{n_\gamma-1})$, then $s(\underline{p}) =$

$$\{\underline{p}\} \cup s(\underline{p}_0) \cup s(\underline{p}_1) \cup \ldots \cup s(\underline{p}_{n_\gamma-1}).$$

A polynomial symbol $\underline{q}$ is a subterm of $\underline{p}$ if $\underline{q} \in s(\underline{p})$.

We speak of the occurrence of a subterm $\underline{q}$ if we wish to emphasize its position in $\underline{p}$ as well as its form. Let $os(\underline{p})$ be the set of all occurrrences of subterms of $\underline{p}$. Then $s(\underline{p}) \subseteq os(\underline{p})$, with distinct occurrences of $\underline{q}$ as a subterm of $\underline{p}$ counting as distinct elements of $os(\underline{p})$.

We define a partial order $\subseteq$ on $os(\underline{p})$ as follows: $\underline{r} \subseteq \underline{q}$ if and only if $\underline{r} \in os(\underline{q})$. If $\underline{p}$ is $\underline{f}_\gamma(\underline{p}_0, \ldots \underline{p}_{n_\gamma-1})$, then the branches of $\langle os(\underline{p}); \subseteq \rangle$ are the partially ordered sets $\langle os(\underline{p}_i); \subseteq \rangle$. It is clear that the inclusion diagram for $\langle os(\underline{p}); \subseteq \rangle$ is a reverse tree, in the sense that distinct branches of $\langle os(\underline{q}); \subseteq \rangle$ are disjoint for any $\underline{q} \in os(\underline{p})$.

Definition 1.11: $\underline{q}$, $\underline{r} \in$ os($\underline{p}$) are said to overlap if there exists $\underline{t} \in$ os($\underline{p}$) such that $\underline{t} \subseteq \underline{q}$, and $\underline{t} \subseteq \underline{r}$.

Lemma 1.12: If $\underline{q}$ and $\underline{r}$ overlap, then $\underline{q} \subseteq \underline{r}$ or $\underline{r} \subseteq \underline{q}$.

Proof: If $\underline{q}$ and $\underline{r}$ are not comparable, then they occur in distinct branches of some subterm of $\underline{p}$. But these distinct branches are disjoint, so that $\underline{t} \subseteq \underline{q}$ and $\underline{t} \subseteq \underline{r}$ is impossible. Hence, $\underline{q}$ and $\underline{r}$ must be comparable.

4. Identities

Definition 1.13: An identity of type τ is an expression of the form $\underline{p} = \underline{q}$, where $\underline{p}$, $\underline{q} \in \underline{P}(\tau)$.

Definition 1.14: An identity $\underline{p} = \underline{q}$ of type τ holds in $\mathfrak{A} \in K(\tau)$ if $\underline{p}$ and $\underline{q}$ induce the same polynomial in $\mathfrak{A}$.

Definition 1.15: Id($\mathfrak{A}$) is the set of all identities which hold in $\mathfrak{A}$. If $K \subseteq K(\tau)$, Id(K) is the set of all identities which hold in every $\mathfrak{A} \in K$.

Definition 1.16: If Σ is a set of identities of type τ, then Σ'' is the class of all algebras $\mathfrak{A}$ of type τ such that each identity in Σ holds in $\mathfrak{A}$.

5. Direct and Subdirect Products

Definition 1.17: Let $\mathfrak{A}_i = \langle A_i; F\rangle$, $i \in I$, be a family of algebras of the same type. The direct product of the algebras $\mathfrak{A}_i$ is the algebra

$$\prod(\mathfrak{A}_i \mid i \in I) = \langle \prod(A_i \mid i \in I); F\rangle$$

where the operations are defined as follows:

$$f_\gamma(p_0, p_1, \dots p_{n_\gamma - 1})(i) = f_\gamma(p_0(i), \dots p_{n_\gamma - 1}(i))$$

for $i \in I$, and the $p_j \in \prod(A_i \mid i \in I)$.

If $I = \{0, 1, \dots n-1\}$, then we write $\mathfrak{A}_0 \times \mathfrak{A}_1 \times \dots \times \mathfrak{A}_{n-1}$ for the direct product of the algebras. If $\mathfrak{A}_i = \mathfrak{A}$ for all $i \in I$, then we write $\mathfrak{A}^I$ for the direct product, and call it a direct power of $\mathfrak{A}$. If, in this case, $I = \{0, 1, \dots n-1\}$, then we write $\mathfrak{A}^n$.

Definition 1.18: The mapping $\delta_i : \prod(\mathfrak{A}_i \mid i \in I) \to \mathfrak{A}_i$ defined by $\delta_i : p \to p(i)$ is called the ith projection. δ_i is a homomorphism onto $\mathfrak{A}_i$.

Definition 1.19: A subalgebra $\mathfrak{b}$ of $\prod(\mathfrak{A}_i \mid i \in I)$ is called a subdirect product of the $\mathfrak{A}_i$, $i \in I$, if the restriction of each δ_i to B is onto A_i.

If $\mathfrak{A}_i = \mathfrak{A}$ for all $i \in I$, then $\mathfrak{B}$ is called a subdirect power of $\mathfrak{A}$.

If ϵ_i is the congruence induced by δ_i, let Θ_i be ϵ_i restricted to $\mathfrak{B}$. Then $\mathfrak{B}/\Theta_i \cong \mathfrak{A}_i$, and $\bigcap(\Theta_i | i \in I)$ is the trivial congruence of equality. Conversely, if $\{\Theta_i | i \in I\}$ is a family of congruences on an algebra $\mathfrak{A}$ such that $\bigcap(\Theta | i \in I)$ is the trivial congruence of equality, then $\mathfrak{A}$ is isomorphic to a subdirect product of the algebras $\mathfrak{A}/\Theta_i$, $i \in I$.

Definition 1.20: $\mathfrak{A}$ is subdirectly irreducible if, for any family of congruences $\{\Theta_i | i \in I\}$ on $\mathfrak{A}$, $\bigcap(\Theta_i | i \in I)$ being equality implies that Θ_i is equality for some $i \in I$.

Birkhoff has shown that every universal algebra is isomorphic to a subdirect product of subdirectly irreducible algebras.

6. Free Algebras

Definition 1.21: Let $K \subseteq K(\tau)$, and let α be an ordinal number. The free algebra over K with α generators, denoted by $\mathfrak{F}_K(\alpha) = \langle F_K(\alpha); F \rangle$, is defined as follows:

(i) $\mathcal{F}_K(\alpha) \in K$.

(ii) $\mathcal{F}_K(\alpha)$ is generated by $x_0, x_1, \ldots x_\gamma, \ldots,$ $\gamma < \alpha$.

(iii) If $a_0, a_1, \ldots a_\gamma, \ldots, \gamma < \alpha$, are elements of an arbitrary algebra $\mathfrak{A} \in K$, then the mapping $x_\gamma \rightarrow a_\gamma$ can be extended to a homomorphism of $\mathcal{F}_K(\alpha) \rightarrow \mathfrak{A}$.

If $\mathcal{F}_K(\alpha)$ exists, it is unique up to isomorphism. Specifically, $\mathcal{F}_K(\alpha) \cong \mathcal{P}^{(\alpha)}(\tau)/\Theta_K$, where $\mathcal{P}^{(\alpha)}(\tau)$ is the polynomial algebra formed on α variable symbols, and Θ_K is the congruence defined by: $\underline{p} \equiv \underline{q}(\Theta_K)$ if and only if $\underline{p} = \underline{q} \in Id(K)$.

7. Equational Classes

Definition 1.22: $K \subseteq K(\tau)$ is an equational class if $K = \Sigma''$, for some set Σ of identities of type τ.

A famous theorem proved by Birkhoff characterizes equational classes as those which are closed under the formation of subalgebras, homomorphic images, and direct products.

Let $\underline{S}(K)$ be the class of subalgebras of algebras of K. Similarly, define $\underline{H}(K)$ and $\underline{P}(K)$ for homomorphic images and direct products. Finally, let $\underline{HSP}(K)$ represent $\underline{H}(\underline{S}(\underline{P}(K)))$. Then if K is any class of algebras, $\underline{HSP}(K)$ is the smallest equational class containing K. If $K = \{\mathfrak{A}\}$, we write $\underline{HSP}(\mathfrak{A})$ for the equational class generated by $\mathfrak{A}$. These equational classes can also be defined as $(\mathrm{Id}(K))''$ and $(\mathrm{Id}(\mathfrak{A}))''$.

If $K = \Sigma''$ is equational, then the free algebra over K on α generators exists, and $\mathcal{F}_K(\alpha)$ is isomorphic to $\mathcal{P}^{(\alpha)}(\tau)/\Theta_K$, where $\underline{p} \equiv \underline{q}(\Theta_K)$ if and only if $\underline{p} = \underline{q} \in \mathrm{Id}(K)$. Furthermore, the free algebra on ω generators, $\mathcal{F}_K(\omega) \cong \mathcal{P}(\tau)/\Theta_K$, satisfies precisely the set of identities $\mathrm{Id}(K)$, and so completely determines K.

CHAPTER II

THE FINITE EQUATIONAL BASIS PROBLEM

This chapter contains a precise statement of the problem with which this thesis is concerned, and some very general results concerning this problem. All the results proved here are well-known to researchers in the field, and are used informally in the various papers on the subject. Since full proofs are not available in the literature, however, they are presented here.

1. Deducibility

Let Σ be a set of identities of type τ. We shall define what is meant by the statement: "$\underline{p} = \underline{q}$ can be deduced from Σ", which is symbolized by:

$$\Sigma \vdash \underline{p} = \underline{q}.$$

We first give the elementary rules of inference in the following:

Definition 2.1:

(i) $\vdash \underline{x}_0 = \underline{x}_0$ (in other words, we can always deduce this identity).

(ii) $\underline{p} = \underline{q} \vdash \underline{q} = \underline{p}$

(iii) $\underline{p} = \underline{q},\ \underline{q} = \underline{r} \vdash \underline{p} = \underline{r}$

(iv) $\underline{p}_i = \underline{q}_i,\ i = 0, 1, \dots n_\gamma - 1 \vdash$

$\underline{f}_\gamma(\underline{p}_0, \underline{p}_1, \dots \underline{p}_{n_\gamma - 1}) = \underline{f}_\gamma(\underline{q}_0, \underline{q}_1, \dots \underline{q}_{n_\gamma - 1})$

(v) If $\underline{p}'$ and $\underline{q}'$ are derived from $\underline{p}$ and $\underline{q}$ by replacing all occurrences of $\underline{x}_i$ by an arbitrary polynomial symbol $\underline{r}$, then $\underline{p} = \underline{q} \vdash \underline{p}' = \underline{q}'$.

Definition 2.2: If Σ is a set of identities, a proof from Σ is a finite sequence of identities:

$$\underline{p}_0 = \underline{q}_0$$
$$\underline{p}_1 = \underline{q}_1$$
$$\vdots$$
$$\underline{p}_{n-1} = \underline{q}_{n-1}$$

such that either $\underline{p}_i = \underline{q}_i \in \Sigma$, or $\underline{p}_i = \underline{q}_i$ follows from previous identities in the sequence by the rules of inference. The sequence is said to be a proof of $\underline{p}_{n-1} = \underline{q}_{n-1}$ from Σ.

Definition 2.3: $\Sigma \vdash \underline{p} = \underline{q}$ means there is a proof from Σ of $\underline{p} = \underline{q}$.

We note that by using rules (i) and (v), that we always have $\vdash \underline{p} = \underline{p}$. Further, rule (iv) can be extended to:

(iv') If $\underline{p}(\underline{x}_0, \ldots \underline{x}_{n-1}) \in \underline{P}(\tau)$, then $\underline{p}_0 = \underline{q}_0, \ldots \underline{p}_{n-1} = \underline{q}_{n-1} \vdash \underline{p}(\underline{p}_0, \ldots \underline{p}_{n-1}) = \underline{p}(\underline{q}_0, \ldots \underline{q}_{n-1})$.

The proof of (iv') is immediate by induction on the number of operation symbols occurring in $\underline{p}$.

Definition 2.4: The closure of Σ, denoted by $\overline{\Sigma}$, is the set of all identities which can be deduced from Σ. Σ is closed if $\Sigma = \overline{\Sigma}$.

Definition 2.5: $\Sigma \vdash W$ means $\Sigma \vdash \underline{p} = \underline{q}$ for each $\underline{p} = \underline{q} \in W$. Equivalently, we could define this to mean $W \subseteq \overline{\Sigma}$.

We note that if $\Sigma \subseteq W$, then $\overline{\Sigma} \subseteq \overline{W}$, and that if $\Sigma \vdash W$, then $\overline{W} \subseteq \overline{\Sigma}$.

If $\Sigma = \mathrm{Id}(\mathfrak{A})$, then Σ is closed. Conversely, if Σ is closed, then $\mathfrak{A} = \mathfrak{P}(\tau)/\Theta$, where $\underline{p} \equiv \underline{q}(\Theta)$ if and only if $\underline{p} = \underline{q} \in \Sigma$, is an algebra with $\mathrm{Id}(\mathfrak{A}) = \Sigma$. Thus rules (i) to (v) provide a complete set of rules of inference in the following sense: if $\underline{p} = \underline{q}$ is satisfied in $\mathfrak{A}$ whenever Σ is satisfied in $\mathfrak{A}$, then $\Sigma \vdash \underline{p} = \underline{q}$.

2. Bases for Sets of Identities

Definition 2.6: A set Σ of identities of type τ is finitely based if there exists a finite set W of identities of type τ such that $\overline{W} = \overline{\Sigma}$.

Theorem 2.7: If Σ is finitely based, then there exists a finite set of identities $\Sigma_0 \subseteq \Sigma$ such that $\overline{\Sigma}_0 = \overline{\Sigma}$.

Proof: Let $W = \left\{ \underline{p}_i = \underline{q}_i \,\middle|\, i = 0, 1, \ldots n-1 \right\}$ be a finite set of identities such that $\overline{W} = \overline{\Sigma}$. Then $W \subseteq \overline{\Sigma}$, so for each $\underline{p}_i = \underline{q}_i$, there is a proof from Σ, involving a finite set of identities $E_i \subseteq \Sigma$. Let $\Sigma_0 = E_0 \cup E_1 \cup \ldots \cup E_{n-1}$. Since $\Sigma_0 \subseteq \Sigma$, $\overline{\Sigma}_0 \subseteq \overline{\Sigma}$. Also, $\Sigma_0 \vdash W$, so $\overline{W} = \overline{\Sigma} \subseteq \overline{\Sigma}_0$. Thus $\overline{\Sigma}_0 = \overline{\Sigma}$.

Such a set Σ_0 will be called a finite basis for Σ. If $\Sigma = \mathrm{Id}(\mathfrak{A})$, then Σ_0 will be called a finite equational basis (FEB) for $\mathfrak{A}$.

The finite equational basis problem, in its most general form, is the following: to find necessary and sufficient conditions for an algebra to have a FEB. A related problem is the following: given an algebra $\mathfrak{A}$ satisfying various properties, to determine whether $\mathfrak{A}$ has a FEB.

3. Extension of Rules of Deduction

Definition 2.8: Let $\underline{p}(\underline{x}_0, \ldots \underline{x}_{n-1})$, $\underline{q}(\underline{x}_0, \ldots \underline{x}_{n-1})$ be polynomial symbols of type τ. Let $\underline{p}'$ and $\underline{q}'$ be $\underline{p}(\underline{p}_0, \ldots \underline{p}_{n-1})$ and $\underline{q}(\underline{p}_0, \ldots \underline{p}_{n-1})$. Let $\underline{r} \in \underline{P}(\tau)$, such that $\underline{p}'$ is a subterm of $\underline{r}$. Let $\underline{t}$ be the result of substituting $\underline{q}'$ for $\underline{p}'$ in $\underline{r}$.

Then $\underline{p} = \underline{q} \overset{S_1}{\vdash} \underline{r} = \underline{t}$.

Definition 2.9: $\underline{p} = \underline{q} \overset{S_2}{\vdash} \underline{r} = \underline{t}$ if and only if $\underline{p} = \underline{q} \overset{S_1}{\vdash} \underline{t} = \underline{r}$.

We will use the symbol S to mean "either S_1 or S_2".

Theorem 2.10: If $\underline{p} = \underline{q} \overset{S}{\vdash} \underline{r} = \underline{t}$, then $\underline{p} = \underline{q} \vdash \underline{r} = \underline{t}$.

Proof: If S is S_1, then $\underline{p} = \underline{q} \vdash \underline{p}' = \underline{q}'$ by a finite number of applications of rule (v). Then a finite number of applications of rule (iv) yields $\underline{p} = \underline{q} \vdash \underline{r} = \underline{t}$. If S is S_2, then we have by the first part of the theorem, that $\underline{p} = \underline{q} \vdash \underline{t} = \underline{r}$, since, by definition, $\underline{p} = \underline{q} \overset{S_1}{\vdash} \underline{t} = \underline{r}$. Then, by rule (ii), $\underline{p} = \underline{q} \vdash \underline{r} = \underline{t}$.

We note, in particular, that if $\underline{p}$ is a subterm of $\underline{r}$ and $\underline{t}$ is the result of substituting $\underline{q}$ for $\underline{p}$ in $\underline{r}$, then $\underline{p} = \underline{q} \vdash \underline{r} = \underline{t}$.

Lemma 2.11: If $\underline{p} = \underline{q} \vdash^{S} \underline{r} = \underline{t}$, and if $\underline{r}'$ and $\underline{t}'$ are obtained from $\underline{r}$ and $\underline{t}$ by substituting $\underline{s}$ for all occurrences of $\underline{x}_i$, then $\underline{p} = \underline{q} \vdash^{S} \underline{r}' = \underline{t}'$.

Proof: It is sufficient to prove the result for $S = S_1$. We recall that, by Definition 2.8, $\underline{r}$ and $\underline{t}$ have subterms $\underline{p}'$ and $\underline{q}'$ respectively, where $\underline{p}'$ is $\underline{p}(\underline{p}_0, \dots \underline{p}_{n-1})$ and $\underline{q}'$ is $\underline{q}(\underline{p}_0, \dots \underline{p}_{n-1})$. Let $\underline{p}_0', \dots \underline{p}_{n-1}'$ be the result of substituting $\underline{s}$ for $\underline{x}_i$ in $\underline{p}_0, \dots \underline{p}_{n-1}$, and let $\underline{p}''$ be $\underline{p}(\underline{p}_0', \dots \underline{p}_{n-1}')$ and let $\underline{q}''$ be $\underline{q}(\underline{p}_0', \dots \underline{p}_{n-1}')$. Then $\underline{r}'$ has $\underline{p}''$ as a subterm, and $\underline{t}'$ is $\underline{r}'$ with $\underline{q}''$ substituted for $\underline{p}''$.

Thus $\underline{p} = \underline{q} \vdash^{S_1} \underline{r}' = \underline{t}'$.

Definition 2.12: Let Σ be a set of identities containing the identities $\underline{p}_i = \underline{q}_i$, for i = 1, 2, ... n. Suppose the following sequence of deductions holds:

$$p_1 = q_1 \overset{S}{\vdash} r = t_1$$
$$p_2 = q_2 \overset{S}{\vdash} t_1 = t_2$$
$$\vdots$$
$$p_n = q_n \overset{S}{\vdash} t_{n-1} = t.$$

Then we say that t is <u>obtainable from r through Σ</u>,

and we write $\Sigma \overset{T}{\vdash} r = t$. The sequence of deductions is called a <u>T-sequence</u> for $r = t$, or a T-sequence connecting r to t.

<u>Theorem 2.13</u>: If $\Sigma \overset{T}{\vdash} r = t$, then $\Sigma \vdash r = t$.

<u>Proof</u>: The proof is immediate from Theorem 2.10, and rule (iii).

<u>Theorem 2.14</u>: If $\Sigma \vdash p = q$, then either p is q,

or $\Sigma \overset{T}{\vdash} p = q$.

<u>Proof</u>: The proof is by induction on k = the length of a proof from Σ of $p = q$. If $k = 1$, then $p = q \in \Sigma$

and we have $p = q \overset{S_1}{\vdash} p = q$, which is a T-sequence for $p = q$.

We now assume that $\underline{p}$ is not $\underline{q}$, and that the theorem is true for all identities which have a proof from Σ of length $< k$. There are four cases to consider, corresponding to the rules of inference (ii), (iii), (iv), and (v).

Case 1: Suppose that $\underline{p} = \underline{q}$ follows from $\underline{q} = \underline{p}$ occurring earlier in the proof, and hence having a proof of length $< k$. Then there is a T-sequence connecting $\underline{q}$ to $\underline{p}$:

$$\underline{p}_1 = \underline{q}_1 \stackrel{S}{\vdash} \underline{q} = \underline{t}_1$$

$$\vdots$$

$$\underline{p}_n = \underline{q}_n \stackrel{S}{\vdash} \underline{t}_{n-1} = \underline{p}.$$

Let $\overline{S}_1 = S_2$, and let $\overline{S}_2 = S_1$. Then

$$\underline{p}_n = \underline{q}_n \stackrel{\overline{S}}{\vdash} \underline{p} = \underline{t}_{n-1}$$

$$\vdots$$

$$\underline{p}_1 = \underline{q}_1 \stackrel{\overline{S}}{\vdash} \underline{t}_1 = \underline{q}$$

is a T-sequence for $\underline{p} = \underline{q}$ from Σ.

Case 2: Suppose $\underline{p} = \underline{q}$ follows from $\underline{p} = \underline{r}$ and $\underline{r} = \underline{q}$ occurring earlier in the proof. Then we have T-sequences connecting $\underline{p}$ to $\underline{r}$, and $\underline{r}$ to $\underline{q}$. The juxtaposition of the two T-sequences is clearly a T-sequence for $\underline{p} = \underline{q}$.

Case 3: Suppose that $\underline{p}$ is $\underline{f}(\underline{p}_0, \ldots \underline{p}_{n-1})$, $\underline{q}$ is $\underline{f}(\underline{q}_0, \ldots \underline{q}_{n-1})$, where $\underline{f}$ is an operation symbol, and $\underline{p}_i = \underline{q}_i$, i = 0, 1, ... n-1, occur earlier in the proof. Then we have a T-sequence for each $\underline{p}_i = \underline{q}_i$. Suppose, that for $\underline{p}_0 = \underline{q}_0$, we have:

$$\underline{r}_1 = \underline{s}_1 \vdash^{S} \underline{p}_0 = \underline{t}_1$$

$$\underline{r}_2 = \underline{s}_2 \vdash^{S} \underline{t}_1 = \underline{t}_2$$

$$\vdots$$

$$\underline{r}_m = \underline{s}_m \vdash^{S} \underline{t}_{m-1} = \underline{q}_0.$$

Then we can construct the T-sequence:

$$\underline{r}_1 = \underline{s}_1 \vdash^{S} \underline{f}(\underline{p}_0, \ldots \underline{p}_{n-1}) = \underline{f}(\underline{t}_1, \underline{p}_1, \ldots \underline{p}_{n-1})$$

$$\underline{r}_2 = \underline{s}_2 \vdash^{S} \underline{f}(\underline{t}_1, \underline{p}_1, \ldots \underline{p}_{n-1}) = \underline{f}(\underline{t}_2, \underline{p}_1, \ldots \underline{p}_{n-1})$$

$$\vdots$$

$$\underline{r}_m = \underline{s}_m \vdash^{S} \underline{f}(\underline{t}_{m-1}, \underline{p}_1, \ldots \underline{p}_{n-1}) = \underline{f}(\underline{q}_0, \underline{p}_1, \ldots \underline{p}_{n-1}).$$

Similarly, using the T-sequence for $\underline{p}_1 = \underline{q}_1$, we can construct a T-sequence connecting $\underline{f}(\underline{q}_0, \underline{p}_1, \ldots \underline{p}_{n-1})$ to $\underline{f}(\underline{q}_0, \underline{q}_1, \underline{p}_2, \ldots \underline{p}_{n-1})$. Finally, we will get a T-sequence connecting $\underline{f}(\underline{q}_0, \ldots \underline{q}_{n-2}, \underline{p}_{n-1})$ to $\underline{q}$, which is $\underline{f}(\underline{q}_0, \ldots \underline{q}_{n-1})$. The juxtaposition of all these T-sequences will yield a T-sequence connecting $\underline{p}$ to $\underline{q}$.

Case 4: Suppose that $\underline{p}$ is derived from $\underline{p}'$ by replacing all occurrences of the variable $\underline{x}_i$ by a polynomial symbol $\underline{s}$, and that $\underline{q}$ is similarly derived from $\underline{q}'$. Further, suppose that $\underline{p}' = \underline{q}'$ occurs earlier in the proof. Then we have a T-sequence connecting $\underline{p}'$ to $\underline{q}'$:

$$\underline{p}_1 = \underline{q}_1 \;\vdash^{S}\; \underline{p}' = \underline{t}_1$$
$$\vdots$$
$$\underline{p}_n = \underline{q}_n \;\vdash^{S}\; \underline{t}_{n-1} = \underline{q}'.$$

Using Lemma 2.11, we can replace all occurrences of $\underline{x}_i$ in all identities on the right by $\underline{s}$, thus obtaining a T-sequence connecting $\underline{p}$ to $\underline{q}$.

This completes the proof of the theorem.

4. Normal Forms

Let Σ be a set of identities of type τ. Then the binary relation Θ on $\underline{P}(\tau)$ defined by $\underline{p} \equiv \underline{q}(\Theta)$ if and only if $\underline{p} = \underline{q} \in \overline{\Sigma}$, is an equivalence relation.

Definition 2.15: A set $N \subseteq \underline{P}(\tau)$ of representatives of equivalence classes of $\underline{P}(\tau)/\Theta$ is called a set of normal forms of Σ.

Thus for each $\underline{p} \in \underline{P}(\tau)$, there is a unique $\underline{p}_N \in N$, the representative of the class $[\underline{p}]\Theta$, such that $\Sigma \vdash \underline{p} = \underline{p}_N$. Σ is said to reduce $\underline{p}$ to normal form $\underline{p}_N$.

Definition 2.16: Let W be any set of identities of type τ. We say Σ normalizes W if there exists a set of normal forms, N, for Σ, such that whenever $\underline{p} = \underline{q} \in W$, then $\underline{p}_N$ is $\underline{q}_N$. Σ is called a normalizer of W.

Theorem 2.17: If Σ normalizes W, then $\Sigma \vdash W$.

Proof: Let $\underline{p} = \underline{q} \in W$. Then $\Sigma \vdash \underline{p} = \underline{p}_N$, and $\Sigma \vdash \underline{q} = \underline{q}_N$. But $\underline{p}_N$ is $\underline{q}_N$, so $\Sigma \vdash \underline{p} = \underline{q}$. Thus, $\Sigma \vdash W$.

Corollary 2.18: If $\Sigma \subseteq W$ is a normalizer of W, then $\overline{\Sigma} = \overline{W}$.

Proof: If $\Sigma \subseteq W$, then $\overline{\Sigma} \subseteq \overline{W}$. Since $\Sigma \vdash W$, $\overline{W} \subseteq \overline{\Sigma}$. Thus $\overline{\Sigma} = \overline{W}$.

We now consider the special case when $W = Id(\mathfrak{A})$, for some algebra $\mathfrak{A}$.

Theorem 2.19: Let $\Sigma \subseteq Id(\mathfrak{A})$. Let $(\underline{p})_{\mathfrak{A}}$ denote the polynomial induced in $\mathfrak{A}$ by $\underline{p}$. Then Σ normalizes $Id(\mathfrak{A})$ if there exists a set N of normal forms such that, for distinct $\underline{p}$, $\underline{q} \in N$, $(\underline{p})_{\mathfrak{A}} \neq (\underline{q})_{\mathfrak{A}}$.

Proof: Let $\underline{p} = \underline{q} \in Id(\mathfrak{A})$, and let N be a set of normal forms of Σ as described in the theorem. We must show that $\underline{p}_N$ is $\underline{q}_N$. Since $\Sigma \vdash \underline{p} = \underline{p}_N$, $\underline{q} = \underline{q}_N$, and $\Sigma \subseteq Id(\mathfrak{A})$, which is a closed set of identities, we have that $\underline{p} = \underline{p}_N \in Id(\mathfrak{A})$, and $\underline{q} = \underline{q}_N \in Id(\mathfrak{A})$. Then $\underline{p} = \underline{q} \in Id(\mathfrak{A})$ implies that $\underline{p}_N = \underline{q}_N \in Id(\mathfrak{A})$; that is, $(\underline{p}_N)_{\mathfrak{A}} = (\underline{q}_N)_{\mathfrak{A}}$. So $\underline{p}_N$ must be $\underline{q}_N$, since if they were distinct, we would have that $(\underline{p}_N)_{\mathfrak{A}} \neq (\underline{q}_N)_{\mathfrak{A}}$.

5. Equivalence of Identities Modulo a Set of Identities

Let $\Sigma \subseteq W$, where W is a closed set of identities.

Definition 2.20: Let $\underline{p} = \underline{q}$, $\underline{r} = \underline{s} \in W$. These identities are equivalent modulo Σ if and only if:

$$\Sigma \cup \{\underline{p} = \underline{q}\} \vdash \underline{r} = \underline{s}$$

and

$$\Sigma \cup \{\underline{r} = \underline{s}\} \vdash \underline{p} = \underline{q} .$$

This is an equivalence relation on W. $\overline{\Sigma}$ is an equivalence class, called the zero class. W/Σ denotes the set of equivalence classes.

Definition 2.21: Let N be a set of representatives of the non-zero equivalence classes of W/Σ. $M \subseteq W$ is a basis modulo Σ for N if $\Sigma \cup M \vdash N$.

Theorem 2.22: If M is a basis modulo Σ for N, then $\Sigma \cup M \vdash W$.

Proof: Let $\underline{p} = \underline{q} \in W$, and $(\underline{p} = \underline{q})_N$ the representative of $[\underline{p} = \underline{q}]$. Then $\Sigma \cup M \vdash (\underline{p} = \underline{q})_N$, and $\Sigma \cup \{(\underline{p} = \underline{q})_N\} \vdash \underline{p} = \underline{q}$. Thus $\Sigma \cup M \vdash \underline{p} = \underline{q}$.

If $W = Id(\mathfrak{A})$ and Σ is finite, then we need only find a finite basis for a set of representatives

N of W/Σ to prove that $\mathfrak{A}$ has a FEB. The theorem, therefore, allows us to assume that any identity holding in $\mathfrak{A}$ has a particular form.

To illustrate this, let $\mathfrak{G}$ be a group, and let Σ be the group identities: $\underline{x}.(\underline{y}.\underline{z}) = (\underline{x}.\underline{y}).\underline{z}$, $\underline{x}.\underline{1} = \underline{x}$, $\underline{1}.\underline{x} = \underline{x}$, $\underline{x}.\underline{x}^{-1} = \underline{1}$, $\underline{x}^{-1}.\underline{x} = \underline{1}$. If $\underline{r} = \underline{s}$ is an identity holding in $\mathfrak{G}$, then

$$\Sigma \cup \{\underline{r} = \underline{s}\} \vdash \underline{r}.\underline{s}^{-1} = \underline{1}$$

and $\Sigma \cup \{\underline{r}.\underline{s}^{-1} = \underline{1}\} \vdash \underline{r} = \underline{s}$.

Thus, in discussing the FEB problem for $\mathfrak{G}$, we may assume that every identity satisfied in $\mathfrak{G}$ can be written in the form $\underline{p} = \underline{1}$. If we add to Σ the identity $\underline{x}.\underline{y} = \underline{y}.\underline{x}$, so that we have abelian groups, then we can assume that every identity has the form:

$$\underline{x}_0^{k_0}.\underline{x}_1^{k_1}. \dots .\underline{x}_{n-1}^{k_{n-1}} = \underline{1}$$

where the k_i are integers, with the understanding that $k_i = 0$ means that $\underline{x}_i$ does not occur on the left.

Suppose that $\underline{p}' = \underline{q}'$ is obtained from $\underline{p} = \underline{q}$ by changing variable symbols in such a way that distinct variable symbols remain distinct. Then $\underline{p}' = \underline{q}'$ and $\underline{p} = \underline{q}$ are equivalent modulo the void set of identities. Hence if $\underline{p} = \underline{q}$ has at most n distinct variable symbols, we can, in most cases, assume that these symbols are $\underline{x}_0, \underline{x}_1, \dots \underline{x}_{n-1}$.

6. Equivalent Algebras

Let $\mathfrak{A} \in K(\tau)$ and $\mathfrak{A}' \in K(\sigma)$ be algebras defined on the same set A. Thus, $\mathfrak{A} = \langle A; F\rangle$ and $\mathfrak{A}' = \langle A; G\rangle$. Let $P(\mathfrak{A})$ and $P(\mathfrak{A}')$ denote the sets of polynomials of $\mathfrak{A}$ and $\mathfrak{A}'$ respectively.

Definition 2.23: $\mathfrak{A}$ and $\mathfrak{A}'$ are equivalent if $P(\mathfrak{A}) = P(\mathfrak{A}')$.

Let $f \in F$ be an n-ary operation on A. Then $f \in P(\mathfrak{A}')$, so there is an n-ary polynomial symbol $\underline{f}'(\underline{x}_0, \ldots \underline{x}_{n-1}) \in \underline{P}(\sigma)$ which induces the same function on A. Similarly, for $g \in G$, there is a polynomial symbol $\underline{g}'(\underline{x}_0, \ldots \underline{x}_{m-1}) \in \underline{P}(\tau)$ which induces the same function on A as does g. We now define a mapping $\underline{p} \rightarrow \underline{p}'$ of $\underline{P}(\tau) \rightarrow \underline{P}(\sigma)$ as follows:

(i) $\underline{x}_i \rightarrow \underline{x}_i$, for $i = 0, 1, \ldots.$

(ii) If $\underline{p}$ is $\underline{f}(\underline{p}_0, \ldots \underline{p}_{n-1})$, and if $\underline{p}_i \rightarrow \underline{p}_i'$, then $\underline{p} \rightarrow \underline{f}'(\underline{p}_0', \ldots \underline{p}_{n-1}')$.

Similarly, we define a mapping $\underline{q} \rightarrow \underline{q}'$ of $\underline{P}(\sigma) \rightarrow \underline{P}(\tau)$.

This mapping makes precise the following procedure: for each operation symbol in $\underline{p} \in \underline{P}(\tau)$, we substitute the corresponding polynomial symbol of $\underline{P}(\sigma)$.

It is clear that the result is independent of the order in which the substitutions are made. Hence, we have the following:

Lemma 2.24: For any polynomial symbol $\underline{t}$ of type τ or σ, let $\underline{t}''$ denote $(\underline{t}')'$. Then if $\underline{p}$ is $\underline{g}(\underline{p}_0, \ldots \underline{p}_{m-1})$, $\underline{p}''$ is $\underline{g}''(\underline{p}_0'', \ldots \underline{p}_{m-1}'')$.

Lemma 2.25: $\underline{p}$ and $\underline{p}'$ induce the same functions on A.

Proof: If $\underline{p}$ is $\underline{x}_i$, the lemma is obvious. Suppose $\underline{p}_i$ and $\underline{p}_i'$ induce the same functions on A, for i = 0, 1. ... n-1. Then, by the definition of $\underline{f}'$, we have that $\underline{f}(\underline{p}_0, \ldots \underline{p}_{n-1})$ and $\underline{f}'(\underline{p}_0', \ldots \underline{p}_{n-1}')$ induce the same function on A.

Lemma 2.26: Let $\Sigma = \left\{ \underline{g}(\underline{x}_0, \ldots \underline{x}_{m-1}) = \underline{g}''(\underline{x}_0, \ldots \underline{x}_{m-1}), \text{ for } g \in G \right\}$. Then $\Sigma \vdash \underline{p} = \underline{p}''$ for all $\underline{p} \in \underline{P}(\sigma)$.

Proof: The result is obvious if $\underline{p}$ is $\underline{x}_i$. Suppose that $\underline{p}$ is $\underline{g}(\underline{p}_0, \ldots \underline{p}_{m-1})$ and that $\Sigma \vdash \underline{p}_i = \underline{p}_i''$ for all i = 0, 1, ... m-1. By rule (iv),

$$\Sigma \vdash \underline{g}(\underline{p}_0, \ldots \underline{p}_{m-1}) = \underline{g}(\underline{p}_0'', \ldots \underline{p}_{m-1}'')$$

But $\underline{g}(\underline{x}_0, \ldots \underline{x}_{m-1}) = \underline{g}''(\underline{x}_0, \ldots \underline{x}_{m-1}) \in \Sigma$. Therefore, $\Sigma \vdash \underline{g}(\underline{p}''_0, \ldots \underline{p}''_{m-1}) = \underline{g}''(\underline{p}''_0, \ldots \underline{p}''_{m-1})$. Thus, $\Sigma \vdash \underline{g}(\underline{p}_0, \ldots \underline{p}_{m-1}) = \underline{g}''(\underline{p}''_0, \ldots \underline{p}''_{m-1})$. But by Lemma 2.26, $\underline{g}''(\underline{p}''_0, \ldots \underline{p}''_{m-1})$ is $\underline{p}''$. So $\Sigma \vdash \underline{p} = \underline{p}''$.

Theorem 2.27: Let $\mathfrak{A} = \langle A; F \rangle$ be an algebra with a FEB, W. Let $\mathfrak{A}' = \langle A; G \rangle$ be an equivalent algebra with G finite. Let $W' = \{\underline{p}' = \underline{q}' \mid \underline{p} = \underline{q} \in W\}$, and let Σ be as in Lemma 2.26. Then $W' \cup \Sigma$ is a FEB for $\mathfrak{A}'$.

Proof: Let $\underline{p} = \underline{q} \in \mathrm{Id}(\mathfrak{A}')$. Then $\underline{p}' = \underline{q}' \in \mathrm{Id}(\mathfrak{A})$, and so there is a proof P from W of $\underline{p}' = \underline{q}'$. Then we have a proof P' from W' of $\underline{p}'' = \underline{q}''$. But $\Sigma \vdash \underline{p} = \underline{p}''$, $\underline{q} = \underline{q}''$. So $\Sigma \cup W' \vdash \underline{p} = \underline{q}$.

Corollary 2.28: If $\mathfrak{A}$ and $\mathfrak{A}'$ are equivalent F-finite algebras, then $\mathfrak{A}$ has a FEB if and only if $\mathfrak{A}'$ has a FEB.

CHAPTER III

THE EFFECT OF FINITENESS CONDITIONS

It was at first supposed by researchers that every finite algebra has a FEB. The first results in this direction were obtained by Lyndon [6], who proved the conjecture for all finite two-element algebras. Lyndon [7] also obtained the first counter-example: a finite seven-element algebra with a single binary operation. Visin [16] then proposed the problem of finding the smallest k for which all finite k-element algebras have a FEB, and in the same paper, exhibited a four-element algebra with a single binary operation having no FEB. Murskii's example [11] of a three-element algebra with a single binary operation having no FEB showed that Lyndon's first result was the best possible.

In this chapter, we present Lyndon's results on the two-element algebras, and Murskii's three-element counter-example.

1. Post's Iterative Systems

Post [15] gives a complete classification of what he calls "closed two-valued iterative systems" (hereafter called Post systems), which are defined as follows:

Definition 3.1: A Post system is a set of operations F on the two-element set $A = \{0, 1\}$ such that if $f(x_{i_1}, x_{i_2}, \dots x_{i_n}) \in F$, and $X_1, X_2, \dots X_n$ are either variables chosen from among $x_1, x_2, \dots x_n, \dots,$ $n < \omega$, or functions from F, then the function $f(X_1, X_2, \dots X_n) \in F$.

The set of polynomials of any two-element algebra is then a Post system, and so Post's classification includes a classification of all two-element algebras, up to equivalence. Not every one of Post's systems corresponds to an algebra since he does not require the system to include the projection functions. In particular, we can immediately discard those systems which do not possess the identity function. From Post's method of classifying these systems, we cannot immediately verify whether a system possessing the identity function also contains all the other projection functions. This need cause no difficulty, however, since by considering each system separately, and assuming that it does contain the projection functions, we can only prove more than is necessary by giving separate proofs for the same (up to equivalence) algebra.

We can effect a further economy by omitting algebras corresponding to systems containing only constant functions and (possibly) projection functions, since such an algebra is equivalent to an algebra with a trivial FEB: either the void set of identities or $\underline{x} = \underline{x}$ will do. We can also omit one of each pair of dual algebras, which are defined as follows:

Definition 3.2: Let $f(x_0, \ldots x_{n-1}): A^n \rightarrow A$, and let $\overline{0} = 1$, $\overline{1} = 0$. Then the dual function $\overline{f}$ is defined by: $\overline{f}(x_0, \ldots x_{n-1}) = \overline{f(\overline{x}_0, \ldots \overline{x}_{n-1})}$.

Definition 3.3: If $\mathfrak{A} = \langle \{0,1\} ; F \rangle$ is a two-element algebra, then its dual algebra is the algebra $\overline{\mathfrak{A}} = \langle \{0,1\} ; \overline{F} \rangle$, where $\overline{F} = \{ \overline{f} \mid f \in F \}$.

Then the omission mentioned is justified by the observation that the mapping δ: $0 \rightarrow 1$, $1 \rightarrow 0$ is an isomorphism between $\mathfrak{A}$ and $\overline{\mathfrak{A}}$.

Post has shown that all of his systems can be finitely generated by functions chosen from among the following:

(i) Constant functions: 0 and 1.

(ii) Unary function: x' where $0' = 1$ and $1' = 0$.

(iii) Binary functions, presented in dual pairs:

Join: $x \vee y$

x \ y	0	1
0	0	1
1	1	1

Meet: $x \wedge y$ or xy

x \ y	0	1
0	0	0
1	0	1

Equivalence: $x \equiv y$

x \ y	0	1
0	1	0
1	0	1

Symmetric Difference: $x + y$

x \ y	0	1
0	0	1
1	1	0

Conditional: $x \supset y$

x \ y	0	1
0	1	1
1	0	1

Set Difference: $x - y$

x \ y	0	1
0	0	0
1	1	0

(iv) Ternary functions: $(x, y, z) = x(y \vee z)$, $[x, y, z] = x(y \equiv z)$, and $x + y + z$. (It is well-known that symmetric difference is an associative operation, so that the latter is well-defined.)

(v) n-ary functions, for $n > 2$: $d_n(x_1, x_2, \ldots x_n) =$ $x_2x_3\ldots x_n \vee x_1x_3\ldots x_n \vee x_1x_2x_4\ldots x_n \vee \ldots \vee x_1x_2\ldots x_{n-1}$.

In the following sections, we shall list the Post systems which have not yet been eliminated. For each, we shall list one or more possible finite sets of generating functions. We shall then prove the existence of a FEB for the two-element algebra with these functions as operations, and hence for any equivalent finite algebra. Post's name for the system (for example, O_4) will also be used for the name of the algebra.

2. Post Systems I

The algebras of this group can be proved to have a FEB using Theorems 2.17 and 2.19 on normal forms. For each algebra $\mathfrak{A}$, we list a finite set of identities $\Sigma(\mathfrak{A})$ and a set of polynomial symbols $N(\mathfrak{A})$. It can readily be verified that these sets satisfy the conditions on Σ and N in the theorems on normal forms, and so $\Sigma(\mathfrak{A})$ will be a FEB for $\mathfrak{A}$.

We list for reference the following identities:

Idempotency: $\mathcal{I}_1$: $\underline{x} \vee \underline{x} = \underline{x}$; $\mathcal{I}_2$: $\underline{xx} = \underline{x}$.

Associativity: $\mathcal{A}_1$: $\underline{x} \vee (\underline{y} \vee \underline{z}) = (\underline{x} \vee \underline{y}) \vee \underline{z}$;

$\mathcal{A}_2$: $\underline{x}(\underline{yz}) = (\underline{xy})\underline{z}$

Commutativity: $\mathcal{C}_1$: $\underline{x} \vee \underline{y} = \underline{y} \vee \underline{x}$; $\mathcal{C}_2$: $\underline{xy} = \underline{yx}$.

Absorption laws: $\mathcal{B}_1$: $\underline{x} \vee (\underline{xy}) = \underline{x}$; $\mathcal{B}_2$: $\underline{x}(\underline{x} \vee \underline{y}) = \underline{x}$.

Distributivity: $\mathcal{D}_1$: $\underline{x} \vee (\underline{yz}) = (\underline{x} \vee \underline{y})(\underline{x} \vee \underline{z})$

$\mathcal{D}_2$: $\underline{x}(\underline{y} \vee \underline{z}) = (\underline{xy}) \vee (\underline{xz})$

Finally, so that there will be no ambiguity, the last set of generating functions given for any Post system will be assumed to be the defining operations of the algebra in question.

(i) O_4: $\{ ' \}$; $\Sigma(O_4) = \{ (\underline{x}')' = \underline{x} \}$; $N(O_4) = \{ \underline{x}_0, \underline{x}_0', \underline{x}_1, \underline{x}_1', \ldots \underline{x}_n, \underline{x}_n', \ldots, n < \omega \}$.

(ii) O_9: $\{ ', 0 \}$; $\Sigma(O_9) = \Sigma(O_4)$; $N(O_9) = \{ \underline{0}, \underline{0}' \} \cup N(O_4)$.

(iii) S_1: $\{ \vee \}$; $\Sigma(S_1) = \{ \mathcal{I}_1, \mathcal{C}_1, \mathcal{A}_1 \}$; $N(S_1) = \{ \underline{x}_{i_1} \vee (\underline{x}_{i_2} \vee (\ldots \vee (\underline{x}_{i_{n-1}} \vee \underline{x}_{i_n}))),$ where $i_1 < i_2 < \ldots < i_n, n < \omega \}$.

(iv) S_4: $\{ \vee , 0 \}$; $\Sigma(S_4) = \{ \underline{x} \vee \underline{0} = \underline{x} \} \cup \Sigma(S_1)$; $N(S_4) = \{ \underline{0} \} \cup N(S_1)$.

(v) S_3: $\{ \vee , 1 \}$; $\Sigma(S_3) = \{ \underline{x} \vee \underline{1} = \underline{1} \} \cup \Sigma(S_1)$; $N(S_3) = \{ \underline{1} \} \cup N(S_1)$.

(vi) S_6: $\{\vee, 0, 1\}$; $\Sigma(S_6) = \Sigma(S_4) \cup \Sigma(S_3)$; $N(S_6) = N(S_4) \cup N(S_3)$.

(vii) A_4: $\{\vee, \wedge\}$; $\Sigma(A_4) = \Sigma(S_1) \cup \{\mathcal{I}_2, \mathcal{L}_2, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2, \mathcal{D}_1, \mathcal{D}_2\}$; $N(A_4) = \{\underline{p}_1 \vee \dots \vee \underline{p}_n \mid n<\omega$, $\underline{p}_i$ is of the form $\underline{x}_{i_1}\underline{x}_{i_2} \dots \underline{x}_{i_{k_i}}$ with $i_1 < i_2 < \dots < i_{k_i}$, the $\underline{p}_i$ are distinct, $k_1 \leqslant k_2 \leqslant \dots \leqslant k_n$, and the $\underline{p}_i$ of the same length are ordered lexicographically with respect to the subscripts on the variable symbols$\}$.

(viii) A_2: $\{\vee, \wedge, 0\}$; $\Sigma(A_2) = \Sigma(A_4) \cup \{\underline{x} \vee \underline{0} = \underline{x}, \underline{x0} = \underline{0}\}$; $N(A_2) = N(A_4) \cup \{\underline{0}\}$.

(ix) A_1: $\{\vee, \wedge, 0, 1\}$; $\Sigma(A_1) = \Sigma(A_2) \cup \{\underline{x} \vee \underline{1} = \underline{1}, \underline{x1} = \underline{x}\}$; $N(A_1) = N(A_2) \cup \{\underline{1}\}$.

(x) L_3: $\{+\}$ or $\{+, 0\}$; $\Sigma(L_3) = \{\underline{x} + \underline{0} = \underline{x}, \underline{x} + \underline{x} = \underline{0}, \underline{x} + \underline{y} = \underline{y} + \underline{x}, \underline{x} + (\underline{y} + \underline{z}) = (\underline{x} + \underline{y}) + \underline{z}\}$; $N(L_3) = \{\underline{0}, \underline{x}_{i_1} + (\underline{x}_{i_2} + (\dots + (\underline{x}_{i_{n-1}} + \underline{x}_{i_n})))$, where $i_1 < i_2 < \dots < i_n\}$.

(xi) L_1: $\{+, '\}$ or $\{+, ', 0, 1\}$; $\Sigma(L_1) = \Sigma(L_3) \cup$ $\{(\underline{x}')' = \underline{x},\ \underline{0}' = \underline{1},\ \underline{x} + \underline{1} = \underline{x}',\ \underline{x}' + \underline{y} = \underline{x} + \underline{y}\}$; $N(L_1) = \{\underline{1}\} \cup N(L_3) \cup \{\underline{p}' \mid \underline{p} \in N(L_3)$, but is not $\underline{0}\}$.

(xii) C_3: $\{-, \vee\}$ or $\{+, \wedge, 0\}$; $\Sigma(C_3) = \Sigma(L_3) \cup$ $\{\mathcal{G}_2, \mathcal{B}_2, \mathcal{A}_2, \underline{x0} = \underline{0},\ \underline{x}(\underline{y} + \underline{z}) = \underline{xy} + \underline{xz}\}$; $N(C_3) =$ $\{\underline{0},\ \underline{p}_1 + \underline{p}_2 + \ldots + \underline{p}_n \mid n < \omega$, where $\underline{p}_i$ is of the form $\underline{x}_{i_1}\underline{x}_{i_2} \ldots \underline{x}_{i_k}$, $i_1 < i_2 < \ldots < i_k$, and the $\underline{p}_i$ are distinct and ordered as for $A_4\}$.

(xiii) C_4: $\{-, '\}$ or $\{+, \wedge, 0, 1\}$ or $\{\vee, \wedge, ', 0, 1\}$; $\Sigma(C_4)$ = the set of identities listed for reference on pages 39 to 40, together with $\{(\underline{x}')' = \underline{x},\ \underline{x} \vee \underline{0} = \underline{x},\ \underline{x0} = \underline{0},$ $\underline{x} \vee \underline{1} = \underline{1},\ \underline{x1} = \underline{x},\ \underline{0}' = \underline{1},\ \underline{x}' \vee \underline{y}' = (\underline{xy})',\ \underline{x}'\underline{y}' = (\underline{x} \vee \underline{y})'\}$; $N(C_4) = \{\underline{0}, \underline{1}\} \cup N(A_4) \cup \{\underline{p}' \mid \underline{p} \in N(A_4)\}$.

We note that C_4 is (up to equivalence) the two-element Boolean algebra.

(xiv) L_4: $\{x + y + z\}$; $\Sigma(L_4)$ = a set of identities asserting that $\underline{x} + \underline{y} + \underline{z}$ is invariant under any permutation of the variable symbols, together with $\{\underline{x} + \underline{y} + \underline{y} = \underline{x},\ \underline{x} + \underline{y} + (\underline{z} + \underline{u} + \underline{v}) = (\underline{x} + \underline{y} + \underline{z}) + \underline{u} + \underline{v}\}$;

$N(L_4) = \{ \underline{x}_0, \ldots \underline{x}_n, \ldots, n < \omega$, and polynomial symbols of the form $\underline{x}_{i_1} + \underline{x}_{i_2} + (\ldots + (\underline{x}_{i_{k-2}} + \underline{x}_{i_{k-1}} + \underline{x}_{i_k})),$ $i_1 < i_2 < \ldots < i_k$, $k = 3, 4, \ldots n, \ldots, n < \omega \}$.

(xv) L_5: $\{ x + y + z, \,' \}$; $\Sigma(L_5) = \Sigma(L_4) \cup \{ (\underline{x}')' = \underline{x}, (\underline{x} + \underline{y} + \underline{z})' = \underline{x}' + \underline{y} + \underline{z} \}$; $N(L_5) = N(L_4) \cup \{ \underline{p}' \mid \underline{p} \in N(L_4) \}$.

3. Post Systems II

The algebras in consideration here are F_4: $\{ \supset \}$ and F_4^n: $\{ \supset, d_n \}$ for $n > 2$. The proof of the existence of a FEB for these algebras will proceed as follows:

(a) We define "a fragment of the propositional calculus containing material implication" (hereafter called a Henkin fragment), and show that in such a formal system, a finite set of axiom schemata can be chosen from which all tautologies are deducible as theorems, using only modus ponens (MP) as a rule of inference.

(b) We show that from any finite two-element algebra $\mathfrak{A} = \langle \{0,1\} ; F \rangle$, where F contains the conditional ($\supset$), we can construct a Henkin fragment $L(\mathfrak{A})$.

(c) From the finite set of axiom schemata of $L(\mathfrak{A})$, we can construct a finite basis for $Id(\mathfrak{A})$.

Step (a): The results here are due to Henkin [4]. The proof is carried out for the case when there is just one other logical connective besides the material implication, but, as Henkin remarks, the modifications necessary for the more general result are notational rather than conceptual. Further, this particular result is sufficient for our purposes here.

Definition 3.4: A Henkin fragment is a formal system defined as follows:

(i) The primitive symbols are a denumerable set of variable symbols: $x_0, x_1, \ldots x_n, \ldots, n < \omega$, connective symbols: $\supset$ and β, and punctuation symbols: (,), and ’.

(ii) A variable alone is a well-formed formula (wff); if A and B are wff's, then so is $A \supset B$; if $A_1, \ldots A_m$ are wff's, then so is $\beta(A_1, \ldots A_m)$. We allow the case $m = 0$, in which case we write β rather than $\beta(\ )$.

(iii) For each logical connective, we have a truth table, the one for material implication being:

x_0	x_1	$x_0 \supset x_1$
0	0	1
0	1	1
1	0	0
1	1	1

Thus, if the variables in a wff are assigned truth values chosen from $\{0, 1\}$, then we can compute a corresponding truth value for the wff. If A is a wff containing variables $x_0, x_1, \ldots x_{n-1}$, we write x_0', $x_1', \ldots x_{n-1}'$ for an assignment of truth values to these variables, and A' for the corresponding truth value of A.

(iv) A wff A is a tautology if A' is 1 for every possible assignment of truth values to its variables.

Definition 3.5: A schema is defined as follows:

(i) $\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_n, \ldots$, $n < \omega$, are schemas.

(ii) If $\mathcal{B}_1$ and $\mathcal{B}_2$ are schemas, so is $\mathcal{B}_1 \supset \mathcal{B}_2$.

(iii) If $\mathcal{B}_1, \mathcal{B}_2, \ldots \mathcal{B}_m$ are schemas, then so is $\beta(\mathcal{B}_1, \mathcal{B}_2, \ldots \mathcal{B}_m)$.

It is clear that if for each $\mathcal{A}_i$ in a schema, we substitute a wff A_i for all occurrences of $\mathcal{A}_i$, then the result is a wff. A property P is said to hold for a schema if and only if it holds for all wff's which can be so derived from the schema. If all wff's derived from a schema $\mathcal{B}$ are tautologies, then $\mathcal{B}$ will be called <u>an instance of a tautology</u>. We note that for every schema $\mathcal{B}$, there is a simplest wff derivable from it by substituting x_i for $\mathcal{A}_i$.

Let an arbitrary set of wff's and/or axiom schemata be designated as axioms and/or axiom schemata (this means that every wff derivable from the axiom schema is an axiom). Let <u>modus ponens</u> (MP) be designated as the single rule of inference: if A_1 and A_2 are wff's, then from A_1 and $A_1 \supset A_2$, we can infer A_2.

<u>Definition 3.6</u>: <u>A proof from the assumptions V</u> is a finite sequence of wff's, each of which is an axiom, an element of some set V of wff's, or results from two preceding wff's of the sequence by MP. If A is the last wff of such a proof, we write $V \vdash A$. If $V = \emptyset$, we call A a <u>theorem</u>, and write $\vdash A$.

<u>Definition 3.7</u>: A Henkin fragment is said to be <u>axiomatizable</u> if there exists a finite set of axioms and/or axiom schemata such that every tautology is a theorem.

We shall show that every Henkin fragment is axiomatizable with the following finite set of axiom schemata:

A1: $\mathfrak{A}_1 \supset (\mathfrak{A}_2 \supset \mathfrak{A}_1)$

A2: $(\mathfrak{A}_1 \supset \mathfrak{A}_2) \supset ((\mathfrak{A}_1 \supset (\mathfrak{A}_2 \supset \mathfrak{A}_3)) \supset (\mathfrak{A}_1 \supset \mathfrak{A}_3))$

A3: $(\mathfrak{A}_1 \supset \mathfrak{A}_3) \supset (((\mathfrak{A}_1 \supset \mathfrak{A}_2) \supset \mathfrak{A}_3) \supset \mathfrak{A}_3)$

In addition, there are 2^m further axiom schemata involving β. Let $x_1, \ldots x_m$ be distinct variables, and select any one of the 2^m assignments of truth values $x_1', \ldots x_m'$ to these variables, and let β' be the associated value of $\beta(x_1, \ldots x_m)$. Let y be any new variable, and let x_i° be either $(x_i \supset y) \supset y$ or $x_i \supset y$, according as x_i' is 1 or 0, for i = 1, 2, ... m. Let β° be $(\beta(x_1, \ldots x_m) \supset y) \supset y$ or $\beta(x_1, \ldots x_m) \supset y$, according as β' is 1 or 0. Then any result of replacing each variable by some wff in:

$$x_1^\circ \supset (x_2^\circ \supset \ \ldots \ \supset (x_m^\circ \supset \beta^\circ))\ldots)$$

is an axiom. This is done for each of the 2^m possible assignments of truth values, thus yielding 2^m axiom schemata. Here, the variables play the role of the $\mathfrak{A}_i$ used in defining schemata, so that these are indeed schemata.

We note that each axiom schema is an instance of a tautology. Since <u>modus ponens</u> preserves the property of being a tautology, Henkin's result will show that the set of theorems is precisely the set of tautologies.

We will make use of the Deduction Theorem: If $V \cup \{A\} \vdash B$, then $V \vdash A \supset B$, for any wff's A and B, and any set V of wff's. This follows from A1, A2, and the rule of <u>modus ponens</u>. A proof can be found in E. Mendelsohn's <u>Introduction to Mathematical Logic</u> [10].

<u>Lemma 3.8</u>: Let $x_1', \ldots x_n'$ be any assignment of truth values to the distinct variables $x_1, \ldots x_n$. Let A be any wff containing no other variables than $x_1, \ldots x_n$, and let A' be the associated value of A. Let C be any wff. Define A° to be $(A \supset C) \supset C$ or $A \supset C$, according as A' is 1 or 0. Then,

$$x_1^\circ, \ldots x_n^\circ \vdash A^\circ.$$

<u>Proof</u>: The lemma is proved by induction on the length of A. First, if A is one of the variables, the proof is immediate.

Now suppose that A is $B \supset D$, and that the lemma holds for B and D. We have three cases to consider:

<u>Case 1</u>: $B' = 0$. Then B° is $B \supset C$. Also, $A' = (B \supset D)' = 1$, so A° is $(A \supset C) \supset C$. By the induction hypothesis, $x_1^\circ, \ldots x_n^\circ \vdash B \supset C$. Using A3, we get that $\vdash (B \supset C) \supset (((B \supset D) \supset C) \supset C)$. So by MP, we get $x_1^\circ, \ldots x_n^\circ \vdash ((B \supset D) \supset C) \supset C$. But $B \supset D$ is A and $(A \supset C) \supset C$ is A°. So $x_1^\circ, \ldots x_n^\circ \vdash A^\circ$.

<u>Case 2</u>: $D' = 1$. Then D° is $(D \supset C) \supset C$. Also, $A' = (B \supset D)' = 1$, so A° is $(A \supset C) \supset C$. By the induction hypothesis, $x_1^\circ, \ldots x_n^\circ \vdash (D \supset C) \supset C$. Consider the following chain of deductions:

$D \vdash B \supset D$ (by A1 and MP)

$D, (B \supset D) \supset C \vdash C$ (by MP)

$(B \supset D) \supset C \vdash D \supset C$ (by Deduction Theorem)

$(B \supset D) \supset C, (D \supset C) \supset C \vdash C$ (by MP)

$(D \supset C) \supset C \vdash ((B \supset D) \supset C) \supset C$ (by Deduction Theorem).

Thus, $x_1^\circ, \ldots x_n^\circ \vdash ((B \supset D) \supset C) \supset C$, and this is A°.

<u>Case 3</u>: $B' = 1$, $D' = 0$. Then B° is $(B \supset C) \supset C$, and D° is $D \supset C$. Then $A' = (B \supset D)' = 0$ and so A° is $A \supset C$. By the induction hypothesis, $x_1^\circ, \ldots x_n^\circ \vdash (B \supset C) \supset C$, and $x_1^\circ, \ldots x_n^\circ \vdash D \supset C$. Consider the deductions:

$B, B \supset D \vdash D$ (by MP)

$B, B \supset D, D \supset C \vdash C$ (by MP)

$B \supset D, D \supset C \vdash B \supset C$ (by Deduction Theorem)

$(B \supset C) \supset C, B \supset D, D \supset C \vdash C$ (by MP)

$(B \supset C) \supset C, D \supset C \vdash (B \supset D) \supset C$ (by Deduction Theorem).

Therefore, $x_1^\circ, \ldots x_n^\circ \vdash A^\circ$. This exhausts all possibilities when A is of the form $B \supset D$.

Suppose that A has the form $\beta(A_1, \ldots A_m)$, and that the lemma holds for $A_1, \ldots A_m$. There are 2^m cases, depending upon the assignment of truth values $A_1', \ldots A_m'$. Suppose that we have such an assignment. Then $A_1^\circ \supset (A_2^\circ \supset \ldots \supset (A_m^\circ \supset A^\circ))\ldots)$ is an axiom. By m successive applications of MP, we have that $A_1^\circ, \ldots A_m^\circ \vdash A^\circ$. By the induction hypothesis, $x_1^\circ, \ldots x_n^\circ \vdash A_i^\circ$, for each $i = 1, 2, \ldots m$. Thus, $x_1^\circ, \ldots x_n^\circ \vdash A^\circ$. This completes the proof of the lemma.

<u>Theorem</u> <u>3. 9</u>: If A is a tautology, then $\vdash A$.

<u>Proof</u>: Let $x_1, \ldots x_n$ be all the distinct variables that appear in A. For each of the 2^n possible assignments $x_1', \ldots x_n'$, A' is 1. Hence, by the preceding

lemma, if C is an arbitrary wff, and x_i° and A° are defined as before, we have, for each of the 2^n possible sets $V_n = \{x_1^\circ, \ldots x_n^\circ\}$, that

$$V_n \vdash (A \supset C) \supset C.$$

This entails that for any of the 2^{n-1} sets $V_{n-1} = \{x_1^\circ, \ldots x_{n-1}^\circ\}$, we have both

$$x_n \supset C, V_{n-1} \vdash (A \supset C) \supset C$$

and $$(x_n \supset C) \supset C, V_{n-1} \vdash (A \supset C) \supset C.$$

By the Deduction Theorem, we obtain:

$$V_{n-1} \vdash (x_n \supset C) \supset ((A \supset C) \supset C)$$

and $$V_{n-1} \vdash ((x_n \supset C) \supset C) \supset ((A \supset C) \supset C).$$

By A3, we have the following:

$$\vdash ((x_n \supset C) \supset ((A \supset C) \supset C)) \supset ((((x_n \supset C) \supset C) \supset ((A \supset C) \supset C)) \supset (A \supset C) \supset C).$$

Then by two applications of MP, we get that

$$V_{n-1} \vdash (A \supset C) \supset C.$$

Continuing thus, for each i = n-1, n-2, ... 2, 1, we obtain for each of the 2^i possible sets $V_i = \{x_1^\circ, \ldots x_i^\circ\}$ that $V_i \vdash (A \supset C) \supset C$. For i = 1, this gives $x_1 \supset C \vdash (A \supset C) \supset C$ and $(x_1 \supset C) \supset C \vdash (A \supset C) \supset C$. A final use of A3 gives $\vdash (A \supset C) \supset C$. Since C is any wff, we have, in particular, that $\vdash (A \supset A) \supset A$.

But from A $\vdash$ A, we obtain $\vdash$ A $\supset$ A by the Deduction Theorem, and hence by MP, $\vdash$ A.

Step (b): We now show how, from a finite two-element algebra $\mathfrak{A} = \langle \{0,1\} ; F\rangle$, where F contains the conditional, we can define a Henkin fragment L($\mathfrak{A}$). Let τ be the type of $\mathfrak{A}$.

(i) The symbols of L($\mathfrak{A}$) are the variable symbols, $\underline{x}_0, \ldots \underline{x}_n, \ldots, n < \omega$; the connective symbols are the operation symbols, $\underline{f}_\gamma$, of type τ. This includes the symbol "$\supset$" for the conditional, which plays the role of material implication here. We also have the usual punctuation symbols.

(ii) The wff's of L($\mathfrak{A}$) are the polynomial symbols of type τ.

(iii) The truth table for $\underline{f}_\gamma(\underline{x}_0, \ldots \underline{x}_{n_\gamma - 1})$ is the operation table for f_γ in $\mathfrak{A}$.

(iv) A wff is a tautology if, as a polynomial symbol, it induces the constant 1 function in $\mathfrak{A}$.

It is clear that L($\mathfrak{A}$) is a Henkin fragment. If α is a schema in L($\mathfrak{A}$), we denote by $\underline{\alpha}$ the simplest wff (hence, polynomial symbol) obtainable from α.

Step (c): If $\mathfrak{A}$ is an algebra satisfying the conditions of Step (b), then L($\mathfrak{A}$) is a Henkin fragment, and so can be axiomatized by a finite set of axiom schemata: $\alpha_1, \alpha_2, \ldots \alpha_n$. Let $\underline{\alpha}_1, \underline{\alpha}_2, \ldots \underline{\alpha}_n$ be the simplest wff's (hence polynomial symbols) derivable from $\alpha_1, \alpha_2, \ldots \alpha_n$. Let $\underline{x}_k$ be a variable symbol other than $\underline{x}$, $\underline{y}$, or any of the variable symbols occurring in $\underline{\alpha}_1, \underline{\alpha}_2, \ldots \underline{\alpha}_n$. If 1 is not a constant (nullary) function in $\mathfrak{A}$, we will use $\underline{1}$ as an abbreviation for $\underline{x}_k \supset \underline{x}_k$.

Theorem 3.10: $\mathfrak{A}$ has the following FEB: $\Sigma = \{$ A1: $\underline{x} \supset \underline{x} = \underline{1}$, A2: $\underline{1} \supset \underline{x} = \underline{x}$, A3: $(\underline{x} \supset \underline{y}) \supset \underline{x} = (\underline{y} \supset \underline{x}) \supset \underline{x}$, Bi: $\underline{\alpha}_i = \underline{1}$, $i = 1, 2, \ldots n.\}$

Proof: A1, A2, A3 clearly hold in $\mathfrak{A}$. Since α_i is an axiom schema of L($\mathfrak{A}$), $\underline{\alpha}_i$ is a tautology, so $\underline{\alpha}_i = \underline{1}$ holds in $\mathfrak{A}$.

We show first that if $\vdash \underline{p}$, then $\Sigma \vdash \underline{p} = \underline{1}$. If $\underline{p}$ is an axiom of L($\mathfrak{A}$), then either $\underline{p}$ is $\underline{\alpha}_i$ for some i, or $\underline{p}$ can be obtained from $\underline{\alpha}_i$ by uniform substitution of wff's (hence, polynomial symbols) for the variable symbols of $\underline{\alpha}_i$. In either case,

$\underline{\alpha}_i = \underline{1} \vdash \underline{p} = \underline{1}$. Now suppose that $/\!\!-\!\!-\ \underline{p}$ and $/\!\!-\!\!-\ \underline{p} \supset \underline{q}$, and that $\Sigma \vdash \underline{p} = \underline{1}$ and $\Sigma \vdash \underline{p} \supset \underline{q} = \underline{1}$. Then by rule S, we can substitute $\underline{1}$ for $\underline{p}$ to get $\Sigma \vdash \underline{1} \supset \underline{q} = \underline{1}$. But by A2, $\Sigma \vdash \underline{1} \supset \underline{q} = \underline{q}$. So $\Sigma \vdash \underline{q} = \underline{1}$. This proves, inductively, that if $/\!\!-\!\!-\ \underline{p}$, then $\Sigma \vdash \underline{p} = \underline{1}$.

Now suppose $\underline{p} = \underline{q} \in \mathrm{Id}(\mathfrak{A})$. We wish to show that $\Sigma \vdash \underline{p} = \underline{q}$. Since $\underline{p} = \underline{q} \in \mathrm{Id}(\mathfrak{A})$, we get by A1 that $\underline{p} \supset \underline{q} = \underline{1}$ and $\underline{q} \supset \underline{p} = \underline{1}$ hold in $\mathfrak{A}$. Then $\underline{p} \supset \underline{q}$ and $\underline{q} \supset \underline{p}$ are tautologies and hence theorems of $L(\mathfrak{A})$. By the first part of the theorem, $\Sigma \vdash \underline{p} \supset \underline{q} = \underline{1}$, and $\Sigma \vdash \underline{q} \supset \underline{p} = \underline{1}$. By A3, $\Sigma \vdash (\underline{q} \supset \underline{p}) \supset \underline{p} = (\underline{p} \supset \underline{q}) \supset \underline{q}$. Using rule S, we can substitute $\underline{1}$ for $\underline{p} \supset \underline{q}$ and $\underline{q} \supset \underline{p}$ to obtain $\Sigma \vdash \underline{1} \supset \underline{p} = \underline{1} \supset \underline{q}$. Using A2, we get: $\Sigma \vdash \underline{p} = \underline{q}$.

Corollary 3.11: The algebras F_4 and F_4^n, $n > 2$, each have a FEB.

4. Post Systems III

The proof in this section is essentially that given by Lyndon, with improvements suggested by G. Gratzer.

The algebras considered in this section are the following:

F_6: $\{(x,y,z)\}$ or $\{(x,y,z),\ xy\}$

F_7: $\{(x,y,z),\ 0\}$ or $\{(x,y,z),\ xy,\ 0\}$

F_5: $\{[x,y,z]\}$ or $\{[x,y,z],\ (x,y,z),\ xy\}$

C_4: $\{[x,y,z],\ x \vee y\}$ or $\{[x,y,z],\ (x,y,z),\ xy,\ x \vee y\}$

F_5^n: $\{[x,y,z],\ d_n\}$ or $\{[x,y,z],\ (x,y,z),\ xy,\ d_n\}$

F_6^n: $\{(x,y,z),\ d_n\}$ or $\{(x,y,z),\ d_n,\ xy\}$

F_7^n: $\{(x,y,z),\ d_n,\ 0\}$ or $\{(x,y,z),\ d_n,\ 0,\ xy\}$

We note that all these algebras have the operations (x,y,z) and xy.

Let Σ consist of the following identities:

(1) $\underline{xx} = \underline{x}$

(2) $\underline{xy} = \underline{yx}$

(3) $\underline{x}(\underline{yz}) = (\underline{xy})\underline{z}$

(4) $(\underline{x},\underline{y},\underline{y}) = \underline{xy}$

(5) $(\underline{x},\underline{x},\underline{y}) = \underline{x}$

(6) $(\underline{x},\underline{y},\underline{z}) = (\underline{x},\underline{z},\underline{y})$

(7) $(\underline{x},\underline{y},\underline{z}) = (\underline{x},\underline{xy},\underline{z})$

(8) $\underline{w}(\underline{x},\underline{y},\underline{z}) = (\underline{wx},\underline{y},\underline{z})$

(9) $\underline{w}(\underline{x},\underline{y},\underline{z}) = (\underline{x},\underline{wy},\underline{wz})$

We note that $\Sigma \subseteq \mathrm{Id}(F_6)$, so that $\underline{HSP}(F_6) \subseteq \Sigma''$. We now proceed to show that $\Sigma'' \subseteq \underline{HSP}(F_6)$, so that Σ will form a FEB for F_6.

Let $\mathfrak{A}$ be any algebra with operations (x,y,z) and xy satisfying Σ. For any $x, y \in A$, we define $x \leqslant y$ to mean $xy = x$. Using the identities Σ, we can easily show that this defines a partial order on A.

Definition 3.12: A dual ideal in $\mathfrak{A}$ is a proper subset $S \subset A$ such that:

(i) $x, y \in S$ implies that $xy \in S$, and

(ii) if $x \leqslant y$, and $x \in S$, then $y \in S$.

Definition 3.13: A dual ideal S is prime if whenever $(x,y,z) \in S$, then either $xy \in S$ or $xz \in S$.

Lemma 3.14: If $a \leqslant b$ does not hold, then there exists a prime dual ideal containing a but not b.

Proof: Let $S_0 = \{ z \mid a \leqslant z \}$. This is a dual ideal containing a but not b. We shall now show that every dual ideal with this property, if not already prime, can be properly extended to a larger dual ideal with the same property. Let S be a dual ideal, not prime, containing a and not b. Then, by definition, S contains some (u,v,w) while neither uv nor $uw \in S$. Suppose there existed $p, q \in S$ such that $puv \leqslant b$ and $quw \leqslant b$. Let $r = pq$, and note that $r \in S$.

Then we have the relations (R): $ruv \leqslant b$ and $ruw \leqslant b$. Now

$$br(u,v,w) = (u,brv,brw) \text{ by identity (9),}$$
$$= (u,ubrv,ubrw) \text{ by (6) and (7),}$$
$$= (u,ruv,ruw) \text{ by the relations (R),}$$
$$= (u,rv,rw) \text{ by (6) and (7),}$$
$$= r(u,v,w) \text{ by (9).}$$

This means that $r(u,v,w) \leqslant b$. But r, $(u,v,w) \in S$ so $r(u,v,w) \in S$, and hence $b \in S$, contradicting $b \notin S$. So such p and q cannot exist. Suppose, by symmetry, that $puv \leqslant b$ holds for no $p \in S$. Now let $S' = \{ z \mid puv \leqslant z,\ p \in S \}$. This is a dual ideal not containing b. Also, $S \subseteq S'$, since $puv \leqslant p$ for all $p \in S$. Finally, the inclusion is proper, for $puv \in S'$ for any $p \in S$, while if $puv \in S$, then we would have $uv \in S$, contradicting the fact that uv and $uw \notin S$.

Now let $\mathcal{S}$ be the set of all dual ideals of $\mathfrak{A}$ containing a and not b, partial ordered by set inclusion. The set union of any chain of such dual ideals is a dual ideal with the same properties, and so Zorn's Lemma can be applied to yield a maximal dual ideal M with these properties. Then M must be prime, for if not, it can be properly extended to a larger dual ideal containing a but not b, contradicting its maximality.

Theorem 3.15: $\mathfrak{A}$ is a subdirect power of F_6.

Proof: Let a, b $\in$ A such that a $\leqslant$ b does not hold, and let S be a prime dual ideal containing a but not b. We define a mapping $\delta_{ab}: A \to F_6$ as follows:

$\delta_{ab}: x \to 1$ if $x \in S$, $\delta_{ab}: x \to 0$ if $x \notin S$.

We show first that δ_{ab} is a homomorphism of $\mathfrak{A}$ into F_6. Since $xy \in S$ if and only if x and $y \in S$, we have that $(xy)\delta_{ab} = (x\delta_{ab})(y\delta_{ab})$ whenever x and y are both in S or both not in S. Now suppose $x \in S$ and $y \notin S$, so that $x\delta_{ab} = 1$ and $y\delta_{ab} = 0$. Now $xy \notin S$, for otherwise we would have $y \in S$. So $(xy)\delta_{ab} = 0 = 1.0 = (x\delta_{ab})(y\delta_{ab})$.

Now consider (x,y,z) and suppose that $(x,y,z) \in S$, so that $(x,y,z)\delta_{ab} = 1$. Now, either $xy \in S$ or $xz \in S$. If $xy \in S$, then both x and $y \in S$, and we get $(x\delta_{ab},y\delta_{ab},z\delta_{ab}) = (1,1,z\delta_{ab}) = 1$. A similar result holds if $xz \in S$. If, on the other hand, $(x,y,z) \notin S$, then $y(x,y,z) \notin S$. But $y(x,y,z) = (xy,y,z)$ by (8), $= (xy,xy,xyz)$ by (6), (7), $= xy$ by (5). Then $xy \notin S$, so $x \notin S$ and $y \notin S$. So we get that $(x\delta_{ab},y\delta_{ab},z\delta_{ab}) = (0,0,z\delta_{ab}) = 0$ as required.

So δ_{ab} is, indeed, a homomorphism.

Let Θ_{ab} be the congruence on $\mathfrak{A}$ induced by δ_{ab}. We note that $a \not\equiv b(\Theta_{ab})$ since $a\delta_{ab} = 1$ while $b\delta_{ab} = 0$. Also, $\mathfrak{A}/\Theta_{ab} \cong F_6$. Now let $J = \{ \Theta_{ab} | \ a \leqslant b$ does not hold in $\mathfrak{A}\}$, and let $\Theta = \bigcap(\Theta_{ab} | \Theta_{ab} \in J)$. Let $x \equiv y(\Theta)$, with $x \neq y$, so that either $x < y$, or $x \leqslant y$ does not hold. If $x < y$, then $y \leqslant x$ does not hold, and $\Theta_{yx} \in J$, and $\Theta \leqslant \Theta_{yx}$. Then we get that $x \equiv y(\Theta_{yx})$ which is a contradiction. Similarly, if $x \leqslant y$ does not hold, we get a contradiction using Θ_{xy}. Then $x \equiv y(\Theta)$ if and only if $x = y$, so Θ is the trivial congruence of equality. Then $\mathfrak{A}$ is a subdirect product of the $\mathfrak{A}/\Theta_{ab}$, that is, a subdirect power of F_6.

Theorem 3.16: Σ is a FEB for F_6.

Proof: If $\mathfrak{A} \in \Sigma''$, then $\mathfrak{A}$ is a subdirect power of F_6, so $\mathfrak{A} \in \underline{HSP}(F_6)$. Thus $\Sigma'' \subseteq \underline{HSP}(F_6)$. We have already noted that $\underline{HSP}(F_6) \subseteq \Sigma''$. Thus $\Sigma'' = \underline{HSP}(F_6)$ and so $Id(F_6) = \overline{\Sigma}$.

The same technique will be used for the remaining algebras in this section; in each case, all that we must show is that the addition of a finite number of identities to Σ will ensure that the additional operations are preserved by δ_{ab}. It should be noted that the additional identities do indeed hold in the algebra in question.

Theorem 3.17: Each of F_7, F_5, C_4, F_6^n, F_5^n, and F_7^n has a FEB.

Proof: (i) F_7: $\{(x,y,z),\ xy,\ 0\}$. We add the identity: (10) $\underline{0x} = \underline{0}$. We must show that $(0)\delta_{ab} = 0$. But if $(0)\delta_{ab} = 1$, then $0 \in S$. Since $0x = 0$ for all $x \in A$, $0 \leqslant x$ for all $x \in A$, and so $S = A$. But S is a proper subset of A. So we must have $(0)\delta_{ab} = 0$.

(ii) F_5: $\{[x,y,z],\ (x,y,z),\ xy\}$. We add the identities:

(11) $[\underline{x},\underline{y},\underline{z}] = [\underline{x},\underline{z},\underline{y}]$

(12) $\underline{x}[\underline{x},\underline{y},\underline{z}] = [\underline{x},\underline{y},\underline{z}]$

(13) $\underline{y}[\underline{x},\underline{y},\underline{z}] = \underline{xyz}$

(14) $(\underline{x},(\underline{x},\underline{y},\underline{z}),[\underline{x},\underline{y},\underline{z}]) = \underline{x}$

Let $[x,y,z] \in S$. By (12), $[x,y,z] \leqslant x$, so $x \in S$. If neither y nor $z \in S$, then $[x\delta_{ab}, y\delta_{ab}, z\delta_{ab}] = [1,0,0] = 1$ as required. Otherwise, suppose $y \in S$.

Then $y[x,y,z] \in S$, and $y[x,y,z] = xyz$, so $z \in S$. Then $[x\delta_{ab}, y\delta_{ab}, z\delta_{ab}] = [1,1,1] = 1$ as required.

For the converse, suppose $[x\delta_{ab}, y\delta_{ab}, z\delta_{ab}] = 1$. Then $x\delta_{ab} = 1$, and $y\delta_{ab} = z\delta_{ab}$. So $x \in S$, and y and z are either both in S or both not in S. If they are both in S, then $xyz \in S$. Now $xyz[x,y,z] = yz[x,y,z]$ by (12), $= z(xyz)$ by (13), $= xyz$. Then $xyz \leqslant [x,y,z]$ implies that $[x,y,z] \in S$, and $[x,y,z]\delta_{ab} = 1$ as required.

On the other hand, if y and z are both not in S, we consider $x = (x,(x,y,z),[x,y,z]) \in S$. Then either $x(x,y,z) = (x,y,z) \in S$, or $x[x,y,z] = [x,y,z] \in S$. The first possibility cannot occur, since it would imply that either xy or $xz \in S$, and hence either y or $z \in S$. So $[x,y,z] \in S$, and $[x,y,z]\delta_{ab} = 1$ as required.

(iii) C_4: $\left\{[x,y,z],\ (x,y,z),\ xy,\ x \vee y\right\}$. We add the identities:

(15) $\underline{x} \vee \underline{y} = \underline{y} \vee \underline{x}$

(16) $\underline{x}(\underline{x} \vee \underline{y}) = \underline{x}$

(17) $(\underline{x} \vee \underline{y}, \underline{x}, \underline{y}) = \underline{x} \vee \underline{y}$

Let $(x \vee y)\delta_{ab} = 1$. Since $(x \vee y, x, y) = x \vee y$, either $x(x \vee y) = x \in S$ or $y(x \vee y) = y \in S$. So $x\delta_{ab} \vee y\delta_{ab} = 1$. Conversely, if $x \vee y \notin S$, then by (16), neither x nor y can be in S. So $x\delta_{ab} \vee y\delta_{ab} = 0 \vee 0 = 0 = (x \vee y)\delta_{ab}$.

(iv) F^n_6; $\left\{(x,y,z),\ d_n,\ xy\right\}$. Let $(x,y_1,\ldots y_m)$ be an abbreviation for $(x,(x,\ldots(x,(x,y_1,y_2),y_3)\ldots y_m)$ and let x^i be an abbreviation for $x_1\ldots x_{i-1}x_{i+1}\ldots x_n$. Note that the n is the one given by d_n. We add the identities:

(18) $\underline{x}^1\underline{d}_n(\underline{x}_1,\ \ldots\ \underline{x}_n) = \underline{x}^1$

(19) $\underline{d}_n(\underline{x}_1,\ldots\underline{x}_n) = (\underline{d}_n(\underline{x}_1,\ldots\underline{x}_n),\underline{x}^1,\underline{x}^2,\ldots\underline{x}^n)$

(20) Identities asserting that $\underline{d}_n(\underline{x}_1,\ \ldots\ \underline{x}_n)$ is invariant under any permutation of the variable symbols.

Now suppose $d_n(x_1\delta_{ab},\ \ldots\ x_n\delta_{ab}) = 1$. Then for some i, $(x_1\delta_{ab})\ldots(x_{i-1}\delta_{ab})(x_{i+1}\delta_{ab})\ldots(x_n\delta_{ab}) = 1$. So $x^i\delta_{ab} = 1$, and $x^i \in S$. But by identities (18) and (20), $x^i = x^i d_n(x_i,x_2,\ldots x_{i-1},x_1,x_{i+1},\ldots x_n)$, so we get $d_n(x_1,\ldots x_n) \in S$, and $d_n(x_1,\ \ldots\ x_n)\delta_{ab} = 1$ as required. Conversely, suppose that $d_n(x_1,\ \ldots\ x_n) \in S$. Then by (19), $(d_n(x_1,\ldots x_n),x^1,\ \ldots\ \ x^n) \in S$. So either

$d_n(x_1,\ldots x_n)(d_n(x_1,\ldots x_n),x^1,\ldots x^{n-1}) = (d_n(x_1,\ldots x_n),x^1,\ldots x^{n-1})$

is in S, or $x^n d_n(x_1,\ \ldots\ x_n) = x^n \in S$. If this latter holds, then $x^n\delta_{ab} = 1$, and $d_n(x_1\delta_{ab},\ \ldots\ x_n\delta_{ab}) = 1$, as required. If not, then $(d_n(x_1,\ldots x_n),x^1,\ldots x^{n-1}) \in S$

and then either $x^{n-1} \in S$, or $(d_n(x_1,\dots x_n), x^1, \dots x^{n-2}) \in S$. Continuing thus, either one of $x^n, x^{n-1}, \dots x^3 \in S$, or else $(d_n(x_1,\dots x_n), x^1, x^2) \in S$. If this latter holds, then either x^1 or $x^2 \in S$. In any case, at least one $x^i \in S$, and $x^i\delta_{ab} = 1$. Then $d_n(x_1\delta_{ab},\dots x_n\delta_{ab}) = 1$ as required.

(v) F_5^n: $\left\{ [x,y,z],\ (x,y,z),\ d_n,\ xy \right\}$. Clearly, the identities (1) - (9), (11) - (14), and (18) - (20) will do.

(vi) F_7^n: $\left\{ (x,y,z),\ d_n,\ 0,\ xy \right\}$. Here, identities (1) - (9), (10), and (18) - (20) will do.

5. <u>Post Systems IV</u>

The algebras to be considered here are the following:

$$D_2: \left\{ d_3 = d \right\}$$
$$D_1: \left\{ d,\ x + y + z \right\}$$
$$D_3: \left\{ d,\ x + y + z,\ ' \right\}$$

The method used for Post Systems III will be adapted here by introducing a zero and partial order into such algebras. This method was devised by G. Gratzer, following a suggestion in Lyndon's paper.

We note, first, that the following identities hold in D_2:

(1') $d(u,x,x) = x$

(2') $d(u,x,y) = d(u,y,x)$

(3') $d(u,x,d(u,y,z)) = d(u,d(u,x,y),z)$

(4') $d(u,x,d(x,y,y)) = d(u,x,y)$

(5') $d(u,x,d(x,x,y)) = x$

(6') $d(u,x,d(x,y,z)) = d(u,x,d(x,z,y))$

(7') $d(u,x,d(x,y,z)) = d(u,x,d(x,d(u,x,y),z))$

(8') $d(u,w,d(u,x,d(x,y,z))) = d(u,d(u,w,x),d(d(u,w,x),y,z))$

(9') $d(u,w,d(u,x,d(x,y,z))) = d(u,x,d(x,d(u,w,y),d(u,w,z)))$

(10') $d(u,u,x) = u$

(18') $d(u,y,d(u,z,d(x,y,z))) = d(u,y,z)$

(19') $d(x,y,z) = d(u,d(x,y,z),$
$d(d(x,y,z), d(u,d(x,y,z),d(d(x,y,z),d(u,y,z),d(u,x,z))),d(u,x,y))$

(20') Identities asseting that $d(x,y,z)$ is invariant under any permutations of x, y, and z.

The numbering and unnecessary repetitions in the list will serve to make the analogy with Systems III more immediate.

Let Σ_1 denote this set of identities. Since $\Sigma_1 \subseteq \mathrm{Id}(D_2)$, we have that $\underline{HSP}(D_2) \subseteq \Sigma_1$. For the other containment, we consider any algebra $\mathfrak{A}$ of the same type as D_2 satisfying Σ_1. Let $u \in A$ be fixed. We introduce the following definitions: $x \wedge_u y = d(u,x,y)$, $(x,y,z)_u = x \wedge_u d(x,y,z)$, and $0_u = u$. Let $\mathfrak{A}_u$ be an algebra on the same set A as $\mathfrak{A}$, but with operations d, $x \wedge_u y$, $(x,y,z)_u$, and 0_u. Thus $\mathfrak{A}_u$ is of the same type as F_7^3.

Now consider (1'): $\underline{d}(\underline{u},\underline{x},\underline{x}) = \underline{x}$. For the fixed u chosen and any $x \in A$, $d(u,x,x) = x$. This means that $x \wedge_u x = x$ for all $x \in A$. Then $\underline{x} \wedge_u \underline{x} = \underline{x}$ holds in $\mathfrak{A}_u$. Proceeding similarly with (2') - (9'), we see that $\mathfrak{A}_u$ satisfies the identities (1) - (9) lised for Systems III. Hence, we can define prime dual ideals in $\mathfrak{A}_u$, and prove an analogue of Lemma 3.14, with a partial order defined in terms of $x \wedge_u y$. Translating identity (10'), we get $\underline{0}_u \wedge_u \underline{x} = \underline{0}_u$, and the identities (18') - (20') yield the identities (18) - (20) listed for F_7^3. We define the algebra D_2' by adding to D_2 the operations $x \wedge_0 y$, $(x,y,z)_0$, and 0 as for $\mathfrak{A}$. The algebra so derived is isomorphic to F_7^3.

It is clear, now, that we can parallel the proof in Systems III to obtain a homomorphism

$$\delta_{ab}: \mathfrak{A}_u \to D_2'$$

which separates any a and b such that $a \leqslant_u b$ does not hold.

The same mapping is a homomorphism of $\mathfrak{A} \to D_2$ which separates a and b. Then $\mathfrak{A}$ is isomorphic to a subdirect power of D_2, and so $\Sigma_1'' \subseteq \underline{HSP}(D_2)$. Thus $Id(D_2) = \overline{\Sigma}_1$, and we have the following:

Theorem 3.18: D_2 has Σ_1 for a FEB.

Theorem 3.19: D_1 and D_3 have FEB's.

Proof: Again, we must show that the addition of a finite number of identities will ensure that δ_{ab} preserves the additional operations x + y + z and x'.

For D_1, we add the following identities:

(A) $\underline{d}(\underline{u},\underline{d}(\underline{x},\underline{y},\underline{z}),\ \underline{x}+\underline{y}+\underline{z}) = \underline{d}(\underline{u},\underline{x},\underline{d}(\underline{u},\underline{y},\underline{z}))$

(B) $\underline{x}+\underline{y}+\underline{z} = \underline{d}(\underline{u},\underline{x}+\underline{y}+\underline{z},\underline{d}(\underline{x}+\underline{y}+\underline{z},\underline{d}(\underline{u},\underline{x}+\underline{y}+\underline{z},\underline{d}(\underline{x}+\underline{y}+\underline{z},\underline{x},\underline{y})),$
$\underline{d}(\underline{u},\underline{x}+\underline{y}+\underline{z},\underline{d}(\underline{x}+\underline{y}+\underline{z},\underline{y},\underline{z}))))$

(C) $\underline{d}(\underline{u},\underline{d}(\underline{u},\underline{x},\underline{d}(\underline{u},\underline{y},\underline{z})),\underline{x}+\underline{y}+\underline{z}) = \underline{d}(\underline{u},\underline{x},\underline{d}(\underline{u},\underline{y},\underline{x}))$

(D) $\underline{d}(\underline{u},\underline{x},\underline{d}(\underline{x},\underline{x}+\underline{y}+\underline{z},\underline{d}(\underline{x},\underline{y},\underline{z}))) = \underline{x}$

The u-translations of these become:

(A') $\underline{d}(\underline{x},\underline{y},\underline{z}) \wedge_u (\underline{x} + \underline{y} + \underline{z}) = \underline{x} \wedge_u \underline{y} \wedge_u \underline{z}$

(B') $\underline{x}+\underline{y}+\underline{z} = (\underline{x}+\underline{y}+\underline{z}, (\underline{x}+\underline{y}+\underline{z},\underline{x},\underline{y})_u, (\underline{x}+\underline{y}+\underline{z},\underline{y},\underline{z})_u)_u$

(C') $(\underline{x} \wedge_u \underline{y} \wedge_u \underline{z}) \wedge_u (\underline{x} + \underline{y} + \underline{z}) = \underline{x} \wedge_u \underline{y} \wedge_u \underline{z}$

(D') $(\underline{x},\ \underline{x} + \underline{y} + \underline{z},\ \underline{d}(\underline{x},\underline{y},\underline{z}))_u = \underline{x}$

Finally, we add identities asserting that $\underline{x} + \underline{y} + \underline{z}$ is invariant under permutations of $\underline{x}$, $\underline{y}$, and $\underline{z}$.

We will now show that $(x + y + z)\delta_{ab} = x\delta_{ab} + y\delta_{ab} + z\delta_{ab}$. Suppose that $(x + y + z)\delta_{ab} = 1$. If $x, y, z \in S$, then $x\delta_{ab} + y\delta_{ab} + z\delta_{ab} = 1 + 1 + 1 = 1$. Now suppose $x \notin S$. If $y, z \in S$, then $d(x,y,z) \in S$, so $d(x,y,z) \wedge_u (x + y + z) = x \wedge_u y \wedge_u z \in S$, by (A'), and so $x \in S$, contradicting $x \notin S$. So at least one of y, z, say y, is not in S. Now $x + y + z \in S$, so by (B'), $(x + y + z, (x+y+z,x,y)_u, (x+y+z,y,z)_u)_u \in S$. So either $(x+y+z) \wedge_u (x+y+z,x,y)_u = (x+y+z,x,y)_u \in S$, or $(x+y+z) \wedge_u (x+y+z,y,z)_u = (x+y+z,y,z)_u \in S$. The first possibility cannot occur, for then we would have that $(x+y+z) \wedge_u x \in S$ or $(x+y+z) \wedge_u y \in S$, which would imply that either $x \in S$ or $y \in S$. So the second alternative must hold, and a similar calculation yields that $z \in S$. Then $x\delta_{ab} + y\delta_{ab} + z\delta_{ab} = 0 + 0 + 1 = 1$ as required.

Conversely, suppose that $x\delta_{ab} + y\delta_{ab} + z\delta_{ab} = 1$. So either $x\delta_{ab} = y\delta_{ab} = z\delta_{ab} = 1$ or, say, $x\delta_{ab} = y\delta_{ab} = 0$ and $z\delta_{ab} = 1$. In the first case, $x, y, z \in S$, and hence $x \wedge_u y \wedge_u z \in S$. By (C'), $x \wedge_u y \wedge_u z \wedge_u (x + y + z) = x \wedge_u y \wedge_u z$, and so $x + y + z \in S$ as required. In the second case, $z \in S$ and $x, y \notin S$. By (D'), $z = (z, x + y + z, d(x,y,z))_u$, and so either $z \wedge_u (x+y+z) \in S$ or $z \wedge_u d(x,y,z) \in S$. But $z \wedge_u d(x,y,z) = (z,x,y)_u \in S$ would imply that $z \wedge_u x$ or $z \wedge_u y \in S$, which is a contradiction, since neither x nor y is in S. So we must have that $z \wedge_u (x + y + z) \in S$, and this implies that $x + y + z \in S$ as required.

For D_3, we add the identity: $\underline{d}(\underline{x},\underline{y},\underline{y}') = \underline{x}$. Then for any $x \in A$, $x \wedge_u u' = d(u,x,u') = x$, so u' is a maximal element. Also, S is non-empty, so there is an element $z \in S$, and $z \leq_u u'$. So $u' \in S$. Also, we note that $x \wedge_u x' = d(u,x,x') = u = 0_u$.

Now let $x' \in S$. If $x \in S$, then $x \wedge_u x' = 0_u$ is in S, which is a contradiction. So $x \notin S$, and $x\delta_{ab} = 0$. Then $(x\delta_{ab})' = 1 = (x')\delta_{ab}$.

Conversely, if $(x\delta_{ab})' = 1$, then $x\delta_{ab} = 0$, and so $x \notin S$. Now $u' \in S$, and $u' = u' \wedge_u u' = u' \wedge_u d(u',x,x') = (u',x,x')_u \in S$. So either $u' \wedge_u x = x \in S$, or $u' \wedge_u x' = x' \in S$. Since $x \notin S$, $x' \in S$, and $(x')\delta_{ab} = 1$ as required.

This now completes the proof that every finite two-element algebra has a FEB. That this is the best possible result in this direction is exhibited in the next section of this chapter.

6. Murskii's Three-Element Counter-Example

x \ y	0	1	2
0	0	0	0
1	0	0	1
2	0	2	2

Let $\mathfrak{A}$ be defined on the set $\{0, 1, 2\}$ with a single binary operation, denoted by xy, with operation table as at left.

Consider the polynomial symbols:

F_n: $\underline{x}_1(\underline{x}_2(\underline{x}_3 \ldots (\underline{x}_{n-1}(\underline{x}_n\underline{x}_1)) \ldots))$

and G_n: $(\underline{x}_1\underline{x}_2)(\underline{x}_n(\underline{x}_{n-1} \ldots (\underline{x}_4(\underline{x}_3\underline{x}_2)) \ldots))$.

We shall show that for $n < 2$, $F_n = G_n$ holds in $\mathfrak{A}$, but cannot be deduced from a set of identities in which any arbitrary term contains occurrences of not more than n-1 different variable symbols.

<u>Lemma 3.20</u>: Let $\underline{p}(\underline{x}_0, \ldots \underline{x}_{n-1})$ be a polynomial synbol of type <2> containing each of $\underline{x}_i$, $i = 0, \ldots n-1$. Then the polynomial $p(x_0, \ldots x_{n-1})$ induced by $\underline{p}$ in $\mathfrak{A}$ is a function depending on all its variables.

<u>Proof</u>: For arbitrary x_i, $p(2,2,\ldots 2) = 2$, whereas $p(2,2,\ldots 2, 0, 2, \ldots 2) = 0$, when the ith variable is allowed to take on the value 0. Thus p depends upon x_i.

Corollary 3.21: If $\underline{p} = \underline{q} \in \mathrm{Id}(\mathfrak{A})$, then $\underline{p}$ and $\underline{q}$ contain the same variable symbols.

Definition 3.22: The term occurrence will denote the occurrence of a variable symbol in a polynomial symbol, and we will use the notation b_1, b_2, ... for occurrences of $\underline{x}_i$, $\underline{x}_j$,....

Definition 3.23: Two occurrences b_1 and b_2 in a polynomial symbol $\underline{p}$ will be called adjacent in $\underline{p}$ if $\underline{p}$ contains a subterm $\underline{p}_1\underline{p}_2$, and b_1 is the left-most occurrence in $\underline{p}_1$ and b_2 is the left-most occurrence in $\underline{p}_2$, or vice-versa. Two variable symbols $\underline{x}_i$ and $\underline{x}_j$ (with possibly $i = j$) are called adjacent in $\underline{p}$ if there is an occurrence b_1 of $\underline{x}_i$ adjacent to an occurrence b_2 of $\underline{x}_j$ in $\underline{p}$. We note that every occurrence of a variable symbol $\underline{x}_i$ in $\underline{p}$ is one of a pair of adjacent occurrences.

Lemma 3.24: Let $\underline{p}(\underline{x}_0, \ldots \underline{x}_{n-1}) \in \underline{P}(\langle 2 \rangle)$, let $p(x_0, \ldots x_{n-1})$ be the induced polynomial in $\mathfrak{A}$, and let $a_0, a_1, \ldots a_{n-1} \in A$. Then the following results hold:

(i) if $p(a_0, \ldots a_{n-1}) \neq 0$, then $p(a_0, \ldots a_{n-1}) = a_i$, where $\underline{x}_i$ is the left variable symbol of $\underline{p}$.

(ii) $p(a_0, \ldots a_{n-1}) = 0$ if and only if some $a_i = 0$, or $a_i = a_j = 1$, where $\underline{x}_i$ and $\underline{x}_j$ are a pair of adjacent variable symbols of $\underline{p}$, possibly identical.

Proof: (i) This follows immediately from the fact that for any $a, b \in A$, if $ab \neq 0$, then $ab = a$.

(ii) If some $a_i = 0$, then $p(a_0, \ldots a_{n-1}) = 0$. If $a_i = a_j = 1$ where $\underline{x}_i$ and $\underline{x}_j$ are adjacent in $\underline{p}$, then $\underline{p}$ has a subterm $\underline{p}_1\underline{p}_2$ such that $\underline{x}_i$ is the left variable of $\underline{p}_1$ and $\underline{x}_j$ is the left variable of $\underline{p}_2$. If $p_1(a_0, \ldots a_{n-1}) = 0$, or $p_2(a_0, \ldots a_{n-1}) = 0$, we are done. Otherwise, by (i), $p_1(a_0, \ldots a_{n-1}) = 1$ and $p_2(a_0, \ldots a_{n-1}) = 1$, and $p_1(a_0, \ldots a_{n-1})p_2(a_0, \ldots a_{n-1}) = 0$. Then $p(a_0, \ldots a_{n-1}) = 0$ as required.

Conversely, let $p(a_0, \ldots a_{n-1}) = 0$. Let $\underline{p}'$ be a subterm of $\underline{p}$ such that $p'(a_0, \ldots a_{n-1}) = 0$ but all proper subterms of $\underline{p}'$ do not have this property. If $\underline{p}'$ is a variable symbol, we are done. Otherwise, $\underline{p}'$ is $\underline{p}_1\underline{p}_2$ and $p_1(a_0, \ldots a_{n-1}) \neq 0$, $p_2(a_0, \ldots a_{n-1}) \neq 0$. But $p_1(a_0, \ldots a_{n-1})p_2(a_0, \ldots a_{n-1}) = 0$, so each must be 1 (this can be seen by checking the operation table). Let $\underline{x}_i$ be the left variable of $\underline{p}_1$ and $\underline{x}_j$ of $\underline{p}_2$. Then $a_i = a_j = 1$ by (i), and $\underline{x}_i$, $\underline{x}_j$ are adjacent in $\underline{p}$.

Corollary 3.25: If p and q have the same left variable symbols, and the same pairs of adjacent variable symbols, then $p = q \in Id(\mathfrak{A})$.

Proof: Note first that the same variable symbols occur in p and q. Let $a_0, \ldots a_{n-1} \in A$, and suppose $p(a_0, \ldots a_{n-1}) = 0$. Then some $a_i = 0$, or $a_i = a_j = 1$, where x_i and x_j are adjacent in p. In either case, $q(a_0, \ldots a_{n-1}) = 0$. Suppose $p(a_0, \ldots a_{n-1}) \neq 0$, Then $p(a_0, \ldots a_{n-1}) = a_i$, where x_i is the left variable symbol of p, and hence of q. Suppose $q(a_0, \ldots a_{n-1}) = 0$. Then by the same reasoning as above, we would get that $p(a_0, \ldots a_{n-1}) = 0$. Hence $q(a_0, \ldots a_{n-1}) \neq 0$, and so must equal a_i. Then $p(a_0, \ldots a_{n-1}) = q(a_0, \ldots a_{n-1})$ for all $a_i \in A$. So $p = q \in Id(\mathfrak{A})$.

Lemma 3.26: Let p be a polynomial symbol in which no variable symbol is adjacent to itself. Then every q for which $p = q \in Id(\mathfrak{A})$ has the same left variable symbol and the same pairs of adjacent variable symbols as p.

Proof: Let $p(x_0, \ldots x_{n-1})$ be built up from variable symbols $x_0, \ldots x_{n-1}$. Then q has the same variable symbols. Now q has no variable symbol x_i adjacent to itself; otherwise, taking $x_i = 1$, $x_j = 2$ for $j \neq i$, we would have $p(x_0, \ldots x_{n-1}) \neq 0$ and $q(x_0, \ldots x_{n-1}) = 0$. Further, if the left variable $\underline{x}_j$ of $\underline{p}$ is not identical with the left variable of $\underline{q}$, then for $x_j = 1$, $x_k = 2$ for $k \neq j$, we would have $p(x_0, \ldots x_{n-1}) = 1$, while $q(x_0, \ldots x_{n-1}) = 2$, since neither $\underline{p}$ nor $\underline{q}$ has a variable adjacent to itself. Finally, if two variables $\underline{x}_i$ and $\underline{x}_j$, $i < j$, adjacent in $\underline{p}$, are not adjacent in $\underline{q}$, then for $x_i = x_j = 1$, and $x_k = 2$ for $k \neq i, j$, we would have $p(x_0, \ldots x_{n-1}) = 0$, but $q(x_0, \ldots x_{n-1}) \neq 0$. This completes the proof.

Lemma 3.27: Let P be a word (that is, a symbol formed by juxtaposition) in the alphabet $\{x_1, \ldots x_n\}$ beginning with x_1, ending with x_3, and not containing some letter x_i, $i > 3$. Furthermore, assume that any (unordered) pair of neighbouring letters of the word P is one of the pairs x_1x_2, x_2x_3, $\ldots$ $x_{n-1}x_n$, x_nx_1. Then P contains the subword $x_1x_2x_3$.

Proof: The proof is a reverse induction on i, where x_i is the missing letter. Suppose x_n is missing. The initial segment of P is x_1x_2. If x_3 follows x_2, we are done. Otherwise, P has the initial segment $x_1x_2x_1x_2$. Again, we have the two alternatives of x_3 and x_1. Eventually, the next alternative must be x_3, or P would not contain x_3.

Suppose the result is true for x_k missing, $k > 3$. Let P be such a word with x_{k-1} missing. Then x_k occurs in P within subwords of the form $x_{k+1}x_kx_{k+1}$. For each such subword, erase x_kx_{k+1}. The resulting subword P' has x_k missing and satisfies the hypotheses of the lemma. So P' has $x_1x_2x_3$ as a subword, and since $k > 3$, P also contains this subword.

Corollary 3.28: If P is a word in the alphabet $\{x_1, x_3, \ldots x_n\}$ beginning with x_1, ending with x_3, and with the same pairs of neighbouring letters as above, then each of $x_1, x_3, x_4, \ldots x_n$ must occur in P.

Lemma 3.29: Let $\underline{p}'$ be a subterm of $\underline{p}$, b_1 an occurrence in $\underline{p}'$ which is not the left occurrence of $\underline{p}'$, and b_2 an occurrence adjacent to b_1. Then b_2 lies in $\underline{p}'$.

Proof: Assume b_2 does not lie in $\underline{p}'$. We have two cases to consider:

Case (i): $\underline{p}$ has a subterm $\underline{p}_1\underline{p}_2$ where b_1 is the left occurrence of $\underline{p}_1$ and b_2 is the left occurrence of $\underline{p}_2$. Then $\underline{p}'$ overlaps $\underline{p}_1\underline{p}_2$. We cannot have $\underline{p}_1\underline{p}_2 \subseteq \underline{p}'$, since b_2 does not lie in $\underline{p}'$. Hence $\underline{p}' \subseteq \underline{p}_1\underline{p}_2$ and the containment is proper for the same reason. Then

$\underline{p}' \subseteq \underline{p}_1$ or $\underline{p}' \subseteq \underline{p}_2$. Since b_1 occurs in $\underline{p}'$, we must have $\underline{p}' \subseteq \underline{p}_1$. But b_1 is the left variable of $\underline{p}_1$ and hence of $\underline{p}'$, contradicting the hypothesis.

Case (ii): $\underline{p}$ contains $\underline{p}_2\underline{p}_1$ where $\underline{p}_1$ and $\underline{p}_2$ are as above. The same argument holds.

Corollary 3.30: Let b_2 be an occurrence in $\underline{p}$ adjacent to the distinct occurrences b_1 and b_3. Let $\underline{p}'$ be a subterm not containing one of these occurrences, and containing at least one of the others not on the left. Then b_2 is the left occurrence of $\underline{p}'$.

Proof: b_2 must occur in $\underline{p}'$, since otherwise, $\underline{p}'$ would contain a non-left occurrence adjacent to an occurrence outside $\underline{p}'$, contradicting Lemma 3.29. By Lemma 3.29, b_2 must be the left occurrence in $\underline{p}'$.

Corollary 3.31: Let $\underline{p}_1$ and $\underline{p}_2$ be non-overlapping subterms of $\underline{p}$. If b_1 occurs in $\underline{p}_1$, b_2 in $\underline{p}_2$, and b_1 is adjacent to b_2, then b_1 and b_2 are the left occurrences of $\underline{p}_1$ and $\underline{p}_2$.

Proof: Immediate from Lemma 3.29.

Lemma 3.32: Let b_1 and b_2 be distinct occurrences in p. Then there exists a sequence of pair-wise distinct occurrences $b_1^\circ, b_2^\circ, \ldots b_m^\circ$, $m > 1$, such that b_1° is b_1, b_m° is b_2, and, for $i = 1, 2, \ldots m-1$, b_i° is adjacent to b_{i+1}°. (We will call such a sequence an A-sequence to b_1 and b_2.)

Proof: The proof is by induction on the number k of distinct occurrences in p. If $k = 2$, p is $x_i x_j$ with b_1 the occurrence of x_i and b_2 the occurrence of x_j, or vice-versa. Then b_1, b_2 is the required A-sequence. Now suppose such a sequence exists for any two distinct occurrences in a polynomial symbol with fewer than k distinct occurrences. Let p have k occurrences, and let b_1 and b_2 be distinct occurrences in p. Let p be $p_1 p_2$. If b_1 and b_2 both occur in one of p_1 of p_2, the result follows from the induction hypothesis. Otherwise, let b_1 be in p_1 and b_2 in p_2. Suppose neither is the left occurrence of p_1 or p_2. Let $b_1, b_2^\circ, \ldots b_s^\circ$ be an A-sequence connecting b_1 to the left occurrence b_s° of p_1. Let b_{k+1}° be the left occurrence of p_2 and $b_{k+1}^\circ, \ldots, b_2$ an A-sequence connecting b_{k+1}° to b_2. Since b_k° and b_{k+1}° are adjacent and $\underline{p}_1$ and $\underline{p}_2$ do not overlap, b_1, b_2°, ... b_k°, b_{k+1}°, ... b_2 is an A-sequence connecting b_1 to b_2. An obvious modification proves the result if either or both b_1, b_2 are the left occurrences in $\underline{p}_1$ and $\underline{p}_2$.

Definition 3.33: We define a subset $K_n \subseteq \underline{P}(<2>)$ as follows: $\underline{p} \in K_n$ if and only if:

(i) $\underline{p}$ contains the variable symbols $\underline{x}_1$, ... $\underline{x}_n$.

(ii) $\underline{x}_1$ is the left variable symbol in $\underline{p}$.

(iii) The pairs of adjacent variable symbols are precisely: $\underline{x}_1\underline{x}_2$, $\underline{x}_2\underline{x}_3$, ... $\underline{x}_{n-1}\underline{x}_n$, $\underline{x}_n\underline{x}_1$.

By Lemmas 3.24 and 3.26, if $\underline{p}$, $\underline{q} \in K_n$, then $\underline{p} = \underline{q} \in Id(\mathfrak{A})$. Furthermore, if $\underline{p} \in K_n$ and $\underline{p} = \underline{q} \in Id(\mathfrak{A})$, then $\underline{q} \in K_n$.

In particular, F_n, $G_n \in K_n$, and so $F_n = G_n$ holds in $\mathfrak{A}$ for each n.

Definition 3.34: $\underline{p} \in \underline{P}(<2>)$ has property P_n if and only if:

(i) $\underline{p} \in K_n$

(ii) There is an occurrence of $\underline{x}_2$ in $\underline{p}$ adjacent both to some occurrence of $\underline{x}_1$ and to some occurrence of $\underline{x}_3$.

We note that F_n has P_n, while G_n does not.

Lemma 3.35: Let $\Sigma \subseteq \mathrm{Id}(\mathfrak{N})$ be such that any identity of Σ contains occurrences of less than n different variable symbols. If $\Sigma \vdash \underline{p} = \underline{q}$, and $\underline{p}$ has P_n, then $\underline{q}$ has P_n.

Proof: If $\underline{p}$ is $\underline{q}$, we are done. Otherwise, by Theorem 2.14, $\Sigma \vdash^{T} \underline{p} = \underline{q}$. Clearly, it is sufficient to show that a single application of rule S_1 preserves P_n; that is, if $\underline{r} = \underline{s} \vdash^{S_1} \underline{p} = \underline{q}$ and one of $\underline{p}$ or $\underline{q}$ has P_n, then so does the other. We will assume that $\underline{p}$ has P_n and show that $\underline{q}$ also has P_n. The other case is proved in a similar manner.

Since $\underline{r} = \underline{s} \in \mathrm{Id}(\mathfrak{A})$, the same set of variable symbols $\underline{y}_1, \ldots \underline{y}_k$, $k < n$, occurs in both $\underline{r}$ and $\underline{s}$. We write $\underline{r}(\underline{y}_1, \ldots \underline{y}_k)$ and $\underline{s}(\underline{y}_1, \ldots \underline{y}_k)$ for $\underline{r}$ and $\underline{s}$. Then for some polynomial symbols $\underline{p}_1$, $\underline{p}_2, \ldots \underline{p}_k$, $\underline{r}(\underline{p}_1, \ldots \underline{p}_k)$ is a subterm of $\underline{p}$ and $\underline{q}$ is the result of replacing this subterm in $\underline{p}$ by the polynomial symbol $\underline{s}(\underline{p}_1, \ldots \underline{p}_k)$. We write $\underline{r}'$ and $\underline{s}'$ respectively for these subterms of $\underline{p}$ and $\underline{q}$.

We note that $\underline{r}'$ can be decomposed into non-overlapping subterms of the form $\underline{p}_i$. These will be called elementary subterms. Analagously, we decompose $\underline{s}'$ into elementary subterms. Since $\underline{r}$ and $\underline{s}$ contain the same variable symbols, $\underline{r}'$ and $\underline{s}'$ contain the same elementary subterms. The left occurrences of two elementary subterms in $\underline{r}'$ ($\underline{s}'$) are adjacent if and only if the variable symbols they replace in $\underline{r}$ ($\underline{s}$) are adjacent. Further, in $\underline{r}$, there is no variable adjacent to itself. For if $\underline{y}_i$ is adjacent to itself in $\underline{r}$, then the left variable symbol of $\underline{p}_i$ is adjacent to itself in $\underline{r}'$ and hence in $\underline{p}$. But $\underline{p}$ has P_n and so the only pairs of adjacent variables are $\underline{x}_1\underline{x}_2, \ldots \underline{x}_{n-1}\underline{x}_n, \underline{x}_n\underline{x}_1$. Therefore, by Lemma 3.26, $\underline{r}$ and $\underline{s}$ have identical left variable symbols, and identical pairs of adjacent variable symbols. In particular, the left elementary subterms of $\underline{r}'$ and $\underline{s}'$ are identical.

We will call the left occurrence in an elementary subterm a supporting occurrence.

We assume that $\underline{p}$ has P_n. Thus $\underline{p} \in K_n$, and so then is $\underline{q} \in K_n$. In $\underline{p}$, there is an occurrence b_2 of $\underline{x}_2$ adjacent both to an occurrence b_1 of $\underline{x}_1$ and an occurrence b_3 of $\underline{x}_3$. We must prove that this also holds for $\underline{q}$. The following cases exhaust all the possibilities;

(i) Each of b_1, b_2, and b_3 lies outside r'.

(ii) Two of b_1, b_2, and b_3 lie outside r' and one inside.

(iii) b_1, b_2, and b_3 lie within r'.

(iv) One of b_1, b_2, and b_2 lies outside r', and two inside.

Case (i): Since q is obtained from p by replacing r' by s', there are occurrences of x_1, x_2, and x_3 in q having the same relationship to each other as do b_1, b_2, and b_3. Hence q has P_n.

Case (ii): The occurrence inside r' must be the left occurrence of r' (by Lemma 3.29). If the two occurrences outside r' are adjacent in p, then they remain adjacent after replacing r' by s'. If the left occurrence of r' is adjacent to an occurrence outside r', then in q, this occurrence outside s' is adjacent to the left occurrence in s'. But the left occurrences of r' and s' are identical. Hence q has P_n.

Case (iii): If b_1, b_2, and b_3 lie in the same elementary subterm, we are done, since the same elementary subterm occurs in q.

Assume that among b_1, b_2, and b_3, there is a non-supporting occurrence, but that not all three occurrences belong to the same elementary subterm. By Lemma 3.29 and its corollaries, b_2 is a supporting occurrence, one of b_1 and b_3 is a supporting occurrence, and the other lies in the same elementary subterm as b_2. Assume that b_1 lies in $\underline{p}_{i_1}$ and b_2 and b_3 in $\underline{p}_{i_2}$. The variable symbols $\underline{y}_{i_1}$ and $\underline{y}_{i_2}$ are adjacent in $\underline{r}$, and so there are adjacent occurrences of $\underline{y}_{i_1}$ and $\underline{y}_{i_2}$ in $\underline{s}$. Then the left occurrence of $\underline{x}_2$ in $\underline{p}_{i_2}$ is adjacent in $\underline{s}'$ to the left occurrence of $\underline{x}_1$ in $\underline{p}_{i_1}$; in addition, in $\underline{p}_{i_2}$, the left occurrence of $\underline{x}_2$ is adjacent to the occurrence of $\underline{x}_3$ in $\underline{p}_{i_2}$. Hence $\underline{q}$ has P_n.

It remains to consider the case when b_1, b_2, b_3 are supporting occurrences. Then in $\underline{s}'$, there are also supporting occurrences b_1°, b_2°, b_3° of the variable symbols $\underline{x}_1$, $\underline{x}_2$, and $\underline{x}_3$. We can construct an A-sequence for b_1° and b_3°: b_1°, b_2', ... b_s', b_3°, where $s \geqslant 0$. All these occurrences are supporting: if, among them, there were some non-left occurrence of some elementary subterm, then the left occurrence of the same subterm would occur twice in the sequence, since by Lemma 3.29, one can "enter" and "leave" a subterm only as a left occurrence. Let $P = \underline{x}_1\underline{x}_{i_1}\underline{x}_{i_2} \ldots \underline{x}_{i_s}\underline{x}_3$ be the corresponding sequence of variable symbols. If P contains each of $\underline{x}_1, \ldots \underline{x}_n$, then $\underline{r}'$ would contain at least n distinct elementary subterms, and so $\underline{r}$ would contain at least n distinct variable symbols, contradicting $k < n$. Further, if $\underline{x}_2$ is missing, P would contain each of $\underline{x}_1, \underline{x}_3, \ldots \underline{x}_n$, by Corollary 3.28. Since $\underline{x}_2$ is also a supporting occurrence, this would again contradict $k < n$. Hence P satisfies the conditions of Lemma 3.27, and so contains a subword $\underline{x}_1\underline{x}_2\underline{x}_3$. In the A-sequence, this yields an occurrence of $\underline{x}_2$ adjacent both to an occurrence of $\underline{x}_1$ and an occurrence of $\underline{x}_3$. Hence $\underline{q}$ has P_n.

Case (iv): By Corollary 3.30, b_2 is the left occurrence of $\underline{r}'$. Assume that b_3 lies outside $\underline{r}'$ and b_1 inside $\underline{r}'$. If b_1 belongs to the left elementary subterm of $\underline{r}'$, the lemma is proved, since the left elementary subterm of $\underline{s}'$ has the same form. Otherwise, by Corollary 3.31, b_1 is a supporting occurrence. Hence, in $\underline{s}'$, there is a supporting occurrence b_1° of $\underline{x}_1$. We join b_1° to the left occurrence b_2° of $\underline{x}_2$ in $\underline{s}'$ by an A-sequence. As before, all occurrences in it are supporting. In this sequence, b_2° adjoins either an occurrence of $\underline{x}_1$ or an occurrence of $\underline{x}_3$. In the first case, we are done, since b_2° is adjacent to the occurrence of $\underline{x}_3$ outside $\underline{s}'$. In the second case, there are supporting occurrences of $\underline{x}_1$, $\underline{x}_2$, and $\underline{x}_3$ in $\underline{s}'$, and the lemma is proved by the argument in Case (iii).

In all cases, then, $\underline{q}$ has P_n.

Theorem 3.36: $\mathfrak{A}$ has no FEB.

Proof: Suppose $\Sigma \subseteq \mathrm{Id}(\mathfrak{A})$ were a finite basis for $\mathrm{Id}(\mathfrak{A})$. There exists, then, a positive integer n such that each polynomial symbol occurring in Σ contains fewer than n variable symbols. Then, since $\Sigma \vdash F_n = G_n$ and F_n has P_n, by the last lemma, G_n must have P_n. But G_n does not have P_n.

CHAPTER IV

A SURVEY OF OTHER RESULTS

The aim of this chapter is to present a summary of all the additional results known to the author concerning the finite equational basis problem. Two of the shorter results, proving the existence of a FEB for any Boolean algebra and any abelian group, are presented in full detail. The remainder of the results are merely stated, with possibly an indication of their proofs.

1. Boolean algebras

Definition 4.1: A Boolean algebra is an algebra $\mathfrak{b} = \langle B; \vee, \wedge, ', 0, 1\rangle$ satisfying the following identities: $\Sigma = \{ \underline{x} \vee \underline{x} = \underline{x},\ \underline{x} \wedge \underline{x} = \underline{x},\ \underline{x} \vee \underline{y} = \underline{y} \vee \underline{x},\ \underline{x} \wedge \underline{y} = \underline{y} \wedge \underline{x},\ \underline{x} \vee (\underline{y} \vee \underline{z}) = (\underline{x} \vee \underline{y}) \vee \underline{z},\ \underline{x} \wedge (\underline{y} \wedge \underline{z}) = (\underline{x} \wedge \underline{y}) \wedge \underline{z},\ \underline{x} \wedge (\underline{x} \vee \underline{y}) = \underline{x},\ \underline{x} \vee (\underline{x} \wedge \underline{y}) = \underline{x},\ \underline{x} \vee (\underline{y} \wedge \underline{z}) = (\underline{x} \vee \underline{y}) \wedge (\underline{x} \vee \underline{z}),\ \underline{x} \wedge (\underline{y} \vee \underline{z}) = (\underline{x} \wedge \underline{y}) \vee (\underline{x} \wedge \underline{z}),\ \underline{0} \vee \underline{x} = \underline{x},\ \underline{1} \wedge \underline{x} = \underline{x},\ \underline{x} \vee \underline{x}' = \underline{1},\ \underline{x} \wedge \underline{x}' = \underline{0} \}$.

Let $\mathfrak{2}$ denote the 2-element Boolean algebra. We have already shown that $Id(\mathfrak{2})$ has a finite basis.

Theorem 4.2: Let $\mathfrak{b}$ be a Boolean algebra with more than two elements. Then $\mathrm{Id}(\mathfrak{b}) = \mathrm{Id}(\mathfrak{2})$.

Proof: Since B has more than two elements, $\mathfrak{b}$ has a two-element subalgebra isomorphic to $\mathfrak{2}$. If $\underline{p} = \underline{q}$ holds in $\mathfrak{b}$, then $\underline{p} = \underline{q}$ holds in the two-element subalgebra, and so in $\mathfrak{2}$. Conversely, let $\underline{p} = \underline{q} \in \mathrm{Id}(\mathfrak{2})$. Every Boolean algebra is a subdirect power of the two-element Boolean algebra (this can be proved by showing that there always exists a prime ideal separating any two distinct elements, as in Post Systems III). Then $\underline{p} = \underline{q}$ must hold in $\mathfrak{b}$.

Corollary 4.3: Any Boolean algebra has a FEB.

2. Abelian Groups

The major result of this section is due to B. H. Neumann [12].

Definition 4.4: A group is an algebra $\mathfrak{G} = \langle G; \cdot, ^{-1}, 1\rangle$ of type $\langle 2,1,0\rangle$, satisfying the group identities Σ (see page 31).

Let $K = \Sigma''$ denote the equational class of groups, and let $\tau = \langle 2,1,0\rangle$. Let Σ also denote the congruence relation on $\mathfrak{P}(\tau)$ defined by $\underline{p} \equiv \underline{q}(\Sigma)$ if and only if $\Sigma \vdash \underline{p} = \underline{q}$.

By Theorem 2.22, any identity $\underline{r} = \underline{s} \in Id(\tau)$ is equivalent modulo Σ to an identity of the form $\underline{p} = \underline{1}$.

Lemma 4.5: Let $\underline{p}(\underline{x}_0, \dots \underline{x}_{n-1}) = \underline{1} \in Id(\tau)$. Let $\mathfrak{G}(n) = \mathcal{P}^{(n)}(\tau)/\Sigma \cong \mathcal{F}_K(n)$, and let $\mathfrak{G}'(n)$ denote the commutator subgroup of $\mathfrak{G}(n)$. Then $\underline{p}(\underline{x}_0, \dots \underline{x}_{n-1}) = \underline{1}$ is equivalent modulo Σ to an identity of the form:

$$\underline{x}_0^{\alpha_0} \cdot \underline{x}_1^{\alpha_1} \cdot \dots \underline{x}_{n-1}^{\alpha_{n-1}} \; \underline{p}' = \underline{1}$$

where $[\underline{p}'] \in G'(n)$. (Note: $\alpha_i = 0$ will indicate non-occurrence of $\underline{x}_i$ in this form of the identity.)

Proof: $\mathfrak{G}(n)$ is generated by $[\underline{x}_0], \dots [\underline{x}_{n-1}]$. Now $[\underline{p}] \in G(n)$, so $[\underline{p}] = [\underline{q}][\underline{r}]$ where $[\underline{r}] \in G'(n)$, and $[\underline{q}] = [\underline{x}_{i_0}]^{\beta_0}[\underline{x}_{i_1}]^{\beta_1} \dots [\underline{x}_{i_{k-1}}]^{\beta_{k-1}}$ where $\{i_0, i_1, \dots i_{k-1}\} = \{0, 1, \dots n-1\}$, and again, $\beta_j = 0$ will be used to indicate non-occurrence of the equivalence class in question. Since $\mathfrak{G}(n)/\mathfrak{G}'(n)$ is abelian, $[\underline{p}] = [\underline{x}_{i_0}]^{\beta_0} \dots [\underline{x}_{i_{k-1}}]^{\beta_{k-1}}[\underline{r}] =$ $[\underline{x}_0]^{\alpha_0}[\underline{x}_1]^{\alpha_1} \dots [\underline{x}_{n-1}]^{\alpha_{n-1}}[\underline{p}']$, where $[\underline{p}'] \in G'(n)$, $= [\underline{x}_0^{\alpha_0} \cdot \underline{x}_1^{\alpha_1} \cdot \dots \underline{x}_{n-1}^{\alpha_{n-1}} \cdot \underline{p}']$. Then $\Sigma \vdash \underline{x}_0^{\alpha_0} \dots \underline{x}_{n-1}^{\alpha_{n-1}} \; \underline{p}' = \underline{p}$.

Then Σ, $\underline{p} = \underline{1} \vdash \underline{x}_0^{\alpha_0} \underline{x}_1^{\alpha_1} \ldots \underline{x}_{n-1}^{\alpha_{n-1}} \underline{p}' = \underline{1}$,

and Σ, $\underline{x}_0^{\alpha_0} \underline{x}_1^{\alpha_1} \ldots \underline{x}_{n-1}^{\alpha_{n-1}} \underline{p}' = \underline{1} \vdash \underline{p} = \underline{1}$, and this is precisely what is required.

Definition 4.6: Consider $\mathfrak{G}(\omega) = \mathfrak{P}(\tau)/\Sigma$, the free group on ω generators, and its commutator subgroup $\mathfrak{G}'(\omega)$. An identity $\underline{p} = \underline{1}$ is called a commutator identity if $[\underline{p}] \in G'(\omega)$.

Theorem 4.7: Let $\mathfrak{G}$ be a group. Then $\mathrm{Id}(\mathfrak{G})$ has a basis consisting of the group identities Σ, the identity $\underline{x}^k = \underline{1}$, where k is the least common multiple of the orders of all the elements of $\mathfrak{G}$ (if such k exists), and commutator identities.

Proof: Note first that k is the smallest positive integer for which $\underline{x}^k = \underline{1}$ holds, for if $\underline{x}^m = \underline{1}$ holds, then the order of every element divides m, and so k divides m, implying that $k \leqslant m$. Now if $\underline{p} = \underline{1}$ holds in $\mathfrak{G}$, we can assume that this identity has the form:

$$\underline{x}_0^{\alpha_0} \underline{x}_1^{\alpha_1} \ldots \underline{x}_{n-1}^{\alpha_{n-1}} \underline{p}' = \underline{1},\ [\underline{p}'] \in G'(n).$$

For each $i = 0, 1, \ldots n-1$, substitute $\underline{x}_i$ for $\underline{x}_i$ and $\underline{1}$ for the $\underline{x}_j$ where $j \neq i$. We get that the following hold in $\mathfrak{G}$: $\underline{x}_0^{\alpha_0} = \underline{1}, \ \ldots \ \underline{x}_{n-1}^{\alpha_{n-1}} = \underline{1}$. Since k divides

α_i, we have that Σ, $\underline{x}^k = \underline{1} \vdash \underline{x}_i^{\alpha_i} = \underline{1}$. Also, since these latter identities hold in $\mathfrak{A}$, we must have that $\underline{p}' = \underline{1}$ holds in $\mathfrak{A}$. Then Σ, $\underline{x}^k = \underline{1}$, $\underline{p}' = \underline{1} \vdash \underline{p} = \underline{1}$, and $\underline{p}' = \underline{1}$ is a commutator identity, since $G'(n) \subseteq G'(\omega)$.

If no positive integer k exists such that $\underline{x}^k = \underline{1}$ holds in $\mathfrak{A}$, then all identities of $\mathfrak{A}$ can be deduced from Σ and commutator identities.

Corollary 4.8: If $\mathfrak{A}$ is abelian, then $Id(\mathfrak{A})$ is finitely based.

Proof: Let $[\underline{p}'] \in G'(\omega)$. Then Σ, $\underline{x}\cdot\underline{y} = \underline{y}\cdot\underline{x} \vdash \underline{p}' = \underline{1}$. Hence Σ, $\underline{x}\cdot\underline{y} = \underline{y}\cdot\underline{x}$, $\underline{x}^k = \underline{1} \vdash Id(\mathfrak{A})$.

3. Further Results

(a) Primal Algebras:

Definition 4.9: An algebra $\mathfrak{A}$ is primal if it is A-finite, with more than one element, and if every function $f: A^n \rightarrow A$ is a polynomial.

Rosenbloom [15a] has shown that every primal algebra which is F-finite has a FEB. Mackenzie [9] has provided a simplified proof of this result. For each $n > 1$, he exhibits a primal algebra $\mathfrak{A}_n$ with n elements which has a FEB. Any primal algebra $\mathfrak{B}$ with n elements, then, can be assumed to be defined on the same set A_n, and so is equivalent to $\mathfrak{A}_n$. Then by Theorem 2.27, if $\mathfrak{B}$ is F-finite, then it has a FEB.

(b) Direct Products of Primal Algebras

Definition 4.10: A class $K = \{\mathfrak{A}_i \mid i \in I\}$ of algebras of the same type is said to be independent if whenever $\{\underline{p}_i \mid i \in I\}$ are polynomial symbols, then there is a polynomial symbol $\underline{p}$ such that $\underline{p}$ induces the same polynomial in $\mathfrak{A}_i$ as does $\underline{p}_i$, for each $i \in I$.

Yaqub [17] has proved the following:

Theorem 4.11: If $K = \{\mathfrak{A}_1, \mathfrak{A}_2, \dots \mathfrak{A}_n\}$ is a finite independent class of primal algebras, then $\mathfrak{A} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \dots \times \mathfrak{A}_n$ has a FEB.

The proof of this theorem depends upon the following lemma due to Foster [2], presented here without proof:

Lemma 4.12: Let K be as above. An algebra $\mathfrak{B}$ of the same type is isomorphic to a subdirect product of subdirect powers of the $\mathfrak{A}_i$ if and only if: $Id(\mathfrak{A}_1 \times \mathfrak{A}_2 \times \dots \times \mathfrak{A}_n) \subseteq Id(\mathfrak{B})$.

Yaqub points out that Foster uses only a finite subset $\Sigma \subseteq \mathrm{Id}(\mathfrak{A}_1 \times \mathfrak{A}_2 \times \dots \times \mathfrak{A}_n)$ in his proof, and that the lemma can be reformulated by replacing $\mathrm{Id}(\mathfrak{A}_1 \times \dots \times \mathfrak{A}_n)$ by Σ. The proof of the theorem then follows easily by considering the free algebra $\mathfrak{F}$ on ω generators satisfying Σ. If $\underline{p} = \underline{q}$ holds in $\mathfrak{A}_1 \times \dots \times \mathfrak{A}_n$, then it holds in each $\mathfrak{A}_i$, and so in $\mathfrak{F}$ which is a subdirect product of subdirect powers of the $\mathfrak{A}_i$. So $\Sigma \vdash \underline{p} = \underline{q}$.

(c) Semi-Groups

Definition 4.13: A uniformly periodic semi-group is one satisfying an identity of the form:

$$\underline{x}^{m+k} = \underline{x}^{m}$$

Definition 4.14: A permutative semi-group is one satisfying an identity of the form:

$$\underline{x}_0\underline{x}_1 \cdots \underline{x}_{n-1} = \underline{x}_{\nu(0)}\underline{x}_{\nu(1)} \cdots \underline{x}_{\nu(n-1)}$$

where ν is a permutation of the symbols 0, 1, ... n-1.

Perkins [14] has obtained the following results:

Theorem 4.15: Every commutative semi-groups has a FEB.

Theorem 4.16: Every uniformly periodic, permutative semi-group has a FEB.

Theorem 4.17: Every three-element semi-group has a FEB.

Theorem 4.17 follows almost immediately from Theorem 4.16, since of the eighteen isomorphism-anti-isomorphism types of three-element semi-groups (enumerated by Forsythe in [1]), seventeen are permutative, while the eighteenth can be shown to have a FEB using normal forms.

Perkins has also displayed a six-element semi-group of matrices under matrix multiplication which does not have a FEB. The matrices are:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

(d) Nilpotent and Finite Groups

Lyndon [8] has proved:

Theorem 4.18: Every nilpotent group has a FEB.

His result has been generalized by Higman [5] as follows:

Theorem 4.19: Let K and L be equational classes of groups, and let $K_\circ L$ denote the equational class of groups with a normal subroup in K with factor group in L. Then $Id(K_\circ L)$ is finitely based if every group in K is nilpotent, and Id(L) is finitely based.

This is indeed a generalization, for let $\mathfrak{G}$ be a nilpotent group. Then the equational class K generated by $\mathfrak{G}$ has every group in it nilpotent, and $Id(K) = Id(\mathfrak{G})$. Since $K = K \circ I$, where I is the equational class of one-element groups (which is trivially finitely based), Id(K) is finitely based, by Higman's theorem. Hence, $Id(\mathfrak{G})$ is finitely based.

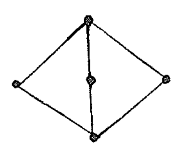
The following theorem has been proved by Oates and Powell [13]:

Theorem 4.20: Every finite group has a FEB.

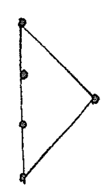
(e) Non-distributive Lattices

It is well-known that any non-distributive lattice contains one of the following as subalgebras:

M_5



N_5



B. Jonson has communicated to G. Gratzer that he has shown that $Id(M_5)$ has a finite basis.

Kirby Baker (in an unpublished result) has shown that there exist an infinite lattice with no FEB. This infinite lattice is, in fact, modular.

BIBLIOGRAPHY

[1] Forsythe, G. E. "SWAC computes 126 distinct semigroups of order 4." Proc. Amer. Math. Soc. Volume 6 (1955). 443 - 447.

[2] Foster, A. L. "The identities of - and unique subdirect factorization within - classes of universal algebras." Math. Z. Volume 62 (1955). 171 - 188.

[3] Gratzer, G. Universal Algebra (preliminary version). The Pennsylvania State University. 1966.

[4] Henkin, L. "Fragments of the propositional calculus." The Journal of Symbolic Logic. Volume 14 (1949). 42 - 48.

[5] Higman, G. "Some remarks on varieties of groups." Quart. J. Math. Oxford Ser. Volume 10 (1959). 165 - 178.

[6] Lyndon, R. C. "Identities in two-valued calculi." Trans. Amer. Math. Soc. Volume 71 (1951). 457 - 465.

[7] ______. "Identities in finite algebras." Proc. Amer. Math. Soc. Volume 5 (1954). 8 - 9.

[8] ______. "Two notes on nilpotent groups." Proc. Amer. Math. Soc. Volume 3 (1952). 579 - 583.

[9] MacKenzie, R. F. Letter to G. Gratzer. August 16, 1966.

[10] Mendelson, E. Introduction to Mathematical Logic. The University Series in Undergraduate Mathematics. D. Van Nostrand Company, Inc. Princeton, New Jersey. 1964.

[11] Murskii, V. L. "The existence in three-valued logic of a closed class with finite basis not having a finite complete system of identities." Soviet Math. Dokl. Volume 6, Number 4 (1965). 1020 - 1024.

[12] Neumann, B. H. "Identical relations in groups I." Math. Ann. Volume 114 (1937). 506 - 525.

[13] Oates and Powell. "Identical relations in finite groups." J. Algebra. Volume 1, Number 1 (1964). 11 - 39.

[14] Perkins, P. "Bases for equational theories of semigroups." (Unpublished preliminary version). Holy Cross College. Worcester, Mass.

[15] Post, E. L. The Two-Valued Iterative Systems of Mathematical Logic. Annals of Mathematics Studies, Number 5. Princeton University Press. Princeton, New Jersey. 1941.

[15a] Rosenbloom, P. C. "Post algebras. I. Postulates and general theory." American Journal of Mathematics. Volume 64 (1942). 167 - 188.

[16] Visin, V. V. "Identical transformations in four place logic." Soviet Math. Dokl. Volume 4, Number 3 (1963). 724 - 726.

[17] Yaqub, A. "On the identities of direct products of certain algebras." Amer. Math. Monthly. Volume 68 (1961). 239 - 241.