ALGEBRAIC METHODS IN LOGIC AND IN COMPUTER SCIENCE
BANACH CENTER PUBLICATIONS, VOLUME 28
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 1993

COMPLETE DESCRIPTION OF SUBSTITUTIONS IN CYLINDRIC ALGEBRAS AND OTHER ALGEBRAIC LOGICS

RICHARD J. THOMPSON

c/o Department of Algebraic Logic
Mathematical Institute of the Hungarian Academy of Sciences
Budapest, P.O. Box 127, H-1364, Hungary

1. Introduction. This paper can be read two ways. It can be read as a paper about algebraic logic, in particular cylindric algebras, and/or it can be read as a paper about transformation semigroups and their presentations or defining relations. On the *cylindric algebraic* level, we look at the so called *substitution operations*, the s^i_j's (which in polyadic algebra theory are denoted as $s_{[i/j]}$'s). When applying algebraic logic to first order logic, s^i_j is the operation which sends the formula φ to $\varphi(v_i/v_j)$ obtained from φ by replacing every free occurrence of v_i with v_j (replacing bound variables to avoid collision, if needed). The formula $\varphi(v_i/v_j)$ is equivalent with $\exists v_i(v_i = v_j \wedge \varphi)$. This is why, in cylindric algebra theory, $s^i_j(x) = c_i(d_{ij} \cdot x)$.

We will look at the "abstract" class CA_α of cylindric algebras. Let ES_α be the set of those equations in the language of CA_α which involve only the s^i_j's. So e.g. $s^0_1 s^0_1 x = s^1_2 x$ is in ES_α (if $\alpha > 2$) though it is not valid in CA_α. In [HMT], §1.5 explores the question, which elements of ES_α are valid in CA_α. Indeed, a great number of such equations are listed there. Here we will give a simple characterization of those elements of ES_α which are valid in CA_α (Theorem 3.6). This characterization provides an easy decision procedure, too.

Let us, next, look at representable CA_α's (RCA_α's). Strictly more elements of ES_α are valid in RCA_α than in CA_α. Our axiom system Σ in §2 below provides a complete axiomatization of the elements of ES_α valid in RCA_α. The same applies to representable quasi-polyadic algebras (RQPA_α's) in place of CA_α (cf. Sain–Thompson [ST]). The following result, taken from an early version of [S], can be

1991 *Mathematics Subject Classification*: 03G15, 20M05, 20M20, 03G99.

provided with a simpler proof using the semigroup-theoretic results herein. Let RSCA_α be the class of subreducts of RCA_α containing only the s^i_j's $(i, j \in \alpha)$ as extra-Boolean operations. (We note that RSCA_α is the same kind of subreduct of RQPA_α, too.) Then the equational theory of RSCA_α is axiomatized by postulates Σ from §2 herein together with the Boolean axioms and an axiom (schema) stating that the s^i_i's are Boolean endomorphisms. Sain's original proof of this relied on the main theorem of [J] as quoted in [HMT II], but it can be given a direct proof on the basis of Theorem 3.3 herein. Other examples for simplifying proofs of cylindric algebraic theorems are given below Theorem 3.3. For a recent overview of the kind of algebraic logic mentioned so far see Németi [N91].

The main purpose of the *semigroup-theoretic part* of this paper is to provide a set of defining relations for full semigroups of finite non-permutational transformations. We deal with the mappings of a set I into itself. To avoid triviality, we will apply throughout this paper the restriction that I contains at least 2 elements. For each such set I there is a set $NP(I)$ consisting of all mappings f of I into itself which are *finite transformations*—that is, $f(x) = x$ for all but finitely many elements x of I—and, in addition, are not permutations of I. In particular, we exclude, as a matter of convenience, the identity on I; the changes in this paper necessary to include this specific permutation in $NP(I)$ are fairly trivial, and we assume that the reader can see how to make them. In partial compensation, we do take account of the empty word on the semigroup generators.

Our method can be used to give a direct proof of the adequacy of Jónsson's defining relations for the semigroup of all finite transformations of a set into itself, which is the main theorem of Bjarni Jónsson's paper [J]. The reader of Jónsson's paper may also notice that in the last section of that paper he gives an application of his main theorem to cylindric algebras; the non-permutational semigroups considered in this paper are even more suitable for use in studying cylindric algebras. In fact, in a subsequent paper, we will report our study (based on the results of the present paper) of semigroups obtained by deleting some of the relations needed to define $NP(I)$; these semigroups correspond to cylindric algebras (or weaker systems of algebraic logic, such as in [N]) that are not (relativized) set algebras.

With a few exceptions we will use the notation of [HMT], [HMT II]. In particular, for a given set I (which will be fixed throughout most of our subsequent discussion) $[x/y]$ will be, for given distinct elements x and y of I, the finite transformation of I such that $[x/y](i) = i$ for $i \in I$ such that $i \neq x$, and $[x/y](x) = y$. This transformation $[x/y]$ will be called the *replacement of x by y in I*, or—more generally—a *replacement on I.* We note that in Jónsson's paper [J] the replacement of x by y in I is represented by exactly the opposite notation (there is also a printing error on page 79 in clause (iv) of his main theorem). We will, however, adopt, for use in Definition 2.1 and §4, Jónsson's notation for the *transposition of*

x and y in I, which we will designate by $[x,y]$ and define as the finite transformation of I such that $[x,y](x)=y$, $[x,y](y)=x$, and $[x,y](i)=i$ for $i\in I$ such that $i\neq x,y$. Such a transposition will be called, more generally, a *transposition on I*. (The notation $[x,y]$ also appears on p. 68 of [HMT II].) In the composition of functions we will take $(f\circ g)(i)=(fg)(i)$ to be the same as $g(f(i))$. (By $f\circ g$ we denote what is usually called the relational composition of f and g, and is denoted by $f|g$ in [HMT].) The empty set is $\emptyset$. As in [HMT], $A\sim B$ is the set-theoretic difference of A and B (those elements belonging to A but not to B) and $A\subset B$ is proper inclusion (that is, $A\subseteq B$ but $A\neq B$). Throughout, $\mathrm{Edm}(\sigma)$, or the *essential domain* of σ, is $\{i\in I:\sigma(i)\neq i\}$ for σ a transformation of I into itself. Also, $|A|$ is the cardinality of A, and $\mathrm{Rg}\,f$ in the proof is, of course, the range of f.

In the rest of the present introductory section we will establish some auxiliary propositions about semigroups we will need later. They are not really new; for the case when I is finite they were already proved in Howie [H].

For completeness (and because we need them for infinite I too) we include their proofs below.

PROPOSITION 1.1. *Suppose that σ is a mapping of the set I into itself which is not a permutation, and $i\in I$ is such that $\sigma(i)\neq i$. Then either σ is a replacement on I or there exists some mapping σ' of I into itself such that σ' is also not a permutation*, $|\{i\in I:\sigma'(i)\neq\sigma(i)\}|\leq 2$, $\mathrm{Edm}(\sigma')\subseteq\mathrm{Edm}(\sigma)$, *and* $i\notin\mathrm{Edm}(\sigma')$, *and σ is either $\varrho\sigma'$, $\sigma'\tau$, or $\varrho\sigma'\tau$, where ϱ and τ are either replacements on I or products of two replacements on I.*

Proof. Let σ be a mapping of I into I which is not a permutation, and let $i\in I$ be such that $\sigma(i)\neq i$.

Case 1: $i\notin\mathrm{Rg}\,\sigma$. If either there is some $k\neq i$ such that $k\notin\mathrm{Rg}\,\sigma$, or else there is *not* exactly one $j\in I$ such that $j\neq i$ and $\sigma(j)=\sigma(i)$, we can set: $\sigma'(i)=i$, $\sigma'(m)=\sigma(m)$ for $m\neq i$ (σ' will not be a permutation, as either there is some $k\neq i$ such that $k\notin\mathrm{Rg}\,\sigma$ and so $k\notin\mathrm{Rg}\,\sigma'$, or there is no $j\in I$ such that $j\neq i$ and $\sigma(j)=\sigma(i)$, and so $\sigma(i)\notin\mathrm{Rg}\,\sigma'$, or there exist $j,k\in I$ with $j\neq k$ and $i\neq j,k$ such that $\sigma(j)=\sigma(i)$ and $\sigma(k)=\sigma(i)$—and then $\sigma'(j)=\sigma(j)=\sigma(i)=\sigma(k)=\sigma'(k)$) and note that $\sigma=\sigma'[i/\sigma(i)]$ (using the fact that $i\notin\mathrm{Rg}\,\sigma$). Otherwise, for $n\neq i$ we have $n\in\mathrm{Rg}\,\sigma$, and there is exactly one $j\in I$ such that $j\neq i$ and $\sigma(j)=\sigma(i)$. If there is some $n\neq i,j$ such that $\sigma(n)\neq n$ we set: $\sigma'(i)=i$, $\sigma'(n)=n$, $\sigma'(m)=\sigma(m)$ for $m\neq i,n$ (σ' will not be a permutation since, as $n\in\mathrm{Rg}\,\sigma$, there is some $k\in I$ such that $\sigma(k)=n$, with $k\neq n$ as $\sigma(n)\neq n$, so either $k\neq i$ and thus $\sigma'(k)=\sigma(k)=n=\sigma'(n)$, or $k=i$ and $\sigma'(j)=\sigma(j)=\sigma(i)=\sigma(k)=n=\sigma'(n)$) and note that $\sigma=[i/j][n/i]\sigma'[i/\sigma(n)]$ (using the facts that $i\notin\mathrm{Rg}\,\sigma$ and $\sigma(i)=\sigma(j)$). Finally, if $\sigma(n)=n$ for all $n\neq i,j$ then $\sigma(i)=j$ (as $\sigma(i)\neq i$, so that if $\sigma(i)\neq j$ then $\sigma(\sigma(i))=\sigma(i)$, which implies $\sigma(i)=j$) so that σ is the replacement $[i/j]$.

Case 2: $i \in \mathrm{Rg}\,\sigma$. If there is some $j \in I$ such that $j \neq i$ and $\sigma(j) = \sigma(i)$ we can set: $\sigma'(i) = i$, $\sigma'(m) = \sigma(m)$ for $m \neq i$ (σ' will not be a permutation since, as $i \in \mathrm{Rg}\,\sigma$, there is some $k \in I$ such that $\sigma(k) = i$, with $k \neq i$ as $\sigma(i) \neq i$, so $\sigma'(k) = \sigma(k) = i = \sigma'(i)$) and note that $\sigma = [i/j]\sigma'$ (using the fact that $\sigma(i) = \sigma(j)$). Otherwise, if σ is not one-one there will be some $j \in I$ such that $j \neq i$, $\sigma(j) = \sigma(k)$ for some $k \in I$ such that $k \neq i, j$, and $\sigma(j) \neq j$. Then we can set: $\sigma'(i) = i$, $\sigma'(j) = \sigma(i)$, and $\sigma'(m) = \sigma(m)$ for $m \neq i, j$ (σ' will not be a permutation since, as $i \in \mathrm{Rg}\,\sigma$, there is some $n \in I$ such that $\sigma(n) = i$, with $n \neq i$ as $\sigma(i) \neq i$, so either $n \neq j$ so that $\sigma'(n) = \sigma(n) = i = \sigma'(i)$, or $n = j$ and $\sigma'(k) = \sigma(k) = \sigma(j) = \sigma(n) = i = \sigma'(i)$) and note that $\mathrm{Edm}(\sigma') \subseteq \mathrm{Edm}(\sigma)$ (as $\sigma(j) \neq j$) and $\sigma = [j/k][i/j]\sigma'$ (using the fact that $\sigma(j) = \sigma(k)$). Finally, if σ is one-one then—as it is not a permutation—there is some $k \in I$ such that $k \notin \mathrm{Rg}\,\sigma$, and some unique $j \in I$ such that $\sigma(j) = i$; since $k \notin \mathrm{Rg}\,\sigma$, $k \neq \sigma(i)$ and $k \neq i$ (as $i \in \mathrm{Rg}\,\sigma$). Then we can set: $\sigma'(i) = i$, $\sigma'(j) = k$, and $\sigma'(m) = \sigma(m)$ for $m \neq i, j$ (σ' will not be a permutation since $\sigma(i) \notin \mathrm{Rg}\,\sigma'$, as σ is one-one so that $\sigma(i) \neq \sigma(m) = \sigma'(m)$ for $m \neq i, j$, and $\sigma(i) \neq i = \sigma'(i)$ and $\sigma(i) \neq k = \sigma'(j)$) and note that $\mathrm{Edm}(\sigma') \subseteq \mathrm{Edm}(\sigma)$ (as $\sigma(j) \neq j$ since $\sigma(j) = i$ and $\sigma(i) \neq i$) and $\sigma = \sigma'[i/\sigma(i)][k/i]$ (using the facts that $k \notin \mathrm{Rg}\,\sigma$ and $\sigma(n) = i$ if and only if $n = j$). ■

COROLLARY 1.2. *Every element of $NP(I)$ is a replacement or a product of replacements.*

Proof. For $|I| < \omega$, Corollary 1.2 is proved as Theorem 1 in Howie [H]. Let $|I|$ be infinite and $\sigma \in NP(I)$. Let $E = \mathrm{Edm}(\sigma)$, and $\tau = \sigma \restriction E$. Then $\tau \in NP(E)$ and $|E| < \omega$. Hence, by [H, Thm. 1], $\tau = [i_1/j_1] \circ \ldots \circ [i_n/j_n]$ for some $i_1, \ldots, i_n, j_1, \ldots, j_n \in E$, with $[i_1/j_1]$ understood in E. But the same remains true if we interpret $[i_1/j_1]$ in I and hence $\sigma = [i_1/j_1] \circ \ldots \circ [i_n/j_n]$ in I as was desired. ■

PROPOSITION 1.3. *If σ is a* (*non-empty*) *product of replacements on I, then there exist $i, j \in I$ with $i \neq j$ such that $\sigma(i) = \sigma(j)$, and there exists some $k \in I$ such that $k \notin \mathrm{Rg}\,\sigma$.*

Proof. Obvious. ■

From the corollary and the proposition above we immediately obtain

COROLLARY 1.4. *$NP(I)$ is a semigroup under functional composition, and it consists of just those finite transformations of I into itself which are replacements on I or* (*non-empty*) *products of replacements on I. Also, $NP(I)$ consists of just those finite transformations on I which are not one-one. Finally, $NP(I)$ consists of just those finite transformations σ on I for which $I \neq \mathrm{Rg}\,\sigma$.* ■

In connection with the last corollary see [CP, Exercise 3 of §1.7, p. 23, p. 2].

In the following sections we will often use Corollary 1.2, Proposition 1.3, and especially Corollary 1.4 without explicit mention. The main theorems are proved in §3; preliminary notions and results appear in §2. The reader's attention is particularly directed to the distinction made in §2 between so called *peripheral elements* and *core elements* of $NP(I)$. This distinction is somewhat like that between the finite transformations of I into itself which are permutations and those which belong to $NP(I)$. In §2 we will show that there are two distinct subsets of our defining relations (which will be in terms of generators that can be interpreted as replacements on I), neither including the other set, such that in deriving equalities between words corresponding to a peripheral element we use one subset, and in deriving equalities between words corresponding to a core element we use another subset.

2. Preliminary results. We will now consider various semigroups given by a set of generators determined by I, and satisfying various sets of relations. For a fixed choice of I the set of generators will be designated by F or H (in a more general context, by $F(I)$ or $H(I)$). The generators belonging to H consist of the elements t^i_j, for all $i, j \in I$ with $i \neq j$, and the generators belonging to F consist of these elements together with the elements q^i_j, for all $i, j \in I$ with $i \neq j$. In the proofs below we will often rely tacitly on the fact that if t^i_j belongs to H (or q^i_j belongs to F) then i and j are distinct elements of I. Also, when u and v are words on H (or on F) and we write "$u = v$" we usually have some particular set of relations in mind from which the equality $u = v$ is derivable; we express the fact that the words u and v are the same word on H (or on F) by writing $u \equiv v$. The following definition indicates the meaning which we usually assign to the generators.

Definition 2.1. Suppose w is a word on the generators belonging to H or F. Then the *associated transformation for* w, designated by $\widehat{w}$ (or by the form $(w)\widehat{\ }$ when w is a complicated expression), is the identity transformation on I if w is the empty word, and otherwise is defined recursively as $\widehat{v}[i/j]$ if $w \equiv vt^i_j$ for some word v, and as $\widehat{v}[i,j]$ if $w \equiv vq^i_j$ for some word v. The *length* of w is 0 if w is the empty word and is defined recursively as $n+1$ if for some word v of length n (and some $i, j \in I$) $w \equiv vt^i_j$ or $w \equiv vq^i_j$. (Thus, if w is the word $t^{i_1}_{j_1} \ldots t^{i_n}_{j_n}$ on H, w has length n and $\widehat{w}$ is the element $[i_1/j_1] \circ \ldots \circ [i_n/j_n]$ of $NP(I)$.) The *vocabulary of* w, or $\mathrm{Voc}(w)$, is the subset of I consisting of all indices appearing in w.

The relations we will now be concerned with involve words on H; these relations will include various instances of some of the following schemas, where the assumption is made that *all indices appearing in a schema are distinct from each other,* and it is assumed that—subject to this condition—the indices can be arbitrary elements of I. (Note that, if $|I|$ is less than 4, schemas—as for instance (QUAD)—will be considered to hold "vacuously" when $|I|$ is too small for the required distinct indices to exist.)

The schemas are as follows:

$$\begin{array}{llll}
\text{(B1)} & t^i_j t^i_j = t^i_j\,, & \text{(B6)} & t^i_j t^m_n t^i_j = t^m_n t^i_j\,, \\
\text{(B2)} & t^i_j t^i_k = t^i_j\,, & \text{(EXC)} & t^i_j t^k_j = t^k_j t^i_j\,, \\
\text{(B3)} & t^i_j t^j_i = t^j_i\,, & \text{(DEXC)} & t^i_j t^m_n = t^m_n t^i_j\,, \\
\text{(B4)} & t^i_j t^j_k = t^i_k t^j_k\,, & \text{(TRI)} & t^k_i t^j_k t^i_j = t^i_k t^j_i t^k_j t^i_k\,, \\
\text{(B5)} & t^i_j t^k_j t^i_j = t^k_j t^i_j\,, & \text{(QUAD)} & t^n_i t^k_n t^j_k t^i_j = t^i_n t^j_i t^n_j t^k_n t^i_k\,.
\end{array}$$

We will let Σ (or, more generally, $\Sigma(I)$) be the set of all the relations appearing in the schemas above. By the *superficial relations* we mean the set Σ_1 of all the relations appearing in the schemas (B1), (B2), and (B3); by the *core relations* we mean the set Σ_2 of all the relations appearing in the schemas (B1)–(B6), (EXC), and (DEXC); and finally, by the *peripheral relations* we mean the set Σ_3 of all the relations appearing in the schemas (TRI) and (QUAD), together with the relations appearing in the schemas (B1), (B2), and (B3).

By examining the relations belonging to Σ it is apparent that, if $u = v$ is such a relation, then $\widehat{u} = \widehat{v}$; thus Proposition 2.2 below holds (this proposition will sometimes be used without explicit mention):

PROPOSITION 2.2. *If u and v are non-empty words on H such that $u = v$ is derivable from Σ then $\widehat{u} = \widehat{v}$. In other words, the function* $\mathrm{hat} : (H^*/\Sigma) \to NP(I)$, *with* $\mathrm{hat}(u/\Sigma) = \widehat{u}$ *for all $u \in H^*$, is a homomorphism (where H^*/Σ is the semigroup presented by Σ and generated by H).* ∎

PROPOSITION 2.3. *Suppose w and w' are words on H, and i and j are distinct elements of I. Then $\widehat{w}(i) = \widehat{w}(j)$ if $w \equiv t^i_j w'$, and $i \notin \operatorname{Rg} \widehat{w}$ if $w \equiv w' t^i_j$.*

Proof. Immediate by the definitions. ∎

The next proposition is merely inserted for convenient future reference, but the definitions and theorems following it concern the basic notions that will be involved in the proofs appearing in §3.

PROPOSITION 2.4. *Suppose i and j are distinct elements of I and u is a word on H. Then*:

(i) *If $i \in \operatorname{Rg}\widehat{u}$ then $\operatorname{Rg}(ut^i_j)^\frown = \{j\} \cup (\operatorname{Rg}\widehat{u} \sim \{i\})$, and if $i \notin \operatorname{Rg}\widehat{u}$ then $\operatorname{Rg}(ut^i_j)^\frown = \operatorname{Rg}\widehat{u}$.*

(ii) *If $i \notin \operatorname{Voc}(u)$ then $\widehat{u}(i) = i$ and $\widehat{u}(j) \neq i$.*

Proof. Obvious. ∎

DEFINITION 2.5. A *block* is a word on H of length 2 which is $t^a_b t^c_d$ for some $a \neq c, d$.

DEFINITION 2.6. A non-empty word on H will be called a *core word* if there is a (contiguous) subword which is a block; otherwise such a non-empty word will be called a *peripheral word.*

Definition 2.7. If σ is an element of $NP(I)$ (so that $\operatorname{Rg}\sigma \neq I$) then we will say that σ is a *peripheral element* just when $|I \sim \operatorname{Rg}\sigma| = 1$, and a *core element* just when $|I \sim \operatorname{Rg}\sigma| > 1$.

Definition 2.8. If σ is a transformation of I into itself we will say that $i \in I$ is *isolated under* σ just in case $\sigma(i) \neq \sigma(j)$ for all $j \in I$ such that $i \neq j$.

Theorem 2.9. *If w is a non-empty word on H then the following conditions are equivalent*:

(1) *There are at most* 2 *elements of I which are not isolated under $\widehat{w}$.*
(2) *$\widehat{w}$ is a peripheral element.*
(3) *w is a peripheral word.*

Proof. First of all, (1) *yields* (2). For if $\sigma = \widehat{w}$ is a core element of $NP(I)$ then by Definition 2.7 there exist $m, n \in I$ with $m \neq n$ such that $m \notin \operatorname{Rg}\sigma$ and $n \notin \operatorname{Rg}\sigma$. By Proposition 1.3 there is some $i \in I$ which is not isolated under σ. We can set: $\sigma'(i) = m$, $\sigma'(x) = \sigma(x)$ for $x \neq i$ (where $x \in I$); σ' belongs to $NP(I)$ as $n \notin \operatorname{Rg}\sigma'$ (since $n \neq m$ and $n \notin \operatorname{Rg}\sigma$), and i is isolated under σ' (as if $\sigma'(x) = m$ for $x \neq i$, then $\sigma(x) = \sigma'(x) = m$, which is impossible as $m \notin \operatorname{Rg}\sigma$). By Proposition 1.3 there exist $j, k \in I$ such that $j \neq k$ and $\sigma'(j) = \sigma'(k)$, so that j and k are not isolated under σ' and thus $i \neq j, k$. But then $\sigma(j) = \sigma'(j) = \sigma'(k) = \sigma(k)$, so that j and k are not isolated under σ either, and thus i, j, and k are 3 distinct elements of I which are not isolated under σ.

Next, (2) *yields* (3). For if w is a core word then w is (by Definitions 2.5 and 2.6) $ut^a_b t^c_d v$ for some (possibly empty) words u and v on H and some $a, b, c, d \in I$ such that $t^a_b t^c_d$ is a block, and thus $a \neq c, d$. By Proposition 2.3, $c \notin \operatorname{Rg}\widehat{t}$, where t is the word $ut^a_b t^c_d$, and $a \notin \operatorname{Rg}(ut^a_b)$ so that $a \notin \operatorname{Rg}\widehat{t}$ by Proposition 2.4(i) (since $a \neq d$); we conclude, as $a \neq c$, that $\widehat{t}$ is a core element. As from Proposition 2.4(i) it follows that, for $m, n \in I$ with $m \neq n$, and every word s on H, $|I \sim \operatorname{Rg}(st^m_n)\widehat{}\,| \geq |I \sim \operatorname{Rg}\widehat{s}\,|$, we must have (as $w \equiv tv$) $|I \sim \operatorname{Rg}\widehat{w}| \geq |I \sim \operatorname{Rg}\widehat{t}\,| \geq 2$, so that $\widehat{w}$ is also a core element.

Finally, (3) *yields* (1). For (1) holds if w has length 1, as (for $i, j \in I$ with $i \neq j$) i and j are the only elements of I not isolated under $[i/j]$. Proceeding by induction, if w has length greater than 1, then $w \equiv ut^a_b t^c_d$ for some word u on H and some $a, b, c, d \in I$ with $a \neq b$ and $c \neq d$, and with $a \in \{c, d\}$ as w is a peripheral word (so that $t^a_b t^c_d$ is not a block). By the inductive hypothesis, it is enough to show, for all $m, n \in I$ with $m \neq n$, that if $\widehat{w}(m) = \widehat{w}(n)$ then $(ut^a_b)\widehat{}\,(m) = (ut^a_b)\widehat{}\,(n)$. But, if $\widehat{w}(m) = \widehat{w}(n)$ then $[c/d]((ut^a_b)\widehat{}\,(m)) = \widehat{w}(m) = \widehat{w}(n) = [c/d]((ut^a_b)\widehat{}\,(n))$, so that either $(ut^a_b)\widehat{}\,(m) = (ut^a_b)\widehat{}\,(n)$ or else $\{c, d\} = \{(ut^a_b)\widehat{}\,(m), (ut^a_b)\widehat{}\,(n)\}$, which is impossible (as $a \notin \operatorname{Rg}(ut^a_b)\widehat{}$ by Proposition 2.3, so that $a \notin \{c, d\}$ would follow). ■

Theorem 2.10. *For every word w on H, if $i \in I$ but $i \notin \operatorname{Rg}\widehat{w}$, and $j \in I$ is such that $i \neq j$, then $wt^i_j = w$ is derivable from* (B1), (B2) *and* (EXC).

Proof. We proceed by induction on the length of w. Suppose the theorem is true for all shorter words, and i and j are distinct elements of I with $i \notin \operatorname{Rg} w$. Then w is not the empty word, so that $w \equiv vt^m_n$ for some word v on H and some distinct $m, n \in I$. If $m = i$ then $wt^i_j = w$ is derivable using (B1) or (B2). If $n = i$ then, as $i \notin \operatorname{Rg} w$, both $m \notin \operatorname{Rg} v$ and $i \notin \operatorname{Rg} v$ follow by Proposition 2.4(i); hence $w \equiv vt^m_n = v = vt^i_j = vt^m_n t^i_j \equiv wt^i_j$ is derivable using the induction hypothesis. If $i \neq m, n$ then, since we can derive $t^i_n t^m_n t^i_j = t^i_n t^m_n$ using (EXC), then (B1) or (B2), and then (EXC) again, we can use the induction hypothesis to derive $wt^i_j \equiv vt^m_n t^i_j = vt^i_n t^m_n t^i_j = vt^i_n t^m_n = vt^m_n \equiv w$ (as $i \notin \operatorname{Rg} w$ and Proposition 2.4(i) again yields $i \notin \operatorname{Rg} v$). So, in all cases, the theorem is also true for w, and thus is true in general, by induction. ∎

Theorem 2.11. *For every word w on H, if i and j are distinct elements of I such that $\widehat{w}(i) = \widehat{w}(j)$, then $t^i_j w = w$ is derivable from* (B1)+((B3)–(B6)).

Proof. This follows by induction on the length of w: suppose w is a word on H and $i, j \in I$ are distinct, with $\widehat{w}(i) = \widehat{w}(j)$, and the theorem is true for all words on H which are shorter than w. As $\widehat{w}(i) = \widehat{w}(j)$, w is not the empty word, so that $w \equiv t^m_n v$ for some word v on H and some distinct $m, n \in I$. If $\{i, j\} = \{m, n\}$ then $t^i_j w = w$ is derivable from (B1) or (B3). If $m = i$ but $n \notin \{i, j\}$ then $\widehat{v}(n) = \widehat{v}([i/n](i)) = \widehat{w}(i) = \widehat{w}(j) = \widehat{v}([i/n](j)) = \widehat{v}(j)$ so that $v = t^n_j v$ is derivable (by the induction hypothesis), and as we can derive $t^i_j t^i_n t^n_j = t^i_n t^n_j$ (using (B4), then (B1), and then (B4) again) it follows that we can derive $t^i_j w \equiv t^i_j t^i_n v = t^i_j t^i_n t^n_j v = t^i_n t^n_j v = t^i_n v \equiv w$. Similarly, if $m = j$ but $n \notin \{i, j\}$ then $t^j_i w = w$ is derivable, from which we can derive $t^i_j w = t^i_j t^j_i w = t^j_i w = w$ using (B3). And finally, if $m \notin \{i, j\}$ then $\widehat{v}(i) = \widehat{v}([m/n](i)) = \widehat{w}(i) = \widehat{w}(j) = \widehat{v}([m/n](j)) = \widehat{v}(j)$ so that $v = t^i_j v$ is derivable (by the induction hypothesis), and as we can derive $t^i_j t^m_i t^i_j = t^m_i t^i_j$ (using (B4), then (B5), and then (B4) again) it follows that we can derive $t^i_j w \equiv t^i_j t^m_n v = t^i_j t^m_n t^i_j v = t^m_n t^i_j v$ (using, if $n = i$, $t^i_j t^m_i t^i_j = t^m_i t^i_j$, (B5) if $n = j$, and (B6) if $n \neq i, j$) $= t^m_n v \equiv w$. So (in all cases) the theorem holds for w, and thus in general, by induction. ∎

3. Main results.

It is not difficult, in regard to Lemma 3.2(i) below, to convince oneself that the lemma must be true for the associated transformations in $NP(I)$ when the non-empty word w and $i \in I$ are such that either w is a core element or i is isolated under $\widehat{w}$; the condition that w is not i-initial is enough (see Definition 3.1), because of Proposition 2.3 and Theorem 2.9, to ensure that this is so. Thus, if Σ were taken to be all the relations holding in $NP(I)$, part (i) of the lemma would hold. But what is really significant is the first part of the proof of the lemma, where it is shown that the lemma holds in general if it holds for all words w of length less than or equal to 4; this means that only a *finite* subset of the relation schemes holding in $NP(I)$ need actually be required, so we can look at Σ as the result of choosing among the relations valid in $NP(I)$ so as to make this proof work, and regard (TRI) and (QUAD) as the most surprising of the relations that we need.

DEFINITION 3.1. Suppose w is a word on H and $i \in I$. Then w is *i-initial* just in case there are $c, d \in I$ and a word w' on H such that w is $t^c_d w'$ (so that $c \neq d$) and either $i = c$ or $i = d$.

LEMMA 3.2 (Standard form lemma). (i) *Suppose w is a non-empty word on H, and $i \in I$ is such that w is not i-initial. Then there is some non-empty word u on H such that $i \notin \mathrm{Voc}(u)$, and some word v on H which has length less than* 2, *or is $t^i_a t^b_i$ for some $a, b \in I$ with i, a, and b distinct, such that $w = uv$ is derivable from Σ and $\mathrm{Voc}(uv) \subseteq \mathrm{Voc}(w)$. Furthermore, v can be chosen so that if $\widehat{w}(i) = i$ then v is either the empty word or is t^b_i for some $b \neq i$, and if $\widehat{w}(i) = a \neq i$ then either v is t^i_a and $i \notin \mathrm{Rg}\, w$, or v is $t^i_a t^b_i$ for some $b \in I$ with $b \neq i, a$.*

(ii) *If w is a word on H, $i \in I$ is such that $i \notin \mathrm{Rg}\, \widehat{w}$, and w is either a core word or not i-initial, then there is some word w' on H such that $\mathrm{Voc}(w') \subseteq \mathrm{Voc}(w)$, $i \notin \mathrm{Voc}(w')$, and $w = w' t^i_j$ is derivable from Σ, where $j = \widehat{w}(i)$. Furthermore, w' can be chosen non-empty.*

Proof. (i) First of all, the last sentence follows from the rest. For if u and v are as in the lemma, $\widehat{w} = (uv)\widehat{\ }$ by Proposition 2.2, and so by (ii) of Proposition 2.4, $\widehat{w}(i) = \widehat{v}(\widehat{u}(i)) = \widehat{v}(i)$. Hence, if v is t^i_a for some $a \neq i$ then $i \notin \mathrm{Rg}\, \widehat{w}$, by Proposition 2.3, and $\widehat{w}(i) = \widehat{v}(i) = [i/a](i) = a \neq i$, and similarly if v is $t^i_a t^b_i$ for some $a, b \in I$ with i, a, and b distinct then $\widehat{w}(i) = \widehat{v}(i) = [b/i]([i/a](i)) = [b/i](a) = a \neq i$; otherwise $\widehat{w}(i) = \widehat{v}(i) = i$ since either $i \notin \mathrm{Voc}(v)$ (when v is the empty word or is t^m_n for some distinct $m, n \in I$ with $i \neq m, n$) or v is t^b_i for some $b \neq i$, so that $\widehat{v}(i) = [b/i](i) = i$. Note that the case where v is t^m_n and $i \neq m, n$ can be disregarded, as we can then re-define u as ut^m_n and v as the empty word.

Assuming that i is a fixed element of I, we will prove (i) by induction on the length of w. We observe that it is actually sufficient to prove the lemma for words of lengths 3 and 4 (if w has length less than 3 we can take u to be the word of length 1 such that $w \equiv uv$ for some word v)—more particulary, for words which are, for some $a, b, c, d, e, f \in I$ with $i \neq c, d$ and $c \neq d$, $a \neq b$, and $e \neq f$, either $t^c_d t^b_a t^e_f$ (these are just the words of length 3 which are not i-initial) or (with $i \neq a, b$ also) $t^c_d t^i_a t^b_i t^e_f$. For if w is not i-initial and has length greater than or equal to 4 it is (for some $e, f \in I$ with $e \neq f$) $w' t^e_f$ for some word w', also not i-initial, of length greater than or equal to 3, so that by the inductive hypothesis $w' = u'v'$ is derivable from Σ, and thus $w = u'v't^e_f$ also, for some words u' and v' such that $\mathrm{Voc}(u'v') \subseteq \mathrm{Voc}(w') \subseteq \mathrm{Voc}(w)$, $i \notin \mathrm{Voc}(u')$, u' is non-empty—so that $u' \equiv u_1 t^c_d$ for some word u_1 on H and some $c, d \in I$ with $c \neq d$ and $i \neq c, d$—and v' is either the empty word (when we can take u to be $u'v'$ and v to be t^e_f) or is, for some $a \neq b$, either t^b_a or (with $i \neq a, b$ also) $t^i_a t^b_i$. In these last two cases, taking w^* to be $t^c_d t^b_a t^e_f$ or $t^c_d t^i_a t^b_i t^e_f$ respectively, the existence of u^* and v^* such that $w = u^* v^*$ is derivable from Σ (and so $w^* = u'v't^e_f \equiv u_1 w^* = u_1 u^* v^*$ is derivable), $\mathrm{Voc}(u^*v^*) \subseteq \mathrm{Voc}(w^*) \subseteq \mathrm{Voc}(u'v') \subseteq \{e,f\} \cup \mathrm{Voc}(w)$, u^* is non-empty, and $i \notin \mathrm{Voc}(u^*)$, while v^* either has length less than or equal to 1 or is $t^i_x t^y_i$ for some distinct $x, y \in I$ with $i \neq x, y$, allows us to take u to be $u_1 u^*$ and v to be v^* (since $\mathrm{Voc}(u_1) \subseteq \mathrm{Voc}(u') \subseteq \mathrm{Voc}(w)$, and $i \notin \mathrm{Voc}(u_1)$ as $i \notin \mathrm{Voc}(u')$) and so satisfy (i) of the lemma.

So we have a limited number of cases to deal with. (And these would be cut in half if we required w in (i) of this lemma to be a peripheral word; then (ii) of this lemma would have to be proved directly for the case where w is a core word—one such proof uses Theorem 2.9 and Theorems 2.10 and 2.11.) The important ones are those in which t^c_d plays a role; in the routine cases we will omit the specification of u, and of v also, except when it is of length 2.

For $t^c_d t^b_a t^e_f$, where $i \neq c, d$ and $c \neq d$, $a \neq b$, and $e \neq f$, we note that if $i \neq a, b$ in addition then we can put $u^* \equiv t^c_d t^b_a$ and $v^* \equiv t^e_f$. So in the following cases we will assume that either $a = i$ or $b = i$.

Case (1): $b = e$. Then $t^b_a t^e_f = t^b_a$ follows from (B1) or (B2).

Case (2): $b \neq e$, and $i \neq e, f$. Then $t^b_a t^e_f = t^e_f t^b_{[e/f](a)}$ using (DEXC), or (EXC) and possibly (B4).

Case (3): $b \neq e, f$ and $i \neq e$, or $i = f$. Then (as $i = a$ or $i = b$) $a = i$ so $t^b_a t^e_f = t^b_{[e,f](a)} t^e_f$ using (B4).

Case (4): $b \neq e$, $b = f$, $a = e$. Then $t^b_a t^e_f = t^e_f$ follows from (B3).

Case (5): $b{\neq}e$, $b{=}f$, $a{\neq}e$, $b{=}i$. Then we can put $v^* \equiv t^i_a t^e_i$ as $t^b_a t^e_f \equiv t^i_a t^e_i$.

Special Case (I): $b \neq e$, $b = f$, $a \neq e$, $a = i$. Then, if $b = c$, we have $t^c_d t^b_a t^e_f = t^c_d t^e_f$ (using (B2)) and we can put $u^* \equiv t^c_d$, $v^* \equiv t^e_f$; if $b \neq c$ then $t^c_d t^b_a t^e_f \equiv t^c_d t^b_i t^e_b = t^c_d t^c_i t^b_i t^e_b$ (using (B2)) $= t^c_d t^b_i t^c_i t^e_b$ (using (EXC)) $= t^c_d t^b_c t^c_i t^e_b$ (using (B4)), and if $c = e$ then $t^c_d t^b_c t^c_i t^e_b = t^c_d t^b_c t^c_i$ (using (B2)) so we can put $u^* \equiv t^c_d t^b_c$ and $v^* \equiv t^c_i$, while if $c \neq e$ then $t^c_d t^b_c t^c_i t^e_b = t^c_d t^b_c t^e_b t^c_i$ using (DEXC), and we can put $u^* \equiv t^c_d t^b_c t^e_b$ and $v^* \equiv t^c_i$.

For $t^c_d t^i_a t^b_i t^e_b$, where $i \neq c, d$ and $c \neq d$, $a \neq b$, $e \neq f$, and $i \neq a, b$, we have these cases:

Case (6): $b = e$. Then $t^i_a t^b_i t^e_f = t^i_a t^b_i$ follows from (B1) or (B2); put $v^* \equiv t^i_a t^b_i$.

Case (7): $b \neq e, f$ and $i \neq e, f$. Then $t^i_a t^b_i t^e_f = t^i_a t^e_f t^b_i$ (using (DEXC)) $= t^e_f t^i_{[e/f](a)} t^b_i$ (using (DEXC), or (EXC) and possibly (B4)); put $v^* \equiv t^i_{[e/f](a)} t^b_i$ ($b \neq [e/f](a)$ since $b \neq a$ and $b \neq f$).

Case (8): $b \neq e, f$ and $i = e$ or $i = f$. Then $[e,f](i) \neq i$ (as $e \neq f$, and either $i = e$ or $i = f$), so $t^i_a t^b_i t^e_f = t^i_a t^b_{[e,f](i)} t^e_f$ (using (B4)) $= t^b_{[e,f](i)} t^i_a t^e_f$ (using (DEXC) or (EXC)), and if $e = i$ then $t^b_{[e,f](i)} t^i_a t^e_f = t^b_{[e,f](i)} t^i_a$ (using (B1) or (B2)), while if $f = i$ and $a \neq e$ then $t^b_{[e,f](i)} t^i_a t^e_f \equiv t^b_{[e,f](i)} t^i_a t^e_i$ and we can put $v^* \equiv t^i_a t^e_i$, and finally if $f = i$ and $a = e$ then, using (B3), $t^b_{[e,f](i)} t^i_a t^e_f = t^b_e t^e_i$.

Case (9): $b \neq e$, $b = f$, and $e = i$. Then $t^i_a t^b_i t^e_f \equiv t^i_a t^b_i t^i_b = t^i_a t^i_b$ (using (B3)) $= t^i_a$ (using (B2)).

Special Case (II): $b \neq e$, $b = f$, $e \neq i$, and $c = b$. Then $t^c_d t^i_a t^b_i t^e_f = t^b_d t^i_a t^b_i t^e_b = t^i_a t^b_d t^b_i t^e_b$ (using (EXC) or (DEXC)) $= t^i_a t^b_d t^e_b$ (using (B2)) $= t^b_d t^i_a t^e_b$ (using (EXC) or (DEXC)) $= t^b_d t^e_b t^i_{[e/b](a)}$ (using (DEXC), or (EXC) and possibly (B4)), and we put $v = t^i_{[e/b](a)}$ and $u = t^b_d t^e_b$.

Special Case (III): $b \neq e$, $b = f$, $e \neq i$, and $c \neq a, b$. Then, using (B1) or (B2), (DEXC), (B4), and (EXC), $t^c_d t^i_a t^b_i t^e_f = t^c_d t^i_a t^b_i t^e_b = t^c_d t^c_b t^i_a t^b_i t^e_b = t^c_d t^i_a t^c_b t^b_i t^e_b = t^c_d t^i_a t^c_i t^b_i t^e_b = t^c_d t^i_a t^b_i t^c_i t^e_b = t^c_d t^i_a t^b_c t^c_i t^e_b$ ((B4) again) $= t^c_d t^b_c t^i_a t^c_i t^e_b$ (using (DEXC) again). If $e = c$ then $t^c_d t^b_c t^i_a t^c_i t^e_b = t^c_d t^b_c t^i_a t^c_i$ using (B2), and we put $u^* \equiv t^c_d t^b_c$ and $v^* \equiv t^i_a t^c_i$ (as $c \neq a$). If $e \neq c$ then $t^c_d t^b_c t^i_a t^c_i t^e_b = t^c_d t^b_c t^i_a t^e_b t^c_i$ (using (DEXC)) $= t^c_d t^b_c t^e_b t^i_{[e/b](a)} t^c_i$ (using (DEXC), or (EXC) and possibly (B4)), so that since $c \neq [e/b](a)$ (because $c \neq a, b$) we can put $u^* \equiv t^c_d t^b_c t^e_b$ and $v^* \equiv t^i_{[e/b](a)} t^c_i$.

Special Case (IV): $b \neq e$, $b = f$, $e \neq i$, $c = a$, and $a = e$. Then $t^c_d t^i_a t^b_i t^e_f \equiv t^a_d t^i_a t^b_i t^a_b = t^a_d t^a_i t^b_a t^i_b t^a_i$ (using (TRI)) $= t^a_d t^b_a t^i_b t^a_i$ (using (B2)), and we can put $u^* \equiv t^a_b t^b_a$ and $v^* \equiv t^i_b t^a_i$. *This case uses* (TRI).

Special Case (V): $b \neq e$, $b = f$, $e \neq i$, $c = a$, and $a \neq e$. Then $t^c_d t^i_a t^b_i t^e_f \equiv t^a_d t^i_a t^b_i t^e_b = t^a_d t^a_e t^i_a t^b_i t^e_b$ (using (B1) or (B2)) $= t^a_d t^e_a t^b_e t^a_b t^i_a t^e_i$ (using (QUAD)), and we can put $u^* \equiv t^a_d t^e_a t^b_e t^a_b$ and $v^* \equiv t^i_a t^e_i$. *This case uses* (QUAD).

Proof of (ii). Suppose first that w is a word on H, $i \in I$ is such that $i \notin \operatorname{Rg} \widehat{w}$, and w is not i-initial. Then, by (i) of this lemma, there are words u and v such that $w = uv$ is derivable from Σ, $\operatorname{Voc}(uv) \subseteq \operatorname{Voc}(w)$, u is a non-empty word, $i \notin \operatorname{Voc}(u)$, and, with $a = \widehat{w}(i) \neq i$ (for $\widehat{w}(i) \neq i$ as $i \notin \operatorname{Rg} \widehat{w}$), v is either t^i_a or (for some $b \in I$ with $b \neq a$) $t^i_a t^b_i$. But, if v is $t^i_a t^b_i$, so that $w = u t^i_a t^b_i$ is derivable from Σ, $b \notin \operatorname{Rg}(u t^i_a)\widehat{\ }$ (as otherwise $i \in \operatorname{Rg} \widehat{w}$, by Proposition 2.4(i)) and thus $w = u t^i_a t^b_i = u t^i_a$ is derivable from Σ by Theorem 2.10. So, as $\operatorname{Voc}(u) \subseteq \operatorname{Voc}(uv) \subseteq \operatorname{Voc}(w)$ and $i \notin \operatorname{Voc}(u)$, we can take w' to be u in either case. Note: w' is non-empty.

Now suppose that w is a core word, so that (by Theorem 2.9) there are at least 3 elements of I which are not isolated under $\widehat{w}$, and thus there are $m, n \in I$ such that $m \neq n$, $i \neq m, n$, and $\widehat{w}(m) = \widehat{w}(n)$ (either $\widehat{w}(k) = \widehat{w}(i)$ for every $k \in I$ which is not isolated, and so $\widehat{w}(m) = \widehat{w}(i) = \widehat{w}(n)$ for any $m, n \in I$ which are not isolated under $\widehat{w}$, or there will be some $m \in I$ which is not isolated such that $\widehat{w}(m) \neq \widehat{w}(i)$, and some $n \in I$ such that $m \neq n$ but $\widehat{w}(m) = \widehat{w}(n)$, so that n is also distinct from i and not isolated). So $w = t^m_n w$ is derivable from Σ by Theorem 2.11, and thus $(t^m_n w)\widehat{\ } = \widehat{w}$ (by Proposititon 2.2). And then, as we proved above, since $t^m_n w$ is not i-initial and $i \notin \operatorname{Rg} \widehat{w} = \operatorname{Rg}(t^m_n w)\widehat{\ }$, $t^m_n w = w' t^i_j$ is derivable from Σ, where $j = (t^m_n w)\widehat{\ }(i) = \widehat{w}(i)$, for some word w' on H such that $i \notin \operatorname{Voc}(w')$ and $\operatorname{Voc}(w') \subseteq \operatorname{Voc}(t^m_n w) \subseteq \operatorname{Voc}(w)$ (in view of Proposition 2.4(ii), $m, n \in \operatorname{Voc}(w)$ as $m \neq n$ and $\widehat{w}(m) = \widehat{w}(n)$). Thus $w = t^m_n w = w' t^i_j$ is derivable from Σ, and w' is as required. (And w', chosen as above, is a non-empty word.) ∎

THEOREM 3.3 (Main semigroup-theoretic result). *For all non-empty words s and t on H, $\widehat{s} = \widehat{t}$ if and only if $s = t$ is derivable from the set of relations Σ.*

Proof. The "if" part follows from Proposition 2.2 (which will be used repeatedly below, without further mention). For the "only if" part we will assume that $\widehat{s} = \widehat{t}$ and proceed by induction on $|\mathrm{Voc}(s)| + |\mathrm{Voc}(t)|$. As s and t are non-empty words on H, $|\mathrm{Voc}(s)| \geq 2$ and $|\mathrm{Voc}(t)| \geq 2$. So, if $|\mathrm{Voc}(s)| + |\mathrm{Voc}(t)| \leq 4$ we have $|\mathrm{Voc}(s)| = 2 = |\mathrm{Voc}(t)|$, and by using (B1) and (B3) repeatedly we can derive $s = t_b^a$ and $t = t_d^c$ for some $a, b, c, d \in I$. As $\widehat{s} = \widehat{t}$, $[a/b] = [c/d]$, so that $a = c$ and $b = d$, and thus $s = t$ is derivable from Σ. Now let us assume that $|\mathrm{Voc}(s)| + |\mathrm{Voc}(t)| \geq 5$, and that for all non-empty words s' and t' on H such that $|\mathrm{Voc}(s')| + |\mathrm{Voc}(t')| < |\mathrm{Voc}(s)| + |\mathrm{Voc}(t)|$ and $\widehat{s}' = \widehat{t}'$ we can derive $s' = t'$ from Σ.

Case 1: Either s is a core word, or there is some $i \in I$ with $i \notin \mathrm{Rg}\,\widehat{s}$ and neither s nor t is i-initial. In view of Proposition 1.3 there is some $i \in I$ with $i \notin \mathrm{Rg}\,\widehat{s} = \mathrm{Rg}\,t$ such that, applying Lemma 3.2(ii), we can obtain words s' and t' on H for which $s = s't_j^i$ and $t = t't_j^i$ are derivable from Σ, where $j = \widehat{s}(i) = \widehat{t}(i)$, and such that $\mathrm{Voc}(s') \subseteq \mathrm{Voc}(s)$, $\mathrm{Voc}(t') \subseteq \mathrm{Voc}(t)$, $i \notin \mathrm{Voc}(s')$, and $i \notin \mathrm{Voc}(t')$. Then $|\mathrm{Voc}(s')| + |\mathrm{Voc}(t')| < |\mathrm{Voc}(s)| + |\mathrm{Voc}(t)|$ as $i \in \mathrm{Voc}(s)$ because of Proposition 2.4(ii) (since $i \notin \mathrm{Rg}\,\widehat{s}$), and $\widehat{s}' = \widehat{t}'$ (as for all $k \in I$, if $\widehat{s}'(k) \neq i$ and $\widehat{t}'(k) \neq i$ then $\widehat{s}'(k) = [i/j](\widehat{s}'(k)) = \widehat{s}(k) = \widehat{t}(k) = [i/j](t'(k)) = t'(k)$, but $\widehat{s}'(k) = i$ if and only if $k = i$, and $\widehat{t}'(k) = i$ if and only if $k = i$, by Proposition 2.4(ii)) so with s' and t' chosen non-empty (as Lemma 3.2(ii) allows) $s' = t'$ is derivable from Σ by the induction hypothesis, and thus $s = s't_j^i = t't_j^i = t$ is derivable from Σ.

Case 2: For every $i \in I$ such that neither s nor t is i-initial, $i \in \mathrm{Rg}\,\widehat{s}$, and s is a peripheral word. It follows, by Theorem 2.9, that $\widehat{s}$ is a peripheral element of $NP(I)$ and that there are at most 2 elements of I which are not isolated under $\widehat{s}$. As s and t are non-empty words on H, $s \equiv t_d^c s_1$ and $t \equiv t_f^e t_1$ for some words s_1 and t_1 on H and some $c, d, e, f \in I$ with $c \neq d$ and $e \neq f$. Note that $\widehat{s}(c) = \widehat{s}(d)$ and similarly $\widehat{s}(e) = \widehat{t}(e) = \widehat{t}(f) = \widehat{s}(f)$, using Proposition 2.3, so that $\{c, d\} = \{e, f\}$ as $\widehat{s}$ has at most 2 elements that are not isolated under it. If $|\mathrm{Voc}(s)| + |\mathrm{Voc}(t)| \leq 4$, then $s = t$ is derivable from Σ, as we saw above. Otherwise either $|\mathrm{Voc}(s)| > 2$ or $|\mathrm{Voc}(t)| > 2$, and thus there is some $k \notin \{c, d\} = \{e, f\}$ (so that k is isolated under $\widehat{s}$) such that either $k \in \mathrm{Voc}(s)$ or $k \in \mathrm{Voc}(t)$. As neither s nor t is k-initial, it follows by the hypothesis of this case that $k \in \mathrm{Rg}\,\widehat{s}$. By Lemma 3.2(i) there exist words s' and s^* on H such that s' is non-empty, $k \notin \mathrm{Voc}(s')$ (so that $\widehat{s}'(k) = k$ by Proposition 2.4(ii)), $\mathrm{Voc}(s's^*) \subseteq \mathrm{Voc}(s)$, and $s = s's^*$ is derivable from Σ. Furthermore, if $\widehat{s}(k) = k$ then $s = s'$ is derivable from Σ (this is immediate if s^* is the empty word; if s^* is t_k^b with $b \neq k$ then $b \notin \mathrm{Rg}\,\widehat{s}'$—as if $m \in I$ is such that $\widehat{s}'(m) = b$ then $\widehat{s}(m) = [b/k](\widehat{s}'(m)) = [b/k](b) = k = \widehat{s}(k)$ so $m = k$, as k is isolated under $\widehat{s}$, and thus $b = \widehat{s}'(m) = \widehat{s}'(k) = k$—and then $s = s't_k^b = s'$ is derivable from Σ by Theorem 2.10) and if $\widehat{s}(k) = a \neq k$ then $s = s't_a^k t_k^b$ is derivable, where b is the unique element of I such that $b \notin \operatorname{Rg} \widehat{s}$ (here s^* cannot be t^k_a, as $k \in \operatorname{Rg} \widehat{s}$, so s^* is $t^k_a t^b_k$ with $b \notin \operatorname{Rg} \widehat{s}$ by Proposition 2.3, and then we note that b is uniquely determined as $\widehat{s}$ is a peripheral element). Similarly, there is a non-empty word t' on H such that $k \notin \operatorname{Voc}(t')$ and $\operatorname{Voc}(t') \subseteq \operatorname{Voc}(t)$, and if $\widehat{t}(k) = k$ then $t = t'$ is derivable from Σ and so, as $\widehat{s}(k) = k$ (since $\widehat{s} = \widehat{t}$), $\widehat{s}' = \widehat{s} = \widehat{t} = \widehat{t}'$, while if $\widehat{t}(k) = a \neq k$ (and so $\widehat{s}(k) = a \neq k$) then $t = t' t^k_a t^b_k$ is derivable, where b is the unique element of I such that $b \notin \operatorname{Rg} \widehat{s} = \operatorname{Rg} \widehat{t}$, and so $\widehat{s}' = \widehat{t}'$ here also. (For by Proposition 2.4(ii), $\widehat{s}'(k) = k = \widehat{t}'(k)$, and for $n \in I$ with $n \neq k$ both $\widehat{s}'(n) \neq \widehat{s}'(k)$ and $\widehat{t}'(n) \neq \widehat{t}'(k)$ so that $[b/k](\widehat{s}'(n)) = [b/k]([k/a](\widehat{s}'(n))) = \widehat{s}(k) = \widehat{t}(k) = [b/k]([k/a](\widehat{t}'(n))) = [b/k](\widehat{t}'(n))$, and thus $\widehat{s}'(n) = \widehat{t}'(n)$ for $n \neq k$, as $\{\widehat{s}'(n), \widehat{t}'(n)\} = \{b, k\}$ is impossible.) Thus $s' = t'$ is derivable from Σ by the induction hypothesis, for $|\operatorname{Voc}(s')| + |\operatorname{Voc}(t')| < |\operatorname{Voc}(s)| + |\operatorname{Voc}(t)|$ as either $k \in \operatorname{Voc}(s)$ or $k \in \operatorname{Voc}(t)$; so finally, if $\widehat{s}(k) = k$ then $s = s' = t' = t$ is derivable from Σ, and if $\widehat{s}(k) \neq k$ then $s = s' t^k_a t^b_k = t' t^k_a t^b_k = t$ is derivable from Σ. ■

The theorem just proved can be used as a more efficient substitute for the use of Jónsson's theorem in the theory of *cylindric algebras*. Namely, the proof of Theorem 3.2.53 in [HMT II], the representation theorem for cylindric algebras of positive characteristic, can be modified to use the (fairly easily proved) fact that in all cylindric algebras of positive characteristic the analogs of (TRI) and (QUAD) hold (the rest of the schemas in Σ hold in arbitrary cylindric algebras); this avoids the 9 pages required to show that the analogs of transpositions can be defined (in a rather complicated way) and demonstrated to have the properties required by Jónsson's theorem. Another use of our Theorem 3.3 is to obtain Lemma 1 in [AT] as an immediate corollary, avoiding Andréka's lengthy argument required to adapt Jónsson's theorem, in Andréka's proof of the Resek–Thompson geometric representation theorem for cylindric algebras (cf. also [A]). So, our theorem can be used to improve Andréka's short proof (in [A] and [AT]) of the Resek–Thompson theorem.

Other kinds of applications to algebraic logic can be obtained as follows. Let us define t^i_j in cylindric algebras by letting $t^i_j(x) = d_{ij} \cdot c_i x$. Then (B1)–(DEXC) hold in arbitrary cylindric algebras (CA's). Hence the consequences of (B1)–(DEXC) exhibited herein are all valid in CA's. Actually, they can be used to characterize those equations involving only the s^i_j's (or equivalently, the t^i_j's) as basic operations that hold in all CA's. E.g. a transparent decision algorithm for these equations follows from the results in this paper. We turn to formulating this result. This formulation is intended to be self-contained only for those readers who are somewhat familiar with the basic concepts of CA theory.

Let α be an ordinal. If w is a word over $H(\alpha)$ then $w(x)$ is a CA_α-term, since $t^i_j(x)$ was defined above as a CA_α-term.

COROLLARY 3.4. *Let w, u be words over $H(\alpha)$. Then* $\mathrm{CA}_\alpha \models w(x) = u(x)$ *iff* (i) *or* (ii) *below holds.*

(i) *$\widehat{w}$ is a core element and $\widehat{w} = \widehat{u}$.*

(ii) *Using only* (B1)–(B3), *we can "reduce" w to w' and u to u' with $w' \equiv u'$.*

Proof. The proof uses the definition $t^i_j(x) = d_{ij} \cdot c_i x$ of the t^i_j's and related considerations immediately preceding the statement of the present corollary. Further, $\mathrm{CA}_\alpha \models$ ((B1)–(DEXC)) is proved in [HMT, 1.5], while for $\mathrm{CA}_\alpha \not\models$ [(TRI) *or* (QUAD)] see [HMT II, 3.2.71 and 3.2.88(2),(3), p. 101]. (TRI) and (QUAD) are called the *merry-go-round* identities, cf. e.g. [HMT II, 3.2.88]. The results we quote from [HMT], [HMT II] are stated there in terms of the s^i_j's instead of the t^i_j's, but, as Lemma 3.5 below says, these are equivalent (from the point of view of validity of equations). Recall that below Definition 2.1 we called (B1)–(DEXC) the core relations (and ((B1)–(B3))+(TRI)+(QUAD) the peripheral relations). The reason for this was that in the semigroup-theoretic part of this paper (ending with Theorem 3.3) we proved that if *$\widehat{w}$ is a core element* and $\widehat{w} = \widehat{u}$ then ((B1)–(DEXC)) $\vdash w = u$. Hence $\mathrm{CA}_\alpha \models w(x) = u(x)$ in this case, too. On the other hand, if *$\widehat{w}$ is not a core element* and $\widehat{w} = \widehat{u}$ then [((B1)–(DEXC)) $\vdash w = u$ iff ((B1)–(B3)) $\vdash w = u$], i.e., of the core relations only (B1)–(B3) are useful in proving peripheral (i.e., non-core) equalities. This was again established in the semigroup-theoretic part of the present paper. Putting all these together yields Corollary 3.4. ■

Note that in (ii), w' is a subword of w. Moreover, one can regard (B1)–(B3) as rather simple postulates saying that certain letters in a word are "superfluous". So (ii) says that dropping the superfluous letters from both sides, we obtain the same word on both sides. In other words, (B1)–(B3) define a normal form. And then part of Corollary 3.4 says that an equation between peripheral words is true in CA_α only if their normal forms coincide. Note that replacing the t^i_j's with s^i_j's in Corollary 3.4 makes no other change than reversing the order of the letters (in the words w and u). This way one can obtain a theorem saying

$$\mathrm{CA}_\alpha \models s^{i_1}_{j_1} \ldots s^{i_n}_{j_n}(x) = s^{k_1}_{m_1} \ldots s^{k_r}_{m_r}(x)$$

iff the (naturally) corresponding version of (i) and (ii) holds. The proof of Corollary 3.4 is straightforward, using the results in this paper and in [HMT, §1.5 (pp. 189–198)].

To make Corollary 3.4 directly applicable to s^i_j's, we state the following simple lemma.

Lemma 3.5. $\mathrm{CA}_\alpha \models s^{i_1}_{j_1} \ldots s^{i_n}_{j_n}(x) = s^{k_1}_{m_1} \ldots s^{k_r}_{m_r}(x)$ *if and only if*

$$\mathrm{CA}_\alpha \models t^{i_n}_{j_n} \ldots t^{i_1}_{j_1}(x) = t^{k_r}_{m_r} \ldots t^{k_1}_{m_1}(x).$$

Proof. We will prove more. Let $\mathfrak{A} = \langle A, \ldots, s^i_j, t^i_j \rangle_{i,j\in\alpha}$ be a Boolean algebra with operators (BAO for short) in the Jónsson–Tarski sense (cf. e.g. [HMT], or [ANS], or [ST]). Assume that s^i_j and t^i_j are conjugates in the standard BAO sense, i.e. $\mathfrak{A} \models t^i_j s^i_j x \le x \le s^i_j t^i_j x$, for all $i, j \in \alpha$. (These conditions are always true for t^i_j and s^i_j in CA_α's.)

Let $\overline{s} = s^{i_1}_{j_1} \ldots s^{i_n}_{j_n}$, $\overline{s_1} = s^{k_1}_{m_1} \ldots s^{k_r}_{m_r}$, and $\overline{t} = t^{i_n}_{j_n} \ldots t^{i_1}_{j_1}$, $\overline{t_1} = t^{k_r}_{m_r} \ldots t^{k_1}_{m_1}$. Then

Claim 3.5.1. *$\mathfrak{A} \models \overline{s}(x) = \overline{s_1}(x)$ iff $\mathfrak{A} \models \overline{t}(x) = \overline{t_1}(x)$.*

We prove direction "$\Rightarrow$" assume $\mathfrak{A} \models \overline{s}(x) = \overline{s_1}(x)$. Then $\mathfrak{A} \models \overline{t}(\overline{s}(x)) = \overline{t}(\overline{s_1}(x))$. Substituting $\overline{t_1}(x)$ for x, we obtain $\overline{t_1}(x) \ge (\overline{t}\overline{s})\overline{t_1}(x) = \overline{t}\overline{s}\overline{t_1}(x) = \overline{t}\overline{s_1}\overline{t_1}(x) = \overline{t}(\overline{s_1}\overline{t_1}(x)) \ge \overline{t}(x)$ by conjugacy (i.e. $y \ge \overline{t}\overline{s}(y)$ and $\overline{s_1}\overline{t_1}(x) \ge x$) and monotonicity of the operators s^i_j, t^i_j. By symmetry (i.e. by applying t_1 to both sides first and then substituting $\overline{t}(x)$ for x) we proved $\mathfrak{A} \models \overline{t_1}(x) = \overline{t}(x)$.

Direction "$\Leftarrow$" is completely analogous. (We apply $\overline{s}$ to both sides first, and then substitute $\overline{s_1}(x)$ for x, etc.) ■

Theorem 3.6 (Main cylindric-algebraic result). *Consider NP(α). Assume that $[i_1/j_1] \circ \ldots \circ [i_n/j_n] = [k_1/m_1] \circ \ldots \circ [k_r/m_r] = f \in {}^\alpha\alpha$ are such that $|\alpha \sim \mathrm{Rg}(f)| \ge 2$. Then, $\mathrm{CA}_\alpha \models s^{i_1}_{j_1} \ldots s^{i_n}_{j_n}(x) = s^{k_1}_{m_1} \ldots s^{k_r}_{m_r}(x)$.*

Proof. Assume f is as above. Let $w = t^{i_n}_{j_n} \ldots t^{i_1}_{j_1}$ and $u = t^{k_r}_{m_r} \ldots t^{k_1}_{m_1}$. Since (i) of Corollary 3.4 is satisfied by w and u, Corollary 3.4 yields $\mathrm{CA}_\alpha \models t^{i_n}_{j_n} \ldots t^{i_1}_{j_1}(x) = t^{k_r}_{m_r} \ldots t^{k_1}_{m_1}(x)$. Then, by Lemma 3.5, $\mathrm{CA}_\alpha \models s^{i_1}_{j_1} \ldots s^{i_n}_{j_n}(x) = s^{k_1}_{m_1} \ldots s^{k_r}_{m_r}(x)$ as was desired. ■

The paper [Sh], together with the ones quoted in [Sh], contain investigations related to the ones in the present paper. The results, however, do not overlap with those in the present paper, and therefore we refrain from going into more specific discussion of the connections with [Sh].

Acknowledgements. Thanks are due to H. Andréka, I. Németi, and I. Sain for extensive help in preparing this paper.

References

[A] H. Andréka, *A combinatorial proof for the celebrated Resek–Thompson theorem*, preprint, Math. Inst. Hungar. Acad. Sci., 1986.

[ANS] H. Andréka, I. Németi and I. Sain, *Algebraic Logic*, Lecture Notes of Logic Graduate School, Budapest 1991, 139 pp. Shortened version is [N91].

[AT] H. Andréka and R. J. Thompson, *A Stone-type representation theorem for algebras of relations of higher rank*, Trans. Amer. Math. Soc. 309 (2) (1988), 671–682.

[CP] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Vol. I, Amer. Math. Soc., Providence, RI, 1961.

[HMT] L. Henkin, J. D. Monk and A. Tarski, *Cylindric Algebras*, *Part I*, North-Holland, Amsterdam 1971.

[HMT II] —, —, —, *Cylindric Algebras*, *Part II*, North-Holland, Amsterdam 1985.

[H] J. M. Howie, *Idempotent generators in finite full transformation semigroups*, Proc. Royal Soc. Edinburgh 81A (1978), 317–323.

[J] B. Jónsson, *Defining relations for full semigroups of finite transformations*, Michigan Math. J. 9 (1962), 77–85.

[N] I. Németi, *Free algebras and decidability in algebraic logic*, dissertation (B) for D.Sc. with Hungar. Acad. Sci., Budapest 1986 (in Hungarian. An abstract in English is available from the author).

[N88] —, *On cylindric algebraic model theory*, in: Algebraic Logic and Universal Algebra in Computer Science (Proc. Conf. Ames 1988), Lecture Notes in Comput. Sci. 425, Springer, 1990, 37–75.

[N91] —, *Algebraizations of Quantifier Logics*, *An Introductory Overview*, Studia Logica 50 (3/4) (1991), Special Volume Dedicated to Algebraic Logic, W. J. Blok and D. Pigozzi (eds.), 485–569. An extended and regularly updated version is available from I. Németi.

[RT] D. Resek and R. J. Thompson, *Characterizing relativized cylindric algebras*, in: Algebraic Logic (Proc. Conf. Budapest 1988), H. Andréka, J. D. Monk and I. Németi (eds.), Colloq. Math. Soc. J. Bolyai 54, North-Holland, Amsterdam 1991, 519–538.

[S] I. Sain, *Searching for a finitizable algebraization of first order logic*, preprint No. 53/1987, Math. Inst. Hungar. Acad. Sci., 1987, 78 pp.

[ST] I. Sain and R. J. Thompson, *Strictly finite schema axiomatization of quasi-polyadic algebras*, in: Algebraic Logic (Proc. Conf. Budapest 1988), H. Andréka, J. D. Monk and I. Németi (eds.), Colloq. Math. Soc. J. Bolyai 54, North-Holland, Amsterdam 1991, 539–571.

[Sh] È. G. Shutov, *Homomorphisms of the semigroup of all near-identity mappings*, Izv. Vyssh. Uchebn. Zaved. Mat. 1963 (2), 176–180 (in Russian).