* Semigroup Forum Vol. ?? (??) ??-?? Version of June 11, 2011

Definability in the lattice of equational theories of semigroups

Jaroslav Ježek and Ralph McKenzie

Communicated by Editor ??

ABSTRACT

We study first-order definability in the lattice $\mathcal{L}$ of equational theories of semigroups. A large collection of individual theories and some interesting sets of theories are definable in $\mathcal{L}$. As examples, if T is either the equational theory of a finite semigroup or a finitely axiomatizable locally finite theory, then the set $\{T, T^{\partial}\}$ is definable, where T^{∂} is the dual theory obtained by inverting the order of occurences of letters in the words. Moreover, the set of locally finite theories, the set of finitely axiomatizable theories, and the set of theories of finite semigroups are all definable.

* The research of both authors was supported by National Science Foundation Grant No. DMS-8302295

Introduction

We study first-order definability in the lattice $\mathcal{L}$ of equational theories of semigroups, adapting the approach used by the first author for studies of definability in the lattice $\mathcal{L}_\Delta$ of all equational theories of a type Δ. In Section 1, we show that the set of ideal theories is definable in $\mathcal{L}$. This allows us to interpret in $\mathcal{L}$ first the lattice of full sets of words, and then the ordered set of patterns. (A pattern is an orbit under the action of automorphisms on the free semigroup; and the order relation on patterns is inherited from the relation "substitutable into" between words.) In fact, $\mathcal{L}$ has a definable subset order isomorphic to the ordered set of patterns. The equational theory corresponding to a pattern is to be thought of as a code (like a Gödel number) for the pattern.

We prove in Section 2 that the set of finite sequences of words can be nicely coded in the ordered set of patterns. Thus we can define all the usual syntactical notions between two equations, within this ordered set. Under the combined interpretations, certain ideal theories serve as codes for equations.

A major goal is to prove that the relation $\mathrm{Code}(S,T)$, which holds between theories S and T iff S is the code for an equation (u,v) and T is the set of consequences of (u,v), is definable in $\mathcal{L}$. We have not been able to prove this; but the results in this paper strongly suggest that it is true. In his papers [2], the first author proved precisely this result for the lattice $\mathcal{L}_\Delta$ of all equational theories of an arbitrary type Δ of operations; and it had some nice consequences—such as the definability in $\mathcal{L}_\Delta$ of the set of one-based theories, the set of finitely based theories, and the set of theories of finite algebras. Also, he proved that the theory generated by any given equation, and the theory of any given finite algebra, is definable up to automorphisms of the lattice $\mathcal{L}_\Delta$. If indeed the relation $\mathrm{Code}(S,T)$ is definable in $\mathcal{L}$ (and we conjecture it is) then all these results can be obtained for equational theories of semigroups.

We call a set U of equations good if the relation

$$\mathrm{Code}_U(S,T) \quad\leftrightarrow\quad [\mathrm{Code}(S,T) \text{ and } S \text{ is the code for an equation in } U]$$

is definable in $\mathcal{L}$. A more precise formulation is given in Section 3; the relation $\mathrm{Code}(S,T)$ has to take, in fact, a third parameter which decides whether each word (like xxy) is to be conceived literally or dually (like yxx). If U is a good set which is closed under duality, then the set of all theories generated by subsets of U, the set of all theories generated by finite subsets of U, and the set of all theories generated by individual equations in U, are definable sets in $\mathcal{L}$. Moreover, any automorphism of $\mathcal{L}$ coincides with either the identity or the duality on all the equational theories generated by subsets of U. (By the duality we mean the automorphism ∂ of $\mathcal{L}$ correlated with the mapping of a semigroup $\mathbf{S}=(S,\cdot)$ to its dual $\mathbf{S}^\partial=(S,\cdot^\partial)$ where $x\cdot^\partial y = y\cdot x$; if the relation $\mathrm{Code}(S,T)$ is definable, or if the set of all equations is good, then ∂ is the only non-identity automorphism of $\mathcal{L}$.) And for each finite subset F of U, the theory T generated by F is an element definable in $\mathcal{L}$ up to duality (by which we mean that the set $\{T, T^\partial\}$ is definable).

In Sections 4 through 9, we prove that some broad sets of semigroup equations are good: most significantly, the set of parallel equations, the set of semi-perfect equations, the set of permutational equations, the set of right- or left-regular equations, the set of absorption equations, and the set of all non-regular equations are good.

In Section 10, we prove that every locally finite theory is generated by a subset of the union of the six good sets mentioned above. This has the consequence that the theory of any finite semigroup is definable up to duality, and it implies the other definability results regarding locally finite theories that we mentioned in the abstract. The set of all finitely axiomatizable theories will be shown to be definable at the end of Section 11.

We have not been able, however, to quite finish our program. We hope that some techniques developed more intimately for the investigation of semigroup identities will enable some researcher to reach the goal outlined in this paper.

The paper by A. A. Iskander [1] is in the same spirit as this work. He obtains some results on definability in the lattice of equational theories of groups.

Preliminaries

Our work has to do with equational theories of semigroups, which we regard to be fully invariant congruences on a free semigroup, freely generated by a denumerably infinite set X. This free semigroup will be denoted by W. We call X the **alphabet**, call the elements of X **letters** and call the elements of W **words**. We use the characters x, y, z with or without subscripts to denote variables ranging over X. Words will be written as strings of letters. Thus the operation of the free semigroup becomes concatenation; if $x, y, z \in X$ then $u = xyxx$ and $v = xzxy$ are words, and $uv = xyxxxzxy$. This word uv is more compactly denoted by xyx^3zxy.

The **length** of a word u, written $|u|$, is the number of occurrences of letters in u; thus

$$|x| = 1,$$
$$|xyz| = 3,$$
$$|x^n| = n$$

Since we are reserving the vertical bars for denoting the length of words, we shall denote the cardinality of a set U by $\mathrm{Card}(U)$. The set of letters that occur in a word w is denoted by

$$\mathrm{supp}(w)$$

A word w is called **linear** iff

$$|w| = \mathrm{Card}(\mathrm{supp}(w))$$

In other words, w is linear iff no letter occurs twice in w.

The symbol $\emptyset$ denotes the empty set, which is also the empty word. The empty word is not a member of W, but it is useful to have it available. For instance, we say that u is a **subword** of v iff there are possibly empty words s and t (meaning $\{s,t\} \subseteq W \cup \{\emptyset\}$) such that $v = sut$. We say that u is an **initial part** of v iff there is a possibly empty word t such that $v = ut$, and we say that u is a **final part** of v iff there is a possibly empty word s such that $v = su$. The relations "u is a subword of v", "u is an initial part of v", "u is a final part of v" are written

$$u \subset v,$$
$$u \subset_l v,$$
$$u \subset_r v$$

The set of endomorphisms of W is denoted $\operatorname{End} W$. Its members are called **substitutions**, and generally denoted by the letters f, g, h, k. The fact that W is freely generated by X means that every function $\alpha : X \to W$ extends uniquely to a substitution. The restriction of a function α to a subset U of its domain is denoted by $\alpha|_U$. If $f \in \operatorname{End} W$ is a substitution and u a word, then $f(u)$ depends only on the values of f on the letters that occur in u. Thus if g is another substitution, then $f|_{\operatorname{supp}(u)} = g|_{\operatorname{supp}(u)}$ implies $f(u) = g(u)$.

The group of all permutations of a set U will be denoted by S_U. The set of automorphisms of W is denoted by $\operatorname{Aut} W$. Thus $f \in \operatorname{Aut} W$ iff $f \in \operatorname{End} W$ and $f|_X \in S_X$.

We use the special notation

$$\sigma_u^x \quad (\text{where } x \in X \text{ and } u \in W)$$

to denote the substitution f determined by $f(x) = u$ and $f(y) = y$ for every letter $y \neq x$. For a mapping p of a subset Y of X into W, we denote by $\bar{p}$ the unique substitution extending both p and the identity on $X \setminus Y$. Often in this situation, if $u \in W$ and $\operatorname{supp}(u) \subseteq Y$ we shall write simply $p(u)$ for $\bar{p}(u)$.

There is a natural quasi-order on W which will be important in our work. Where u and v are words, we put

$$u \leq v \quad \text{iff} \quad (\exists f \in \operatorname{End} W)(f(u) \subset v)$$

We define

$$u \sim v \quad \text{iff} \quad u \leq v \leq u,$$
$$u < v \quad \text{iff} \quad u \leq v \;\&\; \neg u \sim v$$

The relation $\leq$ is transitive and reflexive; therefore $\sim$ is an equivalence relation on words. Two words u and v such that $u \sim v$ are called **similar**. The equivalence classes $w/{\sim}$, $w \in W$, are called **patterns**, and we put

$$P = W/{\sim}$$

(the set of patterns). Given a substitution f and a word u, we say that f is **linear** on u iff f maps $\operatorname{supp}(u)$ one-one into X. Observe that $u \sim f(u)$ iff f is linear on u. Observe also that $u \sim v$ iff $v = g(u)$ for some substitution g such that g is linear on u iff $v = p(u)$ for some $p \in \mathrm{Aut}(W)$.

Patterns will be generally denoted by small Greek letters. The set P of patterns is ordered by putting $\alpha \leq \beta$ iff $u \leq v$, where $\alpha = u/{\sim}$ and $\beta = v/{\sim}$. Thus we have an ordered set $\mathcal{P} = (P, \leq)$. It is obvious that

$$u \leq v \longrightarrow |u| \leq |v|$$

and among the words of length at most n (for any fixed n), there are only a finite number of non-similar ones. Therefore the ordered set $\mathcal{P}$ has the property

$$(\forall \alpha \in P)(\{\beta \in P : \beta \leq \alpha\} \text{ is finite})$$

and every non-empty set of patterns contains a minimal element.

We identify equational theories (of semigroups) with fully invariant congruence relations on the free semigroup W. This means that T is an **equational theory** iff

(1) T is a **congruence relation** on W — i.e. $T \subseteq W^2$, T is an equivalence relation on W, and $(s,t) \in T$ and $u \in W$ imply $(us, ut) \in T$ and $(su, st) \in T$; and
(2) T is **fully invariant** — i.e. for every $f \in \mathrm{End}\, W$ and $(s,t) \in T$ we have $(f(s), f(t)) \in T$.

By an **equation** we mean simply an ordered pair of words. We shall use capital roman letters (avoiding P and W) to denote equational theories. The set of all equational theories is a subuniverse of the lattice of all equivalence relations on W. For equational theories S and T we write $S \leq T$ iff $S \subseteq T$, and $S < T$ iff $S \leq T$ and $S \neq T$. The meet (greatest lower bound) of S and T is their intersection, $S \wedge T = S \cap T$. The join, $S \vee T$, of S and T is the transitive closure of $S \cup T$. Thus an equation (u,v) belongs to $S \vee T$ iff there exist finitely many words $s_0, s_1, \ldots, s_n$ such that $s_0 = u$, $s_n = v$, $(s_i, s_{i+1}) \in S$ for all even $i < n$ and $(s_i, s_{i+1}) \in T$ for all odd $i < n$. We shall use $\mathcal{L}$ to denote both the set of all equational theories, and the lattice of all equational theories.

Because every substitution maps an equational theory T into itself — that is, $(f(u), f(v)) \in T$ whenever $(u,v) \in T$ and $f \in \mathrm{End}\, W$ — a theory T is invariant under every $f \in \mathrm{Aut}\, W$. The free semigroup W has, however, an involutory anti-automorphism, ∂, which induces a non-identity automorphism of $\mathcal{L}$, and will play a role in our work. Where u is a word, the **dual word** u^∂ is the word obtained by reversing the order of occurrence of the letters in u. Thus

$$\text{if } u = x_1 x_2 \ldots x_n \text{ where } x_1, \ldots, x_n \in X, \quad \text{then } u^\partial = x_n x_{n-1} \ldots x_1 .$$

Let Γ be a set of words, (u,v) be an equation, and S be a set of equations. Then we define

$$\begin{aligned} \Gamma^\partial &= \{u^\partial : u \in \Gamma\}, \\ (u,v)^\partial &= (u^\partial, v^\partial), \\ S^\partial &= \{e^\partial : e \in S\} \end{aligned}$$

Notice that if T is an equational theory, then T^∂ is also an equational theory, and $T^{\partial\partial} = T$; but there exist many equational theories which are not equal to their dual. The map ∂ on equational theories is an automorphism of $\mathcal{L}$.

The smallest equational theory containing a set Γ of equations will be denoted by $\mathrm{Eq}(\Gamma)$ (the **equational theory generated by** Γ). The theory generated by a single equation (s,t) will be denoted by $\mathrm{Eq}(s,t)$. A theory is said to be **finitely axiomatizable** (or **finitely generated**) if it is generated by some finite set of equations. Where $T = \mathrm{Eq}(\Gamma)$ and (u,v) is an equation, the notations

$$T \vdash (u,v),$$
$$\Gamma \vdash (u,v),$$
$$u \equiv_T v$$

all will be used with the same meaning; they assert that $(u,v) \in T$. This description of $\mathrm{Eq}(\Gamma)$, due to A. I. Maltsev, is most useful.

> An equation (a,b) belongs to $\mathrm{Eq}(\Gamma)$ iff there exists a Γ-derivation of (a,b), i.e. a finite sequence $a = w_0, \dots, w_n = b$ ($n \geq 1$) such that for every $i \in \{1, \dots, n\}$ either (w_{i-1}, w_i) or (w_i, w_{i-1}) is an immediate consequence of an equation from Γ. An equation (s,t) is said to be an immediate consequence of an equation (c,d) if there exists a substitution f and two possibly empty words u, v such that $(s,t) = (uf(c)v, uf(d)v)$.

Several special types of equations, and special equational theories will frequently enter our discussion, and we now describe some of them. An equation (s,t) will be called **regular** iff $\mathrm{supp}(s) = \mathrm{supp}(t)$; **parallel** iff it is regular and $s \not\lesssim t$ and $t \not\lesssim s$; **permutational** iff it is regular and $s \sim t$.

- C is the set of all equations (u,v) such that if either of u or v belongs to X, then $u = v$ (the constant theory).
- E is the set of all regular equations (the equational theory of semilattices).
- E_ℓ is the set of all equations i (xa, xb) where $x \in X$ and a and b are possibly empty words.
- E_r is the set of all equations (ax, bx) where $x \in X$ and a and b are possibly empty words.
- 0_W is the set of all equations (u,u), $u \in W$ (the least element of the lattice $\mathcal{L}$).
- 1_W $= W \times W$ (the largest element of the lattice $\mathcal{L}$).

1. Defining the set of ideal theories

By a **full set** of words we shall mean a set $J \subseteq W$ (possibly empty) such that $a \in J$ and $a \leq b$ imply $b \in J$. Thus a full set corresponds to an order filter in the ordered set of word patterns. If J is a full set, we define

$$I_J = 0_W \cup J^2$$

It is easy to check that I_J is an equational theory, if J is a full set. By an **ideal theory** we mean any equational theory of the form $T = I_J$ for some full set J. The two largest ideal theories are

$$1_W = I_W \quad \text{and} \quad C = I_{W \setminus X}$$

It is easy to see that the set of all full sets of words constitutes a lattice (ordered by set-inclusion), and that the mapping $J \mapsto I_J$ is a bijective order-preserving mapping of the set of full sets onto the set of all ideal theories. In fact, the ideal theories also constitute a lattice — a sublattice of the lattice of equational theories — and this mapping is an isomorphism between the lattice of full sets and the lattice of ideal theories. We write $\mathcal{F}$ for the lattice of full sets, and write $\mathcal{L}_{\mathrm{id}}$ for the lattice of ideal theories. Notice that the join and meet in $\mathcal{F}$ are set-union and set-intersection, and so $\mathcal{F}$ and $\mathcal{L}_{\mathrm{id}}$ are distributive lattices.

The principal full set corresponding to a word a is the set

$$J(a) = \{b \in W : a \leq b\}$$

The corresponding principal ideal theory is

$$I_a = I_{J(a)}$$

The aim of this section is to prove that the set of ideal theories is definable in the lattice $\mathcal{L}$ (Theorem 1.11). Now the set of principal ideal theories is identical with the set of strictly join-indecomposable members of $\mathcal{L}_{\mathrm{id}}$. This set is defined in the lattice $\mathcal{L}_{\mathrm{id}}$ by the formula

$$\Omega(T): \qquad (\exists S \in \mathcal{L}_{\mathrm{id}})(\forall A \in \mathcal{L}_{\mathrm{id}})[A < T \leftrightarrow A \leq S]$$

Therefore this set is definable in $\mathcal{L}$. Notice that the ordered set $\mathcal{P}$ of patterns, defined in the preliminary section, is isomorphic to the ordered set of principal full sets (ordered by set-inclusion), and therefore isomorphic to the ordered set of principal ideal theories. Thus $\mathcal{P}$ is interpretable in $\mathcal{L}$. In the next section, we investigate definability in $\mathcal{P}$.

In order to see how to define the ideal theories lattice-theoretically, we study the modular elements of $\mathcal{L}$. By a **modular element** of $\mathcal{L}$ we mean a theory T such that for all theories $A, B \in \mathcal{L}$, if $B \leq A$ then $A \wedge (B \vee T) = B \vee (A \wedge T)$. One can easily show that a theory T is a modular element of $\mathcal{L}$ iff for all theories $A, B \in \mathcal{L}$, if $B < A$ then it is not the case that $B \vee T \geq A$ and $A \wedge T \leq B$. In other words, $T \in \mathcal{L}$ is a modular element iff $\mathcal{L}$ has no five-element sublattice isomorphic to the pentagon in which T would correspond to the lonely midpoint.

The set of modular elements is a definable subset of $\mathcal{L}$. We shall now show that every ideal theory is a modular element. After some work, we shall be able to show that, conversely, every modular element stands in close relation to a certain ideal theory. Recall that E is the set of regular equations.

Proposition 1.1. *If T is an ideal theory, then T and $E \wedge T$ are modular elements.*

Proof. Let $T = I_J$ where $J \in \mathcal{F}$. Assume that A and B are theories such that $B \leq A$, $A \wedge T \leq B$, and $B \vee T \geq A$. We must show that $A = B$. For two theories D and D', we denote by $D \circ D'$ their composition; thus,

$$(s,t) \in D \circ D' \text{ iff for some } u,\ (s,u) \in D \text{ and } (u,t) \in D'$$

The theory $B \vee T$ is the equivalence relation join of B and T, and it has a particularly simple description, due to the fact that T is an ideal theory. Namely, $B \vee T = B \circ T \circ B$. To verify this, note that $B \circ T \circ B$ is a reflexive and symmetric binary relation. It is only necessary to show that it is transitive. Since $T = I_J$, if $s \equiv_T u \equiv_B v \equiv_T t$, then either $t = v$, or $s = u$, or $s, t \in J$ and $s \equiv_T t$. This means that $T \circ B \circ T = (B \circ T) \cup (T \circ B)$. From this fact, the transitivity of $B \circ T \circ B$ readily follows.

Now suppose that $(a,b) \in A$; we wish to prove that $(a,b) \in B$. Since $A \leq B \vee T = B \circ T \circ B$, there is $(s,t) \in T$ such that $(a,s) \in B$ and $(b,t) \in B$. Then since $B \leq A$, we have $(s,t) \in A \cap T$. So we have $(s,t) \in A \wedge T \subseteq B$, implying that $(a,b) \in B$ as desired. This completes the proof that I_J is a modular element.

Now let $T = E \wedge I_J$ where $J \in \mathcal{F}$. Let $B \leq A$, $B \vee T \geq A$, $A \wedge T \leq B$. The proof that $A = B$ divides into two cases. Suppose first that $B \leq E$. Then we can easily see that $B \vee T = B \circ T \circ B$ and conclude the proof just as above.

Suppose then that $B \not\leq E$. Let $(a,b) \in A$. If a fails to be B-equivalent to any member of J then, obviously, every word $B \vee T$-equivalent to a is B-equivalent to a; hence $(a,b) \in B$ (since $A \leq B \vee T$). Similarly, if b fails to be B-equivalent to a member of J then we are done. Thus we can assume that $(a,c) \in B$ and $(b,d) \in B$ where $c, d \in J$. Clearly $(c,d) \in A$; and now it suffices to show that $(c,d) \in B$.

If $\mathrm{supp}(c) \not\subseteq \mathrm{supp}(d)$, let f be a substitution such that $f(x) = cd$ for all $x \in \mathrm{supp}(c) \setminus \mathrm{supp}(d)$, and $f(x) = x$ for all other letters x. Then $f(d) = d$ and $f(c) = c'$ where $\mathrm{supp}(c) \subseteq \mathrm{supp}(c')$ and $\mathrm{supp}(d) \subseteq \mathrm{supp}(c')$. Moreover, $(d, c') \in A$ and $(c, c') \in A$. Note also that $c' \in J$.

Thus it will suffice to prove that $(a,b) \in B$ under the assumptions that $(a,b) \in A$, $\mathrm{supp}(a) \subseteq \mathrm{supp}(b)$, and $a, b \in J$. It is easy to see that since $B \not\leq E$, B contains some equation $s(x,y) = s(x,x)$ where x and y are different letters and both occur in the word $s = s(x,y)$. Choosing a letter $x_0 \in \mathrm{supp}(a)$, we define two substitutions. The substitution h is defined by $h(z) = z$ for $z \in \mathrm{supp}(a)$ and $h(z) = s(x_0, z)$ for all other letters z. The substitution k is defined by $k(z) = z$ for $z \in \mathrm{supp}(a)$ and $k(z) = s(x_0, x_0)$ for all other letters z. Observe that $\mathrm{supp}(a) = \mathrm{supp}(k(b))$, $\mathrm{supp}(b) = \mathrm{supp}(h(b))$, and $h(b), k(b) \in J$. Thus

$$(a, k(b)) \in T \quad \text{and} \quad (h(b), b) \in T$$

Since $(h(z), k(z)) \in B$ for all z, it follows that

$$(h(b), k(b)) \in B$$

Finally, we have $h(a) = a = k(a)$, implying that

$$(a, k(b)) \in A \quad \text{and} \quad (h(b), b) \in A$$

The formulas displayed above (and the assumption that $A \cap T \leq B$) imply that $(a, b) \in B$ as claimed. ∎

We proceed to establish some properties of modular elements.

Lemma 1.2. *Let $R \subseteq W^2$ be a binary relation and a be a word satisfying:*

(1) *$(u, v) \in R$ implies $u \neq v$ and u is an initial part of v.*
(2) *$(a, u) \in R$ for some word u.*
(3) *If $(c, d) \in R$ and $c \leq a$ then $c = a$.*

Then $(a, u) \in \mathrm{Eq}(R)$ implies a is an initial part of u.

Proof. We shall prove more: if $(u, w) \in \mathrm{Eq}(R)$ and if a is an initial part of u (possibly $a = u$), then a is an initial part of w. We can use the fact that $\mathrm{Eq}(R)$ is the equivalence relation generated by the relation consisting of the pairs $(sf(c)t, sf(d)t)$ such that s and t are possibly empty words, f is a substitution, and either $(c, d) \in R$ or $(d, c) \in R$. So it suffices to show that if $(c, d) \in R$ and one of $sf(c)t, sf(d)t$ has a as an initial part, then they both do. To begin, suppose that $(c, d) \in R$, f is a substitution, r, s, t are possibly empty words, and $ar = sf(d)t$. By (1) we have $d = ct'$ for some word t'. Thus $ar = sf(c)f(t')t$. If $|a| < |sf(c)|$, then clearly $sf(c)t$ does have a as an initial part. Suppose that $|a| \geq |sf(c)|$. Then $c \leq a$ since $f(c) \subset a$. By (2), $c = a$, and then a consideration of lengths shows that we must have $s = \emptyset$ and $f(c) = a$. Thus a is an initial part of $sf(c)t$ in both events. The same argument will show that if a is an initial part of $sf(c)t$, then it is an initial part of $sf(d)t$. ∎

Recall from the preliminary section that a permutational equation is a regular equation (u, v) such that $u \sim v$. If T is any theory, we put

$$J(T) = \{w \in W : (w, u) \in T \text{ for some non} - \text{permutational } (w, u)\}$$

After giving several lemmas, we shall be able to prove that if T is a modular element of $\mathcal{L}$, then $J(T)$ is a full set of words and $E \cap I_{J(T)} \subseteq T$.

Lemma 1.3. *If T is a modular element and $a \in J(T)$ then there are $s, t \in W$ with $\mathrm{supp}(st) \subseteq \mathrm{supp}(a)$ and $sa \equiv_T a \equiv_T at$.*

Proof. Let T be a modular element and let $a \in J(T)$. We claim that T contains an equation (a, d) with $d \not\leq a$. To see it, choose a non-permutational equation $(a, c) \in T$. If $\mathrm{supp}(a) \neq \mathrm{supp}(c)$, then we can quickly derive an equation $(a, d) \in T$ where $|a| < |d|$ and so $d \not\leq a$. So assume that (a, c) is regular (i.e. $\mathrm{supp}(a) = \mathrm{supp}(c)$) and $c \leq a$. Choose possibly empty words s, t and a substitution f such that $a = sf(c)t$, and put $d = sf(a)t$ so that $(a, d) \in T$. If $d \leq a$ then by length considerations, $s = \emptyset = t$ and $f(c) = a$, and $(a, f(a)) \in T$. Now assume that $f(a) \leq a$. Then since $|f(a)| \geq |a|$, it follows that we have $a = g(f(a))$ for some substitution g. This equality requires that

f maps the set $\mathrm{supp}(a)$ in one-one fashion onto a set of variables. As before, we can assume that $(a, f(a))$ is regular. Then it follows that $f(\mathrm{supp}(a)) = \mathrm{supp}(a)$; and since f is one-one on the set $\mathrm{supp}(a) = \mathrm{supp}(c)$ and $f(c) = a$, we have $a \sim c$. This contradicts our choice of (a, c) to be non-permutational.

So let $(a, d) \in T$ where $d \not\leq a$. Define theories $B = \mathrm{Eq}(d, da), A = \mathrm{Eq}((d, da), (a, a^2))$. Then $B \leq A$ and $(a, a^2) \in A \wedge (B \vee T)$. Since T is modular, we have $(a, a^2) \in B \vee (A \wedge T)$. But since $d \not\leq a$, $da \not\leq a$, the equivalence class of a modulo B contains only a. Therefore there must exist $u \neq a$ with $(a, u) \in A \wedge T$. Now it follows from Lemma 1.2 applied to $R = \{(d, da), (a, a^2)\}$ that we can write $u = at'$ where $t' \in W$. Thus $(a, at') \in T$. We also have $(a, t) \in T$ where t is obtained from t' by a substitution replacing all letters of $\mathrm{supp}(t') \setminus \mathrm{supp}(a)$ by some letter in $\mathrm{supp}(a)$. This t is the word we were looking for, and s can be found through the same procedure. ∎

Recall that we call an equation (r, s) parallel iff $\mathrm{supp}(r) = \mathrm{supp}(s)$ and $r \not\leq s$ and $s \not\leq r$.

Lemma 1.4. *Let T be a modular element and suppose that $T \cup \{(p, q)\} \vdash (r, s)$ where (r, s) is parallel and neither of p or q is $\leq$ r or s. Then $T \vdash (r, s)$.*

Proof. Let $B = \mathrm{Eq}(p, q)$ and $A = \mathrm{Eq}((p, q), (r, s))$. The assumptions on p, q, r, s are easily seen to imply that $r/B = \{r\}$, $s/B = \{s\}$, and $r/A = \{r, s\}$. Now $(r, s) \in A \wedge (B \vee T)$, implying $(r, s) \in B \vee (A \wedge T)$ since T is a modular element. The lemma follows readily from these observations. ∎

Lemma 1.5. *Let T be a modular element and (ac, ad) be a parallel equation where $a \in J(T)$. Then $(ac, ad) \in T$.*

Proof. By Lemma 1.3 we can choose a word s such that $(a, sa) \in T$. Then in Lemma 1.4 take $(p, q) = (sac, sad)$ and $(r, s) = (ac, ad)$. ∎

Proposition 1.6. *If T is a modular element then $J(T)$ is a full set and $E \cap I_{J(T)} \subseteq T$.*

Proof. Let T be a modular element. If $a \in J(T)$ and $a \leq b$, then $b = uf(a)v$ for possibly empty words u and v and a substitution f. There exists, by Lemma 1.3, a word $s \in W$ such that $(b, c) \in T$ where $c = uf(s)f(a)v$. Since $|b| < |c|$, it follows that $b \in J(T)$. Thus $J(T)$ is a full set.

To prove the second assertion, let (a, b) be a regular equation, where $a, b \in J(T)$. We have to show that $(a, b) \in T$. Choose, by Lemma 1.3, a word t such that $(a, at) \in T$ and $\mathrm{supp}(t) \subseteq \mathrm{supp}(a)$. Let x, y be different letters not belonging to the set $\mathrm{supp}(a) = \mathrm{supp}(b)$. By Lemma 1.5, we have

$$(axyy, axxy) \in T$$

Thus taking $x = t$ and $y = b$ gives

$$(ab^2, ab) \in T$$

Now let $m = 2|b|$ and $k = 2|t|$, so that $m > 1$, $k > 1$, and

$$|at^m| = |ab^k|$$

Then it is easy to check that $(at^m xx, axxb^k)$ is a parallel equation, hence belongs to T by Lemma 1.5. Then, taking $x = t$ in this equation yields $(a, ab^k) \in T$. Combined with $(ab^2, ab) \in T$, this gives $(a, ab) \in T$. By a similar (dual) argument, we can show that $(b, ab) \in T$, yielding that $(a, b) \in T$ as desired. ■

Lemma 1.7. *Let $T > 0_W$ be a modular element. Then $J(T) \neq \emptyset$.*

Proof. Choose $(a, b) \in T$, $a \neq b$. If (a, b) is non-permutational, then $a, b \in J(T)$. So assume that this equation is permutational, and let $p \in \operatorname{Aut} W$ be such that $p(\operatorname{supp}(a)) = \operatorname{supp}(a)$ and $p(a) = b$. Since $a \neq b$, there is a letter $x \in \operatorname{supp}(a)$ such that $p(x) \in X \setminus \{x\}$. Consider the equation $(c, d) = (axb, bxa) \in T$. We claim that this equation is parallel, and so non-permutational, implying that $c \in J(T)$. Indeed, if f is a substitution and $f(c) \subset d$, then since $|c| = |d|$ we have $f(c) = d$, and f acts as a permutation of $\operatorname{supp}(c) = \operatorname{supp}(a)$; and since $|a| = |b|$ we have $f(a) = b$, which implies that $f(x) = x$ and $f|_{\operatorname{supp}(a)} = p|_{\operatorname{supp}(a)}$. But this contradicts the fact that $p(x) \neq x$. So we conclude that $c \in J(T)$. ■

We now define a formula in the first-order language of lattices.

$\Phi_1(T)$: T is a modular element, $T > 0$, and for every modular element S satisfying $0 < S < T$, there exists an element $U \leq T$ such that there is no smallest $V \leq T$ satisfying $U \leq (U \wedge S) \vee V$.

Lemma 1.8. *If T is an equational theory such that $\mathcal{L} \models \Phi_1(T)$ then $T = I_J$ or $T = E \wedge I_J$ for some full set J.*

Proof. Let $\mathcal{L} \models \Phi_1(T)$ and put $J = J(T)$. By Proposition 1.6, J is a full set and $E \wedge I_J \subseteq T$. Assume that $E \wedge I_J < T$. Then we shall show that $T = I_J$.

First, assume that $T \leq E$. We shall derive a contradiction from this assumption. Letting $S = E \wedge I_J$, it follows from Proposition 1.1 and Lemma 1.7 that S is a modular element and $0_W < S < T$. Let $U \leq T$ satisfy the condition of $\Phi_1(T)$ for this S. Since $T \leq E$, and by the definition of $J = J(T)$, if $a \in J$ then $a/T = a/S = \{b \in J : \operatorname{supp}(a) = \operatorname{supp}(b)\}$; while if $a \notin J$ then $a/S = \{a\}$ and a/T is contained in the finite set of all words similar to a and with the same letters in them. Thus if $V \leq T$ then $U \leq (U \wedge S) \vee V$ iff $V \supseteq U \cap (W \setminus J)^2$. Hence there does exist a smallest $V \leq T$ satisfying $U \leq (U \wedge S) \vee V$, contradicting our choice of U to satisfy $\Phi_1(T)$. We conclude that $T \not\leq E$.

Now since $T \not\leq E$ there exists an equation $(s(x, y), s(x, x)) \in T$ where x and y are distinct letters, both occurring in $s = s(x, y)$. Clearly, $s \in J$, and so $(s(x, y), s(y, x)) \in T$ since $T \geq E \wedge I_J$. Thus $(s(x, x), s(y, y)) \in T$. Now if $a, b \in J$, we have

$$a \equiv_T s(a, a) \equiv_T s(b, b) \equiv_T b$$

(since $a, s(a, a) \in J$ and $\operatorname{supp}(a) = \operatorname{supp}(s(a, a))$), and the same holds for b and $s(b, b)$). Thus we have proved that $I_J \subseteq T$.

Now if $T > I_J$ then letting $S = I_J$, we see that $a/S = a/T$ for $a \in J$, and $a/s = \{a\}$ for $a \in W \setminus J$. Therefore the same argument used above to show that it is impossible for $E \wedge I_J < T \leq E$ to hold, will produce a contradiction. We conclude that $T = I_J$ in this case. ■

Recall that $J(a)$ denotes the principal full set generated by a word a, and $I_a = I_{J(a)}$.

Lemma 1.9. *For any word a, $\mathcal{L} \models \Phi_1(E \wedge I_a)$.*

Proof. Let $T = E \wedge I_a$. We know that T is a non-zero modular element by Proposition 1.1. Assume that $0_W < S < T$ and S is a modular element. Let $J = J(S)$ and put $U = \mathrm{Eq}(a, a^2)$. Assume that $V \leq T$ and V is the least theory $\leq T$ satisfying $U \leq (U \wedge S) \vee V$. We shall derive a contradiction. By Lemma 1.7, $J \neq \emptyset$, and this implies that $J(S)$ contains x^k for some integer $k > 1$ and $x \in X$; and S contains the equation (x^k, x^{k+1}), by Proposition 1.6.

If $m \geq k$ then, since $(a^m, a^{m+1}) \in U \wedge S$, it follows that $U \leq (U \wedge S) \vee \mathrm{Eq}(a, a^m)$, and so $V \leq \mathrm{Eq}(a, a^m)$. Thus

$$V \leq \bigcap_{m \geq k} \mathrm{Eq}(a, a^m)$$

It is easy to see that $(u, v) \in \mathrm{Eq}(a, a^m)$ implies $m - 1$ divides $|u| - |v|$. Thus $(u, v) \in V$ implies $|u| = |v|$. Letting

$$\Gamma = \{v \in W : |v| = |a| \,\&\, \mathrm{supp}(v) = \mathrm{supp}(a)\},$$

we can conclude that $(u, v) \in V$ and $u \in \Gamma$ imply $v \in \Gamma$. Note that $S < T$ implies $J \subset J(a)$ and $a \notin J$. Note also that $a \leq v \in \Gamma$ implies $a \sim v$. Thus if $(u, v) \in S$ is non-permutational, then $u \in J$, $a < u$, and $u \notin \Gamma$. Hence if $(u, v) \in S$ and $u \in \Gamma$ then $v \in \Gamma$. Now these observations imply, since $U \leq (U \wedge S) \vee V$, that Γ is a union of U-equivalence classes. This is false by definition of U, and the contradiction shows that $\mathcal{L} \models \Phi_1(E \wedge I_a)$. ∎

Now we introduce another formula.

$\Phi_2(T)$: $\Phi_1(T)$ holds, and whenever $T = M_1 \vee M_2$ and M_1 and M_2 are modular elements, then $T = M_1$ or $T = M_2$.

Proposition 1.10. *$\mathcal{L} \models \Phi_2(T)$ iff $T = E \wedge I_a$ for some $a \in W$.*

Proof. First, let $T = E \wedge I_a$ for some word a. Then $\mathcal{L} \models \Phi_1(T)$ by the last lemma. Suppose that $T = M_1 \vee M_2$ and both M_i are modular elements. If $a \in J(M_i)$, then it follows by Proposition 1.6 that $M_i = T$. If $a \notin J(M_1) \cup J(M_2)$, then the set of words $w \sim a$ such that $\mathrm{supp}(w) = \mathrm{supp}(a)$ is the union of M_1-equivalence classes and of M_2-equivalence classes. This is clearly impossible, because $T = M_1 \vee M_2$ and $(a, a^2) \in T$. We conclude that $\mathcal{L} \models \Phi_2(T)$.

Now assume that T is an equational theory and $\mathcal{L} \models \Phi_2(T)$. By Lemma 1.8, there exists a full set J such that $T = I_J$ or $T = E \wedge I_J$. Since $T > 0_W$, then $J \neq \emptyset$. Let a be a minimal member of J with respect to the quasi-ordering $\leq$, so that $b \in J$ and $b \leq a$ imply $b \sim a$. We claim that $J = J(a)$. If this fails to hold then there exists $b \in J$ such that $b \not\geq a$. In this case, letting $J_1 = J(a)$ and $J_2 = \{c \in J : c \not\leq a\}$, we have full sets $J_1, J_2 \subseteq J$ such that $J_1 \neq J \neq J_2$ and $J = J_1 \cup J_2$. It is easy to see that this yields modular elements $M_i = I_{J_i}$ (or $M_i = E \wedge I_{J_i}$) that join to T, while neither is equal to T. We conclude that $J = J(a)$, and thus $T = I_a$ or $T = E \wedge I_a$.

It only remains to observe that $\mathcal{L} \models \neg\Phi_2(I_a)$. Indeed, $I_a = (E \wedge I_a) \vee I_{a^2}$ and neither of the modular elements $E \wedge I_a$ or I_{a^2} is equal to I_a. ∎

Theorem 1.11. *The set of ideal theories is definable in $\mathcal{L}$, and the theories E and C are definable in $\mathcal{L}$.*

Proof. E (the set of regular equations) is the largest theory satisfying the formula Φ_2 of the previous proposition. Thus E is definable. It is not hard to verify, using Propositions 1.1, 1.6, and 1,10, that a theory T is an ideal theory iff T is a modular element, $T \nleq E$, and there does not exist a modular element $S < T$ such that $S \nleq E$ and S contains every theory $T' \leq T$ for which $\mathcal{L} \models \Phi_2(T')$. Thus the set of ideal theories is definable. C (the set of equations (u, v) such that $u = v$ or neither of u, v belongs to X) is definable as the largest ideal theory distinct from 1_W. ∎

The next definition and proposition will be needed later. For any word a we denote by $M(a)$ the set of all equations (u, v) such that either $u = v$, or $a \sim u \sim v$ and $\mathrm{supp}(u) = \mathrm{supp}(v)$, or $a < u$ and $a < v$.

Proposition 1.12. *$M(a)$ is the largest modular element T of $\mathcal{L}$ such that $T < I_a$ and $T \nleq E$.*

Proof. $M(a)$ can be shown to be a modular element by an argument modelled on our proof of Proposition 1.1. That $M(a)$ is the largest modular element satisfying the stated condition can be easily proved using Proposition 1.6. ∎

2. Definability in the ordered set of word patterns

Let α, β be two patterns. We write $\alpha \prec \beta$ if β is a cover of α, i.e. if $\alpha < \beta$ and there is no γ with $\alpha < \gamma < \beta$. The binary relation $\alpha \prec \beta$ is clearly definable in $\mathcal{P}$. In order to show later that many other relations are definable in $\mathcal{P}$, we start by looking at the relation $\alpha \prec \beta$ in more detail.

Proposition 2.1. *Let $\alpha = u/\!\sim$ and $\beta = v/\!\sim$ be two patterns. If $\alpha \prec \beta$ then one of the following four conditions is satisfied:*

(1) *$v \sim xu$ for some letter $x \notin \mathrm{supp}(u)$;*
(2) *$v \sim ux$ for some letter $x \notin \mathrm{supp}(u)$;*
(3) *$v \sim \sigma^x_y(u)$ for some pair x, y of distinct letters from $\mathrm{supp}(u)$;*
(4) *$v \sim \sigma^x_{xy}(u)$ for some $x \in \mathrm{supp}(u)$ and some letter $y \notin \mathrm{supp}(u)$.*

Conversely, if either (1) or (2) or (3) is satisfied then $\alpha \prec \beta$.

Proof. Let $\alpha \prec \beta$. There exists a substitution f such that $f(u)$ is a subword of v. If $f(u)$ is a proper subword then evidently either (1) or (2) takes place. If $f(u) = v$ and f maps $\mathrm{supp}(u)$ into X then (3) takes place; if $f(u) = v$ and $f(x) \notin X$ for some $x \in \mathrm{supp}(u)$ then (4) takes place.

In the converse direction we shall prove only that β is a cover of α if (1) is satisfied. Suppose that there exists a word t with $u < t < xu$. Then either $|t| = |u|$ or $|t| = |xu| = |u| + 1$. In each of these two cases we get a contradiction if we take into account the following two observations which are easy to prove: if w_1, w_2 are two words with $w_1 < w_2$ and $|w_1| = |w_2|$ then $\mathrm{Card}(\mathrm{supp}(w_2)) < \mathrm{Card}(\mathrm{supp}(w_1))$; if w_1, w_2 are two words with $w_1 < w_2$ and $|w_2| = |w_1| + 1$ then $\mathrm{Card}(\mathrm{supp}(w_2)) \leq \mathrm{Card}(\mathrm{supp}(w_1)) + 1$. ■

Let $\beta = v/\sim$ be a cover of $\alpha = u/\sim$. We say that β is a cover of α of type i ($i = 1, 2, 3, 4$) if the condition (i) in Proposition 2.1 is satisfied.

REMARK. If $\alpha = u/\sim$ and $\beta = v/\sim$ are two patterns satisfying the condition (4) in Proposition 2.1 then β is not necessarily a cover of α. For example, put $u = xyx$ and $v = xzyxz$, where x, y, z are three distinct letters. Also, it can happen (in some singular cases only) that a cover is a cover of several different types. For example, if $x_1, \dots, x_{n+1}$ are pairwise distinct letters ($n \geq 1$) then $(x_1 \dots x_{n+1})/\sim$ is a cover of $(x_1 \dots x_n)/\sim$ of each of the types 1,2,4. On the other hand, a cover of type 3 can never be a cover of any of the three types 1,2,4.

Lemma 2.2. *Let $\alpha = u/\sim$ and $\beta = v/\sim$ be two patterns such that β is a cover of α of one of the three types 1,2,3. Then β is a cover of α of type 3 iff for every pattern γ such that $\beta \prec \gamma$ there exists a pattern $\delta \neq \beta$ with $\alpha < \delta < \gamma$.*

Proof. Let $\alpha \prec \beta$ be of type 3, so that $v \sim \sigma_y^x(u)$ for some pair x, y of distinct letters from $\mathrm{supp}(u)$; we can suppose that $v = \sigma_y^x(u)$. Let $\beta \prec \gamma = w/\sim$. If $w \sim zv$ for some letter $z \notin \mathrm{supp}(v)$, we can suppose that $z \notin \mathrm{supp}(u)$ and we can put $\delta = (zu)/\sim$. If $w \sim vz$, the proof is similar. If $w \sim \sigma_p^z(v)$ for some pair z, p of distinct letters from $\mathrm{supp}(v)$, we can put $\delta = \sigma_p^z(u)/\sim$. If $w \sim \sigma_{zp}^z(v)$ for some $z \in \mathrm{supp}(v)$ and some letter $p \notin \mathrm{supp}(v)$, we can put $\delta = \sigma_{zp}^z(u)/\sim$.

Let $\alpha \prec \beta$ be of type 1, $v = xu$, $x \in X \setminus \mathrm{supp}(u)$. Put $\gamma = (yxu)/\sim$ where y is a letter not belonging to $\mathrm{supp}(xu)$. We must prove that $u < w < yxu$ implies $w \sim v$. It is easy to see that if w_1, w_2 are two words with $w_1 < w_2$ and $|w_2| = |w_1| + 2$ then $\mathrm{Card}(\mathrm{supp}(w_2)) \leq \mathrm{Card}(\mathrm{supp}(w_1)) + 2$. This observation together with the two observations from the proof of Proposition 2.1 implies that $|w| = |u|$ is impossible, and $|w| = |u| + 2$ is also impossible; and we are left with the following possibility only: $|w| = |u| + 1$ and $\mathrm{Card}(\mathrm{supp}(w)) = \mathrm{Card}(\mathrm{supp}(u)) + 1$. Moreover, it is easy to see that $u \prec w \prec yxu$. For every word t denote by $\lambda(t)$ the longest linear initial part of t. Since $|\lambda(yxu)| = |\lambda(u)| + 2$, it follows that $|\lambda(w)| = |\lambda(u)| + 1$ and this then yields $w \sim xu$.

If $\alpha \prec \beta$ is of type 2, we can proceed similarly. ■

Lemma 2.3. *Let α be a pattern. Then $\alpha = x^n/\sim$ for some letter x and some positive integer n iff for any cover β of α there exists a cover γ of β such that the interval $[\alpha, \gamma]$ consists of α, β, γ only.*

Proof. Let $\alpha = x^n/\sim$. Let β be a cover of α, so that there is a letter $y \neq x$ such that either $\beta = yx^n/\sim$ or $\beta = x^n y/\sim$ or $\beta = (xy)^n/\sim$. In the first two cases we can use Lemma 2.2. It remains to consider the case $\beta = (xy)^n/\sim$. Then we can put $\gamma = (xyz)^n/\sim$, where $z \in X \setminus \{x, y\}$; it is easy to prove that $[\alpha, \gamma] = \{\alpha, \beta, \gamma\}$.

In order to prove the converse implication, let $\alpha = u/\sim$ where

$$\mathrm{Card}(\mathrm{supp}(u)) \neq 1 .$$

Then α has a cover β of type 3. By Lemma 2.2, for every cover γ of β there exists a pattern $\delta \in [\alpha, \gamma] \setminus \{\alpha, \beta, \gamma\}$. ■

We are now going to establish definability of several relations in $\mathcal{P}$. Let us write $R(\alpha, \beta, \ldots)$ instead of $(\alpha, \beta, \ldots) \in R$.

Proposition 2.4. *The following relations are definable in $\mathcal{P}$:*

$R_1(\alpha)$: $\alpha = x^n/\sim$ *for some letter x and some positive integer n;*

$R_2(\alpha, \beta)$: $\alpha = u/\sim$ *and* $\beta = v/\sim$ *for some words u, v with $|u| \leq |v|$;*

$R_3(\alpha, \beta)$: β *is a cover of* α *of type 3;*

$R_4(\alpha)$: $\alpha = u/\sim$ *where u is a linear word;*

$R_5(\alpha)$: *either* $\alpha = xxy/\sim$ *or* $\alpha = yxx/\sim$ *for a pair x, y of distinct letters.*

Proof. The definability of R_1 follows from Lemma 2.3. We have $R_2(\alpha, \beta)$ iff $\beta \leq \gamma$ implies $\alpha \leq \gamma$ for any pattern γ satisfying $R_1(\gamma)$. We have $R_3(\alpha, \beta)$ iff $\alpha \prec \beta$ and $R_2(\beta, \alpha)$. We have $R_4(\alpha)$ iff there is no β with $R_3(\beta, \alpha)$. The elements $xxy/\sim$ and $yxx/\sim$ are the only two patterns $u/\sim$ such that $|u| = 3$ and $xx/\sim \prec u/\sim$; here $xx/\sim$ (where $x \in X$) is the only cover of type 3 of the only atom in $\mathcal{P}$. ■

Recall that, given a word u, we define the dual word u^∂ as follows: if $u = x_1 \ldots x_n$ where $x_1, \ldots, x_n$ are letters then $u^\partial = x_n \ldots x_1$. Also, put $(u/\sim)^\partial = u^\partial/\sim$. The mapping sending α to α^∂ is obviously an automorphism of the ordered set $\mathcal{P}$; later in this section we shall show that it is, except for the identity, the only automorphism of $\mathcal{P}$.

For any n-ary relation R on $\mathcal{P}$ we define the dual relation R^∂ by $(\alpha_1, \ldots, \alpha_n) \in R^\partial$ iff $(\alpha_1^\partial, \ldots, \alpha_n^\partial) \in R$. A relation R which is definable in $\mathcal{P}$ is necessarily self-dual (i.e. $R = R^\partial$). So, the best we can do with the definability of a non-self-dual relation seems to be to show that it is semi-definable in the following sense.

Let R be an n-ary relation on $\mathcal{P}$. Define an $(n+1)$-ary relation R' on $\mathcal{P}$ as follows: $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in R'$ iff either $\alpha_0 = xxy/\sim$ and $(\alpha_1, \ldots, \alpha_n) \in R$, or else $\alpha_0 = yxx/\sim$ and $(\alpha_1^\partial, \ldots, \alpha_n^\partial) \in R$. If R' is definable in $\mathcal{P}$ then we say that R is **semi-definable**.

Proposition 2.5. *The following relations are semi-definable in $\mathcal{P}$:*

$R_6(\alpha, \beta)$: $\alpha = x^n/\sim$ *and* $\beta = (x^n y)/\sim$ *for some positive integer n and two distinct letters x, y;*

$R_7(\alpha, \beta)$: $\alpha = x^n/\sim$ *and* $\beta = (x^n y_1 \ldots y_m)/\sim$ *for some positive integers n, m and pairwise distinct letters $x, y_1, \ldots, y_m$;*

$R_8(\alpha, \beta)$: $\alpha = x^n/\sim$ *and* $\beta = (x^n yx)/\sim$ *for some positive integer n and two distinct letters x, y;*

$R_9(\alpha, \beta)$: $\alpha = x^n/\sim$ *and* $\beta = (x^n y^m)/\sim$ *for some positive integers n, m with $m \leq n$ and two distinct letters x, y;*

$R_{10}(\alpha, \beta)$: $\alpha = x^n/\sim$ *and* $\beta = (x^n y^n)/\sim$ *for some positive integer n and two distinct letters x, y;*

$R_{11}(\alpha, \beta, \gamma)$: $\alpha = x^n/\sim$, $\beta = x^m/\sim$, *and* $\gamma = (x^n y^m)/\sim$ *for some positive integers n, m and two distinct letters x, y;*

$R_{12}(\alpha, \beta, \gamma)$: $\alpha = u/\sim$, $\beta = v/\sim$, *and* $\gamma = w/\sim$ *for some words u, v, w with $|w| = |u| + |v|$;*

$R_{13}(\alpha,\beta,\gamma)$: *$\alpha = x^i/\sim$, $\beta = x^j/\sim$, and $\gamma = (x_1 \dots x_n)/\sim$ for some $1 \le i < j \le n$ and some letters $x, x_1, \dots, x_n$ that are pairwise distinct except for $x_i = x_j$;*

$R_{14}(\alpha,\beta)$: *$\alpha = x^i/\sim$, $\beta = x^j/\sim$, and $\gamma = u/\sim$ for some letter x, some integers $1 \le i < j$ and some word u of length $\ge j$ in which the i-th letter equals the j-th letter;*

$R_{15}(\alpha,\beta)$: *$\alpha = u/\sim$ and $\beta = v/\sim$ for some words u, v such that u is an initial part of v;*

$R_{16}(\alpha,\beta,\gamma)$: *$\alpha = u/\sim$, $\beta = v/\sim$ and $\gamma = w/\sim$ for some words u, v, w such that $w = uv$.*

Proof. For example, the semi-definability of R_6 means that the ternary relation R defined in the following way is definable: $(\gamma,\alpha,\beta) \in R$ iff either $\gamma = xxy/\sim$, $\alpha = x^n/\sim$ and $\beta = (x^n y)/\sim$ or else $\gamma = yxx/\sim$, $\alpha = x^n/\sim$ and $\beta = (yx^n)/\sim$ for some $n \ge 1$ and two distinct letters x, y. The semi-definability of R_6 follows from the fact that $(u/\sim, v/\sim) \in R_6$ iff $(u/\sim) \in R_1$, $v/\sim$ is a cover of $u/\sim$, $|v| = |u| + 1$ and if t is the largest (with respect to the quasi-ordering $\le$) linear word which is $\le v$ then there is no cover w of t of type 3 such that $w \not\le v$ and $xxy \le w$.

We have $R_7(x^n/\sim, \beta)$ iff $x^n/\sim < \beta$, the interval $[x^n/\sim, \beta]$ is a chain, $x^n/\sim \le p/\sim \prec q/\sim \le \beta$ implies $|q| = |p| + 1$, and $R_6(x^n/\sim, \gamma)$ implies $\gamma \le \beta$.

We have $R_8(x^n/\sim, \beta)$ iff there exists a $u/\sim$ such that $R_7(x^n/\sim, u/\sim)$ is satisfied, $|u| = n + 2$ (so that $u \sim x^n yz$), $u/\sim \prec \beta$ is a cover of type 3, $x^{n+1}/\sim \not\le \beta$ and the following is true: if t is a linear word of length $n+2$ and w is a type 3 cover of t such that $xyy \le w$ and $yyx \not\le w$ then $w/\sim \not\le \beta$.

We have $R_9(x^n/\sim, u/\sim)$ iff u is not longer than the longest cover of x^n and there exists a $v/\sim$ such that $(x^n/\sim, v/\sim) \in R_7$ (so that $v \sim x^n y_1 \dots y_m$ with $m \le n$) and u is maximal among the words u with the following properties: $|u| = |v|$; $v \le u$; $x^{n+1} \not\le u$; $x^n yx \not\le u$.

The semi-definability of R_{10} is clear from that of R_9.

We have $(xxy/\sim, x^n/\sim, x^m/\sim, \alpha) \in R'_{11}$ iff either $m \le n$ and the triple $(xxy/\sim, x^n/\sim, \alpha)$ belongs to $R_9{}'$ and m is maximal such that $w/\sim \le \alpha$ for some word $w = x_1 \cdots x_k y^m$ such that $|w| = |\alpha|$, or else $n < m$, $(xyy/\sim, x^m/\sim, \alpha) \in R'_9$ and n is maximal such that $w/\sim \le \alpha$ for some word $w = x^n y_1 \cdots y_k$ such that $|w| = |\alpha|$.

The definability of R_{12} follows from the semi-definability of R_{11}.

We have $(xxy/\sim, x^i/\sim, x^j/\sim, u/\sim) \in R'_{13}$ iff $i < j$, $|u| \ge j$, $v \prec u$ is a cover of type 3 for some linear word v and the following are true: whenever $(xxy/\sim, x^k/\sim, w/\sim) \in R'_7$ where $|w| = |u|$ then $u \le w$ iff $k \ge j$; whenever $(yxx/\sim, x^k/\sim, w/\sim) \in R'_7$ where $|w| = |u|$ then $u \le w$ iff $k \ge |\alpha| - (i-1)$.

The semi-definability of R_{14} follows from that of R_{13}.

We have $(u/\sim, v/\sim) \in R_{15}$ iff $u \le v$ and the following is true: whenever $(x^i/\sim, x^j/\sim, t_1/\sim) \in R_{13}$ and $(x^i/\sim, x^j/\sim, t_2/\sim) \in R_{13}$ where $|t_1| = |u|$ and $|t_2| = |v|$ then $t_1 \le u$ iff $t_2 \le v$.

The semi-definability of R_{16} is clear from that of R_{15} and R_{12}. ∎

Let us assign to any finite non-empty sequence $u_1, \dots, u_n$ of words a pattern $H(u_1,\dots,u_n)$ in the following way:

$$H(u_1,\dots,u_n)=(xu_1xu_2\dots xu_n)/\sim$$

where x is a letter not contained in $\mathrm{supp}(u_1\dots u_n)$. Notice that this definition does not depend on the choice of the letter x. The sequence $u_1,\dots,u_n$ is recognizable from $H(u_1,\dots,u_n)$ up to similarity; two sequences $u_1,\dots,u_n$ and $v_1,\dots,v_m$ are said to be similar if $n=m$ and there exists an automorphism h of W such that $v_1=h(u_1),\dots,v_n=h(u_n)$.

Proposition 2.6. *The following relations are semi-definable in $\mathcal{P}$:*

$R_{17}(\alpha)$: *$\alpha=H(u_1,\dots,u_n)$ for a finite non-empty sequence $u_1,\dots,u_n$ of words;*

$R_{18}(\alpha,\beta)$: *$\alpha=H(u_1,\dots,u_n)$ for a finite non-empty sequence of words $u_1,\dots,u_n$ and $\beta=u_i/\sim$ for some $i\in\{1,\dots,n\}$;*

$R_{19}(\alpha,\beta)$: *$\alpha=H(u_1,\dots,u_n)$ for a finite sequence $u_1,\dots,u_n$ of words with $n\geq 2$ and $\beta=H(u_i,u_{i+1})$ for some $i\in\{1,\dots,n-1\}$;*

$R_{20}(\alpha,\beta)$: *$\alpha=H(u_1,u_2)$ for a pair u_1,u_2 of words and $\beta=x^i/\sim$ for some positive integer $i\leq\min(|u_1|,|u_2|)$ such that the initial part of u_1 of length i is equal to the initial part of u_2 of length i;*

$R_{21}(\alpha,\beta)$: *$\alpha=u/\sim$ and $\beta=x^n/\sim$ for some word u and a letter x, where n is the number of occurrences of the first letter in u;*

$R_{22}(\alpha,\beta,\gamma)$: *$\alpha=H(u_1,\dots,u_n)$ for a finite non-empty sequence $u_1,\dots,u_n$ of words, $\beta=x^i/\sim$ for some $i\in\{1,\dots,n\}$ and $\gamma=u_i/\sim$;*

$R_{23}(\alpha,\beta)$: *$\alpha=H(u_1,u_2,u_3)$ for a triple u_1,u_2,u_3 of words and $\beta=x^i/\sim$ for a letter x and a number $i\in\{1,\dots,|u_1|\}$ such that $u_2=\sigma^y_{u_3}(u_1)$ where y is the letter occuring at the ith place in u_1;*

$R_{24}(\alpha,\beta)$: *$\alpha=u/\sim$ and $\beta=f(u)/\sim$ for some word u and substitution f;*

$R_{25}(\alpha)$: *$\alpha=H(u_1,u_2,u_3,u_4)$ for some quadruple u_1,u_2,u_3,u_4 such that the equation (u_3,u_4) is an immediate consequence of the equation (u_1,u_2);*

$R_{26}(\alpha)$: *$\alpha=H(u_1,\dots,u_n)$ for some finite sequence $u_1,\dots,u_n$ such that $n\geq 4$ is even and the equation (u_{n-1},u_n) is a consequence of the equations $(u_1,u_2),\dots,(u_{n-3},u_{n-2})$.*

Proof. The semi-definability of the relations $R_{17},\dots,R_{20}$ and of many other relations formulated in similar ways should be clear from Proposition 2.5.

We have $(u/\sim,x^n/\sim)\in R_{21}$ iff there exists a pattern of the form $H(u_1,\dots,u_m)$ such that $u_1/\sim=u/\sim$, $u_m/\sim=x^n/\sim$ and whenever we take a pattern $H(u_i,u_{i+1})$ with $i\in\{1,\dots,m-1\}$ then $|u_{i+1}|=|u_i|-1$ and there exists a j $(1<j\leq|u_i|)$ such that the j-th letter in u_i is different from the first letter in u_i, the initial part of u_i of length $j-1$ is an initial part of u_{i+1} and the final part of u_i of length $|u_i|-j$ is a final part of u_{i+1}.

We have $(H(u_1,\dots,u_n),x^i/\sim,u/\sim)\in R_{22}$ iff there exists a pattern $v/\sim$ such that v is an initial part of some w with $H(u_1,\dots,u_n)=w/\sim$, either $v/\sim=H(u_1,\dots,u_n)$ or the $(|v|+1)$-th letter in w coincides with the first letter in w (so that now $v/\sim=H(u_1,\dots,u_m)$ for some $m\leq n$), i is just the number of occurrences of the first letter in v (so that now $m=i$) and $u/\sim=u_m/\sim$.

We have $(H(u_1, u_2, u_3), x^i/{\sim}) \in R_{23}$ iff there exists a pattern of the form $H(u_1, u_2, u_3, v_1, \ldots, v_m)$ such that $v_1 = u_1$, $v_m = u_2$, $i \leq |u_1|$, the i-th letter y in u_1 occurs neither in u_2 nor in u_3 and for every $j \in \{1, \ldots, m-1\}$ there exist words p, q such that the pair (v_j, v_{j+1}) belongs to the set $\{(pyq, pu_3q), (py, pu_3), (yq, u_3q), (y, u_3)\}$.

We have $(\alpha, \beta) \in R_{24}$ iff there exists a pattern of the form $H(u_1, \ldots, u_n)$ such that $u_1/{\sim} = \alpha$, $u_n/{\sim} = \beta$ and such that for every $i \in \{1, \ldots, n-1\}$ either u_{i+1} is a cover of u_i of type 3 or $(H(u_i, u_{i+1}, t), \gamma) \in R_{23}$ for some t and γ.

The semi-definability of the relations R_{25} and R_{26} is now clear. ■

Proposition 2.7. *Let R be an n-ary relation on $\mathcal{P}$ which can be defined syntactically in a reasonable way. Then R is semi-definable in $\mathcal{P}$.*

Proof. This should be clear from the previous propositions. It would be possible to formulate this result more precisely, of course, but we have chosen not to do so. ■

Proposition 2.8. *Every element of $\mathcal{P}$ is semi-definable in $\mathcal{P}$.*

Proof. This follows, for example, from the semi-definability of R_{14}. ■

Proposition 2.9. *The ordered set $\mathcal{P}$ has no other automorphisms than the duality and the identity.*

Proof. This is a consequence of 2.8. ■

3. Good sets of equations

We say that a set K of equations is **good** if there exists a first-order formula $f(X_1, X_2, X_3)$ with three free variables in the language of lattice theory such that for any triple T_1, T_2, T_3 of equational theories, $f(T_1, T_2, T_3)$ is true in $\mathcal{L}$ iff one of the following two cases takes place: either

$$T_1 = I_{xxy}, \quad T_2 = I_{H(a,b)} \text{ for some } (a,b) \in K, \quad T_3 = \mathrm{Eq}(a,b)$$

or

$$T_1 = I_{yxx}, \quad T_2 = I_{H(a,b)^\partial} \text{ for some } (a,b) \in K, \quad T_3 = \mathrm{Eq}(a,b)^\partial$$

We would like to see that the set of all equations is good. In the present paper we shall not be able to show this. We shall, however, find several large good sets.

Proposition 3.1. *Let K be a good set of equations. Then:*

(1) *The set $\{\mathrm{Eq}(a,b) : (a,b) \in K \cup K^\partial\}$ is definable in $\mathcal{L}$.*
(2) *For every $(a,b) \in K$, the one-based equational theory $\mathrm{Eq}(a,b)$ is an element definable up to duality in $\mathcal{L}$.*
(3) *If α is an automorphism of $\mathcal{L}$ then either $\alpha(T) = T$ for all equational theories T generated by a subset of T or $\alpha(T) = T^\partial$ for all equational theories T generated by a subset of T.*

Proof. This should be obvious. ■

Clearly, the union of a finite collection of good sets is good. Also, if K is good then both K^∂ and $K \cup K^\partial$ are good. Further, if K is good and K_1 is a subset of K that is syntactically definable in a reasonable way (see Proposition 2.7) then K_1 is good.

If K_1 is a set of equations which has already been found to be good, there are several possible ways to use this fact in proving that another set K_2, larger than K_1, is good too. For example, this is the case when for every $(a,b) \in K_2$, $\mathrm{Eq}(a,b)$ is just the greatest (or perhaps the smallest, or the only) equational theory T satisfying some first-order expressible conditions such as the following: Whenever $(c,d) \in K_1$ then $(c,d) \in T$ iff (c,d) is a consequence of (a,b). The fact that K_2 is good follows then from the results of Section 2.

We conclude this section by introducing a notion of semi-definability in $\mathcal{L}$. Let R be a relation between words, equations, and equational theories—i.e., a subset of $W^m \times (W^2)^n \times \mathcal{L}^k$ for some non-negative integers m,n,k. We say that R is **semi-definable** if there exists a first-order formula $f(X,Y,Z_1,\dots,Z_k)$ with $k+2$ free variables such that for any $A,B,T_1,\dots,T_k \in \mathcal{L}^k$, $f(A,B,T_1,\dots,T_k)$ is true in $\mathcal{L}$ iff one of the following two cases takes place: either

$$A = I_{xxy} \text{ and } B = I_{H(\bar{a},\bar{b},\bar{c})}$$

$$\text{where } ((a_i),(b_j,c_j),(T_s)) \in R$$

or

$$A = I_{yxx} \text{ and } B = I_{H(\bar{a},\bar{b},\bar{c})^\partial}$$

$$\text{where } ((a_i),(b_j,c_j),({T_s}^\partial)) \in R\,.$$

We remark that a set K of equations is good iff the relation

$$T = \mathrm{Eq}(a,b) \quad \text{and} \quad (a,b) \in K$$

between equations (a,b) and equational theories T is semi-definable. When K is good, the set of all theories $\mathrm{Eq}(a,b)$ with $(a,b) \in K$ is semi-definable—a semi-definable relation of one argument. For a semi-definable set $\mathcal{S}$ of theories, the set $\mathcal{S} \cup \mathcal{S}^\partial$ is a definable subset of $\mathcal{L}$.

In the next several sections, a number of semi-definable relations are implicitly involved in most arguments and we treat them very informally. In Section 12, where the semi-definable relations we need are rather complicated to define, we shall deal with them more formally and explicitly.

4. Parallel equations

An equation (a,b) is said to be **parallel** if it is regular ($\mathrm{supp}(a) = \mathrm{supp}(b)$) and the words a,b are incomparable ($a \not\leq b$ and $b \not\leq a$).

We start by showing that the set of parallel equations is good in a weaker sense. This result will then be applied to find several good sets, after which we will be able to show that the set of parallel equations is good.

Lemma 4.1. *Let (a,b) be a parallel equation. Denote by A the least ideal theory containing (a,b). Let T be an equational theory. Then $T = \mathrm{Eq}(a,p(b))$ for some permutation p of* $\mathrm{supp}(a)$ *iff the following three conditions are satisfied:*

(1) *$T \subseteq E \cap A$;*

(2) *A is just the least ideal theory containing T;*

(3) *whenever B is a proper subtheory of T then there exists an ideal theory D containing B such that $I_a \not\subseteq D$ and $I_b \not\subseteq D$.*

Proof. First assume that $T = \mathrm{Eq}(a,p(b))$. (1) and (2) are evident. Let B be a proper subtheory of T. Evidently, the set $\{a,p(b)\}$ is a block of T. Hence if $(a,u) \in B$ for some word u then $u = a$; if $(p(b),u) \in B$ for some u then $u = p(b)$. Denote by U the set of words u such that $v \leq u$ for some $(v,w) \in B$ with $v \neq w$. Evidently U is a full set, I_U is an ideal theory, I_U contains B, $I_a \not\subseteq I_U$ and $I_b \not\subseteq I_U$.

Conversely, let T satisfy (1),(2),(3). Denote by U the set of the words u such that $v \leq u$ for some $(v,w) \in T$ with $v \neq w$. Evidently, U is a full set and I_U is just the least ideal theory containing T. By (2), $I_U = A$. Hence $a \in U$; it follows from (1) that there is a word $c \neq a$ with $(a,c) \in T$. Put $B = \mathrm{Eq}(a,c)$. We have $B \subseteq T$ and by (3) we cannot have $B \subset T$. Hence $B = T$. By (2), A is just the least ideal theory containing (a,c). Hence $c \sim b$. Since $T \subseteq E$, we have $c = p(b)$ for some permutation p of $\mathrm{supp}(b) = \mathrm{supp}(a)$. ∎

A word $t = x_1x_2\dots x_{n-1}x_n$ (where $x_i \in X$) is said to be **1-smooth** if $n \geq 2$ and each of the three letters x_1, x_{n-1}, x_n has at least two occurrences in t.

An equation (a,b) is called **1-smooth** if it is regular and the words a,b are both 1-smooth.

Lemma 4.2. *Let (a,b) be a 1-smooth equation. Then* $\mathrm{Eq}(a,b)$ *is just the greatest element T of $\mathcal{L}$ with the following properties:*

(1) *$T \subseteq E$;*

(2) *whenever (u,v) is a parallel equation such that $(u,p(v)) \in T$ for some permutation p of* $\mathrm{supp}(u)$ *then $(u,q(v))$ is a consequence of (a,b) for some permutation q of* $\mathrm{supp}(u)$.

The set of 1-smooth equations is good.

Proof. It is evident that the equational theory $\mathrm{Eq}(a,b)$ has both these properties (put $q = p$ in (2)). Now, let T be an equational theory satisfying (1) and (2) and let $(c,d) \in T$ where $c \neq d$; we need to show that $(c,d) \in \mathrm{Eq}(a,b)$.

Put $m = 3 + |(|c| - |d|)|$, $k = 1 + \mathrm{Card}(\mathrm{supp}(c))$, let

$$x, z_{11}, \dots, z_{1m}, \dots, z_{k1}, \dots, z_{km}$$

be pairwise distinct letters not belonging to $\mathrm{supp}(c)$, and let $\{y_1,\dots,y_k\} = \{x\} \cup \mathrm{supp}(c)$. Then put

$$e = z_{11}\dots z_{1m}y_1z_{21}\dots z_{2m}y_2\dots z_{k1}\dots z_{km}y_k$$

The equation $(xcz_{22}e, xdz_{22}e)$ belongs to T and it is easy to see (making use of the facts that m is large, that the y's have each at least two occurrences and that the z's have each, except for z_{22}, only one occurrence in both $xcz_{22}e$ and $xdz_{22}e$), that it is parallel. By (2) we have $(a,b) \vdash (xcz_{22}e, q(xdz_{22}e))$ for some permutation q of $\mathrm{supp}(xcz_{22}e)$. Consider an (a,b)-derivation $u_1, \dots, u_r$ of $(xcz_{22}e, q(xdz_{22}e))$. As a, b are both 1-smooth, it is easy to prove by induction on i that $u_i = xw_iz_{22}e$ for some word w_i with $\mathrm{supp}(w_i) = \mathrm{supp}(c)$, and if f is a substitution such that either $f(a)$ or $f(b)$ is a subword of $xw_iz_{22}e$ then it is a subword of w_i. From this it follows that $z_{22}e$ is a final part of $q(xdz_{22}e)$, so that q is the identical permutation. Further, it follows that $w_1, \dots, w_r$ is an (a,b)-derivation of (c,d), so that $(c,d) \in \mathrm{Eq}(a,b)$.

The goodness of the set of 1-smooth equations follows by 4.1. ∎

An equation (a,b) is called **2-smooth** if it is parallel and

$$\mathrm{Card}(\mathrm{supp}(a)) = \mathrm{Card}(\mathrm{supp}(b)) = 2\,.$$

Recall from the preliminaries that E_ℓ is the equational theory defined as follows: $(a,b) \in E_\ell$ iff the first letter in a and the first letter in b coincide. Evidently, E_ℓ is the equational theory generated by the equation (x, xy) (where x, y are two distinct letters).

Lemma 4.3. *The set $\{(x,xy) : x, y \in X, x \neq y\}$ is good. Equivalently, the theory E_ℓ is semi-definable.*

Proof. The co-atoms of $\mathcal{L}$ are the theories C, E, E_ℓ, E_r and each theory of a multiplication group of prime order. According to Theorem 1.11, E and C are definable. Now E_ℓ is the only co-atom of $\mathcal{L}$ different from E and C which contains the 1-smooth equation $(xxyy, xxyyx)$. ∎

Lemma 4.4. *Let (a,b) be a 2-smooth equation. Then $\mathrm{Eq}(a,b)$ is the only equational theory T with the following two properties:*

(1) $T = \mathrm{Eq}(a, p(b))$ *for some permutation p of* $\mathrm{supp}(a)$*;*
(2) $T \subseteq E_\ell$ *iff* $(x,xy) \vdash (a,b)$.

The set of 2-smooth equations is good.

Proof. The first assertion follows from the fact that there is exactly one permutation p of $\mathrm{supp}(a)$ which is not the identity, and exactly one of the words $b, p(b)$ has the property that its first letter coincides with that in a. The goodness of the set of 2-smooth equations follows now from 2.7, 4.1 and 4.3. ∎

An equation (a,b) is called **3-smooth** if it is regular, $\mathrm{Card}(\mathrm{supp}(a)) = 2$ and $b = p(a)$ where p is the only transposition of $\mathrm{supp}(a)$.

Lemma 4.5. *Let (a,b) be a 3-smooth equation. Then* $\mathrm{Eq}(a,b)$ *is just the least element T of $\mathcal{L}$ with the following properties:*

(1) *I_a is the least ideal theory containing T;*
(2) *T is contained in the largest modular element $M(a)$ of $\mathcal{L}$ which is a proper subtheory of I_a not included in E.*

The set of 3-smooth equations is good.

Proof. This should be obvious. See Proposition 1.6 for the characterization of $M(a)$. ∎

An equation (a,b) is called **4-smooth** if it is regular, $\mathrm{Card}(\mathrm{supp}(a)) \geq 2$, and $b = p(a)$ for some transposition p of $\mathrm{supp}(a)$.

Lemma 4.6. *Let (a,b) be a 4-smooth equation. Then $\mathrm{Eq}(a,b)$ is just the least element T of $\mathcal{L}$ with the following properties:*

(1) *I_a is the least ideal theory containing T;*
(2) *T is contained in $M(a)$;*
(3) *whenever (c,d) is either 2-smooth or 3-smooth then $(c,d) \in T$ iff (c,d) is a consequence of (a,b).*

The set of 4-smooth equations is good.

Proof. Evidently, the equational theory $\mathrm{Eq}(a,b)$ has all these properties. Now let T be an equational theory satisfying (1),(2),(3). We need to show that $(a,b) \in T$. It follows from (1) and (2) that $(a,q(a)) \in T$ for some nontrivial permutation q of $\mathrm{supp}(a)$. We have $b = p(a)$ for some transposition p of $\mathrm{supp}(a)$. Denote by x,y the two distinct letters from $\mathrm{supp}(a)$ such that $p(x) = y$, $p(y) = x$ and p is identical on $\mathrm{supp}(a) \setminus \{x,y\}$.

Let f be a substitution mapping X into X. Taking (a,b)-derivations into account, it is easy to see that the set $\{f(a), fp(a)\}$ is a block of $\mathrm{Eq}(a,b)$.

Suppose that there exists a letter $z \in \mathrm{supp}(a) \setminus \{x,y\}$ such that $q(z) \neq z$. Define a substitution f as follows: $f(x) = x$; $f(y) = y$; if $q(z) \neq x$ then $f(z) = x$ and $f(u) = y$ for any letter $u \notin \{x,y,z\}$; if $q(z) = x$ then $f(z) = y$ and $f(u) = x$ for any letter $u \notin \{x,y,z\}$. We have $(f(a), fq(a)) \in T$. This equation is evidently either 2-smooth or 3-smooth and so by (3) we get $(f(a), fq(a)) \in \mathrm{Eq}(a,b)$. Since $f(z) \neq fq(z)$, we have $f(a) \neq fq(a)$ and so, by the above observation, $fq(a) = fp(a)$. But then $fq(z) = fp(z)$, so that $fq(z) = f(z)$, a contradiction.

Hence $q(z) = z$ for all the letters $z \in \mathrm{supp}(a) \setminus \{x,y\}$. Since q is a non-trivial permutation, we get $p = q$. But then $(a, p(a)) \in T$, which means that $(a,b) \in T$. ■

An equation (a,b) is called **5-smooth** if it is parallel and $\mathrm{Card}(\mathrm{supp}(a)) = \mathrm{Card}(\mathrm{supp}(b)) \geq 3$.

Lemma 4.7. *Let (a,b) be a 5-smooth equation. Let $T \in \mathcal{L}$. Then $T = \mathrm{Eq}(a,b)$ iff the following two conditions are satisfied:*

(1) *$T = \mathrm{Eq}(a, p(b))$ for some permutation p of $\mathrm{supp}(a)$;*
(2) *for every transposition q of $\mathrm{supp}(a)$, the 4-smooth equation $(b, q(b))$ belongs to $T \vee \mathrm{Eq}(a, q(a))$.*

The set of 5-smooth equations is good.

Proof. Evidently, the equational theory $\mathrm{Eq}(a,b)$ has both these properties. Now let T be an equational theory satisfying (1) and (2). It is enough to prove that p is the identity on $\mathrm{supp}(a)$. Suppose, on the contrary, that there exist two distinct letters $x, y \in \mathrm{supp}(a)$ with $p(x) = y$. Let us take a letter $z \in \mathrm{supp}(a) \setminus \{x,y\}$ and denote by q the transposition of $\mathrm{supp}(a)$ such that $q(x) = z$ and $q(z) = x$. Put $U = T \vee \mathrm{Eq}(a, q(a))$. By (2) we have $(b, q(b)) \in U$ and so $(p(b), pq(b)) \in U$. However, it is easy to see that the set $\{a, q(a), p(b), qp(b)\}$ is a block of U; from this we get $pq(b) = qp(b)$, so that $pq = qp$. But then $y = qpq(z) = p(z) \neq y$, a contradiction. ■

Proposition 4.8. *The set of parallel equations is good.*

Proof. It follows from 4.4 and 4.7. ∎

5. Semi-perfect equations

By a **left-perfect word** we mean a word $t = x_1 \dots x_n$ (where x_i are letters) such that x_1 has at least two occurrences in t. If x_n has at least two occurrences in t then t is said to be **right-perfect**. A word is **perfect** if it is both left- and right-perfect, and **unperfect** if it is neither left- nor right-perfect.

By a **left-perfect equation** we mean an equation (a, b) such that $\mathrm{supp}(a) = \mathrm{supp}(b)$ and the words a, b are both left-perfect. **Right-perfect** and **perfect equations** are defined analogously. By a **semi-perfect equation** we mean an equation (a, b) such that $\mathrm{supp}(a) = \mathrm{supp}(b)$ and neither of the words a, b is unperfect.

The aim of this section is to prove that the set of semi-perfect equations is good. In order to do this, we shall have to start with establishing the goodness of several smaller sets; for example, the set of perfect equations will be among them.

Let us call a word $t = x_1 \dots x_n$ **strongly perfect** if $x_1 = x_n$ and x_1 has exactly two occurrences in t. Further, we say that t is **strictly left-perfect** if $x_1 = x_2$ and x_1 has exactly two occurrences in t. And t is **strictly right-perfect** if $x_n = x_{n-1}$ and x_n has exactly two occurrences in t.

An equation (a, b) is called **directly special** if there exist three distinct letters x, y, z such that

$$a = xyzx \quad \text{and} \quad b \in \{x^n yzz, x^n zyy, y^n xzz, y^n zxx, z^n xyy, z^n yxx\}$$

for some $n \geq 2$; it is called **inversely special** if (b, a) is directly special; and it is called special if it is either directly or inversely special.

Lemma 5.1. *Let (a, b) be a perfect but not special equation. Then $\mathrm{Eq}(a, b)$ is just the greatest equational theory T with the following properties:*

(1) *$T \subseteq E$;*

(2) *whenever (u, v) is a 1-smooth equation then $(u, v) \in T$ iff (u, v) is a consequence of (a, b).*

Proof. Let T have these two properties; we must show that $T \subseteq \mathrm{Eq}(a, b)$. Suppose, on the contrary, that there exists an equation $(c, d) \in T$ not belonging to $\mathrm{Eq}(a, b)$. Let us take five distinct letters x, y, z, u, v not belonging to $\mathrm{supp}(c) = \mathrm{supp}(d)$.

We have $(yxcxy, yxdxy) \in T$. This equation is 1-smooth and so, by (2), belongs to $\mathrm{Eq}(a, b)$. Hence there exists an (a, b)-derivation $t_0, \dots, t_k$ of this equation. If neither a nor b is strongly perfect then it is easy to prove by induction on i that $t_i = yxwxy$ for some word w and $(c, w) \in \mathrm{Eq}(a, b)$; thus

$t_0, \dots, t_k$ is "essentially" an (a,b)-derivation of (c,d). We conclude that either a or b is strongly perfect.

It is enough to consider the case when a is strongly perfect.

We have $(xxcyy, xxdyy) \in T$. Similarly as above, this equation also belongs to $\mathrm{Eq}(a,b)$ and its (a,b)-derivation is essentially an (a,b)-derivation of (c,d), unless b is either strictly left-perfect or strictly right-perfect.

Taking similarly the equation $(xyxczz, xyxdzz)$ into account we conclude that either $a \leq xyx$ or b is strictly right-perfect.

Let $a \leq xyx$. Then $a \sim xyx$ and we can assume that $a = xyx$. We have $b \in \{xxy^n, yyx^n, x^n yy, y^n xx\}$ for some $n \geq 2$. A contradiction can be obtained if we consider the 1-smooth equation $(xxyczuu, xxydzuu)$.

We conclude that $a \not\leq xyx$ and b is right-perfect.

Taking the two equations

$$(xyxczuvzv, xyxdzuvzv) \qquad \text{and} \qquad (xxczuvzv, xxdzuvzv)$$

into consideration we see that a is similar to $zuvz$.

We can assume that $a = xyzx$. Considering the equations

$$(xyxczuu, xyxdzuu) \qquad \text{and} \qquad (xxczuu, xxdzuu)$$

we see that the third to the last letter in b has a single occurrence in b. Hence b is one of the six words

$$x^n yzz, x^n zyy, y^n xzz, y^n zxx, z^n xyy, z^n yxx$$

for some $n \geq 2$.

We have proved that the equation (a,b) is special. However, this is a contradiction. ■

Lemma 5.2. *The set of perfect equations is good.*

Proof. It follows from 5.1 that the set K of non-special perfect equations is good. The set P of perfect equations is the union of K, of the dual of K and of the set of perfect parallel equations; so, we can use Proposition 4.8 to obtain the result. ■

A word $t = x_1 \dots x_k$ is said to be **doubly left-perfect** if $k \geq 2$ and if each of the letters x_1 and x_2 has at least two occurrences in t. An equation (a,b) is called doubly left-perfect if $\mathrm{supp}(a) = \mathrm{supp}(b)$ and a, b are both doubly left-perfect.

Lemma 5.3. *Let (a,b) be a doubly left-perfect equation. Then* $\mathrm{Eq}(a,b)$ *is just the greatest equational theory T with the following properties:*

(1) *$T \subseteq E$;*
(2) *whenever (u,v) is a perfect equation then $(u,v) \in T$ iff (u,v) is a consequence of (a,b).*

Proof. Let T have the two properties and let $(c,d) \in T$; we must prove $(c,d) \in \mathrm{Eq}(a,b)$. Denote by w_1 the last letter in c and by w_2 the last letter in

d. Let x, y, z, u, v be five distinct letters not contained in $\mathrm{supp}(c) = \mathrm{supp}(d)$. If $w_1 \neq w_2$, consider the equation

$$(xyxzw_1uw_2vc, xyxzw_1uw_2vd)$$

If $w_1 = w_2$, consider the equation

$$(xyxzw_1uc, xyxzw_1ud)$$

This equation belongs (in both cases) to T and is perfect, so that it is a consequence of (a, b). Analysing an (a, b)-derivation of this equation and taking into account the fact that (a, b) is doubly left-perfect we see that the derivation is essentially an (a, b)-derivation of (c, d). Hence $(c, d) \in \mathrm{Eq}(a, b)$. ∎

A word $t = x_1 \dots x_k$ is said to be **1-strangely left-perfect** if $k \geq 4$, $x_1 = x_3$, the letter x_1 has exactly two occurrences and each of the letters x_2 and x_4 has exactly one occurrence in t.

A word $t = x_1 \dots x_k$ is said to be **2-strangely left-perfect** if $k \geq 5$, $x_1 = x_4$, x_1 has exactly two and each of the letters x_2, x_3, x_5 has exactly one occurrence in t.

A word $t = x_1 \dots x_k$ is said to be **superstrictly left-perfect** if $k \geq 3$, $x_1 = x_2$, x_1 has exactly two and x_3 has exactly one occurrence in t.

An equation (a, b) is said to be **1-strangely** (or **2-strangely**, resp.) **left-perfect** if $\mathrm{supp}(a) = \mathrm{supp}(b)$, a is 1-strangely (or 2-strangely, resp.) left-perfect and b is superstrictly left-perfect.

An equation (a, b) is said to be **6-smooth** if it is left-perfect but neither (a, b) nor (b, a) is either 1-strangely or 2-strangely left-perfect.

Lemma 5.4. *Let (a, b) be a 6-smooth equation which is neither parallel nor perfect. Then $\mathrm{Eq}(a, b)$ is just the greatest equational theory T with the following properties:*

(1) *$T \subseteq E$;*

(2) *whenever (u, v) is a doubly left-perfect equation then $(u, v) \in T$ iff (u, v) is a consequence of (a, b).*

Proof. Let T have the two properties. Let $(c, d) \in T$ and suppose that $(c, d) \notin \mathrm{Eq}(a, b)$. Let x, y, z, u be four distinct letters not belonging to $\mathrm{supp}(c) = \mathrm{supp}(d)$. The equation $(xxyc, xxyd)$ belongs to T and is doubly left-perfect, so that it is a consequence of (a, b). Analysing an (a, b)-derivation of this equation we see that either a or b is superstrictly left-perfect; it is enough to consider the case when b is. Since (a, b) is 6-smooth, the word a is neither 1- nor 2-strangely left-perfect. The equation $(xyxzyuc, xyxzyud)$ belongs to T and is doubly left-perfect, so that it is a consequence of (a, b). Analysing an (a, b)-derivation of this equation we see that one of the following six cases takes place for the word $a = x_1 \dots x_k$:

(C1) $k \geq 4$, $x_1 = x_3$, x_1 has exactly two occurrences and each of x_2, x_4 has exactly one occurrence in a;

(C2) $k \geq 6$, $x_1 = x_3$, $x_2 = x_5$, each of x_1, x_2 has exactly two occurrences and each of x_4, x_6 exactly one;

(C3) $k = 3$, $x_1 = x_3$, $x_1 \neq x_2$;

(C4) $k = 5$, $x_1 = x_3$, $x_2 = x_5$, $x_1 \neq x_2$, $x_1 \neq x_4$, $x_2 \neq x_4$;

(C5) $k \geq 5$, $x_1 = x_4$, x_1 has exactly two occurrences and each of x_2, x_3, x_5 exactly one;

(C6) $k = 4$, $x_1 = x_4$, $x_1 \neq x_2$, $x_1 \neq x_3$, $x_2 \neq x_3$.

The equation $(xyzyxc, xyzyxd)$ also belongs to $\mathrm{Eq}(a,b)$ and we analogously see that the cases (C2) and (C4) are impossible.

Suppose that (C3) takes place. Then $b \in \{x_1x_1x_2, x_2x_2x_1\}$ and (a,b) is parallel, a contradiction.

Suppose that (C6) takes place. Then

$$b \in \{x_1x_1x_2x_3^n, x_1x_1x_3x_2^n, x_2x_2x_1x_3^n, x_2x_2x_3x_1^n, x_3x_3x_1x_2^n, x_3x_3x_2x_1^n\}$$

for some $n \geq 1$. If $n \geq 2$ then (a,b) is perfect, a contradiction. If $n = 1$ then (a,b) is parallel, a contradiction.

Hence only the cases (C1) and (C5) remain possible. But then a is either 1- or 2-strangely left-perfect, a contradiction. ∎

An equation (a,b) is said to be **7-smooth** if it is left-perfect but neither (a,b) nor (b,a) is 1-strangely left-perfect.

Lemma 5.5. *Let (a,b) be a 7-smooth equation which is not 6-smooth. Then $\mathrm{Eq}(a,b)$ is just the greatest equational theory T with the following properties:*

(1) *$T \subseteq E$;*

(2) *whenever (u,v) is a 6-smooth equation then $(u,v) \in T$ iff (u,v) is a consequence of T.*

Proof. Let T have these two properties and let $(c,d) \in T$. Take two distinct letters x, y not belonging to $\mathrm{supp}(c) = \mathrm{supp}(d)$. The equation $(xyxc, xyxd)$ belongs to T and is 6-smooth, so that it is a consequence of (a,b). Now, either (a,b) or (b,a) is 2-strangely left-perfect. Analysing an (a,b)-derivation of $(xyxc, xyxd)$ we see that $(c,d) \in \mathrm{Eq}(a,b)$. ∎

Lemma 5.6. *Let (a,b) be a 1-strangely left-perfect equation such that $a < b$. Then $\mathrm{Eq}(a,b)$ is just the least equational theory T with the following property: whenever (u,v) is a 7-smooth equation then $(u,v) \in T$ iff (u,v) is a consequence of (a,b).*

Proof. We can write $a = xyxza_0$ and $b = uuvb_1\varphi(a)b_2$ where a_0, b_1, b_2 are three possibly empty words, φ is a substitution, x, y, z are three distinct letters not occurring in a_0 and u, v are two distinct letters not occurring in $b_1\varphi(a)b_2$. Put $U = \{t : (a,t) \in \mathrm{Eq}(a,b)\}$; denote by U_a the set of 1-strangely and by U_b the set of superstrictly left-perfect words from U. The two sets U_a and U_b are disjoint; we have $a \in U_a$ and $b \in U_b$.

Observation 1: For every $n \geq 1$ there exist a substitution ψ, a word c_1 and a possibly empty word c_2 such that $(a, uuvc_1\psi(a)c_2) \in \mathrm{Eq}(a,b)$ and c_1 is of length $\geq n$.

Proof: Clearly, for every $k \geq 1$ we have

$$(a, uuvb_1\varphi(uuvb_1)\dots\varphi^{k-1}(uuvb_1)\varphi^k(a)\varphi^{k-1}(b_2)\dots\varphi(b_2)b_2) \in \mathrm{Eq}(a,b)$$

Thus we can put $\psi = \varphi^k$ and take k so large that the word

$$b_1\varphi(uuvb_1)\dots\varphi^{k-1}(uuvb_1)$$

is of length $\geq n$.

Observation 2: $U \neq U_a \cup U_b$.

Proof: Suppose $U = U_a \cup U_b$. It follows almost immediately from Observation 1 that there exist words d_1, d_2 (the last one possibly empty) and a substitution α such that $(a, uuvd_1\alpha(xyxz)\alpha(a_0)d_2) \in \mathrm{Eq}(a,b)$ and such that the word $d_1\alpha(xyxz)$ is very long; so long that it can be written as

$$d_1\alpha(xyxz) = pqrqs$$

with p,q,r,s nonempty and q,r both of length ≥ 2. Define a substitution β in this way: $\beta(x) = q$, $\beta(y) = r$, $\beta(z) = s$ and $\beta(w) = \alpha(w)$ for any letter $x \notin \{x,y,z\}$. We get

$$(a, uuvp\beta(a)d_2) \in \mathrm{Eq}(a,b)$$

where both $\beta(x)$ and $\beta(y)$ are of length ≥ 2. Then we get

$$(a, uuvp\beta(uuvp)\beta^2(a)\beta(d_2)d_2) \in \mathrm{Eq}(a,b)$$

Define a substitution γ in this way: $\gamma(u) = u$, $\gamma(v) = vp\beta(uuv)$ and $\gamma(w) = \beta(w)$ for any letter $w \notin \{u,v\}$. Then we get

$$\gamma(uuvp\beta(a)d_2) = uuvp\beta(uuv)\beta(p)\beta^2(a)\beta(d_2)$$

and so

$$(a, \gamma(uuvp\beta(a)d_2)d_2) \in \mathrm{Eq}(a,b)$$

But then $(a, \gamma(a)d_2) \in \mathrm{Eq}(a,b)$. We have proved $\gamma(a)d_2 \in U$. Since evidently $\gamma(a)d_2 \notin U_b$, we get $\gamma(a)d_2 \in U_a$. But then both $\gamma(x)$ and $\gamma(y)$ are letters. Since $\gamma(v)$ is a long word, we get $x \neq v$ and $y \neq v$. If $x \neq u$ then $\gamma(x) = \beta(x)$, a contradiction, since $\beta(x)$ is of length ≥ 2. This proves $x = u$. Now, $y \notin \{u,v\}$. Hence $\gamma(y) = \beta(y)$, a contradiction, since $\beta(y)$ is of length ≥ 2.

Now with the proof of Observation 2 finished, we can conclude the proof of 5.6. Let T be an equational theory satisfying the above formulated condition; we need to show that $(a,b) \in T$. It follows from Observation 2 that there exists a word $c \in U$ belonging to neither U_a nor U_b. Taking an (a,b)-derivation of (a,c) into consideration we can easily show that c is left-perfect. Hence both (a,c) and (b,c) are 7-smooth. They, of course, belong to $\mathrm{Eq}(a,b)$. Consequently, they belong to T. But then $(a,b) \in T$. ∎

Lemma 5.7. *Let (a,b) be a 1-strange left-perfect equation such that $b < a$. Then $\mathrm{Eq}(a,b)$ is just the least equational theory T with the following property: whenever (u,v) is either a 7-smooth equation or a parallel equation or a 1-strange left-perfect equation such that $u < v$ then $(u,v) \in T$ iff (u,v) is a consequence of (a,b).*

Proof. Similarly as in the proof of 5.6 we can write $a = xyxza_1\varphi(b)a_2$ and $b = uuvb_0$ and there exists an arbitrarily long word c_1 such that for some c_2 and some substitution ψ we have

$$(a, xyxzc_1\psi(b)c_2) \in \mathrm{Eq}(a,b)$$

Take c_1 to be longer than a. Since $(\psi(b),\psi(a)) \in \mathrm{Eq}(a,b)$, we have

$$(a, xyxzc_1\psi(xyxz)\psi(a_1\varphi(b)a_2)c_2) \in \mathrm{Eq}(a,b)$$

Define a substitution α by $\alpha(x) = x$, $\alpha(y) = y$, $\alpha(z) = zc_1\psi(xyxz)$ and $\alpha(w) = \psi(w)$ for any letter $w \notin \{x,y,z\}$. Then

$$\alpha(a) = xyxzc_1\psi(xyxz)\psi(a_1\varphi(b)a_2),$$

which yields $(a,\alpha(a)c_2) \in \mathrm{Eq}(a,b)$ and so $(a,\alpha(b)c_2) \in \mathrm{Eq}(a,b)$. Here $\alpha(b)c_2$ is longer than a and this word cannot be 1-strangely left-perfect, since it begins with $\alpha(u)\alpha(u)$. The equation $(b,\alpha(b)c_2)$ belongs to $\mathrm{Eq}(a,b)$ and is evidently 7-smooth, so that it belongs to T. The equation $(a,\alpha(b)c_2)$ belongs to $\mathrm{Eq}(a,b)$ and is either 7-smooth or parallel or 1-strangely left-perfect with $a < \alpha(b)c_2$, so that it belongs to T too. Hence $(a,b) \in T$. ∎

Proposition 5.8. *The set of left-perfect equations is good.*

Proof. By 5.3, the set of doubly left-perfect equations is good. By 5.4, the set of 6-smooth equations is good (we can ignore the fact that parallel and perfect 6-smooth equations are not covered by 5.4, since they are covered by the previous results). Similarly, by 5.5, the set of 7-smooth equations is good. The only remaining equations now are the 1-strangely left-perfect ones. These are covered by 5.6 and 5.7 (the parallel ones again by Section 4). ∎

Recall that we deem an equation (a,b) semi-perfect if $\mathrm{supp}(a) = \mathrm{supp}(b)$ and each of a, b is left- or right-perfect.

Proposition 5.9. *The set of semi-perfect equations is good.*

Proof. We will show that for every semi-perfect equation (a,b), the theory $\mathrm{Eq}(a,b)$ is generated by all the left-perfect, the right-perfect, and the parallel consequences of (a,b). Since the sets of left-perfect, right-perfect, and parallel equations are good, this will suffice. Now indeed, every semi-perfect equation is either left-perfect or right-perfect or parallel or has the form (a,b) or (b,a) where a is left-perfect, b is right-perfect, and either $a < b$ or $b < a$. Thus clearly it suffices to consider a semi-perfect equation (a,b) that satisfies $a < b$, $a = xuxvy = ry$ and $b = zu'\sigma(a)v'$ where x,y,z are letters, u,v,r,u',v' are words (possibly empty), y occurs only once in a, z occurs only once in b, σ is some substitution, and b is right-perfect. ($\sigma(a)$ cannot be an initial subword of b since z has no repeat occurence in b.) Letting w be a new letter, we have that (wa,a') is derivable from (a,b) where a' is the result of replacing z everywhere in a by wz. Letting τ be the substitution which behaves like σ on the letters in (a,b) and maps w to zu', we derive $(\tau(wa),\tau(a'))$, i.e., $(zu'\sigma(a),\tau(a'))$. So the equation (b, c) is derivable where $c = \tau(a')v'$. Thus (a, b) is equivalent to the conjunction of the two equations (a, c) and (b, c).

Now c is obviously left-perfect, and can be seen to be right-perfect as well (by checking cases: v' non-empty, v' empty and $z \neq y$, and finally, v' empty and $z = y$). Thus $\mathrm{Eq}(a, b)$ is the least equational theory containing the left-perfect equation (a, c) and the right-perfect equation (b, c). ∎

6. Permutational equations

By a **permutational equation** we mean an equation $(a, p(a))$ where p is a permutation of $\mathrm{supp}(a)$. The aim of this section is to prove that the set of permutational equations is good.

By a **permutational theory** we mean an equational theory T for which there exists a word a and a group G of permutations of $\mathrm{supp}(a)$ such that T is generated by the equations $(a, p(a))$ with $p \in G$. If G is the group of all permutations of $\mathrm{supp}(a)$ then the theory T generated in this way will be denoted by $\mathrm{Perm}(a)$.

Henceforth, the largest ideal theory properly included in I_a will be denoted ${I_a}^\star$. By Proposition 1.12, the theory $M(a) = \mathrm{Perm}(a) \vee {I_a}^\star$ is the largest modular element of $\mathcal{L}$ that is a proper subtheory of I_a not included in E.

Lemma 6.1. *An equational theory T is permutational iff the following three conditions are satisfied for some word a:*

(1) *the least ideal theory containing T is I_a;*
(2) *T is contained in $M(a)$;*
(3) *whenever T' is an equational theory with similar properties (I_a coincides with the least ideal theory containing T' and $T' \subseteq M(a)$) such that $T \vee {I_a}^\star = T' \vee {I_a}^\star$ then $T \subseteq T'$.*

Proof. Easy, and left to the reader. ∎

Lemma 6.2. *The set of permutational equations in at most three letters is good.*

Proof. The set of transpositional, or 4-smooth, equations was shown to be good in Lemma 4.6. Each permutational equation in two or three letters that is neither 4-smooth, left-perfect, right-perfect, nor identical (of the form (a, a)) is equivalent to an equation $(a, p(a))$ where $a = xy^nz$ and $p(a) = yz^nx$ for some $n > 0$ and letters x, y, z. Here, $\mathrm{Eq}(a, p(a))$ is the only permutational theory T such that I_a is the least ideal theory containing T and T contains no 4-smooth equation $(a, q(a))$. ∎

The next lemma accomplishes our goal of proving that the set of permutational equations is good.

Lemma 6.3. *Let (a, b) be a permutational equation with $b \neq a$. Then* $\mathrm{Eq}(a, b)$ *is the greatest element T of $\mathcal{L}$ with the following properties:*

(1) *T is a permutational theory;*
(2) *I_a is the least ideal theory containing T;*
(3) *whenever (c, d) is either parallel or semi-perfect or a permutational equation in at most three letters then $(c, d) \in T$ iff (c, d) is a consequence of (a, b).*

The proof of this lemma occupies the rest of this section and is divided into several lemmas. It is clear that the equational theory $\mathrm{Eq}(a, b)$ has all the three properties. Now let T be an equational theory satisfying (1), (2) and (3) and let q be a permutation of $\mathrm{supp}(a)$ such that $(a, q(a)) \in T$. All we need to prove is that $(a, q(a))$ is a consequence of $(a, p(a))$, where p is a permutation such that $b = p(a)$. In other words, we need to prove that q is a power of p.

Lemma 6.4. *Let f be a substitution mapping* $\mathrm{supp}(a)$ *into itself. Let b be a word such that $(f(a), b)$ is a consequence of $(a, p(a))$. Then $b = fp^j(a)$ for some j.*

Proof. There exists a derivation $f(a) = u_0, \ldots, u_k = b$ of $(f(a), b)$ from $(a, p(a))$. We shall prove by induction on i that $u_i = fp^j(a)$ for some j. If $i = 0$, we can take $j = 0$. Now, suppose that we have already proved $u_i = fp^j(a)$ for some $i < k$ and some j. Since u_i is of the same length as a, there exists a substitution g mapping letters into letters such that either $u_i = g(a)$ and $u_{i+1} = gp(a)$ or else $u_i = gp(a)$ and $u_{i+1} = g(a)$. In the first case $fp^j(a) = g(a)$ gives $fp^j = g$ on $\mathrm{supp}(a)$, so that $u_{i+1} = fp^{j+1}(a)$. In the second case, similarly, $u_{i+1} = fp^{j-1}(a)$. ∎

Lemma 6.5. *Let $x \in \mathrm{supp}(a)$. Then $q(x) = p^i(x)$ for some i.*

Proof. Take $y \in \mathrm{supp}(a) \setminus \{x\}$ and define a substitution f in such a way that $f(z) = x$ if $z = p^i(x)$ for some i and $f(z) = y$ for all other letters z. Since $(f(a), fq(a))$ is a parallel equation or a permutational equation in two letters, the fact that this equation belongs to T implies that the equation is a consequence of $(a, p(a))$. By Lemma 6.4, $fq(a) = fp^j(a)$ for some j. Then fq coincides with fp^j on $\mathrm{supp}(a)$ and thus $fq(x) = fp^j(x) = x$, so that $q(x) = p^i(x)$ for some i by the definition of f. ∎

Lemma 6.6. *Let $x, y \in \mathrm{supp}(a)$. Then there is an i with $q(x) = p^i(x)$ and $q(y) = p^i(y)$.*

Proof. By Lemma 6.5 there exist i, j with $q(x) = p^i(x)$ and $q(y) = p^j(y)$. Take a letter x' different from both $p^i(x)$ and $p^j(y)$ and define a substitution f in such a way that $f(z) = z$ if $z \in \{p^i(x), p^j(y)\}$ and $f(z) = x'$ for all the remaining letters z. Then $(f(a), fq(a))$ is an equation belonging to T; this equation is either parallel or it is a permutational equation in at most three letters, so it is a consequence of $(a, p(a))$. By Lemma 6.4, $fq(a) = fp^k(a)$ for some k. Then $fq(x) = fp^k(x)$ and $fq(y) = fp^k(y)$, i.e., $p^i(x) = fp^k(x)$ and $p^j(y) = fp^k(y)$. By the definition of f it follows that $p^k(x) = p^i(x)$ and $p^k(y) = p^j(y)$. So, $q(x) = p^k(x)$ and $q(y) = p^k(y)$. ∎

Lemma 6.7. *Let p, q be two permutations of a finite set S such that for any $x, y \in S$ there exists an i with $q(x) = p^i(x)$ and $q(y) = p^i(y)$. Then q is a power of p.*

Proof. It is clear that each orbit of p is a union of orbits of q. Considering for a moment, the action of q on one orbit of p it becomes clear that for some i, $q = p^i$ on that orbit. Let $C_1, \dots, C_k$ be the distinct orbits of p and put $n_j = |C_j|$. Thus n_j is the order of the permutation $p|_{C_j}$. Let $q = p^{m_j}$ on C_j for each $j \in \{1, \dots, k\}$. For $j, j' \in \{1, \dots, k\}$ choose $a_j \in C_j$ and $a_{j'} \in C_{j'}$, and then choose an integer r so that $q(a_j) = p^r(a_j)$ and $q(a_{j'}) = p^r(a_{j'})$. Now $p^r(a_j) = p^{m_j}(a_j)$ implies that $r \equiv m_j \pmod{n_j}$. Thus we have that $m_j \equiv r \pmod{n_j}$ and $m_{j'} \equiv r \pmod{n_{j'}}$. Hence the greatest common divisor of $\{n_j, n_{j'}\}$ divides $m_j - m_{j'}$. Now by the Chinese Remainder Theorem, there exists an integer m such that $m \equiv m_j \pmod{n_j}$ for all $j \in \{1, \dots, k\}$. Then $q = p^m$ on each and every orbit of p. ∎

Now, Lemma 6.3 is an easy consequence of Lemmas 6.4, 6.5, 6.6 and 6.7.

Corollary 6.8. *The relation $\{(a, \mathrm{Perm}(a)) : a \in W\}$ is semi-definable, as is the relation $\{(a, M(a)) : a \in W\}$.*

Proof. If $|\mathrm{supp}(a)| > 1$ then $\mathrm{Perm}(a)$ is the largest permutational theory T such that I_a is the least ideal theory containing T. If $|\mathrm{supp}(a)| = 1$ then $\mathrm{Perm}(a) = 0_W$. The second assertion follows from Proposition 1.12. ∎

7. Absorption equations

By a **power equation** we mean an equation of the form (b, b^m) where b is any word and $m > 1$.

Proposition 7.1. *The set of power equations is good.*

Proof. Consider a power equation (b, b^m), where $m > 1$. We claim that $\mathrm{Eq}(b, b^m)$ is the least regular equational theory T such that T is included in $E_\ell \cap E_r \cap I_b$; is not included in $M(b)$; and has the property that the semi-perfect equations contained in T are exactly those derived from (b, b^m).

To prove this, let T satisfy the stated conditions. Then T contains (b, c) for some $c > b$. Thus $(bb^{m-1}, cb^{m-1}) \in T$ and is perfect. So this equation is derivable from (b, b^m); i.e., (b, cb^{m-1}) belongs to $\mathrm{Eq}(b, b^m)$. This implies that b is an initial segment of cb^{m-1}. Since $c > b$, c is at least as long as b, and is $\neq b$. Thus it follows that b is a proper initial seqment of c, i.e., we have $c = bw$ for a nonempty word w. Then $(b^{m-1}c, c)$ is semi-perfect and belongs to $\mathrm{Eq}(b, b^m)$, hence to T. From $(b^{m-1}c, c)$ and (b, c) is derivable (b, b^m). This concludes the proof. ∎

Call an equation **right-regular** if it takes the form (xc, xd) where $\mathrm{supp}(c) = \mathrm{supp}(d)$. Call (a, b) **left-regular** if (a^∂, b^∂) is right-regular. The set of all right-regular equations (respectively, left-regular equations) is a theory.

Proposition 7.2. *The set of all right-regular equations is good.*

Proof. The theory S consisting of all the right-regular equations is the largest regular theory included in $E_\ell \cap I_{xy}$ which includes all the left-perfect equations and does not include any power equation $(xa, (xa)^2)$, $x \notin \mathrm{supp}(a)$.

The set of equations that are both right-regular and left-perfect is good. Hence it suffices to show the goodness of the set of equations $(a,b) = (xc, xd)$ with $x \notin \mathrm{supp}(c) = \mathrm{supp}(d)$. For such an equation (a,b), $\mathrm{Eq}(a,b)$ is the largest subtheory T of S such that every left-perfect equation in T is a consequence of (a,b). For example, suppose that (u,v) belongs to such a theory T. Then $(u,v) = (zr, zs)$ for some variable z and words r, s with $\mathrm{supp}(r) = \mathrm{supp}(s)$. If $z \in \mathrm{supp}(r)$ then (u,v) is left perfect and so belongs to $\mathrm{Eq}(a,b)$. Assume that $z \notin \mathrm{supp}(r)$. Let w be any letter in $\mathrm{supp}(r)$, so that the equation (wr, ws) belongs to $T \cap \mathrm{Eq}(a,b)$ (for it is left-perfect). By examining derivations, we can easily verify that this implies $(r,s) \in \mathrm{Eq}(c,d)$, and that this in turn implies that $(zr, zs) \in \mathrm{Eq}(a,b)$. ∎

Call an equation a **left-absorption equation** (or a **right-absorption equation**) if it takes the form (a, ba) (or, respectively, (a, ab)) where a and b are nonempty. The union of the sets of left- and right- absorption equations is the set of absorption equations. In the next section, we show that the set of all non-regular equations is good. Using that result, we can prove that the set of absorption equations is good.

Proposition 7.3. *The set of all absorption equations is good.*

Proof. It is sufficient to show that the set of left-absorption equations is good. Let (a, ba) be such an equation. With the goodness of the set of non-regular equations (proved in the next section), we can assume that (a, ba) is regular. We claim that $\mathrm{Eq}(a, ba)$ is the largest regular subtheory T of E_r having the property that any right-regular and not left-perfect equation (xc, xd) belongs to T iff (c,d) is derivable from (a, ba).

The proof of the claim just consists in showing that $\mathrm{Eq}(a,b)$ has the property just defined; it should be obvious that any theory possessing this property is a subtheory of $\mathrm{Eq}(a,b)$. Suppose that (exf, g) is an immediate consequence of (a, ba) where the variable x does not occur in the non-empty word f. Since $(a, ba) \in E_r \cap E$ then $g = e'xf'$ where x does not occur in the non-empty word f'. Since every letter in b occurs in a, it is easy to see that either $f = f'$ or else (f, f') is an immediate consequence of (a, ba). From this it follows that if $(exf, e'xf')$ is derivable from (a, ba) where x occurs in neither of the non-empty words f, f', then (f, f') is derivable from (a, ba). The special case of this in which e and e' are the empty word constitutes what we set out to prove. ∎

8. Non-regular equations

In this section, we prove that the set of all non-regular equations is good. Call an equation (a,b) **nr-left-perfect** iff a and b are left-perfect and $\operatorname{supp}(a) \neq \operatorname{supp}(b)$.

Lemma 8.1. *The set of all nr-left-perfect equations is good.*

Proof. Let (a,b) be a non-regular equation where a and b are left-perfect. We claim that $\operatorname{Eq}(a,b)$ is the least theory T not included in E such that any left- or right-perfect (regular) equation belongs to T iff it is a consequence of (a,b).

To prove this, let T satisfy the stated condition. There is a non-regular equation (u,v) included in $T \cap \operatorname{Eq}(a,b)$. We can suppose that $\operatorname{supp}(u) \not\subseteq \operatorname{supp}(v)$. Choosing distinct letters x and y such that $y \in \operatorname{supp}(u) \setminus \operatorname{supp}(v)$, we substitute xxy for y and substitute x for all other letters in u, to obtain a word $c(x,y)$ with support set $\{x,y\}$ such that the equation $(c(x,y), c(x,z))$ belongs to $T \cap \operatorname{Eq}(a,b)$, and moreover, the leftmost letter in $c(x,y)$ is x and x occurs at least twice in $c(x,y)$. Note that it follows that every word of the form $c(r,s)$ is left-perfect.

Now let $Z = \{z_0, \ldots, z_{n-1}\}$ be the set of all the variables that occur in a and not in b. Let f, g, h, k be the substitutions that map $z \mapsto z$ for each letter $z \notin Z$ and for $0 \leq i < n$ satisfy

$$f(z_i) = c(z_i, z_i),$$

$$g(z_i) = c(z_i, b),$$

$$h(z_i) = c(b, z_i),$$

$$k(z_i) = c(b, b).$$

It follows from our choice of $c(x,y)$ and from the fact that a and b are left-perfect, that each of the equations $(a, f(a))$, $(g(a), h(a))$, $(k(a), b)$ is left-perfect (regular), and belongs to $\operatorname{Eq}(a,b)$; thus each of these equations belongs to T. Also, the equations $(f(a), g(a))$ and $(h(a), k(a))$ are consequences of $(c(x,y), c(x,z))$, so they belong to T. The five equations taken together imply (a,b), so it follows that $(a,b) \in T$. ∎

Proposition 8.2. *The set of all non-regular equations is good.*

Proof. Let (a,b) be non-regular. Without loss of generality, we can assume that $a = rxs$ where $x \notin \operatorname{supp}(b)$ and $\operatorname{supp}(r) \subseteq \operatorname{supp}(b)$ (and r may be empty). Clearly (a,b) implies (x^k, x^{k+m-1}) for some $k \geq 1$ and $m > 1$. Also, replacing x in (a,b) by xsa^{k-1}, we find that (a,b) implies $(a^k s', b)$ for some s', hence (a,b) implies (a, a^m) (and (b, b^m)).

Now $\operatorname{Eq}(a,b)$ is the least theory T containing the power equations (a, a^m), (b, b^m) and the nr-left-perfect equation (a^m, b^m)—i.e., it is the least theory containing all the consequences of $\operatorname{Eq}(a,b)$ that happen to be power equations or nr-left-perfect. ∎

9. The sets of 8-smooth and 8-good equations

Call an equation (a,b) **8-smooth** if it is regular and for some $n \geq 1$ and some non-empty words c,d,e and letter x, it implies the equations (x^n, x^{2n}) and $(a, ce^n d)$.

Proposition 9.1. *The set of all 8-smooth equations is good.*

Proof. In view of Propositions 5.9, 7.1 and 7.2, it will suffice to consider just an 8-smooth equation (a,b) which is neither semi-perfect nor right-regular nor a power equation. This means that we can assume that $a = xuy$ where each of the letters x and y has just one occurence in a, and where either $b = xu'xv'$ or else $b = zv'$ with $z \neq x$. Let (a,b) be such an equation with $(x^n, x^{2n}) \in \mathrm{Eq}(a,b)$ and $(a, c\beta d) \in \mathrm{Eq}(a,b)$ where $\beta = e^n$ for some non-empty word e.

Let σ be a substitution which maps x to $c\beta$, and maps y and each variable occuring in u to β. Since $(a, c\beta d)$ and (β, β^2) are derivable from (a,b), then $(c\beta, \sigma(a))$ and $(a, \sigma(a)d)$ is derivable. Thus $(a, \sigma(b)d)$ is derivable. Now in case $b = xu'xv'$ then $(\sigma(b), (c\beta)^k)$ is derivable from (a,b) for some $k > 1$, i.e., $(\sigma(b), (c\beta)^{k-1}\sigma(a))$ is derivable. This yields $(\sigma(a), (c\beta)^{k-1}\sigma(a))$, and then (combined with $(a, \sigma(a)d)$) it yields $(a, (c\beta)^{k-1}a)$. Then (a,b) is equivalent to the set of the two left-absorption equations $(a, (c\beta)^{k-1}a)$, $(b, (c\beta)^{k-1}b)$ and the left-perfect equation $((c\beta)^{k-1}a, (c\beta)^{k-1}b)$.

In case $b = zv'$ with $x \neq z$ then $\sigma(b)$ has β as an initial subword. In this case we find that (a,b) entails $(a, \beta a)$, and we can conclude just as above. In both cases, $\mathrm{Eq}(a,b)$ is the least theory T that includes all left-perfect equations derivable from (a,b) and all left-absorption equations derivable from (a,b). ∎

We call an equation (a,b) $\mathbf{8-good}$ if $\mathrm{Eq}(a,b)$ is the least theory T for which every equation (c,d) that is either non-regular, parallel, semi-perfect, permutational, left- or right-regular, an absorption equation or 8-smooth belongs to T iff (c,d) is derivable from (a,b). Thus an equation is 8-good if and only if it is equivalent to a finite set of equations belonging to the sets that we have already proved to be good. The set of all 8-good equations is obviously a good set.

Lemma 9.2. *Suppose that $\{a,b,c,e\} \subset W$ and d is a possibly empty word. Let Σ be either $\{(a,b),(a,cd),(c,ce)\}$ or $\{(a,b),(a,dc),(c,ec)\}$ and put $T = \mathrm{Eq}(\Sigma)$. Then T is generated by a finite set of 8-good equations.*

Proof. We shall assume that $\Sigma = \{(a,b),(a,cd),(c,ce)\}$. If any two of the words a, b, cd have unequal support, then Σ is equivalent to a set consisting of the absorption equation (c,ce) and two non-regular equations. The lemma is trivial in that case. Then if (c,ce) is non-regular, the non-regular equation (a, ced) is derivable from Σ and again the desired conclusion is trivial. Thus we can assume that $\Sigma \subset E$. We can clearly assume that $\mathrm{supp}(a)$ contains at least two letters.

If each of the words a, b, cd is left- or right-perfect, then $\{(a,b),(a,cd)\}$ is a set of semi-perfect equations and again we are done. So, finally, we can choose an unperfect word $q \in \{a,b,cd\}$, say $q = xry$ where x, y are letters.

Now (c, ce) implies (x^n, x^{2n}) for some $n > 0$ and Σ implies $(q, c\beta d)$ where $\beta = e^n$. We can assume that one of the words in $\{a,b,cd\} \setminus \{q\}$ either begins with a letter other than x or else begins with x and has a second occurence of x (else Σ is equivalent to an absorption equation together with two right-regular equations). Hence, just as in the proof of Proposition 9.1, we find that Σ entails either $(q, c\beta q)$ or else $(q, \beta q)$. Thus we find that Σ is equivalent to a set of four absorption equations and two right-regular equations. ■

Lemma 9.3. *Suppose that (a,b) is a regular but not 8-smooth equation where $a = xuy$ is unperfect, $|a| > 1$, and x, y are letters. Let Σ be the set of all substitutions σ such that $(a, \sigma(a)) \in \mathrm{Eq}(a,b)$. If $\sigma \in \Sigma$, then y can occur in $\sigma(y)$ only as the rightmost letter. Moreover, if $\sigma \in \Sigma$ and $|\sigma(y)| > 1$ then if $\lambda = \sigma^k \in \Sigma$ is a power of σ such that $\lambda(y)$ and $\lambda^2(y)$ end with the same letter (and such powers of σ exist), we have that $\lambda(y)$ ends with y.*

Proof. Throughout the proof, T denotes the theory $\mathrm{Eq}(a,b)$. Suppose first that $\sigma \in \Sigma$ and $|\sigma(y)| > 1$. Let $\tau = \sigma^m$, $m = |\operatorname{supp}(a)|!$. Then it is easy to see that $\tau(z)$ and $\tau^2(z)$ have the same first and last letter, for every $z \in \operatorname{supp}(a)$. Moreover, $\tau \in \Sigma$ and $|\tau(y)| > 1$. We proceed to show that these facts imply that $\tau(y)$ ends in y and has only one occurence of y. Note that the same assumptions hold for τ^k as for τ when $k \geq 1$. (We will need this in the argument.)

For the first of the two claims, suppose that $\tau(y) = vz$ where z is a letter distinct from y. Let γ be the substitution that acts like τ on all letters except y, with $\gamma(y) = v$. (This is legitimate since $|\tau(y)| > 1$ and so $v \neq \emptyset$.) Then $\gamma(a) = \tau(xu)v$, and so $\tau(a) = \gamma(a)z$, and $a \equiv_T \gamma\tau(a)z$. This means that $\tau_1 \in \Sigma$ where τ_1 agrees with $\gamma\tau$ except at y and $\tau_1(y) = \gamma\tau(y)z = \gamma(v)\tau(z)z = v_1 z^2$. (We have used the fact that τ and $\tau^2(y)$ end with the same variable, and so $\tau(z)$ ends with z. Note that for the same reasons, $\tau_1(z)$ ends with z.) Now let γ_1 be the substitution that agrees with τ_1 except at y and $\gamma_1(y) = v_1$. Thus $\tau_1(a) = \gamma_1(a)z^2$. Let τ_2 agree $\gamma_1\tau$ except at y and $\tau_2(y) = \gamma_1\tau(y)z^2$. Thus $\tau_2 \in \Sigma$ and $\tau_2(y) = v_2 z^3$ for a nonempty word v_2, and also $\tau_2(z)$ ends with z. Obviously, this construction can be iterated and we find that $a \equiv_T \gamma_k(a)z^{k+1}$ for all integers k. Then clearly (a,b) is 8-smooth. But this contradicts our assumption. Thus we conclude that $\tau(y) = vy$.

We proceed toward the goal of proving that v cannot contain the letter y. First, we claim that we cannot have $\tau(y) = w'ytwy$ with t a letter distinct from y such that $\tau(t)$ begins with t. Supposing otherwise, let γ be the same as τ except that $\gamma(y) = w'yt$. Then

$$a \equiv_T \gamma(a)wy \equiv_T \gamma\tau(a)wy = \tau_1(a)$$

where $\tau_1(y) = w_1{}'yt^2w_1y$ (since $\gamma(t) = \tau(t)$ begins with t) and $\tau_1(y)$ ends with y and $\tau_1(t)$ begins with t. Let γ_1 be the same as τ_1 except that $\gamma_1(y) = w_1{}'yt^2$. Then

$$a \equiv_T \gamma_1(a)w_1y \equiv_T \gamma_1\tau(a)w_1y = \tau_2(a)$$

where $\tau_2(y) = w_2{}'yt^3w_2y$ and $\tau_2(y)$ ends with y and $\tau_2(t)$ begins with t. Clearly, this construction can be continued and it gives for every positive integer k a substitution $\tau_k \in \Sigma$ such that t^{k+1} occurs in $\tau_k(a)$. Thus it follows that (a,b) is 8-smooth; again a contradiction.

Now we claim that we cannot have $\tau(y) = w'ytwy$ with t a letter distinct from y. Suppose otherwise. If $\tau(t)$ does not begin with y, then replacing τ by τ^2, we get the situation proved impossible in the last paragraph. Thus $\tau(t)$ begins with the letter y. Now again, let γ be like τ except $\gamma(y) = w'yt$, and let λ be like $\gamma\tau$ except $\lambda(y) = \gamma\tau(y)wy$. Thus $\lambda \in \Sigma$ and $\lambda(y) = w_1{}'ytyw_1y$. Moreover, $\lambda(t)$ begins with the same letter z as does $\tau(y)$. If $z \neq y$, then $\lambda^2(t)$ also begins with z. In this case, the substitution $\lambda^m = \tau'$, $m = |\operatorname{supp}(a)|!$, can replace τ in the argument of the last paragraph, since $\tau'(y)$ is of the form $w'yzwy$ with z a letter distinct from y and such that $\tau'(z)$ begins with z. This gives a contradiction. So we conclude that if the claim of this paragraph fails, then $\tau(y)$ begins with y. In the next two paragraphs, we show that $\tau(y)$ cannot begin with y.

Suppose that $\tau(y) = y^2w$ for some possibly empty w. Taking γ like τ except $\gamma(y) = y^2$, we get $\tau_1 \in \Sigma$ with $\tau_1(y) = y^4w_1$. Clearly, the same approach as in previous paragraphs will yield that Σ contains τ_k with $y^{2(k+1)}$ occuring in $\tau_k(a)$ and the usual contradiction.

Next, suppose that $\tau(y) = ytwy$ where t is a letter distinct from y. We have already shown that this implies that $\tau(t)$ begins with y. Then let γ be like τ except $\gamma(y) = y$. This leads to $\tau_1 \in \Sigma$ with $\tau_1(y) = y^2w_1$, which we have just shown is impossible. (The special property of τ was not used in the last paragraph.)

The results of the preceeding three paragraphs, taken together, imply that $\tau(y) = wy^k$ where $k \geq 1$ and y does not occur in w. If $k > 1$ then $\tau^2(y) = w'wy^kwy^k$; but since all the above analysis applies equally well to τ^2, it would follow that w is empty and $\tau(y) = y^k$, $k > 1$. We have already shown that this case cannot occur.

We can now finish the proof of the second assertion of this lemma. Suppose that $\lambda = \sigma^k$ and $\lambda(y)$ and $\lambda^2(y)$ end with the same letter z. Then with $\tau' = \lambda^m$, $\tau'(y)$ ends with z. Moreover, all the above analysis applies to λ and τ', showing that $y = z$, as desired.

Now to finish the proof of this lemma, suppose that $\sigma \in \Sigma$ and $\sigma(y) = w'ywz$ where z is a letter. Our task is to derive a contradiction from this assumption. But this is very easy. Clearly, y occurs in a position other than the last in $\sigma^n(y)$ for all $n \geq 1$. But with $n = m = |\operatorname{supp}(a)|!$, this contradicts what we have already proved. ∎

10. Definable locally finite theories

A theory T is called **locally finite** iff each finitely generated model of T is a finite semigroup—equivalently, for any finite set Y of letters, there are only finitely many T-equivalence classes containing words w with $\mathrm{supp}(w) \subseteq Y$.

If T is the equational theory of a finite semigroup then T is, of course, locally finite. Our aim in this section is to prove that the set of theories of finite semigroups is definable and each individual theory of a finite semigroup is semi-definable. We shall also prove that every finitely axiomatizable locally finite theory is semi-definable; the collection of all such theories is definable; and the collection of all locally finite theories is definable.

Lemma 10.1. *Each locally finite theory is generated by a set of 8-good equations.*

Proof. Assume that T is locally finite, $(a,b) \in T$, and (a,b) is not 8-good. Thus $\mathrm{supp}(a) = \mathrm{supp}(b)$ and without loss of generality we can assume that $a < b$ (since (a,b) is not parallel). This equation is easily seen to generate a sequence of equations (a,b_i), $i \in \omega$, belonging to T with $|a| < |b_0| < |b_1| < \cdots$. Since all these words have the same support and T is locally finite, by choosing n large enough, we can find nonempty words c, e, d so that $b_n = ced$ and $(c, ce) \in T$. By Lemma 9.2, the set $\{(a,b),(a,b_n),(c,ce)\} \subset T$ is equivalent to a finite set of 8-good equations. ∎

Lemma 10.2. *Let* $\mathbf{S}$ *be an* n*-element (finite) semigroup and* T *be its equational theory. There is a finite set* $\Sigma \subset T$ *such that* T *is precisely the largest equational theory* A *having the property that any equation in* n *letters belongs to* A *iff it is entailed by* Σ.

Proof. It is well-known that there is a finite set Σ of equations in n letters such that an equation in n letters belongs to T iff it is entailed by Σ. Suppose that A is some theory not included in T. Let (c,d) be some equation in $A \setminus T$. Since (c,d) fails to hold in $\mathbf{S}$, there is a homomorphism σ of the free semigroup W into $\mathbf{S}$ satisfying $\sigma(c) \neq \sigma(d)$. Since $|\mathbf{S}| = n$, we can choose a substitution τ that maps the set of letters occuring in (c,d) onto an n-element set of letters, and another homomorphism $\sigma' : W \to \mathbf{S}$, so that we have $\sigma = \sigma' \circ \tau$. Then the equation $(\tau(c), \tau(d))$ belongs to A, has at most n letters, and is not implied by Σ (since it does not belong to T). ∎

Lemma 10.3. *A theory* $T \in \mathcal{L}$ *is the equational theory of some finite semigroup iff there is a finite nonvoid set* Y *of letters and a finite set* Σ *of 8-good equations such that:*

(1) *There exist only finitely many* $\mathrm{Eq}(\Sigma)$*-equivalence classes that contain words* u *with* $\mathrm{supp}(u) \subseteq Y$*;*

(2) T *is the largest theory* A *such that* $\Sigma \subset A$ *and every 8-good equation* $(a,b) \in A$ *with* $\mathrm{supp}(a) \cup \mathrm{supp}(b) \subseteq Y$ *is entailed by* Σ.

Proof. Suppose first that T is the theory of $\mathbf{S}$ and $|\mathbf{S}| = n$. Let Y be any n-element set of letters. Using Lemmas 10.1 and 10.2, we conclude the existence of a finite set Σ of 8-good equations so that (1) and (2') hold where (2') reads the same as (2) with the difference that (a,b) ranges over *all* equations with support contained in Y. Here, (2) must hold as well. Indeed, let A be a theory containing Σ and such that every 8-good equation in A built of the letters in Y is entailed by Σ. Then let (a,b) be any equation in A built of the letters in

Y. The proof of Lemma 10.1 shows that (a, b) is entailed by a finite subset of A consisting of 8-good equations also with support contained in Y. Thus (a, b) is entailed by Σ. So (2') implies $A \subseteq T$.

Now suppose that T, Y, Σ satisfy (1) and (2) where Σ is a finite set of 8-good equations and $|Y| = n$. Let $C = \mathrm{Eq}(\Sigma)$, $W' = \{w \in W : \mathrm{supp}(w) \subseteq Y\}$, $\mathbf{S}' = W'/(C|_{W'})$. Condition (1) implies that $\mathbf{S}'$ is a finite semigroup; in fact, it is the free semigroup on n generators in the variety of semigroups defined by C. Let T' be the equational theory of $\mathbf{S}'$. Now $\Sigma \subset T'$ and every equation in T' with support contained in Y belongs to C. Thus we have $T' \leq T$, by (2).

To conclude this proof, we must show that $T \leq T'$. We assume that $(a, b) \in T \setminus T'$ and argue towards a contradiction. Since $\mathbf{S}'$ is n-generated, every equation not belonging to T' entails an equation in n letters not belonging to T'. Thus (a, b) entails an equation $(c, d) \in T \setminus T'$ with $\mathrm{supp}(c) \cup \mathrm{supp}(d) \subseteq Y$. Since T contains Σ and (1) holds, the argument for Lemma 10.1 shows that (c, d) is entailed by a set of 8-good equations contained in $[W' \times W'] \cap T$. Then (2) implies that $(c, d) \in C$, and thus $(c, d) \in T'$, which is our contradiction. ■

Theorem 10.4. *The set of theories of finite semigroups is definable and each theory of a finite semigroup is semi-definable.*

Proof. This follows easily from Lemma 10.3. ■

Theorem 10.5. *The set of finitely axiomatizable locally finite theories is definable and each such theory is semi-definable.*

Proof. This follows easily from Lemma 10.1. T is locally finite and finitely axiomatizable iff there is a finite set Σ of 8-good equations such that $T = \mathrm{Eq}(\Sigma)$ and, moreover, $\mathrm{Eq}(\Sigma)$ is locally finite. These conditions can be expressed using our codes for finite sequences of words. ■

Theorem 10.6. *The set of locally finite theories is definable.*

Proof. By Lemma 10.1, T is locally finite iff for every integer n there is a finite set Σ of 8-good equations such that $\Sigma \subseteq T$ and there are only a finite number of $\mathrm{Eq}(\Sigma)$-equivalence classes containing words with a fixed n-element support set. ■

The remaining two sections of the paper contain fairly technical results directed toward the goal of proving that the set of all equations is good.

11. Reduction to 9-smooth equations

We define two further sets of equations, namely, exact and 9-smooth equations. We show that if both of these sets are good, then the set of all equations is good. Then we prove that the set of exact equations is good. Using these results, prove that the set of all finitely axiomatizable theories is definable.

Call an equation (a,b) **9-smooth** if $\mathrm{supp}(a) = \mathrm{supp}(b)$, $a < b$, a is unperfect and b is perfect—i.e., the initial and final letters of a have no repeat occurences in a while the initial and final letters of b both have repeat occurences in b.

Call an equation (a,b) **left-exact** if the following conditions hold:

(1) $\mathrm{supp}(a) = \mathrm{supp}(b)$ and $a < b$.
(2) a is unperfect.
(3) If c is any left-perfect word, then (a,c) is not derivable from (a,b).
(4) Where Σ is the monoid of substitutions σ such that $(a,\sigma(a))$ is derivable from (a,b), and x is the initial letter in a, the set $X_0 = \{\sigma(x) : \sigma \in \Sigma\}$ is a set of letters, i.e., $|r| = 1$ for all $r \in X$. Let $Y_0 = \mathrm{supp}(a) \setminus X$.
(5) If $\sigma \in \Sigma$, then σ restricted to X_0 is a permutation, and if $z \in Y_0$ then $\mathrm{supp}(\sigma(z)) \subseteq Y_0$.

Call an equation (a,b) **exact** iff both (a,b) and the dual equation are left-exact.

Lemma 11.1. *Let T be a regular equational theory and $a = xry$ be a word, where each of x and y occurs only once in a and $x \neq y$. Suppose that T contains a non-left-regular equation (a,b) with $a \leq b$, and contains some equation $(a,\sigma(a))$ with $|\sigma(y)| > 1$. Then T contains an equation $(a,\tau(a))$ where $\tau(a)$ is right-perfect, $|\tau(y)| > 1$, and $|\tau(x)| > 1$ if $|\sigma(x)| > 1$.*

Proof. By changing the value of σ at y, we can assume that $(a,c) \in T$ where $c = \sigma(xr)\sigma(y)z_1$ and z_1 is a letter, and our task is to produce $d = \tau(a)z_2$, z_2 a letter occuring in $\tau(a)$, such that $(a,d) \in T$ and $|\tau(x)| > 1$ if $|\sigma(x)| > 1$. Now if c is right-perfect, we are done. Thus, we assume that z_1 occurs only once in c. Next, we show that, by changing σ if necessary, we can ensure that $z_1 \neq y$.

Suppose that $z_1 = y$. Since $a \leq b$ (and the initial and terminal letters of a have only one occurence in a), we can write $b = \gamma(a)$. Since (a,b) is not left-regular, then either b is right-perfect or its rightmost letter is different from y. Define σ' to be σ on all letters except y and $\sigma'(y) = \sigma(y)y = \sigma(y)z_1$. Let $\sigma'' = \gamma\sigma'$. Now $c = \sigma'(a)$ and so (a,c) yields $(\gamma(a),\gamma(\sigma'(a)))$ and T contains (a,c') where $c' = \sigma''(a)$. We can also write $c' = \gamma\sigma(a)\gamma(y)$. We can assume that c' is not right-perfect (else we are done). Then if the rightmost letter of $\gamma(y)$ is y, we have that y occurs only at the right end of $\gamma(y)$, and also it follows that b is right-perfect and y occurs in $\gamma(z)$ for some letter $z \in \mathrm{supp}(xr)$ (since y occurs only at the right end of $\gamma(y)$). In this case,

$$z \in \mathrm{supp}(c) \setminus \{y\} = \mathrm{supp}(\sigma(a)),$$

which implies that c' is right-perfect, after all. Thus either the desired conclusion has been reached or else the rightmost letter of $\gamma(y)$ is not y. Redefining c to be this new c' and choosing the obvious substitution, we have that $c = \sigma(a)z_1$ where the letter z_1 occurs only once in c and $z_1 \neq y$.

Choose a word e and substitution τ such that T contains (a,e) where

$$e = \tau(a)z_k \dots z_1$$

with z_1 as above, the letters $z_1, \dots, z_k$ are distinct and each of them occurs only once in e, and k is the largest number for which such an e and τ exist. (Since $k \le |\operatorname{supp}(a)|$, such a maximum k must exist.) Define τ' by $\tau'(y) = \tau(y)z_k \dots z_1$ and $\tau'(z) = \tau(z)$ for all other letters z, so that $\tau'(a) = \tau(xr)\tau'(y)$ and $e = \tau'(a)$. Define $c'' = \tau'(c)$ and note that (a, c'') is derivable from (a, b). If c'' is right-perfect, then we are done, obviously. Assuming that c'' is not right-perfect, we shall derive a contradiction.

Let z_{k+1} be the rightmost letter in $\tau'(z_1)$. We are supposing that z_{k+1} occurs only once in c''. Note that since $z_1 \ne y$ then $\tau'(z_1) = \tau(z_1)$, a subword of $\tau(a)$, implying that none of the letters $z_1, \dots, z_k$ occurs in $\tau'(z_1)$; and in particular, $\{z_{k+1}, z_k, \dots, z_1\}$ is a $k+1$-element set of letters. Now define $d = \tau(c)z_k \dots z_1$ and notice that (a, b) implies (e, d) and (a, d). We have

$$d = \tau(\sigma(a)z_1)z_k \dots z_1 = \tau(\sigma(a))v'z_{k+1}z_k \dots z_1\,;$$

and we claim that each of $z_1, \dots, z_{k+1}$ occurs only once in d. Since d can be written as $\gamma(a)z_{k+1} \dots z_1$, this will contradict the maximality of k.

To establish the claim, observe first that $\operatorname{supp}(\tau(\sigma(a)z_1) = \operatorname{supp}(\tau(a))$ and this set is disjoint from $\{z_1, \dots z_k\}$ (a property of e), which implies that each of $z_1, \dots, z_k$ occurs just once in d. Also, $\operatorname{supp}(\tau(z)) \subseteq \operatorname{supp}(\tau'(z))$ for every letter z and so $\operatorname{supp}(\tau(\sigma(a)) \subseteq \operatorname{supp}(\tau'(\sigma(a))$ which does not contain z_{k+1} (since c'' is not right-perfect). Finally, z_{k+1} occurs only once in $\tau'(z_1) = v'z_{k+1}$, for the same reason. The claim has been proved, and with it this lemma. ∎

Lemma 11.2. *Let (a, b) be a regular equation where $a \le b$ and a is right-perfect. Then (a, b) is equivalent to a set of two equations, one of which is right-perfect and the other right-regular.*

Proof. If b has a final subword identical with a substitution instance of a, then (a, b) is right-perfect. Thus we can assume that $b = ry = u'\sigma(a)v'y$ where the letter y does not occur in r, and we have $a = uzvz$ where z is a letter and any of the words u, v, u', v' may be empty. We repeat the argument of Proposition 5.9. Letting w be a new letter, (a, b) implies (aw, a') where a' is obtained from a by the substitution which maps all letters identically, except y, which maps to yw (since y occurs only once in b). Thus also, (a, b) implies $(\sigma(a)w, \sigma'(a'))$ where σ' behaves like σ except that $\sigma'(w) = w$; hence (a, b) implies (a, c), $c = u'\sigma''(a)$, where σ'' is like σ except that $\sigma''(y) = \sigma(y)v'y$. Now (a, b) is equivalent to $\{(a, c), (c, b)\}$ and (a, c) is right-perfect, while (c, b) is right-regular. ∎

Lemma 11.3. *Every equation is equivalent to a finite set of equations each of which is 8-good, left-exact, the dual of a left-exact equation or 9-smooth.*

Proof. Let (a, b) be any equation that is not 8-good. Then quickly from Lemma 11.2 it follows that we can assume $\operatorname{supp}(a) = \operatorname{supp}(b)$, $a < b$, a is unperfect, and $|a| > 1$. Thus we have $a = xry$ with $\operatorname{supp}(a) \cap \{x, y\} = \emptyset$ and $x \ne y$. Also, (a, b) is neither left- nor right-regular, so we have a possibility of applying Lemma 11.1 or its dual to the theory $T = \operatorname{Eq}(a, b)$.

Let Σ be the set of substitutions σ such that $(a, \sigma(a)) \in T$. Note that $T \subseteq I_a$ and a unperfect imply that whenever $(a, c) \in T$ we have $c = \sigma(a)$ for some $\sigma \in \Sigma$. Let us call (a, b) *right-sharp* if there does not exist a substitution $\sigma \in \Sigma$ such that $|\sigma(y)| > 1$. Call (a, b) *left-sharp* iff the dual condition holds.

Suppose first that (a, b) is neither right-sharp, nor left sharp. Then by Lemma 11.1 and its dual, (a, b) implies equations (a, c) and (a, d) where $c = \sigma(a)z$ and $d = w\tau(a)$ and c is right-perfect while d is left-perfect. Then where $e = \sigma(d)z$ and $f = \sigma(w\tau(b))z$, (a, b) derives the 9-smooth equation (a, e) and the perfect equation (e, f). Here (a, b) is equivalent to the conjunction of (a, e), (e, f) and the equation (b, f). This latter equation is either left-perfect, right-perfect, or 9-smooth. Thus we are done with the case where (a, b) is neither left- nor right-sharp.

Since all our other assumptions are self-dual, we can henceforth assume that (a, b) is left-sharp. Write X_0 for the set of letters $\{\sigma(x) : \sigma \in \Sigma\}$ and denote by Y_0 the set of all letters in $\mathrm{supp}(a)$ that do not belong to X_0. We divide the remainder of the proof into two cases.

Case I: (a, b) is not right-sharp.

By Lemma 11.1, we can choose a substitution λ so that $(a, \lambda(a)z) \in T$ where z is a letter occuring in $\lambda(a)$. We proceed to show that for all $\sigma \in \Sigma$, $\sigma(a)$ fails to be left-perfect. Suppose instead that $\sigma(a)$ is left-perfect for a certain $\sigma \in \Sigma$. This implies that $|a| < |\sigma(a)|$ since $(a, \sigma(a))$ is regular. Let $\tau = \sigma^n$ for a large enough n so that $|b| < |\sigma^n(a)|$ and note that $\tau(a)$ is left-perfect. Then define $c = \lambda\tau(a)z$, where (a, b) implies $(a, \lambda(a)z)$ as above. Note that c is a perfect word. Now the equation (a, c) is 9-smooth and derivable from (a, b). Also, since $|b| < |c|$, the equation (b, c) is either parallel, 9-smooth, left-perfect, or right-perfect. Since (a, b) is equivalent to $\{(a, c), (b, c)\}$, we are done in this case. So we can assume in Case I that $\sigma(a)$ is never left-perfect, for $\sigma \in \Sigma$.

We shall now be able to conclude in Case I that (a, b) is left-exact. All that remains is to show that condition (5) in the definition of left-exactness holds. Let $\sigma \in \Sigma$. Clearly, $\sigma(X_0) \subseteq X_0$. To see that σ restricted to X_0 is one-to-one, suppose to the contrary that $\sigma(x_0) = \sigma(x_1)$ where x_0 and x_1 are two distinct members of X_0. We can choose some $\tau \in \Sigma$ so that $\tau(x) = x_0$. Thus the leftmost letter of $\sigma\tau(a)$ is $\sigma(x_0)$. The letter x_1 occurs somewhere in $\tau(ry)$ since $\tau(a) = x_0\tau(ry)$. Thus $\sigma\tau(a) = \sigma(x_0)\sigma\tau(ry)$ where $\sigma(x_0) = \sigma(x_1)$ occurs in $\sigma\tau(ry)$; but then $\sigma\tau(a)$ is left-perfect. This contradiction establishes that σ is one-to-one on the set X_0.

Finally, suppose that $z \in Y$ and $\sigma \in \Sigma$. Working for a contradiction, suppose that $\sigma(z)$ contains a letter $x_0 \in X_0$. Since σ induces a permutation on X_0, we can choose $x_1 \in X_0$ with $\sigma(x_1) = x_0$, and we pick $\tau \in \Sigma$ so that $\tau(x) = x_1$. Now the word $\tau(a) = x_1\tau(ry)$ contains an occurence of z, i.e., $\tau(ry)$ contains such an occurence. Then $\sigma\tau(a) = x_0\sigma\tau(ry)$ and this contains an occurence of x_0 inside $\sigma\tau(ry)$, contradicting the fact that this word must not be left-perfect. So we have finished the proof that (a, b) is left-exact in Case I.

Case II: (a, b) is right sharp, as well as left-sharp.

Let X_0 be as in Case I and put $X_1 = \{\sigma(y) : \sigma \in \Sigma\}$. As above, we have that X_0 and X_1 are sets of letters. We also define $Y_i = \mathrm{supp}(a) \setminus X_i$.

We deal first with the easy subcase in which for some $\sigma \in \Sigma$, $\sigma(a)$ is a perfect word. Letting $\tau = \sigma^n$ be such that $|b| < |\tau(a)|$, and putting $c = \tau(a)$, we have that (a, b) is equivalent to $\{(a, c), (b, c)\}$ where (a, c) is 9-smooth and (b, c) is either parallel, left-perfect, right-perfect, or 9-smooth.

¿From now on, we assume that for no $\sigma \in \Sigma$ is $\sigma(a)$ perfect. For a time, we adopt the assumption that there is some $\gamma \in \Sigma$ for which $\gamma(a)$ is left-perfect. We define Z to be the set of all $z \in X_1$ such that for all $\sigma \in \Sigma$ and for all $w \in \text{supp}(a) \setminus \{z\}$, $\sigma(z) \notin \text{supp}(\sigma(w))$. Then Z is not empty. Indeed, let $z = \gamma(y)$ where γ is a member of Σ with $\gamma(a)$ left-perfect. If we have $w \in \text{supp}(a)$, $w \neq z$, and $\sigma \in \Sigma$ with $\sigma(z)$ occuring in $\sigma(w)$, then $\sigma\gamma(a)$ is right-perfect—i.e., it is perfect—but this contradicts our assumption above. Thus Z is non-empty. Clearly, Z is closed under all substitutions in Σ. Moreover, equally clearly, for all $\sigma \in \Sigma$, the action of σ on Z is one-to-one. Thus, where z and γ are as above, there exists $z' \in Z$ with $\gamma(z') = z = \gamma(y)$. Since $\gamma(a)$ is not right-perfect (as it is left-perfect), then we must have that $z' = y$. Now from $y \in Z$ it follows that for all $\sigma \in \Sigma$, $\sigma(a)$ is not right-perfect.

Having thus shown that it is impossible for $\{\sigma(a) : \sigma \in \Sigma\}$ to contain both a left-perfect and a right-perfect word, we can now assume that this set contains no left-perfect word—i.e., condition (3) in the definition of left-exactness holds. It follows very quickly that (a, b) is left-exact, using just the same arguments that we used in Case I. [If there is no right-perfect word c with $(a, c) \in \text{Eq}(a, b)$ then the dual arguments will show that the dual of (a, b) is left-exact.] ∎

Lemma 11.4. *Every equation is equivalent to a finite set of equations each of which is 8-good, 9-smooth or exact.*

Proof. In view of Lemma 11.3, it suffices to prove that this is true for any left-exact equation (a, b). Thus assume that (a, b) is left-exact, and write X_0 for the set of letters mentioned in condition (4) of the definition of left-exactness. We adopt all the rest of the notation from that definition, so that, for example, we have $a = xry$. Further, we shall assume, to begin with, that there is some right-perfect word $c = \sigma(a)$ with (a, c) derivable from (a, b).

Now σ on X_0 is a permutation, so there is a power $\sigma^n = \tau$, $n > 0$, such that $\tau(x) = x$. Then the word $d = \tau(a)$ is right-perfect, and the equation (a, d) is right-regular, since a and d begin with the same letter and neither word is left-perfect. Choosing $\gamma \in \Sigma$ with $b = \gamma(a)$, define $e = \gamma\tau(a)$. The word e is right-perfect and, just as above, the equation (e, b) is right-regular. Thus (a, b) is equivalent to the conjunction of the right-regular equations (a, d) and (e, b) and the right-perfect equation (d, e).

Thus we have handled the case where (a, b) fails to satisfy the dual of condition (3). Now assuming that (a, b) is not right-regular, the dual of condition (4) follows by Lemma 11.1. Also, the dual of condition (5) follows just as before. Hence (a, b) is exact, if it is not right-regular. ∎

Proposition 11.5. *The set of exact equations is good.*

Proof. For any exact equation (a, b) let $\Sigma_{a,b}$ denote the set of σ such that (a, b) implies $(a, \sigma(a))$. Call (a, b) 1-exact if it is exact and a has the form

$x_1 \cdots x_k \bar{x} w$ for some $k \geq 1$ with letters $x_1, \ldots, x_k$ each having just one occurence in a and $\bar{x}$ having an occurence in w, and moreover, for all $\sigma \in \Sigma_{a,b}$, the initial subword of length k in $\sigma(a)$ is a string of k distinct letters, each of which occurs only once in $\sigma(a)$.

Given an exact equation (a, b), there are $\sigma \in \Sigma_{a,b}$ such that $\sigma(a)$ has some repeated letter. Thus there must clearly exist $\sigma \in \Sigma_{a,b}$ such that $\sigma(a) = c$ has the form $x_1 \cdots x_k \bar{x} w$ for some $1 \leq k$ with letters $x_1, \ldots, x_k$ each having just one occurence in c and $\bar{x}$ having more than one occurence, and such that for all $\lambda \in \Sigma_{a,b}$, if $|\lambda(a)| \geq k$ then the initial subword of $\lambda(a)$ of length k is a string of k distinct letters each having just one occurence in $\lambda(a)$. For such a c, we have that for all $\lambda \in \Sigma_{a,b}$, the initial subword of $\lambda(c)$ of length k is a string of k distinct letters each occuring just once in $\lambda(c)$. Choosing such a c, note that since (a, b) is exact, there is $\lambda \in \Sigma_{a,b}$ such that $d = \lambda(c) = \lambda\sigma(a)$ has the same initial and final letters as a, and moreover $c < d$. Similarly, we have $\gamma \in \Sigma_{a,b}$ such that $e = \gamma(c)$ has the same initial and final letters as b and $c < e$. Now (a, b) is equivalent to the set of four equations $\{(a, d), (b, e), (c, d), (c, e)\}$, the first two of which are left-regular and the last two of which are 1-exact. (Note that, for example, $\Sigma_{c,d} \subseteq \Sigma_{a,b}$.) Thus, we are reduced to showing that the set of 1-exact equations is good.

Let (a, b) be 1-exact,

$$a = x_1 \cdots x_k \bar{x} w \,,$$

each of $x_1, \ldots, x_k$ occuring just once in a, $\bar{x}$ occuring at least twice. Write Σ for $\Sigma_{a,b}$, X_0 for $\{\sigma(x_1) : \sigma \in \Sigma\}$, and Y_0 for $\operatorname{supp}(a) \setminus X_0$. Now just as above, we can choose $\gamma \in \Sigma$ such that $\gamma(a) = c$ has the form

$$c = v' \bar{y} y_\ell \cdots y_1 = x v \bar{y} y_\ell \cdots y_1 \,,$$

each of $y_1, \ldots, y_\ell$ occurs just once and $\bar{y}$ occurs at least twice in c, and moreover, for all $\lambda \in \Sigma$, the terminal subword of $\lambda(a)$ of length ℓ consists of distinct letters each of which occurs just once in $\lambda(a)$. The initial letter x has, of course, no repeat occurence in c.

We define a new word

$$c' = y_1 x v \bar{y} y_\ell \cdots y_2 \,,$$

a cyclic variant of c. And we make three claims.

Claim 1: If $\lambda \in \Sigma$ then $c' \not\leq \lambda(a)$.

Claim 2: If $\lambda \in \Sigma$ then $a \not\leq \lambda(c')$.

Claim 3: If $\lambda \in \Sigma$ and $\lambda(c') = \lambda'(c')$ then $\lambda(c) = \lambda'(c)$ and $\lambda' \in \Sigma$.

To prove Claim 1, suppose that $\lambda \in \Sigma$ and $c' \leq \lambda(a)$, say $\tau(c')$ occurs as a subword u in $\lambda(a)$. Since $y_\ell, \ldots, y_2$, and y_1 and x, each occur just once in c', if u is not a right end of $\lambda(a)$ or if the right end $\tau(y_\ell \cdots y_2)$ of u has length greater than $\ell - 1$, then τ can be modified to τ' so that $\lambda(a) = \tau'(c')r$ with

$r \neq \emptyset$. Then defining ρ so that $\rho(x) = \tau'(y_1x)$, $\rho(y_1) = r$ and $\rho(z) = \tau'(z)$ for all other letters z, we have that $\lambda(a) = \rho(c) = \rho\gamma(a)$. Thus $\rho\gamma \in \Sigma$. But $\rho\gamma$ maps the leftmost letter of a to $\rho(x) = \tau'(y_1x)$, a word of length greater than one, contradicting that (a, b) is exact. Thus we have that

$$\lambda(a) = s\tau(c') = s\tau(y_1xv)\tau(\bar{y})\tau(y_\ell \cdots y_2)$$

where $\tau(y_\ell \cdots y_2)$ has length $\ell - 1$. By our choice of ℓ, the terminal subword of $\lambda(a)$ of length ℓ consists of distinct letters occuring only once in $\lambda(a)$. Hence we have that the rightmost letter in $\tau(\bar{y})$ occurs only once in $\lambda(a)$. This is impossible, because $\bar{y}$ occurs in v. The contradiction concludes our proof of Claim 1.

The proof of Claim 2 is similar. Suppose that

$$\lambda(c') = r\tau(a)s\,, \quad \lambda \in \Sigma\,.$$

Note that since (a, b) is exact, $\lambda(y_1)$ and $\lambda(x)$ are letters ${y_1}'$ and x'. If r is nonempty, then after subtracting the leftmost letter ${y_1}'$ from r we obtain r' with

$$\lambda(xv\bar{y}y_\ell \cdots y_2) = r'\tau(a)s\,,$$

$$\lambda(c) = r'\tau(a)s{y_1}'\,.$$

Clearly, this gives $\lambda(c) = \tau'(a)$ where τ' maps the final letter of a to a word of length at least two; but $\lambda\gamma(a) = \tau'(a)$ gives $\tau' \in \Sigma$ and so this contradicts the exactness of (a, b). Hence we conclude that r is empty. Now if τ fails to map one of the letters $x_1, \ldots, x_k$ to a letter, then τ can be modified so that we have the above situation with $r \neq \emptyset$. Thus we conclude that $\tau(x_1 \cdots x_k)$ is the initial subword of $\lambda(c')$ of length k. Now since (a, b) is 1-exact, the initial subword of $\lambda(c)$ of length k consists of letters occuring just once in $\lambda(c)$, and so just once in $\lambda(c')$; and likewise the letter ${y_1}'$ occurs just once in $\lambda(c)$, hence in $\lambda(c')$ due to exactness. Thus the first $k+1$ letters in $\lambda(c')$ are occuring just once. The length k initial subword of $\tau(a)$ covers just the first k of these, and we conclude that the initial letter in $\tau(\bar{x})$ occurs just once in $\lambda(c')$. This of course is impossible, since $\bar{x}$ occurs at least twice in a. The contradiction establishes Claim 2.

To prove Claim 3, suppose that $\lambda(c') = \lambda'(c')$ and $\lambda \in \Sigma$. Then where ${y_1}'$ is the letter $\lambda(y_1)$, x' is the letter $\lambda(x)$, and $u = v\bar{y}y_\ell \cdots y_2$, we have $\lambda(c) = x'\lambda(u){y_1}'$ and

$${y_1}'\lambda(c) = \lambda(c'){y_1}' = \lambda'(c'){y_1}' = \lambda'(y_1)\lambda'(x)\lambda'(u){y_1}'\,.$$

We can write $\lambda'(y_1) = {y_1}'r$. Now defining $\rho(y_1) = {y_1}'$, $\rho(x) = r\lambda'(x)$ and $\rho(z) = \lambda'(z)$ for all other letters z, it follows from the above displayed equations that $\lambda(c) = \rho(c)$. Then $\rho \in \Sigma$, implying that $\rho(x)$ is a letter, i.e., that $r = \emptyset$ and $\rho = \lambda'$. Thus Claim 3 is true.

Now we choose $\sigma \in \Sigma$ with $b = \sigma(a)$ and define π to be the permutational substitution such that $\pi|_{X_0} = \sigma^{-1}|_{X_0}$ and $\pi(z) = z$ for all letters $z \notin X_0$. Then put $b' = \pi(b)$. It should be clear, upon consideration, that the next statement furnishes a first-order definition of $\mathrm{Eq}(a, b)$ for the 1-exact equation (a, b).

Claim 4: $\mathrm{Eq}(a,b)$ is the smallest theory T contained in $A \vee B$ such that T contains all the right-regular consequences of (a,b) and $T \vee C \geq D$, where $A = \mathrm{Eq}(a, \pi^{-1}(a))$, $B = \mathrm{Eq}(a,b')$, $C = \mathrm{Eq}(a,c')$, $D = \mathrm{Eq}(b,c')$. Moreover, $(a, \pi^{-1}(a))$ is permutational, (a,b') is right-regular and (a,c') and (b,c') are parallel.

We begin the proof of Claim 4 by noting that it follows from Claims 1 and 2 that (a,c') and (b,c') are parallel, and the claimed properties of the other two equations are obvious. Also it is clear that $\mathrm{Eq}(a,b) \leq A \vee B$ and $\mathrm{Eq}(a,b) \vee C \geq D$. Now suppose that T is a theory satisfying the conditions enumerated in the claim. We have to show that (a,b) belongs to T.

Define Π as the set of all permutational substitutions that leave all letters outside of X_0 fixed, and define U to be the set of all words of the form $\rho\lambda(a)$ with $\rho \in \Pi$ and $\lambda \in \Sigma$. The first step is to show that the set U is a union of equivalence classes in the theory $A \vee B$, i.e., if $(r,s) \in A \vee B$ and $r \in U$ then $s \in U$. We leave this step to the reader—the properties defining left-exactness (concerning Σ, X_0 and Y_0) are essential in the proof. Assume that this step has been accomplished.

Since $T \leq A \vee B$, then U is a union of equivalence classes in T. Let $b/(T \vee C)$ denote the set of all words r such that $r \equiv_{T \vee C} b$. Now we claim that

$$b/(T \vee C) = b/T \cup \{\lambda(c') : \lambda(a) \in b/T\}\ .$$

Denote by R the set defined by the right side of the above-claimed equality. It is clear that $b/(T \vee C)$ includes the set R. To get that $b/(T \vee C) \subseteq R$, we only have to show that the set R is a union of equivalence classes in T and is closed under immediate consequences of (a,c').

First, let $r = \lambda(c')$, $\lambda(a) \in b/T$, and suppose that $(r,s) \in T$. Now $b \in U$ so $\lambda(a) \in U$, i.e., $\lambda(a) = \rho\lambda'(a)$ for some $\rho \in \Pi$ and $\lambda' \in \Sigma$. Thus $\rho^{-1}\lambda = \mu \in \Sigma$ and $\rho^{-1}(r) = \mu(c')$. By Claim 2, it is clear that $\mu(c')/(A \vee B) = \{\mu(c')\}$. Since $(\rho^{-1}(r), \rho^{-1}(s)) \in T$, it then follows that $\rho^{-1}(r) = \rho^{-1}(s)$, and that $r = s$ since ρ is an automorphism of the free semigroup. So we have established that R is a union of equivalence classes in T.

Second, suppose that $r \in R$ and (r,s) is an immediate consequence of (a,c'). Thus we have a substitution τ such that r contains a subword u equal either to $\tau(a)$ or $\tau(c')$ and s is obtained by replacing this subword, either $\tau(a)$ or $\tau(c')$, by $\tau(c')$ or $\tau(a)$ respectively. Since $b/T \subseteq U$, we have that there exist $\rho \in \Pi$ and $\lambda \in \Sigma$ such that one of the following two possibilities holds: either case (a): $r = \rho\lambda(a) \in b/T$; or case (b): $\rho\lambda(a) = \nu(a) \in b/T$ for a substitution ν such that $r = \nu(c')$.

In case (a), we argue as follows. Neither $\lambda(a)$ nor $\rho\lambda(a)$ (since ρ is permutational) can properly contain a substitution instance of a (since (a,b) is exact) or contain any substitution instance of c' (by Claim 1).

Thus we have that $r = \rho\lambda(a) = \tau(a)$. Thus s (obtained by replacing $\tau(a)$ by $\tau(c')$ in r) is identical with $\tau(c')$ and belongs to R by definition.

In case (b), we argue like this. We have $\rho^{-1}\nu = \xi \in \Sigma$ and $\rho^{-1}(r) = \xi(c')$ contains as a subword either $\rho^{-1}\tau(a)$ or $\rho^{-1}\tau(c')$. The first possibility is ruled out by Claim 2. If the occurence of $\rho^{-1}\tau(c')$ in $\rho^{-1}(r)$ is as a proper subword, this easily gives an occurence in $\xi(c)$ of a proper subword which is a substitution instance of a, which is impossible because of the exactness of (a,b). Thus we have that $\rho^{-1}(r) = \rho^{-1}\tau(c')$, and hence $r = \tau(c') = \nu(c')$. Now Claim 3 implies that $\rho^{-1}\tau = \xi' \in \Sigma$ and $\xi'(c) = \xi(c)$. The latter fact clearly implies that $(\xi'(a), \xi(a)) \in \mathrm{Eq}(a,b)$ since $(a,c) \in \mathrm{Eq}(a,b)$. It also implies that ξ' and ξ agree at all the letters in X_0—because if $c = z_1p_1z_2p_2\cdots z_np_n$ where $\{z_1,\dots,z_n\} = X_0$ and $p_1,\dots,p_n$ are possibly empty words built out of the letters in Y_0, then we have

$$\xi'(c) = \xi'(z_1){q_1}'\xi'(z_2){q_2}'\dots\xi'(z_n){q_n}'$$

$$\xi(c) = \xi(z_1)q_1\xi(z_2)q_2\dots\xi(z_n)q_n\,.$$

These are two ways of expressing the same word $\xi(c)$ as a product of letters in X_0 alternating with words on Y_0, and the expressions must be identical, i.e., $\xi'(z_i) = \xi(z_i)$ and ${q_i}' = q_i$ for all $i \in \{1,\dots,n\}$. Then it follows that $\xi'(a)$ and $\xi(a)$ begin with the same letter, and so the equation $(\xi'(a), \xi(a))$ is a right-regular equation in $\mathrm{Eq}(a,b)$. Consequently it belongs to T. Finally, we have

$$s = \tau(a) = \rho\xi'(a) \equiv_T \rho\xi(a) = \nu(a)$$

and since $\nu(a) \in b/T$ we conclude that $s \in R$ as we claimed.

The proof that $b/(T \vee C) = R$ is now concluded. Since we have that $T \vee C \geq D$, it follows that $c' \in R$. So we have that either $c' \in b/T \subseteq U$ or else $c' = \nu(c')$ for some ν such that $\nu(a) \in b/T$. The first case is ruled out by Claim 1. In the second case, the equality $c' = \nu(c')$ implies that ν acts like the identity on the letters that matter, and so $\nu(a) = a$. Thus $(a,b) \in T$, which is just what we had to prove. ∎

Call an equation (a,b) **9-good** if it is equivalent to a finite set of 8-good and exact equations. According to Lemma 11.4 and Proposition 11.5, the set of 9-good equations is good and every equation is equivalent to a finite set of 9-good and 9-smooth equations. The set of all equations is good, provided that the set of 9-smooth equations is good.

Theorem 11.6. *The set of all finitely axiomatizable theories is definable.*

Proof. A theory T is finitely axiomatizable iff there exists a finite set Σ of 9-good equations and a finite set $\Gamma = \{a_0,\dots,a_{n-1}\}$ of words such that for each $i \in \{0,\dots,n-1\}$, $T \wedge E \wedge I_{a_i} \not\leq M(a_i)$, and moreover, if $T' \leq T$ and $T' \wedge E \wedge I_{a_i} \not\leq M(a_i)$ holds for each $i \in \{0,\dots,n-1\}$ then there is a finite set Σ' of 9-good equations such that $T = \mathrm{Eq}(\Sigma \cup \Sigma') \vee T'$. The property just expressed can be formulated as a first-order formula, using the codes for finite sequences of equations and words.

It is trivial to see that if T has the above-expressed property then T is finitely axiomatizable—because T' can be taken to be a finitely generated theory. Now suppose that T is finitely axiomatizable. Thus T is generated by a finite set Σ of 9-good equations together with a finite set $\Phi = \{(a_0,b_0),\dots,(a_{n-1},b_{n-1})\}$ of 9-smooth equations. We can take $\Gamma = \{a_0,\dots,a_{n-1}\}$. It is clear that

$T \wedge E \wedge I_{a_i}$ includes $\mathrm{Eq}(a_i, b_i)$ and thus is not included in $M(a_i)$. Suppose that T' is a subtheory of T and for each $i \in \{0, \ldots, n-1\}$, $T' \wedge E \wedge I_{a_i} \not\leq M(a_i)$. Then for each i we can choose an equation $(a_i, c_i) \in T' \wedge E$ with $a_i < c_i$, and moreover we can choose them so that $|b_i| < |c_i|$. The equation (b_i, c_i) is either parallel or else, by Lemma 11.2, it is equivalent to a set of two 9-good equations. Thus there exists a set Σ' of 9-good equations (consisting of at most $2n$ equations) such that $\Sigma' \subset T$ and $T' \vee \mathrm{Eq}(\Sigma')$ includes the set Φ. Hence we have that $T = \mathrm{Eq}(\Sigma \cup \Sigma') \vee T'$. ∎

12. Reduction of 9-smooth equations

Call an equation (a, b) **exactly-9-smooth** if it is 9-smooth, $a = xry$ where $\{x, y\}$ is a two-element set of letters, and for all $c = \sigma(a)$ such that $(a, c) \in \mathrm{Eq}(a, b)$ and $a < c$, we have: $|\sigma(x)| = 1 = |\sigma(y)|$ and the equation (a, c) belongs neither to E_ℓ nor to E_r.

Call an equation (a, b) **left-amenable** if $a < b$, $|a| > 1$, a is unperfect, b is left-perfect, $(a, b) \in E \cap E_\ell$, and whenever $(a, c) \in \mathrm{Eq}(a, b)$ and $a < c$ then c is left-perfect. Call an equation **right-amenable** if the dual equation is left-amenable.

Throughout this section, where T denotes any theory, we write $g(T)$ to denote the theory generated by all the 9-good equations in T. Our investigation will lead us inevitably to introduce some rather complicated semi-definable relations between words, equations, and theories. (The general concept of semi-definable relation was rather formally defined in Section 3.) Obviously, the relation $\{(T, g(T)) : T \in \mathcal{L}\}$ is semi-definable. It should also be clear upon reflection that the set of exactly-9-smooth equations, the set of left-amenable equations, and the set of right-amenable equations, each is semi-definable.

Proposition 12.1. *Every 9-smooth equation is equivalent to a finite set of equations each of which is either 9-good, exactly-9-smooth, left-amenable or right -amenable.*

Proof. Let us assume that (a, b) is 9-smooth but $\mathrm{Eq}(a, b) > g(\mathrm{Eq}(a, b))$. Then $|a| > 1$ (else (a, b) is a power equation), and so $a = xry$ where the two-element set of letters $\{x, y\}$ is disjoint from $\mathrm{supp}(r)$.

We claim that if $(a, c) \in \mathrm{Eq}(a, b) \cap E_\ell$ and $a < c$, then c is left-perfect. Indeed, suppose not. Then (a, c) is right-regular. We can write $c = \sigma(a)$ where for all $z \in \mathrm{supp}(a) \setminus \{x\}$, we have $x \notin \mathrm{supp}(\sigma(z))$ and moreover, x occurs only as the initial letter in $\sigma(x)$. Then it follows that for all $n > 0$, the equation $(a, \sigma^n(a))$ is right-perfect. Since σ must map at least one letter in $\mathrm{supp}(a)$ to a word of length greater than one, we can choose n so that $d = \sigma^n(a)$ satisfies $|d| > |b|$. Now (a, b) is equivalent to (a, d) together with (b, d) and the latter equation is either parallel, or else is equivalent to a right-perfect together with a right-regular equation, by Lemma 11.2. Thus we would have $\mathrm{Eq}(a, b) = g(\mathrm{Eq}(a, b))$ after all, if the claim fails.

Now we have one of two cases: Either there is no $(a,c) \in \mathrm{Eq}(a,b)$, $a < c$, with (a,c) in E_ℓ or in E_r, and in this case we have that (a,b) is exactly-9-smooth by Lemma 9.3; or else there is such an $(a,c) \in \mathrm{Eq}(a,b)$, $a < c$, with (a,c) in E_ℓ or in E_r. So without loss of generality, we can assume that that we do have an equation $(a,c) \in \mathrm{Eq}(a,b) \cap E_\ell$, $a < c$. By the claim in the last paragraph, if $(a,e) \in \mathrm{Eq}(a,c)$ and $a < e$ then $(a,e) \in \mathrm{Eq}(a,b) \cap E_\ell$ and so e is left-perfect. Now (a,b) is equivalent to the left-perfect (b,c) together with the left-amenable (a,c). This concludes our proof. ∎

We shall now spend some time investigating the class of left-amenable equations. Our aim is to construct a semi-definable binary relation R with domain the set of left-amenable equations such that $R((a,b), \mathrm{Eq}(a,b))$ holds for every left-amenable (a,b) and moreover, for every such (a,b), $\{T : R((a,b),T)\}$ is a finite set.

Let (a,b) be any left-amenable equation. Recall from the first paragraphs of Section 6 that $\mathrm{Perm}(a)$ denotes the theory generated by all permutational equations $(a, \pi(a))$, and $M(a) = \mathrm{Perm}(a) \vee {I_a}^\star$ where ${I_a}^\star$ is the greatest ideal theory properly included in I_a. The relation $\{(a, M(a)) : a \in W\}$ is semi-definable by Corollary 6.8. We define $C(a,b)$ to be the set of all theories T obeying the following conditions:

(1) $g(T) = g(\mathrm{Eq}(a,b))$;
(2) $T \leq I_a \cap E \cap E_\ell$ and $T \not\leq M(a)$;
(3) If $T' \leq T$ and $T' \not\leq M(a)$ then $T = T' \vee g(\mathrm{Eq}(a,b))$.

Note that $\mathrm{Eq}(a,b) \in C(a,b)$. Moreover, the relation "$[T \in C(a,b)]\,\&\,[(a,b)$ is left-amenable$]$" between equations (a,b) and theories T is semi-definable.

For any word c put $T(c) = \mathrm{Eq}(a,c) \vee g(\mathrm{Eq}(a,b))$. Then define $O(a,b)$ to be the set of all words $c > a$ such that $T(c) \in C(a,b)$. ¿From condition (3) we have that

$$C(a,b) = \{T(c) : c \in O(a,b)\}\,.$$

The relation between an equation (p,q) and a word r that holds iff (p,q) is left-amenable and $r \in O(a,b)$ is a semi-definable relation. For $c \in O(a,b)$ we let $\Delta(c) = O(a,b) \cap c/\mathrm{Eq}(a,b)$. Since (a,b) is left-amenable, it is easy to see that if $c \in O(a,b)$ then c is left-perfect and $\Delta(c)$ is the set of all left-perfect words in $c/\mathrm{Eq}(a,b)$; also, $\Delta(c)$ is the set of words $d \in a/T(c)$ such that $d \not\sim a$.

Lemma 12.2. *Suppose that (a,b) is left-amenable, $\{c,v\} \subseteq O(a,b)$, $(u,v) \in T(c)$, and u is not left-perfect. Then (u,a) is permutational and the equation (u,v) is left-amenable.*

Proof. We write $u = \gamma(a)$ and $v = \lambda(a)$. Now if u is right-perfect, then (u,v) is semi-perfect and so must belong to $T(b)$ $(= \mathrm{Eq}(a,b))$ and to $T(v)$, and then (a,u) belongs to $T(v)$. Then since (a,u) is right-regular we will have $(a,u) \in \mathrm{Eq}(a,b)$ implying that $u \sim a$ since u is not left-perfect. But this is impossible since u is right-perfect and a is not. Thus u is unperfect. Similarly, if $\gamma(x)$ or $\gamma(y)$ is not a variable, where x,y are the initial and end letters of a, then we have an equation $(u,w) \in \mathrm{Eq}(a,b)$ with $|w| > |v|$ and (u,w) either left-regular or right-regular, but in this case $(u,w),(w,v)$ belong to $g(T(c))$ by Lemma 11.2 and hence again (u,v) belongs to $g(T(c))$ and to $T(v)$ and u must be similar to a, which certainly implies $|\gamma(x)| = |\gamma(y)| = 1$.

Thus we have established that u is unperfect and $\gamma(x) = x$ and $\gamma(y)$ is a letter.

Now if also $u \sim a$ then it is trivial to see that (u,v) is left-amenable. This lemma is true in that case. So we henceforth assume that u is not similar to a and argue for a contradiction.

If u and v are parallel, or if $v \le u$, then (Lemma 11.2), $(u,v) \in g(T(c))$ leading to the conclusion $u \sim a$ as above. Thus we have that $u < v$.

Let $m = |\operatorname{supp}(a)|$, $\operatorname{supp}(a) = \{x_1, \ldots, x_m\}$, and for any word w with $\operatorname{supp}(w) = \operatorname{supp}(a)$, let $t(w) = (n_1, \ldots, n_m)$ where n_i is the number of occurences of x_i in w. For $i \ge 1$ define $u_i = \gamma^i(a)$. Now we can choose $1 \le k < \ell$ such that $t(u_k) \le t(u_\ell)$, i.e., each x_i occurs at least as often in u_ℓ as in u_k. Since $a < \gamma(a)$ and $\operatorname{supp}(\gamma(a)) = \operatorname{supp}(a)$, it follows that $|u_k| < |u_\ell|$ and some x_i occurs more often in u_ℓ than in u_k. ¿From this together with $t(u_k) \le t(u_\ell)$ it follows that for every substitution ν, $|\nu(u_k)| < |\nu(u_\ell)|$.

Now if $1 \le i < j$ then (u_i, u_j) does not belong to $\mathrm{Eq}(a,b)$. For suppose that it is in $\mathrm{Eq}(a,b)$. Since (u_i,u_j) is right-regular, it belongs to $T(c)$. Thus $(\gamma^{i-1}\lambda(a), \gamma^{j-1}\lambda(a))$ belongs to $T(c)$, since the equation $(\lambda(a), \gamma(a))$ (i.e., (v,u)) belongs to $T(c)$. Since the equation $(\gamma^{i-1}\lambda(a), \gamma^{j-1}\lambda(a))$ is left-perfect, it belongs also to $T(v)$. Thus (u_{i-1}, u_{j-1}) belongs to $T(v)$ (since $(a, \lambda(a)) \in T(v)$), and hence $(u_{i-1}, u_{j-1}) \in \mathrm{Eq}(a,b)$. Continuing in this fashion, we derive $(a, u_{j-i}) \in \mathrm{Eq}(a,b)$ which, because $a < u_{j-i}$, contradicts our assumption that (a,b) is left-amenable.

Now the equation $(u_\ell, \gamma^{\ell-1}\lambda(a))$ which belongs to $T(c)$ does not belong to $g(T(c))$. Because if it did, then it would belong to $g(T(v))$ and hence $(u_\ell, u_{\ell-1})$ would belong to $T(v)$ and to $\mathrm{Eq}(a,b)$, which we proved cannot happen. Note that $(u_\ell, \gamma^{\ell-1}\lambda(a)) \notin g(T(c))$ implies that u_ℓ is unperfect (else this equation would be semi-perfect); by the same token, each word u_i, $i \ge 1$, is unperfect. Now it also follows from $(u_\ell, \gamma^{\ell-1}\lambda(a)) \notin g(T(c))$, by Lemma 11.2, that $u_\ell < \gamma^{\ell-1}\lambda(a)$. Since u_ℓ is unperfect, we have a substitution τ_1 such that

$$\tau_1(u_\ell) = \gamma^{\ell-1}\lambda(a) = r\,.$$

It follows from the above equality that for any word w with $\operatorname{supp}(w) = \operatorname{supp}(a)$ and $(a,w) \in E_\ell$ the word $\tau_1(w)$ is left-perfect. Now the equation $(r, \tau_1(u_{\ell-1}))$ belongs to $T(v)$ since $T(v)$ contains $(a, \lambda(a))$. The equation $(r, \tau_1(u_{\ell-1}))$ is left-perfect and so belongs to $T(c)$. Thus $(r, \tau_1(\gamma^{\ell-2}\lambda(a)))$ belongs to $T(c)$, and to $T(v)$ since this equation is left-perfect. (Recall that $(\gamma(a), \lambda(a)) \in T(c)$.) ¿From this it follows that $(r, \tau_1(u_{\ell-2}))$ belongs to $T(v)$, and to $T(c)$ since this equation is left-perfect.

By continually alternating back and forth in this way between $T(c)$ and $T(v)$, we find that $(r, \tau_1(u_k))$ belongs to $g(T(c))$. This means that also $(u_\ell, \tau_1(u_k))$ belongs to $T(c)$. It cannot belong to $g(T(c))$ for that would force $(u_\ell, r) \in g(T(c))$.

Now just as before, we can find a substitution τ_2 such that

$$\tau_2(u_\ell) = \tau_1(u_k) = r_1\,.$$

Note that we have

$$r_1 \equiv_{T(c)} u_\ell \equiv_{T(c)} r\,.$$

Just as before, we find that $(r_1, \tau_2(u_k))$ belongs to $g(T(c))$ and $(u_\ell, \tau_2(u_k))$ belongs to $T(c)$. We cannot have in addition $(u_\ell, \tau_2(u_k)) \in g(T(c))$ because this would put (u_ℓ, r) in $g(T(c))$.

These arguments generate a sequence τ_i of substitutions such that for all i,

$$\tau_{i+1}(u_\ell) = \tau_i(u_k)\,.$$

Now recall that by our choice of k and ℓ, the above equations imply that

$$|\tau_{i+1}(u_k)| < |\tau_i(u_k)|$$

for all i. This absurdity finishes our proof that $u \sim a$. ∎

Corollary 12.3. *Suppose that (a,b) is left-amenable.*

(1) *For $c, d \in O(a,b)$ and $u \not\sim a$ we have $u \in \Delta(c)$ iff $(u,c) \in T(c)$ iff $(u,c) \in T(d)$ iff $(u,c) \in \mathrm{Eq}(a,b)$ and these equivalent formulas imply that u is left-perfect.*

(2) *For all theories $T \in C(a,b)$, $T \cap O(a,b)^2 = \mathrm{Eq}(a,b) \cap O(a,b)^2$ is an equivalence relation whose classes are the sets $\Delta(c)$, $c \in O(a,b)$. Moreover, if $v \in O(a,b)$, $(u,v) \in T$, and $u \not\sim a$ then $u \in O(a,b)$.*

Proof. Easy, using the preceeding lemma. ∎

We now need another definition. For $c, c' \in O(a,b)$ write $\Delta(c) \sim \Delta(c')$ to mean that for some permutational substitution π we have $\pi(c) \in \Delta(c')$. Note that for a permutational substitution π, the formula $\pi(c) \in \Delta(c')$ is equivalent to $\pi(\Delta(c)) = \Delta(c')$. For $T(c), T(c') \in C(a,b)$ write $T(c) \sim T(c')$ iff $\Delta(c) \sim \Delta(c')$. Thus we have defined an equivalence relation on $C(a,b)$. In order to show that the relation $S((p,q),T,T')$ that holds iff (p,q) is left-amenable, $\{T,T'\} \subseteq C(p,q)$ and $T \sim T'$ is semi-definable, we need two preparatory lemmas. The following definition is helpful. $\Pi'(a,b)$ is the set of all permutational substitutions π such that $\pi(z) = z$ for all $z \notin \mathrm{supp}(a)$ and $\pi(\Delta(c)) = \Delta(d) \neq \Delta(c)$ for some $c, d \in O(a,b)$.

Lemma 12.4. *Let (a,b) be left-amenable and suppose that $\pi \in \Pi'(a,b)$. Let $(u,v) = (r\gamma(a)s, r\gamma\pi(a)s)$ for some possibly empty words r, s and some substitution γ. Then if $r \neq \emptyset$ or $s \neq \emptyset$ or if $\gamma(a)$ is left-perfect (especially if $\gamma(a) \in O(a,b)$) it follows that $(u,v) \in g(\mathrm{Eq}(a,b))$.*

Proof. Choose $c, d \in O(a,b)$ so that $\pi(c) = d$. Let $u_1 = r\gamma(d)s$. Note that $\pi(x) = x$ where x is the left-most variable of a. Assume that $r \neq \emptyset$ or $s \neq \emptyset$ or $\gamma(a)$ is left-perfect, as well as the other hypotheses of this lemma. Then we have that (u, u_1), (u_1, v) are both right-regular, both left-regular, or both left-perfect. Moreover, $(u, u_1) \in T(d)$ and $(u_1, v) \in T(c)$. The lemma follows from these observations. ∎

Lemma 12.5. *Let (a,b) be left-amenable and suppose that $\pi \in \Pi'(a,b)$. Let $c \in O(a,b)$ and put $U = T(c) \vee \mathrm{Eq}(a,\pi(a))$. Then if $u \in O(a,b)$ and $(a,u) \in U \setminus T(c)$ it follows that $(\rho(a),u) \in T(c)$ for some permutational substitution ρ.*

Proof. From Lemma 12.4, we have that if (e,f) is immediately derived from $(a,\pi(a))$ and does not belong to $g(T(c))$, then (e,f) is either $(\gamma(a),\gamma\pi(a))$ or $(\gamma\pi(a),\gamma(a))$ where $\gamma(a)$ is left-unperfect. Assume that $(a,u) \in U \setminus T(c)$ and $u \in O(a,b)$. Then there is a sequence of words $u = u_0,\dots,u_n = a$ such that each (u_i,u_{i+1}) either belongs to $T(c)$ or is immediately derived from $(a,\pi(a))$. We can take such a sequence with n minimal. Then for the first i $(= 0$ or $1)$ such that (u_i,u_{i+1}) is immediately derivable from $(a,\pi(a))$, it follows that $(u_i,u) \in T(c)$ and u_i is left-unperfect. The desired conclusion follows by Lemma 12.2. ∎

Lemma 12.6. *The relation $S((p,q),T,T')$ is semi-definable. In fact, for left-amenable (a,b) and $T,T' \in C(a,b)$ we have $T \sim T'$ iff either $T = T'$ or there is some $\pi \in \Pi'(a,b)$ such that $T \vee \mathrm{Eq}(a,\pi(a)) = T' \vee \mathrm{Eq}(a,\pi(a)) = T \vee T'$.*

Proof. Let $T,T' \in C(a,b)$ and suppose first that we have $\rho \in \Pi'(a,b)$ with $T \vee \mathrm{Eq}(a,\rho(a)) = T' \vee \mathrm{Eq}(a,\rho(a))$. We can write $T = T(c)$ and $T' = T(d)$ for some $c,d \in O(a,b)$. By Lemma 12.5, since $(a,d) \in T(c) \vee \mathrm{Eq}(a,\rho(a))$, it follows that $(\pi(a),d) \in T(c)$ for some permutational π. Then $(a,\pi^{-1}(d)) \in T(c)$ and it follows that $\pi^{-1}(d) \in \Delta(c)$ since $\pi^{-1}(d)$ is left-perfect. So we do have $T \sim T'$.

Now suppose that $T \sim T'$ and $T \neq T'$. Then we can write $T = T(c)$ and $T' = T(d)$ where $d = \pi(c)$ for some $\pi \in \Pi'(a,b)$ and $c,d \in O(a,b)$. Since $T = \mathrm{Eq}(a,c) \vee g(\mathrm{Eq}(a,b))$ and $T' = \mathrm{Eq}(a,d) \vee g(\mathrm{Eq}(a,b))$ and clearly

$$\mathrm{Eq}(a,c) \vee \mathrm{Eq}(a,\pi(a)) = \mathrm{Eq}(a,d) \vee \mathrm{Eq}(a,\pi(a)) = \mathrm{Eq}(a,c) \vee \mathrm{Eq}(a,d)\,,$$

then we have $T \vee \mathrm{Eq}(a,\pi(a)) = T' \vee \mathrm{Eq}(a,\pi(a)) = T \vee T'$. ∎

Lemma 12.7. *Suppose that (a,b) is left-amenable and $\Pi'(a,b) \neq \emptyset$. Then $T \in C(a,b)$ satisfies $T \sim \mathrm{Eq}(a,b)$ iff $\mathrm{Eq}(a,\pi(a)) \leq T \vee \mathrm{Eq}(c,\pi(c))$ for some $c \in O(a,b)$ such that $c \sim b$ and for all (or for some) $\pi \in \Pi'(a,b)$.*

Proof. Let $\pi \in \Pi'(a,b)$. Assume first that $T \sim \mathrm{Eq}(a,b)$. Thus $T = T(c)$ for some $c \sim b$. Clearly $\mathrm{Eq}(a,\pi(a) \leq T \vee \mathrm{Eq}(c,\pi(c))$.

For the converse implication, suppose that $T = T(d)$, $d \in O(a,b)$, and we have

$$\mathrm{Eq}(a,\pi(a)) \leq T \vee \mathrm{Eq}(c,\pi(c))$$

where $c = \rho(b) \in O(a,b)$, ρ a permutational substitution. Note that $(a,\pi(a)) \notin T$, i.e., $(a,\pi(a)) \notin g(T)$, because $\pi(e) \notin \Delta(e)$ for some $e \in O(a,b)$. Now by arguing analogously to the proof of Lemma 12.5, we conclude that T contains an equation $(a,\gamma(b))$ (i.e., $(a,\lambda\rho(b))$ or $(a,\lambda\pi\rho(b))$) where $\gamma(a)$ is left-unperfect. Since $\gamma(b)$ is left-perfect, it follows that $\gamma(b) \in \Delta(d) \subseteq O(a,b)$. And we have $(u,v) = (\gamma(a),\gamma(b)) \in T(b)$. Then from Lemma 12.2 or Corollary 12.3, it follows that $\gamma|_{\mathrm{supp}(a)}$ is a permutation, so we can assume that γ is a permutation with $(a,\gamma(b)) \in T$. Now it follows from our definitions that $T \sim \mathrm{Eq}(a,b)$. ∎

The above lemma shows that if $\sim$ on $C(a,b)$ is not the identity relation, then the finite set $\{T \in C(a,b) : T \sim \mathrm{Eq}(a,b)\}$ is semi-definable from (a,b). Our next lemmas show that if $\sim$ on $C(a,b)$ is the identity relation, then either $\{\mathrm{Eq}(a,b)\}$ is semi-definable from (a,b) or else $C(a,b)$ is a two-element set of theories. Thus in every event, $\mathrm{Eq}(a,b)$ belongs to a finite set semi-definable from (a,b).

Lemma 12.8. *Let (a,b) be left-amenable and $c,d \in O(a,b)$. If $(u,v) = (r\gamma(c)s, r\gamma(d)s)$ and either $r \neq \emptyset$ or $s \neq \emptyset$ or $\gamma(a)$ is left-perfect then $(u,v) \in g(\mathrm{Eq}(a,b))$.*

Proof. The proof is entirely analogous to the proof of Lemma 12.4, and we omit it. ∎

Lemma 12.9. *Suppose that (a,b) is left-amenable and $\Pi'(a,b) = \emptyset$. Let $c,d \in O(a,b)$ and $\{T,T'\}$ be a two-element subset of $C(a,b)$. Then we have $T \vee \mathrm{Eq}(c,d) = T' \vee \mathrm{Eq}(c,d)$ iff $\{T,T'\} = \{T(c),T(d)\}$.*

Proof. We remark that $\mathrm{Eq}(c,d)$ is left-perfect, so this lemma furnishes a semi-definition, relative to (a,b), of the relation "$\{T,T'\} = \{T(c),T(d)\} \,\&\, T \neq T'$."

Assume that $T \vee \mathrm{Eq}(c,d) = T' \vee \mathrm{Eq}(c,d)$. Then write $T = T(e), T' = T(f)$ where $e,f \in O(a,b)$ and of course $\Delta(e) \neq \Delta(f)$. Let $a = u_0, u_1, \ldots, u_n = v$ be a shortest sequence of terms such that $v \in \Delta(f)$ and for each $i < n$, either $(u_i,u_{i+1}) \in T$ or (u_i,u_{i+1}) is immediately derived from (c,d).

Since $(a,v) \notin T$ then we have $(a,u_1) \in T$ and (u_1,u_2) is immediately derived from (c,d), but $(u_1,u_2) \notin T$. Now it follows from Lemma 12.8 that $u_1 \in \{\gamma(c),\gamma(d)\}$ for some γ such that $\gamma(a)$ is left-unperfect. Since u_1 is thus left-perfect, we have $u_1 \in \Delta(e)$. Moreover, $(u_1,\gamma(a))$ belongs either to $T(c)$ or to $T(d)$. Now by Lemma 12.2 we have that $\gamma(a) \sim a$, implying that $\gamma|_{\mathrm{supp}(a)}$ is a permutation, and that u_1 is similar to c or to d. Since $u_1,c,d \in O(a,b)$ and $\Pi'(a,b) = \emptyset$, it follows that $\Delta(u_1) = \Delta(c)$ or $\Delta(u_1) = \Delta(d)$, i.e., that $T = T(c)$ of $T = T(d)$. ∎

Lemma 12.10. *Suppose that (a,b) is left-amenable with $\Pi'(a,b) = \emptyset$ and $|C(a,b)| \neq 2$. Then $\mathrm{Eq}(a,b)$ is the unique theory $T \in C(a,b)$ such that for all $c \in O(a,b)$ with $(b,c) \notin \mathrm{Eq}(a,b)$ there exists a $T' \in C(a,b)$, $T' \neq T$, with $T \vee \mathrm{Eq}(b,c) = T' \vee \mathrm{Eq}(b,c)$.*

Proof. This is a consequence of Lemma 12.9. ∎

We now define a left-amenable equation (a,b) to be of type I just in case $\Pi'(a,b) \neq \emptyset$; to be of type II iff $\Pi'(a,b) = \emptyset$ and $|C(a,b)| = 2$; and to be of type III if it is neither of type I or of type II. We define $R((a,b),T)$ to hold iff (a,b) is left-amenable, and either:

$$(a,b) \text{ has type I and } T \in C(a,b) \text{ and } T \sim \mathrm{Eq}(a,b), \text{ or}$$

$$(a,b) \text{ has type II and } T \in C(a,b), \text{ or}$$

$$(a,b) \text{ has type III and } T = \mathrm{Eq}(a,b)\,.$$

It follows from Lemmas 12.7 and 12.10 that the relation R is semi-definable. To finally conclude that the set of left-amenable equations is good, we will have to find a way to single out $\mathrm{Eq}(a,b)$ from among the finite set of theories T satisfying $R((a,b),T)$.

13. Conclusion

It should be clear that if the set of all equations is good then the results obtained in Part III of [2] for universal algebras would also hold in the lattice of equational theories of semigroups, namely:

(1) The set of one-based equational theories of semigroups is definable in $\mathcal{L}$.
(2) The set of finitely axiomatizable equational theories of semigroups is definable in $\mathcal{L}$.
(3) The identity and the duality (the mapping $T \mapsto T^{\partial}$) are the only two automorphisms of $\mathcal{L}$.
(4) Every finitely axiomatizable equational theory of semigroups is an element definable up to duality in the lattice $\mathcal{L}$.

We hope that by combining the results of the present paper together with appropriate techniques from the combinatorial theory of semigroups, it will be possible to achieve this goal. All that remains is to finish the work begun in Section 12 of showing that the set of 9-smooth equations is good.

We remark that we have been able to prove that the set of all equations in three letters is good.

References

1 Iskander, A. A., *Coverings in the lattice of varieties*, Colloquia Mathematica Societatis János Bolyai **17**. North-Holland, Amsterdam, 1977, pp. 189–203.

2 Ježek, J., *The lattice of equational theories*
Part I: *Modular elements*, Czech. Math. J. **31** (1981), 127–152;
Part II: *The lattice of full sets of terms*, Czech. Math. J. **31** (1981), 573–603;
Part III: *Definability and automorphisms*, Czech. Math. J. **32** (1982), 129–164;
Part IV: *Equational theories of finite algebras*, Czech. Math. J. **36** (1986), 331–341.

3 McKenzie, R., *Definability in lattices of equational theories*, Annals of Math. Logic **3** (1971), 197–237.

Department of Mathematics, University of Hawaii, Honolulu, Hawaii 96822
Department of Mathematics, University of California, Berkeley, California 94720

Received ??and in final form ??