J. Symbolic Computation (2011) **11**, 1–17

PERFECT BASES FOR EQUATIONAL THEORIES

JAROSLAV JEŽEK AND GEORGE F. McNULTY

Charles University, Prague, Czech Republic
Department of Mathematics, University of South Carolina, USA

(Received 26 May 1994)

Perfect bases for equational theories are closely related to confluent and finitely terminating term rewrite systems. The two classes have a large overlap, but neither contains the other. The class of perfect bases is recursive. We also investigate a common generalization of both concepts; we call these more general bases normal, and touch the question of their uniqueness. We also give numerous examples.

1. Introduction and preliminaries

Perhaps the most broadly discussed question of equational logic is to find ways to decide which equations are consequences of a given finite set of equations, that is, to establish decidability of a given finitely based equational theory. This question, which attracts attention of both mathematicians and computer scientists working in equational logic, is undecidable in general, so attention has been focused on special cases, as general as possible, for which there is hope of finding an algorithm. Evans (1951) and Knuth and Bendix (1970) introduced the technique of term rewriting, which has been further developed in a large number of papers; see Dershowitz and Jouannaud (1990) for a nice overview of term rewriting and for an extensive bibliography. In this paper we present an alternative technique, that of perfect bases.

In seeking positive solutions to the decision problem for an equational theory, the standard method is to find a computable normal form function. By a **normal form function** for an equational theory E we mean a mapping ν of the set of terms into itself, satisfying the following three conditions:

(nf 1) $u \approx v \in E$ if and only if $\nu(u) = \nu(v)$;
(nf 2) $t \approx \nu(t) \in E$ for all terms t;
(nf 3) $\nu(\nu(t)) = \nu(t)$ for all terms t.

An equational theory E is decidable if and only if it has a computable normal form function.

Term rewriting systems and the normal form functions associated with them take their inspiration from a complete syntactical notion of proof for equational logic (or, to frame this more algebraically, from a general scheme for generating fully invariant congruence relations on the absolutely free term algebra). In the fortunate circumstance

0747–7171/90/000000 + 00 $03.00/0

that a convergent set of rewrite rules can be found, proofs of equations take on a very simple character, leading to a computable normal form function.

The technique of perfect bases, which we introduce in this paper, relies on a different, though related insight. A normal form function maps the set of all terms onto a subset, the set of normal forms. The normal form function can be made into a homomorphism from the absolutely free term algebra onto another algebra, whose underlying universe is the set of normal forms, by the simple expedient of defining the fundamental operations on the algebra of normal forms in the natural way. In the event that the homomorphism fixes each variable, the resulting algebra will then be freely generated by the set of variables relative to the equational theory (since the condition (nf1) asserts that the kernel of this homomorphism will be the equational theory). We are interested in reversing the process just described. We present a general scheme, which given a set of equations, subject to some restrictions, will produce a map from the set of terms into the set of terms. In the fortunate circumstance that the set of equations is perfect, the resulting map will be a homomorphism onto the algebra free relative to the perfect set, and will also satisfy (nf3). It will be a normal form function.

Both the technique of term rewriting and the technique of perfect bases begin with a set P of equations and use P in the attempt to build a normal form function. In each case, when the process is successful, the normal forms turn out to be precisely those terms which avoid all the terms occurring as left sides of equations belonging to P. We say a term u **avoids** a term t provided no substitution instance of t is a subterm of u. Thus, regarding P as a set of rewrite rules, the normal forms turn out to be exactly thoses terms to which no rewrite rule in P applies.

Classically, examples of normal form functions were obtained for Boolean algebra (Boole 1847), for group theory (Dehn 1911), and for lattice theory (Whitman 1941). General accounts of the method of normal forms can be found in Evans (1951) and Pigozzi (1979) and, of course, in the literature on term rewriting, cf. Dershowitz and Jouannaud (1990). Whitman's normal form function for lattice theory is both efficient and elegant, while (cf. Freese, Ježek, and Nation 1993) there is no finite convergent term rewrite system for lattice theory. Neither do our results here about perfect bases provide a substitute for Whitman's algorithm. Other examples of decidable equational theories without a convergent rewrite system can also be found in Kapur and Narendran (1985) and Squier and Otto (1987). Example 2.10 below provides an equational theory with a finite perfect base (so this equational theory is decidable), but which has not finite convergent term rewrite system.

Let us illustrate both the technique of term rewriting and the technique of perfect bases on a simple example.

Consider the equational theory of groupoids based on the equation $x(x(xx)) \approx (xx)x$, and denote this equation by e. For two terms u and v, write $u \to v$ if u can be rewritten to v in one step on the basis of e, i.e., if v results from u by replacing one arbitrary subterm $t(t(tt))$ (where t is a term) with $(tt)t$. One can easily see that the rewrite system based on e is finitely terminating and confluent, by which we mean that for any term w there is a term $\nu(w)$ such that any sequence $w = w_0 \to w_1 \to \cdots$ is finite, and terminates at $\nu(w)$. (It is sufficient to verify that the rewrite system is finitely terminating and locally confluent in the sense that whenever $w \to u$ and $w \to v$, then there are finite sequences $u \to u_1 \to \cdots \to u_k$ and $v \to v_1 \to \cdots \to v_l$ with $u_k = v_l$.) The mapping ν is then a computable normal form function, and an equation $u \approx v$ is a consequence of e if and only if $\nu(u) = \nu(v)$.

The equation $(xx)x \approx x(x(xx))$ (let us denote it by e^*), is, of course, a base for the same equational theory. While ν always computed the shortest term in its class, it is clear that the normal form function ν^* based on e^* would, on the contrary, always compute the longest term, if this rewrite system is also confluent and finitely terminating. It turns out that it is, but a direct proof of finite termination could be awkward. Instead of trying to give such a proof, let us proceed in the following way. Denote by A the set of the terms that do not contain a subterm of the form $(tt)t$ (for any term t), and define a binary operation $\circ$ on A by

$$u \circ v = \begin{cases} uv & \text{if the term } uv \text{ belongs to } A, \\ v(v(vv)) & \text{if } u = vv. \end{cases}$$

One must verify that this is a correct definition of a binary operation, in which case we say that the base e^* is pre-perfect. The next step is to prove that the resulting groupoid with the underlying set A satisfies the equation e; then we say that the base is perfect. According to Theorem 2.2 below, this is sufficient to claim that the (unique) homomorphism of the term algebra onto the groupoid $(A, \circ)$ which is identical on variables, is a computable normal form function for E.

It is conceivable that the process of verifying the perfection of a given base is not computable, because it requires checking that the equations are satisfied in an infinite algebra. But we shall show (see Theorem 2.4 below) that this can be done in a finite time and, actually, the technique of perfect bases is more algorithmic than that of term rewriting, as the class of perfect bases is recursive, while that of finitely terminating confluent bases is not. The tools used to check the perfection of a set of equations are familiar from unification theory.

The two classes, of perfect bases and of finitely terminating confluent ones, have a large overlap, but neither contains the other. The equation $(xy)z \approx x(yz)$, which is a base for the equational theory of semigroups, is finitely terminating and confluent, but is not perfect. On the other hand, there are examples, admittedly not as natural as the associative law, of perfect bases that are not finitely terminating; see Examples 2.9 and 2.10 below. Due to its simplicity and algorithmicity, perfect bases should serve as a useful technique for decidability of a finitely based equational theory, and as the first choice technique if the finite base is in some sense random. For example, this technique was used in Ježek (1982) to establish decidability of nearly any equational theory of groupoids, based on a single equation $t \approx x$ where x is a variable and t is a term of length at most four; the only exceptional equation in this class, for which the problem of decidability remains open, is the equation $y((yx)y) \approx x$. Also, as the above given example shows, this technique is more suitable than that of term rewriting for various special purposes, like if one needs to decide whether a certain finitely based equational theory E is term finite (i.e., each term is equivalent to only a finite number of terms modulo E): in that case one needs to find a normal form function making terms longer, rather than shorter.

We also investigate a common generalization of both techniques. We call these more general bases normal, as they also provide for a computable normal form function. The idea is that the normal form function ν should be computable according to the following recursive definition:

$$\nu(t) = \begin{cases} F(\nu(t_1), \cdots, \nu(t_n)) & \text{if this term belongs to } A, \\ \nu f(u') & \text{if } F(\nu(t_1), \cdots, \nu(t_n)) = f(u) \text{ for a substitution } f \\ & \quad \text{and an equation } u \approx u' \text{ from the normal base.} \end{cases}$$

Here $t = F(t_1, \cdots, t_n)$ is an arbitrary term and A denotes the set of the terms that do not contain any substitution instance of a left side of an equation from the base. We will touch the question of uniqueness of a normal base for an equational theory in some particular cases.

Preliminaries

For the basics of equational logic the reader is referred to either McNulty (1992) or Taylor (1979), and for the basic facts of general algebra to McKenzie, McNulty and Taylor (1987).

All terms that we are going to deal with will be of a given fixed similarity type, which we assume to be finite. A typical operation symbol will be denoted by F, and its arity by n. The set of variables, from which the terms are built up, is assumed to be countably infinite. The **support** of a term t, i.e., the set of variables occurring in t, will be denoted by $\boldsymbol{S}(t)$. The set of all terms can be made an algebra in a natural way, the **algebra of terms**.

Equations are simply ordered pairs of terms, but an equation (u, v) will be more naturally denoted by $u \approx v$ to emphasize its semantical intent and by $u \to v$ in the context of rewriting. In this last context, equations are also referred to as **rewrite rules**. An **equational theory** is a set of equations which is closed with respect to logical consequences; equivalently, an equational theory is a fully invariant congruence of the term algebra. A set B of equations is called a **base** for an equational theory E, provided E is the set of all equations that are consequences of B. An equational theory with a finite base is said to be **finitely based**.

A **substitution** can be most easily defined as an endomorphism of the term algebra. Clearly, every substitution is uniquely determined by its restriction to the set of variables.

A **unifying pair** for a pair a, b of terms is a pair f, g of substitutions such that $f(a) = g(b)$; such a unifying pair is **minimal** if any other unifying pair for a, b is of the form hf, hg, for some substitution h. A minimal unifying pair is almost uniquely determined by the pair a, b. It is well known that it exists whenever some unifying pair for a, b exists. There is an algorithm deciding whether any given pair of terms has a unifying pair, and producing a minimal one if it has.

A substitution f is said to **expand** a substitution h if $f = gh$ for some substitution g. If a finite nonempty set S of substitutions has a common expansion (a substitution expanding all the substitutions in S), then it has a **minimal common expansion**, i.e., a common expansion f such that all common expansions of S are expansions of f. This follows easily (technical details may be complicated) from the existence of minimal unifying pairs. Also, there is an algorithm deciding for any finite set of finitary substitutions whether it has a common expansion, and producing a minimal one if it has. Instead of specifying what we mean by a finitary substitution, let us say that in a given context we are always interested in the behavior of substitutions on a given finite set X of variables only, so that in the given context any two substitutions coinciding on X can be identified. (However, we cannot say, for example, that a finitary substitution is one which fixes all but finitely many variables, because the minimal common expansion of finitary substitutions would not then necessarily be finitary according to that definition. Also, we cannot simply restrict the set of all variables to a finite set, because then minimal unifying pairs and minimal common expansions would not necessarily exist when they should exist.)

By an **elementary lift** we mean a mapping

$$L(t) = F(u_1, \cdots, u_{i-1}, t, u_{i+1}, \cdots, u_n)$$

where F is an operation symbol of some arity n, $i \in \{1, \cdots, n\}$, and u_j is a fixed term for each $j \leq n$ with $j \neq i$. A composition of a finite (possibly empty) sequence of elementary lifts is called a **lift**. A term s is said to be a **subterm** of a term t if $t = L(s)$ for a lift L; we then write $s \subseteq t$.

Given two terms u and v, we write $u \leq v$ and say that v **encompasses** u if $v = Lf(u)$ for some lift L and some substitution f. This is a quasiordering on the set of terms. When v does not encompass u, we say that v **avoids** u. Two terms u and v are called (**literally**) **similar** if $u \leq v$ and $v \leq u$; we then write $u \sim v$. Also, $u \sim v$ if and only if $v = \alpha(u)$ for an automorphism α of the term algebra. Factored through this equivalence, the set of terms becomes a partially ordered set, every principal ideal of which is finite. (A principal ideal in a partially ordered set is a subset of the form $\{p : p \leq q\}$ for some fixed q.) We write $u < v$ if $u \leq v$ but $u \not\sim v$. Two terms u, v are called **incomparable** if $u \not\leq v$ and $v \not\leq u$. Two equations $u \approx v$ and $p \approx q$ are called **similar** if there is an automorphism α of the term algebra with $p = \alpha(u)$ and $q = \alpha(v)$. Two sets S_1 and S_2 of equations are called similar if each equation from S_1 is similar to an equation from S_2, and vice versa.

An equational theory E is said to be **term finite** if for any term t, the set $\{u : t \approx u \in E\}$ is finite. For example, the equational theory of commutative semigroups is term finite. The paper Ježek and McNulty (1994), whose contents can be detected from its title, contains results that are all relative to a given term finite equational theory. In a similar way, it should be possible to state most definitions and results of the present paper relative to a term finite equational theory; however, we have not pursued this task.

2. Perfect bases

Let P be a set of equations. We denote by A_P the set of all terms t such that whenever $u \approx u' \in P$, then $u \not\leq t$. So A_P consists of all those terms which avoid the left sides of equations in P.

P is said to be **pre-perfect** if the following conditions are satisfied:

(pp1) P is inter-reduced, which means that if $u \approx u' \in P$, $v \approx v' \in P$ and $(u, u') \neq (v, v')$, then $u \not\leq v$;
(pp2) if $u \approx u' \in P$, $v \approx v' \in P$ and $f(u) = g(v)$ for two substitutions f, g such that every proper subterm of $f(u)$ belongs to A_P, then $f(u') = g(v')$;
(pp3) if $u \approx u' \in P$ and f is a substitution such that every proper subterm of $f(u)$ belongs to A_P, then $f(u') \in A_P$.

If P is a pre-perfect set of equations, then we can define a mapping ν_P of the set of terms into A_P as follows:

$$\begin{aligned} \nu_P(x) &= x \text{ for any variable } x; \\ \nu_P(F(t_1, \cdots, t_n)) &= \begin{cases} F(\nu_P(t_1), \cdots, \nu_P(t_n)) & \text{if this term belongs to } A_P; \\ f(u') & \text{if } F(\nu_P(t_1), \cdots, \nu_P(t_n)) = f(u) \text{ for a substitution } f \text{ and } u \approx u' \in P. \end{cases} \end{aligned}$$

In fact, the three conditions above are just a formulation of the correctness of this definition plus a little bit more; since the terms $\nu_P(t_i)$ belong to A_P, we do not have to consider the case $F(\nu_P(t_1), \cdots, \nu_P(t_n)) = Lf(u)$ where L is a nontrivial lift.

If P is a pre-perfect set of equations, we can form an algebra $\mathbf{A} = \mathbf{A}_P$ with the underlying set A_P by interpreting each basic operation symbol F by the operation $F_{\mathbf{A}}$ defined as follows:

$$F_{\mathbf{A}}(t_1, \cdots, t_n) = \nu_P(F(t_1, \cdots, t_n)),$$

where n is the rank of F.

LEMMA 2.1. *Let P be a pre-perfect set of equations. Then:*

(1) *If $u \approx u' \in P$, then u is not a variable, $u' = \nu_P(u)$ and $\boldsymbol{S}(u') \subseteq \boldsymbol{S}(u)$;*
(2) *ν_P is a homomorphism of the term algebra onto $\mathbf{A}_P$.*

PROOF. (1) Let $u \approx u' \in P$. By (pp1), every proper subterm of u belongs to A_P, so that condition (pp3) with respect to the identical substitution says that $u' \in A_P$. In particular, A_P is nonempty; but then u cannot be a variable. It is easy to see that $u' = \nu_P(u)$. Suppose that there is a variable $y \in \boldsymbol{S}(u') - \boldsymbol{S}(u)$. Let f be the identical substitution, and g be the substitution with $g(x) = x$ for any variable $x \neq y$, and $g(y) = x$. We have $f(u) = g(u) = u$ but $f(u') \neq g(u')$, a contradiction with (pp2).

(2) We need to prove $\nu_P F(t_1, \cdots, t_n) = F_A(\nu_P(t_1), \cdots, \nu_P(t_n))$, i.e.,

$$\nu_P F(t_1, \cdots, t_n) = \nu_P F(\nu_P(t_1), \cdots, \nu_P(t_n)).$$

If $F(\nu_P(t_1), \cdots, \nu_P(t_n)) \in A_P$, then both sides are equal to this term. If, on the contrary, this term is of the form $f(u)$ for a substitution f and an equation $u \approx u' \in P$, then both sides are equal to $f(u')$ according to the definition of ν_P. □

By a **perfect base** we mean a pre-perfect set P of equations such that the algebra $\mathbf{A}_P$ satisfies all the equations from P. A subset P of an equational theory E is a perfect base for E if and only if it is pre-perfect and the algebra $\mathbf{A}_P$ satisfies all the equations from E.

THEOREM 2.2. *Let P be a perfect base for E. Then:*

(1) *ν_P is a normal form function for E;*
(2) *$\mathbf{A}_P$ is the free E-algebra over the set of variables;*
(3) *E is decidable if P is recursive, with recursive domain.*

PROOF. (nf 2) is easy by induction on the complexity of t, and (nf 3) is clear. By Lemma 2.1, ν_P is a homomorphism of the term algebra onto $\mathbf{A}_P$. So, if $u \approx v \in E$, then $\nu_P(u) = \nu_P(v)$, because $\mathbf{A}_P$ satisfies all the equations from E. The converse follows from (nf 2), so we have both implications of (nf 1). By the Homomorphism Theorem, it follows that $\mathbf{A}_P$ is isomorphic to the factor of the term algebra through E, and hence $\mathbf{A}_P$ is the free E-algebra over the set of variables. (3) follows from (1). □

LEMMA 2.3. *The set of the finite pre-perfect sets of equations is recursive.*

PROOF. Condition (pp1) is easy to verify, and we can also easily verify that $u \approx u' \in P$ implies $\boldsymbol{S}(u') \subseteq \boldsymbol{S}(u)$, which is necessary according to Lemma 2.1. Under this assumption, conditions (pp2) and (pp3) can be equivalently reformulated in the following way:

(pp2′) if $u \approx u' \in P$, $v \approx v' \in P$, and f and g is the minimal unifying pair for u and v, then, in case that every proper subterm of $f(u)$ belongs to A_P, $f(u') = g(v')$;
(pp3′) if $u \approx u' \in P$, $v \approx v' \in P$, $s \subseteq u'$, and f and g is the minimal unifying pair for s and v, then $f(u)$ contains a proper subterm not in A_P.

The equivalence of (pp2) with (pp2′) is easy, and clearly (pp3) implies (pp3′). It remains to prove that (pp3′) implies (pp3). Let $u \approx u' \in P$ and let f be a substitution such that every proper subterm of $f(u)$ belongs to A_P. Suppose $f(u') \notin A_P$, i.e., $g(v) \subseteq f(u')$ for a substitution g and an equation $v \approx v' \in P$. If $x \in \boldsymbol{S}(u')$, then $x \in \boldsymbol{S}(u') \subseteq \boldsymbol{S}(u)$, $f(x)$ is a proper subterm of $f(u)$ and so, by our assumption, $g(v)$ cannot be a subterm of $f(x)$. The only other possibility for $g(v)$ to be a subterm of $f(u')$ is, that $g(v) = f(s)$ for a subterm s of u'. Let f_0, g_0 be the minimal unifying pair for s and v, so that $f = hf_0$ and $g = hg_0$ for some h. By (pp3′), $f_0(u)$ contains a proper subterm not in A_P. But then clearly $f(u) = hf_0(u)$ also contains a proper subterm not in A_P, a contradiction. □

Let P be a finite pre-perfect set and let $a \approx b$ be an equation from P. We want to decide if the algebra $\mathbf{A}_P$ satisfies $a \approx b$. For this purpose we shall construct a finite set of substitutions which will serve as a test set. By a **permissible substitution** we shall mean one which maps variables into A_P. All our testing substitutions will be permissible. Observe that if gh is a permissible substitution, then h is also permissible, because the complement of A_P is closed under any substitution.

By induction on the complexity of a term t, we are first going to define a finite set $U(t)$ of permissible substitutions with the following property: if $f = gh$ where f is a permissible substitution, and f and h expand precisely the same substitutions from $U(t)$, then

$$\nu_P f(t) = g\nu_P h(t).$$

If t is a variable, let $U(t)$ consist of a single substitution, the identical one. For $f = gh$ as above, clearly both $\nu_P f(t)$ and $g\nu_P h(t)$ are equal $f(t)$.

Now let $t = F(t_1, \cdots, t_n)$. Put $U_0 = U(t_1) \cup \cdots \cup U(t_n)$. Consider an arbitrary nonempty subset S of U_0 which has a common expansion, and let f_S be the minimal common expansion of S. For any $u \approx u' \in P$ such that the terms $F(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n))$ and u have a unifying pair, let $g_{S,u}$ and $l_{S,u}$ be the minimal unifying pair for these terms; so,

$$g_{S,u}F(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n)) = l_{S,u}(u).$$

We define $U(t)$ to be the set of the permissible substitutions that either belong to U_0 or are f_S for some S or are $g_{S,u}f_S$ for some S, u.

We must prove that $U(t)$ has the property stated above. Let $f = gh$ where f is a permissible substitution, and f and h expand the same substitutions from $U(t)$. Denote by S the set of the substitutions from U_0 that can be expanded to f (and to h). Then $h = kf_S$ for some k, and all the three substitutions, f, h and f_S, expand the same substitutions from U_0. For any $i = 1, \cdots, n$, $U(t_i)$ is a subset of U_0, so the three substitutions also expand the same substitutions from $U(t_i)$ and, by induction,

$$\nu_P f(t_i) = gk\nu_P f_S(t_i) \qquad \text{and} \qquad \nu_P h(t_i) = k\nu_P f_S(t_i).$$

Let us consider two cases.

The first case is when $g_{S,u}$ exists for some $u \approx u' \in P$ and f expands $g_{S,u}f_S$. Then also h expands the substitution and we can write $h = pg_{S,u}f_S$; in fact, we can suppose that $k = pg_{S,u}$. Since $f = gkf_S = gpg_{S,u}f_S$, we have

$$F(\nu_P f(t_1), \cdots, \nu_P f(t_n)) = gpg_{S,u}F(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n)) = gpl_{S,u}(u),$$

so that $\nu_P f(t) = gpl_{S,u}(u')$ by the definition of ν_P. Quite similarly, $\nu_P h(t) = pl_{S,u}(u')$ and we get $\nu_P f(t) = g\nu_P h(t)$ as desired.

The second case is when f (and h, as well) does not expand any $g_{S,u}f_S$. Then gk does not expand any $g_{S,u}$. By the defining property of $g_{S,u}$ this means that there is no substitution l with $gkF(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n)) = l(u)$ for any $u \approx u' \in P$. Hence the term

$$\begin{aligned} gkF(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n)) = &\quad F(gk\nu_P f_S(t_1), \cdots, gk\nu_P f_S(t_n)) \\ = &\quad F(\nu_P f(t_1), \cdots, \nu_P f(t_n)) \end{aligned}$$

belongs to A_P, so that, by the definition of ν_P,

$$\nu_P f(t) = F(\nu_P f(t_1), \cdots, \nu_P f(t_n)) = gkF(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n)).$$

Quite similarly $\nu_P h(t) = kF(\nu_P f_S(t_1), \cdots, \nu_P f_S(t_n))$, and we get $\nu_P f(t) = g\nu_P h(t)$ as desired.

This finishes the construction of $U(t)$ together with the proof that it has the desired property.

Clearly, it is possible to construct a finite set V of permissible substitutions such that V contains both $U(a)$ and $U(b)$ and the minimal common expansion of any subset of V belongs to V, under the assumption that it exists and is permissible. These will be our testing substitutions. If $a \approx b$ is satisfied in $\mathbf{A}_P$, then $\nu_P f(a) = \nu_P f(b)$ for any $f \in V$, since $\nu_P f$ is a homomorphism of the term algebra into $\mathbf{A}_P$. Conversely, suppose that $\nu_P f(a) = \nu_P f(b)$ for all $f \in V$, which can be tested in finite time. We shall show that then $a \approx b$ is satisfied in $\mathbf{A}_P$, i.e., that $h(a) = h(b)$ for any homomorphism h of the term algebra into $\mathbf{A}_P$; one can assume that $h(x) = x$ for any variable x not in $\boldsymbol{S}(a) \cup \boldsymbol{S}(b)$. Denote by e the substitution coinciding with h on the variables, so that $h = \nu_P e$. There is a substitution $f \in V$ such that $e = gf$ for some g, and e and f expand the same substitutions from V. We have $h(a) = \nu_P e(a) = g\nu_P f(a) = g\nu_P f(b) = \nu_P e(b) = h(b)$.

Together with Lemma 2.3, this proves the following:

THEOREM 2.4. *The set of the finite sets P of equations that are a perfect base for the equational theory based on P, is recursive.* □

If the perfection test fails for a given finite pre-perfect base P_0, there is still a possibility to modify P_0 to obtain another finite base P_1 for the same equational theory E, which would be either perfect itself or just the next member of a sequence $P_0, P_1, \cdots$ of finite pre-perfect bases for E constructed each from the last one in the same way, the last member of which is perfect. If P_i has already been constructed, a good candidate for P_{i+1} is the union of P_i with the set of the equations $\nu_{P_i} f(a) \approx \nu_{P_i} f(b)$ such that $a \approx b \in P_0$, f is a substitution from the finite set V constructed as above, and $\nu_{P_i} f(a) \neq \nu_{P_i} f(b)$. These added equations seem to play a role similar to one played by critical pairs in the Knuth-Bendix algorithm. It may be necessary, however, to replace some of the added equations $u \approx v$ with their inverses $v \approx u$, and to delete some of the equations or in some cases to

modify the set in other ways to obtain again a pre-perfect set of equations; if some old equations had to be deleted, one must then check that the new set is again a base for E, which can be done by verifying that $\nu_{P_{i+1}}(a) = \nu_{P_{i+1}}(b)$ for any $a \approx b \in P_0$. Clearly, this process of constructing the sequence $P_0, P_1, \cdots$ may stop with failure, if we are not able to modify one of its members to become a pre-perfect base for E. However, it works well for many equational theories; see Ježek (1982) for the examples. If the sequence can be constructed, it has the property that $A_{P_{i+1}}$ is a proper subset of A_{P_i} for any i. It is natural to ask whether it can be constructed to successfully terminate always when there exists some finite perfect base Q for E such that $A_Q \subseteq A_{P_0}$. We do not know the answer to this question, and feel that it deserves a deeper study. The most usual application of the process described (in not very precise terms) above leads either to success, when the sequence can be constructed, is finite, and its last member is a finite perfect base, or to the proof that no perfect base exists (for example, one may find that a nontrivial permutational identity would have to be added), or does not terminate, producing an infinite sequence of finite pre-perfect bases for E. In the last case, it may happen that each P_i is a subset of P_{i+1}, but the union of all these bases still is not a perfect base; we then need to 'construct' a new infinite sequence of pre-perfect bases, starting with this infinite union.

Theorem 2.4 has a simple corollary: For every finitely based and decidable equational theory E, the set of the finite sets of equations that are perfect bases for E is recursive. The same is not true for general bases in place of the perfect ones. For example, the equational theory of idempotent groupoids is decidable (because the equation $xx \approx x$ is a perfect base), but, as it follows from the results of Perkins (1967), Murskiĭ (1971) and McNulty (1976) and (1976a), the set of the finite sets of equations that are a base for this equational theory is not recursive. On the other hand, it follows also from those four papers that there is no algorithm deciding for any finite set B of equations, whether the equational theory based on B has a finite perfect base.

Let us finish this section with several examples, illustrating the technique of perfect bases both in very simple and in more complicated cases. In all our examples we shall suppose that the given similarity type consists of a single binary symbol, denoted multiplicatively; algebras of this type are called **groupoids**. [$xy \cdot z$ is then an abbreviation for $(xy)z$, etc.]

Example 2.5. The equation $xy \cdot yx \approx x$ is a perfect base for the equational theory it generates.

Example 2.6. In order to describe the equational theory based on $xy \cdot zx \approx x$, one can try to prove that this single-equation base is already perfect. The test, as described above, fails and provides two more equations that should be added to a perfect base, namely, $x(y \cdot zx) \approx xz$ and $(xy \cdot z)y \approx xy$. Now the three equations together can be tested to a success; the three-element set of equations is a perfect base for the equational theory.

Example 2.7. The equational theory based on $x(y \cdot zx) \approx x$ has an infinite perfect base consisting of the equations

$$(y_n(y_{n-1}(\cdots(y_2 \cdot y_1 x))))(z_m(z_{m-1}(\cdots(z_2 \cdot z_1 x)))) \approx y_n(y_{n-1}(\cdots(y_2 \cdot y_1 x)))$$

where $n, m \geq 0$ and $n - m - 1$ is divisible by 3. The proof is quite easy.

EXAMPLE 2.8. The equational theory based on $y(x \cdot xy) \approx x$ has an infinite perfect base consisting of the equations $xx \cdot x \approx x$ and $r_e s_e \approx t_e$, where e runs over all finite sequences of elements of $\{0, 1\}$ and the terms r_e, s_e and t_e are defined inductively as follows:

$$\begin{array}{lll} r_\emptyset = y, & s_\emptyset = x \cdot xy, & t_\emptyset = x, \\ r_{e0} = s_e, & s_{e0} = r_e t_e, & t_{e0} = r_e, \\ r_{e1} = s_e \cdot s_e r_e, & s_{e1} = t_e, & t_{e1} = r_e. \end{array}$$

The proof is not very simple.

EXAMPLE 2.9. The set P consisting of the three equations

$$x \cdot yz \approx yz, \qquad xx \cdot x \approx xx, \qquad ((xy \cdot x)y)x \approx (((xy \cdot x)x)y)x$$

will serve as an example of a finite perfect base which is not finitely terminating. The base is not finitely terminating, since the term $((xx \cdot x)x)x$ can be rewritten to an infinite sequence of terms. It is also easy to check that P is a perfect base. Let us give a 'human' proof in this case, rather than say that the algorithm can be mechanically applied. Easily, the set A_P consists of the terms $((x_0 x_1 \cdot x_2) \cdots) x_n$ where $n \geq 0$, $x_0, \cdots, x_n$ are variables, we do not have $x_0 = x_1 = x_2$ if $n \geq 2$ and we do not have $x_0 = x_2 = x_4$ and $x_1 = x_3$ simultaneously if $n \geq 4$. Denote the last of the three equations by $p \approx q$.

One can check easily that P is pre-perfect. For that purpose, it is useful to observe that if $a \cdot bc = dd \cdot d$, then this term contains a proper subterm a not belonging to A_P; and that if f is a substitution such that every proper subterm of $f(p)$ belongs to A_P, then $f(x)$ and $f(y)$ are two distinct variables, so that the term $f(q)$ then belongs to A_P. The multiplication of the groupoid $\mathbf{A}_P$, which we will denote by $\circ$, is then defined by

$$u \circ v = \begin{cases} v & \text{if } v \text{ is not a variable,} \\ u & \text{if } u = vv \text{ (then } v \text{ must be a variable),} \\ \alpha(q) & \text{if } uv = \alpha(p) \text{ for an automorphism } \alpha, \\ uv & \text{otherwise} \end{cases}$$

for any $u, v \in A_P$.

It remains to prove that $\mathbf{A}_P$ satisfies all the three equations. The first thing is to prove $a \circ (b \circ c) = b \circ c$ for any $a, b, c \in A_P$. Clearly, $b \circ c$ can never be a variable, so this is true.

Next we must show that $(a \circ a) \circ a = a \circ a$ for any $a \in A_P$. If a is not a variable, then $a \circ a = a$, so both sides are equal to a. If a is a variable, both sides are equal to aa.

The last is to prove $(((a \circ b) \circ a) \circ b) \circ a = ((((a \circ b) \circ a) \circ a) \circ b) \circ a$ for $a, b \in A_P$. If a is not a variable, then clearly both sides are equal to a. If b is not a variable, then $u \circ b = b$ for any u, so that both sides are equal to $b \circ a$. If both a and b are variables and $a = b$, then both sides are equal to a. If a, b are two distinct variables, then both sides are equal to $(((ab \cdot a)a)b)a$.

We see that a finite perfect base is not necessarily finitely terminating. On the other hand, it is clear that every perfect set is confluent and it is finitely terminating very often. For example, a perfect base with respect to which either every rewrite shortens or every rewrite prolongs terms, is always finitely terminating. In example 2.9, we would obtain a confluent and finitely terminating perfect base for the equational theory based

on P if we simply replaced the equation $p \approx q$ with $q \approx p$. There are situations, however, when we need to consider weirder candidates for a perfect base than the obvious ones. The example in the introduction gives a flavor of such situations.

EXAMPLE 2.10. The set P consisting of the two equations

$$xx \cdot yy \approx xx, \qquad (xx \cdot x) \cdot yy \approx ((xx \cdot x)x)x$$

will serve as an example of a finite perfect base, the equational theory of which has no (either finite or infinite) finitely terminating and confluent base. Denote by E the equational theory based on P and by $\circ$ the multiplication of the groupoid $\mathbf{A}_P$. Based on the following observation, one can easily check that P is perfect: if $a \in A_P$, then

$$a \circ a = \begin{cases} a & \text{if } a \text{ is a square (i.e., } a = tt \text{ for a term } t), \\ aa & \text{if } a \text{ is not a square.} \end{cases}$$

In each case, $a \circ a$ is a square.

Suppose that there is a finitely terminating and confluent base Q for E. It is easy to see that if t is a term with $t \approx xx \in E$, then t contains xx as a subterm and so, because of the finite termination, xx cannot be Q-rewritten to t. It follows that xx is in Q-canonical form and the term $xx \cdot yy$ can be Q-rewritten in finitely many steps to xx. Denote by w the Q-canonical form of $(xx \cdot x) \cdot yy$. We have $w \neq (xx \cdot x) \cdot yy$, since $((xx \cdot x)x)x$ cannot be Q-rewritten to $(xx \cdot x) \cdot yy$, due to finite termination. So we have $(xx \cdot x) \cdot yy$, as well as $xx \cdot yy$, can be Q-rewritten. This implies that w avoids both $(xx \cdot x) \cdot yy$ and $xx \cdot yy$, because w cannot be Q-rewritten, being itself in Q-canonincal form. But then $w \in A_P$ and hence $w = ((xx \cdot x)x)x$, since P is perfect. This means that $(xx \cdot x) \cdot yy$ can be Q-rewritten in finitely many steps to $((xx \cdot x)x)x$. Consequently, the term $((xx \cdot xx) \cdot xx) \cdot xx$ can be Q-rewritten in finitely many steps to $(((xx \cdot xx) \cdot xx) \cdot xx) \cdot xx$, clearly a contradiction.

So there are equational theories with finite perfect bases but without any convergent term rewriting system. The equational theory of semigroups serves as an example of an equational theory with a convergent term rewriting system but with no perfect base.

3. Nonoverlapping bases

A set P of equations is said be **nonoverlapping** if the following are true:

(o1) if $u \approx u' \in P$, then $\boldsymbol{S}(u') \subseteq \boldsymbol{S}(u)$;
(o2) if $u \approx u' \in P$, $v \approx v' \in P$, $s \subseteq v'$, and u and s have a unifying pair, then s is a variable and $s \neq v'$;
(o3) if $u \approx u' \in P$, $v \approx v' \in P$, $s \subseteq v$, and u and s have a unifying pair, then either s is a variable or both $s = u = v$ and $u' = v'$.

THEOREM 3.1. *Let P be a nonoverlapping set of equations. Then P is a perfect base for an equational theory.*

PROOF. If $u \approx u' \in P$, then u and u' do not have a unifying pair, according to (o2); in particular, u is not a variable. Conditions (pp1) and (pp2) are evidently satisfied, and instead of (pp3) it is easier to verify the condition (pp3′) formulated in the proof of Lemma 2.3. So, P is pre-perfect.

In order to prove that the algebra A_P satisfies all the equations from P, we must show that $h(a) = h(b)$ for any equation $a \approx b \in P$ and any homomorphism h of the term algebra into $\mathbf{A}_P$. Denote by f the endomorphism of the term algebra which coincides with h on the set of variables.

Let us prove by induction on the complexity of t that if t is either a subterm of b or a proper subterm of a, then $h(t) = f(t)$. If t is a variable, this follows from the definition of f. Let $t = F(t_1, \cdots, t_n)$. We have

$$\begin{aligned} f(t) &= F(f(t_1), \cdots, f(t_n)), \\ h(t) &= F_{\mathbf{A}}(h(t_1), \cdots, h(t_n)) \quad = F_{\mathbf{A}}(f(t_1), \cdots, f(t_n)) \\ &\qquad\qquad\qquad\qquad = \nu_P(F(f(t_1), \cdots, f(t_n))) = \nu_P(f(t)) \end{aligned}$$

and thus it remains to show that $f(t)$ belongs to A_P. Suppose, on the contrary, that $g(u)$ is a subterm of $f(t)$ for some substitution g and an equation $u \approx u' \in P$. For any variable x, $g(u)$ cannot be a subterm of $f(x)$, because $f(x) \in A_P$. So, $g(u) = f(s)$ for a subterm s of t which is not a variable. This means that u, s have a unifying pair, a contradiction with (o2) and (o3).

In particular, $h(b) = f(b)$. On the other hand, if $a = F(a_1, \cdots, a_n)$,

$$h(a) = F_{\mathbf{A}}(h(a_1), \cdots, h(a_n)) = F_{\mathbf{A}}(f(a_1), \cdots, f(a_n))$$

which is easily seen to be equal $f(b)$ by comparing the definitions. □

A quasiordering $\sqsubseteq$ on the set of terms is said to be **fully compatible** if $F(a_1, \cdots, a_n) \sqsubseteq F(b_1, \cdots, b_n)$ whenever $a_i \sqsubseteq b_i$ for all i, and $a \sqsubseteq b$ implies $f(a) \sqsubseteq f(b)$ for any substitution f. A quasiordering $\sqsubseteq$ such that the set $\{u : u \sqsubseteq a\}$ is finite for any a, is called **downward finite**. A natural example of a fully compatible, downward finite quasiordering on the set of terms is the following: $u \sqsubseteq v$ if and only if every variable, and also every operation symbol, has at least as many occurrences in v as in u.

THEOREM 3.2. *Let an equational theory E have a nonoverlapping base P, such that there is a fully compatible, downward finite quasiordering $\sqsubseteq$ on the set of terms with $u \sqsubseteq u'$ whenever $u \approx u' \in P$. Then E is term finite.*

PROOF. By Theorems 2.2 and 3.1, P is a perfect base and ν_P is a normal form function for E. We have $t \sqsubseteq \nu_P(t)$ for any term t; this can be proved easily by induction on the complexity of t. Since every term u with $u \approx t \in E$ satisfies $\nu_P(u) = \nu_P(t)$, for a given term t the set of all such terms u is contained in the principal ideal of $\nu_P(t)$, which is a finite set. □

EXAMPLE 3.3. The equation

$$((xx \cdot yy)x)x \approx xx$$

is a nonoverlapping base for an equational theory E_1. Similarly, the equation

$$(xx \cdot x)(y \cdot yy) \approx (x(xx \cdot x))(y \cdot yy)$$

is a nonoverlapping base for an equational theory E_2. While E_1 is not term finite, E_2 is term finite, which follows from Theorem 3.2, using the quasiordering described immediately preceding that theorem.

4. Normal bases

Let P be a set of equations. As before, we denote by A_P the set of terms t such that whenever $u \approx u' \in P$, then $u \not\leq t$. We shall suppose that P satisfies the following two conditions:

(n1) if $u \approx u' \in P$, then $u' \in A_P$;
(n2) if $u \approx u' \in P$, $v \approx v' \in P$ and $(u, u') \neq (v, v')$, then $u \not\leq v$.

By induction on a non-negative integer k, we are going to define the set of terms of P-**rank** k, and for each term t of P-rank k a term $\nu_P(t) \in A_P$, in this way:

Terms of P-rank 0 are precisely the variables, and for any term of P-rank 0 we put $\nu_P(t) = t$.

A term $t = F(t_1, \cdots, t_n)$ is of P-rank $k+1$ if and only if it is not of P-rank $\leq k$, every t_i is of P-rank $\leq k$ and if $F(\nu_P(t_1), \cdots, \nu_P(t_n)) = f(u) = g(v)$ for two substitutions f, g and two equations $u \approx u' \in P$ and $v \approx v' \in P$, then both $f(u')$ and $g(v')$ are of P-rank $\leq k$ and $\nu_P f(u') = \nu_P g(v')$. If t is of P-rank $k+1$, we then define

$$\nu_P(t) = \begin{cases} F(\nu_P(t_1), \cdots, \nu_P(t_n)) & \text{if this term belongs to } A_P, \\ \nu_P f(u') & \text{if } F(\nu_P(t_1), \cdots, \nu_P(t_n)) = f(u) \text{ for some } f,\ u \approx u'. \end{cases}$$

If every term has a P-rank, i.e., if $\nu_P(t)$ is defined for every term t, then we can define an algebra $\mathbf{A}_P$ with the underlying set A_P by

$$F_{\mathbf{A}}(t_1, \cdots, t_n) = \nu_P(F(t_1, \cdots, t_n)).$$

Instead of saying that P is a set of equations satisfying (n1) and (n2) and such that every term has a P-rank, we shall more briefly say that the algebra $\mathbf{A}_P$ exists.

LEMMA 4.1. *Let $\mathbf{A}_P$ exist. Then:*

(1) *If P is a recursive set of equations with recursive domain, then $\nu_P(t)$ can be computed for any term t. There is an algorithm taking as an input any finite set of equations P and any term t, and producing the term $\nu_P(t)$ in the case that the algebra $\mathbf{A}_P$ exists.*
(2) *ν_P is a homomorphism of the term algebra onto $\mathbf{A}_P$.*

PROOF. (1) is easy, and the proof of (2) is similar to that of Lemma 2.1. □

By a **normal base** for an equational theory E we mean a base P for E such that the algebra $\mathbf{A}_P$ exists and satisfies all the equations from E.

It will be easy to see that this notion generalizes both perfect bases and finitely terminating confluent bases. Consequently, one cannot expect the class of normal bases to be recursive, or to be able to decide in general whether every term has a P-rank. The notion will serve as a common generalization, suitable for some simple results on the uniqueness.

THEOREM 4.2. *Let P be a normal base for E. Then:*

(1) *ν_P is a normal form function for E;*

(2) $\mathbf{A}_P$ *is the free* E*-algebra over the set of variables;*
(3) E *is decidable if* P *is recursive, with recursive domain.*

PROOF. It is similar to the proof of Theorem 2.2. □

THEOREM 4.3. *Let* R *be a confluent and finitely terminating set of equations. Then the equational theory* E *based on* R *has a normal base* P *with* $|P| \leq |R|$*. If* R *is finite, then* P *can be computed from* R*.*

PROOF. Denote by M the set of the minimal terms (minimal with respect to $\leq$) that do not belong to A_R, and by M_0 a representative subset of M, i.e., a subset such that every term from M is similar to precisely one term from M_0. Clearly, M_0 can be also constructed from R by taking a representative subset of the set of minimal terms in the domain of R. Consequently, $|M_0| \leq |R|$.

For every term t, any sequence of rewrites of t based on R is finite and terminates at the same term. Denote this term by $\nu(t)$. We have $u \approx v \in E$ if and only if $\nu(u) = \nu(v)$.

Denote by P the set of the equations $u \approx \nu(u)$ with $u \in M_0$. Clearly, $A_P = A_R$, $P \subseteq E$ and the conditions (n1) and (n2) are satisfied. If R is finite then P can be computed from R, because the mapping ν is computable. It is easy to prove by induction on k for any term t of P-rank k, that $\nu_P(t) = \nu(t)$.

Suppose there is a term t_0 which has no P-rank. Then there is a subterm $s = F(s_1, \cdots, s_n)$ of t_0 which also has no P-rank, but every s_i has a P-rank, so that $\nu_P(s_i) = \nu(s_i)$. We have $t_0 = L(s)$ for a lift L. If $F(\nu_P(s_1), \cdots, \nu_P(s_n)) = f(u) = g(v)$ for two substitutions f and g and two equations $u \approx u' \in P$ and $v \approx v' \in P$ where both $f(u')$ and $f(v')$ have P-ranks, then $\nu_P f(u') = \nu f(u') = \nu f(u) = \nu g(v) = \nu g(v') = \nu_P g(v')$. So, according to the definition, it is only possible for s to have no P-rank if $F(\nu_P(s_1), \cdots, \nu_P(s_n)) = f(u)$ for a substitution f and an equation $u \approx u' \in P$ such that $f(u')$ has no P-rank. The term $t_1 = L(f(u'))$ also has no P-rank, and can be obtained from t_0 by a nonempty sequence of rewrites based on R. This clearly violates the finite termination property of R. Consequently, every term t has a P-rank and $\nu_P(t) = \nu(t)$.

From this it follows that P is a base for E. Since ν_P is a normal form function, $\mathbf{A}_P$ satisfies all the equations from E. □

The normal base P produced above from the convergent rewrite system R is familiar as a canonical rewrite system (i.e. reduced and convergent). See Dershowitz and Jouannaud (1990), section 7.5, for a brief discussion of these kinds of rewrite systems and for pointers to the literature. The content of the theorem above is that such canonical systems also turn out to be normal bases.

LEMMA 4.4. *Let* P *and* Q *be two normal bases for* E*, and let* $u \approx u' \in Q$ *be such that* $u \in A_P$*. Then* $u' \notin A_P$*, and there is an equation* $v \approx v' \in P$ *with* $v' \leq u$*; we either have* $v \notin A_Q$*, or the equations* $u \approx u'$ *and* $v' \approx v$ *are similar.*

PROOF. Suppose $u' \in A_P$. Since also $u \in A_P$, and $u \approx u' \in E$, we get $u = \nu_P(u) = \nu_P(u') = u'$, a contradiction with $u \approx u' \in Q$.

Since P is a base for E and we have $u \approx u' \in E$ and $u \neq u'$, there is an equation $v \approx v' \in P$ with either $v \leq u$ or $v' \leq u$. We cannot have $v \leq u$, because $v \notin A_P$ and $u \in A_P$. Hence $v' \leq u$ is the only possibility.

Let $v \in A_Q$. Then $v' \notin A_Q$, since $v \approx v' \in E$ and $v \neq v'$. Since u is a minimal term not in A_Q, we get $v' \sim u$. So, $v' = \alpha(u)$ for an automorphism α of the term algebra. Since $u \approx u' \in E$, we have $\alpha(u) \approx \alpha(u') \in E$, i.e., $v' \approx \alpha(u') \in E$. But also $v \approx v' \in E$, so $v \approx \alpha(u') \in E$. Both sides of this last equation belong to A_Q, and thus $v = \alpha(u')$. □

THEOREM 4.5. *Let E have a normal base consisting of a single equation $u \approx u'$. Then any other normal base for E contains an equation similar to either $u \approx u'$ or $u' \approx u$.*

PROOF. Clearly, every normal base P for E is determined uniquely up to the similarity of equations by the set A_P. Indeed, an equation $u \approx u'$ is similar to an equation from P if and only if u is a minimal term not in A_P, and u' is the only term in A_P with $u \approx u' \in E$. So, if P and Q are two bases for E that are not equal up to similarity of their equations, then the sets A_P and A_Q are different; moreover, it is easy to see that they are incomparable with respect to set inclusion. The statement follows from these remarks and Lemma 4.4. □

EXAMPLE 4.6. Let E be the equational theory based on the equation

$$x \cdot xx \approx xx \cdot xx$$

The base P consisting of this equation is perfect; one can easily verify that it is nonoverlapping. Since the equation is in one variable and the right side is longer than the left side, for any term t it is clear that $\nu_P(t)$ is the longest among the terms u with $u \approx t \in E$. For some purposes we would need, however, to have a normal base which shortens terms rather than makes them longer. It turns out that there is precisely one (up to similarity) normal base for E with this property. By Theorem 4.5, such a base must contain the equation $xx \cdot xx \approx x \cdot xx$. The base consisting of this equation is pre-perfect, but not perfect; the algorithm described in Section 2 will yield an equation that must be added, but the resulting two equations still do not provide for a perfect base. If we continue this process, we find that we need to include infinitely many equations $u_i u_i \approx v_i$ $(i = 0, 1, \cdots)$ where

$$\begin{aligned} u_0 &= xx, & v_0 &= x \cdot xx, \\ u_{i+1} &= v_i, & v_{i+1} &= u_i v_i. \end{aligned}$$

It is not difficult to verify that the set Q consisting of these infinitely many equations is a perfect base for E, and the only normal base which shortens terms. So, the requirement to make the terms shorter may be at the cost of the cardinality of the normal base.

THEOREM 4.7. *Let E be an equational theory having a normal base P with the property that $u \approx u' \in P$ implies $u' \leq u$. Then P is, up to similarity of equations, the only normal base for E.*

PROOF. Let Q be another normal base for E. Suppose that there is an equation $u \approx u' \in P$ with $u \in A_Q$. By Lemma 4.4, $u' \notin A_Q$. But $u' \leq u$, so $u \notin A_Q$, a contradiction.

Consequently, $u \in A_Q$ for any $u \approx u' \in P$. This means $A_Q \subseteq A_P$, and hence $A_Q = A_P$. It follows that every equation from P is similar to an equation from Q and vice versa. □

THEOREM 4.8. *Let B be a set of equations of the form*

$$F(u_1, \cdots, u_n) \approx u_1 \qquad (\star)$$

and E be the equational theory based on B. Then E has, up to similarity of equations, precisely one normal base; this normal base is perfect and consists again of equations of the form $(\star)$.

PROOF. For any term u which is neither a variable nor a nullary operation symbol, so that $u = F(u_1, \cdots, u_n)$, put $u^* = u_1$. Then $u \approx u^*$ are just the equations of the form $(\star)$. Let P be a representative set of the equations $u \approx u^*$, where u is a minimal term with the property that u^* exists and $u \approx u^* \in E$; representative in the sense that every such equation is similar to precisely one equation from P.

It is easy to prove by induction on the complexity of a term u that if (u^* exists and) $u \approx u^* \in E$, then $u \approx u^*$ is a consequence of P. In particular, P is a base for E. The three conditions in the definition of a pre-perfect set are evidently satisfied, so in order to see that P is a perfect base, we must verify that the algebra $\mathbf{A} = \mathbf{A}_P$ is a model of P. Let h be a homomorphism of the term algebra into $\mathbf{A}_P$, and denote by f the substitution with $f(x) = h(x)$ for all variables x, so that $h = \nu_P f$. Clearly, for any term $t = F(t_1, \cdots, t_n)$ we have either $h(t) = F(h(t_1), \cdots, h(t_n))$ or $h(t) = h(t_1)$.

Let us prove by induction on the complexity of a term t that $h(t) \approx f(t) \in E$. This is clear if t is a variable, so let $t = F(t_1, \cdots, t_n)$. By induction, $h(t_i) \approx f(t_i) \in E$ for all i. If $F(h(t_1), \cdots, h(t_n)) \in A_P$, then $h(t) = F(h(t_1), \cdots, h(t_n))$ and $f(t) = F(f(t_1), \cdots, f(t_n))$, so that the equation evidently belongs to E. The remaining case is when $F(h(t_1), \cdots, h(t_n)) = s(u)$ for a substitution s and an equation $u \approx u^* \in P$. Then $h(t) = s(u^*) = h(t_1)$. Now $u \approx u^* \in E$ implies $s(u) \approx s(u^*) \in E$, which means that $F(h(t_1), \cdots, h(t_n)) \approx h(t_1) \in E$. But $F(h(t_1), \cdots, h(t_n)) \approx F(f(t_1), \cdots, f(t_n)) \in E$, so $F(f(t_1), \cdots, f(t_n)) \approx h(t_1) \in E$. Since $F(f(t_1), \cdots, f(t_n)) = f(t)$ and $h(t_1) = h(t)$, this gives $f(t) \approx h(t) \in E$.

Let $u \approx u^* \in P$. We need to prove that $h(u) = h(u^*)$. It follows from $f(u) \approx f(u^*) \in E$ and the above observation that $h(u) \approx h(u^*) \in E$. If $h(u) \neq h(u^*)$, then $h(u) = F(h(u_1), \cdots, h(u_n))$, so that $h(u^*) = h(u)^*$ and then $h(u) \approx h(u)^* \in E$ yields $h(u) \notin A_P$, a contradiction.

We have proved that P is a perfect base for E. Its uniqueness follows from Theorem 4.7. □

EXAMPLE 4.9. One can easily see that the equational theory based on the equation $xy \cdot x \approx x$ has no normal base. This means that there is no hope to generalize Theorem 4.8 in such a way that we would allow the right sides of the equations in B to be deeper subterms of the corresponding left sides.

Since the proof of Theorem 4.8 does not tell us whether the perfect base P is recursive (we know that it need not be finite), we leave the following question open:

Problem. Is the equational theory based on any finite set of equations of the form $(\star)$ decidable?

The technique of normal bases may also lead to an answer to the following question:

Problem. Is there an algorithm deciding for any equation $a \approx b$ in a single variable, such that the two terms a and b are incomparable, whether the equational theory based on $a \approx b$ is term finite? Is the answer always yes?

Although there are several essentially different ways in which to understand the notion of a random equation, the following problem should be interesting in any of these formulations:

Problem. Is a random equation $u \approx v$ with $\boldsymbol{S}(u) = \boldsymbol{S}(v)$ a perfect base for the equational theory based on that equation?

References

Boole, G. (1847). *The mathematical analysis of logic, being an essay toward a calculus of deductive reasoning.* Macmillan, Barclay, and Macmillan. Cambridge and London. 82 pp.

Dehn M. (1911). Über unendlicher diskontinuierliche Gruppen. *Math. Ann.* **71**, 116-144.

Dershowitz N., Jouannaud J.-P. (1990). Rewrite systems. Chapter 6, 243–320 in J. van Leeuwen, ed., *Handbook of Theoretical Computer Science, B: Formal Methods and Semantics.* North Holland, Amsterdam.

Evans T. (1951). On multiplicative systems defined by generators and relations. I. Normal form theorems. *Proc. Cambridge Philos. Soc.* **47**, 637–649.

Freese R., Ježek J., Nation J.B. (1993). Term rewrite systems for lattice theory. *J. Symbolic Computation* **16**, 279–288.

Ježek J. (1982). Free groupoids in varieties determined by a short equation. *Acta Universitatis Carolinae – Mathematica et Physica* **23**, 3–24.

Ježek J., McNulty G. (1994). The existence of finitely based lower covers for finitely based equational theories. To appear in *J. Symbolic Logic*.

Kapur D., Narendran P. (1985). A finite Thue system with decidable word probem and without equivalent finite canonical system. *Theoretical Computer Science* **35**, 337–344.

Knuth D.E., Bendix P.B. (1970). Simple word problems in universal algebras, in: J. Leech, ed., *Computational Problems in Abstract Algebra* (Proc. Conf., Oxford, 1967). Pergamon Press, Oxford, 263-297.

McKenzie R., McNulty G., Taylor W. (1987). *Algebras, Lattices, Varieties, Vol. I.* Wadsworth & Brooks/Cole, Monterey, California.

McNulty G. (1976). The decision problem for equational bases of algebras. *Ann. Math. Logic* **10**, 193–259.

McNulty G. (1976a). Undecidable properties of finite sets of equations. *J. Symbolic Logic* **41**, 589–604.

McNulty G. (1992). A field guide to equational logic. *J. Symbolic Computation* **14**, 371–397.

Murskiĭ V.L. (1971). Nondiscernible properties of finite systems of identity relations (Russian). *Dokl. Akad. Nauk SSSR* **196**, 520–522. (English translation: Soviet Math. Dokl. **12**, 183–186.)

Perkins P. (1967). Unsolvable problems for equational theories. *Notre Dame J. Formal Logic* **8**, 175–185.

Pigozzi D. (1979). Universal equational theories and varieties of algebras. *Ann. Math. Logic* **17**, 117–150.

Squier C.C., Otto F. (1987). The word problem for finitely presented monoids and finite canonical rewriting systems. Pages 74–82 in J.-P. Jouannaud, editor, *Proc. 2nd Rewriting Techniques and Applications, Bordeaux*, LNCS **256**.

Taylor W. (1979). Equational logic. *Houston J. Math* (Survey Issue).

Whitman P.M. (1941). Free lattices. *Annals of Math.* **42**, 325–330.