Notes prepared by
Stanley Burris
February 10, 1997

1 E-unification

Just as unification plays a crucial role in the study of term rewrite systems (see Chapter III of LMCS), one has E-unification for work with ETRS's. Indeed the equational theorem prover EQP that William McCune used to verify the Robbins' Conjecture (discussed at the end of Chapter III of LMCS) uses AC-unification.

In the following E will denote a set of equations.

DEFINITION 1 Given a pair of terms $s, t \in \mathrm{T}_n$ we say that a substitution $\sigma : \mathbf{T}_n \to \mathbf{T}_\omega$ is an *E-unifier* of $s, t \in \mathrm{T}_n$ if $\sigma(s)$ and $\sigma(t)$ are equal mod E, i.e.,

$$E \models \sigma(s) \approx \sigma(t).$$

DEFINITION 2 The set of E-unifiers of s and t is denoted by $U_E(s, t)$.

DEFINITION 3 Given two substitutions $\sigma, \sigma' : \mathbf{T}_n \to \mathbf{T}_\omega$ we say σ is *more general (mod E)* than σ', written $\sigma \leq_E \sigma'$, if there is a substitution $\tau : \mathbf{T}_\omega \to \mathbf{T}_\omega$ such that

$$E \vdash \sigma'(x_i) \approx \tau \circ \sigma(x_i) \text{ for } 1 \leq i \leq n.$$

LEMMA 4 $\leq_E$ is a preorder on $\{\sigma : \mathbf{T}_n \to \mathbf{T}_\omega\}$.

PROOF. (Exercise.) ■

DEFINITION 5 Two substitutions σ, σ' mapping $\mathbf{T}_n$ to $\mathbf{T}_\omega$ are *E-equivalent*, written $\sigma \sim_E \sigma'$, if $\sigma \leq_E \sigma'$ and $\sigma' \leq_E \sigma$.

DEFINITION 6 μ is a *most general* E-unifier of s and t if

(a) $\mu \in U_E(s, t)$, and

(b) $\sigma \in U_E(s, t)$ and $\sigma \leq_E \mu$ implies $\sigma \sim_E \mu$.

One can no longer assume that an E-unifiable pair has a most general E-unifier — this depends on the choice of E. The following situations are encountered:

1. There is an E-unifier μ of s and t which is more general than any E-unifier of s and t.
2. There are finitely many most general E-unifiers $\mu_1, \ldots, \mu_n$ of s and t such that for any unifier σ of E some μ_i is more general than σ.
3. There are infinitely many most general E-unifiers $\mu_i (i \in I)$ of s and t such that for any $\sigma \in U_E(s,t)$ some μ_i is more general than σ.
4. There is a $\sigma \in U_E(s,t)$ such that no most general unifier of s and t is more general than σ.

This leads to the following *unification types*:

if $U_E(s,t)$ satisfies	then s, t is (mod E)
(1)	unitary
(2), not (1)	finitary
(3), not (2)	infinitary
(4)	nullary

Using this we can give the unification types for sets of equations E:

i. E is unitary if every E-unifiable s, t is unitary

ii. E is finitary if every E-unifiable s, t is unitary or finitary, and some E-unifiable s, t is finitary.

iii. E is infinitary if every E-unifiable s, t is unitary or finitary or infinitary, and some E-unifiable s, t is infinitary.

iv. E is nullary if some E-unifiable s, t is nullary.

Rather than working with terms modulo E one can phrase the unification types in terms of the homomorphisms between the *free algebras* in the variety V defined by E.

DEFINITION 7 Given a set of equations E let $\mathbf{F}_n$ be the E-free algebra freely generated by $x_1, \cdots, x_n$, and let $\mathbf{F}_\omega$ be the E-free algebra freely generated by countably many generators.

Given a term s in T_n we will adopt the popular convention of using the same symbol s to denote the corresponding element of F_n (which is actually a coset of terms).

DEFINITION 8 For $s, t \in \mathrm{F}_n$ define the set of *E-unifiers* of s, t by

$$U_E(s,t) = \{\sigma \in \mathrm{Hom}(\mathbf{F}_n, \mathbf{F}_\omega)) : \sigma(s) = \sigma(t)\}.$$

We say the pair s, t is *E-unifiable* if $U_E(s,t) \neq \emptyset$.

The problem of determining if $U_E(s,t)$ is the empty set, for arbitrary terms s, t, is called the *unification problem for E*.

DEFINITION 9 Define a relation $\leq_E$ (called *more general than*) on $U_E(S)$ by $\sigma \leq_E \sigma'$ iff there is a $\tau \in \mathrm{Hom}(\mathbf{F}_\omega, \mathbf{F}_\omega)$ such that $\sigma' = \tau \circ \sigma$.

This is expressed by the following diagram:

$$\begin{tikzcd}
 & \mathbf{F}_\omega \\
\mathbf{F}_n \arrow[ur, "\sigma'"] \arrow[dr, "\sigma"'] & \\
 & \mathbf{F}_\omega \arrow[uu, "\tau"']
\end{tikzcd}$$

σ' is more general than σ

LEMMA 10 $\leq_E$ is a preorder on $\{\sigma : \mathbf{T}_n \to \mathbf{T}_\omega\}$.

PROOF. (Exercise.) ■

DEFINITION 11 Two mappings $\sigma, \sigma' \in \mathrm{Hom}(\mathbf{F}_n, \mathbf{F}_\omega)$ are *equivalent* (written $\sigma \sim_E \sigma'$ if each is $\leq_E$ to the other.

DEFINITION 12 Minimal elements (up to equivalence) of $U_E(s,t)$ are called *most general unifiers* of s, t.

DEFINITION 13 A set of equations E (or the variety V determined by E) is:

unitary if for each $\mathbf{F}_n$ and each E-unifiable s, t from $\mathbf{F}_n$ there is a μ from $U_E(s,t)$ such that for every $\sigma \in U_E(s,t)$ we have $\mu \leq_E \sigma$.

finitary if for each $\mathbf{F}_n$ and each E-unifiable s, t from F_n there are most general unifiers $\mu_1, \ldots, \mu_k$ from $U_E(s,t)$ such that for every $\sigma \in U_E(s,t)$ we have some $\mu_i \leq_E \sigma$; and E is not unitary.

infinitary if for each $\mathbf{F}_n$ and each E-unifiable s, t from $\mathbf{F}_n$ there are most general unifiers $\mu_i (i \in I)$ from $U_E(s,t)$ such that for every $\sigma \in U_E(s,t)$ we have some $\mu_i \leq_E \sigma$; and E is not unitary or finitary.

nullary if none of the above hold.

The algebraic approach has proved most useful in determining unification types of some classical theories such as groups — Lawrence pointed out the importance of the Hopf and Schreier properties to establish nonnullary type, as we shall see below.

One can also view E-unification as solving equations in $\mathbf{F}_\omega$. Given an equation $s \approx t$, an E-unifier σ of s, t gives a solution $(\sigma(x_1), \cdots, \sigma(x_n))$ of this equation in $\mathbf{F}_\omega$. And every solution corresponds to an E-unifier.

Thus we can speak of the E-unification type of a single equation. The unification type of E is then the "worst" of the possible E-unification types of equations $s \approx t$.

One can also generalize this to the E-unification type of a finite system of equations; and use this to define the unification type of E. This will agree with the previous type classification, provided the type is either unitary or finitary. In the examples that follow the results are the same for these two definitions of the unification type of E.

EXAMPLE 14 [Vector Spaces]

Solving a system of homogeneous linear equations over a field $\mathbf{K}$ can be formulated in the context of E-unification. Vector spaces over $\mathbf{K}$ can be regarded as an equational class with the usual vector space operations $+, -$, the constant 0, and a collection of unary operations f_k, for $k \in K$, to give the scalar multiplication. We can axiomatize this equational theory by the following set E:

$$\begin{aligned}
x + (y + z) &\approx (x + y) + z \\
x + y &\approx y + x \\
x + 0 &\approx x \\
x + (-x) &\approx 0 \\
f_k(x + y) &\approx f_k(x) + f_k(y) \\
f_{k+l}(x) &\approx f_k(x) + f_l(x) \\
f_k(f_l(x)) &\approx f_{k \cdot l}(x) \\
f_1(x) &\approx x
\end{aligned}$$

The E-free algebra $\mathbf{F}_n$ is the familiar n-dimensional vector space $\mathbf{K}^n$ over K, and the substitutions are linear maps.

A particular solution of an $m \times n$ system of homogeneous linear equations

$$\sum_{j=1}^{n} a_{ij} x_j \approx 0 \qquad 1 \leq i \leq m \tag{1}$$

corresponds to a homomorphism

$$\sigma \,:\, \mathbf{F}(n) \to \mathbf{F}(0)$$

such that each of the left-hand sides of (1) maps to 0. A solution with *parameters* corresponds to a homomorphism

$$\sigma \,:\, \mathbf{F}(n) \to \mathbf{F}(\omega)$$

such that each of the left-hand sides of (1) maps to 0. and in the context of solutions with parameters we can view solutions of a system of homogeneous linear equations as E-unifiers — the unification type is unitary, and Gaussian elimination solves the unification problem and provides a most general unifier when such exists.

However the above formulation will not suffice to discuss linear equations in general since the terms in the above language will be homogeneous, i.e., of the form $\sum_{j=1}^{n} a_j x_j$. To remedy this we merely need to add constants k, for $k \in K$, to our language, and the following axioms to E:

$$\begin{aligned}
f_k(k') &\approx k \cdot k' \text{ for } k' \in K \\
-k_1 &\approx k_2 \text{ if this holds in } K \\
k_1 + k_2 &\approx k_3 \text{ if this holds in } K.
\end{aligned}$$

In this setting the E-free algebra $\mathbf{F}_n$ can be thought of as an $n+1$-dimensional vector-space over $\mathbf{K}$, using the mapping

$$a_1x_1 + \cdots + a_nx_n + b \;\to\; (a_1, \cdots, a_n, b);$$

However the homomorphisms between the free algebras of the equational class defined by E will not correspond to linear maps between the corresponding vector spaces.

A particular solution of an $m \times n$ system of linear equations

$$\sum_{j=1}^{n} a_{ij}x_j + b_i \approx 0 \qquad 1 \leq i \leq m \tag{2}$$

corresponds to a homomorphism

$$\sigma \;:\; \mathbf{F}(n) \to \mathbf{F}(0)$$

such that each of the left-hand sides of (2) maps to 0; and a solution with *parameters* corresponds to a homomorphism

$$\sigma \;:\; \mathbf{F}(n) \to \mathbf{F}(\omega)$$

such that each of the left-hand sides of (2) maps to 0. Solutions with parameters correspond to E-unifiers — and again the unification type is unitary, and Gaussian elimination solves the unification problem and provides a most general unifier when such exists.

EXAMPLE 15 [SEMIGROUPS]

When Plotkin originally proposed that the notion of unification be extended to E-unification in 1972 he presented the example of the associative law for a binary operation — this of course defines semigroups.

- Semigroups are infinitary.

PROOF. Let $E = \{(x \cdot y) \cdot z \approx x \cdot (y \cdot z)\}$. Elements of the free semigroups can be conveniently thought of as strings on an alphabet, and hence we can attach a length $|s|$ to such strings s.

For $\sigma : \mathbf{F}(n) \to \mathbf{F}(\omega)$ we associate a tuple of positive integers

$$\#\sigma \;=\; (|\sigma(x_1)|, \cdots, |\sigma(x_n)|).$$

Now we observe that for any string s from $\mathrm{F}(n)$ we have $|s| \leq |\sigma(s)|$. Consequently, giving N^n the coordinatewise ordering, for $\sigma_i : \mathbf{F}(n) \to \mathbf{F}(\omega)$, $(i = 1, 2)$, we have

$$\sigma_1 \leq_E \sigma_2 \implies \#\sigma_1 \leq \#\sigma_2.$$

Thus for any infinite descending sequence

$$\sigma_1 > \sigma_2 > \cdots \tag{3}$$

there must exist an n_0 such that

$$i \geq n_0 \Longrightarrow \#\sigma_i = \#\sigma_{n_0}.$$

Choose τ_i such that

$$\sigma_i = \tau_i \circ \sigma_{i+1}.$$

Then for $i \geq n_0$ we have τ_i mapping the variables of the range of σ_{i+1} to variables (otherwise $\#\sigma_i > \#\sigma_{i+1}$). Such a τ_i cannot be one-to-one on the variables in the range of σ_{i+1}, for otherwise σ_i and σ_{i+1} would be equivalent under $\leq_E$. This leads to the conclusion that the ranges of $\sigma_{n_0}, \sigma_{n_0+1}, \cdots$ have a strictly decreasing (finite) number of variables in them. This is impossible, and hence so is the existence of an infinite sequence (3).

Thus for semigroups we see that the "more general than" relation on $\mathrm{Hom}(\mathbf{F}(n), \mathbf{F}(\omega))$ has the descending chain property; and thus the unification type of semigroups cannot be nullary.[1]

Now we turn to an example to show that the unification type of semigroups is infinitary. Consider the equation $x \cdot y \approx y \cdot x$. Clearly it can be unified; what is not so obvious is that every unifier σ is of the form

$$\sigma(x) = s^i \tag{4}$$

$$\sigma(y) = s^j \tag{5}$$

for some choice of string s and positive integers i, j. (This is proved below in Example 16 on groups.) Furthermore, every σ of the form (4,5) is a unifier. We leave it as an exercise to show that the most general unifiers of $x \cdot y \approx y \cdot x$ are given by (4,5) with $s = z$, a variable, and $gcd(i, j) = 1$. Consequently we have an equation whose unification type is indeed infinitary. ■

EXAMPLE 16 [Groups]

[1]The failure of the descending chain property does not imply nullary type.

One of the questions posed by Plotkin in 1972 was how to deal with situations like E being defining equations for groups. In this case there is no obvious way to assign a "length" to elements of the free algebras with the property that substitutions are non length decreasing. (Consider the fact that a simple substitution, of x^{-1} for y, can reduce $x \cdot y$ to e.)

The unification type of groups was not determined until 1989, when John Lawrence realized how to use some deep facts about the nature of free groups. His analysis points to the fact that the classification of the type of groups cannot, in all likelihood, be determined by a "local" analysis of terms; but rather one needs to know how the terms interact in a global fashion, i.e., some special properties of the free objects. Recall that the size of a set of free generators in a free group is an invariant, called the *rank* of the free group. (Any variety with a nontrivial finite member has such a rank function.)

Now we give Lawrence's analysis of groups.

- Groups have infinitary unification type.

Let $\mathbf{F}(\kappa)$ be the free group freely generated by κ elements. Two key properties are needed:

[**Schreier**] Subgroups of finitely generated free groups are free.

[**Hopf**] Given a homomorphism $\sigma : \mathbf{F}(n) \to \mathbf{F}(\kappa)$, if σ is not one-to-one then the rank of $\sigma(\mathbf{F}(n))$ is less than n.

Let us first use these properties to show that the unification type of $x \cdot y \approx y \cdot x$ is nullary.

> Let $\sigma : \mathbf{F}(2) \to \mathbf{F}(\omega)$ be a unifier of $x \cdot y \approx y \cdot x$. Then σ is not one-to-one, so the rank of $\sigma(\mathbf{F}(2))$ is either 0 or 1. If it is 0 then we have the trivial unifier which maps x and y to e. If it is 1 then we have $\sigma(x)$ and $\sigma(y)$ in a cyclic subgroup of $\mathbf{F}(\omega)$, so there is an element s of $\mathbf{F}(\omega)$, and integers i and j, such that $\sigma(x) = s^i$, $\sigma(y) = s^j$.
>
> Now we leave it as an exercise to show that the most general unifiers of $x \cdot y \approx y \cdot x$ are obtained by letting s be (the coset of) a variable z, and by choosing i and j to be coprime integers. Thus we have found an equation of infinitary unification type.

Thus the type of groups is either infinitary or nullary. It only remains to rule out nullary.

REMARK 17 This conclusion applies to semigroups and monoids since the ω-generated free object in each case is a subreduct[2] of the ω-generated free group (see the exercises).

Now suppose we are given some finite set S of group equations, and suppose that $\sigma \in U_E(S)$ is not a most general unifier of S. Then there is a $\sigma_0 \in U_E(T)$ such that $\sigma_0 <_E \sigma$. In particular we have a $\tau : \mathbf{F}(\omega) \to \mathbf{F}(\omega)$ such that $\sigma = \tau \circ \sigma_0$.

As $\sigma_0(\mathbf{F}(n))$ is a free group of rank n_1 for some $n_1 \leq n$, and since $\mathbf{F}(n_1) * \mathbf{F}(\omega) \simeq \mathbf{F}(\omega)$, we have a $\sigma' \in U_E(S)$ and a $\tau_0 : \mathbf{F}(\omega) \to \mathbf{F}(\omega)$ such that

- $\sigma_0 = \tau_0 \circ \sigma'$
- τ_0 is one-to-one on the range of σ'
- the range of σ' is the subgroup of $\mathbf{F}(\omega)$ generated by $\{x_1, \cdots, x_{n_1}\}$.

As $\sigma' \leq_E \sigma_0 <_E \sigma$, we have $\sigma' <_E \sigma$.

Now if σ' is not a most general unifier of S, then by repeating this process one can find $n_2 \leq n_1$ and $\sigma'' \in U_E(S)$ such that $\sigma'' <_E \sigma'$, and the range of σ' is the subgroup of $\mathbf{F}(\omega)$ generated by $\{x_1, \cdots, x_{n_2}\}$. Let $\tau' : \mathbf{F}(\omega) \to \mathbf{F}(\omega)$ be such that $\sigma' = \tau' \circ \sigma''$. Then τ' maps the range of σ'' onto the range of σ', so τ' cannot be one-to-one on the range of σ'' (otherwise we could show $\sigma' \leq_E \sigma''$). By the Hopf property it follows that $n_2 < n_1$.

Consequently one can only apply the $'$ operation above finitely many times before reaching a most general unifier. This proves groups are not nullary, and finishes the proof that the type of groups is indeed infinitary. ■

Lawrence continues his work on groups to show that most general unifiers of a finite set S of group equations in the variables $\{x_1, \cdots, x_n\}$ are in one-to-one correspondence with the the minimal normal subgroups $\mathbf{N}$ of $\mathbf{F}(n)$ which identify the left and right hand sides of the various equations in S, and are such that $\mathbf{F}(n)/\mathbf{N}$ is free. Then Lawrence applies a classical algorithm (of Nielsen) to get a set of free generators, and this gives an algorithm for

[2] A subalgebra of a reduct to the appropriate language.

generating the most general unifiers of S. (We note that the unification problem for groups is trivial — terms can always be unified.)

An unsolved problem posed by Lawrence is the following.

<u>Open Problem</u>

Will the unification type of any finite set of group equations be either unitary or infinitary?

For any variety of Abelian groups the unification type is unitary. Albert and Lawrence have carried out a thorough analysis of nilpotent class c groups, for $c > 1$. Such classes are always nullary. Furthermore any finite set of equations is either unitary or nullary, and they have found an algorithm which determines which case holds; and, if the answer is unitary, then it gives the most general unifier.

EXAMPLE 18 [Commutative Rings]

Commutative rings have been studied by computer scientists (sometimes described as algebras related to Hilbert's Tenth Problem). For commutative rings the free objects are the well-known polynomial rings:

$$\begin{aligned} \mathbf{F}(n) &= \mathbf{Z}[x_1, \cdots, x_n] \\ \mathbf{F}(\omega) &= \mathbf{Z}[x_1, x_2, \cdots] \end{aligned}$$

A system of commutative ring equations can be thought of as a system of Diophantine equations, and unification is concerned with finding solutions in the above polynomial ring $\mathbf{Z}[x_1, x_2, \cdots]$. This is actually present in classical number theory, for example the most general solutions of the Pythagorean equation $x^2 + y^2 \approx z^2$ have long been known to be the following eight:

$$\begin{aligned} \sigma(x) &= \pm w(u^2 - v^2) \\ \sigma(y) &= \pm w(2uv) \\ \sigma(z) &= w(u^2 + v^2) \end{aligned}$$

and

$$\begin{aligned} \sigma(x) &= \pm w(2uv) \\ \sigma(y) &= \pm w(u^2 - v^2) \\ \sigma(z) &= w(u^2 + v^2). \end{aligned}$$

There is a close tie between solving a set S of commutative ring equations in the integers $\mathbf{Z}$ and solving them in the polynomial ring $\mathbf{Z}[x_1, x_2, \cdots,$ namely

- S is solvable in $\mathbf{Z}$ iff in $\mathbf{Z}[x_1, x_2, \cdots]$.

This follows from the fact that $\mathbf{Z}$ is both a subring and a homomorphic image of the polynomial ring. Consequently the unification problem for commutative rings is precisely the problem of the solvability of Diophantine systems in the integers, known as Hilbert's Tenth problem. Matijasevic, building on the work of Davis, Putnam, and Robinson, proved that there is no algorithm to determine if a finite system of Diophantine equations can be solved in the integers. Consequently the unification problem for commutative rings is undecidable.

We do not know the exact unification of type of commutative rings, but we have narrowed it down:

- Commutative rings are either infinitary or nullary.

To see this we will show that the Pell equation

$$x^2 - 3y^2 - 1 \approx 0 \tag{6}$$

is infinitary. First we know that (a, b) is a solution in integers iff

$$|a| + \sqrt{3}|b| = (2 + \sqrt{3})^n$$

for some integer n. Thus there are an infinite number of constant solutions to (6). We will show that there are no other solutions in $\mathbf{Z}[x_1, x_2, \cdots]$, and then it follows that the constant solutions are all most general, so the type of (6) is indeed infinitary.

If there is a nonconstant solution $(s_1(x_1, \cdots, x_k), s_2(x_1, \cdots, x_k))$ of (6) then there is a nonconstant solution $(t_1(x), t_2(x))$ in only one variable. Now the sequence

$$|t_1(n)| + \sqrt{3}|t_2(n)|$$

has polynomially bounded growth, and it is eventually strictly increasing. But then it must eventually be a subsequence of $(2 + \sqrt{3})^n$. This is impossible. ■

<u>Open Problem</u>

Is the unification type of commutative rings infinitary? (I.e., does every solution of a finite set of Diophantine equations come from a most general solution?)

EXAMPLE 19 [Boolean Algebras]

Let E be a set of equational axioms for Boolean algebras. In 1987 Büttner & Simonis proved that the unification type of E is unitary. To see this let s, t be E-unifiable terms, and let σ_0 be a fixed E-unifier of s, t. Then we claim that the most general E-unifier of s, t is given by

$$\mu(x_i) = [(s+t)' \wedge x_i] \vee [(s+t) \wedge \sigma_0(x_i)]$$

where $+$ is the usual "symmetric difference" of Boolean algebras, since one has

i. $BA \models \sigma(s) \approx \sigma(t)$, and

ii. for $\sigma \in U_E(s,t)$ we have $\sigma = \sigma \circ \mu$.

EXAMPLE 20 [Discriminator Varieties]

In 1990 Nipkow published a proof that the variety determined by a primal algebra has unitary unification type. Such varieties are special cases of discriminator varieties. For definitions, examples, and a proof that discriminator varieties have unitary unification type. see [7].

A short table of some of the more popular sets of equationally defined classes follows, with their types (if known):

Equational Class	Unification Type	Discovered by
semigroups	infinitary	Plotkin (1972)
commutative semigroups	finitary	Livesey & Siekmann (1976); Stickel (1975, 1981)
semilattices	finitary	Livesey & Siekmann (1976); Büttner (1986)
distributive lattices	nullary	Willard (1989)
Boolean algebras	unitary	Büttner & Simonis (1987)
discriminator varieties	unitary	Burris (1989)
Abelian groups	finitary	Lankford (1979)
groups	infinitary	Lawrence (1989)
commutative rings	infinitary or nullary	Burris & Lawrence (1989)
rings	infinitary	Lawrence (1989)
lattices	nullary	Willard (1991)
Heyting algebras		

Other recent results include

- M. Albert and R. Willard have classified (1989) the unification type of all equational theories of two-element algebras (making use of Post's classification of the clones on 2 elements).

- Willard recently proved that the equational theory of a finite algebra can be of infinitary type.

- If one takes the language $\{+, \times, 0, 1\}$, that is the language of rings without the operation *minus*, then one can write down a finite set of equational axioms E whose consequences are precisely the consequences of commutative ring theory which do not mention minus. Such a system was studied by Franzen in *Hilbert's tenth problem is of unification type zero*, J. Automated Reasoning **9** (1992), 169–178, where he shows the unification type is nullary. In spite of the title of the paper, his result does not resolve the unification type of commutative rings — having the minus operation gives a radically different situation.

EXERCISES

Problem 1 Prove $\leq_E$ is a preorder on $\{\sigma : \mathbf{F}_n \to \mathbf{F}_\omega\}$.

Problem 2 [Freese] Let E be of finitary unification type.

(a) Prove that every chain of substitutions from $\{\sigma : \mathbf{F}_n \to \mathbf{F}_\omega\}$ (under $\leq_E$) has a lower bound.

(b) Prove that every downward directed set of substitutions from $\{\sigma : \mathbf{F}_n \to \mathbf{F}_\omega\}$ (under $\leq_E$) has a lower bound.

Problem 3 Let E define semigroups. Give an algorithm to determine if $\sigma_1 \leq_E \sigma_2$, where $\sigma_1, \sigma_2 : \mathbf{F}_n \to \mathbf{F}_\omega$.

Problem 4 Let E define groups. Let $\mu_{i,j}$ be the substitution defined by

$$\begin{aligned} \mu_{i,j}(x) &= z^i \\ \mu_{i,j}(y) &= z^j. \end{aligned}$$

(a) Prove that, up to equivalence, the most general E-unifiers of $x \cdot y \approx y \cdot x$ are given by the $\mu_{i,j}$ with $i, j \in Z$ and $gcd(i,j) = 1$.

(b) Show that $\mu_{i,j} \sim_E \mu_{-i,-j}$, for $i, j \in Z$.

(c) Show that the $\mu_{i,j}$ with $gcd(i,j) = 1$ and $max(i,j) > 0$ gives a complete list (up to equivalence) of pairwise inequivalent most general E-unifiers of $x \cdot y \approx y \cdot x$.

Problem 5 Let E define semigroups. Prove that the $\mu_{i,j}$ of Problem 4, where $i, j \in N$, give a complete list (up to equivalence) of pairwise inequivalent most general E-unifiers of $x \cdot y \approx y \cdot x$.

Problem 6 Let $E = \{(x \cdot y) \cdot z \approx x \cdot (y \cdot z), x \cdot e \approx x, e \cdot x \approx x\}$; so E defines *monoids*. Prove that the unification type of E is infinitary.

Problem 7 Verify that Boolean algebras have unitary unification type. [Hint: check the claims at the end of Example 19.]

Problem 8 $\star$ Show semilattices (i.e., idempotent commutative semigroups) have finitary unification type.
[Hint: the elements of the free semilattices can be thought of as nonempty sets of variables.]

Problem 9 $\star$ Show commutative semigroups have finitary unification type.

References

[1] M.H. Albert and R.W. Willard, Classification of the unification type of two element algebras. (in preparation)

[2] Franz Baader and Jörg Siekmann, Unification theory. To appear in D.M. Gabbay, C.J. Hogger, and J.A. Robinson (ed.) *Handbook of Logic in Artificial Intelligence and Logic Programming*, Oxford University Press.

[3] W.W. Bledsoe and D.W. Loveland, editors, Automated Theorem Proving after 25 Years. Contemporary Math. **29**, Amer. Math. Soc., 1983.

[4] Stephen L. Bloom and Ralph Tindell, Varieties of "if-then-else". Siam J. Comput. **12** (1983), 677–707.

[5] Ronald V. Book, Thue systems as rewriting systems. J. Symbolic Computation **3** (1987), 39–68.

[6] S. Burris and J. Lawrence, Unification in commutative rings is not finitary. Information Processing Letters **36** (1990), 37–38.

[7] S. Burris, Discriminator varieties and symbolic computation. J. Symbolic Computation **13** (1992), 175–207.

[8] J. Lawrence, Unification in classical algebraic systems. (in preparation)

[9] J. Lawrence, Unification in varieties of groups. (in preparation)

J.H. Siekmann, Unification theory. J. Symbolic Computation **7** (1989), 207–274.