A Refined Version of General E-Unification

Rolf Socher-Ambrosius*

MPI Informatik, Im Stadtwald, D-66123 Saarbrücken, Germany
Tel. +49–681–302–5367
e-mail: socher@mpi-sb.mpg.de

Abstract Transformation-based systems for general E-unification were first investigated by Gallier and Snyder. Their system extends the well-known rules for syntactic unification by Lazy Paramodulation, thus coping with the equational theory. More recently, Dougherty and Johann improved on this method by giving a restriction of the Lazy Paramodulation inferences. In this paper, we show that their system can be further improved by a stronger restriction on the applicability of Lazy Paramodulation. It turns out that the framework of proof transformations provides an elegant and natural means for proving completeness of the inference system.

1 Introduction

This paper describes a transformation based procedure for unification in an arbitrary equational theory representable by an equational system E. Since unification is now commonly being regarded as equation solving, the transformations operate on equational systems. J. Gallier and W. Snyder [2, 3] were the first to study transformation based methods for E-unification. They devised an inference system for general E-unification consisting of the common rules for syntactic unification together with an

* This work was funded by the German Ministry for Research and Technology (BMFT) under grant ITS 9103.

additional *Lazy Paramodulation* rule, which takes the equational theory into account. Paramodulation steps are done lazily so that the nondeterministic algorithm induced by the transformations is complete even when paramodulation into variables is forbidden. For instance, given the equational theory

$$E = \{f(a, b) \approx a,\ a \approx b\}$$

and the E-unification problem $\{f(x, x) \approx x\}$, no paramodulation step applies at a nonvariable position. One would thus have to paramodulate into one of the variables of the term $f(x, x)$. Instead, Gallier and Snyder do allow paramodulation into the term $f(x, x)$, trading the immediate unification of the terms $f(x, x)$ and $f(a, b)$ for an additional E-unification problem $f(x, x) \approx f(a, b)$. Their system thus allows an inference

$$\{f(x, x) \approx x\} \Rightarrow \{f(x, x) \approx f(a, b),\ a \approx x\} \tag{1}$$

In [1], D. Dougherty and P. Johann improve on Gallier and Snyder's system by restricting the applicability of Lazy Paramodulation to so called *top unifiable* term-pairs. Two terms are top unifiable if they agree on those positions that are function positions in both terms. Decomposition of top unifiable term-pairs thus eventually leads to an equational system of the form $\{x_1 \approx t_1, \ldots, x_n \approx t_n\}$. The terms $f(x, x)$ and $f(a, b)$, for instance, are top unifiable, while $f(x, a)$ and $f(a, b)$ are not. Therefore, in solving the E-unification problem of the preceding paragraph, we must consider the inference (1), whereas for the problem $\{f(x, a) \approx x\}$ under the same theory E, it is not necessary to infer the equation $f(x, a) \approx f(a, b)$. Such a restricted Lazy Paramodulation rule, together with the requirement that the top unifiable term-pair is decomposed immediately, is called *Relaxed Paramodulation*. The intuitive argument for this restriction is provided by an innermost strategy applying to the subterm a of $f(x, a)$ rather than to the whole term itself.

This paper provides two additional restrictions to Gallier and Snyder's E-unification transformations. First, we show that Lazy Paramodulation can be constrained even further to apply only to so called *top left unifiable* pairs, without sacrificing completeness. Consider, for instance, the theory

$$E = \{f(x, x) \approx x,\ a \approx b\},$$

and the unification problem $\{f(a, b) \approx a\}$. The terms $f(x, x)$ and $f(a, b)$ are top unifiable, thus giving rise to a Relaxed Paramodulation inference

$$\{f(a, b) \approx a\} \Rightarrow \{x \approx b, x \approx a\}$$

at the root. However, applying an innermost strategy, one would preferably paramodulate into the subterm b of the unification problem, thus deriving

$$\{f(a, b) \approx a\} \Rightarrow \{f(a, a) \approx a\}.$$

The *outermost* inference step is unnecessary, because we can rely on an innermost strategy to yield the same solution $\{x \approx a\}$. This observation is generalized to restrict Lazy Paramodulation to top left unifiable pairs.

We also show that inference steps need not be applied to solved equations. This result, although both intuitive and expected, has not previously been proved.

The rest of the introduction reviews the basic notation used in the text.

Given a signature $\mathcal{F}$ of *function symbols*, each $f \in \mathcal{F}$ coming with an arity $\alpha(f) \geq 0$, and a set $\mathcal{V}$ of *variables*, the set $\mathcal{T}(\mathcal{F}, \mathcal{V})$ is defined to be the set of *terms* built over $\mathcal{V}$ using the function symbols in $\mathcal{F}$. For any object o, $\mathcal{V}ar(o)$ denotes the set of variables occurring in o. A *position* in a term t is a sequence of natural numbers referring to a subterm of t, the root position is denoted by Λ. The set of positions of a term t is denoted by $\mathcal{P}os(t)$, the set of variable positions by $\mathcal{VP}os(t)$, and the set of nonvariable positions by $\mathcal{FP}os(t)$. If $p \in \mathcal{P}os(t)$ is a position in t, then $t|_p$ denotes the subterm of t at position p, $t[s]_p$ denotes replacement of $t|_p$ by s, and $t(p)$ denotes the function or variable symbol at position p.

A *substitution* is the unique extension of a mapping $\sigma : \mathcal{V} \rightarrow \mathcal{T}(\mathcal{F}, \mathcal{V})$ with finite domain $\mathcal{D}om(\sigma)$ to the free $\mathcal{F}$-algebra $\mathcal{T}(\mathcal{F}, \mathcal{V})$ over generators $\mathcal{V}$. We write substitutions in suffix notation. A substitution σ with domain $\{x_1, \ldots, x_n\}$ will be written in the form $\{x_1 \leftarrow x_1\sigma, \ldots, x_n \leftarrow x_n\sigma\}$. The *restriction* $\sigma|_V$ of σ to a set $V \subseteq \mathcal{V}$ is the substitution $\sigma|_V$ defined by $x\sigma|_V = x\sigma$ for $x \in V$, and $y\sigma|_V = y$ for $y \notin V$.

An *equation* is an unordered pair $s \approx t$ of terms, an (equational) *system* is a finite set of equations. If $\sigma = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$ is a substitution, then $[\sigma]$ denotes the equational system $\{x_1 \approx t_1, \ldots, x_n \approx t_n\}$.

The relation $\leftrightarrow$ is defined by

$$s \leftrightarrow_{[p, l \approx r, \sigma]} t$$

iff $s|_p = l\sigma$ and $t = s[r\sigma]_p$. Note that because $l \approx r$ is an unordered pair, $\leftrightarrow$ is a symmetric relation. By $\leftrightarrow^*$, we denote the transitive and reflexive closure of $\leftrightarrow$. If E is an equational system, we write $s \leftrightarrow_{E,\sigma} t$ to denote that $s \leftrightarrow_{[p, l \approx r, \sigma]} t$ holds for some position $p \in \mathcal{Pos}(s)$ and some equation $l \approx r \in E$. The relation $\leftrightarrow^*_E$ is more conveniently denoted by $=_E$. A *proof* P of $s \approx t$ in E is a sequence

$$s \leftrightarrow_{[p_1, l_1 \approx r_1, \sigma_1]} \cdots \leftrightarrow_{[p_n, l_n \approx r_n, \sigma_n]} t$$

of *proof steps*. The p_i are the positions *used by* P. A proof step at the root position Λ is called a *root step*. If $\Pi \subseteq \mathcal{Pos}(s)$, then a proof P of $s \approx t$ is a *proof below* Π if any position q used by P satisfies $q \geq p$ for some $p \in \Pi$.

Let E be an equational system. The substitution σ is said to *E-unify* the equation $s \approx t$ if $s\sigma =_E t\sigma$; it E-unifies the system S if it simultaneously E-unifies each equation in S. By $u_E(S)$, we denote the set of all E-unifiers of S. Given two systems S and S', we write $S \leq_E S'$ if $u_E(S') \subseteq u_E(S)$. The corresponding *subsumption ordering* $\leq_E$ on substitutions is defined by $\sigma \leq_E \theta$ if $\sigma\theta =_E \theta$. It is not hard to see that σ is the smallest substitution that E-unifies the equational system $[\sigma]$.

A system $S = \{x_1 \approx t_1, \ldots, x_n \approx t_n\}$ is in *solved form* if each x_i occurs only once in S. An equation $s \approx t$ is called *solved* provided the system $\{s \approx t\}$ is solved. If $S = [\sigma]$ is a system in solved form and V is a set of variables, then $S|_V$ is defined by

$$S|_V = [\sigma|_V] = \{x \approx t \mid x \approx t \in S \text{ and } x \in V\}.$$

Given a system S, we say that a solved system $[\sigma]$ is an *E-solution* of S if $S \leq_E [\sigma]$. In particular, then $\sigma \in u_E(S)$. If $[\sigma]$ is an E-solution of $t \approx s$, so that $s\sigma =_E t\sigma$, then there exists a proof P of the form

$$t \leftrightarrow^*_{[\sigma],\varepsilon} t\sigma \leftrightarrow_E \ldots \leftrightarrow_E s\sigma \leftrightarrow^*_{[\sigma],\varepsilon} s \tag{1}$$

where ε denotes the identity substitution. Such a proof P is called a *canonical* proof of $t \approx s$ in ($[\sigma]$, E).

By $\mu(P)$, we denote the number of E-steps of P, and by $\mu_\sigma(P)$, the number of $[\sigma]$-steps of P. Similarly, if S is a system and P_i is a canonical proof of $t_i \approx s_i$ in ($[\sigma]$, E) for each $t_i \approx s_i \in S$, then the set $\mathscr{P} = \{P_i \mid t_i \approx s_i \in S\}$ is called a canonical proof of S in ($[\sigma]$, E), and $\mu(\mathscr{P}) = \sum_i \mu(P_i)$, and $\mu_\sigma(\mathscr{P}) = \sum_i \mu_\sigma(P_i)$.

We call the variable $x \in \mathcal{Var}(t)$ *normalized* in P if there is some $p \in \mathcal{VPos}(t)$ with $t|_p = x$ such that no E-step of P is below p. As an example, the variable x is normalized in the proof

$$f(x,x,y) \leftrightarrow_{[\{x \leftarrow a,\, y \leftarrow b\}]} f(a,a,b) \leftrightarrow_{a \approx c} f(a,c,b) \leftrightarrow_{b \approx c} f(a,c,c)$$

because no E-step applies below the first argument position. Unlike x, the variable y is not normalized. However, it is possible to normalize y, too, by using the E-equivalent substitution $\{x \leftarrow a, y \leftarrow c\}$ in the proof

$$f(x,x,y) \leftrightarrow_{[\{x \leftarrow a,\, y \leftarrow c\}]} f(a,a,c) \leftrightarrow_{a \approx c} f(a,c,c).$$

In general, suppose the variable x is not normalized in P. Then P is of the form

$$t[x]_p \leftrightarrow^*_{[\sigma]} t\sigma[x\sigma]_p \leftrightarrow_{(q,l \approx r,\theta)} t\sigma[w]_p \leftrightarrow^*_E s\sigma \leftrightarrow^*_{[\sigma]} s\,,$$

with $q \geq p$. We define a substitution σ' by

$$y\sigma' = \begin{cases} w & \text{if } y = x \\ y\sigma & \text{otherwise} \end{cases}$$

Then $\sigma =_E \sigma'$ and the proof

$$P' = t[x]_p \leftrightarrow^*_{[\sigma']} t\sigma'[w]_p \leftrightarrow^*_E t\sigma[w]_p \leftrightarrow^*_E s\sigma \leftrightarrow^*_E s\sigma' \leftrightarrow^*_{[\sigma']} s$$

is a proof of $t \approx s$ in $([\sigma'], E)$. Continuing this process, we eventually obtain a substitution $\overline{\sigma}$ with $\overline{\sigma} =_E \sigma$, and a proof $\overline{P}$ of $t \approx s$ in $([\overline{\sigma}], E)$ of the form

$$t[x]_p \leftrightarrow^*_{[\overline{\sigma}]} t\overline{\sigma}[w]_p \leftrightarrow^*_E s\overline{\sigma} \leftrightarrow^*_{[\overline{\sigma}]} s,$$

such that no E-step of $\overline{P}$ is below p. Then the variable x is normalized in P. Likewise, we can construct to any proof $\mathscr{P}$ of S a proof $\mathscr{P}'$ such that every variable $x \in \mathscr{Var}(S)$ is normalized in some $P \in \mathscr{P}$. We call such a canonical proof $\mathscr{P}$ of a system S *normalized*.

2 An Inference System For E- Unification

In the following, let E be a fixed but arbitrary equational system. In order to understand the various restrictions of Lazy Paramodulation, it is useful to consider the effects they have on equational proofs. The basic idea is that if $[\sigma]$ is an E-solution of the equation $t \approx s$, then there is a canonical proof P of $t \approx s$ in $([\sigma], E)$. This proof serves as a guide to selecting an inference step. For instance, given such a proof P as in (1), we might guess the following E-step $u \leftrightarrow_{[p, l \approx r, \theta]} v$, with $p \in \mathscr{FPos}(t)$,

$$\begin{array}{ccccccc} t & & u[l]_p & & u[r]_p & & s \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ t\sigma & \leftrightarrow^*_E & u[l\theta]_p & \leftrightarrow^*_E & u[r]_p & \leftrightarrow^*_E & s\sigma \end{array}$$

thus breaking the proof P into two parts

$$t \leftrightarrow^*_{[\sigma]} t\sigma \leftrightarrow^*_E u[l\theta]_p \leftrightarrow^*_{[\theta]} u[l]_p, \tag{2}$$

and

$$u[r]_p \leftrightarrow^*_{[\theta]} u[r\theta]_p \leftrightarrow^*_E s\sigma \leftrightarrow^*_{[\sigma]} s. \tag{3}$$

The proof (2) can be further decomposed into a subproof below the position p and another subproof using the remaining positions to yield

$$t|_p \leftrightarrow^*_{[\sigma]} t\sigma|_p \leftrightarrow^*_E l\theta \leftrightarrow^*_{[\theta]} l \tag{4}$$

and

$$t[*]_p \leftrightarrow_{[\sigma]} t\sigma[*]_p \leftrightarrow^*_E u[*]_p. \tag{5}$$

Here we use the symbol $*$ as a new constant, indicating a "hole" in a term. Now parts (3) and (5) yield a proof

$$t[r]_p \leftrightarrow u[r]_p \leftrightarrow_{[\theta]} u[r\theta]_p \leftrightarrow^*_E s\sigma \leftrightarrow_{[\sigma]} s \tag{6}$$

This proof transformation corresponds to the Lazy Paramodulation inference

$$\{t \approx s\} \Rightarrow \{t|_p \approx l,\ t[r]_p \approx s\}.$$

The derived equations have proofs (4) and (6), respectively. In this manner we can find for every E-step of the proof P that uses a function position of t a corresponding Lazy Paramodulation step.

The effect of our restriction on Lazy Paramodulation inferences now consists in a specification of the E-step to be guessed. *Almost Lazy Paramodulation* tries to guess an *innermost* E-step $u \leftrightarrow_{[p, l\approx r, \theta]} v$, with $p \in \mathcal{FPos}(t)$. For such a step, the subproof

$$t\sigma|_p \leftrightarrow^*_E l\theta \tag{7}$$

in (4) is below $\mathcal{VPos}(t)$. We will therefore require for an almost Lazy Paramodulation step into $t \approx s$ with $l \approx r$ at position $p \in \mathcal{FPos}(t)$ that there exist substitutions σ and θ and a proof of the form (7) below $\mathcal{VPos}(t)$. This condition will be realized by so called *top left unification*, a refinement of the notion of top unification introduced in [1].

Definition 1 (*Top Unification*) *The terms s and t are said to be* **top unifiable** *if $s(p) = t(p)$ for all $p \in \mathcal{FPos}(s) \cap \mathcal{FPos}(t)$. In this case, the set $tu(s,t)$ is defined by*

$$tu(s,t) = \{s|_p \approx t|_p \mid p \in \mathcal{Pos}(s) \cap \mathcal{Pos}(t) \cap (\mathcal{VPos}(s) \cup \mathcal{VPos}(t))\}.$$

In other words, for two terms s and t to be top unifiable means that decomposition of $s \approx t$ does not fail and eventually produces a system of the form $\{x_1 \approx t_1, \ldots, x_n \approx t_n\}$. This system is precisely the set $tu(s,t)$.

Definition 2 (*Top Left Unification*) *Given two variable disjoint terms s and t, define*

$$M(s,t) = \{(u,v) \mid u \approx x, v \approx x \in tu(s,t), x \in \mathcal{Var}(t)\}.$$

The (ordered) pair (s, t) is said to be **top left unifiable** *if it is top unifiable and if additionally every pair $(u, v) \in M(s, t)$ is top unifiable too.*

The following example illustrates the concept of top left unification.

Example 3 *a) Let $s = f(a, b)$ and $t = f(x, x)$. Then the pair (s, t) is top unifiable, because $\mathcal{FPos}(s) \cap \mathcal{FPos}(t) = \{\Lambda\}$ and $s(\Lambda) = f = t(\Lambda)$. It is not top left unifiable, because $M(s, t) = \{(a, b)\}$ and (a, b) is not top unifiable.*

b) Let $s = f(g(u), g(v))$ and $t = f(x, x)$. Then as above, s and t are top unifiable, $M(s, t) = \{(g(u), g(v))\}$ and therefore s and t are also top left unifiable.

The following lemma is crucial for the completeness proof of our inference system for E-unification.

Lemma 4 *Let s and t be variable disjoint terms, and let σ be a substitution.*

If there is a canonical proof $t\sigma \leftrightarrow_E^* s\sigma$ below $\mathcal{VPos}(t)$, then the pair (t, s) is top left unifiable.

Proof. Since there is a proof $t\sigma \leftrightarrow_E^* s\sigma$ below $\mathcal{VPos}(t)$,

$$t(p) = t\sigma(p) = s\sigma(p) = s(p)$$

holds for all $p \in \mathcal{FPos}(s) \cap \mathcal{FPos}(t)$, hence the pair (t, s) is top unifiable. Now let $(u, v) \in M(t, s)$. Then there exists an $x \in \mathcal{Var}(s)$ such that $u \approx x$ and $v \approx x$ are both in $tu(t, s)$, and positions p and q, such that $t|_p = u$, $s|_p = x$, $t|_q = v$, and $s|_q = x$. Hence there is a proof $u\sigma \leftrightarrow_E^* x\sigma$ below $\mathcal{VPos}(u)$ and a proof $v\sigma \leftrightarrow_E^* x\sigma$ below $\mathcal{VPos}(v)$. These combine to form a proof P of the form

$$u\sigma \leftrightarrow_E^* x\sigma \leftrightarrow_E^* v\sigma$$

such that each position used by P is below $\mathcal{VPos}(u)$ or below $\mathcal{VPos}(v)$. This implies that the pair (u, v) is top unifiable. Now we have shown that (t, s) is top unifiable and that any $(u, v) \in M$ is top unifiable. The pair (t, s) thus is top left unifiable. $\square$

The following definition introduces Almost Lazy Paramodulation.

Definition 5 *The inference system* $\mathcal{T}_E$ *comprises the rules shown in Figure* 1.

We write $S \Rightarrow S'$, if S' is obtained from S by application of an inference rule in $\mathcal{T}_E$.

There are two substantial differences between $\mathcal{T}_E$ and the inference systems proposed in [3] and [1]. First, $\mathcal{T}_E$ restricts Lazy Paramodulation to *unsolved equations* $s \approx t$. Second, it replaces *top unifiability* by the stronger condition of *top left unifiability*. Computation with $\mathcal{T}_E$ is illustrated by the following example.

Example 6 *Let*

$$E = \{f(x, x) \approx x,\ a \approx b\}$$

be an equational theory and let $S = \{f(a, b) \approx a\}$ *be an E-unification problem. The terms* $f(x, x)$ *and* $f(a, b)$ *are top unifiable with* $tu(f(x, x), f(a, b)) = \{x \approx a, x \approx b\}$. *The inference system in* [1] *thus admits the Relaxed Paramodulation inference*

$$\{f(a, b) \approx a\} \Rightarrow \{x \approx a, x \approx b, x \approx a\}.$$

This inference step is not possible in the inference system $\mathcal{T}_E$, *because* $tlu(f(a, b), f(x, x))$ *is not defined. Instead, the unification problem* S *is solved via the derivation*

$$\begin{aligned} \{f(a, b) \approx a\} &\Rightarrow \{f(a, a) \approx a\} && \text{(Almost Lazy Paramodulation with } b \approx a\text{)} \\ &\Rightarrow \{x \approx a, a \approx a\} && \text{(Almost Lazy Paramodulation with } f(x,x) \approx x\text{)} \\ &\Rightarrow \{x \approx a\}. && \text{(Trivial)} \end{aligned}$$

Trivial	$$\frac{\{t \approx t\} \cup S}{S}$$
Decomposition	$$\frac{\{ft_1 \ldots t_n \approx fs_1 \ldots s_n\} \cup S}{\{t_1 \approx s_1, \ldots, t_n \approx s_n\} \cup S}$$
Variable Elimination	$$\frac{\{x \approx t\} \cup S}{\{x \approx t\} \cup S\{x \leftarrow t\}}$$
if $x \notin \mathcal{Var}(t)$ *and* $x \in \mathcal{Var}(S)$.	
Almost Lazy Paramodulation	$$\frac{\{s \approx t\} \cup S}{tu(s\|_p \approx l) \cup \{s[r]_p \approx t\} \cup S}$$
if $s \approx t$ *is not solved,* $p \in \mathcal{FPos}(s)$, and $l \approx r \in E$.	

Figure 1*: The Inference System* $\mathcal{T}_E$

We call an inference system T *correct* if $S \Rightarrow_T S'$ implies $S \leq_E S'$. The correctness of our inference system $\mathcal{T}_E$ follows immediately from the soundness of Gallier and Snyder's transformations.

Theorem 7 *The inference system* $\mathcal{T}_E$ *is correct.*

In the following, we show that the inference system $\mathcal{T}_E$ is also complete, that is, given a system S with $\mathcal{Var}(S) = V$ and a solution $[\sigma]$ of S, there exists a derivation $S \Rightarrow^* [\sigma']$ such that $\sigma'|_V \leq \sigma$. Our completeness proof uses a well-founded ordering $>$ on proofs. The basic idea of the proof is as follows: Given a reducible system S, there exists a (normalized canonical) proof $\mathcal{P}$ of S. We construct a system S' with $S \Rightarrow S'$ and a proof $\mathcal{P}'$ of S' such that $\mathcal{P}' < \mathcal{P}$. The proof ordering $>$ is well-founded, so there exists a terminating derivation $S \Rightarrow^* S''$ such that S'' is irreducible by $\mathcal{T}_E$ and hence in solved form. It then remains to verify that for $S'' = [\sigma']$ the relation $\sigma'|_V \leq \sigma$ holds.

Definition 8 *For any proof P of* $t \approx s$*, we define a measure* μ_1 *by*

$$\mu_1(P) = \left|\mathcal{Pos}(t)\right| + \left|\mathcal{Pos}(s)\right|$$

Likewise, if $\mathcal{P}$ *is a proof of a system* S*, we define* $\mu_1(\mathcal{P}) = \Sigma_{P\in\mathcal{P}}\ \mu_1(P)$*. We define orderings* $>_1$*,* $>_2$*,* $>_3$ *on proofs by*

$$\mathcal{P} >_1 \mathcal{P}' \text{ if } \mu(\mathcal{P}) > \mu(\mathcal{P}')$$
$$\mathcal{P} >_2 \mathcal{P}' \text{ if } \mu_\sigma(\mathcal{P}) > \mu_\sigma(\mathcal{P}')$$
$$\mathcal{P} >_3 \mathcal{P}' \text{ if } \mu_1(\mathcal{P}) > \mu_1(\mathcal{P}').$$

Finally, the ordering $>$ *on proofs is defined to be the threefold lexicographic combination* $(>_1,>_2,>_3)$.

It is clear that the proof ordering $>$ is well-founded.

Lemma 9 *Let* S *be a system with* $V = \mathcal{Var}(S)$ *and let* $[\sigma]$ *be an* E*-solution of* S*. Moreover, let* $\mathcal{P}$ *be a normalized canonical proof of* S *in* $([\sigma], E)$.

If S *is reducible by* $\mathcal{T}_E$*, then there exists a system* S' *with* $S \Rightarrow S'$ *and a substitution* σ' *with* $\sigma'\big|_V = \sigma$ *such that* S' *has a normalized canonical proof* $\mathcal{P}'$ *in* $([\sigma'], E)$ *with* $\mathcal{P} > \mathcal{P}'$.

Proof. We can assume without loss of generality that S contains no trivial equations.

Case 1: If $S = \{ft_1 \ldots t_n \approx fs_1 \ldots s_n\} \cup W$ and $P \in \mathcal{P}$ is a normalized canonical proof of $ft_1 \ldots t_n \approx fs_1 \ldots s_n$ in $([\sigma], E)$ that contains no root step, then for each i, $1 \leq i \leq n$, there exists a normalized canonical proof P_i of $t_i \approx s_i$ in $([\sigma], E)$. Now let $\sigma' = \sigma$,

$$S' = \{t_1 \approx s_1,\ldots, t_n \approx s_n\} \cup W$$

and

$$\mathcal{P}' = \{P_1,\ldots, P_n\} \cup \mathcal{P} - \{P\}\ .$$

Then it is clear that $\mathcal{P}'$ is a normalized canonical proof of S' in $([\sigma'], E)$ with $\mu_E(\mathcal{P}) = \mu_E(\mathcal{P}')$ and $\mu_1(\mathcal{P}) > \mu_1(\mathcal{P}')$. This implies $\mathcal{P} > \mathcal{P}'$.

Case 2: Let $S = \{t \approx s\} \cup W$, where neither s nor t is a variable, and assume $P \in \mathcal{P}$ is a normalized canonical proof of $t \approx s$ in $([\sigma], E)$ that contains a root step. Since this step uses the position $\Lambda \in \mathcal{FPos}(t)$, there is at least one proof step of P that applies at a nonvariable position of t. The proof P thus can be written in the form

$$t \leftrightarrow^*_{[\sigma]} t\sigma \leftrightarrow^*_E u \leftrightarrow_{[p,l\approx r,\eta]} u' \leftrightarrow^*_E s\sigma \leftrightarrow^*_{[\sigma]} s\,,$$

where the step $u \leftrightarrow u'$ is the leftmost one that applies at a nonvariable position. Hence $p \in \mathcal{FPos}(t)$, and the proof $t \leftrightarrow^*_{[\sigma]} t\sigma \leftrightarrow^*_E u$ is below $\mathcal{VPos}(t)$. The equation $l \approx r$ can be assumed to be variable disjoint from the terms s and t, and so the union $\sigma' := \sigma \cup \eta$ is well defined. From the normalized canonical proof P, we obtain normalized canonical proofs

$$P_0 = t \leftrightarrow^*_{[\sigma']} t\sigma' \leftrightarrow^*_E u\,,$$
$$P_1 = u \leftrightarrow_{[p,l\approx r,\sigma']} u',$$

and

$$P_2 = u' \leftrightarrow^*_E s\sigma' \leftrightarrow^*_{[\sigma']} s\,.$$

For i = 0,2, let $m_i = \mu(P_i)$, so that

$$\mu(P) = m_0 + m_2 + 1.$$

The proof P_0 can be decomposed into the normalized canonical proofs

$$P_{01} = t\big|_p \leftrightarrow^*_{[\sigma']} t\sigma'\big|_p \leftrightarrow^*_E u\big|_p = l\sigma' \leftrightarrow^*_{[\sigma']} l$$

and

$$P_{02} = t[*]_p \leftrightarrow_{[\sigma']} t\sigma'[*]_p \leftrightarrow^*_E u[*]_p.$$

Let $\mu(P_{01}) = k$, so that $\mu(P_{02}) = m_0 - k$. Since the proof P_{01} is below $\mathcal{VPos}(t)$, by Lemma 4, the pair $(t|_p, l)$ is top left unifiable. Moreover, by decomposing the proof P_{01}, we obtain a normalized canonical proof $\mathcal{P}_1$ of tu$(t|_p, l)$ in $([\sigma'], E)$ with $\mu(\mathcal{P}_1) = k$.

Likewise, from the proof P_{02} we obtain a normalized canonical proof

$$t[r]_p \leftrightarrow^*_{[\sigma']} t\sigma'[r\sigma']_p \leftrightarrow^*_E u[r\sigma']_p = u'$$

of length $m_0 - k$, and together with the proof P_2, we obtain a normalized canonical proof Q of $t[r]_p \approx s$ in $([\sigma'], E)$ with $\mu(Q) = m_0 - k + m_2$.

We define

$$S' = \mathrm{tu}(t|_p, l) \cup \{t[r]_p \approx s\} \cup W$$

and

$$\mathscr{P}' = \mathscr{P}_1 \cup \{Q\} \cup (\mathscr{P} - \{P\}).$$

It is clear that $\mathscr{P}'$ is a normalized canonical proof of S' with

$$\mu(\mathscr{P}') = k + (m_0 - k + m_2) + \mu(\mathscr{P}) - (m_0 + m_2 + 1) = \mu(\mathscr{P}) - 1,$$

which implies $\mathscr{P} > \mathscr{P}'$. Finally, since $\sigma' = \sigma \cup \eta$, where $\mathcal{D}om(\eta)$ is disjoint from V, it is clear that $\sigma'|_V = \sigma$.

Case 3: Let $S = \{t \approx x\} \cup W$, with $x \in \mathcal{V}ar(t)$, and assume $P \in \mathscr{P}$ is a normalized canonical proof of $t \approx x$ in $([\sigma], E)$. Then P must contain a root step. Now the system $(S', \mathscr{P}')$ is obtained as in case 2.

Case 4: If one of cases 1 to 3 applies to S, then the assertion of the lemma is satisfied. We can thus assume any equation in S to be solved. Since S is reducible by Variable Elimination, there exists a variable $x \in V$ occurring more than once in S. Moreover, the variable x is normalized in the proof $\mathscr{P}$. $\mathscr{P}$ therefore contains a proof of the form $x \leftrightarrow_{[\sigma]} t$, and consequently S contains an equation $t \approx x$ with $t = x\sigma$. Then S is of the form $S = \{t \approx x\} \cup W$ with $x \in \mathcal{V}ar(W)$. Let $S' = \{t \approx x\} \cup W\{x \leftarrow t\}$, and let $\mathscr{P}'$ be obtained from $\mathscr{P}$ by replacing each proof step of the form $u[x] \leftrightarrow_{[\sigma]} u[t]$ by the empty proof. Then it is easy to see that $\mathscr{P}'$ is a normalized canonical proof of S' in $([\sigma], E)$. Moreover, $\mu(\mathscr{P}) = \mu(\mathscr{P}')$ and $\mu_\sigma(\mathscr{P}) > \mu_\sigma(\mathscr{P}')$, which implies $\mathscr{P} > \mathscr{P}'$.

Theorem 10 *The inference system $\mathscr{T}_E$ is complete, i.e., given an equational system S with $\mathcal{V}ar(S) = V$ and an E-solution $[\sigma]$ of S, there exists a derivation $S \Rightarrow^* [\sigma']$, such that σ' is an E-solution of S with $\sigma'|_V \leq_E \sigma$.*

Proof. If S is irreducible by $\mathscr{T}_E$, then S is obviously in solved form and the assertion of the theorem is trivially satisfied.

Now suppose S is reducible by $\mathscr{T}_E$. Then by the previous lemma, there exists a derivation

$$S = S_0 \Rightarrow S_1 \Rightarrow \ldots$$

and canonical proofs $\mathscr{P}_0$, $\mathscr{P}_1, \ldots$ such that $\mathscr{P}_i > \mathscr{P}_{i+1}$ for all $i \geq 0$. As the ordering $>$ on proofs is terminating, so is the derivation $S = S_0 \Rightarrow S_1 \Rightarrow \ldots$. If this derivation has length n, then $[\sigma'] = S_n$ is an E-solution of S. Moreover, by the previous lemma, $\sigma' \leq_E \sigma_n$ for some substitution σ_n with $\sigma_n|_V = \sigma$. Hence $\sigma'|_V \leq_E \sigma_n|_V = \sigma$. □

Acknowledgment

I would like to thank Patricia Johann for a thourough reading and for useful discussions on the subject of this paper.

References

1. Dougherty, D.J. and Johann, P. An Improved General E-Unification Method. *J. Symbolic Computation* **14** (1992), 303-320.

2. Gallier, J. and Snyder, W. Complete Sets of Transformations for General E-unification. *Theoretical Computer Science* **67**, 2 & 3 (1989), 203-260.

3. Snyder, W. *A Proof Theory for General E-Unification.* Birkhäuser, Boston 1991.