Nominal Equational Rewriting and Narrowing

Mauricio Ayala-Rincón
University of Brasília, Brazil

Maribel Fernández
King's College London, UK

Daniele Nantes-Sobrinho
University of Brasília, Brazil
Imperial College London, UK

Daniella Santaguida
University of Brasília, Brazil

Narrowing is a well-known technique that adds to term rewriting mechanisms the required power to search for solutions to equational problems. Rewriting and narrowing are well-studied in first-order term languages, but several problems remain to be investigated when dealing with languages with binders using nominal techniques. Applications in programming languages and theorem proving require reasoning modulo α-equivalence considering structural congruences generated by equational axioms, such as commutativity. This paper presents the first definitions of nominal rewriting and narrowing modulo an equational theory. We establish a property called nominal E-coherence and demonstrate its role in identifying normal forms of nominal terms. Additionally, we prove the nominal E-Lifting theorem, which ensures the correspondence between sequences of nominal equational rewriting steps and narrowing, crucial for developing a correct algorithm for nominal equational unification via nominal equational narrowing. We illustrate our results using the equational theory for commutativity.

1 Introduction

The nominal framework [15] has emerged as a promising approach for dealing with languages involving binders such as lambda calculus and first-order logic. In this framework, equality coincides with the α-equivalence relation, denoted as $\approx_\alpha$, and freshness constraints are integrated within the nominal reasoning rather than being relegated to the meta-language. For example, the expression $a\#M$ ("a is fresh for M") indicates that if a name a occurs in a term M, it must be abstracted by some binder, such as the λ in the lambda calculus, or $\exists, \forall$-quantification in first-order logic), i.e., a cannot occur free in M.

To enable reasoning within this framework, nominal unification [11, 22] was developed and formalised in proof assistants such as Isabelle [22], PVS [8] and Coq [4]. Nominal unification involves finding a substitution σ that solves the problem $s \stackrel{?}{\approx}_? t$, meaning $s\sigma \approx_\alpha t\sigma$, where s and t are nominal terms. It is well-known that unification is fundamental for automated reasoning, serving as the foundation for resolution-based proof assistants, type inference, and numerous other applications. While these applications are anticipated to extend to nominal unification, substantial work is required to verify this.

To pursue applications of the nominal framework, extensions of nominal unification with equational theories have been investigated. Initial efforts included integrating the theories of Associativity ($\approx_{\alpha,\mathsf{A}}$), Commutativity ($\approx_{\alpha,\mathsf{C}}$) and Associativity-Commutativity ($\approx_{\alpha,\mathsf{AC}}$) to α-equality [4]. Various algorithms for nominal unification modulo commutativity (C-unification) and formalisations of their correctness in proof assistants PVS and Coq have been developed [1, 2, 7, 5]. These development efforts reveal significant differences between first-order and nominal languages, such as the theory of C-unification, which has nullary unification type if α-equivalence is considered [1], contrasting with the finitary type of first-order C-unification [10].

Submitted to:
LSFA 2024

Further investigations into nominal unification include exploring a *letrec* constructor and extensions involving atom variables [21]. Another example is the development of an algorithm for nominal C-matching [3], a special case of nominal C-unification (dealing with problems $s \stackrel{?}{\approx}^{\mathsf{C}}_{?} t$ where the substitution σ only applies in one side: $s\sigma \approx_{\alpha,\mathsf{C}} t$). Recently, a naive nominal extension of the Stickel-Fages first-order AC-unification algorithm introduced cyclicity in solutions produced by translations of unification problems to Diophantine systems as reported in [9], and this differs from the original (first-order) approach which has a terminating algorithm.

These developments underline the complexity of extending equational unification algorithms to the nominal framework, and new methods need to be proposed to obtain the desired extensions. An alternative approach to solving nominal unification problems modulo equational theories (i.e., nominal E-unification problems), developed in [6], involves the use of *nominal narrowing*[1]. This technique can be used when the equational theory E is presented by a convergent nominal rewriting system [14, 12]. Different extensions are needed for rewriting modulo E when such a presentation is impossible. However, nominal techniques modulo an equational theory E, and in particular, nominal E-rewriting, remain unexplored.

This work represents the first step towards developing nominal E-techniques, when using a convergent nominal rewrite system equivalent to the theory E is not possible. In first-order term languages [18, 23, 13], the standard technique is to split a set of identities T into a term rewriting system R and an equational part E, so that $\mathsf{T} = \mathsf{R} \cup \mathsf{E}$, considering the rewriting relation generated by R on the equivalence classes of terms generated by E. We propose extending this technique to nominal languages by adapting the notions of nominal rewriting [14, 20, 19] and nominal narrowing [6] to work modulo E, incorporating the relation $\approx_{\alpha,\mathsf{E}}$. These extensions result in the first definitions of nominal R/E-rewriting (Definition 3.1) and R,E-rewriting (Definition 3.2) as well as E-narrowing (Definition 3.8).

Nominal R/E-rewriting applies rules from R in the equivalence class modulo $\approx_{\alpha,\mathsf{E}}$ of a nominal term t, while R,E-rewriting uses nominal E-*matching* to determine if a rule in R applies to a nominal term, say t. This nominal term t may have variables, thus the definition of the relations R/E and R,E also feature freshness conditions. We prove that it is possible to identify the normal form of a nominal term, say t, with respect to the relation R/E (denoted $t \downarrow_{\mathsf{R}/\mathsf{E}}$) to the normal form of the same term, but with respect to the relation R,E (that is, $t \downarrow_{\mathsf{R},\mathsf{E}}$), when the relation R,E has a property called *nominal* E-*coherence*, whose extension from a corresponding property in first-order term language [17] is established here.

Proving the correspondence between sequences of nominal R,E-rewriting steps and E-narrowing steps (Nominal E-Lifting Theorem 4.6) is essential to develop an algorithm for nominal T-unification via nominal E-narrowing. Since the decidability of nominal T-unification relies on the decidability of nominal E-unification and E-matching, and so far, the only equational theory for which a nominal unification algorithm exists is commutativity C, a corollary of our developments is that the nominal C-Lifting Theorem holds. Finally, due to the volume of extensions that were necessary to establish nominal E-narrowing and rewriting, the final goal of using E-narrowing as a sound and complete procedure for solving nominal T-unification, remains ongoing work.

Summarising, our main contributions are:

1. We extend the definitions and concepts regarding rewriting modulo E to the nominal framework. For instance, we have nominal versions of the relations $\rightarrow_{\mathsf{R},\mathsf{E}}$ and $\rightarrow_{\mathsf{R}/\mathsf{E}}$ for rewriting, and $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$ for nominal E-narrowing.

[1] Roughly, nominal narrowing is a generalisation of nominal rewriting by using nominal unification instead of nominal matching in its definition.

2. We prove technical auxiliary results relating $\to_{\mathsf{R},\mathsf{E}}$ and $\to_{\mathsf{R}/\mathsf{E}}$. These required the establishment of the nominal E-coherence property for R,E.
3. We prove the nominal E-Lifting Theorem (cf. Theorem 4.6) that establishes a correspondence between sequences of nominal E-narrowing $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$ and nominal R,E-rewriting $\to_{\mathsf{R},\mathsf{E}}$.
4. Since C is the only equational theory for which a nominal unification algorithm exists, we illustrate our results using nominal R,C-rewriting and narrowing.

Organisation. In §2 we present the background necessary to read the paper. Novel material starts in §3, where we extend the notions of rewriting and narrowing modulo an equational theory E to the nominal framework and provide some examples. In §4 we present the classical Lifting Theorem, extended to the nominal framework, taking into account an equational E for which a nominal E-unification algorithm exists. §5 concludes the paper.

2 Preliminaries

While we assume the reader's familiarity with nominal techniques, we briefly recap some basic definitions. For more details, we refer to [14]. In this (and the following) section(s), we will use $\equiv$ for syntactic equality, $=$ for definitions and $\approx_\alpha$ for α-equality.

Syntax. Fix countable infinite pairwise disjoint sets of *atoms* $\mathbb{A} = \{a,b,c,\ldots\}$ and *variables* $\mathscr{X} = \{X,Y,Z,\ldots\}$. Atoms follow the *atom convention*: atoms $a,b,c,\ldots$ over $\mathbb{A}$ represent different names. Let Σ be a finite set of term-formers disjoint from $\mathbb{A}$ and $\mathscr{X}$ such that for each $f \in \Sigma$, a unique non-negative integer n (arity of f) is assigned. A *permutation* π is a bijection on $\mathbb{A}$ with finite domain, i.e., the set $\mathtt{dom}(\pi) = \{a \in \mathbb{A} \mid \pi(a) \neq a\}$ is finite. The identity permutation is denoted id. The composition of permutations π and π' is denoted $\pi \circ \pi'$ and π^{-1} denotes the inverse of the permutation π.

Nominal terms are defined inductively by the grammar:

$$s,t,u ::= a \mid \pi \cdot X \mid [a]t \mid f(t_1,\ldots,t_n),$$

where a is an *atom*, $\pi \cdot X$ is a (moderated/suspended) variable, $[a]t$ is the *abstraction* of a in the term t, and $f(t_1,\ldots,t_n)$ is a *function application* with $f \in \Sigma$ and $f : n$. We abbreviate $id \cdot X$ as X. A term is *ground* if it does not contain (moderated) variables. A *position* $\mathbb{C}$ is defined as a pair $(s,\_)$ of a term and a distinguished variable $\_ \in \mathscr{X}$ that occurs exactly once in s. We write $\mathbb{C}[s']$ for $\mathbb{C}[\_ \mapsto s']$ and if $s \equiv \mathbb{C}[s']$, we say that s' is a subterm of s with position $\mathbb{C}$. The root position will be denoted by $\mathbb{C} = [\_]$.

Remark 2.1 (Positions). Our definition of 'position' is equivalent to the standard notion of a point in the abstract syntax tree of a term, as defined, for example, in [10]. It is more convenient for us to identify this with the corresponding 'initial segment' of a nominal term, in which the 'hole' is a variable in $\mathscr{X}$; thus positions of a term can be expressed within our language.

A *permutation action* of π on a term t is defined by induction on the term structure as expected:

$$\pi \cdot a = \pi(a) \qquad \pi \cdot (\pi' \cdot X) = (\pi \circ \pi') \cdot X \qquad \pi \cdot [a]t = [\pi \cdot a](\pi \cdot t) \qquad \pi \cdot f(t_1,\ldots,t_n) = f(\pi \cdot t_1,\ldots,\pi \cdot t_n).$$

The *difference set* of two permutations $ds(\pi,\pi') := \{n \mid \pi \cdot n \neq \pi' \cdot n\}$. So $ds(\pi,\pi')\#X$ represents the set of constraints $\{n\#X \mid n \in ds(\pi,\pi')\}$. For example, if $\pi = (a\ b)(c\ d)$ and $\pi' = (c\ b)$, then $ds(\pi,\pi') =$

$$\frac{}{\Delta \vdash a\#b}\ (\#\text{ atom}) \qquad \frac{\Delta \vdash a\#t_1 \ \cdots\ \Delta \vdash a\#t_n}{\Delta \vdash a\#f(t_1,\cdots,t_n)}\ (\#\text{ app})$$

$$\frac{}{\Delta \vdash a\#[a]t}\ (\#\text{ a[a]}) \qquad \frac{\Delta \vdash a\#t}{\Delta \vdash a\#[b]t}\ (\#\text{ a[b]}) \qquad \frac{(\pi^{-1}\cdot a\#X) \in \Delta}{\Delta \vdash a\#\pi\cdot X}\ (\#\text{ var})$$

$$\frac{}{\Delta \vdash a \approx_\alpha a}\ (\approx_\alpha \text{ atom}) \qquad \frac{\Delta \vdash s_1 \approx_\alpha t_1 \ \cdots\ \Delta \vdash s_n \approx_\alpha t_n}{\Delta \vdash f(s_1,\cdots,s_n) \approx_\alpha f(t_1,\cdots,t_n)}\ (\approx_\alpha \text{ app})$$

$$\frac{\Delta \vdash s \approx_\alpha t}{\Delta \vdash [a]s \approx_\alpha [a]t}\ (\approx_\alpha \text{ [aa]}) \qquad \frac{\Delta \vdash s \approx_\alpha (a\ b)\cdot t \qquad \Delta \vdash a\#t}{\Delta \vdash [a]s \approx_\alpha [b]t}\ (\approx_\alpha \text{ [ab]})$$

$$\frac{ds(\pi,\pi')\#X \in \Delta}{\Delta \vdash \pi\cdot X \approx_\alpha \pi'\cdot X}\ (\approx_\alpha \text{ var})$$

Figure 1: Rules for # and $\approx_\alpha$

$\{a,b,c,d\}$ since π and π' act differently in each atom: note that $\pi(a) = b$ and $\pi'(a) = a$. In addition, $ds(\pi,\pi')\#X = \{a\#X, b\#X, c\#X, d\#X\}$.

A *substitution* θ is a mapping from a finite set of variables to terms. The *substitution action* $t\theta$ is defined as follows:

$$a\theta = a \qquad (\pi\cdot X)\theta = \pi\cdot(X\theta) \qquad ([a]t)\theta = [a](t\theta) \qquad f(t_1,\ldots,t_n)\theta = f(t_1\theta,\ldots,t_n\theta).$$

The domain of a substitution θ is written as $\mathtt{dom}(\theta)$, and the image is denoted as $\mathtt{Im}(\theta)$. Therefore, if $X \notin \mathtt{dom}(\theta)$ then $X\theta = X$. Also, if we restrict the domain to a certain set $V \subseteq \mathscr{X}$ of variables, we obtain the substitution $\theta|_V$, the *restriction of* θ *to* V. The identity substitution is denoted $\mathtt{Id}$. The composition of two substitutions θ_1 and θ_2 will be denoted by simple juxtaposition as $\theta_1\theta_2$ and it applies to a term as $t\theta_1\theta_2 = (t\theta_1)\theta_2$.

Nominal Constraints, Judgements and Rewriting. There are two kinds of constraints: $s \approx_\alpha t$ is an (alpha-)equality constraint and $a\#t$ is a freshness constraint which means that a cannot occur unabstracted in t. *Primitive constraints* have the form $a\#X$ and ∇, Δ denote finite sets of primitive constraints. We will use the abbreviation $a,b,c\#X$ to denote the set of freshness constraints $\{a\#X, b\#X, c\#X\}$. *Judgements* have the form $\Delta \vdash s \approx_\alpha t$ and $\Delta \vdash a\#t$ and are derived using the rules in Figure 1. A context Δ is called *consistent* if it is a finite set of freshness constraints that do not reduce, via bottom-up application of the rules in Figure 1, to constraints of the form $a\#a$.

Given a finite set of freshness constraints Δ and a substitution θ, $\Delta\theta$ consists of the set of constraints $\{a\#X\theta \mid a\#X \in \Delta\}$ and $\langle\Delta\theta\rangle_{nf}$ consists of the freshness context obtained after applying the rules from Figure 1 in $\Delta\theta$, in a bottom-up manner. A *problem* Pr is a set of constraints, and we write $\Delta \vdash Pr$ when for all $P \in Pr$ there is a derivation proof using the rules in Figure 1, taking elements of the context Δ as assumptions.

Example 2.1. Let $\Sigma_\lambda = \{\mathsf{lam}, \mathsf{app}\}$ denote the signature whose function symbols have arities $\mathsf{lam} : 1$ and $\mathsf{app} : 2$. Let $Pr = \mathsf{lam}[a]\mathsf{app}(a,X) \approx_\alpha \mathsf{lam}[b]\mathsf{app}(b,(a\ c)\cdot X)$ be a problem and $\Delta = \{a,b,c\#X\}$ be a context. We verify the derivability of $\Delta \vdash \mathsf{lam}[a]\mathsf{app}(a,X) \approx_\alpha \mathsf{lam}[b]\mathsf{app}(b,(a\ c)\cdot X)$:

$$\dfrac{\dfrac{}{\Delta \vdash a \approx_\alpha a}\,(\approx_\alpha \text{ atom}) \quad \dfrac{a,b,c\#X \in \Delta}{\Delta \vdash X \approx_\alpha (a\ b)(a\ c)\cdot X}\,(\approx_\alpha \text{ var})}{\dfrac{\Delta \vdash \mathsf{app}(a,X) \approx_\alpha \mathsf{app}(a,(a\ b)(a\ c)\cdot X)}{\dfrac{\Delta \vdash [a]\mathsf{app}(a,X) \approx_\alpha [b]\mathsf{app}(b,(a\ c)\cdot X)}{\Delta \vdash \mathsf{lam}[a]\mathsf{app}(a,X) \approx_\alpha \mathsf{lam}[b]\mathsf{app}(b,(a\ c)\cdot X)}\,(\approx_\alpha \text{ app})}\,(\approx_\alpha [\text{ab}])}\,(\approx_\alpha \text{ app}) \qquad \dfrac{\dfrac{}{\Delta \vdash a\#b}\,(\#\text{ atom}) \quad \dfrac{c\#X \in \Delta}{\Delta \vdash a\#(a\ c)\cdot X}\,(\#\text{ var})}{\Delta \vdash a\#\mathsf{app}(b,(a\ c)\cdot X)}\,(\#\text{ app})$$

A *term in context* $\Delta \vdash t$ expresses that the term t has the freshness constraints imposed by Δ. For example, $a\#X \vdash f(X,h(b))$ expresses that a cannot occur fresh in instances of X. Nominal rewriting rules can be defined under freshness constraints, i.e., $\nabla \vdash l \to r$ denotes a nominal rewriting rule. We denote by R, a finite set of nominal rewriting rules.

The *nominal rewriting relation* $\to_{\mathsf{R}}$ is defined as in [14]:

$$\frac{s \equiv \mathbb{C}[s'] \wedge \Delta \vdash \nabla\theta \wedge s' \approx_\alpha \pi\cdot(l\theta) \wedge t \approx_\alpha \mathbb{C}[\pi\cdot(r\theta)]}{\Delta \vdash s \to_{\mathsf{R}} t}$$

for a substitution θ, a subterm s' of s, a position $\mathbb{C}$ and a nominal rule $\nabla \vdash l \to r \in \mathsf{R}$. We will omit the subscript R and write only $\Delta \vdash s \to t$ when there is no ambiguity.

Equality modulo an equational theory E. A nominal *identity* is a pair in context $\nabla \vdash (l,r)$ of nominal terms l and r under a (possibly empty) freshness context ∇. We denote such identity as $\nabla \vdash l \approx r$. A set E of identities induces an *equational theory*, which we will also denote as E.

The *nominal algebra equality modulo* E, denoted $\Delta \vdash s \approx_{\alpha,\mathsf{E}} t$, is the least transitive reflexive symmetric relation such that for any $(\nabla \vdash l \approx r) \in \mathsf{E}$, position $\mathbb{C}$, permutation π, substitution θ, and fresh context Γ (so if $a\#X \in \Gamma$ then a is not mentioned in Δ, s, t):

$$\frac{\Delta,\Gamma \vdash \big(\nabla\theta, \qquad s \approx_\alpha \mathbb{C}[\pi\cdot(l\theta)], \qquad \mathbb{C}[\pi\cdot(r\theta)] \approx_\alpha t\big)}{\Delta \vdash s \approx_{\alpha,\mathsf{E}} t}\,(Ax_{\mathsf{E}})$$

Remark 2.2. We can also define $\approx_{\alpha,\mathsf{E}}$ by extending the rules of Figure 1 with the dedicated rules for the identities defining E. For example, the identity expressing the commutativity of a function symbol f^{C} is $\mathsf{C} = \{\vdash f^{\mathsf{C}}(X,Y) \approx f^{\mathsf{C}}(Y,X)\}$. In this case, we need to add the following rule:

$$\frac{\Delta \vdash s_0 \ \approx_{\alpha,\mathsf{C}}\ t_i \qquad \Delta \vdash s_1 \ \approx_{\alpha,\mathsf{C}}\ t_{1-i} \qquad i = 0,1 \qquad f^{\mathsf{C}} \in \Sigma^{\mathsf{C}}}{\Delta \vdash f^{\mathsf{C}}(s_0,s_1) \ \approx_{\alpha,\mathsf{C}}\ f^{\mathsf{C}}(t_0,t_1)}\,(\approx_{\alpha,\mathsf{C}}\ \mathrm{C})$$

where Σ^{C} denotes a signature of commutative function symbols. Rule $(\approx_\alpha \text{ app})$ only applies when the function symbol f is not commutative. In addition, we need to modify the rules in Figure 1 to use $\approx_{\alpha,\mathsf{C}}$ instead of $\approx_\alpha$.

Note that if we define an equational theory E using the rule (Ax_{E}), the equational theory is a congruence relation, and $\vdash$ is compatible with substitutions by definition. However, this rule generates a lot of redundant derivations. To avoid this, we will use specific rules for each E, as for the commutative rule in Remark 2.2. This choice comes with a cost, e.g. the rule $(\approx_{\alpha,\mathsf{C}}\ \mathrm{C})$ is not closed by substitutions, and we need to prove the compatibility of $\vdash$ by substitution.

Definition 2.3 (E-Compatibility of $\vdash$ by substitutions)**.** An equational theory E is *compatible with* $\vdash$ *by substitutions* iff the following hold, whenever Δ and $\Delta\theta$ are consistent.

1. If $\Delta \vdash a\#t$ then $\langle\Delta\theta\rangle_{nf} \vdash a\#(t\theta)$.
2. If $\Delta \vdash s \approx_{\alpha,\mathsf{E}} t$ then $\langle\Delta\theta\rangle_{nf} \vdash (s\theta) \approx_{\alpha,\mathsf{E}} (t\theta)$.

3. If $\Delta \vdash Pr$ then $\langle \Delta\theta \rangle_{nf} \vdash Pr\theta$.

The next proposition guarantees the compatibility of judgments by substitutions when the theory C for commutativity is considered. This proposition is technical and will be used in the correspondence of one-step narrowing to one-step rewriting in Lemma 4.2.

Proposition 2.4. *The equational theory* C *is compatible with substitutions.*

Proof. By induction on the derivation of $\Delta \vdash a\#t$ or $\Delta \vdash s \approx_{\alpha,\mathsf{C}} t$, using the rules of Fig. 1 extended for $\approx_{\alpha,\mathsf{C}}$-equality. □

Nominal C-unification algorithm. We consider the rule-based algorithm for nominal C-unification, introduced in [2] and defined by the rules presented in Figure 2. The rules act on triples $\mathscr{P} = (\Delta, \theta, Pr)$, where Δ is a freshness context, θ is a substitution and Pr is a C-problem, i.e., a set of freshness and $\approx_{\alpha,\mathsf{C}}$-equality constraints. We will denote the triples by $\mathscr{P}, \mathscr{Q}, \mathscr{S}, \cdots$.

Definition 2.5. (C-solution) A C-*solution* for a triple $\mathscr{P} = (\Delta, \delta, Pr)$ is a pair (Δ', θ) where the following conditions are satisfied:

1. $\Delta' \vdash \Delta\theta$;
2. $\Delta' \vdash a\#t\theta$, if $a\#t \in Pr$;
3. $\Delta' \vdash s\theta \approx_{\alpha,\mathsf{C}} t\theta$, if $s \approx_{\alpha,\mathsf{C}} t \in Pr$;
4. there is a substitution θ' such that $\Delta' \vdash \delta\theta' \approx_{\alpha,\mathsf{C}} \theta$.

If there is no (Δ', θ), then we say that the problem $\mathscr{P}$ is *unsolvable*. Also $\mathscr{U}_{\mathsf{C}}(\mathscr{P})$ denotes the set of all C-solutions of the triple $\mathscr{P}$.

Let (Δ_1, θ_1) and (Δ_2, θ_2) be solutions in $\mathscr{U}_{\mathsf{C}}(\mathscr{P})$. We say that (Δ_1, θ_1) is *more general than* (Δ_2, θ_2), and denote it as $(\Delta_1, \theta_1) \leq_{\mathsf{C}} (\Delta_2, \theta_2)$, if there exists a substitution θ' such that $\Delta_2 \vdash X\theta_1\theta' \approx_{\alpha,\mathsf{C}} X\theta_2$, for all $X \in \mathscr{X}$ and $\Delta_2 \vdash \Delta_1\theta'$. We write $\leq_{\mathsf{C}}^{V}$ for the restriction of $\leq_{\mathsf{C}}$ to a set V of variables.

Definition 2.6. (Nominal C-unification problem) A *nominal* C-*unification problem (in context)* is a pair $(\nabla \vdash l) \stackrel{\mathsf{C}}{\approx}_? (\Delta \vdash s)$. The pair (Δ', θ) is an C-solution, or C-unifier, of $(\nabla \vdash l) \stackrel{\mathsf{C}}{\approx}_? (\Delta \vdash s)$ iff (Δ', θ) is a C-solution of the triple $\mathscr{P} = (\{\nabla, \Delta\}, \mathtt{Id}, \{l \approx_{\alpha,\mathsf{C}} s\})$, that is, conditions (1)-(4) of Definition 2.5 are satisfied. $\mathscr{U}_{\mathsf{C}}(\nabla \vdash l, \Delta \vdash s)$ denotes the set of all C-solutions of $(\nabla \vdash l) \stackrel{\mathsf{C}}{\approx}_? (\Delta \vdash s)$. If ∇ and Δ are empty we write simply $\mathscr{U}_{\mathsf{C}}(l, s)$. A subset $\mathscr{V} \in \mathscr{U}_{\mathsf{C}}(\mathscr{P})$ is said to be a *complete set of* C-*solutions of* $\mathscr{P}$ if for all $(\Delta_1, \theta_1) \in \mathscr{U}_{\mathsf{C}}(\mathscr{P})$, there exists $(\Delta_2, \theta_2) \in \mathscr{V}$ such that $(\Delta_2, \theta_2) \leq_{\mathsf{C}} (\Delta_1, \theta_1)$.

The following example illustrates the use of the nominal C-unification algorithm to solve a nominal C-unification problem.

Example 2.2. Let $\Sigma = \{h : 1, f^{\mathsf{C}} : 2, \oplus : 2\}$ be a signature, where f^{C} and $\oplus$ are commutative symbols, i.e., and $\mathsf{C} = \{ \vdash f^{\mathsf{C}}(X,Y) \approx f^{\mathsf{C}}(Y,X),\ \vdash X \oplus Y \approx Y \oplus X\}$ be the axioms defining the theory. Consider the C-unification problem $(\emptyset \vdash h(Y)) \stackrel{\mathsf{C}}{\approx}_? (\emptyset \vdash h(f^{\mathsf{C}}([b][a]X, X)))$ which has the associated triple $(\emptyset, \mathtt{Id}, \{h(Y) \stackrel{\mathsf{C}}{\approx}_? h(f^{\mathsf{C}}([b][a]X, X))\})$. By applying the rules from Figure 2 we get the following:

$$
\begin{aligned}
(\emptyset, \mathtt{Id}, \{h(Y) \stackrel{\mathsf{C}}{\approx}_? h(f^{\mathsf{C}}([b][a]X, X))\}) &\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{app})} (\emptyset, \mathtt{Id}, \{Y \stackrel{\mathsf{C}}{\approx}_? f^{\mathsf{C}}([b][a]X, X)\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{inst})} (\emptyset, \theta_0 = [Y \mapsto f^{\mathsf{C}}([b][a]X, X)], \{f^{\mathsf{C}}([b][a]X, X) \stackrel{\mathsf{C}}{\approx}_? f^{\mathsf{C}}([b][a]X, X)\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{refl})} (\emptyset, \theta_0 = [Y \mapsto f^{\mathsf{C}}([b][a]X, X)], \emptyset)
\end{aligned}
$$

$$
\begin{array}{lrcl}
\text{(\# ab)} & (\Delta,\theta,Pr\uplus\{a\#b\}) & \Longrightarrow & (\Delta,\theta,Pr)\\
\text{(\# app)} & (\Delta,\theta,Pr\uplus\{a\#f(t_1,\cdots,t_n)\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\{a\#t_1,\cdots,a\#t_n\})\\
\text{(\# a[a])} & (\Delta,\theta,Pr\uplus\{a\#[a]t\}) & \Longrightarrow & (\Delta,\theta,Pr)\\
\text{(\# a[b])} & (\Delta,\theta,Pr\uplus\{a\#[b]t\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\{a\#t\})\\
\text{(\# var)} & (\Delta,\theta,Pr\uplus\{a\#\pi\cdot X\}) & \Longrightarrow & (\{(\pi^{-1}\cdot a)\#X\}\cup\Delta,\theta,Pr)
\end{array}
$$

$$
\begin{array}{lrcl}
(\approx_{\alpha,\mathsf{C}}\text{ refl}) & (\Delta,\theta,Pr\uplus\{s\approx_{\alpha,\mathsf{C}}s\}) & \Longrightarrow & (\Delta,\theta,Pr)\\
(\approx_{\alpha,\mathsf{C}}\text{ app}) & (\Delta,\theta,Pr\uplus\{f(\bar{s})_n\approx_{\alpha,\mathsf{C}}f(\bar{t})_n\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\bigcup\{s_i\approx_{\alpha,\mathsf{C}}t_i\})\\
(\approx_{\alpha,\mathsf{C}}\text{ C}) & (\Delta,\theta,Pr\uplus\{f^{\mathsf{C}}s\approx_{\alpha,\mathsf{C}}f^{\mathsf{C}}t\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\{s\approx_{\alpha,\mathsf{C}}v\}),\text{where } s=(s_0,s_1)\\
 & & & \text{and } t=(t_0,t_1),v=(t_i,t_{(1-i)}),i=0,1\\
(\approx_{\alpha,\mathsf{C}}\text{ [aa]}) & (\Delta,\theta,Pr\uplus\{[a]s\approx_{\alpha,\mathsf{C}}[a]t\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\{s\approx_{\alpha,\mathsf{C}}t\})\\
(\approx_{\alpha,\mathsf{C}}\text{ [ab]}) & (\Delta,\theta,Pr\uplus\{[a]s\approx_{\alpha,\mathsf{C}}[b]t\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\{s\approx_{\alpha,\mathsf{C}}(a\ b)\cdot t,a\#t\})\\
(\approx_{\alpha,\mathsf{C}}\text{ inst}) & (\Delta,\theta,Pr\uplus\{\pi\cdot X\approx_{\alpha,\mathsf{C}}t\}) & \Longrightarrow & (\Delta,\theta',Pr[X\mapsto\pi^{-1}\cdot t]\cup\bigcup\limits_{\substack{Y\in dom(\theta'),\\ a\#Y\in\Delta}}\{a\#Y\theta'\}),\\
 & & & \text{let } \theta':=\theta[X\mapsto\pi^{-1}\cdot t],\\
 & & & \text{if } X\notin Var(t)\\
(\approx_{\alpha,\mathsf{C}}\text{ inv}) & (\Delta,\theta,Pr\uplus\{\pi\cdot X\approx_{\alpha,\mathsf{C}}\pi'\cdot X\}) & \Longrightarrow & (\Delta,\theta,Pr\cup\{(\pi')^{-1}\circ\pi\cdot X\approx_{\alpha,\mathsf{C}}X\})\\
 & & & \text{if } \pi'\neq\mathtt{Id}
\end{array}
$$

Figure 2: Simplification rules for # and $\approx_{\alpha,\mathsf{C}}$. $\uplus$ denotes disjoint union

Thus, we get the C-solution $(\emptyset,\theta_0)$.

Now consider the C-unification problem $(\emptyset\vdash f^{\mathsf{C}}([a][b]Z,Z))\ {}_?\overset{\mathsf{C}}{\approx}_?\ (\emptyset\vdash f^{\mathsf{C}}([b][a]X,X))$, which has the associated triple $(\emptyset,\mathtt{Id},\{f^{\mathsf{C}}([a][b]Z,Z))\ {}_?\overset{\mathsf{C}}{\approx}_?\ f^{\mathsf{C}}([b][a]X,X)\})$. Using the Nominal C-unification algorithm we get the following:

$$
\begin{array}{l}
(\emptyset,\mathtt{Id},\{f^{\mathsf{C}}([a][b]Z,Z))\ {}_?\overset{\mathsf{C}}{\approx}_?\ f^{\mathsf{C}}([b][a]X,X)\}) \quad \Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\text{ C})}\\
\quad\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\text{ C})}(\emptyset,\mathtt{Id},\{[a][b]Z\ {}_?\overset{\mathsf{C}}{\approx}_?\ [b][a]X,Z\ {}_?\overset{\mathsf{C}}{\approx}_?\ X\})\\
\quad\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\text{ inst})}(\emptyset,\theta_1=[Z\mapsto X],\{[a][b]X\ {}_?\overset{\mathsf{C}}{\approx}_?\ [b][a]X,X\ {}_?\overset{\mathsf{C}}{\approx}_?\ X\})\\
\quad\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\text{ refl})}(\emptyset,\theta_1,\{[a][b]X\ {}_?\overset{\mathsf{C}}{\approx}_?\ [b][a]X\})\\
\quad\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\text{ [ab]})}(\emptyset,\theta_1,\{[b]X\ {}_?\overset{\mathsf{C}}{\approx}_?\ (a\ b)\cdot[a]X,a\#[a]X\})\\
\quad\Longrightarrow_{(\#\text{ a[a]})}(\emptyset,\theta_1,\{[b]X\ {}_?\overset{\mathsf{C}}{\approx}_?\ [b](a\ b)\cdot X\})\\
\quad\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\text{ [bb]})}(\emptyset,\theta_1,\{X\ {}_?\overset{\mathsf{C}}{\approx}_?\ (a\ b)\cdot X\}) \qquad \text{(Fixed-point problem)}
\end{array}
$$

Observe that the first step uses the rule $(\approx_{\alpha,\mathsf{C}}\ \mathrm{C})$, which yields two branches, but here, we are interested in analysing only one branch.

The fixed-point problem has infinite solutions, for example:

- $(\{a\#X,b\#X\},\rho_1=\mathtt{Id})$:

$$
\begin{array}{l}
(\emptyset,\mathtt{Id},\{X\ {}_?\overset{\mathsf{C}}{\approx}_?\ (a\ b)\cdot X\}) \quad \Longrightarrow_{(\text{inverse }\approx_\alpha\text{ var})}\\
\quad\Longrightarrow_{(\text{inverse }\approx_\alpha\text{ var})}(\emptyset,\mathtt{Id},\{ds(id,(a\ b))\#X\})\\
\quad\Longrightarrow^{2}_{(\#\text{ var})}(\{a\#X,b\#X\},\mathtt{Id},\emptyset)
\end{array}
$$

- $(\emptyset,\rho_2=[X\mapsto a\oplus b])$: $X[X\mapsto a\oplus b]=a\oplus b\approx_{\alpha,\mathsf{C}}b\oplus a=(a\ b)\cdot X[X\mapsto a\oplus b]$

- $(\emptyset, \rho_3 = [X \mapsto (a \oplus b) \oplus (a \oplus b)])$:

$$X[X \mapsto (a \oplus b) \oplus (a \oplus b)] = (a \oplus b) \oplus (a \oplus b) \approx_{\alpha,\mathsf{C}} (b \oplus a) \oplus (b \oplus a) = (a\ b) \cdot X[X \mapsto (a \oplus b) \oplus (a \oplus b)]$$

3 Nominal E-rewriting and E-narrowing.

In this section, we introduce our novel definitions of *equational nominal rewriting systems* (ENRS) and *nominal equational narrowing*, sometimes abbreviated to nominal E-rewriting systems and nominal E-narrowing.

3.1 Nominal E-rewriting

An *equational nominal rewrite system* (ENRS) is a set of (nominal) identities T that can be split into a set R of nominal rewrite rules and a set E of identities. Sometimes, we will denote this decomposition as R∪E. Below, $[t]_{\mathsf{E}}$, denotes the equivalence class of the nominal term t modulo E, i.e., $[t]_{\mathsf{E}} = \{t' \mid t' \approx_{\alpha,\mathsf{E}} t\}$.

Definition 3.1 (Nominal R/E-rewriting)**.** Let $\mathsf{T} = \mathsf{R} \cup \mathsf{E}$ be an ENRS. The relation $\rightarrow_{\mathsf{R/E}}$ is induced by the composition $\approx_{\alpha,\mathsf{E}} \circ \rightarrow_{\mathsf{R}} \circ \approx_{\alpha,\mathsf{E}}$. A nominal term-in-context $\Delta \vdash s$ reduces with $\rightarrow_{\mathsf{R/E}}$, when its equivalence class modulo E reduces via $\rightarrow_{\mathsf{R/E}}$ as below:

$$\Delta \vdash ([s]_{\mathsf{E}} \rightarrow_{\mathsf{R/E}} [t]_{\mathsf{E}}) \text{ iff there exist } s', t' \text{ such that } \Delta \vdash (s \approx_{\alpha,\mathsf{E}} s' \rightarrow_{\mathsf{R}} t' \approx_{\alpha,\mathsf{E}} t).$$

The following example illustrates an ENRS for the set of identities that define the prenex normal form of a first-order formula. We consider the commutativity of the connectives $\wedge$ and $\vee$.

Example 3.1 (Prenex normal form rules)**.** Consider the signature for the first-order logic $\Sigma = \{\forall, \exists, \neg, \wedge, \vee\}$, let $\mathsf{C} = \{\vdash P \vee Q \approx Q \vee P, \vdash P \wedge Q \approx Q \wedge P\}$ be the commutative theory. The prenex normal form rules can be specified by the following set R of nominal rewrite rules:

$$\begin{array}{ll} a\#P & \vdash P \wedge \forall[a]Q \rightarrow \forall[a](P \wedge Q) \\ a\#P & \vdash P \vee \forall[a]Q \rightarrow \forall[a](P \vee Q) \\ a\#P & \vdash P \wedge \exists[a]Q \rightarrow \exists[a](P \wedge Q) \\ a\#P & \vdash P \vee \exists[a]Q \rightarrow \exists[a](P \vee Q) \\ & \vdash \neg(\exists[a]Q) \rightarrow \forall[a]\neg Q \\ & \vdash \neg(\forall[a]Q) \rightarrow \exists[a]\neg Q \end{array}$$

Note that in Definition 3.1, the relation $\rightarrow_{\mathsf{R/E}}$ deals with α, E-congruence classes and they are always infinite due to the availability of names for α-renaming. Although the pure $\approx_\alpha$ relation is decidable, when $\approx_\alpha$ is put together with an equational theory E which contains infinite congruence classes, the relation $\rightarrow_{\mathsf{R/E}}$ may not be decidable (as in first-order). We will define the nominal relation $\rightarrow_{\mathsf{R,E}}$ that deals with nominal E-matching instead of inspecting the whole α, E-congruence class of a term.

Definition 3.2 (Nominal R, E-rewriting)**.** The *one-step* E*-rewrite relation* $\Delta \vdash s \rightarrow_{\mathsf{R,E}} t$ is the least relation such that for any $R = (\nabla \vdash l \rightarrow r) \in \mathsf{R}$, position $\mathbb{C}$, term s', permutation π, and substitution θ,

$$\frac{s \equiv \mathbb{C}[s'] \qquad \Delta \vdash \left(\nabla\theta,\ s' \approx_{\alpha,\mathsf{E}} \pi \cdot (l\theta),\ \mathbb{C}[\pi \cdot (r\theta)] \approx_\alpha t\right)}{\Delta \vdash s \rightarrow_{\mathsf{R,E}} t}$$

The E*-rewrite relation* $\Delta \vdash s \rightarrow^*_{\mathsf{R,E}} t$ is the least relation that includes $\rightarrow_{\mathsf{R,E}}$ and is closed by reflexivity and transitivity of $\rightarrow_{\mathsf{R,E}}$, i.e., it satisfies:

1. for all Δ, s, s' we have $\Delta \vdash s \rightarrow^*_{\mathsf{R,E}} s'$ if $\Delta \vdash s \approx_\alpha s'$;

2. for all Δ, s, t, u we have that $\Delta \vdash s \to^*_{\mathsf{R,E}} t$ and $\Delta \vdash t \to^*_{\mathsf{R,E}} u$ implies $\Delta \vdash s \to^*_{\mathsf{R,E}} u$.

If $\Delta \vdash s \to^*_{\mathsf{R,E}} t$ and $\Delta \vdash s \to^*_{\mathsf{R,E}} t'$, then we say that R is E-*confluent* when there exists a term u such that $\Delta \vdash t \to^*_{\mathsf{R,E}} u$ and $\Delta \vdash t' \to^*_{\mathsf{R,E}} u$. Also, R is said to be E-*terminating* if there is no infinite $\to_{\mathsf{R,E}}$ sequence. R is called E-*convergent* if it is E-confluent and E-terminating.

A term t is said to be in $\mathsf{R,E}$-*normal* form ($\mathsf{R/E}$-normal form) whenever one cannot apply another step of $\to_{\mathsf{R,E}}$ ($\to_{\mathsf{R/E}}$).

Example 3.2 (Cont. Example 3.1)**.** This example illustrates the one-step C-rewrite:

$$a\#P' \vdash S' \vee (\exists[a]Q' \vee P') \to_{\mathsf{R,C}} S' \vee (\exists[a](P' \vee Q'))$$

with the rule $a\#P \vdash P \vee \exists[a]Q \to \exists[a](P \vee Q)$. In fact,

- $\Delta = \{a\#P'\}$ and $\nabla = \{a\#P\}$;
- $s = S' \vee (\exists[a]Q' \vee P') \equiv \mathbb{C}[\exists[a]Q' \vee P'] \equiv \mathbb{C}[s']$;

If we fix $\pi = id$ and $\theta = [P \mapsto P', Q \mapsto Q']$ we have:

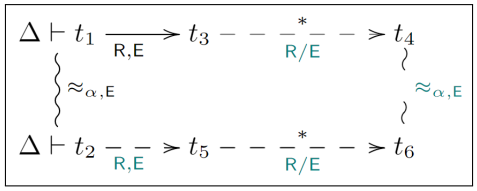
- $\Delta = a\#P' \vdash a\#P' = (a\#P)[P \mapsto P', Q \mapsto Q'] = \nabla\theta$;
- $s' = \exists[a]Q' \vee P' \approx_{\alpha,\mathsf{C}} (P \vee \exists[a]Q)[P \mapsto P', Q \mapsto Q'] = l\theta = \pi \cdot (l\theta)$;
- $\mathbb{C}[\pi \cdot (r\theta)] = \mathbb{C}[r\theta] = \mathbb{C}[(\exists[a](P \vee Q))[P \mapsto P', Q \mapsto Q']] = \mathbb{C}[\exists[a](P' \vee Q')] = S' \vee (\exists[a](P' \vee Q')) \approx_\alpha t$

Thus, $a\#P' \vdash S' \vee (\exists[a]Q' \vee P') \to_{\mathsf{R,C}} S' \vee (\exists[a](P' \vee Q'))$.

Since $\vee$ is a commutative symbol, we could reduce the initial term to three other possible terms because we have two occurrences of the disjunction. Thus, we can "permute" the subterms inside the rewriting modulo C.

Remark 3.3. Following the approach by Jouannaud et al. [18], E-confluence is a consequence of relating $\to_{\mathsf{R/E}}$ and $\to_{\mathsf{R,E}}$, which relies on a property called E-*coherence* which will be extended here, to the nominal framework.

Definition 3.4 (Nominal E-Coherence)**.** The relation $\Delta \vdash \_ \to_{\mathsf{R,E}} \_$ is called E-*coherent* iff for all t_1, t_2, t_3 such that $\Delta \vdash t_1 \approx_{\alpha,\mathsf{E}} t_2$ and $\Delta \vdash t_1 \to_{\mathsf{R,E}} t_3$, there exist t_4, t_5, t_6 such that $\Delta \vdash t_3 \to^*_{\mathsf{R/E}} t_4$, $t_2 \to_{\mathsf{R,E}} t_5 \to^*_{\mathsf{R/E}} t_6$ and $\Delta \vdash t_4 \approx_{\alpha,\mathsf{E}} t_6$, for some Δ.



The diagram above illustrates nominal E-coherence: the dashed lines represent existentially quantified reductions.

Definition 3.5. An equational theory E is called *a first-order equational theory* iff E is defined via a set of first-order axioms, i.e., identities of the form $\emptyset \vdash l = r$, where l, r are first-order terms. First-order terms do not contain atoms, abstractions and suspended permutations on variables.

Theorem 3.6. *Let* E *be a first-order theory and* R *be a nominal rewrite system that is* E*-confluent and* E*-terminating. Then the* $\mathsf{R,E}$*- and* $\mathsf{R/E}$*-normal forms of any term* t *are* E*-equal iff* $\to_{\mathsf{R,E}}$ *is* E*-coherent.*

Proof. The proof is in the Appendix (see A.1). □

In first-order rewriting, it is known that R,E-reducibility is decidable if E-matching is decidable. Following Jouannaud et al. [18], the existence of a finite and complete E-unification algorithm is a sufficient condition for that decidability. However, solving nominal E-unification problems has the additional complication of dealing with α-equality, which significantly impacts obtaining finite and complete sets of nominal E-unifiers.

Remark 3.7. Nominal C-unification is not finitary when one uses freshness constraints and substitutions for representing solutions [2], but the type of problems that generate an infinite set of C-unifiers are fixed-point equations $\pi \cdot X_? \overset{\mathsf{C}}{\approx}_? X$. For example, the nominal C-unification problem $(a\ b) \cdot X_? \overset{\mathsf{C}}{\approx}_? X$ has solutions $[X \mapsto a \oplus b], [X \mapsto (a \oplus b) \oplus (a \oplus b)], \ldots$ (Example 2.2). However, these problems do not appear in nominal C-matching, which is finitary [3]. Thus, the relation $\rightarrow_{\mathsf{R},\mathsf{C}}$ is decidable.

3.2 Nominal E-narrowing

Now we define the nominal narrowing relation modulo E, extending previous works [6].

Definition 3.8 (Nominal E-narrowing)**.** The *one-step* E*-narrowing relation* $(\Delta \vdash s) \rightsquigarrow_{\mathsf{R},\mathsf{E}} (\Delta' \vdash t)$ is the least relation such that for any $(\nabla \vdash l \to r) \in \mathsf{R}$, position $\mathbb{C}$, term s', permutation π, and substitution θ,

$$\frac{s \equiv \mathbb{C}[s'] \qquad \Delta' \vdash \left(\nabla\theta,\ \Delta\theta,\ s'\theta \approx_{\alpha,\mathsf{E}} \pi \cdot (l\theta),\ (\mathbb{C}[\pi \cdot r])\theta \approx_\alpha t\right)}{(\Delta \vdash s) \rightsquigarrow^{\theta}_{\mathsf{R},\mathsf{E}} (\Delta' \vdash t)}\,.$$

where $(\Delta', \theta) \in \mathscr{U}_{\mathsf{E}}(\nabla \vdash l, \Delta \vdash s')$. We will write only $(\Delta \vdash s) \rightsquigarrow_{\mathsf{R},\mathsf{E}} (\Delta' \vdash t)$, omitting the θ, when it is clear in the context.

The *nominal* E*-narrowing relation* $(\Delta \vdash s) \rightsquigarrow^*_{\mathsf{R},\mathsf{E}} (\Delta' \vdash t)$ is the least relation that includes $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$ and is closed by reflexivity and transitivity of $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$, i.e., it satisfies:

1. for all Δ, s, s' we have $(\Delta \vdash s) \rightsquigarrow^*_{\mathsf{R},\mathsf{E}} (\Delta \vdash s')$ if $\Delta \vdash s \approx_\alpha s'$;
2. for all $\Delta, \Delta', \Delta'', s, t$ and u: if $(\Delta \vdash s) \rightsquigarrow^*_{\mathsf{R},\mathsf{E}} (\Delta' \vdash t)$ and $(\Delta' \vdash t) \rightsquigarrow^*_{\mathsf{R},\mathsf{E}} (\Delta'' \vdash u)$ then $(\Delta \vdash s) \rightsquigarrow^*_{\mathsf{R},\mathsf{E}} (\Delta'' \vdash u)$.

The permutation π and substitution θ in the definition above are found by solving the nominal E-unification problem $(\nabla \vdash l) \overset{\mathsf{E}}{\approx}_? (\Delta \vdash s')$.

Remark 3.9. Note that decidability of $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$ relies on the existence of an algorithm for nominal E-unification that generates a finite minimal set of solutions. In this work, we will focus our illustrations on the theory C, for which a nominal unification algorithm exists.

Since nominal C-narrowing uses nominal C-unification, which is not finitary when we use pairs (Δ', θ) of freshness contexts and substitutions to represent solutions, following Remark 3.7, we conclude that our nominal C-narrowing trees are infinitely branching. The following example illustrates these infinite branches.

Example 3.3 (Cont. Example 2.2)**.** Consider the signature $\Sigma = \{h : 1, f^{\mathsf{C}} : 2, \oplus : 2\}$, where f^{C} and $\oplus$ are commutative symbols. Let $R = \{\ \vdash h(Y) \to Y,\ \vdash f^{\mathsf{C}}([a][b] \cdot Z, Z) \to f^{\mathsf{C}}(h(Z), h(Z))\}$ be a set of rewrite[2] rules. Let $\vdash h(f^{\mathsf{C}}([b][a]X, X))$ be a nominal term that we want to apply nominal C-narrowing to. Observe that we can apply one step of narrowing, and then we obtain a branch that yields infinite branches due to the fixed-point equation (see Figure 3).

[2] $\vdash l \to r$ denotes $\emptyset \vdash l \to r$.

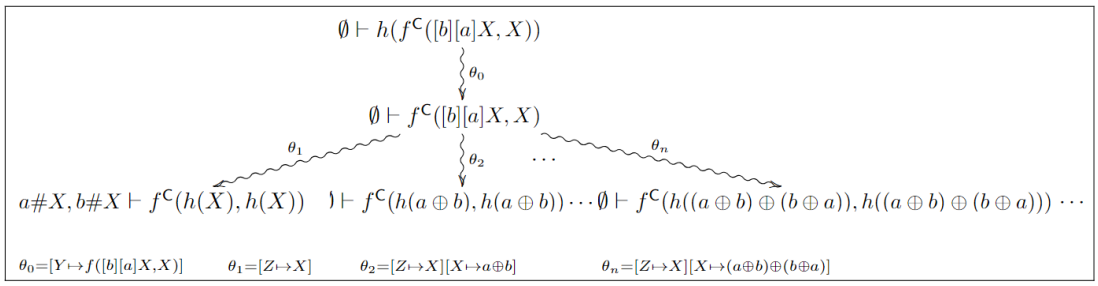


Figure 3: Infinitely branching tree

The first narrowing step is $\emptyset \vdash h(f^{\mathsf{C}}([b][a]X,X)) \rightsquigarrow_{\mathsf{R},\mathsf{C}} \emptyset \vdash f^{\mathsf{C}}([b][a]X,X)$, using the rule $\vdash h(Y) \to Y$. The substitution $\theta_0 = [Y \mapsto f^{\mathsf{C}}([b][a]X,X)]$ was computed in Example 2.2 when solving the C-unification problem $(\emptyset \vdash h(Y)) \overset{\mathsf{C}}{?\approx?} (\emptyset \vdash h(f^{\mathsf{C}}([b][a]X,X)))$.

The other infinite narrowing steps are generated due to the fixed-point equation found in the process of solving the C-unification problem $(\emptyset \vdash f^{\mathsf{C}}([a][b]Z,Z)) \overset{\mathsf{C}}{?\approx?} (\emptyset \vdash f^{\mathsf{C}}([b][a]X,X))$, computed in Example 2.2. Composing the fixed-point solutions with $(\emptyset, \theta_1)$ that we had, we get the substitutions $\theta_1 = [Z \mapsto X]$, $\theta_2 = [Z \mapsto X][X \mapsto a \oplus b]$ and $\theta_3 = [Z \mapsto X][X \mapsto (a \oplus b) \oplus (a \oplus b)]$ of our narrowing steps in Figure 3.

The following proposition shows that each nominal narrowing step corresponds to a nominal rewriting step, using the same substitution θ.

Proposition 3.10. *Let* E *be an equational theory for which a complete* E*-unification algorithm exists.* $(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1)$ *implies* $\Delta_1 \vdash (s_0\theta) \to_{\mathsf{R},\mathsf{E}} s_1$.

Proof. Indeed, suppose we have $(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1)$. The narrowing step guarantees that for a substitution θ, some permutation π, and a rule $\nabla \vdash l \to r \in \mathsf{R}$, the following holds:

- $s_0 \equiv \mathbb{C}[s_0']$ and $\Delta_1 \vdash \big(\nabla\theta,\ \Delta_0\theta,\ s_0'\theta \approx_{\alpha,\mathsf{E}} \pi \cdot (l\theta),\ (\mathbb{C}[\pi \cdot r])\theta \approx_{\alpha} s_1\big)$.

From the items above, it is easy to verify the following:

- $s_0\theta \equiv \mathbb{C}\theta[s_0'\theta]$; and $\Delta_1 \vdash (\nabla\theta', s_0'\theta \approx_{\alpha,\mathsf{E}} \pi \cdot (l\theta'), \mathbb{C}\theta[\pi \cdot (r\theta')] \approx_{\alpha} s_1)$,

and by the definition of rewrite modulo E, it implies that $\Delta_1 \vdash s_0\theta \to_{\mathsf{R},\mathsf{E}} s_1$. We need to fix the substitution θ used in the narrowing step as θ', and the result follows. □

4 Nominal Lifting Theorem modulo E

In this section, we assume $\mathsf{R} \cup \mathsf{E}$ an ENRS such that $\mathsf{R} = \{\nabla_i \vdash l_i \to r_i\}$ is E-convergent NRS, E is compatible with $\vdash$ and substitutions and that there exists a complete E-unification algorithm. We want to extend Proposition 3.10 and establish correspondence between finite sequences of nominal E-narrowing steps and sequences of nominal E-rewriting steps. This result corresponds to the classical Lifting Theorem ([16, 18, 6]) which will be extended to the nominal relations $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$ and $\to_{\mathsf{R},\mathsf{E}}$. The Lifting Theorem relates narrowing steps to rewriting steps. It is fundamental to guarantee that one can use the narrowing relation to solve T-unification problems when T is a convergent equational theory. The extension to the $\mathsf{R} \cup \mathsf{E}$-Lifting Theorem would allow us to solve nominal unification problems modulo $\mathsf{R} \cup \mathsf{E}$.

We start by defining a normalised substitution with respect to the relation $\to_{\mathsf{R},\mathsf{E}}$:

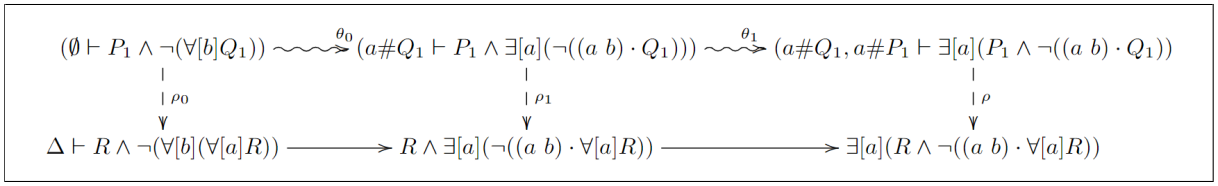


Figure 4: Illustration of Example 4.1

Definition 4.1 (Normalised substitution w.r.t $\to_{\mathsf{R},\mathsf{E}}$)**.** A substitution θ is *normalised in* Δ *with relation to* $\to_{\mathsf{R},\mathsf{E}}$ if $\Delta \vdash X\theta$ is a R,E-normal form for every X. A substitution θ *satisfies the freshness context* Δ iff there exists a freshness context ∇ such that $\nabla \vdash a\#X\theta$ for each $a\#X \in \Delta$. In this case, we say that θ satisfies Δ with ∇. The minimal such ∇ is $\langle \Delta\theta \rangle_{nf}$.

The following example illustrates the technique used in the proof of Lemma 4.2.

Example 4.1. Consider the rules $R_3 : a\#P \vdash P \wedge \exists[a]Q \to \exists[a](P \wedge Q)$ and $R_6 : \emptyset \vdash \neg(\forall[a]Q) \to \exists[a]\neg Q$.

Let $(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta_0}_{R_6} (\Delta_1 \vdash s_1) \rightsquigarrow^{\theta_1}_{R_3} (\Delta_2 \vdash s_2)$ be a narrowing derivation, illustrated in Figure 4 such that:

- $\Delta_0 \equiv \emptyset$ and $s_0 \equiv P_1 \wedge \neg(\forall[b]Q_1)$
- $\Delta_1 \equiv \{a\#Q_1\}$ and $s_1 \equiv P_1 \wedge \exists[a](\neg(a\ b)\cdot Q_1)$
- $\Delta_2 \equiv \{a\#Q_1, a\#P_1\}$ and $s_2 \equiv \exists[a](P_1 \wedge \neg(a\ b)\cdot Q_1)$

Let ρ be a substitution that satisfies Δ_2 with Δ. Then, there exists a rewriting derivation

$$\Delta \vdash s_0\rho_0 \to_{\mathsf{R},\mathsf{C}} s_1\rho_1 \to_{\mathsf{R},\mathsf{C}} s_2\rho$$

where $\Delta \vdash \Delta_0\rho_0$, $\Delta \vdash \Delta_1\rho_1$ and $\rho_0 = \theta_0\theta_1\rho$, $\rho_1 = \theta_1\rho$.

Supposing that $\rho = [Q_1 \mapsto \forall[a]R, P_1 \mapsto R]$, and $\Delta = \{a\#R\}$, we have

- $\Delta \vdash \Delta_2\rho = \{a\#Q_1, a\#P_1\}\rho = \{a\#\forall[a]R, a\#R\} = \{a\#R\}$
- $\theta_0 = [Q \mapsto (a\ b)\cdot Q_1]$ and $\theta_1 = [P' \mapsto P_1, Q' \mapsto \neg((a\ b)\cdot Q_1)]$
- $\rho_1 = \theta_1\rho = [P' \mapsto R, Q' \mapsto \neg((a\ b)\cdot\forall[a]R), Q_1 \mapsto \forall[a]R, P_1 \mapsto R]$
- $\rho_0 = \theta_0\rho_1 = [Q \mapsto (a\ b)\cdot\forall[a]R, P' \mapsto R, Q' \mapsto \neg((a\ b)\cdot\forall[a]R), Q_1 \mapsto \forall[a]R, P_1 \mapsto R]$
- $\Delta \vdash \Delta_1\rho_1 = (a\#Q_1)\rho_1 = a\#\forall[a]R = \emptyset$ and $\Delta \vdash \Delta_0\rho_0 = \emptyset$

Lemma 4.2. *($\rightsquigarrow_{\mathsf{R},\mathsf{E}}$ to $\to_{\mathsf{R},\mathsf{E}}$) Let $(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1)$. Then, for any substitution ρ that satisfies Δ_1 with Δ, the following holds*

$$\Delta \vdash (s_0\theta)\rho \to_{\mathsf{R},\mathsf{E}} s_1\rho$$

In particular, Δ will be $\langle \Delta_1\rho \rangle_{nf}$.

Proof. From Proposition 3.10: $(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1)$ implies $\Delta_1 \vdash (s_0\theta) \to_{\mathsf{R},\mathsf{E}} s_1$. Applying Proposition 2.4 in $\Delta_1 \vdash s_0\theta \to_{\mathsf{R},\mathsf{E}} s_1$ gives:

- $(s_0\theta)\rho \equiv (\mathbb{C}\theta[s'_0\theta])\rho = \mathbb{C}\theta\rho[(s'_0\theta)\rho]$
- $\Delta_1 \vdash \nabla\theta$ implies $\langle \Delta_1\rho \rangle_{nf} \vdash \nabla\theta\rho$
- $\Delta_1 \vdash s'_0\theta \approx_{\alpha,\mathsf{E}} \pi\cdot(l\theta)$ implies $\langle \Delta_1\rho \rangle_{nf} \vdash s'_0\theta\rho \approx_{\alpha,\mathsf{E}} (\pi\cdot(l\theta))\rho = \pi\cdot(l\theta\rho)$

- $\Delta_1 \vdash \mathbb{C}\theta[\pi \cdot (r\theta)] \approx_\alpha s_1$ implies $\langle \Delta_1\rho\rangle_{nf} \vdash \mathbb{C}\theta\rho[\pi \cdot (r\theta\rho)] = (\mathbb{C}\theta[\pi \cdot (r\theta)])\rho \approx_\alpha s_1\rho$

which implies that $\langle \Delta_1\rho\rangle_{nf} \vdash (s_0\theta)\rho \to_{\mathsf{R,E}} s_1\rho$. Note that we need ρ satisfying Δ_1 with Δ to guarantee that when we instantiate Δ_1 we do not have any inconsistency with the freshness constraints in Δ_1. □

The following result (correctness) states that a finite sequence of rewriting steps exists for each finite sequence of narrowing steps.

Lemma 4.3. *($\rightsquigarrow^*_{\mathsf{R,E}}$ to $\to^*_{\mathsf{R,E}}$) Let $(\Delta_0 \vdash s_0) \rightsquigarrow^*_{\mathsf{R,E}} (\Delta_n \vdash s_n)$ be a nominal* E*-narrowing derivation. Let ρ be a substitution satisfying Δ_n with Δ.*

$$(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta_0}_{\mathsf{R,E}} (\Delta_1 \vdash s_1) \rightsquigarrow^{\theta_1}_{\mathsf{R,E}} \dots \rightsquigarrow^{\theta_{n-1}}_{\mathsf{R,E}} (\Delta_n \vdash s_n)$$

Then, there exists a nominal E*-rewriting derivation*

$$\Delta \vdash s_0\rho_0 \to_{\mathsf{R,E}} \dots \to_{\mathsf{R,E}} s_i\rho_i \to_{\mathsf{R,E}} \dots \to_{\mathsf{R,E}} s_{n-1}\rho_{n-1} \to_{\mathsf{R,E}} s_n\rho$$

such that $\Delta \vdash \Delta_i\rho_i$ and $\rho_i = \theta_i \dots \theta_{n-1}\rho$, for all $0 \le i < n$. In other words, $\Delta \vdash (s_0\theta)\rho \to^*_{\mathsf{R,E}} s_n\rho$ where $\theta = \theta_0\theta_1 \dots \theta_{n-1}$.

Proof. By induction on the length $n \ge 1$ of the narrowing derivation $(\Delta_0 \vdash s_0) \rightsquigarrow^n_{\mathsf{R,E}} (\Delta_n \vdash s_n)$, using the one-step result proved in Lemma 4.2. (We start the induction for $n = 1$ because the case for $n = 0$ holds trivially and gives no additional insight.)

- **Base Case:** For $n = 1$, we have $(\Delta_0 \vdash s_0) \rightsquigarrow_{\mathsf{R,E}} (\Delta_1 \vdash s_1)$ and by Lemma 4.2, for any ρ satisfying Δ_1 with Δ we have $\Delta \vdash (s_0\theta_0)\rho \to_{\mathsf{R,E}} s_1\rho$. Since $\Delta \vdash \Delta_1\rho$, and by the narrowing step $\Delta_1 \vdash \Delta_0\theta_0$, we get $\Delta \vdash \Delta_0\theta_0\rho$. Taking $\rho_0 = \theta_0\rho$, we have the result $\Delta \vdash s_0\rho_0 \to_{\mathsf{R,E}} s_1\rho$ such that $\Delta \vdash \Delta_0\rho_0$.
- **Induction Step:** Assume that the result holds for $n > 1$. Then $(\Delta_0 \vdash s_0) \rightsquigarrow^n_{\mathsf{R,E}} (\Delta_n \vdash s_n)$ implies that there exists a rewriting derivation $\Delta \vdash s_0\rho_0 \to^n_{\mathsf{R,E}} s_n\rho$, for some ρ satisfying Δ_n with Δ and Figure 5 illustrates this setting.

  We want to show that the result follows for $n+1$. Consider the narrowing step

  $$(\Delta_n \vdash s_n) \rightsquigarrow^{\theta_n}_{\mathsf{R,E}} (\Delta_{n+1} \vdash s_{n+1}).$$

  By Lemma 4.2, for any substitution, let's name it σ, that satisfies Δ_{n+1} with Δ **(H1)** we have

  $$\Delta \vdash (s_n\theta_n)\sigma \to_{\mathsf{R,E}} s_{n+1}\sigma \tag{1}$$

  Take $\rho = \theta_n\sigma$. Note that ρ satisfies Δ_n with Δ:

  (H1) $\Delta \vdash \Delta_{n+1}\sigma$.

  (H2) By Definition 3.8: $\Delta_{n+1} \vdash \Delta_n\theta_n$.

  (H3) From **(H2)** and Proposition 2.4(1) generalised to E: $\langle \Delta_{n+1}\sigma\rangle_{nf} \vdash \Delta_n\rho$.

  Thus, from **(H1)** and **(H3)** it follows that $\Delta \vdash \Delta_n\rho$. By the induction hypothesis, we have

  $$\Delta \vdash s_0\theta_0 \dots \theta_{n-1}\rho \to^n_{\mathsf{R,E}} s_n\rho$$

  with $\Delta \vdash \Delta_i\rho_i$ and $\rho_i = \theta_i \dots \theta_{n-1}\rho$, for every $i = 1, \dots, n$. Hence,

  $$\Delta \vdash s_0\theta_0 \dots \theta_{n-1}\theta_n\sigma \to^n_{\mathsf{R,E}} s_n\theta_n\sigma \overset{(1)}{\to}_{\mathsf{R,E}} s_{n+1}\sigma,$$

  and the result follows.

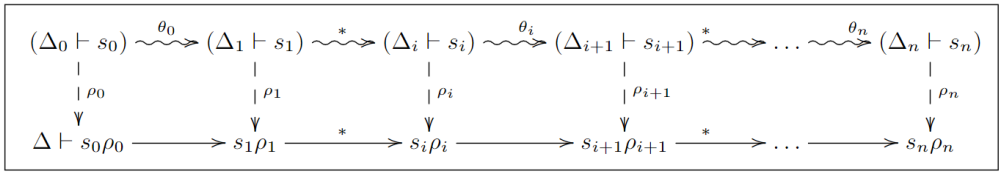


Figure 5: Corresponding Narrowing to Rewriting Derivations

□

The proof of the converse (completeness) is more challenging. Nevertheless, for one-step rewriting to one-step narrowing, the result holds with no further problems:

Lemma 4.4. *($\to_{\mathsf{R},\mathsf{E}}$ to $\rightsquigarrow_{\mathsf{R},\mathsf{E}}$) Let $\Delta_0 \vdash s_0$ be a nominal term in context and V_0 a finite set of variables containing $V = V(\Delta_0, s_0)$. Let ρ_0 be a R,E-normalised substitution, with $\mathtt{dom}(\rho_0) \subseteq V$, that satisfies Δ_0 with Δ and*

$$\Delta \vdash s_0\rho_0 = t_0 \to_{\mathsf{R},\mathsf{E}} t_1.$$

Then, there exists a nominal R,E-narrowing step

$$(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1),$$

for a substitution θ, a finite set of variables $V_1 \supseteq V(s_0)$, and a R,E-normalised substitution ρ_1 with Δ such that

$$(i)\ \Delta \vdash s_1\rho_1 \approx_{\alpha,\mathsf{E}} t_1 \qquad (ii)\ \mathtt{dom}(\rho_1) \subseteq V_1 \qquad (iii)\ \Delta \vdash \rho_0|_V \approx_{\alpha,\mathsf{E}} \theta\rho_1|_V$$

Proof. Suppose that the one-step rewriting is done in a position $\mathbb{C}_0$ of t_0, with substitution σ and rule $R_0 = \nabla_0 \vdash l_0 \to r_0 \in \mathsf{R}$:

$$(*)\ \frac{t_0 \equiv \mathbb{C}_0[t'_0] \qquad \Delta \vdash \nabla_0\sigma,\ t'_0 \approx_{\alpha,\mathsf{E}} \pi \cdot (l_0\sigma),\ \mathbb{C}_0[\pi \cdot (r_0\sigma)] \approx_{\alpha} t_1}{\Delta \vdash t_0 \to_{[\mathbb{C}_0,R_0],\mathsf{E}} t_1}$$

The following hold:

(H1) The variables of R_0 are renamed with respect to $t_0 = s_0\rho_0$ and Δ (to avoid conflicts). Thus, $V(R_0) \cap V(\Delta, t_0) = \emptyset$ and $\mathtt{dom}(\sigma) \cap V_0 = \emptyset$.

(H2) By hypothesis, $\Delta \vdash \Delta_0\rho_0$

(H3) Since ρ_0 is normalised in Δ and $\Delta \vdash s_0\rho_0 \to_{\mathsf{R},\mathsf{E}} t_1$, there must exist a non-variable position $\mathbb{C}'_0$ and a subterm s'_0 of s_0 such that $s_0 \equiv \mathbb{C}'_0[s'_0]$ and $\Delta \vdash s'_0\rho_0 \approx_{\alpha,\mathsf{E}} t'_0 \approx_{\alpha,\mathsf{E}} \pi \cdot (l_0\sigma)$.

Define **(H4)** $\theta = \rho_0\sigma$. Then, we have the following:

(H5) $\Delta \vdash \Delta_0\theta$: from **(H2)** it follows that $\Delta \vdash \Delta_0\rho_0$ and σ does not affect Δ_0 since $\mathtt{dom}(\sigma) = V(R_0)$.

(H6) Note that $s'_0\theta = s'_0\rho_0\sigma = s'_0\rho_0$ from **(H1)**. Therefore, $\Delta \vdash s'_0\theta \approx_{\alpha,\mathsf{E}} \pi \cdot (l_0\theta)$ and $\Delta \vdash \nabla_0\theta$, and (Δ, θ) is a solution for the nominal E-unification problem $(\Delta_0 \vdash s'_0) \stackrel{\mathsf{E}}{?\approx?} (\nabla_0 \vdash \pi \cdot l_0)$. That is, $(\Delta, \theta) \in \mathscr{U}_{\mathsf{E}}(\Delta_0 \vdash s'_0, \nabla_0 \vdash \pi \cdot l_0)$.

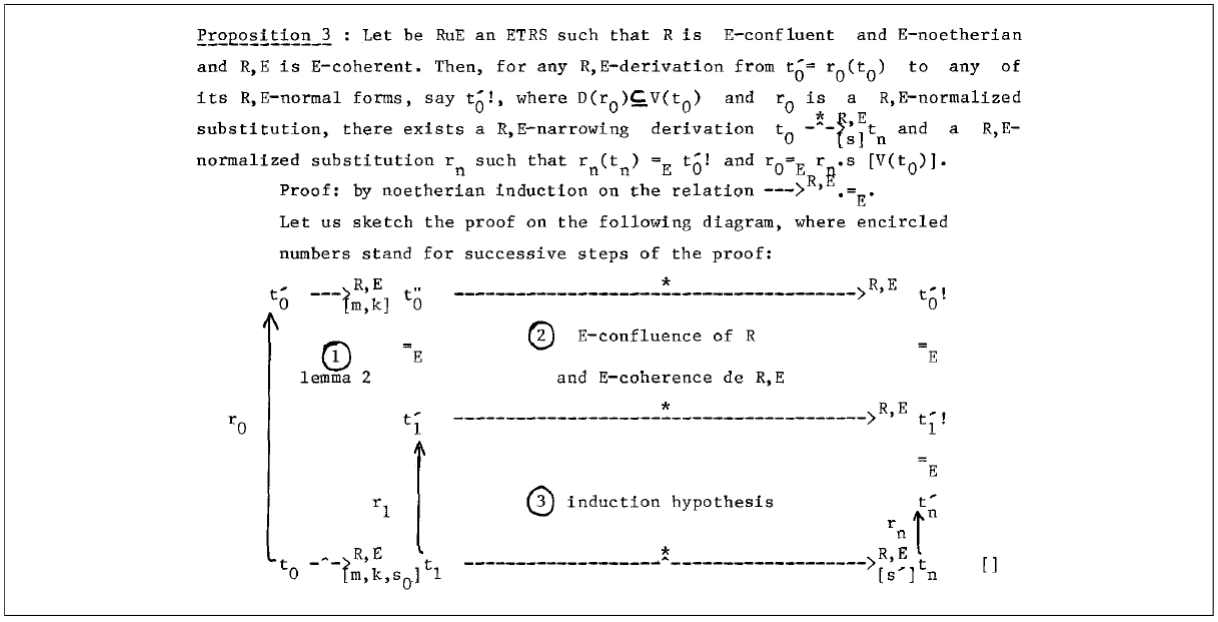


Figure 6: Proposition by Jouannaud [18] used in Lemma 4.5

Define s_1 as $s_1 = \mathbb{C}'_0[\pi \cdot r_0]\theta$ and $\Delta_1 = \Delta$. Conditions **(H4)** to **(H6)** imply the existence of the following nominal E-narrowing step:

$$(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta}_{\mathsf{R,E}} (\Delta_1 \vdash s_1).$$

Also $\Delta \vdash s_1 = \mathbb{C}'_0[\pi \cdot r_0]\theta = (\mathbb{C}'_0[\pi \cdot r_0])\rho_0\sigma \approx_\alpha (\mathbb{C}'_0\rho_0)[\pi \cdot r_0]\rho_0 \overset{(*)}{\approx}_\alpha t_1$. Take $\rho_1 = \mathtt{Id}$ as the identity substitution, and items (i) and (ii) follow with $\mathtt{dom}(\rho_1) = \emptyset$ and $V_1 = V(s_0)$. Finally, it is trivial to check (iii): $\Delta \vdash X\rho_0 \approx_{\alpha,\mathsf{E}} X\theta\rho_1 \equiv X\rho_0\sigma\mathtt{Id}$, for all $X \in V$, and the result follows.

□

Lemma 4.5. *Let* $\mathsf{R} \cup \mathsf{E}$ *be an ENRS such that* R *is* E*-convergent and* $\rightarrow_{\mathsf{R,E}}$ *is* E*-coherent. Let* V_0 *be a finite set of variables containing* $V = V(\Delta_0, s_0)$*. Then, for any* R,E*-derivation*

$$\Delta \vdash t_0 = s_0\rho_0 \rightarrow_{\mathsf{R,E}} t_1 \rightarrow_{\mathsf{R,E}} \ldots \rightarrow_{\mathsf{R,E}} t_n = t_0{\downarrow}$$

to any of its R,E*-normal forms, say* $t_0{\downarrow}$*, where* $\mathtt{dom}(\rho_0) \subseteq V(s_0) \subseteq V_0$ *and* ρ_0 *is a* R,E*-normalised substitution that satisfies* Δ_0 *with* Δ*, there exist a* R,E*-narrowing derivation*

$$(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta_0}_{\mathsf{R,E}} (\Delta_1 \vdash s_1) \rightsquigarrow^{\theta_1}_{\mathsf{R,E}} \ldots \rightsquigarrow^{\theta_{n-1}}_{\mathsf{R,E}} (\Delta_n \vdash s_n)$$

for each i*,* $0 \leq i < n$*, substitutions* ρ *and* ρ_i *normalised in* Δ *w.r.t* $\rightarrow_{\mathsf{R,E}}$ *such that*

$$(1)\ \Delta \vdash \Delta_i\rho_i; \qquad (2)\ \Delta \vdash s_i\rho_i \approx_{\alpha,\mathsf{E}} t_i; \qquad (3)\ \Delta \vdash \rho_0|_V \approx_{\alpha,\mathsf{E}} \theta\rho_n|_V.$$

where $\rho_i = \theta_i \ldots \theta_{n-1}\rho$ *and* $\theta = \theta_0\theta_1 \ldots \theta_{n-1}$.

Proof. By induction on the number of steps n applied in the derivation $\Delta \vdash t_0 = s_0\rho_0 \rightarrow^*_{\mathsf{R,E}} t_0{\downarrow}$.

- **Base Case:** For $n = 1$ the result follows directly from Lemma 4.4.

- **Induction Step:** Let $n > 1$ and assume that the result holds for sequences of $n-1$ rewriting steps. Then,

$$\Delta \vdash t_0 = s_0\rho_0 \to_{\mathsf{R},\mathsf{E}} t_1 \overbrace{\to_{\mathsf{R},\mathsf{E}} \cdots \to_{\mathsf{R},\mathsf{E}}}^{n-1} t_n = t_0{\downarrow}$$

Now using Lemma 4.4 on the rewrite step $\Delta \vdash t_0 \to_{\mathsf{R},\mathsf{E}} t_1$. Then, we get that $(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta_0}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1)$, where ρ_0 is a R,E-normalised substitution that satisfies Δ_0 with Δ, and

(H1) $\Delta \vdash s_1\rho_1 = t_1' \approx_{\alpha,\mathsf{E}} t_1$; and

(H2) $\Delta \vdash \rho_0|_V \approx_{\alpha,\mathsf{E}} \theta\rho_1|_V$.

Now consider the sequence to any of the normal forms of t_1:

$$\Delta \vdash t_1 \overbrace{\to_{\mathsf{R},\mathsf{E}} \cdots \to_{\mathsf{R},\mathsf{E}}}^{n-1} t_n = t_1{\downarrow_{\mathsf{R},\mathsf{E}}}$$

By the induction hypothesis, there exists a narrowing sequence

$$(\Delta_1 \vdash s_1) \rightsquigarrow^{\theta_1}_{\mathsf{R},\mathsf{E}} \cdots \rightsquigarrow^{\theta_{n-1}}_{\mathsf{R},\mathsf{E}} (\Delta_n \vdash s_n)$$

with $\theta = \theta_1 \ldots \theta_{n-1}$, a normalised substitution ρ_n such that

(H3) $\Delta \vdash \Delta_i\rho_i$;

(H4) $\Delta \vdash s_i\rho_i = t_i' \approx_{\alpha,\mathsf{E}} t_i$, for every i;

(H5) $\Delta \vdash \rho_0|_V \approx_{\alpha,\mathsf{E}} \theta\rho_n|_V$.

Note that from **(H4)**, $\Delta \vdash s_n\rho_n = t_n' \approx_{\alpha,\mathsf{E}} t_n$. Since R is E-convergent and $\to_{\mathsf{R},\mathsf{E}}$ is E-coherent, it follows from Theorem 3.6, that all the normal forms of t_0 are $\approx_{\alpha,\mathsf{E}}$-equivalent. That is, $\Delta \vdash t_n' \approx_{\alpha,\mathsf{E}} t_1{\downarrow_{\mathsf{R},\mathsf{E}}} \approx_{\alpha,\mathsf{E}} t_0{\downarrow_{\mathsf{R},\mathsf{E}}} = t_n$. Therefore, there exists a nominal E-narrowing sequence

$$(\Delta_0 \vdash s_0) \rightsquigarrow^{\theta_0}_{\mathsf{R},\mathsf{E}} (\Delta_1 \vdash s_1) \rightsquigarrow^{\theta_1}_{\mathsf{R},\mathsf{E}} \cdots \rightsquigarrow^{\theta_{n-1}}_{\mathsf{R},\mathsf{E}} (\Delta_n \vdash s_n).$$

The diagram that illustrates this proof is analogous to the diagram of the corresponding proof in first-order rewriting and presented in Figure 7.

□

As a consequence of Lemmas 4.5 and 4.3 we obtain:

Theorem 4.6 (E-Lifting Theorem)**.** *To each finite sequence of nominal* E*-rewriting steps corresponds a finite sequence of nominal* E*-narrowing steps, and vice versa.*

Since there exists an algorithm for nominal C-unification and C is compatible with substitutions (Proposition 2.4), we have the following result.

Corollary 4.7. *The* C*-Nominal Lifting theorem holds.*

5 Conclusion and Future Work

In this work, we proposed definitions for nominal R,E-rewriting and R,E-narrowing and proved some properties relating them, obtaining the proof of the E-Lifting Theorem, in the case R is an E-convergent NRS, $\to_{\mathsf{R},\mathsf{E}}$ is E-coherent and a complete algorithm for nominal E-unification exists. As C is the only equational theory for which a complete algorithm for nominal unification exists, we illustrate our results using this theory. Also, since the nominal C-unification problem (when using freshness constraints) only is finitary, our nominal C-narrowing tree is infinitely branching. In future work, we plan to investigate alternative approaches to nominal C-unification for which the representation of solutions is finite, such as the approach using fixed-point constraints.

References

[1] Mauricio Ayala-Rincón, Washington de Carvalho Segundo, Maribel Fernández & Daniele Nantes-Sobrinho (2017): *Nominal C-Unification*. In Fabio Fioravanti & John P. Gallagher, editors: *Logic-Based Program Synthesis and Transformation - 27th International Symposium, LOPSTR 2017, Namur, Belgium, October 10-12, 2017, Revised Selected Papers*, *Lecture Notes in Computer Science* 10855, Springer, pp. 235–251, doi:10.1007/978-3-319-94460-9_14. Available at `https://doi.org/10.1007/978-3-319-94460-9_14`.

[2] Mauricio Ayala-Rincón, Washington de Carvalho Segundo, Maribel Fernández & Daniele Nantes-Sobrinho (2017): *On Solving Nominal Fixpoint Equations*. In Clare Dixon & Marcelo Finger, editors: *Frontiers of Combining Systems - 11th International Symposium, FroCoS 2017, Brasília, Brazil, September 27-29, 2017, Proceedings*, *Lecture Notes in Computer Science* 10483, Springer, pp. 209–226, doi:10.1007/978-3-319-66167-4_12. Available at `https://doi.org/10.1007/978-3-319-66167-4_12`.

[3] Mauricio Ayala-Rincón, Washington de Carvalho Segundo, Maribel Fernández & Daniele Nantes-Sobrinho (2018): *A Formalisation of Nominal C-Matching through Unification with Protected Variables*. In Beniamino Accattoli & Carlos Olarte, editors: *Proceedings of the 13th Workshop on Logical and Semantic Frameworks with Applications, LSFA 2018, Fortaleza, Brazil, September 26-28, 2018*, *Electronic Notes in Theoretical Computer Science* 344, Elsevier, pp. 47–65, doi:10.1016/j.entcs.2019.07.004. Available at `https://doi.org/10.1016/j.entcs.2019.07.004`.

[4] Mauricio Ayala-Rincón, Washington de Carvalho Segundo, Maribel Fernández, Daniele Nantes-Sobrinho & Ana Cristina Rocha Oliveira (2019): *A formalisation of nominal α-equivalence with A, C, and AC function symbols*. *Theor. Comput. Sci.* 781, pp. 3–23, doi:10.1016/j.tcs.2019.02.020. Available at `https://doi.org/10.1016/j.tcs.2019.02.020`.

[5] Mauricio Ayala-Rincón, Washington de Carvalho Segundo, Maribel Fernández, Gabriel Ferreira Silva & Daniele Nantes-Sobrinho (2021): *Formalising nominal C-unification generalised with protected variables*. *Math. Struct. Comput. Sci.* 31(3), pp. 286–311, doi:10.1017/S0960129521000050. Available at `https://doi.org/10.1017/S0960129521000050`.

[6] Mauricio Ayala-Rincón, Maribel Fernández & Daniele Nantes-Sobrinho (2016): *Nominal Narrowing*. In Delia Kesner & Brigitte Pientka, editors: *1st International Conference on Formal Structures for Computation and Deduction, FSCD 2016, June 22-26, 2016, Porto, Portugal*, *LIPIcs* 52, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 11:1–11:17, doi:10.4230/LIPIcs.FSCD.2016.11. Available at `https://doi.org/10.4230/LIPIcs.FSCD.2016.11`.

[7] Mauricio Ayala-Rincón, Maribel Fernández & Daniele Nantes-Sobrinho (2018): *Fixed-Point Constraints for Nominal Equational Unification*. In Hélène Kirchner, editor: *3rd International Conference on Formal Structures for Computation and Deduction, FSCD 2018, July 9-12, 2018, Oxford, UK*, *LIPIcs* 108, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 7:1–7:16, doi:10.4230/LIPIcs.FSCD.2018.7. Available at `https://doi.org/10.4230/LIPIcs.FSCD.2018.7`.

[8] Mauricio Ayala-Rincón, Maribel Fernández & Ana Cristina Rocha Oliveira (2015): *Completeness in PVS of a Nominal Unification Algorithm*. In Mario R. F. Benevides & René Thiemann, editors: *Proceedings of the Tenth Workshop on Logical and Semantic Frameworks, with Applications, LSFA 2015, Natal, Brazil, August 31 - September 1, 2015*, *Electronic Notes in Theoretical Computer Science* 323, Elsevier, pp. 57–74, doi:10.1016/J.ENTCS.2016.06.005. Available at `https://doi.org/10.1016/j.entcs.2016.06.005`.

[9] Mauricio Ayala-Rincón, Maribel Fernández, Gabriel Ferreira Silva, Temur Kutsia & Daniele Nantes-Sobrinho (2023): *Nominal AC-Matching*. In Catherine Dubois & Manfred Kerber, editors: *Intelligent Computer Mathematics - 16th International Conference, CICM 2023, Cambridge, UK, September 5-8, 2023, Proceedings*, *Lecture Notes in Computer Science* 14101, Springer, pp. 53–68, doi:10.1007/978-3-031-42753-4_4. Available at `https://doi.org/10.1007/978-3-031-42753-4_4`.

[10] Franz Baader & Tobias Nipkow (1998): *Term rewriting and all that*. Cambridge University Press.

[11] Christophe Calvès & Maribel Fernández (2010): *Matching and alpha-equivalence check for nominal terms*. *J. Comput. Syst. Sci.* 76(5), pp. 283–301, doi:10.1016/J.JCSS.2009.10.003. Available at `https://doi.org/10.1016/j.jcss.2009.10.003`.

[12] Jesús Domínguez & Maribel Fernández (2019): *Nominal Syntax with Atom Substitutions: Matching, Unification, Rewriting*. In Leszek Antoni Gasieniec, Jesper Jansson & Christos Levcopoulos, editors: *Fundamentals of Computation Theory - 22nd International Symposium, FCT 2019, Copenhagen, Denmark, August 12-14, 2019, Proceedings*, *Lecture Notes in Computer Science* 11651, Springer, pp. 64–79, doi:10.1007/978-3-030-25027-0_5. Available at `https://doi.org/10.1007/978-3-030-25027-0_5`.

[13] Santiago Escobar, José Meseguer & Ralf Sasse (2008): *Variant Narrowing and Equational Unification*. In Grigore Rosu, editor: *Proceedings of the Seventh International Workshop on Rewriting Logic and its Applications, WRLA 2008, Budapest, Hungary, March 29-30, 2008*, *Electronic Notes in Theoretical Computer Science* 238, Elsevier, pp. 103–119, doi:10.1016/j.entcs.2009.05.015. Available at `https://doi.org/10.1016/j.entcs.2009.05.015`.

[14] Maribel Fernández & Murdoch Gabbay (2007): *Nominal rewriting*. *Inf. Comput.* 205(6), pp. 917–965, doi:10.1016/j.ic.2006.12.002. Available at `https://doi.org/10.1016/j.ic.2006.12.002`.

[15] Murdoch Gabbay & Andrew M. Pitts (2002): *A New Approach to Abstract Syntax with Variable Binding*. *Formal Aspects Comput.* 13(3-5), pp. 341–363, doi:10.1007/s001650200016. Available at `https://doi.org/10.1007/s001650200016`.

[16] Jean-Marie Hullot (1980): *Canonical Forms and Unification*. In Wolfgang Bibel & Robert A. Kowalski, editors: *5th Conference on Automated Deduction, Les Arcs, France, July 8-11, 1980, Proceedings*, *Lecture Notes in Computer Science* 87, Springer, pp. 318–334, doi:10.1007/3-540-10009-1_25. Available at `https://doi.org/10.1007/3-540-10009-1_25`.

[17] Jean-Pierre Jouannaud (1983): *Confluent and Coherent Equational Term Rewriting Systems: Application to Proofs in Abstract Data Types*. In Giorgio Ausiello & Marco Protasi, editors: *CAAP'83, Trees in Algebra and Programming, 8th Colloquium, L'Aquila, Italy, March 9-11, 1983, Proceedings*, *Lecture Notes in Computer Science* 159, Springer, pp. 269–283, doi:10.1007/3-540-12727-5_16. Available at `https://doi.org/10.1007/3-540-12727-5_16`.

[18] Jean-Pierre Jouannaud, Claude Kirchner & Hélène Kirchner (1983): *Incremental Construction of Unification Algorithms in Equational Theories*. In Josep Díaz, editor: *Automata, Languages and Programming, 10th Colloquium, Barcelona, Spain, July 18-22, 1983, Proceedings*, *Lecture Notes in Computer Science* 154, Springer, pp. 361–373, doi:10.1007/BFb0036921. Available at `https://doi.org/10.1007/BFb0036921`.

[19] Kentaro Kikuchi (2022): *Ground Confluence and Strong Commutation Modulo Alpha-Equivalence in Nominal Rewriting*. In Helmut Seidl, Zhiming Liu & Corina S. Pasareanu, editors: *Theoretical Aspects of Computing - ICTAC 2022 - 19th International Colloquium, Tbilisi, Georgia, September 27-29, 2022, Proceedings*, *Lecture Notes in Computer Science* 13572, Springer, pp. 255–271, doi:10.1007/978-3-031-17715-6_17. Available at `https://doi.org/10.1007/978-3-031-17715-6_17`.

[20] Kentaro Kikuchi & Takahito Aoto (2020): *Confluence and Commutation for Nominal Rewriting Systems with Atom-Variables*. In Maribel Fernández, editor: *Logic-Based Program Synthesis and Transformation - 30th International Symposium, LOPSTR 2020, Bologna, Italy, September 7-9, 2020, Proceedings*, *Lecture Notes in Computer Science* 12561, Springer, pp. 56–73, doi:10.1007/978-3-030-68446-4_3. Available at `https://doi.org/10.1007/978-3-030-68446-4_3`.

[21] Manfred Schmidt-Schauß, Temur Kutsia, Jordi Levy, Mateu Villaret & Yunus D. K. Kutz (2022): *Nominal Unification and Matching of Higher Order Expressions with Recursive Let*. *Fundam. Informaticae* 185(3), pp. 247–283, doi:10.3233/FI-222110. Available at `https://doi.org/10.3233/FI-222110`.

[22] Christian Urban, Andrew M. Pitts & Murdoch Gabbay (2004): *Nominal unification*. *Theor. Comput. Sci.* 323(1-3), pp. 473–497, doi:10.1016/j.tcs.2004.06.016. Available at `https://doi.org/10.1016/j.tcs.2004.06.016`.

[23] Emanuele Viola (2001): *E-unifiability via Narrowing*. In Antonio Restivo, Simona Ronchi Della Rocca & Luca Roversi, editors: *Theoretical Computer Science, 7th Italian Conference, ICTCS 2001, Torino,*

Italy, October 4-6, 2001, Proceedings, *Lecture Notes in Computer Science* 2202, Springer, pp. 426–438, doi:10.1007/3-540-45446-2_27. Available at `https://doi.org/10.1007/3-540-45446-2_27`.

A Appendix

Lemma A.1. *Substitution and permutation commute, that is,* $\pi \cdot (t\theta) = (\pi \cdot t)\theta$.

Proof. The proof is by induction on the structure of t.

Base Case.

- If $t \equiv a$: the result is trivial since the substitution does not affect atoms;
- If $t \equiv \pi' \cdot X$:

$$\begin{array}{rcl} \pi \cdot ((\pi' \cdot X)\theta) & = & \pi \cdot (\pi' \cdot (X\theta)) \\ & = & (\pi \circ \pi') \cdot (X\theta) \\ & = & ((\pi \circ \pi') \cdot X)\theta \\ & = & (\pi \cdot (\pi' \cdot X))\theta; \end{array}$$

Inductive Step.

- If $t \equiv [a]t'$:

$$\begin{array}{rcl} \pi \cdot (([a]t')\theta) & = & \pi \cdot ([a](t'\theta)) \\ & = & [\pi \cdot a](\pi \cdot (t'\theta)) \\ & \overset{IH}{=} & [\pi \cdot a]((\pi \cdot t')\theta) \\ & = & ([\pi \cdot a](\pi \cdot t'))\theta \\ & = & (\pi \cdot ([a]t'))\theta; \end{array}$$

- If $t \equiv f(t_1, \ldots, t_n)$:

$$\begin{array}{rcl} \pi \cdot (f(t_1, \ldots, t_n)\theta) & = & \pi \cdot (f(t_1\theta, \ldots, t_n\theta)) \\ & = & f(\pi \cdot (t_1\theta), \ldots, \pi \cdot (t_n\theta)) \\ & \overset{IH}{=} & f((\pi \cdot t_1)\theta, \ldots, (\pi \cdot t_n)\theta) \\ & = & f(\pi \cdot t_1, \ldots, \pi \cdot t_n)\theta \\ & = & (\pi \cdot f(t_1, \ldots, t_n))\theta. \end{array}$$

□

Lemma A.2. *Consider Pr and Pr′ problems.*

(1) $\langle Pr \cup Pr' \rangle_{nf} = \langle Pr \rangle_{nf} \cup \langle Pr' \rangle_{nf}$. *If* $Pr \subseteq Pr'$ *then* $\langle Pr \rangle_{nf} \subseteq \langle Pr' \rangle_{nf}$.

(2) Assume $Pr \overset{*}{\Longrightarrow} Pr'$. *Then* $\Gamma \vdash Pr$ *if and only if* $\Gamma \vdash Pr'$.

(3) $\Gamma \vdash Pr$ *if and only if* $\Gamma \vdash \langle Pr \rangle_{nf}$.

Proof. The proof can be found in [14], Corollary 12 and Lemma 15. □

Lemma A.3. *(Compatibility of* $\vdash$ *by substitutions) Suppose* Δ *and* $\Delta\theta$ *are consistent.*

1. *If* $\Delta \vdash a\#t$ *then* $\langle \Delta\theta \rangle_{nf} \vdash a\#(t\theta)$.
2. *If* $\Delta \vdash s \approx_{\alpha,\mathsf{C}} t$ *then* $\langle \Delta\theta \rangle_{nf} \vdash (s\theta) \approx_{\alpha,\mathsf{C}} (t\theta)$.
3. *If* $\Delta \vdash Pr$ *then* $\langle \Delta\theta \rangle_{nf} \vdash Pr\theta$.

Proof. We work by induction on the derivation of $\Delta \vdash a\#t$ or $\Delta \vdash s \approx_{\alpha,\mathsf{C}} t$.

1. We consider all rules in Figure 1, by analysing the last rule applied in $\Delta \vdash a\#t$.
   - Suppose the derivation concludes with (# atom). Then we have the trivial derivation
   $$\frac{}{\Delta \vdash a\#b}\ (\#\ \text{atom})$$
   Notice that applying the rule (# atom) again and that $a\#b\theta \equiv a\#b$ we have
   $$\frac{}{\langle \Delta\theta \rangle_{nf} \vdash a\#b}\ (\#\ \text{atom})$$
   and the result follows.
   - Suppose the derivation concludes with (# var), thus $\Delta \vdash a\#\pi \cdot X$, and consequently, $\pi^{-1} \cdot a\#X \in \Delta$. Therefore, $\pi^{-1} \cdot a\#X\theta \in \Delta\theta$. By Lemma A.2 we have $\langle \Delta\theta \cup \{\pi^{-1} \cdot a\#X\theta\} \rangle_{nf} = \langle \Delta\theta \rangle_{nf} \cup \langle \{\pi^{-1} \cdot a\#X\theta\} \rangle_{nf}$. Since $\{\pi^{-1} \cdot a\#X\theta\} \subseteq \Delta\theta$, one has $\langle \{\pi^{-1} \cdot a\#X\theta\} \rangle_{nf} \subseteq \langle \Delta\theta \rangle_{nf}$. Thus, $\langle \Delta\theta \rangle_{nf} \vdash \langle \{\pi^{-1} \cdot a\#X\theta\} \rangle_{nf}$. From Lemma A.2 $\langle \Delta\theta \rangle_{nf} \vdash \pi^{-1} \cdot a\#X\theta$.
   - Suppose the derivation concludes with (# a[a]). Then we have the trivial derivation
   $$\frac{}{\Delta \vdash a\#[a]t}\ (\#\ \text{a[a]})$$
   Notice that applying the rule (# a[a]) again and that $[a](t\theta) \equiv ([a]t)\theta$ we have
   $$\frac{}{\langle \Delta\theta \rangle_{nf} \vdash a\#[a](t\theta)}\ (\#\ \text{a[a]})$$
   - Suppose the derivation concludes with (# a[b]). Then $t = [b]t'$ and there exists a derivation Π such that
   $$\frac{\begin{array}{c}\Pi \\ \Delta \vdash a\#t'\end{array}}{\Delta \vdash a\#[b]t'}\ (\#\ \text{a[b]})$$
   By the induction hypothesis, there exists a derivation Π' of $\langle \Delta\theta \rangle_{nf} \vdash a\#t'\theta$. Now we can apply (# a[b]) again and obtain
   $$\frac{\begin{array}{c}\Pi' \\ \langle \Delta\theta \rangle_{nf} \vdash a\#t'\theta\end{array}}{\langle \Delta\theta \rangle_{nf} \vdash a\#[b](t'\theta)}\ (\#\ \text{a[b]})$$
   Observing that $[b](t'\theta) \equiv ([b]t')\theta = t\theta$, the result follows.
   - Suppose the derivation concludes with (# app), that is, $t = f(t_1,\ldots,t_n)$ and $\Delta \vdash a\#f(t_1,\ldots,t_n)$. Thus, there exist derivations $\Pi_1,\ldots,\Pi_n$ such that
   $$\frac{\begin{array}{ccc}\Pi_1 & & \Pi_n \\ \Delta \vdash a\#t_1 & \cdots & \Delta \vdash a\#t_n\end{array}}{\Delta \vdash a\#f(t_1,\ldots,t_n)}\ (\#\ \text{app})$$
   By the induction hypothesis, there exist derivations $\Pi'_1,\ldots,\Pi'_n$ for $\langle \Delta\theta \rangle_{nf} \vdash a\#(t_1\theta)$, $\cdots$, $\langle \Delta\theta \rangle_{nf} \vdash a\#(t_n\theta)$, respectively. Now, we can apply the rule (# app) again and obtain
   $$\frac{\begin{array}{ccc}\Pi'_1 & & \Pi'_n \\ \langle \Delta\theta \rangle_{nf} \vdash a\#(t_1\theta) & \cdots & \langle \Delta\theta \rangle_{nf} \vdash a\#(t_n\theta)\end{array}}{\langle \Delta\theta \rangle_{nf} \vdash a\#f(t_1\theta,\ldots,t_n\theta)}\ (\#\ \text{app})$$
   Since $f(t_1\theta,\ldots,t_n\theta) \equiv f(t_1,\ldots,t_n)\theta$, we obtain $\langle \Delta\theta \rangle_{nf} \vdash a\#f(t_1,\ldots,t_n)\theta$, and the result follows.

2. We consider all rules in Figure 1 for α-equivalence modulo C with addition of rule $(\approx_{\alpha,\mathsf{C}}\ C)$, by analysing the last rule applied in $\Delta \vdash s \approx_{\alpha,\mathsf{C}} t$.
   - Suppose the derivation concludes with $(\approx_{\alpha,\mathsf{C}}$ atom). Then we have the trivial derivation
   $$\frac{}{\Delta \vdash a \approx_{\alpha,\mathsf{C}} a}\ (\approx_{\alpha,\mathsf{C}} \text{ atom})$$
   Notice that applying the rule $(\approx_{\alpha,\mathsf{C}}$ atom) again and that $a\theta \approx_{\alpha,\mathsf{C}} a\theta \equiv a \approx_{\alpha,\mathsf{C}} a$ we have
   $$\frac{}{\langle \Delta\theta \rangle_{nf} \vdash a \approx_{\alpha,\mathsf{C}} a}\ (\approx_{\alpha,\mathsf{C}} \text{ atom})$$
   and the result follows.
   - Suppose the derivation concludes with $(\approx_{\alpha,\mathsf{C}}$ var), thus $\Delta \vdash \pi \cdot X \approx_{\alpha,\mathsf{C}} \pi' \cdot X$, and consequently, $ds(\pi,\pi')\#X \in \Delta$. Therefore, for all $a \in ds(\pi,\pi')$, we have that $a\#X\theta \in \Delta\theta$. By Lemma A.2 we have $\langle \Delta\theta \cup \{a\#X\theta\} \rangle_{nf} = \langle \Delta\theta \rangle_{nf} \cup \langle \{a\#X\theta\} \rangle_{nf}$. Since $\{a\#X\theta\} \subseteq \Delta\theta$, one has $\langle \{a\#X\theta\} \rangle_{nf} \subseteq \langle \Delta\theta \rangle_{nf}$. Thereby, $\langle \Delta\theta \rangle_{nf} \vdash \langle \{a\#X\theta\} \rangle_{nf}$, for all $a \in ds(\pi,\pi')$. From Lemma A.2 $\langle \Delta\theta \rangle_{nf} \vdash a\#X\theta$, and consequently $a\#X\theta \in \langle \Delta\theta \rangle_{nf}$, for all $a \in ds(\pi,\pi')$. Applying the rule $(\approx_{\alpha,\mathsf{C}}$ var) again the result follows.
   - Suppose the derivation concludes with $(\approx_{\alpha,\mathsf{C}}$ [aa]). Then $s = [a]s'$, $t = [a]t'$ and there exists a derivation Π such that
   $$\frac{\begin{array}{c}\Pi \\ \Delta \vdash s' \approx_{\alpha,\mathsf{C}} t'\end{array}}{\Delta \vdash [a]s' \approx_{\alpha,\mathsf{C}} [a]t'}\ (\approx_{\alpha,\mathsf{C}} \text{ [aa]})$$
   By the induction hypothesis, a derivation Π' of $\langle \Delta\theta \rangle_{nf} \vdash s'\theta \approx_{\alpha,\mathsf{C}} t'\theta$ exists. Now we can apply $(\approx_{\alpha,\mathsf{C}}$ [aa]) again and obtain
   $$\frac{\begin{array}{c}\Pi' \\ \langle \Delta\theta \rangle_{nf} \vdash s'\theta \approx_{\alpha,\mathsf{C}} t'\theta\end{array}}{\langle \Delta\theta \rangle_{nf} \vdash [a](s'\theta) \approx_{\alpha,\mathsf{C}} [a](t'\theta)}\ (\approx_{\alpha,\mathsf{C}} \text{ [aa]})$$
   Observing that $[a](s'\theta) \equiv ([a]s')\theta = s\theta$ and $[a](t'\theta) \equiv ([a]t')\theta = t\theta$, the result follows.
   - Suppose the derivation concludes with $(\approx_{\alpha,\mathsf{C}}$ [ab]). So $s = [a]s'$, $t = [b]t'$ and there exist derivations Π_1 and Π_2 such that
   $$\frac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ \Delta \vdash s' \approx_{\alpha,\mathsf{C}} (a\ b)\cdot t' & \Delta \vdash a\#t'\end{array}}{\Delta \vdash [a]s' \approx_{\alpha,\mathsf{C}} [b]t'}\ (\approx_{\alpha,\mathsf{C}} \text{ [ab]})$$
   By the induction hypothesis, there exists a derivation Π'_1 of $\langle \Delta\theta \rangle_{nf} \vdash s'\theta \approx_{\alpha,\mathsf{C}} (a\ b)\cdot t'\theta$ and by the first part of this Lemma there exists a derivation Π'_2 of $\langle \Delta\theta \rangle_{nf} \vdash a\#t'\theta$. Now we can apply $(\approx_{\alpha,\mathsf{C}}$ [ab]) again and obtain
   $$\frac{\begin{array}{cc}\Pi'_1 & \Pi'_2 \\ \langle \Delta\theta \rangle_{nf} \vdash s'\theta \approx_{\alpha,\mathsf{C}} (a\ b)\cdot t'\theta & \langle \Delta\theta \rangle_{nf} \vdash a\#t'\theta\end{array}}{\langle \Delta\theta \rangle_{nf} \vdash [a](s'\theta) \approx_{\alpha,\mathsf{C}} [b](t'\theta)}\ (\approx_{\alpha,\mathsf{C}} \text{ [ab]})$$
   Observing that $[a](s'\theta) \equiv ([a]s')\theta = s$ and $[b](t'\theta) \equiv ([b]t')\theta = t$, and using Lemma A.1, i.e., $((a\ b)\cdot t')\theta \equiv (a\ b)\cdot(t'\theta)$, the result follows.
   - Suppose the derivation concludes with $(\approx_{\alpha,\mathsf{C}}$ app). Then $s = f(s_1,\ldots,s_n)$, $t = f(t_1,\ldots,t_n)$ and there exist derivations $\Pi_1, \ldots, \Pi_n$ of $\Delta \vdash s_1 \approx_{\alpha,\mathsf{C}} t_1, \cdots, \Delta \vdash s_n \approx_{\alpha,\mathsf{C}} t_n$, respectively, such that

$$\frac{\begin{array}{ccc}\Pi_1 & & \Pi_n\\ \Delta \vdash s_1 \approx_{\alpha,\mathsf{C}} t_1 & \cdots & \Delta \vdash s_n \approx_{\alpha,\mathsf{C}} t_n\end{array}}{\Delta \vdash f(s_1,\ldots,s_n) \approx_{\alpha,\mathsf{C}} f(t_1,\ldots,t_n)}, f \notin \mathsf{C}\ (\approx_{\alpha,\mathsf{C}} \text{app})$$

By the induction hypothesis, there exist $\Pi'_1,\ldots,\Pi'_n$ for $\langle\Delta\theta\rangle_{nf} \vdash s_1\theta \approx_{\alpha,\mathsf{C}} t_1\theta, \cdots, \langle\Delta\theta\rangle_{nf} \vdash s_n\theta \approx_{\alpha,\mathsf{C}} t_n\theta$, respectively. Now we can apply the rule ($\approx_{\alpha,\mathsf{C}}$ app) again and obtain

$$\frac{\begin{array}{ccc}\Pi'_1 & & \Pi'_n\\ \langle\Delta\theta\rangle_{nf} \vdash s_1\theta \approx_{\alpha,\mathsf{C}} t_1\theta & \cdots & \langle\Delta\theta\rangle_{nf} \vdash s_n\theta \approx_{\alpha,\mathsf{C}} t_n\theta\end{array}}{\langle\Delta\theta\rangle_{nf} \vdash f(s_1\theta,\ldots,s_n\theta) \approx_{\alpha,\mathsf{C}} f(t_1\theta,\ldots,t_n\theta)}, f \notin \mathsf{C}\ (\approx_{\alpha,\mathsf{C}} \text{app})$$

Observing that $f(s_1\theta,\ldots,s_n\theta) \equiv f(s_1,\ldots,s_n)\theta = s\theta$ and also $f(t_1\theta,\ldots,t_n\theta) \equiv f(t_1,\ldots,t_n)\theta = t\theta$, the result follows.

- Suppose the derivation concludes with ($\approx_{\alpha,\mathsf{C}}$ C). Then $s = f(s_0,s_1)$, $t = f(t_0,t_1)$ and there exist derivations Π_1 and Π_2 of $\Delta \vdash s_0 \approx_{\alpha,\mathsf{C}} t_i$ and $\Delta \vdash s_1 \approx_{\alpha,\mathsf{C}} t_{(i+1)mod2}$, respectively, $i = 0,1$, such that

$$\frac{\begin{array}{cc}\Pi_1 & \Pi_2\\ \Delta \vdash s_0 \approx_{\alpha,\mathsf{C}} t_i & \Delta \vdash s_1 \approx_{\alpha,\mathsf{C}} t_{(i+1)mod2}\end{array}}{\Delta \vdash f(s_0,s_1) \approx_{\alpha,\mathsf{C}} f(t_0,t_1)}, i = 0,1\ (\approx_{\alpha,\mathsf{C}} \text{C})$$

By the induction hypothesis, there exist derivations Π'_1 and Π'_2 for $\langle\Delta\theta\rangle_{nf} \vdash s_0\theta \approx_{\alpha,\mathsf{C}} t_i\theta$ and $\langle\Delta\theta\rangle_{nf} \vdash s_1\theta \approx_{\alpha,\mathsf{C}} t_{(i+1)mod2}\theta$, respectively. Now we can apply the rule ($\approx_{\alpha,\mathsf{C}}$ C) again and obtain

$$\frac{\begin{array}{cc}\Pi'_1 & \Pi'_2\\ \langle\Delta\theta\rangle_{nf} \vdash s_0\theta \approx_{\alpha,\mathsf{C}} t_i\theta & \langle\Delta\theta\rangle_{nf} \vdash s_1\theta \approx_{\alpha,\mathsf{C}} t_{(i+1)mod2}\theta\end{array}}{\langle\Delta\theta\rangle_{nf} \vdash f(s_0\theta,s_1\theta) \approx_{\alpha,\mathsf{C}} f(t_0\theta,t_1\theta)}, i = 0,1\ (\approx_{\alpha,\mathsf{C}} \text{C})$$

Observing that $f(s_0\theta,s_1\theta) \equiv f(s_0,s_1)\theta = s$ and $f(t_0\theta,t_1\theta) \equiv f(t_0,t_1)\theta = t$, the result follows.

3. Since Pr is a set of freshness or α,C-equivalence constraints, by items (1) and (2), the result follows.

□

Definition A.1. $\to_{\mathsf{R},\mathsf{E}}$ (or simply R,E) is said to be E-*coherent* iff: $\forall t_1,t_2,t_3$ such that $t_1 \approx_{\mathsf{E}} t_2$ and $t_1 \to_{\mathsf{R},\mathsf{E}} t_3$, $\forall t_4,t_5,t_6$ such that $t_3 \to^*_{\mathsf{R}/\mathsf{E}} t_4$, $t_2 \to_{\mathsf{R},\mathsf{E}} t_5 \to^*_{\mathsf{R}/\mathsf{E}} t_6$ and $t_4 \approx_{\mathsf{E}} t_6$.

$$\begin{array}{ccccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \overset{*}{\underset{\mathsf{R}/\mathsf{E}}{- - \succ}} & t_4 \\ \| & & & & \| \\ \|\,\mathsf{E} & & & & \|\,\mathsf{E} \\ \| & & & & \| \\ t_2 & \underset{\mathsf{R},\mathsf{E}}{- - \succ} & t_5 & \overset{*}{\underset{\mathsf{R}/\mathsf{E}}{- - \succ}} & t_6 \end{array}$$

We want to stress the abuse of notation above, since $t_3 \to^*_{\mathsf{R}/\mathsf{E}} t_4$, for instance, should be written $[t_3]_{\approx_{\mathsf{E}}} \to^*_{\mathsf{R}/\mathsf{E}} [t_4]_{\approx_{\mathsf{E}}}$, and is acting as an abbreviation for $t_3 \approx_{\mathsf{E}} t'_3 \to_{\mathsf{R}} t'_4 \approx_{\mathsf{E}} t_4$.

By definition R is E-*confluent* iff for all terms t,t_1,t_2 such that $t \to^*_{\mathsf{R}/\mathsf{E}} t_1$ and $t \to^*_{\mathsf{R}/\mathsf{E}} t_2$, there exist t'_1,t'_2 such that $t_1 \to^*_{\mathsf{R}/\mathsf{E}} t'_1$, $t_2 \to^*_{\mathsf{R}/\mathsf{E}} t'_2$ and $t'_1 =_{\mathsf{E}} t'_2$.

Lemma A.2. $\to_{\mathsf{R},\mathsf{E}} \subseteq \to_{\mathsf{R}/\mathsf{E}}$.

Proof. Take $(s,t) \in \to_{\mathsf{R},\mathsf{E}}$. Then we have $s \equiv \mathbb{C}[s']$, $s' =_{\mathsf{E}} l\theta$ and $\mathbb{C}[r\theta] = t$, for some rule $l \to_{\mathsf{R}} r$ and a substitution θ. Notice that from $s' =_{\mathsf{E}} l\theta$ we may write $\mathbb{C}[s'] =_{\mathsf{E}} \mathbb{C}[l\theta]$ and with that

$$s \equiv \mathbb{C}[s'] =_{\mathsf{E}} \mathbb{C}[l\theta] \to_{\mathsf{R}} \mathbb{C}[r\theta] = t$$

That is,

$$s =_{\mathsf{E}} \circ \to_{\mathsf{R}} \circ =_{\mathsf{E}} t \qquad \Longrightarrow \qquad s \to_{\mathsf{R}/\mathsf{E}} t.$$

□

Lemma A.3. $\Delta \vdash \_ \to_{\mathsf{R},\mathsf{E}} \_ \subseteq \Delta \vdash \_ \to_{\mathsf{R}/\mathsf{E}} \_$.

Proof. Take $(s,t) \in \Delta \vdash \_ \to_{\mathsf{R},\mathsf{E}} \_$. Then we have $s \equiv \mathbb{C}[s']$, $\Delta \vdash \nabla\theta$, $\Delta \vdash s' \approx_{\alpha,\mathsf{E}} \pi \cdot (l\theta)$ and $\Delta \vdash \mathbb{C}[\pi \cdot (r\theta)] \approx_{\alpha} t$, for some rule $\nabla \vdash l \to_{\mathsf{R}} r$, a permutation π and a substitution θ. Notice that from $s' \approx_{\alpha,\mathsf{E}} \pi \cdot (l\theta)$ we may write $\mathbb{C}[s'] \approx_{\alpha,\mathsf{E}} \mathbb{C}[\pi \cdot (l\theta)]$ and with that

$$\Delta \vdash s \equiv \mathbb{C}[s'] \approx_{\alpha,\mathsf{E}} \mathbb{C}[\pi \cdot (l\theta)] \to_{\mathsf{R}} \mathbb{C}[\pi \cdot (r\theta)] \approx_{\alpha} t$$

That is,

$$\Delta \vdash s \approx_{\alpha,\mathsf{E}} \circ \to_{\mathsf{R}} \circ \approx_{\alpha,\mathsf{E}} t \qquad \Longrightarrow \qquad \Delta \vdash s \to_{\mathsf{R}/\mathsf{E}} t.$$

□

Example A.1. Consider the theory $\mathsf{E} = \{f(x,y) = f(y,x)\}$ and the rewrite system $\mathsf{R} = \{f(x,0) \to x\}$. Note that $f(a,0) \to a$ and $f(a,0) =_{\mathsf{E}} f(0,a)$ but the latter does not reduce with R, but it reduces with R,E.

Proposition A.1 (Jouannaud et al. [18])**.** *Assume* R *is* E*-confluent and* E*-noetherian. Then* R,E*- and* R/E*-normal forms of any term* t *are* E*-equal iff* $\to_{\mathsf{R},\mathsf{E}}$ *is* E*-coherent.*

Proof. Let $s_1 = t{\downarrow_{\mathsf{R},\mathsf{E}}}$ be the R,E-normal form of t. And let $s_2 = t{\downarrow_{\mathsf{R}/\mathsf{E}}}$ be the R/E-normal form of t.
($\Rightarrow$) Suppose that $s_1 =_{\mathsf{E}} s_2$ ($\star$).

We want to prove that $\to_{\mathsf{R},\mathsf{E}}$ is E-coherent. Let $t = t_1, t_2, t_3$ be terms such that

$$\begin{array}{ccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 \\ \| & & \\ t_2 & & \end{array} \quad \mathsf{E}$$

I. Consider the case where $t_3 = s_1 = t{\downarrow_{\mathsf{R},\mathsf{E}}}$:

Observe that we cannot have $t_2 = s_1$, because s_1 is a R,E-normal form and it is not possible to have $t_1 =_{\mathsf{E}} s_1$ and $t_1 \to_{\mathsf{R},\mathsf{E}} s_1$.

Also note that we cannot have $t_2 = s_2$, because since $\to_{\mathsf{R},\mathsf{E}} \subseteq \to_{\mathsf{R}/\mathsf{E}}$ we could not give a R,E-step from t_1, which is one of the representatives of $[s_2]_{\mathsf{E}}$, and that contradicts $t_1 \to_{\mathsf{R},\mathsf{E}} t_3$.

We can conclude that $t_2 \neq s_i$, for $i = 1,2$, hence we can make a one-step R,E-reduction from t_2, that is, there exists a t_5 such that

$$\begin{array}{ccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 \\ \| & & \\ t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 \end{array} \quad \mathsf{E}$$

Now we consider the following cases:

a) If $t_5 = s_1$ then $t_5 = t_3$ which gives us $t_5 =_{\mathsf{E}} t_3$.
Now the diagram in Figure 7 degenerates to $t_1 = t_2$, $t_5 = t_6$ and $t_3 = t_4$ with zero steps of R/E and the diagram becomes a line.

$$t_2 = t_1 \xrightarrow[\mathsf{R},\mathsf{E}]{} t_3 = t_5$$

b) If $t_5 = s_2 = t{\downarrow_{\mathsf{R}/\mathsf{E}}}$ then $t_5 \overset{(\star)}{=}_{\mathsf{E}} t_3$, by the hypothesis. The diagram in Figure 7 here degenerates to the square on the left, where $t_3 = t_4$ and $t_5 = t_6$.

$$\begin{array}{ccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 \\ \| \mathsf{E} & & \| \mathsf{E} \\ t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 \end{array}$$

c) If $t_5 \neq s_i$, for $i = 1,2$, then there exists a R/E-normal form of t_5, named t_6, such that $t_6 = s_2$, and this gives us that $t_6 \overset{(\star)}{=}_{\mathsf{E}} t_3$.

$$\begin{array}{ccccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & & \\ \| \mathsf{E} & & & & \\ t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & t_6 \end{array}$$

Here, note that $t_1 \to_{\mathsf{R}/\mathsf{E}} t_6$ and, by the hypothesis, $s_2 = t{\downarrow_{\mathsf{R}/\mathsf{E}}}$. The diagram in Figure 7 degenerates to $t_3 = t_4$.

$$\begin{array}{ccccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 = t_4 & & \\ \| \mathsf{E} & & & \| \mathsf{E} & \\ t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & t_6 \end{array}$$

II. Consider the case where t_3 is not a R,E-normal form of t. Then there exists a $t_4 = t{\downarrow_{\mathsf{R},\mathsf{E}}}$ such that $t_3 \to^*_{\mathsf{R},\mathsf{E}} t_4$ which implies $t_3 \to^*_{\mathsf{R}/\mathsf{E}} t_4$ since $\mathsf{R},\mathsf{E} \subseteq \mathsf{R}/\mathsf{E}$:

$$\begin{array}{ccccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & t_4 \\ \| \mathsf{E} & & & & \\ t_2 & & & & \end{array}$$

For the same reasons as case I, we can have neither $t_2 = s_1$ nor $t_2 = s_2$. Therefore we must have $t_2 \neq s_i$, for $i = 1,2$, hence we can make a one-step R,E-reduction from t_2, that is, there exists a t_5 such that

$$\begin{array}{ccccc} t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & t_4 \\ \| \mathsf{E} & & & & \\ t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & & \end{array}$$

Now we consider the following cases:

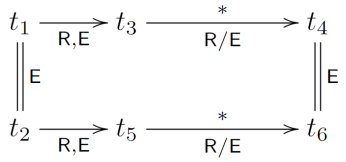
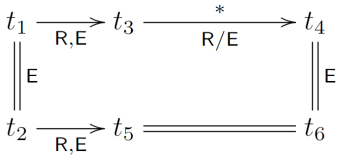
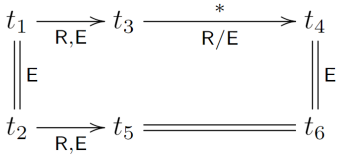


Figure 7: Diagram for E-coherence.

a) If $t_5 = s_1$ then $t_5 = t_4$ which gives us $t_5 =_{\mathsf{E}} t_4$. The diagram in Figure 7 degenerates to $t_5 = t_6$ and $t_4 =_{\mathsf{E}} t_6$.

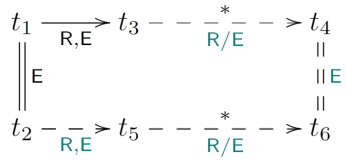


b) If $t_5 = s_2 = t{\downarrow_{\mathsf{R/E}}}$ then $t_5 \overset{(\star)}{=}_{\mathsf{E}} t_4$. The diagram in Figure 7 also degenerates to $t_5 = t_6$ and $t_4 =_{\mathsf{E}} t_6$.



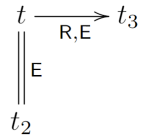
c) If $t_5 \neq s_i$, for $i = 1,2$, then there exists a $\mathsf{R/E}$-normal form of t_5, named t_6, such that $t_6 = s_2$, and this gives us that $t_6 \overset{(\star)}{=}_{\mathsf{E}} t_4$. This gives us exactly the diagram in Figure 7.

($\Leftarrow$) Assume $\rightarrow_{\mathsf{R,E}}$ is E-coherent.

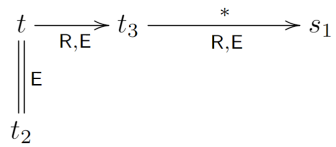


We want to prove that $s_1 =_{\mathsf{E}} s_2$.

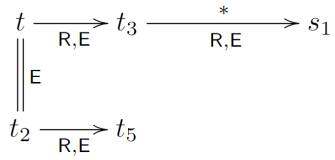
Consider $t_1 = t$, and suppose $t =_{\mathsf{E}} t_2$ and $t \rightarrow_{\mathsf{R,E}} t_3$.



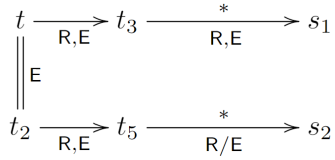
Consider the $\mathsf{R,E}$-normal form of t_3, $s_1 = t_3{\downarrow_{\mathsf{R,E}}} = t{\downarrow_{\mathsf{R,E}}}$ (it is also a $\mathsf{R,E}$-normal form of t).



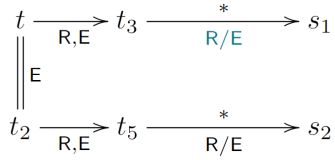
By the E-coherence property, there exists a t_5 such that



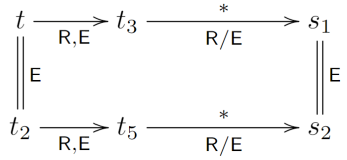
And from $t =_{\mathsf{E}} t_2 \to_{\mathsf{R,E}} t_5$ we have $t \to_{\mathsf{R/E}} t_5$. Consider then the R/E-normal form of t_5, $s_2 = t_5{\downarrow_{\mathsf{R/E}}} = t{\downarrow_{\mathsf{R/E}}}$ (it is also a R/E-normal form of t).



Since $\mathsf{R,E} \subseteq \mathsf{R/E}$, we may write R/E instead of R, E in the step $t_3 \to^*_{\mathsf{R,E}} s_1$:



Now we can apply the E-coherence property and get the result we wanted, $s_1 =_{\mathsf{E}} s_2$:

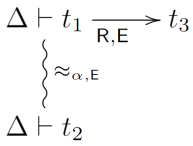


□

Conjecture A.1. *Let* E *be a first-order theory and* R *be a nominal rewrite system that is* E*-confluent and* E*-terminating. Then the* R, E*- and* R/E*-normal forms of any term t are* E*-equal iff* $\to_{\mathsf{R,E}}$ *is* E*-coherent.*

Proof. Let $s_1 \equiv t{\downarrow_{\mathsf{R,E}}}$ be the R, E-normal form of $\Delta \vdash t$. And let $s_2 \equiv t{\downarrow_{\mathsf{R/E}}}$ be the R/E-normal form of $\Delta \vdash t$.
($\Rightarrow$) Suppose that $\Delta \vdash_{\mathsf{E}} s_1 \approx s_2$ ($\star$).

We want to prove that $\to_{\mathsf{R,E}}$ is E-coherent. Let $t \equiv t_1$, t_2, t_3 be terms and Δ be a context such that $\Delta \vdash t_1 \approx_{\alpha,\mathsf{E}} t_2$ (equivalently $\Delta \vdash_{\mathsf{E}} t_1 \approx t_2$) and $\Delta \vdash t_1 \to_{\mathsf{R,E}} t_3$:



I. Consider the case where $t_3 \equiv s_1 \equiv t{\downarrow_{\mathsf{R},\mathsf{E}}}$:

Observe that we cannot have $t_2 \equiv s_1$ because s_1 is a R,E-normal form, and it is not possible to have $\Delta \vdash t_1 \approx_{\alpha,\mathsf{E}} s_1$ and $\Delta \vdash t_1 \to_{\mathsf{R},\mathsf{E}} s_1$.

Also note that we cannot have $t_2 \equiv s_2$, because since $\to_{\mathsf{R},\mathsf{E}} \subseteq \to_{\mathsf{R}/\mathsf{E}}$ we could not give a R,E-step from $\Delta \vdash t_1$, which is one of the representatives of $\Delta \vdash [s_2]_{\mathsf{E}}$, and that contradicts $\Delta \vdash t_1 \to_{\mathsf{R},\mathsf{E}} t_3$.

We can conclude that $t_2 \not\equiv s_i$, for $i = 1,2$, hence we can make a one-step R,E-reduction from $\Delta \vdash t_2$, that is, there exists a t_5 such that $\Delta \vdash t_2 \to_{\mathsf{R},\mathsf{E}} t_5$:

$$\begin{array}{ccc} \Delta \vdash t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 \\ \big\{ \approx_{\alpha,\mathsf{E}} & & \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 \end{array}$$

Now we consider the following cases:

a) If $t_5 \equiv s_1$ then $t_5 \equiv t_3$ which gives us $\Delta \vdash t_5 \approx_{\alpha,\mathsf{E}} t_3$.
Now the diagram in Figure 8 degenerates to $t_1 \equiv t_2$, $t_5 \equiv t_6$ and $t_3 \equiv t_4$ with zero steps of R/E and the diagram becomes a line.

$$\Delta \vdash t_2 = t_1 \xrightarrow[\mathsf{R},\mathsf{E}]{} t_3 = t_5$$

b) If $t_5 \equiv s_2 \equiv t{\downarrow_{\mathsf{R}/\mathsf{E}}}$ then $\Delta \vdash_{\mathsf{E}} t_5 \overset{(\star)}{\approx} t_3$, by the hypothesis. The diagram in Figure 8 degenerates to the square on the left, where $t_3 \equiv t_4$ and $t_5 \equiv t_6$.

$$\begin{array}{ccc} \Delta \vdash t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 \\ \big\{ \approx_{\alpha,\mathsf{E}} & & \big\{ \approx_{\alpha,\mathsf{E}} \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 \end{array}$$

c) If $t_5 \not\equiv s_i$, for $i = 1,2$, then there exists a R/E-normal form of $\Delta \vdash t_5$, named t_6, such that $t_6 \equiv s_2$, and this gives us that $\Delta \vdash_{\mathsf{E}} t_6 \overset{(\star)}{\approx} t_3$.

$$\begin{array}{ccccc} \Delta \vdash t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & & \\ \big\{ \approx_{\alpha,\mathsf{E}} & & & & \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & t_6 \end{array}$$

Here, note that $\Delta \vdash t_1 \to_{\mathsf{R}/\mathsf{E}} t_6$ and, by the hypothesis, $s_2 \equiv t{\downarrow_{\mathsf{R}/\mathsf{E}}}$. The diagram in Figure 8 degenerates to $t_3 \equiv t_4$.

$$\begin{array}{ccccc} \Delta \vdash t_1 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & = & t_4 \\ \big\{ \approx_{\alpha,\mathsf{E}} & & & & \big\{ \approx_{\alpha,\mathsf{E}} \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & t_6 \end{array}$$

II. Consider the case where t_3 is not a R,E-normal form of $\Delta \vdash t$. Then there exists a $t_4 \equiv t{\downarrow_{\mathsf{R},\mathsf{E}}}$ such that $\Delta \vdash t_3 \to^*_{\mathsf{R},\mathsf{E}} t_4$ which implies $\Delta \vdash t_3 \to^*_{\mathsf{R}/\mathsf{E}} t_4$ since $\mathsf{R},\mathsf{E} \subseteq \mathsf{R}/\mathsf{E}$:

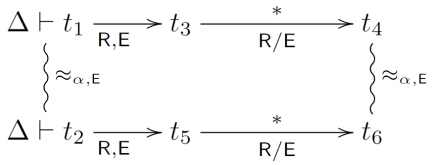
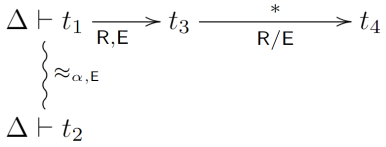
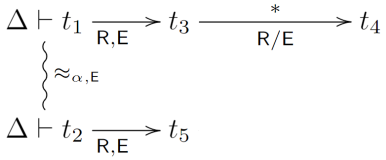


Figure 8: Diagram for nominal E-coherence

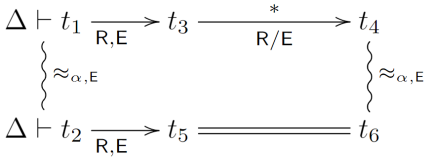


For the same reasons as case I, we can have neither $t_2 \equiv s_1$ nor $t_2 \equiv s_2$. Therefore we must have $t_2 \not\equiv s_i$, for $i = 1,2$, hence we can make a one-step R,E-reduction from $\Delta \vdash t_2$, that is, there exists a t_5 such that $\Delta \vdash t_2 \to_{\mathsf{R},\mathsf{E}} t_5$:

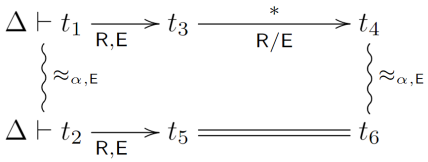


Now we consider the following cases:

a) If $t_5 \equiv s_1$ then $t_5 \equiv t_4$ which gives us $t_5 \approx_{\alpha,\mathsf{E}} t_4$. The diagram in Figure 8 degenerates to $t_5 \equiv t_6$ and $t_4 \approx_{\alpha,\mathsf{E}} t_6$.

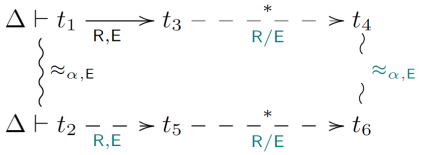


b) If $t_5 \equiv s_2 \equiv t{\downarrow_{\mathsf{R}/\mathsf{E}}}$ then $\Delta \vdash_{\mathsf{E}} t_5 \overset{(\star)}{\approx} t_4$. The diagram in Figure 8 also degenerates to $t_5 \equiv t_6$ and $t_4 \approx_{\alpha,\mathsf{E}} t_6$.



c) If $t_5 \not\equiv s_i$, for $i = 1,2$, then there exists a R/E-normal form of $\Delta \vdash t_5$, named t_6, such that $t_6 \equiv s_2$, and this gives us that $\Delta \vdash_{\mathsf{E}} t_6 \overset{(\star)}{\approx} t_4$. This gives us exactly the diagram in Figure 8.

($\Leftarrow$) Assume $\to_{\mathsf{R},\mathsf{E}}$ is E-coherent.



We want to prove that $\Delta \vdash_{\mathsf{E}} s_1 \approx_{\alpha,\mathsf{E}} s_2$.

Consider $t_1 \equiv t$, and suppose $\Delta \vdash t \approx_{\alpha,\mathsf{E}} t_2$ and $\Delta \vdash t \to_{\mathsf{R},\mathsf{E}} t_3$.

$$\begin{array}{ccc} \Delta \vdash t & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 \\ \big\downarrow \approx_{\alpha,\mathsf{E}} & & \\ \Delta \vdash t_2 & & \end{array}$$

Consider the R,E-normal form of $\Delta \vdash t_3$, $s_1 \equiv t_3{\downarrow_{\mathsf{R},\mathsf{E}}} \equiv t{\downarrow_{\mathsf{R},\mathsf{E}}}$ (it is also a R,E-normal form of $\Delta \vdash t$).

$$\begin{array}{ccccc} \Delta \vdash t & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R},\mathsf{E}]{*} & s_1 \\ \big\downarrow \approx_{\alpha,\mathsf{E}} & & & & \\ \Delta \vdash t_2 & & & & \end{array}$$

By the E-coherence property, there exists a t_5 such that $\Delta \vdash t_2 \to_{\mathsf{R},\mathsf{E}} t_5$:

$$\begin{array}{ccccc} \Delta \vdash t & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R},\mathsf{E}]{*} & s_1 \\ \big\downarrow \approx_{\alpha,\mathsf{E}} & & & & \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & & \end{array}$$

And from $\Delta \vdash t \approx_{\alpha,\mathsf{E}} t_2 \to_{\mathsf{R},\mathsf{E}} t_5$ we have $\Delta \vdash t \to_{\mathsf{R}/\mathsf{E}} t_5$. Consider then the R/E-normal form of $\Delta \vdash t_5$, $s_2 \equiv t_5{\downarrow_{\mathsf{R}/\mathsf{E}}} \equiv t{\downarrow_{\mathsf{R}/\mathsf{E}}}$ (it is also a R/E-normal form of $\Delta \vdash t$).

$$\begin{array}{ccccc} \Delta \vdash t & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R},\mathsf{E}]{*} & s_1 \\ \big\downarrow \approx_{\alpha,\mathsf{E}} & & & & \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & s_2 \end{array}$$

Since $\mathsf{R},\mathsf{E} \subseteq \mathsf{R}/\mathsf{E}$, we may write R/E instead of R,E in the step $\Delta \vdash t_3 \to^*_{\mathsf{R},\mathsf{E}} s_1$:

$$\begin{array}{ccccc} \Delta \vdash t & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & s_1 \\ \big\downarrow \approx_{\alpha,\mathsf{E}} & & & & \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & s_2 \end{array}$$

Now we can apply the E-coherence property and get the result we wanted, $\Delta \vdash_{\mathsf{E}} s_1 \approx s_2$:

$$\begin{array}{ccccc} \Delta \vdash t & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_3 & \xrightarrow[\mathsf{R},\mathsf{E}]{*} & s_1 \\ \big\downarrow \approx_{\alpha,\mathsf{E}} & & & & \big\downarrow \approx_{\alpha,\mathsf{E}} \\ \Delta \vdash t_2 & \xrightarrow[\mathsf{R},\mathsf{E}]{} & t_5 & \xrightarrow[\mathsf{R}/\mathsf{E}]{*} & s_2 \end{array}$$

□

Example A.2 (Cont. example 4.1)**.** We present the computation of θ_0 and θ_1:

$$
\begin{aligned}
(\emptyset, \mathtt{Id}, \{\neg(\forall[b]Q_1) \overset{\mathsf{C}}{\approx}_? \neg(\forall[a]Q)\}) \quad &\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{app})} \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{app})} (\emptyset, \mathtt{Id}, \{\forall[b]Q_1 \overset{\mathsf{C}}{\approx}_? \forall[a]Q\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{app})} (\emptyset, \mathtt{Id}, \{[b]Q_1 \overset{\mathsf{C}}{\approx}_? [a]Q\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{[ab]})} (\emptyset, \mathtt{Id}, \{(a\ b)\cdot Q_1 \overset{\mathsf{C}}{\approx}_? Q, a\#Q_1\}) \\
&\Longrightarrow_{(\#\ \text{var})} (\{a\#Q_1\}, \mathtt{Id}, \{(a\ b)\cdot Q_1 \overset{\mathsf{C}}{\approx}_? Q\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{inst})} (\{a\#Q_1\}, \theta_0 = [Q \mapsto (a\ b)\cdot Q_1], \{(a\ b)\cdot Q_1 \overset{\mathsf{C}}{\approx}_? (a\ b)\cdot Q_1\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{refl})} (\{a\#Q_1\}, \theta_0, \emptyset)
\end{aligned}
$$

$$
\begin{aligned}
(\{a\#Q_1, a\#P'\}, \mathtt{Id}, \{P_1 \wedge \exists[a](\neg(a\ b)\cdot Q_1) \overset{\mathsf{C}}{\approx}_? P' \wedge \exists[a]Q'\}) \quad &\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \mathsf{C})} \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \mathsf{C})} (\{a\#Q_1, a\#P'\}, \mathtt{Id}, \{P_1 \overset{\mathsf{C}}{\approx}_? P', \exists[a](\neg(a\ b)\cdot Q_1) \overset{\mathsf{C}}{\approx}_? \exists[a]Q'\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{app})} (\{a\#Q_1, a\#P'\}, \mathtt{Id}, \{P_1 \overset{\mathsf{C}}{\approx}_? P', [a](\neg(a\ b)\cdot Q_1) \overset{\mathsf{C}}{\approx}_? [a]Q'\}) \\
&\Longrightarrow_{(\approx_{\alpha,\mathsf{C}}\ \text{[aa]})} (\{a\#Q_1, a\#P'\}, \mathtt{Id}, \{P_1 \overset{\mathsf{C}}{\approx}_? P', (\neg(a\ b)\cdot Q_1) \overset{\mathsf{C}}{\approx}_? Q'\}) \\
&\Longrightarrow^2_{(\approx_{\alpha,\mathsf{C}}\ \text{inst})} (\{a\#Q_1, a\#P_1\}, \theta_1 = [P' \mapsto P_1, Q' \mapsto \neg(a\ b)\cdot Q_1], \{P_1 \overset{\mathsf{C}}{\approx}_? P_1, \\
&\qquad\qquad (\neg(a\ b)\cdot Q_1) \overset{\mathsf{C}}{\approx}_? (\neg(a\ b)\cdot Q_1)\}) \\
&\Longrightarrow^2_{(\approx_{\alpha,\mathsf{C}}\ \text{refl})} (\{a\#Q_1, a\#P_1\}, \theta_1, \emptyset)
\end{aligned}
$$