# CS 576 Lecture 7, 2/7/17

J. Meseguer

## 1. More on substitutions

First of all we shall define the relation $\alpha \sqsupseteq_B \beta$ over substitutions a bit more carefully and in full generality.

<u>Def.</u> Let $\alpha, \beta \in [X \to T_\Sigma(X)]$ be (finite) substitutions (i.e., $dom(\alpha)$ and $dom(\beta)$ are finite sets), and $(\Sigma, B)$ an equational theory. We define

$$\alpha \sqsupseteq_B \beta$$

iff there exists a (finite) substitution $\rho$ such that

$$(\alpha\rho)|_{dom(\alpha) \cup dom(\beta)} =_B \beta \qquad (\ast)$$

<u>Exercise</u>. Prove that we can always choose $\rho$ with $dom(\rho) \subseteq ran(\alpha) \cup (dom(\beta) - dom(\alpha))$. <u>Hint</u>: If $\rho_0$ satisfies the above condition $(\ast)$, then can define $\rho = \rho_0|_{ran(\alpha) \cup (dom(\beta) - dom(\alpha))}$.
Prove furthermore that if $(\Sigma, B, R)$ is a rewrite theory and $\beta$ is $R,B$-irreducible, and variables are $R,B$-irred., then both $\alpha$ and the $\rho$ so chosen are $R,B$-irred.

Q: Is the $\alpha \sqsupseteq_B \beta$ relation decidable?

A: Yes if we have a $B$-matching algorithm

Lemma. Suppose $(\Sigma, B)$ has a $B$-matching algorithm, and let $dom(\alpha) = \{x_1, .., x_n\}$, then given $\alpha$ and $\beta$ we can choose a $\rho$ such that $(\alpha\rho)|_{dom(\alpha) \cup dom(\beta)} =_B \beta$ iff

$$\exists \rho_1 \in Match_B(\langle \alpha(x_1), .., \alpha(x_n)\rangle, \langle \beta(x_1), .., \beta(x_n)\rangle)$$

where $\langle -, .., - \rangle$ is a new tupling operator added to $\Sigma$, and then $\rho = \rho_1 \mathbin{\dot{\cup}} \left(\beta|_{dom(\beta) - (dom(\alpha) \cup ran(\alpha))}\right)$.

If such a $B$-matching substitution does not exist, we cannot have a $\rho$ with $(\alpha\rho)_{dom(\alpha) \cup dom(\beta)} =_B \beta$, since this in particular requires $x_i\alpha\rho =_B x_i\beta$, $1 \leq i \leq n$, making $\rho$ a $B$-matching substitution for $\langle \beta(x_1), .., \beta(x_n)\rangle$ as a $B$-instance of $\langle \alpha(x_1), .., \alpha(x_n)\rangle$. $\square$

Corollary. Suppose $dom(\alpha) \supseteq dom(\beta)$, then we can choose $\rho = \rho_1$.

The followup lemma both slightly corrects and generalizes a similar lemma in Lecture 5. The proof is left as an exercise.

<u>Lemma</u>. Let $\alpha$ be any (finite substitution) and $Y \supseteq dom(\alpha)$. We can always choose an idempotent substitution $\alpha'$ with $Y = dom(\alpha')$ such that $\alpha \sqsupseteq_{\emptyset} \alpha'$ and $\alpha' \sqsupseteq_{\emptyset} \alpha$.

## 2. Variants of a Term

Let $(\Sigma, B, \vec{E})$ be a decomposition of an equational theory $(\Sigma, E \cup B)$. Note that the initial $E \cup B$-algebra $\mathcal{T}_{\Sigma/E \cup B}$ is <u>isomorphic</u> to the canonical term algebra $\mathcal{C}_{\Sigma/\vec{E},B}$, whose set of elements is:

$$C_{\Sigma/\vec{E},B} = \{ [t!_{\vec{E},B}]_B \mid t \in T_\Sigma \}$$

and where for each $f$ of $n$ arguments in $\Sigma$ we have,

$$f_{\mathcal{C}_{\Sigma/\vec{E},B}}([t_1], \ldots, [t_n]) = [f(t_1, \ldots, t_n)!_{\vec{E},B}]_B$$

Likewise (as the special case of the initial $(\Sigma(X), E \cup B)$-algebra, we have the following isomorphism of free $(\Sigma, E \cup B)$-algebras:

$$\mathcal{T}_{\Sigma/E \cup B}(X) \simeq \mathcal{C}_{\Sigma/\vec{E},B}(X)$$

where $C_{\Sigma/\vec{E},B}(X) = \{ [t!_{\vec{E},B}]_B \mid t \in T_\Sigma(X) \}$

We can think of the elements $[u] \in C_{\Sigma/\vec{E},B}$ as $\vec{E},B$ - normalized patterns, and we can ask the question: what are the pattern instances of $[u]$ modulo $E \cup B$?

The question is of course tricky, since a substitution instance of $u\theta$ may itself not be a $\vec{E},B$-normalized pattern, so its $\vec{E},B$ - normalized pattern instance should be $(u\theta)!_{\vec{E},B}$, which may be syntactically different from $u$.

Example. Consider $E = \{ x+0 = x,\ x+s(y) = s(x+y) \}$, $B = \emptyset$.

Then $N+M \in C_{\Sigma/\vec{E}}$ and the following are possible pattern instances:

$s(0) + M$ (for $\{N \mapsto s(0)\}$)

$N$ (for $\{M \mapsto 0\}$)

$s(N)$ (for $\{M \mapsto s(0)\}$)

$s(s(0) + M')$ (for $\{N \mapsto s(0), M \mapsto s(M')\}$)

... etc.

The followg definition, essentially due to Comon and Delaune, although they gave a somewhat different one, captures the intuition about the notion of "variant". For technical reasons it will not quite be what we want, but it natural and intuitive

Def. Let $(\Sigma, \mathcal{B}, \vec{E})$ be a decomposition of $(\Sigma, E \cup B)$. Then $v$ is a CD-$\vec{E}, B$-variant of $t$ iff there exists a substitution $\theta$ such that

$$v =_B (t\theta)!_{\vec{E},B} .$$

In terms of our notion of $\vec{E}, B$-pattern in $\mathcal{C}_{\Sigma/\vec{E},B}(X)$ what this exactly means is:

$$\begin{cases} 1. & t \text{ determines the } \vec{E}, B\text{-pattern } u[u] = [t!_{\vec{E},B}] \in \mathcal{C}_{\Sigma/\vec{E},B}(X) \\ 2. & [v]_B \text{ is an } \vec{E}, B\text{-pattern instance of } [u], \end{cases}$$

since we have:

$$v =_B (t\theta)!_{\vec{E},B} =_B ((t!_{\vec{E},B})\theta)!_{\vec{E},B} =_B (u\theta)!_{\vec{E},B} .$$

We can also ask two more questions:

<u>Q1</u>: Given $u$ and $u'$ CD-$\vec{E}$, $B$-variants of $t$, when is $u$ <u>more general</u> than $u'$?

<u>A1</u>: When $u \sqsupseteq_B u'$, i.e., $\exists\, \rho \in Match_B(u, u')$ s.t. $u\rho =_B u'$.

say $\{u_1, .., u_n\}$

<u>Q2</u>: Is there a <u>finite</u> number of CD-variants of $t$ that are most general possible, i.e., such that for any CD-variant $v$ of $t$ there is a $u_i$ with $u_i \sqsupseteq_B v$?

<u>A2</u>: In general this does <u>not</u> happen. For example, the terms

$$s(x'+y'),\quad s(s(x''+y'')),\ \ldots,\ s^n(x^{\prime n}+y^{\prime n})$$

are all CD-$\vec{E}$-variants of $x+y$ for $\vec{E}$ the addition equations, but they are <u>incomparable</u> in the $\sqsupseteq_\emptyset$ preorder.

However, this does happen for any term $t$ in an interesting class of decomposition of equational theories, said to satisfy the CD-<u>finite variant property</u>. For a simple example, consider the theory of lists with head and tail:

```
fmod LIST is
  sorts Elt List NeList . subsort NeList < List .
  op _._ : Elt List -> NeList .
  op nil : -> List .
  op head : NeList -> Elt .
  op tail : NeList -> List .
  var X : Elt . var L : List .
  eq head(X.L) = X .
  eq tail(X.L) = L .
endfm
```

This theory has the CD-finite variant property. For example, the term head(L') with L' : NeList has the following two most general variants:

$$\mathrm{head}(L') \qquad X : Elt$$

It turns out that, although quite intuitive, the Comon-Delaune (CD) notion of variant is not expressive enough and leads to some problematic "corner cases" (see the "Variants of Variants" paper cited later). What the notion is technically missing is that given a pattern $[u] \in \mathcal{C}_{\Sigma/\vec{E},B}(X)$, we do not quite know "where u comes from". That is, there could be different substitutions $\theta, \theta'$ (even if both $\theta$ and $\theta'$ are $\vec{E},B$-normalized) such that

$$(t\,\theta)!_{\vec{E},B} =_B u = (t\,\theta')!_{\vec{E},B}$$

This turns out to be important and leads to the following, technically better behaved notion of variant in the Escobar-Sasse-Meseguer Folding Var. Narr. paper:

Definition. Given a decomposition $(\Sigma, B, \vec{E})$ of an equational theory $(\Sigma, E \cup B)$, an $\vec{E},B$-variant of a term $t \in T_\Sigma(X)$ is a pair $(u, \theta)$ such that:

1. $\theta = \theta!_{\vec{E},B}$ ($\theta$ $\vec{E},B$-normalized)
2. $dom(\theta) \subseteq vars(t)$
3. $u =_B (t\,\theta)!_{\vec{E},B}$.

Remark. Condition (1) involves no loss of generality, since if $\alpha$ is not normalized we in any case have $(t\,\alpha)!_{\vec{E},B} =_B (t\,(\alpha!_{\vec{E},B}))!_{\vec{E},B}$, so it is useless to consider $\theta$ not $\vec{E},B$-normalized.

We can now pose again the question: when is one variant *more general* than another? Since now variants have become "*substitution aware*", the notion is slightly tighter:

*Definition*. Let $(u, \theta)$, $(u', \theta')$ be $\vec{E}, B$-variants of $t \in T_\Sigma(X)$. Then $(u, \theta)$ is *more general* than $(u', \theta')$, denoted $(u, \theta) \sqsupseteq_B (u', \theta')$ iff:

1. $\theta \sqsupseteq_B \theta'$, so that $\exists \rho$ with $dom(\rho) \subseteq ran(\theta) \cup (dom(\theta') - dom(\theta))$ s.t.
$$(\theta \rho)|_{dom(\theta) \cup dom(\theta')} =_B \theta'$$

2. $u' =_B u\rho$

*Remarks*. (i) Note that by Exercise in pg. 1, $\rho$ is itself $\vec{E}, B$-normalized. (ii) Note that, by the Lemma in pg. 3, we can assume without loss of generality that $\theta$ is idempotent with $dom(\theta) = vars(t)$. In such a case $dom(\rho) \subseteq ran(\theta)$ and, furthermore, if $B$ has a $B$-matching algorithm we can easily *decide* the relation $(u, \theta) \sqsupseteq_B (u', \theta')$ as follows:

(a) For $\{x_1, \ldots, x_n\} = vars(t)$ we compute the (finite) set

$$Match_B(\langle \theta(x_1), \ldots, \theta(x_n) \rangle, \langle \theta'(x_1), \ldots, \theta'(x_n) \rangle)$$

(b) we test whether there is $B$-matching substitution $\rho$ in such a set such that $u' =_B u\rho$.

Definition. Let $Var_{\vec{E},B}(t)$ be the set of all $\vec{E},B$-variants of $t \in T_\Sigma(X)$. A complete set of variants of $t$ is a subset $\mathcal{C} \subseteq Var_{\vec{E},B}(t)$ such that:

1. without loss of generality we may assume that if $(u, \theta) \in \mathcal{C}$, then $\theta$ is idempotent, with $dom(\theta) = vars(t)$
2. $\forall\ (u', \theta') \in Var_{\vec{E},B}(t)\ \exists\ (u, \theta) \in \mathcal{C}$ such that $(u, \theta) \sqsupseteq_B (u', \theta')$.

We call $\mathcal{C}$ minimal if $(u, \theta), (v, \gamma) \in \mathcal{C}$ with $(u, \theta) \sqsupseteq_B (v, \gamma)$ and $(v, \theta) \sqsupseteq_B (u, \theta)$ implies $(u, \theta) = (v, \gamma)$.

$(\Sigma, B, \vec{E})$ has the finite variant property iff $\forall\ t \in T_\Sigma(X)$ there is a finite complete set of variants of $t$.

This raises an obvious question. Given a term $t \in T_\Sigma(X)$ how can we <u>symbolically compute</u> a complete set of $\vec{E},B$-variants of $t$?

The, essentially obvious answer is: why, of course, by narrowing! More precisely, let $t \overset{\eta}{\underset{\vec{E},B}{\rightsquigarrow}}{}^{+} u$ be an $n$-step $(n \geq 1)$ narrowing sequence $t \overset{\eta_1 \cdots \eta_n}{\underset{\vec{E},B}{\rightsquigarrow}} u$, where $\eta = \eta_1 \cdots \eta_n$ is the "accumulated substitution". We call $u \overset{\eta}{\rightsquigarrow}{}^{+} u$ a <u>variant narrowing sequence</u> iff:

$$\begin{cases} 1. & u =_B u!_{\vec{E},B} \\ 2. & \eta|_{vars(t)} =_B (\eta|_{vars(t)})!_{\vec{E},B} \end{cases}$$

and then denote it thus: $t \overset{\eta\ v}{\underset{\vec{E},B}{\rightsquigarrow}} u$. Note that then we have $(t\eta)!_{\vec{E},B} =_B u$, so that $(u, \eta|_{vars(t)})$ is an $\vec{E},B$-variant of $t$.

<u>Theorem</u>. If $t$ is $\vec{E},B$-reducible, then the set $\{(u, \eta|_{vars(t)}) \mid t \overset{v}{\underset{\vec{E},B}{\rightsquigarrow}} u\}$ is a complete set of $\vec{E},B$-variants of $t$. If $t$ is $\vec{E},B$-irreducible,

Then $\{(u, \eta|_{vars(t)}) \mid t \overset{\eta}{\underset{\vec{E},B}{\rightsquigarrow}} u\} \cup \{(t\rho, \rho)\}$

where $\rho$ is an idempotent variable renaming of vars$(t)$ is a complete set of $\vec{E}, B$-variants of $t$.

**Proof.** We prove the case for $t$ $\vec{E}, B$-reducible and leave the other case as an easy exercise. Let $(u', \theta')$ be a variant of $t$. Then we must have a sequence

$$t\theta' \xrightarrow[\vec{E},B]{+} (t\theta')!_{\vec{E},B} =_B u'$$

and since $\theta'$ is $\vec{E}, B$-irreducible, by the Lifting Theorem we have $t \overset{\eta\,+}{\underset{\vec{E},B}{\rightsquigarrow}} u$ and normalized $\delta$ such that

$(\eta\delta)|_{vars(t)} =_B \theta'$, $\quad t\eta \xrightarrow[\vec{E},B]{+} u$, and $\quad u' =_B u\delta$

But since $u' =_B u'!_{\vec{E},B}$ and $u' =_B u\delta$, we must have $u = u!_{\vec{E},B}$. Furthermore, since $(\eta\delta)|_{vars(t)} = ((\eta|_{vars(t)})\delta)_{vars(t)}$ and $\eta$ is idempotent, we have dom$(\eta|_{vars(t)}) = $ vars$(t)$ and $\eta|_{vars(t)}$ is also idempotent,

But by Exercise in pg. 1, and $\theta'$ $\vec{E}, B$-irreducible, $\eta|_{vars(t)}$ is

$\vec{E},B$-irreducible and we have $t \overset{\eta}{\underset{\vec{E},B}{\leadsto}}_{v} u$ yielding an $\vec{E},B$-variant of $t$ $(u, \eta|_{var(t)})$ such that

$(u, \eta|_{var(t)}) \sqsupseteq_B (u', \theta')$, as desired. $\square$

References


1. H. Comon and S. Delaune, "The finite variant property: how to get rid of some algebraic properties," Springer LNCS 3467, 294-307, 2005.
2. S. Escobar, R. Sasse, J. Meseguer, "Folding variant narrowing and optimal variant termination," J. Logic and Algebraic Programm., 81, 898-928, 2012
3. A. Cholewa, J. Meseguer, S. Escobar, "Variants of Variants and the Finite Variant Property," UIUC CS Dept. Tech Report, Feb. 2014, http://hdl.handle.net/2142/47117, 2014.