1. More on substitutions

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

**Def.** Let $\alpha, \beta \in [x \mapsto T_\Sigma(x)]$ be (finite) substitutions (i.e., $\text{dom}(\alpha)$ and $\text{dom}(\beta)$ are finite sets), and $(\Sigma, B)$ an equational theory. We define

$$\alpha \models_\beta \beta$$

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

$$\left( \alpha \mid_{\text{dom}(\gamma) \cup \text{dom}(\beta)} \right) \gamma \models_\beta \beta \quad (\star)$$

**Exercise.** Prove that we always choose $\gamma$ with $\text{dom}(\gamma) \subseteq \text{ran}(\alpha) \cup (\text{dom}(\beta) - \text{dom}(\alpha))$.

**Hint:** If $\gamma$ satisfies the above condition $(\star)$, then can define $\gamma = \left( \left. \alpha \mid_{\text{ran}(\beta) \cup (\text{dom}(\beta) - \text{dom}(\alpha))} \right| \right) \gamma$. Then prove further that if $(\Sigma, B, R)$ is a rewrite theory and $\beta$ is $R, B$-irreducible, and variables are $R, B$-imed., then both $\alpha$ and the $\gamma$ so chosen are $R, B$-imed.
Q: Is the $\alpha \not\leq^B \beta$ relation decidable?

A: Yes, if we have a $B$-match algorithm.

Lemma. Suppose $(\Sigma, B)$ has a $B$-match algorithm, and let $\text{dom}(\alpha) = \{x_1, \ldots, x_n\}$, then given $\alpha$ and $\beta$ we can choose a $\gamma$ such that $(x \gamma) \mid \text{dom}(\alpha) \cup \text{dom}(\beta) = B \beta$ if

$$\exists \gamma' \in \text{Match}_B \left( \langle \alpha(x_1), \ldots, \alpha(x_n) \rangle, \langle \beta(x_1), \ldots, \beta(x_n) \rangle \right)$$

where $-\ldots-$ is a new tupel operator added to $\Sigma$,

and then $\gamma = \gamma_1 \cup (B \setminus \text{dom}(\beta) \setminus (\text{dom}(\alpha) \cup \text{ran}(\alpha)))$.

If such a $B$-match substitution does not exist, we cannot have a $\gamma$ with $(x \gamma) \mid \text{dom}(\alpha) \cup \text{dom}(\beta) = B \beta$,

since this in particular requires $\forall i: x \gamma \not= B x : \beta$, $1 \leq i \leq n$, making $\gamma$ a $B$-match substitution for $\langle \beta(x_1), \ldots, \beta(x_n) \rangle$ as a $B$-instance of $\langle \alpha(x_1), \ldots, \alpha(x_n) \rangle$. $\square$

Corollary. Suppose $\text{dom}(\alpha) \supseteq \text{dom}(\beta)$, then we can choose $\gamma = \gamma_1$. 
The following lemma both slightly corrects and generalizes a similar lemma in Lecture 5. The proof is left as an exercise.

**Lemma.** Let $\alpha$ be any (finite substitution) and $Y = \text{dom}(\alpha)$. We can always choose an idempotent substitution $\alpha'$ with $Y = \text{dom}(\alpha')$ such that $\alpha \cup \alpha'$ and $\alpha' \models \alpha$.

2. **Variants of a Term**

Let $(\Sigma, B, \bar{E})$ be a decomposition of an equational theory $(\Sigma, \text{EUB})$. Note that the initial $\text{EUB}$-algebra $\mathcal{T}_{\Sigma/\text{EUB}}$ is isomorphic to the canonical term algebra $\mathcal{U}_{\Sigma/\text{EUB}}$, whose set of elements is:

\[ C_{\Sigma/\text{EUB}} = \{ [t: \bar{e}, B]_B \mid t \in T_\Sigma \} \]

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

\[ f_{\Theta_{\Sigma/\text{EUB}}} ([t_1, \ldots, t_n]) = [f(t_1, \ldots, t_n): \bar{e}, B]_B \]

Likewise (as the special case of the initial $(\Sigma(X), \text{EUB})$-algebra), we have the following isomorphism of free $(\Sigma, \text{EUB})$-algebras:

\[ \mathcal{T}_{\Sigma/\text{EUB}}(X) \sim \mathcal{U}_{\Sigma/\text{EUB}}(X) \]
where \( C_{\Sigma/\bar{E}, B} (X) = \{ t! \bar{E}, B \mid t \in T_{\bar{E}} (X) \} \)

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

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

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

Then \( N + M \in C_{\Sigma/\bar{E}} \) and the following possible pattern instances:

\[
\begin{align*}
3(0) + M \quad & (\text{for } \{ N \mapsto 1(0) \}) \\
N \quad & (\text{for } \{ M \mapsto 0 \}) \\
S(N) \quad & (\text{for } \{ M \mapsto s(0) \}) \\
S(N(0) + M') \quad & (\text{for } \{ N \mapsto s(0), M \mapsto s(M') \}) \\
\ldots & \text{etc.}
\end{align*}
\]
The following definition, essentially due to Conway and Delahaye, 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 is natural and intuitive.

**Def.** Let \((\Sigma, \mathcal{B}, \vec{E})\) be a decomposition of \((\Sigma, \Sigma \cup \mathcal{B})\).

Then \(v\) is a \(\mathcal{CD}\)-\(\vec{E}, \mathcal{B}\)-variant of \(t\), iff there exists a substitution \(\theta\) such that

\[
\vec{v}\vec{=}_{\mathcal{B}} (t, \theta)! \vec{E}, \mathcal{B}.
\]

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

\[
\left\{ \begin{array}{l}
1. \ t \text{ determines the } \vec{E}, \mathcal{B}\text{-pattern } \vec{u}\vec{=}_{\mathcal{B}} (t)! \vec{E}, \mathcal{B} \in \mathcal{P}_{\Sigma/\vec{E}, \mathcal{B}}(X) \\
2. \ [\vec{v}]_{\mathcal{B}} \text{ is an } \vec{E}, \mathcal{B}\text{-pattern instance of } [\vec{u}],
\end{array} \right.
\]

since we have:

\[
\vec{v}\vec{=}_{\mathcal{B}} (t, \theta)! \vec{E}, \mathcal{B} = [\vec{u}]_{\mathcal{B}} (\theta)! \vec{E}, \mathcal{B} = [u\theta]_{\mathcal{B}}! \vec{E}, \mathcal{B}.
\]

We can also ask two more questions:
Q1: Given \( u \) and \( u' \) \( CD-E^2, B \)-variants of \( t \), when is \( u \) more general than \( u' \)?

\[ A1: \] When \( u \models B u' \), i.e., \( \exists y \in \text{match}_B(u, u') \)

s.t. \( uy \models B u' \). (say \( u_1, \ldots, u_m \))

Q2: Is there a finite 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 \( u_i \models B v \)?

\[ A2: \] In general this does not happen. For example, the terms

\[ s(x+y), \ s\left(s\left(x+y\right)\right), \ldots, \ s^n\left(x+y\right) \]

are all \( E \)-variants of \( x+y \) for \( E \) the addition equations, but they are incomparable in the \( \models \) preorder.

However, this does happen for any term in an important class of decomposition of equational theories, said to satisfy the \( CD \)-finite variant property. For a simple example, consider the theory of lists with head and tail.
funct LIST is
  sorts Elt List Nelist, subset 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 .
end-fun

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

    head (L')  x : Elt

It turns out that, although quite intuitive, the Couson-Delane (CD) notion of variant is not expressive enough and leads to some problematic "corner cases" (see the "Variants of V"ariant" paper cited later). What the notion is technically missing is that
given a pattern \([u] \in \Sigma/E_{\bar{E}, \bar{B}}(X)\), 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 \(E_{\bar{E}, \bar{B}}\)-normalized) such that

\[(t^\Theta)_{\bar{E}_{\bar{B}}} = u = (t^\Theta')_{\bar{E}_{\bar{B}}}.

This turns out to be important and leads to the following, technically better behaved notion of variant in the Troelstra-Spiece-Meghia Foldy Van. Van. paper:

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

1. \(\Theta = \Theta^!_{\bar{E}_{\bar{B}}} \quad (\Theta \ E_{\bar{E}, \bar{B}}\text{-normalized})\)

2. \(\text{dom}(\Theta) \subseteq \text{ran}(t)\)

3. \[u = (t^\Theta)^!_{\bar{E}_{\bar{B}}}.

**Remark.** Condition (1) involves no loss of generality, since if \(x\) is not normalized we in any case have

\[(t^x)^!_{\bar{E}_{\bar{B}}} = (t^x_{\bar{E}_{\bar{B}}})^!_{\bar{E}_{\bar{B}}} = (t^x)^!_{\bar{E}_{\bar{B}}},\] so it is useless to consider \(\Theta\) not \(E_{\bar{E}, \bar{B}}\)-normalized.
We can now pose another 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 \(E, B\)-variants of \(t \in T_E(x)\). Then \((u, \Theta)\) is more general than \((u', \Theta')\), denoted \((u, \Theta) \sqsupset_B (u', \Theta')\), iff:

1. \(\Theta \sqsubset \Theta'\), so that \(\exists g\) with \(\text{dom}(g) \subseteq \text{ran}(\Theta) \cup (\text{dom}(\Theta') \setminus \text{dom}(\Theta))\) s.t.
   \[
   (\Theta)_g|_{\text{dom}(\Theta) \cup \text{dom}(\Theta')} =_{B} \Theta'
   \]

2. \(u' =_{B} u g\)

**Remarks.** (i) Note that by Exercise in Fig. 1, \(g\) is itself \(E, B\)-normalized. (ii) Note that, by the Lemma in Fig. 3, we can assume without loss of generality that \(\Theta\) is idempotent with \(\text{dom}(\Theta) = \text{vars}(t)\). In such a case \(\text{dom}(g) \subseteq \text{ran}(\Theta)\) but, furthermore, if \(B\) has a \(B\)-matching algorithm we can easily decide the relation \((u, \Theta) \sqsupset_B (u', \Theta')\) as
(a) For all $x_1, \ldots, x_n$, if $\nu = \nu_\emptyset(t)$ we compute the (finite) set

$$\text{Match}_B(\langle \Theta(x_1), \ldots, \Theta(x_n) \rangle, \langle \Theta'(x_1), \ldots, \Theta'(x_n) \rangle)$$

(b) We test whether there is $B$-match substitution in such a set such that $u' = B(u)p$.

**Definition.** Let $\text{Var}_{E, B}(t)$ be the set of all $E, B$-variants of $t \in T_E(X)$.

A complete set of variants of $t$ is a subset $\mathcal{G} \subseteq \text{Var}_{E, B}(t)$ such that:

1. Without loss of generality, we may assume that if $(u, \Theta) \in \mathcal{G}$, then $\Theta$ is idempotent with $\text{dom}(\Theta) = \nu_\emptyset(t)$

2. $\forall (u', \Theta') \in \text{Var}_{E, B}(t)$ $\exists (u, \Theta) \in \mathcal{G}$ such that $(u, \Theta) \cfrac{E}{B} (u', \Theta')$.

We call $\mathcal{G}$ minimal if $(u, \Theta), (v, \Theta) \in \mathcal{G}$ with $(u, \Theta) \cfrac{E}{B} (v, \Theta)$ and $(v, \Theta) \cfrac{E}{B} (u, \Theta)$ implies $(u, \Theta) = (v, \Theta)$.

$(E, B, \overline{E})$ has the finite variant property iff $\forall t \in T_E(X)$ there is a finite complete set of variants of $t$.
This raises an obvious question. Given a term \( t \in \overline{\mathcal{E}}(X) \), how can we symbolically compute a complete set of \( \overline{E}, \overline{B} \)-variants of \( t \)?

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

\[
\begin{align*}
1. \quad & U \in \overline{B} & \overline{E}, \overline{B} \\
2. \quad & (\eta \mid \text{van}(t)) \xrightarrow{\overline{B}} (\eta \mid \text{van}(t)) & \overline{E}, \overline{B}
\end{align*}
\]

and then denote it thus: \( t \xrightarrow{n} u \). Note that then we have \((t\eta)! \overline{E}, \overline{B} = \overline{B} u\), so that \( (U, \eta \mid \text{van}(t)) \) is an \( \overline{E}, \overline{B} \)-variant of \( t \).

\textbf{Theorem.} If \( t \) is \( \overline{E}, \overline{B} \)-reducible, then the set \[\{(U, \eta \mid \text{van}(t)) \mid t \xrightarrow{n} u \} \] is a complete set of \( \overline{E}, \overline{B} \)-variants of \( t \). If \( t \) is \( \overline{E}, \overline{B} \)-irreducible,
Then \[ \{ (u, \eta_{\mathrm{var}(t)}) \mid t \xrightarrow{\eta} u \} \cup \{ (\xi, \delta) \} \]

where \( \delta \) is an idempotent variable renaming of \( \mathrm{var}(t) \)

is a complete set of \( \overrightarrow{\mathcal{E}}_{\beta} \)-variants of \( t \).

Proof. We prove the case for \( \overrightarrow{\mathcal{E}}_{\beta} \)-reducible and

leave the other case as an easy exercise. Let \( (u', \theta') \) be

a variant of \( t \). Then we must have a sequence

\[ t \xrightarrow{\eta'} t' \xrightarrow{\eta} (t')' \xrightarrow{\eta} \overrightarrow{\mathcal{E}}_{\beta} u' \xrightarrow{\theta'} \overrightarrow{\mathcal{E}}_{\beta} u \\ \overrightarrow{\mathcal{E}}_{\beta} u = \overrightarrow{\mathcal{E}}_{\beta} u' \]

and since \( \theta' \) is \( \overrightarrow{\mathcal{E}}_{\beta} \)-irreducible, by the Lifty Theorem

we have \( t \xrightarrow{\eta} u \) and \( \eta \) normalized \( \delta \) such that

\[ (\eta \delta')_{\mathrm{var}(t)} = \overrightarrow{\mathcal{E}}_{\beta} \theta', \quad t \eta \xrightarrow{\eta} \overrightarrow{\mathcal{E}}_{\beta} u, \quad \text{and} \quad \overrightarrow{\mathcal{E}}_{\beta} u = \overrightarrow{\mathcal{E}}_{\beta} u' \]

But since \( \overrightarrow{\mathcal{E}}_{\beta} u = \overrightarrow{\mathcal{E}}_{\beta} u' \), and \( \overrightarrow{\mathcal{E}}_{\beta} u = \overrightarrow{\mathcal{E}}_{\beta} u' \), we must have

\[ u = \overrightarrow{\mathcal{E}}_{\beta} u. \]

Furthermore, since \( (\eta \delta)_{\mathrm{var}(t)} = (\eta \delta')_{\mathrm{var}(t)} \)

and \( \eta \) is idempotent, we have

\[ \mathrm{dom}(\eta_{\mathrm{var}(t)}) = \mathrm{var}(t) \quad \text{and} \quad \eta_{\mathrm{var}(t)} \quad \text{is also idempotent}, \]

But by Exercise in \( \eta \), \( \delta \) and \( \theta' \) \( \overrightarrow{\mathcal{E}}_{\beta} \)-irreducible, \( \eta_{\mathrm{var}(t)} \) is
$E_{1\beta}$-inreducible and we have $t \xrightarrow{\nu} u$ yielding an $E_{1\beta}$-variant of $t (u, \eta |_{\text{var}(t)})$ such that

$$(u, \eta |_{\text{var}(t)}) \rightarrow_B (u', \theta'),$$
as desired. \hfill \Box

References

