Multi-dimensional Secure Service Orchestration[⋆]

Gabriele Costa[1], Fabio Martinelli[2], and Artsiom Yautsiukhin[2]

[1] Dipartimento di Informatica, Sistemistica e Telematica. Universitá di Genova
gabriele.costa@unige.it
[2] Istituto di Informatica e Telematica Consiglio Nazionale delle Ricerche
{fabio.martinelli,artsiom.yautsiukhin}@iit.cnr.it

Abstract. Web services composition allows a software designer for combining atomic services, for instance taken from a marketplace, in a complex business process fulfilling a desired functional goal. Moreover, among a large number of possible compositions, the designer may want to consider only those which satisfy specific non-functional requirements.

In our work we consider verification of security properties and evaluation quantitative security metrics in a single framework. The main focus of this article is the verification of a composition with several security metrics at once. We provide a general solution for the problem and show how such verification can be made more efficient in specific cases (e.g., when a metric is an abstraction of another one). We employ a mathematical structure called c-semirings granting the generality of our approach.

[⋆] This work was partly supported by EU-FP7-ICT NESSoS, EU-FP7-ICT ANIKETOS and EU-FP7-ICT SPaCIoS projects.

1 Proofs

Technical proofs will not be included in the final version of this paper. Instead, a link to an online version of them will be provided by the authors.

1.1 C-Semiring

Since a c-semiring could be of partial order then for some values addition operation is undefined. For presentational reasons we separate the case of defined addition operation, writing $d_1 \oplus^{-1} d_2 = d_1$ or $d_1 \oplus^{-1} d_2 = d_2$, and the case when this operation is undefined, i.e., $d_1 \oplus^{-1} d_2 = glb(d_1, d_2)$. Naturally, the Definition 3 takes into account both cases, but we do the separation to make the proofs clearer.

Property 1. Operation $\oplus^{-1}$ is idempotent.

Proof. We must prove that $d_1 \oplus^{-1} d_1 = d_1$. Let $d_1 = d_2$. Then, $d_1 \oplus d_2 = d_1 = d_2$. Thus, $d_1 \oplus^{-1} d_2 = d_2 = d_1$ □

Property 2. Operation $\oplus^{-1}$ is commutative.

Proof. We must prove that $d_1 \oplus^{-1} d_2 = d_2 \oplus^{-1} d_1$. Let $d_1 \oplus^{-1} d_2 = d_2$, then $d_2 \oplus d_1 = d_1$. Since $\oplus$ is commutative, then $d_2 \oplus d_1 = d_1$. This means that $d_2 \oplus^{-1} d_1 = d_2 = d_1 \oplus^{-1} d_2$. Using the same reasoning we can prove the same property for $d_1 \oplus^{-1} d_2 = d_1$.

In case $d_1 \oplus^{-1} d_2 = glb(d_1, d_2) = glb(d_2, d_1) = d_1 \oplus^{-1} d_2$, because of commutativeness of lower upper bound operation. □

Property 3. $glb(d_1, glb(d_2, d_3)) = glb(glb(d_1, d_2), d_3)$.

Proof. Let $glb(d_2, d_3) = \bar{d}$, $glb(d_1, glb(d_2, d_3)) = \bar{d}'$, $glb(d_1, d_2) = \hat{d}$, and $glb(glb(d_1, d_2), d_3) = \hat{d}'$. Thus, $\bar{d}' \leq_{\mathsf{S}} d_1$, $\bar{d}' \leq_{\mathsf{S}} \bar{d} \leq_{\mathsf{S}} d_3$, $\bar{d}' \leq_{\mathsf{S}} \bar{d} \leq_{\mathsf{S}} d_2$ and $\hat{d}' \leq_{\mathsf{S}} d_3$, $\hat{d}' \leq_{\mathsf{S}} \hat{d} \leq_{\mathsf{S}} d_1$, $\hat{d}' \leq_{\mathsf{S}} \hat{d} \leq_{\mathsf{S}} d_2$.

Assume, that $\bar{d}' <_{\mathsf{S}} \hat{d}'$. This means, that $\bar{d}' <_{\mathsf{S}} \hat{d}' \leq_{\mathsf{S}} d_3$, $\bar{d}' <_{\mathsf{S}} \hat{d}' \leq_{\mathsf{S}} \hat{d} \leq_{\mathsf{S}} d_1$, $\bar{d}' <_{\mathsf{S}} \hat{d}' \leq_{\mathsf{S}} \hat{d} \leq_{\mathsf{S}} d_2$. Thus, we see, that for $glb(d_1, glb(d_2, d_3)) = \bar{d}'$ there is $\hat{d}'$, which is less that d_1 and $\bar{d}$ ($\hat{d}'$ is less than each of arguments of $glb(d_2, d_3)$). This is impossible by the definition of glb. The same reasoning can be applied to the opposite assumption: $\hat{d}' <_{\mathsf{S}} \bar{d}'$. Thus $glb(d_1, glb(d_2, d_3)) = glb(glb(d_1, d_2), d_3)$. □

Property 4. Operation $\oplus^{-1}$ is associative.

Proof. This property follows from Property 3, since $(d_1 \oplus^{-1} d_2) \oplus^{-1} d_3 = glb(glb(d_1, d_2), d_3)$ and $d_1 \oplus^{-1} (d_2 \oplus^{-1} d_3) = glb(glb(d_1, d_2), d_3)$ □

Property 5. Operation $\oplus^{-1}$ is monotone.

Proof. Monotone. We must prove that if $d_1 \leq_{\mathtt{S}} d_2$ then $\forall d_3\ d_1 \oplus^{-1} d_3 \leq_{\mathtt{S}} d_2 \oplus^{-1} d_3$. Since $d_1 \leq_{\mathtt{S}} d_2$ then $d_1 \oplus^{-1} d_2 = d_1$ and $d_1 \oplus^{-1} d_2 \oplus^{-1} d_3 = d_1 \oplus^{-1} d_3$. By idempotence of $\oplus^{-1}$: $d_1 \oplus^{-1} d_3 = d_1 \oplus^{-1} d_2 \oplus^{-1} d_3 = d_1 \oplus^{-1} d_2 \oplus^{-1} d_3 \oplus^{-1} d_3 = (d_1 \oplus^{-1} d_3) \oplus^{-1} (d_2 \oplus^{-1} d_3)$ (since $\oplus^{-1}$ is commutative and associative operator). The last part implies that $d_1 \oplus^{-1} d_3 \leq_{\mathtt{S}} d_2 \oplus^{-1} d_3$. □

Property 6. Operation $\oplus^{-1}$ is distributive over $\otimes$.

Proof. We must prove that $d_1 \otimes (d_2 \oplus^{-1} d_3) = (d_1 \otimes d_2) \oplus^{-1} (d_1 \otimes d_3)$. Let $d_2 \leq_{\mathtt{S}} d_3$. This means that $d_2 \oplus^{-1} d_3 = d_2$ and $d_2 \oplus d_3 = d_3$. From distribution property of summation we know that $(d_1 \otimes d_2) \oplus (d_1 \otimes d_3) = d_1 \otimes (d_2 \oplus d_3) = d_1 \otimes d_3$. This means that $(d_1 \otimes d_2) \oplus^{-1} (d_1 \otimes d_3) = d_1 \otimes d_2 = d_1 \otimes (d_2 \oplus^{-1} d_3)$. Using the same reasoning we can prove the same property for $d_3 \leq_{\mathtt{S}} d_2$.

The last case left for considering is when $d_2 \oplus^{-1} d_3 = glb(d_2, d_3) = d$. Consider $d_1 \otimes glb(d_2, d_3) = d_1 \otimes d$ first. $d \leq_{\mathtt{S}} d_2$ and $d \leq_{\mathtt{S}} d_3$ by the definition of glb. By monotonicity of $\otimes$: $d_1 \otimes d \leq_{\mathtt{S}} d_1 \otimes d_2$ and $d_1 \otimes d \leq_{\mathtt{S}} d_1 \otimes d_3$.Now, consider $(d_1 \otimes d_2) \oplus^{-1} (d_1 \otimes d_3) = glb((d_1 \otimes d_2), (d_1 \otimes d_3)) = d'$. $d' \leq_{\mathtt{S}} d_1 \otimes d_2$ and $d' \leq_{\mathtt{S}} d_1 \otimes d_3$. Let $d_1 \otimes d <_{\mathtt{S}} d'$, then exists an element d', such that $d' \leq_{\mathtt{S}} d_1 \otimes d_2$ and $d' \leq_{\mathtt{S}} d_1 \otimes d_3$ and $d <_{\mathtt{S}} d'$. This violates the definition of glb in the first case. A similar reasoning can be applied to the case $d' <_{\mathtt{S}} d_1 \otimes d$. Thus $d_1 \otimes d = d'$ □

1.2 Safety

Lemma 1. *Let $\Gamma, H \vdash e : \tau$ and $\eta, d, e \rightarrow_\pi \eta', d', e'$. If $\Gamma, H' \vdash e' : \tau$ then $\forall \delta . \eta' [\![H']\!]^\delta \subseteq \eta [\![H]\!]^\delta$*

Proof. By induction on the depth of $\Gamma, H \vdash_g e : \tau$.

- Case (`T−Unit`), (`T−Res`) and (`T−Var`). Trivial.
- Case (`T−Ev`). We have two further cases
  a) $\eta, d, \alpha(\bar{e}) \rightarrow_\pi \eta', d', \alpha(\bar{e}')$, then we instantiate the hypothesis to

$$\frac{\Gamma, H \vdash_g \bar{e} : \mathcal{R}}{\Gamma, H \cdot \sum_{\mathcal{R}} F(\alpha, r) \# \alpha(r) \vdash_g \alpha(\bar{e}) : \mathbf{1}}$$

and

$$\frac{\eta, d, \bar{e} \rightarrow_\pi \eta', d', \bar{e}'}{\eta, d, \alpha(\bar{e}) \rightarrow_\pi \eta', d', \alpha(\bar{e}')}$$

Assuming the premises of the two rules and applying the inductive hypothesis we infer that $\Gamma, \bar{H}' \vdash_{\bar{g}'} \bar{e}' : \mathcal{R}$ implies that $\forall \delta . \eta' [\![\bar{H}']\!]^\delta \subseteq \eta [\![H]\!]^\delta$ Applying the typing rule for events we have

$$\frac{\Gamma, \bar{H}' \vdash_{\bar{g}'} \bar{e}' : \mathcal{R}}{\Gamma, \bar{H}' \cdot \sum_{\mathcal{R}} F(\alpha, r) \# \alpha(r) \vdash_{\bar{g}'} \bar{e}' : \mathcal{R}}$$

Then $\forall \delta . \eta' [\![\bar{H}']\!]^\delta [\![\sum_{\mathcal{R}} F(\alpha, r) \# \alpha(r)]\!]^\delta \subseteq \eta [\![H]\!]^\delta [\![\sum_{\mathcal{R}} F(\alpha, r) \# \alpha(r)]\!]^\delta$.

b) $\eta, d, \alpha(r) \rightarrow_\pi \eta\alpha(r), d \otimes F(\alpha, r), *$. We assume the premise

$$\frac{\Gamma, \varepsilon \vdash_g r : \mathcal{R}}{\Gamma, \sum_{\mathcal{R}} F(\alpha, r)\#\alpha(r) \vdash_g \alpha(r) : \mathbf{1}}$$

and we simply note that $\forall\delta.\eta\alpha(r)\llbracket\varepsilon\rrbracket^\delta \subseteq \eta\llbracket\sum_{\mathcal{R}} F(\alpha, r)\#\alpha(r)\rrbracket^\delta$.

- Case ($\mathtt{T{-}If}$). We have two symmetric cases (depending on $\mathcal{B}(b)$). Instantiating the rule we obtain

$$\frac{\Gamma, H \vdash e_{tt} : \tau \quad \Gamma, H \vdash e_{\mathit{ff}} : \tau}{\Gamma, H \vdash_g \mathtt{if}\, b\, \mathtt{then}\, e_{tt}\, \mathtt{else}\, e_{\mathit{ff}} : \tau}$$

and

$$\eta, d, \mathtt{if}\, b\, \mathtt{then}\, e_{tt}\, \mathtt{else}\, e_{\mathit{ff}} \rightarrow_\pi \eta, d, e_{\mathcal{B}(b)}$$

By inductive hypothesis we have that $\forall\delta$ the property holds on both e_{tt} and e_{ff}, which suffices to conclude.

- Cases ($\mathtt{T{-}Abs}$) and ($\mathtt{T{-}Req}$). Premises are false, then the property holds.
- Case ($\mathtt{T{-}Frm}$). Instantiating the premises we have

$$\frac{\Gamma, \bar{H} \vdash_g \bar{e} : \tau}{\Gamma, \varphi\big[\bar{H}\big] \vdash_g \varphi[\bar{e}] : \tau}$$

and

$$\frac{\eta, d, \bar{e} \rightarrow_\pi \eta', d', \bar{e}' \quad \eta' \models \varphi}{\eta, d, \varphi[\bar{e}] \rightarrow_\pi \eta', d', \varphi[\bar{e}']}$$

Then, applying the inductive hypothesis we obtain that $\Gamma, \bar{H}' \vdash_{\bar{g}'} \bar{e}' : \tau$ implies that $\forall\delta.\eta'\llbracket\bar{H}'\rrbracket^\delta \subseteq \eta\llbracket\bar{H}\rrbracket^\delta$. Here we must prove that $\forall\delta.\eta'\llbracket\varphi\big[\bar{H}'\big]\rrbracket^\delta \subseteq \eta\llbracket\varphi\big[\bar{H}\big]\rrbracket^\delta$. To do that, we make explicit the two sets

$$A = \eta'\llbracket\varphi\big[\bar{H}'\big]\rrbracket^\delta = \{\eta'\bar{\eta}' \mid \eta'\bar{\eta}' \models \varphi \wedge \exists\hat{\eta}' \in \llbracket\bar{H}'\rrbracket^\delta.\bar{\eta}' \leqslant \hat{\eta}'\}$$

$$B = \eta\llbracket\varphi\big[\bar{H}\big]\rrbracket^\delta = \{\eta\bar{\eta} \mid \eta\bar{\eta} \models \varphi \wedge \exists\hat{\eta} \in \llbracket\bar{H}\rrbracket^\delta.\bar{\eta} \leqslant \hat{\eta}\}$$

and we prove that $\dot{\eta} \in A \Rightarrow \dot{\eta} \in B$. From the definition of A we know that $\dot{\eta} = \eta'\bar{\eta}'$. Then, there must be $\hat{\eta}' \in \llbracket\bar{H}'\rrbracket^\delta$ extending $\bar{\eta}'$. By inductive hypothesis $\eta'\hat{\eta}' \in \eta'\llbracket\bar{H}'\rrbracket^\delta$ implies that $\eta'\hat{\eta}' \in \eta\llbracket\bar{H}\rrbracket^\delta$. As $\eta' = \eta\mathring{\eta}$ for some $\mathring{\eta}$ (execution can only extend traces), $\mathring{\eta}\hat{\eta}' \in \llbracket\bar{H}\rrbracket^\delta$. Since $\mathring{\eta}\bar{\eta}'$ complies with φ and it is a sub-trace of a history $(\mathring{\eta}\hat{\eta}')$ in $\llbracket\bar{H}\rrbracket^\delta$ there must be $\eta\mathring{\eta}\bar{\eta}' \in B$. The thesis follows from $\eta\mathring{\eta}\bar{\eta}' = \eta'\bar{\eta}' = \dot{\eta}$.

- Case ($\mathtt{T{-}Met}$). We follow the same reasoning of the previous case.
- Case ($\mathtt{T{-}App}$). Let $e = e_1e_2$. We have

$$\frac{\Gamma, H_0 \vdash_g e_1 : \tau \xrightarrow{H_2} \tau' \quad \Gamma, H_1 \vdash_g e_2 : \tau}{\Gamma, (H_0 \mid H_1) \cdot H_2 \vdash_g e_1e_2 : \tau'}$$

We must verify three possible subcases depending on the rule used to derive $\langle \eta, d, e_1e_2 \rangle$.

- If ($\texttt{S}-\texttt{App}_1$) is used, then

$$\frac{\eta, d, e_1 \rightarrow_\pi \eta', d', e_1'}{\eta, d', e_1 e_2 \rightarrow_\pi \eta', d', e_1' e_2}$$

  Applying the inductive hypothesis to e_1 we infer that the property holds on $\Gamma, \bar{H} \vdash_{\bar{g}} e_1' : \tau \xrightarrow{H_2} \tau'$. Then, we apply (T-App) and we have

$$\frac{\Gamma, \bar{H} \vdash_{\bar{g}} e_1' : \tau \xrightarrow{H_2} \tau' \quad \Gamma, H_1 \vdash_{\bar{g}} e_2 : \tau}{\Gamma, (\bar{H} \mid H_1) \cdot H_2 \vdash_{\bar{g}} e_1' e_2 : \tau'}$$

  Since $H \sqsubseteq H' \Rightarrow (H \mid \bar{H}) \sqsubseteq (H' \mid barH)$ we know that $\eta' \llbracket (\bar{H} \mid H_1) \cdot H_2 \rrbracket^\delta \subseteq \eta \llbracket (H \mid H_1) \cdot H_2 \rrbracket^\delta$ from which the thesis follows.
- If ($\texttt{S}-\texttt{App}_2$) is used, then we have the symmetrical conditions of the previous case and we can conclude in the same way.
- If ($\texttt{S}-\texttt{App}_3$) is used, then $e = (\lambda_z x.\bar{e})v$ and

$$\eta, d, (\lambda_z x.\bar{e})v \rightarrow_\pi \eta, d, \bar{e}\{v/x, \lambda_z x.\bar{e}/z\}$$

  Also we know that $H_0 = H_1 = \varepsilon$, then we just need to show that $\Gamma, H_2' \vdash \bar{e}\{v/x, \lambda_z x.\bar{e}/z\} : \tau'$ with $H_2' \sqsubseteq H_2$. We obtain it by proving the stronger property that $\forall e.\Gamma; x : \tau', H \vdash_g e : \tau$ and $\Gamma, \varepsilon \vdash_g v : \tau'$ imply that $\Gamma, H \vdash_g e\{v/x\} : \tau$. If x is not free in e the property is trivially satisfied. For all other cases we proceed by induction on e finding that all of them are straightforward ($e = x$) or a direct implication of the inductive hypothesis.
- If ($\texttt{S}-\texttt{Req}$) is used, we have

$$\frac{e_{\bar{\ell}} : \tau \xrightarrow{H^*} \tau' \in \texttt{Srv} \qquad \pi(\rho) = \bar{\ell}}{\eta, (\texttt{req}_\rho\, \tau \rightarrow \tau')v \rightarrow_\pi \eta, e_{\bar{\ell}} v}$$

  By ($\texttt{T}-\texttt{Req}$) follows that

$$\frac{I = \{H \mid e_\ell : \tau \xrightarrow{H} \tau' \in \texttt{Srv}\}}{\Gamma, \varepsilon \vdash_g \texttt{req}_\rho\, \tau \rightarrow \tau' : \tau \xrightarrow{\sum_{H \in I} H} \tau'}$$

  By definition $H^* \in I$, then we reach the stronger property that $\forall \delta.\eta \llbracket \bar{H} \rrbracket^\delta \subseteq \eta \llbracket H^* \rrbracket^\delta \subseteq \eta \llbracket H^* + \hat{H} \rrbracket^\delta$.

– Case ($\texttt{T}-\texttt{Wkn}$). By the inductive hypothesis we know that the property holds on $\Gamma, \bar{H} \vdash_g e' : \tau$. Since $H \sqsubseteq H'$ then $\forall \delta.\eta' \llbracket \bar{H} \rrbracket^\delta \subseteq \eta \llbracket H \rrbracket^\delta \subseteq \eta \llbracket H' \rrbracket^\delta$.

□

Lemma 2. *Let $x \in fv(e)$ then for all Γ, e', τ, τ'*

$$\Gamma[\tau'/x], H \vdash e : \tau \wedge \Gamma, H' \vdash e' : \tau' \Longrightarrow \Gamma, H'' \vdash e\{e'/x\} : \tau$$

for some H, H' and H''.

Proof. By induction over e we have

- $e = *$, $e = r$, $e = \texttt{req}_\rho\, \tau_1 \to \tau_2$. Trivial.
- $e = x$. Here $e\{e'/x\} = e'$ and the property is trivially satisfied because $\tau = \tau'$.
- All the other cases are satisfied by the inductive hypothesis (just note that for conditional we also need to apply the weakening rule).

□

Lemma 3. *If $\Gamma, H \vdash_g e : \tau$ and $\eta, d, e \rightsquigarrow_\pi \eta', d', e'$ then $\exists H'$ such that $\Gamma, H' \vdash_g e' : \tau$*

Proof. We prove this lemma in two steps. We first prove that (1) the property holds for one step reductions and then (2) we prove it on arbitrary long reductions.

1. If $\Gamma, H \vdash_g e : \tau$ and $\eta, d, e \to_\pi \eta', d', e'$ then $\exists H'$ such that $\Gamma, H' \vdash_g e' : \tau$. By induction over e.
   - $e = *$, $e = r$, $e = x$, $e = \lambda_z x.e'$, $e = \texttt{req}_\rho\, \tau_1 \to \tau_2$. Trivial.
   - $e = \alpha(e')$. By ($\texttt{T}{-}\texttt{Ev}$) we have

$$\frac{\Gamma, H \vdash e' : \mathcal{R}}{\Gamma, H \cdot \sum_{r \in \mathcal{R}} (F(\alpha, r) \# \alpha(r)) \vdash \alpha(e) : \mathbf{1}}$$

Hence e can make a transition either according to ($\texttt{S}{-}\texttt{Ev}_1$) or ($\texttt{S}{-}\texttt{Ev}_2$). In the first case we have

$$\frac{\eta, d, e' \to_\pi \eta', d', e''}{\eta, d, \alpha(e') \to_\pi \eta', d', \alpha(e'')}$$

Applying the inductive hypothesis to e'' we know that there exists H'' s.t. $\Gamma, H'' \vdash e'' : R$ hence we conclude by applying ($\texttt{T}{-}\texttt{Ev}$). Instead, in the second case, we obtain

$$\frac{F(\alpha, r) = d'}{\eta, d, \alpha(r) \to_\pi \eta\alpha(r), d \otimes d', *}$$

and the property is trivially satisfied with $\Gamma, \varepsilon \vdash * : \mathbf{1}$.

   - $e = \texttt{if}\, b\, \texttt{then}\, e_{tt}\, \texttt{else}\, e_{ff}$. Here we have two symmetric cases depending on the evaluation of b. By the inductive hypothesis the property holds on both e_{tt} and e_{ff}. However, for ($\texttt{S}{-}\texttt{If}$), e reduces to either e_{tt} or e_{ff}, which suffices to conclude.
   - $e = e_1\, e_2$. By ($\texttt{T}{-}\texttt{App}$) here we have

$$\frac{\Gamma, H_1 \vdash e_1 : \tau_2 \xrightarrow{H_3} \tau \quad \Gamma, H_2 \vdash e_2 : \tau_2}{\Gamma, (H_1 \mid H_2) \cdot H_3 \vdash e_1\, e_2 : \tau}$$

In this case there are three possible rules: ($\mathtt{S}{-}\mathtt{App}_1$), ($\mathtt{S}{-}\mathtt{App}_2$) or ($\mathtt{S}{-}\mathtt{App}_3$). The first two are similar and we solve them at once. Indeed, we just need to apply the inductive hypothesis to the right hand side expression e'_1 (e'_2, respectively) and we can use the typing rule ($\mathtt{T}{-}\mathtt{App}$) to conclude. In the third case we have $e_1 = \lambda_z x.e'$ and $e_2 = v$, then we instantiate ($\mathtt{S}{-}\mathtt{App}_3$) to

$$\eta, d, (\lambda_z x.e')v \to_\pi \eta, d, e'\{v/x, \lambda_z x.e'/z\}$$

We can conclude by applying lemma 2 to e'.

   - $e = \varphi[e']$, $e = \gamma\langle e' \rangle$. Trivially by applying the inductive hypothesis to e'

2. By induction on the length of the derivations. The base case is satisfied by the property at point (1). Then, the inductive step, simply consists of applying (1) to the inductive hypothesis.

□

Lemma 4. *If $\Gamma, H \vdash_{g'} e : \tau$ then there exists $\bar{H}$ such that $\Gamma, \bar{H} \vdash_{g'} e : \tau$ and $\forall H''.\Gamma, H'' \vdash_{g'} e : \tau \Rightarrow \bar{H} \sqsubseteq H''$.*

Proof. By induction on the depth of $\Gamma, H \vdash_g e : \tau$.

- Case ($\mathtt{T}{-}\mathtt{Unit}$), ($\mathtt{T}{-}\mathtt{Res}$), ($\mathtt{T}{-}\mathtt{Var}$), ($\mathtt{T}{-}\mathtt{Abs}$) and ($\mathtt{T}{-}\mathtt{Req}$). Trivially $\bar{H} = \varepsilon$.
- Case ($\mathtt{T}{-}\mathtt{Wkn}$). Trivial, by the inductive hypothesis.
- Case ($\mathtt{T}{-}\mathtt{Ev}$). We have

$$\frac{\Gamma, H \vdash_g \bar{e} : \mathcal{R}}{\Gamma, H \cdot \sum_{\mathcal{R}} F(\alpha, r)\#\alpha(r) \vdash_g \alpha(\bar{e}) : \mathbf{1}}$$

By applying the inductive hypothesis to $\bar{e}$, we find $\bar{H}_e$. Hence, we just need to notice that $\bar{H}_e \cdot \sum_{\mathcal{R}} F(\alpha, r)\#\alpha(r)$ is the minimal history expression typing e (the summation factor cannot be modified/removed by any other rule).

- Case ($\mathtt{T}{-}\mathtt{If}$). We have

$$\frac{\Gamma, H \vdash e_{tt} : \tau \quad \Gamma, H \vdash e_{\mathit{ff}} : \tau}{\Gamma, H \vdash_g \mathtt{if}\, b\, \mathtt{then}\, e_{tt}\, \mathtt{else}\, e_{\mathit{ff}} : \tau}$$

By inductive hypothesis, there exist $\bar{H}_{tt}$ and $\bar{H}_{\mathit{ff}}$. We show by contradiction that $\bar{H} = \bar{H}_{tt} + \bar{H}_{\mathit{ff}}$. Assume there exists $\bar{H}' \sqsubseteq \bar{H}$ such that $\Gamma, \bar{H}' \vdash_g \mathtt{if}\, b\, \mathtt{then}\, e_{tt}\, \mathtt{else}\, e_{\mathit{ff}} : \tau$. By ($\mathtt{T}{-}\mathtt{If}$), we have that $\bar{H}_{tt} \sqsubseteq \bar{H}'$ and $\bar{H}_{\mathit{ff}} \sqsubseteq \bar{H}'$. However, this implies that $\bar{H} \sqsubseteq \bar{H}'\bar{H}$ which suffices to conclude.

- Cases ($\mathtt{T}{-}\mathtt{Frm}$) and ($\mathtt{T}{-}\mathtt{Met}$). Direct consequence of the inductive hypothesis.
- Case ($\mathtt{T}{-}\mathtt{App}$). We have

$$\frac{\Gamma, H_0 \vdash_g e_1 : \tau \xrightarrow{H_2} \tau' \quad \Gamma, H_1 \vdash_g e_2 : \tau}{\Gamma, (H_0 \mid H_1) \cdot H_2 \vdash_g e_1 e_2 : \tau'}$$

Applying the inductive hypothesis we find $\bar{H}_0, \bar{H}_1$ and $\bar{H}_2$ and we show that $\bar{H} = (\bar{H}_0 \mid \bar{H}_1) \cdot \bar{H}_2$. By contradiction, let assume that there exists $\bar{H}' \sqsubseteq \bar{H}$. By rule, (`T−App`) we have that $\bar{H}' = (H_0' \mid H_1') \cdot H_2'$ such that $\bar{H}_i \sqsubseteq H_i'$ (with $i \in \{0, 1, 2\}$). However, this implies $\bar{H} = (\bar{H}_0 \mid \bar{H}_1) \cdot \bar{H}_2 \sqsubseteq (H_0' \mid H_1') \cdot H_2' = \bar{H}' \sqsubseteq \bar{H}$.

□

Lemma 5. ***(Subject reduction)*** *Let $\Gamma, H \vdash_g e : \tau$ and $\eta, d, e \rightsquigarrow_\pi \eta', d', e'$. If $\Gamma, H' \vdash_{g'} e' : \tau$ and $\forall H''.\Gamma, H'' \vdash_{g'} e' : \tau \Rightarrow H' \sqsubseteq H''$ (i.e., H' is the minimal history expression typing e') then $\forall \delta.\eta'[\![H']\!]^\delta \subseteq \eta[\![H]\!]^\delta$.*

Proof. Then, we proceed by induction on the length of the derivations.

- Base case. In this case $e = e'$ and $\eta = \eta'$. By lemma 4, there exists $\bar{H}$ which satisfies the property.
- Inductive step. Here we have $\eta, d, e \rightsquigarrow_\pi \eta', d', e' \rightarrow_\pi \langle \eta'', d'', e'' \rangle$. We apply the inductive hypothesis to the first part of the derivation. Then we need to apply lemma 1 to $\eta', d', e' \rightarrow_\pi \eta'', d'', e''$. For doing that, we have to be sure that there exists H'' such that $\Gamma, H'' \vdash_g e'' : \tau$, which is guaranteed by lemma 3. We conclude by applying lemma 4 to H'' and we find $\bar{H}''$ minimal.

□

Theorem 1. *If $\Gamma, H \vdash_{true} e : \tau$ and $\langle \varepsilon, d, e \rangle \rightarrow_\pi^* \langle \eta, d', v \rangle$ then $\forall \delta.\eta \in [\![H]\!]^\delta$.*

Proof. Theorem 1 is just a corollary of lemma 5 in the particular case in which $e' = v$, $\eta' = \varepsilon$ and $H' = \varepsilon$. □

Property 7. For all history expressions H and H' if $H \equiv H'$ then $\forall \delta.[\![H]\!]^\delta = [\![H']\!]^\delta$

Proof. We proceed by induction on the equational rules. Most cases are trivially implied by the history expressions semantics defined in Table **??**. Here we just show the cases requiring some more explanations.

- Case $d_1\#H_1 \cdot d_2\#H_2 \equiv d_1 \otimes d_2\#(H_1 \cdot H_2)$. By inductive hypothesis and semantics of annotated history expressions we have
$$[\![d_1\#H_1 \cdot d_2\#H_2]\!]^\delta = [\![H_1 \cdot H_2]\!]^\delta = [\![d_1 \otimes d_2\#(H_1 \cdot H_2)]\!]^\delta$$
- Case $d_1\#H_1 + d_2\#H_2 \equiv d_1 \oplus^{-1} d_2\#(H_1 + H_2)$. Following the same reasoning of the previous case
$$[\![d_1\#H_1 + d_2\#H_2]\!]^\delta = [\![H_1 + H_2]\!]^\delta$$
$$= [\![d_1 \otimes^{-1} d_2\#(H_1 + H_2)]\!]^\delta$$
- Case $d_1\#H_1 \mid d_2\#H_2 \equiv d_1 \otimes d_2\#(H_1 \mid H_2)$. Again, we show that
$$[\![d_1\#H_1 \mid d_2\#H_2]\!]^\delta = [\![H_1 \mid H_2]\!]^\delta = [\![d_1 \oplus d_2\#(H_1 \mid H_2)]\!]^\delta$$

$$H \equiv \mathbf{1}\#H \quad \bar{d}_1\#\bar{d}_2\#H \equiv \bar{d}_2\#\bar{d}_1\#H \equiv \bar{d}_1 \otimes \bar{d}_2\#H$$

$$\bar{d}_1\#H_1 \cdot \bar{d}_2\#H_2 \equiv \bar{d}_1 \otimes \bar{d}_2\#(H_1 \cdot H_2) \quad \varphi\left[\bar{d}\#H\right] \equiv \bar{d}\#\varphi[H]$$

$$\bar{d}_1\#H_1 + \bar{d}_2\#H_2 \equiv \bar{d}_1 \oplus^{-1} \bar{d}_2\#(H_1 + H_2) \quad \bar{d}_1\#H_1 \mid \bar{d}_2\#H_2 \equiv \bar{d}_1 \otimes \bar{d}_2\#(H_1 \mid H_2)$$

$$\gamma\left\langle \bar{d}\#H \right\rangle \equiv \bar{\bar{d}}\#\gamma\left\langle H \right\rangle \quad \text{where } \gamma = T \geq_T \bar{d}' \text{ and } \bar{\bar{d}} = \bar{d} \oplus^{-1} \bar{d}'$$

$$\mu h.H \equiv \bar{\bar{d}}\#\mu h.H' \quad \text{where } \bar{\bar{d}} = \bigoplus_n{}^{-1} \Phi^n(\mathbf{0}) \text{ and } \Phi(\bar{d}) = \bar{d}' \Leftrightarrow \begin{cases} H[\bar{d}\#h/h] \equiv \bar{d}'\#H' \\ \qquad\quad \wedge \\ \bar{d}'\#H' \text{ is in MNF} \end{cases}$$

Table 1. Equational rules.

- Case $\mu h.H \equiv \bar{d}\#\mu h.H'$. Here we must prove that $\llbracket \mu h.H \rrbracket^\delta \equiv \llbracket \mu h.H' \rrbracket^\delta$. From the inductive hypothesis and $\llbracket d\#h \rrbracket^\delta = \llbracket h \rrbracket^\delta$, we infer that $\llbracket H \rrbracket^\delta = \llbracket H[d\#h/h] \rrbracket^\delta = \llbracket d'\#H' \rrbracket^\delta = \llbracket H' \rrbracket^\delta$ which suffices to conclude.

□

In Table 1 we report the equational rules given in [1].

Property 8. For each history expression H there exists H' such that $H \equiv H'$ and H' is in metric normal form.

Proof. We proceed by induction over H.

- Cases ε, h and $\alpha(r)$. Trivial.
- Case $H_1 \cdot H_2$. We apply the inductive hypothesis and we find the MNFs $d_1\#H_1'$ and $d_2\#H_2'$. By the rules of Table 1, $d_1 \otimes d_2\#H_1' \cdot H_2' \equiv d_1\#H_1' \cdot d_2\#H_2'$ is a MNF for H.
- Cases $H_1 + H_2$ and $H_1 \mid H_2$. We follow a reasoning analogous to the previous case.
- Case $d\#H$. By the inductive hypothesis we know there exists a MNF $d'\#H'$ for H. We conclude by noticing that $d \otimes d'\#H'$ is a MNF for $d\#H$.
- Case $\varphi[H]$. A direct consequence of the inductive hypothesis.
- Case $\gamma\left\langle H \right\rangle$. A consequence of the inductive hypothesis and the equivalence rule for metric checks.
- Case $\mu h.H$. By inductive hypothesis H has a corresponding MNF $d'\#H'$. Then, we apply the equivalence rule and we find $\mu h.H \equiv \bar{d}\#\mu h.H'$ (for some $\bar{d}$) which is in MNF.

□

Theorem 2. *If $\Gamma, H \vdash e : \tau$ and $H \equiv \bar{d}\#H'$ such that $\bar{d}\#H'$ is in MNF, then for each execution $\eta, d, e \rightsquigarrow_\pi \eta', d', e'$ holds that $d' \leq_S d \otimes \bar{d}$.*

Proof. We first prove that the property holds for single-step computations (by induction on e) and then we prove the theorem by induction on the length of the computations.

- Cases $*$, r and x. Trivial.
- Case $\alpha(e)$. Here we have two possibilities. If $(\mathtt{S}{-}\mathtt{Ev}_1)$ applies, the property is guaranteed by the inductive hypothesis. Instead, if $(\mathtt{S}{-}\mathtt{Ev}_2)$ is used then $e = r$ and we have that $d' = d \otimes F(\alpha, r)$. However, the MNF of the history expression returned by the type system is $\bigoplus_r^{-1} F(\alpha, r)\#\cdots$ which trivially satisfies the property.
- Case if b then e else e'. Here the computation reduces to one between e and e'. However, the MNF for it is always annotated with $d_1 \oplus^{-1} d_2$, which respectively annotate the MNFs for e and e', and the property holds.
- Cases $\lambda_z x.e$ and $\mathtt{req}_\rho\, \tau \to \tau'$. Hypothesis does not apply.
- Case $e\,e'$. Here the MNF is $d_1 \otimes d_2 \otimes d_3$, which annotate the MNF for e, e' and the latent effect of e, respectively. Independently of the rule we apply, i.e., $(\mathtt{S}{-}\mathtt{App}_1)$, $(\mathtt{S}{-}\mathtt{App}_2)$ or $(\mathtt{S}{-}\mathtt{App}_3)$, we always reduce to the inductive hypothesis.
- Case $\varphi[e']$. By inductive hypothesis.
- Case $\gamma\,\langle e' \rangle$. Assuming $\gamma = T \leq_S \dot{d}$, by hypothesis, the term allows one computation steps, that is, it does not violate γ. Hence, $d' \leq \dot{d} \oplus^{-1} d$ which labels the MNF for the history expression of e.

We complete by induction on the derivation length.

- Base case (zero-step computations). Trivially $d' = d$.
- Induction. We have

  $$\eta, d, e \rightsquigarrow_\pi \eta', d', e' \to_\pi \langle \eta'', d'', e'' \rangle$$

  By the inductive hypothesis we know that $d' \leq_S d \otimes \bar{d}$ and we proceed by co-induction on the rules of the operational semantics.
  - Cases $(\mathtt{S}{-}\mathtt{If})$, $(\mathtt{S}{-}\mathtt{App}_3)$, $(\mathtt{S}{-}\mathtt{Sec}_2)$, $(\mathtt{S}{-}\mathtt{Met}_2)$ and $(\mathtt{S}{-}\mathtt{Req})$. Trivial as $d'' = d'$.
  - Cases $(\mathtt{S}{-}\mathtt{Ev}_1)$, $(\mathtt{S}{-}\mathtt{App}_1)$, $(\mathtt{S}{-}\mathtt{App}_2)$, $(\mathtt{S}{-}\mathtt{Sec}_1)$ and $(\mathtt{S}{-}\mathtt{Met}_1)$. Trivially reduce to the inductive hypothesis.
  - Case $(\mathtt{S}{-}\mathtt{Ev}_2)$. Here $d'' = d' \otimes F(\alpha, r)$. However, as $\alpha(r)$ is typed according to rule $(\mathtt{T}{-}\mathtt{Ev})$, we have $d' \otimes F(\alpha, r) \leq_S d' \otimes \bigoplus_{r'}^{-1} F(\alpha, r') = d' \bigoplus_{r'}^{-1} F(\alpha, r') \oplus^{-1} F(\alpha, r)$ (for each specific r, according to the definition of $\oplus^{-1}$). But then we have $\bar{d} \geq_S d' \oplus^{-1} F(\alpha, r)$ which suffices to conclude.

□

References

1. Costa, G., Martinelli, F., Yautsiukhin, A.: Metric-aware secure service orchestration. In: Proc. of ICE-12. EPTCS (2012)