Corrigendum to “Type-driven Gradual Security with References,” by Toro et al., ACM Transactions on Programming Languages and Systems (TOPLAS) Volume 40, Issue 4, Article No. 16

In TOPLAS Volume 40, Issue 4, Article No. 16 (Toro et al., Type-driven Gradual Security with References), Figure 6 has an erroneous reduction rule.¹ The corrected version of rule (r7) is as follows (the change is highlighted in gray):

$$(r7) \varepsilon_1 o_g :=_{\varepsilon_3} \varepsilon_2 u \mid \mu \xrightarrow{\varepsilon g_c} \begin{cases} \text{unit}_\perp \mid \mu[o \mapsto \varepsilon'(u \tilde{\vee} (g_c \tilde{\vee} g))] \\ \text{error} & \text{if } \varepsilon' \text{ is not defined, or } \varepsilon \tilde{\vee} \text{ilbl}(\varepsilon_1) \not\leq \text{ilbl}(\varepsilon'') \text{ does not hold} \end{cases}$$

where:

$$\begin{aligned} \mu(o) &= \varepsilon'' u' \\ \varepsilon' &= (\varepsilon_2 \circ^{<} \text{iref}(\varepsilon_1)) \tilde{\vee} ((\varepsilon \tilde{\vee} \text{ilbl}(\varepsilon_1)) \circ^{\leq} \varepsilon_3 \circ^{\leq} \text{ilbl}(\text{iref}(\varepsilon_1))) \end{aligned}$$

As a consequence, the logical relations presented in Figures 9 and 10 have to be slightly modified and refactored as shown in Figures 1 and 2 (changes highlighted). The updated definition makes use of the following definition:

$$\begin{aligned} \text{obsEq}_{\ell_o}^{g_c, U}(\hat{g}_1, v_1, \hat{g}_2, v_2) &= g_c \vdash \hat{g}_1 \approx_{\ell_o} \hat{g}_2 \wedge (\text{obsEv}_{\ell_o}(\varepsilon_i) \Rightarrow \text{ev}^U(v_1) \approx_{\ell_o} \text{ev}^U(v_2)) \\ \text{ev}^U(\varepsilon u :: U) &= \varepsilon \\ \text{ev}^U(u) &= \mathcal{G}_{<:}(U, U) \\ \varepsilon_1 \approx_{\ell_o} \varepsilon_2 &\iff \forall U_i, U'_i, \varepsilon_i \vdash U'_i \lesssim U_i, (\text{obsEv}_{\ell_o}^{U_i}(\varepsilon_i) \vee \neg \text{obsEv}_{\ell_o}^{U_i}(\varepsilon_i)) \wedge \\ &\quad \text{obsEv}_{\ell_o}^{U_i}(\varepsilon_i) \Rightarrow \begin{cases} \text{idom}(\varepsilon_1) \approx_{\ell_o} \text{idom}(\varepsilon_2) & \text{if defined} \\ \text{icod}(\varepsilon_1) \approx_{\ell_o} \text{icod}(\varepsilon_2) & \text{if defined} \\ \text{iref}(\varepsilon_1) \approx_{\ell_o} \text{iref}(\varepsilon_2) & \text{if defined} \end{cases} \\ \text{and} & \\ \text{obsEv}_{\ell_o}^U(\varepsilon) &= \text{obsEv}_{\ell_o}^{\widehat{\text{label}}(U)}(\text{ilbl}(\varepsilon)) \end{aligned}$$

The proof of noninterference is updated accordingly; it is available in the updated companion technical report TR/DCC-2018-4/v2 (<https://www.dcc.uchile.cl/reportes>).

¹Thanks to Arthur Azevedo de Amorim for detecting and reporting the error.

$$\begin{aligned}
& \Sigma; g_c \vdash \langle \hat{g}_1, v_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \hat{g}_2, v_2, \mu_2 \rangle : U \iff \Sigma \vdash \mu_1 \approx_{\ell_o}^k \mu_2 \wedge \cdot; \Sigma; \hat{g}_i \vdash v_i : U \wedge \\
& \quad (\text{obsEq}_{\ell_o}^{g_c, U}(\hat{g}_1, v_1, \hat{g}_2, v_2)) \wedge ((\text{obsVal}_{\ell_o}^U(v_i) \wedge \text{obsEv}_{\ell_o}^{g_i}(\varepsilon_i)) \implies \text{obsRel}_{k, \ell_o}^{\Sigma, g_c, U}(\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2)) \\
& \text{obsRel}_{k, \ell_o}^{\Sigma, g_c, U}(\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \iff \text{rval}(v_1) = \text{rval}(v_2) \quad \text{if } U \in \{\text{Bool}_g, \text{Unit}_g, \text{Ref}_g U'\} \\
& \text{obsRel}_{k, \ell_o}^{\Sigma, g_c, U_1 \xrightarrow{g_{32}}_{g_{31}} U_2}(\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \iff \forall j \leq k, \forall U' = U_1 \xrightarrow{g'_{32}}_{g'_{31}} U'_2, \forall U''_1, \\
& \quad \forall g'_c, \forall \hat{g}'_1 \approx_{\ell_o} \hat{g}'_2, \hat{g}'_i = \varepsilon'_i g'_i, \text{ where } \varepsilon'_i \vdash g'_i \lesssim g'_c, \text{ s.t. } \hat{g}_i \leq_{\ell_o} \hat{g}'_i, \\
& \quad \varepsilon_{11} \vdash U_1 \xrightarrow{g_{32}}_{g_{31}} U_2 \lesssim U', \varepsilon_{12} \vdash U''_1 \lesssim U'_1, \text{ and } \varepsilon_{3i} \vdash g'_c \vee g'_{31} \preceq g'_{32}, \text{ we have:} \\
& \quad \forall v'_i, \mu'_i, \Sigma', \Sigma \subseteq \Sigma', \Sigma'; g_c \vdash \langle \hat{g}_1, v'_1, \mu'_1 \rangle \approx_{\ell_o}^j \langle \hat{g}_2, v'_2, \mu'_2 \rangle : U''_1, \text{dom}(\mu_i) \subseteq \text{dom}(\mu'_i), \\
& \quad \Sigma'; g_c \vdash \langle \hat{g}_1, (\varepsilon_{11} v_1 @_{\varepsilon_{31}} \varepsilon_{12} v'_1), \mu'_1 \rangle \approx_{\ell_o}^j \langle \hat{g}_2, (\varepsilon_{11} v_2 @_{\varepsilon_{32}} \varepsilon_{12} v'_2), \mu'_2 \rangle : \mathcal{C}(U'_2 \tilde{\vee} g'_{31})
\end{aligned}$$

Fig. 1. Related values.

$$\begin{aligned}
& \Sigma; g_c \vdash \langle \hat{g}_1, t_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \hat{g}_2, t_2, \mu_2 \rangle : \mathcal{C}(U) \iff g_c \vdash \hat{g}_1 \approx_{\ell_o} \hat{g}_2 \wedge \Sigma \vdash \mu_1 \approx_{\ell_o}^k \mu_2 \wedge \forall \hat{g}'_1 \approx_{\ell_o} \hat{g}'_2, \text{ s.t. } \hat{g}_i \leq_{\ell_o} \hat{g}'_i \text{ and} \\
& \quad \cdot; \Sigma; \hat{g}'_i \vdash t_i : U, \forall j < k, (t_i \mid \mu_i \xrightarrow{\hat{g}'_i} j t'_i \mid \mu'_i \implies \exists \Sigma', \Sigma \subseteq \Sigma' \\
& \quad \Sigma' \vdash \mu'_1 \approx_{\ell_o}^{k-j} \mu'_2 \wedge ((\text{irred}(t'_1) \wedge \text{irred}(t'_2)) \implies \Sigma'; g_c \vdash \langle \hat{g}_1, t'_1, \mu'_1 \rangle \approx_{\ell_o}^{k-j} \langle \hat{g}_2, t'_2, \mu'_2 \rangle : U))
\end{aligned}$$

Fig. 2. Related computations.

(See: DOI: <https://doi.org/10.1145/3229061>)