15-812: Programming Language Semantics

Lecture Notes on Uniform Substitution Soundness

André Platzer

Carnegie Mellon University
Lecture 10

1 Introduction

Using the static semantics from the previous lecture, this lecture now proves the soundness of uniform substitution [Pla15, Pla17].

2 Recall: Uniform Substitution

$$\text{US}\ \frac{\phi}{\sigma(\phi)}$$

The result of applying the uniform substitution σ to formula ϕ is denoted $\sigma(\phi)$ and defined in Fig. 1. Likewise, the result of applying the uniform substitution σ to term θ is denoted $\sigma(\theta)$ and the result of applying it to program α is denoted $\sigma(\alpha)$. We use $\Sigma(\phi)$ to denote the signature, so set of all function, predicate, and program constant symbols occurring in ϕ and likewise for θ, α.

Definition 1 (Admissible uniform substitution)**.** A uniform substitution σ is *U-admissible for* ϕ (or θ or α, respectively) with respect to the variables $U \subseteq \mathcal{V}$ iff $\text{FV}(\sigma|_{\Sigma(\phi)}) \cap U = \emptyset$, where $\sigma|_{\Sigma(\phi)}$ is the restriction of σ that only replaces symbols that occur in ϕ, and $\text{FV}(\sigma) = \bigcup_{f \in \sigma} \text{FV}(\sigma f(\cdot)) \cup \bigcup_{p \in \sigma} \text{FV}(\sigma p(\cdot))$ are the *free variables* that σ introduces. A uniform substitution σ is *admissible for* ϕ (or θ or α, respectively) iff the bound variables U of each operator of ϕ are not free in the substitution on its arguments, i.e. σ is U-admissible. These admissibility conditions are listed explicitly in Fig. 1, which defines the result $\sigma(\phi)$ of applying σ to ϕ.

$\sigma(x) = x$	for variable $x \in \mathcal{V}$
$\sigma(f(\theta)) = (\sigma(f))(\sigma(\theta)) \overset{\text{def}}{=} \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))$	for function symbol $f \in \sigma$
$\sigma(g(\theta)) = g(\sigma(\theta))$	for function symbol $g \notin \sigma$
$\sigma(\theta + \eta) = \sigma(\theta) + \sigma(\eta)$	
$\sigma(\theta \cdot \eta) = \sigma(\theta) \cdot \sigma(\eta)$	
$\sigma(\theta \geq \eta) \equiv \sigma(\theta) \geq \sigma(\eta)$	
$\sigma(p(\theta)) \equiv (\sigma(p))(\sigma(\theta)) \overset{\text{def}}{\equiv} \{\cdot \mapsto \sigma(\theta)\}(\sigma p(\cdot))$	for predicate symbol $p \in \sigma$
$\sigma(q(\theta)) \equiv q(\sigma(\theta))$	for predicate symbol $q \notin \sigma$
$\sigma(C(\phi)) \equiv \sigma(C)(\sigma(\phi)) \overset{\text{def}}{\equiv} \{\_ \mapsto \sigma(\phi)\}(\sigma C(\_))$	if σ is $\mathcal{V}$-admissible for ϕ, $C \in \sigma$
$\sigma(C(\phi)) \equiv C(\sigma(\phi))$	if σ is $\mathcal{V}$-admissible for ϕ, $C \notin \sigma$
$\sigma(\neg\phi) \equiv \neg\sigma(\phi)$	
$\sigma(\phi \wedge \psi) \equiv \sigma(\phi) \wedge \sigma(\psi)$	
$\sigma(\forall x\, \phi) \equiv \forall x\, \sigma(\phi)$	if σ is $\{x\}$-admissible for ϕ
$\sigma(\exists x\, \phi) \equiv \exists x\, \sigma(\phi)$	if σ is $\{x\}$-admissible for ϕ
$\sigma([\alpha]\phi) \equiv [\sigma(\alpha)]\sigma(\phi)$	if σ is BV$(\sigma(\alpha))$-admissible for ϕ
$\sigma(\langle\alpha\rangle\phi) \equiv \langle\sigma(\alpha)\rangle\sigma(\phi)$	if σ is BV$(\sigma(\alpha))$-admissible for ϕ
$\sigma(a) \equiv \sigma a$	for program constant $a \in \sigma$
$\sigma(b) \equiv b$	for program constant $b \notin \sigma$
$\sigma(x := \theta) \equiv x := \sigma(\theta)$	
$\sigma(?Q) \equiv ?\sigma(Q)$	
$\sigma(\mathsf{if}(Q)\, \alpha\, \mathsf{else}\, \beta) \equiv \mathsf{if}(\sigma(Q))\, \sigma(\alpha)\, \mathsf{else}\, \sigma(\beta)$	
$\sigma(\alpha; \beta) \equiv \sigma(\alpha); \sigma(\beta)$	if σ is BV$(\sigma(\alpha))$-admissible for β
$\sigma(\alpha^*) \equiv (\sigma(\alpha))^*$	if σ is BV$(\sigma(\alpha))$-admissible for α

Figure 1: Recursive application of uniform substitution σ

3 Soundness of Uniform Substitution

Adjoints capture in semantics the effect that a uniform substitution has on syntax.

Definition 2 (Substitution adjoints)**.** The *adjoint* to substitution σ is the operation that maps I, ω to the *adjoint* interpretation $\sigma^*_\omega I$ in which the interpretation of each function symbol $f \in \sigma$, predicate symbol $p \in \sigma$, quantifier symbol $C \in \sigma$, and program constant $a \in \sigma$ is modified according to σ:

$$\begin{aligned}
&\sigma^*_\omega I(f) : \mathbb{R} \to \mathbb{R};\ d \mapsto I^d_{\cdot}\omega[\![\sigma f(\cdot)]\!] \\
&\sigma^*_\omega I(p) = \{d \in \mathbb{R} \ :\ \omega \in I^d_{\cdot}[\![\sigma p(\cdot)]\!]\} \\
&\sigma^*_\omega I(a) = I[\![\sigma a]\!]
\end{aligned}$$

Adjoints enable the crucial uniform substitution lemma.

Lemma 3 (Uniform substitution for formulas)**.** *The uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I, \omega$ for I, ω have the same semantics for all* formulas *ϕ:*

$$\omega \in I[\![\sigma(\phi)]\!] \text{ iff } \omega \in \sigma^*_\omega I[\![\phi]\!]$$

Theorem 4 (Uniform substitution)**.** *The proof rule US is sound:*

$$\text{US}\ \frac{\phi}{\sigma(\phi)}$$

Proof. The proof [Pla17] uses that truth of the substituted formula is equivalent to truth of the original formula in the adjoint interpretation to conclude that validity of the premise in all interpretations implies validity in the adjoint interpretation so validity of the conclusion. Let the premise ϕ of rule US be valid, i.e., $\omega \in I[\![\phi]\!]$ for all states ω and for all interpretations I of the program, predicate, and function symbols. To show that the conclusion is valid, consider any state ω and any interpretation I and show that $\omega \in I[\![\sigma(\phi)]\!]$. By Lemma 3, the uniformly substituted formula $\sigma(\phi)$ is true in state ω of interpretation I iff the original formula ϕ is true in state ω of the adjoint interpretation $\sigma^*_\omega I$ that has already been modified according to the substitution σ, that is $\omega \in I[\![\sigma(\phi)]\!]$ iff $\omega \in \sigma^*_\omega I[\![\phi]\!]$. Now $\omega \in \sigma^*_\omega I[\![\phi]\!]$ holds, because $\omega \in I[\![\phi]\!]$ for all states ω and interpretations I, including for state ω and interpretation $\sigma^*_\omega I$, by premise. □

The proof of the uniform substitution lemma Lemma 3 that is used crucially in the proof of Theorem 4 crucially relies on correctness properties of the free and bound variable definitions, which we investigated last time.

4 Recall: Static Semantics

Recall the bound effect lemma and a slightly more general version of the coincidence lemmas that you will have the opportunity to prove as an exercise.

Lemma 5 (Bound lemma)**.** *If $(\omega, \nu) \in I[\![\alpha]\!]$, then $\omega = \nu$ on $BV(\alpha)^\complement$.*

Lemma 6 (Coincidence lemma)**.** *If $\omega = \tilde{\omega}$ on $FV(\theta)$ and $I = J$ on $\Sigma(\theta)$, then $I\omega[\![\theta]\!] = J\tilde{\omega}[\![\theta]\!]$.*

Lemma 7 (Coincidence lemma)**.** *If $\omega = \tilde{\omega}$ on $FV(\phi)$ and $I = J$ on $\Sigma(\phi)$, then $\omega \in I[\![\phi]\!]$ iff $\tilde{\omega} \in J[\![\phi]\!]$.*

Corollary 8 (Coincidence lemma)**.** *If $I = J$ on $\Sigma(\alpha)$, then $I[\![\alpha]\!] = J[\![\alpha]\!]$.*

5 Uniform Substitution Lemmas

A crucial element for the proof of Lemma 3 is the following fact about adjoint interpretations.

Corollary 9 (Admissible adjoints). *If $\omega = \nu$ on $FV(\sigma)$, then $\sigma^*_\omega I = \sigma^*_\nu I$. If σ is U-admissible for θ (or ϕ or α, respectively) and $\omega = \nu$ on $U^\complement$, then*

$$\sigma^*_\omega I[\![\theta]\!] = \sigma^*_\nu I[\![\theta]\!] \text{ i.e. } \sigma^*_\omega I\mu[\![\theta]\!] = \sigma^*_\nu I\mu[\![\theta]\!] \text{ for all states } \mu$$
$$\sigma^*_\omega I[\![\phi]\!] = \sigma^*_\nu I[\![\phi]\!]$$
$$\sigma^*_\omega I[\![\alpha]\!] = \sigma^*_\nu I[\![\alpha]\!]$$

Proof. First, $\sigma^*_\omega I(a) = I[\![\sigma a]\!] = \sigma^*_\nu I(a)$ holds because the adjoint to σ for I, ω in the case of programs is independent of ω (programs have access to their initial state at runtime). By Lemma 6, $I^d_{\cdot}\omega[\![\sigma f(\cdot)]\!] = I^d_{\cdot}\nu[\![\sigma f(\cdot)]\!]$ when $\omega = \nu$ on $\mathrm{FV}(\sigma f(\cdot)) \subseteq \mathrm{FV}(\sigma)$. Also $\omega \in I^d_{\cdot}[\![\sigma p(\cdot)]\!]$ iff $\nu \in I^d_{\cdot}[\![\sigma p(\cdot)]\!]$ by Lemma 7 when $\omega = \nu$ on $\mathrm{FV}(\sigma p(\cdot)) \subseteq \mathrm{FV}(\sigma)$. Thus, $\sigma^*_\omega I = \sigma^*_\nu I$ when $\omega = \nu$ on $\mathrm{FV}(\sigma)$.

If σ is U-admissible for ϕ (or θ or α), then $\mathrm{FV}(\sigma f(\cdot)) \cap U = \emptyset$, i.e. $\mathrm{FV}(\sigma f(\cdot)) \subseteq U^\complement$ for every function symbol $f \in \Sigma(\phi)$ (or θ or α) and likewise for predicate symbols $p \in \Sigma(\phi)$. Since $\omega = \nu$ on $U^\complement$ was assumed, $\sigma^*_\nu I = \sigma^*_\omega I$ on the function and predicate symbols in $\Sigma(\phi)$ (or θ or α). Finally $\sigma^*_\nu I = \sigma^*_\omega I$ on $\Sigma(\phi)$ (or $\Sigma(\theta)$ or $\Sigma(\alpha)$, respectively) implies that $\sigma^*_\nu I[\![\phi]\!] = \sigma^*_\omega I[\![\phi]\!]$ by Lemma 7 (since $\mu \in \sigma^*_\nu I[\![\phi]\!]$ iff $\mu \in \sigma^*_\omega I[\![\phi]\!]$ holds for all μ) and that $\sigma^*_\omega I[\![\theta]\!] = \sigma^*_\nu I[\![\theta]\!]$ by Lemma 6 and that $\sigma^*_\nu I[\![\alpha]\!] = \sigma^*_\omega I[\![\alpha]\!]$ by Corollary 8, respectively. □

Lemma 10 (Uniform substitution for terms). *The uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I, \omega$ for I, ω have the same semantics for all* terms *θ:*

$$I\omega[\![\sigma(\theta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$$

Proof of Lemma 3. The proof is by structural induction on ϕ and the structure on σ, simultaneously with Lemma 11.

1. $\omega \in I[\![\sigma(\theta \geq \eta)]\!]$ iff $\omega \in I[\![\sigma(\theta) \geq \sigma(\eta)]\!]$ iff $I\omega[\![\sigma(\theta)]\!] \geq I\omega[\![\sigma(\eta)]\!]$, by Lemma 10, iff $\sigma^*_\omega I\omega[\![\theta]\!] \geq \sigma^*_\omega I\omega[\![\eta]\!]$ iff $\sigma^*_\omega I\omega[\![\theta \geq \eta]\!]$.

2. Let $p \in \sigma$. Then $\omega \in I[\![\sigma(p(\theta))]\!]$ iff $\omega \in I[\![(\sigma(p))(\sigma(\theta))]\!]$ iff $\omega \in I[\![\{\cdot \mapsto \sigma(\theta)\}(\sigma p(\cdot))]\!]$ iff, by IH, $\omega \in I^d_{\cdot}[\![\sigma p(\cdot)]\!]$ iff $d \in \sigma^*_\omega I(p)$ iff $(\sigma^*_\omega I\omega[\![\theta]\!]) \in \sigma^*_\omega I(p)$ iff $\omega \in \sigma^*_\omega I[\![p(\theta)]\!]$ with $d \overset{\text{def}}{=} I\omega[\![\sigma(\theta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$ by using Lemma 10 for $\sigma(\theta)$ and by using the induction hypothesis for $\{\cdot \mapsto \sigma(\theta)\}(\sigma p(\cdot))$ on the possibly bigger formula $\sigma p(\cdot)$ but the structurally simpler uniform substitution $\{\cdot \mapsto \sigma(\theta)\}(\dots)$ that is a mere substitution on function symbol $\cdot$ of arity zero, not a substitution of predicates.

3. Let $q \notin \sigma$. Then $\omega \in I[\![\sigma(q(\theta))]\!]$ iff $\omega \in I[\![q(\sigma(\theta))]\!]$ iff $\big(I\omega[\![\sigma(\theta)]\!]\big) \in I(q)$ so, by Lemma 10, that holds iff $\big(\sigma^*_\omega I\omega[\![\theta]\!]\big) \in I(q)$ iff $\big(\sigma^*_\omega I\omega[\![\theta]\!]\big) \in \sigma^*_\omega I(q)$ iff $\omega \in \sigma^*_\omega I[\![q(\theta)]\!]$ since $I(q) = \sigma^*_\omega I(q)$ as the interpretation of q does not change in $\sigma^*_\omega I$ when $q \notin \sigma$.

4. $\omega \in I[\![\sigma(\neg\phi)]\!]$ iff $\omega \in I[\![\neg\sigma(\phi)]\!]$ iff $\omega \notin I[\![\sigma(\phi)]\!]$, so by IH, iff $\omega \notin \sigma^*_\omega I[\![\phi]\!]$ iff $\omega \in \sigma^*_\omega I[\![\neg\phi]\!]$

5. $\omega \in I[\![\sigma(\phi \wedge \psi)]\!]$ iff $\omega \in I[\![\sigma(\phi) \wedge \sigma(\psi)]\!]$ iff $\omega \in I[\![\sigma(\phi)]\!]$ and $\omega \in I[\![\sigma(\psi)]\!]$, by induction hypothesis, iff $\omega \in \sigma^*_\omega I[\![\phi]\!]$ and $\omega \in \sigma^*_\omega I[\![\psi]\!]$ iff $\omega \in \sigma^*_\omega I[\![\phi \wedge \psi]\!]$

6. $\omega \in I[\![\sigma(\exists x\, \phi)]\!]$ iff $\omega \in I[\![\exists x\, \sigma(\phi)]\!]$ (provided that σ is $\{x\}$-admissible for ϕ) iff $\omega^d_x \in I[\![\sigma(\phi)]\!]$ for some d, so, by induction hypothesis, iff $\omega^d_x \in \sigma^*_{\omega^d_x} I[\![\phi]\!]$ for some d, which is equivalent to $\omega^d_x \in \sigma^*_\omega I[\![\phi]\!]$ by Corollary 9 as σ is $\{x\}$-admissible for ϕ and $\omega = \omega^d_x$ on $\{x\}^\complement$. Thus, this is equivalent to $\omega \in \sigma^*_\omega I[\![\exists x\, \phi]\!]$.

7. The case $\omega \in I[\![\sigma(\forall x\, \phi)]\!]$ follows by duality $\forall x\, \phi \equiv \neg\exists x\, \neg\phi$, which is respected in the definition of uniform substitutions.

8. $\omega \in I[\![\sigma(\langle\alpha\rangle\phi)]\!]$ iff $\omega \in I[\![\langle\sigma(\alpha)\rangle\sigma(\phi)]\!]$ (provided σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for ϕ) iff there is a ν such that $(\omega,\nu) \in I[\![\sigma(\alpha)]\!]$ and $\nu \in I[\![\sigma(\phi)]\!]$, which, by Lemma 11 and induction hypothesis, respectively, is equivalent to: there is a ν such that $(\omega,\nu) \in \sigma^*_\omega I[\![\alpha]\!]$ and $\nu \in \sigma^*_\nu I[\![\phi]\!]$, which is equivalent to $\omega \in \sigma^*_\omega I[\![\langle\alpha\rangle\phi]\!]$, because $\nu \in \sigma^*_\nu I[\![\phi]\!]$ is equivalent to $\nu \in \sigma^*_\omega I[\![\phi]\!]$ by Corollary 9 as σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for ϕ and $\omega = \nu$ on $\mathrm{BV}(\sigma(\alpha))^\complement$ by Lemma 5 since $(\omega,\nu) \in I[\![\sigma(\alpha)]\!]$.

9. The case $\omega \in I[\![\sigma([\alpha]\phi)]\!]$ follows by duality $[\alpha]\phi \equiv \neg\langle\alpha\rangle\neg\phi$, which is respected in the definition of uniform substitutions. □

Lemma 11 (Uniform substitution for programs)**.** *The uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I, \omega$ for I, ω have the same semantics for all* programs *α:*

$$(\omega,\nu) \in I[\![\sigma(\alpha)]\!] \textit{ iff } (\omega,\nu) \in \sigma^*_\omega I[\![\alpha]\!]$$

Proof. The proof is by structural induction on α, simultaneously with Lemma 3.

1. $(\omega,\nu) \in I[\![\sigma(a)]\!] = I[\![\sigma a]\!] = \sigma^*_\omega I(a) = \sigma^*_\omega I[\![a]\!]$ for program constant $a \in \sigma$ (the proof is accordingly for $a \notin \sigma$).

2. $(\omega,\nu) \in I[\![\sigma(x := \theta)]\!] = I[\![x := \sigma(\theta)]\!]$ iff $\nu = \omega^{I\omega[\![\sigma(\theta)]\!]}_x = \omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_x$ by Lemma 10, which is, thus, equivalent to $(\omega,\nu) \in \sigma^*_\omega I[\![x := \theta]\!]$.

3. $(\omega,\nu) \in I[\![\sigma(?Q)]\!] = I[\![?\sigma(Q)]\!]$ iff $\nu = \omega$ and $\omega \in I[\![\sigma(Q)]\!]$, iff, by Lemma 3, $\nu = \omega$ and $\omega \in \sigma^*_\omega I[\![Q]\!]$, which is equivalent to $(\omega,\nu) \in \sigma^*_\omega I[\![?Q]\!]$.

4. $(\omega,\nu) \in I[\![\sigma(\alpha;\beta)]\!] = I[\![\sigma(\alpha);\sigma(\beta)]\!] = I[\![\sigma(\alpha)]\!] \circ I[\![\sigma(\beta)]\!]$ (provided σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for β) iff there is a μ such that $(\omega,\mu) \in I[\![\sigma(\alpha)]\!]$ and $(\mu,\nu) \in I[\![\sigma(\beta)]\!]$, which, by induction hypothesis, is equivalent to $(\omega,\mu) \in \sigma^*_\omega I[\![\alpha]\!]$ and $(\mu,\nu) \in \sigma^*_\mu I[\![\beta]\!]$. Yet, $\sigma^*_\mu I[\![\beta]\!] = \sigma^*_\omega I[\![\beta]\!]$ by Corollary 9, because σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for β and $\omega = \nu$ on $\mathrm{BV}(\sigma(\alpha))^\complement$ by Lemma 5 since $(\omega,\mu) \in I[\![\sigma(\alpha)]\!]$. Finally, $(\omega,\mu) \in \sigma^*_\omega I[\![\alpha]\!]$ and $(\mu,\nu) \in \sigma^*_\omega I[\![\beta]\!]$ for some μ is equivalent to $(\omega,\nu) \in \sigma^*_\omega I[\![\alpha;\beta]\!]$.

5. $(\omega,\nu) \in I[\![\sigma(\mathsf{if}(Q)\,\alpha\,\mathsf{else}\,\beta)]\!]$ is left as an exercise.

6. $(\omega,\nu) \in I[\![\sigma(\alpha^*)]\!] = I[\![(\sigma(\alpha))^*]\!] = \big(I[\![\sigma(\alpha)]\!]\big)^* = \bigcup_{n\in\mathbb{N}} (I[\![\sigma(\alpha)]\!])^n$ (provided that σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for α) iff there are $n \in \mathbb{N}$ and $\nu_0 = \omega, \nu_1, \ldots, \nu_n = \nu$ such that $(\nu_i,\nu_{i+1}) \in I[\![\sigma(\alpha)]\!]$ for all $i < n$. By n uses of the induction hypothesis, this is equivalent to $(\nu_i,\nu_{i+1}) \in \sigma^*_{\nu_i} I[\![\alpha]\!]$ for all $i < n$, which is equivalent

to $(\nu_i, \nu_{i+1}) \in \sigma^*_\omega I[\![\alpha]\!]$ by Corollary 9 since σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for α and $\nu_{i+1} = \nu_i$ on $\mathrm{BV}(\sigma(\alpha))^\complement$ by Lemma 5 as $(\nu_i, \nu_{i+1}) \in I[\![\sigma(\alpha)]\!]$ for all $i < n$. Thus, this is equivalent to $(\omega, \nu) \in \sigma^*_\omega I[\![\alpha^*]\!] = \big(\sigma^*_\omega I[\![\alpha]\!]\big)^*$. □

6 Uniform Substitution of Rules and Proofs

Uniform substitutions can also be used on inferences

$$\frac{\phi_1 \quad \ldots \quad \phi_n}{\psi}$$

or entire proofs that conclude ψ from the premises ϕ_1 and ϕ_2 and so on and ϕ_n (likewise for sequents). An inference or proof rule is *locally sound* iff its conclusion is valid in any interpretation I in which all its premises are valid. All locally sound proof rules are sound.

Theorem 12 (Soundness of uniform substitution of rules)**.** *All uniform substitution instances (with $FV(\sigma) = \emptyset$) of locally sound inferences are* locally sound*:*

$$\frac{\phi_1 \quad \ldots \quad \phi_n}{\psi} \textit{ locally sound} \qquad \textit{implies} \qquad \frac{\sigma(\phi_1) \quad \ldots \quad \sigma(\phi_n)}{\sigma(\psi)} \textit{ locally sound}$$

Proof. The proof is from previous work [Pla17]. Let $\mathcal{D}$ be the inference on the left and let $\sigma(\mathcal{D})$ be the substituted inference on the right. Assume $\mathcal{D}$ to be locally sound. To show that $\sigma(\mathcal{D})$ is locally sound, consider any I in which all premises of $\sigma(\mathcal{D})$ are valid, i.e. $I \models \sigma(\phi_j)$ for all j. That is, $\omega \in I[\![\sigma(\phi_j)]\!]$ for all ω and all j. By Lemma 3, $\omega \in I[\![\sigma(\phi_j)]\!]$ is equivalent to $\omega \in \sigma^*_\omega I[\![\phi_j]\!]$, which, thus, also holds for all ω and all j. By Corollary 9, $\sigma^*_\omega I[\![\phi_j]\!] = \sigma^*_\nu I[\![\phi_j]\!]$ for any ν, since $\mathrm{FV}(\sigma) = \emptyset$. Fix an arbitrary state ν. Then $\nu \in \sigma^*_\nu I[\![\sigma(\phi_j)]\!]$ holds for all ν and all j for the same (arbitrary) ν that determines $\sigma^*_\nu I$.

Consequently, all premises of $\mathcal{D}$ are valid in the same $\sigma^*_\nu I$, i.e. $\sigma^*_\nu I \models \phi_j$ for all j. Thus, $\sigma^*_\nu I \models \psi$ by local soundness of $\mathcal{D}$. That is, $\omega \in \sigma^*_\omega I[\![\psi]\!] = \sigma^*_\nu I[\![\psi]\!]$ by Corollary 9 for all ω. By Lemma 3, $\omega \in \sigma^*_\omega I[\![\psi]\!]$ is equivalent to $\omega \in I[\![\sigma(\psi)]\!]$, which continues to hold for all ω. Thus, $I \models \sigma(\psi)$, i.e. the conclusion of $\sigma(\mathcal{D})$ is valid in I, hence $\sigma(\mathcal{D})$ is locally sound. Consequently, all uniform substitution instances $\sigma(\mathcal{D})$ of locally sound inferences $\mathcal{D}$ with $\mathrm{FV}(\sigma) = \emptyset$ are locally sound. □

Furthermore, if $n = 0$ so that ψ has a proof, then the theorem also holds when $\mathrm{FV}(\sigma) \neq \emptyset$, because soundness and local soundness are equivalent notions for $n = 0$ premises [Pla17].

What is particularly cute about Theorem 12 is that it explains how the proof rules of dynamic logic, which were phrased as proof rule schemata with infinitely many instances, can also be understood as axiomatic proof rules that are merely pairs of concrete dynamic logic formulas. For example generalization rule

$$\mathrm{G}\ \frac{p(\bar{x})}{[a]p(\bar{x})}$$

is a pair of concrete DL formulas. Rule G can be instantiated with Theorem 12 to:

$$\frac{x^2 \geq 0}{[x := x+1; \mathsf{if}(x > 0)\, x := -x \,\mathsf{else}\, x := x^2]x^2 \geq 0}$$

using the uniform substitution

$$\sigma = \{p(\bar{x}) \mapsto x^2 \geq 0, a \mapsto x := x+1; \mathsf{if}(x > 0)\, x := -x \,\mathsf{else}\, x := x^2\}$$

All of a sudden, the only proof rule that needs an implementation as an algorithm is the uniform substitution prove rule itself. All other axioms and axiomatic proof rules are just concrete data.

References

[Pla15] André Platzer. A uniform substitution calculus for differential dynamic logic. In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481, Berlin, 2015. Springer. doi:10.1007/978-3-319-21401-6_32.

[Pla17] André Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reas.*, 59(2):219–265, 2017. doi:10.1007/s10817-016-9385-1.