Uniform Substitution At One Fell Swoop*

André Platzer[1,2]

[1] Computer Science Department, Carnegie Mellon University, Pittsburgh, USA
[2] Fakultät für Informatik, Technische Universität München

Abstract. Uniform substitution of function, predicate, program or game symbols is the core operation in parsimonious provers for hybrid systems and hybrid games. By postponing soundness-critical admissibility checks, this paper introduces a uniform substitution mechanism that proceeds in a linear pass homomorphically along the formula. Soundness is recovered using a simple variable condition at the replacements performed by the substitution. The setting in this paper is that of differential hybrid games, in which discrete, continuous, and adversarial dynamics interact in differential game logic dGL. This paper proves soundness and completeness of one-pass uniform substitutions for dGL.

1 Introduction

After a number of false starts on substitution [11,12,22], even by prominent logicians, did Church's *uniform substitution* [5, §35,40] provide a mechanism for substituting function and predicate symbols with terms and formulas in first-order logic. Given a mechanism for applying a uniform substitution σ to formulas ϕ with result denoted $\sigma\phi$ uniform substitutions are used with Church's proof rule:

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

Contrary to casual belief, quite some care is needed in the substitution process, even of only function symbols [23], in order to prevent replacing functions with terms that denote incompatible values in different places depending on which variables are being used in the replacements and in which formula contexts. Due to their subtleties, there have even been passionate calls for banishing substitutions [10] and using more schemata. This paper moves in the opposite direction, making substitutions even more subtle, but also faster and, nevertheless, sound.

The biggest theoretical advantage of uniform substitutions is that they make instantiation explicit, so that proof calculi can use axioms (concrete object-level formulas) instead of axiom schemata (meta-level concepts standing for infinitely many formulas). Their biggest practical advantage is that this avoidance

* In Shakespeare's Macbeth, "at one fell swoop" was likened to the suddenness with which a bird of prey fiercely attacks a whole nest at once. The idiom has since retained only its meaning of suddenly doing all at once, although the connotation of fierceness is also befitting of the ignorance with which one-pass uniform substitution trespasses operator scopes. This research is supported by the Alexander von Humboldt Foundation and by the AFOSR under grant number FA9550-16-1-0288.

P. Fontaine (Ed): CADE 2019, LNCS 11716, pp. 425–441, 2019.
DOI: 10.1007/978-3-030-29436-6_25

of schemata enables parsimonious theorem prover implementations that only consist of copies of concrete formulas as axioms together with *one* algorithm implementing the application of uniform substitutions (plus renaming). Similar advantages exist for concrete axiomatic proof rules instead of rule schemata [16]. This design obviates the need for algorithms that recognize all of the infinitely many instances of schemata and check all of their (sometimes pretty subtle) side conditions to soundly reject improper reasoning. These practical advantages have first been demonstrated for hybrid systems [8] and for hybrid games [18] proving, where uniform substitution led to significant reductions in soundness-critical size (down from 66000 to 1700 lines of code) or implementation time (down from months to minutes) compared to conventional prover implementations.

These uses of the uniform substitution principle required generalizations from first-order logic [5] to differential dynamic logic dL for hybrid systems [16] and differential game logic dGL for hybrid games [18], including substitutions of programs or games, respectively. The presence of variables whose values change imperatively over time, and of differential equations $x' = \theta$ that cause intrinsic links of variables x and their time-derivatives x', significantly complicate affairs compared to the simplicity of first-order logic [5,23] and λ-calculus [4]. Pure λ-calculus has a single binder and rests on the three pillars of α-conversions (for bound variables), β-reductions (by capture-avoiding substitutions), and η-conversions (versus free variables), which provide an elegant, deep, but solid foundation for functional programs (with similar observations for first-order logic). Despite significant additional challenges,[3] just two elementary operations, nevertheless, suffice as a foundation for imperative programs and even hybrid games: bound renaming and uniform substitution (based on suitably generalized notions of free and bound variables). Uniform substitutions generalize elegantly and in highly modular ways [16,18]. Much of the conceptual simplicity in the correctness arguments in these cases, however, came from the fact that Church-style uniform substitutions are applied by checking *at each operator* admissibility, i.e., that no free variable be introduced into a context in which it is bound. Such checks simplify correctness proofs, because they check each admissibility condition at every operator where they are necessary for soundness. The resulting substitution mechanism is elegant but computationally suboptimal, because it repeatedly checks admissibility recursively again and again at every operator. For example, applying a uniform substitution σ checks at every sequential composition $\alpha;\beta$ again that the entire substitution σ is admissible for the remainder β compared to the bound variables of the result of having applied σ to α:

$$\sigma(\alpha;\beta) = (\sigma(\alpha);\sigma(\beta)) \quad \text{if } \sigma \text{ is } \mathsf{BV}(\sigma(\alpha))\text{-admissible for } \beta \tag{1}$$

[3] The area of effect that an assignment to a variable has is non-computable and even a single occurrence of a variable may have to be both free and bound to ensure correctness. Such overlap is an inherent consequence of change, which is an intrinsic feature of dynamical systems theory (the mathematics of change) and game theory (the mathematics of effects resulting from strategic interaction by player decisions).

where σ is U-admissible for β iff the free variables of the replacements for the part of σ having function/predicate symbols that occur in β do not intersect U, which, here, are the bound variables $\mathsf{BV}(\sigma(\alpha))$ computed from the result of applying the substitution σ to α [18]. This mechanism is sound [16,18], even verified sound for hybrid systems in Isabelle/HOL and Coq [2], but computationally redundant due to its repeated substitution application and admissibility computations.

The point of this paper is to introduce a more liberal form of uniform substitution that *substitutes at one fell swoop*, forgoing admissibility checks during the operators where they would be needed with a monadic computation of taboo sets to make up for that negligence by checking cumulative admissibility conditions locally only *once* at each replacement that the uniform substitution application performs. This *one-pass uniform substitution* is computationally attractive, because it operates linearly in the output, which matters because uniform substitution is the dominant logical inference in uniform substitution provers [8]. The biggest challenge is, precisely, that correctness of substitution can no longer be justified for all operators where it is needed (because admissibility is no longer recursively checked at every operator). The most important technical insight of this paper is that modularity of correctness arguments can be recovered, regardless, using a neighborhood semantics for taboos. Another value of this paper is its straightforward completeness proof based on [15,16]. Overall, the findings of this paper make it possible to verify hybrid games (and systems) with faster small soundness-critical prover cores than before [21,18], which, owing to their challenges, are the only two verification tools for hybrid games. Uniform substitutions extend to differential games [6,7], where soundness is challenging [13], leading to the first basis for a small prover core for differential hybrid games [17]. The accelerated proving primitives are of interest for other dynamic logics [9,1].

All proofs are in [20] and those till Theorem 19 were then formalized [19].

2 Preliminaries: Differential Game Logic

This section recalls the basics of differential game logic [15,18], the logic for specifying and verifying hybrid games of two players with differential equations.

2.1 Syntax

The set of all variables is $\mathbf{V}$, including for each variable x a differential variable x' (e.g., for an ODE for x). Higher-order differential variables x'' etc. are not used in this paper, so a finite set $\mathbf{V}$ suffices. The terms θ of (differential-form) dGL are polynomial terms with real-valued function symbols and *differential terms* $(\theta)'$ that are used to reduce reasoning about differential equations to reasoning about equations of differentials [16]. Hybrid games α describe the permitted discrete and continuous actions by player Angel and player Demon. Besides the operators of first-order logic of real arithmetic, dGL formulas ϕ can be built using $\langle\alpha\rangle\phi$, which expresses that Angel has a winning strategy in the hybrid game α to reach the region satisfying dGL formula ϕ. Likewise, $[\alpha]\phi$ expresses that Demon has a winning strategy in the hybrid game α to reach the region satisfying ϕ.

Definition 1 (Terms). Terms *are defined by the following grammar (with θ,η, θ_1,…,θ_k as terms, $x \in \mathbf{V}$ as variable, and f as function symbol of arity k):*

$$\theta, \eta \ ::= \ x \mid f(\theta_1, \dots, \theta_k) \mid \theta + \eta \mid \theta \cdot \eta \mid (\theta)'$$

Definition 2 (dGL formulas). *The* formulas of differential game logic dGL *are defined by the following grammar (with ϕ, ψ as* dGL *formulas, p as predicate symbol of arity k, θ, η, θ_i as terms, x as variable, and α as hybrid game):*

$$\phi, \psi \ ::= \ \theta \geq \eta \mid p(\theta_1, \dots, \theta_k) \mid \neg\phi \mid \phi \land \psi \mid \exists x\, \phi \mid \langle\alpha\rangle\phi$$

The usual operators can be derived, e.g., $\forall x\, \phi$ is $\neg\exists x\, \neg\phi$ and similarly for $\rightarrow, \leftrightarrow$ and truth $\top$. Existence of Demon's winning strategy in hybrid game α to achieve ϕ is expressed by the dGL formula $[\alpha]\phi$, which can be expressed indirectly as $\neg\langle\alpha\rangle\neg\phi$, thanks to the hybrid game determinacy theorem [15, Thm. 3.1].

Definition 3 (Hybrid games). *The* hybrid games of differential game logic dGL *are defined by the following grammar (with α, β as hybrid games, a as game symbol, x as variable, θ as term, and ψ as* dGL *formula):*

$$\alpha, \beta \ ::= \ a \mid x := \theta \mid x' = \theta \,\&\, \psi \mid ?\psi \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

The operator precedences make all unary operators, including modalities and quantifiers, bind stronger. Just like the meaning of function and predicate symbols is subject to interpretation, the effect of game symbol a is up to interpretation. In contrast, the assignment game $x := \theta$ has the specific effect of changing the value of variable x to that of term θ. The differential equation game $x' = \theta \,\&\, \psi$ allows Angel to choose how long she wants to follow the (vectorial) differential equation $x' = \theta$ for any real duration within the set of states where evolution domain constraint ψ is true. Differential equation games with trivial $\psi = \top$ are just written $x' = \theta$. The test game $?\psi$ challenges Angel to satisfy formula ψ, for if ψ is not true in the present state she loses the game prematurely. The choice game $\alpha \cup \beta$ allows Angel to choose if she wants to play game α or game β. The sequential game $\alpha;\beta$ will play game β after game α terminates (unless a player prematurely lost the game while playing α). The repetition game α^* allows Angel to decide, after having played any number of α repetitions, whether she wants to play another round (but she cannot play forever). Finally, the dual game α^d will have both players switch sides: every choice that Angel had in α will go to Demon in α^d, and vice versa, while every condition that Angel needs to meet in α will be Demon's responsibility in α^d, and vice versa.

Substitutions are fundamental but subtle. For example, a substitution σ that has the effect of replacing $f(x)$ with x^2 and $a(x)$ with zy is unsound for the following formula while a substitution that replaces $a(x)$ with zx^2 would be fine:

$$\text{clash↯}\,\frac{\langle x' = f(x), y' = a(x)y\rangle\, x \geq 1 \leftrightarrow \langle x' = f(x)\rangle\, x \geq 1}{\langle x' = x^2, y' = zyy\rangle\, x \geq 1 \leftrightarrow \langle x' = x^2\rangle\, x \geq 1} \tag{2}$$

The introduction of a new variable z by the substitution σ is acceptable, but, even if y was already present previously, its introduction by σ makes the inference unsound (e.g., when $x = y = 1/z = 1/2$), because this equates a system with a solution that is exponential in y with a hyperbolic solution of more limited duration, even if both solutions are already hyperbolic of limited time from x. By contrast, the use of the previously present variable x to form $x' = x^2$ is fine. The difference is that, unlike z, variable y has a differential equation that changes the value of y and, while x also does, $f(x)$ and $a(x)$ may explicitly depend on x. It is crucial to distinguish correct and incorrect substitutions in all cases.

2.2 Semantics

A *state* ω is a mapping from the set of all variables $\mathbf{V}$ to the reals $\mathbb{R}$. The state ω_x^r agrees with state ω except for variable x whose value is $r \in \mathbb{R}$ in ω_x^r. The set of all states is denoted $\mathcal{S}$ and the set of all its subsets is denoted $\wp(\mathcal{S})$.

The semantics of function, predicate, and game symbols is independent from the state. They are interpreted by an *interpretation* I that maps each arity k function symbol f to a k-ary smooth function $I(f) : \mathbb{R}^k \to \mathbb{R}$, each arity k predicate symbol p to a k-ary relation $I(p) \subseteq \mathbb{R}^k$, and each game symbol a to a monotone $I(a) : \wp(\mathcal{S}) \to \wp(\mathcal{S})$ where $I(a)(X) \subseteq \mathcal{S}$ are the states from which Angel has a winning strategy to achieve $X \subseteq \mathcal{S}$ in game a. Differentials $(\theta)'$ have a differential-form semantics [16]: the sum of partial derivatives by all variables $x \in \mathbf{V}$ multiplied by the values of their associated differential variable x'.

Definition 4 (Semantics of terms). *The* semantics of a term θ *in interpretation I and state $\omega \in \mathcal{S}$ is its value $I\omega[\![\theta]\!]$ in $\mathbb{R}$. It is defined inductively as*

1. $I\omega[\![x]\!] = \omega(x)$ *for variable* $x \in \mathbf{V}$
2. $I\omega[\![f(\theta_1, \dots, \theta_k)]\!] = I(f)\big(I\omega[\![\theta_1]\!], \dots, I\omega[\![\theta_k]\!]\big)$ *for function symbol* f
3. $I\omega[\![\theta + \eta]\!] = I\omega[\![\theta]\!] + I\omega[\![\eta]\!]$
4. $I\omega[\![\theta \cdot \eta]\!] = I\omega[\![\theta]\!] \cdot I\omega[\![\eta]\!]$
5. $I\omega[\![(\theta)']\!] = \sum_{x \in \mathbf{V}} \omega(x') \frac{\partial I\omega[\![\theta]\!]}{\partial x}$ *for the differential* $(\theta)'$ *of* θ

The semantics of differential game logic in interpretation I defines, for each formula ϕ, the set of all states $I[\![\phi]\!]$, in which ϕ is true. Since hybrid games appear in dGL formulas and vice versa, the semantics $I[\![\alpha]\!]\big(X\big)$ of hybrid game α in interpretation I is defined by simultaneous induction as the set of all states from which Angel has a winning strategy in hybrid game α to achieve $X \subseteq \mathcal{S}$.

Definition 5 (dGL semantics). *The* semantics of a dGL formula ϕ *for each interpretation I with a corresponding set of states $\mathcal{S}$ is the subset $I[\![\phi]\!] \subseteq \mathcal{S}$ of states in which ϕ is true. It is defined inductively as follows*

1. $I[\![\theta \geq \eta]\!] = \{\omega \in \mathcal{S} : I\omega[\![\theta]\!] \geq I\omega[\![\eta]\!]\}$
2. $I[\![p(\theta_1, \dots, \theta_k)]\!] = \{\omega \in \mathcal{S} : (I\omega[\![\theta_1]\!], \dots, I\omega[\![\theta_k]\!]) \in I(p)\}$
3. $I[\![\neg\phi]\!] = (I[\![\phi]\!])^{\complement} = \mathcal{S} \setminus I[\![\phi]\!]$ *is the complement of* $I[\![\phi]\!]$
4. $I[\![\phi \wedge \psi]\!] = I[\![\phi]\!] \cap I[\![\psi]\!]$
5. $I[\![\exists x\, \phi]\!] = \{\omega \in \mathcal{S} : \omega_x^r \in I[\![\phi]\!]$ *for some* $r \in \mathbb{R}\}$
6. $I[\![\langle\alpha\rangle\phi]\!] = I[\![\alpha]\!]\big(I[\![\phi]\!]\big)$

A dGL *formula ϕ is* valid in I, *written $I \models \phi$, iff it is true in all states, i.e., $I[\![\phi]\!] = \mathcal{S}$. Formula ϕ is* valid, *written $\vDash \phi$, iff $I \models \phi$ for all interpretations I.*

Definition 6 (Semantics of hybrid games). *The* semantics of a hybrid game *α for each interpretation I is a function $I[\![\alpha]\!]\big(\cdot\big)$ that, for each set of states $X \subseteq \mathcal{S}$ as Angel's winning condition, gives the* winning region, *i.e., the set of states $I[\![\alpha]\!]\big(X\big) \subseteq \mathcal{S}$ from which Angel has a winning strategy to achieve X in α (whatever strategy Demon chooses). It is defined inductively as follows*

1. $I[\![a]\!]\big(X\big) = I(a)(X)$
2. $I[\![x := \theta]\!]\big(X\big) = \{\omega \in \mathcal{S} : \omega_x^{I\omega[\![\theta]\!]} \in X\}$
3. $I[\![x' = \theta \,\&\, \psi]\!]\big(X\big) = \{\omega \in \mathcal{S} : \omega = \varphi(0)$ *on* $\{x'\}^{\complement}$ *and* $\varphi(r) \in X$ *for some function* $\varphi : [0, r] \to \mathcal{S}$ *of some duration* $r \in \mathbb{R}$ *satisfying* $I, \varphi \models x' = \theta \wedge \psi\}$ *where* $I, \varphi \models x' = \theta \wedge \psi$ *iff* $\varphi(\zeta) \in I[\![x' = \theta \wedge \psi]\!]$ *and* $\varphi(0) = \varphi(\zeta)$ *on* $\{x, x'\}^{\complement}$ *for all* $0 \le \zeta \le r$ *and* $\frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(\zeta)$ *exists and equals* $\varphi(\zeta)(x')$ *for all* $0 \le \zeta \le r$ *if* $r > 0$.
4. $I[\![?\psi]\!]\big(X\big) = I[\![\psi]\!] \cap X$
5. $I[\![\alpha \cup \beta]\!]\big(X\big) = I[\![\alpha]\!]\big(X\big) \cup I[\![\beta]\!]\big(X\big)$
6. $I[\![\alpha; \beta]\!]\big(X\big) = I[\![\alpha]\!]\big(I[\![\beta]\!]\big(X\big)\big)$
7. $I[\![\alpha^*]\!]\big(X\big) = \bigcap\{Z \subseteq \mathcal{S} : X \cup I[\![\alpha]\!]\big(Z\big) \subseteq Z\}$ *which is a least fixpoint [15]*
8. $I[\![\alpha^d]\!]\big(X\big) = (I[\![\alpha]\!]\big(X^{\complement}\big))^{\complement}$

Along $x' = \theta \,\&\, \psi$, variables x and x' enjoy an intrinsic link since they co-evolve.

2.3 Static Semantics

Sound uniform substitutions check free and bound occurrences of variables to prevent unsound replacements of expressions that might have incorrect values in the respective replacement contexts. The whole point of this paper is to skip admissibility checks such as that in (1). Free (and, indirectly, bound) variables will still have to be consulted to tell apart acceptable from unsound occurrences.

Hybrid games even make it challenging to characterize free and bound variables. Both are definable based on whether or not their values affect the existence of winning strategies under variations of the winning conditions [18]. The *upward projection* $X{\uparrow}V$ increases the winning condition $X \subseteq \mathcal{S}$ from variables $V \subseteq \mathbf{V}$ to all states that are "on V like X", i.e., similar on V to states in X. The *downward projection* $X{\downarrow}\omega(V)$ shrinks the winning condition X, fixing the values of state ω on variables $V \subseteq \mathbf{V}$ to keep just those states of X that agree with ω on V.

Definition 7. *The set $X{\uparrow}V = \{\nu \in \mathcal{S} : \exists\omega \in X\, \omega = \nu$ on $V\} \supseteq X$ extends $X \subseteq \mathcal{S}$ to the states that agree on $V \subseteq \mathbf{V}$ with some state in X (written $\exists$). The set $X{\downarrow}\omega(V) = \{\nu \in X : \omega = \nu$ on $V\} \subseteq X$ selects state ω on $V \subseteq \mathbf{V}$ in $X \subseteq \mathcal{S}$.*

Projections make it possible to (*semantically!*) define free and bound variables of hybrid games by expressing variable dependence and ignorance. Such semantic characterizations increase modularity and are used for the correctness of syntactic analyzes that compute supersets [16, Sect. 2.4]. Variable x is free in hybrid game α iff two states that only differ in the value of x differ in membership in the winning region of α for some winning condition $X{\uparrow}\{x\}^{\complement}$ that does not distinguish values of x. Variable x is bound in hybrid game α iff it is in the winning region of α for some winning condition X but not for the winning condition $X{\downarrow}\omega(\{x\})$ that limits the new value of x to stay at its initial value $\omega(x)$.

Definition 8 (Static semantics). *The* static semantics *defines the* free variables*, which are all variables that the value of an expression depends on, as well as* bound variables*,* $\mathsf{BV}(\alpha)$*, which can change their value during game* α*, as:*

$$\begin{aligned}
\mathsf{FV}(\theta) &= \big\{x \in \mathbf{V} : \exists I, \omega, \tilde{\omega} \textit{ such that } \omega = \tilde{\omega} \textit{ on } \{x\}^{\complement} \textit{ and } I\omega[\![\theta]\!] \neq I\tilde{\omega}[\![\theta]\!]\big\}\\
\mathsf{FV}(\phi) &= \big\{x \in \mathbf{V} : \exists I, \omega, \tilde{\omega} \textit{ such that } \omega = \tilde{\omega} \textit{ on } \{x\}^{\complement} \textit{ and } \omega \in I[\![\phi]\!] \not\ni \tilde{\omega}\big\}\\
\mathsf{FV}(\alpha) &= \big\{x \in \mathbf{V} : \exists I, \omega, \tilde{\omega}, X \textit{ with } \omega = \tilde{\omega} \textit{ on } \{x\}^{\complement} \textit{ and } \omega \in I[\![\alpha]\!]\big(X{\uparrow}\{x\}^{\complement}\big) \not\ni \tilde{\omega}\big\}\\
\mathsf{BV}(\alpha) &= \big\{x \in \mathbf{V} : \exists I, \omega, X \textit{ such that } I[\![\alpha]\!]\big(X\big) \ni \omega \notin I[\![\alpha]\!]\big(X{\downarrow}\omega(\{x\})\big)\big\}
\end{aligned}$$

Beyond assignments, note complications with ODEs such as (2), where, due to their nature as the solution of a fixpoint condition, the *same* occurrences of variables are free, because they depend on their initial values, but they are also bound, because their values change along the ODE. All occurrences of x and y but not z on the right-hand side of $x' = x^2, y' = zx^2y$ and occurrences of x, y, x', y' also after this ODE are bound, since they are affected by this change. Variables x, y, z but not x', y' are free in this ODE. The crucial need for overlap of free and bound variables is most obvious for ODEs, but also arises for loops, e.g., $(x := x + 1; x' = -x)^*$. If x were not classified as free, its initial value could be overwritten incorrectly. If x were not classified as bound, its initial value could be incorrectly copy-propagated across the loop. This also applies to the *same* occurrence of x in $x + 1$ and $-x$, respectively. If it were not classified as a bound but a free occurrence, it could be incorrectly replaced by a term of the same initial value. If it were not classified as a free but a bound occurrence, it could, e.g., be boundly renamed, incorrectly losing its initial link.[4]

Coincidence lemmas [18] show truth-values of dGL formulas only depend on their free variables (likewise for terms and hybrid games). The bound effect lemma [18] shows only bound variables change their value when playing games. Supersets satisfy the same lemmas, so corresponding *syntactic* free and bound variable computations can be used correctly and are defined accordingly [16,18]. Since $\mathsf{FV}()$ and $\mathsf{BV}()$ are the smallest such sets, no smaller sets can be correct, including, e.g., the usual definitions that classify occurrences mutually exclusively.

Lemma 9 (Coincidence for terms [18]). $\mathsf{FV}(\theta)$ *is the smallest set with the coincidence property for* θ*: If* $\omega = \tilde{\omega}$ *on* $\mathsf{FV}(\theta)$*, then* $I\omega[\![\theta]\!] = I\tilde{\omega}[\![\theta]\!]$.

Lemma 10 (Coincidence for formulas [18]). $\mathsf{FV}(\phi)$ *is the smallest set with the coincidence property for* ϕ*: If* $\omega = \tilde{\omega}$ *on* $\mathsf{FV}(\phi)$*, then* $\omega \in I[\![\phi]\!]$ *iff* $\tilde{\omega} \in I[\![\phi]\!]$.

[4] These intricate variable relationships in games and the intrinsic link of x and x' from ODEs significantly complicate substitutions beyond what is supported for first-order logic [5,23], λ-calculi [4], de Bruijn indices [3], or higher-order abstract syntax [14].

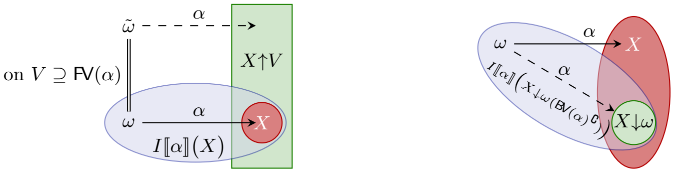

Fig. 1. Illustration of coincidence and bound effect properties of hybrid games

Lemma 11 (Coincidence for games [18]). $\mathsf{FV}(\alpha)$ *is the smallest set with the coincidence property for α: If $\omega = \tilde{\omega}$ on $V \supseteq \mathsf{FV}(\alpha)$, then $\omega \in I[\![\alpha]\!]\big(X{\uparrow}V\big)$ iff $\tilde{\omega} \in I[\![\alpha]\!]\big(X{\uparrow}V\big)$; see Fig. 1(left).*

Lemma 12 (Bound effect [18]). $\mathsf{BV}(\alpha)$ *is the smallest set with the bound effect property for α: $\omega \in I[\![\alpha]\!]\big(X\big)$ iff $\omega \in I[\![\alpha]\!]\big(X{\downarrow}\omega(\mathsf{BV}(\alpha)^\complement)\big)$; see Fig. 1(right).*

The correctness of one-pass uniform substitution will become more transparent after defining when one state is a variation of another on a set of variables. For a set $U \subseteq \mathbf{V}$, state $\tilde{\omega}$ is called a *U-variation* of state ω iff $\tilde{\omega} = \omega$ on complement $U^\complement$. Variations satisfy properties of monotonicity and transitivity. If $\tilde{\omega}$ is a U-variation of ω, then $\tilde{\omega}$ is a V-variation of ω for all $V \supseteq U$. If $\tilde{\omega}$ is a U-variation of ω and ω is a V-variation of μ, then $\tilde{\omega}$ is a $(U \cup V)$-variation of μ. Coincidence lemmas say that the semantics is insensitive to variations of nonfree variables. If $\tilde{\omega}$ is a U-variation of ω and $\mathsf{FV}(\phi) \cap U = \emptyset$, then $\omega \in I[\![\phi]\!]$ iff $\tilde{\omega} \in I[\![\phi]\!]$.

3 Uniform Substitution

Uniform substitutions for dGL affect terms, formulas, and games [18]. A *uniform substitution* σ is a mapping from expressions of the form $f(\cdot)$ to terms $\sigma f(\cdot)$, from $p(\cdot)$ to formulas $\sigma p(\cdot)$, and from game symbols a to hybrid games σa. Here $\cdot$ is a reserved function symbol of arity 0 marking the position where the argument, e.g., argument θ to $p(\cdot)$ in formula $p(\theta)$, will end up in the replacement $\sigma p(\cdot)$ used for $p(\theta)$. Vectorial extensions would be accordingly for other arities $k \geq 0$.

The key idea behind the new recursive one-pass application of uniform substitutions is that it simply applies σ by naïve homomorphic recursion without checking any admissibility conditions along the way. But the mechanism makes up for that soundness-defying negligence by passing a cumulative set U of taboo variables along the recursion that are then forbidden from being introduced free by σ *at the respective replacement* of function $f(\cdot)$ and predicate symbols $p(\cdot)$, respectively. No corresponding condition is required at substitutions of game symbols a, since games already have unlimited access to and effect on the state.

The result $\sigma^U\phi$ of *applying uniform substitution σ for taboo set $U \subseteq \mathbf{V}$ to a* dGL *formula ϕ* (or term θ or hybrid game α, respectively) is defined in Fig. 2. For proof rule US, the expression $\sigma\phi$ is, then, defined to be $\sigma^\emptyset\phi$ without taboos.

The case for $\exists x\,\phi$ in Fig. 2 conjoins the variable x to the taboo set in the homomorphic application of σ to ϕ, because any *newly introduced* free uses of

$$
\begin{array}{rcll}
\sigma^{U}(x) &=& x & \text{for variable } x \in \mathbf{V}\\
\sigma^{U}(f(\theta)) &=& (\sigma^{U} f)(\sigma^{U}\theta) \overset{\text{def}}{=} \{\cdot \mapsto \sigma^{U}\theta\}^{\emptyset}\sigma f(\cdot) & \text{if } \mathsf{FV}(\sigma f(\cdot)) \cap U = \emptyset\\
\sigma^{U}(\theta+\eta) &=& \sigma^{U}\theta + \sigma^{U}\eta & \\
\sigma^{U}(\theta\cdot\eta) &=& \sigma^{U}\theta \cdot \sigma^{U}\eta & \\
\sigma^{U}((\theta)') &=& (\sigma^{\mathbf{V}}\theta)' & \\
\hline
\sigma^{U}(\theta \geq \eta) &=& \sigma^{U}\theta \geq \sigma^{U}\eta & \\
\sigma^{U}(p(\theta)) &=& (\sigma^{U} p)(\sigma^{U}\theta) \overset{\text{def}}{=} \{\cdot \mapsto \sigma^{U}\theta\}^{\emptyset}\sigma p(\cdot) & \text{if } \mathsf{FV}(\sigma p(\cdot)) \cap U = \emptyset\\
\sigma^{U}(\neg\phi) &=& \neg\sigma^{U}\phi & \\
\sigma^{U}(\phi\wedge\psi) &=& \sigma^{U}\phi \wedge \sigma^{U}\psi & \\
\sigma^{U}(\exists x\,\phi) &=& \exists x\,\sigma^{U\cup\{x\}}\phi & \\
\sigma^{U}(\langle\alpha\rangle\phi) &=& \langle\sigma^{U}_{V}\alpha\rangle\sigma^{V}\phi & \\
\hline
\sigma^{U}_{U\cup\mathsf{BV}(\sigma a)}(a) &=& \sigma a & \text{for game symbol } a\\
\sigma^{U}_{U\cup\{x\}}(x:=\theta) &=& x:=\sigma^{U}\theta & \\
\sigma^{U}_{U\cup\{x,x'\}}(x'=\theta\,\&\,\psi) &=& (x'=\sigma^{U\cup\{x,x'\}}\theta\,\&\,\sigma^{U\cup\{x,x'\}}\psi) & \\
\sigma^{U}_{U}(?\psi) &=& ?\sigma^{U}\psi & \\
\sigma^{U}_{V\cup W}(\alpha\cup\beta) &=& \sigma^{U}_{V}\alpha \cup \sigma^{U}_{W}\beta & \\
\sigma^{U}_{W}(\alpha;\beta) &=& \sigma^{U}_{V}\alpha; \sigma^{V}_{W}\beta & \\
\sigma^{U}_{V}(\alpha^{*}) &=& (\sigma^{V}_{V}\alpha)^{*} & \text{where } \sigma^{U}_{V}\alpha \text{ is defined}\\
\sigma^{U}_{V}(\alpha^{d}) &=& (\sigma^{U}_{V}\alpha)^{d} &
\end{array}
$$

Fig. 2. Recursive application of one-pass uniform substitution σ for taboo $U \subseteq \mathbf{V}$

x within that scope would refer to a different semantic value than outside that scope. In addition to computing the substituted hybrid game $\sigma^{U}_{V}\alpha$, the recursive application of one-pass uniform substitution σ to hybrid game α under taboo set U also performs an analysis that results in a new output taboo set V, written in subscript notation, that will be tabooed after this hybrid game. Superscripts as inputs and subscripts as outputs follows static analysis notation and makes the $\alpha;\beta$ case reminiscent of Einstein's summation: the output taboos V of $\sigma^{U}_{V}\alpha$ become the input taboos V for $\sigma^{V}_{W}\beta$, whose output W is that of $\sigma^{U}_{W}(\alpha;\beta)$. Similarly, the output taboos V resulting from the uniform substitute $\sigma^{U}_{V}\alpha$ of a hybrid game α become taboo during the uniform substitution application forming $\sigma^{V}\phi$ in the postcondition of a modality to build $\sigma^{U}(\langle\alpha\rangle\phi)$.

Repetitions $\sigma^{U}_{V}(\alpha^{*})$ are the only complication in Fig. 2, where taboo U would be too lax during the recursion, because earlier repetitions of α bind variables of α itself, so only the taboos V obtained after one round $\sigma^{U}_{V}\alpha$ are correct input taboos for the loop body. These two passes per loop are linear in the output when considering repetitions α^{*} as their equivalent $?\top \cup \alpha;\alpha^{*}$ of double size.

Unlike in Church-style uniform substitution [5,16,18], attention is needed at the replacement sites of function and predicate symbols in order to make up for the neglected admissibility checks during all other operators. The result $\sigma^{U}(p(\theta))$ of applying uniform substitution σ with taboo U to a predicate application $p(\theta)$ is *only* defined if the replacement $\sigma p(\cdot)$ for p does not introduce free any tabooed variable, i.e., $\mathsf{FV}(\sigma p(\cdot)) \cap U = \emptyset$. Arguments are put in for placeholder $\cdot$ recursively by the taboo-free use of uniform substitution $\{\cdot \mapsto \sigma^U\theta\}$, which replaces arity 0 function symbol $\cdot$ by $\sigma^U\theta$. Taboos U are respected when forming (*once!*) the uniform substitution to be used for argument $\cdot$, but empty taboos $\emptyset$ suffice when substituting the resulting $\sigma^U\theta$ for $\cdot$ in the replacement $\sigma p(\cdot)$ for p.

All variables $\mathbf{V}$ become taboos during uniform substitutions into differentials $(\theta)'$, because any newly introduced occurrence of a variable x would cause additional dependencies on its respective associated differential variable x'.

If the conditions in Fig. 2 are not met, the substitution σ is said to *clash* for taboo U and its result $\sigma^U\phi$ is not defined and cannot be used. *All subsequent applications of uniform substitutions are required to be defined* (no clash).

Whether a substitution clashes is only checked once at each replacement, instead of also once per operator around it as in Church style from equation (1). The free variables $\mathsf{FV}(\sigma p(\cdot))$ of each (function and) predicate symbol replacement are best stored with σ to avoid repeated computation of free variables.

This inference would unsoundly equate linear solutions with exponential ones:

$$\text{clash}\lightning\,\frac{\langle v:=f\rangle p(v) \leftrightarrow p(f)}{\langle v:=-x\rangle[x'=v]\,x\geq 0 \leftrightarrow [x'=-x]\,x\geq 0}$$

Indeed, $\sigma = \{p(\cdot) \mapsto [x'=\cdot]\,x\geq 0, f\mapsto -x\}$ clashes so rejects the above inference since the substitute $-x$ for f has free variable x that is taboo in the context $[x'=\cdot]\,x\geq 0$. By contrast, a sound use of rule US, despite its change in multiple binding contexts with $\sigma = \{p(\cdot)\mapsto [(x:=x+\cdot;x'=\cdot)^*]\,x+\cdot\geq 0, f\mapsto -v\}$, is:

$$\text{US}\,\frac{\langle v:=f\rangle p(v) \leftrightarrow p(f)}{\langle v:=-v\rangle[(x:=x+v;x'=v)^*]\,x+v\geq 0 \leftrightarrow [(x:=x-v;x'=-v)^*]\,x-v\geq 0}$$

Uniform substitution accurately distinguishes such sound inferences from unsound ones even if the substitutions take effect deep down within a dGL formula. Uniform substitutions enable other syntactic transformations that require a solid understanding of variable occurrence patterns such as common subexpression elimination, for example, by using the above inference from right to left.

3.1 Taboo Lemmas

The only soundness-critical property of output taboos is that they correctly add bound variables and never forget variables that were already input taboos.

Lemma 13 (Taboo set computation). *One-pass uniform substitution application monotonously computes taboos with correct bound variables for games:*

$$\textit{if } \sigma^U_V\alpha \textit{ is defined, then } V\supseteq U\cup\mathsf{BV}(\sigma^U_V\alpha)$$

Any superset of such taboo computations (or the free variable sets used in Fig. 2) remains correct, just more conservative. The change from input taboo U to output taboo V is a function of the hybrid game α, justifying the construction of $\sigma^U_V(\alpha^*)$: if $\sigma^U_V\alpha$ and $\sigma^V_W\alpha$ are defined, then $\sigma^V_V\alpha$ is defined and equal to $\sigma^V_W\alpha$.

By Lemma 13, no implementation of bound variables is needed when defining game symbols via $\sigma^{U}_{U\cup V}(a) = \sigma a$ where $\{\}^{\emptyset}_{V}(\sigma a)$ with identity substitution $\{\}$. But bound variable computations speed up loops via $\sigma^{U}_{V}(\alpha^*) = (\sigma^{U\cup B}_{V}\alpha)^*$ since $B = \mathsf{BV}(\sigma^{\emptyset}_{M}\alpha)$ can be computed and used correctly in one pass when $U \cup B = V$.

3.2 Uniform Substitution Lemmas

Uniform substitutions are syntactic transformations on syntactic expressions. Their semantic counterpart is the semantic transformation that maps an interpretation I and a state ω to the adjoint interpretation $\sigma^*_\omega I$ that changes the meaning of all symbols according to the syntactic substitution σ. The interpretation $I^d_\cdot$ agrees with I except that function symbol $\cdot$ is interpreted as $d \in \mathbb{R}$.

Definition 14 (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, predicate symbol p, and game symbol a are modified according to σ (it is enough to consider those that σ changes):*

$$\sigma^*_\omega I(f) : \mathbb{R} \to \mathbb{R};\ d \mapsto I^d_\cdot\omega[\![\sigma f(\cdot)]\!]$$

$$\sigma^*_\omega I(p) = \{d \in \mathbb{R} : \omega \in I^d_\cdot[\![\sigma p(\cdot)]\!]\}$$

$$\sigma^*_\omega I(a) : \wp(\mathcal{S}) \to \wp(\mathcal{S});\ X \mapsto I[\![\sigma a]\!]\big(X\big)$$

The uniform substitution lemmas below are key to the soundness and equate the syntactic effect that a uniform substitution σ has on a syntactic expression in I, ω with the semantic effect that the switch to the adjoint interpretation $\sigma^*_\omega I$ has on the original expression. The technical challenge compared to Church-style uniform substitution [16,18] is that no admissibility conditions are checked at the game operators that need them, because the whole point of one-pass uniform substitution is that it homomorphically recurses in a linear complexity sweep by postponing admissibility checks. All that happens during the substitution is that different taboo sets are passed along. Yet, still, there is a crucial interplay of the particular taboos imposed henceforth at binding operators and the retroactive checking at function and predicate symbol replacement sites.

In order to soundly deal with the negligence in admissibility checking of one-pass uniform substitutions in a modular way, the main insight is that it is imperative to generalize the range of applicability of uniform substitution lemmas beyond the state ω of original interest where the adjoint $\sigma^*_\omega I$ was formed, and make them cover *all* variations of states that are so similar that they might arise during soundness justifications. By demanding more comprehensive care at replacement sites, soundness arguments make up for the temporary lapses in attention during all other operators. This gives the uniform substitution algorithm broader liberties at binding operators, while simultaneously demanding broader compatibility in semantic neighborhoods on its parts. Due to the recursive nature of function substitutions, the proof [20] of the following result is by structural induction lexicographically on the structure of σ and θ, for all U, ν, ω.

Lemma 15 (Uniform substitution for terms). *The uniform substitution σ for taboo $U \subseteq \mathbf{V}$ and its adjoint interpretation $\sigma^*_\omega I$ for I, ω have the same semantics on U-variations for all* terms θ*:*

$$\text{for all } U\text{-variations } \nu \text{ of } \omega\text{:}\;\; I\nu[\![\sigma^U\theta]\!] = \sigma^*_\omega I\nu[\![\theta]\!]$$

Recall that all uniform substitutions are only defined when they meet the side conditions from Fig. 2. A mention such as $\sigma^U\theta$ in Lemma 15 implies that its side conditions during the application of σ to θ with taboos U are met. Substitutions are antimonotone in taboos: If $\sigma^U\theta$ is defined, then $\sigma^V\theta$ is defined and equal to $\sigma^U\theta$ for all $V \subseteq U$ (accordingly for ϕ, α). The more taboos a use of a substitution tolerates, the more broadly its adjoint generalizes to state variations.

The corresponding results for formulas and games are proved by simultaneous induction since formulas and games are defined by simultaneous induction, as games may occur in formulas and, vice versa. The inductive proof [20] is lexicographic over the structure of σ and ϕ or α, with a nested induction over the closure ordinals of the loop fixpoints, simultaneously for all ν, ω, U, X.

Lemma 16 (Uniform substitution for formulas). *The uniform substitution σ for taboo $U \subseteq \mathbf{V}$ and its adjoint interpretation $\sigma^*_\omega I$ for I, ω have the same semantics on U-variations for all* formulas ϕ*:*

$$\text{for all } U\text{-variations } \nu \text{ of } \omega\text{:}\;\; \nu \in I[\![\sigma^U\phi]\!] \text{ iff } \nu \in \sigma^*_\omega I[\![\phi]\!]$$

Lemma 17 (Uniform substitution for games). *The uniform substitution σ for taboo $U \subseteq \mathbf{V}$ and its adjoint interpretation $\sigma^*_\omega I$ for I, ω have the same semantics on U-variations for all* games α*:*

$$\text{for all } U\text{-variations } \nu \text{ of } \omega\text{:}\;\; \nu \in I[\![\sigma^U_V\alpha]\!]\big(X\big) \text{ iff } \nu \in \sigma^*_\omega I[\![\alpha]\!]\big(X\big)$$

3.3 Soundness

With the uniform substitution lemmas having established the crucial equivalence of syntactic substitution and adjoint interpretation, the soundness of uniform substitution uses in proofs is now immediate. The notation $\sigma\phi$ in proof rule US is short for $\sigma^\emptyset\phi$, so the result of applying σ to ϕ without taboos (more taboos may still arise during the substitution application), and only defined if $\sigma^\emptyset\phi$ is. A proof rule is *sound* when its conclusion is valid if all its premises are valid.

Theorem 18 (Soundness of uniform substitution). *Proof rule US is sound.*

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

Proof. Let the premise ϕ of US be valid, i.e., $\omega \in I[\![\phi]\!]$ for all interpretations I and states ω. To show that the conclusion is valid, consider any I and state ω and show $\omega \in I[\![\sigma\phi]\!] = I[\![\sigma^\emptyset\phi]\!]$. By Lemma 16, $\omega \in I[\![\sigma^\emptyset\phi]\!]$ iff $\omega \in \sigma^*_\omega I[\![\phi]\!]$. Now $\omega \in \sigma^*_\omega I[\![\phi]\!]$ holds, because $\omega \in I[\![\phi]\!]$ for all I, ω, including $\sigma^*_\omega I, \omega$, by premise. □

Theorem 18 is all it takes to soundly instantiate concrete axioms. Uniform substitutions can instantiate whole inferences [16], which makes it possible to avoid proof rule schemata by instantiating axiomatic proof rules consisting of pairs of concrete formulas. This enables uniformly substituting premises and conclusions of entire proofs of *locally sound* inferences, i.e., those whose conclusion is valid in any interpretation that all their premises are valid in.

Theorem 19 (Soundness of uniform substitution of rules). *All uniform substitution instances for taboo* $\mathbf{V}$ *of locally sound inferences are locally sound:*

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi}\ \textit{locally sound} \quad \textit{implies} \quad \frac{\sigma^{\mathbf{V}}\phi_1 \quad \dots \quad \sigma^{\mathbf{V}}\phi_n}{\sigma^{\mathbf{V}}\psi}\ \textit{locally sound}$$

Proof. Fix any state ω. Let $\mathcal{D}$ be the locally sound inference on the left and $\sigma\mathcal{D}$ the substituted inference on the right. To prove $\sigma\mathcal{D}$ locally sound, consider any interpretation I in which all premises of $\sigma\mathcal{D}$ are valid, i.e., $I \models \sigma^{\mathbf{V}}\phi_j$ for all j, i.e., $\nu \in I[\![\sigma^{\mathbf{V}}\phi_j]\!]$ for all ν and j. By Lemma 16, $\nu \in I[\![\sigma^{\mathbf{V}}\phi_j]\!]$ is equivalent to $\nu \in \sigma^*_\omega I[\![\phi_j]\!]$ (since ν is a $\mathbf{V}$-variation of ω), which also holds for all ν and j.

Consequently, all premises of $\mathcal{D}$ are valid in the same interpretation $\sigma^*_\omega I$, i.e. $\sigma^*_\omega I \models \phi_j$ for all j. Thus, $\sigma^*_\omega I \models \psi$ by local soundness of $\mathcal{D}$. That is, $\nu \in \sigma^*_\omega I[\![\psi]\!]$ for all ν. By Lemma 16, $\nu \in \sigma^*_\omega I[\![\psi]\!]$ is equivalent to $\nu \in I[\![\sigma^{\mathbf{V}}\psi]\!]$ (since ν trivially is a $\mathbf{V}$-variation of ω), which continues to hold for all ν. Thus, $I \models \sigma^{\mathbf{V}}\psi$, i.e., the conclusion of $\sigma\mathcal{D}$ is valid in I, hence $\sigma\mathcal{D}$ is locally sound. □

USR marks the use of Theorem 19 in proofs. If $n = 0$ (so ψ has a proof), USR preserves local soundness for taboo-free $\sigma^{\emptyset}\psi$ instead of $\sigma^{\mathbf{V}}\psi$, as US proves $\sigma^{\emptyset}\psi$ from the provable ψ and soundness is equivalent to local soundness for $n = 0$.

3.4 Completeness

Soundness is the property that every formula with a proof is valid. This is the most important consideration for something as fundamental as a uniform substitution mechanism. But the converse question of completeness, i.e., that every valid formula has a proof, is of interest as well, especially given the fact that one-pass uniform substitutions check differently for soundness during the substitution application, which had better not lose otherwise perfectly valid proofs.

Completeness is proved in an easy modular style based on all the nontrivial findings summarized in schematic relative completeness results, first for schematic dGL [15, Thm. 4.5], and then for a uniform substitution formulation of dL [16, Thm. 40]. The combination of both schematic completeness results makes it fairly easy to lift completeness to the setting in this paper. The challenge is to show that all instances of axiom schemata that are used for dGL's schematic relative completeness result are provable by one-pass uniform substitution.

A dGL formula ϕ is called *surjective* iff rule US can instantiate ϕ to any of its axiom schema instances, i.e., those formulas that are obtained by just replacing game symbols a uniformly by any game, etc. An axiomatic rule is called *surjective* iff USR of Theorem 19 can instantiate it to any of its proof rule schema instances.

$$\begin{array}{rl}
[\cdot] & [a]\langle c\rangle\top \leftrightarrow \neg\langle a\rangle\neg\langle c\rangle\top \\
\langle{:=}\rangle_{=} & \langle x := f\rangle\langle c\rangle\top \leftrightarrow \exists x\,(x = f \land \langle c\rangle\top) \\
\text{DS} & \langle x' = f\rangle\langle c\rangle\top \leftrightarrow \exists t{\geq}0\,\langle x := x{+}ft\rangle\langle x' := f\rangle\langle c\rangle\top \\
\langle ?\rangle & \langle ?q\rangle p \leftrightarrow q \land p \\
\langle\cup\rangle & \langle a \cup b\rangle\langle c\rangle\top \leftrightarrow \langle a\rangle\langle c\rangle\top \lor \langle b\rangle\langle c\rangle\top \\
\langle ;\rangle & \langle a;b\rangle\langle c\rangle\top \leftrightarrow \langle a\rangle\langle b\rangle\langle c\rangle\top \\
\langle ^*\rangle & \langle a^*\rangle\langle c\rangle\top \leftrightarrow \langle c\rangle\top \lor \langle a\rangle\langle a^*\rangle\langle c\rangle\top \\
\langle ^d\rangle & \langle a^d\rangle\langle c\rangle\top \leftrightarrow \neg\langle a\rangle\neg\langle c\rangle\top
\end{array}
\qquad
\begin{array}{rl}
\text{M} & \dfrac{\langle c\rangle\top \to \langle d\rangle\top}{\langle a\rangle\langle c\rangle\top \to \langle a\rangle\langle d\rangle\top} \\
\text{FP} & \dfrac{\langle c\rangle\top \lor \langle a\rangle\langle d\rangle\top \to \langle d\rangle\top}{\langle a^*\rangle\langle c\rangle\top \to \langle d\rangle\top} \\
\text{MP} & \dfrac{p \quad p \to q}{q} \\
\forall & \dfrac{\langle c\rangle\top}{\forall x\,\langle c\rangle\top}
\end{array}$$

Fig. 3. Differential game logic axioms and axiomatic proof rules

Lemma 20 (Surjective axioms). *If ϕ is a* dGL *formula that is built only from game symbols but no function or predicate symbols, then ϕ is surjective. Axiomatic rules consisting of surjective* dGL *formulas are surjective.*

Instead of following previous completeness arguments for uniform substitution [18], this paper presents a pure game-style uniform substitution formulation in Fig. 3 of a dGL axiomatization that makes the overall completeness proof most straightforward. For that purpose, the dGL axiomatization in Fig. 3 uses properties $\langle c\rangle\top$ of a game symbol c, which, as a game, can impose arbitrary conditions on the state even for a trivial postcondition (the formula $\top$ is always true).

All axioms of Fig. 3, except test $\langle ?\rangle$, equational assignment $\langle{:=}\rangle_{=}$, and constant solution DS, are surjective by Lemma 20. The US requirement that no substitute of f may depend on x is important for the soundness of DS and $\langle{:=}\rangle_{=}$. Axiom $\langle ?\rangle$ is surjective, as it has no bound variables, so generates no taboos and none of its instances clash: $\sigma^{\emptyset}(\langle ?q\rangle p \leftrightarrow q \land p) = (\langle \sigma^{\emptyset}_{\emptyset} q\rangle \sigma^{\emptyset} p \leftrightarrow \sigma^{\emptyset} q \land \sigma^{\emptyset} p)$. Similarly, rule MP is surjective [16], and the other rules are surjective by Lemma 20. Other differential equation axioms are elided but work as previously [16].

Besides rule US, *bound variable renaming* (rule BR) is the only schematic principle, mostly for generalizing assignment axiom $\langle{:=}\rangle_{=}$ to other variables.

Lemma 21 (Bound renaming). *Rule BR is locally sound, where ψ_x^y is the result of uniformly renaming x to y in ψ (also x' to y' but no x'', x''' etc. or game symbols occur in ψ, where the rule BR for $[x := \theta]\psi$ is accordingly):*

$$\text{(BR)} \quad \frac{\phi \to \langle y := \theta\rangle\langle y' := x'\rangle\psi_x^y}{\phi \to \langle x := \theta\rangle\psi} \quad (y, y' \notin \psi)$$

Theorem 22 (Relative completeness). *The* dGL *calculus is a* sound and complete axiomatization *of hybrid games relative to* any *differentially expressive logic L, i.e., every valid* dGL *formula is provable in* dGL *from L tautologies.*

This completeness result assumes that no game symbols occur, because uniform renaming otherwise needs to become a syntactic operator. A logic L closed under first-order connectives is *differentially expressive* (for dGL) if every dGL formula ϕ has an equivalent $\phi^\flat$ in L and all differential equation equivalences of the form $\langle x' = \theta\rangle G \leftrightarrow (\langle x' = \theta\rangle G)^\flat$ for G in L are provable in its calculus.

4 Differential Hybrid Games

Uniform substitution generalizes from dGL for hybrid games [15] to dGL for *differential* hybrid games [17], which add differential games as a new atomic game. A *differential game* $x' = \theta \&^d y \in Y \& z \in Z$ allows Angel to control how long to follow the differential equation $x' = \theta$ (in which variables x, y, z may occur) while Demon provides a measurable input for y over time satisfying the formula $y \in Y$ always and Angel, knowing Demon's current input, provides a measurable input for z satisfying the formula $z \in Z$. All occurrences of y, z in $x' = \theta \&^d y \in Y \& z \in Z$ are bound, and $y \in Y$ and $z \in Z$ are formulas in the free variables y or z, respectively. It has been a long-standing challenge to give mathematical meaning [6,7] and sound reasoning principles [17] for differential games. Both outcomes can simply be adopted here under the usual well-definedness assumptions [17].

Uniform substitution application in Fig. 2 lifts to differential games by adding:

$$\sigma^U_{\bar{U}}(x' = \theta \&^d y \in Y \& z \in Z) = (x' = \sigma^{\bar{U}}\theta \&^d y \in \sigma^{\bar{U}} Y \& z \in \sigma^{\bar{U}} Z)$$

where $\bar{U}$ is $U \cup \{x, x', y, y', z, z'\}$. Well-definedness assumptions on differential games [17] need to hold, e.g., only first-order logic formulas denoting compact sets are allowed for controls and the differential equations need to be bounded.

As terms are unaffected by adding differential games to the syntax, Lemma 9 and 15 do not change. The proofs of the coincidence lemmas 10 and 11 and bound effect lemma 12 [18] transfer to dGL with differential hybrid games in verbatim thanks to their use of *semantically defined* free and bound variables, which carry over to differential hybrid games. The proof of Lemma 13 generalizes easily by adding a case for differential games with the above $\bar{U}$. The uniform substitution lemmas 16 and 17 inductively generalize to differential hybrid games because of:

Lemma 23 (Uniform substitution for differential games). *Let $U \subseteq \mathbf{V}$. For all U-variations ν of ω:*

$$\nu \in I[\![\sigma^U_{\bar{U}}(x' = \theta \&^d y \in Y \& z \in Z)]\!]\big(X\big) \text{ iff } \nu \in \sigma^*_\omega I[\![x' = \theta \&^d y \in Y \& z \in Z]\!]\big(X\big)$$

The proof [20] makes clever use of differential game refinements [17] to avoid the significant complexities and semantic subtleties of differential games.

5 Conclusion

This paper introduced significantly faster uniform substitution mechanisms, the dominant logical inference in axiomatic small core hybrid systems/games provers. It is also first in proving soundness of uniform substitution for differential games.

Implementations exhibit a linear runtime complexity compared to the exponential complexity that direct implementations [8] of prior Church-style uniform substitutions exhibit, except when applying aggressive space/time optimization tradeoffs where that drops down to a quadratic runtime in practice.

Acknowledgment. I thank Frank Pfenning for useful discussions and the anonymous reviewers for their helpful feedback. I appreciate the kind advice of the Isabelle group at TU Munich for the subsequent formalization [19] of the proofs.

References

1. Ahrendt, W., Beckert, B., Bubel, R., Hähnle, R., Schmitt, P.H., Ulbrich, M. (eds.): Deductive Software Verification – The KeY Book, LNCS, vol. 10001. Springer (2016). doi:10.1007/978-3-319-49812-6
2. Bohrer, B., Rahli, V., Vukotic, I., Völp, M., Platzer, A.: Formally verified differential dynamic logic. In: Bertot, Y., Vafeiadis, V. (eds.) Certified Programs and Proofs - 6th ACM SIGPLAN Conference, CPP 2017, Paris, France, January 16-17, 2017. pp. 208–221. ACM, New York (2017). doi:10.1145/3018610.3018616
3. de Bruijn, N.: Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem. Indagationes Mathematicae **75**(5), 381 – 392 (1972). doi:10.1016/1385-7258(72)90034-0
4. Church, A.: A formulation of the simple theory of types. J. Symb. Log. **5**(2), 56–68 (1940). doi:10.2307/2266170
5. Church, A.: Introduction to Mathematical Logic. Princeton University Press, Princeton (1956)
6. Elliott, R.J., Kalton, N.J.: Cauchy problems for certain Isaacs-Bellman equations and games of survival. Trans. Amer. Math. Soc. **198**, 45–72 (1974). doi:10.1090/S0002-9947-1974-0347383-8
7. Evans, L.C., Souganidis, P.E.: Differential games and representation formulas for solutions of Hamilton-Jacobi-Isaacs equations. Indiana Univ. Math. J. **33**(5), 773–797 (1984). doi:10.1512/iumj.1984.33.33040
8. Fulton, N., Mitsch, S., Quesel, J.D., Völp, M., Platzer, A.: KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In: Felty, A., Middeldorp, A. (eds.) CADE. LNCS, vol. 9195, pp. 527–538. Springer, Berlin (2015). doi:10.1007/978-3-319-21401-6_36
9. Harel, D., Kozen, D., Tiuryn, J.: Dynamic Logic. MIT Press, Cambridge (2000). doi:10.7551/mitpress/2516.001.0001
10. Henkin, L.: Banishing the rule of substitution for functional variables. J. Symb. Log. **18**(3), pp. 201–208 (1953). doi:10.2307/2267403
11. Hilbert, D., Ackermann, W.: Grundzüge der theoretischen Logik. Springer, Berlin (1928)
12. Hilbert, D., Bernays, P.: Grundlagen der Mathematik, vol. I. Springer, 2 edn. (1934)
13. Mitchell, I., Bayen, A.M., Tomlin, C.: A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. IEEE T. Automat. Contr. **50**(7), 947–957 (2005). doi:10.1109/TAC.2005.851439
14. Pfenning, F., Elliott, C.: Higher-order abstract syntax. In: Wexelblat, R.L. (ed.) PLDI. pp. 199–208. ACM (1988). doi:10.1145/53990.54010
15. Platzer, A.: Differential game logic. ACM Trans. Comput. Log. **17**(1), 1:1–1:51 (2015). doi:10.1145/2817824
16. Platzer, A.: A complete uniform substitution calculus for differential dynamic logic. J. Autom. Reas. **59**(2), 219–265 (2017). doi:10.1007/s10817-016-9385-1
17. Platzer, A.: Differential hybrid games. ACM Trans. Comput. Log. **18**(3), 19:1–19:44 (2017). doi:10.1145/3091123
18. Platzer, A.: Uniform substitution for differential game logic. In: Galmiche, D., Schulz, S., Sebastiani, R. (eds.) IJCAR. LNCS, vol. 10900, pp. 211–227. Springer (2018). doi:10.1007/978-3-319-94205-6_15
19. Platzer, A.: Differential game logic. Archive of Formal Proofs **2019** (2019), http://isa-afp.org/entries/Differential_Game_Logic.html, formal proof development

20. Platzer, A.: Uniform substitution at one fell swoop. CoRR **abs/1902.07230** (2019), http://arxiv.org/abs/1902.07230
21. Quesel, J.D., Platzer, A.: Playing hybrid games with KeYmaera. In: Gramlich, B., Miller, D., Sattler, U. (eds.) IJCAR. LNCS, vol. 7364, pp. 439–453. Springer, Berlin (2012). doi:10.1007/978-3-642-31365-3_34
22. Quine, W.V.O.: A System of Logistic. Harvard Univ. Press (1934)
23. Schneider, H.H.: Substitutions for predicate variables and functional variables. Notre Dame J. Formal Logic **21**(1), 33–44 (01 1980). doi:10.1305/ndjfl/1093882937

A Proofs

This appendix provides all proofs that are not cited or shown inline.

Proof of Lemma 13. The proof is by direct structural induction on α:

1. $\sigma^U_{U\cup\mathsf{BV}(\sigma a)}(a) = \sigma a$, then $V = U \cup \mathsf{BV}(\sigma a) = U \cup \mathsf{BV}(\sigma^U_V a)$
2. $\sigma^U_{U\cup\{x\}}(x := \theta) = (x := \sigma^U\theta)$, then $U \cup \{x\} \supseteq U \cup \mathsf{BV}(x := \sigma^U\theta)$.
3. $\sigma^U_{U\cup\{x,x'\}}(x' = \theta \,\&\, \psi) = (x' = \sigma^{U\cup\{x,x'\}}\theta \,\&\, \sigma^{U\cup\{x,x'\}}\psi)$, then it is, indeed, the case that $U \cup \{x, x'\} \supseteq U \cup \mathsf{BV}(x' = \sigma^{U\cup\{x,x'\}}\theta \,\&\, \sigma^{U\cup\{x,x'\}}\psi)$.
4. $\sigma^U_U(?\psi) = ?\sigma^U\psi$, then output U is correct as $\mathsf{BV}(?\sigma^U\psi) = \emptyset$.
5. $\sigma^U_{V\cup W}(\alpha \cup \beta) = \sigma^U_V\alpha \cup \sigma^U_W\beta$, then, by IH, $V \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha)$ and $W \supseteq U \cup \mathsf{BV}(\sigma^U_W\beta)$. Thus, $V \cup W \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha) \cup U \cup \mathsf{BV}(\sigma^U_W\beta) \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha \cup \sigma^U_W\beta)$.
6. $\sigma^U_W(\alpha;\beta) = \sigma^U_V\alpha; \sigma^V_W\beta$ then, by IH, $V \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha)$ and $W \supseteq V \cup \mathsf{BV}(\sigma^V_W\beta)$. Hence, $W \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha) \cup \mathsf{BV}(\sigma^V_W\beta) \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha; \sigma^V_W\beta)$.
7. $\sigma^U_V(\alpha^*) = (\sigma^V_V\alpha)^*$ if $\sigma^U_V\alpha$ is defined. By IH on $\sigma^U_V\alpha$, $V \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha)$. By IH on $\sigma^V_V\alpha$, $V \supseteq \mathsf{BV}(\sigma^V_V\alpha)$. Hence, $V \supseteq U \cup \mathsf{BV}((\sigma^V_V\alpha)^*)$ as $\mathsf{BV}(\alpha) \supseteq \mathsf{BV}(\alpha^*)$ for all games α.
8. $\sigma^U_V(\alpha^d) = (\sigma^U_V\alpha)^d$, then, by IH, $V \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha)$. So, $V \supseteq U \cup \mathsf{BV}((\sigma^U_V\alpha)^d) \supseteq U \cup \mathsf{BV}(\sigma^U_V\alpha)$. □

Proof of Lemma 15. The proof is by structural induction lexicographically on the structure of σ and of θ, for all U, ν, ω. Fix any U-variation ν of ω.

1. $I\nu[\![\sigma^U x]\!] = I\nu[\![x]\!] = \nu(x) = \sigma^*_\omega I\nu[\![x]\!]$ since σ changes no variables $x \in \mathbf{V}$
2. Consider the arity zero case of function application, written $f()$ for emphasis: $I\nu[\![\sigma^U(f())]\!] = I\nu[\![\sigma f()]\!]$, which, by Lemma 9, equals $I\omega[\![\sigma f()]\!] = \sigma^*_\omega I(f) = \sigma^*_\omega I\nu[\![f()]\!]$, because ν is a U-variation of ω and $\mathsf{FV}(\sigma f()) \cap U = \emptyset$.
3. Let $d \overset{\text{def}}{=} I\nu[\![\sigma^U\theta]\!] \overset{\text{IH}}{=} \sigma^*_\omega I\nu[\![\theta]\!]$ by IH. $I\nu[\![\sigma^U(f(\theta))]\!] = I\nu[\![(\sigma^U f)(\sigma^U\theta)]\!] = I\nu[\![\{\cdot \mapsto \sigma^U\theta\}^\emptyset \sigma f(\cdot)]\!] \overset{\text{IH}}{=} I^d_\cdot\nu[\![\sigma f(\cdot)]\!]$, which equals $I^d_\cdot\omega[\![\sigma f(\cdot)]\!] = (\sigma^*_\omega I(f))(d)$ by Lemma 9 since ν is a U-variation of ω and $\mathsf{FV}(\sigma f(\cdot)) \cap U = \emptyset$. Continuing, $(\sigma^*_\omega I(f))(d) = (\sigma^*_\omega I(f))(\sigma^*_\omega I\nu[\![\theta]\!]) = \sigma^*_\omega I\nu[\![f(\theta)]\!]$.

   This proof used the induction hypothesis twice: once for $\sigma^U\theta$ on the smaller θ and once for $\{\cdot \mapsto \sigma^U\theta\}^\emptyset \sigma f(\cdot)$ on the possibly bigger term $\sigma f(\cdot)$ but the structurally simpler uniform substitution $\{\cdot \mapsto \sigma^U\theta\}$ that substitutes arity 0 symbol $\cdot$ instead of arity 1 function symbol f. For well-foundedness of the induction note that the $\cdot$ substitution only happens for function symbols

f with at least one argument θ so not for $\cdot$ itself, which, as an arity zero function, is covered in case 2.

4. $I\nu\llbracket\sigma^U(\theta+\eta)\rrbracket = I\nu\llbracket\sigma^U\theta+\sigma^U\eta\rrbracket = I\nu\llbracket\sigma^U\theta\rrbracket + I\nu\llbracket\sigma^U\eta\rrbracket \overset{\text{IH}}{=} \sigma^*_\omega I\nu\llbracket\theta\rrbracket + \sigma^*_\omega I\nu\llbracket\eta\rrbracket = \sigma^*_\omega I\nu\llbracket\theta+\eta\rrbracket$. The proof for multiplication $\theta\cdot\eta$ is accordingly.
5. $I\nu\llbracket\sigma^U((\theta)')\rrbracket = I\nu\llbracket(\sigma^{\mathbf{V}}\theta)'\rrbracket = \sum_x \nu(x')\frac{\partial I\nu\llbracket\sigma^{\mathbf{V}}\theta\rrbracket}{\partial x} \overset{\text{IH}}{=} \sum_x \nu(x')\frac{\partial \sigma^*_\omega I\nu\llbracket\theta\rrbracket}{\partial x}$ which is $\sigma^*_\omega I\nu\llbracket(\theta)'\rrbracket$ since IH yields $I\nu\llbracket\sigma^{\mathbf{V}}\theta\rrbracket = \sigma^*_\omega I\nu\llbracket\theta\rrbracket$ for all states ν,ω (which are trivially $\mathbf{V}$-variations), including states used for partial derivatives. □

Proof of Lemma 16. The proof is by structural induction lexicographically on the structure of σ and of ϕ, with a simultaneous induction with the subsequent proof of Lemma 17, simultaneously for all U,ν,ω. Fix any U-variation ν of ω.

1. $\nu \in I\llbracket\sigma^U(\theta\geq\eta)\rrbracket = I\llbracket\sigma^U\theta\geq\sigma^U\eta\rrbracket$ iff $I\nu\llbracket\sigma^U\theta\rrbracket \geq I\nu\llbracket\sigma^U\eta\rrbracket$, by Lemma 15, iff $\sigma^*_\omega I\nu\llbracket\theta\rrbracket \geq \sigma^*_\omega I\nu\llbracket\eta\rrbracket$ iff $\nu\in\sigma^*_\omega I\llbracket\theta\geq\eta\rrbracket$.
2. Consider a predicate symbol q that is not substituted to anything else by σ: $\nu\in I\llbracket\sigma^U(q(\theta))\rrbracket = I\llbracket q(\sigma^U\theta)\rrbracket$ iff $I\nu\llbracket\sigma^U\theta\rrbracket \in I(q)$ iff, by Lemma 15, $\sigma^*_\omega I\nu\llbracket\sigma^U\theta\rrbracket\in I(q)$ iff $\sigma^*_\omega I\nu\llbracket\sigma^U\theta\rrbracket\in\sigma^*_\omega I(q)$ iff $\nu\in\sigma^*_\omega I\llbracket q(\theta)\rrbracket$
3. Let $d \overset{\text{def}}{=} I\nu\llbracket\sigma^U\theta\rrbracket = \sigma^*_\omega I\nu\llbracket\theta\rrbracket$ by Lemma 15 since ν is a U-variation of ω. $\nu\in I\llbracket\sigma^U(p(\theta))\rrbracket = I\llbracket(\sigma^U p)\big(\sigma^U\theta\big)\rrbracket = I\llbracket\{\cdot\mapsto\sigma^U\theta\}^{\emptyset}\sigma p(\cdot)\rrbracket$ iff $\nu\in I_{\cdot}^{d}\llbracket\sigma p(\cdot)\rrbracket$ by IH, iff $\omega\in I_{\cdot}^{d}\llbracket\sigma p(\cdot)\rrbracket$ by Lemma 10 as ν is a U-variation of ω and $\mathsf{FV}(\sigma p(\cdot))\cap U=\emptyset$, iff $d\in\sigma^*_\omega I(p)$ iff $(\sigma^*_\omega I\nu\llbracket\theta\rrbracket)\in\sigma^*_\omega I(p)$ iff $\nu\in\sigma^*_\omega I\llbracket p(\theta)\rrbracket$. The IH for $\{\cdot\mapsto\sigma^U\theta\}^{\emptyset}\sigma p(\cdot)$ is used on the possibly bigger formula $\sigma p(\cdot)$ but the structurally simpler uniform substitution $\{\cdot\mapsto\sigma^U\theta\}$ only substitutes function symbol $\cdot$ of arity zero, not predicates, thus is covered by case 2.
4. $\nu\in I\llbracket\sigma^U(\neg\phi)\rrbracket = I\llbracket\neg\sigma^U\phi\rrbracket$ iff $\nu\notin I\llbracket\sigma^U\phi\rrbracket$ by IH iff $\nu\notin\sigma^*_\omega I\llbracket\phi\rrbracket$ iff $\nu\in\sigma^*_\omega I\llbracket\neg\phi\rrbracket$
5. $\nu\in I\llbracket\sigma^U(\phi\wedge\psi)\rrbracket = I\llbracket\sigma^U\phi\wedge\sigma^U\psi\rrbracket = I\llbracket\sigma^U\phi\rrbracket\cap I\llbracket\sigma^U\psi\rrbracket$, by induction hypothesis, iff $\nu\in\sigma^*_\omega I\llbracket\phi\rrbracket\cap\sigma^*_\omega I\llbracket\psi\rrbracket = \sigma^*_\omega I\llbracket\phi\wedge\psi\rrbracket$
6. $\nu\in I\llbracket\sigma^U(\exists x\,\phi)\rrbracket = I\llbracket\exists x\,\sigma^{U\cup\{x\}}\phi\rrbracket$ iff for some d $\nu_x^d\in I\llbracket\sigma^{U\cup\{x\}}\phi\rrbracket$, so, by IH, iff (for some d for any $(U\cup\{x\})$-variation ν_x^d of ω: $\nu_x^d\in\sigma^*_\omega I\llbracket\phi\rrbracket$), iff (for some d for any U-variation ν of ω: $\nu_x^d\in\sigma^*_\omega I\llbracket\phi\rrbracket$), Thus, this is equivalent to $\nu\in\sigma^*_\omega I\llbracket\exists x\,\phi\rrbracket$, because ν, indeed, is a U-variation of ω.
7. $\nu\in I\llbracket\sigma^U(\langle\alpha\rangle\phi)\rrbracket = I\llbracket\langle\sigma^U_V\alpha\rangle\sigma^V\phi\rrbracket = I\llbracket\sigma^U_V\alpha\rrbracket\big(I\llbracket\sigma^V\phi\rrbracket\big)$ iff (by Lemma 12) $\nu\in I\llbracket\sigma^U_V\alpha\rrbracket\big(I\llbracket\sigma^V\phi\rrbracket\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^\complement)\big)$. Conversely: $\nu\in\sigma^*_\omega I\llbracket\langle\alpha\rangle\phi\rrbracket = \sigma^*_\omega I\llbracket\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\phi\rrbracket\big)$ iff (by Lemma 17) $\nu\in I\llbracket\sigma^U_V\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\phi\rrbracket\big)$ as $\sigma^U_V\alpha$ is defined and ν a U-variation of ω, iff (Lemma 12) $\nu\in I\llbracket\sigma^U_V\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\phi\rrbracket\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^\complement)\big)$. The conditions equate

   $$I\llbracket\sigma^V\phi\rrbracket\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^\complement) = \sigma^*_\omega I\llbracket\phi\rrbracket\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^\complement)$$

   For this, consider any $\mathsf{BV}(\sigma^U_V\alpha)$-variation μ of ν and show: $\mu\in\sigma^*_\omega I\llbracket\phi\rrbracket$ iff $\mu\in I\llbracket\sigma^V\phi\rrbracket$. By induction hypothesis, the latter is equivalent to $\mu\in\sigma^*_\omega I\llbracket\phi\rrbracket$ when μ is a V-variation of ω, which it is, because μ is a $\mathsf{BV}(\sigma^U_V\alpha)$-variation of ν, which is, in turn, a U-variation of ω, so μ is a $(U\cup\mathsf{BV}(\sigma^U_V\alpha))$-variation of ω, hence also a V-variation, because $V\supseteq U\cup\mathsf{BV}(\sigma^U_V\alpha)$ by Lemma 13. □

Proof of Lemma 17. The proof is by lexicographic structural induction on σ and α, simultaneously with Lemma 16, for all U,ν,ω and X. Fix any U-variation ν of ω.

1. $\nu \in I\llbracket\sigma^U_{U\cup\mathsf{BV}(\sigma a)}(a)\rrbracket\big(X\big) = I\llbracket\sigma a\rrbracket\big(X\big) = \sigma^*_\omega I(a)(X) = \sigma^*_\omega I\llbracket a\rrbracket\big(X\big)$ for game a
2. $\nu \in I\llbracket\sigma^U_{U\cup\{x\}}(x:=\theta)\rrbracket\big(X\big) = I\llbracket x:=\sigma^U\theta\rrbracket\big(X\big)$ iff $X \ni \nu_x^{I\nu\llbracket\sigma^U\theta\rrbracket} = \nu_x^{\sigma^*_\omega I\nu\llbracket\theta\rrbracket}$ by Lemma 15, which is, thus, equivalent to $\nu \in \sigma^*_\omega I\llbracket x:=\theta\rrbracket\big(X\big)$.
3. $\nu \in I\llbracket\sigma^U_{U\cup\{x,x'\}}(x'=\theta\,\&\,\psi)\rrbracket\big(X\big) = I\llbracket x'=\sigma^{U\cup\{x,x'\}}\theta\,\&\,\sigma^{U\cup\{x,x'\}}\psi\rrbracket\big(X\big)$ iff $\exists\varphi:[0,T]\to\mathcal{S}$ such that $\varphi(0)=\nu$ on $\{x'\}^{\complement}$, $\varphi(T)\in X$ and for all $t\geq 0$: $\frac{\mathsf{d}\varphi(s)(x)}{\mathsf{d}s}(t) = I\varphi(t)\llbracket\sigma^{U\cup\{x,x'\}}\theta\rrbracket = \sigma^*_\omega I\varphi(t)\llbracket\theta\rrbracket$ by Lemma 15 and it also holds that $\varphi(t)\in I\llbracket\sigma^{U\cup\{x,x'\}}\psi\rrbracket$, which, by Lemma 16, holds iff $\varphi(t)\in\sigma^*_\omega I\llbracket\psi\rrbracket$. Here, Lemma 15 and 16 are applicable, because $\varphi(t)$ is a $(U\cup\{x,x'\})$-variation of ω, since $\varphi(t)$ is a $\{x,x'\}$-variation of ν, which is a U-variation of ω. The latter two conditions are equivalent to $\nu\in\sigma^*_\omega I\llbracket x'=\theta\,\&\,\psi\rrbracket\big(X\big)$.
4. $\nu \in I\llbracket\sigma^U_U(?\psi)\rrbracket\big(X\big) = I\llbracket ?\sigma^U\psi\rrbracket\big(X\big) = I\llbracket\sigma^U\psi\rrbracket\cap X$ iff, by Lemma 16, $\nu \in \sigma^*_\omega I\llbracket\psi\rrbracket\cap X = \sigma^*_\omega I\llbracket ?\psi\rrbracket\big(X\big)$.
5. $\nu \in I\llbracket\sigma^U_{V\cup W}(\alpha\cup\beta)\rrbracket\big(X\big) = I\llbracket\sigma^U_V\alpha\cup\sigma^U_W\beta\rrbracket\big(X\big) = I\llbracket\sigma^U_V\alpha\rrbracket\big(X\big)\cup I\llbracket\sigma^U_W\beta\rrbracket\big(X\big)$, which, by IH, is equivalent to $\nu\in\sigma^*_\omega I\llbracket\alpha\rrbracket\big(X\big)\cup\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big) = \sigma^*_\omega I\llbracket\alpha\cup\beta\rrbracket\big(X\big)$.
6. $\nu \in I\llbracket\sigma^U_W(\alpha;\beta)\rrbracket\big(X\big) = I\llbracket\sigma^U_V\alpha;\sigma^V_W\beta\rrbracket\big(X\big) = I\llbracket\sigma^U_V\alpha\rrbracket\big(I\llbracket\sigma^V_W\beta\rrbracket\big(X\big)\big)$ iff, by Lemma 12, $\nu \in I\llbracket\sigma^U_V\alpha\rrbracket\big(I\llbracket\sigma^V_W\beta\rrbracket\big(X\big)\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^{\complement})\big)$. Starting conversely: $\nu\in\sigma^*_\omega I\llbracket\alpha;\beta\rrbracket\big(X\big) = \sigma^*_\omega I\llbracket\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)\big)$, iff, by IH, $\nu\in I\llbracket\sigma^U_V\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)\big)$ iff, by Lem. 12, $\nu\in I\llbracket\sigma^U_V\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^{\complement})\big)$. Both conditions equate:

   $$I\llbracket\sigma^V_W\beta\rrbracket\big(X\big)\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^{\complement}) = \sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)\downarrow\nu(\mathsf{BV}(\sigma^U_V\alpha)^{\complement})$$

   Consider any $\mathsf{BV}(\sigma^U_V\alpha)$-variation μ of ν to show: $\mu\in I\llbracket\sigma^V_W\beta\rrbracket\big(X\big)$ iff $\mu\in\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)$. This holds by IH, because μ is a V-variation of ω: μ is a $\mathsf{BV}(\sigma^U_V\alpha)$-variation of ν, which, in turn, is a U-variation of ω, so μ is a $(U\cup\mathsf{BV}(\sigma^U_V\alpha))$-variation of ω, hence a V-variation by Lemma 13.
7. The case $\nu\in I\llbracket\sigma^U_V(\alpha^*)\rrbracket\big(X\big) = I\llbracket(\sigma^V_V\alpha)^*\rrbracket\big(X\big)$ (when $\sigma^V_U\alpha$ is defined) uses an equivalent inflationary fixpoint formulation [15, Thm. 3.5]:

   $$\begin{aligned} \tau^0(X) &\overset{\text{def}}{=} X \\ \tau^{\kappa+1}(X) &\overset{\text{def}}{=} X\cup I\llbracket\sigma^V_V\alpha\rrbracket\big(\tau^\kappa(X)\big) && \kappa+1 \text{ a successor ordinal} \\ \tau^\lambda(X) &\overset{\text{def}}{=} \bigcup_{\kappa<\lambda}\tau^\kappa(X) && \lambda\neq 0 \text{ a limit ordinal} \end{aligned}$$

   where the union $\tau^\infty(X) = \bigcup_{\kappa<\infty}\tau^\kappa(X)$ over all ordinals is $I\llbracket(\sigma^V_V\alpha)^*\rrbracket\big(X\big)$. A similar fixpoint works for the other side $\sigma^*_\omega I\llbracket\alpha^*\rrbracket\big(X\big) = \varrho^\infty(X)$ where:

   $$\varrho^{\kappa+1}(X) \overset{\text{def}}{=} X\cup\sigma^*_\omega I\llbracket\alpha\rrbracket\big(\varrho^\kappa(X)\big) \qquad \kappa+1 \text{ a successor ordinal}$$

   The equivalence $\nu\in I\llbracket\sigma^V_V(\alpha^*)\rrbracket\big(X\big) = \tau^\infty(X)$ iff $\nu\in\sigma^*_\omega I\llbracket\alpha^*\rrbracket\big(X\big) = \varrho^\infty(X)$ for all U-variations ν of ω follows, with $V\supseteq U$ by Lemma 13, from proving:

   $$\text{for all } \kappa \text{ and all } X \text{ and all } V\text{-variations } \nu \text{ of } \omega:\ \nu\in\tau^\kappa(X) \text{ iff } \nu\in\varrho^\kappa(X)$$

   This is proved by induction on ordinal κ (0, limit ordinal $\lambda\neq 0$, or successor):

$\kappa = 0$: $\nu \in \tau^0(X)$ iff $\nu \in \varrho^0(X)$, because both sets equal X.

λ: $\nu \in \tau^\lambda(X) = \bigcup_{\kappa<\lambda} \tau^\kappa(X)$ iff there is a $\kappa < \lambda$ such that $\nu \in \tau^\kappa(X)$ iff, by IH, $\nu \in \varrho^\kappa(X)$ for some $\kappa < \lambda$, iff $\nu \in \bigcup_{\kappa<\lambda} \varrho^\kappa(X) = \varrho^\lambda(X)$.

$\kappa+1$: $\nu \in \tau^{\kappa+1}(X) = X \cup I[\![\sigma_V^V\alpha]\!]\big(\tau^\kappa(X)\big)$, is equivalent, by Lemma 12, to $\nu \in X \cup I[\![\sigma_V^V\alpha]\!]\big(\tau^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma_V^V\alpha)^\complement)\big)$. Conversely, $\nu \in \varrho^{\kappa+1}(X) = X \cup \sigma_\omega^* I[\![\alpha]\!]\big(\varrho^\kappa(X)\big)$ iff, by IH on α, $\nu \in X \cup I[\![\sigma_V^V\alpha]\!]\big(\varrho^\kappa(X)\big)$ for any V-variations ν of ω, iff, by Lemma 12, $\nu \in X \cup I[\![\sigma_V^V\alpha]\!]\big(\varrho^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma_V^V\alpha)^\complement)\big)$. Now $\tau^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma_V^V\alpha)^\complement) = \varrho^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma_V^V\alpha)^\complement)$ holds as follows. Consider any $\mathsf{BV}(\sigma_V^V\alpha)$-variation μ of ν and show: $\mu \in \tau^\kappa(X)$ iff $\mu \in \varrho^\kappa(X)$, which is by IH on $\kappa < \kappa+1$, as μ is a V-variation of ω: μ is a $\mathsf{BV}(\sigma_V^V\alpha)$-variation of ν, so by $V \supseteq \mathsf{BV}(\sigma_V^V\alpha)$ from Lemma 13, μ is a V-variation of ν, which, in turn, is a U-variation of ω, hence, by $V \supseteq U$ from Lemma 13 as $\sigma_V^U\alpha$ is defined, also a V-variation of ω, so μ itself is a V-variation of ω.

8. $\nu \in I[\![\sigma_V^U(\alpha^d)]\!]\big(X\big) = I[\![(\sigma_V^U\alpha)^d]\!]\big(X\big) = \big(I[\![\sigma_V^U\alpha]\!]\big(X^\complement\big)\big)^\complement$ iff $\nu \notin I[\![\sigma_V^U\alpha]\!]\big(X^\complement\big)$, iff, by IH, $\nu \notin \sigma_\omega^* I[\![\alpha]\!]\big(X^\complement\big)$, iff $\nu \in \big(\sigma_\omega^* I[\![\alpha]\!]\big(X^\complement\big)\big)^\complement = \sigma_\omega^* I[\![\alpha^d]\!]\big(X\big)$. □

Proof of Lemma 20. Let $\tilde\phi$ be the desired instance of schema ϕ. So, $\tilde\phi$ is obtained from ϕ by uniformly replacing each game symbol a by some hybrid game, naïvely but consistently (same replacement for a in all places). A straightforward structural induction on ϕ proves that there is a uniform substitution σ such that $\sigma^{\mathbf{V}}\phi = \tilde\phi$ simultaneously with showing for games α with desired instance $\tilde\alpha$ that there is a uniform substitution σ such that $\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha = \tilde\alpha$. The output taboo W of $\sigma^{\mathbf{V}}_{W}\alpha$ equals $\mathbf{V}$ by Lemma 13, because all variables $\mathbf{V}$ are already input taboos. Nothing needs to be shown for terms as game symbols cannot occur in terms.

1. Case $\phi \wedge \psi$ with desired instance $\tilde\phi \wedge \tilde\psi$ (which has to have this shape to qualify as a schema instance). By IH, there are substitutions σ, τ such that $\sigma^{\mathbf{V}}\phi = \tilde\phi$ and $\tau^{\mathbf{V}}\psi = \tilde\psi$. The union $\phi \cup \psi$ is defined, because the same replacements have been used consistently in all occurrences of the instantiation. Thus, $(\sigma\cup\tau)^{\mathbf{V}}(\phi \wedge \psi) = (\sigma\cup\tau)^{\mathbf{V}}\phi \wedge (\sigma\cup\tau)^{\mathbf{V}}\psi = \sigma^{\mathbf{V}}\phi \wedge \tau^{\mathbf{V}}\psi = \tilde\phi \wedge \tilde\psi$ as desired. The proof is accordingly for $\neg$ etc.
2. Case $\exists x\, \phi$ with desired instance $\exists x\, \tilde\phi$. By IH, there is a substitution σ such that $\sigma^{\mathbf{V}}\phi = \tilde\phi$. Thus, $\sigma^{\mathbf{V}}(\exists x\, \phi) = \exists x\, \sigma^{\mathbf{V}\cup\{x\}}\phi = \exists x\, \sigma^{\mathbf{V}}\phi = \exists x\, \tilde\phi$ as desired.
3. Case $\langle\alpha\rangle\phi$ with desired instance $\langle\tilde\alpha\rangle\tilde\phi$. By IH, there are substitutions σ, τ such that $\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha = \tilde\alpha$ and $\tau^{\mathbf{V}}\phi = \tilde\phi$. Thus, the union $\sigma \cup \tau$ is defined and $(\sigma\cup\tau)^{\mathbf{V}}(\langle\alpha\rangle\psi) = \langle(\sigma\cup\tau)^{\mathbf{V}}_{\mathbf{V}}\alpha\rangle(\sigma\cup\tau)^{\mathbf{V}}\phi = \langle\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha\rangle\tau^{\mathbf{V}}\phi = \langle\tilde\alpha\rangle\tilde\phi$ as desired.
4. Case a of a game symbol with desired instance $\tilde\alpha$ is handled with the substitution $\sigma = \{a \mapsto \tilde\alpha\}$, which satisfies $\sigma^{\mathbf{V}}_{\mathbf{V}}a = \sigma a = \tilde\alpha$ as desired.
5. Case $x' = \theta \,\&\, \psi$ with desired instance $x' = \tilde\theta \,\&\, \tilde\psi$. By IH, there are substitutions σ, τ such that $\sigma^{\mathbf{V}}\theta = \tilde\theta$ and $\tau^{\mathbf{V}}\psi = \tilde\psi$. Thus, the union $\sigma \cup \tau$ is defined and $(\sigma\cup\tau)^{\mathbf{V}}\theta = \sigma^{\mathbf{V}}\theta = \tilde\theta$ and $(\sigma\cup\tau)^{\mathbf{V}}\psi = \tau^{\mathbf{V}}\psi = \tilde\psi$, hence, $(\sigma\cup\tau)^{\mathbf{V}}(x' = \theta \,\&\, \psi) = (x' = \tilde\theta \,\&\, \tilde\psi)$ as desired.
6. Case $\alpha \cup \beta$ with desired instance $\tilde\alpha \cup \tilde\beta$. By IH there are substitutions σ, τ such that $\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha = \tilde\alpha$ and $\tau^{\mathbf{V}}_{\mathbf{V}}\beta = \tilde\beta$. Thus, the union $\sigma \cup \tau$ is defined and

$(\sigma\cup\tau)^{\mathbf{V}}(\alpha\cup\beta) = (\sigma\cup\tau)^{\mathbf{V}}_{\mathbf{V}}\alpha \cup (\sigma\cup\tau)^{\mathbf{V}}_{\mathbf{V}}\beta = \sigma^{\mathbf{V}}_{\mathbf{V}}\alpha \cup \tau^{\mathbf{V}}_{\mathbf{V}}\beta = \tilde{\alpha}\cup\tilde{\beta}$ using that $\mathbf{V} = \mathbf{V}\cup\mathbf{V}$.

7. Case $\alpha;\beta$ with desired instance $\tilde{\alpha};\tilde{\beta}$. By IH there are substitutions σ,τ such that $\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha = \tilde{\alpha}$ and $\tau^{\mathbf{V}}_{\mathbf{V}}\beta = \tilde{\beta}$. Thus, the union $\sigma\cup\tau$ is defined and $(\sigma\cup\tau)^{\mathbf{V}}(\alpha;\beta) = (\sigma\cup\tau)^{\mathbf{V}}_{\mathbf{V}}\alpha;(\sigma\cup\tau)^{\mathbf{V}}_{\mathbf{V}}\beta = \sigma^{\mathbf{V}}_{\mathbf{V}}\alpha;\tau^{\mathbf{V}}_{\mathbf{V}}\beta = \tilde{\alpha};\tilde{\beta}$ as desired.
8. Case α^* with desired instance $\tilde{\alpha}^*$. By IH there is a substitution σ such that $\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha = \tilde{\alpha}$. Thus, $\sigma^{\mathbf{V}}(\alpha^*) = (\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha)^* = \tilde{\alpha}^*$ as desired, because $\sigma^{\mathbf{V}}_{\mathbf{V}}\alpha$ is defined.

Case α^d is accordingly. Axiomatic proof rules built from surjective formulas are surjective, because USR can instantiate the rule to any instance as long as US can instantiate all premises and the conclusion to any instance. □

Proof of Lemma 21. This proof is the only one using that no higher-order differential variables $x^{(i)}$ for $i \geq 2$ occur. It also assumes that no game symbols a occur, because a_x^y has no syntactic representation. Local soundness follows from:

$$\langle x := \theta\rangle\psi \leftrightarrow \langle y := \theta\rangle\langle y' := x'\rangle\psi_x^y \quad (y, y' \notin \psi)$$

Consider any state ω in which to show this equivalence. Then $\omega \in I[\![\langle x := \theta\rangle\psi]\!]$ iff $\omega_x^{I\omega[\![\theta]\!]} \in I[\![\psi]\!]$ iff, by ($*$) below, $\omega_y^{I\omega[\![\theta]\!]}{}_{y'}^{\omega(x')} \in I[\![\psi_x^y]\!]$ iff $\omega \in I[\![\langle y := \theta\rangle\langle y' := x'\rangle\psi_x^y]\!]$. The values of x, x' are irrelevant for ψ_x^y by Lemma 10. No $y^{(i)}$ for $i \geq 2$ occur. It uses a fact about uniform renaming of $x^{(i)}$ to $y^{(i)}$ and vice versa, for all i:

$$\omega \in I[\![\psi]\!] \text{ iff } \omega_{x^{(i)}}^{\omega(y^{(i)})}{}_{y^{(i)}}^{\omega(x^{(i)})} \in I[\![\psi_x^y]\!] \text{ where the state is modified for all } i \quad (*)$$

Property ($*$) is proved by straightforward induction on the structure of ψ using that x and x' etc. are consistently swapped with y and y' etc. syntactically in the uniformly renamed formula ψ_x^y as well as semantically in the state. □

Proof of Theorem 22. The axioms and axiomatic rules in Fig. 3 are concrete instances of sound schemata or rules from prior work [15,16] except for a slight modification in axiom DS, which is sound, because the effect of a differential equation $x' = f$ on x' is that its value equals f while following the ODE.

The completeness proof is by induction on a well-founded partial order $\prec$ induced by the lexicographic ordering of the overall structural complexity of the hybrid games in the formula and the structural complexity of the formula itself, with the logic L placed at the bottom of the partial order [15]. Even if all axioms and rules in Fig. 3 except $\langle{:=}\rangle_=$,DS are surjective by Lemma 20, most do not have the form used in the schematic completeness result for dGL [15, Thm. 4.5]. All required schematic instances of all axioms (except assignments) for that completeness result can, nevertheless, be obtained by instantiating game symbol c to the test game $?\psi$ for the desired instance ψ, which is possible by Lemma 20. Uniform substitution then turns each respective occurrence of $\langle c\rangle\top$ into $\langle ?\psi\rangle\top$, which an additional use of surjective axiom $\langle ?\rangle$ turns into $\psi \wedge \top$, which first-order logic equivalences in L simplify to the desired ψ.

For example, consider the representative case $\vDash F \rightarrow \langle\beta^d\rangle G$, which implies $\vDash F \rightarrow \neg\langle\beta\rangle\neg G$, which implies $\vDash F \rightarrow [\beta]G$. Since $[\beta]G \prec \langle\beta^d\rangle G$, because β^d is more complex than β even if the modality changed, $\vdash_L F \to [\beta]G$ can be derived by IH. Axiom [$\cdot$], thus, derives $\vdash_L F \to \neg\langle\beta\rangle\neg G$, from which, with Lemma 20 and the above observations about axiom $\langle ? \rangle$, axiom $\langle ^d \rangle$ derives $\vdash_L F \to \langle\beta^d\rangle G$.

Thus, Lemma 20 makes the previous completeness proof [15, Thm. 4.5] with the uniform substitution relative completeness refinements [16, Thm. 40] transfer to Fig. 3, but only if all uses of the assignment axiom, which is not surjective, can be patched. The only such case is in the proof that $\vDash F \to \langle x := \theta\rangle G$ implies that this formula can be proved in the dGL calculus from L, which, because of the different axioms, works differently than the corresponding case of $\vDash F \to [x := \theta]G$ in the completeness proof for dL [16, Thm. 40].

If $\vDash F \to \langle y := \theta\rangle G$, then this formula can be proved, using a fresh variable x not occurring in θ or G, with the following derivation by renaming (Lemma 21)

$$\begin{array}{rl}
 & F \to \exists x\,(x = \theta \land \exists x'\,(x' = y' \land G\tfrac{x}{y})) \\ \cline{2-2}
\langle := \rangle_= & F \to \exists x\,(x = \theta \land \langle x' := y'\rangle G\tfrac{x}{y}) \\ \cline{2-2}
\langle := \rangle_= & F \to \langle x := \theta\rangle\langle x' := y'\rangle G\tfrac{x}{y} \\ \cline{2-2}
\text{BR} & F \to \langle y := \theta\rangle G
\end{array}$$

In the above proof, the two instantiations of axiom $\langle := \rangle_=$ succeed, because x and x' are fresh, so do not occur in either θ or y'. The above proof only used equivalence transformations, so its premise is valid iff its conclusion is, which it is by assumption, so implies $\vDash F \to \exists x\,(x = \theta \land \exists x'\,(x' = y' \land G\frac{x}{y}))$. Since $\big(F \to \exists x\,(x = \theta \land \exists x'\,(x' = y' \land G\frac{x}{y}))\big) \prec (F \to \langle y := \theta\rangle G)$, because there are less hybrid games, $\vdash_L F \to \exists x\,(x = \theta \land \exists x'\,(x' = y' \land G\frac{x}{y}))$ by IH. The above proof, thus, derives $\vdash_L F \to \langle y := \theta\rangle G$. For later, also note the derivability of:

$$G \leftrightarrow \langle x := x\rangle G \tag{3}$$

Since it is valid, this stuttering identity derives with an additional derivation of the converse $\langle x := x\rangle G \to G$. That follows from similarly deriving $\langle x := x\rangle G \to F$ by contraposition like above with a fresh x if $\vDash \langle x := x\rangle G \to F$:

$$\begin{array}{rl}
 & \neg F \to \neg\exists x\,(x = \theta \land \exists x'\,(x' = y' \land G\tfrac{x}{y})) \\ \cline{2-2}
\langle := \rangle_= & \neg F \to \neg\exists x\,(x = \theta \land \langle x' := y'\rangle G\tfrac{x}{y}) \\ \cline{2-2}
\langle := \rangle_= & \neg F \to \neg\langle x := \theta\rangle\langle x' := y'\rangle G\tfrac{x}{y} \\ \cline{2-2}
[\cdot] & \neg F \to [x := \theta][x' := y']\neg G\tfrac{x}{y} \\ \cline{2-2}
\text{BR} & \neg F \to [y := \theta]\neg G \\ \cline{2-2}
[\cdot] & \neg F \to \neg\langle y := \theta\rangle G \\ \cline{2-2}
 & \langle y := \theta\rangle G \to F
\end{array}$$

A final subtlety arises in the case of diamond properties of loops [16]. Let $\vDash F \to \langle\beta^*\rangle G$. Let x be the (*finite!*) vector of free variables $\mathrm{FV}(\langle\beta^*\rangle G)$. Since $\langle\beta^*\rangle G$ is a least pre-fixpoint [15], for all dGL formulas ψ with $\mathrm{FV}(\psi) \subseteq \mathrm{FV}(\langle\beta^*\rangle G)$:

$$\vDash \forall x\,(G \lor \langle\beta\rangle\psi \to \psi) \to (\langle\beta^*\rangle G \to \psi)$$

In particular, this holds for a fresh predicate symbol p with arguments x:

$$\vDash \forall x\, (G \lor \langle\beta\rangle p(x) \to p(x)) \to (\langle\beta^*\rangle G \to p(x))$$

Using $\vDash F \to \langle\beta^*\rangle G$, this implies

$$\vDash \forall x\, (G \lor \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))$$

As $(\forall x\, (G \lor \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))) \prec \phi$, because, even if the formula complexity increased, the structural complexity of the games decreased, since ϕ has one more repetition, this fact is derivable by IH:

$$\vdash_L \forall x\, (G \lor \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))$$

The uniform substitution $\sigma = \{p(\cdot) \mapsto \langle x := \cdot\rangle\langle\beta^*\rangle G\}$ does not clash since $\mathrm{FV}(\langle\beta^*\rangle G) \subseteq \{x\}$. Since p does not occur in F, G or β, rule US derives:

$$\dfrac{\text{US}\;\dfrac{\forall x\, (G \lor \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))}{\forall x\, (G \lor \langle\beta\rangle\langle x := x\rangle\langle\beta^*\rangle G \to \langle x := x\rangle\langle\beta^*\rangle G) \to (F \to \langle x := x\rangle\langle\beta^*\rangle G)}}{\forall x\, (G \lor \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G) \to (F \to \langle\beta^*\rangle G)}$$

where the last inference used the derivable stuttering identity (3) three times. The iteration axiom $\langle^*\rangle$ with Lemma 20 completes this derivation:

$$\text{MP}\;\dfrac{\forall x\, (G \lor \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G) \to (F \to \langle\beta^*\rangle G) \qquad \forall\;\dfrac{\langle^*\rangle\;\dfrac{*}{G \lor \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G}}{\forall x\, (G \lor \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G)}}{F \to \langle\beta^*\rangle G}$$

Observe that rules $\forall$ and MP instantiate as needed with USR by Lemma 20. □

Proof of Lemma 23. The left side is $\nu \in I\llbracket\sigma^U_{\bar{U}}(x' = \theta \&^d y \in Y \& z \in Z)\rrbracket\big(X\big) = I\llbracket x' {=} \sigma^{\bar{U}}\theta \&^d y \in \sigma^{\bar{U}} Y \& z \in \sigma^{\bar{U}} Z\rrbracket\big(X\big) = I\llbracket x' {=} \sigma^{\bar{U}}\theta{}_{y}^{v}{}_{z}^{w} \&^d v \in \sigma^{\bar{U}} Y \& w \in \sigma^{\bar{U}} Z\rrbracket\big(X\big)$ by uniform renaming of y to v and z to w (proof of Lemma 21), which are fresh. Here $\sigma^{\bar{U}}\theta{}_{y}^{v}{}_{z}^{w}$ is the result of uniformly renaming y to v and z to w in the term $\sigma^{\bar{U}}\theta$ and $v \in \sigma^{\bar{U}} Y$ the result of uniformly renaming y to v in $y \in \sigma^{\bar{U}} Y$ (no z occurs), and $w \in \sigma^{\bar{U}} Z$ the result of uniformly renaming z to w in $z \in \sigma^{\bar{U}} Z$, where y does not occur. Without loss of generality (by performing two subsequent uniform substitutions), no symbol that is being replaced by σ occurs in any of σ's replacements. Hence, σ is idempotent and $I\llbracket x' = \sigma^{\bar{U}}\theta{}_{y}^{v}{}_{z}^{w} \&^d v \in \sigma^{\bar{U}} Y \& w \in \sigma^{\bar{U}} Z\rrbracket\big(X\big) = \sigma^*_\omega I\llbracket x' = \sigma^{\bar{U}}\theta{}_{y}^{v}{}_{z}^{w} \&^d v \in \sigma^{\bar{U}} Y \& w \in \sigma^{\bar{U}} Z\rrbracket\big(X\big)$. Now that both are phrased in the same interpretation, the equivalence $\nu \in \sigma^*_\omega I\llbracket x' = \theta \&^d y \in Y \& z \in Z\rrbracket\big(X\big)$ iff $\nu \in \sigma^*_\omega I\llbracket x' = \sigma^{\bar{U}}\theta{}_{y}^{v}{}_{z}^{w} \&^d v \in \sigma^{\bar{U}} Y \& w \in \sigma^{\bar{U}} Z\rrbracket\big(X\big)$ follows provided that the following dGL formula is true in $\sigma^*_\omega I, \nu$ for a fresh game symbol c with $\sigma^*_\omega I\llbracket\langle c\rangle\top\rrbracket = X$:

$$\langle x' = \sigma^{\bar{U}}\theta{}_{y}^{v}{}_{z}^{w} \&^d v \in \sigma^{\bar{U}} Y \& w \in \sigma^{\bar{U}} Z\rangle\langle c\rangle\top \leftrightarrow \langle x' = \theta \&^d y \in Y \& z \in Z\rangle\langle c\rangle\top \quad (4)$$

Without loss of generality, replace free occurrences of variables $\{x, x', y, y', z, z'\}^{\complement}$ by their respective real values in ν. Now (4) is true in $\sigma^*_\omega I, \nu$ by the (locally sound) differential game refinement proof schema [17] for $\langle\rangle$ once per implication:

$$\text{(DGR)}\quad \frac{\forall y \in Y\, \exists v \in V\, \forall w \in W\, \exists z \in Z\, \forall x\, (\eta = \theta)}{\langle x' = \eta \,\&^d v \in V \,\&\, w \in W\rangle F \to \langle x' = \theta \,\&^d y \in Y \,\&\, z \in Z\rangle F}$$

By rule DGR for both implications of (4), it suffices to show validity in $\sigma^*_\omega I$ of:

$$\begin{aligned}
&\forall y \in Y\, \exists v \in \sigma^{\bar{U}} Y\, \forall w \in \sigma^{\bar{U}} Z\, \exists z \in Z\, \forall x\, (\sigma^{\bar{U}} \theta \tfrac{v}{y} \tfrac{w}{z} = \theta)\\
&\forall v \in \sigma^{\bar{U}} Y\, \exists y \in Y\, \forall z \in Z\, \exists w \in \sigma^{\bar{U}} Z\, \forall x\, (\sigma^{\bar{U}} \theta \tfrac{v}{y} \tfrac{w}{z} = \theta)
\end{aligned} \tag{5}$$

Both formulas are shown with $v = y$ and $w = z$ as witnesses. By Lemma 16 all $\bar{U}$-variations μ of ω satisfy $\mu \in \sigma^*_\omega I[\![Y]\!]$ iff $\mu \in I[\![\sigma^{\bar{U}} Y]\!]$ iff, as σ idempotent, $\mu \in \sigma^*_\omega I[\![\sigma^{\bar{U}} Y]\!]$ iff, by uniform renaming and Lemma 10 as y' is not in $\sigma^{\bar{U}} Y$, $\mu \tfrac{v}{y} \in \sigma^*_\omega I[\![(\sigma^{\bar{U}} Y) \tfrac{v}{y}]\!] = \sigma^*_\omega I[\![v \in \sigma^{\bar{U}} Y]\!]$. Here, $\mu \tfrac{v}{y}$ is the state $\mu_v^{\mu(y)}$ as in ($*$) of Lemma 21, where y, y', v' do not occur in $(\sigma^{\bar{U}} Y) \tfrac{v}{y}$. By a similar argument: $\mu \in \sigma^*_\omega I[\![Z]\!]$ iff $\mu \tfrac{w}{z} \in \sigma^*_\omega I[\![(\sigma^{\bar{U}} Z) \tfrac{w}{z}]\!] = \sigma^*_\omega I[\![w \in \sigma^{\bar{U}} Z]\!]$. When $v = y$ and $w = z$, the constraints of (5) are met in a state of $\sigma^*_\omega I$ for y, z iff they are met for v, w.

Finally, by Lemma 15 when μ is a $\bar{U}$-variation of ω: $\sigma^*_\omega I\mu[\![\theta]\!] = I\mu[\![\sigma^{\bar{U}} \theta]\!]$ which by uniform renaming and Lemma 9 as y' and z' are not in $\sigma^{\bar{U}} \theta$ equals $I\mu \tfrac{v}{y} \tfrac{w}{z} [\![(\sigma^{\bar{U}} \theta) \tfrac{v}{y} \tfrac{w}{z}]\!]$, which by idempotence of σ equals $\sigma^*_\omega I\mu \tfrac{v}{y} \tfrac{w}{z} [\![(\sigma^{\bar{U}} \theta) \tfrac{v}{y} \tfrac{w}{z}]\!]$. Thus, the states μ that are $\{x, y, z, v, w\}$-variations of ν so $\bar{U}$-variation of ω satisfying $\mu \in \sigma^*_\omega I[\![v = y \wedge w = z]\!]$ witness (5), because $\mu \in \sigma^*_\omega I[\![(\sigma^{\bar{U}} \theta) \tfrac{v}{y} \tfrac{w}{z} = \theta]\!]$ by Lemma 9 as v, w are not in θ, for all values of y, w, x (with $v := y, z := w$), or for all values of v, z, x ($y := v, w := z$), respectively. □