Uniform Substitution for Differential Game Logic[⋆]

André Platzer

Computer Science Department, Carnegie Mellon University, Pittsburgh, USA
aplatzer@cs.cmu.edu

Abstract. This paper presents a uniform substitution calculus for *differential game logic* (dGL). Church's *uniform substitutions* substitute a term or formula for a function or predicate symbol everywhere. After generalizing them to differential game logic and allowing for the substitution of hybrid games for game symbols, uniform substitutions make it possible to *only* use axioms instead of axiom schemata, thereby substantially simplifying implementations. Instead of subtle schema variables and soundness-critical side conditions on the occurrence patterns of logical variables to restrict infinitely many axiom schema instances to sound ones, the resulting axiomatization adopts only a finite number of ordinary dGL formulas as axioms, which uniform substitutions instantiate soundly. This paper proves soundness and completeness of uniform substitutions for the monotone modal logic dGL. The resulting axiomatization admits a straightforward modular implementation of dGL in theorem provers.

1 Introduction

Church's *uniform substitution* is a classical proof rule for first-order logic [2, §35/40]. Uniform substitutions uniformly instantiate function and predicate symbols with terms and formulas, respectively, as functions of their arguments. If ϕ is valid, then so is any admissible instance $\sigma\phi$ for any uniform substitution σ:

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

Uniform substitution $\sigma = \{p(\cdot) \mapsto x + \cdot^2 \geq \cdot\}$, e.g. turns $\phi \equiv (p(4y) \rightarrow \exists y\, p(x^2+y))$ into $\sigma\phi \equiv (x + (4y)^2 \geq 4y \rightarrow \exists y\, x + (x^2 + y)^2 \geq x^2 + y)$. The introduction of x is sound, but introducing variable y via $\sigma = \{p(\cdot) \mapsto y + \cdot^2 \geq \cdot\}$ would not be. The occurrence of the variable y of the argument $x^2 + y$ that was already present previously, however, can correctly continue to be used in the instantiation.

Differential game logic (dGL), which is the specification and verification logic for *hybrid games* [5], originally adopted uniform substitution for predicates, because they streamline and simplify completeness proofs. A subsequent investigation of uniform substitutions for differential *dynamic* logic (dL) for hybrid

[⋆] This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246.

systems [6] confirmed how impressively Church's original motivation for uniform substitutions manifests in significantly simplifying prover implementations.

Church developed uniform substitutions to relate the study of (object-level) axioms to that of (meta-level) axiom schemata (which stand for an infinite family of axioms). Beyond their philosophical considerations, uniform substitutions significantly impact prover designs by eliminating the usual gap between a logic and its prover. After implementing the recursive application of uniform substitutions, the soundness-critical part of a theorem prover reduces to providing a copy of each concrete logical formula that the logic adopts as axioms. Uniform substitutions provide a modular interface to the static semantics of the logic, because they are the only soundness-critical part of the prover that needs to know free or bound variables of an expression. This simplicity is to be contrasted with the subtle soundness-critical side conditions that usually infest axiom schema and proof rule schema implementations, especially for the more involved binding structures of program logics. The beneficial impact of uniform substitutions on provers made it possible to reduce the size of the soundness-critical core of the differential dynamic logic prover KeYmaera X [3] down to 2% compared to the previous prover KeYmaera [9] and formally verify dL in Isabelle and Coq [1].

This paper generalizes uniform substitution to the significantly more expressive differential game logic for hybrid *games* [5]. The modular structure of the soundness argument for dL is sufficiently robust to work for dGL: *i)* prove correctness of the static semantics, *ii)* relate syntactic effect of uniform substitution to semantic effect of its adjoint interpretation, *iii)* conclude soundness of rule US, and *iv)* separately establish soundness of each axiom. The biggest challenge is that hybrid game semantics cannot use state reachability, so correctness notions and their uses for the static semantics need to be phrased as functions of winning condition projections. The interaction of game operators with repetitions causes transfinite fixpoints instead of the arbitrary finite iterations in hybrid systems. Relative completeness follows from previous results, but exploits the new game symbols to simplify the proof. After new soundness justifications, the resulting uniform substitution mechanism and axioms for dGL end up close to those for hybrid systems [6] (apart from the ones that are unsound for hybrid games [5]). The modularity caused by uniform substitutions explains why it was possible to generalize the KeYmaera X prover kernel from hybrid systems to hybrid games with about 10 lines of code.[1] All proofs are inline or in the report [8].

2 Preliminaries: Differential Game Logic

This section reviews differential game logic (dGL), a specification and verification logic for hybrid games [5,7]. Hybrid games support the discrete, continuous, and

[1] The addition of games to the previous KeYmaera prover was more complex [10], with an implementation effort measured in months not minutes. Unfortunately, this is not quite comparable, because both provers implement markedly different flavors of games for hybrid systems. The game logic for KeYmaera [10] was specifically tuned as an exterior extension to be more easily implementable than dGL in KeYmaera.

adversarial dynamics of two-player games in hybrid systems between players Angel and Demon. Compared to previous work [5], the logic is augmented to form *(differential-form) differential game logic* with differentials and function symbols [6] and with game symbols a that can be substituted with hybrid games.

2.1 Syntax

Differential game logic has three syntactic categories. Its terms θ are polynomial terms, function symbols interpreted over $\mathbb{R}$, and differential terms $(\theta)'$. Its hybrid games α describe the permitted player actions during the game in program notation. Its formulas ϕ include first-order logic of real arithmetic and, for each hybrid game α, a modal formula $\langle\alpha\rangle\phi$, which expresses that player Angel has a winning strategy in the hybrid game α to reach the region satisfying dGL formula ϕ. In the formula $\langle\alpha\rangle\phi$, the dGL formula ϕ describes Angel's objective while the hybrid game α describes the moves permitted for the two players, respectively.

The set of all *variables* is $\mathcal{V}$. Variables of the form x' for a variable $x \in \mathcal{V}$ are called *differential variables*, which are just independent variables associated to variable x. For any subset $V \subseteq \mathcal{V}$ is $V' \stackrel{\text{def}}{=} \{x' : x \in V\}$ the set of *differential variables* x' for the variables in V. The set of all variables is assumed to contain all its differential variables $\mathcal{V}' \subseteq \mathcal{V}$ (although x'', x''' are not usually used).

Definition 1 (Terms). Terms *are defined by this grammar (with $\theta, \eta, \theta_1, \ldots, \theta_k$ as terms, $x \in \mathcal{V}$ as variable, and f as function symbol of arity k):*

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

As in dL [6], *differentials* $(\theta)'$ of terms θ are exploited for the purpose of axiomatically internalizing reasoning about differential equations. The differential $(\theta)'$ describes how the value of θ changes locally depending on how the values of its variables x change, i.e., as a function of the values of the corresponding differential variables x'. Differentials reduce reasoning about *differential equations* to reasoning about *equations of differentials* [6] with their single-state semantics.

Definition 2 (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):*

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

Atomic games are the following. *Game symbols a* are uninterpreted. The *discrete assignment game* $x := \theta$ evaluates term θ and assigns it to variable x. The *continuous evolution game* $x' = \theta \,\&\, \psi$ allows Angel to follow differential equation $x' = \theta$ for any real duration during which the evolution domain constraint ψ is true ($x' = \theta$ stands for $x' = \theta \,\&\, \mathit{true}$). If ψ is not true in the current state, then no solution exists and Angel loses the game. *Test game* $?\psi$ has no effect except that Angel loses the game prematurely unless ψ is true in the current state.

Compound games are the following. The *game of choice* $\alpha \cup \beta$ allows Angel to choose whether she wants to play game α or, instead, play game β. The *sequential game* $\alpha;\beta$ first plays α and then plays β (unless a player lost prematurely during α). The *repeated game* α^* allows Angel to decide how often to repeat game α by inspecting the state reached after the respective α game to decide whether she wants to play another round. The *dual game* α^d makes the players switch sides: all of Angel's decisions are now Demon's and all of Demon's decisions are now Angel's. Where Angel would have lost prematurely in α (for failing a test or evolution domain) now Demon does in α^d, and vice versa. This makes game play interactive but semantically quite rich [5]. All other operations are definable, e.g., the game where Demon chooses between α and β as $(\alpha^d \cup \beta^d)^d$.

Definition 3 (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 box modality $[\alpha]$ in formula $[\alpha]\phi$ describes that the player Demon has a winning strategy to achieve ϕ in hybrid game α. But dGL satisfies the determinacy duality $[\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$ [5, Theorem 3.1], which we now take as its definition to simplify matters. Other operators are definable as usual, e.g., $\forall x\, \phi$ as $\neg\exists x\, \neg\phi$. The following dGL formula, for example, expresses that Angel has a winning strategy to follow the differential equation $x' = v$ to a state where $x > 0$ even after Demon chooses $v := 2$ or $v := x^2+1$ first: $\langle(v := 2 \cup v := x^2+1)^d; x' = v\rangle\, x > 0$.

2.2 Semantics

While the syntax of dGL is close to that of dL (with the only change being the addition of the duality operator ^{d}), its semantics is significantly more involved, because it needs to recursively support *interactive* game play, instead of mere reachability. Variables may have different values in different states of the game. A *state* ω is a mapping from the set of all variables $\mathcal{V}$ to the reals $\mathbb{R}$. Also, ω_x^r is the state that agrees with state ω except for variable x whose value is $r \in \mathbb{R}$. The set of all states is denoted $\mathcal{S}$. The set of all subsets of $\mathcal{S}$ 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 $I(f) : \mathbb{R}^k \to \mathbb{R}$, and each arity k predicate symbol p to a k-ary relation $I(p) \subseteq \mathbb{R}^k$. 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 (Def. 5) as the set of all states from which Angel has a winning strategy in hybrid game α to achieve X. The real value of term θ in state

ω for interpretation I is denoted $I\omega[\![\theta]\!]$ and defined as usual.[2] An interpretation I maps each game symbol a to a function $I(a) : \wp(\mathcal{S}) \to \wp(\mathcal{S})$, where $I(a)(X) \subseteq \mathcal{S}$ are the states from which Angel has a winning strategy to achieve $X \subseteq \mathcal{S}$.

Definition 4 (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. $I[\![p(\theta_1, \ldots, \theta_k)]\!] = \{\omega \in \mathcal{S} : (I\omega[\![\theta_1]\!], \ldots, I\omega[\![\theta_k]\!]) \in I(p)\}$
3. $I[\![\neg\phi]\!] = (I[\![\phi]\!])^{\complement} = \mathcal{S} \setminus I[\![\phi]\!]$ *is the complement of* $I[\![\phi]\!]$
4. $I[\![\phi \land \psi]\!] = I[\![\phi]\!] \cap I[\![\psi]\!]$
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 $\models \phi$, iff $I \models \phi$ for all interpretations I.*

Definition 5 (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 Angel's winning states $X \subseteq \mathcal{S}$, 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 *satisfying* $I, \varphi \models x' = \theta \land \psi\}$ *where* $I, \varphi \models x' = \theta \land \psi$ *iff* $\varphi(\zeta) \in I[\![x' = \theta \land \psi]\!]$ *and* $\varphi(0) = \varphi(\zeta)$ *on* $\{x, x'\}^{\complement}$ *for all* $0 \leq \zeta \leq r$ *and* $\frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(\zeta)$ *exists and equals* $\varphi(\zeta)(x')$ *for all* $0 \leq \zeta \leq r$ *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. $I[\![\alpha^*]\!]\big(X\big) = \bigcap\{Z \subseteq \mathcal{S} : X \cup I[\![\alpha]\!]\big(Z\big) \subseteq Z\}$
8. $I[\![\alpha^d]\!]\big(X\big) = (I[\![\alpha]\!]\big(X^{\complement}\big))^{\complement}$

The semantics $I[\![x' = \theta \,\&\, \psi]\!]\big(X\big)$ is the set of all states from which there is a solution of the differential equation $x' = \theta$ of some duration that reaches a state in X without ever leaving the set of all states $I[\![\psi]\!]$ where evolution domain constraint ψ is true. The initial value of x' in state ω is ignored for that solution. It is crucial that $I[\![\alpha^*]\!]\big(X\big)$ gives a least fixpoint semantics to repetition [5].

Lemma 6 (Monotonicity [5, Lem. 2.7]). *The semantics is* monotone, *i.e., $I[\![\alpha]\!]\big(X\big) \subseteq I[\![\alpha]\!]\big(Y\big)$ for all $X \subseteq Y$.*

[2] Even if not critical here, differentials have a differential-form semantics [6] as the sum of all partial derivatives by $x \in \mathcal{V}$ multiplied by the corresponding values of x': $I\omega[\![(\theta)']\!] = \sum_{x\in\mathcal{V}} \omega(x') \frac{\partial I[\![\theta]\!]}{\partial x}(\omega) = \sum_{x\in\mathcal{V}} \omega(x') \frac{\partial I\omega[\![\theta]\!]}{\partial x}$

3 Static Semantics

The central bridge between a logic and its uniform substitutions is the definition of its static semantics via its free and bound variables. The static semantics captures static variable relationships that are more tractable than the full nuances of the dynamic semantics. It will be used in crucial ways to ensure that no variable is introduced free into a context within which it is bound during the uniform substitution application. It is imperative for the soundness of uniform substitution that the static semantics be sound, so expressions only depend on their free variables and only their bound variables change during hybrid games.

The most tricky part for the soundness justification for dGL is that the semantics of hybrid games is not a reachability relation, such that the usual semantic characterizations of free and bound variables from programs do not work for hybrid games. Hybrid games have a more involved winning region semantics.

The first step is to define *upward projections* $X{\uparrow}V$ that increase the winning region $X \subseteq \mathcal{S}$ from the variables $V \subseteq \mathcal{V}$ to all states that are "on V like X", i.e., similar on V to states in X (and arbitrary on complement $V^{\complement}$). The *downward projection* $X{\downarrow}\omega(V)$ shrinks the winning region X and selects the values of state ω on variables $V \subseteq \mathcal{V}$ to keep just those states of X that agree with ω on V.

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

Remark 8. It is easy to check these properties of up and down projections:

1. Composition: $X{\uparrow}V{\uparrow}W = X{\uparrow}(V \cap W)$
2. Antimonotone: $X{\uparrow}W \subseteq X{\uparrow}V$ for all $W \supseteq V$
3. $X{\uparrow}\emptyset = \mathcal{S}$ (unless $X = \emptyset$) and $X{\uparrow}\mathcal{V} = X$, where $\mathcal{V}$ is the set of all variables
4. Composition: $X{\downarrow}\omega(V){\downarrow}\omega(W) = X{\downarrow}\omega(V \cup W)$
5. Antimonotone: $X{\downarrow}\omega(W) \subseteq X{\downarrow}\omega(V)$ for all $W \supseteq V$
6. $X{\downarrow}\omega(\emptyset) = X$ and $X{\downarrow}\omega(\mathcal{V}) = X \cap \{\omega\}$. Thus, $\omega \in X{\downarrow}\omega(V)$ for any V iff $\omega \in X$.

Projections make it possible to define (*semantic!*) free and bound variables of hybrid games by expressing suitable variable dependence and ignorance. Variable x is free iff two states that only differ in the value of x have different membership in the winning region for hybrid game α for some winning region $X{\uparrow}\{x\}^{\complement}$ that is insensitive to the value of x. Variable x is bound iff it is in the winning region for hybrid game 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 9 (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:*

$$\mathsf{FV}(\theta) = \big\{x \in \mathcal{V} : \exists I, \omega, \tilde{\omega} \text{ such that } \omega = \tilde{\omega} \text{ on } \{x\}^{\complement} \text{ and } I\omega[\![\theta]\!] \neq I\tilde{\omega}[\![\theta]\!]\big\}$$

$$\mathsf{FV}(\phi) = \big\{x \in \mathcal{V} : \exists I, \omega, \tilde{\omega} \text{ such that } \omega = \tilde{\omega} \text{ on } \{x\}^{\complement} \text{ and } \omega \in I[\![\phi]\!] \not\ni \tilde{\omega}\big\}$$

$$\mathsf{FV}(\alpha) = \big\{x \in \mathcal{V} : \exists I, \omega, \tilde\omega, X \ \textit{with}\ \omega = \tilde\omega \ \textit{on}\ \{x\}^\complement \ \textit{and}\ \omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}\{x\}^\complement\big) \not\ni \tilde\omega\big\}$$
$$\mathsf{BV}(\alpha) = \big\{x \in \mathcal{V} : \exists I, \omega, X \ \textit{such that}\ I\llbracket\alpha\rrbracket\big(X\big) \ni \omega \notin I\llbracket\alpha\rrbracket\big(X{\downarrow}\omega(\{x\})\big)\big\}$$

The signature*, i.e., set of function, predicate, and game symbols in ϕ is denoted $\Sigma(\phi)$; accordingly $\Sigma(\theta)$ for term θ and $\Sigma(\alpha)$ for hybrid game α.*

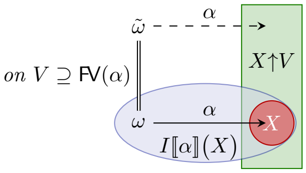
The static semantics from Def. 9 satisfies the coincidence property (the value of an expression only depends on the values of its free variables) and bound effect property (a hybrid game only changes the values of its bound variables).

Lemma 10 (Coincidence for terms). *$\mathsf{FV}(\theta)$ is the smallest set with the coincidence property for θ: If $\omega = \tilde\omega$ on $\mathsf{FV}(\theta)$ and $I = J$ on $\Sigma(\theta)$ then $I\omega\llbracket\theta\rrbracket = J\tilde\omega\llbracket\theta\rrbracket$.*

Lemma 11 (Coincidence for formulas). *$\mathsf{FV}(\phi)$ is the smallest set with the coincidence property for ϕ: If $\omega = \tilde\omega$ on $\mathsf{FV}(\phi)$ and $I = J$ on $\Sigma(\phi)$, then $\omega \in I\llbracket\phi\rrbracket$ iff $\tilde\omega \in J\llbracket\phi\rrbracket$.*

From which states a hybrid game α can be won only depends on α, the winning region, and the values of its free variables, as $X{\uparrow}\,\mathsf{FV}(\alpha)$ is only sensitive to $\mathsf{FV}(\alpha)$.

Lemma 12 (Coincidence for games). *The set $\mathsf{FV}(\alpha)$ is the smallest set with the coincidence property for α: If $\omega = \tilde\omega$ on $V \supseteq \mathsf{FV}(\alpha)$ and $I = J$ on $\Sigma(\alpha)$, then $\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$ iff $\tilde\omega \in J\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$.*


$\tilde\omega$
α
$X{\uparrow}V$
on $V \supseteq \mathsf{FV}(\alpha)$
ω
α
X
$I\llbracket\alpha\rrbracket(X)$

Proof. Let $\mathcal{M}$ be the set of all sets $M \subseteq \mathcal{V}$ satisfying for all $I, \omega, \tilde\omega, X$ that $\omega = \tilde\omega$ on $M^\complement$ implies: $\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$ iff $\tilde\omega \in I\llbracket\alpha\rrbracket\big(V\big)$. One implication suffices.

1. If $x \notin V$, then $\{x\} \in \mathcal{M}$: Assume $\omega = \tilde\omega$ on $\{x\}^\complement$ and $\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big) \subseteq I\llbracket\alpha\rrbracket\big(X{\uparrow}V{\uparrow}\{x\}\big)$ by Lem. 6, Def. 7. Then, as $x \notin \mathsf{FV}(\alpha)$, $\tilde\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V{\uparrow}\{x\}\big)$ $= I\llbracket\alpha\rrbracket\big(X{\uparrow}(V \cap \{x\}^\complement)\big)$ by Rem. 8(1). Finally, $X{\uparrow}(V \cap \{x\}^\complement) = X{\uparrow}V$ as $x \notin V$.
2. If $M_i \in \mathcal{M}$ is a sequence of sets in $\mathcal{M}$, then $\bigcup_{i\in\mathbb{N}} M_i \in \mathcal{M}$: Assume $\omega = \tilde\omega$ on $(\bigcup_i M_i)^\complement$ and $\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$. The state ω_n defined as $\tilde\omega$ on $\bigcup_{i<n} M_i$ and as ω on $(\bigcup_{i<n} M_i)^\complement$ satisfies $\omega_n \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$ by induction on n. For $n = 0$, $\omega_0 = \omega$. Since $\omega_n = \omega_{n+1}$ on $M_n^\complement$ and $M_n \in \mathcal{M}$, $\omega_n \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$ implies $\omega_{n+1} \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$. Finally, $\omega = \tilde\omega = \omega_n$ on $(\bigcup_i M_i)^\complement$ already.

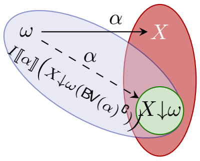
This argument succeeds for any $V \supseteq \mathsf{FV}(\alpha)$, so $\mathsf{FV}(\alpha)^\complement \in \mathcal{M}$ as a (countable) union of $\{x\}$ for all $x \notin \mathsf{FV}(\alpha)$. Finally, if $I = J$ on $\Sigma(\alpha)$ then also $\tilde\omega \in J\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$ by a simple induction, since I gives meaning to function, predicate, and game symbols, but only those that occur in α are relevant.

No set $W \not\supseteq \mathsf{FV}(\alpha)$ has the coincidence property for α, because there, then, is a variable $x \in \mathsf{FV}(\alpha) \setminus W$, which implies there are $I, X, \omega = \tilde\omega$ on $\{x\}^\complement \supseteq W$ such that $\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}\{x\}^\complement\big) \not\ni \tilde\omega$. But for the set $V \overset{\text{def}}{=} \{x\}^\complement \supseteq W$ it is, then, the case that $\omega \in I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$ but $\tilde\omega \notin I\llbracket\alpha\rrbracket\big(X{\uparrow}V\big)$. □

By Def. 7 and Lemma 6, $\omega \in I[\![\alpha]\!]\big(X\big)$ implies $\omega \in I[\![\alpha]\!]\big(X{\uparrow}V\big)$ for all $V \subseteq \mathcal{V}$. All supersets of $\mathsf{FV}(\theta)$ or $\mathsf{FV}(\phi)$ or $\mathsf{FV}(\alpha)$ have the respective coincidence property.

Only its bound variables $\mathsf{BV}(\alpha)$ change their values during hybrid game α, because from any state from which α can be won to achieve X, one can already win α to achieve $X{\downarrow}\omega(\mathsf{BV}(\alpha)^{\complement})$, which stays at ω except for the values of $\mathsf{BV}(\alpha)$.

Lemma 13 (Bound effect). *The set* $\mathsf{BV}(\alpha)$ *is the smallest set with the bound effect property:* $\omega \in I[\![\alpha]\!]\big(X\big)$ *iff* $\omega \in I[\![\alpha]\!]\big(X{\downarrow}\omega(\mathsf{BV}(\alpha)^{\complement})\big)$.


ω
α
X
α
$I[\![\alpha]\!]\big(X{\downarrow}\omega(\mathsf{BV}(\alpha)^{\complement})\big)$
$X{\downarrow}\omega$

All supersets $V \supseteq \mathsf{BV}(\alpha)$ have the bound effect property, as $I[\![\alpha]\!]\big(X{\downarrow}\omega(V^{\complement})\big) \supseteq I[\![\alpha]\!]\big(X{\downarrow}\omega(\mathsf{BV}(\alpha)^{\complement})\big)$ by Rem. 8(5) because $V^{\complement} \subseteq \mathsf{BV}(\alpha)^{\complement}$. Other states that agree except on the bound variables share the same selection of the winning region: if $\omega = \tilde{\omega}$ on $\mathsf{BV}(\alpha)^{\complement}$, then $\tilde{\omega} \in I[\![\alpha]\!]\big(X\big)$ iff $\tilde{\omega} \in I[\![\alpha]\!]\big(X{\downarrow}\omega(\mathsf{BV}(\alpha)^{\complement})\big)$.

Since all supersets of the free variables have the coincidence property and all supersets of the bound variables have the bound effect property, algorithms that *syntactically compute* supersets FV and BV of free and bound variables [6, Lem. 17] can be soundly augmented by $\mathrm{FV}(\alpha^d) = \mathrm{FV}(\alpha)$ and $\mathrm{BV}(\alpha^d) = \mathrm{BV}(\alpha)$.

4 Uniform Substitution

The static semantics provides, in a modular way, what is needed to define the application $\sigma\phi$ of uniform substitution σ to dGL formula ϕ. The dGL axiomatization uses uniform substitutions that affect terms, formulas, and games, whose application $\sigma\phi$ will be defined in Def. 14 using Fig. 1. 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. Vectorial extensions are accordingly for other arities $k \geq 0$. Here $\cdot$ is a reserved function symbol of arity 0, marking the position where the respective argument, e.g., argument θ to $p(\cdot)$ in formula $p(\theta)$, will end up in the replacement $\sigma p(\cdot)$ used for $p(\theta)$.

Definition 14 (Admissible uniform substitution). *A uniform substitution* σ *is* U-admissible *for* ϕ *(or* θ *or* α*, respectively) with respect to the variables* $U \subseteq \mathcal{V}$ *iff* $\mathsf{FV}(\sigma|_{\Sigma(\phi)}) \cap U = \emptyset$*, where* $\sigma|_{\Sigma(\phi)}$ *is the* restriction *of* σ *that only replaces symbols that occur in* ϕ*, and* $\mathsf{FV}(\sigma) = \bigcup_f \mathsf{FV}(\sigma f(\cdot)) \cup \bigcup_p \mathsf{FV}(\sigma p(\cdot))$ *are the* free variables *that* σ *introduces. A uniform substitution* σ *is* admissible *for* ϕ *(*θ *or* α*, respectively) iff the bound variables* U *of each operator of* ϕ *are not free in the substitution on its arguments, i.e.,* σ *is* U*-admissible. These admissibility conditions are listed in Fig. 1, which defines the result* $\sigma\phi$ *of applying* σ *to* ϕ*.*

The remainder of this section proves soundness of uniform substitution for dGL. *All subsequent uses of uniform substitutions are required to be admissible.*

$$\begin{array}{rll}
\sigma(x) & = x & \text{for variable } x \in \mathcal{V} \\
\sigma(f(\theta)) & = (\sigma f)(\sigma\theta) \overset{\text{def}}{=} \{\cdot \mapsto \sigma\theta\}\sigma f(\cdot) & \text{for function symbol } f \\
\sigma(\theta + \eta) & = \sigma\theta + \sigma\eta & \\
\sigma(\theta \cdot \eta) & = \sigma\theta \cdot \sigma\eta & \\
\sigma((\theta)') & = (\sigma\theta)' & \text{if } \sigma \text{ is } \mathcal{V}\text{-admissible for } \theta \\
\hline
\sigma(\theta \geq \eta) & = \sigma\theta \geq \sigma\eta & \\
\sigma(p(\theta)) & = (\sigma p)(\sigma\theta) \overset{\text{def}}{=} \{\cdot \mapsto \sigma\theta\}\sigma p(\cdot) & \text{for predicate symbol } p \\
\sigma(\neg\phi) & = \neg\sigma\phi & \\
\sigma(\phi \land \psi) & = \sigma\phi \land \sigma\psi & \\
\sigma(\exists x\, \phi) & = \exists x\, \sigma\phi & \text{if } \sigma \text{ is } \{x\}\text{-admissible for } \phi \\
\sigma(\langle\alpha\rangle\phi) & = \langle\sigma\alpha\rangle\sigma\phi & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma\alpha)\text{-admissible for } \phi \\
\hline
\sigma(a) & = \sigma a & \text{for game symbol } a \\
\sigma(x := \theta) & = x := \sigma\theta & \\
\sigma(x' = \theta \,\&\, \psi) & = (x' = \sigma\theta \,\&\, \sigma\psi) & \text{if } \sigma \text{ is } \{x, x'\}\text{-admissible for } \theta, \psi \\
\sigma(?\psi) & = ?\sigma\psi & \\
\sigma(\alpha \cup \beta) & = \sigma\alpha \cup \sigma\beta & \\
\sigma(\alpha; \beta) & = \sigma\alpha; \sigma\beta & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma\alpha)\text{-admissible for } \beta \\
\sigma(\alpha^*) & = (\sigma\alpha)^* & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma\alpha)\text{-admissible for } \alpha \\
\sigma(\alpha^d) & = (\sigma\alpha)^d &
\end{array}$$

Fig. 1. Recursive application of uniform substitution σ

4.1 Uniform Substitution Lemmas

Uniform substitution lemmas equate the syntactic effect that a uniform substitution σ has on a syntactic expression in a state ω and interpretation I with the semantic effect that the switch to the adjoint interpretation $\sigma^*_\omega I$ has on the original expression. Adjoints make it possible to capture in semantics the effect that a uniform substitution has on the syntax.

Let $I^d_{\boldsymbol{\cdot}}$ denote the interpretation that agrees with interpretation I except for the interpretation of arity 0 function symbol $\cdot$ which is changed to $d \in \mathbb{R}$.

Definition 15 (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):*

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

Corollary 16 (Admissible adjoints). *If $\omega = \nu$ on $\mathsf{FV}(\sigma)$, then $\sigma^*_\omega I = \sigma^*_\nu I$. If $\omega = \nu$ on $U^\complement$ and σ is U-admissible for θ (or ϕ or α, respectively), then*

$$\begin{aligned}
&\sigma^*_\omega I[\![\theta]\!] = \sigma^*_\nu I[\![\theta]\!] \ \textit{i.e., } \sigma^*_\omega I\mu[\![\theta]\!] = \sigma^*_\nu I\mu[\![\theta]\!] \textit{ for all states } \mu \in \mathcal{S} \\
&\sigma^*_\omega I[\![\phi]\!] = \sigma^*_\nu I[\![\phi]\!] \\
&\sigma^*_\omega I[\![\alpha]\!] = \sigma^*_\nu I[\![\alpha]\!] \ \textit{i.e., } \sigma^*_\omega I[\![\alpha]\!]\big(X\big) = \sigma^*_\nu I[\![\alpha]\!]\big(X\big) \textit{ for all sets } X \subseteq \mathcal{S}
\end{aligned}$$

Substituting equals for equals is sound by the compositional semantics of dL. The more general uniform substitutions are still sound, because the semantics of uniform substitutes of expressions agrees with the semantics of the expressions themselves in the adjoint interpretations. The semantic modification of adjoint interpretations has the same effect as the syntactic uniform substitution.

Lemma 17 (Uniform substitution for terms). *The uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I, \omega$ for I, ω have the same semantics for all* terms *θ:*

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

The uniform substitute of a formula is true in an interpretation iff the formula itself is true in its adjoint interpretation. Uniform substitution lemmas are proved by simultaneous induction, since formulas and games are mutually recursive.

Lemma 18 (Uniform substitution for formulas). *The uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I, \omega$ for I, ω have the same semantics for all* formulas *ϕ:*

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

Proof. The proof is by structural induction on ϕ and the structure of σ, simultaneously with Lemma 19. It is in [8] with this case for modalities:

6. $\omega \in I[\![\sigma(\langle\alpha\rangle\phi)]\!]$ iff $\omega \in I[\![\langle\sigma\alpha\rangle\sigma\phi]\!] = I[\![\sigma\alpha]\!]\big(I[\![\sigma\phi]\!]\big)$ (provided σ is $\mathsf{BV}(\sigma\alpha)$-admissible for ϕ) iff (by Lemma 13) $\omega \in I[\![\sigma\alpha]\!]\big(I[\![\sigma\phi]\!]{\downarrow}\omega(\mathsf{BV}(\sigma\alpha)^\complement)\big)$.
Starting conversely: $\omega \in \sigma^*_\omega I[\![\langle\alpha\rangle\phi]\!] = \sigma^*_\omega I[\![\alpha]\!]\big(\sigma^*_\omega I[\![\phi]\!]\big)$ iff (by Lemma 19) $\omega \in I[\![\sigma\alpha]\!]\big(\sigma^*_\omega I[\![\phi]\!]\big)$ iff (by Lemma 13) $\omega \in I[\![\sigma\alpha]\!]\big(\sigma^*_\omega I[\![\phi]\!]{\downarrow}\omega(\mathsf{BV}(\sigma\alpha)^\complement)\big)$.
Consequently, it suffices to show that both winning conditions are equal:
$$I[\![\sigma\phi]\!]{\downarrow}\omega(\mathsf{BV}(\sigma\alpha)^\complement) = \sigma^*_\omega I[\![\phi]\!]{\downarrow}\omega(\mathsf{BV}(\sigma\alpha)^\complement)$$
For this, consider any $\nu = \omega$ on $\mathsf{BV}(\sigma\alpha)^\complement$ and show: $\nu \in I[\![\sigma\phi]\!]$ iff $\nu \in \sigma^*_\omega I[\![\phi]\!]$. By induction hypothesis, $\nu \in I[\![\sigma\phi]\!]$ iff $\nu \in \sigma^*_\nu I[\![\phi]\!]$ iff $\nu \in \sigma^*_\omega I[\![\phi]\!]$ by Corollary 16, because $\nu = \omega$ on $\mathsf{BV}(\sigma\alpha)^\complement$ and σ is $\mathsf{BV}(\sigma\alpha)$-admissible for ϕ. □

The uniform substitute of a game can be won into X from state ω in an interpretation iff the game itself can be won into X from ω in its adjoint interpretation. The most complicated part of the uniform substitution lemma proofs is the case of repetition α^*, because it has a least fixpoint semantics. The proof needs to be set up carefully by transfinite induction (instead of induction along the number of program loop iterations, which is finite for hybrid systems).

Lemma 19 (Uniform substitution for games). *The uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I, \omega$ for I, ω have the same semantics for all* games *α:*

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

Proof. The proof is by structural induction on α, simultaneously with Lemma 18, simultaneously for all ω and X.

1. $\omega \in I\llbracket\sigma(a)\rrbracket\big(X\big) = I\llbracket\sigma a\rrbracket\big(X\big) = \sigma^*_\omega I(a)(X) = \sigma^*_\omega I\llbracket a\rrbracket\big(X\big)$ for game symbol a
2. $\omega \in I\llbracket\sigma(x:=\theta)\rrbracket\big(X\big) = I\llbracket x:=\sigma\theta\rrbracket\big(X\big)$ iff $X \ni \omega_x^{I\omega\llbracket\sigma\theta\rrbracket} = \omega_x^{\sigma^*_\omega I\omega\llbracket\theta\rrbracket}$ by using Lemma 17, which is, thus, equivalent to $\omega \in \sigma^*_\omega I\llbracket x:=\theta\rrbracket\big(X\big)$.
3. $\omega \in I\llbracket\sigma(x'=\theta\,\&\,\psi)\rrbracket\big(X\big) = I\llbracket x'=\sigma\theta\,\&\,\sigma\psi\rrbracket\big(X\big)$ (provided that σ is $\{x,x'\}$-admissible for θ,ψ) iff $\exists\varphi : [0,T]\to\mathcal{S}$ with $\varphi(0)=\omega$ on $\{x'\}^\complement$, $\varphi(T)\in X$ and for all $t\geq 0$: $\frac{\mathrm{d}\varphi(s)}{\mathrm{d}s}(t) = I\varphi(t)\llbracket\sigma\theta\rrbracket = \sigma^*_{\varphi(t)}I\varphi(t)\llbracket\theta\rrbracket$ by Lemma 17 and $\varphi(t)\in I\llbracket\sigma\psi\rrbracket$, which, by Lemma 18, holds iff $\varphi(t)\in\sigma^*_{\varphi(t)}I\llbracket\psi\rrbracket$.

   Conversely, $\omega \in \sigma^*_\omega I\llbracket x'=\theta\,\&\,\psi\rrbracket\big(X\big)$ iff $\exists\varphi : [0,T]\to\mathcal{S}$ with $\varphi(0)=\omega$ on $\{x'\}^\complement$ and $\varphi(T)\in X$ and for all $t\geq 0$: $\frac{\mathrm{d}\varphi(s)}{\mathrm{d}s}(t) = \sigma^*_\omega I\varphi(t)\llbracket\theta\rrbracket$ and $\varphi(t)\in\sigma^*_\omega I\llbracket\psi\rrbracket$. Both sides agree since $\sigma^*_\omega I\llbracket\theta\rrbracket = \sigma^*_{\varphi(t)}I\llbracket\theta\rrbracket$ and $\sigma^*_{\varphi(t)}I\llbracket\psi\rrbracket = \sigma^*_\omega I\llbracket\psi\rrbracket$ by Corollary 16 as σ is $\{x,x'\}$-admissible for θ and ψ and $\omega=\varphi(t)$ on $\mathsf{BV}(x'=\theta\,\&\,\psi)^\complement \supseteq \{x,x'\}^\complement$ by Lemma 13.
4. $\omega \in I\llbracket\sigma(?\psi)\rrbracket\big(X\big) = I\llbracket ?\sigma\psi\rrbracket\big(X\big) = I\llbracket\sigma\psi\rrbracket\cap X$ iff, by Lemma 18, it is the case that $\omega\in\sigma^*_\omega I\llbracket\psi\rrbracket\cap X = \sigma^*_\omega I\llbracket ?\psi\rrbracket\big(X\big)$.
5. $\omega \in I\llbracket\sigma(\alpha\cup\beta)\rrbracket\big(X\big) = I\llbracket\sigma\alpha\cup\sigma\beta\rrbracket\big(X\big) = I\llbracket\sigma\alpha\rrbracket\big(X\big)\cup I\llbracket\sigma\beta\rrbracket\big(X\big)$, which, by induction hypothesis, is equivalent to $\omega\in\sigma^*_\omega I\llbracket\alpha\rrbracket\big(X\big)$ or $\omega\in\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)$, which is $\omega\in\sigma^*_\omega I\llbracket\alpha\rrbracket\big(X\big)\cup\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big) = \sigma^*_\omega I\llbracket\alpha\cup\beta\rrbracket\big(X\big)$.
6. $\omega \in I\llbracket\sigma(\alpha;\beta)\rrbracket\big(X\big) = I\llbracket\sigma\alpha;\sigma\beta\rrbracket\big(X\big) = I\llbracket\sigma\alpha\rrbracket\big(I\llbracket\sigma\beta\rrbracket\big(X\big)\big)$ (provided σ is $\mathsf{BV}(\sigma\alpha)$-admissible for β), which holds iff $\omega\in I\llbracket\sigma\alpha\rrbracket\big(I\llbracket\sigma\beta\rrbracket\big(X\big){\downarrow}\omega(\mathsf{BV}(\sigma\alpha)^\complement)\big)$ by Lemma 13.

   Starting conversely: $\omega\in\sigma^*_\omega I\llbracket\alpha;\beta\rrbracket\big(X\big) = \sigma^*_\omega I\llbracket\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)\big)$, iff, by IH, $\omega\in I\llbracket\sigma\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)\big)$ iff, by Lem. 13, $\omega\in I\llbracket\sigma\alpha\rrbracket\big(\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big){\downarrow}\omega(\mathsf{BV}(\sigma\alpha)^\complement)\big)$. Consequently, it suffices to show that both winning conditions are equal:

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

   Consider any $\nu=\omega$ on $\mathsf{BV}(\sigma\alpha)^\complement$ to show: $\nu\in I\llbracket\sigma\beta\rrbracket\big(X\big)$ iff $\nu\in\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)$. By IH, $\nu\in I\llbracket\sigma\beta\rrbracket\big(X\big)$ iff $\nu\in\sigma^*_\nu I\llbracket\beta\rrbracket\big(X\big)$ iff $\nu\in\sigma^*_\omega I\llbracket\beta\rrbracket\big(X\big)$ by Corollary 16, because $\nu=\omega$ on $\mathsf{BV}(\sigma\alpha)^\complement$ and σ is $\mathsf{BV}(\sigma\alpha)$-admissible for β.
7. The case $\omega\in I\llbracket\sigma(\alpha^*)\rrbracket\big(X\big) = I\llbracket(\sigma\alpha)^*\rrbracket\big(X\big)$ (provided σ is $\mathsf{BV}(\sigma\alpha)$-admissible for α) uses an equivalent inflationary fixpoint formulation [5, Thm. 3.5]:

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

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

$$\begin{aligned}
\varrho^0(X) &\overset{\text{def}}{=} X \\
\varrho^{\kappa+1}(X) &\overset{\text{def}}{=} X\cup\sigma^*_\omega I\llbracket\alpha\rrbracket\big(\varrho^\kappa(X)\big) && \kappa+1 \text{ a successor ordinal}
\end{aligned}$$

$$\varrho^\lambda(X) \overset{\text{def}}{=} \bigcup_{\kappa<\lambda} \varrho^\kappa(X) \qquad\qquad \lambda \neq 0 \text{ a limit ordinal}$$

The equivalence $\omega \in I[\![\sigma(\alpha^*)]\!]\big(X\big) = \tau^\infty(X)$ iff $\omega \in \sigma^*_\omega I[\![\alpha^*]\!]\big(X\big) = \varrho^\infty(X)$ follows from a proof that:

$$\text{for all } \kappa \text{ and all } X \text{ and all } \nu = \omega \text{ on } \mathsf{BV}(\sigma\alpha)^\complement:\ \nu \in \tau^\kappa(X) \text{ iff } \nu \in \varrho^\kappa(X)$$

This is proved by induction on ordinal κ, which is either 0, a limit ordinal $\lambda \neq 0$, or a successor ordinal.

$\kappa = 0$: $\nu \in \tau^0(X)$ 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 $\nu \in \bigcup_{\kappa<\lambda} \varrho^\kappa(X) = \varrho^\lambda(X)$.

$\kappa + 1$: $\nu \in \tau^{\kappa+1}(X) = X \cup I[\![\sigma\alpha]\!]\big(\tau^\kappa(X)\big)$, which, by Lemma 13, is equivalent to $\nu \in X \cup I[\![\sigma\alpha]\!]\big(\tau^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma\alpha)^\complement)\big)$
Starting from the other end, $\nu \in \varrho^{\kappa+1}(X) = X \cup \sigma^*_\omega I[\![\alpha]\!]\big(\varrho^\kappa(X)\big)$ iff, by Corollary 16 using $\nu = \omega$ on $\mathsf{BV}(\sigma\alpha)^\complement \supseteq \mathsf{BV}(\alpha)^\complement$, $\nu \in X \cup \sigma^*_\nu I[\![\alpha]\!]\big(\varrho^\kappa(X)\big)$ iff, by induction hypothesis on α, $\nu \in X \cup I[\![\sigma\alpha]\!]\big(\varrho^\kappa(X)\big)$ iff, by Lemma 13, $\nu \in X \cup I[\![\sigma\alpha]\!]\big(\varrho^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma\alpha)^\complement)\big)$ Consequently, it suffices to show that both winning conditions are equal: $\tau^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma\alpha)^\complement) = \varrho^\kappa(X){\downarrow}\nu(\mathsf{BV}(\sigma\alpha)^\complement)$. Consider any state $\mu = \omega$ on $\mathsf{BV}(\sigma\alpha)^\complement$, then $\mu \in \tau^\kappa(X)$ iff $\mu \in \varrho^\kappa(X)$ by induction hypothesis on $\kappa < \kappa + 1$.

8. $\omega \in I[\![\sigma(\alpha^d)]\!]\big(X\big) = I[\![(\sigma\alpha)^d]\!]\big(X\big) = \big(I[\![\sigma\alpha]\!]\big(X^\complement\big)\big)^\complement$ iff $\omega \notin I[\![\sigma\alpha]\!]\big(X^\complement\big)$, which, by IH, is equivalent to $\omega \notin \sigma^*_\omega I[\![\alpha]\!]\big(X^\complement\big)$, which is, in turn, equivalent to $\omega \in \big(\sigma^*_\omega I[\![\alpha]\!]\big(X^\complement\big)\big)^\complement = \sigma^*_\omega I[\![\alpha^d]\!]\big(X\big)$. □

4.2 Soundness

Soundness of uniform substitution for dGL now follows from the above uniform substitution lemmas with the same proof that it had from corresponding lemmas in dL [6] (see [8]). Due to the modular setup of uniform substitutions, the change from dL to dGL is reflected in how the uniform substitution lemmas are proved, not in how they are used for the soundness of proof rule US. A proof rule is *sound* iff validity of all its premises implies validity of its conclusion.

Theorem 20 (Soundness of uniform substitution). *Proof rule US is sound.*

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

As in dL, uniform substitutions can soundly instantiate locally sound proof rules or proofs [6] just like proof rule US soundly instantiates axioms or other valid formulas (Theorem 20). An inference or proof rule is *locally sound* iff its conclusion is valid in any interpretation I in which all its premises are valid. All locally sound proof rules are sound. The use of Theorem 21 in a proof is marked USR.

$$[\cdot]\quad [a]p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})$$

$$\langle{:=}\rangle\quad \langle x := f\rangle p(x) \leftrightarrow p(f)$$

$$\mathrm{DS}\quad \langle x' = f\rangle p(x) \leftrightarrow \exists t{\geq}0\, \langle x := x + ft\rangle p(x)$$

$$\langle ?\rangle\quad \langle ?q\rangle p \leftrightarrow q \land p$$

$$\langle\cup\rangle\quad \langle a \cup b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle p(\bar{x}) \lor \langle b\rangle p(\bar{x})$$

$$\langle ;\rangle\quad \langle a; b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle\langle b\rangle p(\bar{x})$$

$$\langle {}^*\rangle\quad \langle a^*\rangle p(\bar{x}) \leftrightarrow p(\bar{x}) \lor \langle a\rangle\langle a^*\rangle p(\bar{x})$$

$$\langle {}^d\rangle\quad \langle a^d\rangle p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})$$

$$\mathrm{M}\quad \frac{p(\bar{x}) \rightarrow q(\bar{x})}{\langle a\rangle p(\bar{x}) \rightarrow \langle a\rangle q(\bar{x})}$$

$$\mathrm{FP}\quad \frac{p(\bar{x}) \lor \langle a\rangle q(\bar{x}) \rightarrow q(\bar{x})}{\langle a^*\rangle p(\bar{x}) \rightarrow q(\bar{x})}$$

$$\mathrm{MP}\quad \frac{p \quad p \rightarrow q}{q}$$

$$\forall\quad \frac{p(x)}{\forall x\, p(x)}$$

Fig. 2. Differential game logic axioms and axiomatic proof rules

Theorem 21 (Soundness of uniform substitution of rules). *If* $\mathsf{FV}(\sigma) = \emptyset$*, all uniform substitution instances of locally sound inferences are locally sound:*

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi}\ \textit{locally sound} \qquad \textit{implies} \qquad \frac{\sigma\phi_1 \quad \dots \quad \sigma\phi_n}{\sigma\psi}\ \textit{locally sound}$$

5 Axioms

Axioms and axiomatic proof rules for differential game logic are listed in Fig. 2, where $\bar{x}$ is the (finite-dimensional) vector of all relevant variables. The axioms are concrete dGL formulas that are valid. The axiomatic proof rules are concrete formulas for the premises and concrete formulas for the conclusion that are locally sound. This makes Fig. 2 straightforward to implement by copy-and-paste. Theorem 20 can be used to instantiate axioms to other dGL formulas. Theorem 21 can be used to instantiate axiomatic proof rules to other concrete dGL inferences. Complete axioms for first-order logic from elsewhere [6] and a proof rule (written $\mathbb{R}$) for decidable real arithmetic [11] are assumed as a basis.

The axiom $\langle ;\rangle$, for example, expresses that Angel has a winning strategy in game $a; b$ to achieve $p(\bar{x})$ if and only if she has a winning strategy in game a to achieve $\langle b\rangle p(\bar{x})$, i.e., to reach the region from which she has a winning strategy in game b to achieve $p(\bar{x})$. Rule US can instantiate axiom $\langle ;\rangle$, for example, with $\sigma = \{a \mapsto (v := 2 \cup v := x{+}1)^d, b \mapsto x' = v, p(\bar{x}) \mapsto x > 0\}$ to prove

$$\langle (v := 2 \cup v := x{+}1)^d; x' = v\rangle x > 0 \leftrightarrow \langle (v := 2 \cup v := x{+}1)^d\rangle\langle x' = v\rangle x > 0$$

The right-hand formula can be simplified when using US again to instantiate axiom $\langle {}^d\rangle$ with $\sigma = \{a \mapsto v := 2 \cup v := x{+}1, p(\bar{x}) \mapsto \langle x' = v\rangle x > 0\}$ to prove

$$\langle (v := 2 \cup v := x{+}1)^d\rangle\langle x' = v\rangle x > 0 \leftrightarrow \neg\langle v := 2 \cup v := x{+}1\rangle\neg\langle x' = v\rangle x > 0$$

When eliding the equivalences and writing down the resulting formula along with the axiom that was uniformly substituted to obtain it, this yields a proof:

$$\begin{array}{rl}
 & j(x) \to\neg(\neg\exists t{\geq}0\, x+2t>0 \lor \neg\exists t{\geq}0\, x+(x{+}1)t>0) \\ \hline
\langle{:=}\rangle & j(x) \to\neg(\neg\exists t{\geq}0\, \langle x:=x+2t\rangle x>0 \lor \langle v:=x{+}1\rangle\neg\exists t{\geq}0\, \langle x:=x+vt\rangle x>0) \\ \hline
\mathrm{DS} & j(x) \to\neg(\neg\langle x'=2\rangle x>0 \lor \langle v:=x{+}1\rangle\neg\langle x'=v\rangle x>0) \\ \hline
\langle{:=}\rangle & j(x) \to\neg(\langle v:=2\rangle\neg\langle x'=v\rangle x>0 \lor \langle v:=x{+}1\rangle\neg\langle x'=v\rangle x>0) \\ \hline
\langle\cup\rangle & j(x) \to\neg\langle v:=2 \cup v:=x{+}1\rangle\neg\langle x'=v\rangle x>0 \\ \hline
\langle{}^{d}\rangle & j(x) \to\langle(v:=2 \cup v:=x{+}1)^d\rangle\langle x'=v\rangle x>0 \\ \hline
\langle;\rangle & j(x) \to\langle(v:=2 \cup v:=x{+}1)^d; x'=v\rangle x>0
\end{array}$$

It is soundness-critical that US checks velocity v is not bound in the ODE when substituting it for f in DS, since $x+vt$ is not, otherwise, the correct solution of $x'=v$. Likewise, the velocity assignment $v:=x{+}1$ cannot soundly be substituted into the differential equation via $\langle{:=}\rangle$, which US prevents as x is bound in $x'=v$. Instead, axiom $\langle{:=}\rangle$ for $v:=x{+}1$ needs to be delayed until after solving by DS. If it were $v:=x^2{+}1$ instead of $v:=x{+}1$, then rule $\mathbb{R}$ would finish the proof. But for the above proof with $v:=x{+}1$ to finish, extra assumptions need to be identified.

With $\sigma = \{a \mapsto (v:=2 \cup v:=x{+}1)^d; x'=v, p(\bar{x}) \mapsto x{>}0, q(\bar{x}) \mapsto x^2{>}0\}$, USR instantiates axiomatic rule M to prove an inference continuing the proof:

$$\mathrm{USR,M}\;\dfrac{x{>}0 \to x^2{>}0}{\langle(v:=2 \cup v:=x{+}1)^d; x'=v\rangle x{>}0 \to \langle(v:=2 \cup v:=x{+}1)^d; x'=v\rangle x^2{>}0}$$

Variable x can be used in the postconditions despite being bound in the game. Likewise, rule USR can instantiate the above proof with $\sigma = \{j(\cdot) \mapsto \cdot{>}{-1}\}$ to:

$$\begin{array}{rl}
\mathbb{R} & \overline{x>-1 \to\neg(\neg\exists t{\geq}0\, x+2t>0 \lor \neg\exists t{\geq}0\, x+(x{+}1)t>0)} \\ \hline
\mathrm{USR} & x>-1 \to\langle(v:=2 \cup v:=x{+}1)^d; x'=v\rangle x>0
\end{array}$$

USR soundly instantiates the inference from premise to conclusion of the proof without having to change or repeat any part of the proof. Uniform substitutions enable flexible but sound reasoning forwards, backwards, on proofs, or mixed [6]. Without USR, these features would complicate soundness-critical prover cores.

Since the axioms and axiomatic proof rules in Fig. 2 are themselves instances of axiom schemata and proof rule schemata that axiomatize dGL [5], they are (even locally!) *sound*. Axiom DS stems from dL [6] and is for solving constant differential equations. Now that differentials are available, all differential axioms such as the Leibniz axiom $(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$ and all other axioms for differential equations [6] can be added to dGL. Furthermore, hybrid games make it possible to equivalently replace differential equations with evolution domains by hybrid games without domain constraints [5, Lem. 3.4].

The converse challenge for *completeness* is to prove that uniform substitutions are flexible enough to prove all required instances of dGL axioms and axiomatic proof rules. A dGL formula ϕ is called *surjective* iff rule US can instantiate ϕ to any of its axiom schema instances, which are those formulas that are obtained by just replacing game symbols a uniformly by any hybrid game etc. An axiomatic rule is called *surjective* iff USR can instantiate it to any of its proof rule schema instances. The axiom $\langle ? \rangle$ is surjective, as it does not have any bound variables, so its instances are admissible. Similarly rules MP and rule $\forall$ become surjective [6]. The proof of the following lemma transfers from prior work [6, Lem. 39], since any hybrid game can be substituted for a game symbol.

Lemma 22 (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.*

Unfortunately, none of the axioms from Fig. 2 satisfy the assumptions of Lemma 22. While the argument from previous work would succeed [6], the trick to simplify the proof is to consider $p(\bar{x})$ to be $\langle c \rangle true$ for some game symbol c. Then any formula φ can be instantiated for $p(\bar{x})$ alias $\langle c \rangle true$ by substituting the game symbol c with the game $?\varphi$ and subsequently using the surjective axiom $\langle ? \rangle$ to replace the resulting $\langle ?\varphi \rangle true$ by $\varphi \land true$ or its equivalent φ as intended. This makes axioms $[\cdot]$,$\langle ? \rangle$,$\langle \cup \rangle$,$\langle ; \rangle$,$\langle ^* \rangle$,$\langle ^d \rangle$ and all axiomatic rules in Fig. 2 surjective.

With Lemma 22 to show that all schema instantiations required for completeness are provable by US,USR from axioms or axiomatic rules, relative completeness of dGL follows immediately from a previous schematic completeness result for dGL [5] and relative completeness of uniform substitution for dL [6].

Theorem 23 (Relative completeness). *The* dGL *calculus is a* sound and complete axiomatization *of hybrid games relative to* any *differentially expressive logic*[3] *L, i.e., every valid* dGL *formula is provable in* dGL *from L tautologies.*

6 Related Work

Since the primary impact of uniform substitution is on conceptual simplicity and a significantly simpler prover implementation, this related work discussion focuses on hybrid games theorem proving. A broader discussion of both hybrid games and uniform substitution themselves is provided in the literature [5,6]. The approach presented here also helps discrete game logic [4], but that is only challenging after a suitable generalization beyond the propositional case.

Prior approaches to hybrid games theorem proving are either based on differential game logic [5,7] or on an exterior game embedding of differential dynamic logic [10]. This paper is based on prior findings on differential game logic [5] that it complements by giving an *explicit construction* for uniform substitution. This enables a purely axiomatic version of dGL that does not need the axiom schemata or proof rule schemata from previous approaches [5,7]. This change makes it substantially simpler to implement dGL soundly in a theorem prover. The exterior

[3] 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.

game embedding of differential dynamic logic [10] was implemented with proof rule schemata in KeYmaera and was, thus, significantly more complex.

The primary and significant challenge of this paper compared to previous uniform substitution approaches [2,6,1] arose from the semantics of hybrid games, which need a significantly different set-valued winning region style. The root-cause is that, unlike the normal modal logic dL, dGL is a subregular modal logic [5]. Especially, Kripke's axiom $[\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi)$ is unsound for dGL.

7 Conclusion and Future Work

This paper provides an explicit construction of uniform substitutions and proves it sound for differential game logic. It also indicates that uniform substitutions are flexible when a logic is changed. The modularity principles of uniform substitution hold what they promise, making an implementation in a theorem prover exceedingly straightforward. The biggest challenge was the semantic generalization of the soundness proofs to the subtle interactions caused by hybrid games.

In future work it could be interesting to devise a framework for the general construction of uniform substitutions for arbitrary logics from a certain family. The challenge is that such an approach partially goes against the spirit of uniform substitution, which is built for flexibility (straightforward and easy to change), not necessarily generality (already preequipped to reconfigure for all possible future changes). Such generality seems to require a schematic understanding, possibly self-defeating for the simplicity advantages of uniform substitutions.

References

1. Bohrer, B., Rahli, V., Vukotic, I., Völp, M., Platzer, A.: Formally verified differential dynamic logic. In: Bertot, Y., Vafeiadis, V. (eds.) CPP. ACM (2017)
2. Church, A.: Introduction to Mathematical Logic. Princeton Univ. Press (1956)
3. 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)
4. Parikh, R.: Propositional game logic. In: FOCS. pp. 195–200. IEEE (1983)
5. Platzer, A.: Differential game logic. ACM Trans. Comput. Log. 17(1) (2015)
6. Platzer, A.: A complete uniform substitution calculus for differential dynamic logic. J. Autom. Reas. 59(2), 219–265 (2017)
7. Platzer, A.: Differential hybrid games. ACM Trans. Comput. Log. 18(3) (2017)
8. Platzer, A.: Uniform substitution for differential game logic. CoRR abs/1804.05880 (2018)
9. Platzer, A., Quesel, J.D.: KeYmaera: A hybrid theorem prover for hybrid systems. In: Armando, A., Baumgartner, P., Dowek, G. (eds.) IJCAR. LNCS, vol. 5195, pp. 171–178. Springer, Berlin (2008)
10. 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 (2012)
11. Tarski, A.: A Decision Method for Elementary Algebra and Geometry. University of California Press, Berkeley, 2nd edn. (1951)