2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science

The Complete Proof Theory of Hybrid Systems

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

***Abstract*—Hybrid systems are a fusion of continuous dynamical systems and discrete dynamical systems. They freely combine dynamical features from both worlds. For that reason, it has often been claimed that hybrid systems are more challenging than continuous dynamical systems and than discrete systems. We now show that, proof-theoretically, this is not the case. We present a complete proof-theoretical alignment that interreduces the discrete dynamics and the continuous dynamics of hybrid systems. We give a *sound and complete axiomatization* of hybrid systems relative to continuous dynamical systems and a sound and complete axiomatization of hybrid systems relative to discrete dynamical systems. Thanks to our axiomatization, proving properties of hybrid systems is exactly the same as proving properties of continuous dynamical systems and again, exactly the same as proving properties of discrete dynamical systems. This fundamental cornerstone sheds light on the nature of hybridness and enables flexible and provably perfect combinations of discrete reasoning with continuous reasoning that lift to all aspects of hybrid systems and their fragments.**

***Index Terms*—proof theory; hybrid dynamical systems; differential dynamic logic; axiomatization; completeness**

I. Introduction

Hybrid systems are dynamical systems that combine discrete dynamics and continuous dynamics. They play an important role, e.g., in modeling systems that use computers to control physical systems. Hybrid systems feature (iterated) difference equations for discrete dynamics and differential equations for continuous dynamics. They, further, combine conditional switching, nondeterminism, and repetition. The theory of hybrid systems concluded that very limited classes of systems are undecidable [4], [6], [15]. Most hybrid systems research since focused on practical approaches for efficient approximate reachability analysis for classes of hybrid systems [3], [7], [12], [25]. Undecidability also did not stop researchers in program verification from making impressive progress. This progress, however, concerned both the practice and the theory, where logic was the key to studying the theory beyond undecidability [8], [13], [14], [20], [26].

We take a logical perspective, with which we study the logical foundations of hybrid systems and obtain interesting proof-theoretical relationships in spite of undecidability. We have developed a logic and proof calculus for hybrid systems [21], [23] in which it becomes meaningful to investigate concepts like "what is true for a hybrid system" and "what can be proved about a hybrid system" and investigate how they are related. Our proof calculus is *sound*, i.e., all it can prove is true. Soundness should be *sine qua non* for formal verification, but is so complex for hybrid systems [7], [25] that it is often inadvertently forsaken. In logic, we can simply ensure soundness by checking it locally per proof rule.

More intriguingly, however, our logical setting also enables us to ask the converse: is the proof calculus *complete*, i.e., can it prove all that is true? A corollary to Gödel's incompleteness theorem shows that hybrid systems do not have a sound and complete calculus that is fully effective, because both their discrete fragment and their continuous fragment alone are nonaxiomatizable since each can define integer arithmetic [21, Theorem 2]. But logic can do better. The suitability of an axiomatization can still be established by showing completeness relative to a fragment [8], [14]. This *relative completeness*, in which we assume we were able to prove valid formulas in a fragment and prove that we can then prove all others, also tells us how subproblems are related computationally. It tells us whether one subproblem dominates the others. Standard relative completeness [8], [14], however, which works relative to the data logic, is inadequate for hybrid systems, whose complexity comes from the dynamics, not the data logic, first-order real arithmetic, which is decidable [28].

In this paper, we answer an open problem about hybrid systems proof theory [21]. We prove that differential dynamic logic ($\mathsf{d}\mathcal{L}$), which is a logic of hybrid systems, has a sound and complete axiomatization relative to its discrete fragment. This is the first discrete relative completeness result for hybrid systems.

Together with our previous result of a sound and complete axiomatization of hybrid systems relative to the continuous fragment of $\mathsf{d}\mathcal{L}$ [21], we obtain a complete alignment of the proof theories of hybrid systems, of continuous dynamical systems, and of discrete dynamical systems. Even though these classes of dynamical systems seem to have quite different intuitive expressiveness, their proof theories actually align perfectly and make them (provably) interreducible. Our $\mathsf{d}\mathcal{L}$ calculus can prove properties of hybrid systems exactly as good as properties of continuous systems can be proved, which, in turn, our calculus can do exactly as good as discrete systems can be proved. Exactly as good as any one of those subquestions can be solved, $\mathsf{d}\mathcal{L}$ can solve all others. Relative to the fragment for either system class, our $\mathsf{d}\mathcal{L}$ calculus can prove all valid properties for the others. It lifts any approximation for the fragment perfectly to all hybrid systems. This also defines a relative decision procedure for $\mathsf{d}\mathcal{L}$ sentences, because our completeness proofs are constructive.

1043-6871/12 $26.00 © 2012 IEEE
DOI 10.1109/LICS.2012.64

On top of its theoretical value and the full provability alignment that our new result shows, our discrete completeness result is significant in that—in computer science and verification—programs are closer to being understood than differential equations. Well-established and (partially) automated machinery exists for classical program verification, which, according to our result, has unexpected direct applications in hybrid systems. Completeness relative to discrete systems increases the confidence that discrete computers can solve hybrid systems questions at all. Conversely, control theory provides valuable tools for understanding continuous systems. Previously, it had been just as hard to generalize discrete computer science techniques to continuous questions as it has been to generalize continuous control approaches to discrete phenomena, let alone to the mixed case of hybrid systems.

Overall, our results provide a perfect link between both worlds and allow—in a sound and complete, and constructive way—to combine the best of both worlds. dL allows discrete reasoning as well as continuous reasoning within one single logic and proof system. The dL calculus links and transfers one side of reasoning in a provably perfect (that is sound and complete) way to the other side. For whatever question about a hybrid system (or its fragments) a discrete approach is more natural or promising, dL lifts this reasoning in a perfect way to continuous systems, and to hybrid systems, and vice versa for any part where a continuous approach is more useful.

This complete alignment of the proof theories is a fundamental cornerstone for understanding hybridness and relations between discrete and continuous dynamics. In a nutshell, we show that we can proof-theoretically equate:

"*hybrid* = *continuous* = *discrete*"

II. Differential Dynamic Logic

A. Regular Hybrid Programs

We use (regular) *hybrid programs* (HP) [21] as hybrid system models. HPs form a Kleene algebra with tests [18]. The *atomic HPs* are instantaneous discrete jump *assignments* $x := \theta$, *tests* $?\chi$ of a first-order formula[1] χ of real arithmetic, and *differential equation (systems)* $x' = \theta \,\&\, \chi$ for a continuous evolution restricted to the domain of evolution described by a first-order formula χ. Compound HPs are generated from these atomic HPs by nondeterministic choice ($\cup$), sequential composition (;), and Kleene's nondeterministic repetition (*). We use polynomials with rational coefficients as terms. HPs are defined by the following grammar (α, β are HPs, x a variable, θ a term possibly containing x, and χ a formula of first-order logic of real arithmetic):

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

The first three cases are called atomic HPs, the last three compound HPs. These operations can define all hybrid systems [23]. We, e.g., write $x' = \theta$ for the unrestricted differential equation $x' = \theta \,\&\, true$. We allow differential equation systems and use vectorial notation. Vectorial assignments are definable from scalar assignments (and ;).

A *state* ν is a mapping from variables to $\mathbb{R}$. Hence $\nu(x) \in \mathbb{R}$ is the value of variable x in state ν. The set of states is denoted $\mathcal{S}$. We denote the value of term θ in ν by $[\![\theta]\!]_\nu$. Each HP α is interpreted semantically as a binary reachability relation $\rho(\alpha)$ over states, defined inductively by:

- $\rho(x := \theta) = \{(\nu, \omega) : \omega = \nu$ except that $[\![x]\!]_\omega = [\![\theta]\!]_\nu\}$
- $\rho(?\chi) = \{(\nu, \nu) : \nu \models \chi\}$
- $\rho(x' = \theta \,\&\, \chi) = \{(\varphi(0), \varphi(r)) \;:\; \varphi(t) \models x' = \theta$ and $\varphi(t) \models \chi$ for all $0 \leq t \leq r$ for a solution $\varphi : [0, r] \to \mathcal{S}$ of any duration $r\}$; i.e., with $\varphi(t)(x') \overset{\text{def}}{=} \frac{\mathsf{d}\varphi(\zeta)(x)}{\mathsf{d}\zeta}(t)$, φ solves the differential equation and satisfies χ at all times [21]
- $\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$
- $\rho(\alpha; \beta) = \rho(\beta) \circ \rho(\alpha)$
- $\rho(\alpha^*) = \bigcup_{n \in \mathbb{N}} \rho(\alpha^n)$ with $\alpha^{n+1} \equiv \alpha^n; \alpha$ and $\alpha^0 \equiv ?true$.

We refer to our book [23] for a comprehensive background. We also refer to [23] for an elaboration how the case $r = 0$ (in which the only condition is $\varphi(0) \models \chi$) is captured by the above definition. To avoid technicalities, we consider only polynomial differential equations, which are all smooth.

B. dL Formulas

The *formulas of differential dynamic logic* (dL) are defined by the grammar (where ϕ, ψ are dL formulas, θ_1, θ_2 terms, x a variable, α a HP):

$$\phi, \psi \;::=\; \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid [\alpha]\phi$$

The *satisfaction relation* $\nu \models \phi$ is as usual in first-order logic (of real arithmetic) with the addition that $\nu \models [\alpha]\phi$ iff $\omega \models \phi$ for all ω with $(\nu, \omega) \in \rho(\alpha)$. The operator $\langle\alpha\rangle$ dual to $[\alpha]$ is defined by $\langle\alpha\rangle\phi \equiv \neg[\alpha]\neg\phi$. Consequently, $\nu \models \langle\alpha\rangle\phi$ iff $\omega \models \phi$ for some ω with $(\nu, \omega) \in \rho(\alpha)$. Operators $=, >, \leq, <, \vee, \rightarrow, \leftrightarrow, \exists x$ can be defined as usual in first-order logic. A dL formula ϕ is *valid*, written $\vDash \phi$, iff $\nu \models \phi$ for all states ν.

C. Axiomatization

Our axiomatization of dL is shown in Fig. 1. To highlight the logical essentials, we present a significantly simplified axiomatization in comparison to our earlier work [21], which was tuned for automation. The axiomatization we use here is closer to that of Pratt's dynamic logic for conventional discrete programs [14], [26]. We use the first-order Hilbert calculus (modus ponens and $\forall$-generalization) as a basis and allow all instances of valid formulas of first-order real arithmetic as axioms. The first-order theory of real-closed fields is decidable [28]. We write $\vdash \phi$ iff dL formula ϕ can be *proved* with dL rules from dL axioms (including first-order rules and axioms).

Axiom [:=] is Hoare's assignment rule. Formula $\phi(\theta)$ is obtained from $\phi(x)$ by *substituting* θ for x, provided x does not occur in the scope of a quantifier or modality binding x or a variable of θ. A modality $[\alpha]$ containing $z :=$ or z' *binds* z (written $z \in BV(\alpha)$). In axiom ['], $y(\cdot)$ is the (unique [30,

[1]The test $?\chi$ means "if χ then *skip* else *abort*". Our results generalize to rich-test dL, where $?\chi$ is a HP for any dL formula χ (Sect. II-B).

$$[:=]\quad [x:=\theta]\phi(x) \leftrightarrow \phi(\theta)$$

$$[?]\quad [?\chi]\phi \leftrightarrow (\chi \rightarrow \phi)$$

$$[']\quad [x'=\theta]\phi \leftrightarrow \forall t{\geq}0\,[x:=y(t)]\phi \qquad (y'(t)=\theta)$$

$$[\&]\quad \begin{array}{l}[x'=\theta\,\&\,\chi]\phi \\ \leftrightarrow \forall t_0{=}x_0\,[x'=\theta]\big([x'=-\theta](x_0 \geq t_0 \rightarrow \chi) \rightarrow \phi\big)\end{array}$$

$$[\cup]\quad [\alpha\cup\beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$$

$$[;]\quad [\alpha;\beta]\phi \leftrightarrow [\alpha][\beta]\phi$$

$$[^*]\quad [\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$$

$$\mathrm{K}\quad [\alpha](\phi\rightarrow\psi)\rightarrow([\alpha]\phi\rightarrow[\alpha]\psi)$$

$$\mathrm{I}\quad [\alpha^*](\phi\rightarrow[\alpha]\phi)\rightarrow(\phi\rightarrow[\alpha^*]\phi)$$

$$\mathrm{C}\quad \begin{array}{l}[\alpha^*]\forall v{>}0\,(\varphi(v)\rightarrow\langle\alpha\rangle\varphi(v-1)) \\ \rightarrow \forall v\,(\varphi(v)\rightarrow\langle\alpha^*\rangle\exists v{\leq}0\,\varphi(v))\end{array} \qquad (v\notin\alpha)$$

$$\mathrm{B}\quad \forall x\,[\alpha]\phi\rightarrow[\alpha]\forall x\,\phi \qquad (x\notin\alpha)$$

$$\mathrm{V}\quad \phi\rightarrow[\alpha]\phi \qquad (FV(\phi)\cap BV(\alpha)=\emptyset)$$

$$\mathrm{G}\quad \frac{\phi}{[\alpha]\phi}$$

Fig. 1. Differential dynamic logic axiomatization

Theorem 10.VI]) solution of the symbolic initial value problem $y'(t)=\theta, y(0)=x$. It goes without saying that variables like t are fresh in Fig. 1. Axiom $[^*]$ is the iteration axiom. Axiom K is the modal modus ponens from modal logic [17]. Axiom I is an induction schema for repetitions. Axiom C, in which v does not occur in α (written $v\notin\alpha$), is a variation of Harel's convergence rule, suitably adapted to hybrid systems over $\mathbb{R}$. Axiom B is the Barcan formula of first-order modal logic, characterizing anti-monotonic domains [17]. In order for it to be sound for dL, x must not occur in α. The converse of B is provable[2] [17, BFC p. 245] and we also call it B. Axiom V is for vacuous modalities and requires that no free variable of ϕ (written $FV(\phi)$) is bound by α. The converse holds, but we do not need it. Rule G is Gödel's necessitation rule for modal logic [17]. Note that, unlike rule G, axiom V crucially requires the variable condition that ensures that the value of ϕ is not affected by running α.

We add the new modular dL axiom [&] that reduces differential equations with evolution domain constraints to differential equations without them by checking the evolution domain constraint backwards along the reverse flow. It checks χ backwards from the end up to the initial time t_0, using that $x'=-\theta$ follows the same flow as $x'=\theta$, but backwards. See Fig. 2 for an illustration. To simplify notation, we assume that the (vector) differential equation $x'=\theta$ in axiom [&]

[2]From $\forall x\,\phi\rightarrow\phi$, derive $[\alpha](\forall x\,\phi\rightarrow\phi)$ by G, from which K and propositional logic derive $[\alpha]\forall x\,\phi\rightarrow[\alpha]\phi$. Then, first-order logic derives $[\alpha]\forall x\,\phi\rightarrow\forall x\,[\alpha]\phi$, as x is not free in the antecedent.

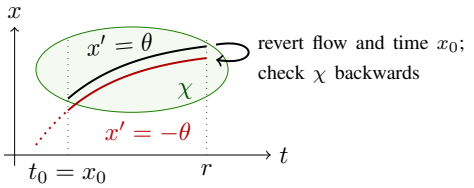

Fig. 2. "There and back again" axiom [&] checks evolution domain along backwards flow over time

already includes a clock $x_0'=1$ for tracking time. The idea behind axiom [&] is that the fresh variable t_0 remembers the initial time x_0, then x evolves forward along $x'=\theta$ for any amount of time. Afterwards, ϕ has to hold if, for all ways of evolving backwards along $x'=-\theta$ for any amount of time, $x_0\geq t_0\rightarrow\chi$ holds, i.e., χ holds at all previous times that are later than the initial time t_0. Thus, ϕ is not required to hold after a forward evolution if the evolution domain constraint χ can be left by evolving backwards for less time than the forward evolution took.

The following loop invariant rule *ind* derives from G and I. The subsequent convergence rule *con* derives from $\forall$-generalization, G, and C (like in C, v does not occur in α):

$$(ind)\quad \frac{\phi\rightarrow[\alpha]\phi}{\phi\rightarrow[\alpha^*]\phi} \qquad (con)\quad \frac{\varphi(v)\wedge v>0\rightarrow\langle\alpha\rangle\varphi(v-1)}{\varphi(v)\rightarrow\langle\alpha^*\rangle\exists v{\leq}0\,\varphi(v)}$$

While this is not the focus of this paper, we note that we have successfully used a refined sequent calculus variant of the Hilbert calculus in Fig. 1 for automatic verification of hybrid systems, including trains, cars, and aircraft; see [21], [23].

The dL calculus is sound, i.e., every dL formula provable in the dL calculus is valid. That is, $\vDash\phi$ implies $\vdash\phi$. In this paper, we study the converse question of completeness, i.e., to what extent every valid dL formula is provable.

III. Continuous Completeness

In this section, we present our result on continuous completeness, i.e., the fact that the dL calculus is a sound and complete axiomatization of dL relative to its continuous fragment. We have shown that our previous dL calculus [21] is a sound and complete axiomatization of dL relative to the continuous fragment (FOD). FOD is the *first-order logic of differential equations*, i.e., first-order real arithmetic augmented with formulas expressing properties of differential equations, that is, dL formulas of the form $[x'=\theta]F$ with a first-order formula F. We prove that our simplified dL axiomatization in Fig. 1 is sound and complete relative to FOD (the proof is in [24]):

Theorem 1 (Continuous relative completeness of dL)**.** *The* dL *calculus is a* sound and complete axiomatization *of hybrid systems relative to FOD, i.e., every valid* dL *formula can be derived from FOD tautologies.*

Axioms B and V are not needed for the proof of Theorem 1; see [24]. They are included in Fig. 1 for subsequent results.

$$\overleftarrow{\Delta}\quad [x'=f(x)]F \leftarrow \exists h_0{>}0\,\forall 0{<}h{<}h_0\,[(x:=x+hf(x))^*]F \qquad (\textit{closed } F)$$

$$\overrightarrow{\Delta}\quad [x'=f(x)]F \rightarrow \forall t{\geq}0\,\exists h_0{>}0\,\forall 0{<}h{<}h_0\,[(x:=x+hf(x))^*](t\geq 0 \rightarrow F) \qquad (\textit{open } F)$$

$$\overleftrightarrow{\Delta}\quad [x'=f(x)]F \leftrightarrow \forall t{\geq}0\,\exists \varepsilon{>}0\,\exists h_0{>}0\,\forall 0{<}h{<}h_0\,[(x:=x+hf(x))^*]\big(t\geq 0 \rightarrow \neg\mathcal{U}_\varepsilon(\neg F)\big) \qquad (\textit{open } F)$$

Fig. 3. Discrete Euler approximation axioms (for $f\in C^2$, fresh variables, $\overrightarrow{\Delta}$ and $\overleftrightarrow{\Delta}$ assume $t'=-1$)

IV. Discrete Completeness

In this section, we study discrete completeness, by which we mean that the $\mathsf{d}\mathcal{L}$ calculus is a sound and complete axiomatization of $\mathsf{d}\mathcal{L}$ relative to its discrete fragment. We denote the *discrete fragment* of $\mathsf{d}\mathcal{L}$ by DL, i.e., the fragment without differential equations (for our purposes we can restrict DL to the operators $:=,^*$ and allow either ; or vector assignments). The axiomatization in Fig. 1 is *not* complete relative to the discrete fragment, since not all differential equations even have closed-form solutions, let alone polynomial solutions. We develop an extension of the $\mathsf{d}\mathcal{L}$ calculus that is complete relative to the discrete fragment by adding one axiom for differential equations. First, we consider the case of open postconditions (Sect. IV-A), then extend it to closed postconditions (Sect. IV-B), and then to general $\mathsf{d}\mathcal{L}$ formulas with nested quantifiers and modalities (Sect. IV-C).

A. Open Discrete Completeness

Axioms like $[']$ that require solutions for differential equations cannot be complete, because most differential equations do not have closed-form solutions. We can understand properties of differential equations from a discrete perspective using discretizations of the dynamics. The question is why that should be complete or even sound. All discretization schemes have errors. Could errors for difficult cases become so large that we cannot obtain conclusive evidence? Or could errors be so unmanageable that they may mislead us into concluding incorrect properties from approximations? Our first step for an answer is for open postconditions.

The way to understand continuous dynamics as discrete dynamics is by discrete approximation. The discrete HP $(x:=x+hf(x))^*$ represents an Euler discretization of the continuous HP $x'=f(x)$ with step size $h>0$. What is the relationship of the DL formula $[(x:=x+hf(x))^*]F$ to the FOD formula $[x'=f(x)]F$? If the discrete approximation leaves F, we cannot conclude that $x'=f(x)$ leaves F, because the discretization might leave F only due to approximation errors. So we could try a smaller step size $\frac{h}{2}$. But even if we ultimately find a discrete approximation that never leaves F, we still cannot conclude that $x'=f(x)$ will stay in F, again because of approximation errors. Instead, axiom $\overleftarrow{\Delta}$ in Fig. 3 quantifies over all sufficiently fine discretizations h. For reasons that we illustrate below, axiom $\overrightarrow{\Delta}$ quantifies over all time bounds t and axiom $\overleftrightarrow{\Delta}$ quantifies over a small approximation tolerances ε. Note the nontrivial similarities when comparing the axioms in Fig. 3 with axiom $[']$. The difference is that axiom $[']$ requires a closed-form solution $y(t)$, whereas the axioms in Fig. 3 use a repeated assignment with the right-hand side $f(x)$ of the differential equation. The latter is appropriate thanks to the extra quantifiers for the approximations. The conditions of the axioms in Fig. 3 about F being open/closed can be axiomatized and are decidable over real-closed fields [28].

Theorem 2 (Soundness of approximation)**.** *The approximation axioms in Fig. 3 are sound. To simplify notation, we assume that the (vector) differential equation $x'=f(x)$ in $\overrightarrow{\Delta}$ and $\overleftrightarrow{\Delta}$ already includes an extra clock $t'=-1$.*

Before we prove Theorem 2, we develop a number of auxiliary results and consider examples that demonstrate why the conditions for the axioms in Fig. 3 are necessary. For a set $S\subseteq\mathbb{R}^n$ and a number $\varepsilon>0$ we denote the open set $\{x:\|x-y\|<\varepsilon \text{ for a } y\in S\}$ around S by $\mathcal{U}_\varepsilon(S)$. $\overline{\mathcal{U}}_\varepsilon(S)$ is $\{x:\|x-y\|\leq\varepsilon \text{ for a } y\in S\}$. For a logical formula F with the free variable (vector) x and a term ε we define the formula representing the *ε-neighborhood* around F as

$$\mathcal{U}_\varepsilon(F) \overset{\text{def}}{\equiv} \exists y\,(\|x-y\|<\varepsilon\wedge F(y))$$

The logical formula $\mathcal{U}_\varepsilon(F)$ is indeed true for exactly those values of x that are within distance $<\varepsilon$ from a y satisfying F. Before we explain the crucial equivalence axiom $\overleftrightarrow{\Delta}$, we first explain the simpler axioms $\overleftarrow{\Delta}$ and $\overrightarrow{\Delta}$, which only have an implication in one direction, not a bi-implication.

Axiom $\overleftarrow{\Delta}$ is sound for closed F. Axiom $\overleftarrow{\Delta}$ is incomplete, however, since the following valid closed property is not provable by $\overleftarrow{\Delta}$, as no approximation, however small h is, works for all time horizons t (see Fig. 4 for an illustration):

$$x^2+y^2\leq 1.1 \rightarrow [x'=y,y'=-x]x^2+y^2\leq 1.1$$

For completeness of approximation schemes, the reverse implication axiom $\overrightarrow{\Delta}$, thus, only states the existence of a step size h_0 for each time bound t. Axiom $\overleftarrow{\Delta}$ alone is insufficient for another reason, because it would be unsound for open F, since the following formula is invalid (Fig. 4):

$$x=1\wedge y=0 \rightarrow [x'=y,y'=-x](x\leq 0\rightarrow x^2+y^2>1)$$

All Euler approximations stay in $x^2+y^2>1$, e.g., when $x\leq 0$, but the dynamics only remains inside its closure $x^2+y^2\geq 1$. For the same reason, the converse of $\overrightarrow{\Delta}$ would be unsound for open F, and, thus, is insufficient. For closed F, instead, the converse of $\overrightarrow{\Delta}$ is sound and can be derived from $\overleftarrow{\Delta}$ and simple extra arguments. Unlike its converse, axiom $\overrightarrow{\Delta}$ itself, however, would not be sound for closed F, because

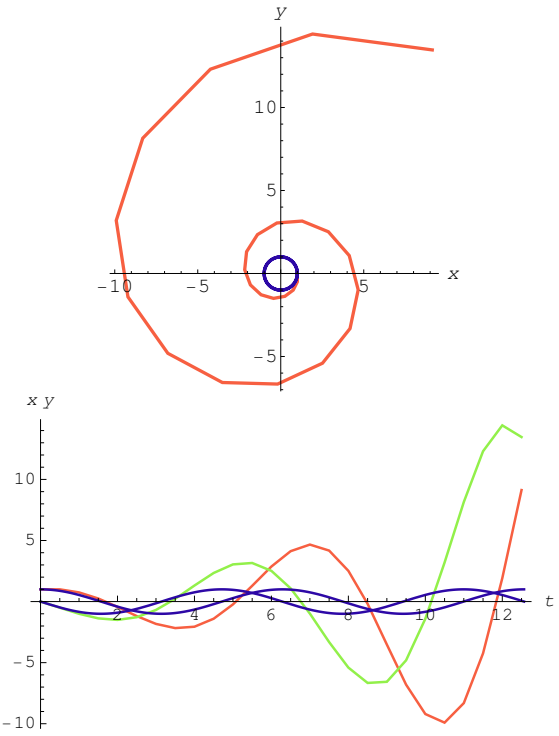

Fig. 4. **(top)** Dark circle shows true solution, light line segments show Euler approximation for $h = \frac{1}{4}$ **(bottom)** Dark true bounded trigonometric solution and Euler approximation in lighter colors with increasing errors over time t

no approximation for the following valid formula stays in $x^2 + y^2 = 1$ for any positive duration:

$$x^2 + y^2 = 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 = 1$$

This property *only* holds in the limit case that defines the solution of the differential equation and does not hold for *any* approximation with piecewise polynomial functions. Soundness of axiom $\overrightarrow{\Delta}$ implies, however, that the converse of $\overrightarrow{\Delta}$ can completely prove by approximation that a system does not leave the closure $\overline{F}$ of a postcondition, provided the true dynamics never even leaves its interior $\mathring{F}$. The above examples show, however, that this pair of axioms is incomplete, because they do not align and only prove a weaker closed property and need a stronger open assumption.

To handle properties of differential equations by approximation schemes more completely, we use axiom $\overleftrightarrow{\Delta}$, instead, which, for each time bound t, in addition, quantifies universally over a small tolerance ε that the discrete approximation tolerates around the reachable states without violating F (as reflected in $\neg\mathcal{U}_\varepsilon(\neg F)$). It is this nesting of quantifiers where $\overleftarrow{\Delta}$ and $\overrightarrow{\Delta}$ "meet" in the sense that both directions of the implication hold. The equivalence axiom $\overleftrightarrow{\Delta}$ completely handles open F. But there are valid properties with closed postconditions F that are still not provable just by $\overleftrightarrow{\Delta}$. The following formula is valid (e.g., provable by a differential invariant [22]):

$$x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1 \qquad (1)$$

Unfortunately, no Euler approximation for the dynamics, however small h is, satisfies $x^2 + y^2 \leq 1$ for any duration $t > 0$; see Fig. 4 for an illustration. The otherwise (i.e., using $\overleftrightarrow{\Delta}$) provable open property

$$x^2 + y^2 < 1.1 \rightarrow [x' = y, y' = -x]x^2 + y^2 < 1.1$$

illustrates that $\overleftrightarrow{\Delta}$ would be incomplete if we inverted the order of the quantifiers in $\overleftrightarrow{\Delta}$ to be $\exists\varepsilon{>}0\,\forall t{\geq}0$. Such time-uniform approximations are rare. Our approach, instead, uses "proof-uniform" approximations, i.e., one proof for all t, not one value ε for all t. We will answer the question to what extent our approach can always work.

To justify $\overleftrightarrow{\Delta}$, we use an estimate of the global error of Euler approximations in a neighborhood of the solution [27, Theorem 7.2.2.3]. For the sake of a self-contained presentation, we develop a proof of Theorem 3 in [24].

Theorem 3 (Global error)**.** *Let $f \in C^2$, $\hat{x}^0 \in \mathbb{R}^n$, and x a solution on $[0,t]$ of $x' = f(x), x(0) = \hat{x}^0$. Let f be Lipschitz-continuous with Lipschitz-constant L on $\mathcal{U}_E(x([0,t]))$ for some $E > 0$. Then there is an $h_0 > 0$ such that for all h with $0 < h \leq h_0$ and all $n \in \mathbb{N}$ with $nh \leq t$, the sequence $\hat{x}^{n+1} = \hat{x}^n + hf(\hat{x}^n)$ satisfies:*

$$\|x(nh) - \hat{x}^n\| \leq \frac{h}{2} \max_{\zeta\in[0,t]} \|x''(\zeta)\| \frac{e^{Lt} - 1}{L}$$

Note that we do *not* need to know the Lipschitz-constant L for our approach, only that it exists, and, in fact, only that it exists locally, which is the case for all C^1 functions, e.g., polynomials.

The following classical results are proved in [24].

Lemma 4 (Continuous distance)**.** *For a set $S \subseteq \mathbb{R}^n$ distance $d(\cdot, S) : \mathbb{R}^n \to \mathbb{R}; x \mapsto \inf_{y\in S} \|x - y\|$ is a continuous map.*

Lemma 5. *Let $K \subseteq F$ a* compact *subset of an open set F. Then $\inf_{x\in K} d(x, F^\complement) > 0$ for the complement $F^\complement$ of F.*

Equipped with this prelude of lemmas and cautionary examples we proceed to prove Theorem 2 one rule at a time.

Proof of Theorem 2: $\overleftarrow{\Delta}$: Assume the antecedent is true in a state ν. In order to show that the succedent is true in ν, consider any solution $x(\cdot)$ of $x' = f(x)$ with initial value according to ν. Let $t \geq 0$ be the duration of $x(\cdot)$. We need to show that $x(t) \models F$. Since f is C^1, it is locally Lipschitz continuous and, thus, Lipschitz continuous on every compact subset (these conditions are equivalent for locally compact spaces). Fix an arbitrary $E > 0$. As a continuous image of the compact $x([0,t]) \times \overline{\mathcal{U}}_E(0)$ under addition, $U \overset{\text{def}}{=} \overline{\mathcal{U}}_E(x([0,t])) = \bigcup_{q\in x([0,t])} \overline{\mathcal{U}}_E(q)$ is compact. See Fig. 5 for a partial illustration. Let L a Lipschitz constant for f on U. Consider any small h (and obeying $0 < h < h_0$ according to the antecedent). Let $\hat{x}^n$ be the value of variable x after n

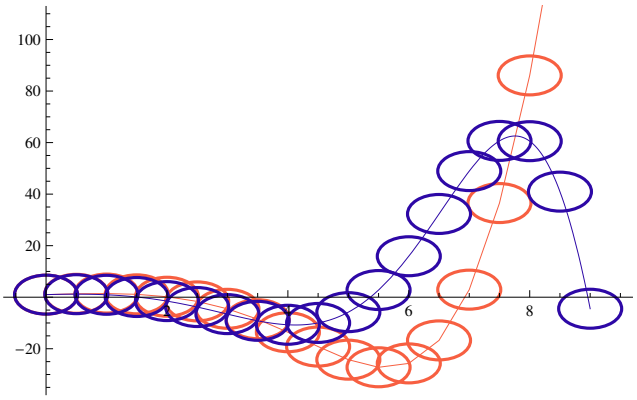

Fig. 5. Dark partial covering for dark solution and light partial covering for light approximation

iterations of the discrete program in the antecedent of $\overleftarrow{\Delta}$. By Theorem 3, for sufficiently small h with $nh \leq t$:

$$\|x(nh) - \hat{x}^n\| \leq h \underbrace{\max_{\zeta\in[0,t]} \|x''(\zeta)\| \frac{e^{Lt}-1}{2L}}_{C(t)} < \varepsilon \qquad (2)$$

The last inequality holds on $[0,t]$ for all sufficiently small $h > 0$ for the following reason. Since f is C^1, the solution[3] $x(\cdot)$ is C^2. Given the initial state ν, the remaining factor $C(t)$ is a constant depending on t, because the continuous function $x''(\zeta)$ is bounded on the compact set $[0,t]$. Here we need that L for $x' = f(x)$ is determined by ν and t and the choice of E. In short, for any $0 < \varepsilon < E$ inequality (2) holds for all sufficiently small $h > 0$ (also satisfying $h < h_0$) and all n with $nh \leq t$. Consider $n \overset{\text{def}}{=} \lfloor \frac{t}{h} \rfloor$, which satisfies $nh \leq t$ but $(n+1)h > t$. By mean-value theorem, there is a $\xi \in (nh, t)$ such that

$$\begin{aligned}\|x(t) - x(nh)\| &= \|x'(\xi)\|(t-nh) = \|f(x(\xi))\|(t-nh) \\ &\leq \underbrace{\max_{\xi\in[0,t]} \|f(x(\xi))\|}_{=:D(t)} (t-nh) < \varepsilon \qquad (3)\end{aligned}$$

The last inequality holds for all sufficiently small $h > 0$ (with $h < h_0$), because $nh \to t$ as $h \to 0$ with $n \overset{\text{def}}{=} \lfloor \frac{t}{h} \rfloor$ and $D(t)$ is a constant. Constant $D(t)$ is determined by t and the initial state for $x' = f(x)$ corresponding to ν, because the continuous function $f(x(\xi))$ is bounded on the compact set $[0,t]$. Combining (2) with (3) we obtain that for any $0 < \varepsilon < E$ and all sufficiently small $h > 0$ (also still with $h < h_0$) and $n \overset{\text{def}}{=} \lfloor \frac{t}{h} \rfloor$:

$$\|x(t) - \hat{x}^n\| \leq \|x(t) - x(nh)\| + \|x(nh) - \hat{x}^n\| < 2\varepsilon \qquad (4)$$

By antecedent, $\hat{x}^n \models F$ for all these h and n. By (4), there, thus, is a sequence of $\hat{x}^n$ in F that converges to $x(t)$ as $h \to 0$. Thus, $x(t) \models F$, because F is *closed*.

[3] x solves $x' = f(x)$, hence $x \in C$. So the composition $x' = f(x)$ is continuous, hence, $x \in C^1$. Yet, then again the composition $x' = f(x)$ is C^1, because $f \in C^1$. Henceforth, $x \in C^2$.

$\overrightarrow{\Delta}$: Assume $[x' = f(x)]F$ is true in a state ν, which fixes the initial state of the differential equation. According to Picard-Lindelöf [30, Theorem 10.VI], let $x(\cdot)$ be the unique solution (of maximal duration) of $x' = f(x)$ starting with the initial value corresponding to ν. Consider any duration $t \geq 0$ for which $x(\cdot)$ is defined. By assumption, the compact set $x([0,t])$ lies in the region where F is true, which is *open*. Thus Lemma 5 implies that there is a $\varepsilon_1 \overset{\text{def}}{=} \inf_{q\in x([0,t])} d(q, F^{\complement}) > 0$ so that the open ε_1 ball around each point of $x([0,t])$ is still in F. Here, $F^{\complement}$ is the region of states q with $q \not\models F$. Fix any $0 < E < \varepsilon_1$. Then $U \overset{\text{def}}{=} \overline{\mathcal{U}}_E(x([0,t]))$ is in F by construction and, again, compact. Part of this construction is illustrated in Fig. 5. Let L be a Lipschitz constant for f on U. Now (2), which follows from Theorem 3, implies for sufficiently small h with $nh \leq t$, that $\|x(nh) - \hat{x}^n\| < E$. Thus, $\hat{x}^n \models F$ for sufficiently small h with $nh \leq t$. Thus,

$$\exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t \geq 0 \to F)$$

is true in ν where the initial time horizon t was arbitrary. Recall that the decreasing clock $t' = -1$ was assumed to be part of the differential equation $x' = f(x)$ for simplicity. Thus, $nh \leq t$ iff, after the loop, $t \geq 0$ holds. Note that h_0 depends on t. Relation (4) relates different points in time and bounds the maximum difference of solution $x(\cdot)$ and its discrete approximation $\hat{x}^n$ when they exist for different durations by choosing sufficiently small h.

$\overleftrightarrow{\Delta}$: First, like in the proof for axiom $\overrightarrow{\Delta}$, we assume that $\nu \models [x' = f(x)]F$ and, using that F is *open*, conclude that $\overline{\mathcal{U}}_E(x([0,t]))$ is in F for an $E > 0$ that depends on ν and t. Thus (recall that t is a decreasing clock with $t' = -1$):

$$\nu \models [x' = f(x)]\big(t \geq 0 \to \forall z\, (\|z - x\| < E \to F(z))\big) \qquad (5)$$

By (2) we conclude for arbitrary $0 < \varepsilon < \frac{E}{2}$ and sufficiently small h with $nh \leq t$ that $\|x(nh) - \hat{x}^n\| < \varepsilon$. Thus,

$$\|x(nh) - z\| \leq \|x(nh) - \hat{x}^n\| + \|\hat{x}^n - z\| < 2\varepsilon \leq E$$

for all z with $\|\hat{x}^n - z\| < \varepsilon$. Hence, $F(z)$ holds by (5). Let ν_n the state reached after n iterations of the loop in $\overleftrightarrow{\Delta}$, then $\nu_n \models t \geq 0 \to \forall z\, (\|z - \hat{x}\| < \varepsilon \to F(z))$, as $\nu_n \models t \geq 0$ iff $\nu \models nh \leq t$, since t is a decreasing clock. Soundness of the "$\to$" direction of $\overleftrightarrow{\Delta}$ follows with the respective choice $\varepsilon \overset{\text{def}}{=} \frac{E}{2}$ for each t and ν.

The converse "$\leftarrow$" direction of $\overleftrightarrow{\Delta}$ follows from the soundness of axiom $\overleftarrow{\Delta}$ using that $\neg\mathcal{U}_\varepsilon(\neg F)$, which is equivalent to $\forall z\, (\|z - x\| < \varepsilon \to F(z))$, is closed since the union $\mathcal{U}_\varepsilon(S)$ is open for any S. The proof follows by observing that, for each time bound $t > 0$, the region $t{\geq}0 \to \neg\mathcal{U}_\varepsilon(\neg F)$ is closed for the purpose of $\overleftrightarrow{\Delta}$, because the solution $x(\cdot)$ cannot leave a closed region on a compact time interval $[0,t]$ (whose image is compact) unless it already leaves it on $[0,t)$. It is easy to derive this direction formally from $\overleftarrow{\Delta}$ with corresponding arithmetic. ∎

To prove Theorem 2, one could simply try a finite covering of the open balls for domain U, which exists by compactness

of $x([0,t])$. The ε neighborhoods of all points of an arbitrary finite covering, however, are not guaranteed to remain within F, see Fig. 5 at $t \approx 6$.

B. Closed Discrete Completeness

Axiom $\overleftrightarrow{\Delta}$ handles open postconditions of differential equations but not closed postconditions. Even though the property in (1) is a closed region and not provable using $\overleftrightarrow{\Delta}$ alone, this property and other closed F are still provable indirectly using $\mathsf{d}\mathcal{L}$ axioms together with $\overleftrightarrow{\Delta}$. We need the following formula that we derive[4] when no free variable of ϕ is bound in α

$$(\mathrm{V}\vee)\quad \phi \vee [\alpha]\psi \leftrightarrow [\alpha](\phi \vee \psi)$$

Proposition 6. *For every (topologically) closed F, the following formula is provable in $\mathsf{d}\mathcal{L}$:*

$$(\mathring{U})\quad [x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)]\mathcal{U}_{\check{\varepsilon}}(F)$$

Proof: For a set $S \subseteq \mathbb{R}^n$ we denote its (topological) closure by $\overline{S}$. Since $\mathbb{R}^n$ has a regular topology:

$$\begin{aligned} x \in \overline{S} &\iff \forall \check{\varepsilon}{>}0\ \exists y \in S\ \|x-y\| < \check{\varepsilon} \\ &\iff \forall \check{\varepsilon}{>}0\ \mathcal{U}_{\check{\varepsilon}}(x) \cap S \neq \emptyset \\ &\iff \forall \check{\varepsilon}{>}0\ x \in \mathcal{U}_{\check{\varepsilon}}(S) \\ &\iff x \in \bigcap_{\check{\varepsilon}>0} \mathcal{U}_{\check{\varepsilon}}(S) \end{aligned}$$

Set S is closed iff $S = \overline{S}$, i.e., iff $S = \bigcap_{\check{\varepsilon}>0} \mathcal{U}_{\check{\varepsilon}}(S)$. Since F is closed, the following equivalence is valid, hence, provable in real arithmetic

$$F \leftrightarrow \forall \check{\varepsilon}{>}0\, \mathcal{U}_{\check{\varepsilon}}(F) \quad \text{i.e.,} \quad F \leftrightarrow \forall \check{\varepsilon}\, (\neg(\check{\varepsilon}{>}0) \vee \mathcal{U}_{\check{\varepsilon}}(F))$$

Since $\check{\varepsilon}$ does not occur in the dynamics, both sides of $\mathring{U}$ are, thus, equivalent using B and V$\vee$. ∎

With an extra quantifier, $\mathring{U}$ transforms closed postconditions to open postconditions, which $\overleftrightarrow{\Delta}$ handles. Recall that $\overleftarrow{\Delta}$ also handles closed postconditions, but, unlike $\overleftrightarrow{\Delta}$ together with $\mathring{U}$, axiom $\overleftarrow{\Delta}$ cannot prove them all.

C. Discrete Completeness of $\mathsf{d}\mathcal{L}_\Delta = \mathsf{d}\mathcal{L} + \overleftrightarrow{\Delta}$

Locally closed postconditions (conjunctions $O \wedge C$ of a closed C and an open O) are handled in a sound and complete way when combining $\overleftrightarrow{\Delta}$,$\mathring{U}$, and the following formula derived from K [17, K3 p. 28]

$$([]\wedge)\quad [\alpha](\phi \wedge \psi) \leftrightarrow [\alpha]\phi \wedge [\alpha]\psi$$

One missing case is where postcondition F is a union $O \vee C$ of an open O and a closed C. We generalize the idea behind Proposition 6 to this case.

[4]"$\rightarrow$": Trivially, $(\phi \vee [\alpha]\psi) \rightarrow (\phi \vee [\alpha]\psi)$, from which V derives $(\phi \vee [\alpha]\psi) \rightarrow ([\alpha]\phi \vee [\alpha]\psi)$. Thus, $(\phi \vee [\alpha]\psi) \rightarrow [\alpha](\phi \vee \psi)$ derives by a consequence [17, K4 p. 31] of G.
"$\leftarrow$": Conversely, K derives $[\alpha](\neg\phi \rightarrow \psi) \rightarrow ([\alpha]\neg\phi \rightarrow [\alpha]\psi)$, from which V derives $[\alpha](\neg\phi \rightarrow \psi) \rightarrow (\neg\phi \rightarrow [\alpha]\psi)$.

Proposition 7. *For every (topologically) open O and (topologically) closed C, the following formula is provable in $\mathsf{d}\mathcal{L}$:*

$$(\check{U})\quad [x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \vee \mathcal{U}_{\check{\varepsilon}}(C))$$

Proof: As in the proof of Proposition 6, C is closed and $C \leftrightarrow \forall \check{\varepsilon}{>}0\, \mathcal{U}_{\check{\varepsilon}}(C)$ valid, and, thus, provable in real arithmetic. Since $\check{\varepsilon}$ is fresh, we, thus, derive equivalence of both sides of $\check{U}$ using V$\vee$ and B

$$\begin{aligned} [x' = f(x)](O \vee C) &\equiv [x' = f(x)](O \vee \forall \check{\varepsilon}{>}0 \mathcal{U}_{\check{\varepsilon}}(C)) \\ &\equiv [x' = f(x)] \forall \check{\varepsilon}{>}0\, (O \vee \mathcal{U}_{\check{\varepsilon}}(C)) \\ &\equiv \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \vee \mathcal{U}_{\check{\varepsilon}}(C)) \end{aligned}$$

∎

Like $\mathring{U}$, $\check{U}$ reduces non-open postconditions to (quantified) open postconditions, which we then want to prove by $\overleftrightarrow{\Delta}$. Can we prove all resulting formulas when they are valid? More generally, can we prove all valid $\mathsf{d}\mathcal{L}$ formulas from discrete DL this way, even if they have nested quantifiers and modalities?

The $\mathsf{d}\mathcal{L}$ calculus is complete relative to the continuous fragment (Theorem 1), but incomplete relative to the discrete fragment. We study the $\mathsf{d}\mathcal{L}$ calculus in Fig. 1 enriched with the approximation axiom $\overleftrightarrow{\Delta}$ in Fig. 3 and denote this calculus by $\mathsf{d}\mathcal{L}_\Delta$. The $\mathsf{d}\mathcal{L}_\Delta$ calculus inherits completeness relative to the continuous fragment from Theorem 1. We now prove that $\mathsf{d}\mathcal{L}_\Delta$ is a *sound and complete axiomatization* of $\mathsf{d}\mathcal{L}$ relative to discrete DL, i.e., every valid $\mathsf{d}\mathcal{L}$ formula can be proved in the $\mathsf{d}\mathcal{L}_\Delta$ calculus from valid DL formulas.

In particular, we need to prove that $\mathsf{d}\mathcal{L}$ can express all required invariants and variants, and the resulting formulas with all their nested quantifiers, repetitions, assignments, differential equations and so on are provable in the $\mathsf{d}\mathcal{L}_\Delta$ calculus from valid DL facts. This would be a tricky proof. Instead, we prove completeness in an unusual way. We leverage the fact that we have already proved $\mathsf{d}\mathcal{L}$ to be complete relative to the continuous fragment FOD in Theorem 1. Thus, every valid $\mathsf{d}\mathcal{L}$ formula can be proved in the $\mathsf{d}\mathcal{L}$ calculus (and the $\mathsf{d}\mathcal{L}_\Delta$ calculus) from valid FOD formulas. FOD is, in a sense, farthest away from $\mathsf{d}\mathcal{L}_\Delta$, because it only involves differential equations, which is precisely what is missing in DL. But by basing our proof on Theorem 1, we can piggyback on its proof how proofs about repetitions and interactions of discrete and continuous dynamics reduce in a sound and complete way to FOD formulas. So we only need to prove the remaining step that $\mathsf{d}\mathcal{L}_\Delta$ can prove all valid FOD formulas from DL tautologies, which is significantly easier than having to worry about all formulas of $\mathsf{d}\mathcal{L}$.

Theorem 8 (Discrete relative completeness of $\mathsf{d}\mathcal{L}_\Delta$)**.** *The $\mathsf{d}\mathcal{L}_\Delta$ calculus is a* sound and complete axiomatization *of hybrid systems relative to its discrete fragment DL, i.e., every valid $\mathsf{d}\mathcal{L}$ formula can be derived from DL tautologies.*

Proof: Theorems 1 and 2 show that the $\mathsf{d}\mathcal{L}_\Delta$ calculus is sound. We need to show that the $\mathsf{d}\mathcal{L}_\Delta$ calculus can prove all valid $\mathsf{d}\mathcal{L}$ formulas from instances of DL tautologies. By Theorem 1, $\mathsf{d}\mathcal{L}$ is complete relative to its continuous fragment,

i.e., elementary properties of differential equations in FOD. Consequently, all valid $\mathsf{d}\mathcal{L}$ formulas can be proved in the $\mathsf{d}\mathcal{L}$ (and $\mathsf{d}\mathcal{L}_\Delta$) calculus from instances of valid FOD formulas. All that remains to be shown is that we can then prove all those valid FOD formulas from valid formulas of discrete DL in the $\mathsf{d}\mathcal{L}_\Delta$ calculus. Consider any valid FOD formula ϕ. We proceed by induction on the structure of ϕ and show that $\mathsf{d}\mathcal{L}_\Delta$ can (provably) translate ϕ into an equivalent DL formula $\phi^\#$ (with the same free variables), which can be proved by assumption. Observe that the construction of $\phi^\#$ from ϕ is effective.

1) When ϕ is a (valid) formula of first-order real arithmetic, then $\phi^\# \overset{\text{def}}{\equiv} \phi$ is already in DL and provable by assumption. First-order real arithmetic is even decidable by quantifier elimination [28].
2) When ϕ is of the form $[x' = f(x)]F$ with a first-order (or semialgebraic) formula F of real arithmetic[5], then, by a standard boolean argument for normal forms applied to semialgebraic sets obtained by quantifier elimination [28], F is *provably* equivalent to a formula of the form
$$\bigwedge_{i=1}^{m} \left(\bigvee_j p_{i,j} > 0 \vee \bigvee_k q_{i,k} \geq 0 \right)$$
with polynomials $p_{i,j}$ and $q_{i,k}$. As a preimage of an open set, the set $\{x \in \mathbb{R}^n : p_{i,j}(x) > 0\}$ is an open set, since $p_{i,j}$ is a continuous function. Dually, the set where $q_{i,k} \geq 0$ is a closed set, because it is the complement of the open set where $-q_{i,k} > 0$. As a union of open sets, the set where $O_i \overset{\text{def}}{\equiv} \bigvee_j p_{i,j} > 0$ holds is open. As a *finite* union of closed sets, the set where $C_i \overset{\text{def}}{\equiv} \bigvee_k q_{i,k} \geq 0$ holds is closed. This gives the following (provable) equivalence:
$$\vdash F \leftrightarrow \bigwedge_{i=1}^{m} (O_i \vee C_i)$$
Formula $[]\wedge$, which derives from K, thus, derives
$$\vdash \phi \leftrightarrow \bigwedge_{i=1}^{m} [x' = f(x)](O_i \vee C_i)$$
With m uses of $\check{U}$, we derive
$$\vdash \phi \leftrightarrow \bigwedge_{i=1}^{m} \forall \check{\varepsilon}{>}0\, [x' = f(x)](O_i \vee \mathcal{U}_{\check{\varepsilon}}(C_i))$$
Since, for $\check{\varepsilon} > 0$, each $O_i \vee \mathcal{U}_{\check{\varepsilon}}(C_i)$ is open for every i, we, therefore, derive with m uses of axiom $\overleftrightarrow{\Delta}$ that $\vdash \phi \leftrightarrow \phi^\#$ where
$$\phi^\# \overset{\text{def}}{\equiv} \bigwedge_{i=1}^{m} \forall \check{\varepsilon}{>}0\, \psi(O_i \vee \mathcal{U}_{\check{\varepsilon}}(C_i))$$
By $\psi(O_i \vee \mathcal{U}_{\check{\varepsilon}}(C_i))$ we denote the DL formula in the right-hand side of axiom $\overleftrightarrow{\Delta}$ with $O_i \vee \mathcal{U}_{\check{\varepsilon}}(C_i)$ in place of F. Thus, $\vdash \phi \leftrightarrow \phi^\#$ is provable in the $\mathsf{d}\mathcal{L}_\Delta$ calculus, $\phi^\#$ is in DL, and, thus, provable by assumption.
3) When ϕ is of the form $[x' = f(x)\,\&\,\chi]F$, then it is by axiom $[\&]$ provably equivalent to a formula without evolution domain restrictions, which is structurally simpler and, thus, provable from DL by induction hypothesis.
4) When ϕ is of the form $\neg\psi$, then, by induction hypothesis, the simpler formula ψ is provably equivalent to the DL formula $\psi^\#$. This equivalence $\psi \leftrightarrow \psi^\#$ is provable in $\mathsf{d}\mathcal{L}_\Delta$ by induction hypothesis. Consequently, ϕ is (in $\mathsf{d}\mathcal{L}_\Delta$) provably equivalent to $\phi^\# \overset{\text{def}}{\equiv} \neg(\psi^\#)$, which is a DL formula and, thus, provable by assumption.
5) When ϕ is of the form $\phi_1 \wedge \phi_2$, then ϕ is provable from DL by induction hypothesis, because both ϕ_1 and ϕ_2 can be turned into DL formulas $\phi_1^\#$ and $\phi_2^\#$, respectively, with provable $\phi_i \leftrightarrow \phi_i^\#$. Thus, $\phi_1 \wedge \phi_2 \leftrightarrow \phi_1^\# \wedge \phi_2^\#$ is provable in $\mathsf{d}\mathcal{L}_\Delta$.
6) When ϕ is of the form $\forall x\, \psi$, then, by induction hypothesis, ψ is provably equivalent to a DL formula $\psi^\#$, i.e., $\psi \leftrightarrow \psi^\#$ is provable in $\mathsf{d}\mathcal{L}_\Delta$. Thus, $\forall x\, \psi$ is, by congruence, provably equivalent to $\phi^\# \overset{\text{def}}{\equiv} \forall x\, (\psi^\#)$, which is a DL formula and, thus, provable by assumption. ∎

As a corollary to this proof and Lemma 16 in the long version [24], we obtain another interesting result relating the expressiveness of the discrete and continuous fragments of $\mathsf{d}\mathcal{L}$.

Theorem 9 ($\mathsf{d}\mathcal{L}$ equi-expressibility)**.** *The logic $\mathsf{d}\mathcal{L}$ is* expressible *in FOD and in DL: for each $\mathsf{d}\mathcal{L}$ formula ϕ there is a FOD formula $\phi^\flat$ that is equivalent, i.e., $\vDash \phi \leftrightarrow \phi^\flat$ and a DL formula $\phi^\#$ that is equivalent, i.e., $\vDash \phi \leftrightarrow \phi^\#$. The converse holds trivially. Furthermore, the construction of $\phi^\flat$ and $\phi^\#$ is effective.*

The proof of Theorem 8 and its base Theorem 1 and the other proofs in this section are constructive. Hence, there is a constructive way of proving $\mathsf{d}\mathcal{L}$ formulas by systematic reduction to discrete program properties. The resulting formulas may be unnecessarily complicated, because of the way our proof reduces the completeness of $\mathsf{d}\mathcal{L}_\Delta$ relative to DL to the completeness of $\mathsf{d}\mathcal{L}$ relative to FOD, which may require turning $\mathsf{d}\mathcal{L}$ into continuous FOD and then back into discrete DL. Still, the proof is constructive and shows an upper bound on how quantifier alternations increase in the reduction. A more efficient reduction may be sought in practice. Thanks to our result, we now know that this reduction is possible at all.

Note that recursive reductions would be flawed. The validity of $\mathsf{d}\mathcal{L}$ formulas reduces to that of FOD, which reduces to DL, which again reduces to FOD etc. But we need an approximation to handle either fragment, for we cannot otherwise break this cycle of mutual reductions. This makes approximations of either fragment (or even several approximations of several combined fragments) interesting and ensures that they all lift to full $\mathsf{d}\mathcal{L}$ and full hybrid systems perfectly in our calculus.

V. Relative Decidability

Our relative completeness results entail relative decidability results for free. Since our relative completeness proofs are

[5]We can assume F to be semialgebraic, because, by Theorem 1, FOD does not need nested modalities since it has quantifiers.

constructive and the rules automatable [21], they even define a relative decision procedure. The proof of relative decidability rests on the coincidence lemma for $\mathsf{d}\mathcal{L}$, which shows that only the values of free variables of a formula affect its truth-value.

Lemma 10 (Coincidence lemma)**.** *If the states ν and ω agree on all free variables of formula ϕ, then $\nu \models \phi$ iff $\omega \models \phi$.*

Proof: The proof is by a simple structural induction using the definitions of $\nu \models \cdot$ and $\rho(\cdot)$. ∎

Theorem 11 (Relative decidability)**.** *Validity of $\mathsf{d}\mathcal{L}$ sentences (i.e., formulas without free variables) is decidable relative to either an oracle for continuous FOD or an oracle for discrete DL.*

Proof: Let ϕ by a sentence in $\mathsf{d}\mathcal{L}$ and ν a state. Then either $\nu \models \phi$ or $\nu \not\models \phi$. Thus, either $\nu \models \phi$ or $\nu \models \neg\phi$. By coincidence lemma 10, however, $\nu \models \phi$ iff $\omega \models \phi$ for arbitrary ω, because the truth-value of $\mathsf{d}\mathcal{L}$ formula ϕ is determined entirely[6] by the value of its free variables, of which there are none. Consequently, either $\vDash \phi$ or $\vDash \neg\phi$. In either case, Theorems 1 and 8 imply that the respective valid formula is provable in $\mathsf{d}\mathcal{L}_\Delta$ from valid DL (or FOD) formulas. ∎

VI. Related Work

A general overview of hybrid systems and logics can be found in [3], [9], [12], [23]. Hybrid systems are undecidable and do not have finite-state bisimulations [2], [15], so abstractions and approximations are often used. Euler approximations are standard. Discrete approximations have been considered many times before [7], [19], [25]. Discretizations have been used for linear systems [12], to obtain abstractions of fragments of hybrid systems [1], [2], [29], and to approximate nonlinear systems by hybrid systems [16] or by piecewise linear dynamics [3] when assuming that error bounds or Lipschitz constants are given. See [7], [15], [25] for a discussion of the limits and decidability frontier. These are interesting uses of approximation. But we use approximations for a different, proof-theoretical purpose: to obtain a sound and complete axiomatization relative to properties of discrete programs.

Related approaches do not take a perspective of logic and proofs. That made it difficult to formulate appropriate completeness notions, which are natural in logic. Previous completeness-type arguments for hybrid systems were restricted to bounded model checking [1], continuous systems [29], discrete linear systems on compact domains that are assumed to be so robustly save that simulation is enough [10], or assume the system could be changed without affecting the property [16]. We, instead, prove full relative completeness of an expressive logic relative to a small fragment. Our results identify a more fundamental, proof-theoretical connection between discrete, continuous, and hybrid dynamics. They are also not limited to simple properties like reachability or safety but extend to the full expressivity of $\mathsf{d}\mathcal{L}$.

[6]The semantics of $\mathsf{d}\mathcal{L}$ function and predicate symbols is fixed.

Our notion of relative completeness is inspired by relative completeness for conventional programs, which has been pioneered by Cook [8] and, for dynamic logic of conventional discrete programs [26], by Harel et al. [13], [14]. They show that Hoare's and Pratt's program logics are complete relative to an oracle for the first-order logic of the program data. Relative completeness is the standard approach to showing adequacy of calculi for undecidable classical program logics. Those completeness notions are inadequate for hybrid systems, however, because the data logic of hybrid systems is real arithmetic, hence decidable [28]. It is not the data, but the dynamics proper, that causes incompleteness. We, thus, prove completeness relative to fragments of the dynamics.

As an alternative to arithmetical relative completeness notions, Leivant [20] considered completeness of discrete program logics by alignment with proof schemes in higher-order logic. It is not clear how that would generalize to a compelling completeness notion for hybrid systems, whose semantics intimately depends on arithmetical models that are rich enough to give differential equations a well-defined semantics. It is an interesting question, though.

Discrete Turing machines have been encoded into classes of hybrid [4], [6], [15] or continuous systems [5], [11]. Our proof works the other way around and handles full hybrid systems not just discrete Turing machines on a grid. We use discrete dynamics to understand hybrid dynamics. Our results are also about provability not encodability.

VII. Conclusions

We have presented a significantly simplified axiomatization of differential dynamic logic ($\mathsf{d}\mathcal{L}$), our logic for hybrid systems. We have introduced a new axiom for discrete approximation of differential equations based on Euler discretizations. We prove the calculus to be a sound and complete axiomatization of $\mathsf{d}\mathcal{L}$ relative to the continuous fragment (differential equations) and also a sound and complete axiomatization relative to the discrete fragment. Our results show that the proof theory of hybrid systems aligns completely with that of continuous systems *and* with that of discrete systems. Our axiomatization defines a perfect lifting. Because our proofs are constructive, our axiomatization even defines relative decision procedures for $\mathsf{d}\mathcal{L}$ sentences. Our construction shows how quantifier alternations increase when interreducing dynamics. Finally, our simplified axiomatization makes it easier to transfer our completeness results to other verification approaches just by deriving our axioms.

Our complete alignment shows that any reasoning technique in one domain has a counterpart in the other. (In)variants, which are the predominant proof technique for loops, have differential (in)variants [22] as a counterpart of induction for differential equations. Our results indicate a high potential for identifying other practical consequences of our theoretical alignment. They also revitalize and justify the hope that control and computer science techniques *can* work together to understand hybrid systems and can even work together to understand purely discrete or purely continuous systems.

In the interest of obtaining a computational approach that can lift and use quantifier elimination in real-closed fields, we have phrased our results for the case where differential dynamic logic is built over polynomial arithmetic. With the usual caveats about choosing evolution domain constraints and tests that safeguard against singularities in the domain of definition (of the functions and their relevant derivatives), they continue to hold for rational functions. In fact, they even continue to hold for more general functions as long as those are sufficiently smooth (C^2) on the relevant domains. Unlike with polynomial and rational functions, it is then more challenging to handle the resulting arithmetic, however, or could generally become undecidable. Our discrete relative completeness result also proves that we can handle properties of hybrid systems with complicated (non-polynomial or non-rational) functions in their differential equations to exactly the same extent to which discrete properties about the arithmetic resulting from their right-hand sides can be handled. This is another consequence of our alignment that has been foreshadowed by a corresponding observation about differential (in)variants [22], but has now been shown in general.

ACKNOWLEDGMENT

I would like to thank the anonymous reviewers for their helpful feedback. This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246.

REFERENCES

[1] R. Alur, T. Dang, and F. Ivancic, "Predicate abstraction for reachability analysis of hybrid systems," *ACM Trans. Embedded Comput. Syst.*, vol. 5, no. 1, pp. 152–199, 2006.

[2] R. Alur, T. Henzinger, G. Lafferriere, and G. J. Pappas, "Discrete abstractions of hybrid systems," *Proc. IEEE*, vol. 88, no. 7, pp. 971–984, 2000.

[3] E. Asarin, T. Dang, and A. Girard, "Reachability analysis of nonlinear systems using conservative approximation," in *HSCC*, ser. LNCS, O. Maler and A. Pnueli, Eds., vol. 2623. Springer, 2003, pp. 20–35.

[4] E. Asarin and O. Maler, "Achilles and the tortoise climbing up the arithmetical hierarchy," *J. Comput. Syst. Sci.*, vol. 57, no. 3, pp. 389–398, 1998.

[5] M. S. Branicky, "Universal computation and other capabilities of hybrid and continuous dynamical systems," *Theor. Comput. Sci.*, vol. 138, no. 1, pp. 67–100, 1995.

[6] F. Cassez and K. G. Larsen, "The impressive power of stopwatches," in *CONCUR*, 2000, pp. 138–152.

[7] P. Collins, "Optimal semicomputable approximations to reachable and invariant sets," *Theory Comput. Syst.*, vol. 41, no. 1, pp. 33–48, 2007.

[8] S. A. Cook, "Soundness and completeness of an axiom system for program verification." *SIAM J. Comput.*, vol. 7, no. 1, pp. 70–90, 1978.

[9] J. M. Davoren and A. Nerode, "Logics for hybrid systems," *IEEE*, vol. 88, no. 7, pp. 985–1010, July 2000.

[10] A. Girard and G. J. Pappas, "Verification using simulation," in *HSCC*, ser. LNCS, J. P. Hespanha and A. Tiwari, Eds., vol. 3927. Springer, 2006, pp. 272–286.

[11] D. S. Graça, M. L. Campagnolo, and J. Buescu, "Computability with polynomial differential equations," *Advances in Applied Mathematics*, 2007.

[12] C. L. Guernic and A. Girard, "Reachability analysis of hybrid systems using support functions," in *CAV*, ser. LNCS, A. Bouajjani and O. Maler, Eds., vol. 5643. Springer, 2009, pp. 540–554.

[13] D. Harel, D. Kozen, and J. Tiuryn, *Dynamic logic*. Cambridge: MIT Press, 2000.

[14] D. Harel, A. R. Meyer, and V. R. Pratt, "Computability and completeness in logics of programs (preliminary report)," in *STOC*. ACM, 1977, pp. 261–268.

[15] T. A. Henzinger, "The theory of hybrid automata." in *LICS*. Los Alamitos: IEEE Computer Society, 1996, pp. 278–292.

[16] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi, "Algorithmic analysis of nonlinear hybrid systems." *IEEE T. Automat. Contr.*, vol. 43, pp. 540–554, 1998.

[17] G. E. Hughes and M. J. Cresswell, *A New Introduction to Modal Logic*. Routledge, 1996.

[18] D. Kozen, "Kleene algebra with tests," *ACM Trans. Program. Lang. Syst.*, vol. 19, no. 3, pp. 427–443, 1997.

[19] R. Lanotte and S. Tini, "Taylor approximation for hybrid systems." in *HSCC*, ser. LNCS, M. Morari and L. Thiele, Eds., vol. 3414. Springer, 2005, pp. 402–416.

[20] D. Leivant, "Matching explicit and modal reasoning about programs: A proof theoretic delineation of dynamic logic," in *LICS*. IEEE Computer Society, 2006, pp. 157–168.

[21] A. Platzer, "Differential dynamic logic for hybrid systems." *J. Autom. Reas.*, vol. 41, no. 2, pp. 143–189, 2008.

[22] ——, "Differential-algebraic dynamic logic for differential-algebraic programs," *J. Log. Comput.*, vol. 20, no. 1, pp. 309–352, 2010.

[23] ——, *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Heidelberg: Springer, 2010.

[24] ——, "The complete proof theory of hybrid systems," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU-CS-11-144, Nov 2011.

[25] A. Platzer and E. M. Clarke, "The image computation problem in hybrid systems model checking." in *HSCC*, ser. LNCS, A. Bemporad, A. Bicchi, and G. Buttazzo, Eds., vol. 4416. Springer, 2007, pp. 473–486.

[26] V. R. Pratt, "Semantical considerations on Floyd-Hoare logic," in *FOCS*. IEEE, 1976, pp. 109–121.

[27] J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis*, 3rd ed. New York: Springer, 2002.

[28] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, 2nd ed. Berkeley: University of California Press, 1951.

[29] A. Tiwari, "Abstractions for hybrid systems," *Form. Methods Syst. Des.*, vol. 32, no. 1, pp. 57–83, 2008.

[30] W. Walter, *Ordinary Differential Equations*. Springer, 1998.