Logical Dynamics

David Fernández Duque

Habilitation à Diriger des Recherches
(HDR)

Logical Dynamics

David Fernández-Duque

david.fernandez@irit.fr

davidfernandez.co.nf

Under the supervision of Philippe Balbiani

Paul Sabatier University, Toulouse, France

Contents

1 Introduction **3**
1.1 Verification of dynamical systems 3
1.2 Completeness and Incompleteness in Logical Theories 5

2 Modal logic **6**
2.1 Syntax and semantics 6
2.2 Basic modal axioms 9
2.3 Simulation and bisimulation 11
2.4 The tangled closure operator 12
2.5 The Lebesgue measure algebra 13

3 Logic applied to dynamical systems **16**
3.1 Dynamic topological logic 16
3.2 Intuitionistic temporal logic 19
3.3 Compass logics of positions 21
3.4 Lexicographic products of modal logics 23

4 Dynamical systems applied to logic **25**
4.1 The polymodal provability logic 26
4.2 Ordinal dynamical systems 27
4.3 Turing-Feferman progressions and provability spectra 29
4.4 The closed fragment 30
4.5 Topological semantics of provability logic 31
4.6 Subsystems of second-order arithmetic 32
4.7 Iterated ω-rules 34

5 Dynamics of information **37**
5.1 Learning and forgetting 37
5.2 Agents with bounded rationality 38
5.3 Applications to secure communication 41

6 Perspectives **45**
6.1 Feasible logics for dynamical systems 45
6.2 Calibration of formal systems 47
6.3 Secure aggretation of distributed information 50
6.4 Concluding remarks 51

A List of publications **59**

1 Introduction

Dynamical systems are mathematical models of change or motion over time. They are ubiquitous in physics, computer science, biology, and many other branches of pure and applied science. In view of several recent developments, there is great opportunity and demand for powerful tools based on mathematical and computational logic for a qualitative formal analysis of these systems. The central question that concerns us is:

Question 1.1. *Which logical theories are appropriate for describing and reasoning about dynamical systems that appear in various branches of science and technology?*

Each logical theory may have several advantages and disadvantages, and the criteria for choosing a suitable framework varies by discipline. Thus we will work both with highly expressive logics stemming from foundations of mathematics, and less expressive but more computationally effective logics stemming from computer science.

Specifically, will develop tools for efficient, automated reasoning about continuous dynamical systems applicable in real-world scenarios, such as the modeling of controlled ecosystems for sustainable farming. We will also study frameworks for formal reasoning about transfinite dynamics in discontinuous systems. Such dynamical systems are of interest in proof theory to model Turing progressions, which in turn can be used to produce mathematically natural statements independent from strong formal theories in the spirit of Gödel's incompleteness theorems.

1.1 Verification of dynamical systems

Consider an example from biology, where we model wolf (predator) and sheep (prey) populations. One natural question we may ask is whether the populations will eventually disappear from the ecosystem, remain stable, or proliferate. One approach to answer this question would be to model the problem numerically and observe the evolution of the two populations over a long period of time. If, indeed, we observe that they eventually disappear, we have a definite answer. If, on the other hand, they exhibit (say) a seemingly cyclic behavior, this might be suggestive that the populations will continue to follow such a cycle forever, but it may be that we are truly observing a downward spiral and the two species will become extinct over a long period of time.

Thus while a numerical simulation may provide evidence that our populations will not die out, we may wish to take a different approach in order to *certify* that this will be the case. The prototypical tool for such a certificate is to provide a mathematical proof; if we *prove* that, given the laws governing the evolution of our populations, they will forever cycle around a steady state and never die out, we can safely assume that this will be the case (provided the behavior of the system does not change exogenously).

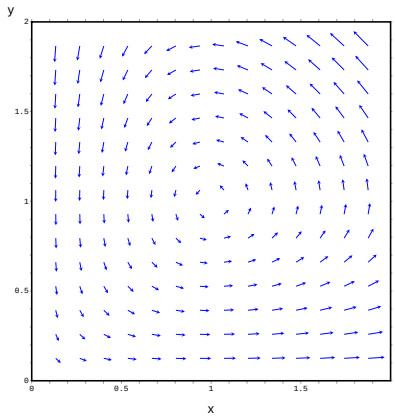

Figure 1: Direction field for a model of sheep (x) and wolf (y) populations. When there are many wolves and few sheep, the wolves tend to die out given lack of food, which then allows the sheep to reproduce freely. Eventually this leads to more food sources for the wolves, which in turn proliferate, starting the cycle anew.

The need for such a certificate is seen very clearly in computer science. An algorithm (say, modeled as a Turing machine or an automaton) may be viewed as a discrete-time dynamical system, and often we want to ensure that it will behave according to its specifications; for example, that it will eventually reach a terminating state, or that it will avoid an unsafe one. Once again we may simply run the algorithm on distinct outputs and observe whether they tend to terminate, or we may instead provide a certificate of correctness using logical tools. While the 'gold standard' of mathematical proof is arguably the Zermelo-Franekel set theory ZFC, this is usually overkill for such a task, and has several computational disadvantages. Instead, we will focus on weaker formalisms that are still sufficient for reasoning about dynamical systems.

There are several computational tools available to analyze dynamical systems, but we are specifically concerned with logical methods for understanding them which allow for qualitative, certifiable reasoning about their behavior. These are based on *formal languages,* which are sets $\mathcal{L}$ of *formulas*, typically closed under Boolean operations (for example, if φ, ψ are formulas, then their conjunction $\varphi \wedge \psi$ is also a formula), as well as possibly quantifiers or other constructions. Formulas of $\mathcal{L}$ are interpreted over a class $\mathcal{C}$ of structures, where for $X \in \mathcal{C}$ we write $X \models \varphi$ to say that φ is *true* (or *valid*) in X. A *theory* is a set $T \subseteq \mathcal{L}$ of formulas, typically assumed to have certain closure properties (e.g., if $\varphi, \psi \in T$, then $\varphi \wedge \psi \in T$). We usually write $T \vdash \varphi$ instead of $\varphi \in T$. The intention is for T to prove only true statements, i.e. $T \vdash \varphi$ implies that $X \models \varphi$ for all $X \in \mathcal{C}$, in which case we say that T is *sound;* ideally, T should also be able to prove *all* true statements, that is, $T \vdash \varphi$ whenever $X \models \varphi$ for all

$X \in \mathcal{C}$, in which case we say that T is *complete.*

In order to answer Question 1.1, we must work both with highly expressive logics stemming from foundations of mathematics, and less expressive but more computationally effective logics stemming from computer science. As is evidenced from my research results, different applications may have very different priorities, and thus a suitable answer requires what we may call *logic engineering.*

1.2 Completeness and Incompleteness in Logical Theories

From Gödel's incompleteness theorems [51], we know that no computably enumerable theory T can be both sound and complete for the structure $(\mathbb{N}, +, \times)$ of natural numbers. We may then ask if a certain (formalized) theorem φ is provable within T, obtaining one of two outcomes:

1. T can prove φ, in which case T may give us *additional* information not included in φ itself; for example, we may extract algorithmic or computational information about φ from its proof in T. This information can often be used to strengthen φ and obtain a more powerful result [61].

2. T cannot prove φ, in which case φ provides us with a natural mathematical statement that is independent from T. Such a statement may be used to separate theories; if we know that U can prove φ, then φ is evidence that $U \neq T$. By systematically searching for such statements, this can provide us with a tool for classifying formal theories.

Thus, understanding the power and limitations of logical systems gives us benefits in two directions: we obtain new information about dynamical systems from the logical tools we use to analyze them, and we obtain new information about the power of logical theories from their ability to reason about dynamical systems. On the other hand, Gödel's incompleteness theorems only apply to arithmetical theories, and thus we may instead use logics that cannot formalize arithmetic, as is typically the case for modal logics.

In my research, I explore both of these directions; that is, applications of logic to dynamical systems, as well as applications of dynamical systems to logic. In this report we will discuss both; for this, let us begin by giving a general overview of modal logic, and discuss some of my results in the field.

2 Modal logic

Understanding the world can be viewed as a process of separating those statements that are true from those that are false. However, even two true statements can be true in different ways; for example, one may say that the statement 'seven is a prime number' has a different status from 'Barack Obama is not the president of the United States'. One may argue that the first statement is *necessary,* while the second is not. Alternately, one may point out the fact that the first statement has *always* been true, while the second is only true *now.*

Modal logics aim to capture the different modes of truth that a statement may have. In its simplest form, given a statement φ, we introduce a new statement $\Box\varphi$ which could be interpreted as φ *is necessarily true,* φ *is always true,* or φ *is provably true,* among other readings. While the exact interpretation depends on the application at hand, there is a general theoretical framework for understanding such logics.

In this section we will give a brief introduction to modal logics with a focus on *neighborhood semantics,* which will be useful for understanding the results presented later in this report.

2.1 Syntax and semantics

Modal logic is an extension of propositional logic with an operator $\Box$ and its dual, $\Diamond$, so that if φ is any formula, $\Box\varphi$ and $\Diamond\varphi$ are formulas too. There are several semantics for these operators, but possibly the first was studied by Tarski [72], who proposed a topological reading of modalities. The latter has regained interest in the last decades, due to its potential for spatial reasoning, especially when modal logic is augmented with a universal modality [77] or fixpoint operators, as proposed by myself in [32] and studied further by Goldblatt and Hodkinson[53].

Thus we will consider logics over variants of the language $\mathcal{L}_\Box$ given by the following grammar (in Backus-Naur form). Fix a set $\mathbb{P}$ of propositional variables, and define:

$$\varphi, \psi := \quad \top \;\mid\; p \;\mid\; \varphi \wedge \psi \;\mid\; \neg\varphi \;\mid\; \Box\varphi,$$

where $p \in \mathbb{P}$; in other words, $\mathcal{L}_\Box$ is the least set such that $\{\top\} \cup \mathbb{P} \subseteq \mathcal{L}_\Box$, and $\mathcal{L}_\Box$ is closed under conjunction, negation, and $\varphi \mapsto \Box\varphi$.

We define $\vee, \rightarrow, \Diamond$ using the standard abbreviations (e.g., $\Diamond \equiv \neg\Box\neg$). Often we will want to interpret formulas of $\mathcal{L}_\Box$ as subsets of a 'spatial' structure, such as $\mathbb{R}^n$. To do this, we need to define *neighborhoods* of points $x \in \mathbb{R}^n$. Intuitively, U is a neighborhood of x if x has positive distance from its complement, $X \setminus U$. To make this precise, for $x, y \in \mathbb{R}^n$, let $\delta(x, y)$ denote the standard Euclidean distance between x and y. It is well-known that δ satisfies

(i) $\delta(x, y) \geq 0$,

(ii) $\delta(x, y) = 0$ iff $x = y$,

(iii) $\delta(x, y) = \delta(y, x)$ and

(iv) the triangle inequality, $\delta(x, z) \leq \delta(x, y) + \delta(y, z)$.

More generally, a set X with a function $\delta\colon X \times X \to \mathbb{R}$ satisfying these four properties is a *metric space.* The Euclidean spaces $\mathbb{R}^n$ are metric spaces, but there are other important examples, such as the set of continuous functions on $[0, 1]$ (with a suitable metric).

Definition 2.1. *Given a metric space X and $A \subseteq X$, we define the* interior *of A, denoted $i(A)$, to be the set of points $x \in X$ such that for some $\varepsilon > 0$, if $\delta(x, y) < \varepsilon$, it follows that $y \in A$.*

The basic properties of i are well-known:

Proposition 2.2. *If X is a metric space and i is the interior operator on X, then, given sets $A, B \subseteq X$,*

(i) $i(X) = X$,

(ii) $i(A) \subseteq A$,

(iii) $i(A) = i(i(A))$ *and*

(iv) $i(A \cap B) = i(A) \cap i(B)$.

We will say that any function $i\colon 2^X \to 2^X$ satisfying these four properties is an *interior operator.* Interior operators are more generally defined over any topological space:

Definition 2.3. *A* topological space *is a pair $(X, \mathcal{T})$, where X is a set and $\mathcal{T}$ a family of subsets of X satisfying*

1. $\varnothing, X \in \mathcal{T}$;
2. *if* $U, V \in \mathcal{T}$ *then* $U \cap V \in \mathcal{T}$, *and*
3. *if* $\mathcal{O} \subseteq \mathcal{T}$, *then* $\bigcup \mathcal{O} \in \mathcal{T}$.

The elements of $\mathcal{T}$ are called open sets. *Complements of open sets are* closed sets.

Then, in any topological space, we may define $i(A)$ to be the union of all open sets contained in A, and we say that $U \subseteq X$ is a *neighborhood* of $x \in X$ if $x \in i(U)$. In any topological space, we may also define the *closure* of A by $c(A) = X \setminus i(X \setminus A)$. From a computational perspective, it can be more convenient to work with arbitrary topological spaces than with metric spaces, as finite, non-trivial topological spaces can be defined in a straightforward way, and thus spatial relations can be represented using finite structures. To be precise, let W be a set and $R \subseteq W \times W$ be a binary relation; the structure (W, R) is a *frame.* Then, if R is a preorder (i.e., a transitive, reflexive relation), we can define a topology on W by letting U be open if and only if it is of the form $\bigcup_{u \in U} R(u)$ for some $U \subseteq W$.

However, if R is not transitive and reflexive, this definition does not necessarily produce a topology. It does, however, give rise to a *neighborhood space,* and it will be convenient to define such spaces in full generality in order to give a uniform treatment of topological spaces and Kripke models.

Definition 2.4. *A* neighborhood space *is a tuple $\mathcal{A} = (A, \vartriangleleft)$, where $\vartriangleleft \subseteq A \times 2^A$ is a* neighborhood relation. *We say that $\vartriangleleft$ is:*

1. monotone *if $x \vartriangleleft X \subseteq Y$ implies that $x \vartriangleleft Y$,*
2. non-degenerate *if for every $x \in A$ there is $X \subseteq A$ such that $x \vartriangleleft X$,*
3. filtered *if whenever $x \vartriangleleft A$ and $x \vartriangleleft B$, it follows that $x \vartriangleleft A \cap B$,*
4. normal *if it is monotone, non-degenerate and filtered, and*
5. uniform *if the relation $\vartriangleleft$ is constant (i.e., $w \vartriangleleft X$ implies that $v \vartriangleleft X$ for all $w, v \in A$ and $X \subseteq A$).*

We let $\mathcal{A}$ inherit the properties of $\vartriangleleft$, so that for example $\mathcal{A}$ is monotone if $\vartriangleleft$ is.

This general presentation will allow us to unify semantics over topological spaces with those over arbitrary relational structures. As mentioned before, a Kripke frame is simply a structure $\mathcal{A} = (A, R)$, where A is a set and $R \subseteq A \times A$ is an arbitrary binary relation. We will implicitly identify $\mathcal{A}$ with the neighborhood space $(A, \vartriangleleft_R)$, where $x \vartriangleleft_R U$ if and only if

$$R(x) = \{y \in A : x \; R \; y\} \subseteq U.$$

It is readily checked that $\vartriangleleft_R$ is always normal. With this in mind, let us define some important classes of frames.

Definition 2.5. *Define* **K** *to be the class of all Kripke frames,* **S4** *to be the class of all Kripke frames with a transitive, reflexive relation, and* **S5** *to be the class of Kripke frames with an equivalence relation.*

The names for these classes are derived from their corresponding modal logics, which will be defined in Section 2.2. Now we are ready to define the semantics for $\mathcal{L}_\Box$, or, more generally, languages of the form $\mathcal{L}_\Lambda$, where Λ is a set of objects we call *modals,* given by the grammar

$$\varphi, \psi := \quad \top \;\mid\; p \;\mid\; \varphi \wedge \psi \;\mid\; \neg\varphi \;\mid\; [\lambda]\varphi,$$

where $p \in \mathbb{P}$ and $\lambda \in \Lambda$.

Definition 2.6. *Given a set of modals Λ, a* Λ-neighborhood space *is a pair $(A, (\vartriangleleft_\lambda)_{\lambda \in \Lambda})$, where for each $\lambda \in \Lambda$, $(A, \vartriangleleft_\lambda)$ is a neighborhood space.*

A valuation *on $(A, (\vartriangleleft_\lambda)_{\lambda \in \Lambda})$ is any function $V \colon \mathbb{P} \to 2^A$ (that is, every propositional variable is assigned a set of points). A* Λ-model *is a tuple $\mathcal{A} = (A, (\vartriangleleft_\lambda)_{\lambda \in \Lambda}, V)$ consisting of a Λ-neighborhood space equipped with a valuation.*

We define the truth set

$$[\![\varphi]\!]_{\mathcal{A}} = \{w \in A : (\mathcal{A}, w) \models \varphi\}$$

by structural induction on φ as follows:

$$\begin{array}{lcl} [\![p]\!]_{\mathcal{A}} & = & V(p) \\ [\![\varphi \wedge \psi]\!]_{\mathcal{A}} & = & [\![\varphi]\!]_{\mathcal{A}} \cap [\![\psi]\!]_{\mathcal{A}} \\ [\![\neg\varphi]\!]_{\mathcal{A}} & = & A \setminus [\![\varphi]\!]_{\mathcal{A}} \\ [\![[\lambda]\varphi]\!]_{\mathcal{A}} & = & \{w \in A : w \prec_\lambda [\![\varphi]\!]_{\mathcal{A}}\}. \end{array}$$

Given a model $\mathcal{A} = (A, (\prec_\lambda)_{\lambda\in\Lambda}, V)$ and formulas $\varphi, \psi \in \mathcal{L}_\Lambda$, we say that φ is equivalent to ψ *on $\mathcal{A}$ if $[\![\varphi]\!]_V = [\![\psi]\!]_V$. If $\mathcal{A}$ is a modal space, φ, ψ are equivalent on $\mathcal{A}$ if they are equivalent on any model of the form $(\mathcal{A}, V)$, and if $\mathbf{A}$ is a class of structures, we say that φ, ψ are equivalent over $\mathbf{A}$ if they are equivalent on any element of $\mathbf{A}$. When $\mathcal{A}$ or $\mathbf{A}$ is clear from context, we may write $\varphi \equiv \psi$, and if $\psi = \top$ we say φ is* valid.

Often Λ will be a singleton (say, $\Lambda = \{0\}$), in which case we write $\Box, \prec$ instead of $[0], \prec_0$. Moreover, if $\prec_\lambda$ is replaced by a binary relation R_λ, then in the above definition, $\prec_\lambda$ is to be understood as $\prec_{R_\lambda}$. We will also use $\forall$ to denote the *universal modality,* interpreted by the neighborhood relation defined by $w \prec_\forall U$ if and only if U is the entire space.

The clause for $[\lambda]\varphi$ may need some explanation, as one often defines $w \in [\![[\lambda]\varphi]\!]_{\mathcal{A}}$ if there is U so that $w \prec_\lambda U \subseteq [\![\varphi]\!]_{\mathcal{A}}$. Note, first, that the two clauses are equivalent over the class of monotone frames, and we have defined the neighborhood structure on both topological spaces and Kripke frames to be monotone for this reason. However, we will also consider non-monotone structures later in order to give semantics for weak modal logics, and in this setting we need the clause given in Definition 2.6.

With this in mind, let us review the axioms for important modal logics over $\mathcal{L}_\Box$ and the extension with a universal modality, $\mathcal{L}_{\Box\forall}$.

2.2 Basic modal axioms

A central focus in much of the literature on modal logics of space lies in finding sound and complete axiomatizations for several important classes of topologies. Let us list some of the basic axioms that have appeared in this enterprise:

- TAUT all propositional tautologies
- K $\Box(p \to q) \to (\Box p \to \Box q)$
- T $p \to \Diamond p$
- 4 $\Diamond\Diamond p \to \Diamond p$
- 5 $\Diamond p \to \Box\Diamond p$
- L $\Box(\Box p \to p) \to \Box p$
- MP $\dfrac{\varphi \quad \varphi \to \psi}{\psi}$
- NEC $\dfrac{\varphi}{\Box\varphi}$

A *logic* is any set Λ of formulas closed under modus ponens, substitution and necessitation. Given a logic Λ and a formula φ, $\Lambda + \varphi$ is the least logic containing $\Lambda \cup \{\varphi\}$. The most 'basic' modal logic is

$$\mathsf{K} \equiv \textsc{Taut} + \mathrm{K} + \mathrm{MP} + \textsc{Nec};$$

this is the logic of all (finite) frames and is the standard minimal logic used in modal reasoning (to be precise, it is the least *normal* logic; in Section 5, we will also consider logics that do not extend K). Other key modal logics are:

$$\mathsf{K4} \equiv \mathsf{K} + 4 \qquad \mathsf{S4} \equiv \mathsf{K4} + \mathrm{T} \qquad \mathsf{S5} \equiv \mathsf{S4} + 5 \qquad \mathsf{GL} \equiv \mathsf{K} + \mathrm{L}.$$

The logics we have listed characterize several important classes of spaces. As usual, a logic Λ is *sound* for a class of spaces $\mathbf{C}$ if all theorems of Λ are valid in $\mathbf{C}$, and *complete* if all valid formulas in $\mathbf{C}$ are provable in Λ.

Theorem 2.7.

1. *The logic* K *is sound and complete for the class of (finite)* $\mathbf{K}$ *frames [18].*
2. *The logic* $\mathsf{K4}$ *is sound and complete for the class of all (finite)* $\mathbf{K4}$ *frames.*
3. *The logic* $\mathsf{S4}$ *is sound and complete for the class of all (finite)* $\mathbf{S4}$ *frames, for the class of all all metric spaces, and for* $\mathbb{R}^n$ *for any* $n > 0$ *[72].*
4. *The logic* $\mathsf{S5}$ *is sound and complete for the class of all (finite)* $\mathbf{S5}$ *frames.*

The operator $\Box$ is useful for capturing local properties of $\mathbb{R}^n$, whereas $\forall$ is useful for describing global behavior. The logic GL also enjoys natural semantics, as we will see next.

Definition 2.8. *Let* W *be any set. A relation* R *on* W *is* converse well-founded *if either of the following, equivalent, properties holds:*

1. *if* $A \subseteq W$ *is non-empty, there is* $w \in A$ *such that* $R(w) \cap A = \varnothing$.
2. *there are no infinite sequences*

$$w_0 \; R \; w_1 \; R \; w_2 \; R \ldots$$

The relation R *is* well-founded *if* R^{-1} *is converse well-founded.*

Transitive, converse well-founded frames can be generalized to a topological setting. To this end, if $(X, \mathcal{T})$ is a topological space, $x \in X$ and $U \subseteq X$, say that U is a *punctured neighborhood of* x if $U \cup \{x\}$ is a neighborhood of x. Then, transitive, converse well-founded frames can be seen as a special case of punctured neighborhood structures over *scattered spaces,* as defined below:

Definition 2.9. *Let* $(X, \mathcal{T})$ *be a topological space. If* $A \subseteq X$ *and* $x \in A$*, we say that* x is isolated in A *if there is a neighborhood* U *of* x *such that* $U \cap A = \{x\}$.

A topological space $(X, \mathcal{T})$ *is* scattered *if whenever* $A \subseteq X$ *is non-empty, then* A *has an isolated point.*

Then, we have the following completeness resutls:

Theorem 2.10. *The logic* GL *is sound and complete for the class of all (finite) transitive, converse well-founded frames [76], as well as for the class of all punctured neighborhood structures based on a scattered space [13].*

Next, let us discuss logics with the universal modality. Given a logic L, by LU we denote the logic extending L to the language with a universal modality and the axioms $T, 5$ for $\forall$. Spatial logics with the universal modality have been studied by Shehtman [77], where he proves the following:

Theorem 2.11. *The logic* S4U *is sound and complete for the class of all (finite)* **S4** *frames.*

Note, however, that S4U is *not* complete for $\mathbb{R}^n$ for any n, given that this space is *connected;* that is, it cannot be partitioned into two disjoint, open sets. More formally, if $\mathbb{R}^n = A \cup B$ where A, B are open and disjoint, then either $A = \varnothing$ or $B = \varnothing$. This property is characterized by the connectedness axiom

$$\mathrm{C} \quad \forall(\Box p \vee \Box\neg p) \to (\forall p \vee \forall\neg p).$$

Theorem 2.12. *The logic* $\mathsf{S4UC} = \mathsf{S4U} + \mathrm{C}$ *is sound and complete for* $\mathbb{R}^n$ *for any* $n > 0$.

Next, let us discuss some basic relations for comparing neighborhood spaces.

2.3 Simulation and bisimulation

In this section we will define *simulations* and *bisimulations*, both in the Kripke and in the neighborhood setting.

Definition 2.13. *If* $\mathcal{A} = (A, R_{\mathcal{A}}, V_{\mathcal{A}})$, $\mathcal{B} = (B, R_{\mathcal{B}}, V_{\mathcal{B}})$ *are Kripke frames, a* simulation *between* $\mathcal{A}$ *and* $\mathcal{B}$ *is a binary relation* χ *such that*

Atoms *for every* $w\ \chi\ v$ *and every propositional variable* p,

$$w \in V_{\mathcal{A}}(p) \Leftrightarrow v \in V_{\mathcal{B}}(p),$$

and

Forth *if* $w\ R_{\mathcal{A}}\ w'$ *and* $w\ \chi\ v$, *there is* v' *so that* $v\ R_{\mathcal{B}}\ v'$ *and* $w'\ \chi\ v'$.

The relation χ *is a* bisimulation *if it further satisfies*

Back *if* $v\ R_{\mathcal{B}}\ v'$ *and* $w\ \chi\ v$, *there is* w' *so that* $w\ R_{\mathcal{A}}\ w'$ *and* $w'\ \chi\ v'$.

This definition readily extends to the neighborhood setting. For this, we borrow terminology from the theory of functions on topological spaces, although we warn that this usage is not standard.

Definition 2.14 (Neighborhood bisimulation)**.** *Let $\mathcal{A} = (A, \lessdot_{\mathcal{A}})$ and $\mathcal{B} = (B, \lessdot_{\mathcal{B}})$ be neighborhood spaces. Say that a binary relation $\chi \subseteq A \times B$ is* continuous *if, whenever $w \ \chi \ v \lessdot_{\mathcal{B}} Y$, it follows that $w \lessdot_{\mathcal{A}} \chi^{-1}[Y]$, and* open *if whenever $w \ \chi \ v$ and $w \lessdot_{\mathcal{A}} X$, it follows that $v \lessdot_{\mathcal{B}} \chi[X]$.*

The relation χ between models $(A, \lessdot_{\mathcal{A}}, V_{\mathcal{A}})$ and $(B, \lessdot_{\mathcal{B}}, V_{\mathcal{B}})$ is a simulation *if it is continuous and, whenever $p \in \mathbb{P}$ and $w \ \chi \ v$, then $w \in V_{\mathcal{A}}(p)$ if and only if $v \in V_{\mathcal{B}}(p)$. If moreover χ is open, then χ is a* bisimulation.

A point $b \in B$ simulates *$a \in A$ if there exists a simulation $\chi \subseteq A \times B$ such that $a \ \chi \ b$; we will write $(\mathcal{A}, a) \trianglelefteq (\mathcal{B}, b)$. If a bisimulation β exists between $\mathcal{A}$ and $\mathcal{B}$ such that $a \ \beta \ b$, we will write $(\mathcal{A}, a) \leftrightarrows (\mathcal{B}, b)$.*

It is not hard to check that both definitions agree on Kripke frames if we identify them with their neighborhood structure as we have defined it.

2.4 The tangled closure operator

The language $\mathcal{L}_{\Box}$ can naturally be enriched by adding fixed point operators, in the spirit of the μ-calculus [83]. However, by results of Dawar and Otto [22], we know that the fixed points that can be defined in the topological setting can be reduced to a simpler construction, which is a natural polyadic extension of the usual topological closure.

Definition 2.15 (Tangled closure)**.** *Let $(X, \mathcal{T})$ be a topological space and $\mathcal{S} \subseteq 2^X$. Given $E \subseteq X$, we say $\mathcal{S}$ is* tangled *in E if, for all $A \in \mathcal{S}$, $A \cap E$ is dense in E. We then define $\mathcal{S}^*$ to be the union of all sets E such that $\mathcal{S}$ is tangled in E.*

It is important for us to note that the tangled closure is defined over any topological space; however, it is instructive to consider the tangled closure over finite, transitive, reflexive Kripke frames, in which case the tangled closure takes on a particularly simple form.

Lemma 2.16. *Let $(W, \preccurlyeq)$ be a finite preorder, $x \in S$ and $\mathcal{O} \subseteq 2^W$. Then, $x \in \mathcal{O}^*$ if and only if there exist $(y_O)_{O \in \mathcal{O}} \subseteq W$ such that $y_O \in O$, $y_O \preccurlyeq x$ for all $O \in \mathcal{O}$ and $y_O \sim y_{O'}$ for all $O, O' \in \mathcal{O}$.*

We can then enrich the modal language to the language $\mathcal{L}^*_{\Box}$, where $\Box$ can be applied to finite sets of formulas, and in the topological setting define

$$[\![\Diamond \Gamma]\!] = \{[\![\gamma]\!] : \gamma \in \Gamma\}^*.$$

In [31], I proved the following:

Theorem 2.17 (DFD)**.** *Given a finite, transitive reflexive Kripke frame $\mathcal{A} = (A, \preccurlyeq, V_{\mathcal{A}})$ and $a \in A$, there exists a formula $\mathrm{Sim}(\mathcal{A}, a) \in \mathcal{L}^*_{\Box}$ such that, for every topological model $\mathcal{X} = (X, \mathcal{T}, V)$ and $x \in X$, $x \in [\![\mathrm{Sim}(\mathcal{A}, a)]\!]_{\mathcal{X}}$ if and only if $(\mathcal{A}, a) \trianglelefteq (\mathcal{X}, x)$.*

Moreover, such a formula does not always exist in $\mathcal{L}_{\Box}$, even when $\mathcal{A}$ has only two worlds.

Note that the property of being *bisimilar* to $(\mathcal{A}, a)$ *is* definable in $\mathcal{L}_\Box$ [31]. As it turns out, these simulation formulas can be a great technical advantage in completeness proofs for logics over certain extensions of $\mathcal{L}_\Box$. For this, one first needs to axiomatize the topologically valid formulas of $\mathcal{L}^*_\Box$ itself, as I have done in [32].

Theorem 2.18 (DFD)**.** *Given $\varphi \in \mathcal{L}^*_\Box$, the following are equivalent:*

1. *φ is valid over the class of finite, transitive reflexive Kripke frames,*
2. *φ is valid over the class of all topological spaces,*
3. *φ is derivable in the logic $\mathsf{S4}^*$, axiomatized by $\mathsf{S4}$ together with the following:*

   $\mathrm{Fix}_\Diamond$ $\Diamond\Gamma \to \bigwedge_{\gamma\in\Gamma} \Diamond(\gamma \wedge \Diamond\Gamma)$

   $\mathrm{Ind}_\Diamond$ *Induction for $\Diamond$:*

$$\Box\Big(p \to \bigwedge_{\gamma\in\Gamma} \Diamond(p \wedge \gamma)\Big) \to (p \to \Diamond\Gamma).$$

Later we will see that the tangled closure is an essential ingredient in axiomatizing the logic of dynamical systems. Before this, however, let us discuss a variant of topological semantics, where validity is regarded up to a set of measure zero.

2.5 The Lebesgue measure algebra

If a set X is endowed with a measure (for example, representing volumes or probabilities), it is often useful to disregard sets of measure zero. One can use this to give a different interpretation to modal logics. In this setting, the truth values of formulas are no longer sets, but rather equivalence classes of sets, as defined below.

Recall that a *measure space* is a triple $(X, \mathcal{A}, \mu)$ where X is a set, $\mathcal{A} \subseteq 2^X$ is a σ-algebra (that is, a collection of sets containing $\varnothing$ and X which is closed under set difference and countable unions) and $\mu : \mathcal{A} \to [0, \infty]$ (the non-negative reals with a maximal element ∞ added) satisfying

1. $\mu(\varnothing) = 0$
2. $\mu(A \setminus B) = \mu(A) - \mu(B)$ if $B \subseteq A$ and
3. if $(A_n)_{n<\omega}$ is an increasing sequence of elements of $\mathcal{A}$,

$$\mu\left(\bigcup_{n<\omega} A_n\right) = \lim_{n\to\infty} \mu(A_n).$$

Elements of $\mathcal{A}$ will be called *μ-measurable*. We say μ is *σ-finite* if there are countably many sets $S_n \subseteq X$ such that $\mu(S_n)$ is finite for all $n < \omega$ and $X = \bigcup_{n<\omega} S_n$. Measure spaces which are σ-finite cannot contain an uncountable collection of disjoint sets of positive measure.

We always assume that Euclidean space $\mathbb{R}^n$ is equipped with the standard Euclidean metric and Lebesgue measure; the latter will be denoted $|\cdot|$.

Definition 2.19 (Measure algebra)**.** *Let $\mathfrak{X} = (X, \mathcal{A}, \mu)$ be a measure space. We define the* measure algebra *of $\mathfrak{X}$, which we will denote $\mathbb{A}_\mu$, to be the set of equivalence classes of $\mathcal{A}$ under the relation $\overset{\mu}{\sim}$ given by $E \overset{\mu}{\sim} F$ if and only if $\mu((E \setminus F) \cup (F \setminus E)) = 0$.*

We will refer to elements of $\mathbb{A}_\mu$ as *regions*. Denote the equivalence class of $S \in \mathcal{A}$ by $[S]_\mu$. Boolean operations can be defined on $\mathbb{A}_\mu$ in the obvious way; $[E]_\mu \sqcap [F]_\mu = [E \cap F]_\mu$, $[E]_\mu - [F]_\mu = [E \setminus F]_\mu$. We can also define $[E]_\mu \sqsubseteq [F]_\mu$ by $\mu(E \setminus F) = 0$. In general we will use 'square' symbols for notation of the measure algebra and 'round' symbols for set notation in order to avoid confusion. As a slight abuse of notation, if $o \in \mathbb{A}_\mu$ and $o = [S]_\mu$ we may write $\mu(o)$ instead of $\mu(S)$; note that this is well-defined, independently of our choice of $S \in o$.

In order to interpret our modal operators, we need to consider measure spaces which also have a topological structure:

Definition 2.20 (topological measure space)**.** *A* topological measure space *is a triple $(X, \mathcal{T}, \mu)$ where X is a set, $\mathcal{T}$ a topology on X and μ a σ-finite measure such that every open set is μ-measurable.*

A set $S \subseteq X$ is almost open *if $S \overset{\mu}{\sim} U$ for some $U \in \mathcal{T}$. The region $[S]_\mu$ is* open *if S is almost open.*

Equivalently, we can say $o \in \mathbb{A}_\mu$ is open if $o = [U]_\mu$ for some open set U. Given a σ-finite measure space (X, μ) and $\mathcal{O} \subseteq \mathbb{A}_\mu$, the supremum of $\mathcal{O}$, which we will denote $\bigsqcup \mathcal{O}$, always exists. With this operation we can define an interior operator on any measure algebra:

Definition 2.21 (measure-theoretic interior)**.** *Let $(X, \mathcal{T}, \mu)$ be a topological measure space and $o \in \mathbb{A}_\mu$. We define the* (measure-theoretic) interior *of o by $o^\square = \bigsqcup \{[U]_\mu \sqsubseteq o : U \in \mathcal{T}\}$.*

Proposition 2.22. *If $(X, \mathcal{T}, \mu)$ is a topological measure space and $o \in \mathbb{A}_\mu$,*

1. *$o^\square$ is open,*
2. *$o^\square \sqsubseteq o$,*
3. *$(o^\square)^\square = o^\square$.*

We are now ready to define our measure-theoretic semantics:

Definition 2.23 (measure-theoretic semantics)**.** *If $(X, \mathcal{T}, \mu)$ is a topological measure space, a* measurable valuation *on X is a function $[\![\cdot]\!] : \mathcal{L}_\square \to \mathbb{A}_\mu$*

satisfying

$$\begin{array}{lcl} [\![\alpha \wedge \beta]\!] & = & [\![\alpha]\!] \sqcap [\![\beta]\!] \\ [\![\neg\alpha]\!] & = & [X]_\mu - [\![\alpha]\!] \\ [\![\Box\alpha]\!] & = & [\![\alpha]\!]^\Box \\ [\![\forall\alpha]\!] & = & \begin{cases} [X]_\mu & \text{if } [\![\alpha]\!] = [X]_\mu \\ [\varnothing]_\mu & \text{otherwise.} \end{cases} \end{array}$$

A topological measure model *is a topological measure space equipped with a measurable valuation.*

The system S4U is sound and *absolutely complete* for our semantics, as I proved in [29]:

Theorem 2.24 (DFD)**.** *Given $\varphi \in \mathcal{L}_{\Box\forall}$, the following are equivalent:*

1. $\mathsf{S4U} \nvdash \varphi$,
2. *for every $\varepsilon \in (0,1)$ there is a measurable valuation $[\![\cdot]\!]$ on the interval $[0,1]$ equipped with the Lebesgue measure such that $|\,[\![\varphi]\!]\,| \geq \varepsilon$.*

Although we will not discuss it here, measure-theoretic semantics readily extend to the dynamical systems setting, as shown by Lando [69]. We now turn to discussing extensions of $\mathcal{L}_\Box$ suitable for the study of such systems.

3 Logic applied to dynamical systems

Despite the success of second-order arithmetic in formalizing mathematical analysis, it has certain drawbacks: due to Gödel's second incompleteness theorem [51], we know that not every true statement expressible in that formalism will be derivable, and, moreover, there is no algorithm for telling whether a theory T in that language can derive a formula φ. However, for many applications, a complete, or even decidable, logic is desirable. One strategy for obtaining this is to reason about dynamical systems in a framework that cannot directly formalize arithmetic, and modal logics are particularly attractive for this purpose.

3.1 Dynamic topological logic

By a dynamical system we mean the following:

Definition 3.1. *A* dynamic topological system *is a tuple* $(X, \mathcal{T}, f)$ *where* $(X, \mathcal{T})$ *is a topological space and* $f\colon X \to X$ *is continuous.*

Artemov et al. proposed a bimodal logic S4C for reasoning about dynamical systems [4]. It includes the interior modality $\Box$, and a 'next-time' modality, which we will denote $\circ$, interpreted using the function f. They the proved that S4C is decidable, as well as being sound and complete for the class of all dynamical systems. Kremer and Mints [67] considered a similar logic, called S4H, and also showed it to be sound and complete for the class of dynamical systems where f is a homeomorphism. They also observed that adding a 'henceforh' operator, G, would allow us to express and reason about the asymptotic properties of dynamical systems, including e.g. recurrence phenomena. 'Eventually', the dual of G, is defined by $F = \neg G \neg$. Let us denote the resulting tri-modal language by $\mathcal{L}^{\circ G}_{\Box}$, and its corresponding logic *dynamic topological logic* (DTL).

To be precise, a *dynamic topological model* is a tuple $\mathcal{X} = (X, f, V)$, where (X, f) is a dynamical system and V is a valuation on X. Semantics for the temporal operators are given by

- $[\![\circ\varphi]\!] = f^{-1}[\![\varphi]\!]$, and
- $[\![G\varphi]\!] = \bigcap_{n<\omega} f^{-n}[\![\varphi]\!]$.

The universal modality $\forall$ is sometimes included. Unfortunately, it was soon shown by Konev et. al. that dynamic topological logic is undecidable [62] over the class of all dynamical systems. Konev et al. also showed that DTL over the class of dynamical systems with a homeomorphism is not even computably enumerable [63]. This led to a search for variants of DTL which retained the capacity for reasoning about asymptotic behavior but remained decidable. Gabelaia et al. proposed to consider dynamic topological logics with finite, but unbounded, time and showed them to be decidable, although not in primitive recursive time [47]. Kremer instead proposed a restriction to dynamical systems where the topology is a partition [66], which gives rise to a decidable DTL.

Despite these negative results, in [28] I proved that DTL is computably enumerable, for which I earned the ***Gödel Centenary Research Prize***. I noted that the tangled closure operator had some natural advantages for working in DTL. With this, I provided an axiomatization for the resulting polyadic logic in [32]. Tangled modalities have since been pursued by other researchers (see, for example, [52]). My work in tangled modal logic was then used in [33, 34] to provide a sound and complete axiomatization for DTL:

Theorem 3.2 (DFD)**.** *The logic* DTL^* *axiomatized by* $\mathsf{S4}^*$*, together with the following:*

Temporal axioms

$\mathrm{Neg}_\circ$ $\neg\circ p \leftrightarrow \circ\neg p$

$\mathrm{And}_\circ$ $\circ(p \wedge q) \leftrightarrow \circ p \wedge \circ q$

Fix_G $Gp \rightarrow p \wedge \circ Gp$

Ind_G $G(p \rightarrow \circ p) \rightarrow (p \rightarrow Gp)$

TCont $\Diamond\circ\Gamma \rightarrow \circ\Diamond\Gamma$

Rules

$\mathsf{N}_\circ$ *Necessitation for* $\circ$

N_G *Necessitation for* G

is sound and complete for the class of dynamic topological systems.

Moreover, my work in [35] shows that the tangled modality is in fact an essential component of this axiomatization, as previously proposed axiomatizations are incomplete:

Theorem 3.3 (DFD)**.** *The logic* DTL *is not finitely axiomatizable.*

However, in the intended applications, one usually does not study arbitrary dynamical systems, but rather systems that have additional structure. One important such class of systems is that of *minimal systems,* i.e., systems that contain no proper, closed, f-closed subsystems. As an example of a minimal system, consider the circle S^1 parametrized by $(\cos(\theta), \sin(\theta))$, and let f be a rotation by an angle γ, where γ is an irrational multiple of π. Given $x_0 \in S^1$, the orbit of x_0 is dense on all of S^1; from this it follows that there can be no proper, non-empty, closed subset of S^1 that is also closed under f; in this sense, the system is minimal. Let

$$V(p) = \{(\cos(\theta), \sin(\theta)) : \alpha < \theta < \beta\}$$

be a small arc in the circle, where p is some propositional variable. Then, $f^n(x_0) \in [\![p]\!]$ for some n, and in general, if $\exists\Box p$ holds, then so does $\forall Fp$; that is, $\exists\Box p \rightarrow \forall Fp$ is valid over the class of minimal systems. (This is not true for arbitrary dynamical systems, as we can see by replacing f by the identity

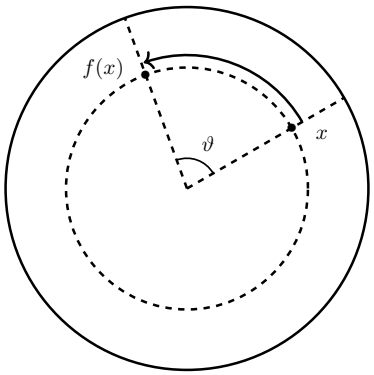

Figure 2: A rotation f of a disk by an angle ϑ gives rise to a probability-preserving system, where the probability of a set is defined to be proportional to its area. Moreover, such a system is not minimal, as (for example) the dashed circle is a closed, f-closed subsystem.

in the same example and choosing $x_0 \notin V(p)$). In [30], I proved that when restricting to this class of systems, DTL becomes decidable, paving the road towards possible future applications in automated deduction:

Theorem 3.4 (DFD)**.** *The set of formulas of $\mathcal{L}^{\circ G}_{\Box\forall}$ formulas valid over the class of minimal systems is decidable.*

Nevertheless, the decision procedure is not primitive recursive, and further simplifications or modifications are needed before such a logic can be implemented.

There are other classes of spaces of mathematical interest where the decidability of DTL has not been established. Minimal systems in the literature are assumed to be compact and Hausorff, and my results do not apply to such spaces. Another class is that of *measure-preserving spaces,* where $\mu(A) = \mu(f^{-1}A)$ for all measurable A (here, μ is any measure, e.g. the volume of a set in $\mathbb{R}^3$). The following result is well-known [82]:

Theorem 3.5 (Poincaré)**.** *If (X, μ, f) is a measure-preserving dynamical system on a complete metric space and $A \subseteq X$ is open, then A contains an* infinitely recurrent point, *that is, there are $x \in A$ and infinitely many values of n such that $f^n(x) \in A$.*

A typical example of a minimal system is a rotation of the unit ball in $\mathbb{R}^2$, i.e., the set of points (x, y) such that $x^2 + y^2 \leq 1$. The DTL of such systems is different from the DTL of arbitrary systems, since in particular the Poincaré recurrence theorem can be formalized as $\Box p \to \Diamond \circ Fp$. The decidability of DTL over this class is also unknown.

Many of the positive results we have obtained reduce the topological semantics to alternative semantics using *non-deterministic quasimodels* [28]. Rather

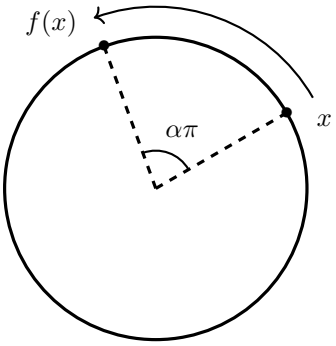

Figure 3: If α is irrational, then a rotation by $\alpha\pi$ gives rise to a minimal system on the unit circle.

than interpreting formulas over a structure (X, f) where X is a topological space, we use structures $(W, \preccurlyeq, S, \ell)$, where $\preccurlyeq$ is a partial order, S a successor relation, and ℓ a 'labeling function', used to record the set of formulas that are to be satisfied at a point $w \in W$. We take S to be continuous in the sense that preimage of open sets is open (where $U \subseteq W$ is open if it is upwards-closed under $\preccurlyeq$); such semantics are a special case of topological semantics, and are known to have a different set of validities if S is a function, but not if it is a binary relation. With this, I proved that the logic of (not necessarily Hausdorff or compact) minimal spaces does not have the finite model property, but it does have the finite *quasi*model property, with which I showed that it is decidable.

3.2 Intuitionistic temporal logic

As a general rule, all of the decidable variants of DTL with continuous functions that are currently known are obtained by either restricting the class of dynamical systems over which they are interpreted, or restricting the logics to reason about finitely many iterations of f. However, there is another variant of DTL, which does not have either of these restrictions, yet whose decidability was never settled. Namely, there is an intuitionistic version of DTL, proposed by Kremer in unpublished work [65]. It is well-known that propositional intuitionistic logic can be seen as a fragment of S4 via the Gödel-Tarski translation [80], and indeed the two share very similar semantics. In particular, intuitionistic logic can be interpreted over topological spaces. One can use this idea to present a version of dynamic topological logic which removes the modality $\Box$, and instead interprets Boolean connectives topologically [74].

To be precise, consider the language $\mathcal{L}^{\circ F}$ whose primitive symbols are

$$\bot, \wedge, \vee, \to, \circ, F,$$

and for $\varphi \in \mathcal{L}^{\circ F}$, define $\varphi^{\Box}$ by recursively replacing each subformula ψ of φ

Class	Notation	$\mathcal{L}^{\circ F}_{\Box\forall}$	$\mathcal{L}^{\circ F}_{\forall}$	$\mathcal{L}^{\circ FG}$
All dynamical systems	c	Undecidable [62] but c.e. [28]	Decidable	Unknown but c.e.
Dynamical systems with a homeomorphism	h	Non-c.e. [63]	Unknown	Unknown
Expanding frames	e	Undecidable [62]	Decidable	Decidable [16]
Persistent frames	p	Non-c.e. [63]	Unknown	Unknown
Minimal systems	m	Decidable, but not primitive recursive [30]	Decidable	Decidable
Poincaré recurrent systems	r	Unknown	Unknown	Unknown

Table 1: This table indicates whether the set of formulas of a given language is decidable over different classes of dynamical systems. Note that languages with $\Box$ use the classical semantics, and languages without it use intuitionistic semantics.

by $\Box\psi$ (for example, $(p \to q)^{\Box} = \Box(\Box p \to \Box q)$). Then, if $\varphi \in \mathcal{L}^{\circ F}$ and $\mathcal{X} = (X, f, V)$ is any dynamic topological model, it follows that $[\![\varphi^{\Box}]\!]_{\mathcal{X}}$ is an open set. With this we can define $\mathsf{ITL}^{\mathsf{c}}$ to be the set of formulas $\varphi \in \mathcal{L}^{\circ F}$ such that $\varphi^{\Box}$ is valid. In [38], I use techniques based on non-deterministic quasimodels, first introduced in [28], to prove the following:

Theorem 3.6 (DFD)**.** *The set of intuitionistically valid $\mathcal{L}^{\circ F}_{\forall}$ formulas over the class of all dynamical systems is decidable.*

Note that we omit G, which is not intuitionistically definable in terms of F. The reason for this is that the semantics for G require an infinite intersection, which is typically not an open set, causing technical difficulties. However, this issue does not occur over topologies generated by a preorder. Dynamical systems over such topologies are closely related to *expanding products of modal logics* [47], and as such we sometimes call them *expanding frames.* We proved the following in [16]:

Theorem 3.7 (Boudou, Diéguez, DFD)**.** *The set of intuitionistically valid $\mathcal{L}^{\circ FG}_{\forall}$ formulas over the class of all expanding frames is decidable.*

It is worth noting the contrast with dynamic topological logics, which are typically undecidable. Thus intuitionistic temporal logic may be the tool of choice for automated reasoning about dynamical systems. However, research

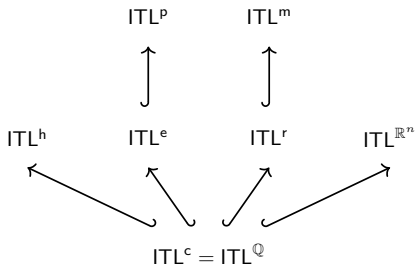

Figure 4: Inclusions among intuitionistic temporal logics we have considered, with notation as in Table 1.

on intuitionistic temporal logic is at an early stage, and there is much to be explored; no complete calculus is available, and a lower bound on complexity is unknown. It is also likely that intuitionistic temporal logic based on special classes of dynamical systems may lead to more feasible logics; for example, DTL over the class of minimal systems only decidable in non-primitive recursive time. It is likely that the intuitionistic temporal logic of minimal systems is feasible. Moreover, minimality may be expressed succinctly in the intuitionistic setting by $\exists p \to \Diamond p$.

However, even the decidable logics in this table are non-elementary. To this end, let us see how the validity problem can be greatly simplified by passing the focus from *regions* to *positions.*

3.3 Compass logics of positions

The logics we have described above are tailored for mathematical applications, but this is not the only setting in which automated reasoning about dynamical systems may be employed. In artificial intelligence, one is often faced with a situation where a robot must reason and plan within an ever-changing environment.

Consider, for example, a robot designed to play a team sport such as basketball. Such a robot would need to model the positions of other members of its team, as well as the opposing team, update this information as other players move, and anticipate possible changes that may occur in their position.

In this setting, mathematical precision takes a back seat to simplicity and efficiency. For example, the two-dimensional plane may be modeled as a discrete grid with a high enough resolution. With this in mind, in [7] we developed a general framework for spatial reasoning based on $\mathbb{Z}^d$. In this setting, an agent is mainly concerned with the position of other agents, modeled as points in the grid. To this end, fix a set $\mathbb{A}$ of 'agents'. Fix also a dimension $d \in \mathbb{N}$; typically we take $d \in \{2, 3\}$, but all of our main results apply to arbitrary d. The set of actions $\mathcal{A}_d^{\mathsf{DL\text{-}S}^*}$ and the set of formulas $\mathcal{L}_d^{\mathsf{DL\text{-}S}^*}$ of $\mathsf{DL\text{-}S}_d^*$ are defined by the following grammar:

$$\begin{array}{lcl} \alpha & ::= & \oplus_k \mid \ominus_k \mid \alpha;\alpha' \mid \alpha \cup \alpha' \mid \alpha^* \\ \varphi & ::= & p \mid \mathsf{h}_i \mid \neg\varphi \mid \varphi \wedge \psi \mid [\alpha]\varphi \end{array}$$

Here, $k < d$ denotes a dimension. In this setting, we assume that robots model space as a discrete grid, and hence the models we consider are based on $\mathbb{Z}^d$. We call these *discrete models.*

Definition 3.8 (Discrete model)**.** *A discrete model is a pair (P, V) where:*

- $P : \mathbb{A} \to \mathbb{Z}^d$*;*
- $V : \mathbb{P} \to 2^{\mathbb{Z}^d}$*.*

For every $\vec{x} \in \mathbb{Z}^d$, $P(i) = \vec{x}$ means that the agent i is in the position $\vec{x}$, whereas $\vec{x} \in V(p)$ means that p is true at the position $\vec{x}$. Formulas are evaluated with respect to a discrete model (P, V) and a vector $\vec{x}$. Below, let $\vec{e}_i$ denote the vector whose i^{th} component is 1, and whose other components are zero.

Definition 3.9 (R_α and truth conditions)**.** *Let (P, V) be a discrete model. For all spatial programs α and for all formulas φ, the binary relation R_α is defined recursively as follows:*

$$\begin{array}{lcl} R_{\oplus_k} & = & \{(\vec{x}, \vec{x} + \vec{e}_k) : \vec{x} \in \mathbb{Z}^d\}, \\ R_{\ominus_k} & = & \{(\vec{x}, \vec{x} - \vec{e}_k) : \vec{x} \in \mathbb{Z}^d\}, \\ R_{\alpha_1;\alpha_2} & = & R_{\alpha_2} \circ R_{\alpha_1} \\ R_{\alpha_1 \cup \alpha_2} & = & R_{\alpha_1} \cup R_{\alpha_2} \\ R_{\alpha^*} & = & (R_\alpha)^* \\ R_{?\varphi} & = & \{(\vec{x}, \vec{x}) \in \mathbb{Z}^d \times \mathbb{Z}^d : (P, V), \vec{x} \models \varphi\} \end{array}$$

Extend V to a valuation V^+ on $\mathbb{P} \cup \{\mathsf{h}_i : i \in \mathbb{A}\}$ by letting $V^+(p) = V(p)$ for $p \in \mathbb{P}$, and letting $V^+(\mathsf{h}_i) = \{P(i)\}$ for $i \in \mathbb{A}$. Then, we identify (P, V) with the multirelational Kripke model $\mathcal{M} = (\mathbb{Z}^d, (R_\alpha)_{\alpha \in \mathcal{A}_d^{\mathsf{DL\text{-}S}^*}}, V^+)$, and we define $(P, V), \vec{x} \models \varphi$ if and only if $(\mathcal{M}, \vec{x})] \models \varphi$, in the sense of Definition 2.6.

It readily follows from well-known results [47] that the logic $\mathsf{DL\text{-}S}_d^*$ is undecidable, and even non-axiomatizable. However, as agents will mainly be concerned with modeling other agents' positions, rather than regions in space, we may disregard the propositional atoms. We may also somewhat simplify the set of spatial actions. To be precise, we define the *language of discrete compass logic* by the sublanguage $\mathcal{L}_d^{\mathsf{CL\text{-}P}^*}$ of $\mathcal{L}_d^{\mathsf{DL\text{-}S}^*}$, where propositional atoms are omitted and $*$ is only allowed to be applied to atomic programs (i.e., of the forms $\oplus_k$ or $\ominus_k$). In [7], we prove the following:

Theorem 3.10 (Balbiani, DFD, Lorini)**.** *The satisfiability problem for $\mathsf{CL\text{-}P}_d^*$ is in* NP*.*

The proof in [7] is stated for $d = 2$, but readily extends to arbitrary d. This result is quite surprising; note that NP is the best-case scenario for any logic that extends propositional logic, as is the case of $\mathsf{CL\text{-}P}_d^*$ (if we regard the position atoms as propositions).

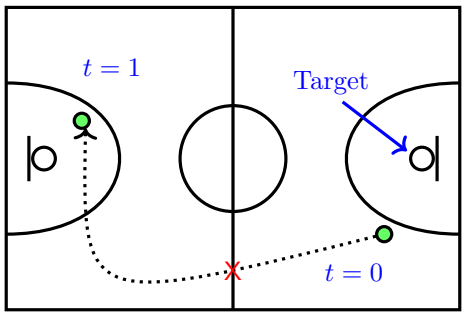

Figure 5: The robot should be able to recognize that a back-court violation has occurred based only on the observations at $t = 0$ and $t = 1$.

3.4 Lexicographic products of modal logics

As we have mentioned before, dynamic topological systems are related to expanding products of modal logics, which are often undecidable when one of the products is LTL. While we will not define expanding products here, a different way to obtain decidable variants is to work with slightly modified products, called *lexicographic producs.* In particular, we are interested in products of (say) **K** frames with $\mathbb{N}$. The *lexicographic product of a* $\mathbf{K}$*-frame* $\mathcal{F} = (W, R)$ *with* $\mathbb{N}$ is the relational structure $\mathcal{F} \triangleleft \mathbb{N} = (W', R', S', <')$ defined as follows:

1. $W' = W \times \mathbb{N}$,
2. R' is the binary relation on W' defined by $(s, i)\ R'\ (t, j)$ iff $s\ R\ t$ and $i = j$,
3. S' is the binary relation on W' defined by $(s, i)\ S'\ (t, j)$ iff $i + 1 = j$,
4. $<'$ is the binary relation on W' defined by $(s, i) <' (t, j)$ iff $i < j$.

We then interpret $\mathcal{L}_{\Box}^{\circ G}$-formulas as in Definition 2.6, where $\Box$ is interpreted by R', $\circ$ by S' and G by $<'$. In the case that $\mathcal{F}$ is an **S4** frame, we obtain a close relative of DTL. However, as we showed in [5], these products often enjoy natural axiomatizations:

Theorem 3.11 (Balbiani, DFD)**.** *If* $\mathbf{C}$ *is any of*

$$\mathbf{KD}, \mathbf{T}, \mathbf{KD4}, \mathbf{S4}, \mathbf{S5},$$

then the set of $\mathcal{L}_{\Box}^{\circ G}$ *formulas valid over the class* $\{\mathbb{N} \triangleleft \mathcal{F} : \mathcal{F} \in \mathbf{C}\}$ *is finitely axiomatizable, as is the set of valid* $\mathcal{L}_{\Box\forall}^{\circ G}$ *formulas.*

Indeed, the results of [5] are more general and apply to a wider class of logics. Note that $\circ$ is no longer interpreted using a function, and hence it is not equivalent to its dual, $\hat{\circ} \equiv \neg\circ\neg$. The key axioms involving temporal modalities are as follows:

1. $\circ(p \to q) \to (\circ p \to \circ q)$,
2. $G(p \to q) \to (Gp \to Gq)$,
3. $\hat{\circ}\top$,
4. $\hat{\circ}\hat{\circ}p \to \circ\hat{\circ}p$,
5. $Gp \to GGp$,
6. $Gp \to \circ p$,
7. $\circ p \to \circ\Box p$,
8. $\circ p \to \Box\circ p$,
9. $\Diamond\circ p \to \circ p$,
10. $Gp \to G\Box p$,
11. $Gp \to \Box Gp$,
12. $\Diamond Gp \to Gp$.

Note that some lexicographically valid formulas are not valid on dynamical systems, and vice-versa. Nevertheless, the techniques used in [5] suggest that all of the logics we have mentioned are in PSPACE (although we leave a proof of this for future work), making lexicographic logics an attractive candidate for 'approximate' reasoning about topological dynamics.

4 Dynamical systems applied to logic

In this section we will be concerned with another fruitful interpretation of modality, suggested by Gödel. Namely, we may use $\Box_T\varphi$ to mean "φ is provable in T", where T is Peano arithmetic (PA), or some other arithmetical theory [15]. As usual, $\Diamond_T\varphi$ is defined as $\neg\Box_T\neg\varphi$. Gödel's own second incompleteness theorem may then be formalized as $\Diamond_T\top \to \Diamond_T\Box_T\bot$.

In order to formalize this, let us review the language of first-order arithmetic. We will use the language Π_ω of first-order arithmetic containing the signature

$$\{\mathtt{0}, \mathtt{1}, +, \cdot, \mathtt{2}^{\cdot}, =\},$$

so that we have symbols for addition, multiplication, and exponentiation, as well as Boolean connectives and quantifiers ranging over the natural numbers. Elements of Π_ω are *formulas.* The set of all formulas where all quantifiers are *bounded,* that is, of the form $\forall\, x{<}t\ \varphi$ or $\exists\, x{<}t\ \varphi$ (where t is any term), is denoted Δ_0. A formula of the form $\exists x_n \forall x_{n-1} \ldots \delta(x_1, \ldots, x_n)$, with $\delta \in \Delta_0$, is Σ_n, and a formula of the form $\forall x_n \exists x_{n-1} \ldots \delta(x_1, \ldots, x_n)$ is Π_n. These classes are extended modulo provable equivalence, so that every formula falls into one of them. Note that the negation of a Σ_n formula is Π_n and vice-versa.

In order to formalize provability within arithmetic, we fix some Gödel numbering mapping a formula $\psi \in \Pi_\omega$ to its corresponding Gödel number $\ulcorner\psi\urcorner$, and similarly for terms and sequences of formulas, which can be used to represent derivations. We also define the *numeral* of $n \in \mathbb{N}$ to be the term

$$\bar{n} = \mathtt{0} + \underbrace{\mathtt{1} + \ldots + \mathtt{1}}_{n \text{ times}}.$$

In order to simplify notation, we will often identify ψ with $\ulcorner\psi\urcorner$.

We will assume that every theory T contains classical predicate logic, is closed under modus ponens, and that there is a Δ_0 formula $\mathtt{Proof}_T(x, y)$ which holds if and only if x codes a derivation in T of a formula coded by y. Using Craig's trick, any theory with a computably enumerable set of axioms is deductively equivalent to one in this form, so we do not lose generality by these assumptions.

If φ is a natural number (supposedly coding a formula), we use $\Box_T\varphi$ as shorthand for $\exists y\, \mathtt{Proof}_T(y, \bar{\varphi})$. To get started on proving theorems about arithmetic, we need a minimal 'background theory'. This will use Robinson's arithmetic Q enriched with axioms for the exponential; call the resulting theory Q^+. To be precise, Q^+ is axiomatized by classical first-order logic with equality, together with the following:

- $\forall x\ (x + \mathtt{0} = x)$
- $\forall x\ (x \neq \mathtt{0} \leftrightarrow \exists y\ x = y + \mathtt{1})$
- $\forall x \forall y\ (x + \mathtt{1} = y + \mathtt{1} \to x = y)$
- $\forall x \forall y\ \big(x + (y + \mathtt{1}) = (x + y) + \mathtt{1}\big)$
- $\forall x\ (x \times \mathtt{0} = \mathtt{0})$
- $\forall x \forall y\ \big(x \times (y + \mathtt{1}) = (x \times y) + y\big)$

- $2^0 = 1$
- $\forall x \ \big(2^{x+1} = 2^x + 2^x\big)$

Aside from these basic axioms, the induction schema for Γ is defined by

$$\mathtt{I}\Gamma\text{:}\ \ \varphi(\overline{0}) \wedge \forall x\big(\varphi(x) \to \varphi(x+\overline{1})\big) \to \forall x \varphi(x), \qquad \text{where } \varphi \in \Gamma.$$

Elementary arithmetic is the first-order theory

$$\mathrm{EA} = \mathrm{Q}^+ + \mathrm{I}\Delta_0,$$

and *Peano arithmetic* is the first-order theory

$$\mathrm{PA} = \mathrm{Q}^+ + \mathrm{I}\Pi_\omega.$$

In 1986, Japaridze proposed a poly-modal variant of provability logic with an increasing sequence of modalities $[0]_T, [1]_T, [2]_T, \ldots$, which we denote GLP_ω. The expression $[n]_T\varphi$ is interpreted as "φ is provable in T from a true Π_n statement" [58]. More precisely, let $\mathtt{True}_{\Pi_n}$ be the standard partial truth-predicate for Π_n formulas, which is itself of complexity Π_n (see [54] for information about partial truth definitions within EA). Then, we define

$$[n]_T\varphi \leftrightarrow \exists \pi \ \big(\mathtt{True}_{\Pi_n}(\pi) \wedge \Box_T(\pi \to \varphi)\big).$$

Statements of the form "What is provable in T is true" are called *reflection principles. Uniform reflection over* T is the schema

$$\mathtt{RFN}(T) \equiv \forall n \ \big(\Box_T\varphi(\bar{n}) \to \varphi(n)\big).$$

Such principles often give rise to mathematically natural theories, e.g.

$$\mathrm{PA} \equiv \mathrm{EA} + \mathtt{RFN}(\mathrm{EA}), \tag{1}$$

as shown by Kreisel and Lévy [64]. Beklemishev has shown that this representation of PA can be used to give a consistency proof of PA using only a single transfinite induction [8]. They key insight behind this proof uses Turing progressions, which are a transfinite-time dynamical system defined over the set of formal theories, and these in turn can be represented within Japaridze's polymodal provability logic and its transfinite extensions, which we discuss next.

4.1 The polymodal provability logic

Given an ordinal Λ, we define a polymodal language $\mathcal{L}_\Lambda$ built from propositional variables in a countably infinite set $\mathbb{P}$ and the constant $\top$ together with the Boolean connectives $\neg, \wedge$ and a unary modal operator $[\alpha]$ for each $\alpha < \Lambda$. As before, we write $\langle\alpha\rangle$ as a shorthand for $\neg[\alpha]\neg$.

Definition 4.1 (GLP_Λ)**.** *Given an ordinal* Λ*,* GLP_Λ *is the logic over* $\mathcal{L}_\Lambda$ *given by the following axioms and rules:*

- *All substitution instances of propositional tautologies,*

- *For all $\alpha, \beta < \Lambda$ and formulas $\varphi, \psi \in \mathcal{L}_\Lambda$,*

(i)	$[\alpha](\varphi \to \psi) \to ([\alpha]\varphi \to [\alpha]\psi)$	
(ii)	$[\alpha]([\alpha]\varphi \to \varphi) \to [\alpha]\varphi$	
(iv)	$\langle\alpha\rangle\varphi \to [\beta]\langle\alpha\rangle\varphi$	*for $\alpha < \beta$,*
(v)	$[\alpha]\varphi \to [\beta]\varphi$	*for $\alpha \leq \beta$.*

- *Modus Ponens and the necessitation rule* $\dfrac{\varphi}{[\alpha]\varphi}$ *for each modality $\alpha < \Lambda$.*

Unfortunately, GLP_Λ has no non-trivial Kripke models, although its *variable-free* or *closed fragment* (defined below) does [57]. Because of this, the study of topological semantics of GLP_Λ is crucial; fortunately, in this setting we do have several completeness results. These models are based on ordinals; more specifically, they rely on considering dynamical systems on the class of ordinal numbers. Dynamical systems on transfinite time will also be useful for defining Turing progressions, and hence we discuss transfinite dynamics before continuing with GLP_Λ and its semantics.

4.2 Ordinal dynamical systems

Consider a marble placed on a concave surface (such as the inside of a bowl). Assuming that both the marble and the bowl are smooth, the marble will roll towards the bottom and eventually settle there. In fact, if the marble is initially placed at the very bottom, it will not move at all; such a steady state of a dynamical system is a *fixed point.* But suppose that we replace the bowl with a jagged, uneven surface. Instead of rolling smoothly, the marble may bounce chaotically; a very small change in the marble's initial state may send it in an entirely different direction. Nevertheless, as the marble bounces, it should lose potential energy, and, as in the smooth case, eventually reach a fixed point; however, it may be difficult to predict where exactly it will end up.

In either case, we may model the marble's movement using a *flow,* that is, a family of functions $\{\varphi^t : t \in \mathbb{R}\}$ with $\varphi^{t+s} = \varphi^t \circ \varphi^s$, so that $\varphi^t(x)$ would be the state of the marble at time t if it it were originally in state x. For simplicity, this flow can be approximated by a discrete-time dynamical system by defining $f(x) = \varphi^\varepsilon(x)$ for suitably small ε (possibly depending on x). In the case of a smooth bowl, the function f thus defined would be continuous, but this is not necessarily the case once we replace it by a jagged surface. We may then study the function f to predict the marble's behavior. In particular, if we wish to know where it will stabilize, we may ask whether f has a fixed point, i.e., if there is x_* such that $x_* = f(x_*)$.

If f is indeed continuous, then the marble will reach a fixed point by $f^\omega(x_0)$, where x_0 is the marble's original state and $f^\omega(x_0) = \lim_{n\to\infty} f^n(x_0)$. However, if it so happens that at this point the surface is jagged, the marble may jump again to $f^{\omega+1}(x_0)$. This process may continue transfinitely, but if the marble loses potential energy at each stage, it will finally reach a fixed point at some countable ordinal ξ_*. In such a setting, it makes sense to consider *ordinal flows,*

where t may take transfinite values. Recall that addition, multiplication and exponentiation can be defined on the ordinals in a natural way (see e.g. [59]). Thus we may consider families of functions $\{\varphi^\xi : \xi \in \mathsf{On}\}$, where On denotes the class of ordinal numbers, and such that $\varphi^\xi \circ \varphi^\zeta = \varphi^{\xi+\zeta}$.

Taking this idea farther, we may let the domain of each φ^ξ also be a set of ordinals. To be precise, let Γ, Λ be ordinals, and say that a Λ-*flow over* Γ is a homomorphism φ from $(\Lambda, +)$ into the class of continuous functions on Γ. Of particular interest is the case when each φ^λ is normal (that is, both continuous and increasing), in which case we will call φ a *normal flow.* We then have the following result [42]:

Theorem 4.2 (DFD, Joosten)**.** *Given a normal function $f\colon \mathsf{On} \to \mathsf{On}$, there is a unique normal flow $(f^\lambda)_{\lambda\in\mathsf{On}}$ such that $f^1 = f$ and, if $(g^\lambda)_{\lambda\in\mathsf{On}}$ is any other normal flow with $g^1 = f$, then $f^\lambda(\gamma) \leq g^\lambda(\gamma)$ for all λ, γ.*

We call the minimal normal flow given by the theorem the *hyperation* of f. We will use $(\varphi^\lambda)_{\xi\in\mathsf{On}}$ to denote the hyperation of the function $\gamma \mapsto \omega^\gamma$, where ω is the first infinite ordinal. Beklemishev's consistency proof uses transfinite induction over the ordinal $\varepsilon_0 = \varphi^\omega(0)$, which is also the first fixed point of the function $\lambda \mapsto \omega^\lambda$.

Then, just as in the case of real flows, we may ask for which $\Gamma > 0$ there are normal Γ-flows over Γ. Let us say that such an ordinal is a *dynamically autonomous number.* The answer was given by Joosten and I in [42]:

Theorem 4.3 (DFD, Joosten)**.** *The first dynamically autonomous number is Γ_0, the least fixed point of the function $\lambda \mapsto \varphi^\lambda(0)$.*

In fact, for those familiar with Veblen functions [81], which we denote $(\varphi_\lambda)_{\lambda\in\mathsf{On}}$, we mention that $\varphi_\lambda = \varphi^{\omega^\lambda}$ for all λ. This gives us an alternative notation system for ordinals below Γ_0. Define $\varphi(\xi) = \omega^\xi$, so that $(\varphi^\zeta)_{\zeta\in\mathsf{On}}$ denotes the hyperation of the function $\xi \mapsto \omega^\xi$. Then we obtain the following, which I showed with my student, Aguilera [1]:

Theorem 4.4 (Aguilera, DFD)**.** *Given an ordinal $\xi > 0$, there are uniquely defined α, β such that $\xi = \varphi^\alpha(\beta)$, where β is either zero or additively decomposable.*

Recall that a non-zero ordinal is additively decomposable if it cannot be written as the sum of two smaller ordinals. Thus we may regard the number α obtained above is the *degree of indecomposability* of ξ.

For technical reasons, it is convenient to work with a slight modification of the functions φ^ξ. Namely, we work instead with the function $e(\xi) = -1 + \omega^\xi$ (i.e., $e(0) = 0$ and otherwise $e(\xi) = \omega^\xi$), and call its hyperation $(e^\xi)_{\xi\in\mathsf{Ord}}$ the *hyperexponential function.* In particular, this function is a right-inverse to the *hyperlogarithm,* defined as follows:

Definition 4.5 (Hyperlogarithms)**.** *Any ordinal $\xi > 0$ can be written uniquely in the form $\alpha + \omega^\beta$, and we define $\ell\xi = \beta$. We also set $\ell 0 = 0$.*

Then, we define the sequence $\langle \ell^\xi \rangle_{\xi\in\mathsf{On}}$ to be the unique family of initial functions such that

1. $\ell^1 = \ell$,
2. $\ell^{\alpha+\beta} = \ell^\beta \ell^\alpha$ *for all ordinals* α, β,
3. $(\ell^\xi)_{\xi \in \mathsf{On}}$ *is pointwise maximal among all families of functions satisfying the above clauses.*

The correctness of this definition is also shown in [42]. Hyplogarithms give another family of transfinite dynamical systems. Note that, while $e^{\alpha+\beta} = e^\alpha \circ e^\beta$, we have that $\ell^{\alpha+\beta} = \ell^\beta \circ \ell^\alpha$, and in general ordinal addition does not commute, so the two are not equivalent. Moreover, hyperexponentials and hyperlogarithms cancel each other out, in the sense that $\ell^\xi \circ e^\xi(\alpha) = \alpha$ for all ξ, α. These operations will be essential later for describing topological models of GLP_Λ.

4.3 Turing-Feferman progressions and provability spectra

In his thesis, Turing proposed to extend a theory T by iteratively adding its own consistency assertions [27]. This gives a strictly increasing sequence of theories, provided they are consistent, and may be seen as a transfinite dynamical system on the set of all theories in the language of first- or second-order arithmetic, and thus many of the tools proposed above can be used to formalize them. To be precise, let Θ be the set of all formal theories (say, in the language of arithmetic), and define a transfinite-time flow $(\tau^\xi)_{\xi<\Lambda}$ given by

1. $\tau^0(X) = X$,
2. $\tau^{\xi+1}(X) = X_\xi + \Diamond_{\tau^\xi(X)} \top$,
3. $\tau^\lambda(X) = \bigcup_{\xi<\lambda} \tau^\xi(X)$ for λ a limit ordinal,

where $X \in \Theta$.

The flow $\vec{\tau}$ can be generalized to obtain the *n-progression of* X, denoted $(\tau_n^\xi)_{\xi<\Lambda}$, where τ_n^ξ is defined as τ^ξ but setting

$$\tau_n^{\xi+1}(X) = \tau_n^\xi(X) + \langle n \rangle_{\tau_n^\xi(X)} \top.$$

Joosten has developed a systematic study of *Turing-Taylor progressions* [60], i.e. the representation of a theory T in the form

$$U + \tau^{\alpha_0}(U) + \tau_1^{\alpha_1}(U) + \tau_2^{\alpha_2}(U) + \dots$$

Then, the *provability spectrum* of T is the sequence $(\alpha_i)_{i<\omega}$. In particular, α_0 is the Π^0_1 *ordinal,* or *consistency measure,* of T. Beklemishev's consistency proof of PA uses the fact that PA has ε_0 as its Π^0_1 ordinal. Thus if we want to produce similar consistency proofs for stronger theories, a natural first step is to compute their provability spectra, and this requires understanding the logics GLP_Λ for $\Lambda > \omega$. Later we will give proof-theoretic interpretations for these logics, but first let us discuss their Kripke and topologial semantics. We begin with semantics for the variable-free fragment.

4.4 The closed fragment

As it turns out, the variable-free, or *closed,* fragment of GLP_Λ, is sufficient for Beklemishev's proof-theoretic applications. Let us denote by $\mathcal{L}^0_\Lambda$ the fragment of $\mathcal{L}_\Lambda$ that does not allow any propositional variables aside from $\top$, and by GLP^0_Λ the set of derivable formulas within this fragment.

Of particular interest in this fragment are *worms.* A worm is a formula of the form

$$\langle\lambda_0\rangle\dots\langle\lambda_I\rangle\top.$$

These formulas correspond to iterated consistency statements, and indeed can be used to study the proof-theoretic strength of many theories related to Peano Arithmetic, as Beklemishev has shown [8].

Worms are well-ordered by their *consistency strength.* Let us denote the set of worms with entries less than Λ by $\mathbb{W}^\Lambda$; then, given worms $\mathfrak{v},\mathfrak{w}\in\mathbb{W}^\Lambda$, define $\mathfrak{v}\lhd\mathfrak{w}$ if $\mathsf{GLP}_\Lambda\vdash\mathfrak{w}\to\Diamond\mathfrak{v}$.

The relation $\lhd$ we have just defined is a well-order [8, 45]. Thus we may compute the order-type of a worm $\mathfrak{w}\in\mathbb{W}^\Lambda$:

$$o(\mathfrak{w})=\sup_{\mathfrak{v}\lhd\mathfrak{w}}(o(\mathfrak{v})+1).$$

It will be convenient to review the calculus for computing o that is given in [45]. First, if $\mathfrak{v}=\langle\xi_1\rangle\dots\langle\xi_N\rangle\top$ and $\mathfrak{w}=\langle\zeta_1\rangle\dots\langle\zeta_M\rangle\top$, define

$$\mathfrak{v}\Diamond\mathfrak{w}=\langle\xi_1\rangle\dots\langle\xi_N\rangle\langle0\rangle\langle\zeta_1\rangle\dots\langle\zeta_M\rangle\top.$$

Further, if α is any ordinal, set

$$\alpha\uparrow\mathfrak{w}=\langle\alpha+\zeta_1\rangle\dots\langle\alpha+\zeta_M\rangle\top.$$

Theorem 4.6 (DFD, Joosten)**.** *Let $\mathfrak{v},\mathfrak{w}$ be worms and α an ordinal.*

Then,

$$o(\top)=0 \tag{2}$$

$$o(\mathfrak{v}\Diamond\mathfrak{w})=o(\mathfrak{w})+1+o(\mathfrak{v}) \tag{3}$$

$$o(\alpha\uparrow\mathfrak{w})=e^\alpha o(\mathfrak{w}). \tag{4}$$

Here we see an advantage of using e rather than φ as a basis of our ordinal notation system, as these expressions become somewhat more cumbersome with the latter. Moreover, as shown by Ignatiev in the case of $\Lambda=\omega$ and Joosten and I for arbitrary Λ, the fragment GLP^0_Λ is indeed Kripke-complete. Here, we present the general version of Ignatiev's model, as introduced by Joosten and I in [43].

Definition 4.7 (generalized Ignatiev models)**.** *Let Θ,Λ be ordinals.*

We define an ℓ-sequence *(of depth Θ and length Λ) to be a function*

$$f:\Lambda\to\Theta$$

such that, for every $\zeta \in (0, \Lambda)$, we have that

$$f(\zeta) \leq \ell^{-\xi+\zeta} f(\xi) \tag{5}$$

provided $\xi < \zeta$ is large enough.[1]

Given ordinals Θ, Λ, define a structure

$$\mathfrak{Ig}^{\Theta}_{\Lambda} = (D^{\Theta}_{\Lambda}, (<_{\xi})_{\xi<\Lambda})$$

by setting D^{Θ}_{Λ} to be the set of all ℓ-sequences of depth Θ and length Λ. Define $f <_{\xi} g$ if and only if $f(\zeta) = g(\zeta)$ for all $\zeta < \xi$ and $f(\xi) < g(\xi)$.

In [43], we also prove the following, which was proven by Ignatiev in [57] in the case $\Lambda \leq \omega$:

Theorem 4.8 (DFD, Joosten)**.** *Let Λ be any ordinal and $\varphi \in \mathcal{L}^0_{\Lambda}$. Then, $\mathsf{GLP}^0_{\Lambda} \vdash \varphi$ if and only if $\mathfrak{Ig}^{e_{\Lambda}1}_{\Lambda} \models \varphi$.*

However, as we have discussed previously, the full logic GLP_{Λ} cannot be sound and complete for any class of Kripke frames, and hence we turn instead to topological models of these logics.

4.5 Topological semantics of provability logic

The logic GLP_{ω} (or even GLP_2) is not Kripke-complete, so much of the study of these logics relies heavily on topological semantics, including [1], which is based on the thesis of my student, Juan Pablo Aguilera. It also required a new system of ordinal notations reported by Joosten and I in [42, 45].

Given an ordinal Θ, there are several natural topologies we may consider on Θ. We define, first, the topology $\mathcal{I}_0$, consisting of all initial segments $[0, \beta)$ of Θ. Second, we have the usual order topology (as used, say, on the real line), generated by sets of the form (α, β) (where we allow $\alpha = -1$ so that initial segments are open). However, this readily extends to all λ to produce the *generalized λ-Icard topologies,* introduced by Icard for $\lambda < \omega$ in [56] and for arbitrary λ by myself in [36].

Definition 4.9. *Fix ordinals Θ, Λ. For $1 < \lambda < \Lambda$ define a topology $\mathcal{I}_{\lambda}$ on Θ by setting, for $\lambda < \Lambda$, $\mathcal{I}_{\lambda}$ to be the topology generated by sets of the form*

$$(\alpha, \beta]_{\xi} = \left\{ \vartheta : \alpha < \ell^{\xi}\vartheta \leq \beta \right\}.$$

We will denote the resulting polytopological space $(\Theta, (\mathcal{I}_{\lambda})_{\lambda<\Lambda})$ by $\mathfrak{Ic}^{\Theta}_{\Lambda}$.

We can view $\mathfrak{Ic}^{\Theta}_{\Lambda}$ as a polytopological space, or regard the topologies $(\Theta, \mathcal{I}_{\lambda})$ in isolation. The latter gives us semantics for GLP_1, and indeed, as I showed with Aguilera in [1], we obtain strong completeness:

[1] More precisely, given $\zeta \in (0, \Lambda)$ there is $\vartheta < \zeta$ such that (5) holds whenever $\xi \in [\vartheta, \zeta)$.

Theorem 4.10 (Aguilera, DFD)**.** *Let λ be a nonzero ordinal and $\Theta > e^\lambda\omega$. Then,* **GL** *is strongly complete with respect to $(\Theta, \mathcal{I}_\lambda)$.*

Moreover, an analogue of Theorem 4.8 holds for generalized Icard spaces:

Theorem 4.11 (DFD, Joosten)**.** *Let Λ be any ordinal and $\varphi \in \mathcal{L}^0_\Lambda$. Then, $\mathsf{GLP}^0_\Lambda \vdash \varphi$ if and only if $\mathfrak{Ic}^{e^\Lambda 1}_\Lambda \models \varphi$.*

Unfortunately, as was the case with Ignatiev's models, Icard topologies do not give a model of the full GLP_Λ. However, as shown by Beklemishev and Gabelaia [10] for $\Lambda = \omega$ and myself for countable Λ [36], they can be used as the 'backbone' of a model of the full logic.

Theorem 4.12 (DFD)**.** *Given a countable ordinal Λ and a GLP_Λ-consistent formula $\varphi \in \mathcal{L}_\Lambda$, there exist a family of topologies $(\mathcal{T}_\lambda)_{\lambda<\Lambda}$ on $\Theta = e^{1+\Lambda}1$ such that*

1. *$\mathcal{I}_{1+\lambda} \subseteq \mathcal{T}_\lambda$ for each $\lambda < \lambda$,*
2. *$(\Theta, (\mathcal{T}_\lambda)_{\lambda<\Lambda}) \models \mathsf{GLP}_\Lambda$, and*
3. *there is a valuation V on Θ and $\theta \in \Theta$ such that*

$$(\Theta, (\mathcal{T}_\lambda)_{\lambda<\Lambda}, V, \theta) \models \varphi.$$

Thus the logics GLP_Λ are sound and complete for their topological semantics. However, the 'intended' interpretation of these logics is proof-theoretic, and for this we turn to the language of second-order arithmetic.

4.6 Subsystems of second-order arithmetic

In order to define proof-theoretical semantics for GLP_Λ, it will be convenient to pass to the language Π^1_ω of second-order arithmetic. This language extends that of first-order arithmetic with new variables $X, Y, Z, \ldots$ denoting sets of natural numbers, along with new atomic formulas $t \in X$ and second-order quantifiers $\forall X, \exists X$. As is standard, we may define $X \subseteq Y$ by $\forall x(x \in X \to x \in Y)$, and $X = Y$ by $X \subseteq Y \wedge Y \subseteq X$.

When working in a second-order context, we write Π^0_n instead of Π_n (note that these formulas could contain second-order parameters, but no quantifiers over sets). The classes Σ^1_n, Π^1_n are defined analogously to their first-order counterparts, but using alternating second-order quantifiers and setting $\Sigma^1_0 = \Pi^1_0 = \Delta^1_0 = \Pi^0_\omega$. It is well-known that every second-order formula is equivalent to another in one of the above forms.

When axiomatizing second-order arithmetic, the focus passes from induction to *comprehension;* that is, axioms stating the existence of sets whole elements satisfy a prescribed property. Some important axioms and schemes are:

Γ-`CA`: $\exists X \forall x \left(x \in X \leftrightarrow \varphi(x)\right)$, where $\varphi \in \Gamma$ and X is not free in φ;

Δ^0_1-CA: $\forall x\big(\pi(w) \leftrightarrow \sigma(x)\big) \to \exists X \forall x\ \big(x \in X \leftrightarrow \sigma(x)\big)$, where $\sigma \in \Sigma^0_1$, $\pi \in \Pi^0_1$, and X is not free in σ or π;

Ind: $0 \in X \wedge \forall x\ \big(x \in X \to x + 1 \in X\big)\ \to\ \forall x\,(x \in X)$.

We mention one further axiom that requires a more elaborate setup. We may represent well-orders in second-order arithmetic as pairs of sets $\Lambda = \langle |\Lambda|, \leq_\Lambda \rangle$, and define

$$\mathtt{WO}(\Lambda) = \mathtt{linear}(\Lambda) \wedge \forall X \subseteq |\Lambda|\ (\exists x \in X \to \exists y \in X \forall z \in X y \leq_\Lambda z),$$

where $\mathtt{linear}(\Lambda)$ is a formula expressing that Λ is a linear order.

Given a set X whose elements we will regard as ordered pairs $\langle \lambda, n \rangle$, let $X_{<_\Lambda \lambda}$ be the set of all $\langle \mu, n \rangle$ with $\mu <_\Lambda \lambda$. With this, we define the *transfinite recursion* scheme by

$$\mathtt{TR}_\varphi(X, \Lambda) = \forall \lambda \in |\Lambda|\ \forall n\ \big(n \in X \leftrightarrow \varphi(n, X_{<_\Lambda \lambda})\big).$$

Intuitively, $\mathtt{TR}_\varphi(X, \Lambda)$ states that X is made up of "layers" indexed by elements of Λ, and the elements of the λ^{th} layer are those natural numbers n satisfying $\varphi(n, X_{<_\Lambda \lambda})$, where $X_{<_\Lambda \lambda}$ is the union of all previous layers. If Γ is a set of formulas, we denote the Γ-*transfinite recursion* scheme by

$$\Gamma\text{-}\mathtt{TR} = \Big\{\forall \Lambda\big(\mathtt{WO}(\Lambda) \to \exists X\ \mathtt{TR}_\varphi(X, \Lambda)\big) : \varphi \in \Pi^0_\omega\Big\}.$$

Now we are ready to define some important theories:

$$\begin{array}{ll}
\mathrm{ECA}_0: & \mathrm{Q}^+ + \mathtt{Ind} + \Delta^0_0\text{-}\mathtt{CA}; \\
\mathrm{RCA}^*_0: & \mathrm{Q}^+ + \mathtt{Ind} + \Delta^0_1\text{-}\mathtt{CA}; \\
\mathrm{RCA}_0: & \mathrm{Q}^+ + \mathrm{I}\Sigma^0_1 + \Delta^0_1\text{-}\mathtt{CA}; \\
\mathrm{ACA}_0: & \mathrm{Q}^+ + \mathtt{Ind} + \Sigma^0_1\text{-}\mathtt{CA}; \\
\mathrm{ATR}_0: & \mathrm{Q}^+ + \mathtt{Ind} + \Pi^0_\omega\text{-}\mathtt{TR}; \\
\boldsymbol{\Pi}^1_1\text{-}\mathrm{CA}_0: & \mathrm{Q}^+ + \mathtt{Ind} + \Pi^1_1\text{-}\mathtt{CA}.
\end{array}$$

These are listed from weakest to strongest. The theories RCA_0, ACA_0 ATR_0 and $\boldsymbol{\Pi}^1_1$-CA_0, together with the theory of *weak König's lemma,* WKL_0, are the 'Big Five' theories of reverse mathematics, where RCA_0 functions as a 'constructive base theory', and the stronger four theories are all equivalent to many well-known theorems in mathematical analysis. For a detailed treatment of these and other subsystems of second-order arithmetic, see [78].

ECA_0 (the theory of *elementary comprehension*) is the second-order analogue of elementary arithmetic, and is a bit weaker than the more standard RCA^*_0. Meanwhile, *arithmetical comprehension* (ACA_0) is essentially the second-order version of PA, and has the same proof-theoretic ordinal, ε_0. Thus the next milestone in the Π^0_1 ordinal analysis program is naturally ATR_0, the theory of *arithmetical transfinite recursion.* Appropriately, the constructions we will use to interpret the modalities $[\lambda]$ for countable $\lambda > \omega$ may be carried out within ATR_0.

4.7 Iterated ω-rules

If we wish to interpret $[\lambda]_T\,\varphi$ for transfinite λ, we need to consider a notion of provability that naturally extends beyond ω. One such notion, which is well-studied in proof theory (see, e.g., [75]), considers infinitary derivations with the *ω-rule*. Intuitively, this rule has the form

$$\frac{\varphi(\bar{0}) \quad \varphi(\bar{1}) \quad \varphi(\bar{2}) \quad \varphi(\bar{3}) \quad \varphi(\bar{4}) \quad \dots}{\forall x\,\varphi(x)}$$

The parameter λ in $[\lambda]_T\,\varphi$ denotes the nesting depth of ω-rules that may be used for proving φ. The notion of λ-provability is defined as follows:

Definition 4.13. *Let T be a theory of second-order arithmetic and $\varphi \in \Pi^1_\omega$. For an ordinal λ, we define $[\lambda]_T\varphi$ recursively if either*

(i) $\Box_T\varphi$, or

(ii) there are an ordinal $\mu < \lambda$ and a formula $\psi(x)$ such that

(a) for all $n < \omega$, $[\mu]_T\psi(\bar{n})$, and
(b) $\Box_T(\forall x\psi(x) \to \varphi)$.

This notion can be formalized by representing ω-proofs as infinite trees, as presented by Arai [3] and Girard [49]. Here we will instead use the formalization from [44], where Joosten and I showed that this can be formalized in second-order arithmetic for countable λ. To do this, we use a set P as an *iterated provability class*. Its elements are codes of pairs $\langle\lambda,\varphi\rangle$, with λ a code for an ordinal and φ a code for a formula. The idea is that we want P to be a set of pairs $\langle\lambda,\varphi\rangle$ satisfying Definition 4.13 if we set $[\lambda]_T\,\varphi = \langle\lambda,\varphi\rangle \in P$. Thus we may write $[\lambda]_P\varphi$ instead of $\langle\lambda,\varphi\rangle \in P$.

Definition 4.14. *Fix a well-order Λ on $\mathbb{N}$. Say that a set P of natural numbers is an* iterated provability class for Λ *if it satisfies the expression*

$$[\lambda]_P\,\varphi \;\leftrightarrow\; \Big(\Box_T\varphi \vee \exists\,\psi\,\exists\,\xi{<_\Lambda}\lambda\;\big(\forall n\;[\xi]_P\,\psi(\dot{n}) \;\wedge\; \Box_T(\forall x\psi(x)\to\varphi)\big)\Big).$$

Let $\mathtt{IPC}^\Lambda_T(P)$ be a Π^0_ω formula stating that P is an iterated provabiltiy class for Λ. Then, define

$$[\lambda]^\Lambda_T\,\varphi \;:=\; \forall P\,\big(\mathtt{IPC}^\Lambda_T(P) \to [\lambda]_P\varphi\big).$$

Note that $[\lambda]^\Lambda_T$ is a Π^1_1 formula. Alternately, one could define $[\lambda]^\Lambda_T$ as a Σ^1_1 formula, but the two definitions are equivalent due to the following.

Lemma 4.15.

1. *It is provable in* ACA_0 *that if Λ is a countable well-order and P, Q are both iterated provability classes for Λ, then $P = Q$.*
2. *It is provable in* ATR_0 *that if Λ is a countable well-order, then there exists an iterated provability class for Λ.*

The first claim is proven by considering two IPC's P, Q and showing by transfinite induction on λ that $[\lambda]_P \varphi \leftrightarrow [\lambda]_Q \varphi$; this induction is readily available in ACA_0 since the expression $[\lambda]_P \varphi$ is arithmetical. For the second, we simply observe that the construction of an IPC is a special case of arithmetical transfinite recursion. See [44] for more details.

An *arithmetical intepretation* is any function $V \colon \mathbb{P} \to \Pi^1_\omega$ so that $V(p)$ is always a sentence (i.e., contains no free variables). If we fix a computable well-order Λ and a theory T in the language of second-order arithmetic, we can readily extend V to a map $V^\Lambda_T \colon \mathcal{L}_\Lambda \to \Pi^1_\omega$ by letting V^Λ_T commute with all Booleans and setting

$$V^\Lambda_T([\lambda]\varphi) = [\bar{\lambda}]^\Lambda_T V^\Lambda_T(\varphi).$$

In [44], Joosten and I proved the following:

Theorem 4.16 (DFD, Joosten)**.** *Let Λ be a computable well-order and T be a theory extending ACA_0 such that it is provable in T that Λ is well-ordered, and that there is a set P satisfying $\mathtt{IPC}^\Lambda_T(P)$.*

Then, for any $\varphi \in \mathcal{L}_\Lambda$, the following are equivalent:

1. $\mathsf{GLP}_\Lambda \vdash \varphi$*;*
2. *for every arithmetical interpretation V,*

$$T \vdash V^\Lambda_T(\varphi).$$

The computability condition in Λ is included due to the fact that in the proof of Theorem 4.16, we need to be able to prove properties about Λ within T; for example, we need for

$$\forall x \, \forall y \left(x \leq_\Lambda y \to \Box_T(\bar{x} \leq_\Lambda \bar{y}) \right)$$

to hold. However, we can drop this condition if we allow an *oracle* for Λ; or, more generally, for any set of natural numbers. To do this, we add a set-constant O to the language of second-order arithmetic in order to 'feed' information about any set of numbers into T.

To be precise, given a theory T and $A \subseteq \mathbb{N}$, define $T|A$ to be the theory whose rules and axioms are those of T together with all instances of $\bar{n} \in O$ for $n \in A$, and all instances of $\bar{n} \notin O$ for $n \notin A$. Then, for any formula φ, we define

$$[\lambda|A]^\Lambda_T \varphi = [\lambda]^\Lambda_{T|A} \varphi.$$

Its dual, $\langle \lambda|A \rangle^\Lambda_T \varphi$, is defined in the usual way. With this, we obtain an analogue of (1) for ATR_0, proven by Cordón-Franco, Joosten, Lara-Martín and myself in [20]:

Theorem 4.17 (Cordón-Franco, DFD, Joosten, Lara)**.**

$$\mathrm{ATR}_0 \equiv \mathrm{ECA}_0 + \forall \Lambda \, \forall X \, \langle \lambda|X \rangle^\Lambda_{\mathrm{ECA}_0} \top.$$

We have discussed before how the ω-rule can be iterated along a well-order. However, we may also consider full ω-logic based on a theory T; that is, the set of formulas that can be derived using the ω-rule and reasoning in T, regardless of the nesting depth of these ω-rules. Let us write $[\infty]_T\varphi$ if φ is derivable in this fashion. To be precise, we want $[\infty]_T\varphi$ to hold whenever:

(i) $\Box_T\varphi$,

(ii) $\varphi = \forall x \psi(x)$ and for all n, $[\infty]_T\psi(\bar{n})$, or

(iii) there is ψ such that $[\infty]_T\psi$ and $[\infty]_T(\psi \to \varphi)$.

In words, $[\infty]_T$ is closed under T and the ω-rule. This notion may be formalized using ω-trees to represent infinite derivations, as in [3, 49]. We follow a different approach, using a fixed-point construction as in [37].

Definition 4.18. *Fix a theory T, possibly with oracles. Let $\mathtt{SPC}_T(Q)$ be a Π^1_1 formula naturally expressing that Q is the least set such that $\varphi \in Q$ whenever (i) $\Box_T\varphi$ holds, (ii) $\varphi = \forall v\, \psi(v)$ and for all n, $\psi(\bar{n}) \in Q$, or (iii) there exists $\psi \in Q$ such that $\psi \to \varphi \in Q$.*

Then, define

$$[\infty]_T\varphi \;\equiv\; \forall Q\big(\mathtt{SPC}_T(Q) \to \varphi \in Q\big).$$

As before, we may also consider saturated provabiltiy operators with oracles, and we write $[\infty|A]_T\varphi$ instead of $[\infty]_{T|A}\varphi$. This notion of provability allows us to represent $\mathbf{\Pi}^1_1$-CA_0 in terms of a strong consistency assertion, in the spirit of (1). I proved the following in [37]:

Theorem 4.19 (DFD)**.** $\mathbf{\Pi}^1_1$-$\mathrm{CA}_0 \equiv \mathrm{ECA}_0 + \forall X\, \langle\infty|X\rangle_T\top$.

This tells us that Kreisel and Lévy's result for Peano arithmetic readily extends to many natural theories of second-order arithmetic. These results may well be the first step in consistency proofs for theories of second-order arithmetic in the style of Beklemishev.

5 Dynamics of information

As we have seen, modal logics can be used to model dynamics in formal systems. Now we will show how they can also be used to model dynamics in epistemic states, e.g., in the beliefs and knowledge of rational agents, including humans and robots. Central to these dynamics are the notions of learning and forgetting.

5.1 Learning and forgetting

We consider the basic language of epistemic logic $\mathcal{L} = \mathcal{L}_{\mathbb{A}}$, where $\mathbb{A}$ is a non-empty finite set of 'agents'. The language $\mathcal{L}_{\mathbb{A}}$ is a variant of the basic modal language with one modality K_a for each agent, interpreted as 'the agent a knows that'. The language $\mathcal{L}^C_{\mathbb{A}}$ is an extension of $\mathcal{L}_{\mathbb{A}}$ which introduces an operator C_B ('common knowledge') for each $B \subseteq \mathbb{A}$.

We are interested in interpreting L and L^C over *epistemic frames*, which are Kripke frames $(W, (\sim_a)_{a\in\mathbb{A}})$, where each $\sim_a$ is an equivalence relation. As usual, an epistemic frame equipped with a valuation is an *epistemic model,* and semantics are defined as in Definition 2.6.

It is well-known [26, 73] that multimodal $\mathsf{S5}$, given by the axiomatization below, is complete for such interpretations:

Axioms

All propositional tautologies
$K_a(\varphi \to \psi) \ \to \ K_a\varphi \to K_a\psi$;
$K_a\varphi \ \to \ \varphi$
$K_a\varphi \ \to \ K_aK_a\varphi$;
$\neg K_a\varphi \ \to \ K_a\neg K_a\varphi$.

Rules: Modus ponens and Necessitation:

$$\frac{\varphi, \varphi \to \psi}{\psi} \qquad\qquad \frac{\varphi}{K_a\varphi}$$

From an epistemic perspetive, if $(\mathcal{A}, a) \trianglelefteq (\mathcal{B}, b)$ (i.e., $(\mathcal{A}, a)$ is simulated by $(\mathcal{B}, b)$ in the sense of Definition 2.13), we may think that an agent passing from the epistemic state $(\mathcal{B}, b)$ to the epistemic state $(\mathcal{A}, a)$ has gained information, or *learned,* as they now entertain fewer possible states of the world. Conversely, passing from $(\mathcal{A}, a)$ to $(\mathcal{B}, b)$ may be seen as *forgetting.* Thus it is of interest to describe such situations in the context of epistemic logic. In [24], we prove the following variant of Theorem 2.17:

Theorem 5.1 (van Ditmarsch, DFD, van der Hoek)**.** *Let $\mathbb{A}$ be a set of at least two agents. Then:*

1. *Bisimulation to finite epistemic states (i.e., pointed models) is not definable in $\mathcal{L}_{\mathbb{A}}$.*
2. Global *bisimulation to finite epistemic models is definable using model validity in $\mathcal{L}_{\mathbb{A}}$.*

3. Simulation by finite epistemic states is not always definable, even over $\mathcal{L}^C_{\mathbb{A}}$.

Note that van Benthem has already shown that bisimulation to finite epistemic states (i.e., pointed models) is definable in $\mathcal{L}^C_{\mathbb{A}}$ [11]. Later, in [46], we present a general framework which allows agents to forget propositional information. The act of forgetting is modeled in a non-deterministic fashion: for example, if a forgets that $p \wedge q$, this may be because a has forgotten that p, or because a has forgotten that q, leading to two new epistemic scenarios for a.

Nevertheless, the use of Kripke models implicitly assumes that agents are perfectly rational. Next, we see how general neighborhood spaces can be used to weaken this assumption.

5.2 Agents with bounded rationality

Most existing logical theories of epistemic attitudes developed in the area of epistemic logic assume that agents are omniscient, in the sense that: (i) their beliefs are closed under conjunction and implication, *i.e.*, if φ is believed and ψ is believed then $\varphi \wedge \psi$ is believed and if φ is believed and $\varphi \to \psi$ is believed then ψ is believed; (ii) their explicit beliefs are closed under logical consequence (*alias* valid implication), *i.e.*, if φ is believed and φ logically implies ψ, *i.e.*, $\varphi \to \psi$ is valid, then ψ is believed as well; (iii) they believe valid sentences or tautologies; (iv) they have introspection over their beliefs, *i.e.*, if φ is believed then it is believed that φ is believed.

As pointed out in [55, 70], relaxing the assumption of logical omniscience allows for a resource-bounded agent who might fail to draw any connection between φ and its logical consequence ψ and, consequently, who might not believe some valid sentences and who might need time to infer and form new beliefs from her existing knowledge and beliefs.

In order to model such situations, in [12], van Benthem, Pacuit and I define an *evidence space* to be a monotone, non-degenerate neighborhood space $\mathcal{E} = (W, \lessdot)$. We interpret formulas of the language $\mathcal{L}_{\Box\forall}$ in the usual way, but add two relations:

1. A w-**scenario** is a maximal collection $\mathcal{X} \subseteq 2^W$ of neighborhoods of w that has the finite intersection property: for each finite subfamily $\{X_1, \ldots, X_n\} \subseteq \mathcal{X}$ we have that $\bigcap_{i=1}^n X_i \neq \varnothing$. A collection is called a **scenario** if it is a w-scenario for some state w.

   Then, define $w \; B \; v$ if $v \in \bigcap \mathcal{X}$ for some w-scenario $\mathcal{X}$.

2. Define a binary relation $\preccurlyeq$ by $w \preccurlyeq v$ if whenever $u \lessdot X$ are such that $w \in X$, then $v \in X$.

These new relations give us a new structure $\mathcal{E}^{\triangle} = (W, \lessdot, \preccurlyeq, B)$. The basic intuitions are as follows:

- That $w \; B \; v$ indicates that the agent considers v to be maximally likely among all possible worlds.

The idea is that agent in a state w possesses evidence from many possibly contradictory sources. Thus she cannot simultaneously believe all of the evidence she has in case that it is incompatible; instead, she will form her beliefs by putting together as much evidence as possible without obtaining a contradiction. The (non-deterministic) result of putting her evidence together is a scenario, but she only believes the information that holds in *all* scenarios she may form from her evidence.

- That $w \preccurlyeq v$ means that any evidence supporting w also supports v. This means that, given the evidence an agent has access to, v is at least as likely as w. Note that it does not mean that she finds v to be maximally likely, since there may be states even more likely than v.

It is convenient to define some special classes of evidence spaces.

Definition 5.2. *Let $\mathcal{E} = (W, \lessdot)$ be an evidence space, and $\mathcal{E}^{\triangle} = (W, \lessdot, \preccurlyeq, B)$ be its extended evidence structure.*

We say that $\mathcal{E}$ is flat *if B is serial (i.e., for all $w \in W$ there is $v \in W$ such that $w\ B\ v$).*

Let $\mathbf{Ev}$ *be the class of all evidence models,* $\mathbf{Ev}_u$ *the class of all uniform evidence models (as in Definition 2.4),* $\mathbf{Ev}_\flat$ *be the class of all flat evidence models, and* $\mathbf{Ev}_{u\flat}$ *be the class of all flat, uniform evidence models.*

With this, we are ready to define evidence logics.

Definition 5.3. *Let* At *be a fixed set of atomic propositions. Let* $\mathcal{L}^{\preccurlyeq B}_{\Box\forall}$ *be the smallest set of formulas generated by the following grammar*

$$p \mid \neg\varphi \mid \varphi \wedge \psi \mid [B]\varphi \mid \Box\varphi \mid \forall\varphi \mid [\preccurlyeq]\varphi$$

where $p \in \mathbb{P}$.

For $\lambda \subseteq \{u, \flat\}$, we let EL_λ *be the set of valid formulas of* $\mathcal{L}^{\preccurlyeq B}_{\Box\forall}$ *over* $\mathbf{Ev}_\lambda$.

Our main result in [12] is the following:

Theorem 5.4 (van Benthem, DFD, Pacuit)**.** *Each evidence logic* EL_λ *has a natural sound and complete axiomatization and is decidable. Moreover,*

1. $\mathsf{EL}, \mathsf{EL}_\flat$ *and* $\mathsf{EL}_{\flat u}$ *are sound and strongly complete for their class of evidence models,*

2. $\mathsf{EL}_{\flat u}$ *is sound and weakly complete for its class of finite evidence models.*

Nevertheless, since evidence models are monotone, this means that

$$\forall(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$$

is valid, so that agents have a sort of logical omniscience: their knowledge is closed under derivable implication.

In order to remove such omniscience, Balbiani, Lorinin and I consider models of *explicit* vs. *implicit knowledge* [6]; essentially, explicit knowledge is knowledge

that an agent is aware of possessing, and implicit knowledge is that which follows deductively from the agent's knowledge base, but may not be actively entertained at the moment. We then define models of explicit knowledge as follows:

Definition 5.5 (explicit knowledge space)**.** *Fix a set of agents* $\mathbb{A}$*. We define an* explicit knowledge space *to be a structure*

$$(W, (\lessdot_i)_{i\in\mathbb{A}}, (\sim_a)_{a\in\mathbb{A}})$$

where:

1. *for every* $i \in \mathbb{A}$, $\sim_i \subseteq W \times W$ *is an equivalence relation on* W*;*
2. *for every* $i \in \mathbb{A}$, $\lessdot_i \subseteq W \times W$ *is a neighborhood relation such that:*
   (a) *if* $w \lessdot_i X$ *and* $v \in X$ *then* $v \sim_i w$*, and*
   (b) *if* $w \lessdot_i X$ *and* $v \sim_i w$ *then* $v \lessdot_i X$*.*

We define $\mathcal{L}^{BK}_{\mathbb{A}}$ *to be the modal language with one modality* B_i *and one modality* K_i *for each* $i \in \mathbb{A}$*. Formulas of* $\mathcal{L}^{BK}_{\mathbb{A}}$ *are interpreted over explicit knowledge models according to Definition 2.6, with* B_i *interpreted using* $\lessdot_i$ *and* K_i *interpreted using* $\sim_i$*.*

The set of valid formulas for these semantics is denoted DL-S**.*

The intuition is that $B_i\varphi$ holds if the agent i explicitly knows that φ, while $K_i\varphi$ means that φ is deducible from i's knowledge. Then, in [6] we prove the following:

Theorem 5.6 (Balbiani, Lorini, DFD)**.** *The logic* DL-S* *enjoys a strongly complete axiomatization for the class of explicit knowledge models.*

Moreover it has the finite model property, and hence is decidable.

Indeed the axiomatization for DL-S* is fairly standard, except that the K axiom fails for B_i. Instead, it is replaced by the weaker

$$K_i(\varphi \leftrightarrow \psi) \rightarrow (B_i\varphi \leftrightarrow B_i\psi),$$

which means that agents are incapable of distinguishing between logically equivalent statements. Nevertheless, it is not generally the case that $K_i(\varphi \rightarrow \psi) \rightarrow (B_i\varphi \rightarrow B_i\psi)$ holds, meaning that agents' knowledge is not closed under logical consequence.

Thus evidence logics and explicit knowledge logics give us natural frameworks in which to model agents with imperfect evidence, or with bounded reasoning resources, respectively. Such frameworks can be used, for example, to model scenarios in cryptography, where an eavesdropper is assumed to have limited computational capacity. However, in the next section, we will discuss cryptographic protocols that are safe even against intruders without such limitations.

5.3 Applications to secure communication

As we have seen, dynamical systems can be used to model change in information. This has very concrete applications, including information security. In cryptographic systems, two or more agents ('Alice', 'Bob', etc.) must communicate in such a way that a potential eavesdropper ('Eve') is unable to obtain the data being shared. To verify that a cryptographic system is correct, we need to model the messages being sent and Eve's capabilities for processing such messages. Many encryption methods used in practice are based on the difficulty of solving NP problems using conventional computers; on another extreme, we have *unconditionally secure* cryptosystems, where Eve may not obtain the protected data from the messages being sent by Alice and Bob.

In order to share information, Alice and Bob must exchange messages, each of which modifies the state of agents' knowledge. When a larger number of agents is involved, the exchange may require more steps, and we must ensure that at no point does Eve learn sensitive information. By viewing this as a dynamical system, we can employ many of the tools mentioned above to guarantee that such a communication protocol is secure.

One setting where these methods have already been successful uses a deck of cards to model information; namely, the *Russian cards problem* [23]. This is a family of combinatorial puzzles about secure secret-sharing between card players. It is parametrized by a triple of natural numbers (a, b, e), which we call its *size*, and can be stated as follows:

> **The generalized Russian cards problem**
>
> Alice, Bob and Eve each draw a, b and e cards, respectively, from a deck containing a total of $a + b + e$. All players know which cards were in the deck and how many of them the other players drew, but may only see the cards in their own hand.
>
> Alice and Bob want to know exactly which cards the other holds. Meanwhile, they do not want for Eve to learn who holds any card whatsoever, aside of course from her own cards.
>
> However, they may only communicate by making true, clear, public announcements, so that Eve can learn all the information that they exchange.
>
> Can Alice and Bob achieve this?

Many solutions to this problem are known, depending on the specific choice of parameters (a, b, e), called a *size* [2, 79]. A solution takes the form of a *protocol.*

Formally, a *deal* is a partition $\delta = (A, B, E)$ of the deck, such that Alice's hand A has a elements, Bob's hand B has b and Eve's hand E has e. The agents are not able to distinguish between different deals where they hold the same hand. We model this by equivalence relations between deals; since from Alice's perspective, (A, B, E) is indistinguishable from (A, B', E'), we define $(A, B, E) \overset{Alice}{\sim} (A', B', E')$ if and only if $A = A'$. We also define analogous equivalence relations for Bob and Eve.

Definition 5.7 (Protocol)**.** *Fix a formal language $\mathcal{L}$, which for simplicity could be the set of natural numbers. An* announcement *is a pair (i, φ), where i is either Alice or Bob and $\varphi \in \mathcal{L}$.*

A sequence of announcements $\vec{\alpha} = (i_0, \varphi_0), (i_1, \varphi_1), \ldots, (i_n, \varphi_n)$ is a run*. We shall write $\mathrm{Run}_{<N}$ the set of runs of length less than N.*

A protocol of length N *(with (a, b, e) as parameters) is a pair of functions (j, π) assigning to every deal δ and every run $\vec{\alpha} \in \mathrm{Run}_{<N}$ an agent $j(\vec{\alpha}) \in \{Alice, Bob\}$ and a finite, non-empty set $\pi(\delta, \vec{\alpha}) \subseteq \mathcal{L}$ such that if $\delta' \overset{j(\vec{\alpha})}{\sim} \delta$, then $\pi(\delta', \vec{\alpha}) = \pi(\delta, \vec{\alpha})$.*

Thus once a deal has been given, a protocol assigns to each run a player who is to make the next announcement and a set of possible announcements for the player to make; players then choose their announcement randomly. These announcements are determined exclusively by the information an agent has access to, which is assumed to be *only* (*i*) their hand, (*ii*) the parameters a, b, e, (*iii*) the announcements that have been made previously and (*iv*) the protocol π being executed.

Protocols are non-deterministic in principle and hence may be executed in many ways; an *execution of a protocol* is a pair $(\delta, \vec{\alpha})$, where δ is a deal, $\vec{\alpha} = (i_0, \varphi_0), \ldots, (i_n, \varphi_n)$ a run and, for all $k < n$, $i_{k+1} = j\big((i_0, \varphi_0), \ldots, (i_k, \varphi_k)\big)$ and $\varphi_{k+1} \in \pi\big(\delta, (i_0, \varphi_0), \ldots, (i_k, \varphi_k)\big)$.

Now we must define what it means for a protocol to be a solution to the Russian Cards Problem. The first property that must hold is that Alice and Bob know each other's cards (and hence the entire deal) after its execution:

Definition 5.8 (Informativity)**.** *An execution $((A, B, E), \vec{\alpha})$ is informative for Alice if there is no execution $((A, B', E'), \vec{\alpha})$ with $E' \neq E$.*

Similarly, an execution $((A, B, E), \vec{\alpha})$ is informative for Bob if there is no execution $((A', B, E'), \vec{\alpha})$ with $E' \neq E$.

A protocol of length N is informative *if every execution of length N is informative both for Alice and for Bob.*

The second property is that, given k cards $x_1 \ldots x_k$ (possibly with repetitions) which Eve does not hold, she should consider it possible that either Alice holds it or she does not:

Definition 5.9 (k-safety)**.** *Let k be a natural number. An execution $((A, B, E), \vec{\alpha})$ of a protocol (j, π) is* k-safe *if for every $x_1, \ldots, x_k \notin E$ there is*

1. *a deal $\delta' = (A', B', E)$ such that $x_1, \ldots, x_k \in A'$ and $(\delta', \vec{\alpha})$ is also an execution of (j, π), as well as*
2. *a deal $\delta'' = (A'', B'', E)$ such that $x_i \notin A$ for some $i \leq k$ and $(\delta'', \vec{\alpha})$ is also an execution of (j, π).*

The protocol (j, π) is safe if every execution of (j, π) is safe.

We usually write *safe* instead of 1-*safe*. Then, in [19], we proved the following:

Theorem 5.10 (Cordón-Franco, van Ditmarsch, DFD, Soler-Toscano)**.** *Assume that a, b, e, p, d, k are such that p is a prime power, $a = kp^d$, $a + b + e = p^{d+1}$ and*

$$e < kp^d - k^2 p^{d-1}, \tag{6}$$

$$\max\{e + k, ek\} \leq p. \tag{7}$$

Then, there is a k-safe and informative protocol for (a, b, e).

The protocol uses ideas from finite linear algebra; roughly, Alice arranges her cards into a union of k hyperplanes in a finite vector space in order to produce her announcement.

Safety can also be described in probabilistic terms. For this, we need to assign weights to the possible outcomes of a protocol. Say a *weighing function* for a protocol (j, π) is a function w assigning a number $w(\varphi, \delta, \vec{\alpha}) \in (0, 1]$ to each $\varphi \in \pi(\delta, \vec{\alpha})$ such that

$$\sum_{\varphi \in \pi(\delta, \vec{\alpha})} w(\varphi, \delta, \vec{\alpha}) = 1$$

and if $\delta' \overset{j(\vec{\alpha})}{\sim} \delta$ and $\varphi \in \pi(\delta, \vec{\alpha})$, then $w(\varphi, \delta', \vec{\alpha}) = w(\varphi, \delta', \vec{\alpha})$.

We may use weights to define probabilities on sets of runs in the standard way. Safety is then equivalent to the statement that for all E, $x \notin E$ and every execution $\vec{\alpha}$ of the protocol,

$$0 < \mathsf{Pr}(x \in A | E, \vec{\alpha}) < 1$$

(where $\mathsf{Pr}(X|Y)$ denotes conditional probability). This is equivalent to *weak 1-security* as defined by Swanson and Stinson [79], which is not the only notion of security they discuss.

Observe that weak security does not depend on the particular weights we assign to announcements. However, this changes for *perfect security* [79], which demands that Eve does not gain probabilistic information, so that

$$\mathsf{Pr}(x \in A | E, \vec{\alpha}) = \frac{a}{a + b}.$$

Nevertheless, it is shown in [79] that this notion of security is quite restrictive, as it is difficult to provide solutions when Eve holds five or more cards. To this end, my student Esteban Landerreche and I introduced the notion of ε-strong security.

Definition 5.11. *Let $\varepsilon > 0$ and a size (a, b, e). A protocol π is ε-**strongly secure for** (a, b, e) if for every deal δ, every card x not in E, and every announcement $\mathcal{A}$ with $\mathsf{Pr}(\mathcal{A}|E) \neq 0$, we have that*

$$\left| \frac{\mathsf{Pr}(x \in A | E, \mathcal{A})}{\mathsf{Pr}(x \in A | E)} - 1 \right| < \varepsilon. \tag{8}$$

a	b	e	q	α	δ	ρ	**Lower**	**Upper**
8	117	3	2	3	7	$3/8$	0.9968	1.0041
9	231	3	3	2	5	$1/3$	0.9986	1.0357
16	489	7	2	4	9	$7/16$	0.9926	1.0081
25	3,091	9	5	2	5	$9/25$	0.999	1.0482
32	2,001	15	2	5	11	$9/20$	0.9895	1.0109
64	8,105	23	2	6	13	$7/20$	0.9952	1.0048

Figure 6: Choices of parameters (a, b, e) with $b < a^{2+\beta}$ and $e \approx \rho a$ such that there is an informative and at least 0.05-strongly safe protocol for (a, b, e), as in Theorem 5.12. We show the lower and upper bounds for (8).

Essentially, ε-strongly secure protocols are perfectly secure up to a margin of error of ε. Our main results in [68] is as follows:

Theorem 5.12 (Landerreche, DFD)**.** *Let $\varepsilon, \beta > 0$ and $\rho \in (0, 1)$ be rational numbers. Then:*

1. *There are infinitely many values of a such that for any $e < \rho a$ there is $b < a^{2+\beta}$ so that there is an informative and ε-strongly safe strategy for (a, b, e).*
2. *There are infinitely many values of a such that for any $e < a^{\rho}$ there is $b < a^{1+\beta}$ such that there is an informative and ε-strongly safe strategy for (a, b, e).*

We can further extend the Russian cards to a multi-agent setting. The *secure aggregation of distributed information* problem, introduced by Goranko and I [41] considers agents $\mathcal{A}_1, \ldots, \mathcal{A}_n$, each holding a_i cards, who must then inform each other of their hand without Eve, who holds the remaining e cards, to learn the ownership of any card. Solutions to this problem may well lead to applications in e.g. password safeguarding [14], and this model of communication is amenable to analysis using our formal tools. Although there is some exploratory work, many more advances are needed for applications. In [41] we gave a natural generalization of the notions of informativity and safety, obtaining the following:

Theorem 5.13 (DFD, Goranko)**.** *Given m there is N such that for any size $\vec{a} = (a_1, \ldots, a_m, 0)$ (i.e., such that Eve holds no cards) such that*

$$s = \sum_{i=1}^{m} a_i > N$$

and each player holds at least $\frac{1}{2}\sqrt{s/m}$ cards, there is a safe and informative protocol for $\vec{a}$.

The notion of perfect safety also readily extends to the multiagent setting, as I showed in [39], where I showed the following:

$(a, b_1, \ldots, b_m)$	m	q	d
$(18, 4, 5)$	2	3	2
$(54, 13, 14)$	2	3	3
$(162, 40, 41)$	2	3	4
$(486, 121, 122)$	2	3	5

$(a, b_1, \ldots, b_m)$	m	q	d
$(48, 5, 5, 6)$	3	4	2
$(192, 21, 21, 22)$	3	4	3
$(100, 6, 6, 6, 7)$	4	5	2
$(500, 31, 31, 31, 32)$	4	5	3

Figure 7: Some choices of suitable parameters for which perfectly safe solutions exist. Note that there are $m + 1$ agents, as Alice is counted separately.

Theorem 5.14 (DFD). *Given a set $\mathbb{A} = \{\mathcal{A}, \mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of $m+1$ agents, there are infinitely many values of a such that there is an informative and perfectly safe protocol for some size $(a, b_1, \ldots, b_m)$ such that*

$$\{a, b_1, \ldots, b_m\} \subseteq (a, 4m^2 a).$$

6 Perspectives

In my research, I have explored multiple connections between logic and dynamical systems. This has led to the development of numerous tools and techniques designed for applications in automated reasoning, artificial intelligence and other fields. The focus of my future research will be to fine-tune and fully implement said tools so that these applications may be fully realized in the near future.

6.1 Feasible logics for dynamical systems

As we have seen in Theorem 3.6, the set of intuitionistically valid $\mathcal{L}^{\circ F}_{\forall}$ formulas over the class of all dynamical systems is decidable, unlike the classical validities of $\mathcal{L}^{\circ F}_{\Box\forall}$. This suggests that intuitionistic temporal logic is the 'right' tool for automated theorem-proving in dynamical systems, and thus these logics will be the focus of my future research in the field. Moreover, $\mathcal{L}^{\circ F}_{\forall}$ is expressive enough to characterize minimality and Poincaré recurrence, two key properties which sparked interest in dynamic topological logic. This makes intuitionistic temporal logic arguably be the first decidable logic suitable for reasoning about non-trivial asymptotic behavior of dynamical topological systems. Nevertheless, our techniques are model-theoretic and do not yield an axiomatization, raising the following:

Question 6.1. *Is there a natural axiomatization for the set of valid formulas of $\mathcal{L}^{\circ FG}_{\forall}$ and/or its fragments?*

Note also that the decision procedure we have given is not elementary. Nevertheless, there is little reason to assume that this procedure is optimal. Hence, a sharp lower bound on the complexity of intuitionistic temporal logic remains to be found.

Question 6.2. *What is the complexity of the intuitionistic validity problem for* $\mathcal{L}_\forall^{\circ F}$*?*

In case that such a bound is untractable, there are other natural variants of dynamic topological logic which may have lower complexity. One could view the topological semantics of intuitionistic logic as a restriction of the classical semantics to the algebra of open sets. However, this is not the only important topologically-defined algebra: the sub-algebra of regular open (or closed) sets has already been studied in the context of spatial reasoning [25, 71], and Lando has studied dynamic topological logic modulo sets of measure zero [69]. Reduced semantics modulo *meager* sets (i.e., countable unions of nowhere-dense sets) would also be meaningful in the context of dynamical systems. For the definitions and basic properties of these algebras, we refer the reader to a text such as [50].

A separate strategy for finding tractable fragments could be to impose additional syntactical restrictions to $\mathcal{L}_\forall^{\circ F}$, such as limiting the number of embedded implications. Minimality is characterized using only one implication, and Poincaré recurrence uses two, so that such restricted systems might suffice for applications. This strategy has been successfully employed to obtain tractable fragments of the polymodal provability logic GLP [21], which, like DTL, is topologically complete but not Kripke complete [10]. This raises the following:

Question 6.3. *Can tractable and useful variants of* $\mathsf{ITL}^{\mathsf{c}}$ *be obtained by*

(a) using different spatial algebras, or

(b) restricting the syntax to suitable fragments?

Most of the classes of systems we have considered give rise to logics different from $\mathsf{ITL}^{\mathsf{c}}$, as depicted in Figure 4. Only the following questions are left open by this analysis:

Question 6.4. *Do the following inclusions hold:*

(a) $\mathsf{ITL}^{\mathsf{e}} \subseteq \mathsf{ITL}^{\mathsf{r}}$ *or* $\mathsf{ITL}^{\mathsf{e}} \subseteq \mathsf{ITL}^{\mathsf{m}}$*,*

(b) $\mathsf{ITL}^{\mathsf{e}}_F \subseteq \mathsf{ITL}^{\mathbb{R}^n}_F$*?*

Above, the subindex F means that G is not included in the language (otherwise, the inclusion fails). Aside from this, Figure 4 is complete (in the sense that all inclusions are shown), aside from possibly (a), and remains complete if we replace the logics by the respective $\mathcal{L}_\forall^{\circ F}$-fragments, except for possibly (a) or (b). Given that these logics are mostly distinct, it is an interesting open problem whether intuitionistic temporal logics over special classes of systems are more feasible than their classical counterparts. For example, $\mathsf{DTL}^{\mathsf{m}}$ is decidable, unlike the unrestricted DTL: perhaps $\mathsf{ITL}^{\mathsf{m}}$ also has lower complexity than $\mathsf{ITL}^{\mathsf{c}}$? Similarly, it is not known if DTL over Poincaré recurrent systems is decidable, but settling the decidability of intuitionistic temporal logic over this class may be a more accessible problem.

Question 6.5. *Which of the unknown logics of Table 1 are decidable, and what is their complexity?*

Once the theoretical aspects of these logics are well-understood, the next step is to implement them and test them in applications. For this, I will collaborate with researchers in dynamical systems to develop benchmark expressions to be proven or refuted by our automated theorem-provers. With this, we will finally be ready to settle the following:

Question 6.6. *From the above-mentioned variants of* ITL *mentioned avove,*

(a) which are better suited for representing the problems that arise in dynamical systems research, and

(b) which perform more efficiently in solving said problems?

6.2 Calibration of formal systems

Japaridze's stratified modal logic GLP_ω has been successful in proof-theoretic applications, and its extension to GLP_Λ for countable Λ should suffice for analyzing predicative theories of arithmetic (i.e., systems up to ATR_0). However, for more powerful theories, we should consider expressions of the form $[\Omega]\varphi$, where Ω is uncountable. Extensions of GLP_Λ which accommodate uncountable ordinals will be useful for studying theories capable of proving strong fixed point theorems and would give notation systems for large proof-theoretic ordinals [17].

One possible approach for formalizing such modalities stems from generalizing Beklemishev's "brackets" notation from [9]. Here, consistency assertions are generated exclusively from parentheses: '(' and ')'. These may be combined in many ways, interpreted as different reflection principles, and naturally ordered by consistency strength: for example, $(()) > ()() > ()$. The resulting order-type of such expressions is Γ_0.

Theories of proof-theoretic strength beyond Γ_0 are often regarded as *impredicative,* which roughly means that, implicitly or explicitly, they regard the real numbers, $\mathbb{R}$ (or, equivalently, $2^{\mathbb{N}}$) as a complete totality. Ordinal notation systems for such theories are characterized by including representations for uncountable ordinals, including ω_1, denoted Ω, as well as *collapsing functions,* including the collapse $\psi_\Omega\colon \mathsf{Ord} \to \Omega$ which can be used to define countable ordinals in terms of uncountable ones. The prototypical impredicative ordinal is the Bachmann-Howard ordinal, $\psi_\Omega(\varphi^\omega(\Omega+1))$ (using our hyperexponential notation).

The symbol Ω can also be represented proof-theoretically by setting $[\Omega]\varphi$ to be true if φ is derivable in unrestricted ω-logic. We can then extend Beklemishev's brackets notations so that $(\mathfrak{w})$ represents:

(a) $\langle o\mathfrak{w}\rangle$ if $o\mathfrak{w}$ is countable,

(b) $\langle \psi_\Omega o\mathfrak{w}\rangle$ otherwise.

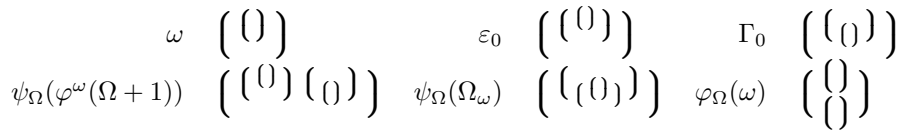

Figure 8: Some ordinals represented as spiders.

The countable reflection principles representable in the extended system would have order-type greater than $\psi_\Omega(\varphi^\omega(\Omega+1))$; to be precise, the first ordinal that we may not represent using this notation system is $\psi_\Omega(\varphi^\Omega(0))$. This idea readily extends to represent even stronger reflection principles, by instead using a hierarchy of parentheses $()_\xi$ with $\xi \leq \omega$, interpreted using higher collapsing functions ψ_{Ω_n} in the style of Buchholz [17]. For this, we would more likely interpret provability logics within the language of set-theory, which allows us to naturally reason about multiple cardinals. This naturally extends to two-layered modalities of the form $\binom{\mathfrak{w}}{\mathfrak{v}}$, where $\mathfrak{w}$ represents the 'height' of a derivation and $\mathfrak{v}$ its 'width', allowing us to represent extremely strong reflection principles as well as very large proof-theoretic ordinals, well beyond the strength of $\mathbf{\Pi}^1_1$-CA$_0$. We call these notations *spiders* [40].

Our extensions of Japaridze's graded modal logics will be used to give alternative representations of strong formal theories that are amenable to a proof-theoretic calibration. As a first milestone, we will pursue an analysis of the theory ATR$_0$ of arithmetical transfinite recursion.

Question 6.7. *What is the provability spectrum of* ATR$_0$ *relative to* EA*?*

This analysis involves three theories: the 'consistency unit', U the 'target theory', T, and the 'base theory', B (over which the meta-theory is developed). In [8], Beklemishev uses first-order Peano Arithmetic as T, Elementary Arithmetic as U and EA$^+$ as B. In Elementary Arithmetic, one may only apply induction to formulas without unbounded quantifiers along with an axiom asserting the totality of the exponential function, and EA$^+$ has an additional axiom asserting he totality of the superexponential. Using the equivalence

$$\mathrm{PA} \equiv \mathrm{EA} + \mathtt{RFN}(\mathrm{EA}),$$

he gives a consistency proof of Peano Arithmetic by induction on worms (which, as mentioned before, are well-ordered). This induction is of order-type ε_0, and thus one obtains a consistency proof of PA which is quite a bit different from Gentzen's classic proof [48]. From this, one may readily compute the provability spectrum of PA relative to EA.

When extending this analysis to a second-order setting, we will always take our finitary base theory B to be PRA or a proper subtheory, such as EA$^+$. At first, we will take ATR$_0$ as our target theory, and as consistency unit ECA$_0$. Analogously to Beklemishev's work, we will make use of Theorem 4.17. However,

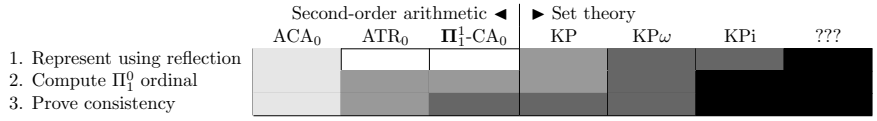

Table 2: The ordinal analysis program is represented in this table. A darker square represents a higher risk, so that tasks corresponding to a white square are previous work, whereas tasks in black are speculative. Note that the table is not meant to be exhaustive; there are many intermediate theories which may be added to the list according to how the project progresses.

despite the similarities to the analysis of Peano Arithmetic, many of the steps required in a semi-finitary consistency proof do not yet have an analogue for treating ATR$_0$. Our approach will be to prove that ATR$_0$ is conservative over a system similar to $\mathrm{ECA}_0 + \{\langle\gamma\rangle_{\mathrm{ECA}_0}\top : \gamma < \Gamma_0\}$, which is more amenable to the form of transfinite induction used by Beklemishev. Using this, we conjecture that $\mathrm{EA}^+ + \mathtt{TI}(\Gamma_0, \Delta^0_0)$ proves the consistency of ATR$_0$.

Question 6.8. *Can the consistency of* ATR$_0$ *be proven using iterated reflection, in the spirit of Beklemishev's consistency proof for* PA*?*

Similarly, our strategy for our analysis of $\mathbf{\Pi}^1_1$-CA$_0$ will be to find large enough Λ so that $\mathbf{\Pi}^1_1$-CA$_0$ is conservative over $\mathrm{ECA}_0 + \{\langle\lambda\rangle_{\mathrm{ECA}_0}\top : \lambda < \Lambda\}$, possibly $\Lambda = \psi_\Omega(\Omega_\omega)$. However, the situation here should be substantially more difficult to deal with than in the predicative case. The Π^1_1 ordinal of $\mathbf{\Pi}^1_1$-CA$_0$ uses a notation system which includes notations for some uncountable ordinals, which must be dealt with in a computable framework. Nevertheless, these ordinals may be represented using spiders, and the reflection principles they give rise to.

The next step is to pass to the language of set theory, to Kripke-Platek set theory and stronger systems. Some of our target theories are the following:

1. Kripke-Platek set theory KP, a weak form of Zermelo-Fraenkel set theory which allows comprehension only for Δ_0 predicates and does not include the powerset axiom.

2. Kripke-Platek set theory with infinity, KPω.

3. Extensions of Kripke-Platek whith axioms asserting the existence of large ordinals, such as KPi, which posits that the universe is computably inaccessible.

My goal is to give an affirmative answer to the following:

Question 6.9. *Are reflection principles suitable for computing provability spectra and proving the consistency of impredicative theories of arithmetic and set-theory?*

6.3 Secure aggretation of distributed information

The *secure aggregation of distributed information* is a generalization of the Russian cards problem. In its general form, it reads as follows:

> *A team of m agents draw $a_1, \ldots, a_m$ cards, respectively, from a deck Ω, while Eve, the eavesdropper, draws the rest of the cards. The agents wish to communicate their hand to each other, without Eve learning any protected information. Can the team achieve this?*

While it is generally accepted that the team wishes for all agents to learn the entire deal (although there are variants of the problem), the safety conditions that must be met vary, both regarding the *qualitative* information that Eve may learn and the *quantitative* certainty with which she may learn it. Regarding the first, we may consider:

(a) *deal-security.* Eve must not know the entire deal after the exchange.

(b) *partial k-card-security.* Given a set of at most k cards held by an agent $\mathcal{A}$, Eve should not learn that $\mathcal{A}$ holds the k cards.

(c) *full k card-security.* Given any set of at most k cards not held by Eve, Eve should consider it possible that any of the other agents holds all of the k cards.

Regarding her level of certainty, we may consider the notions introduced in Section 5.3:

(i) weak security

(ii) ε-strong security

(iii) perfect security.

The ideal goal of the project would be to settle the following question:

Question 6.10. *For each combination of safety conditions as defined above, determine the set of parameters for which a solution to the secure aggregation of distributed information problem exists.*

However, it is possible that a full answer to this problem is unfeasible, and as such we may instead give some partial answers. Specifically, I will focus on those aspects which would make card-based protocols most competitive with respect to alternative methods. Some of the drawbacks of current solutions are the following:

1. The number of cards held by the agents is often heavily biased towards a single agent.

2. The eavesdropper must hold a very small portion of the deck.

3. Methods for perfect security are overly restrictive, relying on the construction of designs.

To this end, I propose to build upon current techniques in order to fill these gaps. The first question I will consider is the following:

Question 6.11. *Is the secure aggregation of distributed information problem solvable in cases where there are more than two communicating agents and the eavesdropper has cards?*

I am currently exploring the answer to this question with my student, Esteban Landerreche. As a first approach we aim to develop partially card-safe methods, to be later improved to obtain ε-strong security. The next question deals with tweaking the set of possible parameters:

Question 6.12. *Is the secure aggregation of distributed information solvable in cases where the agents' hands grow linearly on Eve's?*

Current techniques yield a quadratic blow-up of the deck with respect to Eve's hand. However, current work with van Ditmarsch suggests that this may be greatly improved if we weaken the amount of information that is to be shared among the agents. Note that this question is asymptotic, and refers to infinite families of solvable instances, rather than specific configurations.

If Question 6.12 has a negative answer, a weaker version, also not settled by current methods, is as follows:

Question 6.13. *Are there fully card-safe solutions to the secure aggregation of distributed information problem such that the communicating agents' hands are linearly bounded with respect to each other?*

As before, we clarify that the question is meant to be interpreted asymptotically. Note that the answer is positive if we drop the security condition to weak card safety, as witnessed by Theorem 5.13. However, even in this setting, Eve is assumed to not hold any cards.

Finally, in case that any of these questions have a negative answer, it would also be convenient to have a proof of that. Current techniques are very limited in this respect, as impossibility results are only known with respect to two-step protocols. Thus, we conclude with the following question:

Question 6.14. *Can we find suitable criteria or techniques for establishing that a certain instance of the secure aggregation of distributed information problem is unsolvable, regardless of the number of steps allowed in a protocol?*

6.4 Concluding remarks

My research has been devoted to exploring the relationship between dynamical systems and logic. As it turns out, there is an intricate web of interaction between the two. This has led to a fruitful research career, producing many exciting developments:

1. Computational tools for automated deduction for theorems about dynamical systems.

2. Analytic tools inspired on dynamical systems for the study of logical theories.

3. Efficient conceptual frameworks in which to model changes in knowledge, belief and information.

4. Applications to information-theoretic communication.

Each of these directions has posed many technical challenges, which have led to new techniques in several branches of computer science and mathematics. Nevertheless, it is clear that there are many more questions to answer. In the medium term, I foresee this efforts leading to powerful new tools to understand dynamical systems, logical theories, and changes in information.

References

[1] J. P. Aguilera and D. Fernández-Duque. Strong completeness of provability logic for ordinal spaces. *Journal of Symbolic Logic*, 82(2):608628, 2017.

[2] M. H. Albert, R. E. L. Aldred, M. D. Atkinson, H. van Ditmarsch, and C. C. Handley. Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, 33:33–46, 2005.

[3] T. Arai. Some results on cut-elimination, provable well-orderings, induction and reflection. *Annals of Pure and Applied Logic*, 95(1):93 – 184, 1998.

[4] S.N. Artemov, J.M. Davoren, and A. Nerode. Modal logics and topological semantics for hybrid systems. *Technical Report MSI 97-05*, 1997.

[5] P. Balbiani and D. Fernández-Duque. Axiomatizing the lexicographic products of modal logics with linear temporal logic. In *Advances in Modal Logic*, 2016.

[6] P. Balbiani, D. Fernández-Duque, and E. Lorini. A logical theory of belief dynamics for resource-bounded agents. In *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems, AAMAS 2016, Singapore, May 9-13, 2016*, pages 644–652, 2016.

[7] P. Balbiani, D. Fernández-Duque, and E. Lorini. Exploring the bidimensional space: A dynamic logic point of view. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems, AAMAS 2017, São Paulo, Brazil, May 8-12, 2017*, pages 132–140, 2017.

[8] L. D. Beklemishev. Provability algebras and proof-theoretic ordinals, I. *Annals of Pure and Applied Logic*, 128:103–124, 2004.

[9] L. D. Beklemishev. Veblen hierarchy in the context of provability algebras. In P. Hájek, L. Valdés-Villanueva, and D. Westerståhl, editors, *Logic, Methodology and Philosophy of Science, Proceedings of the Twelfth International Congress*, pages 65–78. Kings College Publications, 2005.

[10] L. D. Beklemishev and D. Gabelaia. Topological completeness of the provability logic GLP. *Annals of Pure and Applied Logic*, 164(12):1201–1223, 2013.

[11] J. van Benthem. Dynamic odds and ends. Technical report, University of Amsterdam, 1998. ILLC Research Report ML-1998-08.

[12] J. van Benthem, D. Fernández-Duque, and E. Pacuit. Evidence and plausibility in neighborhood structures. *Annals of Pure and Applied Logic*, 165(1):106–133, 2014.

[13] G. Bezhanishvili, L. Esakia, and D. Gabelaia. Some results on modal axiomatization and definability for topological spaces. *Studia Logica*, 81(3):325–355, 2005.

[14] G. R. Blakley. Safeguarding Cryptographic Keys. In *Proceedings of the 1979 AFIPS National Computer Conference*, volume 48, pages 313–317, June 1979.

[15] G. S. Boolos. *The Logic of Provability*. Cambridge University Press, Cambridge, 1993.

[16] J. Boudou, M. Diéguez, and D. Fernández-Duque. A decidable intuitionistic temporal logic. *CSL*, 2017.

[17] W. Buchholz. A new system of proof-theoretic ordinal functions. *Annals of Pure and Applied Logic*, 32:195 – 207, 1986.

[18] A. Chagrov and M. Zakharyaschev. *Modal Logic*, volume 35 of *Oxford logic guides*. Oxford University Press, 1997.

[19] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque, and F. Soler-Toscano. A geometric protocol for cryptography with cards. *Designs, Codes and Cryptography*, 74(1):113–125, 2015.

[20] A. Cordón Franco, D. Fernández-Duque, J. J. Joosten, and F. Lara Martín. Predicativity through transfinite reflection. *Journal of Symbolic Logic*, 2017.

[21] E. V. Dashkov. On the positive fragment of the polymodal provability logic glp. *Mathematical Notes*, 91(3-4):318–333, 2012.

[22] A. Dawar and M. Otto. Modal characterisation theorems over special classes of frames. *Annals of Pure and Applied Logic*, 161:1–42, 2009. Extended journal version LICS 2005 paper.

[23] H. van Ditmarsch. The Russian cards problem. *Studia Logica*, 75:31–62, 2003.

[24] H. van Ditmarsch, D. Fernández-Duque, and W. van der Hoek. On the definability of simulation and bisimulation in epistemic logic. *Journal of Logic and Computation*, 24(6):1209–1227, 2014.

[25] I. Düntsch and M. Winter. A representation theorem for boolean contact algebras. *Theoretical Computer Science*, 347(3):498–512, 2005.

[26] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning About Knowledge*. MIT Press, 1995.

[27] S. Feferman. Transfinite recursive progressions of axiomatic theories. *Journal of Symbolic Logic*, 27(3):259–316, 1962.

[28] D. Fernández-Duque. Non-deterministic semantics for dynamic topological logic. *Annals of Pure and Applied Logic*, 157(2-3):110–121, 2009.

[29] D. Fernández-Duque. Absolute completeness of $\mathsf{S4}u$ for its measure-theoretic semantics. In *Advances in Modal Logic*, pages 100–119. College Publications, 2010.

[30] D. Fernández-Duque. Dynamic topological logic interpreted over minimal systems. *Journal of Philosophical Logic*, 40(6):767–804, 2011.

[31] D. Fernández-Duque. On the modal definability of simulability by finite transitive models. *Studia Logica*, 98:347–373, August 2011.

[32] D. Fernández-Duque. Tangled modal logic for spatial reasoning. In T. Walsh, editor, *Proceedings of IJCAI*, pages 857–862, 2011.

[33] D. Fernández-Duque. A sound and complete axiomatization for dynamic topological logic. *Journal of Symbolic Logic*, 77(3):947–969, 2012.

[34] D. Fernández-Duque. Tangled modal logic for topological dynamics. *Annals of Pure and Applied Logic*, 163(4):467–481, 2012.

[35] D. Fernández-Duque. Non-finite axiomatizability of dynamic topological logic. *ACM Transactions on Computational Logic*, 15(1):4, 2014.

[36] D. Fernández-Duque. The polytopologies of transfinite provability logic. *Archive for Mathematical Logic*, 53(3-4):385–431, 2014.

[37] D. Fernández-Duque. Impredicative consistency and reflection. *arXiv*, 1509.04547 [math.LO], 2015.

[38] D. Fernández-Duque. The intuitionistic temporal logic of dynamical systems. *arXiv*, 1611.06929 [math.LO], 2016.

[39] D. Fernández-Duque. Perfectly secure data aggregation via shifted projections. *Information Sciences*, 354:153–164, 2016.

[40] D. Fernández-Duque. Worms and spiders: Reflection calculi and ordinal notation systems. *arXiv*, 1605.08867 [math.LO], 2016.

[41] D. Fernández-Duque and V. Goranko. Secure aggregation of distributed information: How a team of agents can safely share secrets in front of a spy. *Discrete Applied Mathematics*, 198:118–135, 2016.

[42] D. Fernández-Duque and J. J. Joosten. Hyperations, Veblen progressions and transfinite iteration of ordinal functions. *Annals of Pure and Applied Logic*, 164(7-8):785–801, 2013.

[43] D. Fernández-Duque and J. J. Joosten. Models of transfinite provability logics. *Journal of Symbolic Logic*, 78(2):543–561, 2013.

[44] D. Fernández-Duque and J. J. Joosten. The omega-rule interpretation of transfinite provability logic. *arXiv*, 1205.2036 [math.LO], 2013.

[45] D. Fernández-Duque and J. J. Joosten. Well-orders in the transfinite japaridze algebra. *Logic Journal of the IGPL*, 22(6):933–963, 2014.

[46] D. Fernández-Duque, Á. Nepomuceno-Fernández, E. Sarrión-Morillo, F. Soler-Toscano, and F. R. Velázquez-Quesada. Forgetting complex propositions. *Logic Journal of the IGPL*, 23(6):942–965, 2015.

[47] D. Gabelaia, A. Kurucz, F. Wolter, and M. Zakharyaschev. Non-primitive recursive decidability of products of modal logics with expanding domains. *Annals of Pure and Applied Logic*, 142(1-3):245–268, 2006.

[48] G. Gentzen. Die Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische Annalen*, 112:493–565, 1936.

[49] J.-Y. Girard. *Proof theory and logical complexity. Vol. 1.* Studies in proof theory. Bibliopolis, Napoli, 1987.

[50] S. Givant and P. Halmos. *Introduction to Boolean Algebras.* Undergraduate Texts in Mathematics. Springer, New York, 2009.

[51] K. Gödel. Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme, I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[52] R. Goldblatt and I. Hodkinson. The tangled derivative logic of the real line and zero-dimensional spaces. In *Advances in Modal Logic*, 2016.

[53] R. Goldblatt and I. Hodkinson. Spatial logic of tangled closure operators and modal mu-calculus. *Annals of Pure and Applied Logic*, 168(5):1032 – 1090, 2017.

[54] P. Hájek and P. Pudlák. *Metamathematics of First Order Arithmetic.* Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[55] J. Hintikka. Impossible possible worlds vindicated. *Journal of Philosophical Logic*, 4:475–484, 1975.

[56] T. F. Icard III. A topological study of the closed fragment of GLP. *Journal of Logic and Computation*, 21:683–696, 2011.

[57] K. N. Ignatiev. On strong provability predicates and the associated modal logics. *Journal of Symbolic Logic*, 58:249–290, 1993.

[58] G. Japaridze. The polymodal provability logic. In *Intensional logics and logical structure of theories: material from the Fourth Soviet-Finnish Symposium on Logic.* Metsniereba, Telavi, 1988. In Russian.

[59] T. Jech. *Set Theory.* Springer monographs in Mathematics, 2006.

[60] J. J. Joosten. Turing–taylor expansions for arithmetic theories. *Studia Logica*, 104(6):1225–1243, 2016.

[61] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer Monographs in Mathematics. Springer, 2008.

[62] B. Konev, R. Kontchakov, F. Wolter, and M. Zakharyaschev. Dynamic topological logics over spaces with continuous functions. In G. Governatori, I. Hodkinson, and Y. Venema, editors, *Advances in Modal Logic*, volume 6, pages 299–318, London, 2006. College Publications.

[63] B. Konev, R. Kontchakov, F. Wolter, and M. Zakharyaschev. On dynamic topological and metric logics. *Studia Logica*, 84:129–160, 2006.

[64] G. Kreisel and A. Lévy. Reflection principles and their use for establishing the complexity of axiomatic systems. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 14:97–142, 1968.

[65] P. Kremer. A small counterexample in intuitionistic dynamic topological logic, 2004. Unpublished.

[66] P. Kremer. Dynamic topological S5. *Annals of Pure and Applied Logic*, 160:96–116, 2009.

[67] P. Kremer and G. Mints. Dynamic topological logic. *Annals of Pure and Applied Logic*, 131:133–158, 2005.

[68] E. Landerreche and D. Fernández-Duque. A case study in almost-perfect security for unconditionally secure communication. *Designs, Codes and Cryptography*, 83(1):145–168, 2017.

[69] T. Lando. Dynamic measure logic. *Annals of Pure and Applied Logic*, 163(12):1719–1737, 2012.

[70] H. Levesque. A logic of implicit and explicit belief. In *Proceedings of AAAI-84*, pages 198–202. AAAI Press, 1984.

[71] C. Lutz and F. Wolter. Modal logics of topological relations. *Logical Methods in Computer Science*, 2(2), 2006.

[72] J. C. C. McKinsey and A. Tarski. The algebra of topology. *Annals of Mathematics*, 2:141–191, 1944.

[73] J.-J. Ch. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge Tracts in Theoretical Computer Science 41. Cambridge University Press, Cambridge, 1995.

[74] G. Mints. *A Short Introduction to Intuitionistic Logic*. Springer, 2000.

[75] W. Pohlers. *Proof Theory, The First Step into Impredicativity*. Springer-Verlag, Berlin Heidelberg, 2009.

[76] K. Segerberg. An essay in classical modal logic. *Filosofiska Fóreningen och Filosofiska Institutionen vid Uppsala Universitet*, 1971.

[77] V. Shehtman. 'Everywhere' and 'here'. *Journal of Applied Non-Classical Logics*, 9(2-3):369–379, 1999.

[78] S. G. Simpson. *Subsystems of Second Order Arithmetic*. Cambridge University Press, New York, 2009.

[79] C. M. Swanson and D. R. Stinson. Combinatorial solutions providing improved security for the generalized russian cards problem. *Designs, Codes and Cryptography*, 72(2):345–367, 2014.

[80] A. Tarski. Der Aussagenkalkül und die Topologie. *Fundamenta Mathematica*, 31:103–134, 1938.

[81] O. Veblen. Continuous increasing functions of finite and transfinite ordinals. *Transactions of the American Mathematical Society*, 9:280–292, 1908.

[82] P. Walters. *An Introduction to Ergodic Theory*. Springer-Verlag, 1982.

[83] I. Walukiewicz. Completeness of kozen's axiomatisation of the propositional μ-calculus. *Inf. Comput.*, 157(1-2):142–182, February 2000.

A List of publications

Journal publications

Predicativity through transfinite reflection. Joint work with Andrés Cordón-Franco, Francisco Félix Lara and Joost Joosten. Journal of Symbolic Logic, 2017 (accepted for publication).

Strong completeness of provability logic for ordinal spaces. Joint work with Juan Pablo Aguilera. Journal of Symbolic Logic, 2017 (accepted for publication).

A case study in almost-perfect security for unconditionally secure communication. Joint work with Esteban Landerreche. Designs, Codes and Cryptography, 83(1): 145-168, 2017.

Perfectly secure data aggregation via shifted projections. Information Sciences 354: 153-164, 2016.

Secure aggregation of distributed information: How a team of agents can safely share secrets in front of a spy. Joint work with Valentin Goranko. Discrete Applied Mathematics 198: 118-135, 2016.

A geometric protocol for cryptography with cards. Joint work with Andrés Cordón-Franco, Hans van Ditmarsch and Fernando Soler-Toscano. Designs, Codes and Cryptography, 74(1): 113-125, 2015.

Forgetting complex propositions. Joint work with Ángel Nepomuceno-Fernández, Enrique Sarrión-Morrillo, Fernando Soler-Toscano and Fernando R. Velázquez-Quesada. Logic Journal of the IGPL, 23(6): 942-965, 2015.

Well-orders in the transfinite Japaridze algebra. Joint work with Joost Joosten. Logic Journal of the IGPL, 22(6): 933-963, 2014.

The polytopologies of transfinite provability logic. Archive for Mathematical Logic 53(3-4): 385-431, 2014.

Evidence and plausibility in neighborhood structures. Joint work with Johan van Benthem and Eric Pacuit. Annals of Pure and Applied Logic 165 (1), 106-133, 2014.

On the definability of simulability and bisimilarity to finite epistemic models. Joint work with Wiebe van der Hoek and Hans van Ditmarsch. Journal of Logic and Computation 24(6): 1209-1227, 2014.

On provability logics with linearly ordered modalities. Joint work with Lev Beklemishev and Joost Joosten. Studia Logica, 102(3): 541-566, 2014.

Non-finite axiomatizability of Dynamic Topological Logic. ACM Transactions on Computational Logic, 15(1): 4, 2014.

A colouring protocol for the generalized Russian cards problem. Joint work with Andrés Cordón-Franco, Hans van Ditmarsch and Fernando Soler-Toscano. Theoretical Computer Science 495(15), 81–95, 2013.

Hyperations, Veblen progressions, and transfinite iteration of ordinal functions. Joint work with Joost Joosten. Annals of Pure and Applied Logic 164 (7-8), 2013.

Models of Transfinite Provability Logic. Joint work with Joost Joosten. Journal of Symbolic Logic, 78 (2), 543-561, 2013.

Tableaux for structural abduction. Joint work with Ángel Nepomuceno-Fernández and Francisco J. Salguero-Lamillar. Logic Journal of the IGPL 20(2): 388-399, 2012.

A modal framework for modelling abductive reasoning. Joint work with Fernando Soler-Toscano and Ángel Nepomuceno-Fernández. Logic Journal of the IGPL 20(2): 438-444, 2012.

A sound and complete axiomatization for Dynamic Topological Logic. Journal of Symbolic Logic, 77(3), pp. 947-969, 2012.

Tangled modal logic for topological dynamics. Annals of Pure and Applied Logic 163, 467–481, 2012.

Dynamic Topological Logic of metric spaces. Journal of Symbolic Logic 77(1): 308-328, 2012.

A secure additive protocol for card players. Joint work with Andrés Cordón-Franco, Hans van Ditmarsch, Joost J. Joosten and Fernando Soler-Toscano. Australasian Journal of Combinatorics, 54: 163-176, 2012.

On the modal definability of simulability by finite transitive models. Studia Logica, 98(3), Pages 347-373, 2011.

Dynamic Topological Logic interpreted over Minimal Systems. Journal of Philosophical Logic, 40(6), 767–804, 2011.

Non-deterministic semantics for Dynamic Topological Logic. Annals of Pure and Applied Logic, 157, 110–121, 2009.

Dynamic Topological Logic for $\mathbb{R}^2$. Logic Journal of the IGPL, 15, 77–107, 2007.

A polynomial translation of S4 *into Intuitionistic Logic.* Journal of Symbolic Logic, 71, 989–1001, 2006.

Publications in conference proceedings

A decidable intuitionistic temporal logic. Joint work with Joseph Boudou and Martín Diéguez. CSL, 2017.

Bisimulations for intuitionistic temporal logics. Joint work with Philippe Balbiani, Joseph Boudou, and Martín Diéguez. Intuitionistic Modal Logic and Applications, 2017.

Exploring the bidimensional space: A dynamic logic point of view. Joint work with Philippe Balbiani and Emiliano Lorini. AAMAS, 2017.

Verification logic: An arithmetical interpretation of negative introspection. Joint work with Juan Pablo Aguilera. Advances in Modal Logic, 2016.

Axiomatizing the lexicographic products of modal logics with LTL. Joint work with Philippe Balbiani. Advances in Modal Logic, 2016.

A Logical Theory of Belief Dynamics for Resource-Bounded Agents. Joint work with Philippe Balbiani and Emiliano Lorini. AAMAS, 644-652, 2016.

Non-finite axiomatizability of Dynamic Topological Logic. Advances in Modal Logic, 2012.

Kripke models of Transfinite Provability Logic, Advances in Modal Logic, 2012.

Axiomatizing evidence logic: a new look at neighborhood structures. Joint work with Johan van Benthem and Eric Pacuit. Advances in Modal Logic, 2012.

Turing progressions and their well-orders. Joint work with Joost Joosten. Computability in Europe, 2012.

On the definability of simulability and bisimilarity to finite epistemic models. Joint work with Wiebe van der Hoek and Hans van Ditmarsch. Computational Logic in Multi-Agent Systems, 2011.

Secure communication of local states in multi-agent systems. Joint with Michael Albert, Andres Cordón-Franco, Hans van Ditmarsch, Joost J Joosten and Fernando Soler-Toscano. Proceedings of the International Symposium on Distributed Computing and Artificial Intelligence, Pages 1–19, 2011.

Tangled modal logic for spatial reasoning. Proceedings of the 22nd Joint Conference on Artificial Intelligence, 2011.

Two mischievous dynamic consequence relations. Joint work with Andrés Cordon-Franco, Hans van Ditmarsch, David Fernández-Duque, Emilio Gómez-Caminero, and Ángel Nepomuceno-Fernández. Proceedings of the International Workshop on Logic and Philosophy of Knowledge, Communication and Action, pp.197-208, 2010.

Absolute completeness of $\mathsf{S4}_u$ *for its measure-theoretic semantics.* Advances in Modal Logic 8, 100–119, 2010.

Edited volume

Proceedings for the 7th Methods for Modalities workshop, with H. P. van Ditmarsch, V. Goranko, W. Jamroga and M. Ojeda-Aciego, Electronic Notes in Theoretical Computer Science 278: 1-2, 2011.

Popular articles

Turing y Gödel en el monte de Sísifo, Miscelánea Matemática 56, 55-76, 2013.

Dimensiones desconocidas, Laberintos e Infinitos 28: 37-44, 2012.