

# DRAFT

## Legal Abstract State Machines, L4, and Formal Verification of Contracts

Report on Computational Law Research by [Legalese](#)\*

April 18, 2018

### Abstract

This report is intended for industry and academics in Computational Law. However, by publication time it should be readable by anyone with an undergraduate level background in computer science or mathematics. We recommend joining [the #dsl channel](#) on [our Slack workspace](#)<sup>1</sup> and introducing yourself if you're planning on spending more than half an hour with this document.

The primary focus of this report is the definition of the programming language-independent mathematical model for computational legal contracts that we've settled on after a comprehensive review of the literature and many months of research. The model, tentatively called *Legal Abstract State Machines* (LASMs), provides the formal semantics for our prototype open source computational legal contracts DSL L4, but it is intended to be a *necessary substructure of the semantics of any computational legal contracts language that is worth a damn* (and we eagerly invite disputes).<sup>2</sup> In programming language theory jargon, LASMs are a denotational semantics.

---

\*Contact: [dustin.wehr@gmail.com](mailto:dustin.wehr@gmail.com) or [collective@legalese.com](mailto:collective@legalese.com)

<sup>1</sup><https://legalese.slack.com>

<sup>2</sup>L4's typesystem (Section 7.1), though we are quite proud of it, is an example of a feature that does not meet this high standard. It is plausible that the complication it introduces, when in the presence of other optional language features that L4 does not have, makes its inclusion unjustified. In fact, it would be hard to add L4's typesystem to the definition of LASMs, as LASMs do not even have a term language!

# DRAFT

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Time, Actors, and Events</b>	<b>3</b>
<b>3</b>	<b>Legal Abstract State Machines</b>	<b>5</b>
<b>4</b>	<b>Formal Verification for <b>LASM</b></b>	<b>8</b>
4.1	Satisfiability Modulo Theories (SMT) Technology . . . . .	8
4.2	Symbolic Execution . . . . .	8
<b>5</b>	<b>MiniL4 - A Minimal <b>LASM</b>-Compatible DSL</b>	<b>9</b>
<b>6</b>	<b>Formal Verification for <b>MiniL4</b></b>	<b>9</b>
6.1	Symbolic Execution . . . . .	9
6.2	Exhaustive Model Checking for finite or tamely-infinite state spaces . . . . .	9
6.3	Unbounded-Trace Formal Verification with Pre/Postconditions and Invariants . . . . .	10
6.4	Unexplored: Hard Unbounded-Trace Formal Verification with Interactive Theorem Proving . . . . .	10
<b>7</b>	<b>L4: Experimental-But-Practical <b>LASM</b> DSL</b>	<b>10</b>
7.1	Type Checking with Subtyping and Intersection Types . . . . .	10
<b>8</b>	<b>Related Work</b>	<b>10</b>

## 1 Introduction

We expect the Computational Law community will develop a number of independent, open source, computational contract DSLs, to suit different tastes and focuses, but we hope that the bulk of the work done by the community will be effectively reusable, particularly in statute and contract libraries, formal verification, and visualization. For this reason, not only have we made our DSL L4 completely free and open source, we have also ensured that none of our work on formal verification of contracts depends strongly on L4 - only

# DRAFT

on the much simpler mathematical model of Legal Abstract State Machines that one can use L4 (or your own DSL!) to construct.

Sections 2 and 3 define Legal Abstract State Machines. Section ?? documents our progress on static analysis for LASMs.

Hovering over (resp. clicking on) most terms in `sf font` should show you a popup of (resp. take you to) where the term is defined, where the term is styled like [this](#). This might not work in all PDF viewers.

## 2 Time, Actors, and Events

We will always be working with a fixed minimal [timeunit](#), which will be one of days, hours, minutes, seconds, etc. It is a parameter of Legal Abstract State Machines (LASMs), and should be set to the smallest unit of time that one writes constraints about, or does arithmetic with, in the text of the legal contract one is modelling. A [timestamp](#) is just a nonnegative real number<sup>3</sup> that we *think of* as being in units `timeunit`, which marks the time since the designated start of the LASM execution, which is always 0 by definition. It is worth emphasizing that timestamps are distinct from both `DateTimes` (some standard for calendar dates with optional within-day times) and `TimeDeltas` (i.e. durations), both of which are important datatypes in DSLs such as L4. We have found that there is no advantage, and significant disadvantage (when it comes to formal verification), to having `DateTimes` or `TimeDeltas` in the mathematical model.

Fix a set  $\mathbb{D}$  of basic datatypes, which includes at least `Bool`,  $\mathbb{Z}$ , and  $\mathbb{R}$ . These datatypes should be definable types of SMT-LIB. It is important to note that SMT-LIB itself allows for rich datatypes, including recursive datatypes, but also that a computational contracts DSL such as L4 or Ergo can include types beyond those easily definable in SMT-LIB (see Section 7.1).

Fix a finite set of symbols [actor](#), which includes:

- The parties to the contract.
- Any “oracles” that send information to the contract from the environment.
- The special symbol [Code](#), for events that are initiated by the code of the contract.

---

<sup>3</sup>See a few paragraph below for why it is  $\mathbb{R}$  and not  $\mathbb{N}$ .

# DRAFT

Before publication of this document, we will likely replace the finite set of party-actors with a finite set of *roles*, and allow for an unbounded number of party-actors in each role; that seems to be necessary to model many blockchain smart contracts in a natural way.

Fix a finite set of symbols [event](#), and for each such  $e$  a parameter type assignment  $\text{param-types}_e \in \mathbb{D}^*$ . Furthermore, partition **event** into three kinds of events:

- party-events, which are actions done by a party-to-the-contract,
- oracle events, which provide information from the environment, and
- deadline events, which are transitions mandated by the contract.

An [event instance](#) is a tuple  $\langle e, a, t, \sigma \rangle$  where  $e$  is an **event**,  $a$  is an **actor**,  $t$  is a **timestamp**, and  $\sigma \in \text{param-types}_e$ . The **actor** for a deadline **event** is always **Code**.

Event instances are instantaneous,<sup>4</sup> occurring at a particular **timestamp**; a real world event with duration is modelled by two such instantaneous **event-instances**, for the start and end of the real world event. That convention is quite flexible; it easily allows modelling overlapping real-world events, for example. We will see in the next section that a sequence of **event-instances** that constitutes a valid execution of an **LASM** requires strictly increasing time stamps. For example, if the **timeunit** is days, then three real-world events that happen in some sequence on the second day would happen at **timestamps**  $1, 1 + \epsilon_1, 1 + \epsilon_1 + \epsilon_2$ , for some  $\epsilon_1, \epsilon_2 > 0$ . When we need to model two real-world events as truly-simultaneous, we use one event instance to model their cooccurrence ([todo: example](#)).

For our intended domain of legal contracts, we are not aware of any cogent criticism of requiring instantaneous event instances with strictly increasing timestamps; and **we welcome attempts**. An earlier version of the model, in fact, did not require that timestamps are *strictly* increasing, used discrete time, and had what we believe was a very satisfying<sup>5</sup> justification. However, the justification requires at least another paragraph, and probably several more to adequately defend it. Meanwhile, it offered no advantages in examples, and had one clear disadvantage for formal verification, where the use of integer variables is costly for SMT solvers.<sup>6</sup>

---

<sup>4</sup>We might relax this before publication, after discussion with others in the Computational Law community.

<sup>5</sup>Or “elegant”, as unscrupulous researchers put it.

<sup>6</sup>The best explanation we have for this is not simple. It starts with noting that real

## 3 Legal Abstract State Machines

A Legal Abstract State Machine (LASM) first of all fixes the definitions of the terms introduced in Section 2: `timeunit`,  $\mathbb{D}$ , `actor`, and `event`. It also includes a finite set of symbols `situation` that must contain at least the symbols:

- fulfilled
- `breachedX` for each nonempty subset  $X$  of `actor` \ `{Code}`.<sup>7</sup>

An LASM  $M$  also has an ordered finite set of symbols `statevars`, and an assignment `statevar-domains` of a datatype from  $\mathbb{D}$  to each. Since the `statevars` are ordered, we can take `statevar-domains` to be an element of  $\mathbb{D}^*$ .  $M$  also includes an initial setting `initvals` of its `statevars`.

The `state space` of  $M$  is the product set

$$\text{situation} \times \text{statevar-domains} \times \text{timestamp}$$

and a `state` is an element of the `state space`.

The remainder and bulk of the definition of an LASM is a mapping from `situation` to *situation handlers*, and a mapping from `event` to *event handlers*. An `event-handler` for event  $e$  consists of:

- a destination `situation`.
- a function `statetransforme` of type

$$\text{timestamp}^2 \times \text{statevar-domains} \times \text{param-types}_e \rightarrow \text{statevar-domains}$$

where the two `timestamp` arguments provided to `statetransforme` will always be the `timestamps` of the previous and next `event-instances`.

A `situation-handler` is a finite set of *event rules*, where an `event-rule` is one of three types: a *party rule*, *oracle rule*, or *deadline rule*. Every `event-rule` governs the applicability of a unique `event` by a unique `actor`.<sup>8</sup> Every `event-rule`

---

arithmetic is decidable (real closed fields), but even quantifier free integer arithmetic is undecidable (diophantine equations). This does not necessarily mean that simple uses of integer variables will be costly, but in practice, as of April 2018, it seems to, at least to us outsiders. We are not aware of any particularly-useful decidable restriction of quantifier free combined real/integer arithmetic, and the currently-implemented heuristics, at least in Z3, are easily fooled.

<sup>7</sup>These are breaches and oracle errors analogous to undifferentiated unhandled exceptions in software. Some well-drafted computational contracts might avoid using them completely.

<sup>8</sup>In L4, we offer syntax for concisely expressing a set of such rules that apply to different elements of `event` and `actor`.

# DRAFT

$r$  has a relation enabled-guard <sub>$r$</sub>  on

$$\text{timestamp} \times \text{statevar-domains}$$

where the **timestamp** argument is the **timestamp** of the previous **event-instance**. Frequently in our examples, **enabled-guard <sub>$r$</sub>**  is just the trivial relation **true**.  $r$  is **enabled** upon entering its parent situation at the **timestamp**  $t$  of the previous **event-instance** iff **enabled-guard <sub>$r$</sub>**  is true when evaluated at  $t$  and the current statevar assignment.

A deadline event rule  $r$  governing the applicability of a deadline event  $e$  has an additional *deadline function* deadline <sub>$r$</sub>  of type

$$\text{timestamp} \times \text{statevar-domains} \rightarrow \text{timestamp}$$

where the **timestamp** argument is the **timestamp** of the previous **event-instance**.  $r$  also has a *parameter setter* params <sub>$r$</sub>  of type

$$\text{timestamp}^2 \times \text{statevar-domains} \rightarrow \text{param-types}_e$$

where the two **timestamp** arguments are the **timestamps** of the previous and next **event-instances**.

Since deadline **event-rules** cause an event to occur automatically when the rule activates, we would need to either specify what happens when two such rules activate at the same time, or else ensure that can't happen. We take the latter approach.<sup>9</sup> For now, we adopt a constraint that is stronger than necessary but especially simple:<sup>10</sup>

unambiguous default condition: if a situation has multiple **event-rules**, their **enabled-guards** must be disjoint relations.

Each party and oracle event rule  $r$  governing the applicability of a party or oracle event  $e$  has an additional *parameter constraint relation* param-constraint <sub>$r$</sub>  on

$$\text{timestamp}^2 \times \text{statevar-domains} \times \text{param-types}_e$$

---

<sup>9</sup>Because we see no natural way to pick one over the other. Note that the **event-rules** are not ordered.

<sup>10</sup>A closer-to-minimal constraint is: when the **enabled-guards** of two deadline **event-rules** are simultaneously true, their **deadline functions** cannot yield the same **timestamp** (and then the earlier of the two deadlines is used). We have not yet experienced any desire for the extra leniency, but in case we do, it would be easy to allow it.

where the two **timestamp** arguments are the **timestamps** of the previous and next **event-instances**. Note that a *parameter setter* is a special case of a *parameter constraint relation*. Because that special case is used fairly frequently, in L4 we allow party and oracle event rules to use the *parameter setter* syntax of deadline event rules instead of their own *parameter constraint relation* syntax.

That completes the definition of a Legal Abstract State Machine.

We now define the *well-formed event sequences* of an LASM  $M$ , which are a superset of the *traces* of  $M$  defined next.

**Definition 1** (event-rule compatible with event-instance). An event-rule  $r$  is compatible with an event-instance  $\langle e, a, t, \sigma \rangle$  iff  $e$  and  $a$  are the event and actor that  $r$  governs the applicability of.

**Definition 2** (well-formed event sequence). Fix an LASM  $M$ .

A well-formed event sequence of  $M$  is a sequence of event-instances  $E_0, E_1, \dots$  with strictly-increasing timestamps such that, if  $\langle e_i, a_i, t_i, \sigma_i \rangle$  is  $E_i$ , then

- The start-situation  $s_0$  of  $M$  has an event-rule compatible with  $E_0$
- Either the destination situation  $s_{i+1}$  of  $e_i$  has an event-rule compatible with  $E_{i+1}$ , or else  $E_i$  is the final element of the sequence and  $s_i$  is fulfilled or  $\text{breached}_X$  for some  $X \subseteq \text{actor}$ .

## Execution of LASMs

Let  $\tau = E_1, E_2, \dots$  be a (finite or infinite) well-formed event sequence of  $M$ . The starting state  $G_0$  is always  $\langle \text{start-situation}, 0, \text{initvals} \rangle$ . Let  $i \geq 0$  be arbitrary. Assume the sequence is a valid trace up to entering  $G_i = \langle s, t, \pi \rangle$ . Let  $E_i$  be  $\langle e, a, t', \sigma \rangle$ . We now define the valid values of  $G_{i+1} = \langle s', t', \pi' \rangle$ :

- If  $E_i$  is a party (resp. oracle) event, then it must be compatible with some party (resp. oracle) event-rule  $r$  of  $s$  that is enabled in  $G_i$  such that  $\text{param-constraint}_r$  is true at  $\langle t, t', \pi, \sigma \rangle$ .
- If  $E_i$  is a deadline event, then it must be compatible with the unique<sup>11</sup> deadline event-rule  $r$  of  $s$  that is enabled in  $G_i$  such that  $\text{deadline}_r(t, \pi) = t'$ .
- $\pi' = \text{statetransform}_e(t, t', \pi, \sigma)$ .

Any well-formed event sequence where  $G_i, E_i$  satisfy the above requirements for all  $i$  is a valid trace for  $M$ .

---

<sup>11</sup>by the unambiguous default condition

## 4 Formal Verification for LASM

### 4.1 Satisfiability Modulo Theories (SMT) Technology

Familiarity with SMT is not a prerequisite for this document, but if you are unfamiliar and interested, Microsoft’s [Z3 tutorial](#) is a fine place to start.

### 4.2 Symbolic Execution

In model checking for expressive models (say, with at least nonlinear integer arithmetic available), usually<sup>12</sup> an infinite-state model is approximated by a finite or tamely-infinite state model, and correctness properties of the approximation model are checked exhaustively, or exhaustively up to a certain maximum computation path length. In Section 6.2 we will consider some cases where approximation is not necessary.

Symbolic execution is a technique for avoiding some of the approximation, especially for avoiding having to approximate unbounded datatypes with bounded ones (e.g.  $\mathbb{R}$  approximated by `float`). We do not do this for the sake of more accurate/faithful correctness theorems. Indeed, most of the time software is executed with bounded numeric datatypes anyway, and even when not, no fixed computer can actually compute with arbitrarily large numbers. Rather, we use symbolic execution because, if there is not actually complex math going on (e.g. any cryptographic functions) in a program, but only the use of functions that puts us outside decidable theories, then we should be able to save a lot of time by analyzing computation paths in axiomatically-defined batches.

When we symbolically execute an LASM, we have a choice about whether to use some, all, or none of the machine’s `initvals` of its `statevars`. Generally, the more of them used, the faster `state space` exploration will be. For example, in a loan agreement, we could treat an interest rate as an arbitrary element of  $(0, 1)$ . We would then be proving correctness of the agreement for interest rates that we’ll never use, which of course is perfectly fine if the analysis finishes in a reasonable amount of time. Alternatively, we could use fixed values of the interest rate only, and whenever we use a fixed interest rate for the first time, we simply rerun symbolic execution.

---

<sup>12</sup>The term “model checking” is used rather inconsistently.



## 5 MiniL4 - A Minimal LASM-Compatible DSL

In Section 4, we gave as much detail as we could about our formal verification progress for LASMs. To go further, we need a complete language, which LASM is not. In particular, we specified that certain components are mathematical *functions* or *relations*, rather than expressions that define such functions or relations. Those components are:

- $\text{statetransform}_e : \text{timestamp}^2 \times \text{statevar-domains} \times \text{param-types}_e \rightarrow \text{statevar-domains}$  for each event  $e$ .
- $\text{enabled-guard}_r \subseteq \text{timestamp} \times \text{statevar-domains}$  for each deadline event-rule  $r$ .
- $\text{params}_r : \text{timestamp}^2 \times \text{statevar-domains} \rightarrow \text{param-types}_e$  for each deadline event-rule  $r$  that governs an event  $e$ .
- $\text{param-constraint}_r \subseteq \text{timestamp}^2 \times \text{statevar-domains} \times \text{param-types}_e$  for each party or oracle event-rule  $r$  that governs an event  $e$ .

## 6 Formal Verification for MiniL4

### 6.1 Symbolic Execution

### 6.2 Exhaustive Model Checking for finite or tamely-infinite state spaces

Suppose the only statevars in an LASM  $M$  are boolean, and suppose that for every event-rule  $r$  none of  $\text{enabled-guard}_r$ ,  $\text{enabled-guard}_r$ ,  $\text{deadline}_r$ , or  $\text{param-constraint}_r$  depend on their **timestamp** arguments. Then  $M$  is equivalent for formal verification purposes to a kind of compressed<sup>13</sup> deterministic finite state machine (FSM). If there are no **statevars**, then  $M$  is equivalent for formal verification purposes to a normal FSM. Many important properties about FSMs are decidable. If the specification of such a model  $M$  is given entirely in terms of a **state space** invariant, then full formal verification can be checked exhaustively by well-known methods.

We may relax the constraint on the functions/predicates that take **timestamp** arguments somewhat, which results in a computation model similar to [Timed Automata](#) with a single clock (but we have not yet mapped the correspondence carefully!).

---

<sup>13</sup>via the boolean statevars

# DRAFT

- 6.3 Unbounded-Trace Formal Verification with Pre/Postconditions and Invariants
- 6.4 Unexplored: Hard Unbounded-Trace Formal Verification with Interactive Theorem Proving
- 7 L4: Experimental-But-Practical **LASM** DSL
  - 7.1 Type Checking with Subtyping and Intersection Types
- 8 Related Work

This is thoroughly covered by [Meng's book chapter](#) and Appendix B of the [CodeX whitepaper](#) *Developing a Legal Specification Protocol: Technological Considerations and Requirements*.