Formulog: Datalog for SMT-based Static Analysis

AARON BEMBENEK, Harvard University, USA
MICHAEL GREENBERG*, Pomona College, USA
STEPHEN CHONG, Harvard University, USA

' Satisfiability modulo theories (SMT) solving has become a critical part of many static analyses, including symbolic execution, refinement type checking, and model checking. We propose Formulog, a domain-specific language that makes it possible to write a range of SMT-based static analyses in a way that is both close to their formal specifications and amenable to high-level optimizations and efficient evaluation.
Formulog extends the logic programming language Datalog with a first-order functional language and mechanisms for representing and reasoning about SMT formulas; a novel type system supports the construction of expressive formulas, while ensuring that neither normal evaluation nor SMT solving goes wrong. Our case studies demonstrate that a range of SMT-based analyses can naturally and concisely be encoded in Formulog, and that — thanks to this encoding — high-level Datalog-style optimizations can be automatically and advantageously applied to these analyses.

Additional Key Words and Phrases: Datalog, SMT, static analysis, refinement type systems, symbolic execution

1 INTRODUCTION

Satisfiability modulo theories (SMT) solving provides a way to reason logically about common program constructs such as arrays and bit vectors, and as such has become a key component of many static analyses. For example, symbolic execution tools use SMT solving to prune infeasible execution paths [Cadar et al. 2008; Cadar and Sen 2013]; type checkers use it to prove subtyping relations between refinement types [Bierman et al. 2012; Rondon et al. 2008]; and model checkers use it to abstract program states [Cimatti and Griggio 2012; McMillan 2006]. This paper presents Formulog, a domain-specific language for writing SMT-based static analyses. Formulog makes it possible to concisely encode a range of SMT-based static analyses in a way that is close to their formal specifications. Furthermore, Formulog is designed so that analyses implemented in it are amenable to efficient evaluation and powerful, high-level optimizations, including parallelization and automatic transformation of exhaustive analyses into goal-directed ones.

Formulog is based on Datalog, a logic programming language used to implement static analyses ranging from points-to analyses [Bravenboer and Smaragdakis 2009; Whaley and Lam 2004] to decompilers [Flores-Montoya and Schulte 2019; Grech et al. 2019] to security analyses [Grech et al. 2018; Guarnieri and Livshits 2009; Jordan et al. 2016; Livshits and Lam 2005; Tsankov et al. 2018]. Embodying the principle of separating the logic of a computation from the control necessary to perform that computation [Kowalski 1979], Datalog frees analysis designers from low-level implementation details and enables them to program at the level of specifications (such as formal inference rules). This leads to concise implementations [Whaley et al. 2005] that can be easier to reason about and improve at the algorithmic level compared to analyses in more traditional languages [Smaragdakis and Bravenboer 2011]. Datalog-based analyses can be fast and scalable, even outperforming the non-Datalog state-of-the-art [Bravenboer and Smaragdakis 2009]. Indeed, Datalog's high-level

*Work done while on sabbatical at Harvard University.

Authors' addresses: Aaron Bembenek, Harvard University, USA, bembenek@g.harvard.edu; Michael Greenberg, Pomona College, USA, michael@cs.pomona.edu; Stephen Chong, Harvard University, USA, chong@seas.harvard.edu.

nature makes it amenable to high-level optimizations, such as parallelization [Scholz et al. 2016] and synthesis of goal-directed analyses from exhaustive ones [Reps 1995].

However, despite the appeal of Datalog for static analysis and the importance of SMT solving in static analysis, until now there has not been a focused study of how to effectively extend the benefits of Datalog to SMT-based analyses; our work bridges this gap.

Formulog augments Datalog with an interface to an external SMT solver and a first-order fragment of the functional language ML. It provides a library of constructors for building terms that are interpreted as logical formulas when applied to special SMT operators; in the backend, these operators are implemented by calls to an external SMT solver. A Formulog program is essentially a set of ML-style function definitions and Datalog-style rules; both pieces can refer to each other and invoke the SMT operators. As in Datalog, the goal of Formulog evaluation is to compute all possible inferences with respect to the rules, which correspond to logical implications. Unlike Datalog, rule evaluation might involve both ML evaluation and calls to an SMT solver.

The way this design combines Datalog, ML, and SMT solving gives Formulog some desirable properties. First, Formulog programs can use SMT solving the way it is used in SMT-based analyses. This results from the choice to represent SMT formulas as ML terms, and contrasts with the approach of most prior work combining logic programming and constraint solving (where, e.g., checking for formula validity is hard). Second, the combination of Datalog-style rules and ML-style functions mirrors the combination of inference rules and helper functions commonly used in analysis specifications, making it easier to translate formal analysis specifications into executable code. This close correspondence between specification and implementation means that specification-level reasoning is still applicable to analysis implementations (and vice versa: unexpected behavior in Formulog programs has revealed bugs in specifications). Third, because Formulog is based on Datalog, analyses written in it can be effectively optimized and evaluated via powerful Datalog algorithms, making them competitive with analyses written in more mature languages.

It takes care to fit Datalog, ML, and SMT solving together in a way that truly achieves these properties. Along these lines, part of our technical contribution is a novel bimodal type system that treats terms appearing in SMT formulas more liberally than terms appearing outside of formulas, making it possible to construct expressive logical formulas, while still ensuring that neither concrete (i.e., Datalog/ML) evaluation nor SMT solving goes wrong.

To test the practicality of Formulog, we implemented a fully-featured, prototype Formulog runtime and wrote three substantial SMT-based analyses in Formulog: a type checker for a refinement type system, a bottom-up points-to analysis for JVM bytecode, and a bounded symbolic evaluator for a subset of LLVM bitcode. Our implementations for the first two case studies are almost direct translations of previously published formal specifications [Bierman et al. 2012; Feng et al. 2015]; indeed, Formulog allowed us to program close enough to the specifications to uncover bugs in both of them. Despite encoding complex analysis logic, each of our analyses is concise (no more than 1.5K LOC). Furthermore, our Formulog-based implementations have acceptable performance, even when compared against reference implementations running on more mature language platforms. In some cases, we actually achieve substantial speedups over the reference implementations.

These performance results are possible only because Formulog's design allows our runtime to automatically and effectively apply high-level optimizations to Formulog programs. Our third case study makes this point emphatically. Due to automatic parallelization, our symbolic evaluator achieves a speedup of 7× over the symbolic execution tool KLEE [Cadar et al. 2008]. Moreover, this speedup increases to 12× when we use the magic set transformation [Bancilhon et al. 1985; Beeri and Ramakrishnan 1991] to automatically transform our exhaustive symbolic evaluator into a goal-directed one that explores only paths potentially leading to assertion failures. That Datalog

Programs	prog	::=	H^*	Variables	X	$\in$	Var
Horn clauses	H	::=	$p(e^*) :- P^*$	Constructors	c	$\in$	CtorVar
Premises	P	::=	$A \mid !A$	Predicates	p	$\in$	PredVar
Atoms	A	::=	$p(e^*) \mid e = e$				
Expressions	e	::=	$X \mid c$				

Fig. 1. A Datalog program is a collection of Horn clauses that represent rules for making inferences.

can speed up analyses like points-to analysis is well established [Bravenboer and Smaragdakis 2009; Whaley and Lam 2004]; that it can automatically scale symbolic evaluation is a novel result.

In sum, this paper makes the following contributions:

- the design of Formulog (Section 3), a domain-specific language for writing SMT-based static analyses that judiciously combines Datalog, a fragment of ML, and SMT solving;
- a lightweight bimodal type system (Section 4) that mediates the interface between concrete evaluation and SMT solving, enabling the construction of expressive formulas while preventing many kinds of runtime errors in both concrete evaluation and SMT solving;
- a fully-featured prototype and three substantial case studies (Section 5), showing that the design of Formulog can be the basis of a practical tool for writing SMT-based analyses; and
- an evaluation of Formulog's design in light of these case studies (Section 6), demonstrating how careful design decisions make Formulog an effective medium for encoding a range of SMT-based analyses in a way that is both close to their formal specifications and amenable to efficient evaluation and high-level optimizations.

2 BACKGROUND

The starting point for Formulog is Datalog with stratified negation (Figure 1) [Apt et al. 1988; Gallaire and Minker 1978; Green et al. 2013; Przymusinski 1988; Van Gelder 1989]. A Datalog program is a collection of Horn clauses, where a *clause* H consists of a head predicate $p(e^*)$ and a sequence of body premises P. Each *premise* P is either a positive atom A or a negated atom $!A$. An *atom* A has one of two forms: It is either a predicate symbol applied to a list of expressions, or the special equality predicate $e = e$. An *expression* e is a variable X or a nullary constructor c, i.e., an uninterpreted constant. Each predicate symbol p is associated with an extensional database (EDB) relation or an intensional database (IDB) relation. An *EDB relation* is tabulated explicitly through *facts* (clauses with empty bodies), whereas an *IDB relation* is computed through *rules* (clauses with non-empty bodies). A rule should be read as a universally quantified logical implication, with the conjunction of the body premises implying the predicate in the head. Datalog evaluation amounts to computing every possible inference with respect to these implications; the restriction to stratified negation (a relation cannot be defined, either directly or indirectly, by its complement) ensures that this can be done via a sequence of fixed point computations.

Datalog has proven to be a natural and effective way to encode a range of static analyses [Bravenboer and Smaragdakis 2009; Flores-Montoya and Schulte 2019; Grech et al. 2019, 2018; Guarnieri and Livshits 2009; Jordan et al. 2016; Livshits and Lam 2005; Tsankov et al. 2018; Whaley and Lam 2004]. EDB relations are used to represent the program under analysis; for example, EDB relations might encode a control flow graph of the input program. The logic of the analysis is encoded using rules that define IDB relations; these rules are fixed and do not depend on the program under analysis (which is already captured by the EDB relations). The Datalog program will compute the contents of the IDB relations, which can be thought of as the analysis results.

```
fun mem(X: 'a, Xs: 'a list) : bool =
  match Xs with [] => false | H :: T => X = H || mem(X, T) end

reaches(X, Y, [Y], Phi) :-  (* reaches is an IDB relation *)
  edge(X, Y, Phi),          (* edge is an EDB relation, defined below *)
  is_sat(Phi) = true.

reaches(X, Z, Y :: Path, `Phi /\ Constraint`) :-
  edge(X, Y, Phi),
  reaches(Y, Z, Path, Constraint),
  mem(Y, Path) = false,
  is_sat(`Phi /\ Constraint`) = true.

edge(1, 2, `#x[bool]`).  (* Constraint: SMT variable #x[bool] is true *)
edge(2, 3, `true`).      (* Constraint: true is true *)
edge(3, 4, `~#x[bool]`). (* Constraint: negation of #x[bool] is true *)
```

Fig. 2. This Formulog program computes a form of (non-reflexive) reachability for graphs where edges are labeled with propositions; here reachability requires the satisfiability of edge labels along a path.

That being said, standard Datalog is a very restricted language and there are many other analyses that cannot easily be encoded in it, if at all. Recent variants extend Datalog for analyses that operate over interesting lattices [Madsen et al. 2016; Szabó et al. 2018]. Following in this spirit, Formulog proposes a way to support analyses that need access to SMT solving.

3 LANGUAGE DESIGN

The design of Formulog is driven by three main desiderata. First, it should be possible to implement SMT-based static analyses in a form close to their formal specifications. Second, it should be easy to use logical terms the way that they are commonly used in many analyses. For example, analyses often need to create formulas about entities such as arrays and machine integers, test those formulas for satisfiability or validity, and generate models of them. Third, Formulog programs should still be amenable to powerful Datalog optimizations and evaluable using scalable Datalog algorithms.

Section 6 demonstrates how the design of Formulog largely meets these desiderata. Here, we give a warm-up example of Formulog, provide an overview of its language features, discuss how these features support logical formulas, and conclude with its operational semantics.

3.1 Formulog by example

To give the flavor of Formulog, we first present a small example (Figure 2). The "hello world" program of Datalog is graph transitive closure; here we give a Formulog analogue for directed graphs where edges are labeled with propositions, and we want to compute non-reflexive reachability modulo the satisfiability of the edge labels on a path.[1] The input to our program is an EDB relation `edge`, where `edge`(x,y,ϕ) denotes that there is an edge from node x to node y labeled with proposition ϕ. Our program computes an IDB relation `reaches`, where `reaches`(x,y,p,ϕ) denotes that node y is transitively reachable from node x through path $x::p$ with cumulative constraint ϕ.

[1] Computing reflexive reachability is also straightforward, but requires extra machinery (as it does for standard Datalog).

Types

Types	τ	::=	$t \mid t$ smt $\mid t$ sym $\mid$ model
Pre-types	t	::=	$B \mid D\,\tau^* \mid \alpha$
Base types	B	::=	bool $\mid$ string $\mid$ bv[k]$_{k \in \mathbb{N}^+}$ $\mid \ldots$

Terms

Programs	prog	::=	$H^*\ T^*\ F^*\ Z^*$
Horn clauses	H	::=	$p(e^*) :- P^*$
Premises	P	::=	$A \mid !A$
Atoms	A	::=	$p(e^*) \mid e = e$
Type definitions	T	::=	type $\alpha^*\ D = [c(\tau^*)]^*$
Functions	F	::=	fun $f([X : \tau]^*) : \tau = e$
SMT declarations	Z	::=	uninterpreted fun $c([t$ smt$]^*) : t$ smt $\mid$ uninterpreted sort $\alpha^*\ D$
Expressions	e	::=	$X \mid c(e^*) \mid k \mid f(e^*) \mid$ match e with $[c(X^*) \to e]^* \mid$ let $X = e$ in $e \mid$ if e then e else $e \mid \otimes(e^*) \mid$ `` `$\phi$` `` $\mid p(w^*)$
Constants	k	::=	true $\mid$ false $\mid$ 0 $\mid$ 1 $\mid \ldots$
SMT formulas	ϕ	::=	,$e \mid c^{\mathsf{SMT}}_{\mathsf{forall}}(\phi, \phi) \mid c^{\mathsf{SMT}}_{\mathsf{let}}(\phi, \phi, \phi) \mid c^{\mathsf{SMT}}_{\mathsf{ctor}}[c](\phi^*) \mid \ldots$
Wildcard	w	::=	?? $\mid e$
Values	$v \in$ Val	::=	$k \mid c(v^*)$

Namespaces

Data type names	D	$\in$	ADTVar	Variables	X	$\in$	Var
Type variables	α	$\in$	TVar	Predicates	p	$\in$	PredVar
Constructors	c	$\in$	CtorVar	Functions	f	$\in$	FunVar

Fig. 3. Formulog extends the abstract syntax of Datalog with type definitions, functions, SMT declarations, and a richer language of expressions.

After using the ML fragment to define a simple function `mem` that decides list membership, our program states two rules defining our `reaches` relation. The first represents the base case: if there is an edge between nodes `X` and `Y` with a satisfiable label `Phi`, then `Y` is reachable from `X` along the path `[X, Y]` with condition `Phi`. The built-in operator `is_sat` queries an external SMT solver for the satisfiability of its argument (an SMT proposition). The second rule computes the recursive case, making sure that the edge being used to extend the transitive closure is not redundant and that the labels along the prospective new path are satisfiable when taken together.

Given the `edge` relation in Figure 2, these rules compute that node `1` reaches nodes `2` and `3`, node `2` reaches nodes `3` and `4`, and node `3` reaches node `4`, but node `1` does not reach node `4`, since the path constraint `` `#x[bool] /\ true /\ ~#x[bool]` `` is not satisfiable.

3.2 Overview

Formulog extends Datalog with a fragment of first-order ML and a language of SMT formulas (Figure 3). Accordingly, a program consists of Horn clauses, type and function definitions, and SMT declarations. The Horn clause fragment is the same as in Datalog, except with a richer variety of expressions e that can occur as arguments to predicates.

Type definitions. Formulog users can define ML-style algebraic data types, which can be polymorphic and mutually recursive. An algebraic data type definition consists of a list of type variables α, a type name D, and a list of constructors c with their argument types τ. Section 4 explains Formulog's type system in more detail; we provide a brief sketch now. Algebraic data types $D\ \tau^*$, base types B, and type variables α are treated as *pre-types*; intuitively, a pre-type t is the type of a concrete (non-formula) term. In addition to pre-types, there are types that represent SMT-relevant terms: a t-valued SMT formula has type t smt, a t-valued SMT variable has type t sym, and an SMT model — a finite map from formula variables to concrete terms — has type model. The Formulog type system distinguishes the first three types where it is computationally relevant (i.e., during concrete evaluation, where confusing a t-valued formula for a concrete t term might lead to a computation getting stuck), and collapses them where it is not (i.e., during SMT evaluation, where there is no meaningful distinction between a t-valued formula and a concrete t value). It also prevents SMT models, which are not representable as SMT expressions, from flowing into SMT formulas.

Functions. Formulog supports ML-style function definitions, although functions are limited to being first-order and are not first-class values. They can be polymorphic and mutually recursive.

SMT declarations. Formulog users can declare uninterpreted functions and polymorphic uninterpreted sorts. An uninterpreted function amounts to a special constructor for building a purely symbolic term of type t smt (for some pre-type t). An uninterpreted sort amounts to a special symbolic pre-type t, where t is not inhabited by any value, but t sym and t smt are.

Expressions and formulas. Expressions e occur as function bodies and as predicate arguments in Horn clauses. Although Datalog traditionally limits ground terms to nullary constructors, we admit n-ary constructors. While this comes with the cost of possibly-diverging programs — adding n-ary constructors makes Datalog Turing-complete [Green et al. 2013] — many recent Datalog variants allow complex terms, including Soufflé [Scholz et al. 2016], LogicBlox [Aref et al. 2015], and Flix [Madsen et al. 2016]. For us, complex terms provide a natural way to reify logical formulas, and they also can be used to create data structures that make it easier to encode certain analyses.

Additional Formulog expressions include standard ML fare like constants (booleans, strings, machine integers, and floats), function calls, and match, let, and if-then-else expressions. The expression $\otimes(e^*)$ represents the application of a primitive operator to a sequence of subexpressions. These cover both basic arithmetic operations (e.g., addition) and SMT-specific operations (e.g., checking for satisfiability, generating models; see Section 3.3.2).

The expression `` `$\phi$` `` is a quasi-quoted SMT formula, where the language of formulas ϕ consists of unquoted expressions **,**e and formula constructors of the form $c_{c'}^{\mathsf{SMT}}$ applied to SMT formulas. Some of these constructors directly reflect SMT formula constructs; for example, the constructor $c_{\mathsf{forall}}^{\mathsf{SMT}}$ builds a universally quantified formula, and the constructor $c_{\mathsf{let}}^{\mathsf{SMT}}$ builds an SMT let formula. Formula constructors can appear only in formulas, and non-formula constructors cannot appear directly in formulas. We embed algebraic data type constructors in formulas using a family of *formula constructors*. Each formula constructor $c_{\mathsf{ctor}}^{\mathsf{SMT}}[c]$ lifts the user-defined algebraic data type constructor c to SMT. Quotes are used to delineate formulas and trigger a different type checking mode, in which the types t, t smt, and t sym are conflated (with some restrictions, as explained in Section 4). The unquote operator **,** escapes from this type checking mode and makes it possible to inject a non-formula expression into a formula. Section 3.3 discusses formulas in more detail.

We have already seen how the Datalog fragment of Formulog can include expressions from the ML fragment; the final expression $p(w^*)$ ties the loop by providing a way for the ML fragment to reference the Datalog fragment. The expression $p(w^*)$ acts like a function call that queries the contents of the relation p. Its exact behavior depends on its arguments, which are either

Negation	`~`	:	`bool smt` ⟶ `bool smt`
Conjunction	`/\`	:	(`bool smt`, `bool smt`) ⟶ `bool smt`
Implication	`==>`	:	(`bool smt`, `bool smt`) ⟶ `bool smt`
Equality	`#=[`t`]`	:	(t`smt`, t`smt`) ⟶ `bool smt`
SMT variable	`#{·}[`t`]`	:	`'a` ⟶ t `sym`
Bit vector constant	`bv_const[`k`]`	:	`bv[32]` ⟶ `bv[`k`] smt`
Bit vector addition	`bv_add`	:	(`bv[`k`] smt`, `bv[`k`] smt`) ⟶ `bv[`k`] smt`

Fig. 4. Logical formulas are created in Formulog via built-in constructors, such as the ones shown here.

expressions or the special wildcard term ??. If its arguments contain no wildcards, then $p(e^*)$ returns a boolean indicating whether the tuple identified by its arguments is in the p relation. If it has $k > 0$ wildcards, it returns a list of k-tuples: For each tuple v^* in the relation corresponding to p, there is a corresponding k-tuple in this list that is v^* projected to the wildcard positions; if there are n matching tuples in p, then the list is of length n. In other words, given complete arguments, a predicate is really just a predicate; given partial arguments with wildcards, a predicate is the multiset consisting of matching tuples after they have been appropriately projected.

Remarks. Extending Datalog with our fragment of ML is not foundational, as it can relatively easily be translated to Datalog rules (this would not necessarily be the case for a higher-order fragment of ML). However, despite the fact that the ML fragment could be treated as just syntactic sugar, it has a significant positive impact on the usability of Formulog, as we argue in Section 6.

The concrete syntax of formulas in our prototype (and in the examples we give in this paper) differs from the abstract syntax given here. First, algebraic data type constructors are allowed to appear directly in formulas, and are implicitly lifted to the appropriate formula constructor (so data type constructor c is automatically lifted to $c^{\mathsf{SMT}}_{\mathsf{ctor}}[c]$). Second, we do not support an explicit unquote operator; instead, we implicitly unquote variables, constants, and invocations of nullary functions.

3.3 Logical formulas

Formulog uses data types and operators to support constructing and reasoning about logical formulas. Formulog provides a library of data types that define logical terms. Most of the time during evaluation, these terms are unremarkable and treated just like any other ground term. However, these terms are interpreted as logical formulas when they are used as arguments to built-in operators that make calls to an external SMT solver. In our current prototype, it is possible to create logical terms in first-order logic extended with (fragments of) the SMT-LIB theories of uninterpreted functions, integers, bit vectors, floating point numbers, arrays, and algebraic data types [Barrett et al. 2017], as well as the theory of strings shared by the SMT solvers Z3 [de Moura and Bjørner 2008] and CVC4 [Barrett et al. 2011].

3.3.1 Representing formulas. Users create logical terms through constants and formula constructors. For example, to represent the formula $False \implies True$, one would use the term `` `false ==> true` ``, where `false` and `true` are the standard boolean values and `==>` is the infix constructor for implication.

Formulog offers around 70 constructors for creating logical terms ranging from symbolic string concatenation to logical quantifiers. Figure 4 shows a sample of these constructors and their types. Some constructors require explicit indices, either to guarantee that type information is available at runtime when the formula is serialized to SMT-LIB, or to make sure that the type of the arguments can be determined by the type of the constructed term (which makes type checking easier). For example, `bv_const[`k`]` creates a symbolic k-bit vector value from a concrete 32-bit vector; at runtime,

Satisfiability	`is_sat`	:	`bool smt` → `bool`
	`is_sat_opt`	:	(`bool smt list`, `bv[32] option`) → `bool option`
Validity	`is_valid`	:	`bool smt` → `bool`
Model generation	`get_model`	:	(`bool smt`, `bv[32] option`) → `model option`
Model inspection	`query_model`	:	(`'a sym`, `model`) → `'a option`

Fig. 5. Formulog provides built-in operators for reasoning about logical terms.

it is necessary to know the width k so that we can serialize it correctly. On the other hand, in the case of the constructor `#=[`t`]`, denoting the equality of two terms of type t `smt`, the index makes sure that the type checker knows what types the arguments should have. A programmer typically does not need to provide these indices explicitly, as they can often be inferred (our prototype does this).

Formulog distinguishes between logic programming variables and formula variables. A formula variable is a ground term that, when interpreted logically, represents a symbolic value. The term `#{`v`}[`t`]` is a formula variable of type t `sym` identified by the value v (which can be of arbitrary type). Intuitively, v is the "name" of the variable. The term `#{`v`}[`t`]` is guaranteed not to occur in v, which means that the variable it represents is fresh with respect to the set of formula variables in v; this makes it easy to deterministically construct a new variable that is fresh with respect to an environment, a trick we use often in our case studies. For example, if `X` is bound to a list of boolean formula variables, the formula variable `#{X}[bool]` will not unify with any term in `X`. The shorthand `#`*id*`[`t`]` is equivalent to `#{"`*id*`"}[`t`]`, where *id* is a syntactically valid identifier.

Importantly, because formula variables are ground terms, we can derive facts containing formula variables without violating Datalog's range restriction, which requires that every derived fact is variable-free. This restriction enables efficient evaluation by simplifying table lookups, one of the fundamental operations in Datalog evaluation.

3.3.2 Using formulas. Built-in operators provide a way to reason about logical terms as formulas (Figure 5). When an operator in the SMT interface is invoked, its formula argument is serialized into the SMT-LIB format and a call is made to an external SMT solver. These operators are assumed to act deterministically during a single Formulog run; an implementation can achieve this in the presence of a non-deterministic SMT solver by memoizing operations.

For example, to test the validity of the principle of explosion (any proposition follows from false premises), one could make the call `is_valid(\`false ==> #x[bool]\`)`. Like other operators, the SMT interface operators can be invoked from the bodies of rules, as here:

```
ok :-  #x[bool] != #y[bool],
       is_sat(`#x[bool] #= #y[bool]`) = true,
       is_sat(`~(#x[bool] #= #y[bool])`) = true.
```

This rule derives the fact `ok`: The term `#x[bool]` is not unifiable with the term `#y[bool]`, since they are different formulas, representing different SMT variables. But these terms both may and may not be equal when interpreted as formula variables via the operator `is_sat`. Within an invocation of `is_sat`, constraints are formed between `#x[bool]` and `#y[bool]` — in the first case they must be equal, and in the second case they must not be — but these constraints do not leak into the larger context. This is an intentional design decision and differs from the approach taken by paradigms like constraint logic programming (see Section 6).

Formulog provides two sets of operators for testing the satisfiability and logical validity of propositions. In general, an SMT solver can return three possible answers to such a query: "yes," "no," and "unknown." The operators `is_sat` and `is_valid` return booleans. In the case that the

backend SMT solver is not be able to determine whether a formula ϕ is satisfiable, these operators fail (as explained in Section 4). The operator `is_sat_opt(`ϕ^*`, timeout)` provides more fine-grained control: it takes a list of propositions (interpreted as conjuncts) and an optional timeout, and returns an optional boolean, with `none` corresponding to "unknown." While we suspect that the simpler versions will be sufficient for most applications, this more complex version does allow applications to explicitly handle the "unknown" case if need be (e.g., pruning paths in symbolic execution).

The operator `get_model` takes a proposition and an optional timeout; it returns a model for the proposition if the SMT solver is able to find one in time, and `none` otherwise. The values of formula variables in this model can be inspected using `query_model`, which returns `none` if the variable does not occur free in the formula or if a concrete value for it is not representable in Formulog (for example, Formulog does not have a type for a concrete 13-bit vector). The values of symbolic expressions can be indirectly extracted through formula variables: Before finding the model, add the equality `` `x #= e` `` to the formula, where x is a fresh formula variable and e is an expression; in the extracted satisfying model, x will be assigned the value of e in that model.

3.3.3 Custom types in formulas. Formulog's algebraic data types can be reflected in SMT formulas via SMT-LIB's support for algebraic data types. Thus, Formulog permits arbitrary term constructors to be used within logical formulas. For example, we can define a type `foo` with a single nullary constructor `bar` and then write formulas involving `foo`-valued terms:

```
type foo = | bar
ok :- is_valid(`#x[foo] #= bar`) = true.
```

This program would derive the fact `ok`: Since there is only one way to construct a `foo` — through the constructor `bar` — any symbolic value of type `foo` must be the term `bar`.

For each algebraic data type, we automatically generate two kinds of constructors that make it easier to write formulas involving terms of that type. The first kind is a constructor tester. For each constructor c of a type t, Formulog provides a constructor `#is_`c of type t `smt` $\rightarrow$ `bool smt`. The proposition `#is_`c`(`e`)` holds if the outermost constructor of e is c. The second kind is an argument getter. If c is a constructor for type t with n arguments of types t_i for $1 \leq 1 \leq n$, Formulog generates n argument getters of the form `#`c`_`i, where `#`c`_`i has the type t `smt` $\rightarrow$ t_i `smt`. When interpreted as a formula, the term `#`c`_`i`(`e`)` represents the value of the i^{th} argument of e. For example, we can state that a symbolic list of booleans is non-empty and its first argument is `true`:

```
`#is_cons(#x[bool list]) /\ #cons_1(#x[bool list])`
```

We could use the operator `get_model` to find a model of this satisfiable formula; in this model, `#x[bool list]` might be assigned the concrete value `cons(true, nil)`.

3.4 Operational semantics

This section presents Formulog's operational semantics, making reference to a selection of the formal rules (Figures 6).[2,3] Formulog imposes the standard stratification requirements upon programs: no recursive dependencies involving negation or aggregation between relations. As a stratifiable program can be evaluated one stratum at a time, we focus on the evaluation of a single stratum.

A stratum is evaluated by repeatedly evaluating its Horn clauses until no new inferences can be made. The semantics of a Horn clause H is defined through the judgment $\vec{F}; \mathcal{W} \vdash H \rightarrow \mathcal{W}_\perp$, where

[2]Formulog can also be given a model-theoretic semantics: because the ML features can be desugared into Datalog rules, the model theory of Formulog is essentially that of stratified Datalog. Appendix F sketches this out further.

[3]In the boxed rule schemata, implicit parameters are in gray; we conserve space by stating the rules without threading implicit parameters through, which are unchanging. We write $\vec{x_i}$ for some metavariable x to mean a possibly empty sequence of xs indexed by i, and write $S_\perp$ for some set S to mean the set S + Err.

Namespaces and constructs

$$\begin{array}{llll} \text{World} & \mathcal{W} & \in & \text{PredVar} \to \mathcal{P}(\text{Val}^*) \\ \text{Substitution} & \theta & \in & \text{Var} \rightharpoonup \text{Val} \end{array} \qquad \begin{array}{llll} \text{Error} & \bot & \in & \text{Err} \\ u\text{-term} & u & ::= & X \mid k \mid c(\vec{u_i}) \end{array}$$

Clause semantics $\boxed{\vec{F}; \mathcal{W} \vdash H \to \mathcal{W}_\bot}$

$$\frac{|\vec{P_i}| = n \quad \theta_0 = \cdot \quad \forall i \in [0, n),\ \theta_i \vdash P_i \to \theta_{i+1}}{\vec{F}; \mathcal{W} \vdash p(\vec{X_j}) :\!- \vec{P_i} \to \mathcal{W}[p \mapsto \mathcal{W}(p) \cup \{\theta_n(\vec{X_j})\}]}\ \textsc{Clause}$$

Premise semantics $\boxed{\vec{F}; \mathcal{W}; \theta \vdash P \to \theta_\bot}$

$$\frac{\vec{v} \in \mathcal{W}(p) \qquad \theta \vdash \vec{X} \sim \vec{v} : \theta'_\bot}{\mathcal{W}; \theta \vdash p(\vec{X}) \to \theta'_\bot}\ \textsc{PosAtom} \qquad \frac{\theta \vdash Y \sim c(\vec{X}) : \theta'_\bot}{\mathcal{W}; \theta \vdash Y = c(\vec{X}) \to \theta'_\bot}\ \textsc{EqCtor}$$

Expression semantics $\boxed{\vec{F}; \mathcal{W}; \theta \vdash e \Downarrow_e v_\bot}$ $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v}_\bot}$

$$\frac{\mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v} \qquad [\![\otimes]\!](\vec{v}) = v}{\mathcal{W}; \theta \vdash \otimes(\vec{e}) \Downarrow_e v}\ \Downarrow_e\text{-Op} \qquad \frac{\mathcal{W}; \theta \vdash \phi \Downarrow_\phi v_\bot}{\mathcal{W}; \theta \vdash \text{`}\phi\text{`} \Downarrow_e v_\bot}\ \Downarrow_e\text{-Quote}$$

Formula semantics $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \phi \Downarrow_\phi v_\bot}$ $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \vec{\phi} \Downarrow_{\vec{\phi}} \vec{v}_\bot}$

$$\frac{\mathcal{W}; \theta \vdash \vec{\phi} \Downarrow_{\vec{\phi}} \vec{v}}{\mathcal{W}; \theta \vdash c^{\text{SMT}}_{c'}(\vec{\phi}) \Downarrow_\phi c^{\text{SMT}}_{c'}(\vec{v})}\ \Downarrow_\phi\text{-Ctor} \qquad \frac{\mathcal{W}; \theta \vdash e \Downarrow_e v}{\mathcal{W}; \theta \vdash \text{,}e \Downarrow_\phi \text{toSMT}(v)}\ \Downarrow_\phi\text{-Unquote}$$

SMT conversion $\boxed{\text{toSMT}(v) = v}$

$$\begin{array}{rcl} \text{toSMT}(c^{\text{SMT}}_{\text{let}}(v_1, v_2, v_3)) & = & c^{\text{SMT}}_{\text{let}}(v_1, v_2, v_3) \\ \text{toSMT}(c^{\text{SMT}}_{\text{forall}}(v_1, v_2)) & = & c^{\text{SMT}}_{\text{forall}}(v_1, v_2) \end{array} \qquad \begin{array}{rcl} \text{toSMT}(c(\vec{v_i})) & = & c^{\text{SMT}}_{\text{ctor}}[c](\overrightarrow{\text{toSMT}(v_i)}) \\ & \ldots & \end{array}$$

Fig. 6. A fragment of Formulog's operational semantics (see Appendix C for full formalization).

a world $\mathcal{W}$ is a map from predicate symbols to sets of tuples (i.e., those that have been derived so far). A Horn clause takes a world to either a new world or the error value $\bot$. Going wrong can result for two reasons: either because a variable is unbound at a point where it needs to be bound, or because an operator is applied to a value outside of its domain. It is important to distinguish between a rule going wrong and a rule failing to complete because two terms fail to unify: The first is an undesirable error (ruled out by our type system), whereas the second is expected behavior.

A rule is evaluated by evaluating its premises one-by-one, using a left-to-right order (Clause). The judgment $\vec{F}; \mathcal{W}; \theta \vdash P \to \theta_\bot$ defines the semantics of a premise, which takes a world and a substitution θ (a partial function from variables to values) and returns a new substitution or an error. The substitution produced by one premise is used as the input to the next one. A successful inference extends the input world with a (potentially novel) tuple $\theta_n(\vec{X_j})$, i.e., the result of element-wise applying the substitution produced by the rightmost premise to the variables in the head of the rule. Clause evaluation goes wrong if the evaluation of one of the premises goes wrong.

Without loss of generality, we assume that premises occur in a limited form: predicates are applied to only variables, written $p(\vec{X}_i)$, and equality predicates bind variables, as in $Y = e$. (Our prototype similarly desugars premises.) An atom $p(\vec{X})$ is evaluated by non-deterministically choosing a tuple $\vec{v}$ from the tuples in $\mathcal{W}(p)$, and then pairwise unifying its elements with the variables $\vec{X}$ (PosAtom). The premise $Y = c(\vec{X})$ unifies its two terms (EqCtor). The judgment $\theta \vdash u_1 \sim u_2 : \theta_\perp$ defines the unification of terms u_1 and u_2 under the substitution θ; it results in an error if u_1 and u_2 both contain unbound variables, and a new substitution if they are otherwise unifiable.

The semantics for many Formulog expressions are standard. The evaluation of an operator produces a value if its arguments are evaluated to values in its domain ($\Downarrow_e$-Op); it goes wrong if the argument values are outside of its domain, e.g., if a string and number are added together. A quoted formula `` `$\phi$` `` evaluates to whatever ϕ evaluates to ($\Downarrow_e$-Quote). Formula $c^{\text{SMT}}_{c'}(\vec{\phi})$ evaluates to formula $c^{\text{SMT}}_{c'}(\vec{v})$ if arguments $\vec{\phi}$ evaluate to values $\vec{v}$ ($\Downarrow_\phi$-Ctor). If the expression e evaluates to the value v, then the formula `,`e evaluates to the term toSMT(v) ($\Downarrow_\phi$-Unquote), where the helper function toSMT lifts a term to its formula version.

4 TYPE SYSTEM

Formulog's type system is designed to meet three desiderata. The first desideratum is that concrete evaluation should never go wrong, which might happen if an operator is applied to an operand outside its domain or a variable is unbound at a point when it needs to be evaluated. The second desideratum is that SMT solving should never go wrong, which might happen if a term that does not represent a well-sorted formula under the SMT-LIB standard reaches the external SMT solver (e.g., a formula representing the addition of a 16-bit vector and 32-bit vector). The third desideratum is that the type system should make it easy to construct expressive logical formulas, including formulas that involve terms drawn from user-defined types.

There is some tension between the first and third of these desiderata. The first one requires that we differentiate between, for example, a concrete bit vector value and a symbolic bit vector value (e.g., a bit vector-valued formula) since an operator that is expecting a concrete bit vector might get stuck if its argument is a symbolic bit vector. For instance, we want to rule out this program:

Example 1 (A bad program we would want to reject)**.**

```
type foo = | bar(bv[32])
fun f(F: foo) : bv[32] = match F with bar(Y) => Y + Y end
not_ok :-  X = #x[bv[32]],
           f(bar(X)) = 42.
```

This program gets stuck evaluating `f(bar(X))`, since `Y` is bound to a symbolic value in `f` but the ML fragment's addition operator needs concrete arguments. On the other hand, we are able to construct more expressive formulas if we can occasionally conflate concrete and symbolic expressions:

Example 2 (A good program we would want to accept)**.**

```
ok :-  X = #x[bv[32]],
       is_sat(`bar(X) #= bar(5)`) = true.
```

This rule asks whether there exists a symbolic bit vector x such that `bar(`x`)` equals `bar(5)`, where `bar` is the constructor defined above. This reasonable formula is not well-typed under a type system that uniformly distinguishes between concrete and symbolic values, since the constructor `bar` expects a concrete bit vector argument but instead receives the symbolic one x.

Contexts

$$\begin{array}{lrcl} \text{Data type declarations} & \Delta & ::= & \cdot \mid \Delta, D : \forall \vec{\alpha}_i.\ \{\overrightarrow{c_j : \vec{\tau}_k}\} \\ \text{Program declarations} & \Phi & ::= & \cdot \mid \Phi, f : \forall \vec{\alpha}, \vec{\tau} \to \tau \mid \Phi, p \subseteq \vec{\tau} \\ \text{Variable contexts} & \Gamma & ::= & \cdot \mid \Gamma, x : \tau \mid \Gamma, \alpha \end{array}$$

Clause typing $\boxed{\Delta; \Phi \vdash H}$

$$\frac{\cdot \vdash P_0 \rhd \Gamma_1 \qquad \ldots \qquad \Gamma_j \vdash P_j \rhd \Gamma_{j+1} \qquad \ldots \qquad \Gamma_n \vdash P_n \rhd \Gamma' \qquad p \subseteq \vec{\tau}_i \in \Phi \qquad \Gamma' \vdash \vec{X}_i, \vec{\tau}_i \rhd \Gamma'}{\vdash p(\vec{X}_i) :\!-\ \vec{P}_j} \; H\text{-Clause}$$

Variable binding and typing $\boxed{\Gamma \vdash x, \tau \rhd \Gamma}$ $\boxed{\Gamma \vdash \vec{x}, \vec{\tau} \rhd \Gamma}$

$$\frac{X \notin \mathrm{dom}(\Gamma)}{\Gamma \vdash X, \tau \rhd \Gamma, X{:}\tau} \; X\tau\text{-Bind} \qquad \frac{\Gamma(X) = \tau}{\Gamma \vdash X, \tau \rhd \Gamma} \; X\tau\text{-Check}$$

Premise typing $\boxed{\Delta; \Phi; \Gamma \vdash P \rhd \Gamma}$

$$\frac{p \subseteq \vec{\tau}_i \in \Phi \qquad \Gamma \vdash \vec{X}_i, \vec{\tau}_i \rhd \Gamma'}{\Gamma \vdash p(\vec{X}_i) \rhd \Gamma'} \; P\text{-PosAtom} \qquad \frac{\Gamma \vdash e : \tau \qquad \Gamma \vdash Y, \tau \rhd \Gamma'}{\Gamma \vdash Y = e \rhd \Gamma'} \; P\text{-Eq-FB}$$

Function and expression well formedness $\boxed{\Delta; \Phi \vdash F}$ $\boxed{\Delta; \Phi; \Gamma \vdash e : \tau}$

$$\frac{\mathrm{typeof}(\otimes) = \vec{\tau}_i \to \tau \qquad \Gamma \vdash e_i : \tau_i}{\Gamma \vdash \otimes(\vec{e}_i) : \tau} \; e\text{-Op} \qquad \frac{\Gamma \vdash \phi : \tau}{\Gamma \vdash \grave{}\phi\grave{} : \tau} \; e\text{-Quote}$$

SMT constructors and formula well formedness $\boxed{\Delta; \Phi; \Gamma \vdash c^{\mathsf{SMT}}_{\cdots} : \vec{\tau}_i \to \tau}$ $\boxed{\Delta; \Phi; \Gamma \vdash \phi : \tau}$

$$\frac{\Gamma \vdash c^{\mathsf{SMT}}_{\mathrm{c}} : \vec{\tau}_i \to \tau \qquad \Gamma \vdash \phi_i : \tau_i}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathrm{c}}(\vec{\phi}_i) : \tau} \; \phi\text{-Ctor} \qquad \frac{\Gamma \vdash e : \tau}{\Gamma \vdash ,e : \mathrm{toSMT}(\tau)} \; \phi\text{-Unquote} \qquad \frac{\Gamma \vdash \phi : t\ \mathsf{sym}}{\Gamma \vdash \phi : t\ \mathsf{smt}} \; \phi\text{-Promote}$$

SMT representations $\boxed{\mathrm{erase}(\tau) = t}$ $\boxed{\mathrm{toSMT}(\tau) = \tau}$

$$\begin{array}{rcl} \mathrm{erase}(B) & = & B \\ \mathrm{erase}(D\ \vec{\tau}_i) & = & D\ \overrightarrow{\mathrm{erase}(\tau_i)} \end{array} \qquad \begin{array}{rcl} \mathrm{erase}(t\ \mathsf{smt}) & = & \mathrm{erase}(t) \\ \mathrm{erase}(t\ \mathsf{sym}) & = & \mathrm{erase}(t) \end{array} \qquad \begin{array}{rcl} \mathrm{toSMT}(t) & = & \mathrm{erase}(t)\ \mathsf{smt} \\ \mathrm{toSMT}(t\ \mathsf{smt}) & = & \mathrm{erase}(t)\ \mathsf{smt} \\ \mathrm{toSMT}(t\ \mathsf{sym}) & = & \mathrm{erase}(t)\ \mathsf{sym} \end{array}$$

Fig. 7. A fragment of Formulog's type system (see Appendix B for full formalization).

Formulog resolves the tension between these desiderata through a bimodal type system that acts differently inside and outside formulas (which are demarcated by quotations). In essence, the Formulog type system differentiates between the pre-type t, the SMT formula type t smt, and the SMT variable type t sym outside of formulas, but typically conflates them within formulas.[4]

[4]It does not conflate them in binding positions where formula variables are required, such as in quantifiers.

This bimodal approach disallows Example 1 (since outside a formula, a term of type bv[32] sym cannot be used where a term of type bv[32] is expected), while permitting Example 2 (since within a formula, a term of type bv[32] sym can be used anywhere a term of type bv[32] is expected).

Intuitively, this bimodal approach is safe because it distinguishes between concrete and symbolic values during concrete evaluation — where conflating them might lead to going wrong — and conflates them only during SMT evaluation, where the distinction is not meaningful. We have formalized the Formulog type system and proven it sound with respect to the operational semantics of Formulog. We present only a small subset of it here (Figure 7); the full system is in Appendix B.

The rule defining a well-typed Horn clause (H-Clause) depends on two notable judgments. The premise typing judgment $\Gamma \vdash P \rhd \Gamma'$ takes a variable typing context Γ and a premise P and produces a new variable typing context Γ'. The variable binding and typing judgment $\Gamma \vdash x, \tau \rhd \Gamma'$ holds if either X is not in Γ, in which case Γ' extends Γ with X mapped to τ ($X\tau$-Bind), or X is mapped to τ by Γ, in which case $\Gamma = \Gamma'$ ($X\tau$-Check). As can be seen from rule H-clause, the type checking of Horn clauses is flow-sensitive and proceeds left-to-right across the clause, with the "output" context of checking premise P_i used as the "input" context for checking premise P_{i+1}. This left-to-right type checking mirrors the left-to-right evaluation strategy Formulog uses; this is important for ensuring that variables are bound at the correct points.[5] The second line of premises in rule H-clause ensures that every variable in the head of the rule is bound at the type specified by the head relation's signature.

A positive atom is well typed if each of its variable arguments has the type given to that argument by the relation's signature (P-PosAtom). A premise of the form $Y = e$ is typed according to a few different rules depending on which side of the equation is ground with respect to the input context Γ. The key is that our type system only types premises of the form $Y = e$ when unification is guaranteed to not go wrong at runtime.

The typing rules for most expressions are standard. An operation is well-typed if its arguments match its type signature (ϕ-Ctor). A quoted formula `` `$\phi$` `` types at whatever ϕ types at (e-Quote). The formula constructor c_c^{SMT} is well typed if the types of its arguments match its type signature (ϕ-Ctor); in the case of a constructor for an algebraic data type that has been lifted to a formula constructor, that signature will require the constructed term and all of its arguments to have types of the form t smt. If an expression types at τ, then the formula ,e types at toSMT(τ) (ϕ-Unquote). The helper function toSMT lifts a type to a formula type; for example, it lifts bool to bool smt. The typing rules for formulas also include a rule promoting from t sym to t smt, reflecting the fact that, within a formula, a t-valued formula variable can be used anywhere a t-valued formula can be.[6]

Type soundness with respect to the semantics of Formulog comes from safety and preservation:

Theorem 4.1 (Safety). *If* $\Delta; \Phi \vdash \vec{F}_i\ \vec{H}_j$ *and* $\Delta; \Phi \models \mathcal{W}$ *then for all* $H \in \vec{H}_j$, $\neg(\vec{F}_i; \mathcal{W} \vdash H \longrightarrow \bot)$.

Theorem 4.2 (Preservation). *If* $\Delta; \Phi \vdash \vec{F}_i\ \vec{H}_j$ *and* $\Delta; \Phi \models \mathcal{W}$ *and* $\vec{F}_i; \mathcal{W} \vdash H \longrightarrow \mathcal{W}'$ *for some* $H \in \vec{H}_j$ *then* $\Delta; \Phi \models \mathcal{W}'$.

Safety (Theorem 4.1) guarantees that a Horn clause from a well-typed program, evaluated on a well-typed world (i.e., one where all the tuples have the right types), cannot step to error. Thus, safety means that an operator is never applied to an operand outside its domain, and a variable is never unbound when it needs to be bound. Preservation (Theorem 4.1) guarantees that if a Horn

[5]The fact that the operational semantics and type system assume a certain order of evaluation does not prohibit a Formulog runtime from reordering premises within rules (for example, when applying database-style query planning optimizations); it just needs to check that the new order is also well typed. This type of rewriting does not affect the result of running the rule provided that all subexpressions terminate (an assumption we make).

[6]The opposite is not true, since some formula constructors (i.e., quantifiers and let expressions) bind formula variables.

clause, from a well-typed program, is evaluated on a well-typed world and results in a new world, then that new world is also well-typed. Taken together, these theorems imply that a well-typed Formulog program does not go wrong during concrete evaluation (see Appendix E for proofs).

The type system is sound with respect to the semantics of SMT-LIB because the types of the formula constructors provided by Formulog are consistent with the types given by the SMT-LIB standard. The Formulog type system guarantees that, at runtime, terms (including formulas) are well-typed, and the type system prevents terms that are not representable in SMT (such as those of type model) from flowing into SMT formulas. We distinguish between SMT-compatible types and non-SMT types formally by indexing the type well formedness judgment with a *mode*, which is either smt (for those types that can be sent to the solver) or exp (for those types that cannot). It is fair to think of these modes as kinds with a subkinding relationship: types of kind smt can safely be treated as general types of kind exp, but not the other way round (Lemma D.1).

Assumptions. An actual implementation of Formulog, such as our prototype, has to contend with a few sources of going wrong that are not captured in our formal model. First, our model assumes that patterns in match clauses are exhaustive; this is just for simplicity, and could be statically checked using standard algorithms. Second, our model assumes that operators are total with respect to terms with the correct type. There are three places where this assumption might break: 1) division or remainder by zero; 2) the operators `is_sat` or `is_valid` may induce an "unknown" response from the external SMT solver; and 3) the SMT solver may reject patterns used in trigger-based quantifier instantiation that it considers to be ill formed (for example, if the pattern contains a binding operation). The first case is standard for many languages; the second can be avoided if the programmer uses the option-returning SMT operator `is_sat_opt`. The last case would be hard to check statically; however, an implementation could dynamically check patterns before making a call to the SMT solver, dropping invalid patterns and issuing a warning to the user. Our prototype uses "hard exceptions" by default, aborting the program. We also support a "soft exception" mode, which treats all these cases analogously to unification failures, halting execution on the current path but allowing execution on other paths to continue.

5 IMPLEMENTATION AND CASE STUDIES

In this section we briefly describe our prototype implementation of Formulog, and then discuss three analyses we have built as case studies: refinement type checking, bottom-up points-to analysis, and bounded symbolic evaluation.

5.1 Prototype

Our prototype runtime (~17.5K LOC Java) works in five stages: parsing, type checking, rewriting (for query specialization), validation, and evaluation. Stratification and the range restriction are checked during the validation phase. Our parallel implementation of semi-naive evaluation [Bancilhon 1986] uses a work-stealing thread pool; worker threads dispatch SMT queries to a pool of Z3 instances [de Moura and Bjørner 2008]. Our prototype is feature complete, but not heavily optimized.

Unless otherwise noted, we ran experiments on an Ubuntu Server 16.04 LTS machine with a 3.1 GHz Intel Xeon Platinum 8175 processor (24 physical CPUs, each hyperthreaded) and 192 GiB of memory. We configured our Formulog runtime to use up to 40 threads and up to 40 Z3 instances (v4.8.7); all comparison systems were set to use the same version of Z3 (with one exception, noted later). For each result, we report the median of three trials.[7] Times are given as minutes:seconds.

[7] For each case study, we use a tool to take a program in the input language (e.g., Java) and turn it into Formulog facts. We do not include these times, as they are typically quite short. Extracting facts from libraries can take a few minutes, but this needs to be done only once per library.

```
fun accum_nil_axiom : bool smt =
  let (F, I) = (#func[closure], #init[enc_val]) in
  `forall F, I : accum(F, v_zero, I). accum(F, v_zero, I) #= I`
```

Fig. 8. This axiom encodes the denotation of a Dminor accumulate expression over an empty multiset. The term in the formula between `:` and `.` is a quantifier pattern [Detlefs et al. 2005].

5.2 Refinement type checking

We have implemented a type checker in Formulog for Dminor, a first-order functional programming language for data processing that combines refinement types with dynamic type tests [Bierman et al. 2012]. This type system can, e.g., prove that

```
x in Int ? x : (x ? 1 : 0)
```

type checks as `Int` in a context in which `x` has the union type `(Int|Bool)`. Proving this entails encoding types and expressions as logical formulas and invoking an SMT solver over these formulas. We built a type checker for Dminor by almost directly translating the formal inference rules used to describe the bidirectional Dminor type system. In fact, we programmed so closely to the formalism that debugging an infinite loop in our implementation helped us, along with the Dminor authors, uncover a subtle typo in the formal presentation! Our Dminor type checker is 1.2K lines of Formulog. The implementation of Bierman et al. is 3.2K lines of F$^\sharp$ and 400 lines of SMT-LIB; we estimate that the functionality we implemented accounts for over two thousand of these lines.[8]

The encoding of Dminor types and expressions is complex, requiring uninterpreted sorts, uninterpreted functions, universally quantified axioms, and arrays (among other features). The fact that we were able to code this relatively concisely speaks to the expressiveness of Formulog's formula language. For example, Figure 8 shows an axiom describing the denotation of the base case of a Dminor accumulate expression, which is essentially a fold over a multiset. Here, the type `closure` is an uninterpreted sort, `enc_val` is an algebraic data type that represents an encoded Dminor value, and `accum` and `v_zero` are uninterpreted functions, where the latter represents an empty multiset.

We defined a set of mutually-recursive functions that encode expressions, environments, and types. For example, the type encoding function (fragment, Figure 9) takes a type τ and an (encoded) Dminor value v, and returns two propositions. The first is true when v has type τ. The second is a conjunction of axioms: new axioms are created to describe the denotation of the bodies of accumulate expressions as they are encountered when encoding expressions. The first case in the figure encodes the fact that any value has type `Any`. The second one says that a value has type `Bool` if it is constructed using the constructor `ev_bool`; the constructor `#is_ev_bool` is an automatically-generated constructor tester. The third case handles multiset types. It creates a fresh encoded value `X`, uses `X` to recursively create a proposition representing the encoding of the type `S` of items in the multiset, and then returns a proposition requiring the value to be a "good" collection (defined using the uninterpreted function `good_c`) and every item in the multiset to have type `S` (where `mem` is another uninterpreted function).

Although we use ML-style functions to define the logical denotation of expressions, environments, and types, we use logic programming rules to define the bidirectional type checker, which allows us to write rules that are very similar to the inference rules given in the paper. Figure 10 gives the one rule defining the subtype relation: `T` is a subtype of `T1` in environment `Env` if `T1` is well formed

[8] The reference implementation is closed source; the authors have kindly provided us with line counts for each file.

```
fun encode_type(T: typ, V: enc_val smt) : bool smt * bool smt =
  match T with
  | t_any => (`true`, `true`)
  | t_bool => (`#is_ev_bool(V)`, `true`)
  | t_coll(S) =>
    let X = #{(S, V)}[enc_val] in
    let (Phi, Ax) = encode_type(S, `X`) in
    (`good_c(V) /\ forall X : mem(X, V). mem(X, V) ==> Phi`, Ax)
```

Fig. 9. This function (fragment) constructs a formula capturing the logical denotation of a Dminor type.

```
subtype(Env, T, T1) :-
  type_wf(Env, T1),
  encode_env(Env) = Phi_env,
  X = `#{(Env, T, T1)}[enc_val]`,
  encode_type(T, X) = (Phi_t, Axioms1),
  encode_type(T1, X) = (Phi_t1, Axioms2),
  Premises = [Phi_t, Phi_env, Axioms2, Axioms1, axiomatization],
  is_sat_opt(`~Phi_t1` :: Premises, z3_timeout) = some(false).
```

Fig. 10. This rule defines Dminor's semantic subtyping relation. It uses the operator `is_sat_opt` instead of `is_valid` because its SMT queries can sometimes result in "unknown."

and the denotation of `T`, given our axioms and the denotation of `Env`, implies the denotation of `T1`. This rule is an almost exact translation of the inference rule given in the paper.

Finally, the type checker needs to ensure that any expressions that occur in refinements are pure (i.e., terminate and are deterministic). We have written a termination checker based on the size-change principle [Lee et al. 2001]. Our implementation is another good example of the synergy between ML-style functions and Datalog rules, as we use the former to define the composition of two size-change graphs and use the latter to find the fixed point of composing size-change graphs.

We tested our type checker on six of the sample programs included in the Dminor documentation (the other three examples make use of a feature — the ability to generate an instance of a type — that we did not implement, although it should be possible to do so; to the best of our knowledge, these are the only publicly available Dminor programs). We combined these examples into a single aggregate program of ~150 LOC. The reference implementation type checked this program in 1.5 seconds using an optimization that tries syntactic subtyping before semantic subtyping; with this optimization disabled, it took 3.6 seconds.[9] Our implementation completed in 5 seconds; it did not use this optimization (which is not detailed in the paper), but did use a newer version of Z3. Thanks to parallelization, our implementation automatically scaled to larger programs: On a synthetic program consisting of ten copies of the original aggregate program, it completed in 21.4 seconds (2.1 seconds per program copy); on a synthetic program consisting of 100 copies, it completed in 183.9 seconds (1.8 seconds per program copy). In contrast, the reference implementation did not scale: even with the syntactic-subtyping optimization enabled, it took 68 seconds on the ten-copy program and over 100 minutes on the 100-copy program.

[9]Here we used a machine with Microsoft Windows Server 2019 and the same hardware specs as our Ubuntu machine.

```
instantiate_ptsto(C, O1, Phi1, O2, widen(C, Phi_all)) :-
  instantiate_loc(C, heap(O1), heap(O2), Phi2),
  instantiate_constraint(C, Phi1, Phi3),
  Phi_all = conjoin(Phi2, Phi3).
```

Fig. 11. This rule describes how a points-to edge to object `O1` labeled with constraint `Phi1` is instantiated at a call site `C`: if at `C` a heap location `heap(O1)` can be instantiated to a heap location `heap(O2)` under constraint `Phi2`, and the original constraint on the edge `Phi1` can be instantiated to a constraint `Phi3`, then the points-to edge to `O1` labeled with `Phi1` instantiates to a points-to edge to `O2` labeled with `widen(C, Phi_all)`, where `Phi_all` is the conjunction of `Phi2` and `Phi3` and `widen` is a function that widens constraints in mutually-recursive functions (one of the heuristics we borrowed from Scuba).

5.3 Bottom-up points-to analysis

We have implemented the bottom-up context-sensitive points-to analysis for Java proposed by Feng et al. [2015]. A points-to analysis computes a static approximation of the objects that stack variables and heap locations can point to at runtime. A bottom-up points-to analysis does this through constructing method summaries that describe the effect of a method on the heap; it is bottom-up in the sense that summaries are propagated up the call graph, from callees to callers.

In Feng et al.'s algorithm, a method summary is an abstract heap that maps abstract locations to heap objects, where an abstract location might be a stack variable, an explicitly allocated heap object, or an argument-derived heap location. Edges in the abstract heap are labeled with logical formulas that describe the conditions under which the edges hold; when a method summary is instantiated at a call site, a constraint solver can be used to filter out edges with unsatisfiable labels.

Feng et al.'s tool based on this algorithm, Scuba, is ∼15K lines of Java, builds on the Chord analysis framework [Naik 2011], and uses Z3 to discharge constraints. As for many realistic static analysis tools, there is a gap between what is implemented in Scuba and the formal specification of the analysis. This is partly because Scuba is written in Java: Object-oriented programming does not naturally capture inference rules, the form of the specification. In contrast, our Formulog implementation, which is ∼1.5K LOC, closely mirrors the inference rules. For example, we can directly state how a points-to edge is instantiated at a call site (Figure 11), one step of summary instantiation, a complex process defined through half a dozen mutually recursive relations that need to be computed as a fixed point. The Java code for encoding this logic is more complex and further from the formal specification. Programming close to the specification also helps check the specifications' correctness: while implementing in Formulog one of the judgments specified by Feng et al., we discovered an inconsistency between the judgment's definition and its type signature.

Scuba employs a range of sophisticated heuristics that are essential to making the algorithm perform in practice, as they tune precision to achieve scalability. Some go far beyond the algorithm described in the paper and are interesting in their own right. Our implementation uses some heuristics based on the ones in Scuba. The fact that we were able to implement useful heuristics — a necessity for a realistic static analysis tool — argues for the practicality of Formulog. Moreover, we were able to do so such that our code still closely reflects the core algorithm specified in the paper.

We ran both tools on the benchmarks used in the evaluation by Feng et al., which represent a selection from the pjbench suite plus the benchmark polyglot.[10] These experiments include library code and use a context-sensitivity of two call sites; reflection is ignored, as are many native methods. Given an hour timeout, our implementation completed on eight of the ten benchmarks, with times ranging from five to 18 minutes (Table 1). In the median, we were 6.7× slower than Scuba. However,

[10]The pjbench suite is available at https://bitbucket.org/psl-lab/pjbench/src/master/.

	Scuba		Formulog	
Benchmark	Time	# `main` edges	Time	# `main` edges
antlr	1:11	3,313	12:16	112,415
avrora	1:05	714	7:40	127,535
hedc	0:57	867	5:04	2,962
hsqldb	0:51	780	4:53	7,039
luindex	1:40	3,395	T/O	-
polyglot	0:55	117	4:52	4,245
sunflow	3:48	7,456	T/O	-
toba-s	0:58	521	4:57	12,284
weblech	1:10	1,262	17:58	6,785
xalan	0:54	183	5:40	55,722

Table 1. In the median, our implementation of a bottom-up points-to analysis for Java was 6.7× slower than Scuba, the reference implementation; however, the two tools use different heuristics and thus compute very different things, as indicated by the discrepancy in the number of points-to edges computed in the summary for `main` (which also captures the effect on the heap of methods invoked transitively from it).

a performance comparison between the tools should be taken with a grain of salt: Since they use different heuristics, they compute very different things.

In sum, we were able to implement the algorithm in a way that is still very close to its specification and achieve decent performance on many realistic benchmarks while implementing only a small selection of heuristics. Other heuristics might have helped our version complete on the two benchmarks it timed out on. Making the algorithm practical is a significant engineering challenge: Even with its sophisticated heuristics, Scuba does not complete on all benchmarks in pjbench.[11]

Moreover, our implementation could be used as a platform for exploring potential optimizations to Scuba. First, because it is automatically parallelized (with a user-chosen number of worker threads), it could be used to evaluate how well the underlying points-to algorithm parallelizes before going through all the trouble of parallelizing Scuba, which uses mutable state in a complex way. Second, thanks to the magic set transformation, we have automatically derived a goal-directed version of the analysis that computes only the summaries necessary for constructing user-requested summaries. The points-to algorithm resulting from this transformation could be used as a road map for implementing a demand-driven version of Scuba, which Feng et al. describe as future work.

5.4 Bounded symbolic evaluation

We have written a symbolic evaluator (~800 LOC) for a fragment of LLVM bitcode [Lattner and Adve 2004] corresponding to a simple imperative language with integer arrays and symbolic integers (a symbolic integer represents a set of integer values that might occur at runtime). It implements a form of bounded symbolic execution [King 1976], exploring all feasible program paths up to a given length, evaluating concretely whenever possible, and aggressively pruning infeasible paths.

Our implementation uses a different logic rule to define each of the possible cases during evaluation, and uses ML functions to manipulate and reason about complex terms representing evaluator state. For example, one rule defines when an assertion fails (Figure 12). This rule says that the path `Path` ends in a failure with evaluator state `St` if: (1) there is an assert instruction `Instr` with argument `X`, (2) following `Path` has led the evaluator to that instruction with state `St`, (3) `X` could have the (possibly symbolic) integer value `V` in state `St`, and (4) `V` may be zero. The function

[11] For example, we found it timed out on batik, chart, fop, lusearch, and pmd (as did our implementation).

```
failed_assert(Path, St) :-
  assert_instruction(Instr, X),
  stepped(Instr, St, _, Path),
  has_value(X, St, v_int(V)),
  may_be_zero(V, St) = true.
```

Fig. 12. This rule states that the symbolic evaluator has reached a failing assertion when the argument of the assert instruction may be zero.

```
a := array of N symbolic ints;
b := symbolic int;
if (b) { sort a; }
else { sort a; assert a sorted; }
```

Fig. 13. This pseudocode sketches a C program that creates an array, branches, sorts it in each branch, but only asserts that the result is sorted in one branch.

Benchmark	# paths	KLEE	Formulog	Benchmark	# paths	KLEE	Formulog
shuffle-4	125	0:08	0:04 (↑2.0×)	sort-7	22,070	25:45	3:48 (↑6.8×)
shuffle-5	1,296	2:53	0:19 (↑9.1×)	numbrix-sat	1	0:14	1:19 (↓5.6×)
sort-6	2,718	2:25	0:18 (↑8.1×)	numbrix-unsat	1	0:09	1:08 (↓7.6×)

Table 2. We report absolute times for KLEE and a Formulog-based symbolic evaluation tool on six benchmark programs; for the latter, we also report speedups (↑) and slowdowns (↓) relative to KLEE.

`may_be_zero(V, St)` returns true if and only if `V` may be zero given `St`. We represent symbolic values as SMT formulas, so when `V` is symbolic, this function invokes the SMT solver.

We have evaluated our symbolic evaluator on six benchmarks based on three template programs. The first template (shuffle-N) non-deterministically shuffles an array of size N and asserts that the resulting array represents the same set as the input array. The second template (sort-N; Figure 13) splits into two branches, sorts an array using selection sort in both branches, and asserts that the resulting array is sorted in the second branch. The third template completes a partially filled-in 4×4 grid of integers, such that there is a path from 1 to 16 where each integer follows its predecessor and only horizontal and vertical movements are used; the benchmark numbrix-sat runs this program on a satisfiable instance, while the benchmark numbrix-unsat runs it on an unsatisfiable one.

We compared our times on these benchmarks against KLEE (v2.1) [Cadar et al. 2008], a well-known symbolic execution tool (Table 2). On programs with a single path to explore, KLEE has speedups over our version ranging from 5.6× (numbrix-sat) to 7.6× (numbrix-unsat). However, thanks to its automatic parallelization, Formulog scales better as the number of paths increases: For programs with more than 1000 paths, our version achieves speedups over KLEE ranging from 6.8× (sort-7) to 9.1× (shuffle-5). While the comparison is not totally apples-to-apples (for example, KLEE handles all of LLVM and needs to maintain a more complex symbolic state), we are encouraged by the fact that the Formulog-based version seems to scale automatically in a way that KLEE does not.

Furthermore, the Formulog-based symbolic evaluator can be run in a goal-directed mode: If we only want to check that no assertion fails, we can add the query `failed_assert(_Path, _St)`, triggering the Formulog runtime to rewrite our evaluator to explore only paths that could potentially lead to a failed assertion. On the sorting benchmarks (Figure 13), this leads to substantial speedups over KLEE — 10.4× for sort-6 and 11.8× for sort-7 — as the symbolic evaluator can ignore the first branch of the program. To further evaluate the effectiveness of this optimization, we compared our implementation against the bounded model checker CBMC (v5.11) [Clarke et al. 2004], which uses program slicing [Weiser 1984] to achieve a similar effect. On sort-6 and sort-7, CBMC has speedups over our symbolic evaluator of 1.3× and 1.4×, respectively. Thus, our automatic optimizations can put Formulog-based analyses within a reasonable factor of hand-optimized systems.

6 DESIGN EVALUATION

In this section, we evaluate the design of Formulog with respect to our case studies. We argue that Formulog is an effective and usable tool for writing SMT-based analyses.

Formulog makes it possible to write SMT-based analyses in a way that is close to their mathematical specification, leading to concise encodings. Our implementations of the Dminor type checker (Section 5.2) and the bottom-up points-to analysis (Section 5.3) directly mirror their published formal specifications; our third case study (Section 5.4), which was not based on any particular formalization, would itself be the basis of a reasonable specification of symbolic evaluation. Formulog provides language features that are a good match for the way that SMT-based analyses are specified: algebraic data types naturally encode BNF grammars (a common feature in analysis specifications); Horn clauses match judgments; ML functions fit helper functions; and the reification of formulas as terms captures the way that formulas are treated in analysis specifications.

As a corollary, analyses written in Formulog can be concise. Despite encoding quite complex logic, each of our case studies is less than 1.5K lines of code. In the case of the points-to analysis, this is 10× smaller than the reference implementation (which also uses functionality defined externally in Chord). This is partly because Scuba implements heuristics that we do not and Java is a verbose language; however, we suggest that much of the difference is because Formulog is a better fit for encoding the logic of the analysis than an imperative, object-oriented language like Java. The relative concision of Formulog matches the results reported by previous work on Datalog-based static analysis, which found that Datalog-based analyses can be orders of magnitude more concise than counterparts written in more traditional languages [Whaley et al. 2005]. The ML fragment of Formulog also helps it be concise, since ML expressions — through supporting sequenced, nested, and scoped computation — can encode logic that would be more verbose to write in Datalog.

We have shown that three diverse case studies can be naturally encoded in Formulog, suggesting that its design is a good match for a range of SMT-based analyses. However, not all analysis logic can be easily encoded in Formulog. There is currently no way to join facts, a useful operation for abstract interpretation-based analyses [Cousot and Cousot 1977]. The restriction to stratified negation is sometimes too severe: For example, one Dminor rule for the type synthesis relation `synth` is not directly expressible in Formulog, because it is defined in terms of the negation of the type well formedness relation, which is in turn defined using the relation `synth`.[12] Finally, given its lack of mutable state, Formulog is probably not a good fit for analyses that can most naturally be specified in an imperative manner, such as lazy abstraction model checking [Henzinger et al. 2002].

Because Formulog is designed to be compatible with Datalog, we can expand the type of analysis logic it supports by taking advantage of research on Datalog extensions. For instance, lattice-based recursive aggregation [Madsen et al. 2016; Szabó et al. 2018] would make it possible to join facts, and local stratification [Przymusinski 1988] would support the Dminor logic we previously cited.

Formulog provides a rich and flexible language of formulas that supports the type of logic-based reasoning found in SMT-based analyses. The formula fragment of Formulog makes it possible to use formulas the way they need to be used by static analyses. A good example of this is the decision to reify logical formulas as terms, a departure from the approach taken by constraint logic programming [Jaffar and Lassez 1987; Jaffar and Maher 1994] and constrained Horn clause (CHC) solving [Bjørner et al. 2015; Grebenshchikov et al. 2012; Gurfinkel et al. 2015; Hoder and Bjørner 2012], the two major previous paradigms for combining logic programming and constraint solving. In these systems, constraints are represented as predicates, not terms, and an inference is made if the constraints in the body of a rule are satisfiable. This approach makes sense in the

[12] To get around this, our implementation uses a less precise rule that drops the negated premise.

context of programming with *constraints*; however, it seems overly restrictive in the context of programming with *formulas*, which do not necessarily have to be used directly as constraints. For example, analyses like our Dminor type checker need to check the validity of a formula, which is the unsatisfiability of its negation. Checking validity does not easily fit in constraint-based paradigms, since constraint programming is built around satisfiability. Similarly, we might want to write an analysis that uses Craig interpolants [Craig 1957]. One could imagine extending Formulog's SMT interface to include an operator `interpolate` that takes two formulas and returns a third (optional) formula, the interpolant; it is not clear how to do this in one of the constraint-based paradigms.

Our treatment of formula variables through the constructor $\#\{e\}[t]$ provides further evidence. This mechanism makes it easy to identify a formula variable with an object-level construct (e.g., a variable in the input program) by choosing for e the expression representing that construct. It also makes it easy to create a variable that is guaranteed to be fresh relative to a set of constructs (e.g., fresh with respect to an environment), an extremely useful operation. This is done by choosing for e a tuple of the constructs that the variable needs to be fresh with respect to. We use this trick in both the Dminor type checker and the symbolic evaluator. Crucially, this freshness mechanism is deterministic, which means that we can safely rewrite Formulog programs and parallelize them. The logic programming language Calypso [Aiken et al. 2007; Hackett 2010] provides a similar mechanism, except that it requires that all the variables in a formula are identified by terms with the same type; this severely limits its usability and is too restrictive for our case studies.

Our case studies exercise a range of the SMT-LIB standard and demonstrate the richness of our formula language. The case studies variously use algebraic data types and uninterpreted functions (the Dminor type checker and the bottom-up points-to analysis); bit vectors and arrays (the Dminor type checker and the symbolic evaluator); and integers, uninterpreted sorts, and quantifiers (the Dminor type checker). It is easy to extend Formulog with additional theories (by adding new constructors) and different types of logical reasoning (by adding new operators, like `interpolate`). As Formulog so loosely couples Datalog evaluation and constraint solving, it is easy to swap in new solver backends without major changes to the Formulog runtime; our prototype currently supports Z3 [de Moura and Bjørner 2008], CVC4 [Barrett et al. 2011], and Yices 2 [Dutertre 2014].

The design of Formulog makes it possible to advantageously apply Datalog-style optimizations to SMT-based analyses, with the result that Formulog programs can compete with analyses written in more mature languages. All of our case study implementations benefit from automatic parallelization: this scales our Dminor type checker and symbolic evaluator over the reference implementations, and helps our bottom-up points-to analysis be reasonably performant. The points-to analysis and symbolic evaluator also demonstrate the potential of the magic set transformation, as we have used it to derive demand-driven versions of these SMT-based analyses. While these types of optimizations could be added by hand to the reference implementations we compare against, the point is that the design of Formulog means that Formulog-based analyses get these optimizations for free, without the explicit effort of the analysis designer. Moreover, because of Formulog's close affinity to Datalog, a Formulog runtime can be augmented with additional Datalog-style optimizations. For instance, a Formulog runtime could use an incremental Datalog evaluation algorithm, which efficiently evaluates Datalog programs while facts are added or retracted from EDB relations [Gupta et al. 1993; Szabó et al. 2018]. This would be helpful for using SMT-based analyses in situations where the code under analysis changes, such as in IDEs or rapidly evolving codebases.

It speaks to the design of Formulog that the high-level optimizations it enables can, in many cases, make up for the naivety of our prototype runtime. Nonetheless, we are optimistic that significantly better performance can be achieved with a sophisticated backend. As we have designed Formulog to be close to Datalog, we can take advantage of many of the optimizations that have helped Datalog

systems scale. For example, since we maintain the range restriction (which entails that every derived fact is ground), we can use concurrent data structures specialized for Datalog evaluation [Jordan et al. 2019]; since Formulog can be evaluated using standard semi-naive evaluation, we can compile Formulog programs to C++ following Soufflé's strategy [Jordan et al. 2016].

The ML fragment is an integral part of Formulog and has a substantial impact on its usability. As discussed in Section 3.2, the first-order fragment of ML we use can be translated in a pretty straightforward way to Datalog rules, and hence can be thought of as syntactic sugar. Despite this, the ML fragment is an integral part of the Formulog programming experience. First, it improves the ergonomics of Formulog, by making it more natural to manipulate complex terms. In particular, pattern matching and let expressions provide a structured way to reflect on complex terms and sequence computation on them; this same effect is not always as easy to achieve in Datalog rules. Second, it helps Formulog achieve its design goal of allowing SMT-based analyses to be implemented in a style close to their specification, since formal specifications often involve functions in addition to inference rules. Third, it improves the performance of Formulog, as there is more overhead involved with evaluating Datalog rules than evaluating an ML expression. A substantial amount of our case study code is in the ML fragment: To give rough estimates, 65% of the Dminor type checker, 30% of the bottom-up points-to analysis, and 40% of the symbolic evaluator are in the ML fragment. Typically, the case studies use Horn clauses to define the overall structure of the analysis, and ML functions for structuring lower-level control flow, mirroring the use of judgments and helper functions in analysis specifications.

The limitation to first-order ML has several advantages. From a theoretical perspective, it means that there is an easy translation from it to Datalog rules, which allows us to give the standard Herbrand model-based semantics to Formulog programs. From a practical perspective, it ensures that we never have to unify functions, which would require higher-order unification. The specifications of our case studies did not make heavy use of higher-order functions, so they were not much missed. However, a future version of Formulog could allow a limited use of higher-order functions (for example, those programs that can be compiled to the first-order fragment).

7 RELATED WORK

Datalog-based frameworks and domain-specific languages for static analysis. A variety of static analysis frameworks have been developed based on more-or-less standard Datalog, such as bddbddb [Whaley et al. 2005], Chord [Naik 2011], Doop [Bravenboer and Smaragdakis 2009], QL [Avgustinov et al. 2016], and Soufflé [Scholz et al. 2016]. Recent work has explored synthesizing Datalog-based analyses [Albarghouthi et al. 2017; Raghothaman et al. 2019]. Flix [Madsen et al. 2016] and IncA [Szabó et al. 2018] extend Datalog for analyses that operate over lattices besides the powerset lattice. IncA supports incremental evaluation, while Flix (like Formulog) includes algebraic data types and a pure functional language. Dataflow analysis is used as a case study for Datafun, a language combining Datalog and higher-order functional programming [Arntzenius and Krishnaswami 2016]. It might be possible to encode something like Formulog in Datafun; however, although it has recently been shown that Datafun can be evaluated using semi-naive evaluation [Arntzenius and Krishnaswami 2020], it is not clear to what extent other Datalog optimizations can be applied to Datafun programs. By combining Datalog with functional programming, Formulog, Flix, and Datafun are related to functional logic programming [Antoy and Hanus 2010]. The functional fragment of Formulog is less expressive than what is typically found in such languages, as Formulog functions are not first-class values and not higher-order.

Logic programming with constraints and formulas. The two dominant prior paradigms for combining logic programming and constraint solving are constraint logic programming (CLP) [Jaffar and

Lassez 1987; Jaffar and Maher 1994] and constrained Horn clause (CHC) solving [Bjørner et al. 2015; Grebenshchikov et al. 2012; Gurfinkel et al. 2015; Hoder and Bjørner 2012]. As discussed in Section 6, these systems typically encode constraints as predicates, not terms, and thus support programming with constraints as things to be satisfied, rather than programming with formulas, which can be manipulated in more interesting ways (e.g., validity checking). In the context of static analysis, these systems have been used primarily for model checking, where a model of the input system is encoded using Horn clauses [Bjørner et al. 2015; Delzanno and Podelski 1999; Flanagan 2004; Fribourg and Richardson 1996; Grebenshchikov et al. 2012]. The rules depend on the program being analyzed, and the solutions to these rules reveal properties of the model; e.g., SeaHorn [Gurfinkel et al. 2015] checks programs by solving a CHC representation of their verification conditions. This differs than the approach taken in this paper, where the rules encode an analysis independent of the input program. The Datalog mode of μZ [Hoder et al. 2011] can be thought of as a bottom-up CLP system with special support for abstract interpretation.

A few existing logic programming systems support programming with formulas (vs constraints); we would argue that none do so with the same richness and flexibility as Formulog. Codish et al. [2008] extend Prolog with an interface to a SAT solver. SICStus Prolog [Carlsson and Mildner 2012], with its CLP extensions, has been used to write model checkers [Delzanno and Podelski 1999; Fribourg and Richardson 1996; Grebenshchikov et al. 2012; Podelski and Rybalchenko 2007]; these implementations typically rely on Prolog's non-logical features, like `assert`, making it harder to apply high-level optimizations like parallelization. Calypso [Aiken et al. 2007; Hackett 2010] is a Datalog variant that interfaces with external constraint solvers and has specialized support for bottom-up analyses. Calypso has been used with SAT and integer constraint solvers; in theory, it could be connected to an SMT solver. However, Formulog offers several advantages over Calypso for SMT-based analyses. First, Formulog's approach to constructing formulas (via complex terms) and manipulating them (via its ML fragment) scales to the complex and heterogeneous formulas that arise in the SMT context, whereas Calypso's approach to formulas (opaque terms, constructed via predicates) would be cumbersome in this setting. Second, Formulog's type system supports the construction of expressive (and safe) formulas involving user-defined terms such as algebraic data types and uninterpreted functions. Third, the ML fragment of Formulog goes a long way towards making it practical for SMT-based analyses, by closing the gap between specification and implementation, and improving ergonomics and performance.

The logic programming language λProlog provides a natural way to represent logical formulas using a form of higher-order abstract syntax based on λ-terms and higher-order unification [Miller and Nadathur 1987; Pfenning and Elliott 1988]. Although this representation simplifies some aspects of using formulas, moving to a higher-order setting would complicate Formulog, widen the gap between Formulog and other Datalog variants, and potentially be an impediment to building a performant and scalable Formulog implementation. Answer set programming (ASP) uses specialized solvers to find a *stable model* (if it exists) of a set of Horn clauses [Brewka et al. 2011; Gelfond and Lifschitz 1988]. Common extensions support constraints on the shape of the stable model that will be found. ASP enables concise encoding of classic NP-complete constraint problems such as graph k-coloring, but it is not obviously applicable to static analysis problems.

Type system engineering. PLT Redex [Felleisen et al. 2009] and Spoofax [Kats and Visser 2010] support exploratory type system engineering. PLT Redex supports a notion of judgment modeled explicitly on inference rules. Spoofax's type engineering framework, Statix, uses a logic programming syntax to specify type systems, with a custom solver for resolving the binding information in scope graphs simultaneously with solving typing constraints [van Antwerpen et al. 2018]. Both of these

systems use custom approaches to finding typing derivations; neither supports SMT queries, but Statix's custom solver can resolve constraint systems that might not always terminate in Formulog.

Solver-aided languages. Scala^{Z3} [Köksal et al. 2011] supports mixed computations combining normal Scala evaluation and Z3 solving; we avoid this level of integration. Smten [Uhler and Dave 2013] is a solver-aided language that supports both concrete and symbolic evaluation; Rosette [Torlak and Bodik 2013] is a framework for creating solver-aided languages that have this property.

8 CONCLUSION

Formulog is a domain-specific language for writing SMT-based static analyses that judiciously combines Datalog, ML, and SMT solving (via an external SMT solver). As demonstrated by our case studies, it makes it possible to concisely implement a range of SMT-based analyses — refinement type checking, bottom-up points-to analysis, and symbolic evaluation — in a way close to their formal specifications, while also making it possible to automatically and advantageously apply high-level optimizations to these analyses like parallelization and goal-directed rewriting.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. nnnnnnn and Grant No. mmmmmmm. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

Alex Aiken, Suhabe Bugrara, Isil Dillig, Thomas Dillig, Brian Hackett, and Peter Hawkins. 2007. An Overview of the Saturn Project. In *Proceedings of the 7th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering*. 43–48.

Aws Albarghouthi, Paraschos Koutris, Mayur Naik, and Calvin Smith. 2017. Constraint-Based Synthesis of Datalog Programs. In *Proceedings of the 23rd International Conference on Principles and Practice of Constraint Programming*. 689–706.

Sergio Antoy and Michael Hanus. 2010. Functional Logic Programming. *Commun. ACM* 53, 4 (2010), 74–85.

Krzysztof R Apt, Howard A Blair, and Adrian Walker. 1988. Towards a Theory of Declarative Knowledge. In *Foundations of Deductive Databases and Logic Programming*. Elsevier, 89–148.

Molham Aref, Balder ten Cate, Todd J Green, Benny Kimelfeld, Dan Olteanu, Emir Pasalic, Todd L Veldhuizen, and Geoffrey Washburn. 2015. Design and Implementation of the LogicBlox System. In *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data*. 1371–1382.

Michael Arntzenius and Neel Krishnaswami. 2020. Seminäive Evaluation for a Higher-Order Functional Language. *Proceedings of the ACM on Programming Languages* 4, POPL (2020), 22:1–22:28.

Michael Arntzenius and Neelakantan R. Krishnaswami. 2016. Datafun: A Functional Datalog. In *Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming*. 214–227.

Pavel Avgustinov, Oege De Moor, Michael Peyton Jones, and Max Schäfer. 2016. QL: Object-Oriented Queries on Relational Data. In *Proceedings of the 30th European Conference on Object-Oriented Programming*. 2:1–2:25.

Francois Bancilhon. 1986. Naive Evaluation of Recursively Defined Relations. In *On Knowledge Base Management Systems*. Springer, 165–178.

Francois Bancilhon, David Maier, Yehoshua Sagiv, and Jeffrey D Ullman. 1985. Magic Sets and Other Strange Ways to Implement Logic Programs. In *Proceedings of the Fifth ACM SIGACT-SIGMOD Symposium on Principles of Database Systems*. 1–15.

Clark Barrett, Christopher L. Conway, Morgan Deters, Liana Hadarean, Dejan Jovanović, Tim King, Andrew Reynolds, and Cesare Tinelli. 2011. CVC4. In *Proceedings of the 23rd International Conference on Computer Aided Verification*. 171–177.

Clark Barrett, Pascal Fontaine, and Cesare Tinelli. 2017. *The SMT-LIB Standard: Version 2.6*. Technical Report. Department of Computer Science, The University of Iowa.

Catriel Beeri and Raghu Ramakrishnan. 1991. On the Power of Magic. *The Journal of Logic Programming* 10, 3-4 (1991), 255–299.

Gavin M. Bierman, Andrew D. Gordon, Cătălin Hriţcu, and David Langworthy. 2012. Semantic Subtyping with an SMT Solver. *Journal of Functional Programming* 22, 1 (2012), 31–105.

Nikolaj Bjørner, Arie Gurfinkel, Ken McMillan, and Andrey Rybalchenko. 2015. Horn Clause Solvers for Program Verification. In *Fields of Logic and Computation II*. Springer, 24–51.

Martin Bravenboer and Yannis Smaragdakis. 2009. Strictly Declarative Specification of Sophisticated Points-to Analyses. In *Proceedings of the 24th ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications*. 243–262.

Gerhard Brewka, Thomas Eiter, and Mirosław Truszczyński. 2011. Answer Set Programming at a Glance. *Commun. ACM* 54, 12 (2011), 92–103.

Cristian Cadar, Daniel Dunbar, and Dawson Engler. 2008. KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs. In *Proceedings of the 8th USENIX Conference on Operating Systems Design and Implementation*. 209–224.

Cristian Cadar and Koushik Sen. 2013. Symbolic Execution for Software Testing: Three Decades Later. *Commun. ACM* 56, 2 (Feb. 2013), 82–90.

Mats Carlsson and Per Mildner. 2012. SICStus Prolog–The First 25 years. *Theory and Practice of Logic Programming* 12, 1-2 (2012), 35–66.

Alessandro Cimatti and Alberto Griggio. 2012. Software Model Checking via IC3. In *Proceedings of the 24th International Conference on Computer Aided Verification*. 277–293.

Edmund Clarke, Daniel Kroening, and Flavio Lerda. 2004. A Tool for Checking ANSI-C Programs. In *Proceedings of the 10th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. 168–176.

Michael Codish, Vitaly Lagoon, and Peter J Stuckey. 2008. Logic Programming with Satisfiability. *Theory and Practice of Logic Programming* 8, 1 (2008), 121–128.

Patrick Cousot and Radhia Cousot. 1977. Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. In *Proceedings of the 4th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*. 238–252.

William Craig. 1957. Three Uses of the Herbrand-Gentzen Theorem in Relating Model Theory and Proof Theory. *The Journal of Symbolic Logic* 22, 3 (1957), 269–285.

Luis Damas and Robin Milner. 1982. Principal Type-Schemes for Functional Programs. In *Proceedings of the 9th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. 207–212.

Leonardo de Moura and Nikolaj Bjørner. 2008. Z3: An Efficient SMT Solver. In *Proceedings of the 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. 337–340.

Giorgio Delzanno and Andreas Podelski. 1999. Model Checking in CLP. In *Proceedings of the 5th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. 223–239.

David Detlefs, Greg Nelson, and James B. Saxe. 2005. Simplify: A Theorem Prover for Program Checking. *J. ACM* 52, 3 (2005), 365–473.

Bruno Dutertre. 2014. Yices 2.2. In *Proceedings of the 26th International Conference on Computer Aided Verification*. 737–744.

Matthias Felleisen, Robert Bruce Findler, and Matthew Flatt. 2009. *Semantics Engineering with PLT Redex* (1st ed.). The MIT Press.

Yu Feng, Xinyu Wang, Isil Dillig, and Thomas Dillig. 2015. Bottom-up Context-Sensitive Pointer Analysis for Java. In *Proceedings of the 13th Asian Symposium on Programming Languages and Systems*. 465–484.

Cormac Flanagan. 2004. Automatic Software Model Checking via Constraint Logic. *Science of Computer Programming* 50, 1-3 (2004), 253–270.

Antonio Flores-Montoya and Eric Schulte. 2019. Datalog Disassembly. arXiv:arXiv:1906.03969

Laurent Fribourg and Julian Richardson. 1996. Symbolic Verification with Gap-Order Constraints. In *Proceedings of the 6th International Workshop on Logic Programming Synthesis and Transformation*. 20–37.

Hervé Gallaire and Jack Minker (Eds.). 1978. *Logic and Data Bases*. Plenum Press.

Michael Gelfond and Vladimir Lifschitz. 1988. The Stable Model Semantics for Logic Programming. In *Proceedings of the 5th International Conference and Symposium on Logic Programming*. 1070–1080.

Sergey Grebenshchikov, Nuno Lopes, Corneliu Popeea, and Andrey Rybalchenko. 2012. Synthesizing Software Verifiers from Proof Rules. In *Proceedings of the 33rd ACM SIGPLAN Conference on Programming Language Design and Implementation*. 405–416.

Neville Grech, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. 2019. Gigahorse: Thorough, Declarative Decompilation of Smart Contracts. In *Proceedings of the 41st International Conference on Software Engineering*. 1176–1186.

Neville Grech, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. 2018. Madmax: Surviving Out-of-Gas Conditions in Ethereum Smart Contracts. *Proceedings of the ACM on Programming Languages* 2, OOPSLA (2018), 116:1–116:27.

Todd J. Green, Shan Shan Huang, Boon Thau Loo, and Wenchao Zhou. 2013. Datalog and Recursive Query Processing. *Foundations and Trends in Databases* 5, 2 (2013), 105–195.

Salvatore Guarnieri and V Benjamin Livshits. 2009. GATEKEEPER: Mostly Static Enforcement of Security and Reliability Policies for JavaScript Code. In *Proceedings of the 18th USENIX Security Symposium*. 78–85.

Ashish Gupta, Inderpal Singh Mumick, and Venkatramanan Siva Subrahmanian. 1993. Maintaining Views Incrementally. *ACM SIGMOD Record* 22, 2 (1993), 157–166.

Arie Gurfinkel, Temesghen Kahsai, Anvesh Komuravelli, and Jorge A Navas. 2015. The SeaHorn Verification Framework. In *Proceedings of the 27th International Conference on Computer Aided Verification*. 343–361.

Brian Hackett. 2010. *Type Safety in the Linux Kernel*. Ph.D. Dissertation. Stanford University.

Thomas A. Henzinger, Ranjit Jhala, Rupak Majumdar, and Grégoire Sutre. 2002. Lazy Abstraction. In *Proceedings of the 29th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. 58–70.

Roger Hindley. 1969. The Principal Type-Scheme of an Object in Combinatory Logic. *Trans. Amer. Math. Soc.* 146 (1969), 29–60.

Kryštof Hoder and Nikolaj Bjørner. 2012. Generalized Property Directed Reachability. In *Proceedings of the 15th International Conference on Theory and Applications of Satisfiability Testing*. Springer, 157–171.

Kryštof Hoder, Nikolaj Bjørner, and Leonardo De Moura. 2011. μZ–An Efficient Engine for Fixed Points with Constraints. In *Proceedings of the 23rd International Conference on Computer Aided Verification*. 457–462.

Joxan Jaffar and Jean-Louis Lassez. 1987. Constraint Logic Programming. In *Proceedings of the 14th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*. 111–119.

Joxan Jaffar and Michael J. Maher. 1994. Constraint Logic Programming: A Survey. *The Journal of Logic Programming* 19 (1994), 503–581.

Herbert Jordan, Bernhard Scholz, and Pavle Subotić. 2016. Soufflé: On Synthesis of Program Analyzers. In *Proceedings of the 28th International Conference on Computer Aided Verification*. 422–430.

Herbert Jordan, Pavle Subotic, David Zhao, and Bernhard Scholz. 2019. A Specialized B-tree for Concurrent Datalog Evaluation. In *Proceedings of the 24th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*. 327–339.

Lennart C.L. Kats and Eelco Visser. 2010. The Spoofax Language Workbench: Rules for Declarative Specification of Languages and IDEs. In *Proceedings of the 25th ACM International Conference on Object-Oriented Programming, Systems, Languages, and Applications*. 444–463.

James C. King. 1976. Symbolic Execution and Program Testing. *Commun. ACM* 19, 7 (1976), 385–394.

Ali Sinan Köksal, Viktor Kuncak, and Philippe Suter. 2011. Scala to the Power of Z3: Integrating SMT and Programming. In *Proceedings of the 23rd International Conference on Automated Deduction*. 400–406.

Robert Kowalski. 1979. Algorithm = Logic + Control. *Commun. ACM* 22, 7 (1979), 424–436.

Chris Lattner and Vikram Adve. 2004. LLVM: A Compilation Framework for Lifelong Program Analysis & Transformation. In *Proceedings of the 2nd IEEE/ACM International Symposium on Code Generation and Optimization*. 75–88.

Chin Soon Lee, Neil D. Jones, and Amir M. Ben-Amram. 2001. The Size-Change Principle for Program Termination. In *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. 81–92.

V. Benjamin Livshits and Monica S. Lam. 2005. Finding Security Vulnerabilities in Java Applications with Static Analysis. In *Proceedings of the 14th USENIX Security Symposium*. 271–286.

Magnus Madsen, Ming-Ho Yee, and Ondřej Lhoták. 2016. From Datalog to Flix: a Declarative Language for Fixed Points on Lattices. In *Proceedings of the 37th ACM SIGPLAN Conference on Programming Language Design and Implementation*. 194–208.

Kenneth L McMillan. 2006. Lazy Abstraction with Interpolants. In *Proceedings of the 18th International Conference on Computer Aided Verification*. Springer, 123–136.

Michael Meskes and Jörg Noack. 1993. The Generalized Supplementary Magic-Sets Transformation for Stratified Datalog. *Inform. Process. Lett.* 47, 1 (1993), 31–41.

Dale Miller and Gopalan Nadathur. 1987. A Logic Programming Approach to Manipulating Formulas and Programs. In *Proceedings of the 1987 Symposium on Logic Programming*. 379–388.

Inderpal Singh Mumick, Hamid Pirahesh, and Raghu Ramakrishnan. 1990. The Magic of Duplicates and Aggregates. In *Proceedings of the 16th International Conference on Very Large Data Bases*. 264–277.

Mayur Naik. 2011. Chord: A Program Analysis Platform for Java. https://www.seas.upenn.edu/~mhnaik/chord/user_guide/index.html. Accessed: 2020-04-01.

Frank Pfenning and Conal Elliott. 1988. Higher-Order Abstract Syntax. In *Proceedings of the ACM SIGPLAN 1988 Conference on Programming Language Design and Implementation*. 199–208.

Andreas Podelski and Andrey Rybalchenko. 2007. ARMC: The Logical Choice for Software Model Checking with Abstraction Refinement. In *Proceedings of the 9th International Symposium on Practical Aspects of Declarative Languages*. 245–259.

Teodor C Przymusinski. 1988. On the Declarative Semantics of Deductive Databases and Logic Programs. In *Foundations of Deductive Databases and Logic Programming*. Elsevier, 193–216.

Mukund Raghothaman, Jonathan Mendelson, David Zhao, Mayur Naik, and Bernhard Scholz. 2019. Provenance-Guided Synthesis of Datalog Programs. *Proceedings of the ACM on Programming Languages* 4, POPL (2019), 1–27.

Thomas W. Reps. 1995. Demand Interprocedural Program Analysis Using Logic Databases. In *Proceedings of the 3rd ACM SIGSOFT Symposium on Foundations of Software Engineering*. 163–196.

Patrick M. Rondon, Ming Kawaguci, and Ranjit Jhala. 2008. Liquid Types. In *Proceedings of the 29th ACM SIGPLAN Conference on Programming Language Design and Implementation*. 159–169.

Bernhard Scholz, Herbert Jordan, Pavle Subotić, and Till Westmann. 2016. On Fast Large-Scale Program Analysis in Datalog. In *Proceedings of the 25th International Conference on Compiler Construction*. 196–206.

Yannis Smaragdakis and Martin Bravenboer. 2011. Using Datalog for Fast and Easy Program Analysis. In *Datalog Reloaded*. Springer, 245–251.

Tamás Szabó, Gábor Bergmann, Sebastian Erdweg, and Markus Voelter. 2018. Incrementalizing Lattice-Based Program Analyses in Datalog. *Proceedings of the ACM on Programming Languages* 2, OOPSLA (2018), 139:1–139:29.

Emina Torlak and Rastislav Bodik. 2013. Growing Solver-Aided Languages with Rosette. In *Proceedings of the 2013 ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming & Software*. 135–152.

Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Buenzli, and Martin Vechev. 2018. Securify: Practical Security Analysis of Smart Contracts. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 67–82.

Richard Uhler and Nirav Dave. 2013. Smten: Automatic Translation of High-Level Symbolic Computations into SMT Queries. In *Proceedings of the 25th International Conference on Computer Aided Verification*. 678–683.

Hendrik van Antwerpen, Casper Bach Poulsen, Arjen Rouvoet, and Eelco Visser. 2018. Scopes as Types. *Proceedings of the ACM on Programming Languages* 2, OOPSLA (2018), 114:1–114:30.

Allen Van Gelder. 1989. Negation as Failure Using Tight Derivations for General Logic Programs. *The Journal of Logic Programming* 6, 1-2 (1989), 109–133.

Mark Weiser. 1984. Program Slicing. *IEEE Transactions on Software Engineering* 4 (1984), 352–357.

John Whaley, Dzintars Avots, Michael Carbin, and Monica S. Lam. 2005. Using Datalog with Binary Decision Diagrams for Program Analysis. In *Proceedings of the Third Asian Symposium on Programming Languages and Systems*. 97–118.

John Whaley and Monica S. Lam. 2004. Cloning-Based Context-Sensitive Pointer Alias Analysis Using Binary Decision Diagrams. In *Proceedings of the ACM SIGPLAN 2004 Conference on Programming Language Design and Implementation*. 131–144.

Types			
Types	τ	::=	$t \mid t\ \mathsf{smt} \mid t\ \mathsf{sym} \mid \mathsf{model}$
Pre-types	t	::=	$B \mid D\ \vec{\tau} \mid \alpha$
Base types	B	::=	$\mathsf{bool} \mid \mathsf{bv[k]}_{k \in \mathbb{N}^+} \mid \ldots$
Contexts			
Data type declarations	Δ	::=	$\cdot \mid \Delta, D : \forall \vec{\alpha_i}.\ \{\overrightarrow{c_j : \vec{\tau_k}}\}$
Program declarations	Φ	::=	$\cdot \mid \Phi, f : \forall \vec{\alpha}, \vec{\tau} \to \tau \mid \Phi, uf : \vec{t} \to t \mid \Phi, p \subseteq \vec{\tau}$
Variable contexts	Γ	::=	$\cdot \mid \Gamma, x : \tau \mid \Gamma, \alpha$
Terms			
Programs	prog	::=	$\vec{F_i}\ \vec{H_j}$
Functions	F	::=	$\mathsf{fun}\ f(\vec{X_i} : \vec{\tau_i}) : \tau = e$
Horn clauses	H	::=	$p(\vec{X_i})\ \mathsf{:-}\ \vec{P_j}$
Premises	P	::=	$A \mid \mathsf{!}A$
Atoms	A	::=	$p(\vec{e_i}) \mid X = e$
Expressions	e	::=	$k \mid X \mid c(\vec{e_i}) \mid f(\vec{e_i}) \mid p(\vec{e_i}) \mid \otimes(\vec{e_i}) \mid \texttt{`}\phi\texttt{`}$
			$\mathsf{let}\ X = e_1\ \mathsf{in}\ e_2 \mid \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 \mid$
			$\mathsf{match}\ e\ \mathsf{with}\ \overrightarrow{c_i(\vec{X_j}) \to e_i}$
SMT formulas	ϕ	::=	$c^{\mathsf{SMT}}_{\mathsf{var}}[x,t]() \mid c^{\mathsf{SMT}}_{\mathsf{const}}[k]() \mid c^{\mathsf{SMT}}_{\mathsf{let}}(\phi_1,\phi_2,\phi_3) \mid$
			$c^{\mathsf{SMT}}_{\mathsf{ctor}}[c](\vec{\phi_i}) \mid c^{\mathsf{SMT}}_{\mathsf{forall}}(\phi_1,\phi_2) \mid c^{\mathsf{SMT}}_{\mathsf{uf}}[uf](\vec{\phi_i}) \mid \mathsf{,}e$
Constants	k	::=	$\mathsf{true} \mid \mathsf{false} \mid 0 \mid 1 \mid \ldots$
Namespaces			
Type modes	m	::=	$\mathsf{exp} \mid \mathsf{smt}$
Data type names	D	$\in$	ADTVar
Type variables	α	$\in$	TVar
Constructors	c	$\in$	CtorVar
Formulog variables	X	$\in$	Var
SMT variables	x	$\in$	SMTVar
Predicates	p	$\in$	PredVar
Functions	f	$\in$	FunVar
Uninterpreted functions	uf	$\in$	UninterpFunVar

Fig. 14. Syntax of Formulog's formal model

A FORMULOG'S FORMAL MODEL

We define a 'middleweight' formal model of Formulog, designing a type system (Section B) and an operational semantics (Section C), relating the two in a proof of type safety (Section D).

Our model characterizes Formulog as a two-level system (Figure 14), comprising Datalog-esque Horn clauses H and first-order functions F; Horn clause "rules" are made up of premises P, where each premise is a series of (possibly negated) atoms A. Each atom A either references a Datalog predicate or binds a variable to an expression e. Expressions themselves have two mutually recursive

modes: ordinary functional computation e and quoted SMT terms `$\phi$`, which can include unquoted expressions ,e.

The Datalog fragment of Formulog is fairly standard syntactically, up to the addition of the atomic form $X = e$. We constrain premises to a sort of administrative normal form: predicate references apply only to variables, written $p(\vec{X}_i)$, and expression constraints bind variables, as in $Y = e$. Our implementation can handle compound premises like $p(e_1, e_2)$; our formal model would require rewriting such a premise to three premises: $p(X, Y)$, $X = e_1$, and $Y = e_2$ (for some fresh X and Y).

The functional programming fragment fully annotates the types on its functions F; variable names in both fragments are written in capital letters. (Our implementation merely demands that the first letter be capitalized.) SMT variables are written using lowercase letters and annotated with their type, as in $c^{\text{SMT}}_{\text{var}}[x, t]()$. As described in Section 3.3, our implementation allows any value to be used as the name of an SMT variable; here, without loss of generality, we treat SMT variables as being drawn from a distinct universe. Code in the functional fragment can treat Datalog relations as predicates, i.e., $p(\vec{v}_i)$ returns true when $\vec{v}_i \in p$. In our implementation, some elements of $\vec{v}_i$ can be the wildcard ??, turning a Datalog predicate into a list. For example, if $p \subseteq \text{bool} \times \text{bv}[32]$, then: $p(\text{true}, 42)$ yields a bool; $p(??, 42)$ returns a list of bools b such that $p(b, 42)$ holds; $p(\text{true}, ??)$ returns a list of bv[32]s n such that $p(\text{true}, n)$ holds; $p(??, ??)$ returns a list of bool $\times$ bv[32], i.e., the relation p. We don't include this behavior in our formal model.

The set of available base types B must include bool at a minimum; any other SMT-embeddable base types are acceptable, e.g., k-width bit vectors for a statically known k.

As a matter of notation, we write $\vec{e}_i$ for a metavariable e to mean a possibly empty sequence of es, indexed by i. When more than one variable shares the same index, we mean that those sequences must be of the same length (e.g., in the match syntax, each branch of a match is a triple of a constructor c, a vector of variable names for c's arguments, and a corresponding single expression).

B FORMULOG'S TYPE SYSTEM

We begin by presenting type checking rules for Formulog (Figures 15, 16, 17, and 18). Our *implementation* of Formulog not only performs type checking, but can also perform type inference, e.g., automatically finding type variable substitutions.

Our types are broken into two levels: types τ and pre-types t. Every pre-type t can be directly considered as a type, but there are two additional types: t smt, the type of SMT formulas yielding t, and t sym, the type of SMT variables of type t. We factor the syntax in this way to prevent anomalies like bool smt smt, which would mean SMT formulas that yield SMT formulas that yield booleans. It is *not* the case, however, that every pre-type t is necessarily representable as an SMT type, because data types may contain SMT formulas as arguments; we discuss how we categorize SMT-representable types shortly.

Before we begin, some further notational clarification. Rules are named by their primary subjects followed by a hyphen and a descriptive name. Whenever we use indices in rules, we will always map (stating a single premise in terms of the index, e.g., prog-WF) or fold (stating first, indexed, and last, e.g., $\vec{X}\vec{\tau}$-All) over the sequence. We omit the indices when selecting an element of a sequence or set (as in, e.g., e-Match in Figure 17).

All of our typing rules are in terms of a fixed set of data type declarations Δ and program declarations Φ (Figure 14). Data type declarations Δ map data type names D to some number of type arguments $\vec{\alpha}_i$ and a set of constructors $\vec{c}_j$, each of which takes some number of arguments of type $\vec{\tau}_k$; each c_j can have a different number of arguments. Program declarations Φ collect the

Type and typing context well formedness $\boxed{\Delta \vdash \Gamma}$ $\boxed{\Delta; \Gamma \vdash_m \tau}$

$$\frac{}{\vdash \cdot}\ \Gamma\text{-Empty} \qquad \frac{\vdash \Gamma \qquad \Gamma \vdash_{\text{exp}} \tau}{\vdash \Gamma, x : \tau}\ \Gamma\text{-Var} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \alpha}\ \Gamma\text{-TVar}$$

$$\frac{}{\Gamma \vdash_m B}\ t\text{-Base} \qquad \frac{\alpha \in \Gamma}{\Gamma \vdash_{\text{exp}} \alpha}\ t\text{-TVar} \qquad \frac{\Delta(D) = \forall \vec{\alpha}_i, \{\dots\} \qquad \Gamma \vdash_m \tau_i}{\Gamma \vdash_m D\ \vec{\tau}_i}\ t\text{-ADT}$$

$$\frac{\Gamma \vdash_{\text{smt}} t}{\Gamma \vdash_m t\ \text{smt}}\ \tau\text{-SMT} \qquad \frac{\Gamma \vdash_{\text{smt}} t}{\Gamma \vdash_m t\ \text{sym}}\ \tau\text{-Sym} \qquad \frac{}{\Gamma \vdash_{\text{exp}} \text{model}}\ \tau\text{-Model}$$

Data type and program signature well formedness $\boxed{\vdash \Delta}$ $\boxed{\vdash \Phi}$

$$\begin{aligned} \vdash \Delta \quad \Leftrightarrow \quad & \forall D : \forall \vec{\alpha}.\ \{c_1 : \vec{\tau}_1, \dots, c_n : \vec{\tau}_n\} \in \Delta \forall i, \\ & (1)\ \forall D' \in \text{dom}(\Delta),\ c_i \in \Delta(D') \Rightarrow D = D' \\ & (2)\ \vec{\alpha} \vdash_{\text{exp}} \tau_i \\ & (3)\ \forall \beta \in \vec{\alpha}, \beta \in \vec{\tau}_i \end{aligned}$$

$$\frac{}{\vdash \cdot}\ \Phi\text{-empty} \qquad \frac{\vdash \Phi \qquad \forall \beta \in \vec{\alpha}_i,\ \beta \in \vec{\tau}_j, \tau \qquad \vec{\alpha}_i \vdash_{\text{exp}} \tau_j \qquad \vec{\alpha}_i \vdash_{\text{exp}} \tau}{\vdash \Phi, f : \forall \vec{\alpha}_i, \vec{\tau}_j \to \tau}\ \Phi\text{-Fun}$$

$$\frac{\vdash \Phi \qquad \cdot \vdash_{\text{exp}} \tau_i}{\vdash \Phi, p \subseteq \vec{\tau}_i}\ \Phi\text{-Rel} \qquad \frac{\vdash \Phi \qquad \cdot \vdash_{\text{smt}} t_i \qquad \cdot \vdash_{\text{smt}} t}{\vdash \Phi, uf : \vec{t}_i \to t}\ \Phi\text{-UFun}$$

Program and function typing $\boxed{\Delta; \Phi \vdash \text{prog}}$

$$\frac{\vdash \Delta \qquad \vdash \Phi \qquad \Delta; \Phi \vdash F_i \qquad \Delta; \Phi \vdash H_j}{\Delta; \Phi \vdash \vec{F}_i\ \vec{H}_j}\ \text{prog-WF}$$

Fig. 15. Type, context, and definition well formedness; top-level program typing

signatures of first-order polymorphic functions $f : \forall \vec{\alpha}, \vec{\tau} \to \tau$, uninterpreted functions for use in the SMT solver $uf : \vec{t} \to t$, and relations $p \subseteq \vec{\tau}_i$.

The highest level typing rule is prog-WF (Figure 15), which ensures that the declarations are well formed and each part of the program is well formed.

The context and type well formedness rules (Figure 15) are mostly straightforward, type well formedness being the most interesting. Each type can be found to be well formed in either SMT mode smt—i.e., it can be exported to the SMT solver–or in expression mode exp, meaning it cannot be. There is a sub-moding relationship: well formed types at smt are also well formed at exp, but not necessarily vice-versa: for example, there is no way to export an SMT formula or variable as the *object* of another SMT formula, only as a constituent. We assume that all Formulog constants are SMT representable, i.e., $\cdot \vdash_{\text{smt}} \text{typeof}(k)$ for all constants k. Data type declarations are polymorphic, but we disallow phantom type variables. Data types can freely mutually recurse. Uninterpreted functions must be in terms of pre-types, and those pre-types must be closed and SMT representable (smt); functions and relations can use any well formed types (exp). Functions can be polymorphic but we disallow phantom type variables; relations have monomorphic types. Disallowing phantom types in constructors and functions and keeping relations monomorphic ensure that these forms are "reverse determinate", i.e., the types of their arguments uniquely determine their types.

Variable binding and typing $\boxed{\Gamma \vdash x, \tau \rhd \Gamma}$ $\boxed{\Gamma \vdash \vec{x}, \vec{\tau} \rhd \Gamma}$

$$\frac{X \notin \mathrm{dom}(\Gamma)}{\Gamma \vdash X, \tau \rhd \Gamma, X{:}\tau}\ X\tau\text{-Bind} \qquad \frac{\Gamma(X) = \tau}{\Gamma \vdash X, \tau \rhd \Gamma}\ X\tau\text{-Check}$$

$$\frac{\Gamma \vdash X_0, \tau_0 \rhd \Gamma_1 \quad \ldots \quad \Gamma_i \vdash X_i, \tau_i \rhd \Gamma_{i+1} \quad \ldots \quad \Gamma_n \vdash X_n, \tau_n \rhd \Gamma'}{\Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'}\ \vec{X}\vec{\tau}\text{-All}$$

Premise typing $\boxed{\Delta; \Phi; \Gamma \vdash P \rhd \Gamma}$

$$\frac{p \subseteq \vec{\tau_i} \in \Phi \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'}{\Gamma \vdash p(\vec{X_i}) \rhd \Gamma'}\ P\text{-PosAtom} \qquad \frac{p \subseteq \vec{\tau_i} \in \Phi \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma}{\Gamma \vdash\ !p(\vec{X_i}) \rhd \Gamma}\ P\text{-NegAtom}$$

$$\frac{\vec{X_i} \not\subseteq \Gamma \qquad \Delta(D) = \forall \vec{\alpha_j}, \{\ldots, c : \vec{\tau_i}, \ldots\} \qquad \Gamma \vdash Y, D\ \vec{\tau'_j} \rhd \Gamma \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i}[\vec{\tau'_j}/\vec{\alpha_j}] \rhd \Gamma'}{\Gamma \vdash Y = c(\vec{X_i}) \rhd \Gamma'}\ P\text{-EqCtor-BF}$$

$$\frac{\vec{X_i} \not\subseteq \Gamma \qquad \Gamma \vdash c^{\mathsf{SMT}}_{c'} : \vec{\tau_i} \to \tau \qquad \Gamma \vdash Y, \tau \rhd \Gamma \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'}{\Gamma \vdash Y = \grave{}\, c^{\mathsf{SMT}}_{c'}(,\vec{X_i})\grave{} \rhd \Gamma'}\ P\text{-EqSMT-BF}$$

$$\frac{\Gamma \vdash e : \tau \qquad \Gamma \vdash Y, \tau \rhd \Gamma'}{\Gamma \vdash Y = e \rhd \Gamma'}\ P\text{-Eq-FB} \qquad \frac{\Gamma \vdash e : \tau \qquad \Gamma \vdash Y, \tau \rhd \Gamma}{\Gamma \vdash\ !(Y = e) \rhd \Gamma}\ P\text{-NegEq}$$

Clause typing $\boxed{\Delta; \Phi \vdash H}$

$$\frac{\cdot \vdash P_0 \rhd \Gamma_1 \quad \ldots \quad \Gamma_j \vdash P_j \rhd \Gamma_{j+1} \quad \ldots \quad \Gamma_n \vdash P_n \rhd \Gamma' \qquad p \subseteq \vec{\tau_i} \in \Phi \qquad \Gamma' \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'}{\vdash p(\vec{X_i}) :\!-\ \vec{P_j}}\ H\text{-Clause}$$

Fig. 16. Typing rules: Horn clauses (rules)

Since the declaration environments Δ and Φ are statically determined for an entire program, we typically leave them *implicit*. Implicit parameters are in gray in the boxed rule schemata in the figures. In proofs we will treat these parameters explicitly, but we conserve space by stating the rules without threading implicit parameters through. For example, the data type declarations Δ are necessary to ensure that t-ADT only allows us to name data types that have actually been defined. Rather than threading Δ through every rule for context and type well formedness, we write Δ in the rule schemata.

The type checking of the Datalog fragment of Formulog (Figure 16) must encode two Datalog invariants in addition to conventional typing constraints: the range restriction, i.e., every variable in the head of a rule appears somewhere in a premise; and appropriate binding, i.e., it is possible to interpret a Horn clause in such a way that all of the variables will be bound at the end. Our formal rules ensure that the program has correct binding structure for a left-to-right evaluation of each

Horn clause. An implementation could determine whether or not an ordering would work and could reorder programs into an appropriate order automatically. Our formal model does not enforce that the dependencies between relations are appropriately stratified, though doing so would be easy: the relation-and-function call graph should not have any "negative" edge in a cycle, where a negative edge is created whenever there is a negated predicate in a rule body or a predicate is invoked as a function.

Concretely, H-Clause ensures that (a) a left-to-right binding order produces some appropriate final context Γ' (via the premise typing judgment), (b) the range restriction is satisfied, ($\vec{X}_i \subseteq \Gamma'$) by making sure that (c) every variable is well typed and bound ($\Gamma' \vdash \vec{X}_i, \vec{\tau}_i \rhd \Gamma'$—having the same Γ' means no new bindings were introduce when checking the head variables).

Premise typing $\Gamma \vdash P \rhd \Gamma$ and variable binding and typing $\Gamma \vdash x, \tau \rhd \Gamma$ work together to generate appropriate types for each premise. Positive references to relations are well formed in binding Γ' according to P-PosAtom when (a) the use is well typed ($p \subseteq \vec{\tau}_i \in \Phi$) and (b) the variables used in the premise yield the binding Γ'. Negative references to relations $!p(\vec{X}_i)$ additionally require that all of the X_i be already bound, i.e., the resulting Γ is the same as the starting one. We split expression equality constraints $Y = e$ into three main cases:

(1) Y is bound and e is a constructor $c(\vec{X}_i)$ where all of $\vec{X}_i$ are unbound (P-EqCtor-BF).
(2) Y is bound and e is a quoted SMT constructor $\texttt{`}c^{\mathsf{SMT}}_{c'}(\texttt{,}\vec{X}_i)\texttt{`}$ where all of $\vec{X}_i$ are unbound (P-EqSMT-BF).
(3) Y is possibly unbound and e has no unbound variables (P-Eq-FB).

It is critical that we avoid the case where both Y and some of the X_i are unbound, in which case we would need to perform true unification (or even higher-order unification, depending on our treatment of functional programs). In the case where Y is bound and the expression has no unbound variables, only the P-Eq-FB case could apply. There is a fourth, irrelevant case: P-NegEq. No binding can possibly occur there, so the constraint is imply checked by running e and making sure it isn't equal to Y.

The binding rules come in three forms: $X\tau$-Bind for adding a new binding, $X\tau$-Check for ensuring that an already bound variable is matched at appropriate type, and a vectorized form $\vec{X}\vec{\tau}$-All for folding over a sequence of such bindings. Note that the resulting bindings are the same, i.e., $\Gamma \vdash X, \tau \rhd \Gamma$, if and only if $X \in \mathrm{dom}(\Gamma)$; the same holds for vectors of variables and types, as well (Lemma E.5).

We split the rules for expressions e and formulas ϕ in two parts (Figures 17 and 18, respectively). Expression typing is conventional for functional languages. We adopt a declarative style for type substitutions (e-Ctor, e-Fun, e-Op, e-Match). Our actual implementation uses Hindley–Damas–Milner type inference [Damas and Milner 1982; Hindley 1969] to find the correct types to use. As to Formulog-specific features, we ensure type well formedness is in exp-mode; the $\texttt{`}\phi\texttt{`}$ expression switches from expression mode to formula mode. Relations $p \subseteq \vec{\tau}_i \in \Phi$ are treated as if they are functions of type $\vec{\tau}_i \to \mathrm{bool}$. Since Datalog predicates can occur in functional terms, we must use the control-flow graph of the program when analyzing for stratification. Consider the following program:

```
fun f(X : bv[32]) : bv[32] = if p(X) then ... else X
p(Y) :- q(Y, Y).
q(A, B) :- r(A), B = f(A).
r(42).
```

Here the relation `q` calls the function `f`, which in turn relies on the negation of the relation `p` (since the behavior of `f` is conditioned on the contents of `p`). As `p` is defined in terms of `q`, this leads to a

Function and expression well formedness $\boxed{\Delta;\Phi \vdash F}$ $\boxed{\Delta;\Phi;\Gamma \vdash e : \tau}$

$$\frac{f : \forall \vec{\alpha}_j, \vec{\tau}_i \to \tau \in \Phi \qquad \vec{\alpha}_j, \overrightarrow{X_i : \tau_i} \vdash e : \tau}{\vdash \mathsf{fun}\ f(\vec{X}_i : \vec{\tau}_i) : \tau = e}\ F\text{-WF}$$

$$\frac{\vdash \Gamma \qquad \Gamma(X) = \tau}{\Gamma \vdash X : \tau}\ e\text{-Var} \qquad \frac{}{\Gamma \vdash k : \mathsf{typeof}(k)}\ e\text{-Const} \qquad \frac{\Gamma \vdash e_1 : \tau_1 \qquad \Gamma, X : \tau_1 \vdash e_2 : \tau_2}{\Gamma \vdash \mathsf{let}\ X = e_1\ \mathsf{in}\ e_2 : \tau_2}\ e\text{-Let}$$

$$\frac{\Delta(D) = \forall \vec{\alpha}_j, \{\ldots, c : \vec{\tau}_i, \ldots\} \qquad \Gamma \vdash_{\mathsf{exp}} \tau'_j \qquad \Gamma \vdash e_i : \tau_i[\tau'_j/\alpha_j]}{\Gamma \vdash c(\vec{e}_i) : D\ \vec{\tau}'_j}\ e\text{-Ctor} \qquad \frac{\Gamma \vdash \phi : \tau}{\Gamma \vdash \grave{}\phi\grave{} : \tau}\ e\text{-Quote}$$

$$\frac{p \subseteq \vec{\tau}_i \in \Phi \qquad \Gamma \vdash e_i : \tau_i}{\Gamma \vdash p(\vec{e}_i) : \mathsf{bool}}\ e\text{-Rel} \qquad \frac{f : \forall \vec{\alpha}_j, \vec{\tau}_i \to \tau \in \Phi \qquad \Gamma \vdash_{\mathsf{exp}} \tau'_j \qquad \Gamma \vdash e_i : \tau_i[\tau'_j/\alpha_j]}{\Gamma \vdash f(\vec{e}_i) : \tau[\tau'_j/\alpha_j]}\ e\text{-Fun}$$

$$\frac{\mathsf{typeof}(\otimes) = \forall \vec{\alpha}_j, \vec{\tau}_i \to \tau \qquad \Gamma \vdash_{\mathsf{exp}} \tau'_j \qquad \Gamma \vdash e_i : \tau_i[\tau'_j/\alpha_j]}{\Gamma \vdash \otimes(\vec{e}_i) : \tau}\ e\text{-Op}$$

$$\frac{\Gamma \vdash e_1 : \mathsf{bool} \qquad \Gamma \vdash e_2 : \tau \qquad \Gamma \vdash e_3 : \tau}{\Gamma \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 : \tau}\ e\text{-If}$$

$$\frac{\Gamma \vdash e : D\ \vec{\tau}_j \qquad \Delta(D) = \forall \vec{\alpha}_j, \{\ldots, c_i : \vec{\tau}_k, \ldots\} \qquad \Gamma, \overrightarrow{X_k : \tau_k[\tau_j/\alpha_j]} \vdash e_i : \tau}{\Gamma \vdash \mathsf{match}\ e\ \mathsf{with}\ \overrightarrow{c_i(\vec{X}_k) \to e_i} : \tau}\ e\text{-Match}$$

Fig. 17. Typing rules: expressions; implicit parameters are in gray

circularity we want to avoid: It is possible to derive `q(42, 42)`, but this derivation nonsensically relies on `q(42, 42)` being false (since it requires that `p(42)` is false).

While Formulog's expressions *compute* values, the Formulog's formulas *construct* ASTs, to be shipped off to an SMT solver. Our formal account here uniformly uses SMT constructors to model the SMT syntax, but our implementation offers special-purpose syntax. For example, we write $c^{\mathsf{SMT}}_{\mathsf{var}}[x, \mathsf{bv}[32]]$ in our formalism to name a 32-bit integer variable x, while in our implementation one might write `#x[bv[32]]`.

Every ϕ-... typing rule generates a value with an SMT type, i.e., either t sym or t smt for SMT types t, i.e., $\Gamma \vdash_{\mathsf{smt}} t$ (Lemma D.9). The c-SMT-* rules yield t sym and t smt. SMT variables $c^{\mathsf{SMT}}_{\mathsf{var}}[x, t]$ are written in lowercase to emphasize their distinction from expression variables X; these SMT variables will be used as names in the formulas sent to the SMT solver. We keep track of which terms are SMT variables $c^{\mathsf{SMT}}_{\mathsf{var}}[x, t]$ of type t sym (generated by c-SMT-Var) and which are plain SMT formulas of type t smt (all other rules). We treat t sym as a subtype of t smt (ϕ-Promote).

The $\grave{}\phi\grave{}$ operator is an expression term that introduces quoted SMT formulas represented as special, SMT constructors of the form $c^{\mathsf{SMT}}_{\ldots}$ (described below); the $,e$ operator is the corresponding 'unquote' operator that introduces an expression (ϕ-Unquote).

While unquoting generally suffices for embedding the results of expressions in formulas, we treat constructors specially so that we can mix concrete and symbolic (i.e., SMT) arguments in a single data type constructor (c-SMT-Ctor): we assign them types that are fully SMT-ized via the

SMT constructors and formula well formedness $\boxed{\Delta; \Phi; \Gamma \vdash c^{\mathsf{SMT}}_{\cdots} : \vec{\tau_i} \to \tau}$ $\boxed{\Delta; \Phi; \Gamma \vdash \phi : \tau}$

$$\frac{\Gamma \vdash_{\mathsf{smt}} t}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{var}}[x,t] : \cdot \to t\ \mathsf{sym}}\ c\text{-SMT-Var} \qquad \frac{}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{const}}[k] : \cdot \to \mathsf{typeof}(k)\ \mathsf{smt}}\ c\text{-SMT-Const}$$

$$\frac{\Gamma \vdash_{\mathsf{smt}} t_1 \qquad \Gamma \vdash_{\mathsf{smt}} t_2}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{let}} : t_1\ \mathsf{sym} \times t_1\ \mathsf{smt} \times t_2\ \mathsf{smt} \to t_2\ \mathsf{smt}}\ c\text{-SMT-Let}$$

$$\frac{\Delta(D) = \forall \vec{\alpha_j}, \{\ldots, c : \vec{\tau_i}, \ldots\} \qquad \Gamma \vdash_{\mathsf{smt}} \tau_i[t'_j/\alpha_j] \qquad \Gamma \vdash_{\mathsf{smt}} t'_j}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{ctor}}[c] : \overrightarrow{\mathsf{toSMT}(\tau_i[t'_j/\alpha_j])} \to (D\ \overrightarrow{t'_j})\ \mathsf{smt}}\ c\text{-SMT-Ctor}$$

$$\frac{\Gamma \vdash_{\mathsf{smt}} t_1}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{forall}} : t_1\ \mathsf{sym} \times \mathsf{bool}\ \mathsf{smt} \to \mathsf{bool}\ \mathsf{smt}}\ c\text{-SMT-Forall}$$

$$\frac{uf : \vec{t_i} \to t \in \Phi}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{uf}}[uf] : \overrightarrow{t_i\ \mathsf{smt}} \to t\ \mathsf{smt}}\ c\text{-SMT-UFun}$$

$$\frac{\Gamma \vdash \phi : t\ \mathsf{sym}}{\Gamma \vdash \phi : t\ \mathsf{smt}}\ \phi\text{-Promote} \qquad \frac{\Gamma \vdash e : \tau \qquad \Gamma \vdash_{\mathsf{smt}} \tau}{\Gamma \vdash \text{,}e : \mathsf{toSMT}(\tau)}\ \phi\text{-Unquote} \qquad \frac{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{c}} : \vec{\tau_i} \to \tau \qquad \Gamma \vdash \phi_i : \tau'_i}{\Gamma \vdash c^{\mathsf{SMT}}_{\mathsf{c}}(\vec{\phi_i}) : \tau}\ \phi\text{-Ctor}$$

Conversion to SMT types $\boxed{\mathsf{erase}(\tau) = t}$ $\boxed{\mathsf{toSMT}(\tau) = \tau}$

$$\begin{array}{rcl} \mathsf{erase}(B) & = & B \\ \mathsf{erase}(D\ \vec{\tau_i}) & = & D\ \overrightarrow{\mathsf{erase}(\tau_i)} \\ \mathsf{erase}(t\ \mathsf{smt}) & = & \mathsf{erase}(t) \\ \mathsf{erase}(t\ \mathsf{sym}) & = & \mathsf{erase}(t) \end{array} \qquad \begin{array}{rcl} \mathsf{toSMT}(t) & = & \mathsf{erase}(t)\ \mathsf{smt} \\ \mathsf{toSMT}(t\ \mathsf{smt}) & = & \mathsf{erase}(t)\ \mathsf{smt} \\ \mathsf{toSMT}(t\ \mathsf{sym}) & = & \mathsf{erase}(t)\ \mathsf{sym} \end{array}$$

Fig. 18. Typing rules: SMT constructors and formulas; conversion to SMT types

toSMT function, but unquoting allows for easy mixing of values of SMT-types t as if they were of type t smt. The toSMT metafunction alters the type of e to make sure it is SMT representable; toSMT relies on an erase function to avoid nesting ... smt and ... sym type constructors. One can only run these functions on SMT types. For example, we can write terms like the following in concrete syntax:

$$\mathsf{let}\ H = 5\ \mathsf{in}\ \texttt{`cons(}H, \#l[\mathsf{bv}[32]\ \mathsf{list}]\texttt{)`}$$

which desugars to the SMT constructors:

$$\mathsf{let}\ H = 5\ \mathsf{in}\ \texttt{`}c^{\mathsf{SMT}}_{\mathsf{ctor}}[\mathsf{cons}](\text{,}H, c^{\mathsf{SMT}}_{\mathsf{var}}[l, \mathsf{bv}[32]\ \mathsf{list}]())\texttt{`}$$

Note that H is an expression variable and l is an SMT variable; the type conversion in ϕ-Unquote lets us mix them in the same list of 32-bit numbers. The t sym type is used in ϕ-Let and ϕ-Forall, which construct SMT formuale that use binders. The only way to get a value of type t sym is either with c-SMT-Var/ϕ-Ctor or with ϕ-Unquote, as in $\mathsf{let}\ X = \texttt{`}c^{\mathsf{SMT}}_{\mathsf{var}}[x, \mathsf{bv}[32]]\texttt{`}\ \mathsf{in}\ \texttt{`,}X\texttt{`}$.

Uninterpreted functions must be applied to appropriate SMT types (ϕ-UFun); recall that Φ-UFun ensures that each uninterpreted function's types are SMT representable.

Finally, there are a suite of SMT constructors of the form $c^{\text{SMT}}_{\ldots}$. Each of these special $c^{\text{SMT}}_{\ldots}$ constructors is treated as an ordinary constructor by the operational semantics, even though the constructors don't appear in Δ. Rather than making SMT terms opaque, we model them with constructors to allow for matching on generated formulae in P-EqSMT-BF and P-Eq-FB. The types of the SMT constructors $c^{\text{SMT}}_{\ldots}$ are given in Figure 18. It is a crucial invariant that all of these types be SMT types: we would not want to treat an SMT variable $c^{\text{SMT}}_{\text{var}}[x, \text{bool}]$ as though it were an *actual* bool! Reusing the c-SMT-... rules is convenient—we need only state the types of these constructors once and we get precise types in our premises. Several SMT constructors take special arguments in square brackets: $c^{\text{SMT}}_{\text{var}}[x, t]$ is a 0-ary SMT constructor, while $c^{\text{SMT}}_{\text{var}}$ itself is a family of SMT constructors for given variable names x and pre-types t; similarly, $c^{\text{SMT}}_{\text{const}}[k]$ is a 0-ary SMT constructor, while $c^{\text{SMT}}_{\text{const}}$ itself is a family of SMT constructors for given constants k. The embedding of data type constructors $c^{\text{SMT}}_{\text{ctor}}[c]$ is similarly parameterized on a constructor name c, and the embedding of uninterpreted functions $c^{\text{SMT}}_{\text{uf}}[uf]$ takes an uninterpereted function as a parameter. Separating these parameters from the interesting, ϕ-shaped subparts of each SMT constructor lets us reuse the c-SMT-... rules when typing premises that might bind to subparts of an SMT formula (P-EqSMT-..., Figure 16).

Our formal model elides some of the detail of our SMT encoding, such as constructors for SMT operations like bit vector manipulation or equality. These operations are all encoded as more SMT-specific constructors, i.e., $c^{\text{SMT}}_{\text{ctor}}[\text{bv}_{32}\_\text{add}](c^{\text{SMT}}_{\text{var}}[x, \text{bv}[32]], c^{\text{SMT}}_{\text{const}}[1]))$ represents result of adding the 32-bit vector x and 1. There are some subtle issues around polymorphism and determinacy. We give a monomorphic interpretation of SMT here, though our SMT constructors can work with our polymorphic data types. Our implementation treats equality and other polymorphic SMT operations specially, where each use of a polymorphic operator must be fully instantiated. In practice our implementation can usually infer the instantiation; users must annotate in those places we cannot infer.

C OPERATIONAL SEMANTICS

Formulog's operational semantics operates over *worlds* $\mathcal{W}$ and substitutions θ (Figure 19); the semantics is a mix of small-step rules modeling a single application of a Datalog rule (Figure 20), which depend on a small-step rules explaining how premises unify (Figures 21 and 22); the premise semantics in turn depends on a semantics of expressions (Figures 23 and 24) and formulas (Figure 25).

Our worlds $\mathcal{W}$ are (subsets of) Herbrand models. Our small-step semantics iteratively builds up a world that is in fact a Herbrand model of the original relations in the program. We could have modeled our semi-naive evaluation model for Formulog in more detail, showing that all programs generate a world $\mathcal{W}$ that is a well typed Herbrand model of the user's program (possibly taking infinite time to do so). Doing so wouldn't add anything materially interesting to our formulation.

Throughout, the type system's goal is prevent a program yielding $\bot$, the bottom "wrong" value. Such a value denotes a serious, unrecoverable error, such as using a relation with the wrong arity or conditioning on a non-boolean. It is important to distinguish bad, $\bot$-yielding programs from those that simply fail to step. The goal of Datalog evaluation is to reach a fixed point, i.e., to be unable to step! Finally, as is common, we assume that built-in operations do not yield $\bot$, i.e., they are total. While we could in principle design a type system for Formulog that avoids, say, division by zero, we are more interested in making the hard parts easy (generating well typed SMT formulas) rather than making the easy parts foolproof (statically protecting partial functions).

Namespaces			
World	$\mathcal{W}$	$\in$	$\text{PredVar} \rightharpoonup \mathcal{P}(\text{Val} \times \cdots \times \text{Val})$
World or error	$\mathcal{W}_\bot$	$\in$	World + Error
Substitution	θ	$\in$	$\text{Var} \rightharpoonup \text{Val}$
Substitution or error	$\theta_\bot$	$\in$	Substitution + Error
Values			
Results	$v_\bot$	$::=$	$v \mid \bot$
Values	$v \in \text{Val}$	$::=$	$k \mid c(\vec{v}_i)$
Unifiable term	$u \in \text{UTerm}$	$::=$	$X \mid k \mid c(\vec{u}_i)$

Substitution and world well formedness $\boxed{\Delta;\Phi;\Gamma \models \theta}$ $\boxed{\Delta;\Phi \models \mathcal{W}}$

$$\Gamma \models \theta \iff \forall X \in \text{dom}(\Gamma) \begin{cases} (1)\ X \in \text{dom}(\theta) \\ (2)\ \cdot \vdash \theta(X) : \Gamma(X) \end{cases}$$

$$\Delta;\Phi \models \mathcal{W} \iff \forall p \subseteq \vec{\tau}_i \in \Phi \begin{cases} (1)\ p \in \text{dom}(\mathcal{W}) \\ (2)\ \vec{v}_j \in \mathcal{W}(p) \Rightarrow i = j \\ (3)\ \forall \vec{v}_i \in \mathcal{W}(p),\ \Delta;\Phi;\cdot \vdash v_i : \tau_i \end{cases}$$

Fig. 19. Definitions for semantics

Clause semantics $\boxed{\vec{F};\mathcal{W} \vdash H \to \mathcal{W}_\bot}$

$$\frac{\cdot \vdash P_0 \to \theta_1 \quad \ldots \quad \theta_i \vdash P_i \to \theta_{i+1} \quad \ldots \quad \theta_n \vdash P_n \to \theta}{\vec{F};\mathcal{W} \vdash p(\vec{X}_j) :- \vec{P}_i \to \mathcal{W}[p \mapsto \mathcal{W}(p) \cup \{\theta(\vec{X}_j)\}]} \textsc{Clause}$$

$$\frac{\cdot \vdash P_0 \to \theta_1 \quad \ldots \quad \theta_i \vdash P_j \to \bot}{\vec{F};\mathcal{W} \vdash p(\vec{X}_j) :- \vec{P}_i \to \bot} \textsc{Clause-E1}$$

$$\frac{\cdot \vdash P_0 \to \theta_1 \quad \ldots \quad \theta_i \vdash P_i \to \theta_{i+1} \quad \ldots \quad \theta_n \vdash P_n \to \theta \qquad \vec{X}_j \not\subseteq \text{dom}(\theta)}{\vec{F};\mathcal{W} \vdash p(\vec{X}_j) :- \vec{P}_i \to \bot} \textsc{Clause-E2}$$

Fig. 20. Clause semantics

Rules of the form . . . -En denote $\bot$-yielding rules. Each such rule characterizes a form of wrongness avoided by our static type system. We write $v_\bot$ to denote the disjoint sum of values v and the wrong value $\bot$.

During correct execution, Clause takes a Horn clause $p(\vec{X}_j) :- \vec{P}_i$, executes each premise P_i from left to right, yielding a final substitution for the variables $\vec{X}_j$ in the head of the rule. There are two possible failing rules. Clause-E1 simply propagates the first error from a premise; Clause-E2 fails because not every X_j in the head of the rule is bound by the end. Since Formulog enforces the range restriction (H-Clause), Clause-E2 can never apply in a well typed program. Finally, the Clause* operational rules and the H-Clause typing rule both use the fixed, given order of premises

Premise semantics $\boxed{\vec{F}; \mathcal{W}; \theta \vdash P \to \theta_\perp}$

$$\frac{\vec{v} \in \mathcal{W}(p) \qquad \theta \vdash \vec{X} \sim \vec{v} : \theta'_\perp}{\mathcal{W}; \theta \vdash p(\vec{X}) \to \theta'_\perp}\ \textsc{PosAtom} \qquad \frac{\theta(\vec{X}) = \vec{v} \qquad \vec{v} \notin \mathcal{W}(p)}{\mathcal{W}; \theta \vdash !p(\vec{X}) \to \theta}\ \textsc{NegAtom}$$

$$\frac{\theta \vdash Y \sim c(\vec{X}) : \theta'_\perp}{\mathcal{W}; \theta \vdash Y = c(\vec{X}) \to \theta'_\perp}\ \textsc{EqCtor} \qquad \frac{\theta \vdash Y \sim c^{\mathsf{SMT}}_{c'}(\vec{X}) : \theta'_\perp}{\mathcal{W}; \theta \vdash Y = \grave{}c^{\mathsf{SMT}}_{c'}(\acute{,}\vec{X})\grave{} \to \theta'_\perp}\ \textsc{EqSMT}$$

$$\frac{e \text{ is not a constructor} \qquad \mathcal{W}; \theta \vdash e \Downarrow_e v \qquad \theta \vdash Y \sim v : \theta'_\perp}{\mathcal{W}; \theta \vdash Y = e \to \theta'_\perp}\ \textsc{EqExpr}$$

$$\frac{\vec{X} \nsubseteq \mathrm{dom}(\theta)}{\mathcal{W}; \theta \vdash !p(\vec{X}) \to \bot}\ \textsc{NegAtom-E} \qquad \frac{e \text{ is not a constructor} \qquad \mathcal{W}; \theta \vdash e \Downarrow_e \bot}{\mathcal{W}; \theta \vdash Y = e \to \bot}\ \textsc{EqExpr-E}$$

$$\frac{\mathcal{W}; \theta \vdash e \Downarrow_e v \qquad \theta(Y) \neq v}{\mathcal{W}; \theta \vdash !(Y = e) \to \theta}\ \textsc{NegExpr} \qquad \frac{\mathcal{W}; \theta \vdash e \Downarrow_e \bot}{\mathcal{W}; \theta \vdash !(Y = e) \to \bot}\ \textsc{NegExpr-E1} \qquad \frac{Y \notin \mathrm{dom}(\theta)}{\mathcal{W}; \theta \vdash !(Y = e) \to \bot}\ \textsc{NegExpr-E2}$$

Fig. 21. Premise semantics

for checking. Different orderings induce different binding orders, some of which may succeed and some of which may not.

The premise semantics (Figure 21) uses unification (Figure 22) to match and bind variables. Positive atoms $p(\vec{X}_i)$ try to unify their arguments with a tuple for p drawn from the world $\mathcal{W}$ (PosAtom). Negative atoms $p(\vec{X}_i)$ require that all of their arguments X_i are already bound (NegAtom); failing to find such bound terms yields an error (NegAtom-E). Rules for equations also use unification, whether for a constructor over variables (EqCtor) or an expression (EqExpr). The latter can fail if evaluation fails (EqExpr-E). Before discussing term evaluation, we give rules for unification.

Unification is split into two levels. *Unification* proper takes a pair of unifiable terms—values with variables in them—and tries to yield a substitution. *Value unification* takes a unifiable term and a value and tries to yield a substitution. The unification rules are of the form *uu*-.... These rules analyze the two unifiable terms to find which side is completely bound—i.e., applying θ can completely fill in the variables—and so can be passed to value unification as a value. The B and F in these rules stand for Bound and Free. The only error in unification is in *uu*-FF, when neither unifiable term is bound to a value. We write a case for when both unifiable terms are bound (*uu*-BB) and require that they are directly equal—but it would also work to drop this rule and rely on value unification to identify the equality.

Value unification rules are of the form *uv*-.... The rules here lookup variables in the unifiable term and either check that the binding conforms to the given value (*uv*-Eq-Var, cf. $X\tau$-Check) or binds the value (*uv*-Bind-Var, cf. $X\tau$-Bind). The remaining value unification rules match the structure of the unifiable term to the structure of the value (*uv*-Constant, *uv*-Ctor) or fold value unification along a vector ($\vec{u}\vec{v}$-All). Value unification never produces $\bot$. It isn't an error when two values fail to unify, since one might have to search through many tuples for a relation in $\mathcal{W}$ to find a one that matches, say, a given constructor.

Value unification $\boxed{\theta \vdash u \sim v \rhd \theta}$ $\boxed{\theta \vdash \vec{u} \sim \vec{v} \rhd \theta}$

$$\frac{\theta(X) = v}{\theta \vdash X \sim v \rhd \theta}\ uv\text{-Eq-Var} \qquad \frac{X \notin \mathrm{dom}(\theta)}{\theta \vdash X \sim v \rhd \theta[X \mapsto v]}\ uv\text{-Bind-Var}$$

$$\frac{}{\theta \vdash k \sim k \rhd \theta}\ uv\text{-Constant} \qquad \frac{\theta \vdash \vec{u}_i \sim \vec{v}_i \rhd \theta'}{\theta \vdash c(\vec{u}_i) \sim c(\vec{v}_i) \rhd \theta'}\ uv\text{-Ctor}$$

$$\frac{\theta \vdash u_0 \sim v_0 \rhd \theta_1 \quad \ldots \quad \theta_1 \vdash u_i \sim v_i \rhd \theta_i \quad \ldots \quad \theta_n \vdash u_n \sim v_n \rhd \theta'}{\theta \vdash \vec{u}_i \sim \vec{v}_i \rhd \theta}\ \vec{u}\vec{v}\text{-All}$$

Unification $\boxed{\theta \vdash u \sim u : \theta_\perp}$ $\boxed{\theta \vdash \vec{u} \sim \vec{u} : \theta_\perp}$

$$\frac{\theta(u_1) = v_1 \qquad \theta(u_2) = v_2 \qquad v_1 = v_2}{\theta \vdash u_1 \sim u_2 : \theta}\ uu\text{-BB} \qquad \frac{\nexists v_1, \theta(u_1) = v_1 \qquad \theta(u_2) = v_2 \qquad \theta \vdash u_1 \sim v_2 \rhd \theta'}{\theta \vdash u_1 \sim u_2 : \theta'}\ uu\text{-FB}$$

$$\frac{\theta(u_1) = v_1 \quad \nexists v_2, \theta(u_2) = v_2 \quad \theta \vdash u_2 \sim v_1 \rhd \theta'}{\theta \vdash u_1 \sim u_2 : \theta'}\ uu\text{-BF} \qquad \frac{\nexists v_1, \theta(u_1) = v_1 \quad \nexists v_2, \theta(u_2) = v_2}{\theta \vdash u_1 \sim u_2 : \bot}\ uu\text{-FF}$$

$$\frac{\theta \vdash u_i \sim u_i' \rhd \theta_i}{\theta \vdash \vec{u}_i \sim \vec{u_i'} \rhd \theta\vec{\theta}_i}\ \vec{u}\vec{u}\text{-All} \qquad \frac{\ldots \qquad \theta \vdash u \sim u' \rhd \bot \qquad \ldots}{\theta \vdash \vec{u}_i \sim \vec{u_i'} \rhd \bot}\ \vec{u}\vec{u}\text{-All-E}$$

$$\theta(c(\vec{u}_i)) = c(\overrightarrow{\theta(u_i)})$$

Fig. 22. Unification

The expression semantics is an entirely conventional big-step semantics using explicit substitutions. The operational rules implicitly take the function definitions $\vec{F}$ for use in applications ($\Downarrow_e$-Fun).

There are a variety of wrong behaviors prevented by our type system, mostly concerning mismatches between values and elimination forms: unbound variables ($\Downarrow_e$-Var-E); mistyped arguments to built-in operations ($\Downarrow_e$-Op-E2); function, relation and constructor arity errors ($\Downarrow_e$-Fun-E2, $\Downarrow_e$-Rel-E2, $\Downarrow_e$-Match-E4); non-existent functions and relations ($\Downarrow_e$-Fun-E3, $\Downarrow_e$-Rel-E3); conditionals on inappropriate values ($\Downarrow_e$-Match-E2, $\Downarrow_e$-Ite-E2); and ill formed constructor names ($\Downarrow_e$-Match-E3); The remaining rules propagate errors ($\Downarrow_e$-Let-E, $\Downarrow_e$-Op-E1, $\Downarrow_e$-Fun-E1, $\Downarrow_e$-Rel-E1, $\Downarrow_e$-Match-E1, $\Downarrow_e$-Ite-E1). As mentioned in the early discussion of our semantics in this section, $\Downarrow_e$-Op-E2 is *not* about division by zero (a form of going wrong our type system *doesn't* prevent), but about mis-application of built-in functions, e.g., taking the boolean negation of a number.

The operational semantics on formulas is simple: the rules generate ASTs for the SMT solver using the c^{SMT} constructors: constants ($c^{\mathsf{SMT}}_{\mathsf{const}}$), SMT variables ($c^{\mathsf{SMT}}_{\mathsf{var}}$), SMT data types ($c^{\mathsf{SMT}}_{\mathsf{ctor}}$), let bindings ($c^{\mathsf{SMT}}_{\mathsf{let}}$), quantification ($c^{\mathsf{SMT}}_{\mathsf{forall}}$), and uninterpreted function application ($c^{\mathsf{SMT}}_{\mathsf{uf}}$).

When unquoting values resulting from evaluating expressions, we use the toSMT function to translate expression values into the SMT's AST. The toSMT function is an identity on SMT ASTs, but it explicitly tags the constants and Formulog-defined constructors using $c^{\mathsf{SMT}}_{\mathsf{const}}$ and $c^{\mathsf{SMT}}_{\mathsf{ctor}}$.

Expression semantics $\boxed{\vec{F}; \mathcal{W}; \theta \vdash e \Downarrow_e v_\perp}$ $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v}_\perp}$

$$\frac{}{\mathcal{W}; \theta \vdash \cdot \Downarrow_{\vec{e}} \cdot} \Downarrow_{\vec{e}}\text{-Empty} \qquad \frac{\mathcal{W}; \theta \vdash e \Downarrow_e v \qquad \mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v}}{\mathcal{W}; \theta \vdash e, \vec{e} \Downarrow_{\vec{e}} v, \vec{v}} \Downarrow_{\vec{e}}\text{-All}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{e_i} \Downarrow_{\vec{e}} \vec{v_i}}{\mathcal{W}; \theta \vdash c(\vec{e_i}) \Downarrow_{\vec{e}} c(\vec{v_i})} \Downarrow_e\text{-Ctor} \qquad \frac{\mathcal{W}; \theta \vdash \vec{e_i} \Downarrow_{\vec{e}} \perp}{\mathcal{W}; \theta \vdash c(\vec{e_i}) \Downarrow_e \perp} \Downarrow_e\text{-Ctor-E}$$

$$\frac{}{\mathcal{W}; \theta \vdash k \Downarrow_e k} \Downarrow_e\text{-Const} \qquad \frac{\theta(X) = v}{\mathcal{W}; \theta \vdash X \Downarrow_e v} \Downarrow_e\text{-Var} \qquad \frac{\mathcal{W}; \theta \vdash \phi \Downarrow_\phi v_\perp}{\mathcal{W}; \theta \vdash \text{`}\phi\text{`} \Downarrow_e v_\perp} \Downarrow_e\text{-Quote}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v} \qquad [\![\otimes]\!](\vec{v}) = v}{\mathcal{W}; \theta \vdash \otimes(\vec{e}) \Downarrow_e v} \Downarrow_e\text{-Op}$$

$$\frac{\text{fun } f(\vec{X_i} : \vec{\tau_i}) : \tau = e \in \vec{F} \qquad \mathcal{W}; \theta \vdash \vec{e_i} \Downarrow_{\vec{e}} \vec{v_i} \qquad \mathcal{W}; \theta[\vec{X_i} \mapsto \vec{v_i}] \vdash e \Downarrow_e v_\perp}{\mathcal{W}; \theta \vdash f(\vec{e_i}) \Downarrow_e v_\perp} \Downarrow_e\text{-Fun}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{e_i} \Downarrow_{\vec{e}} \vec{v_i} \qquad \vec{v_i} \in \mathcal{W}(p)}{\mathcal{W}; \theta \vdash p(\vec{e_i}) \Downarrow_e \text{true}} \Downarrow_e\text{-Rel-T} \qquad \frac{\mathcal{W}; \theta \vdash \vec{e_i} \Downarrow_{\vec{e}} \vec{v_i} \qquad \vec{v_i} \notin \mathcal{W}(p)}{\mathcal{W}; \theta \vdash p(\vec{e_i}) \Downarrow_e \text{false}} \Downarrow_e\text{-Rel-F}$$

$$\frac{\mathcal{W}; \theta \vdash e_1 \Downarrow_e v_1 \qquad \mathcal{W}; \theta[X \mapsto v_1] \vdash e_2 \Downarrow_e v_\perp}{\mathcal{W}; \theta \vdash \text{let } X = e_1 \text{ in } e_2 \Downarrow_e v_\perp} \Downarrow_e\text{-Let}$$

$$\frac{\mathcal{W}; \theta \vdash e \Downarrow_e c(\vec{v_i}) \qquad \mathcal{W}; \theta[\overrightarrow{X_i \mapsto v_i}] \vdash e \Downarrow_e v_\perp}{\mathcal{W}; \theta \vdash \text{match } e \text{ with } \ldots c(\vec{X_i}) \to e \ldots \Downarrow_e v_\perp} \Downarrow_e\text{-Match}$$

$$\frac{\mathcal{W}; \theta \vdash e_1 \Downarrow_e \text{true} \qquad \mathcal{W}; \theta \vdash e_2 \Downarrow_e v_\perp}{\mathcal{W}; \theta \vdash \text{if } e_1 \text{ then } e_2 \text{ else } e_3 \Downarrow_e v_\perp} \Downarrow_e\text{-IteT} \qquad \frac{\mathcal{W}; \theta \vdash e_1 \Downarrow_e \text{false} \qquad \mathcal{W}; \theta \vdash e_3 \Downarrow_e v_\perp}{\mathcal{W}; \theta \vdash \text{if } e_1 \text{ then } e_2 \text{ else } e_3 \Downarrow_e v_\perp} \Downarrow_e\text{-IteF}$$

Fig. 23. Expression semantics

D METATHEORY

We break the metatheory into two parts: lemmas characterizing the SMT conversion (Section D.1) and lemmas showing type safety (Section E). The SMT lemmas culminate in two proofs: first, regularity (Lemma D.9) guarantees that (a) every type or context generated by the operational semantics is well formed and (b) that formula evaluation generates well typed SMT ASTs; second, we show that SMT conversion of values agrees with SMT conversion of types (Lemma D.10). Type safety culminates in theorems showing that premises don't yield $\perp$ and generate well typed substitutions (Lemma E.4) and so Horn clauses (a) never yield $\perp$ (Theorem E.6) and (b) take well typed worlds to well typed worlds (Theorem E.7).

D.1 SMT conversion

We show a variety of properties of the erasure and SMT conversion functions: smt is a sub-kind of exp (Lemma D.1); erasures and SMT conversion yield well formed types from SMT types

Expression semantics (continued) $\boxed{\vec{F}; \mathcal{W}; \theta \vdash e \Downarrow_e v_\perp}$ $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v}_\perp}$

$$\frac{\mathcal{W}; \theta \vdash \vec{e}_i \Downarrow_{\vec{e}} \vec{v}_i \qquad \mathcal{W}; \theta \vdash e \Downarrow_e \perp}{\mathcal{W}; \theta \vdash \vec{e}_i, e, \vec{e}_j \Downarrow_{\vec{e}} \perp} \Downarrow_{\vec{e}}\text{-All-E}$$

$$\frac{X \notin \mathrm{dom}(\theta)}{\mathcal{W}; \theta \vdash X \Downarrow_e \perp} \Downarrow_e\text{-Var-E} \qquad \frac{\mathcal{W}; \theta \vdash e_1 \Downarrow_e \perp}{\mathcal{W}; \theta \vdash \mathsf{let}\ X = e_1\ \mathsf{in}\ e_2 \Downarrow_e \perp} \Downarrow_e\text{-Let-E}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \perp}{\mathcal{W}; \theta \vdash \otimes(\vec{e}) \Downarrow_e \perp} \Downarrow_e\text{-Op-E1} \qquad \frac{\mathcal{W}; \theta \vdash \vec{e} \Downarrow_{\vec{e}} \vec{v} \qquad \vec{v} \notin \mathrm{dom}([\![\otimes]\!])}{\mathcal{W}; \theta \vdash \otimes(\vec{e}) \Downarrow_e \perp} \Downarrow_e\text{-Op-E2}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{e}_i \Downarrow_{\vec{e}} \perp}{\mathcal{W}; \theta \vdash f(\vec{e}_i) \Downarrow_e \perp} \Downarrow_e\text{-Fun-E1} \qquad \frac{\mathsf{fun}\ f(\vec{X}_i : \vec{\tau}_i) : \tau = e \in \vec{F} \qquad i \neq j}{\mathcal{W}; \theta \vdash f(\vec{e}_j) \Downarrow_e \perp} \Downarrow_e\text{-Fun-E2} \qquad \frac{f \notin \vec{F}}{\mathcal{W}; \theta \vdash f(\vec{e}_j) \Downarrow_e \perp} \Downarrow_e\text{-Fun-E3}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{e}_i \Downarrow_{\vec{e}} \perp}{\mathcal{W}; \theta \vdash p(\vec{e}_i) \Downarrow_e \perp} \Downarrow_e\text{-Rel-E1} \qquad \frac{\mathcal{W}(p) \subseteq \mathcal{P}(\overrightarrow{\mathrm{Val}_i}) \qquad i \neq j}{\mathcal{W}; \theta \vdash p(\vec{e}_j) \Downarrow_e \perp} \Downarrow_e\text{-Rel-E2} \qquad \frac{p \notin \mathrm{dom}(\mathcal{W})}{\mathcal{W}; \theta \vdash p(\vec{e}_j) \Downarrow_e \perp} \Downarrow_e\text{-Rel-E3}$$

$$\frac{\mathcal{W}; \theta \vdash e \Downarrow_e \perp}{\mathcal{W}; \theta \vdash \mathsf{match}\ e\ \mathsf{with}\ \overrightarrow{c_i(\vec{X}_j) \to e_i} \Downarrow_e \perp} \Downarrow_e\text{-Match-E1} \qquad \frac{\mathcal{W}; \theta \vdash e \Downarrow_e v \qquad v \neq c(\vec{v}')}{\mathcal{W}; \theta \vdash \mathsf{match}\ e\ \mathsf{with}\ \overrightarrow{c_i(\vec{X}_j) \to e_i} \Downarrow_e \perp} \Downarrow_e\text{-Match-E2}$$

$$\frac{\mathcal{W}; \theta \vdash e \Downarrow_e c(\vec{v}_k) \qquad c \notin \{\vec{c}_i\}}{\mathcal{W}; \theta \vdash \mathsf{match}\ e\ \mathsf{with}\ \overrightarrow{c_i(\vec{X}_j) \to e_i} \Downarrow_e \perp} \Downarrow_e\text{-Match-E3} \qquad \frac{\mathcal{W}; \theta \vdash e \Downarrow_e c(\vec{v}_k) \qquad j \neq k}{\mathcal{W}; \theta \vdash \mathsf{match}\ e\ \mathsf{with}\ \overrightarrow{\ldots c(\vec{X}_j \ldots) \to e_i} \Downarrow_e \perp} \Downarrow_e\text{-Match-E4}$$

$$\frac{\mathcal{W}; \theta \vdash e_1 \Downarrow_e \perp}{\mathcal{W}; \theta \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 \Downarrow_e \perp} \Downarrow_e\text{-Ite-E1} \qquad \frac{\mathcal{W}; \theta \vdash e_1 \Downarrow_e v \qquad v \notin \{\mathsf{true}, \mathsf{false}\}}{\mathcal{W}; \theta \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 \Downarrow_e \perp} \Downarrow_e\text{-Ite-E2}$$

Fig. 24. Expression semantics (error rules)

(Lemmas D.2, D.3, D.4, and D.5); weakening and strengthening of typing contexts (Lemmas D.6 and D.7); type variable substitution (Lemma D.8)—we have no need of a value substitution lemma because our semantics uses environments; regularity (Lemma D.9); and, finally, that SMT conversion of values agrees with SMT conversion of types (Lemma D.10).

Lemma D.1 (smt is a subkind of exp). *If* $\Gamma \vdash_{\mathsf{smt}} \tau$ *then* $\Gamma \vdash_{\mathsf{exp}} \tau$.

Proof. By induction on τ.

($\tau = B$) Immediate: τ-Base allows any m.

($\tau = \alpha$) Contradictory—type variables are only well formed at exp.

($\tau = D\ \vec{\tau}_i$) By the IH on each τ_i and t-ADT.

Formula semantics $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \phi \Downarrow_\phi v_\perp}$ $\boxed{\vec{F}; \mathcal{W}; \theta \vdash \vec{\phi} \Downarrow_{\vec{\phi}} \vec{v}_\perp}$

$$\frac{}{\mathcal{W}; \theta \vdash \cdot \Downarrow_{\vec{\phi}} \cdot} \Downarrow_{\vec{\phi}}\text{-Empty} \qquad \frac{\mathcal{W}; \theta \vdash \phi \Downarrow_\phi v \qquad \mathcal{W}; \theta \vdash \vec{\phi}_i \Downarrow_{\vec{\phi}} \vec{v}_i}{\mathcal{W}; \theta \vdash \phi, \vec{\phi}_i \Downarrow_{\vec{\phi}} v, \vec{v}_i} \Downarrow_{\vec{\phi}}\text{-All}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{\phi}_i \Downarrow_{\vec{\phi}} \vec{v}_i \qquad \mathcal{W}; \theta \vdash \phi \Downarrow_\phi \perp}{\mathcal{W}; \theta \vdash \vec{\phi}_i, \phi, \vec{\phi}_j \Downarrow_{\vec{\phi}} \perp} \Downarrow_{\vec{\phi}}\text{-All-E}$$

$$\frac{\mathcal{W}; \theta \vdash e \Downarrow_e v}{\mathcal{W}; \theta \vdash \text{,}e \Downarrow_\phi \text{toSMT}(v)} \Downarrow_\phi\text{-Unquote} \qquad \frac{\mathcal{W}; \theta \vdash e \Downarrow_e \perp}{\mathcal{W}; \theta \vdash \text{,}e \Downarrow_\phi \perp} \Downarrow_\phi\text{-Unquote-E}$$

$$\frac{\mathcal{W}; \theta \vdash \vec{\phi}_i \Downarrow_{\vec{\phi}} \vec{v}_i}{\mathcal{W}; \theta \vdash c_{\text{c}}^{\text{SMT}}(\vec{\phi}) \Downarrow_\phi c_{\text{c}}^{\text{SMT}}(\vec{v})} \Downarrow_\phi\text{-Ctor} \qquad \frac{\mathcal{W}; \theta \vdash \vec{\phi}_i \Downarrow_{\vec{\phi}} \perp}{\mathcal{W}; \theta \vdash c_{\text{c}}^{\text{SMT}}(\vec{\phi}_i) \Downarrow_\phi \perp} \Downarrow_\phi\text{-Ctor-E}$$

$$\frac{}{\mathcal{W}; \theta \vdash c_{\text{c}}^{\text{SMT}}(\vec{v}_i) \Downarrow_\phi c_{\text{c}}^{\text{SMT}}(\vec{v}_i)} \Downarrow_\phi\text{-SMT-Value}$$

SMT conversion $\boxed{\text{toSMT}(v) = v}$

$$\begin{aligned}
\text{toSMT}(k) &= c_{\text{const}}^{\text{SMT}}[k]() & \qquad \text{toSMT}(c_{\text{ctor}}^{\text{SMT}}[c](\vec{v}_i)) &= c_{\text{ctor}}^{\text{SMT}}[c](\vec{v}_i) \\
\text{toSMT}(c(\vec{v}_i)) &= c_{\text{ctor}}^{\text{SMT}}[c](\overrightarrow{\text{toSMT}(v_i)}) & \qquad \text{toSMT}(c_{\text{let}}^{\text{SMT}}(v_1, v_2, v_3)) &= c_{\text{let}}^{\text{SMT}}(v_1, v_2, v_3) \\
\text{toSMT}(c_{\text{const}}^{\text{SMT}}[k]()) &= c_{\text{const}}^{\text{SMT}}[k]() & \qquad \text{toSMT}(c_{\text{forall}}^{\text{SMT}}(v_1, v_2)) &= c_{\text{forall}}^{\text{SMT}}(v_1, v_2) \\
\text{toSMT}(c_{\text{var}}^{\text{SMT}}[x, t]()) &= c_{\text{var}}^{\text{SMT}}[x, t]() & \qquad \text{toSMT}(c_{\text{uf}}^{\text{SMT}}[uf](\vec{v}_i)) &= c_{\text{uf}}^{\text{SMT}}[uf](\vec{v}_i)
\end{aligned}$$

Fig. 25. Formula semantics

($\tau = t$ smt) Immediate: τ-SMT allows any m.

($\tau = t$ sym) Immediate: τ-SMT allows any m.

(τ = model) Contradictory—model is only well formed at exp. □

Lemma D.2 (Erasure is well formed). *If* $\Gamma \vdash_{\text{smt}} \tau$ *then* $\Gamma \vdash_{\text{smt}} \text{erase}(\tau)$.

Proof. By induction on the well formedness derivation.

(t-Base) Immediate, since $\text{erase}(B) = B$.

(t-TVar) Contradictory—type variables aren't well typed at smt.

(t-ADT) By the IH on each constituent of $D\ \vec{\tau}_i$, and then by t-ADT.

(τ-SMT) Since $\text{erase}(t \text{ smt}) = \text{erase}(t)$, by the IH on $\Gamma \vdash_{\text{smt}} t$.

(τ-Sym) Since $\text{erase}(t \text{ sym}) = \text{erase}(t)$, by the IH on $\Gamma \vdash_{\text{smt}} t$.

(τ-Model) Contradictory—model isn't well typed at smt. □

Lemma D.3 (SMT types have only SMT parts). *If* $\Gamma \vdash_{\text{smt}} \tau$*, then all of* τ*'s subparts are also well formed at* smt.

Proof. By induction on τ.

($\tau = B$) Immediate.

($\tau = \alpha$) Contradictory—type variables are only well formed at exp.

($\tau = D\ \vec{\tau_i}$) By the IH on each τ_i.

($\tau = t$ smt) By the IH on t.

($\tau = t$ sym) By the IH on t.

(τ = model) Contradictory—model is only well formed at exp. □

Lemma D.4 (SMT conversion is well formed). *If* $\Gamma \vdash_{\mathsf{smt}} \tau$ *then* $\mathrm{toSMT}(\tau) = t$ sym *or* t smt *such that* $\Gamma \vdash_{\mathsf{smt}} t$ *(and so* $\Gamma \vdash_{\mathsf{smt}} \mathrm{toSMT}(\tau)$*).*

Proof. By induction on the well formedness derivation.

(t-Base) $\mathrm{toSMT}(B) = B$ smt, which is well formed by τ-SMT and t-B.

(t-TVar) Contradictory—type variables are only well formed at exp.

(t-ADT) We know that $\mathrm{erase}(D\ \vec{\tau_i})$ is still well formed by Lemma D.2; then by τ-SMT.

(τ-SMT) Since it must be that $\Gamma \vdash_{\mathsf{smt}} t$, then $\mathrm{erase}(t)$ is also well formed by Lemma D.2; then by τ-SMT.

(τ-Sym) Since it must be that $\Gamma \vdash_{\mathsf{smt}} t$, then $\mathrm{erase}(t)$ is also well formed by Lemma D.2; then by τ-Sym.

(τ-Model) Contradictory—model is only well formed at smt □

Lemma D.5 (SMT conversion is only for SMT types). $\mathrm{toSMT}(\tau)$ *is defined iff* $\Gamma \vdash_{\mathsf{smt}} \tau$.

Proof. The right-to-left direction is proved by Lemma D.4. For left-to-right, we go by induction on τ.

($\tau = B$) By t-Base.

($\tau = \alpha$) Contradictory—type variables are undefined for erase.

($\tau = D\ \vec{\tau_i}$) By the IH on each τ_i and t-ADT.

($\tau = t$ smt) By the IH on t and τ-SMT.

($\tau = t$ sym) By the IH on t and τ-Sym.

(τ = model) Contradictory—model is undefined for erase. □

We say a type t is an "SMT type" when $\Gamma \vdash_{\mathsf{smt}} t$; a type τ is an SMT type when it is equal to an SMT type t or when it is of the form t smt or t sym. Note that toSMT always produces an SMT type, but does not work on types that contain type variables or the unrepresentable model type.

Lemma D.6 (Weakening). *If* $\vdash \Gamma$ *and* $\vdash \Gamma'$ *and* $\mathrm{dom}(\Gamma) \cap \mathrm{dom}(\Gamma') = \emptyset$ *then:*

(1) $\vdash \Gamma, \Gamma'$

(2) If $\Gamma \vdash_m \tau$ *then* $\Gamma, \Gamma' \vdash_m \tau$*;*

(3) If $\Gamma \vdash e : \tau$ *then* $\Gamma, \Gamma' \vdash e : \tau$*; and*

(4) If $\Gamma \vdash \phi : \tau$ *then* $\Gamma, \Gamma' \vdash \phi : \tau$.

Proof. By mutual induction on the derivations.

Contexts.

(Γ-Empty) We have $\Gamma' = \cdot$; immediate by assumption.

(Γ-Var) We have $\Gamma' = \Gamma'', X : \tau$. By the IH on Γ'' and Γ-Var, finding $\Gamma, \Gamma'' \vdash_m \tau$ by part (2) of the IH.

(Γ-TVar) We have $\Gamma' = \Gamma'', \alpha$. By the IH on Γ'' and Γ-TVar.

Type well formedness.

(t-Base) Immediate, by t-Base.

(t-TVar) Since Γ and Γ' have disjoint domains, we know $\alpha \in \Gamma$—by t-TVar.

(t-ADT) By the IH on each constituent of $D\ \vec{\tau}_i$, followed by t-ADT.

(τ-SMT) By the IH on $\Gamma \vdash_{\mathsf{smt}} t$ and then τ-SMT.

(τ-Sym) By the IH on $\Gamma \vdash_{\mathsf{smt}} t$ and then τ-Sym.

(τ-Model) Immediate, by τ-Model. □

Expressions.

(e-Var) Since the domains are disjoint, $(\Gamma, \Gamma')(X) = \tau$ and we can still find e-Var.

(e-Const) Immediate, by e-Const.

(e-Let) By the e-Let and the IH on e_1 and e_2, α-renaming X appropriately.

(e-Ctor) By e-Ctor and the IH, using part (2) on τ'_j and part (3) on e_i.

(e-Quote) By the part (4) of the IH.

(e-Rel) By e-Rel and the IH on each e_i.

(e-Fun) By e-Fun and the the IH, using part (2) on τ'_j and part (3) on e_i.

(e-Op) By e-Op and the the IH, using part (2) on τ'_j and part (3) on e_i.

(e-If) By e-If and the IH on each of the e_i.

(e-Match) By e-Match and the IH on e and each of the e_i, α-renaming each X_k appropriately.

Formulas.

(ϕ-Var) By ϕ-Var and part (2) of the IH.

(ϕ-Promote) By ϕ-Promote and the IH.

(ϕ-Unquote) By ϕ-Unquote and part (3) of the IH.

(ϕ-Ctor) By ϕ-Ctor and the IH, using part (2) on the τ_i and part (4) on ϕ_i, observing that the actual types are unchanged, and so the toSMT conversions are the same.

Lemma D.7 (Type well formedness strengthening). *If* $\Gamma, X : \tau, \Gamma' \vdash_m \tau'$ *then* $\Gamma, \Gamma' \vdash \tau'$.

Proof. (t-Base) Immediate.

(t-TVar) Immediate: removing the variable binding can't affect α.

(t-ADT) By the IH on each constituent of $D\ \vec{\tau}_i$.

(τ-SMT) By the IH on $\Gamma \vdash_{\mathsf{smt}} t$.

(τ-Sym) By the IH on $\Gamma \vdash_{\mathsf{smt}} t$.

(τ-Model) Immediate. □

Lemma D.8 (Type variable substitution). *If* $\vdash \Gamma, \alpha, \Gamma'$ *and* $\Gamma \vdash_m \tau'$*, then:*

(1) $\vdash \Gamma, \Gamma'[\tau/\alpha]$*;*

(2) If $\Gamma, \alpha, \Gamma' \vdash_m \tau$ *then* $\Gamma, \Gamma'[\tau/\alpha] \vdash_m \tau'[\tau/\alpha]$*;*

(3) If $\Gamma, \alpha, \Gamma' \vdash X, \tau' \rhd \Gamma''$ *then* $\Gamma, \Gamma'[\tau/\alpha] \vdash X, \tau'[\tau/\alpha] \rhd \Gamma''[\tau/\alpha]$*; and*

(4) If $\Gamma, \alpha, \Gamma' \vdash \vec{X}_i, \vec{\tau}'_i \rhd \Gamma''$ *then* $\Gamma, \Gamma'[\tau/\alpha] \vdash \vec{X}_i, \vec{\tau}'_i[\tau/\alpha] \rhd \Gamma''[\tau/\alpha]$.

Proof. For parts (1) and (2), by mutual induction on the derivations. Note that if α actually occurs in the type, we could only have found well formedness at exp.

(Γ-Empty) Contradictory: $\cdot \neq \Gamma, \alpha, \Gamma'$.

(Γ-Var) We have $\Gamma' = \Gamma'', X : \tau'$ where $\Gamma, \Gamma'' \vdash_{\text{exp}} \tau'$. By the IH on Γ'', we know that $\vdash \Gamma, \Gamma''[\tau/\alpha]$; by part (2), we have $\Gamma, \Gamma''[\tau/\alpha] \vdash_{\text{exp}} \tau'[\tau/\alpha]$; and so we have $\vdash \Gamma, \Gamma'[\tau/\alpha]$ by Γ-Var.

(Γ-TVar) We have $\Gamma' = \Gamma'', \beta$; by the IH on Γ'', we have $\vdash \Gamma, \Gamma''[\tau/\alpha]$; since $\beta[\tau/\alpha] = \beta$, we can apply Γ-TVar to find $\vdash \Gamma, \Gamma'[\tau/\alpha]$ as desired.

(t-B) Immediate by t-B, since $B[\tau/\alpha] = B$.

(t-TVar) We have $\tau' = \beta$. If $\alpha = \beta$, then we have $\Gamma \vdash_m \alpha[\tau/\alpha]$ by assumption. If $\alpha \neq \beta$, then it must be that $\beta \in \Gamma$ or Γ'—either way, β is unaffected by the substitution and we have $\beta \in \Gamma, \Gamma'[\tau/\alpha]$ and so $\Gamma, \Gamma'[\tau/\alpha] \vdash_m \beta$ by t-TVar.

(t-ADT) By the IH on each premise, followed by t-ADT.

(τ-SMT) By the IH on $\Gamma, \alpha, \Gamma' \vdash_{\text{smt}} t$ and then by τ-SMT.

(τ-Sym) By the IH on $\Gamma, \alpha, \Gamma' \vdash_{\text{smt}} t$ and then by τ-Sym.

(τ-Model) Immediate by τ-Model.

For parts (3) and (4), by mutual induction on the derivations.

($X\tau$-Bind) We have $X \notin \text{dom}(\Gamma, \alpha, \Gamma')$, so it must also be the case that $X \notin \text{dom}(\Gamma, \Gamma'[\tau/\alpha])$. We therefore find $\Gamma, \Gamma'[\tau/\alpha] \vdash X, \tau'[\tau/\alpha] \rhd \Gamma, \Gamma'[\tau/\alpha], \tau'[\tau/\alpha]$ by $X\tau$-Bind.

($X\tau$-Check) We have $(\Gamma, \alpha, \Gamma')(X) = \tau'$. Is $X : \tau'$ in Γ or Γ'? Either way we will find $\Gamma, \Gamma'[\tau/\alpha] \vdash X, \tau'[\tau/\alpha] \rhd \Gamma, \Gamma'[\tau/\alpha]$ by $X\tau$-Check.

If $\tau' \in \text{dom}(\Gamma)$, then $\Gamma \vdash \tau'$ and so $\tau'[\tau/\alpha] = \tau'$ $(\Gamma, \Gamma'[\tau/\alpha])(X) = \tau'$ and we have $\Gamma, \Gamma'[\tau/\alpha] \vdash X, \tau' \rhd \Gamma, \Gamma'[\tau/\alpha]$.

If, on the other hand, $\tau' \in \text{dom}(\Gamma')$, then $(\Gamma, \Gamma'[\tau/\alpha])(X) = \tau'[\tau/\alpha]$. We therefore have $\Gamma, \Gamma'[\tau/\alpha] \vdash X, \tau'[\tau/\alpha] \rhd \Gamma, \Gamma'[\tau/\alpha]$.

($\vec{X}\vec{\tau}$-All) By part (3) of the IH on each premise. □

Lemma D.9 (Regularity; formulas have SMT types). *(1) If* $\vdash \Gamma$ *and* $\Gamma(X) = \tau$ *then* $\Gamma \vdash_{\text{exp}} \tau$.
(2) If $\vdash \Phi$ *then (a) if* $f : \forall \vec{\alpha}_j, \vec{\tau}_i \to \tau \in \Phi$ *then* $\vec{\alpha}_j \vdash_{\text{exp}} \tau$, *and (b) if* $uf : \vec{t}'_i \to t \in \Phi$ *then* $\cdot \vdash_{\text{smt}} t$.
(3) If $\Delta; \Phi; \Gamma \vdash e : \tau$ *then* $\Gamma \vdash_{\text{exp}} \tau$.
(4) If $\Delta; \Phi; \Gamma \vdash c_{\text{c}}^{\text{SMT}}(\vec{\phi}_i) : \vec{\tau}_i \to \tau$ *then* $\tau_i = t_i$ smt *or* $\tau_i = t_i$ sym *and* $\tau = t$ smt *or* $\tau = t$ sym *and* $\Gamma \vdash_{\text{smt}} \tau_i$ *and* $\Gamma \vdash_{\text{smt}} \tau$.
(5) If $\Delta; \Phi; \Gamma \vdash \phi : \tau$ *then* $\tau = t$ smt *or* $\tau = t$ sym *and* $\Gamma \vdash_{\text{smt}} \tau$.
(6) If $\Delta; \Phi; \Gamma \vdash \vec{e}_i : \vec{\tau}_i$ *then* $\Gamma \vdash_{\text{exp}} \tau_i$.
(7) If $\Delta; \Phi; \Gamma \vdash \vec{\phi}_i : \vec{\tau}_i$ *then* $\tau_i = t_i$ smt *or* $\tau = t_i$ sym *and* $\Gamma \vdash_{\text{smt}} t_i$ *(and so* $\Gamma \vdash_{\text{exp}} \tau_i$*).*

Proof. By induction on the typing derivation.

Contexts.

(Γ-Empty) Contradictory—there's no way $\cdot$ has a binding for X.

(Γ-Var) $\Gamma = \Gamma', Y : \tau$. If $X = Y$, then we know $\Gamma \vdash_{\text{exp}} \tau$ by assumption; otherwise, by the IH on Γ'.

(Γ-TVar) $\Gamma = \Gamma', \alpha$. By the IH on Γ.

Program signatures.

(Φ-Empty) Contradictory—there are no function definitions in $\cdot$.

(Φ-Fun) $\Phi = \Phi', g : \ldots$. For case (a) when $f = g$, then by assumption. Otherwise, by the IH on Φ'.

(Φ-Rel) $\Phi = \Phi', p \subseteq \vec{\tau}_i$. By the IH on Φ.

(Φ-UFun) $\Phi = \Phi', uf' : \vec{t}'_i \to t$. For case (b) when $uf = uf'$, then by assumption. Otherwise, by the IH on Φ'.

Expressions.

(*e*-Var) By the part (1) on $\vdash \Gamma$.

(*e*-Const) By assumption, we know that $\Gamma \vdash_{\mathsf{smt}} \mathrm{typeof}(k)$; by Lemma D.1 we can find $\Gamma \vdash_{\mathsf{exp}} \mathrm{typeof}(k)$.

(*e*-Let) By the IH on $\Gamma, X : \tau_1 \vdash e_2 : \tau_2$, using strengthening (Lemma D.7) to find that if $\Gamma, X : \tau_1 \vdash_{\mathsf{exp}} \tau_2$ then $\Gamma \vdash_{\mathsf{exp}} \tau_2$.

(*e*-Ctor) Since $\Gamma \vdash_{\mathsf{exp}} \tau'_j$, we know by t-ADT that $\Gamma \vdash_{\mathsf{exp}} D\ \vec{\tau}'_j$.

(*e*-Quote) By the IH on part (5), we know that $\Gamma \vdash_{\mathsf{smt}} \tau$ (and, less relevantly, that $\tau = t$ smt or t sym). We can find the same well formedness at exp by Lemma D.1.

(*e*-Rel) Immediate by t-B.

(*e*-Fun) Since $f : \forall \vec{\alpha}_j, \vec{\tau}_i \to \tau \in \Phi$ and $\vdash \Phi$, we know by part (2) of the IH know that $\vec{\alpha}_j \vdash_{\mathsf{exp}} \tau$. By weakening (Lemma D.6) we can lift that well formedness judgment to Γ. Since each $\Gamma \vdash_{\mathsf{exp}} \tau'_j$, we can find that $\Gamma \vdash \tau[\tau'_j/\alpha_j]$ by substitution (Lemma D.8).

(*e*-Fun) We have by assumption that $\mathrm{typeof}(\otimes)$ yields a well-formed type, i.e., $\vec{\alpha}_j \vdash_{\mathsf{exp}} \tau$ (and also for each τ_i). By weakening (Lemma D.6) we can lift that well formedness judgment to Γ. Since each $\Gamma \vdash_{\mathsf{exp}} \tau'_j$, we can find that $\Gamma \vdash \tau[\tau'_j/\alpha_j]$ by substitution (Lemma D.8).

(*e*-If) By the IH on $\Gamma \vdash e_2 : t$.

(*e*-Match) By the IH on $\Gamma, \overrightarrow{X_1 : \tau_1[\tau_j/\alpha_j]} \vdash e_1 : \tau$ we have $\Gamma, \overrightarrow{X_1 : \tau_1[\tau_j/\alpha_j]} \vdash \tau$; we can use strengthening (Lemma D.7) to find $\Gamma \vdash_{\mathsf{exp}} \tau$.

SMT constructors.

(*c*-SMT-Var) Immediate, with $\Gamma \vdash_{\mathsf{smt}} t$ coming from the rule itself.

(*c*-SMT-Const) Immediate, since we have by assumption that $\cdot \vdash_{\mathsf{smt}} \mathrm{typeof}(k)$.

(*c*-SMT-Let) Immediate, with the necessary well formedness assumptions coming from the rule itself.

(*c*-SMT-Ctor) We know that $D\ \vec{t}'_j$ is well formed by t-ADT. We can find the translation of the argument types well formed by Lemma D.4 on each of the $\Gamma \vdash_{\mathsf{smt}} \tau_i[t'_j/\alpha_j]$ derivations.

(*c*-SMT-Forall) Immediate, with the necessary $\Gamma \vdash_{\mathsf{smt}} t_1$ coming from the rule itself.

(*c*-SMT-UFun) Since $\vdash \Phi$ and $uf : \vec{t}_i \to t \in \Phi$, we know that $\cdot \vdash_{\mathsf{smt}} t$ by part (2) of the IH and so $\cdot \vdash_{\mathsf{smt}} t$ smt, which we can lift to Γ by weakening (Lemma D.6).

Formulas.

(ϕ-Promote) Since $\Delta; \Phi; \Gamma \vdash \phi : t$ sym, we know that $\Gamma \vdash_{\mathsf{smt}} t$ and so we are correct in yielding $\tau = t$ smt.

(ϕ-Unquote) We have $\Delta;\Phi;\Gamma \vdash e : \tau$ such that $\Gamma \vdash_{\mathsf{smt}} \tau$. By Lemma D.4 we know that toSMT(τ) is a well formed SMT type.

(ϕ-Ctor) By the IH part (4) on $\Gamma \vdash c_{\mathsf{c}}^{\mathsf{SMT}} : \vec{\tau_i} \to \tau$.

Vectored expressions and formulas. By the IH for parts (3) and (5), respectively.

□

Lemma D.10 (SMT value conversion is type correct). *If* $\Delta;\Phi;\Gamma \vdash v : \tau$ *and* $\Gamma \vdash_{\mathsf{smt}} \tau$ *then* $\Delta;\Phi;\Gamma \vdash \mathrm{toSMT}(v) : \mathrm{toSMT}(\tau)$.

Proof. First, observe that τ and all of its parts must be well formed at smt, by Lemmas D.5 and D.3. By induction on the typing derivation. In expression mode, the applicable rules are e-Const and e-Ctor; only a few typing rules could even have applied to a value in formula mode: the ϕ-Ctor and ϕ-Promote.

(e-Const) We have $\Gamma \vdash k : \mathrm{typeof}(k)$; since $\mathrm{toSMT}(k) = c_{\mathsf{const}}^{\mathsf{SMT}}[k]()$ and $\mathrm{toSMT}(\mathrm{typeof}(k)) = k$ smt (since $\Gamma \vdash_{\mathsf{smt}} \mathrm{typeof}(k)$ by assumption), we must show that $\Gamma \vdash c_{\mathsf{const}}^{\mathsf{SMT}}[k]() : \mathrm{typeof}(k)$ smt, which we have by ϕ-SMT-Const.

(e-Ctor) We have $v = c(\vec{v_i})$ and:

$$\Delta(D) = \forall \vec{\alpha_j}, \{\ldots, c : \vec{\tau_i}, \ldots\} \qquad \Gamma \vdash_{\mathsf{exp}} \tau'_j \qquad \Gamma \vdash v_i : \tau_i[\tau'_j/\alpha_j]$$

Further, we know that $\Gamma \vdash_{\mathsf{smt}} D\ \vec{\tau'_j}$ (and so each of the subderivations must also be smt) and that $\mathrm{toSMT}(c(\vec{v_i})) = c_{\mathsf{ctor}}^{\mathsf{SMT}}[c](\overrightarrow{\mathrm{toSMT}(v_i)})$. By the IH on each of these v_i, we know that we find appropriate values at appropriately converted types, i.e., $\Gamma \vdash \mathrm{toSMT}(v_i) : \mathrm{toSMT}(\tau_i[\tau'_j/\alpha_j])$. By Lemma D.4, we know $\mathrm{toSMT}(\tau_i[\tau'_j/\alpha_j])$ is some well formed SMT type. We are *almost* able to apply ϕ-SMT-Ctor, but we must pick appropriate t'_j. We know that $\mathrm{toSMT}(\tau'_j)$ is a well formed SMT type of the form t'_j smt or t'_j sym (Lemma D.4). Whether it's symbolic or not, let the inner t'_j there be our t'_j. We can now apply ϕ-SMT-Ctor to find that $\Gamma \vdash \mathrm{toSMT}(c(\vec{v_i})) : \mathrm{toSMT}(D\ \vec{\tau'_j})$.

(ϕ-Promote) By the IH on $\Gamma \vdash v : t$ sym, we know that $\Gamma \vdash \mathrm{toSMT}(v) : \mathrm{toSMT}(t\ \mathsf{sym})$, i.e., $\Gamma \vdash \mathrm{toSMT}(v) : t$ sym. By reapplying ϕ-Promote we can find that $\Gamma \vdash \mathrm{toSMT}(v) : v$ smt.

(ϕ-Ctor) Immediate: toSMT does nothing to the $c_{\cdots}^{\mathsf{SMT}}$ constructed value nor to the SMT-type τ assigned to it (which is t smt in all cases except for $c_{\mathsf{var}}^{\mathsf{SMT}}$).

□

E TYPE SAFETY

To prove type safety, we prove two properties for every mode of evaluation: first, it is *safe*, i.e, never yields $\bot$; and second, it is *type preserving*, i.e., well typed inputs yield well typed outputs.

The proofs are fairly conventional. For all but the last step, we prove safety and type preservation simultaneously. We start with expressions and formulas (Lemma E.2), which requires a modest notion of canonical forms (Lemma E.1). Next, we prove that value unification (Lemma E.3) is type preserving, reasoning about unification in general within the lemma showing safety and type preservation for premises (Lemma E.4). After a brief lemma about bindings (Lemma E.5), we can prove that program evaluation is safe (Theorem E.6) and type preserving (Theorem E.7).

Lemma E.1 (Canonical forms for t sym). *If* $\Delta;\Phi;\Gamma \vdash v : t\ \mathsf{sym}$ *then* $v = c_{\mathsf{var}}^{\mathsf{SMT}}[x,t]()$.

Proof. The only typing rule that could have applied is ϕ-SMT-Var. □

Lemma E.2 (Term and formula type safety). *If* $\Delta;\Phi \models \mathcal{W}$ *and* $\Delta;\Phi \vdash \vec{F}$ *and* $\Gamma \models \theta$*, when either:*

(1) $\Delta;\Phi;\Gamma \vdash e : \tau$ *and* $\mathcal{W};\theta \vdash e \Downarrow_e v_\perp$*; or*

(2) $\Delta;\Phi;\Gamma \vdash \phi : \tau$ *and* $\mathcal{W};\theta \vdash \phi \Downarrow_\phi v_\perp$

(3) $\Delta;\Phi \vdash \mathsf{fun}\ f(\vec{X}_i : \vec{\tau}_i) : \tau = e$ *and* $\vec{\alpha}_j, \overrightarrow{X_i : \tau_i} \models \theta'$ *and* $\mathcal{W};\theta' \vdash e \Downarrow_e v_\perp$

then $v_\perp = v$ *(i.e.,* $v_\perp \neq \perp$*) and* $\Delta;\Phi;\Gamma \vdash v : \tau$*.*

Similarly, when either:

(1) if $\Delta;\Phi;\Gamma \vdash e_i : \tau_i$ *and* $\mathcal{W};\theta \vdash \vec{e_i} \Downarrow_e \vec{v_i}$ *then* $\Delta;\Phi;\Gamma \vdash \vec{v}_{i\perp} : \vec{\tau}_i$*; and*

(2) if $\Delta;\Phi;\Gamma \vdash \phi_i : \tau_i$ *and* $\mathcal{W};\theta \vdash \vec{\phi_i} \Downarrow_{\vec{\phi}} \vec{v_i}$ *then* $\Delta;\Phi;\Gamma \vdash \vec{v}_{i\perp} : \tau$

then $\vec{v}_{i\perp} = \vec{v_i}$ *(i.e., it is not* $\perp$*) and* $\Delta;\Phi;\Gamma \vdash v_i : \tau_i$*.*

Proof. By mutual induction on derivations and the length of the vectored expressions/formulas, leaving θ general (for, e.g., e-Let and e-Match).

Expressions.

(e-Var) We have $\Gamma(X) = \tau$; since $\Gamma \models \theta$, we have $\theta(X) = v$ (and so $\Downarrow_e$-Var-E didn't apply). So it must be the case that $\Downarrow_e$-Var applied. We can see further that $\Delta;\Phi;\cdot \vdash v : \tau$, and we are done by weakening (Lemma D.6).

(e-Const) It must be that $\Downarrow_e$-Const applied, and we immediately see that $v_\perp \neq \perp$ and k is well typed in any well formed context by assumption and e-Const.

(e-Let) We know that $\Gamma \vdash e_1 : \tau_1$ and $\Gamma, X : \tau_1 \vdash e_2 : \tau_2$. By the IH on e_1, we know that $\theta;\mathcal{W} \vdash e_1 \Downarrow_e v_1$, so it can't be the case that $\Downarrow_e$-Let-E applied—it must hae been $\Downarrow_e$-Let. By the IH on e_2, we know that the final result is also not $\perp$ and is well typed.

(e-Ctor) We have $\Delta(D) = \forall\vec{\alpha}_j, \{\ldots, c : \vec{\tau}_i, \ldots\}$ and $\Gamma \vdash e_i : \tau_i[\tau'_j/\alpha_j]$. By the IH, we know that each of the $\vec{e_i}$ must have reduced to non-$\perp$ values, and so $\Downarrow_e$-Ctor-E could not have applied. We can therefore see that each e_i reduces to an appropriately typed v_i, and our resulting value is well typed by e-Ctor.

(e-Quote) Only $\Downarrow_e$-Quote could have applied. By the IH, we know that ϕ reduces to a non-$\perp$ value v well typed at τ.

(e-Rel) We know that $p \subseteq \vec{\tau}_i \in \Phi$ and $\Gamma \vdash e_i : \tau_i$. The IH on $\vec{e_i}$ rules out *StepstoE*-Rel-E1; the typing rule rules out the arity mismatch in $\Downarrow_e$-Rel-E2 and the missing relation in $\Downarrow_e$-Rel-E3. So it must be the case that $\Downarrow_e$-Rel-True or $\Downarrow_e$-Rel-False applied; either way, we yield a bool, which is appropriately typed by e-Const.

(e-Fun) We know that $f : \forall\vec{\alpha}_j, \vec{\tau}_i \to \tau \in \Phi$ and $\Gamma \vdash e_i : \tau_i[\tau'_j/\alpha_j]$. The IH on $\vec{e_i}$ rules out *StepstoE*-Fun-E1; the typing rule rules out the arity mismatch in $\Downarrow_e$-Fun-E2 and the missing function in $\Downarrow_e$-Fun-E3. So it must be the case that $\Downarrow_e$-Fun applied. Since $\Delta;\Phi \vdash F$, we know by the IH on part (3) that the resulting value is non-$\perp$ and well typed at $\tau[\tau'_j/\alpha_j]$.

(e-Op) We know that $\mathrm{typeof}(\otimes) = \forall\vec{\alpha}_j, \vec{\tau}_i \to \tau$ and $\Gamma \vdash e_i : \tau_i[\tau'_j/\alpha_j]$. The IH on $\vec{e_i}$ rules out *StepstoE*-Op-E1; the typing rule rules out the arity/domain mismatch in $\Downarrow_e$-Op-E2. So it must be the case that $\Downarrow_e$-Op applied. We know that the result is well typed by our assumption that $\mathrm{typeof}(\otimes)$ and $[\![\otimes]\!]$ agree.

(e-If) We have $\Gamma \vdash e_1 : \mathrm{bool}$ and $\Gamma \vdash e_2 : \tau$ and $\Gamma \vdash e_3 : \tau$. By the IH on e_1, we know that e_1 reduces to true or false (since those are the only values of type bool). So we

can rule out $\Downarrow_e$-Ite-E1 and $\Downarrow_e$-Ite-E2—we must have stepped by either $\Downarrow_e$-Ite-T or $\Downarrow_e$-Ite-F. The IH on e_2 or e_3 (respectively) guarantees we step to a non-$\bot$, well typed value.

(e-Match) We have $\Gamma \vdash e : D\ \vec{\tau_j}$ and $\Delta(D) = \forall \vec{\alpha_j}, \{\ldots, c_i : \vec{\tau_k}, \ldots\}$ and $\Gamma, \overrightarrow{X_k : \tau_k[\tau_j/\alpha_j]} \vdash e_i : \tau$. The IH on e guarantees that we get a non-$\bot$ value at type $D\ \vec{\tau_j}$, which rules out the error case $\Downarrow_e$-Match-E1, the non-constructor value of $\Downarrow_e$-Match-E2, the misnamed constructor of $\Downarrow_e$-Match-E3, and the arity error of $\Downarrow_e$-Match-E4. So it must be the case that we applied $\Downarrow_e$-Match; by the IH, the matching pattern reduces to a well typed non-$\bot$ value.

Formulas.

(ϕ-Promote) We have $\Delta; \Phi; \Gamma \vdash \phi : t$ sym; by the IH, we know that ϕ steps to a non-$\bot$ value v well typed at t sym; by ϕ-Promote we can see that v is also well typed at t smt.

(ϕ-Unquote) We have $,e$; since $\Delta; \Phi; \Gamma \vdash e : \tau$, we know by the IH that e reduces to a non-$\bot$ value v that is also well typed at τ. We can therefore rule out $\Downarrow_\phi$-Unquote-E, so we must have stepped by $\Downarrow_\phi$-Unquote.

Since $\Delta; \Phi; \Gamma \vdash v : \tau$ and $\Gamma \vdash_{\mathsf{smt}} \tau$, we have $\Delta; \Phi; \Gamma \vdash \mathrm{toSMT}(v) : \mathrm{toSMT}(\tau)$ by Lemma D.10, as desired.

(ϕ-Ctor) We have $c_{\mathsf{c}}^{\mathsf{SMT}}(\vec{\phi_i})$ such that $\Gamma \vdash c_{\mathsf{c}}^{\mathsf{SMT}} : \vec{\tau_i} \to \tau$ and $\Gamma \vdash \phi_i : \tau_i$. We know by the IH that each ϕ_i is well typed at τ_i and so none of them step to $\bot$, and so $\Downarrow_\phi$-Ctor-E cannot apply.

Therefore either $\Downarrow_\phi$-Ctor or $\Downarrow_\phi$-Value applied; the resulting value is well typed by the IH or remains well typed, respectively.

Functions. By part (1) on $\vec{\alpha_j}, \overrightarrow{X_i : \tau_i} \vdash e : \tau$, using weakening (Lemma D.6) to recover typing in Γ.

Vectored expressions and formulas. By induction on the vector length, using parts (1) and (2) in each case. □

Lemma E.3 (Value unification preservation). *If* $\Gamma \models \theta$ *when either:*

(1) $\Gamma \vdash \vec{X}, \vec{\tau} \rhd \Gamma'$ *and* $\Gamma \vdash \vec{v} : \vec{\tau}$ *and* $\theta \vdash \vec{X} \sim \vec{v} : \theta'$*; or*
(2) $\Gamma \vdash X, \tau \rhd \Gamma'$ *and* $\Gamma \vdash v : \tau$ *and* $\theta \vdash X \sim v \rhd \theta'$*;*

then $\Gamma' \models \theta'$.

Proof. By induction on the derivation of well typing.

($X\tau$-Bind) Only uv-Bind-Var could have applied, so we have $\Gamma \vdash v : \tau$ and $\Gamma \models \theta$ and must show that $\Gamma, X : \tau \models \theta[X \mapsto v]$, which we have immediately.

($X\tau$-Check) Here $X \in \Gamma$, so it must be that $\theta(X)$ is defined. One of three rules could have applied:

(uv-Eq-Var) We have $\Gamma' = \Gamma$ and $\theta' = \theta$, so $\Gamma' \models \theta'$ by assumption.

(uv-Ctor) By the IH, we know that $\Gamma' \mathit{models} \theta'$.

(uv-Constant) As for uv-Eq-Var, we have $\Gamma' = \Gamma$ and $\theta' = \theta$, so $\Gamma' \models \theta'$ by assumption.

($X\tau$-All) It must be that $\vec{u}\vec{v}$-All applied; by the IH on each sub-derivation, we can find that $\Gamma_i \models \theta_i$, and so $\Gamma' \models \theta'$ in particular.

□

User code will never *directly* trigger a use of uv-Eq-Var directly, because the unification rules won't call value unification with a defined LHS (we'd just use uu-BB instead). But a use of $\vec{u}\vec{v}$-All could lead to a variable being unified early on and then used again in the same unification process.

Lemma E.4 (Premise preservation and safety). *If* $\Delta;\Phi;\Gamma \vdash P \rhd \Gamma'$ *and* $\Delta;\Phi \models \vec{F}$ *and* $\Delta;\Phi \models \mathcal{W}$ *and* $\Gamma \models \theta$ *then if* $\vec{F};\mathcal{W};\theta \vdash P \to \theta'_\perp$ *then:*

(1) $\theta'_\perp = \theta'$ *(i.e., it is not* $\perp$*); and*
(2) $\Gamma' \models \theta'$.

Proof. By induction on the premise typing derivation, followed by cases on the step taken.

(P-PosAtom) We have:

$$p \subseteq \vec{\tau_i} \in \Phi \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'$$

The only rule that could have applied is PosAtom, i.e., $\vec{v} \in \mathcal{W}(p)$ and $\theta \vdash \vec{X_i} \sim \vec{v_i} : \theta'_\perp$. We must show that $\theta'_\perp = \theta'$ and $\Gamma' \models \theta'$.

Since $\Delta;\Phi \models \mathcal{W}$, we know that $\cdot \vdash \vec{v_i} : \vec{\tau_i}$; by weakening we have $\Gamma \vdash \vec{v_i} : \vec{\tau_i}$ (Lemma D.6).

Syntactically, we know that $\vec{X_i}$ are all variables and that $\vec{v_i}$ are all values. For each one, therefore only two unification rules could possibly apply: uu-BB (X_i is bound) and uu-FB (X_i is free). In particular, uu-FF cannot apply, and so we cannot produce $\perp$, so $\theta'_\perp = \theta' = \theta\vec{\theta_i}$. By Lemma E.3, we know that $\Gamma' \models \theta\theta_i$ for each i, and so $\Gamma' \models \theta\vec{\theta_i}$.

(P-NegAtom) We have:

$$p \subseteq \vec{\tau_i} \in \Phi \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma$$

Two rules are possible: NegAtom and NegAtom-E. We must show that the latter cannot apply and that the former preserves typing.

Since $\Gamma \models \theta$, it must be that case that each $\vec{X_i} \in \mathrm{dom}(\theta)$, and so NegAtom-E cannot have applied. It remains to be seen that $\Gamma \models \theta'$—but in NegAtom we have $\theta = \theta'$, and so we are done.

(P-EqCtor-BF) We have:

$$\Delta(D) = \forall\vec{\alpha_j}, \{\ldots, c : \vec{\tau_i}, \ldots\}$$
$$\Gamma \vdash Y, \tau[\vec{\tau'_j}/\vec{\alpha_j}] \rhd \Gamma \qquad \vec{X_i} \not\subseteq \Gamma \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i}[\vec{\tau'_j}/\vec{\alpha_j}] \rhd \Gamma'$$

The only rule that could have applied is EqCtor, where $\theta \vdash Y\ c(\vec{X_i}) : \theta'_\perp$. We must show that $\theta'_\perp = \theta'$ (i.e., it is not $\perp$) and that $\Gamma' \models \theta'$.

Since $\Gamma \vdash Y, \tau[\vec{\tau'_j}/\vec{\alpha_j}] \rhd \Gamma$, it must be the case that $Y \in \mathrm{dom}(\Gamma)$ and so $\theta(Y) = v$ (and so $\cdot \vdash v : \tau[\vec{\tau'_j}/\vec{\alpha_j}]$, which also holds under Γ thanks to weakening (Lemma D.6)).

Only two rules could have applied to show $\theta \vdash Y\ c(\vec{X_i}) : \theta'_\perp$: uu-BF (when some of $\vec{X_i}$ are unbound) or uu-BB (when all of the $\vec{X_i}$ are bound). In either case, uu-FF can't have a applied, and so $\theta'_\perp = \theta'$.

One of two rules could have applied: uv-Eq-Var or uv-Ctor.

In the former case, we applied uu-BB, because $\theta(c(\vec{X_i})) = c(\vec{v_i})$. We have $\theta' = \theta[X \mapsto c(\vec{v_i})$ and $\Gamma' \models \theta'$ by substitution on $\Gamma \vdash \vec{X_i}, \vec{\tau_i}[\vec{\tau'_j}/\vec{\alpha_j}] \rhd \Gamma'$ (Lemma D.8).

In the latter case, we can find that $\Gamma' \models \theta'$ by Lemma E.3 on the assumption that $\Gamma \vdash \vec{X_i}, \vec{\tau_i}[\vec{\tau'_j}/\vec{\alpha_j}] \rhd \Gamma'$, and the fact $\theta(Y) = v$ is well typed in Γ.

(P-EqSMT-BF) We have:

$$\Gamma \vdash c^{\mathsf{SMT}}_{c'} : \vec{\tau_i} \to \tau \qquad \Gamma \vdash Y, \tau \rhd \Gamma \qquad \vec{X_i} \not\subseteq \Gamma \qquad \Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'$$

The only rule that could have applied is EqSMT, where $\theta \vdash Y \sim c^{\mathsf{SMT}}_{c'}(\vec{X_i}) : \theta'_\perp$. We must show that $\theta'_\perp = \theta'$ (i.e., it is not $\perp$ and that $\Gamma \models \theta'$.

Since $\Gamma \vdash Y, \tau \rhd \Gamma$, it must be the case that $Y \in \mathrm{dom}(\Gamma)$ and so $\theta(Y) = v$. We can conclude that $\cdot \vdash v : \tau$ and so $\Gamma \vdash v : \tau$ (Lemma D.6).

Only two rules could have applied to show $\theta \vdash Y\ c^{\mathsf{SMT}}_{c'}(\vec{X_i}) : \theta'_\perp$, noting the removal of the unquote, since unification doesn't care: *uu*-BF (when some of $\vec{X_i}$ are unbound) or *uu*-BB (when all of the $\vec{X_i}$ are bound). In either case, *uu*-FF can't have a applied, and so $\theta'_\perp = \theta'$.

It remains to show that $\Gamma \models \theta'$. If the outer unification rule was *uu*-BB, we have $\theta = \theta'$ and so $\Gamma \models \theta'$ by assumption. If outer unification rule was *uu*-BF, one of two rules could have applied to find value unification: either *uv*-Eq-Var or *uv*-Ctor.

In the former case, we apply *uu*-BB inside, because $\theta(Y) = c^{\mathsf{SMT}}_{c'}(\vec{v_i})$. We have $\theta' = \theta[X \mapsto c^{\mathsf{SMT}}_{c'}(\vec{v_i})$ and $\Gamma' \models \theta'$ by substitution on $\Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'$ (Lemma D.8).

In the latter case, we can find that $\Gamma' \models \theta'$ by Lemma E.3 on the assumption that $\Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma'$, and the fact $\theta(Y) = v$ is well typed in Γ.

(P-Eq-FB) We have:

$$\Gamma \vdash e : \tau \qquad \Gamma \vdash Y, \tau \rhd \Gamma'$$

The two possible rules are EqExpr and EqExpr-E. We must show that the latter could not have applied (and so $\theta'_\perp = \theta'$) and that $\Gamma' \models \theta'$. By Lemma E.2, we know that EqExpr-E cannot apply and that $\mathcal{W}; \theta \vdash e \Downarrow_e v$ (and so $\Gamma \vdash v : \tau$).

Since v is a value, either *uu*-FB or *uu*-BB applied, depending on whether or not Y is bound. Either way, *uu*-FF couldn't have applied, and so $\theta'_\perp = \theta'$.

We can find that $\Gamma' \models \theta'$ by Lemma E.3 on $\Gamma \vdash Y, \tau \rhd \Gamma'$ (along with the well typing of v).

(P-NegEq) We have $\Gamma \vdash e : \tau$ and $\Gamma \vdash Y, \tau \rhd \Gamma$. By Lemma E.2, we know that NegEqExpr-E1 cannot apply and that $\mathcal{W}; \theta \vdash e \Downarrow_e v$ (and so $\Gamma \vdash v : \tau$). Since $\Gamma \models \theta$, it must be that case that $Y \in \mathrm{dom}(\theta)$, and so NegAtom-E2 cannot have applied. It remains to be seen that $\Gamma \models \theta'$—but in NegExpr we have $\theta = \theta'$, and so we are done. □

Lemma E.5 (Identical bindings implies containment). *If* $\Gamma \vdash X, \tau \rhd \Gamma$, *then* $X \in \mathrm{dom}(\Gamma)$. *Similarly, if* $\Gamma \vdash \vec{X_i}, \vec{\tau_i} \rhd \Gamma$, *then* $\vec{X_i} \subseteq \mathrm{dom}(\Gamma)$.

Proof. By induction on the derivation.

($X\tau$-Bind) Contradictory: this rule could not have applied, since $\Gamma \neq \Gamma, X : \tau$.

($X\tau$-Check) We have $X \in \mathrm{dom}(\Gamma)$ by assumption.

($\vec{X}\vec{\tau}$-All) By the IH on each of our premises. □

Theorem E.6 (Program safety). *If* $\Delta; \Phi \vdash \vec{F_i}\ \vec{H_j}$ *and* $\Delta; \Phi \models \mathcal{W}$ *then for all* $H \in \vec{H_j}$, $\neg(\vec{F_i}; \mathcal{W} \vdash H \to \perp)$.

Proof. The program prog = $\vec{F}_i\ \vec{H}_j$ must have been well typed according to prog-WF, and so we have $\vdash \Delta$ and $\vdash \Phi$ along with derivations for each F and H:

$$\begin{array}{ccccccc} \Delta;\Phi \vdash F_0 & \ldots & \Delta;\Phi \vdash F_i & \ldots & \Delta;\Phi \vdash F_n \\ \Delta;\Phi \vdash H_0 & \ldots & \Delta;\Phi \vdash H_j & \ldots & \Delta;\Phi \vdash H_m \end{array}$$

Let an $H = p(X_k) :- \vec{P}_\ell \in \vec{H}_j$ be given. We know that $\Delta;\Phi \vdash H$ by H-Clause, i.e.:

$$\begin{array}{ccccc} \cdot \vdash P_0 \rhd \Gamma_1 & \ldots & \Gamma_\ell \vdash P_\ell \rhd \Gamma_{\ell+1} & \ldots & \Gamma_p \vdash P_p \rhd \Gamma' \\ & & p \subseteq \vec{\tau_k} \in \Phi & \Gamma' \vdash \vec{X_k}, \vec{\tau_k} \rhd \Gamma' & \end{array}$$

Let $\mathcal{W}$ be given such that $\Delta;\Phi \models \mathcal{W}$. We must show that it is not the case that $\vec{F}_i;\mathcal{W} \vdash H \to \bot$, i.e., Clause-E1 and Clause-E2 cannot apply. We can rule out Clause-E1 by Lemma E.4(1: it is not the case that a typesafe premise steps to $\bot$. To rule out Clause-E2, we need to know that if we can build a final substitution, i.e.:

$$\cdot \vdash P_0 \to \theta_1 \quad \ldots \quad \theta_\ell \vdash P_\ell \to \theta_{\ell+1} \quad \ldots \quad \theta_p \vdash P_p \to \theta$$

then $\vec{X_k} \in \mathrm{dom}(\theta)$. We know that $\vec{X_k} \subseteq \mathrm{dom}(\Gamma')$ by Lemma E.5 on $\Gamma' \vdash \vec{X_k}, \vec{\tau_k} \rhd \Gamma'$; since $\Gamma_p \vdash P_p \rhd \Gamma'$, we know by Lemma E.4(2) that $\Gamma' \models \theta$. We can therefore conclude that $\forall X \in \mathrm{dom}(\Gamma'),\ X \in \mathrm{dom}(\theta)$, and so $\vec{X_k} \in \mathrm{dom}(\theta)$... and Clause-E2 cannot apply. □

Theorem E.7 (Program preservation). *If $\Delta;\Phi \vdash \vec{F}_i\ \vec{H}_j$ and $\Delta;\Phi \models \mathcal{W}$ and $\vec{F}_i;\mathcal{W} \vdash H \to \mathcal{W}'$ for some $H \in \vec{H}_j$ then $\Delta;\Phi \models \mathcal{W}'$.*

Proof. The program prog = $\vec{F}_i\ \vec{H}_j$ must have been well typed according to prog-WF, and so we have $\vdash \Delta$ and $\vdash \Phi$ along with derivations for each F and H:

$$\begin{array}{ccccccc} \Delta;\Phi \vdash F_0 & \ldots & \Delta;\Phi \vdash F_i & \ldots & \Delta;\Phi \vdash F_n \\ \Delta;\Phi \vdash H_0 & \ldots & \Delta;\Phi \vdash H_j & \ldots & \Delta;\Phi \vdash H_m \end{array}$$

Let an $H = p(X_k) :- \vec{P}_\ell \in \vec{H}_j$ be given. We know that $\Delta;\Phi \vdash H$ by H-Clause, i.e.:

$$\begin{array}{ccccc} \cdot \vdash P_0 \rhd \Gamma_1 & \ldots & \Gamma_\ell \vdash P_\ell \rhd \Gamma_{\ell+1} & \ldots & \Gamma_p \vdash P_p \rhd \Gamma' \\ & & p \subseteq \vec{\tau_k} \in \Phi & \Gamma' \vdash \vec{X_k}, \vec{\tau_k} \rhd \Gamma' & \end{array}$$

Let $\mathcal{W}$ be given such that $\Delta;\Phi \models \mathcal{W}$. It must have been the case that we stepped by Clause, and so:

$$\begin{array}{c} \cdot \vdash P_0 \to \theta_1 \quad \ldots \quad \theta_i \vdash P_i \to \theta_{i+1} \quad \ldots \quad \theta_n \vdash P_n \to \theta \\ \mathcal{W}' = \mathcal{W}[p \mapsto \mathcal{W}(p) \cup \theta(\vec{X_j})] \end{array}$$

By Lemma E.4(2), we know that $\Gamma_i \models \theta_i$ and $\Gamma' \models \theta$. We have $\vec{X_k} \subseteq \mathrm{dom}(\Gamma')$ by Lemma E.5 on $\Gamma' \vdash \vec{X_k}, \vec{\tau_k} \rhd \Gamma'$, we can conclude that $\vec{X_k} \subseteq \mathrm{dom}(\theta)$ and that $\Delta;\Phi;\cdot \vdash \theta(X_k) : \tau_k$ by Lemma E.3 on $\Gamma' \vdash \vec{X_k}, \vec{\tau_k} \rhd \Gamma'$.

To see that $\Delta;\Phi \models \mathcal{W}$, we need to see that adding $\theta(\vec{X_k})$ to $\mathcal{W}(p)$ is safe. We already knew that $p \subseteq \vec{\tau_k} \in \Phi$ and $p \in \mathrm{dom}(\mathcal{W})$; we have $k = k$ immediately, and we have seen that each $\theta(X_k)$ is well typed at τ_k. □

F MODEL-THEORETIC SEMANTICS

We have focused on the operational semantics of Formulog, as it helps us to reason about type safety. However, since we have kept Formulog close to Datalog, it is also possible to give a model-theoretic semantics to a Formulog program. First, all ML functions and expressions are desugared into Datalog rules; this translation is relatively straightforward, with the trickiest part being the translation of non-mutually exclusive patterns occurring in match expressions. For each primitive

operator, we introduce a (possibly infinite) EDB relation that defines that operator; for example, the addition operator `+` is represented through a ternary relation `add(`x`,`y`,`z`)`, which states that z is the sum of x and y. Terms of the form $p(w^*)$ (i.e., invocations of predicates as functions) are translated to aggregate predicates. Formulog requires the use of these terms, as well as negation, to be stratified; thus, the program resulting from the translation can be given a perfect model semantics in line with stratified negation [Apt et al. 1988; Przymusinski 1988; Van Gelder 1989] and stratified aggregation [Mumick et al. 1990].

For a small example, consider this Formulog program:

```
fun length(Xs: 'a list) : bv[32] =
  match Xs with
  | [] => 0
  | _ :: T => 1 + length(T)
  end
ok :- length([1, 2, 3]) = 3.
```

This would be translated into a program like this:

```
length([], 0).
length(_ :: T, Z) :-
  length(T, L),
  add(1, L, Z).
ok :- length([1, 2, 3], 3).
```

Note that the rules defining the `length` predicate violate the range restriction, and in fact define an infinite relation. This does not pose a fundamental problem to the model theory. To make this program evaluable, we could rewrite the `length` predicate's definition (and its uses) via the magic set transformation; the resulting relations would meet the range restriction. While the magic set transformation can turn a stratified program into a non-stratified program, there are techniques to either restore stratification [Meskes and Noack 1993] or correctly evaluate the non-stratified program [Mumick et al. 1990].