A Verified Type System for CakeML

Yong Kiam Tan
IHPC, A*STAR
tanyk@ihpc.a-star.edu.sg

Scott Owens
University of Kent
S.A.Owens@kent.ac.uk

Ramana Kumar
NICTA and UNSW
Ramana.Kumar@nicta.com.au

ABSTRACT

CakeML is a dialect of the (strongly typed) ML family of programming languages, designed to play a central role in high-assurance software systems. To date, the main artefact supporting this is a verified compiler from CakeML source code to x86-64 machine code. The verification effort addresses each phase of compilation from parsing through to code generation and garbage collection.

In this paper, we focus on the type system: its declarative specification, type soundness theorem, and the soundness and completeness of an implementation of type inference – all formally verified in the HOL4 proof assistant. Each of these aspects of a type system is important in any design and implementation of a typed functional programming language. They allow the programmer to soundly employ (informal) type-based reasoning, and the compiler to apply optimisations that assume type-correctness. So naturally, their verification is a critical part of a verified compiler.

CCS Concepts

•**Theory of computation** → **Logic and verification;** *Type theory;*
•**Software and its engineering** → *Functional languages;*

Keywords

Type inference; Compiler verification; ML

1. CONTEXT

A formally verified compiler comes with a proven theorem that any observable behaviour of the object code is a permissible behaviour of the source code. Put more colloquially, we know that a verified compiler introduces no bugs. When we are concerned with the proper functioning of a safety- or security-critical software system, using a verified compiler means that we do not have to inspect what the compiler is doing. This can make building an assurance case for the system easier. If we have gone to the extent of formally verifying the system, then we know – without any lower confidence – that the system as actually executed has the properties we verified about it.

IFL '15, September 14 - 16, 2015, Koblenz, Germany

ISBN 978-1-4503-4273-5/15/09...$15.00

DOI: http://dx.doi.org/10.1145/2897336.2897344

Since 2012, the CakeML project (https://cakeml.org) has been building a verified compiler for an ML-like programming language. The overall goal is to create an optimising compiler with mechanically checked proofs of an end-to-end correctness theorem. An important additional goal is to verify (again with mechanically checked proofs) that the correctness theorem applies to the code of the compiler that is actually executed, and not just to the compilation algorithm in the abstract. Here 'end-to-end' means that the correctness theorem relates source code, represented as a string, with machine code, represented as a list of bytes. Thus, the verification must address a lexer, a parser, a type checker, a sequence of optimisations and translations between various intermediate languages, a code generator, and a run-time system. A previous paper [5] outlined how all of these phases fit together, and detailed the interactive theorem proving techniques used to verify a non-optimising version of the compiler.

In this paper, we focus on the type checking phase of the compiler. The external interface to the type checker is simple. Given (an AST for) a program, it returns a boolean: whether the program obeys CakeML's typing discipline. Its importance stems from the type soundness theorem which guarantees that well-typed programs have well-defined semantics.[1] This is important for any typed programming language: most compilers assume that the input program has well-defined semantics, and make optimisation decisions based on that. It is doubly important in the context of verified compilers: their correctness theorem has a well-definedness pre-condition, and so we cannot use the theorem until we first prove that the source program is well-defined. For some languages, well-definedness is an undecidable property (e.g., C), but for CakeML (and type-safe languages in general), a type inference algorithm can prove that the program obeys the typing discipline. The type soundness theorem then allows us to dispense with the pre-condition and give a compiler correctness theorem that applies to all programs, and characterises which ones the compiler will accept/reject during type checking.

Contributions.

Our previous work [5] briefly mentioned CakeML's type checker, which at that point had a type soundness theorem, and an inferencer soundness theorem, but not an inferencer completeness theorem. Here, we give a thorough account of these theorems, and additionally present

- a completeness theorem for the inferencer,
- an improved type system that dispenses with the elaboration phase,

[1] Equivalently, well-typed programs do not crash, get stuck, go wrong, have undefined behaviour, etc.

- an improved type soundness proof for an operational semantics with more uniform handling of data constructors and modules,
- support for a few extra language features, especially type abbreviations, and
- the design constraints imposed by combining the value restriction with principal typings (§3.3).

On the proofs.

All of the theorems in this paper have been mechanically verified in the HOL4 theorem prover and are available from CakeML's code repository (https://code.cakeml.org). The type system's definition is in the `semantics` directory, along with the operational semantics; the type soundness proof is in the `semantics/proofs` directory; and everything to do with the inferencer is in the `compiler/inference` directory. Overall the big technical challenges were in properly formulating the theorem statements and invariants, rather than in applying theorem proving technology, and so the former is our focus here.

Contents.

We first describe the CakeML language itself (§2), then we give a declarative type system (§3) with a corresponding type inference algorithm (§4). Then we move on to the correctness proofs: soundness and completeness for the inferencer with respect to the type system (§5), and type soundness with respect to an operational semantics via preservation and progress lemmas (§6).

2. THE CAKEML LANGUAGE

CakeML is a strongly typed, strict, impure functional language that mostly follows the design of Standard ML (SML) [10]. It supports a substantial subset of the core language features including (possibly mutually) recursive datatypes, higher-order functions, pattern matching, references, and exceptions. Notable omissions are records, and local (non-top-level) definitions of datatypes and exceptions. The module system supports non-nested structures and signatures, but not functors. See Fig. 1 for the syntax.

CakeML has a small-step operational semantics based on a CEK machine [3], and it also has a big-step semantics that is proven equivalent. Most of our compiler proofs use the latter semantics, while the type soundness proof uses the small-step semantics. There are a few minor differences in behaviour to SML which are not relevant to us here.

3. TYPE SYSTEM

CakeML has a declarative type system defined by a syntax-directed, inductively defined relation. The type system has four relevant simplifications: it does not support equality types, type annotations, operator overloading, or let polymorphism. Top-level and module-top-level definitions can be polymorphic, and we plan to add support for polymorphic let bindings and type annotations in the future. Fig. 2 gives the definition of the various environments and the shape of the main judgements.

Typing environments Γ_t are records containing four different sub-environments M, T, C and V in fields called `m`, `t`, `c`, and `v` respectively. The definition typing judgements build environment fragments that describe the defined things, and we refer to those using m, τ, c and vs.

Type definition environments T support type abbreviations, mapping a type constructor name to the type that it abbreviates, along

$$
\begin{array}{lcl}
op & := & \texttt{div} \mid \texttt{mod} \mid \texttt{+} \mid \texttt{-} \mid \texttt{<} \mid \texttt{>} \mid \texttt{<=} \mid \texttt{>=} \mid \texttt{<>} \mid \texttt{=} \mid \texttt{:=} \mid \texttt{::} \\
 & \mid & \texttt{andalso} \mid \texttt{orelse} \\
id & := & x \mid mn\texttt{.}x \\
cid & := & cn \mid mn\texttt{.}cn \\
t & := & \alpha \mid id \mid t\ id \mid \texttt{(}t\texttt{,}t\texttt{(,}t\texttt{)*)}\ id \mid t\ \texttt{*}\ t \mid t\ \texttt{->}\ t \mid \texttt{(}t\texttt{)} \\
l & := & Const \mid \texttt{()} \mid \texttt{[]} \\
p & := & x \mid l \mid cid \mid cid\ p \mid \texttt{\_} \mid \texttt{(}p\texttt{(,}p\texttt{)*)} \mid \texttt{[}p\ \texttt{(,}p\texttt{)*]} \mid p\ \texttt{::}\ p \\
e & := & l \mid id \mid cid \mid cid\ e \mid \texttt{(}e\texttt{,}e\ \texttt{(,}e\texttt{)*)} \mid \texttt{[}e\ \texttt{(,}e\texttt{)*]} \\
 & \mid & \texttt{raise}\ e \mid e\ \texttt{handle}\ p\ \texttt{=>}\ e\ \texttt{(|}\ p\ \texttt{=>}\ e\texttt{)*} \\
 & \mid & \texttt{fn}\ p\ \texttt{=>}\ e \mid e\ e \mid e\ op\ e \mid \texttt{((}e\ \texttt{;)*}\ e\texttt{)} \\
 & \mid & \texttt{if}\ e\ \texttt{then}\ e\ \texttt{else}\ e \mid \texttt{case}\ e\ \texttt{of}\ p\ \texttt{=>}\ e\ \texttt{(|}\ p\ \texttt{=>}\ e\texttt{)*} \\
 & \mid & \texttt{let}\ \texttt{(}ld\ \texttt{|}\ \texttt{;)*}\ \texttt{in}\ \texttt{(}e\ \texttt{;)*}\ e\ \texttt{end} \\
ld & := & \texttt{val}\ x\ \texttt{=}\ e \mid \texttt{fun}\ x\ p^{+}\ \texttt{=}\ e\ \texttt{(and}\ x\ p^{+}\ \texttt{=}\ e\texttt{)*} \\
c & := & cn \mid cn\ \texttt{of}\ t \\
tyd & := & tyn\ \texttt{=}\ c\ \texttt{(|}\ c\texttt{)*} \\
tyn & := & \texttt{(}\alpha\texttt{(,}\alpha\texttt{)*)}\ x \mid \alpha\ x \mid x \\
d & := & \texttt{val}\ p\ \texttt{=}\ e \mid \texttt{fun}\ x\ p^{+}\ \texttt{=}\ e\ \texttt{(and}\ x\ p^{+}\ \texttt{=}\ e\texttt{)*} \\
 & \mid & \texttt{datatype}\ tyd\ \texttt{(and}\ tyd\texttt{)*} \mid \texttt{type}\ tyn\ \texttt{=}\ t \\
 & \mid & \texttt{exception}\ c \\
sl & := & \texttt{val}\ x\ \texttt{:}\ t \mid \texttt{type}\ tyn\ \texttt{(=}\ t\texttt{)}^{?} \mid \texttt{datatype}\ tyd\ \texttt{(and}\ tyd\texttt{)*} \\
sig & := & \texttt{:>}\ \texttt{sig}\ \texttt{(}sl\ \texttt{|}\ \texttt{;)*}\ \texttt{end} \\
top & := & \texttt{structure}\ mn\ sig^{?}\ \texttt{=}\ \texttt{struct}\ \texttt{(}d\ \texttt{|}\ \texttt{;)*}\ \texttt{end;} \mid d\texttt{;} \\
prog & := & top^{*}
\end{array}
$$

where x ranges over identifiers (must not start with a capital letter and must not be an infix operator from op), α over SML-style type variables (*e.g.*, `'a`), cn over constructor names (must start with a capital letter, or be `true`, `false`, `ref`, or `nil`), mn over module names, and $Const$ over integer, string and character constants. We use $^{?}$ to denote things that are optional.

Figure 1: CakeML syntax

Let $\hat{t}$ be a de Bruijn indexed version of t. That is, instead of containing named type variables `'a`, `'b`, etc., $\hat{t}$ types contain natural number de Bruijn indices.
We need the following environments, and auxillaries:

$stamp$	:=	$id \mid cid$	stamps
$\hat{V}$	:=	ϵ	empty type env.
	$\mid$	$\mathbb{N}, \hat{V}$	bind de Bruijn type variables
	$\mid$	$x : \langle \mathbb{N}, \hat{t} \rangle, \hat{V}$	bind a type scheme

$T \equiv id \mapsto (\alpha^{*} \times t)$	type def. env.
$M \equiv mn \mapsto (x \times \mathbb{N} \times \hat{t})\ \texttt{list}$	module env.
$C \equiv cid \mapsto (\alpha^{*} \times t^{*} \times stamp)$	constructor env.

We will use V to refer to the subset of $\hat{V}$ that has no de Bruijn type variable bindings (the second line above). Similarly, $\hat{\Gamma}_t$ are typing environments whose variable environments are of the form $\hat{V}$. Type schemes are pairs containing the number of bound de Bruijn indices and a (de Bruijn-indexed) type.
Typing judgements:

$\mathbb{N},\ C \vdash_p p : \hat{t},\ vs$	pattern typing
$\hat{\Gamma}_t \vdash_e e : \hat{t}$	expression typing
$u,\ mn^{?},\ \delta,\ \Gamma_t \vdash_d d : \delta',\ (\tau\texttt{,}c\texttt{,}vs)$	definition typing
$u,\ \delta,\ \Gamma_t \vdash_t top : \delta',\ (m\texttt{,}\tau\texttt{,}c\texttt{,}vs)$	top-level typing

Figure 2: Typing judgements

with a list of type parameters. A type definition can appear inside of a module, or at the top-level, so the module name mn is optional. Since CakeML does not have nested structures, all identifiers either refer to the current module or a different top-level module, and so use optional module names rather than a list of module names. Constructor environments C similarly record information for all constructors introduced by a `datatype` or `exception` definition. They record the type's parameters, the types of the constructors arguments, which may refer to the type parameters. Each constructor is given a *stamp*, that either records which type the constructor creates (for datatype constructors) or which exception it is (for exception constructors).

Module environments M map module names to the list of identifiers defined in that module, along with their type schemes. Since type variables are represented using de Bruijn indices, we use a number rather than a set of syntactic type variables, to represent how many of them are quantified in the type scheme. Finally, variable environments $\hat{V}$ map variables to type schemes, but retain enough structure to record where new type variables are bound. This structural information is only needed at the expression level so we distinguish between $\hat{\Gamma}_t$ used in expressions typing and Γ_t used for everything above that. Because of this separation, M and V are kept as distinct environments rather than using id or cid as the domain of a finite map as in T and C.

Definition environments δ are records containing the set of names of defined modules, the set of identifiers for defined types and the set of identifiers for defined exceptions. The fields are named `defined_mods`, `defined_types` and `defined_exns` respectively.

We will see more detail on how stamps and δ work in the discussion of the typing rules in §3.2. Their purpose is to separate the notion of globally unique identity for each module, type, and constructor from the scoping mechanisms of the language. The Definition of Standard ML [10] uses a stamp generation mechanism for this purpose, but this kind of stateful computation tends to complicate proofs, so we instead adopt a mild syntactic restriction. Top-level modules must have unique names, and the types defined inside a module must have different names from each other. Thus, fully qualified names of types are unique, and can be directly used as stamps. Since we do not support (generative, higher-order) functors, we can avoid stamp generation without having to implement the kind of sophisticated module system calculus that more typically supports the purely syntactic (i.e., stamp-generation-free) approach [4, 8].

The next sections explain the typing rules in more detail. As a running example, we shall examine how the top-level definition, `val k = fn x => fn y => x`, is typed. Note that we use syntactic type variables, e.g. `'a`, in our exposition although the formalisation actually uses de Bruijn indices.

3.1 Expressions

The pattern- and expression-level typing judgements are mostly typical, with the structure of $\hat{V}$ being perhaps the only surprising thing. Expression typing gives a type to an expression in a context, whereas pattern typing gives a type to a pattern in a context, and also gives types for all of the variables bound by the pattern. Fig. 3 gives the rules for pattern and expression variables, functions, and `let` expressions, to show how $\hat{V}$ is used.

The Fun rule binds a type scheme with no quantified type variables[2], and a type whose free variables are also bound in $\hat{V}$. The

$$\text{(Pvar)}\ \frac{\texttt{check\_freevars}\ tvs\ []\ t}{tvs,\ C \vdash_p x : t,\ [(x,t)]}$$

$$\text{(Var)}\ \frac{\begin{array}{c} tvs = \texttt{LENGTH}\ ts \\ \texttt{EVERY (check\_freevars (num\_tvs}\ \hat{\Gamma}_t\texttt{.v) [])}\ ts \\ \texttt{lookup}\ x\ \hat{\Gamma}_t = \texttt{SOME}\ (tvs,t) \end{array}}{\hat{\Gamma}_t \vdash_e x : \texttt{deBruijn\_subst}\ ts\ t}$$

$$\text{(Fun)}\ \frac{\begin{array}{c} \texttt{check\_freevars (num\_tvs}\ \hat{\Gamma}_t\texttt{.v) []}\ t_1 \\ \hat{\Gamma}_t, x : (0,t_1) \vdash_e e : t_2 \end{array}}{\hat{\Gamma}_t \vdash_e \texttt{fn}\ x\ \texttt{=>}\ e : t_1\ \texttt{->}\ t_2}$$

$$\text{(Let)}\ \frac{\begin{array}{c} \hat{\Gamma}_t \vdash_e e_1 : t_1 \\ \hat{\Gamma}_t, x : (0,t_1) \vdash_e e_2 : t_2 \end{array}}{\hat{\Gamma}_t \vdash_e \texttt{let}\ x = e_1\ \texttt{in}\ e_2 : t_2}$$

Figure 3: Selected pattern and expression typing rules

free variable restriction is checked by `check_freevars`, whose first argument limits the free variables, and `num_tvs` which returns the number of bound type variables in the typing environment. The second argument to `check_freevars` is used to rule out syntactic type variables which should not occur internal to the type system. Because the Let rule is monomorphic, it similarly uses no quantified type variables in the type scheme of x.

The Var rule finds the type scheme bound to the identifier in the M or $\hat{V}$ environments, depending on whether the identifier has a module name or not. It can then make an arbitrary instantiation of the tvs quantified type variables as long as their free variables are all bound in $\hat{V}$.

Using two applications of Fun and one application of Var, we can derive a number of types for the RHS expression in our example, e.g. `int -> int -> int`, `'a -> 'a -> 'a` and `'a -> 'b -> 'a`, as long as `'a` and `'b` are bound in the $\hat{\Gamma}_t$ that we use.

The pattern typing rules are used for top-level definitions and for expression-level pattern matches. They return a type for the whole pattern, and a list of variables bound in the pattern along with their types. The types chosen for the variables satisfy all of the pattern's typing constraints. In the simplest case, the Pvar rule allows a single pattern variable, like k, to be given any type t whose free variables are bound by tvs (recall the de Bruijn representation). It then returns t, along with a singleton list, $[(k,t)]$.

3.2 Definitions

Fig. 4 presents the rules for top-level (and module-top-level) definitions. It omits the rule for `fun` definitions, which is similar to the Dlet_poly rule, but specialised to making recursive functions. It also specialises the Dtype rule to a single recursive datatype, whereas the actual rule in CakeML handles a list of mutually recursive datatypes.

There are two rules for value definitions, since CakeML, with its imperative features, has a value restriction. Both rules ensure that the LHS pattern does not try to bind the same value twice, ensure that the pattern and expression have the same type, and then return the pattern's variable bindings. Neither, defines any new modules, types, or constructors so there are no new identifiers in

[2]We use $\hat{\Gamma}_t, x : (tvs, t)$ to mean $\hat{\Gamma}_t$ with its variable environment field extended with the mapping of x to the type scheme (tvs, t).

their conclusions. The DLET_MONO rule binds 0 new type variables when performing the pattern and expression typing judgements, so that the resulting types from these judgements will not have any type variables. It then uses `add_tvs` to convert each of the types in vs in to type schemes with 0 quantified type variables. In contrast, DLET_POLY binds tvs type variables in its premises and it uses `add_tvs` to generate type schemes with tvs bound type variables. The last premise of each rule is used to ensure determinism with the value restriction, which we explain further in §3.3. The u parameter is used to control whether these checks should be carried out; more detail on that in §6.

Since the RHS expression of our running example is a value, DLET_POLY is used to type it. Setting the tvs parameter to 2 allows PVAR to give `k` a polymorphic type with two bound type variables, `'a -> 'b -> 'a`, which is one of the possible types for the RHS expression. This would not be possible with DLET_MONO, since the number of type variables is explicitly set to 0.

The rule for type abbreviations (DTABBREV) checks that the abbreviated type is well formed i.e. that the raw type variables it mentions are bound in $targs$. It introduces no new modules, data types, or constructors. It binds the name of the abbreviation in the type definition environment, after first expanding out all of the other abbreviations mentioned in the type. Abbreviations cannot be recursive because the well-formedness check uses the previous scope that does not contain a binding for this abbreviation yet. It could contain a reference to a *previous* abbreviation with the same name, and that would be expanded to the previous definition. The effect of all of this is that type names for abbreviations are lexically scoped (i.e., uses of a type name refer to the most recent enclosing type abbreviation), and that the type system internally keeps all abbreviations maximally expanded.

The rule for defining a new exception constructor (DEXN) checks that the exception has not already been declared (although an exception with the same name in a different module is allowed), and that its argument types are well-formed. It records that an exception has been declared with its full module path, and binds the exception name in the constructor environment with no type parameters, fully abbreviation-expanded argument types, and the stamp of the exception.

The rule for defining a new datatype (DTYPE) checks that the datatype is not already defined (although a datatype with the same name in a different module is allowed, as are datatypes that have the same name as a type abbreviation in the same module). The constructors must be distinct from each other, but could have the same name as constructors in other datatypes. The argument types to the constructors must be well formed. Since the datatype is allowed to be recursive, the type definition environment is first extended with a binding for the type being defined. This treats the datatype's name as an abbreviation for the stamp that represents the true identity of the type. Lastly, the constructor environment is extended with each constructor mapping to the type parameters, fully abbreviation-expanded argument types, and the type that is being constructed.

3.3 The value restriction and principal types

Although application of the value restriction is straightforward, subtleties arise when considering the type of a top-level definition at an intermediate program point. To illustrate, consider adding a second definition to our running example:

```
val k = fn x => fn y => x;
val k_mono = ref (k 5);
```

The RHS expression of the new definition can have a variety of types according to the expression typing relation, e.g. `(int -> int) ref` and `(string -> int) ref`. However, the value restriction prevents the definition of `k_mono` from being given a polymorphic type. The key question: is what type should `k_mono` be given when there is no usage of the function to disambiguate? For example, the two definitions might have been entered at the REPL, or they might be defined, but not used, in a separately compiled module with no explicit signature. In CakeML, such definitions do not type check, and the CakeML type system thereby maintains the principal type property: every expression with a type has a unique principal type. This is the critical property that supports a complete inference algorithm. See the online appendix[3] for a comparison of the decisions made by other ML implementations. We specify this principal type property in two parts, corresponding to non-values and values.

The DLET_MONO rule uses `type_pe_determ` to ensure that ambiguously typed non-values are not type-able. Any bindings vs and vs' that can arise from the pattern and expression of a `val` definition must be equivalent.

$$\begin{array}{l}\texttt{type\_pe\_determ}\ \Gamma_t\ p\ e \iff \\ \forall\, t_1\ vs\ t_2\ vs'. \\ \quad 0,\ \Gamma_t.\texttt{c} \vdash_p p : t_1,\ vs \wedge \Gamma_t \vdash_e e : t_1 \wedge \\ \quad 0,\ \Gamma_t.\texttt{c} \vdash_p p : t_2,\ vs' \wedge \Gamma_t \vdash_e e : t_2 \Rightarrow \\ \quad vs = vs'\end{array}$$

Since `ref (k 5)` is not a value but it can be given distinct types under the expression typing relation, we cannot type `k_mono` in our type system.

A more exotic problem arises if the typing relation were to allow defined values to have types that are not principal. Our discussion above implicitly assumed that `k` was assigned a principal type, `'a -> 'b -> 'a`. As a result, the expression typing for `ref (k 5)` could pick more than one type to instantiate `'b`, and so we obtained a type error.

If we allowed the type system to choose to type `k` with a less general type, e.g. `'a -> 'a -> 'a`, then `ref (k 5)` could be uniquely typed as `(int -> int) ref` and so the definition of `k_mono` would be accepted. However, we cannot choose a less general type for `k` without prior knowledge of the subsequent definition. The DLET_POLY rule uses `most_gen_env` to ensure that the typing relation always gives the most general environments, and that the definition of `k_mono` is a type error. It checks that any other environment `add_tvs` tvs' vs' derived from the pattern and expression typing rules is generalised by `add_tvs` tvs vs. The generalisation condition `weakE` holds iff we can apply substitutions on de Bruijn variables bound in `add_tvs` tvs vs to obtain `add_tvs` tvs' vs'.

$$\begin{array}{l}\texttt{most\_gen\_env}\ \Gamma_t\ p\ e\ tvs\ vs \iff \\ \forall\, tvs'\ vs'\ t'. \\ \quad tvs',\ \Gamma_t.\texttt{c} \vdash_p p : t',\ vs' \wedge \texttt{bind\_tvar}\ tvs'\ \Gamma_t \vdash_e e : t' \Rightarrow \\ \quad \texttt{weakE (add\_tvs}\ tvs\ vs\texttt{) (add\_tvs}\ tvs'\ vs'\texttt{)}\end{array}$$

4. INFERENCE ALGORITHM

Our type inference algorithm is based on Milner's Algorithm $\mathcal{W}$ [9], extended to top-level definitions. Internally, the inferencer uses a state-exception monad to track its progress when it performs type inference at the expression level. The monadic state is a record consisting of a substitution (field name `subst`) that maps unification variables to types, and a counter (field name `next_uvar`) that generates fresh unification variables. As in Algorithm $\mathcal{W}$, the substitution is used to backtrack and apply unification constraints as the inferencer walks an expression recursively; using a monad allows

[3] https://cakeml.org/ifl15/appendix.pdf

We need auxiliary functions where

- `is_value` e holds iff e is a literal constant, variable, function, or constructor fully applied to values,
- `distinct` holds iff its argument list does not contain the same element twice,
- `pat_bindings` p `[]` returns the variables bound by pattern p,
- `bind_tvar` tvs Γ_t binds an additional tvs de Bruijn type variables in the variable environment of Γ_t,
- `add_tvs` tvs vs quantifies tvs type variables in each type in vs,
- `most_gen_env` and `type_pe_determ` are defined in §3.3 to ensure that we only get principal types under the value restriction,
- `check_abbrev` T t ensures that all of the type abbreviations in t exist in the environment T, while `expand_abbrev` T t expands those abbreviations according to the environment,
- `mk_id` makes names fully qualified by adding the module name (if one exists),
- `TypeExn` is the exception type constructor, `Tapp` applies some type constructor,
- `merge_t` merges the type definition environments, and
- `check_ctor_tenv` checks that each constructor being defined (and their types) are well-formed, while `build_ctor_tenv` adds those constructors to the typing environment.

$$\text{(DLET\_POLY)}\ \frac{\begin{array}{c}\texttt{is\_value}\ e \\ \texttt{distinct (pat\_bindings}\ p\ \texttt{[])} \\ tvs,\ \Gamma_t\texttt{.c} \vdash_p p : t,\ vs \\ \texttt{bind\_tvar}\ tvs\ \Gamma_t \vdash_e e : t \\ u \Rightarrow \texttt{most\_gen\_env}\ \Gamma_t\ p\ e\ tvs\ vs\end{array}}{u,\ mn^?,\ \delta,\ \Gamma_t \vdash_d \texttt{val}\ p = e : \delta_\emptyset,\ (\emptyset\texttt{,[],}\ \texttt{add\_tvs}\ tvs\ vs)}$$

$$\text{(DLET\_MONO)}\ \frac{\begin{array}{c}\texttt{distinct (pat\_bindings}\ p\ \texttt{[])} \\ 0,\ \Gamma_t\texttt{.c} \vdash_p p : t,\ vs \\ \Gamma_t \vdash_e e : t \\ u \Rightarrow \neg\texttt{is\_value}\ e \wedge \texttt{type\_pe\_determ}\ \Gamma_t\ p\ e\end{array}}{u,\ mn^?,\ \delta,\ \Gamma_t \vdash_d \texttt{val}\ p = e : \delta_\emptyset,\ (\emptyset\texttt{,[],}\ \texttt{add\_tvs}\ 0\ vs)}$$

$$\text{(DTABBREV)}\ \frac{\begin{array}{c}\texttt{check\_freevars}\ 0\ targs\ t \\ \texttt{check\_abbrev}\ \Gamma_t\texttt{.t}\ t \\ \texttt{distinct}\ targs \\ t' = \texttt{expand\_abbrev}\ \Gamma_t\texttt{.t}\ t\end{array}}{u,\ mn^?,\ \delta,\ \Gamma_t \vdash_d \texttt{type}\ (targs)\ tn = t : \delta_\emptyset,\ (tn \mapsto (targs\texttt{,}t')\texttt{,[],}\ \texttt{[]})}$$

$$\text{(DEXN)}\ \frac{\begin{array}{c}\texttt{EVERY (check\_freevars 0 [])}\ ts \\ \texttt{mk\_id}\ mn^?\ cn \notin \delta\texttt{.defined\_exns} \\ \texttt{EVERY (check\_abbrev}\ \Gamma_t\texttt{.t)}\ ts \\ \delta' = \delta_\emptyset\ \texttt{with defined\_exns :=}\ \{\texttt{mk\_id}\ mn^?\ cn\} \\ ts' = \texttt{MAP (expand\_abbrev}\ \Gamma_t\texttt{.t)}\ ts\end{array}}{u,\ mn^?,\ \delta,\ \Gamma_t \vdash_d \texttt{exception}\ cn\ \texttt{of}\ ts : \delta',\ (\emptyset\texttt{,[(}cn\texttt{,[],}ts'\texttt{,TypeExn (mk\_id}\ mn^?\ cn\texttt{))],}\ \texttt{[]})}$$

$$\text{(DTYPE)}\ \frac{\begin{array}{c}t' = tn \mapsto (tvs\texttt{, Tapp (MAP Tvar}\ tvs\texttt{) (TC\_name (mk\_id}\ mn^?\ tn\texttt{)))} \\ merged\_t = \texttt{merge\_t}\ (\emptyset\texttt{,}t')\ \Gamma_t\texttt{.t} \\ \texttt{check\_ctor\_tenv}\ mn^?\ merged\_t\ \texttt{[(}tvs\texttt{,}tn\texttt{,}ctors\texttt{)]} \\ \texttt{mk\_id}\ mn^?\ tn \notin \delta\texttt{.defined\_types} \\ \delta' = \delta_\emptyset\ \texttt{with defined\_types :=}\ \{\texttt{mk\_id}\ mn^?\ tn\}\end{array}}{u,\ mn^?,\ \delta,\ \Gamma_t \vdash_d \texttt{datatype}\ tvs\ tn = ctors : \delta',\ (t'\texttt{,build\_ctor\_tenv}\ mn^?\ merged\_t\ \texttt{[(}tvs\texttt{,}tn\texttt{,}ctors\texttt{)],}\ \texttt{[]})}$$

Figure 4: Definition typing rules (`fun` rule omitted, `datatype` rule simplified)

```
infer_e Γi x =
do
  (tvs,t) ← lookup x Γi.inf_v;
  uvs ← n_fresh_uvar tvs;
  return (infer_deBruijn_subst uvs t)
od

infer_e Γi (fn x => e) =
do
  u ← fresh_uvar;
  t ← infer_e (Γi,x : (0,u)) e;
  return (u -> t)
od

infer_e Γi (e1 e2) =
do
  t1 ← infer_e Γi e1;
  t2 ← infer_e Γi e2;
  u ← fresh_uvar;
  add_constraint t1 (t2 -> u);
  return u
od
```

Figure 5: Selected expression inference cases.

```
infer_d mn? δi Γi (val p = e) =
do
  init_state;
  t1 ← infer_e Γi e;
  (t2,env′) ← infer_p Γi.inf_c p;
  names ← return (MAP FST env′);
  guard (distinct names)
    "Duplicate pattern variable";
  add_constraint t1 t2;
  ts ← subst_list (MAP SND env′);
  (tvs,s,ts′) ← return (gen_list ts);
  guard (tvs = 0 ∨ is_value e)
    "Value restriction violated";
  return (δ∅,∅,[],ZIP (names,MAP (λ t. (tvs,t)) ts′))
od

infer_d mn? δi Γi (type (targs) tn = t) =
do
  guard (distinct targs) "Duplicate type variables";
  guard
    (check_freevars 0 targs t ∧
     check_abbrev Γi.inf_t t) "Bad type definition";
  return
    (δ∅,tn ↦ (targs,expand_abbrev Γi.inf_t t),[],[])
od
```

Figure 6: Selected definition inference cases.

us to represent this cleanly in higher-order logic. Our unification algorithm is based on triangular substitutions and was verified previously [6]; we define encoding and decoding functions to convert between the inferencer types and the generic terms over which the verified unification algorithm operates. Like the type system, we also keep track of a typing environment Γ_i and the defined names δ_i. These environments are similar to their type system counterparts but we can use more efficient representations in the inferencer. To emphasize this difference, we prefix both environment's record fields with `inf_`.

4.1 Expressions

Type inference for expressions, `infer_e`, is where we make primary use of unification. Every call to `infer_e` either fails with a type error or succeeds and returns a type. On successful inference, we obtain the inferred type by applying the substitution in the final monad state, $subst$, to the returned type, t. We write this as t`[`$subst$`]` and refer to it as a *solution* of the inferencer.

The important cases, corresponding to variables, functions and applications respectively, are shown in Fig. 5. Various helper functions are used to interact with the monad: `fresh_uvar` and `n_fresh_uvar` respectively extract 1 and tvs fresh unification variables for use in the inference rules, `infer_deBruijn_subst` replaces bound de Bruijn variables with fresh unification variables while `add_constraint` adds unification constraints to the current substitution.

For functions, we recursively call `infer_e` on the nested expression e after adding x to the variable environment with a fresh unification variable, u, for its type. This unification variable may get constrained inside the recursive call but it might also be left unconstrained. In our running example, the type for the RHS expression is inferred in 3 recursive calls to `infer_e`. The first two bind x and y to two fresh unification variables `(0,`u`)` and `(0,`v`)` respectively. The final call looks up x in the variable environment and returns u, since there are no bound de Bruijn variables in its type scheme. The returned type is therefore u `->` v `->` u, and the final substitution is empty since no unification constraints were applied. Notice that unlike in Algorithm $\mathcal{W}$, unconstrained unification variables are handled at the top-level.

4.2 Definitions

At the top-level, our inferencer essentially applies the typing rules directly to type check its input. We focus here on two illustrative cases of the type inferencer for definitions, shown in Fig. 6. The various `guard` expressions are used to check the preconditions of the type system rules. The rest of the inferencer, e.g. top-level module definitions, corresponds closely to the type system and so we do not discuss it further.

The first case in Fig. 6 corresponds to type inference for new value definitions of the form `val` p `=` e. Starting from an empty substitution in the initial monadic state, we infer a type for e and ensure the typing constraints introduced by the bindings in pattern p are satisfied. Next, `subst_list` applies the internal substitution over the types in env'. Using `gen_list`, we replace all the remaining, unconstrained unification variables in ts with bound type variables, returning the resulting types as ts' and the number of bound variables, tvs. If the value restriction applies, we additionally check that this step did not end up generalising any variables, i.e. that tvs `=` 0. For our running example, the pattern inference simply returns a fresh unification variable w along with a singleton list `[(`k`,`w`)]`. After applying the unification constraints and substitution, we get ts `= [`u `->` v `->` u`]`. The generalisation step then produces our desired type, `'a -> 'b -> 'a`. Since the expression was a value, this is accepted and returned as the type for the new binding `k`.

The latter case corresponds to type inference for a new type abbreviation. Like the type system, new type abbreviations are checked for well-formedness before they are added to the typing environment. Notice that it corresponds very closely to the type system's DTABBREV rule.

On successful inference in either case, we return a 4-tuple consisting of the newly defined names, type definitions, constructor definitions and value definitions respectively. These are added to the typing environment as we move on to subsequent definitions.

5. INFERENCER VERIFICATION

We divide the verification effort for our type inferencer into soundness and completeness theorems. Informally, inferencer soundness shows that any program with an inferred type has a valid typing derivation in the type system while inferencer completeness shows that any type that can be derived in the type system for a program is generalised by the inferred type. In both directions, we further divide the proofs into expression-level and top-level theorems. This division is useful as it turns out that both expression-level theorems are required for each of the top-level proofs. Several conversion functions, e.g. `conv_decl` will appear in the theorems below. These convert between representations of the type system and the inferencer, e.g. from sets to lists, but are otherwise non-crucial to the proofs. Similarly, we use ellipses to abbreviate some parts of theorems that are not relevant to the discussion.

5.1 Expression-level theorems

The key difference between type system judgements and inferencer solutions at the expression level is the presence of unification variables in their respective typing judgements. Moreover, the inferencer is completely deterministic while the relational type system can have several typing judgements for a single expression. Hence, the inferred type needs to generalise all possible types for an expression; unification variables allow it to do this deterministically: they should appear wherever there is a free choice of type.

We define a formal *substitution completion* relation (below) that allows us to fully constrain any unconstrained unification variables. The 3-ary relation `pure_add_constraints` holds iff s_2 is the result of successfully adding some additional unification constraints, $constraints$, to s_1. To be in the `sub_complete` relation, `check_t` further ensures that applying the substitution of s_2 on any unification variables present in the domain of s_2 results in a type, u`[`s_2`]` with no further unification variables. This implies that any inferred type, t`[`s_2`]`, has no unification variables. The extra argument tvs gives the number of de Bruijn variables allowed, while $next\_uvar$ is used to restrict the domain of s_2; `count` tvs is the set of natural numbers less than tvs. Our soundness and completeness theorems relate the type system and inferencer using this relation.

$$\texttt{sub\_complete}\ tvs\ next\_uvar\ s_1\ constraints\ s_2 \iff \texttt{pure\_add\_constraints}\ s_1\ constraints\ s_2 \wedge \texttt{count}\ next\_uvar \subseteq \texttt{FDOM}\ s_2 \wedge \forall u.\ u \in \texttt{FDOM}\ s_2 \Rightarrow \texttt{check\_t}\ tvs\ \emptyset\ u[s_2]$$

Next, we need a few invariants on the inferencer state. The first invariant, `check_state`, checks that the monadic state is consistent with the variable environment, e.g. unification variables that have not been generated yet should neither be present in the variable environment nor the internal substitution. The second invariant, `check_env_e`, checks for consistency between parts of the constructor and module environments of $\hat{\Gamma}_t$ and Γ_i, e.g. that all the constructors are present in both environments. These parts of the typing environments are used but not modified at the expression level. The last invariant we need links the changing parts of both typing environments, namely, the variables and their types. These will be explained separately in the corresponding theorems.

The soundness theorem shows that (under suitable consistency assumptions) *any* completion of a (converted) solution from the inferencer, `conv_t` t`[`s`]`, corresponds to a typing judgement in the type system. The soundness invariant[4], `tenv_inv`, carries this property up to the variable typing environment: it states that whenever we successfully lookup a variable x in Γ_i with type t, a corresponding lookup of x in $\hat{\Gamma}_t$ yields type t' such that t' `= conv_t` t`[`s`]`.

THEOREM 5.1. Expression-level soundness.

$$\vdash \texttt{infer\_e}\ \Gamma_i\ e\ st = (\texttt{Success}\ t, st') \wedge \texttt{check\_env\_e}\ \hat{\Gamma}_t\ \Gamma_i \wedge \texttt{check\_state}\ st\ \Gamma_i\texttt{.inf\_v} \wedge \texttt{sub\_complete}\ (\texttt{num\_tvs}\ \hat{\Gamma}_t\texttt{.v})\ st'\texttt{.next\_uvar}\ st'\texttt{.subst}\ constraints\ s \wedge \texttt{tenv\_inv}\ s\ \Gamma_i\texttt{.inf\_v}\ \hat{\Gamma}_t\texttt{.v} \Rightarrow \hat{\Gamma}_t \vdash_e e : \texttt{conv\_t}\ t[s]$$

PROOF. By induction using the induction theorem for `infer_e` and case analysis. Our `tenv_inv` invariant is motivated by the cases where we add variables into the typing environment i.e. `Fun`, `Let` and variable lookups `Var`. The proof is otherwise routine with the correct choice of invariant. □

The completeness theorem shows that (under suitable consistency assumptions) for any typing judgement, the inferencer succeeds and we can find *some* completion of its solution, `conv_t` t'`[`s'`]`, to match that typing judgement. Like Theorem 5.1, we need a completeness invariant, `tenv_invC`, that carries this property up to the variable typing environment. Namely, we assume that the inferencer is started in some state from which we already know a completion under which lookups in $\hat{\Gamma}_t$ correspond to lookups in Γ_i.

THEOREM 5.2. Expression-level completeness.

$$\vdash \hat{\Gamma}_t \vdash_e e : t \wedge \texttt{check\_env\_e}\ \hat{\Gamma}_t\ \Gamma_i \wedge \texttt{check\_state}\ st\ \Gamma_i\texttt{.inf\_v} \wedge \texttt{sub\_complete}\ (\texttt{num\_tvs}\ \hat{\Gamma}_t\texttt{.v})\ st\texttt{.next\_uvar}\ st\texttt{.subst}\ constraints\ s \wedge \texttt{tenv\_invC}\ s\ \Gamma_i\texttt{.inf\_v}\ \hat{\Gamma}_t\texttt{.v} \wedge \ldots \Rightarrow \exists t'\ st'\ s'\ constraints'.\ \texttt{infer\_e}\ \Gamma_i\ e\ st = (\texttt{Success}\ t', st') \wedge \texttt{sub\_complete}\ (\texttt{num\_tvs}\ \hat{\Gamma}_t\texttt{.v})\ st'\texttt{.next\_uvar}\ st'\texttt{.subst}\ constraints'\ s' \wedge t = \texttt{conv\_t}\ t'[s'] \wedge \ldots$$

PROOF. By rule induction on typing derivations. Interesting cases occur when we add variables to the typing environment and when we need to apply unification constraints in the inferencer.

To illustrate, let us consider `fn x => x + 5`. By inversion, the last rule used in the type system to type this expression must be FUN. The premise of FUN adds some (valid) type scheme, say, `x:(0,int)` to its environment. The inferencer on the other hand, uses a fresh unification variable u in place of `int`. Since we generated a new unification variable, we need to constrain it in the substitution completion in a way that satisfies `tenv_invC` for our inductive hypothesis between the function bodies. To do this, we precisely apply the constraint corresponding to the type picked by the type system i.e. we constrain u to `int`.

When we type the function body, `x + 5`, we inductively know a list of the unification constraints, $constraints$ (including the one for u) that completes the inferencer's initial internal substitution, st, to match the type system. However, the inferencer now attempts to apply its own unification constraint $constraints'$ between u and `int` on st. Our general strategy for these cases is to first show that applying $constraints'$ after applying $constraints$ succeeds but has no effect since it must be implied by $constraints$. Then, we show that unification constraints can be re-ordered without changing the resulting substitution. This implies that (1) applying $constraints'$ on st succeeds and (2) further applying $constraints$ on the result gives us a completed substitution. These can then be used as suitable witnesses for the conclusion of this theorem. □

[4]Our actual invariants also deal with alpha equivalence between the environments that can be introduced at the definitions level. Even though we use a de Bruijn representation, we still need alpha equivalence to treat polymorphic types such as `0 -> 1 -> 0` as equivalent to `1 -> 0 -> 1`.

5.2 Top-level theorems

Our top-level soundness and completeness theorems apply to the type checking phase of an entire CakeML program. As before, we focus here on the handling of new definitions as the type system and inferencer behave similarly above the definitions level. The main difficulty is to reconcile the high-level specification of the value restriction rules in the type system with the direct implementation in the inferencer. The form of our value restrictions leads to an interesting interplay between the expression-level soundness/completeness theorems and both top-level theorems. Note that the first argument to the typing rules is set to true, i.e. the additional principal type restrictions are turned on.

To begin, we define `env_rel`, an invariant between Γ_t and Γ_i that checks consistency of the typing environments. It encompasses `check_env_e` shown above and uses `check_env_d` to make additional checks on the variable and type abbreviation environments that we did not need at the expression level. Crucially, we also assume that `tenv_alpha` holds between the two variable environments. It is the conjunction of `tenv_inv` and `tenv_invC` used at the expression level. This means that the variables defined so far at the top level are the same in both environments and their corresponding types are alpha equivalent with respect to bound type variables. Since we do not need to consider any types with unification variables at this level, the first argument to both relations is set to $\emptyset$.

```
env_rel Γt Γi ⟺
check_env_e Γt Γi ∧ check_env_d Γt Γi ∧
tenv_alpha Γi.inf_v Γt.v

tenv_alpha Γi.inf_v Γt.v ⟺
tenv_inv ∅ Γi.inf_v Γt.v ∧ tenv_invC ∅ Γi.inf_v Γt.v
```

The soundness theorem has a shape very similar to Theorem 5.1. We show that any new definition made by the inferencer corresponds to one that can be made by the type system.

THEOREM 5.3. Definition-level soundness.

```
⊢ infer_d mn? δi Γi d st = (Success (δi',τ,c,v),st') ∧
  env_rel Γt Γi ⇒
  T, mn?, conv_decl δi, Γt
    ⊢d d : conv_decl δi', (τ,c,conv_v v)
```

PROOF. By case analysis on the input definition. The important cases arise in value definitions, `val` p `=` e.

Case: e is not a value. By Theorem 5.1, we have that the inferred solution for e is a valid typing in the type system. The inferencer additionally checks that no unconstrained unification variables are in the inferred type, t. To use the DLET_MONO rule, we need to show additionally that t is the unique choice of type for e. Consider any type for e in the type system, t'; by Theorem 5.2, there is a completion of our inferred solution to yield t'. However, since there are no unconstrained unification variables in the solution, the additional unification constraints from this completion cannot change the inferred type. Hence, $t = t'$ and the inferred type is unique.

Case: e is a value. We need to show that the inferred type for e is (1) a valid typing judgement in the type system and (2) a most general type. For (1), we first note that the generalisation process replaces unconstrained unification variables with bound type variables. We can equivalently apply a set of unification constraints between unification variables and type variables. This is a substitution completion, and hence by Theorem 5.1, the generalised type is a valid type for e. For (2), any other type for e in the type system, t', has, by Theorem 5.2, a corresponding completion of the inferencer's solution that yields it. The inferencer generalises unification variables that are unconstrained but these are precisely the variables that get constrained by the completion. Hence, we can construct the required type variable substitution by matching each type variable to the substituted type of the unification variable it generalises. To illustrate further, consider the identity function `val f = fn x => x`. The right-hand expression is typed as *u* `->` *u* by the inferencer which then generalises it to `'a -> 'a`. For any other valid type, e.g. `int -> int`, we know by Theorem 5.2 a completion which, in this case maps *u* to `int`. We can use this to produce a corresponding de Bruijn substitution, namely, mapping `'a` to `int`. □

The completeness theorem shows that for any valid definition-level typing judgement, the inferencer also succeeds and that all of the newly defined variables in v' are alpha equivalent to those that were produced by the type system. Here, `bind_env` is a helper function that converts v to a variable environment.

THEOREM 5.4. Definition-level completeness.

```
⊢ T, mn?, δ, Γt ⊢d d : δ', (τ,c,v) ∧ env_rel Γt Γi ∧
  conv_decl δi = δ ⇒
  ∃ st' δi' v'.
    conv_decl δi' = δ' ∧
    infer_d mn? δi Γi d st =
    (Success (δi',τ,c,v'),st') ∧
    tenv_alpha v' (bind_env v) ∧ ...
```

PROOF. By case analysis on the input definition. The important cases arise in value definitions, `val` p `=` e.

Case: e is not a value. By DLET_MONO, we have a unique type, t, for e and by Theorem 5.2 the inferencer succeeds and there is a completion of its solution to yield t. Suppose for contradiction that the inferencer's solution has at least one unconstrained unification variable. We now construct two distinct completions by unifying all such unconstrained unification variables with `int` and `bool` respectively. By Theorem 5.1, the resulting (distinct) types are both valid typing judgements in the type system. This contradicts the uniqueness of t so we have no unification variables in the solution and the value restriction check in the inferencer succeeds.

Case: e is a value. We need to show that (1) the inferencer succeeds and (2) any most general type for e is alpha equivalent to the inferred solution. For (1), we note directly that by Theorem 5.2, there exists a completion of the inferencer's solution for that type. We prove (2) by constructing type variable substitutions from (2.1) the type system's type to the inferred type and (2.2) the inferred type to the type system's type. The proof of (2.1) is similar to soundness: we construct a substitution completion from the generalisation step and by Theorem 5.1, this is a valid typing of e in the type system which must be generalised by a most general type. The proof of (2.2) uses Theorem 5.2 to construct type variable substitutions for the generalised unification variables. □

6. TYPE SOUNDNESS

While the soundness and completeness theorems for the inferencer give us a practical algorithm for type checking CakeML programs, the type soundness theorem tells us that those programs that do have a type will not get stuck. This is important for the usual software engineering reasons, but also because the rest of the verified compiler uses the knowledge that the source program does not get stuck. For example, for a function application, the compiler can generate code that directly pulls a pointer from a closure record and jumps to it. It does not have to also generate a check that the value

$$
\begin{array}{rl}
Mv \equiv id \mapsto v & \text{module environments} \\
Cv \equiv cid \mapsto (\mathbb{N} \times stamp) & \text{constructor environments} \\
\Delta \equiv (cn \times stamp) \mapsto (\alpha^* \times t^*) & \text{constructor stamp environments} \\
S \equiv \ldots & \text{store typing (definition omitted)}
\end{array}
$$

$$
\begin{array}{rcll}
v & := & \texttt{Lit}\ l & \text{literals} \\
 & | & \texttt{Conv}\ (cid\ stamp)^?\ v^* & \text{constructors} \\
 & | & \texttt{Closure}\ env\ x\ e & \text{closure values} \\
 & | & \texttt{RecClosure}\ env\ (\langle x, x, e\rangle)^*\ x & \text{recursive closures} \\
 & | & \texttt{Loc}\ loc & \text{heap locations} \\
 & | & \texttt{Vector}\ v^* & \text{immutable vectors} \\
Vv & := & \epsilon & \text{empty environment} \\
 & | & x : v, Vv & \text{bind a value}
\end{array}
$$

where loc ranges over numbers and env is a record containing Mv, Cv, and Vv, similar to Γ_t.

$$
\begin{array}{ll}
tvs,\ \Delta,\ S \vdash_v v : \hat{t} & \text{value typing} \\
\Delta,\ S \vdash_{env} Vv : V & \text{environment typing} \\
S,\ \Delta \vdash_{mod} Mv : M & \text{module env. typing} \\
\Delta \vdash_{con} Cv : C & \text{constructor env. typing}
\end{array}
$$

Figure 7: Values and typing judgements

being called is actually a closure, because the operational semantics would get stuck if a non-closure value ends up being applied as a function.

We prove type soundness in two stages. The first, for expressions, is proved via preservation and progress lemmas with respect to a small-step operational semantics [15]. The second uses a big-step semantics for definitions, and is proved directly by induction over the list of definitions. This is relatively straightforward, since a definition cannot diverge, unless one of its constituent expressions does. Most of the interesting details occur at the expression level, and so we focus on it here.

A typical type soundness proof uses a structural operational semantics or a reduction semantics, where function application is modelled with substitution. In contrast, our semantics is based on the CEK-machine [3].[5] Thus, we have environments that give values to free variables, continuation stacks that explicitly model control flow, and closures to represent function values; we also have a store. We chose this style of semantics because it fit well with our big-step semantics for expressions, which is what the compiler verification uses – we have proved the two semantics equivalent, so we can use either according to convenience. If we had chosen a different form of small-step semantics our proofs (especially our big-step/small-step equivalence proofs) would be structured differently, but the more intricate details would be essentially similar.

6.1 Values and environments

Figure 7 gives the definition of environments and values, as well as the shape of additional typing judgements to give them types. Constructor values contain the unique stamp of their constructor, or none in the case of a tuple. Closures contain an expression, the name of the function's argument, and all three kinds of environments, since the expression can refer to free variables, constructor names, and module names. Recursive closures contain a bundle of named recursive functions with at least one named argument, in addition to the environments.

The Mv and Vv environments are the counterparts to the M and V type environments, mapping identifiers to values rather than types. Although Mv is straightforward, Vv has a small subtlety.

Type environments V can both bind variables to types and bind new type variables, but Vv can only bind variables to values and cannot bind type variables. This is sufficient because of the value restriction. To type a `let`-expression (or top-level definition), the type environment is extended with the type variables (implicitly) bound by the `let`, before typing the bound expression. However, the value restriction requires that that expression is a syntactic value, and so the environment does not need to be extended because the syntactic value can immediately be converted to a value (element of v) without consulting the environment. This supports a simplification for looking up a value in Vv: it can directly have the same type as it had when it was added to Vv. Thus, we avoid shifting de Bruijn in the preservation lemma that would otherwise occur, corresponding to the possibility of evaluation under a type variable binder.

Constructors need two additional environments, Cv which models the lexical scoping of constructors, and maps identifiers to the constructor's number of arguments and its unique identity (i.e., its stamp). By including the number of arguments, the small-step semantics can get stuck if the constructor is given the wrong number, and hence the compiler can assume that constructors are never applied to the wrong number of arguments. The Δ environment is not used by the small-step semantics, or the type system, but it is needed in the value typing judgements. It maps constructor stamps to the type information for that constructor. This separation supports our type soundness proof. Consider the following program:

```
datatype t = D of int
val x = D 4
datatype u = D of bool
val y = x
val z = D true
```

After executing the first 2 definitions, we have a state with the following environments:

$$
\begin{aligned}
Cv &= \{\texttt{D} \mapsto \langle 1, \texttt{t}\rangle\} \\
\Delta &= \{\langle \texttt{D}, \texttt{t}\rangle \mapsto \langle [], \texttt{int}\rangle\} \\
Vv &= \texttt{x} : \texttt{Conv}\ (\texttt{D}\ \texttt{t})\ \texttt{4}, \epsilon
\end{aligned}
$$

Thus, looking ahead, `y` has type `t`, as does `x`, and `z` has type `u`. If we evaluate the next definition, the environments change:

$$
\begin{aligned}
Cv &= \{\texttt{D} \mapsto \langle 1, \texttt{u}\rangle\} \\
\Delta &= \{\langle \texttt{D}, \texttt{u}\rangle \mapsto \langle [], \texttt{bool}\rangle; \langle \texttt{D}, \texttt{t}\rangle \mapsto \langle [], \texttt{int}\rangle\} \\
Vv &= \texttt{x} : \texttt{Conv}\ (\texttt{D}\ \texttt{t})\ \texttt{4}, \epsilon
\end{aligned}
$$

Because the binding of constructor names in Cv follow lexical scoping, the new binding for constructor `D` shadows the previous one. This allows `z` to retain type `u`. Because Δ uses the stamp, it keeps both bindings, and since the value for `x` already in the environment also uses the stamp, the type of `x` remains `t`. It is essential that neither type changes.

The value typing judgement uses three pieces of data: a set of bound type variables `tvs` for closures that were created with those variables; a constructor stamp environment Δ for constructor values (N.B., it does not take a lexical Cv because once something is a value, it should have no free lexically scoped identifiers of any sort, variables or constructor names); and a store for location values. The environment and module environment judgements do not need the

[5] We are not aware of any type soundness proof in the literature that uses such a semantics.

type variable input, because their rules existentially quantify one when needed. The constructor environment judgement additionally does not need the store typing.

Figure 8 gives selected rules for typing values. All the `_ok` functions check for well-formedness of their respecive environments. The VTuple rule simply types all of the argument values ($\vdash_{vs}$ does $\vdash_v$ for all of its arguments) and returns the tuple constructor applied to those types.

The VCon rule finds the type parameters and argument types of the constructor in Δ. It makes an arbitrary (well-formed) instantiation of those parameters in the argument types, and checks that those are the actual types of the argument values. Note that `type_subst` substitutes on syntactic type variables rather than deBruijn ones. The returned type is the type constructor that corresponds to $stamp$ (obtained via `stamp_to_tc`) applied to the instantiating types.

The VClosure rule types all of the environments in the closure, and uses the resulting type environments to type the expression.

The EnvBind rule types an environment, one binding at a time. It uses an arbitrary tvs to ensure that closures originating from polymorphic bindings maintain enough polymorphism. Consider the following example:

```
fun f x = x
val a = f 1
val b = f true
```

After evaluating the first definition, the environment is

$$Vv = \mathtt{f} : \mathtt{Closure}\ \{\}\ \mathtt{x}\ \mathtt{x}, \epsilon$$

If we are not allowed to use a polymorphic type for `f`, then we have to make a choice, say `int`, and we get the following, which cannot type both subsequent definitions.

$$V = \mathtt{f} : \langle 0, \mathtt{int} \to \mathtt{int} \rangle, \epsilon$$

Allowing type variables lets us instead get the following, which can type both definitions (recall that types use de Bruijn indices).

$$V = \mathtt{f} : \langle 1, 0 \to 0 \rangle, \epsilon$$

Lastly, the ConEnv rule checks for various consistency conditions on the three forms of constructor environments. For example, `check_con_env` is used to check that the same constructor names appear in all three environments and have corresponding types.

6.2 Definitions

The definition level type soundness does not introduce any new environments or intermediate types. The only challenge is in carefully managing the various invariants about which names are defined in δ, to ensure that the stamp uniqueness guarantees that we rely on are maintained. Most of these are straightforward, but tedious, so we omit them here, and only explain the u parameter to the definition-level judgements in Figure 4.

Recall that we use u to control whether the type of a value-restricted definition must be principal. The inferencer completeness theorem relies on principal types; however, the induction in the type soundness proof does not go through with the principal typing check present. Therefore, we prove type soundness with u being false, and then prove the (obvious) fact that any program with a type when u is true, also has the same type when it is false. This lets us move the top-level type soundness theorem from the more permissive type system, to the one that corresponds to the inference algorithm.

The following program illustrates how type preservation fails when the check is left on.

```
val f x = x
val x = ref [1]
val _ = x := []
val y = f x
```

Here `x` and `y` have type `int list ref`, and the type checker accepts the program. However, after evaluating the first three statements, we are left with the following environment (omitting the indirection through the store to simplify):

$$Vv = \mathtt{x} : \mathtt{ref}\ [\,]; \mathtt{f} : \ldots, \epsilon$$

From this, we can generate many different type environments, and all of them will give y a different type, and thus, the `type_pe_determ` check of Dlet_mono will fail.

$$V = \mathtt{x} : \langle 0, \mathtt{int\ list\ ref} \rangle; \mathtt{f} : \ldots, \epsilon$$
$$V' = \mathtt{x} : \langle 0, \mathtt{bool\ list\ ref} \rangle; \mathtt{f} : \ldots, \epsilon$$

Without the check, the type system can give `y` the now non-principal type of `int list ref` to satisfy the preservation theorem.

Modules and signatures, instead of the store, can also provide an example.

```
structure M :> sig val f : int -> int end =
struct
  fun f x = x
end;
val v = (fn y => y) M.f;
```

Here, once evaluation has put `f` into the module environment and the signature is lost, `v` no longer has a principal type.

7. DISCUSSION AND RELATED WORK

7.1 Type system design

Our type system is simpler than Standard ML's in two key respects. The first is that we do not (yet) support let polymorphism. The main reason is that adding it will make our proofs, especially inferencer completeness, significantly more complex while not necessarily adding much utility to a CakeML user. For example, Vytiniotis et al. [13] suggest that the feature should be removed entirely. Although their work is in the context of a more sophisticated type system, they also experimentally showed that let polymorphism is rarely used in existing Haskell code bases, including in the Haskell boot libraries.

The second, and arguably more important omission is type annotations. This is work in progress for our compiler, since we need to extend the verified parser to support annotations in many places. However, we expect that adding annotations will not significantly change any of our proofs.

7.2 Type inference

Damas and Milner proved Algorithm $\mathcal{W}$ to be a sound, principal type inferencer for ML expressions [1]. Our work formalises this result for a real ML implementation, namely CakeML, and further extends it to modules, constructors, references, and exceptions. This required us to develop a declarative type system with principal types for value restricted definitions.

Type system design is delicate, and adding features beyond the basic Hindley-Milner system can easily ruin principal types – hence the hope for a complete inferencer – and possibly render the system undecidable. Despite these complications, the mainstream of typed functional programming language design seems to be for increasing the features, and living without principal types, or requiring some type annotations. Sometimes the trouble comes from a subtle

$$\text{(VTuple)}\ \frac{tvs,\ \Delta,\ S \vdash_{vs} vs : ts}{tvs,\ \Delta,\ S \vdash_{v} \texttt{Conv NONE}\ vs : \texttt{Tapp}\ ts\ \texttt{TC\_tup}}$$

$$\text{(VCon)}\ \frac{\begin{array}{c}\texttt{EVERY (check\_freevars}\ tvs\ \texttt{[])}\ ts' \\ \texttt{LENGTH}\ tvs' = \texttt{LENGTH}\ ts' \\ tvs,\ \Delta,\ S \vdash_{vs} vs : \texttt{MAP (type\_subst}\ tvs'\ ts')\ ts \\ \texttt{lookup}\ \Delta\ (cn,\ stamp) = \texttt{SOME}\ (tvs', ts)\end{array}}{tvs,\ \Delta,\ S \vdash_{v} \texttt{Conv (SOME}\ (cn, stamp))\ vs : \texttt{Tapp}\ ts'\ \texttt{(stamp\_to\_tc}\ stamp)}$$

$$\text{(VClosure)}\ \frac{\begin{array}{c}\Delta \vdash_{con} env.\texttt{c} : \Gamma_t.\texttt{c} \\ \texttt{tenv\_mod\_ok}\ \Gamma_t.\texttt{m} \\ S,\ \Delta \vdash_{mod} env.\texttt{m} : \Gamma_t.\texttt{m} \\ \Delta,\ S \vdash_{env} env.\texttt{v} : \Gamma_t.\texttt{v} \\ \texttt{check\_freevars}\ tvs\ \texttt{[]}\ t_1 \\ \texttt{(bind\_tvar}\ tvs\ \Gamma_t),\ n : (0, t_1) \vdash_{e} e : t_2\end{array}}{tvs,\ \Delta,\ S \vdash_{v} \texttt{Closure}\ env\ n\ e : t_1\ \texttt{->}\ t_2}$$

$$\text{(EnvBind)}\ \frac{tvs,\ \Delta,\ S \vdash_{v} v : t \quad \Delta,\ S \vdash_{env} Vv : V}{\Delta,\ S \vdash_{env} n : v,\ Vv : V, n : (tvs, t)} \qquad \text{(ConEnv)}\ \frac{\begin{array}{c}\texttt{tenv\_ctor\_ok}\ C \\ \texttt{ctMap\_ok}\ \Delta \\ \texttt{check\_con\_env}\ \Delta\ Cv\ C\end{array}}{\Delta \vdash_{con} Cv : C}$$

Figure 8: Selected value typing rules

interaction of seemingly innocuous features (as in the "avoidance problem" from the SML module system [2]). That is the case here, with the value restriction; we were able to restrict the type system enough to regain principal types, but the value restriction is a very minor tweak to the type system. For other popular features, including GADTs, there is no solution for now, and one must be resigned to using the type inference algorithm as the most precise specification of the type system [14].

Naraschewski and Nipkow have mechanised a soundness and completeness proof for Algorithm $\mathcal{W}$ [11]. Their underlying language is a MiniML, with similar features to Damas and Milner's language, lacking imperative features, or any value restriction. They also axiomatized the specification of the unification algorithm, whereas we tie into an existing verified implementation. In contrast, they verify completeness for a system that generalises nested lets, whereas we have not yet done that.

7.3 Type soundness

Our type system and type soundness proof broadly follow our previous work in OCaml$_{light}$ [12], with the main extension being support for modules and signatures. Similar to OCaml$_{light}$, we use de Bruijn indices for type variables, and concrete names for other variables. We also explicitly bind type variables in the environment. However, our operational semantics is different (CEK-style, rather than SOS-style), and we have a more flexible treatment of constructor names that follow lexical scoping, whereas OCaml$_{light}$ required them to be unique.

Lee et al. [7] give a semantics for Standard ML in Twelf via elaboration into an internal language that includes support for translucent sums and singleton kinds. They then prove type soundness for the internal language. In contrast, our operational semantics and proofs do away with elaboration and instead directly work with the abstract syntax of CakeML, although we do not support the higher-order functors that motivated the design of their internal language.

8. CONCLUSION

We have formally specified a type system and type inferencer for CakeML. We provide a type soundness theorem for the type system as well as soundness and completeness theorems linking the type inferencer's behaviour to the type system's. CakeML aims to be a practical programming language that is both easy to program in and easy to reason about. The theorems in this paper are steps toward the latter goal: any input CakeML program that is accepted by the inferencer is guaranteed to have well-defined semantics.

Without completeness, our specification [5] of the top-level CakeML read-eval-print loop (REPL) was unsatisfactory. When a type-incorrect definition is entered, the REPL should print `<type error>`, and await a new definition, and not execute any part of the type-incorrect one. Ideally, whether a definition is type correct is specified with respect to the type system, whereas the implementation of the REPL uses the inferencer. However, without an inferencer completeness theorem, we could not prove that the implementation of the REPL did not signal a type error even when the specification said it should not. Thus, we had to use the inferencer to specify which definitions had type errors, even as the inferencer soundness theorem allowed us to use the type system to specify what type good definitions had. By verifying completeness, we have significantly improved the semantics of the CakeML REPL.

Acknowledgements

NICTA is funded by the Australian Government through the Department of Communications and the Australian Research Council through the ICT Centre of Excellence Program.

References

[1] L. Damas and R. Milner. Principal type-schemes for functional programs. In *Proc. 9th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '82, pages 207–212. ACM, 1982.

[2] D. Dreyer. *Understanding and Evolving the ML Module System*. PhD thesis, Carnegie Mellon University, 2005.

[3] M. Felleisen, R. B. Findler, and M. Flatt. *Semantics Engineering with PLT Redex*. MIT Press, 2009.

[4] R. Harper and M. Lillibridge. A type-theoretic approach to higher-order modules with sharing. In *POPL'94: 21st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 123–137, 1994.

[5] R. Kumar, M. O. Myreen, M. Norrish, and S. Owens. CakeML: A verified implementation of ML. In *POPL '14: Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 179–191. ACM Press, Jan. 2014.

[6] R. Kumar and M. Norrish. (Nominal) Unification by recursive descent with triangular substitutions. In *Interactive Theorem Proving, First International Conference, ITP 2010*, volume 6172 of *LNCS*, 2010.

[7] D. K. Lee, K. Crary, and R. Harper. Towards a mechanized metatheory of Standard ML. In *Proceedings of the 34th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '07, pages 173–184. ACM, 2007.

[8] X. Leroy. Manifest types, modules, and separate compilation. In *POPL'94: 21st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 109–122, 1994.

[9] R. Milner. A theory of type polymorphism in programming. *J. Comput. Syst. Sci.*, 17(3), 1978.

[10] R. Milner, M. Tofte, R. Harper, and D. MacQueen. *The Definition of Standard ML (Revised)*. MIT Press, 1997.

[11] W. Naraschewski and T. Nipkow. Type inference verified: Algorithm W in Isabelle/HOL. *Journal of Automated Reasoning*, 23:299–318, 1999.

[12] S. Owens. A sound semantics for OCaml light. In *Programming Languages and Systems: 17th European Symposium on Programming, ESOP 2008*, volume 4960 of *LNCS*, pages 1–15. Springer, Mar. 2008.

[13] D. Vytiniotis, S. Peyton Jones, and T. Schrijvers. Let should not be generalized. In *Proceedings of the 5th ACM SIGPLAN Workshop on Types in Language Design and Implementation*, TLDI '10. ACM, 2010.

[14] D. Vytiniotis, S. Peyton Jones, T. Schrijvers, and M. Sulzmann. OutsideIn(X) Modular type inference with local assumptions. *J. Funct. Program.*, 21(4-5), 2011.

[15] A. K. Wright and M. Felleisen. A syntactic approach to type soundness. *Inf. Comput.*, 115(1):38–94, 1994.