HOL Light QE[*]

Jacques Carette, William M. Farmer, and Patrick Laskowski

Computing and Software, McMaster University, Canada
http://www.cas.mcmaster.ca/~carette
http://imps.mcmaster.ca/wmfarmer

25 January 2018

> Changed HOL Light from sc to rm as used by J. Harrison.

Abstract. We are interested in algorithms that manipulate mathematical expressions in mathematically meaningful ways. Expressions are syntactic, but most logics do not allow one to discuss syntax. CTT_{qe} is a version of Church's type theory that includes quotation and evaluation operators that are similar to quote and eval in the Lisp programming language. Since the HOL logic is also a version of Church's type theory, we decided to add quotation and evaluation to HOL Light to demonstrate the implementability of CTT_{qe} and the benefits of having quotation and evaluation in a proof assistant. The resulting system is called HOL Light QE. Here we document the design of HOL Light QE and the challenges that needed to be overcome.

1 Introduction

A *syntax-based mathematical algorithm (SBMA)* manipulates mathematical expressions in a mathematically meaningful way. SBMAs are commonplace in mathematics. Examples include algorithms that compute arithmetic operations by manipulating numerals, linear transformations by manipulating matrices, and derivatives by manipulating functional expressions. Reasoning about the mathematical meaning of an SBMA requires reasoning about the relationship between how the expressions are manipulated by the SBMA and what the manipulations mean mathematically.

We argue in [23] that the combination of quotation and evaluation, along with some inference rules, provides the means to reason about the interplay between syntax and semantics, which is what is needed for reasoning about SBMAs. *Quotation* is an operation that maps an expression e to a special value called a *syntactic value* that represents the syntax tree of e. Quotation enables expressions to be manipulated as syntactic entities. *Evaluation* is an operation that maps a syntactic value s to the value of the expression that is represented by s. Evaluation enables meta-level reasoning via syntactic values to be reflected into object-level reasoning. Quotation and evaluation thus form an infrastructure for integrating meta-level and object-level reasoning. Quotation gives a form of *reification* of object-level values which allows introspection. Along with inference rules, this gives a certain amount of *logical reflection*. Evaluation adds to this

> Reference?

---

some aspects of *computational reflection*.

Incorporating quotation and evaluation operators — like quote and eval in the Lisp programming language — into a traditional logic like first-order logic or simple type theory is not a straightforward task. Several challenging design problems stand in the way. The three design problems that most concern us are the following. We will write the quotation and evaluation operators applied to an expression e as $\ulcorner e \urcorner$ and $[\![e]\!]$, respectively.

1. *Evaluation Problem.* An evaluation operator is applicable to syntactic values that represent formulas and thus is effectively a truth predicate. Hence, by the proof of Alfred Tarski's theorem on the undefinability of truth [49], if the evaluation operator is total in the context of a sufficiently strong theory like first-order Peano arithmetic, then it is possible to express the liar paradox using the quotation and evaluation operators. Therefore, the evaluation operator must be partial and the law of disquotation cannot hold universally (i.e., for some expressions e, $[\![\ulcorner e \urcorner]\!] \neq e$). As a result, reasoning with evaluation can be cumbersome and leads to undefined expressions.

2. *Variable Problem.* The variable x is not free in the expression $\ulcorner x+3 \urcorner$ (or in any quotation). However, x is free in $[\![\ulcorner x+3 \urcorner]\!]$ because $[\![\ulcorner x+3 \urcorner]\!] = x+3$. If the value of a constant c is $\ulcorner x+3 \urcorner$, then x is free in $[\![c]\!]$ because $[\![c]\!] = [\![\ulcorner x+3 \urcorner]\!] = x+3$. Hence, in the presence of an evaluation operator, whether or not a variable is free in an expression may depend on the values of the expression's components. As a consequence, the substitution of an expression for the free occurrences of a variable in another expression depends on the semantics (as well as the syntax) of the expressions involved and must be integrated with the proof system for the logic. That is, a logic with quotation and evaluation requires a semantics-dependent form of substitution in which side conditions, like whether a variable is free in an expression, are proved within the proof system. This is a major departure from traditional logic.

3. *Double Substitution Problem.* By the semantics of evaluation, the value of $[\![e]\!]$ is the *value* of the expression whose syntax tree is represented by the *value* of e. Hence the semantics of evaluation involves a double valuation. This is most apparent when the value of a variable involves a syntax tree which refers to the name of that same variable. For example, if the value of a variable x is $\ulcorner x \urcorner$, then $[\![x]\!] = [\![\ulcorner x \urcorner]\!] = x = \ulcorner x \urcorner$. Hence the substitution of $\ulcorner x \urcorner$ for x in $[\![x]\!]$ requires one substitution inside the argument of the evaluation operator and another substitution after the evaluation operator is eliminated. This double substitution is another major departure from traditional logic.

CTT_{qe} [24,25] is version of Church's type theory [15] with quotation and evaluation that solves these three design problems. It is based on $\mathcal{Q}_0$ [2], Peter Andrews' version of Church's type theory. We believe CTT_{qe} is the first readily implementable version of simple type theory that includes *global* quotation and evaluation operators. We show in [24] that it is suitable for defining, applying, and reasoning about SBMAs.

To demonstrate that CTT_{qe} is indeed implementable, we have implemented CTT_{qe} by modifying HOL Light [34], a compact implementation of the HOL

logic [31]. The resulting version of HOL Light is called HOL Light QE. Here we present its design, implementation, and the challenges to doing so.

The rest of the paper is organized as follows. Section 2 presents the key ideas underlying $\mathrm{CTT_{qe}}$ and explains how $\mathrm{CTT_{qe}}$ solves the three design problems given above. Section 3 offers a brief overview of HOL Light. The HOL Light QE implementation is described in section 4, and examples of how quotation and evaluation are used in it are discussed in section 5. Section 6 is devoted to related work. And the paper ends with some final remarks in section 7 including a brief discussion on future work.

2 $\mathrm{CTT_{qe}}$

The syntax and semantics of $\mathrm{CTT_{qe}}$ as well as the proof system for $\mathrm{CTT_{qe}}$ are defined in [24]. In this section we will only introduce the definitions and results of $\mathrm{CTT_{qe}}$ that are key to understanding how HOL Light QE implements $\mathrm{CTT_{qe}}$. The reader is encouraged to consult [24] when additional details are required.

2.1 Syntax

The syntax of $\mathrm{CTT_{qe}}$ has the same machinery as $\mathcal{Q}_0$ plus an inductive type ϵ of syntactic values, a partial quotation operator, and a typed evaluation operator.

A *type* of $\mathrm{CTT_{qe}}$ is defined inductively by the following formation rules:

1. *Type of individuals*: ι is a type.
2. *Type of truth values*: o is a type.
3. *Type of constructions*: ϵ is a type.
4. *Function type*: If α and β are types, then $(\alpha \to \beta)$ is a type.

Let $\mathcal{T}$ denote the set of types of $\mathrm{CTT_{qe}}$.

A *typed symbol* is a symbol with a subscript from $\mathcal{T}$. Let $\mathcal{V}$ be a set of typed symbols such that, for each $\alpha \in \mathcal{T}$, $\mathcal{V}$ contains denumerably many typed symbols with subscript α. A *variable of type* α of $\mathrm{CTT_{qe}}$ is a member of $\mathcal{V}$ with subscript α. $\mathbf{x}_\alpha, \mathbf{y}_\alpha, \mathbf{z}_\alpha, \ldots$ are syntactic variables ranging over variables of type α. Let $\mathcal{C}$ be a set of typed symbols disjoint from $\mathcal{V}$. A *constant of type* α of $\mathrm{CTT_{qe}}$ is a member of $\mathcal{C}$ with subscript α. $\mathbf{c}_\alpha, \mathbf{d}_\alpha, \ldots$ are syntactic variables ranging over constants of type α. $\mathcal{C}$ contains a set of *logical constants* that include $\mathsf{app}_{\epsilon \to \epsilon \to \epsilon}$, $\mathsf{abs}_{\epsilon \to \epsilon \to \epsilon}$, and $\mathsf{quo}_{\epsilon \to \epsilon}$.

An *expression of type* α of $\mathrm{CTT_{qe}}$ is defined inductively by the formation rules below. $\mathbf{A}_\alpha, \mathbf{B}_\alpha, \mathbf{C}_\alpha, \ldots$ are syntactic variables ranging over expressions of type α. An expression is *eval-free* if it is constructed using just the first five formation rules.

1. *Variable*: $\mathbf{x}_\alpha$ is an expression of type α.
2. *Constant*: $\mathbf{c}_\alpha$ is an expression of type α.
3. *Function application*: $(\mathbf{F}_{\alpha \to \beta}\, \mathbf{A}_\alpha)$ is an expression of type β.
4. *Function abstraction*: $(\lambda\, \mathbf{x}_\alpha\, .\, \mathbf{B}_\beta)$ is an expression of type $\alpha \to \beta$.

5. *Quotation*: $\ulcorner \mathbf{A}_\alpha \urcorner$ is an expression of type ϵ if $\mathbf{A}_\alpha$ is eval-free.
6. *Evaluation*: $\llbracket \mathbf{A}_\epsilon \rrbracket_{\mathbf{B}_\beta}$ is an expression of type β.

The sole purpose of the second component $\mathbf{B}_\beta$ in an evaluation $\llbracket \mathbf{A}_\epsilon \rrbracket_{\mathbf{B}_\beta}$ is to establish the type of the evaluation; we will thus write $\llbracket \mathbf{A}_\epsilon \rrbracket_{\mathbf{B}_\beta}$ as $\llbracket \mathbf{A}_\epsilon \rrbracket_\beta$.

A *construction* of $\mathrm{CTT_{qe}}$ is an expression of type ϵ defined inductively as follows:

1. $\ulcorner \mathbf{x}_\alpha \urcorner$ is a construction.
2. $\ulcorner \mathbf{c}_\alpha \urcorner$ is a construction.
3. If $\mathbf{A}_\epsilon$ and $\mathbf{B}_\epsilon$ are constructions, then $\mathsf{app}_{\epsilon \to \epsilon \to \epsilon} \mathbf{A}_\epsilon \mathbf{B}_\epsilon$, $\mathsf{abs}_{\epsilon \to \epsilon \to \epsilon} \mathbf{A}_\epsilon \mathbf{B}_\epsilon$, and $\mathsf{quo}_{\epsilon \to \epsilon} \mathbf{A}_\epsilon$ are constructions.

The set of constructions is thus an inductive type whose base elements are quotations of variables and constants and whose constructors are $\mathsf{app}_{\epsilon \to \epsilon \to \epsilon}$, $\mathsf{abs}_{\epsilon \to \epsilon \to \epsilon}$, and $\mathsf{quo}_{\epsilon \to \epsilon}$. As we will see shortly, constructions serve as syntactic values.

Let $\mathcal{E}$ be the function mapping eval-free expressions to constructions that is defined inductively as follows:

<div style="color:#cc3333; font-size:small">The definition below seems trivial, it just maps from one syntax to another. On the flip-side, if a reader is expecting a λ-calculus, then $\mathcal{E}$ in the app case is ill-defined as you can't pattern match on an application.</div>

1. $\mathcal{E}(\mathbf{x}_\alpha) = \ulcorner \mathbf{x}_\alpha \urcorner$.
2. $\mathcal{E}(\mathbf{c}_\alpha) = \ulcorner \mathbf{c}_\alpha \urcorner$.
3. $\mathcal{E}(\mathbf{F}_{\alpha \to \beta} \mathbf{A}_\alpha) = \mathsf{app}_{\epsilon \to \epsilon \to \epsilon} \mathcal{E}(\mathbf{F}_{\alpha \to \beta}) \mathcal{E}(\mathbf{A}_\alpha)$.
4. $\mathcal{E}(\lambda \mathbf{x}_\alpha . \mathbf{B}_\beta) = \mathsf{abs}_{\epsilon \to \epsilon \to \epsilon} \mathcal{E}(\mathbf{x}_\alpha) \mathcal{E}(\mathbf{B}_\beta)$.
5. $\mathcal{E}(\ulcorner \mathbf{A}_\alpha \urcorner) = \mathsf{quo}_{\epsilon \to \epsilon} \mathcal{E}(\mathbf{A}_\alpha)$.

When $\mathbf{A}_\alpha$ is eval-free, $\mathcal{E}(\mathbf{A}_\alpha)$ is the unique construction that represents the syntax tree of $\mathbf{A}_\alpha$. That is, $\mathcal{E}(\mathbf{A}_\alpha)$ is a syntactic value that represents how $\mathbf{A}_\alpha$ is syntactically constructed. For every eval-free expression, there is a construction that represents its syntax tree, but not every construction represents the syntax tree of an eval-free expression. For example, $\mathsf{app}_{\epsilon \to \epsilon \to \epsilon} \ulcorner \mathbf{x}_\alpha \urcorner \ulcorner \mathbf{x}_\alpha \urcorner$ represents the syntax tree of $(\mathbf{x}_\alpha \mathbf{x}_\alpha)$ which is not an expression of $\mathrm{CTT_{qe}}$ since the types are mismatched. A construction is *proper* if it is in the range of $\mathcal{E}$, i.e., it represents the syntax tree of an eval-free expression.

The purpose of $\mathcal{E}$ is to define the semantics of quotation: the meaning of $\ulcorner \mathbf{A}_\alpha \urcorner$ is $\mathcal{E}(\mathbf{A}_\alpha)$.

2.2 Semantics

The semantics of $\mathrm{CTT_{qe}}$ is based on Henkin-style general models [35]. An expression $\mathbf{A}_\epsilon$ of type ϵ denotes a construction, and when $\mathbf{A}_\epsilon$ is a construction, it denotes itself. The semantics of the quotation and evaluation operators are defined so that the following theorems hold:

Theorem 2.21 (Law of Quotation) $\ulcorner A_\alpha \urcorner = \mathcal{E}(A_\alpha)$ *is valid in* $\mathrm{CTT_{qe}}$.

Theorem 2.22 (Law of Disquotation) $\llbracket \ulcorner A_\alpha \urcorner \rrbracket_\alpha = A_\alpha$ *is valid in* $\mathrm{CTT_{qe}}$.

<div style="color:#cc6600; font-size:small">Some comments that = is not up to αβ, otherwise the Law of Quotation does not hold – $\ulcorner 2 + 3 \urcorner$ is not the same as $\mathcal{E}(5)$.</div>

2.3 Proof System

The proof system for CTT_{qe} consists of the axioms for $\mathcal{Q}_0$, the single rule of inference for $\mathcal{Q}_0$, and additional axioms that extend the rules for beta-reduction, define the logical constants of CTT_{qe}, specify ϵ as an inductive type, and state the properties of quotation and evaluation. We prove in [24] that this proof system is sound for all formulas and complete for eval-free formulas.

Substitution is performed in the proof system for CTT_{qe} using the properties of beta-reduction as Andrews does in the proof system for $\mathcal{Q}_0$ [2, p. 213]. The syntactic notion of "a variable is free in an expression" is replaced in Andrews' beta-reduction axioms by the semantic notion of "a variable is effective in an expression" when the expression is not necessarily eval-free, and beta-reduction axioms for quotation and evaluation are added to Andrews' beta-reduction axioms. "$\mathbf{x}_\alpha$ is effective in $\mathbf{B}_\beta$" means the value of $\mathbf{B}_\beta$ depends on the value of $\mathbf{x}_\alpha$. Clearly, if $\mathbf{B}_\beta$ is eval-free, "$\mathbf{x}_\alpha$ is effective in $\mathbf{B}_\beta$" implies "$\mathbf{x}_\alpha$ is free in $\mathbf{B}_\beta$". However, "$\mathbf{x}_\alpha$ is effective in B_β" is a refinement of "$\mathbf{x}_\alpha$ is free in $\mathbf{B}_\beta$" on eval-free expressions since $\mathbf{x}_\alpha$ is free in $\mathbf{x}_\alpha = \mathbf{x}_\alpha$, but $\mathbf{x}_\alpha$ is not effective in $\mathbf{x}_\alpha = \mathbf{x}_\alpha$.

> I think that some, if not most, of these rules should be shown. They either need to be here or in the implementation section, with a forward pointer.

> Because substitution is so important, I think more will be needed – in the same vein as above.

2.4 Design Problems

CTT_{qe} solves the three design problems given in section 1. The Evaluation Problem is completely avoided by restricting the quotation operator to eval-free expressions and thus making it impossible to express the liar paradox. The Variable Problem is overcome by modifying Andrews' beta-reduction axioms as described above. The Double Substitution Problem is eluded by using a beta-reduction axiom for evaluations that excludes beta-reductions that embody a double substitution.

3 HOL Light

HOL Light [34] is an open-source proof assistant developed by John Harrison. It implements a logic (HOL) which is a version of Church's type theory. It is a simple implementation of the HOL proof assistant [31] written in OCaml and hosted on GitHub at `https://github.com/jrh13/hol-light/`. Although it is a relatively small system, it has been used to formalize many kinds of mathematics and to check many proofs including the lion's share of Tom Hale's proof of the Kepler conjecture [22].

HOL Light is very well suited to serve as a foundation on which to build an implementation of CTT_{qe}: First, it is an open-source system that can be freely modified as long as certain very minimal conditions are satisfied. Second, it is an implementation of a version of simple type theory that is essentially $\mathcal{Q}_0$, the version of Church's type theory underlying CTT_{qe}, plus (1) polymorphic type variables, (2) an axiom of choice expressed by asserting that the Hilbert ϵ operator is a choice (indefinite description) operator, and (3) an axiom of infinity that asserts that `ind`, the type of individuals, is infinite [34]. The type

variables in the implemented logic are not a hindrance; they actually facilitate the implementation of $\mathrm{CTT_{qe}}$. The presence of the axioms of choice and infinity in HOL Light alter the semantics of $\mathrm{CTT_{qe}}$ without compromising in any way the semantics of quotation and evaluation. And third, HOL Light supports the definition of inductive types so that ϵ can be straightforwardly defined.

4 Implementation

4.1 Overview

HOL Light QE was implemented in four stages:

1. The set of HOL Light terms was extended so that $\mathrm{CTT_{qe}}$ expressions could be mapped to HOL Light terms. This required the introduction of ϵ, the type of construction, and term constructors for quotations and evaluations. See subsection 4.2.
2. The HOL Light proof system was modified to include the machinery in $\mathrm{CTT_{qe}}$ for reasoning about quotations and evaluations. This required adding new rules of inference to HOL Light and modifying the HOL Light `INST` rule of inference that simultaneously substitutes terms $t_1, \ldots, t_n$ for the free variables $x_1, \ldots, x_n$ in a sequent. See subsection 4.3.
3. Machinery, consisting of HOL functions definitions, tactics, and theorems, was created for supporting reasoning about quotations and evaluations in the new system. See subsection 4.4.
4. Examples were developed in the new system to test the implementation and to demonstrate the benefits of having quotation and evaluation in higher-order logic. See section 5.

The first and second stages have been essentially completed; both stages involved modifying the kernel of HOL Light. The third and fourth stages are ongoing; they did not include any changes to the HOL Light kernel.

The HOL Light QE system was developed by the third author under the supervision of the first two authors on an undergraduate NSERC USRA research project at McMaster University. HOL Light QE is available at

```
https://github.com/JacquesCarette/hol-light,
```

4.2 Mapping of $\mathrm{CTT_{qe}}$ Expressions to HOL Terms

Tables 1 and 2 illustrates how the $\mathrm{CTT_{qe}}$ types and expressions are mapped to the HOL types and terms, respectively. The HOL types and terms are written in the the internal representation form employed in HOL Light QE. The type `epsilon` and the term constructors `Quote` and `Eval` are additions to HOL Light explained below. Since $\mathrm{CTT_{qe}}$ does not have type variables, there is a logical constant $=_{\alpha \to \alpha \to o}$ representing equality for each $\alpha \in \mathcal{T}$. The members of this family of

constants are all mapped to a single HOL constant with the polymorphic type `a_ty_var->a_ty_var->bool` where `a_ty_var` is any chosen HOL type variable.

The other logical constants of CTT_{qe} [24, Table 1] are not mapped to primitive HOL constants. $\text{app}_{\epsilon\to\epsilon\to\epsilon}$, $\text{abs}_{\epsilon\to\epsilon\to\epsilon}$, and $\text{quo}_{\epsilon\to\epsilon}$ are implemented by `App`, `Abs`, and `Quo`, constructors for the inductive type `epsilon` given below. The remaining logical constants are predicates on constructions that are implemented by HOL functions.

$\textbf{CTT}_{\textbf{qe}}$ **Type** α	**HOL Type** $\mu(\alpha)$	**Abbreviation for** $\mu(\alpha)$
o	`Tyapp("bool",[])`	`bool`
ι	`Tyapp("ind",[])`	`ind`
ϵ	`Tyapp("epsilon",[])`	`epsilon`
$\beta\to\gamma$	`Tyapp("fun",[`$\mu(\beta),\mu(\gamma)$`])`	$\mu(\beta)$`->`$\mu(\gamma)$

Table 1. Mapping of CTT_{qe} Types to HOL Types

$\textbf{CTT}_{\textbf{qe}}$ **Expression** e	**HOL Term** $\nu(e)$
$\mathbf{x}_\alpha$	`Var("x",`$\mu(\alpha)$`)`
$\mathbf{c}_\alpha$	`Const("c",`$\mu(\alpha)$`)`
$=_{\alpha\to\alpha\to o}$	`Const("=",a_ty_var->a_ty_var->bool)`
$(\mathbf{F}_{\alpha\to\beta}\mathbf{A}_\alpha)$	`Comb(`$\nu(\mathbf{F}_{\alpha\to\beta}),\nu(\mathbf{A}_\alpha)$`)`
$(\lambda\mathbf{x}_\alpha\,.\,\mathbf{B}_\beta)$	`Abs(Var("x",`$\mu(\alpha)$`),`$\nu(\mathbf{B}_\beta)$`)`
$\ulcorner\mathbf{A}_\alpha\urcorner$	`Quote(`$\nu(\mathbf{A}_\alpha),\mu(\alpha)$`)`
$[\![\mathbf{A}_\epsilon]\!]_{\mathbf{B}_\beta}$	`Eval(`$\nu(\mathbf{A}_\epsilon),\mu(\beta)$`)`

Table 2. Mapping of CTT_{qe} Expressions to HOL Terms

The CTT_{qe} type ϵ is the type of constructions, the syntactic values constructions that represent the syntax trees of eval-free expressions. ϵ is defined as an inductive type `epsilon` in HOL Light QE. The following inductive types `type` and `epsilon` are defined in HOL Light QE:

```
define_type "type = TyVar string
                  | TyBase string
                  | TyMonoCons string type
                  | TyBiCons string type type";;

define_type "epsilon = QuoVar string type
                     | QuoConst string type
                     | App epsilon epsilon
                     | Abs epsilon epsilon
                     | Quo epsilon";;
```

Terms of type `type` denote the syntax trees of HOL Light QE types (which are the same as HOL types). The terms of type `epsilon` denote the syntax trees of HOL Light QE terms that are eval-free (i.e., do not contain evaluations).

The OCaml type of HOL types in HOL Light QE

```
type hol_type = Tyvar of string
              | Tyapp of string *  hol_type list
```

is the same as in HOL Light, but the OCaml type of HOL terms in HOL Light QE

```
type term = Var of string * hol_type
          | Const of string * hol_type
          | Comb of term * term
          | Abs of term * term
          | Quote of term * hol_type
          | Hole of term * hol_type
          | Eval of term * hol_type
```

has three new constructors — `Quote`, `Hole`, and `Eval` — that are not in HOL Light.

`Quote` constructs a quotation of type `epsilon` with components t and α from a term t of type α that is is eval-free. `Eval` constructs an evaluation of type α with components t and α from a term t of type `epsilon` and a type α. `Hole` is used to construct "holes" of type `epsilon` in an quasiquotation as described in [24]. A HOL Light QE quotation that contains holes is a quasiquotation, while a quotation without any holes is a normal quotation. The construction of terms in HOL Light QE has been modified to allow a hole (of type `epsilon`) to be used where a term of some other type is expected.

The external representation of a quotation `Quote(t,ty)` is `Q_ t _Q`. Similarly, the external representation of a hole `Hole(t,ty)` is `H_ t _H`. The external representation of an evaluation `Quote(t,ty)` is

```
eval t to ty.
```

4.3   Modification of the HOL Light **Proof System**

4.4   **Creation of Support Machinery**

The HOL Light QE contains a number of HOL functions, tactics, and theorems that are useful for reasoning about constructions, quotations, and evaluations. An important example is the HOL function `isExprType` that implements the $\mathrm{CTT_{qe}}$ family of logical constants $\mathsf{is\text{-}expr}^{\alpha}_{\epsilon \to o}$ where α ranges over members of $\mathcal{T}$. This function takes terms s_1 and s_1 of type `epsilon` and `type`, respectively, and returns true iff s_1 represents the syntax tree of a term t, s_2 represents the syntax tree of a type α, and t is of type α.

5 Examples

5.1 Law of Excluded Middle

5.2 Induction Schema

6 Related Work

Quotation, evaluation, reflection, reification, issues of intensionality versus extensionality, metaprogramming and metareasoning each have extensive literature – sometimes in more than one field. For example, one can find a vast literature on reflection in logic, programming languages and theorem proving. Due to space restrictions, we cannot do justice to the full breadth of issues. For a full discussion, please see the related work section in [26]. The surveys of Costantini [20], Harrison [33] are excellent. From a programming perspective, the discussion and extensive bibliography of Kavvos' D.Phil. thesis [41] are well worth reading.

Focusing just on interactive proof assistants, we find that Robert Boyer and J Moore developed a global infrastructure [5], for incorporating symbolic algorithms into the Nqthm [6] theorem prover. This approach is also used in ACL2 [40], the successor to Nqthm; see [39]. Over the last 30 years, the Nuprl group lead by Robert Constable has produced a large body of work on metareasoning and reflection for theorem proving [1,3,17,37,42,44,53] that has been implemented in the Nuprl [18] and MetaPRL [36] systems. Proof by reflection has become a mainstream technique in the Coq [19] proof assistant with the development of tactics based on symbolic computations like the Coq ring tactic [4,32] and the formalizations of the *four color theorem* [28] and the *Feit-Thompson odd-order theorem* [29] led by Georges Gonthier. See [4,7,11,30,32,38,46] for a selection of the work done on using reflection in Coq. Many other systems also support metareasoning and reflection: Agda [45,50,51], Idris [13,12,14] Isabelle/HOL [10], Lean [21], Maude [16], PVS [52], reFLect [43], and Theorema [27,8].

The semantics of the quotation operator $\ulcorner \cdot \urcorner$ is based on the *disquotational theory of quotation* [9]. According to this theory, a quotation of an expression e is an expression that denotes e itself. In $\mathrm{CTT_{qe}}$, $\ulcorner \mathbf{A}_\alpha \urcorner$ denotes a value that represents the syntactic structure of $\mathbf{A}_\alpha$. Polonsky [47] presents a set of axioms for quotation operators of this kind. Other theories of quotation have been proposed – see [9] for an overview.. For instance, quotation can be viewed as an operation that constructs literals for syntactic values [48].

7 Conclusion

References

1. S. F. Allen, R. L. Constable, D. J. Howe, and W. E. Aitken. The semantics of reflected proof. In *Proceedings of the Fifth Annual Symposium on Logic in Computer Science (LICS '90)*, pages 95–105. IEEE Computer Society, 1990.

2. P. B. Andrews. *An Introduction to Mathematical Logic and Type Theory: To Truth through Proof, Second Edition*. Kluwer, 2002.

3. E. Barzilay. *Implementing Reflection in Nuprl*. PhD thesis, Cornell University, 2005.

4. S. Boutin. Using reflection to build efficient and certified decision procedures. In M. Abadi and T. Ito, editors, *Theoretical Aspects of Computer Software*, volume 1281 of *Lecture Notes in Computer Science*, pages 515–529. Springer, 1997.

5. R. Boyer and J Moore. Metafunctions: Proving them correct and using them efficiently as new proof procedures. In R. Boyer and J Moore, editors, *The Correctness Problem in Computer Science*, pages 103–185. Academic Press, 1981.

6. R. Boyer and J Moore. *A Computational Logic Handbook*. Academic Press, 1988.

7. T. Braibant and D. Pous. Tactics for reasoning modulo AC in Coq. In J.-P. Jouannaud and Z. Shao, editors, *Certified Programs and Proofs (CPP 2011)*, volume 7086 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 2011.

8. B. Buchberger, A. Craciun, T. Jebelean, L. Kovacs, T. Kutsia, K. Nakagawa, F. Piroi, N. Popov, J. Robu, M. Rosenkranz, and W. Windsteiger. Theorema: Towards computer-aided mathematical theory exploration. *Journal of Applied Logic*, 4:470–504, 2006.

9. H. Cappelen and E. LePore. Quotation. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Spring 2012 edition, 2012.

10. A. Chaieb and T. Nipkow. Proof synthesis and reflection for linear arithmetic. *Journal of Automated Reasoning*, 41:33–59, 2008.

11. A. Chlipala. *Certified Programming with Dependent Types: A Pragmatic Introduction to the Coq Proof Assistant*. MIT Press, 2013.

12. David Christiansen and Edwin Brady. Elaborator reflection: Extending idris in idris. *SIGPLAN Not.*, 51(9):284–297, September 2016.

13. David Raymond Christiansen. Type-directed elaboration of quasiquotations: A high-level syntax for low-level reflection. In *Proceedings of the 26Nd 2014 International Symposium on Implementation and Application of Functional Languages*, IFL '14, pages 1:1–1:9, New York, NY, USA, 2014. ACM.

14. David Raymond Christiansen. *Practical Reflection and Metaprogramming for Dependent Types*. PhD thesis, IT University of Copenhagen, 2016.

15. A. Church. A formulation of the simple theory of types. *Journal of Symbolic Logic*, 5:56–68, 1940.

16. M. Clavel and J. Meseguer. Reflection in conditional rewriting logic. *Theoretical Computer Science*, 285:245–288, 2002.

17. R. L. Constable. Using reflection to explain and enhance type theory. In H. Schwichtenberg, editor, *Proof and Computation*, volume 139 of *NATO ASI Series*, pages 109–144. Springer, 1995.

18. R. L. Constable, S. F. Allen, H. M. Bromley, W. R. Cleaveland, J. F. Cremer, R. W. Harper, D. J. Howe, T. B. Knoblock, N. P. Mendler, P. Panangaden, J. T. Sasaki, and S. F. Smith. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, Englewood Cliffs, New Jersey, 1986.

19. Coq Development Team. *The Coq Proof Assistant Reference Manual, Version 8.5*, 2016. Available at `https://coq.inria.fr/distrib/current/refman/`.

20. S. Costantini. Meta-reasoning: A survey. In A. C. Kakas and F. Sadri, editors, *Computational Logic: Logic Programming and Beyond, Essays in Honour of Robert A. Kowalski, Part II*, volume 2408 of *Lecture Notes in Computer Science*, pages 253–288, 2002.

21. Gabriel Ebner, Sebastian Ullrich, Jared Roesch, Jeremy Avigad, and Leonardo de Moura. A metaprogramming framework for formal verification. *Proceedings of the ACM on Programming Languages*, 1(ICFP):34, 2017.

22. T. Hales et al. A formal proof of the Kepler conjecture. *Forum of Mathematics, Pi*, 5, 2017.

23. W. M. Farmer. The formalization of syntax-based mathematical algorithms using quotation and evaluation. In J. Carette, D. Aspinall, C. Lange, P. Sojka, and W. Windsteiger, editors, *Intelligent Computer Mathematics*, volume 7961 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2013.

24. W. M. Farmer. Incorporating quotation and evaluation into Church's type theory. *Computing Research Repository (CoRR)*, abs/1612.02785 (72 pp.), 2016.

25. W. M. Farmer. Incorporating quotation and evaluation into Church's type theory: Syntax and semantics. In M. Kohlhase, M. Johansson, B. Miller, L. de Moura, and F. Tompa, editors, *Intelligent Computer Mathematics*, volume 9791 of *Lecture Notes in Computer Science*, pages 83–98. Springer, 2016.

26. W. M. Farmer. Theory morphisms in Church's Type theory with quotation and evaluation. *Computing Research Repository (CoRR)*, abs/1703.02117 (15 pp.), 2017.

27. M. Giese and B. Buchberger. Towards practical reflection for formal mathematics. RISC Report Series 07-05, Research Institute for Symbolic Computation (RISC), Johannes Kepler University, 2007.

28. G. Gonthier. The four colour theorem: Engineering of a formal proof. In D. Kapur, editor, *Computer Mathematics (ASCM 2007)*, volume 5081 of *Lecture Notes in Computer Science*, page 333. Springer, 2008.

29. G. Gonthier, A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. Le Roux, A. Mahboubi, R. O'Connor, S. Ould Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi, and L. Théry. A machine-checked proof of the odd order theorem. In *Interactive Theorem Proving (ITP 2013)*, volume 7998 of *Lecture Notes in Computer Science*, pages 163–179. Springer, 2013.

30. G. Gonthier, A. Mahboubi, and E. Tassi. A Small Scale Reflection Extension for the Coq system. Research Report RR-6455, Inria Saclay Ile de France, 2015.

31. M. J. C. Gordon and T. F. Melham. *Introduction to HOL: A Theorem Proving Environment for Higher Order Logic*. Cambridge University Press, 1993.

32. B. Grégoire and A. Mahboubi. Proving equalities in a commutative ring done right in Coq. In J. Hurd and T. F. Melham, editors, *Theorem Proving in Higher Order Logics (TPHOLs 2005)*, volume 3603 of *Lecture Notes in Computer Science*, pages 98–113. Springer, 2005.

33. J. Harrison. Metatheory and reflection in theorem proving: A survey and critique. Technical Report CRC-053, SRI Cambridge, 1995. Available at `http://www.cl.cam.ac.uk/~jrh13/papers/reflect.ps.gz`.

34. J. Harrison. HOL Light: An overview. In S. Berghofer, T. Nipkow, C. Urban, and M. Wenzel, editors, *Theorem Proving in Higher Order Logics*, volume 5674 of *Lecture Notes in Computer Science*, pages 60–66. Springer, 2009.

35. L. Henkin. Completeness in the theory of types. *Journal of Symbolic Logic*, 15:81–91, 1950.

36. J. Hickey, A. Nogin, R. L. Constable, B. E. Aydemir, E. Barzilay, Y. Bryukhov, R. Eaton, A. Granicz, A. Kopylov, C. Kreitz, V. Krupski, L. Lorigo, S. Schmitt, C. Witty, and X. Yu. MetaPRL — A modular logical environment. In D. Basin and B. Wolff, editors, *Theorem Proving in Higher Order Logics (TPHOLs 2003)*, volume 2758 of *Lecture Notes in Computer Science*, pages 287–303, 2003.

37. D. Howe. Reflecting the semantics of reflected proof. In P. Aczel, H. Simmons, and S. Wainer, editors, *Proof Theory*, pages 229–250. Cambridge University Press, 1992.

38. D. W. H. James and R. Hinze. A reflection-based proof tactic for lattices in Coq. In Horváth Z, V. Zsók, P. Achten, and P. W. M. Koopman, editors, *Proceedings of the Tenth Symposium on Trends in Functional Programming (TFP 2009)*, volume 10 of *Trends in Functional Programming*, pages 97–112. Intellect, 2009.

39. W. A. Hunt Jr., M. Kaufmann, R. B. Krug, J S. Moore, and E. W. Smith. Meta reasoning in ACL2. In J. Hurd and T. F. Melham, editors, *Theorem Proving in Higher Order Logics (TPHOLs 2005)*, volume 3603 of *Lecture Notes in Computer Science*, pages 163–178. Springer, 2005.

40. M. Kaufmann and J S. Moore. An industrial strength theorem prover for a logic based on common lisp. *IEEE Transactions on Software Engineering*, 23:203–213, 1997.

41. G. A. Kavvos. On the Semantics of Intensionality and Intensional Recursion. Available from `http://arxiv.org/abs/1712.09302`, December 2017.

42. T. B. Knoblock and R. L. Constable. Formalized metareasoning in type theory. In *Proceedings of the Symposium on Logic in Computer Science (LICS '86)*, pages 237–248. IEEE Computer Society, 1986.

43. T. Melham, R. Cohn, and I. Childs. On the semantics of ReFLect as a basis for a reflective theorem prover. *Computing Research Repository (CoRR)*, abs/1309.5742, 2013.

44. A. Nogin, A. Kopylov, X. Yu, and J. Hickey. A computational approach to reflective meta-reasoning about languages with bindings. In R. Pollack, editor, *ACM SIGPLAN International Conference on Functional Programming, Workshop on Mechanized Reasoning about Languages with Variable Binding, (MERLIN 2005)*, pages 2–12. ACM, 2005.

45. U. Norell. Dependently typed programming in Agda. In A. Kennedy and A. Ahmed, editors, *Proceedings of TLDI'09*, pages 1–2. ACM, 2009.

46. M. Oostdijk and H. Geuvers. Proof by computation in the Coq system. *Theoretical Computer Science*, 272, 2002.

47. A. Polonsky. Axiomatizing the Quote. In M. Bezem, editor, *Computer Science Logic (CSL'11) — 25th International Workshop/20th Annual Conference of the EACSL*, volume 12 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 458–469. Schloss Dagstuhl — Leibniz-Zentrum für Informatik, 2011.

48. F. Rabe. Generic literals. In M. Kerber, J. Carette, C. Kaliszyk, F. Rabe, and V. Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 102–117. Springer, 2015.

49. A. Tarski. The concept of truth in formalized languages. In J. Corcoran, editor, *Logic, Semantics, Meta-Mathematics*, pages 152–278. Hackett, second edition, 1983.

50. P. van der Walt. Reflection in Agda. Master's thesis, Universiteit Utrecht, 2012.

51. P. van der Walt and W. Swierstra. Engineering proof by reflection in Agda. In R. Hinze, editor, *Implementation and Application of Functional Languages*, volume 8241 of *Lecture Notes in Computer Science*, pages 157–173. Springer, 2012.

52. F. W. von Henke, S. Pfab, H. Pfeifer, and H. Rueß. Case studies in meta-level theorem proving. In J. Grundy and M. Newey, editors, *Theorem Proving in Higher Order Logics (TPHOLs'98*, volume 1479, pages 461–478. Springer, 1998.

53. X. Yu. *Reflection and Its Application to Mechanized Metareasoning about Programming Languages*. PhD thesis, California Institute of Technology, 2007.

Todo list