Construction and Deduction Methods for the Formal Development of Software

F. W. von Henke, A. Dold, H. Rueß, D. Schwier, M. Strecker
Abt. Künstliche Intelligenz
Fakultät für Informatik
Universität Ulm
Oberer Eselsberg
D-89069 Ulm/Donau

June 16, 1994

Abstract

In this paper we present an approach towards a framework based on the type theory ECC (Extended Calculus of Constructions) in which specifications, programs and operators for modular development by stepwise refinement can be formally described and reasoned about. We show that generic software development steps can be expressed as higher-order functions and demonstrate that proofs about their asserted effects can be carried out in the underlying logical calculus.

For transformations requiring syntactic manipulations of objects, a two-level system comprising a Meta- and an Object-level is provided, and it is shown how transformations can be formalized that faithfully represent operators on the object level.

1 Introduction

Modern software engineering regards software development as an evolutionary process [12, 4]. One view of this process is that, starting from abstract, high-level requirement specifications, a series of refinement or implementation steps is applied to successive levels of specification, eventually yielding a program as the final result of the process. In a more formal context, it must be demonstrated for each step that the refined specification or implementation satisfies the properties postulated by the previous (higher level) specification. Then the final program will satisfy the initial requirements, provided suitable properties of compositionality of steps hold.

Past experience has shown that formal verification of software developments requires more effort and higher costs than can be justified in most situations, making traditional *post mortem* verification rather impractical. As an alternative, we may analyze the development process further and identify certain steps that are applied repeatedly as refinement patterns. If we succeed in formalizing such patterns and verifying their properties, we may considerably reduce the effort required for the formal verification of the development process. In particular, it is desirable to formalize a development pattern as an *operator* that transforms specifications into new specifications and to prove that the result of applying the operator yields, for example, a refinement of the argument specification. Accordingly, the demonstration of correctness for each development step that is an instance of a formalized pattern has been reduced to showing that the operator is applicable.

In this paper we present an approach towards a framework in which we can formally describe and reason about specifications, programs and development operators and apply the method outlined above. Our approach is based on a type theory, the *Extended Calculus of Constructions* (ECC) [21, 22], as the unifying logical foundation. Building on ECC, we define a specification language, QED; roughly, it introduces syntactic constructs that are closer to the style of algebraic specifications and more readable than the language of the "raw" logic, while its semantics is grounded in the type theory. In essence, a specification represents a type, and a member of that type is a realization of that specification. Obviously, such a notion of types as specifications requires types to convey semantic information; as a consequence, demonstrating that an object has a particular type, i.e. type checking, may involve verifying that it satisfies the semantic properties of the type – which, in general, requires theorem proving.

The language is rich enough for expressing specifications, assertions about specifications, and relations between specifications in a natural way. In particular, many generic development steps can be expressed as higher-order functions, and proofs that they have the asserted effect can be carried out in the underlying logical calculus; a formalization of this kind will be presented in Sect. 4. It seems, however, that in many cases the formalization of development patterns requires a direct description of how the text of a specification has to be modified, for instance for optimizing transformations; thus, such patterns must be formalized as operators on syntactic representations of specifications. Then the verification that applying an operator indeed establishes the asserted relationship between its source and target typically requires relating the *syntactic* manipulation (i.e., how the text of the source specification is modified to yield the text of the target) to the *semantic* relationship between the meanings of those texts. To facilitate this kind of reasoning a two-level formal system has to be provided: the syntax of the object language is represented by data types of the meta-level, and a reflection principle serves to link syntactic structures to their meaning at the object level. In Sect. 4 we develop such a two-level system for QED and show by means of a simple example how operators can be formalized and reasoned about.

The remainder of the paper is organized as follows. Section 2 contains a brief description of the type theory used. In Sect. 3 we introduce the specification language QED. Section 4 presents the two main approaches to formalizing development steps: using higher-order functions, and using meta-operators; for the latter approach the two-level formal system is developed. Section 5 discusses aspects of the QED implementation. The final section contains a brief summary and conclusions.

2 Type-theoretic Foundation

The formal basis of our approach is the type theory *Extended Calculus of Constructions* (ECC) [21, 22] augmented by inductive types. We briefly summarize those features of the type theory that are needed in this paper.

ECC, like all advanced type theories, may be regarded as an extension of the (simply typed) lambda calculus [5] by a more powerful type system. In our context, the most important extensions are the addition of *dependent types* and *type universes*.

Σ-types (strong sum types) generalize Cartesian products: $\Sigma x : A.\ B$ is the type of pairs (a, b) such that a is a member of type A and b is in $B\,[x := a]$.[1] Π-types (abstraction types) generalize function types. Intuitively, $\Pi x : A.\ B$ is the type of dependent functions with domain A and codomain B where B may depend on the element to which the function is applied.

[1] Capital letters and a, b denote terms of the term calculus of ECC, while x, y denote variables. $N\,[x := M]$ denotes the substitution of a term M for all free occurrences of x in the term N.

A *type universe* is a type which has types as its members. ECC offers two kind of universes, *Prop* and $Type_i$, for natural numbers i. By the Curry-Howard principle of *propositions-as-types* [7, 17], logical formulas are considered as the types of their proofs. They are included in the universe *Prop* and data types reside in the universes $Type_i$. Coquand and Huet [6] demonstrate how logical connectives ($\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$), logical quantification ($\forall$, $\exists$) and *Leibniz equality* ($a = b$) are coded. Strong sums and type universes in ECC prove to be useful for encoding program specifications and abstract implementations between specifications, and for modular development by stepwise refinement [23].

The treatment of rules and proofs is based on the notion of *judgement.* Typing judgements are of the form $\Gamma \vdash M : A$ and express the fact that in context Γ term M is of type A, where a context is defined as a finite sequence of declarations $x{:}A$. Depending on the situation, $a : A$ may be interpreted as "a is of type A", "a is a proof of formula A", or "a meets specification A". A term M is *well-typed* in context Γ, if $\Gamma \vdash M : A$ for some A. A type A is *inhabited* under context Γ if and only if there exists a term M such that $\Gamma \vdash M : A$ is derivable. For a complete presentation of typing rules and a notion of derivability of judgements see [21]. ECC has many good meta-theoretic properties. It obeys the Church-Rosser property, is strongly normalizable, and type checking is decidable.

3 Specification in QED

In the following we extend the calculus ECC by constructs for representing units of the software development process [12]. The design of these constructs is influenced mainly by the PVS specification language [28] and Extended ML [29]. The extensions to ECC are quite expressive in the sense that most of the mathematical and computational concepts we wish to describe can be formulated very directly and naturally. A more comprehensive informal introduction to the QED language can be found in [27], while [31] provides a formal account of the rules for the extended calculus.

Type constructors are introduced to form Cartesian products, (dependent) record types, semantic subtypes, and specifications. All these constructs are special forms of strong sum types in ECC; they are, however, handled differently by the typing system and therefore require special syntax. Cartesian products and record types are of the form $A_1 \times \ldots \times A_n$ and $\ll x_1 : A_1, \ldots, x_n : A_n \gg$ respectively; their elements are tuples $(a_1, \ldots, a_n)$. The common dot notation denotes selection of record fields.

A semantic subtype $\{x : A \mid P\}$ comprises those members of type A which satisfy predicate P. Elements of the semantic subtype are denoted by $a[p]$, where a is a member of type A and p is a proof term of type $P[x := a]$. (This notation is possible because proofs can be expressed as usual terms). A distinctive feature of the typing system is a conversion mechanism that is able to convert members of one type to members of a different type automatically. For example, applying a function that requires a member of $\{x : \mathbb{N} \mid Odd(x)\}$ to the natural number 5 is illegal, because 5 is not a member of the subtype. But if one can find a term p which is a proof of $Odd(5)$, we may rewrite the application using $5[p]$ instead of 5. Since in general it is not possible to find the required proofs automatically, proof obligations are generated. A proof obligation is a placeholder for a term which will be filled in later by the prover. These proof obligations can be postponed because the type checker only requires type information.

A specification consists, as usual, of a signature part and an axiom part; the signature part normally corresponds to a dependent Σ-type, the axiom part is a collection of propositions (elements of type *Prop*) that restrict the set of acceptable "models" of the signature. For instance, the following specification declares a type *Setoid* as consisting of a type T together with a binary Boolean function *eq* on T that is restricted to be an equivalence relation:

$$
\begin{array}{ll}
\mathit{Setoid} := & \textsc{spec} \\
& \quad T : \mathit{Type},\ eq : T \times T \to \mathbb{B} \\
& \textsc{with} \\
& \quad Ax :\ \mathit{equivalence}(eq) \\
& \textsc{end}
\end{array}
$$

Realizations of such specifications are structures that satisfy the axioms. For example, the structure $\textsc{struc}\ T := \mathbb{B},\ eq := eq_{\mathbb{B}}\ \textsc{end}$ is of type *Setoid* if the condition $\mathit{equivalence}(eq_{\mathbb{B}})$ holds. Whenever a structure is type checked and no proof terms are given, proof obligations are generated to fill out any missing proofs. The proof obligations are derived from the specification by substituting terms from the structure into the axioms. In this example the obligation is $\mathit{equivalence}(eq_{\mathbb{B}})$. Let p be a proof of this proof obligation, then the structure above is converted into:

$$
\textsc{struc}\ T := \mathbb{B},\ eq := eq_{\mathbb{B}}\ \textsc{end}\ [p]\ : \mathit{Setoid}
$$

The conversion mechanism is also used by the casting construct (::) of QED. A term $M :: A$ causes the typing system to check if M is a member of type A. If the type check fails, the system tries to generate a term M' of type A from M by introducing proof obligations. This feature is used to generate the proof obligations that are necessary to establish the correctness of the development process. The following function, for example, realizes a refinement map with import specifications imp_1 and imp_2, and the export specification exp.

$$
\begin{array}{ll}
\rho := & \lambda\ r_1 : \mathit{imp}_1,\ r_2 : \mathit{imp}_2. \\
& \quad \textsc{struc} \\
& \quad\quad \ldots \\
& \quad \textsc{end}\ \ ::\ \mathit{exp}
\end{array}
$$

Type casting of the function body produces proof obligations that intuitively state: if realization r_i, $i = 1, 2$, fulfills the axiom part of specification imp_i then $\rho(r_1, r_2)$ fulfills the axioms of exp.

The mechanisms to form *inductive datatypes* follow Ore's extension of ECC [24]. Polymorphic lists, for example, are defined by means of

$$
\mathit{List} :=\ \lambda\ T : \mathit{Type}.\ \textsc{datatype}\ X : \mathit{Type}.\ \mathit{nil}\ \mid\ \mathit{cons} : T \times X
$$

Note that the names of the constructors for inductive datatypes have to be introduced explicitly (e.g. $\mathit{mkNil} :=\ \lambda\ T : \mathit{Type}.\ \textsc{intro}(\mathit{List}(T), \mathit{nil})$). The $\textsc{case}$ construct allows both for structural induction over inductively defined datatypes and for the definition of functions by means of (higher–order) primitive recursion; it can be seen as a variant of the concept of *hom–functionals* [33] and exhibits the natural correspondence between the structure of a program (or proof) and the data structure. For example, the function *map* on polymorphic lists[2]

$$
\begin{array}{ll}
\mathit{map} := & \lambda\ T, S \mid \mathit{Type}, l : \mathit{List}(T), f : \mathit{List}(T) \to \mathit{List}(S). \\
& \quad \textsc{case}\ l\ \textsc{of} \\
& \quad\quad \mathit{nil} : \mathit{mkNil}(S), \\
& \quad\quad \mathit{cons} :\ \lambda\ (t, l_1) : T \times \mathit{List}(T),\ \mathit{rec} : \mathit{List}(S). \\
& \quad\quad\quad\quad \mathit{mkCons}(f(t), \mathit{rec}) \\
& \quad \textsc{end}
\end{array}
$$

[2] The notation $\lambda\ T \mid \mathit{Type}.\ \ldots$ is used to denote type parameters which usually are not provided explicitly, i.e. are left implicit and deduced by type checking.

is completely specified by describing its behavior for each of the constructors separately. In the second case of the CASE construct, the function f applied to head element t is concatenated to the result *rec* of the recursive call of *map*. Inductive datatypes representing Booleans ($\mathbb{B}$), natural numbers ($\mathbb{N}$) and polymorphic lists ($List$) together with appropriate operators are predefined.

The FIX construct allows for defining recursive functions in a restricted form: mutual recursion is not allowed, and functions must be proven to be total. Consider, for example, the definition of the factorial function:

$$\begin{array}{l} \textsc{fix}\ f : \mathbb{N} \to \mathbb{N}. \\ \quad \lambda\ n : \mathbb{N}.\ \textsc{if}\ \mathit{isZero}(n)\ \textsc{then}\ 1\ \textsc{else}\ n * f(n-1)\ \textsc{end} \\ \textsc{measure}\ \ \lambda\ x : \mathbb{N}.\ x \end{array}$$

The MEASURE -function is a function with the same domain as f and, in this case, of range type $\mathbb{N}$. The definition generates the *termination correctness condition*

$$\forall\, n : \mathbb{N}.\ \mathit{isZero}(n) \neq \mathit{true}\ \Rightarrow\ n - 1 <_{\mathbb{N}} n$$

using the standard ordering $<_{\mathbb{N}}$ on $\mathbb{N}$ as default. This condition must be discharged to ensure well-typedness of f. Measure functions can also be utilized in the obvious way to prove properties about recursive functions by means of *Noetherian induction*.

4 Formalizing Development Steps

In this section we present two approaches to formally representing and reasoning about software development steps in QED:

- by higher-order functions,
- by meta-functions.

4.1 Representation of Steps by Higher-Order Functions

The formalization of transformations using higher-order patterns has been considered by several researchers. In [19], for example, program transformations for recursion removal are expressed as second-order patterns defined in the simply typed λ-calculus [5]. As opposed to this treatment we use the powerful framework of QED and demonstrate that it is possible to formalize and verify a "large" development step illustrated by a schematic algorithm *global-search*. Due to space limitations, only the most essential features can be sketched, the rigorous mathematical treatment and verification is presented in [9].

Global-search is a generalization of well-known search strategies such as *backtracking* and *depth-first-search*; see [32] for details. Starting from a requirement specification an extension of this specification is needed which defines additional datatypes and operations to realize the global-search algorithm. This extended structure is combined in a specification called *global_search_theory*. Based on this theory an abstract generic algorithm can be defined. Instantiating the abstract scheme with the specific problem structure together with a proof that the structure fulfills the axioms of *global_search_theory* suffices to synthesize an algorithm realizing a constructive solution of the problem. Using this method, in [9] we derive a *key-search* algorithm and show that its verification is easily obtained by applying the correctness proof of the transformation to the specific problem structure.

One starts with the following specification:

$$\mathit{Problemspec} := \ll D : \mathit{Type}, R : \mathit{Type}, I : D \to \mathit{Prop}, O : D \times R \to \mathit{Prop} \gg$$

$\mathit{global\_search\_theory} := \lambda\ (D, R, I, O) : \mathit{Problemspec}.$

SPEC

$S : \mathit{Type}$

$J : D \times S \to \mathit{Prop}$

$\mathit{init} : D \to S$

$\mathit{satisfies} : R \times S \to \mathit{Prop}$

$\mathit{split?} : D \to (S \times S \to \mathit{Prop})$

$\mathit{split} : D \times S \to \mathit{Set}(S)$

$\mathit{extract?} : R \times S \to \mathit{Prop}$

$\mathit{extract} : D \times S \to \mathit{Set}(R)$

WITH

$ax1 : \forall\, x : D.\ I(x) \Rightarrow J(x, \mathit{init}(x)),$

$ax2 : \forall\, x : D,\ r, s : S.\ (I(x) \wedge J(x, r) \wedge \mathit{split?}(x)(r, s)) \Rightarrow J(x, s),$

$ax3 : \forall\, x : D, z : R.\ (I(x) \wedge O(x, z)) \Rightarrow \mathit{satisfies}(z, \mathit{init}(x)),$

$\ldots$

END

Figure 1: Definition of a global_search_theory

where D is the domain type, R the range type, I the input condition restricting D to legal inputs and O the input/output relation. The problem is then formally described by[3]

$$\begin{aligned} \mathit{req\_spec} := \ & \lambda\ (D, R, I, O) : \mathit{Problemspec}. \\ & \forall\, x : D.\ I(x) \Rightarrow \exists\, S : \mathit{Set}(R).\ \forall\, \mathit{elem} : R. \\ & ((\mathit{elem} \in S) = \mathit{true}) \Leftrightarrow O(x, \mathit{elem})) \end{aligned}$$

req_spec is a function which takes a 4-tuple (a member of type *Problemspec*) as input and provides a proposition which states that there exists a set which contains all solutions *elem* for which $O(x, \mathit{elem})$ holds. The schematic algorithm defined below realizes a constructive proof of this proposition.

A *global_search_theory* is a parameterized specification with a member of *Problemspec* as parameter. The basic idea of global-search is to represent and manipulate sets of candidate solutions. Starting from an *initial* set containing all solutions, a global-search algorithm repeatedly *extracts* solutions, *splits* sets into subsets until no sets remain to be split. Sets are represented implicitly by *descriptors* and a predicate *satisfies* determines when a candidate solution is in the set denoted by the descriptor. Furthermore, a predicate J describes legal descriptors. The whole process can be regarded as a tree search procedure where nodes represent sets implicitly described by the type S of set descriptors and arcs represent the *split* operation. The theory is briefly sketched in Fig.1.

The function F_{gs} (Fig.2) defines the schematic algorithm which realizes the global search procedure. It receives as input a realization of a *global_search_theory* and two additional functions *arbsplit* and *tcl*. The result is then a function f which implements the search strategy for the given *global_search_theory*. The function *arbsplit* takes a set s and provides an arbitrary element of s and the remaining set. The function *tcl* is used for termination. It produces for a given set of nodes in the search tree its (finite) set of successors with respect to the *split?* relation, i.e. it calculates the transitive closure of *split?*. This specifies a finite depth of the search tree. One implicitly yields a finite width by using the polymorphic type *Set* of finite

[3] We suppose that the type $\mathit{Set}(T)$ of finite sets over a type T together with suitable operations is given.

```
$F_{gs}$ := $\lambda$ $(D, R, I, O) : Problemspec,\ gs : global\_search\_theory((D, R, I, O)),$
        $arbsplit : \ldots,\ tcl : \ldots.$
    LET
        $F\_Type := \ll active : Set(gs.S), solution : Set(R),$
                $x : \{D \mid Invar((D, R, I, O), gs, active, solution, x)\} \gg$
    IN
        FIX $f : F\_Type \to Set(R).\ \ \lambda\ (active, solution, x) : F\_Type.$
            IF $empty?(active)$ THEN $solution$
                ELSE
                LET
                    $(r, A_1) := arbsplit(active),$
                    $Newactive := A_1 \cup gs.split(x, r),$
                    $Newsolution := solution \cup gs.extract(x, r)$
                IN
                    $f(Newactive, Newsolution, x)$
        MEASURE
            $\lambda\ (active, solution, x) : F\_Type.\ card(tcl(active, solution, x))$
```

Figure 2: The schematic algorithm *Global Search*

sets, i.e. *split* produces for a given node the finite set of its (direct) descendants. The resulting function f is given by means of wellfounded recursion. To guarantee well-typedness of F_{gs} we must supply a *measure* function. Here we use the cardinality of the transitive closure of the active set of nodes which have to be considered. An *invariant* is used in the domain *F_Type* of f to ensure the following basic properties:

1. every node of the active set is a legal descriptor
2. all elements of the set *solution* fulfill the condition O
3. for two arbitrary nodes s_1, s_2 of the active set, s_2 is not a successor of s_1 w. r. t the *split*? relation.

The concept of semantic subtypes is an adequate tool to represent invariants of functions.

To establish the correctness of the defined development step one has to show that for an arbitrary problem specification and global search theory the instantiated function f is indeed a constructive solution, i.e. f calculates the set of all elements of the range type R which satisfy the condition O. The initial parameters for f are $init(x)$ for *active* and $\varnothing_R$ for *solution*. The soundness theorem is given in Fig.3. Additionally, to ensure type correctness some type correctness conditions are generated. The first one states that the measure function applied to the parameters of the recursive call yields a smaller value than the function called with the actual parameters. Furthermore, the parameter of the recursive call and the initial parameters must satisfy the invariant of f. All proof obligations have successfully been discharged using the (interactive) higher-order Gentzen prover of the PVS specification system [25, 28].

The techniques outlined above can readily be used to formalize many generic development steps including "large" transformations such as *divide-and-conquer*, *dynamic programming* and those investigated by the Munich CIP group [15, 26].

$$\begin{array}{l}
\mathit{Soundness\_Theorem} := \\
\quad \forall\,(D, R, I, O) : \mathit{Problemspec},\ \mathit{gs} : \mathit{global\_search\_theory}((D, R, I, O)), \\
\quad\ \ \mathit{arbsplit} : \ldots,\ \ \mathit{tcl} : \ldots,\ \ x : \{D \mid I(x)\},\ \ y : R. \\
\quad\ \ \ \text{LET} \\
\qquad\quad \mathit{F\_inst} := F_{gs}((D, R, I, O), \mathit{gs}, \mathit{arbsplit}, \mathit{tcl}), \\
\qquad\quad \mathit{init\_set} := \mathit{insert}(\mathit{gs.init}(x), \varnothing_{gs.S}), \\
\qquad\quad \mathit{init\_sol} := \varnothing_R, \\
\qquad\quad \mathit{sol\_set} := \mathit{F\_inst}(\mathit{init\_set}, \mathit{init\_sol}, x) \\
\quad\ \ \ \text{IN} \\
\qquad\quad (y \in \mathit{sol\_set} = \mathit{true}) \Leftrightarrow O(x, y)
\end{array}$$

Figure 3: Soundness Theorem of *Global Search*

4.2 Meta-Operators

Many typical development steps are not representable with the language constructs introduced in Sect. 3. Consider, for example, the simple task of replacing a certain axiom P_i in a specification text by another axiom Q. If Q implies P_i then one can construct a refinement map from the modified specification to the original one. More precisely: let Γ be the current context, abbreviate $x_1 : A_1, \ldots, x_n : A_n$ by $\mathbf{x} : \mathbf{A}$, and define a specification

$$\mathit{sp}_1 :=\ \ \text{SPEC}\ \ \mathbf{x} : \mathbf{A}\ \ \text{WITH}\ p_1 : P_1, \ldots,\ p_i : P_i, \ldots,\ p_m : P_m\ \text{END}$$

that is well-typed in Γ. Furthermore, assume that the judgement $\Gamma, \mathbf{x} : \mathbf{A} \vdash p : Q \Rightarrow P_i$ is derivable.[4] It is our task to construct a realization of sp_1 relative to a realization of specification

$$\mathit{sp}_2 :=\ \ \text{SPEC}\ \ \mathbf{x} : \mathbf{A}\ \ \text{WITH}\ p_1 : P_1, \ldots,\ q : Q, \ldots,\ p_m : P_m\ \text{END}$$

A refinement map from specification sp_2 to specification sp_1 is constructed as

$$\begin{array}{l}
\rho :=\ \ \lambda\ r : \mathit{sp}_2. \\
\qquad\qquad \text{STRUC}\ x_1 := r.x_1, \ldots, x_n := r.x_n\ \text{END}\ [r.p_1, \ldots, p(r.q), \ldots, r.p_m]
\end{array}$$

and the type introduction rule for structures immediately yields:

$$\Gamma \vdash \rho : \mathit{sp}_2 \to \mathit{sp}_1$$

A transformation of this kind which takes a specification sp_1, a formula Q, and an index i and results in a new specification sp_2 by replacing the i-th axiom in sp_1 by Q needs both access to internal structure in order to manipulate syntactical text and the correctness of this formalization involves reasoning about derivability of judgements, i. e. meta-reasoning. Furthermore, this development step deals with a term Q that is not necessarily well-typed in the current context Γ but only in $\Gamma, \mathbf{x} : \mathbf{A}$.

In the following we describe a *meta architecture* that allows one to express such development steps and transformations by means of functions on representations of programs (proofs) and specification texts. These functions are called *meta functions* and are amenable to formal treatment; e.g. one can state and prove characteristic properties about them.

Historically, meta architectures were first formalized and investigated by logicians, where the pioneering work has been carried out by Gödel [14]. From a more application oriented

[4] Note that Q need not be well-typed in context Γ if some x_i occurs free in Q.

view, meta level architectures have been used extensively in the realm of mechanical theorem proving [3, 2, 18, 20], since in many cases it is quite straightforward to construct a proof by means of syntactic analysis of the problem at hand [34, 1]. Here, the important issue is how meta programming and meta reasoning can be used to represent software development steps together with expressing a certain semantics of these steps.

In a first step one encodes syntactic categories and the proof theory of QED within itself following the approach of Gödel. This encoding constitutes the *meta level.* On this encoding one can write (almost) arbitrary functions and express relations like "x is a free variable in M" or "the result of substituting the term N for all free occurrences of the variable x in M yields L". A particularly important predicate is the derivability predicate expressing the relation that "M is of type A in context Γ". These features allow to encode development steps (proof steps) by meta functions, and to express and prove "semantic" relations between arguments and results. The adequacy and faithfulness of the encoding yield *reflection principles* that allow one to exchange results between the meta level and the object level in a sound way.

Due to lack of space we can merely present a fragmentary sketch of the architecture. One first represents syntactical categories of the object language syntax by means of the inductive datatype *AbsTrm*. The elements of this data type can be seen as abstract syntax of terms. This abstract syntax does not necessarily represent well-typed terms. Representations of specifications, for example, can be formed by means of the constructor *mkSpec* of type $\mathit{List}(\mathit{Id} \times \mathit{AbsTrm}) \times \mathit{List}(\mathit{Id} \times \mathit{AbsTrm}) \to \mathit{AbsTrm}$. The first argument represents the signature, while the second one represents the axiom part; *Id* is just the type for identifiers. It is straightforward to introduce recognizers and selectors for each alternative in the datatype *AbsTrm*. For specifications we have the recognizer *isSpec* and selectors *specSig* and *specAxms*. Recognizer $\mathit{isSpec}(M)$ yields *true* if and only if M represents a specification, while *specSig* and *specAxms* respectively select the (representations of the) signature and the axiom part. In the following we also utilize the constructor *mkStruc* with corresponding selectors *strucDefs* and *strucPrfs*.

Contexts are represented by elements of type *Ctxt* which is a list of (representations of) type assignments $x : A$ while judgements are represented by elements of $\mathit{Jdgmt} := \mathit{Ctxt} \times \mathit{AbsTrm} \times \mathit{AbsTrm}$. The data types *AbsTrm*, *Ctxt*, and *Jdgmt* are called *representation types* and elements of them are meta terms.

A quoting mechanism '.' associates syntactic categories of the object level like terms, contexts, and judgements with meta terms; for example:

$$\begin{array}{l} \text{'}\ \textsc{spec}\ x_1 : A_1, x_2 : A_2\ \textsc{with}\ p_1 : P_1, p_2 : P_2\ \textsc{end}\ \text{'} := \\ \quad \mathit{mkSpec}(\langle(\text{'}x_1\text{'}, \text{'}A_1\text{'}), (\text{'}x_2\text{'}, \text{'}A_2\text{'})\rangle, \langle(\text{'}p_1\text{'}, \text{'}P_1\text{'}), (\text{'}p_2\text{'}, \text{'}P_2\text{'})\rangle) \end{array}$$

Through the mapping '.' object-level constructs become available for discourse on the meta-level.

It is a standard exercise to encode the term calculus. One defines functions *occurs* of type $\mathit{AbsTrm} \times \mathit{Var} \to \mathbb{B}$ and *substVar* of type $\mathit{AbsTrm} \times \mathit{Var} \times \mathit{AbsTrm} \to \mathit{AbsTrm}$ by means of higher–order primitive recursion such that $\mathit{occurs}(\text{'}M\text{'}, \text{'}x\text{'})$ reduces to *true* if and only if x occurs free in M and $\mathit{substVar}(\text{'}M\text{'}, \text{'}x\text{'}, \text{'}N\text{'})$ reduces to $\text{'}M[x := N]\text{'}$. Binary relations on terms like syntactic equality (modulo *alpha*-convertibility) and convertibility can be coded in a type-theoretic setting by closures of the appropriate binary relations. Likewise derivability of a judgement , denoted by $\mathit{deriv}(.)$, is encoded as the least set (one-place predicate) closed under the rules of the type calculus of QED. The following fact expresses adequacy and faithfulness of this encoding of derivability

> $\Gamma \vdash M : A$ is derivable if and only if there exists a term p such that $\vdash p : \mathit{deriv}(\text{'}\Gamma\text{'}, \text{'}M\text{'}, \text{'}A\text{'})$

Obviously, a proof of this can neither be carried out on the object level nor on the meta level, but is rather accomplished in the (informal) theory that allows one to reason about both of these levels. The result above allows one to deduce from the derivability of $\Gamma \vdash M : A$ on the object level the existence of a term of type $\mathit{deriv}(\text{'}\Gamma\text{'}, \text{'}M\text{'}, \text{'}A\text{'})$. This transition from object level to meta level is named *reflection upwards* while the corresponding change from meta level to object level is called *reflection downwards* [13]. These reflection rules are admissible inferences, and thus, in principle, dispensible. From a practical point of view, however, reflection rules are crucial since they allow to exchange results between object level and meta level as exemplified in the following.

In the remaining we formalize the development step described in the beginning of this section within our meta architecture and demonstrate how to apply meta functions and corresponding correctness results. The meta function *replaceAxInSpec* replaces in (the representation of) a specification *sp* the (representation of the) i-th axiom by (the representation of) another term *axm*, where *replace* is the replacement on lists:

$$
\begin{array}{l}
\mathit{replaceAxInSpec} := \\
\qquad \lambda\ \mathit{sp} : \{\mathit{AbsTrm} \mid \mathit{isSpec}(\mathit{sp}) = \mathit{true}\}, i : \mathit{Nat}, \mathit{axm} : \mathit{AbsTrm}. \\
\qquad\quad \mathit{mkSpec}(\mathit{specSig}(\mathit{sp}), \mathit{replace}(\mathit{specAxms}(\mathit{sp}), i, \mathit{axm}))
\end{array}
$$

It simply replaces the i-th element in the list of axiom representations with the argument *axm*. The following predicate states that the resulting (representation of a) specification is indeed a refinement of the argument (representation of a) specification

$$
\begin{array}{l}
\forall\, \mathit{ctxt} : \mathit{Ctxt}, \mathit{sp} : \{\mathit{AbsTrm} \mid \mathit{isSpec}(\mathit{sp}) = \mathit{true}\}, i : \mathit{Nat}, \mathit{axm}, M : \mathit{AbsTrm}. \\
\mathit{deriv}(\mathit{append}(\mathit{ctxt}, \mathit{specSig}(\mathit{sp})), M, \mathit{mkImpl}(\mathit{axm}, \mathit{nth}(i, \mathit{specAxms}(\mathit{sp})))) \\
\qquad \Rightarrow\ \text{LET } \mathit{Res} := \mathit{replaceAxInSpec}(\mathit{sp}, i, \mathit{axm}), \\
\qquad\qquad\qquad N := \mathit{mkLambda}((\text{'}r\text{'}, \mathit{Res}), \\
\qquad\qquad\qquad\qquad\qquad \mathit{mkStruc}(\mathit{strucDefs}(\mathit{mkRef}(\text{'}r\text{'})), \\
\qquad\qquad\qquad\qquad\qquad\quad \mathit{replace}(\mathit{strucPrfs}(\mathit{mkRef}(\text{'}r\text{'})), i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathit{mkApp}(M, \mathit{mkProj}(\mathit{mkRef}(\text{'}r\text{'}), i))))) \\
\qquad\qquad \text{IN } \mathit{deriv}(\mathit{ctxt}, N, \mathit{mkImpl}(\mathit{Res}, \mathit{sp})) \quad ,
\end{array}
$$

where $\mathit{mkImpl}(\text{'}A\text{'}, \text{'}B\text{'})$ is the representation of $A \to B$, and the term N is, despite the ugliness of abstract syntax, a mere formalization of the refinement term constructed in the beginning of this (meta) exposition. The functions *append* and *nth* denote concatenation of lists and selection of the n-th element from a list, respectively. The proof of this correctness result is straightforward and a direct formalization of the informal exposition above; call the corresponding proof $\mathit{correct}_{\mathit{prf}}$. This proof and the reflection principles can be utilized to construct a refinement map between the specification *sp* and the result of the transformation *replaceAxInSpec*.

Let's go back to our running example and apply *replaceAxInSpec* together with its corresponding correctness result. Again we assume a certain context Γ and a specification *sp*. Furthermore, let $\text{'}Q\text{'}$ be the representation of a certain axiom and i be a fixed natural number. In order to apply $\mathit{correct}_{\mathit{prf}}$ one has to construct an element $\text{'}M\text{'}$ such that

$$
\begin{array}{l}
\mathit{deriv}(\mathit{append}(\text{'}\Gamma\text{'}, \mathit{specSig}(\text{'}\mathit{sp}\text{'})), \\
\qquad \text{'}M\text{'}, \mathit{mkImpl}(\text{'}Q\text{'}, \mathit{nth}(i, \mathit{specAxms}(\text{'}\mathit{sp}\text{'}))))
\end{array}
$$

holds. This construction can, of course, be completely done within the meta level. In many situations, however, it is more appropriate to prove the corresponding problem in the object level; i.e. one has to find a term M such that $M : Q \Rightarrow P_i$ is derivable in context $\Gamma, \mathbf{x} : \mathbf{A}$. The resulting judgement is reflected upwards yielding a proof p of the predicate above. A simple instantiation of $correct_{prf}$ gives:

$$\begin{array}{l} \vdash correct_{prf}(\,'\Gamma'\,,\ 'sp'\,, i,\ 'Q'\,,\ 'M'\,, p) \\ \quad :\ \text{LET}\ Res := replaceAxInSpec(\,'sp'\,, i,\ 'Q'\,),\ N := \ldots \\ \quad\quad \text{IN}\ deriv(\,'\Gamma'\,, N, mkImpl(Res,\ 'sp'\,)) \end{array}$$

This judgement, finally, is reflected down to the object level in order to get the result that the resulting specification *Res* indeed is a refinement of the argument specification. Moreover, downward reflection explicitly constructs the object-level refinement map.

The two-level framework as depicted above has been utilized, for example, for formal constructions of a lexical scanner [8] and a symbol table [10]. A particularly interesting meta function in the latter case study involves the partial implementation of a function in a specifiction. This meta function takes a specification sp_1, a function f declared in sp_1, and a realization f_{imp} of f by means of other entities declared in sp_1 and delivers a new specification sp_2 in which the declaration of f is deleted from the signature part and all formulas where f occurs free are removed from the axiom part. This simplified specification sp_2 is amenable to further refinement.

As demonstrated above, we are able to formalize conclusions about the object calculus by means of a meta architecture. This allows one to encode formal development steps *once and for ever*; applications of such steps are instances of some meta level argument, while, in the case of pure object level reasoning, one has to do the same kind of tedious development over and over for each instance of a given problem. Software development systems incorporating a meta architecture allow users of such systems to add new development (proof) steps only in a sound way. The importance of such features lies in the fact that it is unrealistic to incorporate each conceivable development step in a general–purpose development system [11]. Finally note that, in our approach, meta functions and meta properties are essentially the same as object functions and object properties; they only differ in the data types they are operating on. Thus, encoding, specification, and proof methods apply for both object and meta level entities.

5 Some Notes on the experimental QED Implementation

An interactive support system for experiments with QED has been developed. The system implements a parser, type checker and pretty printer for the QED language. The heart of the system is the type checker. It is mainly built around an evaluation function for *pre-terms*. A pre-term is a syntactically correct term that may be ill-typed. The evaluation function takes a pre-term and a set of definitions and, if possible, converts the pre-term to a well-typed term, see also Sect. 3.

In ECC all types belong to exactly one type universe. However, in most cases the specific universe to which a term belongs is irrelevant. For this reason the system offers the possibility to use the anonymous universe *Type* instead of $Type_i$ for a given level i. The system tries then to exactly determine the universe level i by maintaining a set of inequalities and checking for consistency [16].

Parametric polymorphism is handled by unification. Although higher-order unification is undecidable most problems which arise in practice from type checking polymorphic functions can be solved correctly by the implemented unification algorithm. This result is obtained by coding the universe polymorphism, reductions, alpha convertibility and other features into the unification algorithm.

In an interactive top-down program development process it is desirable to type check specifications and their realizations before the whole development is complete. To achive this goal, incomplete terms containing placeholders together with suitable type information may be used. Later in the development process these placeholders will be replaced by members of the appropriate type. This feature, together with a refinement editor, provides for a refinement process similar to the one described for Extended ML [29, 30].

6 Conclusions and Future Work

In this paper we have presented an approach to formal specification and software development based on type theory. We have discussed the logical basis and illustrated the elementary principles by means of simple examples. Our experience gained so far with the approach supports our hypothesis that specification based on type theory is a viable alternative to the more common algebraic specifications and that many, if not most, interesting operations on, and relationships among, development units can be dealt with by a combination of object-level and meta-level formalization.

The work described here is part of an ongoing investigation into formal methods for software development and effort to develop a suitable framework. Specifically, we plan to develop a basic set of generic algorithms and meta-operators representing development steps, with the long-term goal of compiling some sort of reusable "knowledge base" of programming techniques, and to test whether this approach can be made practical by attacking non-trivial software problems.

References

[1] L. Aiello and R.W. Weyhrauch. Using meta-theoretic reasoning to do algebra. In W. Bibel and R. Kowalksi, editors, *5th Conference on Automated Deduction*, pages 1–13. Springer Verlag, 1980.

[2] S.F. Allen, R.L. Constable, D.J. Howe, and W.E. Aitken. The semantics of reflected proof. In *Proc. 5th Annual IEEE Symposium on Logic in Computer Science*, pages 95–105. IEEE CS Press, 1990.

[3] R.S. Boyer and J.S. Moore. Metafunctions: proving them correct and using them efficiently as new proof procedures. In R.S. Boyer and J.S. Moore, editors, *The Correctness Problem in Computer Science*, chapter 3. Academic Press, 1981.

[4] M. Broy and P. Pepper. Programming as a Formal Activity. *IEEE Transactions on Software Engineering*, SE-7:1:10–22, 1981.

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

[6] T. Coquand and G. Huet. Constructions: a Higher-Order Proof System for Mechanizing Mathematics. In B. Buchberger, editor, *EUROCAL'85: European Conference on Computer Algebra*, Lecture Notes in Computer Science 203, pages 151–184. Springer-Verlag, 1985.

[7] H.B. Curry and R. Feys. *Combinatory Logic*, volume 1. North Holland Publishing Company, 1958.

[8] A. Dold. A Constructive Program Development Methodology - exemplified by the case-study LEX. Korso paper, Universität Ulm, 1994.

[9] A. Dold. Formalisierung schematischer Algorithmen. Technical report, Abt. KI, Universität Ulm, 1994.

[10] A. Dold and D. Schwier. Formal construction of a symbol table. Korso paper, Universität Ulm, 1994.

[11] B. Krieg-Brückner et al. System architecture framework for KORSO. In M. Broy and S. Jähnichen, editors, *KORSO, Correct Software by Formal Methods*. Springer-Verlag, LNCS (1994). Erscheint im Laufe des Jahres.

[12] M. Wirsing et al. A Methodology for the Development of Correct Software. In M. Broy and S. Jähnichen, editors, *KORSO, Correct Software by Formal Methods*. Springer-Verlag, LNCS (1994). Erscheint im Laufe des Jahres.

[13] F. Giunchiglia and A. Smaill. Reflection in Constructive and Non-Constructive Automated Reasoning. In *Meta-Programming in Logic Programming*, chapter 6, pages 123–140. The MIT Press, 1989.

[14] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. *I. Monatsh. Math. Phys.*, 38:173–198, 1931.

[15] CIP System Group. *The Munich Project CIP - Volume II.* Lecture Notes in Computer Science 292. Springer-Verlag, 1987.

[16] R. Harper and R. Pollack. Type checking, universal polymorphism, and type ambiguity in the Calculus of Constructions. In *TAPSOFT'89, volume II*, Lecture Notes in Computer Science, pages 240–256. Springer-Verlag, 1989.

[17] W.A. Howard. The Formulae-as-Types Notion of Construction. In J. Hindley and J. Seldin, editors, *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism.* Academic Press, 1980.

[18] D.J. Howe. Computational metatheory in Nuprl. In *Proc. 9th International Conference on Automated Deduction*, pages 238–257. Springer-Verlag Lecture Notes in Computer Science 310, 1988.

[19] G. Huet and B. Lang. Proving and applying program transformations expressed with second-order-patterns. *Acta Informatica*, 11:31–55, 1978.

[20] T.B. Knoblock and R.L. Constable. Formalized metareasoning in type theory. In *Proceedings of LICS*, pages 237–248. IEEE, 1986. Also available as technical report TR 86-742, Department of Computer Science, Cornell University.

[21] Z. Luo. An Extended Calculus of Constructions. Technical Report CST-65-90, University of Edinburgh, July 1990.

[22] Z. Luo. A Higher-Order Calculus and Theory Abstraction. *Information and Computation*, 90:107–137, 1991.

[23] Z. Luo. Program Specification and Data Refinement in Type Theory. In S. Abramsky and T.S.E. Maibaum, editors, *TAPSOFT'91, volume I*, Lecture Notes in Computer Science 494, pages 143–168. Springer-Verlag, 1991.

[24] Ch.E. Ore. The extended calculus of constructions (ECC) with inductive types. *Information and Computation*, 99:231–264, 1992.

[25] S. Owre, J. M. Rushby, and N. Shankar. PVS: A prototype verification system. In Deepak Kapur, editor, *11th International Conference on Automated Deduction (CADE)*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 748–752, Saratoga, NY, 1992. Springer-Verlag.

[26] H.A. Partsch. *Specification and Transformation of Programs.* Springer-Verlag, 1990.

[27] H. Rueß. Report on the specification language QED. Korso working paper, Universität Ulm, 1993.

[28] J.M. Rushby S. Owre, N. Shankar. *The PVS Specification Language.* Computer Science Lab, SRI International, Menlo Park CA 94025, March 1993.

[29] D. Sannella and A. Tarlecki. Toward formal development of ML programs: foundations and methodology. In *Proc. TAPSOFT 89, Barcelona*, number 352 in LNCS, pages 375–389. Springer, 1989.

[30] D. Sannella and A. Tarlecki. Toward formal development of programs from algebraic specifications: model-theoretic foundations. In *Proc. Intl. Colloq. on Automata, Languages and Programming, Vienna*, number 623 in LNCS, pages 656–671. Springer, 1992.

[31] D. Schwier. Type checking the specification language QED. Korso working paper, Universität Ulm, 1994.

[32] D. R. Smith. Structure and design of global search algorithms. Technical Report KES.U.87.12, Kestrel Institute, Palo Alto, CA, 1987.

[33] F. W. von Henke. An algebraic approach to data types, program verification, and program synthesis. In *Mathematical Foundations of Computer Science, Proceedings.* Springer-Verlag Lecture Notes in Computer Science 45, 1976.

[34] R. W. Weyhrauch. Prolegomena to a Theory of Mechanized Formal Reasoning. *Artificial Intelligence*, 13(1):133–170, 1980.