On the Representation of Data Structures in LCF with Applications to Program Generation

by

Frederich W. von Henke

Research sponsored by

Advanced Research Projects Agency
ARPA Order No. 2494
and
Deutsche Akademische Austauschdienst
On the Representation of Data Structures in LCF with Applications to Program Generation

by

Frederich W. von Henke

ABSTRACT

In this paper we discuss techniques of exploiting the obvious relationship between program structure and data structure for program generation. We develop methods of program specification that are derived from a representation of recursive data structures in the Logic for Computable Functions (LCF). As a step towards a formal problem specification language we define definitional extensions of LCF. These include a calculus for (computable) homogeneous sets and restricted quantification. Concepts that are obtained by interpreting data types as algebras are used to derive function definition schemes from an LCF term representing a data structure; they also lead to techniques for the simplification of expressions in the extended language. The specification methods are illustrated with a detailed example.

Authors' present address: Gesellschaft fuer Mathematik und Datenverarbeitung Bonn, 5205 St. Augustin, Schloss Birlinghoven, West Germany

This research was supported by the Advanced Research Projects Agency of the Department of Defense under Contract DAHC 15-73-C-0435 and the Deutsche Akademische Austauschdienst. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as necessarily representing the official policies, either expressed or implied, of Stanford University, ARPA, Deutsche Akademische Austauschdienst, or the U. S. Government.

Reproduced in the U.S.A. Available from the National Technical Information Service, Springfield, Virginia 22151.
Contents

1. Introduction

2. The type-free Logic for Computable Functions
   2.1 Type-free LCF
   2.2 Retracts, Domains, Types

3. Abstract Data Types in the Type Free Logic
   3.1 Data Type Definitions
   3.2 Representing Data Structures in tfLCF
   3.3 Algebraic Interpretation of Data Types
   3.4 Non-generic Data Types
   3.5 An Example: Infix to Post-fix Translation

4. Elements of a Problem Specification Language
   4.1 Sets, Set Operations and Quantification
   4.2 Schemes for Function Definition
   4.3 Transformation of Function Definitions into Programs

5. An Example: Substitution with α-Conversion
   5.1 The Data Types
   5.2 The Problem

6. Concluding Remarks

R. References

A. Appendices
   A.1 Logic for Computable Functions
   A.2 Special functions in tfLCF
   A.3 Structural Induction


1. Introduction

In this paper we are concerned with the use of data structures in generating correct programs from formal problem statements.

Present experimental systems for automatic program synthesis (see [BuL], [MaW] for recent work) are based on a rather large amount of knowledge in the form of individual axioms and problem solving methods. At each step in the synthesis process the system has to search for an applicable piece of knowledge in the data base. One of the main problems is the automatic construction of iterative loops or recursive calls. However, it can be observed that the structure of the data is reflected more or less in the structure of any program operating on them, both in the analysis of subcases and (iterative or recursive) loops. In fact, if a recursion or iteration is possible (and reasonable) at all it is because of a corresponding data structure. So it is safe to say that the generation of a program is always guided by an underlying domain structure. Thus, by "strengthening" the guide lines we can avoid the system having to "retrieve" anew the underlying structure each time it is synthesizing a program. Organizing the knowledge about the data domain and representing it in such a way that it directly assists a system in constructing a program can possibly eliminate some complicated problem solving processes.

In the case of recursive data types the relationship between program structure and data structure is particularly obvious. For this kind of data types the Logic for Computable Functions (LCF) [Mi1, Mi2, WM] provides a natural basis for reasoning about program generation, since both the problem and the prospective structure can be expressed in the same formal system. Obviously, the crucial point is to find an appropriate representation of the data structure. A large portion of this paper is devoted to this problem; it attempts to develop a sufficient mathematical framework for dealing with abstract data types within LCF. Based on this theory methods of function specification are investigated that are directly derivable from the data structure representation and do not require general problem solving methods. They include extensions of the term language of LCF, in particular a calculus for (a restricted kind of) sets and restricted quantification, and certain "definition schemes"; both kinds are based on concepts obtained by interpreting data types as algebras.

The definition techniques are meant to be a step towards a "problem specification language" that allows easy and concise definition of functions on a level of abstraction that is close to the intuitive conception of the user. This approach to program specification bears a resemblance with what has been called "very high level" or "non-procedural" programming languages. Indeed, programming language features similar to some of the constructions to be discussed here have been proposed elsewhere (e.g. [Ea]) and are available in SETL. However, we are not dealing with a programming language, but a formal system that permits formal reasoning. Emphasis is given to interpreting the added constructions in terms of LCF in order to make feasible meaning preserving transformations.
Introduction

of expressions. Only the fact that every LCF term also has an interpretation as a computation rule for the function denoted by it, allows us to regard it as a kind of program.

The following section provides the logical and mathematical framework as needed in the subsequent sections. It gives a short overview of the type free version of LCF and the mathematical theory of subdomains. Section 3 discusses the axiomatization of abstract data types, their representation in LCF, and the interpretation of types as heterogeneous algebras. Section 4 is devoted to introducing elements of a specification language, which include (computable) sets, set operations and bounded quantification. The algebraic concepts of section 3 lead to methods for defining and simplifying functions over data types. In section 5, the definition methods are demonstrated in an example that is based on the data types of LCF terms and is taken from a LCF implementation. Finally, possible directions of future work are indicated in the concluding section.

The paper is intended to be essentially self-contained. The letters "T.P." that can often be found instead of a proof are meant to indicate that a prove has been generated by means of the interactive theorem prover for LCF. The amount of user interaction required to generate a proof is not indicated; in general, the proofs for simple lemmas can be generated fully automatically. The automatic theorem prover component of the system employed for proof generation will be described in detail in a forthcoming paper [He].
2. The type-free Logic for Computable Functions

The Logic for Computable Functions (LCF) was invented by D. Scott (unpublished) and, in a modified form, mechanized by R. Milner [Mil, Mi2]. Using this interactive proving system the logic has subsequently been applied to various problems in the Mathematical Theory of Computation: schematology, formalization of syntax and semantics of programming languages, proving properties of programs and the correctness of interpreters and compilers (cf. [AAW, N2] for more recent work on PASCAL and LISP and comprehensive references). In these experiments LCF proved very useful for formalizing and proving problems involving (possibly partial) recursive functions.

In the following the reader is assumed to be familiar at least with the basics of LCF. For the sake of self-containment a syntax of the language is given in appendix A.

2.1 Type-free LCF

In this subsection the type free version of LCF (or tfLCF for short) is described briefly as needed for the further development. This version of the logic was developed by D. Scott, R. Milner and R. Weyhrauch [unpublished notes]. Most of the material and the ideas presented here is essentially due to them; part of it can also be found in [Sc2].

Essentially, tfLCF axiomatizes one of Scott's models for the \( \lambda \)-calculus [Sc1]: the domain \( I \) which is constructed over the 4-element lattice \( T \) of truth values:

\[
\begin{array}{c}
T \\
\downarrow \\
\uparrow \quad / \\
\downarrow \\
\uparrow \\
\downarrow \\
\downarrow \\
\end{array}
\]

The main characteristic of the domain \( I \) is that it is isomorphic to its domain of continuous functions; thus, each element of \( I \) can also be regarded as a function from \( I \) to \( I \).

The language of the logic itself is essentially the same as for the typed version (see appendix A.1.1), with two exceptions:

(a) the restrictions for building expressions that result from the types are abolished;
(b) besides the 4 truth values, the language includes constants \( I \) for the "universe", i.e. the domain of the model, and \( T \) for the domain of truth values.

The main problem in extending the semantics of expressions to the type free case is defining the meaning of the conditional \( p \to q, r \) for any term \( p \). This is done by mapping the elements of \( I \) onto the truth values (this will be made clearer in the following subsection). The meaning of \( T = x, y \) is not further specified except that \( T = x, x \) is. However, it turns out that it can be taken as the join of \( x \) and \( y \) (see below).
The type-free Logic for Computable Functions

For details about axioms and inference rules of the logic, see appendix A.1.2.

The element $\bot$ is called *undefined*, and the element $\top$ is called *overdefined*; all other elements are called *defined*. A predicate $d$ can be defined in $I$ such that

$$d(x) = \top \text{ iff } "x \text{ is defined;" } \quad \delta(\bot) = \bot, \quad \delta(\top) = \top$$

i.e., $\delta$ yields the distinction between defined and non-defined elements in $I$. $\delta$ is definable in the logic by a mapping onto the 3-element lattice $\{\bot, \top, \#\}$ The definition depends on the fact that the truth values are isolated elements in the lattice $I$. For details see appendix A.2.1.

A function $f$ is called strict if it returns $\bot$ or $\top$ whenever the argument is $\bot$ or $\top$ resp., that is if the following wff is true of $f$.

$$\forall x. (\delta(x) \Rightarrow \delta(f(x))) = \top$$

$f$ is called $\bot$-strict if $f(\bot) = \bot$, and $\top$-strict if $f(\top) = \top$. $f$ is called total if it never returns $\bot$ or $\top$ for a defined argument, i.e., if

$$\delta(x) \Rightarrow \delta(f(x)) = \top$$

holds. Thus, if a function $f$ is strict and total then $\delta(x) = \delta(f(x))$.

Any function $f$ can be made into a strict one by first applying $\delta$ to the argument: For

$$f' := [\lambda x. \delta(x) \Rightarrow f(x), \bot]$$

we obviously have

$$f'(x) = \begin{cases} \top & \text{if } x = \top \\ \bot & \text{if } x = \bot \\ f(x) & \text{otherwise} \end{cases}$$

In the next section a functional $\text{str}$ will be defined that turns any function into a strict one.

In the following we define some standard operators on $I$ that will be used throughout the paper.

- $o := [\lambda x y z. x(y(z))]$ function composition
- $\text{pair} := [\lambda x y z. z \Rightarrow x, y]$ ordered pair
- $\pi_1 := [\lambda x. x(\top)]$ projection onto first component
- $\pi_2 := [\lambda x. x(\#)]$ projection onto second component
- $x := [\lambda x y z. \text{pair}(x(z \top), y(z \#))]$ cartesian product
The type-free Logic for Computable Functions

\[\ast : [\lambda \cdot (x, y, n_1(x) \vee n_2(x)) \Rightarrow \text{pair}(\mathbb{T}, a(r_2 x)), \text{pair}(\mathbb{F}, b(r_2 x)))]\] disjoint union

\[\text{Id} : [\lambda x. x]\]

\[u : [\lambda x y. \mathbb{T} \Rightarrow x, y]\]

\[\wedge : [\lambda x y. (\mathbb{A}(x) \vee \mathbb{A}(y)) \Rightarrow (x \Rightarrow y, \mathbb{F})]\]

\[\vee : [\lambda x y. (\mathbb{A}(x) \vee \mathbb{A}(y)) \Rightarrow (x \Rightarrow \mathbb{T}, y)]\]

\[\neg : [\lambda x. x \Rightarrow \mathbb{F}, \mathbb{T}]\]

For \text{pair}(x, y) we also use the notation \langle x, y \rangle.

The standard properties of these functions are easily derivable; for example,

\[
\forall x y. n_1(\langle x, y \rangle) = x
\]

\[
\forall x y. n_2(\langle x, y \rangle) = y
\]

Milner and Weyhrauch have shown that \(u\) has all the properties of the join operation in a lattice, also with respect to the partial order defined by \(\preceq\). In particular, \(\mathbb{U} \mathbb{U} \mathbb{T} \Rightarrow \mathbb{T}\) and \(x \mathbb{U} \mathbb{T} \Rightarrow \mathbb{T}\) for all \(x \preceq l\).

A strict conditional \(\Rightarrow\), i.e. \(\vdash x, y \Rightarrow \mathbb{T}\) for all \(x\) and \(y\), is definable in terms of the normal conditional \(\Rightarrow\):

\[
\Rightarrow : [\lambda x y. z \Rightarrow (x \Rightarrow x, \mathbb{T}), (x \Rightarrow \mathbb{T}, y)]
\]

Since the normal conditional will not be used in this paper except in the join operation, we will henceforth use the character \(\Rightarrow\) to denote the strict conditional.

The propositional connectives are strict in all arguments; they extend the standard functions (for two-valued logic) to four truth values in such a way that the standard relationships like \(x \vee y = \neg (\neg x \wedge \neg y)\) still hold.

### 2.2 Retracts, Domains, Types

The type-free logic essentially axiomatizes the "universal" domain \(I\). However, one would like to talk also about domains other than \(I\), like "lists" or "integers." It turns out that they can be "embedded" into the universal domain; there are subdomains of \(I\) that correspond to those particular domains in a sense to be made precise in the following section. As Scott [Sc2] has shown, \(I\) is so rich in subdomains that one can find a corresponding subdomain for all those domains or "data types" computer scientists are normally interested in.

The standard way of defining a subdomain is by using retracts. A retract is an idempotent function, i.e., an \(f \in I\) with \(f \circ f = f\). The idempotency property implies that all elements in the range of a retract \(f\) remain unchanged, i.e. the range of \(f\) is exactly its set of fixed points. subdomain \(D_f\) of \(I\)
The type-free Logic for Computable Functions

The range of \( f \). This domain \( D_f \) can be shown to be a complete lattice. In the remainder of this paper, the term "domain" always means "subdomain of \( I \) as defined by a retract." Very often the domain and the function (the retract) defining it will be confused by using the same notation for both; however, from the context it will be clear what exactly is meant. For emphasis, we will say retraction if we mean the function in particular.

The category of retracts

It may be helpful to look at retracts from a categorical point of view. The retracts of \( I \) form a category \( R \) in the following way:

- The objects of \( R \) are the retractions in \( I \).
- A function \( f \in I \) is a morphism from the retraction \( r \) to the retraction \( s \) iff \( f \circ r = s \).
- Composition of morphisms in \( R \) is just composition of functions in \( I \).

Obviously, \( R \) is a category. Note that two functions \( f \) and \( g \) in \( I \) will be identical morphisms in \( R \) if they agree on their source domain ("source retract"), i.e. if \( f \circ r = g \circ r \). An identity on a retract \( r \) is a function \( F \) with \( F \circ r = r \). We write \( \text{Id}_r \) for the identity on \( r \).

Let \( r, s \) be retracts. \( D_r \) is called subdomain of \( D_s \) iff \( s \circ r = r \), i.e. iff the fixed points of \( r \) are also fixed points of \( s \). \( D_s \) is called retract of \( D_r \) iff \( s \circ r = r \) and \( r \circ s = r \).

A particular retract is the truth value domain \( T \). Trivially, the universal domain \( I \) is also a retract. However, the property of being a retract cannot be proved; the corresponding retractions

\[
T = \{ \lambda x.x \Rightarrow 
\}
\]

and

\[
I = \{ \text{end} \ T \downarrow (I \rightarrow J) \}
\]

are rather part of the axiomatization of tFLCF. Obviously, "retract" and "retract of \( I \)" mean the same thing.

It should be noted that \( R \) is not the category of those subdomains of \( I \) that are defined by retractions; different retractions can define the same domain but will be different objects in \( R \). For example, the retractions \( T \) and \( \text{istrue} \) (see appendix) both define the domain \( \{ \text{t}, \# \} \) but are completely different functions. However, \( T \) and \( \text{istrue} \) are isomorphic in the category \( R \). Incidentally, if two domains are isomorphic one of them need not be a retract of the other: for instance, it is

\[
T \circ \text{istrue} = \text{istrue} \quad \text{and} \quad \text{istrue} \circ T = T
\]

i.e. \( T \) and \( \text{istrue} \) are subdomains of each other, but

\[
\text{istrue} \circ T \neq \text{istrue} \quad \text{and} \quad T \circ \text{istrue} \neq T
\]
Thus neither of \( T \) and \( \text{istrue} \) is a retract of the other. This discussion shows how retractions that define the same domain are related in the category \( \mathbb{R} \):

**Corollary 2.1:** For retractions \( r \) and \( s \), if \( D_r = D_s \) then \( r \) and \( s \) are isomorphic, that is, from a structural point of view, they cannot be distinguished.

The category \( \mathbb{R} \) has many useful closure properties we are going to exploit.

**Lemma 2.2:** \( \mathbb{R} \) is closed under the operations \( +, \times \) and \( \rightarrow \), i.e. if \( a \) and \( b \) are retracts, then so are \( a + b \), \( a \times b \), and \( a \rightarrow b \).

*Proof:* by T.P.

**Lemma 2.3:** \( \mathbb{R} \) is cartesian-closed.

*Proof:* We have to prove that \([r \rightarrow [s \rightarrow t]]\) and \([r \times s \rightarrow t]\) are isomorphic in \( \mathbb{R} \) for any retracts \( r, s \) and \( t \). Let \( F, G \) be defined by

\[
F = [\lambda f \, x. \, (f(n_1 \, x)(n_2 \, x))] \\
G = [\lambda g \, r \, s. \, g(r,s)]
\]

The T.P. proofs for

\[
G \circ F = \text{Id}_{[R \rightarrow (S \times P)]} \\
F \circ G = \text{Id}_{[R \rightarrow S \rightarrow P]}
\]

are almost straightforward.

Lemma 2.3 is the basis for what is commonly called “currying”. It allows to restrict attention to monadic functions.

Let the function \( \text{str} \) be defined by

\[
\text{str} := [\lambda f \, x. \, \delta(x) \times f(x), \perp]
\]

By T.P. we can show that \( \text{str} \) turns any function into one that is strict (with respect to the first argument) and that it is a retract. This shows that the set of strict functions is a proper subdomain of \( I \).

A domain is called flat if it contains, besides \( \perp \) and \( T \), only pairwise incomparable elements. For flat domains there is a computable equality relation \( "=\" \) with:

\[
\delta(x) = \perp, \quad \delta(y) = \perp, \quad x = y \\
x \times y = \perp \\
x \times y = \perp \\
\vdash x = y, \quad \delta(x) = \perp, \quad \delta(y) = \perp
\]
In many cases it is very convenient to use the (computable) equality instead of the equivalence $\equiv$ since it may appear inside a term and thus gives greater expressive power.

**Lemma 2.4:** If $F = [\lambda e. \text{t}((e))]$ and $G = [\lambda e. \text{t}(g)]$, where $t$ is any term, then $F = G$.

**Proof:** T.P.

Essentially, the lemma means that constant parameters can be bound "globally", i.e. they need not be passed on with every call. The lemma will be used quite often in the remainder of the paper without being referred to explicitly.
Abstract Data Types in the Type Free Logic

In this section we introduce data types and discuss the representation of data structures in tfLCF. We investigate properties of data types by looking at them from a more algebraic point of view, which allows us to derive various function definition schemes. The basic function definition method is illustrated in an example dealing with the translation of arithmetical expressions from infix to postfix form.

What is intuitively meant by the notion abstract data type? There is a common understanding that, in programming, a data type is not just a set, but also comprises information about the structure of the elements and how to construct them and to operate on them. This can be done in an abstract way, i.e. the only information available is the set of primitive operations (constructors, selectors, recognizers) and relationships between them; it does not matter what the elements of the type look like and how the primitive operations are implemented. In the context of a formal calculus the relationships between the primitive operations are expressed by axioms.

The presentation concentrates on generic recursive types; however, in subsection 3.4 extensions to non-free types are discussed.

3.1 Data Type Definitions

We start with discussing free data types. The type system will be extended later to comprise a wider class of types. A type definition is made by listing alternative subtypes. A subtype is either a constant or a composed type. Composed data types are defined best by their abstract syntax [Mc], using constructors, selectors and recognizers to describe the structure of the type. In a more formal BNF-like notation (using "constr" for constructor, "sel" for selector, and "dt" for data type):

```
<type_def>  ← <type_name> := <subtype> | <subtype> | <comptype>
<subtype>  ← <constant> | <comptype>
<comptype> ← <constr> ( <sel1>:<dt1>,...,<seln>:<dt > )
<constant> ← <identifier>
```

with the restriction that the names of all constructors in a type definition and all selectors in one composed type have to be distinct. A data type definition may be recursive, that is, any of the dt in a subtype may be the name of the type to be defined. Also mutually recursive data type definitions are permitted.

For example, the data type "sequence (linear list) of atoms" can be defined using this formalism by

```
Seq := emptysq | mksq(hd:atom, tl:Seq).
```

Strictly speaking, this data type definition is a type scheme, that is,
Abstract Data Types in the Type Free Logic

\[ \text{seq} := \text{emptyseq} | \text{mkseq} (\text{hd} : \text{dtype}, \text{tl} : \text{seq}) \]

defines a type "sequence of elements of type dtype" for any data type dtype. This will be made more
precise in the following subsection. Beside seq we will use other standard data types (type schemes)
like binary trees, natural numbers, and pairs, defined by

\[ \begin{align*}
\text{bin|tree} & := \text{mkbt} (\text{subtype}) | \text{comp} (\text{bin|tree}, \text{sec|bin|tree}) \\
\text{n|num} & := \text{zero} | \text{succ} (\text{n|num}) \\
\text{dpair} & := \text{mkpair} (\text{dtype}_1, \text{sec|dtype}_2)
\end{align*} \]

3.2 Representing Data Structures in tfLCF

In section 2 it was explained that retracts can be regarded as the "types" in the type-free logic. The
data types are now to be represented in LCF in such a way that the resulting terms are retractions.

What exactly is implied by a data type definition? Intuitively, a data type should have the following
properties:

a) A data type is the disjoint union of subtypes. A subtype is either a constant or a composed
subtype. For each subtype there is a predicate (characteristic function) which will be named
"is_const" or "is_<constr>" resp. These recognizers permit to decide membership in one of the
subtypes relative to the whole data type.

b) Each constructor is a one-to-one function; in particular, the corresponding selector functions allow
to "retrieve" the respective arguments of a constructor.

c) A subtype has to be embedded explicitly into the type by a constructor function. For example,
"atoms" are not lists unless they are "converted" into lists. This helps us to keep all data types
disjoint.

These statements can be expressed more precisely in terms of LCF axioms.

Definition 3.1 (Axioms for generic data types):
The data type definition

\[ \text{type} := \text{constant}_1 | \ldots | \text{constant}_n \mid \text{comptype}_1 | \ldots | \text{comptype}_n \]

with

\[ \text{comptype}_k := \text{comp}_n (\text{sel}_{k1}; \text{dl}_{k1}, \ldots, \text{sel}_{kn}; \text{dl}_{nk}) \quad \text{for } k=1, \ldots, n \]

is considered to correspond to the fixed point equation

\( (1) \quad \text{type} = [\lceil F. \lambda x. \text{is constant}_1(x) \Rightarrow x, \ldots, \text{is constant}_n(x) \Rightarrow x, \\
\text{is comp}_1(x) \Rightarrow \text{comp}_1 (\text{dt}_1 (\text{sel}_1 (x)), \ldots, \text{dt}_n (\text{sel}_n (x))), \ldots, \\
\text{is comp}_n(x) \Rightarrow \text{comp}_n (\text{dt}_n (\text{sel}_n (x)), \ldots, \text{dt}_n (\text{sel}_n (x)))) \\
\downarrow ] \]

where dt\textbf{k} is the type and dt\textbf{k} is the type otherwise, and for i,j=1,\ldots,m; k,l=1,\ldots,n
Abstract Data Types in the Type Free Logic

(2) \( \delta(\text{constant}) = \top \)
\( \text{is\_constant}(\text{constant}) = \top \)

(3) \( \delta(\text{comp}_k(\text{dt}_k(x_1), \ldots, \text{dt}_k(x_{p_k}))) = \delta(\text{dt}_k(x_1)) \wedge \ldots \wedge \delta(\text{dt}_k(x_{p_k})) \)
\( \delta \circ \text{comp}_k = \text{is\_comp}_k \circ \text{comp}_k \)

(4) \( \forall x. \text{is\_comp}_k(x) \Rightarrow \text{is\_comp}_i(x) = \text{if} \)
\( \forall x. \text{is\_const}(x) \Rightarrow \text{is\_const}(x) = \text{if} \)
\( \forall x. \text{is\_const}(x) \Rightarrow \text{is\_comp}_k(x) = \text{if} \)

(5) \( \delta \circ \text{is\_comp}_k = \delta \circ \text{is\_comp}_i \)
\( \delta \circ \text{is\_const}_i = \delta \circ \text{is\_const}_i \)
\( \delta \circ \text{is\_const}_j = \delta \circ \text{is\_comp}_k \)

(6) \( \delta(\text{comp}((x_1, \ldots, x_{r-1}, x_n))) = \text{sel}_r(\text{comp}((x_1, \ldots, x_{n-1}, x_n))) = x_r \)
for \( r = 1, \ldots, n \)

Axiom (1) is a mere transcription of the type definition. It contains the basic information about the type structure; therefore, it will be called the characterizing function of the type. The goal is to prove that it is a retract. However, this cannot be done without further specifying the primitives occurring in (1) by adding axioms expressing the statements a)-c). They make sure that the recognizers for the subtypes are complementary (axiom 4) and that they are defined exactly for the elements of the type (axiom 5). Axioms no. 6 state the generic nature of the type (This is equivalent to saying that constructor and selector functions are essentially tupling and projections). All constructors are assumed to be strict in each argument and total for arguments of correct types (axioms 3).

Example: The data type definition for (homogeneous) sequences

\[ \text{Seq} \equiv \text{emptyseq} \mid \text{mkseq} (\text{hd} : \text{Atom}, \text{tl} : \text{Seq}) \]

will generate the axioms

(S1) \[ \text{seq} = [\forall S. \left( \forall x. \text{is\_emptyseq}(x) \Rightarrow \text{emptyseq}, \text{is\_mkseq}(x) \Rightarrow \text{mkseq}(\text{atom}(x)), S(\text{tl}(x))) \right] \]

where \( \text{atom} \) is the characterizing function for the data type \( \text{Atom} \),

(S2) \( \delta(\text{emptyseq}) = \text{if} \)
(S3) \( \text{is\_emptyseq}(\text{emptyseq}) = \text{if} \)
(S4) \( \forall x. y. \delta(\text{mkseq}(\text{atom}(x), \text{seq}(y)))) = \delta(\text{atom}(x)) \wedge \delta(\text{seq}(y)) \)
(S5) \( \delta \circ \text{mkseq} = \text{is\_mkseq} \circ \text{mkseq} \)
(S6) \( \text{is\_emptyseq} = \neg \circ \text{is\_mkseq} \)
(S7) \( \forall x. y. \delta(\text{mkseq}(x,y)) \Rightarrow \text{hd}(\text{mkseq}(x,y)) = x \)
(S8) \( \forall x. y. \delta(\text{mkseq}(x,y)) \Rightarrow \text{tl}(\text{mkseq}(x,y)) = y \)

Any type \( t_i \) that occurs in the definition of another type \( t_j \) is considered a base type for \( t_j \). The notion
"base type" does not imply "basic" or "simpler"; on the contrary, since mutual dependence of data types is permitted, t, itself may be a base type for t; (hence the relation "is-base-type-of" is only a quasi-order). If data types are mutually dependent the corresponding characterizing functions form a system of mutually recursive functions. Those base types that do not depend on the type to be defined are called generating types (in fact, they generate the type in an algebraic sense; see the following sub-section).

At this point it has to be clarified what it means for a characteristic function to be a retraction. The logical type of type is (type→type). In order to make it a function in I the primitives (constants, constructors and selectors etc.) have to be specified as elements of I. This amounts to defining a model of (the axioms describing) the data type in I. However, the retraction property can be proved just from the axioms; more precisely, what can be proved is that type is an "abstract retraction", meaning that every model is a retraction. All the models will be isomorphic retractions (in the categorical sense). Thus the abstract retraction represents an equivalence class of objects in R.

It should be noted that the standard representation of data types in a LCF-like language is by "domain equations" (involving * and ×; see [Sc2]). For example, the data type Seq of sequences of atoms is completely specified by the least fixed point of the equation

(i) \( \text{Seq} = \text{emptyseq} : (\text{Atom} :\to \text{Seq}) \)

(where * and × are strict versions of * and ×) given a representation of the type Atom and the constant emptyseq. However, we do not follow this line. The syntax of data type definitions, as given in the preceding section, involves constructors and selectors; they are the primitives for defining functions operating on the data type. But they do not appear in (i), in fact, (i) is an implementation of the data type Seq (by functions in I) rather than an abstract definition; the primitives are hidden in the construction of sum and product. In order to keep the previous higher level of abstraction the primitives have to be axiomatized, as has been done for special types in [Ne1]. Although an axiomatization as in definition 3.1 is by far less elegant than a definition like (i) it is more appropriate for the purpose of program specification.

Incidentally, this discussion shows that every (generic) data type has the following standard model:
The data type definition

\[
\text{type} := \text{constant}_1 | \ldots | \text{constant}_n | \text{comptype}_1 | \ldots | \text{comptype}_n
\]

with

\[
\text{comptype}_k := \text{comp}_k(\text{sel}_k : \text{dt}_k | \ldots | \text{sel}_k : \text{dt}_k) \quad \text{for } k = 1, \ldots, n
\]

is simply translated into

\[
\text{type} := \uparrow^1 : \text{type} \uparrow^1 \uparrow^1 \uparrow^1 \uparrow^{\text{comp}_1} : \ldots : \uparrow^{\text{comp}_n}
\]

with

\[
\text{comp}_k := (\text{dt}_k : \uparrow^1 \uparrow^{\text{comp}_k} \uparrow^1 \text{dt}_k) \quad \text{for } k = 1, \ldots, n
\]

It is easy to figure out what the primitives look like, and the proof that the axioms of definition 3.1 hold is straightforward.
Lemma 3.2: type is strict.

Proof: Simple consequence of the fact that all functions involved are strict (by definition).

Theorem 3.3: type is a retract if all base types of type are retracts.

Proof: See appendix A.3.

From the characterizing function of a type we are going to derive a variety of function definition schemes and functions. In particular, a type predicate (characteristic function) \texttt{is\_type} can be derived which yields \texttt{tt} exactly for the defined elements of the type, i.e. which satisfies:

\[ \forall x. \text{is\_type}(x) \Rightarrow \text{type}(x) = x \]
\[ \forall x. \text{is\_type}(x) \Rightarrow \delta(x) = \texttt{tt} \]

and
\[ \text{type}(x) = x, \ \delta(x) = \texttt{tt} \vdash \text{is\_type}(x) = \texttt{tt} \]

This predicate will be discussed in greater detail in the following subsection.

For a recursive data type we can derive the standard structural induction rule from the characterizing function (the retraction).

Theorem 3.4 (Structural Induction):

For a recursive data type type defined by

\[
\text{type} := \text{constant}_1 \mid \ldots \mid \text{constant}_m \mid \text{comptype}_1 \mid \ldots \mid \text{comptype}_n
\]

with

\[
\text{comptype}_n := \text{comptype}(\text{sel}_{k_1}:d_{k_1}, \ldots, \text{sel}_{k_p}:d_{k_p}) \quad \text{for } k=1,...,n
\]

there is an induction rule that allows to conclude

\[ Q \vdash \forall x. \text{is\_type}(x) \Rightarrow P(x) \]

(where the conclusion is meant to be a wff involving \(x\) each of whose aww's is prefixed by \( \forall x. \text{is\_type}(x) \ldots \)) from the following antecedents:

(a) For each constant \text{constant}_i, (i=1,..,m)

\[ Q \vdash P(\text{constant}_i) \]
Abstract Datatypes in the Type Free Logic

(b) For each composed subtype \( \text{comp}_{k_i} \) \((k=1,...,n)\)

\[
P(y_{k_1},...,P(\text{comp}_{k}(...)) = \text{tt} \quad |\quad P(\text{comp}_{k}(...))
\]

with an antecedent \( P(y_{k_1}) \) for each recursion arguments, i.e. for those arguments of \( \text{comp}_{k} \) with \( d_{k_j} = \text{type} \).

Proof: see appendix A.3.

For example, the induction rule corresponding to the characterizing function \( \text{seq} \) is

\[
\begin{align*}
P(\text{emptyseq}) & \quad P(y), \delta(\text{mkseq}(x,y)) = \text{tt} \quad |\quad P(\text{mkseq}(x,y)) \\
Vx. \text{is_seq}(x) & \Rightarrow P(x)
\end{align*}
\]

Note that the constructor arguments in the induction step need not be restricted by type predicates (the restriction is implied by the definedness predicate). A discussion of other forms of the induction rule that involve the retraction can be found in appendix A.3.

As mentioned above, the type definition for \( \text{seq} \) is a type scheme, defining a data type for any type \( \text{dtyp} \). This means that in the corresponding retraction \( \text{seq} \) the retract atom can be replaced by any other retract. We therefore can define the functional

\[
\text{seqof} := \lambda \text{type}. [\lambda \text{x}. \text{is_emptyseq}(x) \Rightarrow \text{emptyseq}, \\
\text{is_mkseq}(x) \Rightarrow \text{mkseq}(\text{type}(hd(x)), S(\text{tl}(x)))]
\]

By theorem 3.3 \( \text{seqof}(\text{type}) \) is a retract for any retract \( \text{type} \). In other word, \( \text{seqof} \) maps retracts on retracts. Obviously, any generic type construction yields such a mapping on retracts. Properties of these functionals will be studied in the following subsection.

3.3 Algebraic Interpretation of Data Types

Interpreting data types in terms of universal algebra helps to clarify certain concepts and properties. As a data type may involve several subtypes and functions of heterogeneous type the appropriate notion is that of "heterogeneous algebra" (Birkhoff and Lipsom [BI]; see also Higgins [HI]).

Definition 3.3 (Heterogeneous algebra)

A heterogeneous algebra \( A \) consists of
- a family \( \{A_i\}_{i \in J} \) of (non-empty) sets; the \( A_i \) are called phyla.
- a family \( \{f_k\}_{i \in k} \) of operations; for each \( f_k \) there is an associated tuple \( \text{index}_k = (i_{k_1},...,i_{k_{nk_k}},1) \) of elements of \( J \).
The index of the operation $f_k$ indicates the phyla from which the arguments of $f_k$ are taken (i.e., the argument types) and the target phylum. $nk$ is the arity of $f_k$ (possibly 0). In the present framework, the index is simply the type of the operation.

The triple $(J, K, (\text{index}_k)_{k \in K})$ is called the signature of the algebra; it characterizes the basic structure. Algebras are called similar if they have the same signature. As the structure of similar algebras is comparable, it is possible to define structure-preserving mappings between them.

**Definition 3.6 (Homomorphism)**

Let $A = ((A_i)^k_{i \in J}, (f_k)^k_{k \in K})$ and $B = ((B_i)^k_{i \in J}, (g_k)^k_{k \in K})$ be similar algebras. A homomorphism $h$ from $A$ to $B$ is a family of mappings $(h^i)_{i \in J}$ such that $h_j$ maps $A_i$ into $B_i$, and for each $k \in K$

$$h^i_k, (f_k(a_1, \ldots, a_{nk})) = g_k(h^1_{j_1}(a_1), \ldots, h^i_{j_k}(a_k))$$

where $\text{index}_k = (j_1, \ldots, j_{nk}, k_{i \in J})$.

As mentioned in the previous section, a data type (or, its domain) forms a complete lattice. So, the appropriate algebraic structure is that of a heterogeneous lattice-algebra. Although the lattice structure of the domains considered here is not very interesting - apart from the elements $\bot$ and $\top$, the domains are flat - we have to take it into account by requiring that all functions preserve the lattice structure. However, because of the simple structure it is sufficient to require that all functions involved in the algebraic structure, i.e., the operations, are strict and total. Similarly, all the mappings $h_j$ constituting a homomorphism have to be strict (it is, however, not necessary to assume totality). Henceforth, these assumptions will be made throughout the remainder of the paper.

**Example.** The data type $\text{Seq}$, regarded as a heterogeneous algebra, consists of the two phyla $\text{atom}$ and $\text{seq}$ and operations

- $\text{emptyseq} : 0 \rightarrow \text{seq}$ (nullary)
- $\text{mkseq} : \text{atom} \times \text{seq} \rightarrow \text{seq}$

The axioms in the previous section indicate that a data type corresponds to an absolutely free (or "generic") algebra which is generated by the constants, the base types and the constructor functions as operations. As it is well-known in algebra, an absolutely free algebra has characterizing universal properties:

1. There is (upto isomorphisms) only one absolutely free algebra for given generating base types and operations.
2. Any homomorphism from an absolutely free algebra $F$ into another algebra $A$ of the same type (in the algebraic sense) is determined uniquely by functions mapping the generating sets into $A$.

Properties (1) and (2) can be proved in LCF for each (free) data type without relying on an algebraic interpretation. It is these properties we are going to exploit.
Abstract Data Types in the Type Free Logic

In order to define a homomorphism it is sufficient to map the base types into target sets and the constructors onto operations on the target structure. Then, by property (2) there is a unique function that homomorphically extends the base function(s). Due to the fact that in LCF homomorphisms can be "pushed through" conditionals, homomorphic extension is representable by a simple modification of the function characterizing the data type: we have only to replace the base type retracts by the base functions and the constructors by the operations on the target algebra.

To continue our example based on the data type seq, we notice that a homomorphism from seq into an appropriate algebra is determined completely by

1. a constant that is the image of emptyseq,
2. a function that maps the base type atom into the corresponding set, and
3. a binary operation on the target algebra.

In LCF, this is written as the functional

\[ Sfun : \lambda f \text{ const op.} \prec S. [\lambda x. \text{ is_emptyseq}(x) \Rightarrow \text{ const}, \text{ is_mkseq}(x) \Rightarrow \text{ op}(f(hd(x)), S(tl(x))), \downarrow] \]

Assume \( R \) is the target structure with phyla \( R_1 \) and \( R_2 \), \( c \) an element of \( R_2 \), \( \text{op} : R_1 \times R_2 \rightarrow R_2 \) a binary operation and \( \text{fun} \) a function from \( \text{atom} \) to \( R_1 \). Then property (2) above yields the following theorem:

**Theorem 3.7:** \( F = Sfun(\text{fun}, c, \text{op}) \) is the unique homomorphic extension of \( \text{fun} \) with respect to \( c \) and \( \text{op} \), i.e., it is the only homomorphism from \( \text{seq} \) to \( R \) with \( F(\text{emptyseq}) = c \) and \( F \circ \text{mkseq} = [\lambda x y. \text{op}(\text{fun}(x), F(y))] \).

The proof is straightforward; it crucially depends on the "freeness" of the type definition (i.e. axioms (S7), (S8)) which is necessary to establish the homomorphism property of \( F \).

A simple example is the type predicate (characteristic function) for seq: The function \( \text{is_seq : seq} \rightarrow T \) with

\[ \text{is_seq}(x) \equiv \text{tt} \text{ iff seq}(x) \equiv x \text{ and } \text{is_atom}(x) \equiv \text{tt} \]

is definable simply by extending the type predicate \( \text{is_atom} \) of the generating base type to a homomorphism into \( T \):

\[ \text{is_seq} = Sfun(\text{is_atom}, \text{tt}, \Lambda) \]

A further property of the homomorphic extension functional \( Sfun \) is that it carries over a structural induction rule from the source domain. E.g. for sequences:

\[ P(x), P(y), \text{ is_seq}(x) \equiv \text{tt} \vdash P(y) \]

\[ \text{V z. is_seq}(z) \Rightarrow P(F(z)) \]
thus permitting induction on (target) domains originally not structured appropriately.

The mathematical content of the discussion on interpreting data types as absolutely free algebras and the homomorphic extension functionals amounts to a well-established fact known from category theory: the correspondence between free constructions (free objects) and representable functors. The pair \((\text{dom}, \text{fun})\) defines a functor from \(\mathcal{R}\) into a subcategory of \(\mathcal{R}\) of "suitably structured" retracts. The point is that this correspondence can be established within the framework of LCF. Due to the fact that everything is represented as LCF terms, objects and morphisms as well as functors, it allows to carry out mechanically assisted proofs rather easily. For the time being, theorems like the one mentioned above have to be proved in LCF for each data type separately, although the structure of the proof is always the same. However, there is some hope that formal proofs of general statements about, e.g., all generic data types will be feasible using a metatheory of LCF being developed on the basis of representing the LCF notions as data types (see section 6 for part of the data type definition).

The usefulness of homomorphisms as a structuring principle has been observed elsewhere, in particular in the context of program translation [Mo, MiW]. However, though homomorphic extension is a rather powerful scheme for function definition it is by far not powerful enough. It turns out that properties similar to those proved for homomorphic extension can be shown for a more general class of definition schemes; this will be discussed in section 5.

### 3.4 Non-generic Data Types

Although the class of generic data types covers many of the structures needed in programming it is not comprehensive enough. Relaxing the restriction to generic structures is tantamount to, in algebraic terms, allowing to add further relations to a type definition. In a way, the generic data types can be regarded as the "context-free types," and adding relations as "introducing context." In the context of this paper it is sensible to consider only relations that are expressible as recursive predicates.

The general method will be discussed by means of an example. Let \(\text{norep}(x)\) be a predicate on sequences which is true iff \(x\) does not contain repetitions of elements (the explicit definition is straightforward). Then the data type \(\text{norepseq}\) of "sequences without repetitions" is just the restriction of \(\text{seq}\) by \(\text{norep}\). The new type can be represented in the following way: Whenever an element is added to a sequence it is checked first if it already occurs in it, in which case nothing is done. That is, if the constructor \(\text{mksseq}\) is modified to

\[
\text{mknorepseq} : = \{x \ y. \ \text{norep}(\text{mksseq}(x, y)) \Rightarrow \text{mksseq}(x, y), y\}
\]

then all sequences constructed by \(\text{mknorepseq}\) have the "no-repetition" property, i.e., they satisfy the predicate \(\text{norep}\). This is just another application of the homomorphic extension functional. The range of the function
Abstract Data Types in the Type Free Logic

norepseq := ʃ fun(dtype, emptyseq, mknorepseq)

is exactly the desired subset of sequences without repetitions (it is obvious that only elements of seq are constructed). In other words, norepseq represents ordered sets of elements of type dtype.

Obviously, norepseq is a retract of seq. Since norepseq defines a subdomain of seq it is also a retract of 1, which means that norepseq makes sense (in the present context) as a data type. This construction for new retracts works at least in the case where a new type is defined by a restrictive predicate. The full extent of the method, however, needs to be explored further. It is conjectured that any data type (given a reasonable definition in terms of computability) is representable as a retract of a generic type; this would parallel the fact that, in formal language theory, any recursively enumerable set is the image of context free sets under suitable mappings.

3.5 An Example: Infix to Postfix Translation

As an example we show how to generate a function that translates arithmetical expressions from infix to postfix notation (the example was suggested by J. Allen). The abstract syntax of the structures is defined by

\[
\begin{align*}
\text{exp} & := \text{mkexp} \left( \text{term} \right) | \text{mkseq} \left( \text{exp}, \text{exp} \right) \\
\text{term} & := \text{mkterm} \left( \text{fact} \right) | \text{mkplerm} \left( \text{pr}_1, \text{term}, \text{pr}_2, \text{fact} \right) \\
\text{fact} & := \text{mkvfact} \left( \text{tv}: \text{var} \right) | \text{mkfact} \left( \text{tv}: \text{exp} \right)
\end{align*}
\]

and

\[
\begin{align*}
\text{post} & := \text{mkvpost} \left( \text{pv}: \text{var} \right) | \text{msum} \left( \text{p}_1, \text{post}, \text{p}_2, \text{post} \right) | \text{mkprod} \left( \text{p}_1, \text{post}, \text{p}_2, \text{post} \right)
\end{align*}
\]

which may be thought of as abstraction from the "concrete" infix grammar

\[
\begin{align*}
\langle \text{exp} \rangle & := \langle \text{exp} \rangle \cdot ^+ \langle \text{term} \rangle | \langle \text{term} \rangle \\
\langle \text{term} \rangle & := \langle \text{term} \rangle \cdot ^+ \langle \text{fact} \rangle | \langle \text{fact} \rangle \\
\langle \text{fact} \rangle & := \langle \text{var} \rangle | ^\prime \langle \langle \text{exp} \rangle ^\prime \rangle
\end{align*}
\]

and the postfix grammar

\[
\begin{align*}
\langle \text{post} \rangle & := \langle \text{var} \rangle | \langle \text{post} \rangle \cdot ^+ \langle \text{post} \rangle ^\prime | \langle \text{post} \rangle ^\prime \cdot ^+
\end{align*}
\]

Now, the problem is to find a function that translates variables into variables and infix-sums and infix-products into postfix-sums and postfix-products resp. This is a simple example of a homomorphism between heterogeneous algebras. The algebra Exp includes the 4 phyla \text{exp}, \text{term}, \text{fact} and \text{var}, the algebra Post the phyla \text{post} and \text{var}. The homomorphism maps \text{exp}, \text{term} and \text{fact} into the phylum \text{post} and \text{var} onto \text{var}, that is, the homomorphism consists of 4 mappings

\[
\begin{align*}
\text{id:} & \quad \text{var} \to \text{var} \\
T\text{exp:} & \quad \text{exp} \to \text{post} \\
T\text{term:} & \quad \text{term} \to \text{post} \\
T\text{fact:} & \quad \text{fact} \to \text{post}
\end{align*}
\]
These mappings have to respect the corresponding algebraic operations

\[
\begin{align*}
\text{mksexp}: \quad & \exp \times \text{term} \rightarrow \exp \quad \leftrightarrow \quad \text{mksum}: \quad \text{post} \times \text{post} \rightarrow \text{post} \\
\text{mkpterm}: \quad & \text{term} \times \text{fact} \rightarrow \text{term} \quad \leftrightarrow \quad \text{mkprod}: \quad \text{post} \times \text{post} \rightarrow \text{post} \\
\text{mkvifact}: \quad & \text{var} \rightarrow \text{fact} \quad \leftrightarrow \quad \text{mkvpost}: \quad \text{var} \rightarrow \text{post}
\end{align*}
\]

i.e., they must satisfy equivalences

\[
\text{Texp}(\text{mksexp}(x,y)) = \text{mksum}(\text{Texp}(x), \text{Tterm}(y))
\]

etc. Since the distinction between \(\exp\), \(\text{term}\) and \(\text{fact}\) disappears in \(\text{Post}\), the "operations" corresponding to \(\text{mksexp}\), \(\text{mkpterm}\) and \(\text{mkvifact}\) are just identities on \(\text{post}\). Having established all the algebraic correspondences, homomorphic extension immediately yields the desired functions (slightly simplified):

\[
\begin{align*}
\text{Texp} &= \{x. \text{is SEXP}(x) \Rightarrow \text{Tterm}(\text{te}(x)), \\
& \quad \text{is exp}(x) \Rightarrow \text{mksum}(\text{E}(\text{su}_1(x)), \text{Tterm}(\text{su}_2(x))), \\
& \quad \perp \} \\
\text{Tterm} &= \{x. \text{is TTERM}(x) \Rightarrow \text{Tfact}(\text{tf}(x)), \\
& \quad \text{is pterm}(x) \Rightarrow \text{mkprod}(\text{F}(\text{pr}_1(x)), \text{Tfact}(\text{pr}_2(x))), \\
& \quad \perp \} \\
\text{Tfact} &= \{x. \text{is VFACT}(x) \Rightarrow \text{mkvpost}(\text{var}(\text{fv}(x))), \\
& \quad \text{is efact}(x) \Rightarrow \text{Texp}(\text{e}(x)), \\
& \quad \perp \}
\end{align*}
\]
4. Elements of a Problem Specification Language

This section is devoted to discussing a rudimentary "problem specification language." The language consists of the terms of typed LCF, augmented by certain constructions that are considered natural or helpful for concise specification of problems or, more precisely, functions over data types. The main extension is a first-order like calculus that enables to talk about sets and quantification in a way consistent with the computational logic. It is an extension of the LCF terms in their typed form. Using the definition techniques developed in the preceding section, the added constructions are interpreted as LCF terms which gives them the intended meaning as computation rules or "programs."

4.1 Sets, Set Operations and Quantification

Syntax
Types. The language is typed, i.e. a type is associated with each term. There is a predefined type: T, the domain of truth values. New types can be defined explicitly as data types (see below). For each type t we have a type setof(t) denoting the powerset type "sets of elements of type t". More formally:

Definition 4.1 (Types):
1. T is a type.
2. Data types are types.
3. If t1 and t2 are types, then (t1→t2) is a type (the type of functions from t1 to t2).
4. If t is a type then setof(t) is a type.
5. These are all the types.

Types built by (4) are called set types. No data type is a set type. Although types are not sets, we use the type name also to denote the set of individuals of that type. There are no equalities between types; different type expressions, in particular different type names, denote different types.

Note the distinction between "types" and "data types". Types are the sorts in the logic, whereas the notion data type is used more in the sense of data types in programming languages which involves certain assumptions about the (internal) structure of the typed objects. By (2) in definition 4.1 data types are assumed to coincide with certain logical types.

Terms. We use the notation s:t to denote a term s of type t. If t is a set type then s:t is called set term. All LCF terms (1 - 6) are terms of our language (cf. [Mil] and appendix A.1.1). Beside the LCF terms the language includes terms for expressions involving sets and bounded quantification (7 - 9).

Definition 4.2 (Terms):
1. The constants ↓, ↑, #, T are terms of type T.
Elements of a Problem Specification Language

(2) Any identifier is a term.
(3) If \( s_1, t_1 \) are terms then \( s(s_1)t_1 \) is a term.
(4) If \( s_2 \) is a term then \( \lambda x.s(x)s_2 \) is a term.
(5) If \( p, q, r, t \) are terms then \( p \equiv q, r \equiv t \) a term.
(6) If \( x_1, t_1 \) are terms then \( \tau x_1.t_1 \) is a term.
(7) If \( x_1 \) is an identifier and \( S \) is a set term then \( x \in S \) is a term.
(8) If \( x_1 \) is an identifier, \( S \) is a set term and \( p \) is a predicate term then \( \forall x \in S. P(x) : t \) and \( \exists x \in S. P(x) : t \) are truth value terms.

As usual parentheses and brackets can be omitted as long as parsing is unambiguous. The notions \( \text{term} \) and \( \text{wff} \) are used as in typed LCF (see appendix A.1.1).

Note that the use of the sign \( \forall \) for quantification in (8) cannot be confused with the use of \( \forall \) in abbreviations for \( \lambda x.t \alpha x. s \). The former \textit{always} requires a restricting set whereas the wff-\( \forall \) is never restricted.

Semantics

The aim is to interpret the extended typed language in the \( \lambda \)-free calculus. This is done by showing that every type corresponds to a retract in tLCF. Since the representation of data types as retracts has already been discussed, it remains to show how sets are to be represented. Based on the set representation we then have to find interpretations for the set operations and quantifications.

The most common way of introducing sets into an environment of structures is by representing them as sequences (linear lists) of non-repeating elements. As we are not interested in axiomatizing set theory but rather look for convenient definition of function meanings we rely on such a representation in LCF (cf. [Nei]). It will turn out later that sets are needed mainly as a conceptual intermediate step which can be eliminated in actual “programs”. Besides, representing sets by sequences fits nicely into the algebraic framework. Actually, what is to be represented is a rather restricted kind of sets: we are only dealing with homogeneous and computable (mainly even finite) sets. However, the required homogeneity is not really restrictive as one can always define the “sum type.”

The first step is to define a membership predicate \( x \in S \) for sequences, yielding \( \text{tt} \) if \( x \) occurs in \( S \) and \( \text{ff} \) otherwise (if it is defined). It is definable as a homomorphism from \( \text{Seq} \) into \( \text{T} \) by homomorphically extending equality on atoms:

\[
\epsilon := [\lambda x. \text{Seq}([\lambda y. x \neq y], \text{tf}, \text{tv})]
\]

Note that \( \epsilon \) is defined for appropriate types only, if \( x \) does not have the same type as the elements of \( S \), \( \epsilon \) is undefined, thus also \( x \in S \).
Using the predicate \( \epsilon \) a function \( U_1 \) on \( \text{atom} \times \text{seq} \) is definable by

\[
U_1 := [\lambda x. S. x(S = S, \text{mkseq}(x, S))]
\]

\( U_1 \) guarantees that elements already occurring in a sequence will not be added; sequences built up using \( U_1 \) are those directly representing sets. If \( \text{Seq} \) is the data type of sequences of elements of type \( t \), the type \( \text{setof}(t) \) is the image of \( \text{Seq} \) under the homomorphism

\[
\text{set} := \text{Sfun}(\text{id}, \text{emptyseq}, U_1).
\]

Moreover, \( \text{set} \) is a \\textit{retract} on \( \text{seq} \); it defines the same subdomain of \( \text{seq} \) as the function no \( \text{seq} \) discussed in subsection 3.4. \( \text{setof}(t) \) corresponds to the subset of sequences without repetitions of elements. (However, it is not a \textit{subalgebra} of \( \text{seq} \).) From this it follows that functions defined on \( \text{Seq} \) are equally defined on \( \text{setof}(t) \). Furthermore, the (generic) structure of \( \text{Seq} \) can be used for defining functions on \( \text{setof}(t) \). More specifically, we have the embedding \( \text{iset}: \text{setof}(t) \to \text{seq} \) with

\[
\text{set} \circ \text{iset} = \text{id}_{\text{set}}.
\]

Thus, any function \( f: \text{seq} \to D \) can be restricted to \( \text{set} \) by composing with \( \text{iset} \). In this way, the predicate \( \epsilon \) defined above becomes the set-theoretic element relation. Similarly, we obtain an interpretation of quantified terms by applying homomorphic extension to any predicate \( P \). Let operators \( \text{all} \) and \( \text{exist} \) be defined by

\[
\text{all} := [\lambda P. \text{Sfun}(P, \text{id}, \wedge)]
\]

\[
\text{exist} := [\lambda P. \text{Sfun}(P, \text{id}, \vee)]
\]

Then

\[
\forall x(S. P(x)) := \text{all}(P, S)
\]

and

\[
\exists x(S. P(x)) := \text{exist}(P, S).
\]

Note that this form of quantification is well-defined if \( S \) and \( P \) are defined; since \( \bot \) or \( \top \) is never an element of a set, it will not appear in quantifications (and cause a non-defined truth value). Furthermore, a quantified term denotes a computable function if the predicate \( P \) and the term denoting the restricting set \( S \) are computable, which is guaranteed by the way terms can be built up.

Using these constructs set inclusion is easily expressed by

\[
S_i \subseteq S_j := \forall x(S_i, x(S_j)
\]

and similarly set equality by the "extensionality" property

\[
S_i = S_j := (\forall x(S_i, x(S_j)) \land (\forall x(S_j, x(S_i))
\]

Note again that these relations will be undefined for sets over different types. The empty set is the image under \( \text{set} \) of the empty sequence; we will identify the former with the latter.
The function \( u_1 \), taken as a function from \( \text{setof}(t) \) to \( \text{setof}(t) \), inserts a single element into a set; extending this function homomorphically in the first argument yields ordinary set union \( u \). As a short hand notation we will use \( u_n \) for \( n \)-ary union (\( n \)-fold composition of \( u \)).

Similarly, set intersection and set difference are definable by means of the function \( \text{remove} : \text{setof}(t \times t) \to \text{setof}(t) \) that removes an element from a set. \( \text{remove} \) is defined by

\[
\text{remove} := \lambda x s. x \in s \Rightarrow \text{rem}(x,s), s
\]

where \( \text{rem} \) is the endomorphic extension of

\[
\text{rem}_1 := \lambda x y. x \in y \Rightarrow [\lambda], [y].
\]

If \( \{ x | x \in S \} \) is used as an equivalent notation for \( S \), the term language can be extended to include sets that are characterized by predicates. However, one has to be careful: a set \( \{ x | P(x) \} \) need not be constructive even for computable \( P \), if no domain is indicated. Therefore, predicates for set formation have to be restricted to those based on set expressions, i.e. elementary predicates \( x \in S \). All other predicates have to be restrictive in the sense that they restrict a set to a subset ("filter predicates").

**Definition 4.3 (admissible set predicates):**

The set of admissible set predicates is defined by

1. The elementary predicates \( x \in S \) are admissible set predicates.
2. If \( P \) is an admissible set predicate and \( Q \) any predicate, then \( PAQ \) is an admissible set predicate.
3. If \( P \) and \( Q \) are admissible set predicates, then \( PVQ \) and \( PvQ \) are admissible set predicates.

**Lemma 4.4:**

If \( P \) and \( Q \) are admissible set predicates, then

\[
\{ x | P(x) \lor Q(x) \} = \{ x | P(x) \} \cup \{ x | Q(x) \}
\]

and

\[
\{ x | P(x) \land Q(x) \} = \{ x | P(x) \} \cap \{ x | Q(x) \}
\]

It can be shown that the operations defined here have most of the standard properties. However, the well-known problems caused by only partial recursive predicates still remain. For example,

\[
-\ ( \forall x \in S. P(x) ) = \exists x \in S. - P(x)
\]

is true only if \( P \) is total on the domain under consideration.

It is obvious that the representation of sets and set operations provide a model for a theory of (finite) sets. In particular, a first-order like calculus based on the restricted quantifiers is available for
proving properties of functions. Note that this calculus is constructive in the sense that all expressions denote computable functions (cf. [Co]).

As the type system does not include basic set types, sets have to be generated from objects that are not sets. There is a canonical way of deriving set-valued functions from types. Recall that a type \( t \) is a base type for a data type \( l \), if it occurs in its definition. For each type \( t \), that is a base type for \( t \), a function

\[
\text{set-of}_t \: t \rightarrow \text{set}(t)
\]

is obtained by homomorphically extending the mapping base-type \( t \rightarrow \) singleton-set. More precisely, in the homomorphic extension constructors are replaced by set union (with appropriate arity); those parts of a structure that do not involve elements of type \( t \), are mapped onto the empty set. An example can be found in section 5.

### 4.2 Schemes for Function Definition

In section 3 we introduced a method called "homomorphic extension" for defining new functions over a data type. A particularly simple special case of this method is the endomorphic extension of a function. An endomorphism is a homomorphism from an algebra into itself. Since all the algebraic operations remain unchanged, the only parameters of endomorphic extension are the functions on the base types to be extended. A typical example is substitution of terms for variables. Recall the data type definition for binary trees over atoms from section 3:

\[
bintree := \text{mkbt}(\text{subatom}) | \text{comp}(\text{first} : \text{bintree}, \text{sec} : \text{bintree})
\]

where \( \text{atom} \) is the generating base type. The corresponding endomorphic extension functional is

\[
\text{BTend} := [\lambda x. \text{is}_\text{mkbt}(x) \Rightarrow (\text{atom} (\text{sub}(x))), \text{is}_\text{comp}(x) \Rightarrow \text{comp}(E(\text{first}(x)), E(\text{sec}(x))), \bot]]
\]

Now, if we want to solve the problem

"Find a function \( \text{varsubst} : \text{bintree} \rightarrow \text{bintree} \) such that \( \text{varsubst} \) replaces all atoms in a binary tree by their values under the function \( \text{varsub} : \text{atom} \rightarrow \text{bintree}. "

then a solution is simply

\[
\text{varsubst} = \text{BTend}(\text{varsub}),
\]

and this solution is even unique, as it was shown in section 3.

So far, we have been looking at homomorphisms only. Unfortunately, many interesting functions cannot be represented as homomorphisms. But we can apply a similar definition technique to a larger class of functions simply by explicitly stating the non-homomorphic part of the function and
using the extension functional for the homomorphic rest. This situation occurs often with data types which include several composed subtypes; an example can be found in the next section.

The functionals derived from a data type definition (for homomorphic, endomorphic extension etc.) not only permit definition of new functions in a concise way, they also facilitate proving properties. In fact, certain properties of those functions derive from properties of the functionals, like the induction proof rule already mentioned above.

Lemma 4.5:

If the argument functions of an extension functional are strict/total then the resulting function is strict/total.

Note that totality entails that any program derived from a function by "meaning-preserving" transformations terminates on defined inputs.

There are other definition schemes that hitherto have defied a natural algebraic interpretation. Consider, for example, the following form of function iteration. Let the expression

\[ \forall x \in S : f(x,z) \]

be interpreted as "For each \( x \) in \( S \) apply \( \lambda y. f(x,y) \) to \( z \)." This can be made more precise by a recursion on the sequence representing \( S \):

\[ \forall z \in S \left[ \forall x \in S : f(x,z) \right] = \left[ \forall F \left[ \lambda S z. \exists \text{ _emptyseq}(S) \Rightarrow z, F(S(z), f(hd(S), z)) \right] \right] \]

However, this interpretation causes some problems. In order to be a conservative extension of the specification language as defined so far the given interpretation has to be consistent with the notions introduced previously. In particular, if two sets \( S \) and \( S' \) are equal one would expect

\[ \forall x \in S : f(x,z) = \forall x \in S' : f(x,z) \]

This implies that the applications of the \( f(x,\_) \) must be independent of the particular representation of \( S \), i.e. the "hidden order" on \( S \); or, at least, it must be guaranteed that the sequence of applications of \( f \) can be executed in any order. This virtually restricts applicability of the construction; in many cases it may not be easy or even possible to verify this kind of commutativity. Although operators like function iteration are necessary to make the specification language powerful enough, they will not be discussed further in this paper.

4.3 Transformation of Function Definitions into Programs

So far we have been discussing methods for defining functions over structured data and their interpretation in LCF. Now, every LCF term also has an interpretation as a computation rule for
the function denoted by it. Given such an interpreter for LCF this allows to compute all the functions definable in the language. However, the resulting computations would be quite inefficient, in particular because of nestings of unnecessary recursions resulting from direct interpretation of the constructs. Consider, for example, the expression

\[ F(y) = \forall x \in S(y). P(x) \]

where the type of \( y \) is the data type list as defined above and \( S \) the standard set-valued function \texttt{set_of_atom}. Since list is a recursive type, one recursion is required to compute \( S(y) \) and another one to compute the quantified expression; but we can do much better by utilizing the underlying algebraic structure. Note that the value of \( F \) is determined by the values of \( P(x) \); moreover, we have

\[ P = F \circ \text{mkbl} \]

which means that \( F \) is a homomorphic extension of \( P \). Because of the uniqueness property it follows that

\[ F = \text{BThom}(P, \wedge) \]

where \( \text{BThom} \) is the homomorphic extension functional for \texttt{bintree}. This means that \( F \) can be replaced by an equivalent function that involves only one recursion. Apart from that, the explicit representation of the set \( S(y) \) is eliminated.

This is an example of how the algebraic concepts can be used to simplify function definitions considerably. It shows that the interpretation of the specification language is not a case of simple macro expansion, but a possibly non-deterministic process of simplifying expressions in a suitable way, which is similar to, e.g., theorem proving. More heuristic methods for recursion removal have been studied by R. Burstall and J. Darlington [BD].

The regular expression structure that results from defining functions by means of definition schemes is of advantage at all levels of program development. Apart from the techniques for proving properties about them (see above) it permits uniform application of optimizing transformations, like replacing recursion by iteration. Even at the implementation level it can be advantageous. For example, functions defined by endomorphic extension can be implemented in such a way that no additional storage (for data) is required (cf. selective updating in [Ho]). If it has been proved that the transformation and implementation techniques preserve meanings, then the "correctness" of resulting programs can be guaranteed. Meaning preserving transformations will be studied in greater detail in a subsequent paper.
5. An Example: Substitution with $\alpha$-Conversion

5.1 The Data Types
In the example now to be discussed we have four data types, defined by

$$\text{term} := \text{mkcterm(constof:const)} \mid \text{mkvterm(varof:var)} \mid \text{mkapply(funeof:term, argof:term)} \mid \text{mklambda(bvarof:bvar, termof:term)} \mid \text{mkmu(bvarof:bvar, termof:term)} \mid \text{mkcond(condof:term, truem:term, falseof:term)}$$

$$\text{bvar} := \text{mkbvar(varof:var)}$$
$$\text{const} := \text{uu | tt | ff | oo}$$

var is taken as basic and not further specified.

The reader will notice that these data types represent the abstract syntax of LCF terms. In algebraic terms the types form a heterogeneous algebra with the four phyla term, bvar, var, and const and operations

- \text{(op1)} mkcterm: const $\rightarrow$ term
- \text{(op2)} mkvterm: var $\rightarrow$ term
- \text{(op3)} mkapply: term x term $\rightarrow$ term
- \text{(op4)} mklambda: bvar x term $\rightarrow$ term
- \text{(op5)} mkmu: bvar x term $\rightarrow$ term
- \text{(op6)} mkcond: term x term x term $\rightarrow$ term
- \text{(op7)} mkbvar: var $\rightarrow$ bvar

The generating phyla (data types) are const and var. Obviously the phyla var and bvar are isomorphic; the reason for introducing the data type bvar is that it is more convenient to separate the binding occurrences of variables from the other ones.

From the data type definitions the following characterizing functions are generated:

$$\text{term} := [\lambda F. [\lambda x. \text{is_const}(x) = \text{mkcterm(constof:const}(x)), \text{is_mkvterm}(x) = \text{mkvterm(varof:var}(x)), \text{is_mkapply}(x) = \text{mkapply(F(funeof:term}(x), F(argof:term}(x))), \text{is_mklambda}(x) = \text{mklambda(bvarof:bvar}(x), F(termof:term}(x)), \text{is_mkmu}(x) = \text{mkmu(bvarof:bvar}(x), F(termof:term}(x)), \text{is_mkcond}(x) = \text{mkcond(F(condof:term}(x), F(truem:term}(x), F(falseof:term}(x)), \top ] ]$$

$$\text{bvar} := [\lambda x. \text{mkbvar(varof:var}(x)))]$$

In order to define a homomorphism we have to supply 7 operations of appropriate types. 6 of them correspond to the constructors occurring in the characteristic function term; the last one is to replace mkbvar. By substituting the characteristic function for bvar in term we obtain an expression that
includes all operations and completely defines homomorphic extension. For endomorphic extension
only the operations on the generating subtypes (i.e. op1, op2 and op7) are required. Let

\[\text{termhom} := [\lambda\text{op1 op2 ... op7} [\alpha] F \ldots]\]

and

\[\text{termend} := [\lambda\text{op1 op2 op7} [\alpha] F \ldots]\]

be the functionals for homomorphic and endomorphic extension.

5.2 The Problem
We want to formalize the following (cf. [AW]):

Replace any free occurrence of the variable \( v \) in the expression \( \text{term} \) by the term \( t \) after renaming bound variables in \( \text{term} \) suitably (i.e. so that no free variable in \( t \) will become bound in \( \text{term} \))
(a common notation is \( \text{term}[t/v] \)).

What is described above is the basic conversion rule of the \( \lambda \)-calculus as it is incorporated in the
LCF system. It may be desirable to have a system that is smart enough to understand this
description of substitution and to translate it from English into a programming language. At
present, such a system is not available. It would require knowledge about what exactly is meant by
"free occurrence", "replace", "renaming" etc. For the time being we have to be satisfied with specifying
those notions in some kind of formal language and having a less ambitious system transform the
specification statements into executable code. In any case, we need a formal definition in order to be
able to prove anything about the function.

We construct a function \( \text{subst} : \text{var} \times \text{term} \times \text{term} \to \text{term} \) by stepwise specifying the informal notion in
our language. Let \( \text{subst} \) be defined by

\[\text{subst} := [\lambda v \in o. \text{subffree}(v, t, \text{renamebvar}(e, t))]
\]

where

\[\text{subffree}(v, t, e) := \text{"replace all free occurrences of } v \text{ in } t \text{ by } t\"
\]

\[\text{renamebvar}(e, t) := \text{"rename bound variables in } e \text{ that occur free in } t \text{ appropriately"}
\]

a) bound variables in term. The function \( \text{boundvarsin} : \text{term} \to \text{setof}(\text{var}) \) returns a set of variables for
which there is a binding occurrence in the term. This is just the standard set function \( \text{setof-bvar} \)
composed with the isomorphism \( \text{variso} \) from \( \text{bvar} \) to \( \text{var} \), extended to sets. Here we can see how
the separation of the type \( \text{bvar} \) from \( \text{var} \) facilitates definition of set-valued functions. \( \text{setof-bvar} \) is the
homomorphism defined by the operations

\[
\begin{align*}
b_1 := b_2 := [\lambda x. \emptyset] & \quad \text{(empty set)} \\
b_3 := b_4 := b_5 := U & \\
b_6 := U_3 & \\
b_7 := [\lambda x. x] & \quad \text{(singleton map)}
\end{align*}
\]
An Example: Substitution with α-Conversion

i.e., \( \text{set-of-bvar} = \text{termhom}(b_1, \ldots, b_7) \).

Then

\[
\text{boundvars} := \text{variso} \circ \text{set-of-bvar}
\]

b) free variables in \( t \). The standard function \( \text{set-of-vars} \) returns all occurring variables regardless of whether they are free or not. So we have to update that function appropriately to get a function that returns only free variables. If we had separated the \( \lambda \)- and \( \alpha \)-terms from the type \( \text{term} \) we could use a standard set-of-dtype function for defining \( \text{freevars} \). Instead, we define it directly as as a homomorphism

\[
\text{freevars} : \text{term} \to \text{setof}(\text{var}).
\]

Using the set-valued functions

\[
\begin{align*}
&f_1 := [\lambda x. \{\}] \\
&f_2 := f_7 := [\lambda x. \{x\}] \\
&f_3 := \emptyset \\
&f_4 := f_5 := [\lambda x. y. y \setminus x] \quad \text{(set difference)} \\
&f_6 := \emptyset
\end{align*}
\]

the function is definable by

\[
\text{freevars} := \text{termhom}(f_1, \ldots, f_7)
\]

c) Renaming bound variables. We need a function \( \text{newvar} \) that "invents" new variables (which do not occur in either \( e \) or \( t \)). Strictly speaking the existence of \( \text{newvar} \) depends on a function that enumerates all variables and returns the first element with a certain property. In any practical implementation we "know" all the variable names available to the user, so a function that generates new names is available. In the abstract context it is sufficient to assume the existence of a strict and total function \( \text{newvar} \) that returns a variable with the property

\[
\text{newvar}(v, e, t) \notin \text{varsin}(e) \cup \text{varsin}(t) \cup \{v\}.
\]

Using this function we can specify renaming of bound variables:

\[
\text{renamevar}(e, t) := "\text{rename in } e \text{ each variable that occurs free in } t \text{ and bound in } e"\]

formally:

\[
\begin{align*}
\text{renamevar} & := [\lambda e. t. \{[\forall x \in \text{freevars}(t) \cap \text{bvarsin}(e) : \text{rename}(l, x, e)]\}] \\
\text{rename} & := [\lambda t. \{\forall x : \text{term}(\text{mkterm}, \text{replacevar}, \text{mkbvar} \circ \text{replacevar})\}]
\end{align*}
\]

where \( \text{replacevar} \) denotes the term \( [\lambda z. z = x \Rightarrow \text{newvar}(x, e, l), z] \). Note that the use of the iteration construction is justified by the fact that renaming of bound variables can be done in any order; all resulting terms are equivalent.
d) \textit{substfree}. "Free occurrence" means "not bound", i.e. "not in the range of a \( \lambda \) or \( \alpha \) binding that variable." So, in order to find occurrences of a variable \( v \) we have to search (recur in) the tree representing the term \( t \). Whenever we come across a \( \lambda \) or \( \alpha \) (that is, a mklambda or mkmu) that binds \( v \), we stop and return. Then any remaining occurrence of \( v \) is a free one and is to be replaced by \( t \). In the formal language this is expressed by a construction using a modified functional for endomorphic extension:

\[
\text{substfree} := \exists S. [\lambda t. [\lambda e. \text{is_mKterm}(e) \Rightarrow \text{varof}(e)v = t, e, \\
\text{is_lambda}(e) \vee \text{is_mKmu}(e) \wedge \text{bvarof}(e)v = t, \text{term}(S(v,t),e))].
\]

Here \( \text{term} \) is the operator on \( F \) that defines \( \text{term} \), i.e. \( \text{term} = [\alpha F; [\lambda x. \text{term}(F,x)]] \).

This finishes the formal specification of the substitution function. The collection of all the function definitions

\[
\begin{align*}
\text{subst} & := [\lambda v t e. \text{substfree}(v,t,\text{renamevar}(e,t))], \\
\text{substfree} & := [\alpha S. [\lambda v t e. [\lambda e. \text{is_mKterm}(e) \Rightarrow \text{varof}(e)v = t, e, \\
\text{is_lambda}(e) \vee \text{is_mKmu}(e) \wedge \text{bvarof}(e)v = t, \text{term}(S(v,t),e))]], \\
\text{renamevar} & := [\lambda t. [\forall x \in \text{freevars}(t) \wedge \text{bvar}(e) = \text{rename}(t,x,e)]], \\
\text{rename} & := [\lambda t. [\lambda x e. \text{term}(\text{mkterm}(\text{mkmu}(t), \text{replacevar}(\text{mkvar} = \text{replacevar})))]], \\
\text{replacevar} & := [\lambda z x. \text{newvar}(x,z,t,e)], \\
\text{bvar} & := \text{variso} \circ \text{set-of-bvar}, \\
\text{set-of-bvar} & := \text{term}(\text{hom}(\lambda x.1), [\lambda x.1], U, U, U, U, [\lambda x.1]), \\
\text{freevars} & := \text{term}(\text{hom}(\lambda x.1), [\lambda x.1], U, U, U, U, U, [\lambda x.1]).
\end{align*}
\]

is somewhat longer than the informal description in English, yet it is complete in the sense that a sufficiently smart system can transform it into a reasonably efficient program, using transformations of the sort indicated in the preceding section.
6. Concluding Remarks

In this paper, the representation of abstract data types in LCF and the algebraic interpretation of structures were discussed. This led to constructions that permit to specify functions operating on data structures in a concise way and close to what may be considered "natural." The methods were demonstrated in an example taken from the actual LCF system.

The construction methods considered here constitute only a first step towards an elaborated language that will allow easy and concise definition of complex functions as they are needed in, e.g., structure manipulating systems. There are many directions in which the work presented here has to be extended. Some have already been mentioned in the preceding sections: systematic extension of the system of data type; more general function definition schemes; general methods for transforming and optimizing function definitions, in particular for removal of redundant recursions; the translation of logical expressions into a "real-life" programming language. In the paper, only methods for explicit function definition have been discussed. However, it appears that techniques for solving equations that define functions implicitly can similarly be derived from the explicit representation of the data structure by a retract. The retract could serve for guiding the search for solutions and for structuring the resulting program. The development of such problem solving methods in the framework of LCF has to be left to future studies.

How much of the methods discussed here can be automated? It is obvious that the generation of the appropriate set of axioms, of function definition schemes and rules for structural induction from the data type definitions is straightforward and can be completely automated. Furthermore, many checks for simplifications and transformations can be done on a purely syntactic level accessible to automation. So it should be easy to incorporated all these features and special knowledge about the restricted set calculus into an interactive system for developing programs and proving theorems about them.
References

R. Reference


Appendices

A.

A.1 Logic for Computable Functions

A.1.1 Syntax of Typed LCF

The following is an extract taken from [Mil].

Types At bottom tr and ind are types. Further if \( A_1 \) and \( A_2 \) are types then \( (A_1 \rightarrow A_2) \) is a type.

With each term of the logic there is an unambiguously associated type. For a term \( t \) we write \( t : \beta \) to mean that the type associated with \( t \) is \( \beta \).

Terms (metavariables \( s,t,s_1,t_1,\ldots \)) The following are terms:

- Identifiers (metavariables \( x,y \)) - sequences of upper or lower letters and digits. We assume that the type of each identifier is uniquely determined in some manner.
- Applications - \( s(t) : A_2 \), where \( s : A_1 \rightarrow A_2 \) and \( t : A_1 \).
- Conditionals - \((s \rightarrow t_1,t_2) : \beta\), where \( s : A_1 \rightarrow A_2 \) and \( t_1,t_2 : \beta \).
- \( \lambda \)-expressions - \([\lambda x.s] : A_2 \), where \( x : A_1 \) and \( s : A_2 \).
- \( \alpha \)-expressions - \([\alpha x.s] : \beta \), where \( x : A \).

The intended interpretation of the \( \alpha \)-expression \([\alpha f.s] \) is the minimal fixed-point of the function or functional denoted by \([\alpha f.s] \). For example:

\[ [\alpha f.[\lambda x.(p(x) \rightarrow f(a(x)),b(x))]] \]

denotes the function defined recursively as follows:

\[ f(x) = \begin{cases} p(x) & \text{if } p(x) \\ f(a(x)) & \text{else } b(x) \end{cases} \]

Constants The identifiers \( \tt, \# \) denote truthvalues true and false. \( \perp \) denotes the totally undefined object of any type; in particular, the undefined truthvalue.

Atomic well-formed formulae (awffs) The following is an awff:

\[ s \sqsubseteq t \]

where \( s \) and \( t \) are of the same type. The intended interpretation of \( s \sqsubseteq t \) is, roughly, that \( t \) is at least as well defined as, and consistent with, \( s \).

Well-formed formulae (wffs) (metavariables \( P,Q,P_1,Q_1,\ldots \)) Wffs are sets of zero or more awffs, written as lists with separating commas. They are interpreted as conjunctions. We use
to abbreviate set, tes.

Sentences Sentences are implications between wffs, written

\[ P \vdash Q \]

or, if \( P \) is empty, just \( \vdash Q \).

Proofs A proof is a sequence of sentences, each being derived from zero or more preceding sentences by a rule of inference.

The strict syntax for terms and wffs is relaxed in the machine implementation to allow a saving of parentheses and brackets. In addition, we use the abbreviation

\[
\begin{align*}
& f(x,y) \quad \text{for} \quad f(x,y) \\
& \forall x.t = s \quad \text{for} \quad \lambda x.t = \lambda x.s \\
& p :: q = r \quad \text{for} \quad p \supset q, \bot = p \supset r, \bot
\end{align*}
\]

Functions are used in infix notation where it is obvious what is meant.

A.1.2 Type free LCF

The type free version of LCF differs from the typed one essentially in the handling of truth values and conditional expressions. Apart from that it also specifies the structure of the domain. Besides the truth values there are constants \( T \) for the truth values retract and \( I \) for the universal domain. In the following the additional axioms and rules of inference are listed.

\[ \text{MAX} \vdash s \in T \]

\[ \text{COND} \vdash T \rightarrow s, s = s \]

\[ \vdash r \rightarrow s, t = T(r) \rightarrow s, t \]

\[ \vdash T(s)(t) = T(s) \]

\[ \vdash T = T \rightarrow T \]

\[ \vdash I = [\alpha \land T \lor (J \rightarrow J)] \]

The CASES-rule is changed to

\[
\begin{align*}
P \vdash Q(\bot/x) & \quad P \vdash Q(\emptyset/x) & \quad P \vdash Q(\ast/x) & \quad P \vdash Q(T/x) \\
\text{CASES} & \quad \vdash Q(T/x)
\end{align*}
\]
Appendices

Other defined standard terms:

\[ \equiv : \lambda x y z. x \equiv x \equiv y, T, z \]

\[ \rightarrow : \lambda x y. \lambda z. y z x x \]
Appendices

A.2 Special Functions in tfLCF

A.2.1 Definedness predicate

We want a predicate $d$ such that

$\vdash d(x) \leftrightarrow x \neq \bot, x \neq T$

Define $d$ by

$d = \text{upt} \cup \text{down}$

where

$\text{down} = \left(\lambda x. : \bot \rightarrow \bot, \bot\right)$

and

$\text{upt} = \left[\lambda x. : (x = \bot) \cup P(x(T))\right] \cup \left(\lambda x. \text{upt}(x) \cup \bot, \bot\right)$

down maps everything to $\bot$ except $T$ which goes to $T$:

$\down(x) = \bot \rightarrow T \neq \bot$ (i) $\down(x) \neq T$

upt maps everything to $\top$ except $\bot$ which is mapped to $\bot$. The desired properties of $d$ are then obvious.

A.2.4 istrue

Our aim is to give a function that

- maps everything on a truth value and
- gives the values $\bot$ and $\top$ exactly for the arguments $\bot$ and $\top$ resp.

This function will enable us to test effectively variables for "well defined" truth values. In the type-
free logic, the simple conditional does not provide this function as it is defined "relative to the truth
values retract $T". However, we can define istrue using a limit construction. That such a definition is
possible at all is due to the fact that the truth values are isolated points in the lattice $I$.

Definition: $\text{istrue} = \left[\lambda S. \left(\lambda x. x : \bot \cup S(x,T), \bot \cup S(x,T)\right)\right]$

It is easy to show by cases that

1) $T \subseteq \text{istrue}$

Since $\forall x. T(x) \subseteq x$ we also have

2) $\bot \circ \text{istrue} \subseteq \text{istrue}$

From the definition follows immediately

$\vdash \text{istrue}(x) = \bot \rightarrow \text{istrue}(x(T)) \subseteq \text{istrue}(x)$

$\vdash \text{istrue}(x) = \bot \rightarrow \text{istrue}(x(T)) \subseteq \text{istrue}(x)$
also

(4) \( T(x) \models TV \models \text{istrue}(x) \models TV \) for \( TV = \bot, T \)

Next we show by induction on istrue

(5) \( \forall x. \text{istrue}(x) \subseteq T(\text{istrue}(x)) \)

I. \( \bot(x) = \ldots \) ok.

II. Assume \( \forall x. S(x) \subseteq T(\text{istrue}(x)) \). We have to show
\[ x :\rightarrow \, tt \cup S(x \, T) \Rightarrow \, tt \cup S(x \, T) \subseteq T(\text{istrue}(x)). \]

By cases \( T(x) \):

- \( T(x) = \bot \): trivial
- \( T(x) = T \): implies \( \text{istrue}(x) = T \), trivial.

\[ \begin{align*}
T(x) = & \, \text{tt} : \\
\text{lhs} = & \, \text{tt} \cup S(x \, T) \subseteq \, \text{tt} \cup T(\text{istrue}(x \, T)) \text{ by Ind.Hyp.} \\
= & \, T(\text{tt} \cup \text{istrue}(x \, T)) \text{ by L54 Mi-We} \\
= & \, T(\text{istrue}(x)).
\end{align*} \]

\( T(x) = \# \) : analog

With (2) we have shown

(6) \( \text{istrue} = T \circ \text{istrue} \)

which means that the range of \( \text{istrue} \) is a set of truth-values.

On the other hand we already mentioned that

(6a) \( \text{istrue}(tv) = tv \)

holds for each truth value \( tv \). Thus, in a short notation

(7) \( \text{istrue} \circ T = T \)

i.e. \( \text{istrue} \) is an identity on \( T \). From (6) and (7) we deduce the retract property for \( \text{istrue} \):

\[ \begin{align*}
\text{istrue} \circ \text{istrue} &= \text{istrue} \circ (T \circ \text{istrue}) \\
&= (\text{istrue} \circ T) \circ \text{istrue} \\
&= T \circ \text{istrue} \\
&= \text{istrue}
\end{align*} \]
The ultimate goal is to show

\[(*)\] istru\(x\) = \(\texttt{tt}\) \(\vdash x = \texttt{tt}\)

\[(*)\] istru\(x\) = \(\texttt{ff}\) \(\vdash x = \texttt{ff}\)

i.e. istru is a truth-valued function that gives the values \(\texttt{tt}\) or \(\texttt{ff}\) exactly for \(\texttt{tt}\) and \(\texttt{ff}\) resp. In order to do so we introduce another truth-valued function:

Definition: \(\text{uptf} = \{ x \in P. [\lambda x. T(x) \cup P(x(T))]\}\)

By definition we have

(U1) \(T \subseteq \text{uptf}\)

We prove the following facts about \(\text{uptf}\):

(U2) \(x \subseteq \text{uptf}\)

(9) \(\text{istru} \subseteq \text{uptf}\)

(10) \(\text{istru}\(x\) = \(\texttt{tt}\) \(\vdash \text{uptf}(x) \subseteq \text{istru}(x)\)

(9) and (10) together show

(11) \(\text{istru}\(x\) = \(\texttt{tt}\) \(\vdash \text{uptf}(x) \subseteq \text{istru}(x)\)

With (U2) it follows that

(12) \(x \subseteq \texttt{tt}\)

on the other hand, since \(\texttt{tt} = T(x) \subseteq x\) we have

(13) \(\text{istru}\(x\) = \(\texttt{tt}\) \(\vdash x = \texttt{tt}\).

The proof for the corresponding statement for \(\texttt{ff}\) follows the same line.

A.3 Structural induction

The basic idea of how to do structural induction in LCF is that it can actually be simulated if a recursive function "describing" the structure is available. For the kind of structures we are interested in in this paper the retraction constructed from the type definition serves this purpose. So, structural induction becomes a mere application of computational induction. The derivation of the induction rule as in theorem 3.x is done in two steps: 1) first derive a rule involving the retraction; 2) modify the rule in 1) by using the type-predicate. Since proving the rule in full generality would be rather tedious, it is demonstrate by means of the example seq.
Appendices

Recall that \texttt{seq} is defined by the retraction
\begin{verbatim}
  \texttt{seq} = \{ \lambda S. [ \lambda x. \texttt{is_emptyseq}(x) \Rightarrow \texttt{emptyseq},
                     \texttt{is_mkseq}(x) \Rightarrow \texttt{mkseq}(\texttt{atom}(\texttt{hd}(x)), \texttt{S}(\texttt{tl}(x))),
                     \perp] ] \}
\end{verbatim}

First, we prove the rule
\begin{equation}
  \begin{array}{c}
    \texttt{(a$_1$) } \texttt{P}(\perp) \quad \texttt{(a$_2$) } \texttt{P}(\top) \quad \texttt{(a$_3$) } \texttt{P}(\texttt{emptyseq}) \quad \texttt{(a$_4$) } \forall x. \texttt{P}(y) \vdash \forall x. \texttt{P}(\texttt{mkseq}(x,y)) \\
  \texttt{Vx. } \texttt{P}(\texttt{seq}(x))
  \end{array}
\end{equation}

where \(x\) and \(y\) do not occur in \(P\). By computational induction, we can deduce
\begin{verbatim}
\forall x. \texttt{P}(\texttt{seq}(x))
\end{verbatim}
from
\begin{verbatim}
\forall x. \texttt{P}(\perp x) \quad \texttt{and} \quad \forall x. \texttt{P}(\texttt{S}(x)) \vdash \forall x. \texttt{P}(\texttt{tau}(\texttt{S})(x)).
\end{verbatim}
Since
\begin{verbatim}
\texttt{P}(\perp x) \iff \texttt{P}(\perp)
\end{verbatim}
the base case is proved by premise (a$_1$).

Now assume
\begin{verbatim}
\forall x. \texttt{P}(\texttt{S}(x))
\end{verbatim}
In order to prove
\begin{verbatim}
\forall x. \texttt{P}(\texttt{tau}(\texttt{S})(x))
\end{verbatim}
we expand \(\texttt{tau}(\texttt{S})\) to
\begin{verbatim}
\texttt{tau}(\texttt{S})(x) = \{ \lambda x. \texttt{is_emptyseq}(x) \Rightarrow \texttt{emptyseq},
                  \texttt{is_mkseq}(x) \Rightarrow \texttt{mkseq}(\texttt{atom}(\texttt{hd}(x)), \texttt{S}(\texttt{tl}(x))),
                  \perp] \}
\end{verbatim}
and split into cases which then can be deduced from appropriate premises:
\begin{verbatim}
\texttt{is_emptyseq}(x) = \perp : \quad \texttt{tau}(\texttt{S})(x) = \perp \quad \texttt{by premise (a$_1$)}
\texttt{tt} : \quad \texttt{emptyseq} \quad \texttt{by (a$_3$)}
\texttt{\top} : \quad \texttt{\top} \quad \texttt{by (a$_2$)}
\texttt{if : case split for is_mkseq(x) : only \texttt{tt} is interesting:}
\quad \texttt{mkseq}(\texttt{atom}(y), S(x)) \quad \texttt{by (a$_4$)}
\end{verbatim}

Now, the rule
\begin{equation}
  \begin{array}{c}
    \texttt{(b$_1$) } \texttt{P}(\texttt{emptyseq}) \quad \texttt{(b$_2$) } \texttt{P}(y) \vdash \texttt{P}(\texttt{mkseq}(x,y)) \quad \forall x. \texttt{is_seq}(x) \Rightarrow \texttt{P}(x)
  \end{array}
\end{equation}
follows from (R1) by virtue of the facts that the relativizing type predicate eliminates the cases \(\perp\) and \(\top\).
In this paper we discuss techniques of exploiting the obvious relationship between program structure and data structure for program generation. We develop methods of program specification that are derived from a representation of recursive data structures in the Logic for Computable Functions (LCF). As a step towards a formal problem specification language we define definitional extensions of LCF. These include a calculus for (computable) homogeneous sets and restricted quantification. Concepts that are obtained by interpreting data types as algebras are used to derive function definition schemes from an LCF term representing a data structure; they also lead to techniques for the simplification of expressions in the extended language. The specification methods are illustrated with a detailed example.