Applicative Functors in Isabelle/HOL: Notes

Joshua Schneider

August 18, 2015

1 Project Overview

1.1 Introduction

Our primary goal is to implement an Isabelle/HOL proof method which reduces lifted equations to their base form. Here, lifting refers to a transition from operations on base types to related operations on some structure. Hinze [1] studied the conditions under which lifting preserves the validity of equations. He noticed that lifting can be defined in an intuitive fashion if the target structure is an applicative functor [2]: a unary type constructor f with associated constants[1]

$$\begin{aligned} \mathit{pure}_f &:: \alpha \Rightarrow \alpha f, \\ (\diamond_f) &:: (\alpha \Rightarrow \beta) f \Rightarrow \alpha f \Rightarrow \beta f. \end{aligned}$$

The operator $\diamond_f$ is left-associative. We omit the subscripts if the functor is clear from the context. Moreover, the following laws must be satisfied:

$$\begin{aligned} \mathit{pure}\, \mathit{id} \diamond u &= u && \text{(identity)} \\ \mathit{pure}\, (\cdot) \diamond u \diamond v \diamond w &= u \diamond (v \diamond w) && \text{(composition)} \\ \mathit{pure}\, f \diamond \mathit{pure}\, x &= \mathit{pure}\, (f x) && \text{(homomorphism)} \\ u \diamond \mathit{pure}\, x &= \mathit{pure}\, (\lambda f.\, f x) \diamond u && \text{(interchange)} \end{aligned}$$

The identity type constructor defined by $\alpha\, \mathit{id} = \alpha$ is a trivial applicative functor for $\mathit{pure}\, x = x$, $f \diamond x = f x$. We can take any abstraction-free term t and replace each constant c by $\mathit{pure}\, c$, and each instance of function application $f x$ by $f \diamond x$. The rewritten term is equivalent to t under the identity functor interpretation, or identity "idiom" as coined in [2]. By choosing a different applicative functor, we obtain a different interpretation of the same term structure. In fact, this is how we define the lifting of t to an idiom. We also permit variables, which remain as such in the lifted term, but range over the structure instead. A term consisting only of pure and $\diamond$ applications and free variables is called an idiomatic expression.

Example 1. Another applicative functor can be constructed from sets. For each type α there is a corresponding type $\alpha\, \mathit{set}$ of sets with elements in α; pure denotes the singleton set constructor $x \mapsto \{x\}$; $F \diamond X$ takes a set of functions F

[1] Types are given in Isabelle notation.

and a set of arguments X with compatible type, applying each function to each argument:

$$F \diamond X = \{f x \mid f \in F,\, x \in X\}.$$

We can lift addition on natural numbers to the set idiom by defining the operator

$$(\oplus) :: \mathit{nat\ set} \Rightarrow \mathit{nat\ set} \Rightarrow \mathit{nat\ set},$$
$$X \oplus Y = \mathit{pure}\,(+) \diamond X \diamond Y = \{x + y \mid x \in X,\, y \in Y\}.$$

The associative property of addition

$$\forall xyz.\ (x + y) + z = x + (y + z)$$

can be translated to sets of natural numbers

$$\forall XYZ.\ (X \oplus Y) \oplus Z = X \oplus (Y \oplus Z),$$

where it holds as well, as one can check with a slightly laborious proof. Note that the two sides of the latter equation are the lifted counterparts of the former, respectively. ▲

As we have seen, lifting can be generalized to equations. There is actually a more fundamental relationship between the two equations from above example—the lifted form can be proven for all applicative functors, not just *set*, using only the base property and the applicative functor laws. We want to automate this step with a proof method.

Not all equations can be lifted in all idioms, though. Stronger conditions are required if the list of quantified variables is different for each side of the equation. (The left-to-right order is relevant, but not the nesting within the terms.) These conditions must basically ensure that the functor does not add "too many effects" which go beyond the simple embedding of a base type. Such effects may be evoked if a variable takes an impure value, i.e., a value which is not equal to $\mathit{pure}\,x$ for any x.

Example 2. We try to lift the fact that zero is a left absorbing element for multiplication of integers, $\forall x :: \mathit{int}.\ 0 \cdot x = 0$, to sets. Note that the variable x occurs only on the left. But the lifted equation does not hold: If x, now generalized to *int set*, is instantiated with the empty set, then

$$\mathit{pure}\,(\cdot) \diamond \mathit{pure}\,0 \diamond \{\} = \{\} \neq \mathit{pure}\,0.$$

Here the effect of $\{\}$ is that it cancels out everything else if it occurs somewhere in an idiomatic expression. This makes it impossible to lift any equation with a variable occuring only on one side to *set*. ▲

1.2 User Interface

Since Isabelle's core logic does not allow parameterization of type constructors, we need a custom mechanism for registering applicative functors with the system. In order to apply the proof method, the user must provide beforehand

a) corresponding *pure* and $\diamond$ instances, and

b) a proof of the applicative functor laws, optionally with extended properties.

Lifted constants may be registered with an attribute, which can be applied to facts $lhs = rhs$, where rhs is an idiomatic expression. These must be suitable for rewriting.

The complete set of subgoal forms to support has not been determined yet. $\boxed{\text{To do.}}$ As a minimal requirement, after unfolding lifted constants, HOL equations of idiomatic expressions shall be handled. Only the outermost functor f is considered per invocation. The conceptual variables of the lifted expressions may be instantiated with arbitrary terms. However, the method actually proves the fully universally quantified form—for every subterm not matching pure_f _ or _ $\diamond_f$ _, a new, locally quantified variable is introduced. We call these subterms *opaque*. The method attempts to transform the first subgoal to the base form of the equation, in other words, its identity functor interpretation. Variable names shall be preserved, if possible. Finally, it is desirable to have some kind of debugging facility for tracing intermediate steps. This may be especially useful if the proof fails because additional laws are required.

Example 3. Continuing with the set idiom from Example 1, assume that the user wants to prove an instantiation of the associativity law for $\oplus$ as part of a larger proof. *set* and $\oplus$ have been declared to the enclosing theory. The current Isabelle goal state is

$$1. \quad (X \oplus Y) \oplus f Z = X \oplus (Y \oplus f Z).$$

The variables X, Y and Z have been fixed in the proof context, and f is some constant, all of appropriate type. This illustrates how we allow a larger variety of propositions, making it easier to apply the method without too much preparation. After applying the proof method, the new proof obligation reads

$$1. \quad \bigwedge xyu.\ (x + y) + u = x + (y + u),$$

which is easily discharged. The corresponding Isabelle/Isar fragment could be

fix $X\ Y\ Z$
...
have "$(X \oplus Y) \oplus f Z = X \oplus (Y \oplus f Z)$" **by** *af_lifting algebra*

af_lifting is our new proof method, and the standard *algebra* method completes the subproof. ▲

1.3 Proof Strategy

The proof method starts with testing the first subgoal for the expected structure. If the test succeeds, the applicative functor f is known, such that the relevant theorems can be accessed subsequently. We then rewrite the subgoal using the declared rules for lifted constants. Only those related to f are used, the reason being that overeager, unwanted unfolding may be difficult to reverse. The result of this preparation is a subgoal which is simple equation of two idiomatic expressions.

The following step depends on which additional properties of f have been provided. All approaches have in common that both expressions are replaced by others in *canonical form*:

$$\mathit{pure}\, g \diamond s_1 \diamond \cdots \diamond s_m = \mathit{pure}\, h \diamond t_1 \diamond \cdots \diamond t_n,$$

If either $m \neq n$ or $t_i \neq s_i$ for some i (as terms modulo $\alpha\beta\eta$-conversion), the proof method fails. Otherwise, we apply appropriate congruence rules until the subgoal is reduced to $g = h$. Since g and h are at least n-ary functions, we can further apply extensionality, reaching the subgoal

$$\bigwedge x_1 \ldots x_n.\, g x_1 \cdots x_n = h x_1 \cdots x_n.$$

This is the transformed proof state presented to the user.

Hinze's Normal Form Lemma [1, p. 7] asserts the existence of a certain normal form for idiomatic expressions where each variable occurs only once. This normal form has the desired structure. As it turns out, we can compute it for arbitrary terms. This is convenient because opaque parts are handled implicitly. However, the result might be too general and unprovable, so we will use the normal form only if no other properties are available. The details of the normalization algorithm are described in Section 2. There we will also show that the transformed equation is exactly the generalized base form of the original equation.

Hinze then explored under what circumstances a larger variety of equations can be lifted. He found that sufficient conditions can be expressed in terms of combinators as known from combinatory logic. We take this idea and adapt it our framework in Section 3. In contrast to the normal form approach, we gain flexibility regarding the opaque terms in the canonical form. This means that the algorithm must determine the sequence $\vec{t} = \vec{s}$ of opaque terms prior to the transformations. The set of available combinators further limits the admissible sequences. Because this relationship cannot be generalized easily, we restrict ourselves to certain combinator sets.

1.4 Choice of Embedding

In Isabelle, it is not possible to construct an abstract framework for applicative functors in such a way that it is inhabited by all instances. We already referred to the fact that type constructors are fixed. Another issue is the lack of polymorphism in the inner logic: We cannot have, say, a schematic variable *?pure* and use it with different types within the same proposition or proof. One solution is to define a custom logic, including a term language, axioms and meta theorems, and formalize it using the available specification tools. This is a *deep embedding* [3] of the logic. Then it would be possible to derive the Normal Form Lemma as a regular inference rule, for example. However, we want to prove propositions about arbitrary HOL objects, not just their encodings in the embedded logic. Some machinery is necessary, which performs the encoding and transfers results.

- finite number of types involved per term $\Longrightarrow$ could use sum types
- number of types in sum is linear in size of terms

- would introduce a large number of projections/abstractions

$\boxed{\text{To do.}}$

A different approach, which we will take, is a *shallow embedding*. The "formulæ" (here, idiomatic terms) are expressed directly in HOL. Due to aforementioned restrictions, meta-theorectical results must be provided in specialized form for each case. We make use of the powerful ML interface of Isabelle to program the proof construction. The correctness of the proofs is still verified by the system, of course.

2 Normal Form Conversion

McBride and Paterson [2] noted that idiomatic expressions can be transformed into an application of a pure function to a sequence of impure arguments. They called this the *canonical form* of the expression. Hinze [1, Section 3.3] gave an explicit construction based on the monoidal variant of applicative functors. Transforming the terms in this way is useful for our purpose, because the arguments of the remaining *pure* terms reflect the equation that was lifted. The soundness of the algorithm depends only on the applicative laws, making it the most general approach regarding functors (but not regarding lifted equalities). We will later show that all transformations based on the applicative laws yield a unique canonical form, modulo $\alpha\beta\eta$-conversion. Therefore, we follow Hinze and denote by *normal form* this particular canonical form. The distinction is necessary, as we will consider other canonical forms in Section 3, which are justified by additional laws.

In the following, we define lifting and normalization formally, based on a syntactic representation of idiomatic terms. While this presentation is more abstract than what is actually happening in Isabelle, it makes it easier to demonstrate correctness and some other properties. Unlike Hinze, we use the *pure*/$\diamond$ formalism. Then we describe the implementation of the normalization procedure in Isabelle/ML.

2.1 The Idiomatic Calculus

In Section 1.1, we introduced idiomatic expressions built from *pure* and $\diamond$ constants of an applicative functor. This structure maps straightforward to a recursive datatype, given that there is a representation for arguments of *pure*. These must have some structure as well such that the applicative laws can be expressed. It should also be possible to have "opaque" idiomatic subterms, which cannot (or should not) be written as a combination of *pure* and $\diamond$. This is primarily useful for variables ranging over lifted types, but as demonstrated in Example 3, more complex terms may occur too. Therefore it makes sense to refer to general lambda terms in both cases; then we can define semantics consistently. Types are ignored here for simplicity. However, all results are compatible with the restrictions of simply typed lambda calculus.

Definition 1 (Untyped lambda terms)**.** Let $\mathcal{V}$ be an infinite set of variable symbols. We assume that f, g, x, y are disjoint variables in the following formulas. The set of untyped lambda terms is defined as

$$\mathcal{T} ::= \mathcal{V} \mid (\mathcal{T}\,\mathcal{T}) \mid \boldsymbol{\lambda}\mathcal{V}.\,\mathcal{T} \tag{2.1}$$

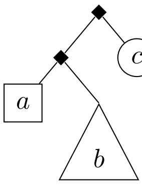

Figure 1: $(\mathsf{pure}\, a \text{ `}\mathsf{ap}\text{` } b) \text{ `}\mathsf{ap}\text{` } \mathsf{term}\, c$ as a tree.

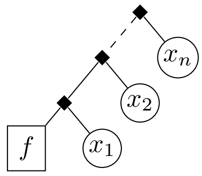

Figure 2: A term in canonical form.

An equivalence relation on $\mathcal{T}$ is a $\mathcal{T}$-congruence iff it is closed under application and abstraction. Let $=_{\alpha\beta\eta}$ be the smallest $\mathcal{T}$-congruence containing α-, β-, and η-conversion. ▲

Definition 2 (Idiomatic terms)**.** The set of idiomatic terms is defined as

$$\mathcal{I} ::= \mathsf{term}\, \mathcal{T} \mid \mathsf{pure}\, \mathcal{T} \mid \mathcal{I} \text{ `}\mathsf{ap}\text{` } \mathcal{I}. \tag{2.2}$$

By convention, the binary operator `ap` associates to the left. An $\mathcal{I}$-congruence is an equivalence relation closed under `ap`. We overload notation and reuse $=_{\alpha\beta\eta}$ for idiomatic terms, where it stands for structural equality modulo substitution of $=_{\alpha\beta\eta}$-equivalent lambda terms. The $\mathcal{I}$-congruence $\simeq$ is induced by the rules

$$x \simeq \mathsf{pure}\, (\boldsymbol{\lambda} x.\, x) \text{ `}\mathsf{ap}\text{` } x \tag{2.3}$$
$$g \text{ `}\mathsf{ap}\text{` } (f \text{ `}\mathsf{ap}\text{` } x) \simeq \mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } g \text{ `}\mathsf{ap}\text{` } f \text{ `}\mathsf{ap}\text{` } x \tag{2.4}$$
$$\mathsf{pure}\, f \text{ `}\mathsf{ap}\text{` } \mathsf{pure}\, x \simeq \mathsf{pure}\, (f\ x) \tag{2.5}$$
$$f \text{ `}\mathsf{ap}\text{` } \mathsf{pure}\, x \simeq \mathsf{pure}\, ((\boldsymbol{\lambda} x.\, \boldsymbol{\lambda} f.\, f\ x)\ x) \text{ `}\mathsf{ap}\text{` } f \tag{2.6}$$
$$s =_{\alpha\beta\eta} t \implies s \simeq t \tag{2.7}$$

where $\mathbf{B}$ abbreviates $\mathbf{B} \equiv \boldsymbol{\lambda} g.\, \boldsymbol{\lambda} f.\, \boldsymbol{\lambda} x.\, g\ (f\ x)$. ▲

term represents arbitrary values in the lifted domain, whereas pure lifts a value. The introduction rules for the relation $\simeq$ are obviously the syntactical counterparts of the applicative laws. Together with symmetry, substitution, etc., they give rise to a simple calculus of equivalence judgements. The intuitive meaning of $s \simeq t$ is that the terms can be used interchangeably. For example, there is a derivation for

$$\mathsf{pure}\, g \text{ `}\mathsf{ap}\text{` } (f \text{ `}\mathsf{ap}\text{` } x) \simeq \mathsf{pure}\, (\mathbf{B}\ g) \text{ `}\mathsf{ap}\text{` } f \text{ `}\mathsf{ap}\text{` } x \tag{2.8}$$

from (2.4), where g is instantied with $\mathsf{pure}\, g$, and a substitution along (2.5) on the right-hand side.

Idiomatic terms are visualized naturally as trees. This will be helpful in explaining term transformations. Figure 1 shows the conventions: Inner nodes correspond to `ap`, leaves are either pure terms (boxes) or opaque terms (circles). Whole subterms may be abbreviated by a triangle. A term has canonical form if it consists of a single pure node to which a number of opaque terms (or none) are applied in sequence. Figure 2 gives a general example. A formal construction follows:

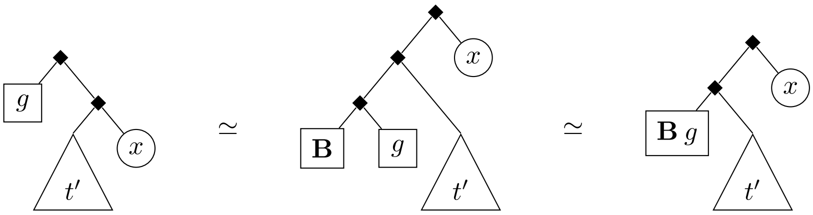

Figure 3: The "pure-rotate" step.

Definition 3 (Canonical form)**.** The set $\mathcal{C} \subset \mathcal{I}$ of idiomatic terms in canonical form is defined inductively as

$$\mathsf{pure}\, x \in \mathcal{C}, \tag{2.9}$$

$$t \in \mathcal{C} \implies t \,\text{`}\mathsf{ap}\text{`}\, \mathsf{term}\, s \in \mathcal{C}. \tag{2.10}$$

▲

It is not entirely obvious how a canonical form can be derived from equations (2.3)–(2.6). Rewriting blindly with these is prone to infinite recursion. Therefore we need a more controlled algorithm. As we have said before, we use *normal form* to refer to the particular canonical form derived from those equations. Consider an idiomatic term t. If t is a single pure term, then it is already in normal form. The case $t = \mathsf{term}\, x$ is also easy: Due to (2.3), we have $t \simeq \mathsf{pure}\,(\boldsymbol{\lambda} x.\, x) \,\text{`}\mathsf{ap}\text{`}\, t$, which is in normal form. But in the case of $t = u \,\text{`}\mathsf{ap}\text{`}\, v$, various steps could be performed, depending on the subterms. We simplify the situation by normalizing each subterm recursively, so we get an equivalent term $u' \,\text{`}\mathsf{ap}\text{`}\, v'$ where $u', v' \in \mathcal{C}$.

Now let us assume that u' is just $\mathsf{pure}\, g$. If v' is also a pure term, they can be combined along (2.5). Otherwise, the term looks like the one on the left of Figure 3. As is shown there, the term tree can be rotated such that one opaque term moves to the outer-most level. This is the same equivalence as stated in (2.8). Because the remaining part again has the shape "pure term applied to normal form", we proceed recursively. In pattern-matching style, the transformation 'pure-nf' reads

$$\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, (f \,\text{`}\mathsf{ap}\text{`}\, x)) = \text{pure-nf}\,(\mathsf{pure}\,(\mathbf{B} g) \,\text{`}\mathsf{ap}\text{`}\, f) \,\text{`}\mathsf{ap}\text{`}\, x \tag{2.11}$$

$$\text{pure-nf}(\mathsf{pure}\, f \,\text{`}\mathsf{ap}\text{`}\, \mathsf{pure}\, x) = \mathsf{pure}\,(f x) \tag{2.12}$$

Lemma 1. *For all $g \in \mathcal{T}$ and $t \in \mathcal{C}$,* $\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t)$ *is well-defined, and*[2] $\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t) \in \mathcal{C} \simeq \mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t$*.*

Proof. We prove all claims simultaneously by induction on $t \in \mathcal{C}$, where g is arbitrary.

Case 1. Assume $t = \mathsf{pure}\, x$ for some $x \in \mathcal{T}$. Only the second equation applies, so we have

$$\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t) = \mathsf{pure}\,(g\, x).$$

All pure terms are in $\mathcal{C}$, and equivalence follows from (2.5).

[2] $a \in S \simeq b$ abbreviates "$a \in S$ and $a \simeq b$".

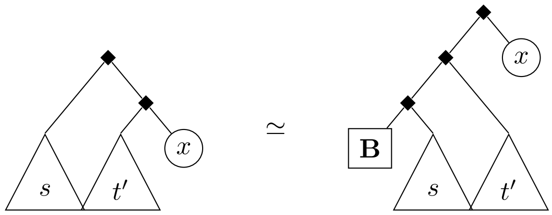

Figure 4: The "rotate" step.

Case 2. Assume $t = t' \,\text{`}\mathsf{ap}\text{`}\, \mathsf{term}\, x$ for some $t' \in \mathcal{C}$, $x \in \mathcal{T}$, and that the hypothesis holds for t' and all g. Only the first equation applies, so

$$\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t) = \text{pure-nf}(\mathsf{pure}\, (\mathbf{B} g) \,\text{`}\mathsf{ap}\text{`}\, t') \,\text{`}\mathsf{ap}\text{`}\, \mathsf{term}\, x.$$

Instantiating the induction hypothesis, we find that

$$\text{pure-nf}(\mathsf{pure}\, (\mathbf{B}\, g) \,\text{`}\mathsf{ap}\text{`}\, t') \in \mathcal{C} \simeq \mathsf{pure}\, (\mathbf{B}\, g) \,\text{`}\mathsf{ap}\text{`}\, t'$$

is well-defined. $\mathcal{C}$ is closed under application to opaque terms (2.10), hence $\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t) \in \mathcal{C}$. Finally, we have

$$\begin{aligned}\text{pure-nf}(\mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t) &\simeq \mathsf{pure}\, (\mathbf{B}\, g) \,\text{`}\mathsf{ap}\text{`}\, t' \,\text{`}\mathsf{ap}\text{`}\, \mathsf{term}\, x \\ &\overset{(2.8)}{\simeq} \mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, (\mathsf{pure}\, t' \,\text{`}\mathsf{ap}\text{`}\, \mathsf{term}\, x) = \mathsf{pure}\, g \,\text{`}\mathsf{ap}\text{`}\, t. \quad \square\end{aligned}$$

Going back to $u' \,\text{`}\mathsf{ap}\text{`}\, v'$, we assumed that u' is a pure term. The case where v' is pure instead can be translated to the former by

$$\text{nf-pure}(f \,\text{`}\mathsf{ap}\text{`}\, \mathsf{pure}\, x) = \text{pure-nf}\,(\mathsf{pure}\, ((\boldsymbol{\lambda} x.\, \boldsymbol{\lambda} f.\, f x)\, x) \,\text{`}\mathsf{ap}\text{`}\, f) \tag{2.13}$$

Lemma 2. *For all $t \in \mathcal{C}$ and $x \in \mathcal{T}$,* $\text{nf-pure}(t \,\text{`}\mathsf{ap}\text{`}\, \mathsf{pure}\, x)$ *is well-defined, and* $\text{nf-pure}(t \,\text{`}\mathsf{ap}\text{`}\, \mathsf{pure}\, x) \in \mathcal{C} \simeq t \,\text{`}\mathsf{ap}\text{`}\, \mathsf{pure}\, x$.

Proof. Follows from Lemma 1 and (2.6). $\square$

Finally, we look at general u', v'. A term rotation is useful again, see Figure 4. Before recursion, we must normalize the subterm $\mathsf{pure}\, \mathbf{B} \,\text{`}\mathsf{ap}\text{`}\, s$. But we already know how to do this: by 'pure-nf'. The base case is reached when v' is a single pure term, which is the domain of 'nf-pure'. The corresponding transformation is therefore

$$\text{nf-nf}(g \,\text{`}\mathsf{ap}\text{`}\, (f \,\text{`}\mathsf{ap}\text{`}\, x)) = \text{nf-nf}\,(\text{pure-nf}\,(\mathsf{pure}\, \mathbf{B} \,\text{`}\mathsf{ap}\text{`}\, g) \,\text{`}\mathsf{ap}\text{`}\, f) \,\text{`}\mathsf{ap}\text{`}\, x \tag{2.14}$$

$$\text{nf-nf}(t) = \text{nf-pure}(t) \quad \text{(otherwise)} \tag{2.15}$$

Lemma 3. *For all $s, t \in \mathcal{C}$,* $\text{nf-nf}(s \,\text{`}\mathsf{ap}\text{`}\, t)$ *is well-defined, and* $\text{nf-nf}(s \,\text{`}\mathsf{ap}\text{`}\, t) \in \mathcal{C} \simeq s \,\text{`}\mathsf{ap}\text{`}\, t$.

Proof. The proof is similar to the one of Lemma 1, by induction on $t \in \mathcal{C}$ and arbitrary $s \in \mathcal{C}$.

Algorithm 1 Normalization of idiomatic terms.

$$\begin{aligned}
\text{normalize}(\mathsf{pure}\, x) &= \mathsf{pure}\, x \\
\text{normalize}(\mathsf{term}\, x) &= \mathsf{pure}\, (\boldsymbol{\lambda} x.\, x) \text{ `}\mathsf{ap}\text{` } \mathsf{term}\, x \\
\text{normalize}(x \text{ `}\mathsf{ap}\text{` } y) &= \text{nf-nf}(\text{normalize}\, x \text{ `}\mathsf{ap}\text{` } \text{normalize}\, y)
\end{aligned}$$

$$\begin{aligned}
\text{nf-nf}(g \text{ `}\mathsf{ap}\text{` } (f \text{ `}\mathsf{ap}\text{` } x)) &= \text{nf-nf}\, (\text{pure-nf}\, (\mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } g) \text{ `}\mathsf{ap}\text{` } f) \text{ `}\mathsf{ap}\text{` } x \\
\text{nf-nf}(t) &= \text{nf-pure}(t) \quad \text{(otherwise)}
\end{aligned}$$

$$\begin{aligned}
\text{pure-nf}(\mathsf{pure}\, g \text{ `}\mathsf{ap}\text{` } (f \text{ `}\mathsf{ap}\text{` } x)) &= \text{pure-nf}\, (\mathsf{pure}\, (\mathbf{B} g) \text{ `}\mathsf{ap}\text{` } f) \text{ `}\mathsf{ap}\text{` } x \\
\text{pure-nf}(\mathsf{pure}\, f \text{ `}\mathsf{ap}\text{` } \mathsf{pure}\, x) &= \mathsf{pure}\, (f x)
\end{aligned}$$

$$\text{nf-pure}(f \text{ `}\mathsf{ap}\text{` } \mathsf{pure}\, x) = \text{pure-nf}\, (\mathsf{pure}\, ((\boldsymbol{\lambda} x.\, \boldsymbol{\lambda} f.\, f x)\, x) \text{ `}\mathsf{ap}\text{` } f)$$

Case 1. Assume $t = \mathsf{pure}\, x$ for some $x \in \mathcal{T}$. The second equation applies, so we have

$$\text{nf-nf}(s \text{ `}\mathsf{ap}\text{` } t) = \text{nf-pure}(s \text{ `}\mathsf{ap}\text{` } \mathsf{pure}\, x).$$

Since $s \in \mathcal{C}$, the claim follows directly from Lemma 2.

Case 2. Assume $t = t' \text{ `}\mathsf{ap}\text{`} \mathsf{term}\, x$ for some $t' \in \mathcal{C}$, $x \in \mathcal{T}$, and that the hypothesis holds for t' and all $s \in \mathcal{C}$. Only the first equation applies,

$$\text{nf-nf}(s \text{ `}\mathsf{ap}\text{` } t) = \text{nf-nf}(\text{pure-nf}(\mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } s) \text{ `}\mathsf{ap}\text{` } t') \text{ `}\mathsf{ap}\text{` } \mathsf{term}\, x.$$

We have $\text{pure-nf}(\mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } s) \in \mathcal{C} \simeq \mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } s$ from Lemma 1. Thus we can instantiate the induction hypothesis, and the transformed term is indeed in normal form. Furthermore,

$$\begin{aligned}
\text{nf-nf}(s \text{ `}\mathsf{ap}\text{` } t) &\overset{\text{(IH)}}{\simeq} \text{pure-nf}(\mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } s) \text{ `}\mathsf{ap}\text{` } t' \text{ `}\mathsf{ap}\text{` } \mathsf{term}\, x \\
&\simeq \mathsf{pure}\, \mathbf{B} \text{ `}\mathsf{ap}\text{` } s \text{ `}\mathsf{ap}\text{` } t' \text{ `}\mathsf{ap}\text{` } \mathsf{term}\, x \\
&\overset{(2.4)}{\simeq} s \text{ `}\mathsf{ap}\text{` } (t' \text{ `}\mathsf{ap}\text{` } \mathsf{term}\, x) = s \text{ `}\mathsf{ap}\text{` } t.
\end{aligned}$$ ☐

Algorithm 1 summarizes all pieces of the normal form transformation. ‘normalize’ is the entry point and performs the main recursion mentioned in the beginning. We haven’t proved the desired property for ‘normalize’ yet, but this is just a straightforward induction.

Lemma 4. *For all* $t \in \mathcal{I}$, normalize t *is well-defined, and* normalize $t \in \mathcal{C} \simeq t$.

Proof. By induction on t, Lemma 3, and equation (2.3). ☐

At this point, we know that it is always possible to obtain a certain canonical form. This is not sufficient to setup the complete proving process, though. We need to learn a bit more about the structure of idiomatic terms and how it relates to lifting.

Definition 4 (Opaque subterms)**.** The sequence of opaque subterms of an idiomatic term is defined by the recursive function

$$\mathrm{opaq}(\mathsf{pure}\,x) = [], \quad \mathrm{opaq}(\mathsf{term}\,x) = [x], \quad \mathrm{opaq}(s \text{ `}\mathsf{ap}\text{` } t) = \mathrm{opaq}\,s @ \mathrm{opaq}\,t.$$

@ denotes concatenation of lists. ▲

Definition 5 (Unlifting)**.** Let t be some idiomatic term, and $n = |\,\mathrm{opaq}\,t|$. Let $v_{i\in\{1..n\}}$ be new variable symbols that do not occur anywhere in t. The "unlifted" lambda term corresponding to t is defined as

$$\downarrow\!t = \boldsymbol{\lambda} v_1.\ \cdots \boldsymbol{\lambda} v_n.\ \mathrm{vary}_1\, t,$$

where

$$\mathrm{vary}_i(\mathsf{pure}\,x) = x, \tag{2.16}$$

$$\mathrm{vary}_i(\mathsf{term}\,x) = v_i, \tag{2.17}$$

$$\mathrm{vary}_i(s \text{ `}\mathsf{ap}\text{` } t) = (\mathrm{vary}_i\, s)\ (\mathrm{vary}_{i+|\,\mathrm{opaq}\,s|}\, t). \tag{2.18}$$

▲

Example 4. The definition of $\downarrow$ may need some explanation. Consider the idiomatic term

$$t \equiv \mathsf{pure}\,f \text{ `}\mathsf{ap}\text{` } x \text{ `}\mathsf{ap}\text{` } (\mathsf{pure}\,g \text{ `}\mathsf{ap}\text{` } y \text{ `}\mathsf{ap}\text{` } z).$$

Its unlifted term is

$$\downarrow\!t = \boldsymbol{\lambda} a.\ \boldsymbol{\lambda} b.\ \boldsymbol{\lambda} c.\ f\ a\ (g\ b\ c).$$

The applicative structure is the same, but all opaque terms have been substituted for new bound variables, which are assigned from left to right. We do not define lifting formally here, but it should be clear that this is some sort of inverse operation, given that variables appear only once. ▲

The interesting properties about these two concepts is that they are preserved by the equivalence relation $\simeq$, and can be directly read from the canonical form. Furthermore, we can leverage them to show the uniqueness of the normal form.

Lemma 5. *For equivalent terms $s \simeq t$, the sequences of opaque terms are equivalent w.r.t $=_{\alpha\beta\eta}$, and $\downarrow\!s =_{\alpha\beta\eta} \downarrow\!t$.*

Proof. (Sketch.) By induction on the relation $s \simeq t$, where we show $\mathrm{vary}_i\, s =_{\alpha\beta\eta} \mathrm{vary}_i\, t$ instead. The index i is arbitrary. The part regarding opaque terms is shown easily for each case: We note that in (2.3)–(2.6), the opaque terms are identical for both sides. By the induction hypothesis, this is also true for the necessary closure rules for symmetry, transitivity, and substitution. It is obvious that (2.7) also preserves opaque terms. Regarding unlifted terms, we have

Case 1. (2.3)

$$\mathrm{vary}_i(\mathsf{pure}\,(\boldsymbol{\lambda} x.\ x) \text{ `}\mathsf{ap}\text{` } x) = (\boldsymbol{\lambda} x.\ x)\ (\mathrm{vary}_i\, x) =_{\alpha\beta\eta} \mathrm{vary}_i\, x.$$

Case 2. (2.4) Let $j = i + |\operatorname{opaq} g|$ and $k = j + |\operatorname{opaq} f|$.

$$\begin{aligned}\operatorname{vary}_i(\mathsf{pure}\,\mathbf{B}\ \text{‘}\mathsf{ap}\text{‘}\ g\ \text{‘}\mathsf{ap}\text{‘}\ f\ \text{‘}\mathsf{ap}\text{‘}\ x) &= \mathbf{B}\ (\operatorname{vary}_i g)\ (\operatorname{vary}_j f)\ (\operatorname{vary}_k g) \\ &=_{\alpha\beta\eta} (\operatorname{vary}_i g)\ ((\operatorname{vary}_j f)\ (\operatorname{vary}_k g)) \\ &= \operatorname{vary}_i(g\ \text{‘}\mathsf{ap}\text{‘}\ (f\ \text{‘}\mathsf{ap}\text{‘}\ x)).\end{aligned}$$

Case 3. (2.5) and (2.6) are similar.

Case 4. (2.7) By induction.

Case 5. Symmetry, transitivity, and substitution: These follow from the induction hypothesis and the corresponding properties of $=_{\alpha\beta\eta}$.

□

Lemma 6. *Let* $\mathsf{pure}\, f$ *be the single pure term in* $t \in \mathcal{C}$. *Then* $f =_{\alpha\beta\eta} {\downarrow}t$.

Proof. By induction on $\mathcal{C}$. The base case is trivial. For the step case, we need to prove that

$$f' =_{\alpha\beta\eta} \big\downarrow(g\ \text{‘}\mathsf{ap}\text{‘}\ \mathsf{term}\, x) = \boldsymbol{\lambda} v_1.\ \ldots \boldsymbol{\lambda} v_n.\ \boldsymbol{\lambda} v_{n+1}.\ (\operatorname{vary}_1 g)\ v_{n+1},$$

where $\mathsf{pure}\, f'$ is the single pure term in g, $n = |\operatorname{opaq} g|$, and v_i are new variables. The right-hand side can be eta-reduced to

$$\boldsymbol{\lambda} v_1.\ \ldots \boldsymbol{\lambda} v_n.\ (\operatorname{vary}_1 g) = {\downarrow}g\ .$$

From the induction hypothesis we get $f' =_{\alpha\beta\eta} {\downarrow}g$, which concludes the proof. □

This lemma is why we need eta-equivalence and not just use $=_{\alpha\beta}$. In fact, we can find a counterexample of equivalent canonical forms that do not agree in the pure function if $\rightarrow_\eta$ is not available:

$$\mathsf{pure}\,(\boldsymbol{\lambda} x.\ x)\ \text{‘}\mathsf{ap}\text{‘}\ (\mathsf{pure}\, f\ \text{‘}\mathsf{ap}\text{‘}\ x) \simeq \mathsf{pure}\, f\ \text{‘}\mathsf{ap}\text{‘}\ x \simeq \mathsf{pure}\,(\boldsymbol{\lambda} x.\ f\ x)\ \text{‘}\mathsf{ap}\text{‘}\ x.$$

The middle term is derived from (2.3), the latter from (2.4).

Corollary 1. *The normal form is structurally unique. Formally, if* $s, t \in \mathcal{C}$ *and* $s \simeq t$, *then* $s =_{\alpha\beta\eta} t$.

Now we have all tools ready to complete the picture. The following theorem shows that (limited) lifting is possible with just the applicative laws. Its proof hints towards the implementation in Isabelle, which is of course based on the normal form: Under the condition that the opaque terms are equivalent, normalizing two idiomatic terms reduces the problem to the “unlifted” terms.

Theorem 1. *Let* $s, t \in \mathcal{I}$ *with* $\operatorname{opaq} s =_{\alpha\beta\eta} \operatorname{opaq} t$. *If* ${\downarrow}s =_{\alpha\beta\eta} {\downarrow}t$ *(the base equation), then* $s \simeq t$.

Proof. From Lemma 4 we obtain normal forms $s' \simeq s$ and $t' \simeq t$. With the base equation and Lemma 5 we get $\big\downarrow s' =_{\alpha\beta\eta} \big\downarrow t'$. By Lemma 6 and the condition on the opaque subterms, it follows that $s' =_{\alpha\beta\eta} t'$ and further $s \simeq t$. □

3 Lifting with Combinators

3.1 Motivation

The normalization approach to solving lifted equations works only if the opaque terms on both sides coincide. This is not true for all equations of interest. Let's revisit the set version of addition of natural numbers, $\oplus$ from Example 1. This operator is also commutative, so it should be possible to prove

$$X \oplus Y = Y \oplus X.$$

After unfolding and normalization, we get

$$\mathit{pure}\,(\lambda xy.\, x + y) \diamond X \diamond Y = \mathit{pure}\,(\lambda yx.\, y + x) \diamond Y \diamond X. \tag{3.1}$$

Clearly, this can't be solved with a standard congruence rule, because we would have to to prove that X is equal to Y. Since we are concerned with transferring properties from a base domain, we don't want to assume anything about those opaque subterms, which may carry additional information of the functor. Note that the arguments of both *pure* terms are actually the same function $(+)$, so we can't even make use of the base equation there. Expressed as an equality of functions, it reads

$$\lambda xy.\, x + y = \lambda xy.\, y + x.$$

The left-hand side is an eta-expanded from of $(+)$, while the other has the arguments reversed. We can use the flip function, defined as $\mathrm{flip}\, f x y = f y x$, to write it consistently in point-free style: $(+) = \mathrm{flip}\,(+)$. From this one derives

$$\mathit{pure}\,(+) \diamond X \diamond Y = \mathit{pure}\,\mathrm{flip} \diamond \mathit{pure}\,(+) \diamond X \diamond Y. \tag{3.2}$$

Now it would be very convenient if the defining equation of flip can be lifted, that is

$$\mathit{pure}\,\mathrm{flip} \diamond f \diamond x \diamond y = f \diamond y \diamond x. \tag{3.3}$$

And indeed, this is true for the set idiom! The term $\mathit{pure}\,(\mathrm{flip}\,(+)) \diamond X \diamond Y$, which is equivalent to the right-hand side of (3.2), is not the canonical normal form of $Y \oplus X$. Yet the overall structure is similar: a pure function applied to some opaque arguments. The availability of equation (3.3) is a quite powerful condition, because it will allow us to permute opaque terms freely.[3] If permutations exist such that both sides of the (transformed) equation align regarding their opaque terms, reduction by congruence is possible again. Furthermore, the effect of rewriting with the flip function in one domain can be reversed in the other. This guarantees that the corresponding base equation is always applicable.

As opposed to $\lambda yx.\, y + x$, the term $\mathrm{flip}\,(+)$ does not contain any lambda abstractions or bound variables. Being able to express terms this way is the general idea behind *combinators* from combinatory logic. These are certain functions with characteristic defining equations, and using them in terms eliminates the need for explicit naming of variables. In this context, flip is usually referred to as combinator **C**, which is the name we will use in the following. We have

[3] Strictly speaking, a weaker property with $\mathit{pure}\, f$ instead of f is sufficient for this example. Section 3.3 attempts to give a rationale why the "full" property is desirable.

Symbol	Reduction
$\mathbf{B}$	$\mathbf{B}xyz = x(yz)$
$\mathbf{I}$	$\mathbf{I}x = x$
$\mathbf{C}$	$\mathbf{C}xyz = xzy$
$\mathbf{K}$	$\mathbf{K}xy = x$
$\mathbf{W}$	$\mathbf{W}xy = xyy$
$\mathbf{S}$	$\mathbf{S}xyz = xz(yz)$
$\mathbf{H}$	$\mathbf{H}xyz = xy(zy)$

Table 1: Useful combinators.

already used different combinators extensively: $\mathbf{B}$ and $\mathbf{I} = \lambda x.\, x$. Both can be lifted in each idiom due to the composition and identity laws. We say that the combinators $\mathbf{B}$ and $\mathbf{I}$ *exist* in each idiom. Table 1 lists all combinators which are used throughout this text.

There are certain sets of combinators which are sufficient to express all lambda terms, $\{\mathbf{S}, \mathbf{K}\}$ being one of them. Hinze's Lifting Lemma shows that all terms and thus all equations can be lifted if $\mathbf{S}$ and $\mathbf{K}$ exist. He also notes that other combinator set are useful, because there are idioms where more than $\{\mathbf{B}, \mathbf{I}\}$, but not all combinators exist. In this section we present an implementation of this generalized lifting for solving a broader class of equation than with normalization. The abstract concept works with arbitrary combinators. It depends on an abstraction algorithm and the structure of representable terms, which are difficult to derive automatically. Therefore we will restrict ourselves to certain sets ("bases") with hard-coded algorithms.

3.2 Algorithm Outline

The high-level method of proof is the same as with the one based on plain normalization: Rewriting both sides of the equation, stripping equal terms by congruence and finally resolving with the base equation. The generalized approach differs in the rewriting step: With additional combinators, the normal form of a given idiomatic term is not necessarily unique.

We will first discuss how one goes from the base equation to its lifted form. In general, the base equation looks like this:

$$\forall \vec{x}.\, s[\vec{x}] = t[\vec{x}],$$

where $u[\vec{x}]$ means that variables $\vec{x}$ may occur freely in u. By function extensionality, which is an axiom of HOL, this is true iff

$$\lambda \vec{x}.\, s[\vec{x}] = \lambda \vec{x}.\, t[\vec{x}].$$

Now we attempt to translate both terms to their combinator representation, using those combinators which exists for the idiom we are working with. The exact process depends on the combinator set, and may also fail if a term is not representable with that set. The details are discussed in the next section. Let s' and t' be the translated terms. Each can be viewed as an function application tree of some atomic terms. We derive $\mathit{pure}_f\, s' = \mathit{pure}_f\, t'$ by simple substitution. This is an equation of functions of type

$$\tau_1 f \Rightarrow \cdots \Rightarrow \tau_n f \Rightarrow \sigma f,$$

Base	Example idioms
BI	state, list
BIC	set
BIK	
BIW	either
BCK	
BKW	
BICW	maybe
BCKW	stream, $\alpha \rightarrow$

Table 2: Substructures of BCKW.

with τ_i is the type of x_i, and σ is the type of $s[\vec{x}]$. It follows that

$$\forall \vec{y}.\ \mathit{pure}\, s' \diamond y_1 \diamond \cdots \diamond y_n = \mathit{pure}\, t' \diamond y_1 \cdots \diamond y_n.$$

The type of y_i is $\tau_i f$. The homomorphism law allows us to distribute *pure* over the applications in s' and t', which makes it possible to unfold all lifted combinators. For example, a subterm

$$\mathit{pure}\, \mathbf{S} \diamond \mathit{pure}\, f \diamond x \diamond y$$

gets rewritten to $\mathit{pure}\, f \diamond y \diamond (x \diamond y)$. The result is the lifted equation (modulo splitting/joining of adjacent *pure*s), because the combinators capture the term–variable structure and transfer it to the idiom.

However, a user should able to use the proof method without supplying the base equation beforehand. To do this, the procedure we have just described is essentially done backwards. (The direction of logical implication remains the same, though.) This may cause some issues if the proof goal cannot be represented using the available combinators, but is an instantiation of a more general proposition which can be proven. An example is

$$X \oplus (X \oplus Y) = (X \oplus X) \oplus Y.$$

We want this to be handled automatically, if possible. In terms of above presentation, the algorithm has to determine the variables $\vec{y}$ and find an assignment of all opaque terms to this variables, such that the proof goes through.

3.3 Combinator Bases

To do.

References

[1] Ralf Hinze. “Lifting Operators and Laws”. 2010. URL: `http://www.cs.ox.ac.uk/ralf.hinze/Lifting.pdf` (visited on June 6, 2015).

[2] Conor McBride and Ross Paterson. “Applicative Programming with Effects”. In: *Journal of Functional Programming* 18.01 (2008), pp. 1–13.

[3] Martin Wildmoser and Tobias Nipkow. “Certifying Machine Code Safety: Shallow Versus Deep Embedding”. In: *Theorem Proving in Higher Order Logics*. Ed. by Konrad Slind, Annette Bunker, and Ganesh Gopalakrishnan. Vol. 3223. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, pp. 305–320.