THE ROYAL
SWEDISH
ACADEMY OF
SCIENCES

INSTITUT
MITTAG-LEFFLER

Auravägen 17, SE-182 60 Djursholm, Sweden
Tel. +46 8 622 05 60 Fax. +46 8 622 05 89
info@mittag-leffler.se www.mittag-leffler.se

Remarks on the relation between families of setoids and identity in type theory

E. Palmgren

REPORT No. 36, 2009/2010, fall

ISSN 1103-467X
ISRN IML-R- -36-09/10- -SE+fall

Remarks on the relation between families of setoids and identity in type theory

Erik Palmgren *

March 26, 2010

1 Introduction

In set theories, such as ZF or its constructive version CZF, a family of sets may always be represented as a function $\beta : B \to A$. Its fibers $B_x = \beta^{-1}(x) = \{b \in B : \beta(b) = x\}$, for $x \in A$, represent the sets of the family. This representation is always possible by the replacement scheme, since any family specified by a set-theoretic formula $\varphi(x, F)$

$$(\forall x \in A)(\exists! F)\varphi(x, F)$$

can be turned into a family represented by a function. This can be contrasted to Martin-Löf type theory [10], and other theories of dependent types, where a family of types is a basic mathematical object. Following the tradition in constructive mathematics (see [2]) a set is commonly understood in type theory as a setoid, that is, a type together with an equivalence relation. However the notion of a family of setoids present some choices for conceptualisation. In this note we consider two choices, so-called proof-irrelevant and proof-relevant families (see [3]), and their relation to the identity types of Martin-Löf. As shown by Streicher [12] and Hofmann and Streicher [6] an important distinction regarding identity types is whether their proof-objects are unique or not. In the former case a proof-irrelevant family of setoids can always be associated to each family of types. In the latter case a more involved proof-relevant notion of family of setoids seems be necessary to use; see Theorems 4.1 and 4.3. The distinction between proof-relevant and proof-irrelevant does not appear in classical set-theoretic models of Martin-Löf type theory, in view of a result by Hedberg [5] on uniqueness of identity proof-objects (UIP). We present a slight strengthening of this result in Section 6. In Section 7 we address the question whether there is a natural axiomatisation of general UIP by presenting a new elimination rule for identity types.

*Supported by a grant from the Swedish Research Council (VR).

2 Families of setoids

A *setoid* $B = (|B|, =_B)$ consists of a type $|B|$ and an equivalence relation, $=_B$, on the type. An extensional function between two setoids is taken to be a function between underlying types that respects the equivalence relations. If $B_x = (|B_x|, =_{B_x})$ are setoids indexed by a type $x : |A|$, there seems to be two principal choices how to extend this into a family indexed by a setoid. Suppose the type $|A|$ is equipped with an equivalence relation, $=_A$. Each proof $p : x =_A y$ should give rise to an extensional "reindexing" bijection $\phi_p : B_x \to B_y$. Starting from a set-theoretic intuition it is natural to require the following equalities of extensional functions to hold (see [2, Problem 3.2])

(i) $\phi_p =_{\text{ext}} \text{id}_{B_x}$ whenever $p : (x =_A x)$,

(ii) $\phi_q \circ \phi_p =_{\text{ext}} \phi_r$, whenever $p : (x =_A y), q : (y =_A z), r : (x =_A z)$.

Together the two conditions (i) and (ii), implies that the proof p is irrelevant, only its existence matter, i.e. $\phi_p =_{\text{ext}} \phi_q$ for any $p : x =_A y$ and $q : x =_A y$. This is the standard *proof-irrelevant* version of family of setoid, and seems to be the most widely used notion. The other principal version is the *proof-relevant* family, where ϕ_p may depend on p. Conditions (i) and (ii) are replaced by (a) – (d):

(a) $\phi_{\text{ref}(x)} =_{\text{ext}} \text{id}_{B_x}$

(b) $\phi_{\text{trans}(q,p)} =_{\text{ext}} \phi_q \circ \phi_p$ for $p : x =_A y$ and $q : y =_A z$

(c) $\phi_{\text{sym}(p)} \circ \phi_p =_{\text{ext}} \text{id}_{B_x}$ for $p : x =_A y$,

(d) $\phi_p \circ \phi_{\text{sym}(p)} =_{\text{ext}} \text{id}_{B_y}$ for $p : x =_A y$.

Here $\text{ref}(x) : x =_A x$ is a proof object for reflexivity. Moreover the proof objects associated with symmetry and transitivity are $\text{sym}(p) : y =_A x$, for $p : x =_A y$, and $\text{trans}(q, p) : x =_A z$ for $p : x =_A y$ and $q : y =_A z$.

We note that $\phi_p : B_x \to B_x$ is an automorphism on B_x for each $p : x =_A x$. There may be non-trivial automorphism, i.e. other than the identity map. If we add proof-irrelevance

(Irr) $\phi_p =_{\text{ext}} \phi_q$ for any $p : x =_A y$ and $q : x =_A y$.

to (a) – (d) then (i) and (ii) follows, and clearly there are then only trivial automorphisms.

Example. As motivation for the standard proof-irrelevant version of family, consider the construction of a category $\mathcal{B}$ of setoids with equality on objects. (Compare to the axiomatisation of categories in [7, Section 5.5]). Let (B, ϕ) be a family of setoids indexed by the setoid A. The collection of objects of the category $\mathcal{B}$ is the setoid A. We think of an element a of A as code for the setoid B_a. An arrow of the category is a triple (a, f, b) where $a, b : |A|$ and $f : B_a \longrightarrow B_b$ is an extensional function. Two arrows (a, f, b) and (a', f', b') are equivalent if there are $p : a =_A a'$ and $q : b =_A b'$ so that

$$\begin{array}{ccc} B_a & \xrightarrow{f} & B_b \\ {\scriptstyle \phi_p}\downarrow & & \downarrow{\scriptstyle \phi_q} \\ B_{a'} & \xrightarrow[f']{} & B_{b'} \end{array}$$

commutes (extensionally). Arrows (a, f, b) and (c, g, d) are composable if there is $t : b =_A c$. Their composition is $(a, g \circ \phi_t \circ f, d)$. Now a problem arises when proving that composition respects equality of arrows: suppose that (a, b, f) and (a', b', f') are equivalent, and that (c, g, d) and (c', g', d') are equivalent so that the left and right squares in the following diagram commute:

$$\begin{array}{ccccccc} B_a & \xrightarrow{f} & B_b & \xrightarrow{\phi_t} & B_c & \xrightarrow{g} & B_d \\ {\scriptstyle \phi_p}\downarrow & & \downarrow{\scriptstyle \phi_q} & & \downarrow{\scriptstyle \phi_r} & & \downarrow{\scriptstyle \phi_s} \\ B_{a'} & \xrightarrow[f']{} & B_{b'} & \xrightarrow[\phi_{t'}]{} & B_{c'} & \xrightarrow[g']{} & B_{d'} \end{array}$$

Suppose moreover that $t : b =_A c$ and $t' : b' =_A c'$. If we have a proof-irrelevant family the centre square commutes automatically, proving that composition respects equality of arrows. This is in general impossible if the family is proof-relevant.

3 Identity types

We shall here follow the presentation of Martin-Löf type theory given in [10]. However we shall use the older terminology of *type* for which is now called a *set*, and *large type* or *Type* for what is now called just *type*. The identity type construction provides for each type A a minimal equivalence relation $\mathrm{I}(A, \cdot, \cdot)$ on A. This makes $(A, \mathrm{I}(A, \cdot, \cdot))$ a projective object (cf. [8]) in the category of setoids.

For any type A of type theory the identity type $\mathrm{I}(A, a, b)$ is the set of proofs that a and b are propositionally equal in A. The formation rule for the identity type is that $\mathrm{I}(A, a, b)$ is a type if A is a type and $a, b : A$. We shall also write $\mathrm{I}_A(a, b)$, or even $\mathrm{I}(a, b)$, for $\mathrm{I}(A, a, b)$ if this should appear typographically clearer. The introduction rule is

$$\frac{a : A}{\mathrm{r}(a) : \mathrm{I}(A, a, a)}.$$

The elimination rule for I with respect to the family $C(x, y, z)$ type $(x, y : A, z : \mathrm{I}(A, x, y))$ is

$$\frac{a, b : A \qquad c : \mathrm{I}(A, a, b) \qquad d(x) : C(x, x, r(x))\ (x : A)}{\mathrm{J}_{C,a,b}(c, d) : C(a, b, c)}. \tag{1}$$

The associated computation rule is $\mathrm{J}_{C,a,a}(\mathrm{r}(a), d) = d(a)$. A typical use is to derive a rule for substituting equals for equals in a proposition, or equivalently, derive a reindexing operation for families. For $B(x)$ type $(x : A)$, define $C(x, y, z) = B(x) \to B(y)$. Then $d(x) = \mathrm{id}_{B(x)} = \lambda p : B(x).p : C(x, x, \mathrm{r}(x))$. Hence for $c : \mathrm{I}(A, a, b)$

$$\mathrm{J}_{C,a,b}(c, (x)\mathrm{id}_{B(x)}) : C(a, b, c) = B(a) \to B(b). \tag{2}$$

Define

$$\mathrm{R}_{B,a,b}(c, q) = \mathrm{J}_{C,a,b}(c, (x)\mathrm{id}_{B(x)})(q) : B(b)$$

for $q : B(a)$. Clearly $\mathrm{R}_{B,a,a}(\mathrm{r}(a), q) = q$.

A very useful elimination rule, equivalent to the standard one (1), is the rule of Paulin-Mohring [12]. It says that for any parameter $a : A$ and any family $D(x, z)$ type $(x : A, z : \mathrm{I}(A, a, x))$ if

$$\frac{b : A \qquad c : \mathrm{I}(A, a, b) \qquad d : D(a, r(a))}{\mathrm{J}'_{a,D,b}(c, d) : D(b, c)} \tag{3}$$

The computation rule is $\mathrm{J}'_{a,D,a}(r(a), d) = d$.

The identity proofs of A are unique in case

$$(\forall z, w : \mathrm{I}_A(a, b))\mathrm{I}(z, w) \qquad\qquad (\mathrm{UIP}_A) \tag{4}$$

holds. We say that UIP holds if for each type A satisfies UIP_A. Hofmann and Streicher [6] showed that this need not hold for general types by exhibiting a groupoid model of type theory. The structure of identity types is thus more complicated than might have been expected. In fact they showed that using the standard elimination rule one constructs operations for proofs of symmetry and transitivity

$c^{-1} : \mathrm{I}(A, b, a) \qquad (a, b : A, c : \mathrm{I}(A, a, b)),$

where $c^{-1} = J_{C,a,b}(c, \mathrm{r})$ and $C(x, y, z) = \mathrm{I}(A, y, x)$,

$w \circ z : \mathrm{I}(A, a, u) \qquad (a, b, u : A, z : \mathrm{I}(A, a, b), w : \mathrm{I}(A, b, u)),$

where $w \circ z = \mathrm{J}_{C,a,b}(z, d)(w)$, $C(x, y, z') = \mathrm{I}(A, y, u) \to \mathrm{I}(A, x, u)$ and $d(x) = \mathrm{id}_{\mathrm{I}(A,x,u)}$.

These operations satisfy the *groupoid laws* with $\mathrm{id}_x =_{\mathrm{def}} \mathrm{r}(x)$ as identity in the sense that the following identity statements hold:

(G1) $\mathrm{I}(\mathrm{id}_y \circ z, z)$ for $z : I(A, x, y)$,

(G2) $\mathrm{I}(z \circ \mathrm{id}_x, z)$ for $z : I(A, x, y)$,

(G3) $\mathrm{I}(z \circ z^{-1}, \mathrm{id}_y)$ for $z : I(A, x, y)$,

(G4) $\mathrm{I}(z^{-1} \circ z, \mathrm{id}_x)$ for $z : I(A, x, y)$,

(G5) $\mathrm{I}((z \circ w) \circ p, z \circ (w \circ p))$ for $p : I(A, x, y)$, $w : I(A, y, u)$, $z : I(A, u, v)$.

The type-theoretic version of a groupoid is an E-category where all morphisms are invertible. To be explicit: A *groupoid* $A = (|A|, \mathrm{Hom}, \mathrm{id}, \circ, (\ )^{-1})$ consists of

(1) a type $|A|$,

(2) a setoid $\mathrm{Hom}(a, b)$ of morphisms for any $a, b : |A|$,

(3) an identity morphism $\mathrm{id}_a \in \mathrm{Hom}(a, a)$ for each $a : |A|$,

(4) a composition operation $\circ : \mathrm{Hom}(b, c) \times \mathrm{Hom}(a, b) \longrightarrow \mathrm{Hom}(a, c)$ for all $a, b, c : |A|$,

(5) an inversion $(\ )^{-1} : \mathrm{Hom}(a, b) \longrightarrow \mathrm{Hom}(b, a)$ for $a, b : |A|$,

satisfying the usual identities. From (G1-G5) above follows that each type A yields a groupoid $A^\star = (A, \mathrm{Hom}, \mathrm{id}, \circ, (\ )^{-1})$ where $\mathrm{Hom}(a, b) = (\mathrm{I}(A, a, b), \mathrm{I}_{\mathrm{I}(A,a,b)}(\cdot, \cdot))$.

4 Families of setoids induced by families of types

For a family of types $B : (A)\mathrm{type}$ define $A^* = (A, \mathrm{I}(A, \cdot, \cdot))$ and $B^*(a) = (B(a), \mathrm{I}(B(a), \cdot, \cdot))$ and define $\phi_p : B(a) \to B(b)$, by $\phi_p(x) = \mathrm{R}_{B,a,b}(p, x)$. The reindexing operation R is functorial in the sense that

(R1) $\mathrm{I}(\mathrm{R}_{B,a,a}(\mathrm{r}(a), w), w)$ holds for $a : A$, $w : B(a)$,

(R2) $\mathrm{I}(\mathrm{R}_{B,b,c}(t, \mathrm{R}_{B,a,b}(z, w)), \mathrm{R}_{B,a,c}((t \circ z), w))$ holds for $a, b, c : A$ and $z : \mathrm{I}(A, a, b)$ and $t : \mathrm{I}(A, b, c)$ and $w : B(a)$.

We shall also write B^*_p for ϕ_p. I-elimination gives

$$\mathrm{I}(\mathrm{I}(A, a, b), p, q) \Longrightarrow B^*_p =_{\mathrm{ext}} B^*_q.$$

The groupoid laws G1 – G5 gives with ref(x) $= \mathrm{id}_x$, $\mathrm{sym}(p) = p^{-1}$ and $\mathrm{trans}(q, p) = q \circ p$ the following theorem:

Theorem 4.1 *For any family of types* $B : (A)\mathrm{type}$ *the construction* (A^*, B^*) *is a proof-relevant family of setoids.* □

We give a condition on the index setoid of this family, in order for the family to be proof-irrelevant. For this we use that in a special case the reindexing operation is a composition operation:

Lemma 4.2 *For* $u : A$ *and* $B(x) = \mathrm{I}(A, u, x)$, *we have*

$$\mathrm{I}(\mathrm{R}_{B,a,b}(z, v), z \circ v)$$

for $z : \mathrm{I}(A, a, b)$ *and* $v : \mathrm{I}(A, u, a)$.

Proof. Let $C(a, b, z)$ be the formula

$$(\forall v : \mathrm{I}(A, u, a))\mathrm{I}_{B(b)}(\mathrm{R}_{B,a,b}(z, v), z \circ v).$$

Now $C(a, a, r(a))$ is

$$(\forall v : \mathrm{I}(A, u, a))\mathrm{I}_{B(a)}(\mathrm{R}_{B,a,a}(\mathrm{r}(a), v), \mathrm{r}(a) \circ v),$$

which by the groupoid laws and $\mathrm{R}_{B,a,a}(\mathrm{r}(a), q) = q$ is equivalent to

$$(\forall v : \mathrm{I}(A, u, a))\mathrm{I}_{B(a)}(v, v).$$

But this follows by the reflexivity law, so by I-elimination $C(a, b, z)$ is true. Hence the lemma is proved. □

Theorem 4.3 *Let* $A : \mathrm{type}$ *be fixed. Then UIP holds for* A *if and only if* (A^*, B^*) *is a proof-irrelevant family of setoids, for any family* $B : (A)\mathrm{type}$.

Proof. In view of Theorem 4.1 we may concentrate on the condition (Irr) for proof-irrelevance.

(⇒): Assume that UIP holds for A. For $p, p' : \mathrm{I}(A, a, b)$ there is $c : \mathrm{I}(\mathrm{I}(A, a, b), p, p')$. Let

$$C(u, v, z) = (\forall x : B(a))(B^*_u(x) =_{B(b)} B^*_v(x)),$$

where $u, v : \mathrm{I}(A, a, b)$. Clearly, $C(u, u, \mathrm{r}(u))$ is inhabited since $=_{B(b)}$ is reflexive. Hence by the elimination rule for I, we get that $C(p, p', c)$ is true, which says that B^* is proof irrelevant.

(⇐): Suppose that (A^*, B^*) is a family of setoids, for any $B : (A)\mathrm{type}$. Fix $a : A$, and let $B(x) = \mathrm{I}(A, a, x)$. Then condition (Irr) for B^* is that

$$\mathrm{I}(\mathrm{I}(A, a, b), B^*_p(q), B^*_{p'}(q)) \tag{5}$$

holds for $a, b : A$, $p, p' : \mathrm{I}(A, a, b)$, $q : \mathrm{I}(A, a, a)$. Now by Lemma 4.2 and $B^*_p(q) = \mathrm{R}_{B,a,b}(p, q)$ the equation (5) is equivalent to

$$\mathrm{I}(\mathrm{I}(A, a, b), p \circ q, p' \circ q).$$

Putting $q = \mathrm{r}(b)$, we get $\mathrm{I}(\mathrm{I}(A, a, b), p \circ \mathrm{r}(b), p' \circ \mathrm{r}(b))$, and since $\mathrm{r}(b)$ is the identity of the groupoid, we have $\mathrm{I}(\mathrm{I}(A, a, b), p, p')$ for all $p, p' : \mathrm{I}(A, a, b)$. That is UIP holds for A. □

5 Families of setoids induced by fibers of maps.

Analogous to set theory, we may present a family of setoids in type theory via fibers of functions $f : S \to A$ between setoids. Define the *fiber of f over a* as the setoid

$$f^{-1}(a) =_{\text{def}} ((\Sigma z : S)(f(z) =_A a), \sim),$$

where $(z, p) \sim (z', p')$ holds if and only if $z =_S z'$. For $q : a =_A b$ let $f^{-1}(q) : f^{-1}(a) \to f^{-1}(b)$ be given by

$$f^{-1}(q)(z, p) = (z, q \circ p).$$

This clearly defines a proof-irrelevant family of setoids.

Using the UIP it is possible to obtain each family (B^*, A^*) as fibers of a certain projection function $\pi_1 : S \longrightarrow A^*$. For this we need a lemma about identity types.

Lemma 5.1 *On a sigma type $S = (\Sigma x : A)B(x)$, the I-equality is characterised by*

$$\mathrm{I}(S, (a, b), (a', b')) \Longleftrightarrow (\exists p : \mathrm{I}(A, a, a'))\mathrm{I}(B(a'), \mathrm{R}_{B,a,a'}(p, b), b').$$

Proof. ($\Leftarrow$) We show that $(\forall a, a' : A)(\forall p : \mathrm{I}(A, a, a'))C(a, a', p)$ where

$$C(a, a', p) = (\forall b : B(a))(\forall b' : B(a'))[\mathrm{I}(B(a'), \mathrm{R}_{B,a,a'}(p, b), b') \to \mathrm{I}(S, (a, b), (a', b'))].$$

By I-elimination it suffices to show $C(a, a, \mathrm{r}(a))$ which using $\mathrm{R}_{B,a,a}(\mathrm{r}(a), b) = b$ is

$$(\forall b : B(a))(\forall b' : B(a))[\mathrm{I}(B(a), b, b') \to \mathrm{I}(S, (a, b), (a, b'))].$$

But this follows by another application of I-elimination.

($\Rightarrow$) By Σ-elimination we find for $z : S$ terms $\pi_1(z) : A$ and $\pi_2(z) : B(\pi_2(z))$ so that $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$. For $z, z' : S$ and $q : \mathrm{I}(S, z, z')$, let $C(z, z', q)$ be

$$(\exists p : \mathrm{I}(A, \pi_1(z), \pi_1(z')))\mathrm{I}(B(\pi_1(z')), \mathrm{R}_{B,\pi_1(z),\pi_1(z')}(p, \pi_2(z)), \pi_2(z')).$$

By I-elimination it is sufficient to prove $C(z, z, \mathrm{r}(z))$ for all $z : S$. By Σ-elimination it is enough that $C((a, b), (a, b), \mathrm{r}(a, b))$ holds, i.e.

$$(\exists p : \mathrm{I}(A, a, a))\mathrm{I}(B(a), \mathrm{R}_{B,a,a}(p, b), b).$$

This can be achieved by letting $p = \mathrm{r}(a)$ and using $\mathrm{R}_{B,a,a}(\mathrm{r}(a), b) = b$ and I-introduction. Consequently, if $q : \mathrm{I}(S, (a, b), (a', b'))$, then $C((a, b), (a', b'), q)$ which was desired. □

Theorem 5.2 *Let A be a fixed type. For a family $B : (A)$type, let $S = (\Sigma x : A)B(x)$ and let $\pi_1 : S^* \to A^*$ be the first projection. For each $a : A$ define $\theta_a : \pi_1^{-1}(a) \to B(a)^*$ by letting*

$$\theta_a((u, v), p) = \mathrm{R}_{B,u,a}(p, v).$$

Then θ_a is a well-defined bijection for any $a : A$ and any choice of $B : (A)$type if and only if A satisfies UIP.

Proof. ($\Leftarrow$): Assume that A satisfies UIP. Suppose $((u,v),p)$ and $((u',v'),p')$ are equal in $\pi_1^{-1}(a)$. Thus $p : \mathrm{I}(A,u,a)$, $p' : \mathrm{I}(A,u',a)$ and $\mathrm{I}(S,(u,v),(u',v'))$ holds. By Lemma 5.1 follows that there is some $q : \mathrm{I}(A,u,u')$ with $\mathrm{I}(B(u'),\mathrm{R}_{B,u,u'}(q,v),v')$. Thus $\mathrm{I}(B(a),\mathrm{R}_{B,u',a}(p',(\mathrm{R}_{B,u,u'}(q,v)),\mathrm{R}_{B,u',a}(p',v'))$. By functoriality

$$\mathrm{I}(B(a),\mathrm{R}_{B,u,a}(p'\circ q,v),\mathrm{R}_{B,u',a}(p',v')).$$

But UIP for A gives that $\mathrm{I}(A,p'\circ q,p)$ holds, and hence by I-elimination we have that

$$\mathrm{I}(B(a),\mathrm{R}_{B,u,a}(p,v),\mathrm{R}_{B,u',a}(p',v')) \tag{6}$$

holds, thus proving θ_a well-defined. Suppose (6) where $p : \mathrm{I}(A,u,a)$ and $p' : \mathrm{I}(A,u',a)$. Hence $(p')^{-1}\circ p : \mathrm{I}(A,u,u')$ and applying $\mathrm{R}((p')^{-1},\cdot)$ to (6) we obtain by functoriality and (G4)

$$\mathrm{I}(B(a),\mathrm{R}_{B,u,u'}((p')^{-1}\circ p,v),v').$$

Hence by Lemma 5.1,

$$\mathrm{I}(S,(u,v),(u',v')).$$

Thus θ_a is injective. To prove surjectivity, let $b : B(a)$ and consider $\theta_a((a,b),\mathrm{r}(a)) = \mathrm{R}_{B,a,a}(\mathrm{r}(a),b) = b$. Thus θ_a is a well-defined bijection.

($\Rightarrow$): Suppose that θ_a is a well-defined bijection for each choice of B, and any $a : A$. Let $a,b : A$ be fixed. Define $B(x) = \mathrm{I}(A,a,x)$. Let $z : B(b)$ and $w : B(b)$. Hence $p = w\circ z^{-1} : \mathrm{I}(A,b,b)$. Then $\mathrm{I}(B(b),p\circ z,w)$ holds. But $\mathrm{I}(B(b),\mathrm{R}_{B,b,b}(p,z),p\circ z)$ by Lemma 4.2, and hence $\mathrm{I}(B(b),\mathrm{R}_{B,b,b}(p,z),w)$. It follows by Lemma 5.1 that $\mathrm{I}(S,(b,z),(b,w))$, and hence that $((b,z),\mathrm{r}(b))$ and $((b,w),\mathrm{r}(b))$ are equal in $\pi_1^{-1}(b)$. Now θ_b is well-defined, so $\mathrm{I}(B(b),\theta_b((b,z),\mathrm{r}(b)),\theta_b((b,w),\mathrm{r}(b)))$ holds, i.e. $\mathrm{I}(B(b),z,w) = \mathrm{I}(\mathrm{I}(A,a,b),z,w)$ is inhabited. $\square$

Remark 5.3 This result shows that the statement that θ_a is a well-defined bijection in Moerdijk and Palmgren [9, p. 196, line 13 – 15] actually need the assumption UIP to be true. This assumption was unfortunately not made in that paper.

6 Decidable identity types

Hedberg [5] proved that decidable identity types satisfy UIP in the following sense:

Theorem 6.1 (Hedberg) *If* $(\forall x,y : A)(\mathrm{I}_A(x,y)\vee\neg\mathrm{I}_A(x,y))$, *then*

$$(\forall x,y : A)(\forall u,v : \mathrm{I}_A(x,y))\mathrm{I}(u,v).$$

This result shows that UIP is always true in classical extensions of type theory. Examining the proof in [5] one can see that the same argument proves the somewhat stronger statement

Theorem 6.2 *Let $x : A$ be fixed. If $(\forall y : A)(\mathrm{I}_A(x,y) \vee \neg \mathrm{I}_A(x,y))$, then*

$$(\forall y : A)(\forall u, v : \mathrm{I}_A(x,y))\mathrm{I}(u,v).$$

Note that to apply this theorem one does not need to assume that $\mathrm{I}(A,x,y)$ is decidable for every pair x and y. For instance, if A is an infinitary tree, say given by the introduction rules

$$0 : A \qquad\qquad \frac{f : N \to A}{\sup(f) : A}$$

we may not able to decide this in general. However, for $x = 0$, $\mathrm{I}(A,x,y)$ can be decided for all $y : A$, using the appropriate elimination rule.

The main ingredients of Hedberg's theorem are two lemmas of which we modify the second.

Lemma 6.3 *If $S \vee \neg S$, then there is $f : S \to S$ with*

$$(\forall x, y : S)\mathrm{I}_S(f(x), f(y)).$$

Proof. If $a : S$, then we may let $f(x) = a$. If $a : \neg S$, then take $f(x) = x$. □

Lemma 6.4 *Let $x : A$. If $f : (\Pi y : A)(\mathrm{I}(A,x,y) \to \mathrm{I}(A,x,y))$, then there is $g : (\Pi y : A)(\mathrm{I}(A,x,y) \to \mathrm{I}(A,x,y))$ with*

$$(\forall y : A)(\forall z : \mathrm{I}_A(x,y))\mathrm{I}(g(y, f(y,z)), z).$$

Proof. Employing the groupoid operations construct g as follows

$$g(y,w) = w \circ (f(x, r(x)))^{-1}$$

for $y : A$, $w : \mathrm{I}(A,x,y)$. Instead of using the standard elimination rule as in [5], we shall use Paulin-Mohring's rule (3). Take $D(u,z)$ to be

$$\mathrm{I}(\mathrm{I}(A,x,u), g(u, f(u,z)), z),$$

where $u : A, z : \mathrm{I}(A,x,u)$. Now $D(x, r(x))$ is

$$\mathrm{I}(\mathrm{I}(A,x,x), f(x,r(x)) \circ (f(x,r(x)))^{-1}, r(x)),$$

which is true in virtue of the groupoid laws. Say the type is inhabited by the proof object p. Thus for any $y : A$ and $z : \mathrm{I}(A,x,y)$ we have that $\mathrm{J}'_{x,D,y}(z,p) : D(y,z)$. That is we have proved

$$(\forall y : A)(\forall z : \mathrm{I}_A(x,y))\mathrm{I}(g(y, f(y,z)), z). \ \square$$

Proof of Theorem 6.2. Let $x : A$ and suppose that $(\forall y : A)(\mathrm{I}_A(x, y) \vee \neg \mathrm{I}_A(x, y))$. Thus by Lemma 6.3 we find for each $y : A$, $f(y) : \mathrm{I}(A, x, y) \to \mathrm{I}(A, x, y)$ with

$$(\forall z, w : \mathrm{I}_A(x, y))\mathrm{I}(f(y, z), f(y, w)). \tag{7}$$

Lemma 6.4 gives $g : (\Pi y : A)(\mathrm{I}(A, x, y) \to \mathrm{I}(A, x, y))$ with

$$(\forall y : A)(\forall z : \mathrm{I}_A(x, y))\mathrm{I}(g(y, f(y, z)), z). \tag{8}$$

Thus applying g to (7) we get for each $y : A$

$$(\forall z, w : \mathrm{I}_A(x, y))\mathrm{I}(g(y, f(y, z)), g(y, f(y, w))). \tag{9}$$

By (8) twice we obtain

$$(\forall z, w : \mathrm{I}_A(x, y))\mathrm{I}(z, w). \ \square$$

7 Axiomatising uniqueness of identity proofs

Streicher [12] suggested to supplement the standard elimination operator for identity types with a second elimination operator K given by the rule: for $D(x, z)$ type $(x : A, z : \mathrm{I}(A, x, x))$

$$\frac{c : \mathrm{I}(A, a, a) \qquad d(x) : D(x, r(x)) \quad (x : A)}{\mathrm{K}_{D,a}(c, d) : D(a, c)}$$

and the computation rule $\mathrm{K}_{D,a}(r(a), d) = d(a)$.

We show here that the operators J and K may be combined into a single operator J^2 given by the elimination rule: for $C(x, y, u, v)$ type $(x : A, y : A, u : \mathrm{I}(A, x, y), v : \mathrm{I}(A, x, y))$ we have

$$\frac{c : \mathrm{I}(A, a, b) \quad c' : \mathrm{I}(A, a, b) \qquad d(x) : C(x, x, r(x), r(x)) \quad (x : A)}{\mathrm{J}^2_{C,a,b}(c, c', d) : C(a, b, c, c')}$$

with computation rule $\mathrm{J}^2_{C,a,a}(r(a), r(a), d) = d(a)$.

This is a sort of double recursion operator on identity types.

Theorem 7.1 J^2 *is equivalent to the combination of* J *and* K.

Proof. $(\mathrm{J} + \mathrm{K} \Rightarrow \mathrm{J}^2)$: Define $D(x, v) = C(x, x, r(x), v)$ $(x : A, v : \mathrm{I}(A, x, x))$. Thus $d(x) : D(x, r(x))$ $(x : A)$, so $K_{D,x}(v, d) : D(x, v)$ for $x : A$ and $v : \mathrm{I}(A, x, x)$ by the K-rule. Abbreviate $K_{D,x}$ by K_x. Define

$$E(x, y, z) = (\Pi w : \mathrm{I}(A, x, y))C(x, y, z, w).$$

Thus we have $\lambda v.K_x(v,d) : E(x,x,\mathrm{r}(x))$. By the J-rule we have $\mathrm{J}_{E,a,b}(c,(x)\lambda v.\mathrm{K}_x(v,d)) : E(a,b,c)$. Thus define

$$\mathrm{J}^2_{C,a,b}(c,c',d) = \mathrm{J}_{E,a,b}(c,(x)\lambda v.\mathrm{K}_x(v,d))(c') : C(a,b,c,c').$$

Clearly, $\mathrm{J}^2_{C,a,a}(\mathrm{r}(a),\mathrm{r}(a),d) = \mathrm{J}_{E,a,a}(\mathrm{r}(a),(x)\lambda v.\mathrm{K}_x(v,d))(\mathrm{r}(a)) = \mathrm{K}_a(\mathrm{r}(a),d) = d(a)$. This proves $(\mathrm{J}+\mathrm{K} \Rightarrow \mathrm{J}^2)$.

($\mathrm{J}^2 \Longrightarrow \mathrm{J}$): Suppose $E(x,y,z)$ type $\quad (x,y : A, z : \mathrm{I}(A,x,y))$ and $e(x) : E(x,x,\mathrm{r}(x)) \quad (x : A)$. Define $C(x,y,u,v) = E(x,y,u)$. Thus also $e(x) : C(x,x,\mathrm{r}(x),\mathrm{r}(x)) \quad (x : A)$. For $c : \mathrm{I}(A,a,b)$ we have $\mathrm{J}^2_{C,a,b}(c,c,e) : C(a,b,c,c)$. We define $\mathrm{J}_{E,a,b}(c,e) = \mathrm{J}^2_{C,a,b}(c,c,e)$. Clearly then $\mathrm{J}(\mathrm{r}(a),e) = e(a)$.

($\mathrm{J}^2 \Rightarrow \mathrm{K}$): First we show that ($\mathrm{J}^2$) implies UIP. Clearly taking $C(x,y,u,v) = \mathrm{I}(\mathrm{I}(A,x,y),u,v)$ we have $d(x) = \mathrm{r}(\mathrm{r}(x)) : C(x,x,\mathrm{r}(x),\mathrm{r}(x))$. Hence for any $u,v : \mathrm{I}(A,x,y)$,

$$\mathrm{J}^2_{C,x,y}(u,v,(x)\mathrm{r}(\mathrm{r}(x))) : \mathrm{I}(\mathrm{I}(A,x,y),u,v), \tag{10}$$

that is, identity proofs are unique.

We construct K. Let $D(x,v)$ type $\quad (x : A, v : \mathrm{I}(A,x,x))$ and suppose $d(x) : D(x,\mathrm{r}(x)) \quad (x : A)$. Let $a : A$ and $c : \mathrm{I}(A,a,a)$. We have $\mathrm{J}^2_{C,a,a}(\mathrm{r}(a),c,(x)\mathrm{r}(\mathrm{r}(x))) : \mathrm{I}(\mathrm{I}(A,a,a),\mathrm{r}(a),c)$ by (10). Define K using reindexing:

$$\mathrm{K}_{D,a}(c,d) =_{\mathrm{def}} \mathrm{R}_{B,\mathrm{r}(a),c}(\mathrm{J}^2_{C,a,a}(\mathrm{r}(a),c,(x)\mathrm{r}(\mathrm{r}(x))),d(a)) : D(a,c)$$

where $B(u) = D(a,u)$. Thus

$$\mathrm{K}_{D,a}(\mathrm{r}(a),d) = \mathrm{R}_{B,\mathrm{r}(a),\mathrm{r}(a)}(\mathrm{r}(\mathrm{r}(a)),d(a)) = d(a).$$

This shows the equivalence of the elimination rules. $\square$

Remark 7.2 Both Streicher's solution of adding the K-axiom and the J^2-axiom suggested here apparently fall outside the usual pattern of inductively defined sets and families in Martin-Löf type theory.

8 Concluding discussion

We have seen that proof-relevant families of setoids appear in abundance in standard Martin-Löf type theory. Each family of types $B : (A)$type yields such a family (A^*, B^*). However this kind of families seems difficult to use for certain purposes, e.g. construction of categories with equality on objects. For such purposes the standard proof-irrelevant families are more suitable. They are, on the other hand, not easy to construct in standard type theory. Roughly speaking, it seems that we need to construct extensional collapses of the types involved in the families. This procedure is well-known from set theory, and indeed, one way of constructing such families is to use Aczel's method [1] for modelling constructive set theory CZF: apply the W-type construction to a universe of types and define equality of sets by W-recursion as bisimilarity of trees.

Another possibility is to try to use proof-relevant families, inspired by the Hofmann-Streicher model [6]. This seems to involve developing some new ways of thinking about basic mathematical objects as groupoids. We refer to [11] for some examples of this in a classical setting.

Acknowledgement

I am grateful to Olov Wilander for discussions on categories of setoids.

References

[1] Peter Aczel. The type-theoretic interpretation of constructive set theory. In: A. Macintyre, L. Pacholski and J. Paris (eds.), *Logic Colloquium '77.* North-Holland, Amsterdam 1978.

[2] Errett Bishop and Douglas S. Bridges. *Constructive analysis.* Springer 1985.

[3] Alexandre Buisse and Peter Dybjer. The interpretation of intuitionistic type theory in locally cartesian closed categories - an intuitionistic perspective, in Proceedings of MFPS XXIV, Philadelphia 2008. *Electr. Notes Theor. Comput. Sci.* 218(2008), 21-32.

[4] Richard Garner. Two-dimensional models of type theory. *Mathematical Structures in Computer Science* 19(2009), 687-736.

[5] Michael Hedberg. A coherence theorem for Martin-Löf's type theory. *J. Funct. Programming* 8 (1998), no. 4, 413–436.

[6] Martin Hofmann and Thomas Streicher. The groupoid interpretation of type theory. In: G. Sambin and J. Smith (eds.) *Twenty-five years of constructive type theory (Venice, 1995),* 83–111, Oxford Logic Guides, 36, Oxford Univ. Press, New York, 1998.

[7] Martin Hofmann and Thomas Streicher. *The groupoid interpretation of type theory.* Longer preprint version of [6]. URL: `http://www2.tcs.ifi.lmu.de/~mhofmann/`

[8] Ray Mines, Fred Richman and Wim Ruitenburg. *A course on constructive algebra.* Springer 1988.

[9] Ieke Moerdijk and Erik Palmgren. Type theories, toposes and constructive set theory: predicative aspects of AST, *Annals of Pure and Applied Logic* 114(2002), 155–201.

[10] Bengt Nordström, Kent Peterson and Jan M. Smith. *Programming in Martin-Löf type theory.* Oxford University Press 1990.

[11] Erik Palmgren. *Groupoids and local cartesian closure.* Uppsala University, Department of Mathematics Report 2003:21. `www.math.uu.se/research/pub`

[12] Thomas Streicher. *Investigations into intensional type theory.* Habilitation Thesis, Ludwig-Maximilians Universität, Munich 1993. `www.mathematik.tu-darmstadt.de/~streicher/`

Erik Palmgren
Department of Mathematics, Uppsala University
PO Box 480, SE-751 06 Uppsala, Sweden
E-mail: `palmgren@math.uu.se`
URL: `www.math.uu.se`