Proof-relevance of families of setoids and identity in type theory

Erik Palmgren *

October 13, 2010

Abstract

Families of types are fundamental objects in Martin-Löf type theory. When extending the notion of setoid (type with an equivalence relation) to families of setoids, a choice between proof-relevant or proof-irrelevant indexing appears. It is shown that a family of types may be canonically extended to a proof-relevant family of setoids via the identity types, but that such a family is in general proof-irrelevant if, and only if, the proof-objects of identity types are unique. A similar result is shown for fibre representations of families. The ubiquitous role of proof-irrelevant families is discussed.

1 Introduction

In set theory, the notion of a family of sets may readily be reduced to the notion of set. A family of sets may be represented by a function $\beta : B \to A$. Its fibres $B_x = \beta^{-1}(x) = \{b \in B : \beta(b) = x\}$, for $x \in A$, represent the sets of the family. This representation is always possible in systems such as ZF, or in its constructive versions [1], since by the replacement scheme, 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

*Supported by a grant from the Swedish Research Council (VR). Research reported here was partly done during a stay at Institut Mittag-Leffler.

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 [11] 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.

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 $A = (|A|, =_A)$. 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 $p : (x =_A y), q : (y =_A z), r : (x =_A z)$.

Here $=_{\text{ext}}$ denotes the extensional equality of functions. 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 it 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 $p : x =_A y$.

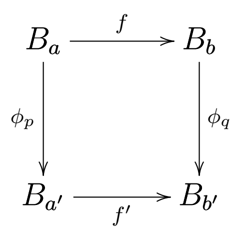
Here $\text{ref}(x) : x =_A x$ is a proof object for reflexivity. Moreover the proof objects associated with symmetry and transitivity are $\text{sym}(p) : y =_A x$, for $p : x =_A y$, and $\text{trans}(q, p) : x =_A z$ for $p : x =_A y$ and $q : y =_A z$.

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. However, if we add proof-irrelevance

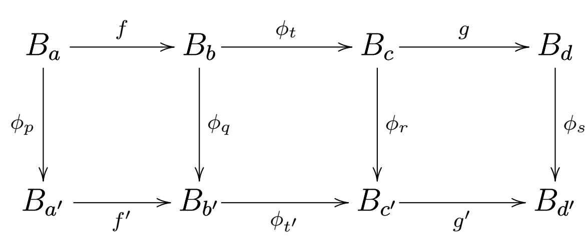
(Irr) $\phi_p =_{\text{ext}} \phi_q$ for any $p : x =_A y$ and $q : x =_A y$.

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, we consider the construction of a category $\mathcal{B}$ of setoids with a new equality on objects. 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 a 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



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:



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

3 Identity types

The presentation of Martin-Löf type theory given in [10] will be followed here, but 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, 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 whenever 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 appears to be 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 $\quad (x,y : A, z : \mathrm{I}(A,x,y))$ 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 application 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 $\quad (x : A)$, 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

$$\mathrm{R}_{B,a,b}(c,q) = \mathrm{J}_{C,a,b}(c,(x)\mathrm{id}_{B(x)})(q) : B(b) \tag{3}$$

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

A very useful elimination rule, equivalent to the standard (1), is the rule of Paulin-Mohring [11]. It says that for any parameter $a : A$ and any family $D(x,z)$ type $\quad (x : A, z : \mathrm{I}(A,a,x))$ if

$$\frac{b : A \qquad c : \mathrm{I}(A,a,b) \qquad d : D(a,r(a))}{\mathrm{J'}_{a,D,b}(c,d) : D(b,c)} \tag{4}$$

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

The identity proofs of A are said to be *unique* in case

$$(\forall z, w : \mathrm{I}_A(a,b))\mathrm{I}(z,w) \qquad\qquad (\mathrm{UIP}_A) \tag{5}$$

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, and the structure of identity types thus turned out to be more complicated than expected. In fact they showed that it induces as groupoid structure on each type. 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

- a type $|A|$,
- a setoid $\mathrm{Hom}(a, b)$ of morphisms for any $a, b : |A|$,
- an identity morphism $\mathrm{id}_a \in \mathrm{Hom}(a, a)$ for each $a : |A|$,
- a composition operation $\circ : \mathrm{Hom}(b, c) \times \mathrm{Hom}(a, b) \longrightarrow \mathrm{Hom}(a, c)$ for all $a, b, c : |A|$,
- 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

Any family B of types over A, i.e. a type-valued function $B : (A)\mathrm{type}$ in the notation of [10], gives rise to a proof-relevant family of setoids. 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 of (3) 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 show that UIP gives a precise 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 $B(x) = \mathrm{I}(A, u, x)$, it holds that*

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

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 be a fixed type. 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.

($\Rightarrow$): 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.

($\Leftarrow$): Suppose that (A^*, B^*) is a proof-irrelevant 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

$$\mathrm{I}(\mathrm{I}(A, a, b), B^*_p(q), B^*_{p'}(q)) \tag{6}$$

holds for $a, b : A$, $p, p' : \mathrm{I}(A, a, b)$, $q : B(a) = \mathrm{I}(A, a, a)$. Now by Lemma 4.2 and $B^*_p(q) = \mathrm{R}_{B,a,b}(p, q)$ the equation (6) is equivalent to

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

Putting $q = \mathrm{r}(a)$, we get $\mathrm{I}(\mathrm{I}(A, a, b), p \circ \mathrm{r}(a), p' \circ \mathrm{r}(a))$, and since $\mathrm{r}(a)$ is an 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. $\square$

5 Families of setoids induced by fibres of maps.

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

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

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 the fibres 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 directly 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 $C((a, b), (a', b'), q)$ as was desired. $\Box$

Theorem 5.2 *Let A be a fixed type. For a family $B : (A)\mathrm{type}$, 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 of setoids for any $a : A$ and any choice of $B : (A)\mathrm{type}$ 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 by definition $p : \mathrm{I}(A, u, a)$, $p' : \mathrm{I}(A, u', a)$ 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 the functoriality property (R2) it follows

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

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

$$\mathrm{I}(B(a), \mathrm{R}_{B,u,a}(p, v), \mathrm{R}_{B,u',a}(p', v')) \tag{7}$$

holds, thus proving θ_a well-defined. Suppose now (7) 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 (7) 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 by the groupoid laws. But $\mathrm{I}(B(b), \mathrm{R}_{B,b,b}(p,z), p \circ z)$ by Lemma 4.2 with $a = b$ and $u = a$, 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. □

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 omitted 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

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

we may not able to decide equality 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 $f(x) = x$. $\square$

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 (4). 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

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

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

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

Thus applying g to (8) we get for each $y : A$

$$(\forall z, w : \mathrm{I}_A(x, y))\mathrm{I}(g(y, f(y, z)), g(y, f(y, w))). \tag{10}$$

By (9) twice we obtain

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

7 Concluding discussion

We have seen that proof-relevant families of setoids appear in abundance in standard Martin-Löf type theory. Each family of types $B : (A)\mathrm{type}$ 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.

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] 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`