Some remarks and questions on uniqueness of elements in identity types

Erik Palmgren

October 13, 2009

For any set A of type theory the identity type $I(A,a,b)$ is the set of proofs that a and b are propositionally equal in A. The identity proofs of $I(A,a,b)$ are unique in case

$$(\forall z, w : I(A,a,b))I(I(A,a,b),z,w) \tag{1}$$

holds. Hofmann and Streicher (1994) showed that this is need not hold for general types by exhibiting a groupoid model of type theory. However it is not known how to refute (1) for types A in a empty context of standard type theory. (Still open?)

1 Decidable identity types

Hedberg (1998) showed that decidable identity types have unique proofs of identity in the following sense:

Theorem 1.1 *If* $(\forall x, y : A)(I(A,x,y) \vee \neg I(A,x,y))$*, then*

$$(\forall x, y : A)(\forall u, v : I(A,x,y))I(I(A,x,y),u,v).$$

This result shows that uniqueness of identity proofs is always true in classical extensions of type theory. Examining the proof in (Hedberg 1998) one can see that the same argument proves the somewhat stronger statement

Theorem 1.2 *Let* $x : A$ *be fixed. If* $(\forall y : A)(I(A,x,y) \vee \neg I(A,x,y))$*, then*

$$(\forall y : A)(\forall u, v : I(A,x,y))I(I(A,x,y),u,v).$$

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

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

we may not able to decide this in general. However if $x = 0$, $I(A, x, y)$ can be decided for all $y : A$.

The main ingredients are two lemmas.

Lemma 1.3 *If $S \vee \neg S$, then there is $f : S \longrightarrow S$ with*

$$(\forall x, y : S)I(S, f(x), f(y)).$$

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

Lemma 1.4 *Let $x \in A$. If $f : (\Pi y : A)(I(A, x, y) \longrightarrow I(A, x, y))$, then there is $g : (\Pi y : A)(I(A, x, y) \longrightarrow I(A, x, y))$ with*

$$(\forall y : A)(\forall z : I(A, x, y))I(I(A, x, y), g(y, f(y, z)), z).$$

Proof. Employing the groupoid operations construct g as follows

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

Instead of using the standard elimination rule (as in Hedberg 1998), we shall use the following derived rule (Paulin-Mohring's rule): From $a : A$, $D(u, z)$ set $(u : A, z : I(A, a, u))$, $d : D(a, r(a))$, $b : A$ and $c : I(A, a, b)$ infer $J'(a, b, d) : D(b, c)$. Take $a = x$ and $D(u, z)$ to be

$$I(I(A, a, u), g(u, f(u, z)), z).$$

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

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

which is true in virtue of the groupoid laws. Thus for any $y : A$ and $z : I(A, x, y)$ we have that $D(y, z)$ is true. That is we have proved

$$(\forall y : A)(\forall z : I(A, x, y))I(I(A, x, y), g(y, f(y, z)), z). \ \Box$$

Proof of Theorem 1.1. Let $x : A$ and suppose that $(\forall y : A)(I(A, x, y) \vee \neg I(A, x, y))$. Thus by Lemma 1.3 we find for each $y : A$, $f(y) : I(A, x, y) \longrightarrow I(A, x, y)$ with

$$(\forall z, w : I(A, x, y))I(I(A, x, y), f(y, z), f(y, w)). \tag{2}$$

Lemma 1.4 gives $g : (\Pi y : A)(I(A, x, y) \longrightarrow I(A, x, y))$ with

$$(\forall y : A)(\forall z : I(A, x, y))I(I(A, x, y), g(y, f(y, z)), z). \tag{3}$$

Thus applying g to (2) we get for each $y : A$

$$(\forall z, w : I(A, x, y))I(I(A, x, y), g(y, f(y, z)), g(y, f(y, w))). \tag{4}$$

By (4) twice we obtain

$$(\forall z, w : I(A, x, y))I(I(A, x, y), z, w). \ \Box$$

2 Axiomatizing uniqueness of identity proofs

Streicher (1993)[1] suggested to supplement the standard J operator with an additional elimination operator K given by the rules for $D(x,z)$ set $\quad (x : A, z : I(A,x,x))$

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

and where $K_{D,a}(d, r(a)) = d(a)$.

We show here that the rules J and K may be combined into a single elimination rule: for $C(x,y,u,v)$ set $\quad (x : A, y : A, u : I(A,x,y), v : I(A,x,y))$ we have

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

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

Is it possible to justify of the rule following standard meaning explanations with closed terms?

$(J + K \Rightarrow J^2)$: Define $D(x,v) = C(x,x,r(x),v) \quad (x : A, v : I(A,x,x))$. Thus $d(x) : D(x, r(x)) \quad (x : A)$, so $K_x(d,v) : D(x,v)$ for $x : A$ and $v : I(A,x,x)$. Define

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

Thus we have $\lambda v.K_x(d,v) : E(x,x,r(x))$. By J we have $J_{a,b}((x)\lambda v.K_x(d,v),c) : E(a,b,c)$. Thus define

$$J^2_{a,b}(d,c,c') = J_{a,b}((x)\lambda v.K_x(d,v),c)(c') : C(a,b,c,c').$$

Clearly, $J^2_{a,a}(d,r(a),r(a)) = J_{a,a}((x)\lambda v.K_x(d,v),r(a))(r(a)) = K_a(d,r(a)) = d(a)$. This proves $(J + K \Rightarrow J^2)$.

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

$(J^2 \Rightarrow K)$: First we show that (J^2) implies uniqueness of identity proofs.

Clearly taking $C(x,y,u,v) = I(I(A,x,y),u,v)$ we have $d(x) = r(r(x)) : C(x,x,r(x),r(x))$. Hence for any $u,v : I(A,x,y)$,

$$J^2_{x,y}((x)r(r(x)),u,v) : I(I(A,x,y),u,v),$$

that is, identity proofs are unique.

[1] Investigations into intensional type theory. Habilitationsschrift LMU.

Let $D(x,v)$ set $\quad (x : A, v : I(A,x,x))$ and suppose $d(x) : D(x, r(x)) \quad (x : A)$. Let $a : A$ and $c : I(A,a,a)$. We have $J^2_{a,a}((x)r(r(x)), r(a), c) : I(I(A,a,a), r(a), c)$ and hence $K_{D,a}(d,c) =_{\mathrm{def}} \mathrm{Sub}_{B,r(a),c}(J^2_{a,a}((x)r(r(x)), r(a), c), d(a)) : D(a,c)$ where $B(u) = D(a,u)$. Thus

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

Appendix: identity types

The formation rule for the identity type is that $I(A,a,b)$ set if A set and $a, b : A$. The introduction rule is

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

The elimination rule for $C(x,y,z)$ set $\quad (x, y : A, z : I(A,x,y))$ is

$$\frac{c : I(A,a,b) \qquad d(x) : C(x,x,r(x))\ (x : A)}{J_{C,a,b}(d,c) : C(a,b,c)}.$$

The associated computation rule is $J_{C,a,a}(d, r(a)) = d(a)$.

For $B(x)$ set $\quad (x : A)$, define $C(x,y,z) = B(x) \longrightarrow B(y)$. Then $d(x) = \lambda p : B(x).p : C(x,x,r(x))$. Hence for $c : I(A,a,b)$

$$J_{a,b}((x)\lambda p : B(x).p, c) : C(a,b,c) = B(a) \longrightarrow B(c).$$

Define $\mathrm{Sub}_{a,b}(q,c) = J_{a,b}((x)\lambda p : B(x).p, c)(q) : B(b)$ for $q : B(a)$. Clearly $\mathrm{Sub}_{a,b}(q, r(a)) = q$

Using the elimination rule one constructs groupoid operations

- $z^{-1} : I(A,y,x) \qquad (x, y : A, z : I(A,x,y))$,
- $w \circ z : I(A,x,u) \qquad (x, y, u : A, z : I(A,x,y), w : I(A,y,u))$.

These satisfies the groupoid laws, i.e. the following types are inhabited:

- $I(I(A,x,y), r(y) \circ z, z)$,
- $I(I(A,x,y), z \circ r(x), z)$,
- $I(I(A,x,x), z \circ z^{-1}, r(x))$,
- $I(I(A,x,x), z^{-1} \circ z, r(x))$,
- $I(I(A,x,v), (z \circ w) \circ p, z \circ (w \circ p))$.

References

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

[2] Martin Hofmann, 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.