Notes on axiomatising Hurkens’s Paradox

Arnaud Spiwack

July 15, 2015

Abstract

An axiomatisation of Hurkens’s paradox in dependent type theory is given without assuming any impredicative feature of said type theory.

Hurkens’s paradox \[\text{[8]}\] is a very economic, though rather hard to understand, paradox of the $\text{U}^-$ impredicative type theory, described in Section\[1.1\] whose main characteristic is to feature to nested impredicative sorts. Its terseness makes it the weapon of choice to derive inconsistencies from logical principle or experimental language features of your favourite proof assistant. Or, rather, embedding $\text{U}^-$ in some way is the weapon of choice, Hurkens’s paradox serves as a way to turn this into a proof of false.

It may sound like a futile game to play: if you are the ideal mathematician you will never implement inconsistent feature in your proof assistant. Unfortunately, you are not, and deriving contradiction will happen to you from time to time. Having a tool for that may turn out to be of tremendous help. As a bonus, the inconsistency of $\text{U}^-$ can serve to derive potentially useful principles, such as the fact that if the principle of excluded middle holds in an impredicative sort, then types in that sort have the proof irrelevance property (see Section\[2.4\]).

The downside in all that is that there does not seem to be a good way to express, within dependent type theory, the existence of an impredicative sort. Coquand \[\text{[3]}\] gave a sufficient condition, albeit much stronger, to derive contradictions in a generic way. His proof was based on Girard’s \[\text{[6]}\] paradox rather than Hurkens’s one (which came out ten years later). Geuvers \[\text{[5]}\] later gave a proof based more directly on Hurkens’s one and relying on a single impredicative sort, but this proof wasn’t very generic. The result was that Hurkens’s proof was included \textit{twice} in the distribution of the Coq proof assistant \[\text{[9]}\]: Geuvers’s proof, and a variant due to Hugo Herbelin to prove slightly different results.

This situation is certainly unsatisfactory, as adapting Hurkens’s proof for every little variation around the same theme is significantly more work than describing an encoding of $\text{U}^-$. It prevents good people from finding perfectly good proof of contradictions: it isn’t fair to assume that everyone is an expert in Hurkens’s proof.

As it happens, however, there is a perfectly good axiomatisation of $\text{U}^-$ in your favourite dependently typed proof assistant (in actuality, a sufficient
subsystem). And the corresponding proof of contradiction is, *mutatis mutandis*, Geuvers's, where conversion rules are replaced by equalities.

1 Axiomatic Hurkens's paradox

The trick, so to speak, of the axiomatix presentation of \( U^- \) is generally attributed to Martin-Löf: a universe is given by an type \( U : \text{Type} \) describing the types in the universe, and an decoding function \( \text{El} : U \rightarrow \text{Type} \) describing, for each type in \( U \) the elements of that types. Sorts are to be encoded as such universes. System \( U^- \) has two of these, commonly called *large* and *small*, together with rules to combine them. Each of these rules take the form of a product formation rule (see Barendregt's presentations of pure type systems, formerly known as generalised type systems [1][2] Section 5.2). Instead of the usual presentation where there is a single dependent product with a number of formation rules, we will have a distinct dependent product – with its own introduction rule (\( \lambda \)-abstraction) and elimination rule (application) – for each of the formation rule. For each pair \( \lambda \)-abstraction & application, there may be a \( \beta \)-equivalence rule, modelled as an equality; only the \( \beta \)-equivalence rules which are effectively used in the proof are axiomatised.

1.1 Axiomatic \( U^- \)

The full axiomatic presentation appears below, in Coq syntax. It is also part of Coq's distribution and can be found, at the time these notes are being written, in the file theories/Logic/Hurkens.v.

Large universe

```
Variable U1 : Type.
Variable El1 : U1 \rightarrow \text{Type}.
```

The large universe \( U1 \) is closed by dependent products over types in \( U1 \). The definition of dependent product and \( \lambda \)-abstraction are defined using the function space of the dependent type theory. Notations are defined for dependent product, \( \lambda \)-abstraction and application. As usual, an arrow notation is used when the dependent product has a constant range.

```
Variable Forall1 : forall u1 : U1, (El1 u1 \rightarrow U1) \rightarrow U1.
Notation "'\forall'_1 x : A , B" := (Forall1 A (fun x \Rightarrow B)).
Notation "'A' =\rightarrow '_1 ' B" := (Forall1 A (fun _ \Rightarrow B)).
Variable lam1 : forall u B, (forall x :El1 u, El1 (B x)) \rightarrow El1 (\forall '_1 x : u, B x).
Notation "'\lambda'_1 x , u" := (lam1 _ _ (fun x \Rightarrow u)).
Variable app1 : forall u B (f:El1 (\forall '_1 x :u, B x)) (x:El1 u), El1 (B x).
Notation "f '·' '_1 ' x" := (app1 _ _ f x).
Variable beta1 : forall u B (f:f:forall x:El1 u, El1 (B x)) x,
(\lambda y, f y) · '_1 x = f x.
```

The large universe \( U1 \) is made impredicative by a dependent product with large domain. The standard presentation would use a sort \( U2 \), of which \( U1 \) is a member; the dependent product would then have, as a domain, some
\( U_2 \). This would be unnecessary complexity as \( U_2 \) is so restricted that the only interesting type in it would be \( U_1 \). So, instead, we simply restrict the domain of the product to be \( U_1 \).

**Variable** \( \text{forall} U_1 : (U_1 \to U_1) \to U_1 \).

**Notation** \( \forall x : A, B : (\text{forall} U_1 (\text{fun} x \Rightarrow B)) \).

**Variable** \( \text{lam} U_1 : \text{forall} F, (\text{forall} A : U_1, E_1 (F A)) \to E_1 (\forall x : A, A) \).

**Notation** \( \forall x : A, u : (\text{lam} U_1 \_ (\text{fun} x \Rightarrow u)) \).

**Variable** \( \text{app} U_1 : \text{forall} F, (\text{forall} F : (E_1 (\forall x : A, F A)) (A : U_1), E_1 (F A)) \).

**Notation** \( \forall x : A, F : (\text{forall} F : (E_1 (\forall x : A, F A)) (A : U_1), E_1 (F A)) \).

**Variable** \( \text{beta} U_1 : \text{forall} F, (\text{forall} A : U_1, E_1 (F A)) A, (\forall x : A, F A) \). \( \forall x : A, F : (\text{forall} F : (E_1 (\forall x : A, F A)) (A : U_1), E_1 (F A)) \).

**Notation** \( \forall x : A, F : (\text{forall} F : (E_1 (\forall x : A, F A)) (A : U_1), E_1 (F A)) \).

**Small universe** The small universe \( U_0 \) is an element of the larger one. Therefore we need an \( U_0 : U_1 \) and \( U_0 \) is taken to be \( E_1 u_0 \) rather than a variable.

**Variable** \( u_0 : U_1 \).

**Notation** \( U_0 := (E_1 u_0) \).

**Variable** \( E_0 : U_0 \to \text{Type} \).

The small universe \( U_0 \) is closed by dependent products in \( U_0 \). The definitions are symmetric to the corresponding ones of \( U_1 \). Notice, however, the lack of \( \beta \)-rule, which is unnecessary to derive a contradiction.

**Variable** \( \text{forall} U_0 : \text{forall} u : U_0, (E_0 (u \Rightarrow U_0)) \to U_0 \).

**Notation** \( \forall x : A, B : (\text{forall} U_0 (\text{fun} x \Rightarrow B)) \).

**Notation** \( \forall x : A, B : (\text{forall} U_0 (\text{fun} x \Rightarrow B)) \).

**Variable** \( \text{lam} U_0 : \text{forall} u : U_0, (\text{forall} x : U_0, E_0 (B x)) \to E_0 (\forall x : U_0, B x) \).

**Notation** \( \forall x : U_0, u : (\text{lam} U_0 \_ (\text{fun} x \Rightarrow u)) \).

**Variable** \( \text{app} U_0 : \text{forall} u : U_0, (\text{forall} F : (E_0 (\forall x : U_0, B x)) (x : E_0 u), E_0 (B x)) \).

**Notation** \( \forall x : U_0, u : E_0 u \).

The small universe \( U_0 \) is made impredicative by a dependent whose range is in \( U_1 \). Contrary to the impredicative product of \( U_1 \), the range cannot be restricted to be only \( U_0 \). Here again, the \( \beta \)-rule is not needed.

**Variable** \( \text{forall} U_{01} : \text{forall} u : U_{01}, (E_1 (u \Rightarrow U_{01})) \to U_{01} \).

**Notation** \( \forall x : A, B : (\text{forall} U_{01} (\text{fun} x \Rightarrow B)) \).

**Notation** \( \forall x : A, B : (\text{forall} U_{01} (\text{fun} x \Rightarrow B)) \).

**Variable** \( \text{lam} U_{01} : \text{forall} u : U_{01}, (\text{forall} F, (\text{forall} A : U_{01}, E_1 (F A)) \to E_1 (\forall x : A, F A)) \).

**Notation** \( \forall x : A, B : (\text{forall} U_{01} (\text{fun} x \Rightarrow B)) \).

**Variable** \( \text{app} U_{01} : \text{forall} U_{01} F, (\text{forall} F : (\text{forall} F : (E_1 (\forall x : A, F A)) (A : U_{01}), E_1 (F A)) \).

**Notation** \( \forall x : A, F : (\text{forall} F : (E_1 (\forall x : A, F A)) (A : U_{01}), E_1 (F A)) \).

**1.2 Proof of contradiction**

From there, we can proceed to use Hurkens’s argument to derive a contradiction. Let’s be precise: we shall prove that every type in \( U_0 \) is inhabited. It will only be an actual contradiction if \( U_0 \) contains the empty type. For this purpose, let’s assume a type in \( U_0 \), we will then prove it is inhabited.
Variable F:U0.

The proof will require simplifying $\beta$-redexes. We provide tactics to that effect.

\[
\text{Ltac simplify} :=
(\text{repeat rewrite} \ ? \text{beta1,} \ ? \text{betaU1});
\text{lazy beta}.
\]

\[
\text{Ltac simplify_in h} :=
(\text{repeat rewrite} \ ? \text{beta1,} \ ? \text{betaU1 in h});
\text{lazy beta in h}.
\]

These tactics are rather brute-force, in that they will $\beta$-reduce as much as possible without any particular strategy. On the other hand, they, crucially, don't unfold Coq definitions so that we can give them hints by manually unfolding the appropriate terms to be simplified. Allowing the simplification tactics to unfold Coq definitions turns out to be intractable.

It is traditional to regard $U1$ as the type of datatypes and $U0$ as the type of proposition. This view is justified by the fact that $U0$ is not equipped with $\beta$-conversion rules. In the proof, following Geuvers [5], data is explicitly given, while propositions are proved with tactics. Here are the data definitions (I'm playing a bit loose here, since I consider propositions to be data, they are according to the above definition at least):

\[
\text{Definition V : U1 := } \forall \alpha A, ((A \rightarrow u0) \rightarrow A) \rightarrow u0.
\]

\[
\text{Definition U : U1 := V \rightarrow u0}.
\]

\[
\text{Definition sb (z:El1 V) : El1 V := } \lambda \alpha A, \lambda r, \lambda a, r \cdot (z[A] \cdot r) \cdot a.
\]

\[
\text{Definition le (i:El1 (U \rightarrow u0)) (x:El1 U) : U0 :=}
\lambda \alpha x, (i(xu) \cdot [A] \cdot r) \cdot (z[A] \cdot r) \cdot a.
\]

\[
\text{Definition le' : El1 ((U \rightarrow u0) \rightarrow U) \rightarrow u0 := } \lambda i, \lambda x, \lambda e i x.
\]

\[
\text{Definition induct (i:El1 (U \rightarrow u0)) : U0 :=}
\forall x_1 u, \lambda x, x \rightarrow \rightarrow_1 \rightarrow_1 x.
\]

\[
\text{Definition WF : El1 U := } \lambda z, (\text{induct (z[U] \cdot le')}).
\]

\[
\text{Definition I (x:El1 U) : U0 :=}
\lambda (x \rightarrow u0, \lambda i x \rightarrow \rightarrow_0 \rightarrow_1 (\lambda \alpha x, (sb v) \cdot [U] \cdot le' \cdot x)) \rightarrow_0 F.
\]

The proofs follow Geuvers [5] as well. The main difference is that we must explicitly call to simplify where conversion was used implicitly and that standard Coq tactics calls to the \text{intro} and \text{apply} tactics are generally replaced by tactics of the form \text{refine (\lambda x \_)} and \text{refine (h \_ \_)} respectively.
Lemma Omega : EI0 (∀ i : U →→₀ i u₀, induct i →→₀ i · WF).

Proof.
refine (λ₀ i, λ₀ y, _).
refine (γ₀[1]₀, _).
unfold le, WF, induct. simplify.
refine (λ₀ i, λ₀ h₀, _). simplify.
refine (γ₀[1]₀, _).
unfold le, simplify. unfold sb at 1. simplify. unfold le’ at 1. simplify.
effect h₀.
Qed.

Lemma lemma1 : EI0 (induct (λ₁ u, I u)).

Proof.
unfold induct.
refine (λ₀ x, λ₀ p, _). simplify.
refine (λ₀ q, _).
assert (EI0 (I (λ₁ v, (sb v) · [U] · le’ · x))) as h.
  intros q’. exact q’. }
refine (h₀, _).
refine (λ₀ i, _).
refine (λ₀ h₀’, _).
intros q’.
refine (q’₀, _). clear q’.
unfold le at 1 in h’. simplify in h’.
unfold sb at 1 in h’. simplify in h’.
unfold le’ at 1 in h’. simplify in h’.
effect h’.
Qed.

Lemma lemma2 : EI0 ((∀ i : U →→₀ i u₀, induct i →→₀ i · WF) →→₀ F).

Proof.
refine (λ₀ x, _).
assert (EI0 (I WF)) as h.
  intros q,
  exact q, }
refine (h₀, _). clear h.
refine (λ₀ i, λ₀ h₀, _).
intros q.
refine (q₀, _). clear q.
unfold le in h₀. simplify in h₀.
unfold WF in h₀. simplify in h₀.
effect h₀.
Qed.
**Theorem** paradox : El0 F.

**Proof.**

```
exact (lemma2_i0Omega).
Qed.
```

The takeaway insight is that because the paradox does not actually make use of the reduction rules in propositions of \( U_0 \), using equality to model conversion in these propositions doesn’t raise any obstacle to the completion of the proof.

Nothing in this proof is particularly specific to Coq: it could be done in any variant of Martin-Löf type theory, provided that an identity type is available. Of course, the support of Coq for rewriting significantly helps, if your favourite proof assistant doesn’t have a similar feature it may be painful to port this generic paradox.

## 2 Applications

In this section we will see a few instances of the generic axiomatisation of Hurkens’s proof can help derive contradictions. They come from the file `theories/Logic/Hurkens.v` of the Coq distribution (version 8.5).

### 2.1 Sorts

A common implementation of universes is to use a sort of the dependent type theory for a universe of \( U^- \). In that case, \( \text{El} \) is just the identity.

```
Variable U := Type.
Let El := fun X ⇒ X.
```

For universes defined this way, small products and their \( \lambda \)-abstraction, application and \( \beta \)-rule are defined straightforwardly (eq_refl is Coq’s witness of reflexivity of equality).

```
Let Forall (A:U) (B:A → U) : U := forall x:A, B x
Let lam u B (f:forall x:A,B x) := f
Let app u B (f:forall x:A,B x) (x:A) := f x
Let beta u B f x : f x = f x := eq_refl
```

### 2.2 Impredicative sort

Impredicativity, for a sort \( U \), can also be characterised to some degree. The idea is that there must be a bigger sort \( U' \) which can be projected onto \( U \). See, for example, the bracketing construction in [7]. This projection could be implemented, for instance, for Coq’s impredicative \( \text{Prop} \) sort as

```
fun X:Type ⇒ forall P:Prop, (X→P)→P.
```

The signature of Section 2.1 is extended with the constraint that \( U' \) is bigger than \( U \) and a projection.
Let \( U' := Type \).
Let \( U : U' \) := Type.
Variable \( \text{proj} : U' \rightarrow U \).

With the following laws.

Hypothesis \( \text{proj\_unit} : \forall (A : U'), A \rightarrow \text{proj} A \).
Hypothesis \( \text{proj\_coherent} : \forall (F : U \rightarrow U), \text{proj\_forall} (A : U, F A) \rightarrow (\forall (A : U, F A)) \).

The \( \text{proj\_unit} \) law expresses that if \( \text{proj} \) generally diminishes the ability to distinguish between elements of \( A : U2 \), it does not lose elements. We don’t have a way back from \( \text{proj} A \) to \( A \) in general, but \( \text{proj} \) forms a monad. The \( \text{proj\_unit} \) law expresses a small variation on this latter remark.

These properties are sufficient to show that \( U \) is closed by large product.

The \( \beta \)-rule, omitted, is easily derived from \( \text{proj\_coherent} \).

Let \( \text{forall} L (F : U \rightarrow U) : U := \text{proj\_forall} (A : U, F A) \).
Let \( \text{lam} L (f : \forall (A : U, F A)) : \text{proj\_forall} (A : U, F A) := \text{proj\_unit \_ f} \).
Let \( \text{app} L (f : \forall (A : U, F A)) (A : U) : F A := \text{proj\_counit \_ f} \).

We can exploit Coq’s universe polymorphism (form version 8.5) to turn this section into a generic definition of impredicative sort. Indeed, under the polymorphic interpretation \( Type \) represents an arbitrary type, including the impredicative sort \( \text{Prop} \), which is indeed impredicative in the above sense.

2.3 Generalising Geuvers’s proof

Geuvers [5] proves that an impredicative sort \( U1 \) cannot be a retract of an \( U0 : U1 \). His proof is made for \( U1 = \text{Prop} \), but we can instantiate the proof of Section 1 to obtain the same result for any sort which is impredicative sort in the sense of Section 2.2.

Let \( U2 := Type \).
Let \( U1 : U2 := Type \).
Variable \( U0 : U1 \).

Where \( U1 \) is impredicative over \( U2 \) as in Section 2.2. The retraction is given by the following functions. Only a weak form of retraction is needed were types in \( U1 \) which are “logically equivalent” are considered equal.

Variable \( \text{proj}0 : U0 \rightarrow U1 \).
Variable \( \text{inj}0 : U1 \rightarrow U0 \).
Hypothesis \( \text{inj}\_0\_unit : \forall (b : U1), b \rightarrow \text{proj}0 (\text{inj}0 b) \).
Hypothesis \( \text{inj}\_0\_counit : \forall (b : U1), \text{proj}0 (\text{inj}0 b) \rightarrow b \).

From this (weak) retraction we can define \( \text{El}0 \) and corresponding products for \( U0 \) despite the fact that \( U0 \) is not necessarily a sort.
Large products are define much the same:

Let \( \text{Forall0} (u : U0) (B : u \rightarrow U0) : U0 := \text{inj0} (\text{forall} x : \text{proj0} u, \text{proj0} (B x)) \)
Let \( \text{Lambda0} u B (f : \text{forall} x : \text{proj0} u, \text{proj0} (B x)) : \text{proj0} (\text{inj0} (\text{forall} x : \text{proj0} u, \text{proj0} (B x)))) := \text{inj0}_0 \_ f \_\_ .

Let \( \text{app0} \text{forall} u B (f : \text{proj0} (\text{inj0} (\text{forall} x : \text{proj0} u, \text{proj0} (B x)))) (x : \text{proj0} u) : \text{proj0} (B x) := \text{inj0}_0 \text{counit}_\_ f \_ x \)

From this, the paradox is set up, so we can deduce that every proposition of \( P : U0 \) is “inhabited” in that \( \text{Ei0} P = \text{proj0} P \) is inhabited, and therefore, that every proposition of \( F : U1 \) is inhabited since \( \text{inj0} F : U0 \) is “inhabited” in the sense of \( U0 \), i.e. \( \text{proj0} (\text{inj0} F) \) is inhabited, then \( \text{inj0}_0 \text{counit} \) concludes.

Since \( \text{Prop} \) is an instance of the signature of Section 2.2, we prove, like Geuvers, that \( \text{Prop} \) is not a retract of a proposition \( P : \text{Prop} \).

2.4 Excluded middle and proof irrelevance

Geuvers proof, from Section 2.3 helps proving a result, by Coquand [4], that excluded middle, in an impredicative sort makes it proof irrelevant, i.e. every type in that sort have at most one element. This proof appear in the Coq distribution in the file theories/Logic/ClassicalFact.v, presumably written by Hugo Herbelin. It uses Geuvers result and was mostly unmodified with the new proof of said result. With the characterisation of Section 2.2 this could be done in an arbitrary impredicative sort, but the Coq proof is done only for the impredicative sort \( \text{Prop} \), and we will present it that way for simplicity.

The basic idea is that excluded middle:

Variable \( \text{em} : \text{forall} A : \text{Prop}, A \lor \neg A. \)

turns the \( \text{Prop} \) sort into a boolean universe with only two elements. So assuming a proposition with two distinct values

Variable \( U0 : \text{Prop}. \)
Variables \( t, f : U0. \)
Hypothesis \( \text{not_eq_t_f} : t \neq f. \)

we can reflect \( \text{Prop} \) into \( U0 \) proposition as in Section 2.3. Where \( \text{True} \) is reflected as \( t \) and \( \text{False} \) as \( f \), as the names suggest.

This is formalised as a retraction given by:

Let \( \text{inj0} (A : \text{Prop}) : U0 := \text{or_ind} A (\neg A) U0 (\text{fun } _ \Rightarrow t) (\text{fun } _ \Rightarrow f) (\text{em} A). \)
Let \( \text{proj0} (x : U0) : \text{Prop} := t = x. \)

Where \( \text{or_ind : forall} A B P : \text{Prop}, (A \rightarrow P) \rightarrow (B \rightarrow P) \rightarrow A \lor B \rightarrow P \) is the elimination principle of disjunction.
We are left to prove the unit and counit laws of inj0 and proj0 to satisfy the premises of the paradox in Section 2.3. The unit law is direct:

**Lemma inj0_unit :** for all A : Prop, A → proj0 (inj0 A).
**Proof.**
in intros A x. unfold proj0, inj0.
destruct (em A) as [h | h].
+ reflexivity.
+ contradiction.
Qed.

The counit law is the step that makes a crucial use of the not_eq_t_f hypothesis:

**Lemma inj0_counit :** for all A : Prop, proj0 (inj0 A) → A.
**Proof.**
in intros A h. unfold proj0, inj0 in *.
destruct (em A) as [l | l].
+ apply l.
+ absurd (t=f).
  + apply not_eq_t_f.
  + apply h.
Qed.

Section 2.3 then yields a contradiction. Since U0 is arbitrary we have: for all (A:Prop) (x y:A), ~(x=y). A last application of the excluded middle yields the expected result:

for all (A:Prop) (x y:A), x=y

### 2.5 Variants of Prop

A (monadic) modality on Prop is given by a mapping:

**Variable M :** Prop → Prop.

Together with the following laws:

**Hypothesis unit :** for all A:Prop, A → M A.
**Hypothesis join :** for all A:Prop, M(M A) → M A.
**Hypothesis incr :** for all A B:Prop, (A→B) → M A → M B.

Such a modality is automatically equipped with a distribution property over arbitrary conjunctions:

**Lemma strength :** for all (P:A→Prop), M(forall x:A, P x) → forall x:A, M(P x).
**Proof.**
eauto.
Qed.

With a modality we can define the type of modal propositions, where the unit law is actually an equivalence (modalities are closure operators, by the join law, so the type of modal propositions is the image of M up to logical equivalence):

**Definition MProp :=** { P:Prop | M P → P }.
Despite not being a sort, MProp can be seen as a subtype of Prop and, therefore, as a universe in the sense of Section 1.1.

**Definition** \( \text{El} (P: \text{MProp}) : \text{Prop} := \text{proj1} \_ \text{sig} P \).

Because of strength, the MProp universe is closed by products of arbitrary types. The Program keyword makes it possible to populate MProp by giving the proposition \( P \) (first projection) explicitly and discharging the proof that \( M P \to P \) to tactics.

**Program Definition**

\[
\text{forall} (A:\text{Type}) (F:A \to \text{MProp}) : \text{MProp} :=
\text{forall x:A, El (F x)}.
\]

**Next Obligation.**

\[
\text{intros A F h x. apply strength with (x:=x) in h. destruct (F x). cbn in *. eauto. Qed.}
\]

Definitions of \( U^- \) products, small and large, for MProp follow immediately:

- **Let** \( \text{forall1} (u: \text{MProp}) (F:\text{El} u \to \text{MProp}) : \text{MProp} := \text{forall1} \_ \text{El} (\text{proj0} (\text{inj0} A)) \).
- **Let** \( \text{forallU1} (F:\text{MProp} \to \text{MProp}) : \text{MProp} := \text{forall MProp F} \).

Because \( \text{El} (\text{forall A F}) = \text{forall x:A, F} \), introduction, elimination and \( \beta \)-rules for the products are immediate.

Just like in Section 2.3, a retraction of MProp into a modal proposition can be used to trigger Hurkens’s paradox. This is an example of instance of Hurkens’s paradox where neither of the universes are sorts of the system.

**Variable** \( U0: \text{MProp} \).
- **Variable** \( \text{proj0} : U0 \to \text{MProp} \).
- **Variable** \( \text{inj0} : \text{MProp} \to U0 \).

**Hypothesis** \( \text{inj0} \_ \text{unit} \_ \text{unit} : \text{forall} (A:\text{MProp}), \text{El} A \to \text{El} (\text{proj0} (\text{inj0} A)) \).

**Hypothesis** \( \text{inj0} \_ \text{counit} \_ \text{counit} : \text{forall} (A:\text{MProp}), \text{El} (\text{proj0} (\text{inj0} A)) \to \text{El} A \).

Following the the proof of Section 2.3, we conclude from this context that every modal proposition is inhabited. This is not necessarily a contradiction, as falsity need not be modal. For instance the trivial modality, whose only modal proposition in True.

**Definition** \( M (A:\text{Prop}) : \text{Prop} := \text{True} \)

A more interesting modality is, for a given \( X \):

**Definition** \( M (A:\text{Prop}) : \text{Prop} := A \lor X \)

for such a modality exhibiting a retraction into a modal proposition only prove \( \neg X \); it is always the case that the smallest modal proposition is \( M \text{ False} \).
2.6 Weak excluded middle and proof irrelevance

In this section we will be concerned with the double-negation modality, whose modal propositions are also called negative propositions:

**Definition** \( \text{M} (A:\text{Prop}) : \text{Prop} := \neg\neg A \)

and will use the paradox from Section 2.5 to prove that the weak principle of excluded middle

**Hypothesis** \( \text{we}m : \forall A: \text{Prop}, \neg\neg A \lor \neg A. \)

entails a weak form of proof irrelevance. This is a new proof I added to theories/Logic/ClassicalFact.v and is available from version 8.5.

Looking closely at \( \text{we}m \) it becomes clear that it claims decidability of exactly the negative propositions.

**Remark** \( \text{we}m' : \forall A: \text{MProp}, \text{El} A \lor \neg \text{El} A. \)

The proof, therefore, proceeds just like the proof of Section 2.4: We begin by postulating a proposition with two proofs.

**Variable** \( U0: \text{Prop}. \)

**Variables** \( t, f : U0. \)

**Hypothesis** \( \text{not}_\text{eq}_t_f : t \neq f. \)

Notice that \( U0 \) is negative, since \( U0 \) has a proof, in particular \( \neg\neg U0 \rightarrow U0 \) holds. So we only need to construct a retraction into \( U0 \). The retraction is given by \( \text{inj0} \) and \( \text{proj0} \) which are, *mutatis mutandis* the same as in Section 2.4: double negations have to be inserted for propositions which need to be negative, and proofs of negativity have to be provided when building negative propositions.

\[
\begin{align*}
\text{Let} \ \text{inj0} \ (A: \text{MProp}) : U0 & := \\
& \text{or}_\text{ind} \ (\text{El} A) \ (\neg \text{El} A) \ U0 \ (\text{fun} _ \Rightarrow t) \ (\text{fun} _ \Rightarrow f) \ (\text{we}m' \ A).
\end{align*}
\]

\[
\begin{align*}
\text{Let} \ \text{proj0} \ (x: U0) : \text{MProp} & := \\
& \exists (\text{fun} P \Rightarrow \neg\neg P \rightarrow P) \ (\neg\neg (t = x)) \ (\text{fun} h x \Rightarrow h \ (\text{fun} k \Rightarrow k x)).
\end{align*}
\]

The unit and counit laws follow and we eventually derive a contradiction. That is, since \( U0: \text{Prop} \) is arbitrary a proof that:

\[
\text{forall} (A: \text{Prop}) (x y: A), \neg\neg (x = y)
\]

Contrary to to the case of (strong) excluded middle, we cannot eliminate this last double-negative. So proof irrelevance doesn’t follow from weak excluded middle. However, this section proves that weak excluded middle is incompatible with any sort of proof relevance principle. In particular, in Coq lingo, weak excluded middle cannot hold in impredicative Set, that is an impredicative sort with strong elimination.

3 Conclusion

The axiomatisation of Hurkens’s paradox presented in Section 2.7 is very versatile. It can be used, mostly, to prove that some combination of logical
principles are incompatible, but also to detect bugs in a dependent-type-theory implementation. Which is a completely fair and healthy activity if you ask this author.

It is, certainly, an improvement over a situation where each paradox would need a careful redesign of Hurkens’s proof to fit the specific premises. In practice it meant that paradoxes were not derived, because the brave paradox-finder didn’t have the energy or expertise to translate Hurkens’s paradox.

As per the axiomatisation itself. It has the pleasant property of requiring only a subset of $U^-$ where the “proofs” of “propositions” don’t require $\beta$-rules or any kind of equality rule. So something was learned. Adapting the proof to the axiomatisation doesn’t present any new difficulty, except from controlling rewriting a little. It wasn’t discovered before solely by the virtue of nobody looking. The reader who enjoyed this axiomatisation can celebrate the bout of optimism which made me look the right way, and the night I lost over it.

Bibliography


