

The meta theory of the Incredible Proof Machine

Joachim Breitner Denis Lohner

May 26, 2024

The Incredible Proof Machine is an interactive visual theorem prover which represents proofs as port graphs. We model this proof representation in Isabelle, and prove that it is just as powerful as natural deduction.

Contents

1	Introduction	2
2	Auxiliary theories	4
2.1	Entailment	4
2.2	Indexed_FSet	4
2.3	Rose_Tree	5
2.3.1	The rose tree data type	5
2.3.2	The set of paths in a rose tree	6
2.3.3	Indexing into a rose tree	6
3	Abstract formulas, rules and tasks	8
3.1	Abstract_Formula	8
3.2	Abstract_Rules	9
4	Incredible Proof Graphs	13
4.1	Incredible_Signatures	13
4.2	Incredible_Deduction	14
4.3	Abstract_Rules_To_Incredible	20
5	Natural Deduction	23
5.1	Natural_Deduction	23
6	Correctness	25
6.1	Incredible_Correctness	25
7	Completeness	28
7.1	Incredible_Trees	28
7.2	Build_Incredible_Tree	34
7.3	Incredible_Completeness	35

8	Instantiations	41
8.1	Propositional_Formulas	41
8.2	Incredible_Propositional	41
8.3	Incredible_Propositional_Tasks	43
8.3.1	Task 1.1	43
8.3.2	Task 2.11	45
8.4	Predicate_Formulas	46
8.5	Incredible_Predicate	50
8.6	Incredible_Predicate_Tasks	51

1 Introduction

The Incredible Proof Machine (<http://incredible.pm>) is an educational tool that allows the user to prove theorems just by dragging proof blocks (corresponding to proof rules) onto a canvas, and connecting them correctly.

In the ITP 2016 paper [Bre16] the first author formally describes the shape of these graphs, as port graphs, and gives the necessary conditions for when we consider such a graph a valid proof graph. The present Isabelle formalization implements these definitions in Isabelle, and furthermore proves that such proof graphs are just as powerful as natural deduction.

All this happens with regard to an abstract set of formulas (theory *Abstract_Formula*) and an abstract set of logic rules (theory *Abstract_Rules*) and can thus be instantiated with various logics.

This formalization covers the following aspects:

- We formalize the definition of port graphs, proof graphs and the conditions for such a proof graph to be a valid graph (theory *Incredible_Deduction*).
- We provide a formal description of natural deduction (theory *Natural_Deduction*), which connects to the existing theories in the AFP entry Abstract Completeness [BPT14].
- For every proof graph, we construct a corresponding natural deduction derivation tree (theory *Incredible_Correctness*).
- Conversely, if we have a natural deduction derivation tree, we can construct a proof graph thereof (theory *Incredible_Completeness*).

This is the much harder direction, mostly because the freshness side condition for locally fixed constants (such as in the introduction rule for the universal quantifier) is a local check in natural deduction, but a global check in proofs graphs, and thus some elaborate renaming has to occur (*globalize* in *Incredible_Trees*).

- To explain our abstract locales, and ensure that the assumptions are consistent, we provide example instantiations for them.

It does not cover the unification procedure and expects that a suitable instantiation is already given. It also does not cover the creation and use of custom blocks, which abstract over proofs and thus correspond to lemmas in Isabelle.

Acknowledgements

We would like to thank Andreas Lochbihler for helpful comments.

References

- [BPT14] Jasmin Christian Blanchette, Andrei Popescu, and Dmitriy Traytel, *Abstract completeness*, Archive of Formal Proofs (2014), http://isa-afp.org/entries/Abstract_Completeness.shtml, Formal proof development.
- [Bre16] Joachim Breitner, *Visual theorem proving with the Incredible Proof Machine*, ITP, 2016.

2 Auxiliary theories

2.1 Entailment

```
theory Entailment
imports Main HOL-Library.FSet
begin

type-synonym 'form entailment = ('form fset × 'form)

abbreviation entails :: 'form fset ⇒ 'form ⇒ 'form entailment (infix † 50)
  where a † c ≡ (a, c)

fun add-ctxt :: 'form fset ⇒ 'form entailment ⇒ 'form entailment where
  add-ctxt Δ (Γ † c) = (Γ |∪| Δ † c)

end
```

2.2 Indexed_FSet

```
theory Indexed-FSet
imports
  HOL-Library.FSet
begin
```

It is convenient to address the members of a finite set by a natural number, and also to convert a finite set to a list.

```
context includes fset.lifting
begin
lift-definition fset-from-list :: 'a list => 'a fset is set <proof>
lemma mem-fset-from-list[simp]: x |∈| fset-from-list l ↔ x ∈ set l <proof>
lemma fimage-fset-from-list[simp]: f |`| fset-from-list l = fset-from-list (map f l) <proof>
lemma fset-fset-from-list[simp]: fset (fset-from-list l) = set l <proof>
lemmas fset-simps[simp] = set-simps[Transfer.transferred]
lemma size-fset-from-list[simp]: distinct l ⇒ size (fset-from-list l) = length l
  <proof>

definition list-of-fset :: 'a fset ⇒ 'a list where
  list-of-fset s = (SOME l. fset-from-list l = s ∧ distinct l)

lemma fset-from-list-of-fset[simp]: fset-from-list (list-of-fset s) = s
  and distinct-list-of-fset[simp]: distinct (list-of-fset s)
  <proof>

lemma length-list-of-fset[simp]: length (list-of-fset s) = size s
  <proof>

lemma nth-list-of-fset-mem[simp]: i < size s ⇒ list-of-fset s ! i |∈| s
  <proof>

inductive indexed-fmember :: 'a ⇒ nat ⇒ 'a fset ⇒ bool (- |∈| - [50,50,50] 50) where
  i < size s ⇒ list-of-fset s ! i |∈|i s

lemma indexed-fmember-is-fmember: x |∈|i s ⇒ x |∈| s
  <proof>
```

lemma *fmember-is-indexed-fmember*:

assumes $x \in s$
shows $\exists i. x \in_i s$

<proof>

lemma *indexed-fmember-unique*: $x \in_i s \implies y \in_j s \implies x = y \iff i = j$

<proof>

definition *indexed-members* :: $'a \text{ fset} \Rightarrow (\text{nat} \times 'a) \text{ list}$ **where**
indexed-members $s = \text{zip } [0..<\text{size } s] (\text{list-of-fset } s)$

lemma *mem-set-indexed-members*:

$(i,x) \in \text{set } (\text{indexed-members } s) \iff x \in_i s$

<proof>

lemma *mem-set-indexed-members'[simp]*:

$t \in \text{set } (\text{indexed-members } s) \iff \text{snd } t \in_{fst} t s$

<proof>

definition *fnth* (**infixl** $||$ 100) **where**

$s || n = \text{list-of-fset } s ! n$

lemma *fnth-indexed-fmember*: $i < \text{size } s \implies s || i \in_i s$

<proof>

lemma *indexed-fmember-fnth*: $x \in_i s \iff (s || i = x \wedge i < \text{size } s)$

<proof>

end

definition *fidx* :: $'a \text{ fset} \Rightarrow 'a \Rightarrow \text{nat}$ **where**

fidx $s x = (\text{SOME } i. x \in_i s)$

lemma *fidx-eq[simp]*: $x \in_i s \implies \text{fidx } s x = i$

<proof>

lemma *fidx-inj[simp]*: $x \in s \implies y \in s \implies \text{fidx } s x = \text{fidx } s y \iff x = y$

<proof>

lemma *inj-on-fidx*: *inj-on* (*fidx vertices*) (*fset vertices*)

<proof>

end

2.3 Rose_Tree

theory *Rose-Tree*

imports *Main HOL-Library.Sublist*

begin

For theory *Incredible-Trees* we need rose trees; this theory contains the generally useful part of that development.

2.3.1 The rose tree data type

datatype $'a \text{ rose-tree} = \text{RNode } (\text{root: } 'a) (\text{children: } 'a \text{ rose-tree list})$

2.3.2 The set of paths in a rose tree

Too bad that **inductive-set** does not allow for varying parameters...

inductive *it-pathsP* :: 'a rose-tree \Rightarrow nat list \Rightarrow bool **where**
it-paths-Nil: *it-pathsP* t []
| *it-paths-Cons*: $i < \text{length} (\text{children } t) \Longrightarrow \text{children } t ! i = t' \Longrightarrow \text{it-pathsP } t' \text{ is} \Longrightarrow \text{it-pathsP } t (i\#is)$

inductive-cases *it-pathP-ConsE*: *it-pathsP* t (i#is)

inductive-cases *it-pathP-RNodeE*: *it-pathsP* (RNode r ants) is

definition *it-paths*:: 'a rose-tree \Rightarrow nat list set **where**
it-paths t = Collect (*it-pathsP* t)

lemma *it-paths-eq* [*pred-set-conv*]: *it-pathsP* t = $(\lambda x. x \in \text{it-paths } t)$
<proof>

lemmas *it-paths-intros* [*intro?*] = *it-pathsP.intros*[*to-set*]

lemmas *it-paths-induct* [*consumes 1, induct set: it-paths*] = *it-pathsP.induct*[*to-set*]

lemmas *it-paths-cases* [*consumes 1, cases set: it-paths*] = *it-pathsP.cases*[*to-set*]

lemmas *it-paths-ConsE* = *it-pathP-ConsE*[*to-set*]

lemmas *it-paths-RNodeE* = *it-pathP-RNodeE*[*to-set*]

lemmas *it-paths-simps* = *it-pathsP.simps*[*to-set*]

lemmas *it-paths-intros*(1)[*simp*]

lemma *it-paths-RNode-Nil*[*simp*]: *it-paths* (RNode r []) = {[]}
<proof>

lemma *it-paths-Union*: *it-paths* t $\subseteq \text{insert } [] (\text{Union } (((\lambda (i,t). ((\#) i) \text{'it-paths } t) \text{'set } (\text{List.enumerate } (0::\text{nat}) (\text{children } t))))))$
<proof>

lemma *finite-it-paths*[*simp*]: *finite* (*it-paths* t)
<proof>

2.3.3 Indexing into a rose tree

fun *tree-at* :: 'a rose-tree \Rightarrow nat list \Rightarrow 'a rose-tree **where**
tree-at t [] = t
| *tree-at* t (i#is) = *tree-at* (*children* t ! i) is

lemma *it-paths-SnocE*[*elim-format*]:
assumes is @ [i] \in *it-paths* t
shows is \in *it-paths* t \wedge $i < \text{length} (\text{children } (\text{tree-at } t \text{ is}))$
<proof>

lemma *it-paths-strict-prefix*:
assumes is \in *it-paths* t
assumes *strict-prefix* is' is
shows is' \in *it-paths* t
<proof>

lemma *it-paths-prefix*:
assumes is \in *it-paths* t
assumes *prefix* is' is

shows $is' \in it\text{-paths } t$
 $\langle proof \rangle$

lemma *it-paths-butlast*:
assumes $is \in it\text{-paths } t$
shows $butlast\ is \in it\text{-paths } t$
 $\langle proof \rangle$

lemma *it-path-SnocI*:
assumes $is \in it\text{-paths } t$
assumes $i < length\ (children\ (tree\text{-at } t\ is))$
shows $is\ @\ [i] \in it\text{-paths } t$
 $\langle proof \rangle$

end

3 Abstract formulas, rules and tasks

3.1 Abstract_Formula

theory *Abstract-Formula*

imports

Main

HOL-Library.FSet

HOL-Library.Stream

Indexed-FSet

begin

The following locale describes an abstract interface for a set of formulas, without fixing the concret shape, or set of variables.

The variables mentioned in this locale are only the *locally fixed constants* occurring in formulas, e.g. in the introduction rule for the universal quantifier. Normal variables are not something we care about at this point; they are handled completely abstractly by the abstract notion of a substitution.

locale *Abstract-Formulas* =

— Variables can be renamed injectively

fixes *freshenLC* :: *nat* \Rightarrow *'var* \Rightarrow *'var*

— A variable-changing function can be mapped over a formula

fixes *renameLCs* :: (*'var* \Rightarrow *'var*) \Rightarrow (*'form* \Rightarrow *'form*)

— The set of variables occurring in a formula

fixes *lconsts* :: *'form* \Rightarrow *'var set*

— A closed formula has no variables, and substitutions do not affect it.

fixes *closed* :: *'form* \Rightarrow *bool*

— A substitution can be applied to a formula.

fixes *subst* :: *'subst* \Rightarrow *'form* \Rightarrow *'form*

— The set of variables occurring (in the image) of a substitution.

fixes *subst-lconsts* :: *'subst* \Rightarrow *'var set*

— A variable-changing function can be mapped over a substitution

fixes *subst-renameLCs* :: (*'var* \Rightarrow *'var*) \Rightarrow (*'subst* \Rightarrow *'subst*)

— A most generic formula, can be substituted to anything.

fixes *anyP* :: *'form*

assumes *freshenLC-eq-iff[simp]*: *freshenLC* *a v* = *freshenLC* *a' v'* \iff *a* = *a'* \wedge *v* = *v'*

assumes *lconsts-renameLCs*: *lconsts* (*renameLCs* *p f*) = *p* ' *lconsts* *f*

assumes *rename-closed*: *lconsts* *f* = {} \implies *renameLCs* *p f* = *f*

assumes *subst-closed*: *closed* *f* \implies *subst* *s f* = *f*

assumes *closed-no-lconsts*: *closed* *f* \implies *lconsts* *f* = {}

assumes *fv-subst*: *lconsts* (*subst* *s f*) \subseteq *lconsts* *f* \cup *subst-lconsts* *s*

assumes *rename-rename*: *renameLCs* *p1* (*renameLCs* *p2 f*) = *renameLCs* (*p1* \circ *p2*) *f*

assumes *rename-subst*: *renameLCs* *p* (*subst* *s f*) = *subst* (*subst-renameLCs* *p s*) (*renameLCs* *p f*)

assumes *renameLCs-cong*: ($\bigwedge x. x \in \text{lconsts } f \implies f1\ x = f2\ x$) \implies *renameLCs* *f1 f* = *renameLCs* *f2 f*

assumes *subst-renameLCs-cong*: ($\bigwedge x. x \in \text{subst-lconsts } s \implies f1\ x = f2\ x$) \implies *subst-renameLCs* *f1 s* = *subst-renameLCs* *f2 s*

assumes *subst-lconsts-subst-renameLCs*: *subst-lconsts* (*subst-renameLCs* *p s*) = *p* ' *subst-lconsts* *s*

assumes *lconsts-anyP*: *lconsts* *anyP* = {}

assumes *empty-subst*: $\exists s. (\forall f. \text{subst } s\ f = f) \wedge \text{subst-lconsts } s = \{\}$

assumes *anyP-is-any*: $\exists s. \text{subst } s\ \text{anyP} = f$

begin

definition *freshen* :: *nat* \Rightarrow *'form* \Rightarrow *'form* **where**

freshen *n* = *renameLCs* (*freshenLC* *n*)

definition *empty-subst* :: *'subst* **where**

$empty_subst = (SOME\ s.\ (\forall\ f.\ subst\ s\ f = f) \wedge subst_lconsts\ s = \{\})$

lemma *empty-subst-spec*:

$(\forall\ f.\ subst\ empty_subst\ f = f) \wedge subst_lconsts\ empty_subst = \{\}$
 $\langle proof \rangle$

lemma *subst-empty-subst[simp]*: $subst\ empty_subst\ f = f$

$\langle proof \rangle$

lemma *subst-lconsts-empty-subst[simp]*: $subst_lconsts\ empty_subst = \{\}$

$\langle proof \rangle$

lemma *lconsts-freshen*: $lconsts\ (freshen\ a\ f) = freshenLC\ a\ 'lconsts\ f$

$\langle proof \rangle$

lemma *freshen-closed*: $lconsts\ f = \{\} \implies freshen\ a\ f = f$

$\langle proof \rangle$

lemma *closed-eq*:

assumes *closed f1*

assumes *closed f2*

shows $subst\ s1\ (freshen\ a1\ f1) = subst\ s2\ (freshen\ a2\ f2) \longleftrightarrow f1 = f2$

$\langle proof \rangle$

lemma *freshenLC-range-eq-iff[simp]*: $freshenLC\ a\ v \in range\ (freshenLC\ a') \longleftrightarrow a = a'$

$\langle proof \rangle$

definition *rename* :: $'var\ set \Rightarrow nat \Rightarrow nat \Rightarrow ('var \Rightarrow 'var) \Rightarrow ('var \Rightarrow 'var)$ **where**

$rename\ V\ from\ to\ f\ x = (if\ x \in freshenLC\ from\ 'V\ then\ freshenLC\ to\ (inv\ (freshenLC\ from)\ x)\ else\ f\ x)$

lemma *inj-freshenLC[simp]*: $inj\ (freshenLC\ i)$

$\langle proof \rangle$

lemma *rename-freshen[simp]*: $x \in V \implies rename\ V\ i\ (isidx\ is)\ f\ (freshenLC\ i\ x) = freshenLC\ (isidx\ is)$

x

$\langle proof \rangle$

lemma *range-rename*: $range\ (rename\ V\ from\ to\ f) \subseteq freshenLC\ to\ 'V \cup range\ f$

$\langle proof \rangle$

lemma *rename-noop*:

$x \notin freshenLC\ from\ 'V \implies rename\ V\ from\ to\ f\ x = f\ x$

$\langle proof \rangle$

lemma *rename-rename-noop*:

$freshenLC\ from\ 'V \cap lconsts\ form = \{\} \implies renameLCs\ (rename\ V\ from\ to\ f)\ form = renameLCs\ f$

$form$

$\langle proof \rangle$

lemma *rename-subst-noop*:

$freshenLC\ from\ 'V \cap subst_lconsts\ s = \{\} \implies subst_renameLCs\ (rename\ V\ from\ to\ f)\ s =$

$subst_renameLCs\ f\ s$

$\langle proof \rangle$

end

end

3.2 Abstract_Rules

theory *Abstract-Rules*

```

imports
  Abstract-Formula
begin

```

Next, we can define a logic, by giving a set of rules.

In order to connect to the AFP entry Abstract Completeness, the set of rules is a stream; the only relevant effect of this is that the set is guaranteed to be non-empty and at most countable. This has no further significance in our development.

Each antecedent of a rule consists of

- a set of fresh variables
- a set of hypotheses that may be used in proving the conclusion of the antecedent and
- the conclusion of the antecedent.

Our rules allow for multiple conclusions (but must have at least one).

In order to prove the completeness (but incidentally not to prove correctness) of the incredible proof graphs, there are some extra conditions about the fresh variables in a rule.

- These need to be disjoint for different antecedents.
- They need to list all local variables occurring in either the hypothesis and the conclusion.
- The conclusions of a rule must not contain any local variables.

```

datatype ('form, 'var) antecedent =
  Antecedent (a-hyps: 'form fset) (a-conc: 'form) (a-fresh: 'var set)

```

```

abbreviation plain-ant :: 'form  $\Rightarrow$  ('form, 'var) antecedent
where plain-ant f  $\equiv$  Antecedent {||} f {}

```

```

locale Abstract-Rules =
  Abstract-Formulas freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP
for freshenLC :: nat  $\Rightarrow$  'var  $\Rightarrow$  'var
and renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  ('form  $\Rightarrow$  'form)
and lconsts :: 'form  $\Rightarrow$  'var set
and closed :: 'form  $\Rightarrow$  bool
and subst :: 'subst  $\Rightarrow$  'form  $\Rightarrow$  'form
and subst-lconsts :: 'subst  $\Rightarrow$  'var set
and subst-renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  ('subst  $\Rightarrow$  'subst)
and anyP :: 'form +

```

```

fixes antecedent :: 'rule  $\Rightarrow$  ('form, 'var) antecedent list
and consequent :: 'rule  $\Rightarrow$  'form list
and rules :: 'rule stream

```

```

assumes no-empty-conclusions:  $\forall xs \in sset \text{ rules. consequent } xs \neq []$ 

```

```

assumes no-local-consts-in-consequences:  $\forall xs \in sset \text{ rules. } \bigcup (lconsts \text{ ' (set (consequent } xs))) = \{\}$ 

```

```

assumes no-multiple-local-consts:

```

```

 $\bigwedge r \ i \ i'. r \in sset \text{ rules} \implies$ 
   $i < \text{length (antecedent } r) \implies$ 
   $i' < \text{length (antecedent } r) \implies$ 
   $a\text{-fresh (antecedent } r \ ! \ i) \cap a\text{-fresh (antecedent } r \ ! \ i') = \{\} \vee i = i'$ 

```

```

assumes all-local-consts-listed:

```

```

 $\bigwedge r \ p. r \in sset \text{ rules} \implies p \in \text{set (antecedent } r) \implies$ 

```

$$lconsts (a-conc p) \cup (\bigcup (lconsts 'fset (a-hyps p))) \subseteq a-fresh p$$

begin
definition *f-antecedent* :: 'rule \Rightarrow ('form, 'var) antecedent fset
where *f-antecedent* r = fset-from-list (antecedent r)
definition *f-consequent* r = fset-from-list (consequent r)
end

Finally, an abstract task specifies what a specific proof should prove. In particular, it gives a set of assumptions that may be used, and lists the conclusions that need to be proven.

Both assumptions and conclusions are closed expressions that may not be changed by substitutions.

locale *Abstract-Task* =

Abstract-Rules freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP antecedent consequent rules

for *freshenLC* :: nat \Rightarrow 'var \Rightarrow 'var
and *renameLCs* :: ('var \Rightarrow 'var) \Rightarrow ('form \Rightarrow 'form)
and *lconsts* :: 'form \Rightarrow 'var set
and *closed* :: 'form \Rightarrow bool
and *subst* :: 'subst \Rightarrow 'form \Rightarrow 'form
and *subst-lconsts* :: 'subst \Rightarrow 'var set
and *subst-renameLCs* :: ('var \Rightarrow 'var) \Rightarrow ('subst \Rightarrow 'subst)
and *anyP* :: 'form
and *antecedent* :: 'rule \Rightarrow ('form, 'var) antecedent list
and *consequent* :: 'rule \Rightarrow 'form list
and *rules* :: 'rule stream +

fixes *assumptions* :: 'form list

fixes *conclusions* :: 'form list

assumes *assumptions-closed*: $\bigwedge a. a \in \text{set } assumptions \implies \text{closed } a$

assumes *conclusions-closed*: $\bigwedge c. c \in \text{set } conclusions \implies \text{closed } c$

begin

definition *ass-forms* **where** *ass-forms* = fset-from-list *assumptions*

definition *conc-forms* **where** *conc-forms* = fset-from-list *conclusions*

lemma *mem-ass-forms[simp]*: $a \in | \text{ass-forms} \iff a \in \text{set } assumptions$
 <proof>

lemma *mem-conc-forms[simp]*: $a \in | \text{conc-forms} \iff a \in \text{set } conclusions$
 <proof>

lemma *subst-freshen-assumptions[simp]*:

assumes $pf \in \text{set } assumptions$

shows $\text{subst } s (\text{freshen } a \text{ } pf) = pf$

<proof>

lemma *subst-freshen-conclusions[simp]*:

assumes $pf \in \text{set } conclusions$

shows $\text{subst } s (\text{freshen } a \text{ } pf) = pf$

<proof>

lemma *subst-freshen-in-ass-formsI*:

assumes $pf \in \text{set } assumptions$

shows $\text{subst } s (\text{freshen } a \text{ } pf) \in | \text{ass-forms}$

<proof>

lemma *subst-freshen-in-conc-formsI*:

assumes $pf \in \text{set } conclusions$

shows *subst s (freshen a pf) |∈| conc-forms*
 <proof>
end

end

4 Incredible Proof Graphs

4.1 Incredible_Signatures

```
theory Incredible-Signatures
imports
  Main
  HOL-Library.FSet
  HOL-Library.Stream
  Abstract-Formula
begin
```

This theory contains the definition for proof graph signatures, in the variants

- Plain port graph
- Port graph with local hypotheses
- Labeled port graph
- Port graph with local constants

```
locale Port-Graph-Signature =
  fixes nodes :: 'node stream
  fixes inPorts :: 'node  $\Rightarrow$  'inPort fset
  fixes outPorts :: 'node  $\Rightarrow$  'outPort fset

locale Port-Graph-Signature-Scoped =
  Port-Graph-Signature +
  fixes hysps :: 'node  $\Rightarrow$  'outPort  $\rightarrow$  'inPort
  assumes hysps-correct: hysps n p1 = Some p2  $\implies$  p1  $\in$  outPorts n  $\wedge$  p2  $\in$  inPorts n
begin
  inductive-set hysps-for' :: 'node  $\Rightarrow$  'inPort  $\Rightarrow$  'outPort set for n p
    where hysps n h = Some p  $\implies$  h  $\in$  hysps-for' n p

  lemma hysps-for'-subset: hysps-for' n p  $\subseteq$  fset (outPorts n)
    <proof>

  context includes fset.lifting
  begin
  lift-definition hysps-for :: 'node  $\Rightarrow$  'inPort  $\Rightarrow$  'outPort fset is hysps-for'
    <proof>
  lemma hysps-for-simp[simp]: h  $\in$  hysps-for n p  $\longleftrightarrow$  hysps n h = Some p
    <proof>
  lemma hysps-for-simp'[simp]: h  $\in$  fset (hysps-for n p)  $\longleftrightarrow$  hysps n h = Some p
    <proof>
  lemma hysps-for-collect: fset (hysps-for n p) = {h . hysps n h = Some p}
    <proof>
  end
  lemma hysps-for-subset: hysps-for n p  $\subseteq$  outPorts n
    <proof>
end

locale Labeled-Signature =
  Port-Graph-Signature-Scoped +
  fixes labelsIn :: 'node  $\Rightarrow$  'inPort  $\Rightarrow$  'form
  fixes labelsOut :: 'node  $\Rightarrow$  'outPort  $\Rightarrow$  'form
```

```

locale Port-Graph-Signature-Scoped-Vars =
  Port-Graph-Signature nodes inPorts outPorts +
  Abstract-Formulas freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP
for nodes :: 'node stream and inPorts :: 'node  $\Rightarrow$  'inPort fset and outPorts :: 'node  $\Rightarrow$  'outPort fset
and freshenLC :: nat  $\Rightarrow$  'var  $\Rightarrow$  'var
  and renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  'form  $\Rightarrow$  'form
  and lconsts :: 'form  $\Rightarrow$  'var set
  and closed :: 'form  $\Rightarrow$  bool
  and subst :: 'subst  $\Rightarrow$  'form  $\Rightarrow$  'form
  and subst-lconsts :: 'subst  $\Rightarrow$  'var set
  and subst-renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  ('subst  $\Rightarrow$  'subst)
  and anyP :: 'form +

  fixes local-vars :: 'node  $\Rightarrow$  'inPort  $\Rightarrow$  'var set

end

```

4.2 Incredible_Deduction

```

theory Incredible-Deduction
imports
  Main
  HOL-Library.FSet
  HOL-Library.Stream
  Incredible-Signatures
  HOL-Eisbach.Eisbach
begin

```

This theory contains the definition for actual proof graphs, and their various possible properties.

The following locale first defines graphs, without edges.

```

locale Vertex-Graph =
  Port-Graph-Signature nodes inPorts outPorts
  for nodes :: 'node stream
  and inPorts :: 'node  $\Rightarrow$  'inPort fset
  and outPorts :: 'node  $\Rightarrow$  'outPort fset +
  fixes vertices :: 'v fset
  fixes nodeOf :: 'v  $\Rightarrow$  'node
begin
  fun valid-out-port where valid-out-port (v,p)  $\longleftrightarrow$  v  $\in$  vertices  $\wedge$  p  $\in$  outPorts (nodeOf v)
  fun valid-in-port where valid-in-port (v,p)  $\longleftrightarrow$  v  $\in$  vertices  $\wedge$  p  $\in$  inPorts (nodeOf v)

  fun terminal-node where
    terminal-node n  $\longleftrightarrow$  outPorts n = {}
  fun terminal-vertex where
    terminal-vertex v  $\longleftrightarrow$  v  $\in$  vertices  $\wedge$  terminal-node (nodeOf v)
end

```

And now we add the edges. This allows us to define paths and scopes.

```

type-synonym ('v, 'outPort, 'inPort) edge = (('v  $\times$  'outPort)  $\times$  ('v  $\times$  'inPort))

```

```

locale Pre-Port-Graph =
  Vertex-Graph nodes inPorts outPorts vertices nodeOf
  for nodes :: 'node stream

```

```

and inPorts :: 'node ⇒ 'inPort fset
and outPorts :: 'node ⇒ 'outPort fset
and vertices :: 'v fset
and nodeOf :: 'v ⇒ 'node +
fixes edges :: ('v, 'outPort, 'inPort) edge set
begin
fun edge-begin :: (('v × 'outPort) × ('v × 'inPort)) ⇒ 'v where
  edge-begin ((v1,p1),(v2,p2)) = v1
fun edge-end :: (('v × 'outPort) × ('v × 'inPort)) ⇒ 'v where
  edge-end ((v1,p1),(v2,p2)) = v2

lemma edge-begin-tup: edge-begin x = fst (fst x) ⟨proof⟩
lemma edge-end-tup: edge-end x = fst (snd x) ⟨proof⟩

inductive path :: 'v ⇒ 'v ⇒ ('v, 'outPort, 'inPort) edge list ⇒ bool where
  path-empty: path v v [] |
  path-cons: e ∈ edges ⇒ path (edge-end e) v' pth ⇒ path (edge-begin e) v' (e#pth)

inductive-simps path-cons-simp': path v v' (e#pth)
inductive-simps path-empty-simp[simp]: path v v' []
lemma path-cons-simp: path v v' (e # pth) ⟷ fst (fst e) = v ∧ e ∈ edges ∧ path (fst (snd e)) v' pth
  ⟨proof⟩

lemma path-appendI: path v v' pth1 ⇒ path v' v'' pth2 ⇒ path v v'' (pth1@pth2)
  ⟨proof⟩

lemma path-split: path v v' (pth1@[e]@pth2) ⟷ path v (edge-end e) (pth1@[e]) ∧ path (edge-end e) v'
pth2
  ⟨proof⟩

lemma path-split2: path v v' (pth1@(e#pth2)) ⟷ path v (edge-begin e) pth1 ∧ path (edge-begin e) v'
(e#pth2)
  ⟨proof⟩

lemma path-snoc: path v v' (pth1@[e]) ⟷ e ∈ edges ∧ path v (edge-begin e) pth1 ∧ edge-end e = v'
  ⟨proof⟩

inductive-set scope :: 'v × 'inPort ⇒ 'v set for ps where
  v |e| vertices ⇒ (∧ pth v'. path v v' pth ⇒ terminal-vertex v' ⇒ ps ∈ snd ' set pth)
  ⇒ v ∈ scope ps

lemma scope-find:
  assumes v ∈ scope ps
  assumes terminal-vertex v'
  assumes path v v' pth
  shows ps ∈ snd ' set pth
  ⟨proof⟩

lemma snd-set-split:
  assumes ps ∈ snd ' set pth
  obtains pth1 pth2 e where pth = pth1@[e]@pth2 and snd e = ps and ps ∉ snd ' set pth1
  ⟨proof⟩

lemma scope-split:
  assumes v ∈ scope ps
  assumes path v v' pth
  assumes terminal-vertex v'

```

```

obtains  $pth1\ e\ pth2$ 
where  $pth = (pth1@[e])@pth2$  and  $path\ v\ (fst\ ps)\ (pth1@[e])$  and  $path\ (fst\ ps)\ v'\ pth2$  and  $snd\ e = ps$ 
and  $ps \notin\ snd\ 'set\ pth1$ 
 $\langle proof \rangle$ 
end

```

This adds well-formedness conditions to the edges and vertices.

```

locale  $Port-Graph = Pre-Port-Graph +$ 
assumes  $valid-nodes: nodeOf\ 'fset\ vertices \subseteq\ sset\ nodes$ 
assumes  $valid-edges: \forall\ (ps1,ps2) \in\ edges.\ valid-out-port\ ps1 \wedge\ valid-in-port\ ps2$ 
begin
lemma  $snd-set-path-verties: path\ v\ v'\ pth \implies\ fst\ 'snd\ 'set\ pth \subseteq\ fset\ vertices$ 
 $\langle proof \rangle$ 

lemma  $fst-set-path-verties: path\ v\ v'\ pth \implies\ fst\ 'fst\ 'set\ pth \subseteq\ fset\ vertices$ 
 $\langle proof \rangle$ 
end

```

A pruned graph is one where every node has a path to a terminal node (which will be the conclusions).

```

locale  $Pruned-Port-Graph = Port-Graph +$ 
assumes  $pruned: \bigwedge\ v.\ v\ |\in|\ vertices \implies\ (\exists\ pth\ v'.\ path\ v\ v'\ pth \wedge\ terminal-vertex\ v')$ 
begin
lemma  $scopes-not-refl:$ 
assumes  $v\ |\in|\ vertices$ 
shows  $v \notin\ scope\ (v,p)$ 
 $\langle proof \rangle$ 

```

This lemma can be found in [Bre16], but it is otherwise inconsequential.

```

lemma  $scopes-nest:$ 
fixes  $ps1\ ps2$ 
shows  $scope\ ps1 \subseteq\ scope\ ps2 \vee\ scope\ ps2 \subseteq\ scope\ ps1 \vee\ scope\ ps1 \cap\ scope\ ps2 = \{\}$ 
 $\langle proof \rangle$ 
end

```

A well-scoped graph is one where a port marked to be a local hypothesis is only connected to the corresponding input port, either directly or via a path. It must not be, however, that there is a path from such a hypothesis to a terminal node that does not pass by the dedicated input port; this is expressed via scopes.

```

locale  $Scoped-Graph = Port-Graph + Port-Graph-Signature-Scoped$ 
locale  $Well-Scoped-Graph = Scoped-Graph +$ 
assumes  $well-scoped: ((v_1,p_1),(v_2,p_2)) \in\ edges \implies\ hyps\ (nodeOf\ v_1)\ p_1 = Some\ p' \implies\ (v_2,p_2) = (v_1,p') \vee\ v_2 \in\ scope\ (v_1,p')$ 

```

```

context  $Scoped-Graph$ 
begin

```

```

definition  $hyps-free\ where$ 
 $hyps-free\ pth = (\forall\ v_1\ p_1\ v_2\ p_2.\ ((v_1,p_1),(v_2,p_2)) \in\ set\ pth \longrightarrow\ hyps\ (nodeOf\ v_1)\ p_1 = None)$ 

```

```

lemma  $hyps-free-Nil[simp]: hyps-free\ []\ \langle proof \rangle$ 

```

```

lemma  $hyps-free-Cons[simp]: hyps-free\ (e\#\ pth) \longleftrightarrow\ hyps-free\ pth \wedge\ hyps\ (nodeOf\ (fst\ (fst\ e)))\ (snd\ (fst\ e)) = None$ 
 $\langle proof \rangle$ 

```


lemma *path-vertices-shift*:
assumes *path v v' pth*
shows $\text{map fst (map fst pth)}@[v'] = v\#\text{map fst (map snd pth)}$
 $\langle\text{proof}\rangle$

inductive *terminal-path* **where**
terminal-path-empty: $\text{terminal-vertex } v \implies \text{terminal-path } v \ [] \ |$
terminal-path-cons: $((v_1,p_1),(v_2,p_2)) \in \text{edges} \implies \text{terminal-path } v_2 \ v' \ pth \implies \text{hyps (nodeOf } v_1) \ p_1 = \text{None}$
 $\implies \text{terminal-path } v_1 \ v' \ (((v_1,p_1),(v_2,p_2))\#pth)$

lemma *terminal-path-is-path*:
assumes *terminal-path v v' pth*
shows *path v v' pth*
 $\langle\text{proof}\rangle$

lemma *terminal-path-is-hyps-free*:
assumes *terminal-path v v' pth*
shows *hyps-free pth*
 $\langle\text{proof}\rangle$

lemma *terminal-path-end-is-terminal*:
assumes *terminal-path v v' pth*
shows *terminal-vertex v'*
 $\langle\text{proof}\rangle$

lemma *terminal-pathI*:
assumes *path v v' pth*
assumes *hyps-free pth*
assumes *terminal-vertex v'*
shows *terminal-path v v' pth*
 $\langle\text{proof}\rangle$
end

An acyclic graph is one where there are no non-trivial cyclic paths (disregarding edges that are local hypotheses – these are naturally and benignly cyclic).

locale *Acyclic-Graph = Scoped-Graph +*
assumes *hyps-free-acyclic*: $\text{path } v \ v \ pth \implies \text{hyps-free } pth \implies pth = []$
begin

lemma *hyps-free-vertices-distinct*:
assumes *terminal-path v v' pth*
shows $\text{distinct (map fst (map fst pth)}@[v'])$
 $\langle\text{proof}\rangle$

lemma *hyps-free-vertices-distinct'*:
assumes *terminal-path v v' pth*
shows $\text{distinct (v \# map fst (map snd pth))}$
 $\langle\text{proof}\rangle$

lemma *hyps-free-limited*:
assumes *terminal-path v v' pth*
shows $\text{length } pth \leq \text{fcard vertices}$
 $\langle\text{proof}\rangle$

lemma *hyps-free-path-not-in-scope*:
assumes *terminal-path v t pth*
assumes $(v',p') \in \text{snd ' set } pth$

shows $v' \notin \text{scope}(v, p)$
 $\langle \text{proof} \rangle$

end

A saturated graph is one where every input port is incident to an edge.

locale *Saturated-Graph* = *Port-Graph* +
assumes *saturated*: $\text{valid-in-port}(v, p) \implies \exists e \in \text{edges} . \text{snd } e = (v, p)$

These four conditions make up a well-shaped graph.

locale *Well-Shaped-Graph* = *Well-Scoped-Graph* + *Acyclic-Graph* + *Saturated-Graph* + *Pruned-Port-Graph*

Next we demand an instantiation. This consists of a unique natural number per vertex, in order to rename the local constants apart, and furthermore a substitution per block which instantiates the schematic formulas given in *Labeled-Signature*.

locale *Instantiation* =
Vertex-Graph nodes - - *vertices* - +
Labeled-Signature nodes - - - *labelsIn labelsOut* +
Abstract-Formulas freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP
for *nodes* :: 'node stream **and** *edges* :: ('vertex, 'outPort, 'inPort) edge set **and** *vertices* :: 'vertex fset **and**
labelsIn :: 'node \Rightarrow 'inPort \Rightarrow 'form **and** *labelsOut* :: 'node \Rightarrow 'outPort \Rightarrow 'form
and *freshenLC* :: nat \Rightarrow 'var \Rightarrow 'var
and *renameLCs* :: ('var \Rightarrow 'var) \Rightarrow 'form \Rightarrow 'form
and *lconsts* :: 'form \Rightarrow 'var set
and *closed* :: 'form \Rightarrow bool
and *subst* :: 'subst \Rightarrow 'form \Rightarrow 'form
and *subst-lconsts* :: 'subst \Rightarrow 'var set
and *subst-renameLCs* :: ('var \Rightarrow 'var) \Rightarrow ('subst \Rightarrow 'subst)
and *anyP* :: 'form +
fixes *vidx* :: 'vertex \Rightarrow nat
and *inst* :: 'vertex \Rightarrow 'subst
assumes *vidx-inj*: *inj-on vidx* (fset *vertices*)
begin
definition *labelAtIn* :: 'vertex \Rightarrow 'inPort \Rightarrow 'form **where**
labelAtIn v p = *subst* (*inst* v) (*freshen* (*vidx* v) (*labelsIn* (*nodeOf* v) p))
definition *labelAtOut* :: 'vertex \Rightarrow 'outPort \Rightarrow 'form **where**
labelAtOut v p = *subst* (*inst* v) (*freshen* (*vidx* v) (*labelsOut* (*nodeOf* v) p))
end

A solution is an instantiation where on every edge, both incident ports are labeled with the same formula.

locale *Solution* =
Instantiation - - - - *edges* **for** *edges* :: (('vertex \times 'outPort) \times 'vertex \times 'inPort) set +
assumes *solved*: $((v_1, p_1), (v_2, p_2)) \in \text{edges} \implies \text{labelAtOut } v_1 \ p_1 = \text{labelAtIn } v_2 \ p_2$

locale *Proof-Graph* = *Well-Shaped-Graph* + *Solution*

If we have locally scoped constants, we demand that only blocks in the scope of the corresponding input port may mention such a locally scoped variable in its substitution.

locale *Well-Scoped-Instantiation* =
Pre-Port-Graph nodes inPorts outPorts vertices nodeOf edges +
Instantiation inPorts outPorts nodeOf hyps nodes edges vertices labelsIn labelsOut freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP vidx inst +

```

Port-Graph-Signature-Scoped-Vars nodes inPorts outPorts freshenLC renameLCs lconsts closed subst subst-lconsts
subst-renameLCs anyP local-vars
for freshenLC :: nat ⇒ 'var ⇒ 'var
and renameLCs :: ('var ⇒ 'var) ⇒ 'form ⇒ 'form
and lconsts :: 'form ⇒ 'var set
and closed :: 'form ⇒ bool
and subst :: 'subst ⇒ 'form ⇒ 'form
and subst-lconsts :: 'subst ⇒ 'var set
and subst-renameLCs :: ('var ⇒ 'var) ⇒ ('subst ⇒ 'subst)
and anyP :: 'form
and inPorts :: 'node ⇒ 'inPort fset
and outPorts :: 'node ⇒ 'outPort fset
and nodeOf :: 'vertex ⇒ 'node
and hyps :: 'node ⇒ 'outPort ⇒ 'inPort option
and nodes :: 'node stream
and vertices :: 'vertex fset
and labelsIn :: 'node ⇒ 'inPort ⇒ 'form
and labelsOut :: 'node ⇒ 'outPort ⇒ 'form
and vidx :: 'vertex ⇒ nat
and inst :: 'vertex ⇒ 'subst
and edges :: ('vertex, 'outPort, 'inPort) edge set
and local-vars :: 'node ⇒ 'inPort ⇒ 'var set +
assumes well-scoped-inst:
  valid-in-port (v,p) ⇒
    var ∈ local-vars (nodeOf v) p ⇒
    v' |∈| vertices ⇒
    freshenLC (vidx v) var ∈ subst-lconsts (inst v') ⇒
    v' ∈ scope (v,p)
begin
  lemma out-of-scope: valid-in-port (v,p) ⇒ v' |∈| vertices ⇒ v' ∉ scope (v,p) ⇒ freshenLC (vidx v) '
    local-vars (nodeOf v) p ∩ subst-lconsts (inst v') = {}
    ⟨proof⟩
end

```

The following locale assembles all these conditions.

```

locale Scoped-Proof-Graph =
  Instantiation inPorts outPorts nodeOf hyps nodes edges vertices labelsIn labelsOut freshenLC renameLCs
  lconsts closed subst subst-lconsts subst-renameLCs anyP vidx inst +
  Well-Shaped-Graph nodes inPorts outPorts vertices nodeOf edges hyps +
  Solution inPorts outPorts nodeOf hyps nodes vertices labelsIn labelsOut freshenLC renameLCs lconsts closed
  subst subst-lconsts subst-renameLCs anyP vidx inst edges +
  Well-Scoped-Instantiation freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP
  inPorts outPorts nodeOf hyps nodes vertices labelsIn labelsOut vidx inst edges local-vars
for freshenLC :: nat ⇒ 'var ⇒ 'var
and renameLCs :: ('var ⇒ 'var) ⇒ 'form ⇒ 'form
and lconsts :: 'form ⇒ 'var set
and closed :: 'form ⇒ bool
and subst :: 'subst ⇒ 'form ⇒ 'form
and subst-lconsts :: 'subst ⇒ 'var set
and subst-renameLCs :: ('var ⇒ 'var) ⇒ ('subst ⇒ 'subst)
and anyP :: 'form
and inPorts :: 'node ⇒ 'inPort fset
and outPorts :: 'node ⇒ 'outPort fset
and nodeOf :: 'vertex ⇒ 'node
and hyps :: 'node ⇒ 'outPort ⇒ 'inPort option
and nodes :: 'node stream
and vertices :: 'vertex fset

```

```

and labelsIn :: 'node ⇒ 'inPort ⇒ 'form
and labelsOut :: 'node ⇒ 'outPort ⇒ 'form
and vidx :: 'vertex ⇒ nat
and inst :: 'vertex ⇒ 'subst
and edges :: ('vertex, 'outPort, 'inPort) edge set
and local-vars :: 'node ⇒ 'inPort ⇒ 'var set

```

end

4.3 Abstract_Rules_To_Incredible

```

theory Abstract-Rules-To-Incredible
imports
  Main
  HOL-Library.FSet
  HOL-Library.Stream
  Incredible-Deduction
  Abstract-Rules
begin

```

In this theory, the abstract rules given in *Incredible-Proof-Machine.Abstract-Rules* are used to create a proper signature.

Besides the rules given there, we have nodes for assumptions, conclusions, and the helper block.

```

datatype ('form, 'rule) graph-node = Assumption 'form | Conclusion 'form | Rule 'rule | Helper

```

```

type-synonym ('form, 'var) in-port = ('form, 'var) antecedent

```

```

type-synonym 'form reg-out-port = 'form

```

```

type-synonym 'form hyp = 'form

```

```

datatype ('form, 'var) out-port = Reg 'form reg-out-port | Hyp 'form hyp ('form, 'var) in-port

```

```

type-synonym ('v, 'form, 'var) edge' = (('v × ('form, 'var) out-port) × ('v × ('form, 'var) in-port))

```

```

context Abstract-Task

```

```

begin

```

```

definition nodes :: ('form, 'rule) graph-node stream where

```

```

  nodes = Helper ## shift (map Assumption assumptions) (shift (map Conclusion conclusions) (smap Rule
rules))

```

```

lemma Helper-in-nodes[simp]:

```

```

  Helper ∈ sset nodes ⟨proof⟩

```

```

lemma Assumption-in-nodes[simp]:

```

```

  Assumption a ∈ sset nodes ⟷ a ∈ set assumptions ⟨proof⟩

```

```

lemma Conclusion-in-nodes[simp]:

```

```

  Conclusion c ∈ sset nodes ⟷ c ∈ set conclusions ⟨proof⟩

```

```

lemma Rule-in-nodes[simp]:

```

```

  Rule r ∈ sset nodes ⟷ r ∈ sset rules ⟨proof⟩

```

```

fun inPorts' :: ('form, 'rule) graph-node ⇒ ('form, 'var) in-port list where

```

```

  inPorts' (Rule r) = antecedent r

```

```

| inPorts' (Assumption r) = []

```

```

| inPorts' (Conclusion r) = [ plain-ant r ]

```

```

| inPorts' Helper = [ plain-ant anyP ]

```

```

fun inPorts :: ('form, 'rule) graph-node ⇒ ('form, 'var) in-port fset where

```

```

  inPorts (Rule r) = f-antecedent r

```

```

| inPorts (Assumption r) = {||}

```

```

|inPorts (Conclusion r) = {| plain-ant r |}
|inPorts Helper = {| plain-ant anyP |}

```

lemma *inPorts-fset-of*:

```

inPorts n = fset-from-list (inPorts' n)
⟨proof⟩

```

definition *outPortsRule* **where**

```

outPortsRule r = ffUnion ((λ a. (λ h. Hyp h a) |' a-hyps a) |' f-antecedent r) |∪| Reg |' f-consequent r

```

lemma *Reg-in-outPortsRule[simp]*: $Reg\ c\ |\in|\ outPortsRule\ r\ \longleftrightarrow\ c\ |\in|\ f-consequent\ r$

⟨proof⟩

lemma *Hyp-in-outPortsRule[simp]*: $Hyp\ h\ c\ |\in|\ outPortsRule\ r\ \longleftrightarrow\ c\ |\in|\ f-antecedent\ r\ \wedge\ h\ |\in|\ a-hyps\ c$

⟨proof⟩

fun *outPorts* **where**

```

outPorts (Rule r) = outPortsRule r
|outPorts (Assumption r) = {| Reg r |}
|outPorts (Conclusion r) = {| |}
|outPorts Helper = {| Reg anyP |}

```

fun *labelsIn* **where**

```

labelsIn - p = a-conc p

```

fun *labelsOut* **where**

```

labelsOut - (Reg p) = p
| labelsOut - (Hyp h c) = h

```

fun *hyps* **where**

```

hyps (Rule r) (Hyp h a) = (if a |\in| f-antecedent r \wedge h |\in| a-hyps a then Some a else None)
| hyps - - = None

```

fun *local-vars* :: ('form, 'rule) graph-node \Rightarrow ('form, 'var) in-port \Rightarrow 'var set **where**

```

local-vars - a = a-fresh a

```

sublocale *Labeled-Signature nodes inPorts outPorts hyps labelsIn labelsOut*

⟨proof⟩

lemma *hyps-for-conclusion[simp]*: $hyps-for\ (Conclusion\ n)\ p = \{| |}$

⟨proof⟩

lemma *hyps-for-Helper[simp]*: $hyps-for\ Helper\ p = \{| |}$

⟨proof⟩

lemma *hyps-for-Rule[simp]*: $ip\ |\in|\ f-antecedent\ r\ \Longrightarrow\ hyps-for\ (Rule\ r)\ ip = (\lambda\ h.\ Hyp\ h\ ip)\ |' a-hyps\ ip$

⟨proof⟩

end

Finally, a given proof graph solves the task at hand if all the given conclusions are present as conclusion blocks in the graph.

locale *Tasked-Proof-Graph* =

Abstract-Task freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP antecedent consequent rules assumptions conclusions +

Scoped-Proof-Graph freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP inPorts outPorts nodeOf hyps nodes vertices labelsIn labelsOut vidx inst edges local-vars

for freshenLC :: nat \Rightarrow 'var \Rightarrow 'var

and renameLCs :: ('var \Rightarrow 'var) \Rightarrow 'form \Rightarrow 'form

and lconsts :: 'form \Rightarrow 'var set

```

and closed :: 'form  $\Rightarrow$  bool
and subst :: 'subst  $\Rightarrow$  'form  $\Rightarrow$  'form
and subst-lconsts :: 'subst  $\Rightarrow$  'var set
and subst-renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  ('subst  $\Rightarrow$  'subst)
and anyP :: 'form

and antecedent :: 'rule  $\Rightarrow$  ('form, 'var) antecedent list
and consequent :: 'rule  $\Rightarrow$  'form list
and rules :: 'rule stream

and assumptions :: 'form list
and conclusions :: 'form list

and vertices :: 'vertex fset
and nodeOf :: 'vertex  $\Rightarrow$  ('form, 'rule) graph-node
and edges :: ('vertex, 'form, 'var) edge' set
and vidx :: 'vertex  $\Rightarrow$  nat
and inst :: 'vertex  $\Rightarrow$  'subst +
assumes conclusions-present: set (map Conclusion conclusions)  $\subseteq$  nodeOf ' fset vertices

end

```

5 Natural Deduction

5.1 Natural_Deduction

```
theory Natural-Deduction
imports
  Abstract-Completeness.Abstract-Completeness
  Abstract-Rules
  Entailment
begin
```

Our formalization of natural deduction builds on *Abstract-Completeness.Abstract-Completeness* and refines and concretizes the structure given there as follows

- The judgements are entailments consisting of a finite set of assumptions and a conclusion, which are abstract formulas in the sense of *Incredible-Proof-Machine.Abstract-Formula*.
- The abstract rules given in *Incredible-Proof-Machine.Abstract-Rules* are used to decide the validity of a step in the derivation.

A single setep in the derivation can either be the axiom rule, the cut rule, or one of the given rules in *Incredible-Proof-Machine.Abstract-Rules*.

```
datatype 'rule NatRule = Axiom | NatRule 'rule | Cut
```

The following locale is still abstract in the set of rules (*nat-rule*), but implements the bookkeeping logic for assumptions, the *Axiom* rule and the *Cut* rule.

```
locale ND-Rules-Inst =
  Abstract-Formulas freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP
  for freshenLC :: nat  $\Rightarrow$  'var  $\Rightarrow$  'var
  and renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  'form  $\Rightarrow$  'form
  and lconsts :: 'form  $\Rightarrow$  'var set
  and closed :: 'form  $\Rightarrow$  bool
  and subst :: 'subst  $\Rightarrow$  'form  $\Rightarrow$  'form
  and subst-lconsts :: 'subst  $\Rightarrow$  'var set
  and subst-renameLCs :: ('var  $\Rightarrow$  'var)  $\Rightarrow$  ('subst  $\Rightarrow$  'subst)
  and anyP :: 'form +

  fixes nat-rule :: 'rule  $\Rightarrow$  'form  $\Rightarrow$  ('form, 'var) antecedent fset  $\Rightarrow$  bool
  and rules :: 'rule stream
begin
```

- An application of the *Axiom* rule is valid if the conclusion is among the assumptions.
- An application of a *NatRule* is more complicated. This requires some natural number a to rename local variables, and some instantiation s . It checks that
 - none of the local variables occur in the context of the judgement.
 - none of the local variables occur in the instantiation. Together, this implements the usual freshness side-conditions. Furthermore, for every antecedent of the rule, the (correctly renamed and instantiated) hypotheses need to be added to the context.
- The *Cut* rule is again easy.

```
inductive eff :: 'rule NatRule  $\Rightarrow$  'form entailment  $\Rightarrow$  'form entailment fset  $\Rightarrow$  bool where
```

```

con |∈| Γ
⇒ eff Axiom (Γ ⊢ con) {||}
|nat-rule rule c ants
⇒ (∧ ant f. ant |∈| ants ⇒ f |∈| Γ ⇒ freshenLC a ‘(a-fresh ant) ∩ lconsts f = { })
⇒ (∧ ant. ant |∈| ants ⇒ freshenLC a ‘(a-fresh ant) ∩ subst-lconsts s = { })
⇒ eff (NatRule rule)
  (Γ ⊢ subst s (freshen a c))
  ((λant. ((λp. subst s (freshen a p)) |‘ a-hyps ant |∪| Γ ⊢ subst s (freshen a (a-conc ant)))) |‘ ants)
|eff Cut (Γ ⊢ c’) { | (Γ ⊢ c’) |}

```

inductive-simps *eff-Cut-simps*[simp]: *eff Cut (Γ ⊢ c) S*

sublocale *RuleSystem-Defs* **where**

eff = *eff* **and** *rules* = *Cut* ## *Axiom* ## *smap NatRule rules*⟨*proof*⟩

end

Now we instantiate the above locale. We duplicate each abstract rule (which can have multiple consequents) for each consequent, as the natural deduction formulation can only handle a single consequent per rule

context *Abstract-Task*

begin

inductive *natEff-Inst* **where**

c ∈ *set* (consequent *r*) ⇒ *natEff-Inst* (*r*,*c*) *c* (*f*-antecedent *r*)

definition *n-rules* **where**

n-rules = *flat* (*smap* (λ*r*. *map* (λ*c*. (*r*,*c*)) (consequent *r*)) *rules*)

sublocale *ND-Rules-Inst* - - - - - *natEff-Inst n-rules* ⟨*proof*⟩

A task is solved if for every conclusion, there is a well-formed and finite tree that proves this conclusion, using only assumptions given in the task.

definition *solved* **where**

solved ↔ (∀ *c*. *c* |∈| *conc-forms* → (∃ Γ *t*. *fst* (*root t*) = (Γ ⊢ *c*) ∧ Γ |⊆| *ass-forms* ∧ *wf t* ∧ *tfinite t*)

end

end

6 Correctness

6.1 Incredible_Correctness

```
theory Incredible-Correctness
imports
  Abstract-Rules-To-Incredible
  Natural-Deduction
begin
```

In this theory, we prove that if we have a graph that proves a given abstract task (which is represented as the context *Tasked-Proof-Graph*), then we can prove *solved*.

```
context Tasked-Proof-Graph
begin
```

```
definition adjacentTo :: 'vertex  $\Rightarrow$  ('form, 'var) in-port  $\Rightarrow$  ('vertex  $\times$  ('form, 'var) out-port) where
  adjacentTo v p = (SOME ps. (ps, (v,p))  $\in$  edges)
```

```
fun isReg where
  isReg v p = (case p of Hyp h c  $\Rightarrow$  False | Reg c  $\Rightarrow$ 
    (case nodeOf v of
      Conclusion a  $\Rightarrow$  False
    | Assumption a  $\Rightarrow$  False
    | Rule r  $\Rightarrow$  True
    | Helper  $\Rightarrow$  True
    ))
```

```
fun toNatRule where
  toNatRule v p = (case p of Hyp h c  $\Rightarrow$  Axiom | Reg c  $\Rightarrow$ 
    (case nodeOf v of
      Conclusion a  $\Rightarrow$  Axiom — a lie
    | Assumption a  $\Rightarrow$  Axiom
    | Rule r  $\Rightarrow$  NatRule (r,c)
    | Helper  $\Rightarrow$  Cut
    ))
```

```
inductive-set global-assms' :: 'var itself  $\Rightarrow$  'form set for i where
  v  $\in$  | vertices  $\Longrightarrow$  nodeOf v = Assumption p  $\Longrightarrow$  labelAtOut v (Reg p)  $\in$  global-assms' i
```

```
lemma finite-global-assms': finite (global-assms' i)
<proof>
```

```
context includes fset.lifting
```

```
begin
  lift-definition global-assms :: 'var itself  $\Rightarrow$  'form fset is global-assms' <proof>
  lemmas global-assmsI = global-assms'.intros[Transfer.transferred]
  lemmas global-assms-simps = global-assms'.simps[Transfer.transferred]
end
```

```
fun extra-assms :: ('vertex  $\times$  ('form, 'var) in-port)  $\Rightarrow$  'form fset where
  extra-assms (v, p) = ( $\lambda$  p. labelAtOut v p) |' hyps-for (nodeOf v) p
```

```
fun hyps-along :: ('vertex, 'form, 'var) edge' list  $\Rightarrow$  'form fset where
  hyps-along pth = ffUnion (extra-assms |' snd |' fset-from-list pth)  $\cup$  global-assms TYPE('var)
```

lemma *hyps-alongE*[*consumes 1, case-names Hyp Assumption*]:

assumes $f \mid \in \mid$ *hyps-along pth*

obtains $v \ p \ h$ **where** $(v,p) \in \text{snd } \text{'set pth}$ **and** $f = \text{labelAtOut } v \ h$ **and** $h \mid \in \mid$ *hyps-for (nodeOf v) p*
 $\mid v \ pf$ **where** $v \mid \in \mid$ *vertices* **and** $\text{nodeOf } v = \text{Assumption } pf \ f = \text{labelAtOut } v \ (\text{Reg } pf)$

$\langle \text{proof} \rangle$

Here we build the natural deduction tree, by walking the graph.

primcorec *tree* :: *'vertex* \Rightarrow (*'form, 'var*) *in-port* \Rightarrow (*'vertex, 'form, 'var*) *edge' list* \Rightarrow ((*'form entailment*),
(*'rule* \times *'form*) *NatRule*) *dtree* **where**

root (*tree v p pth*) =

((*hyps-along* ((*adjacentTo v p, (v,p)*)#*pth*) \vdash *labelAtIn v p*),
(*case adjacentTo v p of (v', p')* \Rightarrow *toNatRule v' p'*
))

\mid *cont* (*tree v p pth*) =

(*case adjacentTo v p of (v', p')* \Rightarrow
(*if isReg v' p'* then (($\lambda p''.$ *tree v' p'' ((adjacentTo v p, (v,p))#pth)*) $\mid \mid$ *inPorts (nodeOf v')*) else $\{\mid\}$
))

lemma *fst-root-tree[simp]*: *fst* (*root (tree v p pth)*) = (*hyps-along* ((*adjacentTo v p, (v,p)*)#*pth*) \vdash *labelAtIn v p*)
 $\langle \text{proof} \rangle$

lemma *out-port-cases*[*consumes 1, case-names Assumption Hyp Rule Helper*]:

assumes $p \mid \in \mid$ *outPorts n*

obtains

a **where** $n = \text{Assumption } a$ **and** $p = \text{Reg } a$
 $\mid r \ h \ c$ **where** $n = \text{Rule } r$ **and** $p = \text{Hyp } h \ c$
 $\mid r \ f$ **where** $n = \text{Rule } r$ **and** $p = \text{Reg } f$
 $\mid n = \text{Helper}$ **and** $p = \text{Reg } \text{anyP}$

$\langle \text{proof} \rangle$

lemma *hyps-for-fimage*: *hyps-for* (*Rule r*) $x =$ (*if* $x \mid \in \mid$ *f-antecedent r* then $(\lambda f.$ *Hyp f x*) $\mid \mid$ (*a-hyps x*) else
 $\{\mid\}$)

$\langle \text{proof} \rangle$

Now we prove that the thus produced tree is well-formed.

theorem *wf-tree*:

assumes *valid-in-port (v,p)*

assumes *terminal-path v t pth*

shows *wf (tree v p pth)*

$\langle \text{proof} \rangle$

lemma *global-in-ass*: *global-assms* *TYPE('var)* $\mid \subseteq \mid$ *ass-forms*

$\langle \text{proof} \rangle$

primcorec *edge-tree* :: *'vertex* \Rightarrow (*'form, 'var*) *in-port* \Rightarrow (*'vertex, 'form, 'var*) *edge' tree* **where**

root (*edge-tree v p*) = (*adjacentTo v p, (v,p)*)

\mid *cont* (*edge-tree v p*) =

(*case adjacentTo v p of (v', p')* \Rightarrow
(*if isReg v' p'* then (($\lambda p.$ *edge-tree v' p*) $\mid \mid$ *inPorts (nodeOf v')*) else $\{\mid\}$
))

lemma *tfinite-map-tree*: *tfinite* (*map-tree f t*) \longleftrightarrow *tfinite t*

$\langle \text{proof} \rangle$

lemma *finite-tree-edge-tree*:
tfinite (tree v p pth) \longleftrightarrow tfinite (edge-tree v p)
 ⟨*proof*⟩

coinductive *forbidden-path* :: 'vertex \Rightarrow ('vertex, 'form, 'var) edge' stream \Rightarrow bool **where**
forbidden-path: ((v₁,p₁),(v₂,p₂)) \in edges \implies hyps (nodeOf v₁) p₁ = None \implies forbidden-path v₁ pth \implies
forbidden-path v₂ (((v₁,p₁),(v₂,p₂))##pth)

lemma *path-is-forbidden*:
assumes *valid-in-port (v,p)*
assumes *ipath (edge-tree v p) es*
shows *forbidden-path v es*
 ⟨*proof*⟩

lemma *forbidden-path-prefix-is-path*:
assumes *forbidden-path v es*
obtains *v' where path v' v (rev (stake n es))*
 ⟨*proof*⟩

lemma *forbidden-path-prefix-is-hyp-free*:
assumes *forbidden-path v es*
shows *hyps-free (rev (stake n es))*
 ⟨*proof*⟩

And now we prove that the tree is finite, which requires the above notion of a *forbidden-path*, i.e. an infinite path.

theorem *finite-tree*:
assumes *valid-in-port (v,p)*
assumes *terminal-vertex v*
shows *tfinite (tree v p pth)*
 ⟨*proof*⟩

The main result of this theory.

theorem *solved*
 ⟨*proof*⟩

end

end

7 Completeness

7.1 Incredible_Trees

```
theory Incredible-Trees
imports
  HOL-Library.Sublist
  HOL-Library.Countable
  Entailment
  Rose-Tree
  Abstract-Rules-To-Incredible
begin
```

This theory defines incredible trees, which carry roughly the same information as a (tree-shaped) incredible graph, but where the structure is still given by the data type, and not by a set of edges etc.

Tree-shape, but incredible-graph-like content (port names, explicit annotation and substitution)

```
datatype ('form,'rule,'subst,'var) itnode =
  I (iNodeOf': ('form, 'rule) graph-node)
    (iOutPort': 'form reg-out-port)
    (iAnnot': nat)
    (iSubst': 'subst)
  | H (iAnnot': nat)
    (iSubst': 'subst)
```

```
abbreviation INode n p i s ants  $\equiv$  RNode (I n p i s) ants
```

```
abbreviation HNode i s ants  $\equiv$  RNode (H i s) ants
```

```
type-synonym ('form,'rule,'subst,'var) itree = ('form,'rule,'subst,'var) itnode rose-tree
```

```
fun iNodeOf where
  iNodeOf (INode n p i s ants) = n
  | iNodeOf (HNode i s ants) = Helper
```

```
context Abstract-Formulas begin
```

```
fun iOutPort where
  iOutPort (INode n p i s ants) = p
  | iOutPort (HNode i s ants) = anyP
end
```

```
fun iAnnot where iAnnot it = iAnnot' (root it)
```

```
fun iSubst where iSubst it = iSubst' (root it)
```

```
fun iAnts where iAnts it = children it
```

```
type-synonym ('form, 'rule, 'subst) fresh-check = ('form, 'rule) graph-node  $\Rightarrow$  nat  $\Rightarrow$  'subst  $\Rightarrow$  'form entailment  $\Rightarrow$  bool
```

```
context Abstract-Task
begin
```

The well-formedness of the tree. The first argument can be varied, depending on whether we are interested in the local freshness side-conditions or not.

```
inductive iwf :: ('form, 'rule, 'subst) fresh-check  $\Rightarrow$  ('form,'rule,'subst,'var) itree  $\Rightarrow$  'form entailment  $\Rightarrow$  bool
```

```

for  $fc$ 
where
   $iwf$ :  $\llbracket$ 
     $n \in sset\ nodes$ ;
     $Reg\ p\ |\in|\ outPorts\ n$ ;
     $list-all2\ (\lambda\ ip\ t.\ iwfc\ t\ ((\lambda\ h.\ subst\ s\ (freshen\ i\ (labelsOut\ n\ h))))\ |\uparrow\ hyps-for\ n\ ip\ |\cup|\ \Gamma \vdash\ subst\ s\ (freshen$ 
 $i\ (labelsIn\ n\ ip))))$ 
     $(inPorts'\ n)\ ants$ ;
     $fc\ n\ i\ s\ (\Gamma \vdash\ c)$ ;
     $c = subst\ s\ (freshen\ i\ p)$ 
   $\rrbracket \implies iwfc\ (INode\ n\ p\ i\ s\ ants)\ (\Gamma \vdash\ c)$ 
|  $iwfH$ :  $\llbracket$ 
   $c\ |\notin|\ ass-forms$ ;
   $c\ |\in|\ \Gamma$ ;
   $c = subst\ s\ (freshen\ i\ anyP)$ 
   $\rrbracket \implies iwfc\ (HNode\ i\ s\ [])\ (\Gamma \vdash\ c)$ 

```

lemma $iwf-subst-freshen-outPort$:

```

 $iwfc\ ts\ ent \implies$ 
 $snd\ ent = subst\ (iSubst\ ts)\ (freshen\ (iAnnot\ ts)\ (iOutPort\ ts))$ 
 $\langle proof \rangle$ 

```

definition $all-local-vars$:: ($'form$, $'rule$) $graph-node \implies 'var\ set$ **where**
 $all-local-vars\ n = \bigcup (local-vars\ n\ 'fset\ (inPorts\ n))$

lemma $all-local-vars-Helper[simp]$:

```

 $all-local-vars\ Helper = \{\}$ 
 $\langle proof \rangle$ 

```

lemma $all-local-vars-Assumption[simp]$:

```

 $all-local-vars\ (Assumption\ c) = \{\}$ 
 $\langle proof \rangle$ 

```

Local freshness side-conditions, corresponding what we have in the theory *Natural-Deduction*.

inductive $local-fresh-check$:: ($'form$, $'rule$, $'subst$) $fresh-check$ **where**

```

 $\llbracket \wedge\ f.\ f\ |\in|\ \Gamma \implies freshenLC\ i\ ' (all-local-vars\ n) \cap\ lconsts\ f = \{\}$ ;
 $freshenLC\ i\ ' (all-local-vars\ n) \cap\ subst-lconsts\ s = \{\}$ 
   $\rrbracket \implies local-fresh-check\ n\ i\ s\ (\Gamma \vdash\ c)$ 

```

abbreviation $local-iwf \equiv iwfc\ local-fresh-check$

No freshness side-conditions. Used with the tree that comes out of *globalize*, where we establish the (global) freshness conditions separately.

inductive $no-fresh-check$:: ($'form$, $'rule$, $'subst$) $fresh-check$ **where**

```

 $no-fresh-check\ n\ i\ s\ (\Gamma \vdash\ c)$ 

```

abbreviation $plain-iwf \equiv iwfc\ no-fresh-check$

fun $isHNode$ **where**

```

 $isHNode\ (HNode\ -\ -\ -) = True$ 
 $isHNode\ - = False$ 

```

lemma $iwf-edge-match$:

```

assumes  $iwfc\ t\ ent$ 
assumes  $is@[i] \in it-paths\ t$ 
shows  $subst\ (iSubst\ (tree-at\ t\ (is@[i])))\ (freshen\ (iAnnot\ (tree-at\ t\ (is@[i])))\ (iOutPort\ (tree-at\ t\ (is@[i])))$ )

```

$= \text{subst } (i\text{Subst } (\text{tree-at } t \text{ is})) (\text{freshen } (i\text{Annot } (\text{tree-at } t \text{ is})) (a\text{-conc } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is})) ! i)))$
 ⟨proof⟩

lemma *iwf-length-inPorts*:
assumes *iwf fc t ent*
assumes $is \in \text{it-paths } t$
shows $\text{length } (i\text{Ants } (\text{tree-at } t \text{ is})) \leq \text{length } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is})))$
 ⟨proof⟩

lemma *iwf-local-not-in-subst*:
assumes *local-iwf t ent*
assumes $is \in \text{it-paths } t$
assumes $var \in \text{all-local-vars } (i\text{NodeOf } (\text{tree-at } t \text{ is}))$
shows $\text{freshenLC } (i\text{Annot } (\text{tree-at } t \text{ is})) \text{ var} \notin \text{subst-lconsts } (i\text{Subst } (\text{tree-at } t \text{ is}))$
 ⟨proof⟩

lemma *iwf-length-inPorts-not-HNode*:
assumes *iwf fc t ent*
assumes $is \in \text{it-paths } t$
assumes $\neg (i\text{HNode } (\text{tree-at } t \text{ is}))$
shows $\text{length } (i\text{Ants } (\text{tree-at } t \text{ is})) = \text{length } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is})))$
 ⟨proof⟩

lemma *iNodeOf-outPorts*:
 $i\text{wf fc } t \text{ ent} \implies is \in \text{it-paths } t \implies \text{outPorts } (i\text{NodeOf } (\text{tree-at } t \text{ is})) = \{\}\implies \text{False}$
 ⟨proof⟩

lemma *iNodeOf-tree-at*:
 $i\text{wf fc } t \text{ ent} \implies is \in \text{it-paths } t \implies i\text{NodeOf } (\text{tree-at } t \text{ is}) \in \text{sset nodes}$
 ⟨proof⟩

lemma *iwf-outPort*:
assumes *iwf fc t ent*
assumes $is \in \text{it-paths } t$
shows $\text{Reg } (i\text{OutPort } (\text{tree-at } t \text{ is})) \mid \in \mid \text{outPorts } (i\text{NodeOf } (\text{tree-at } t \text{ is}))$
 ⟨proof⟩

inductive-set *hypos-along for t is where*
prefix $(is'@[i]) \text{ is} \implies$
 $i < \text{length } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is}))) \implies$
 $\text{hypos } (i\text{NodeOf } (\text{tree-at } t \text{ is}')) \text{ h} = \text{Some } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is}')) ! i) \implies$
 $\text{subst } (i\text{Subst } (\text{tree-at } t \text{ is}')) (\text{freshen } (i\text{Annot } (\text{tree-at } t \text{ is}')) (\text{labelsOut } (i\text{NodeOf } (\text{tree-at } t \text{ is}')) \text{ h})) \in \text{hypos-along } t \text{ is}$

lemma *hypos-along-Nil[simp]*: $\text{hypos-along } t \ [] = \{\}$
 ⟨proof⟩

lemma *prefix-app-Cons-elim*:
assumes *prefix* $(xs@[y]) (z\#zs)$
obtains $xs = []$ **and** $y = z$
 $\mid xs' \text{ where } xs = z\#xs' \text{ and } \text{prefix } (xs'@[y]) \text{ zs}$
 ⟨proof⟩

lemma *hypos-along-Cons*:
assumes *iwf fc t ent*
assumes $i\#is \in \text{it-paths } t$

shows *hyp*s-along t ($i \# is$) =
 $(\lambda h. \text{subst } (i\text{Subst } t) (\text{freshen } (i\text{Annot } t) (\text{labelsOut } (i\text{NodeOf } t) h))) \text{ 'fset } (hyp\text{-for } (i\text{NodeOf } t) (\text{inPorts}'$
 $(i\text{NodeOf } t) ! i))$
 $\cup \text{hyp}\text{-along } (i\text{Ants } t ! i) \text{ is } (\text{is } ?S1 = ?S2 \cup ?S3)$
 $\langle \text{proof} \rangle$

lemma *iwf-hyps-exist*:
assumes *iwf* lc it ent
assumes $is \in \text{it}\text{-paths } it$
assumes $\text{tree-at } it \text{ is} = (H\text{Node } i \text{ s } \text{ants}')$
assumes $\text{fst } ent \sqsubseteq | \text{ass-forms}$
shows $\text{subst } s (\text{freshen } i \text{ anyP}) \in \text{hyp}\text{-along } it \text{ is}$
 $\langle \text{proof} \rangle$

definition *hyp-port-for'* :: $('form, 'rule, 'subst, 'var) \text{ itree} \Rightarrow \text{nat list} \Rightarrow 'form \Rightarrow \text{nat list} \times \text{nat} \times ('form, 'var)$
 out-port where
 $\text{hyp-port-for}' t \text{ is } f = (\text{SOME } x.$
 $(\text{case } x \text{ of } (is', i, h) \Rightarrow$
 $\text{prefix } (is' @ [i]) \text{ is} \wedge$
 $i < \text{length } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is}')))) \wedge$
 $\text{hyps } (i\text{NodeOf } (\text{tree-at } t \text{ is}')) h = \text{Some } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is}')) ! i) \wedge$
 $f = \text{subst } (i\text{Subst } (\text{tree-at } t \text{ is}')) (\text{freshen } (i\text{Annot } (\text{tree-at } t \text{ is}')) (\text{labelsOut } (i\text{NodeOf } (\text{tree-at } t \text{ is}')) h))$
 $))$

lemma *hyp-port-for-spec'*:
assumes $f \in \text{hyp}\text{-along } t \text{ is}$
shows $(\text{case } \text{hyp-port-for}' t \text{ is } f \text{ of } (is', i, h) \Rightarrow$
 $\text{prefix } (is' @ [i]) \text{ is} \wedge$
 $i < \text{length } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is}')))) \wedge$
 $\text{hyps } (i\text{NodeOf } (\text{tree-at } t \text{ is}')) h = \text{Some } (\text{inPorts}' (i\text{NodeOf } (\text{tree-at } t \text{ is}')) ! i) \wedge$
 $f = \text{subst } (i\text{Subst } (\text{tree-at } t \text{ is}')) (\text{freshen } (i\text{Annot } (\text{tree-at } t \text{ is}')) (\text{labelsOut } (i\text{NodeOf } (\text{tree-at } t \text{ is}')) h))$
 $\langle \text{proof} \rangle$

definition *hyp-port-path-for* :: $('form, 'rule, 'subst, 'var) \text{ itree} \Rightarrow \text{nat list} \Rightarrow 'form \Rightarrow \text{nat list}$
where $\text{hyp-port-path-for } t \text{ is } f = \text{fst } (\text{hyp-port-for}' t \text{ is } f)$

definition *hyp-port-i-for* :: $('form, 'rule, 'subst, 'var) \text{ itree} \Rightarrow \text{nat list} \Rightarrow 'form \Rightarrow \text{nat}$
where $\text{hyp-port-i-for } t \text{ is } f = \text{fst } (\text{snd } (\text{hyp-port-for}' t \text{ is } f))$

definition *hyp-port-h-for* :: $('form, 'rule, 'subst, 'var) \text{ itree} \Rightarrow \text{nat list} \Rightarrow 'form \Rightarrow ('form, 'var) \text{ out-port}$
where $\text{hyp-port-h-for } t \text{ is } f = \text{snd } (\text{snd } (\text{hyp-port-for}' t \text{ is } f))$

lemma *hyp-port-prefix*:
assumes $f \in \text{hyp}\text{-along } t \text{ is}$
shows $\text{prefix } (\text{hyp-port-path-for } t \text{ is } f @ [\text{hyp-port-i-for } t \text{ is } f]) \text{ is}$
 $\langle \text{proof} \rangle$

lemma *hyp-port-strict-prefix*:
assumes $f \in \text{hyp}\text{-along } t \text{ is}$
shows $\text{strict-prefix } (\text{hyp-port-path-for } t \text{ is } f) \text{ is}$
 $\langle \text{proof} \rangle$

lemma *hyp-port-it-paths*:
assumes $is \in \text{it}\text{-paths } t$
assumes $f \in \text{hyp}\text{-along } t \text{ is}$
shows $\text{hyp-port-path-for } t \text{ is } f \in \text{it}\text{-paths } t$
 $\langle \text{proof} \rangle$

lemma *hyp-port-hyps*:
assumes $f \in \text{hyps-along } t \text{ is}$
shows $\text{hyps } (iNodeOf (tree-at t (hyp-port-path-for t is f))) (hyp-port-h-for t is f) = \text{Some } (inPorts' (iNodeOf (tree-at t (hyp-port-path-for t is f)))) ! \text{hyp-port-i-for } t \text{ is } f$
 $\langle \text{proof} \rangle$

lemma *hyp-port-outPort*:
assumes $f \in \text{hyps-along } t \text{ is}$
shows $(hyp-port-h-for t is f) \in | \text{outPorts } (iNodeOf (tree-at t (hyp-port-path-for t is f)))$
 $\langle \text{proof} \rangle$

lemma *hyp-port-eq*:
assumes $f \in \text{hyps-along } t \text{ is}$
shows $f = \text{subst } (iSubst (tree-at t (hyp-port-path-for t is f))) (\text{freshen } (iAnnot (tree-at t (hyp-port-path-for t is f)))) (\text{labelsOut } (iNodeOf (tree-at t (hyp-port-path-for t is f)))) (hyp-port-h-for t is f)$
 $\langle \text{proof} \rangle$

definition *isidx* :: $\text{nat list} \Rightarrow \text{nat}$ **where** $\text{isidx } xs = \text{to-nat } (\text{Some } xs)$

definition *v-away* :: nat **where** $v\text{-away} = \text{to-nat } (\text{None} :: \text{nat list option})$

lemma *isidx-inj[simp]*: $\text{isidx } xs = \text{isidx } ys \iff xs = ys$
 $\langle \text{proof} \rangle$

lemma *isidx-v-away[simp]*: $\text{isidx } xs \neq v\text{-away}$
 $\langle \text{proof} \rangle$

definition *mapWithIndex* **where** $\text{mapWithIndex } f \ xs = \text{map } (\lambda (i,t) . f \ i \ t) \ (\text{List.enumerate } 0 \ xs)$

lemma *mapWithIndex-cong* [fundef-cong]:

$xs = ys \implies (\bigwedge x \ i. x \in \text{set } ys \implies f \ i \ x = g \ i \ x) \implies \text{mapWithIndex } f \ xs = \text{mapWithIndex } g \ ys$
 $\langle \text{proof} \rangle$

lemma *mapWithIndex-Nil[simp]*: $\text{mapWithIndex } f \ [] = []$
 $\langle \text{proof} \rangle$

lemma *length-mapWithIndex[simp]*: $\text{length } (\text{mapWithIndex } f \ xs) = \text{length } xs$
 $\langle \text{proof} \rangle$

lemma *nth-mapWithIndex[simp]*: $i < \text{length } xs \implies \text{mapWithIndex } f \ xs ! i = f \ i \ (xs ! i)$
 $\langle \text{proof} \rangle$

lemma *list-all2-mapWithIndex2E*:

assumes $\text{list-all2 } P \ as \ bs$

assumes $\bigwedge i \ a \ b . i < \text{length } bs \implies P \ a \ b \implies Q \ a \ (f \ i \ b)$

shows $\text{list-all2 } Q \ as \ (\text{mapWithIndex } f \ bs)$

$\langle \text{proof} \rangle$

The *globalize* function, which renames all local constants so that they cannot clash with local constants occurring anywhere else in the tree.

fun *globalize-node* :: $\text{nat list} \Rightarrow ('var \Rightarrow 'var) \Rightarrow ('form, 'rule, 'subst, 'var) \text{ itnode} \Rightarrow ('form, 'rule, 'subst, 'var) \text{ itnode}$ **where**

$\text{globalize-node } is \ f \ (I \ n \ p \ i \ s) = I \ n \ p \ (\text{isidx } is) \ (\text{subst-renameLCs } f \ s)$
 $| \text{globalize-node } is \ f \ (H \ i \ s) = H \ (\text{isidx } is) \ (\text{subst-renameLCs } f \ s)$

fun *globalize* :: $\text{nat list} \Rightarrow ('var \Rightarrow 'var) \Rightarrow ('form, 'rule, 'subst, 'var) \text{ itree} \Rightarrow ('form, 'rule, 'subst, 'var) \text{ itree}$ **where**

$\text{globalize } is \ f \ (RNode \ r \ ants) = RNode$
 $(\text{globalize-node } is \ f \ r)$

$(\text{mapWithIndex } (\lambda i' t.$
 $\text{globalize } (is@[i'])$
 $\text{rename } (a\text{-fresh } (inPorts' (iNodeOf (RNode r ants)) ! i'))$
 $\text{rename } (iAnnot (RNode r ants)) (isidx is) f)$
 t
 $) \text{ ants})$

lemma *iAnnot'-globalize-node[simp]*: $iAnnot' (\text{globalize-node } is f n) = isidx is$
 $\langle \text{proof} \rangle$

lemma *iAnnot-globalize*:
assumes $is' \in \text{it-paths } (\text{globalize } is f t)$
shows $iAnnot (\text{tree-at } (\text{globalize } is f t) is') = isidx (is@is')$
 $\langle \text{proof} \rangle$

lemma *all-local-consts-listed'*:
assumes $n \in \text{sset nodes}$
assumes $p \in | \text{inPorts } n$
shows $\text{lconsts } (a\text{-conc } p) \cup (\bigcup (\text{lconsts } ' \text{fset } (a\text{-hyps } p))) \subseteq a\text{-fresh } p$
 $\langle \text{proof} \rangle$

lemma *no-local-consts-in-consequences'*:
 $n \in \text{sset nodes} \implies \text{Reg } p \in | \text{outPorts } n \implies \text{lconsts } p = \{\}$
 $\langle \text{proof} \rangle$

lemma *iwf-globalize*:
assumes $\text{local-iwf } t (\Gamma \vdash c)$
shows $\text{plain-iwf } (\text{globalize } is f t) (\text{renameLCs } f | \Gamma \vdash \text{renameLCs } f c)$
 $\langle \text{proof} \rangle$

definition *fresh-at where*
 $\text{fresh-at } t \text{ xs} =$
 $(\text{case rev xs of } [] \Rightarrow \{\}$
 $| (i\#is') \Rightarrow \text{freshenLC } (iAnnot (\text{tree-at } t (\text{rev } is'))) ' (a\text{-fresh } (inPorts' (iNodeOf (\text{tree-at } t (\text{rev } is')) ! i)))$

lemma *fresh-at-Nil[simp]*:
 $\text{fresh-at } t [] = \{\}$
 $\langle \text{proof} \rangle$

lemma *fresh-at-snoc[simp]*:
 $\text{fresh-at } t (is@[i]) = \text{freshenLC } (iAnnot (\text{tree-at } t is)) ' (a\text{-fresh } (inPorts' (iNodeOf (\text{tree-at } t is)) ! i))$
 $\langle \text{proof} \rangle$

lemma *fresh-at-def'*:
 $\text{fresh-at } t is =$
 $(\text{if } is = [] \text{ then } \{\}$
 $\text{else } \text{freshenLC } (iAnnot (\text{tree-at } t (\text{butlast } is))) ' (a\text{-fresh } (inPorts' (iNodeOf (\text{tree-at } t (\text{butlast } is)) ! \text{last } is)))$
 $\langle \text{proof} \rangle$

lemma *fresh-at-Cons[simp]*:
 $\text{fresh-at } t (i\#is) = (\text{if } is = [] \text{ then } \text{freshenLC } (iAnnot t) ' (a\text{-fresh } (inPorts' (iNodeOf t) ! i)) \text{ else } (\text{let } t' =$
 $i\text{Ants } t ! i \text{ in } \text{fresh-at } t' is))$
 $\langle \text{proof} \rangle$

definition *fresh-at-path where*

$fresh-at-path\ t\ is = \bigcup (fresh-at\ t\ \text{'set}\ (prefixes\ is))$

lemma *fresh-at-path-Nil*[simp]:

$fresh-at-path\ t\ [] = \{\}$

$\langle proof \rangle$

lemma *fresh-at-path-Cons*[simp]:

$fresh-at-path\ t\ (i\#\!is) = fresh-at\ t\ [i] \cup fresh-at-path\ (iAnts\ t\ !\ i)\ is$

$\langle proof \rangle$

lemma *globalize-local-consts*:

assumes $is' \in it\text{-paths}\ (globalize\ is\ f\ t)$

shows $subst\text{-lconsts}\ (iSubst\ (tree\text{-at}\ (globalize\ is\ f\ t)\ is')) \subseteq$

$fresh-at-path\ (globalize\ is\ f\ t)\ is' \cup range\ f$

$\langle proof \rangle$

lemma *iwf-globalize'*:

assumes $local\text{-iwf}\ t\ ent$

assumes $\bigwedge x. x\ |\in|\ fst\ ent \implies closed\ x$

assumes $closed\ (snd\ ent)$

shows $plain\text{-iwf}\ (globalize\ is\ (freshenLC\ v\text{-away})\ t)\ ent$

$\langle proof \rangle$

end

end

7.2 Build_Incredible_Tree

theory *Build-Incredible-Tree*

imports *Incredible-Trees Natural-Deduction*

begin

This theory constructs an incredible tree (with freshness checked only locally) from a natural deduction tree.

lemma *image-eq-to-f*:

assumes $f1\ \text{'}S1 = f2\ \text{'}S2$

obtains $f\ \mathbf{where}\ \bigwedge x. x \in S2 \implies f\ x \in S1 \wedge f1\ (f\ x) = f2\ x$

$\langle proof \rangle$

context **includes** *fset.lifting*

begin

lemma *fimage-eq-to-f*:

assumes $f1\ |\uparrow S1 = f2\ |\uparrow S2$

obtains $f\ \mathbf{where}\ \bigwedge x. x\ |\in|\ S2 \implies f\ x\ |\in|\ S1 \wedge f1\ (f\ x) = f2\ x$

$\langle proof \rangle$

end

context *Abstract-Task*

begin

lemma *build-local-iwf*:

fixes $t :: ('form\ entailment \times ('rule \times 'form)\ NatRule)\ tree$

assumes $tfinite\ t$

assumes $wf\ t$

shows $\exists it. local\text{-iwf}\ it\ (fst\ (root\ t))$

$\langle proof \rangle$

definition *to-it* :: ('form entailment × ('rule × 'form) NatRule) tree ⇒ ('form, 'rule, 'subst, 'var) itree **where**
to-it t = (SOME it. local-iwf it (fst (root t)))

lemma *iwf-to-it*:
assumes *tfinite* t **and** *wf* t
shows *local-iwf* (*to-it* t) (fst (root t))
⟨*proof*⟩
end
end

7.3 Incredible_Completeness

theory *Incredible-Completeness*
imports *Natural-Deduction Incredible-Deduction Build-Incredible-Tree*
begin

This theory takes the tree produced in *Incredible-Proof-Machine.Build-Incredible-Tree*, globalizes it using *globalize*, and then builds the incredible proof graph out of it.

type-synonym *'form vertex* = ('form × nat list)
type-synonym ('form, 'var) *edge''* = ('form vertex, 'form, 'var) *edge'*

locale *Solved-Task* =
Abstract-Task *freshenLC* *renameLCs* *lconsts* *closed* *subst* *subst-lconsts* *subst-renameLCs* *anyP* *antecedent*
consequent *rules* *assumptions* *conclusions*
for *freshenLC* :: nat ⇒ 'var ⇒ 'var
and *renameLCs* :: ('var ⇒ 'var) ⇒ 'form ⇒ 'form
and *lconsts* :: 'form ⇒ 'var set
and *closed* :: 'form ⇒ bool
and *subst* :: 'subst ⇒ 'form ⇒ 'form
and *subst-lconsts* :: 'subst ⇒ 'var set
and *subst-renameLCs* :: ('var ⇒ 'var) ⇒ ('subst ⇒ 'subst)
and *anyP* :: 'form
and *antecedent* :: 'rule ⇒ ('form, 'var) antecedent list
and *consequent* :: 'rule ⇒ 'form list
and *rules* :: 'rule stream
and *assumptions* :: 'form list
and *conclusions* :: 'form list +
assumes *solved*: *solved*
begin

Let us get our hand on concrete trees.

definition *ts* :: 'form ⇒ (('form entailment) × ('rule × 'form) NatRule) tree **where**
ts c = (SOME t. snd (fst (root t)) = c ∧ fst (fst (root t)) |⊆| *ass-forms* ∧ wf t ∧ *tfinite* t)

lemma
assumes c |∈| *conc-forms*
shows *ts-conc*: snd (fst (root (ts c))) = c
and *ts-context*: fst (fst (root (ts c))) |⊆| *ass-forms*
and *ts-wf*: wf (ts c)
and *ts-finite[simp]*: *tfinite* (ts c)
⟨*proof*⟩

abbreviation *it'* **where**
it' c ≡ *globalize* [*fidx conc-forms* c, 0] (*freshenLC* *v-away*) (*to-it* (ts c))

lemma *iwf-it*:

assumes $c \in \text{set conclusions}$

shows $\text{plain-iwf } (it' c) (\text{fst } (\text{root } (ts c)))$

$\langle \text{proof} \rangle$

definition *vertices* :: 'form vertex fset **where**

$\text{vertices} = \text{Abs-fset } (\text{Union } (\text{set } (\text{map } (\lambda c. \text{insert } (c, []) ((\lambda p. (c, 0 \# p)) ' (it-paths (it' c)))) \text{ conclusions})))$

lemma *mem-vertices*: $v \in \text{vertices} \longleftrightarrow (\text{fst } v \in \text{set conclusions} \wedge (\text{snd } v = [] \vee \text{snd } v \in ((\#) 0) ' \text{it-paths } (it' (\text{fst } v))))$

$\langle \text{proof} \rangle$

lemma *prefixeq-vertices*: $(c, is) \in \text{vertices} \implies \text{prefix } is' is \implies (c, is') \in \text{vertices}$

$\langle \text{proof} \rangle$

lemma *none-vertices[simp]*: $(c, []) \in \text{vertices} \longleftrightarrow c \in \text{set conclusions}$

$\langle \text{proof} \rangle$

lemma *some-vertices[simp]*: $(c, i \# is) \in \text{vertices} \longleftrightarrow c \in \text{set conclusions} \wedge i = 0 \wedge is \in \text{it-paths } (it' c)$

$\langle \text{proof} \rangle$

lemma *vertices-cases[consumes 1, case-names None Some]*:

assumes $v \in \text{vertices}$

obtains c **where** $c \in \text{set conclusions}$ **and** $v = (c, [])$

| c **is** **where** $c \in \text{set conclusions}$ **and** $is \in \text{it-paths } (it' c)$ **and** $v = (c, 0 \# is)$

$\langle \text{proof} \rangle$

lemma *vertices-induct[consumes 1, case-names None Some]*:

assumes $v \in \text{vertices}$

assumes $\bigwedge c. c \in \text{set conclusions} \implies P (c, [])$

assumes $\bigwedge c is. c \in \text{set conclusions} \implies is \in \text{it-paths } (it' c) \implies P (c, 0 \# is)$

shows $P v$

$\langle \text{proof} \rangle$

fun *nodeOf* :: 'form vertex \Rightarrow ('form, 'rule) graph-node **where**

$\text{nodeOf } (pf, []) = \text{Conclusion } pf$

| $\text{nodeOf } (pf, i \# is) = \text{iNodeOf } (\text{tree-at } (it' pf) is)$

fun *inst* **where**

$\text{inst } (c, []) = \text{empty-subst}$

| $\text{inst } (c, i \# is) = \text{iSubst } (\text{tree-at } (it' c) is)$

lemma *terminal-is-nil[simp]*: $v \in \text{vertices} \implies \text{outPorts } (\text{nodeOf } v) = \{[]\} \longleftrightarrow \text{snd } v = []$

$\langle \text{proof} \rangle$

sublocale *Vertex-Graph* nodes inPorts outPorts vertices nodeOf $\langle \text{proof} \rangle$

definition *edge-from* :: 'form \Rightarrow nat list \Rightarrow ('form vertex \times ('form, 'var) out-port) **where**

$\text{edge-from } c is = ((c, 0 \# is), \text{Reg } (\text{iOutPort } (\text{tree-at } (it' c) is)))$

lemma *fst-edge-from[simp]*: $\text{fst } (\text{edge-from } c is) = (c, 0 \# is)$

$\langle \text{proof} \rangle$

fun *in-port-at* :: ('form \times nat list) \Rightarrow nat \Rightarrow ('form, 'var) in-port **where**

$\text{in-port-at } (c, []) - = \text{plain-ant } c$

| $\text{in-port-at } (c, - \# is) i = \text{inPorts}' (\text{iNodeOf } (\text{tree-at } (it' c) is)) ! i$

definition *edge-to* :: 'form \Rightarrow nat list \Rightarrow ('form vertex \times ('form,'var) in-port) **where**
edge-to c is =
 (case rev is of [] \Rightarrow ((c, []), in-port-at (c, []) 0)
 | i#is \Rightarrow ((c, 0 # (rev is)), in-port-at (c, (0#rev is)) i))

lemma *edge-to-Nil[simp]*: *edge-to* c [] = ((c, []), plain-ant c)
 ⟨proof⟩

lemma *edge-to-Snoc[simp]*: *edge-to* c (is@[i]) = ((c, 0 # is), in-port-at ((c, 0 # is)) i)
 ⟨proof⟩

definition *edge-at* :: 'form \Rightarrow nat list \Rightarrow ('form, 'var) edge'' **where**
edge-at c is = (edge-from c is, *edge-to* c is)

lemma *fst-edge-at[simp]*: fst (*edge-at* c is) = edge-from c is ⟨proof⟩

lemma *snd-edge-at[simp]*: snd (*edge-at* c is) = *edge-to* c is ⟨proof⟩

lemma *hyps-exist'*:
 assumes c \in set conclusions
 assumes is \in it-paths (it' c)
 assumes tree-at (it' c) is = (HNode i s ants)
 shows subst s (freshen i anyP) \in hyps-along (it' c) is
 ⟨proof⟩

definition *hyp-edge-to* :: 'form \Rightarrow nat list \Rightarrow ('form vertex \times ('form,'var) in-port) **where**
hyp-edge-to c is = ((c, 0 # is), plain-ant anyP)

definition *hyp-edge-from* :: 'form \Rightarrow nat list \Rightarrow nat \Rightarrow 'subst \Rightarrow ('form vertex \times ('form,'var) out-port)
where
hyp-edge-from c is n s =
 ((c, 0 # hyp-port-path-for (it' c) is (subst s (freshen n anyP))),
 hyp-port-h-for (it' c) is (subst s (freshen n anyP)))

definition *hyp-edge-at* :: 'form \Rightarrow nat list \Rightarrow nat \Rightarrow 'subst \Rightarrow ('form, 'var) edge'' **where**
hyp-edge-at c is n s = (*hyp-edge-from* c is n s, *hyp-edge-to* c is)

lemma *fst-hyp-edge-at[simp]*:
 fst (*hyp-edge-at* c is n s) = *hyp-edge-from* c is n s ⟨proof⟩

lemma *snd-hyp-edge-at[simp]*:
 snd (*hyp-edge-at* c is n s) = *hyp-edge-to* c is ⟨proof⟩

inductive-set *edges* **where**

regular-edge: c \in set conclusions \Longrightarrow is \in it-paths (it' c) \Longrightarrow *edge-at* c is \in edges
 | *hyp-edge*: c \in set conclusions \Longrightarrow is \in it-paths (it' c) \Longrightarrow tree-at (it' c) is = HNode n s ants \Longrightarrow *hyp-edge-at*
 c is n s \in edges

sublocale *Pre-Port-Graph* nodes inPorts outPorts vertices nodeOf edges ⟨proof⟩

lemma *edge-from-valid-out-port*:

assumes p \in it-paths (it' c)
 assumes c \in set conclusions
 shows valid-out-port (edge-from c p)
 ⟨proof⟩

lemma *edge-to-valid-in-port*:
assumes $p \in \text{it-paths } (it' c)$
assumes $c \in \text{set conclusions}$
shows *valid-in-port* (*edge-to* $c p$)
 $\langle \text{proof} \rangle$

lemma *hyp-edge-from-valid-out-port*:
assumes $is \in \text{it-paths } (it' c)$
assumes $c \in \text{set conclusions}$
assumes $\text{tree-at } (it' c) \text{ is} = \text{HNode } n \text{ s ants}$
shows *valid-out-port* (*hyp-edge-from* $c \text{ is } n \text{ s}$)
 $\langle \text{proof} \rangle$

lemma *hyp-edge-to-valid-in-port*:
assumes $is \in \text{it-paths } (it' c)$
assumes $c \in \text{set conclusions}$
assumes $\text{tree-at } (it' c) \text{ is} = \text{HNode } n \text{ s ants}$
shows *valid-in-port* (*hyp-edge-to* $c \text{ is}$)
 $\langle \text{proof} \rangle$

inductive *scope'* :: $'\text{form vertex} \Rightarrow ('form, 'var) \text{ in-port} \Rightarrow 'form \times \text{nat list} \Rightarrow \text{bool}$ **where**
 $c \in \text{set conclusions} \Longrightarrow$
 $is' \in ((\#) 0) \text{ 'it-paths } (it' c) \Longrightarrow$
 $\text{prefix } (is@[i]) \text{ is}' \Longrightarrow$
 $ip = \text{in-port-at } (c, is) \text{ i} \Longrightarrow$
 $\text{scope}' (c, is) \text{ ip } (c, is')$

inductive-simps *scope-simp*: $\text{scope}' v \text{ i } v'$
inductive-cases *scope-cases*: $\text{scope}' v \text{ i } v'$

lemma *scope-valid*:
 $\text{scope}' v \text{ i } v' \Longrightarrow v' \in \text{vertices}$
 $\langle \text{proof} \rangle$

lemma *scope-valid-inport*:
 $v' \in \text{vertices} \Longrightarrow \text{scope}' v \text{ ip } v' \longleftrightarrow (\exists i. \text{fst } v = \text{fst } v' \wedge \text{prefix } (\text{snd } v@[i]) (\text{snd } v') \wedge \text{ip} = \text{in-port-at } v \text{ i})$
 $\langle \text{proof} \rangle$

definition *terminal-path-from* :: $'form \Rightarrow \text{nat list} \Rightarrow ('form, 'var) \text{ edge'' list}$ **where**
 $\text{terminal-path-from } c \text{ is} = \text{map } (\text{edge-at } c) (\text{rev } (\text{prefixes } is))$

lemma *terminal-path-from-Nil[simp]*:
 $\text{terminal-path-from } c [] = [\text{edge-at } c []]$
 $\langle \text{proof} \rangle$

lemma *terminal-path-from-Snoc[simp]*:
 $\text{terminal-path-from } c (is @ [i]) = \text{edge-at } c (is@[i]) \# \text{terminal-path-from } c \text{ is}$
 $\langle \text{proof} \rangle$

lemma *path-terminal-path-from*:
 $c \in \text{set conclusions} \Longrightarrow$
 $is \in \text{it-paths } (it' c) \Longrightarrow$
 $\text{path } (c, 0 \# is) (c, []) (\text{terminal-path-from } c \text{ is})$
 $\langle \text{proof} \rangle$

lemma *edge-step*:

assumes $((a, b), ba), ((aa, bb), bc) \in \text{edges}$

obtains

i **where** $a = aa$ **and** $b = bb@[i]$ **and** $bc = \text{in-port-at } (aa, bb) \ i$ **and** $\text{hyps } (\text{nodeOf } (a, b)) \ ba = \text{None}$
| i **where** $a = aa$ **and** $\text{prefix } (b@[i]) \ bb$ **and** $\text{hyps } (\text{nodeOf } (a, b)) \ ba = \text{Some } (\text{in-port-at } (a, b) \ i)$

$\langle \text{proof} \rangle$

lemma *path-has-prefixes*:

assumes $\text{path } v \ v' \ pth$

assumes $\text{snd } v' = []$

assumes $\text{prefix } (is' @ [i]) \ (\text{snd } v)$

shows $((\text{fst } v, is'), (\text{in-port-at } (\text{fst } v, is') \ i)) \in \text{snd ' set } pth$

$\langle \text{proof} \rangle$

lemma *in-scope*: $\text{valid-in-port } (v', p') \implies v \in \text{scope } (v', p') \iff \text{scope}' \ v' \ p' \ v$

$\langle \text{proof} \rangle$

sublocale *Port-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges}$

$\langle \text{proof} \rangle$

sublocale *Scoped-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges } \text{hyps} \langle \text{proof} \rangle$

lemma *hyps-free-path-length*:

assumes $\text{path } v \ v' \ pth$

assumes $\text{hyps-free } pth$

shows $\text{length } pth + \text{length } (\text{snd } v') = \text{length } (\text{snd } v)$

$\langle \text{proof} \rangle$

fun *vidx* :: $'\text{form vertex} \Rightarrow \text{nat}$ **where**

$\text{vidx } (c, []) = \text{isidx } [\text{fidx } \text{conc-forms } c]$

| $\text{vidx } (c, -\#is) = \text{iAnnot } (\text{tree-at } (it' \ c) \ is)$

lemma *my-vidx-inj*: $\text{inj-on } \text{vidx } (\text{fset } \text{vertices})$

$\langle \text{proof} \rangle$

lemma *vidx-not-v-away[simp]*: $v \in \text{vertices} \implies \text{vidx } v \neq \text{v-away}$

$\langle \text{proof} \rangle$

sublocale *Instantiation* $\text{inPorts } \text{outPorts } \text{nodeOf } \text{hyps } \text{nodes } \text{edges } \text{vertices } \text{labelsIn } \text{labelsOut } \text{freshenLC } \text{renameLCs } \text{lconsts } \text{closed } \text{subst } \text{subst-lconsts } \text{subst-renameLCs } \text{anyP } \text{vidx } \text{inst}$

$\langle \text{proof} \rangle$

sublocale *Well-Scoped-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges } \text{hyps}$

$\langle \text{proof} \rangle$

sublocale *Acyclic-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges } \text{hyps}$

$\langle \text{proof} \rangle$

sublocale *Saturated-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges}$

$\langle \text{proof} \rangle$

sublocale *Pruned-Port-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges}$

$\langle \text{proof} \rangle$

sublocale *Well-Shaped-Graph* $\text{nodes } \text{inPorts } \text{outPorts } \text{vertices } \text{nodeOf } \text{edges } \text{hyps} \langle \text{proof} \rangle$

sublocale *sol:Solution inPorts outPorts nodeOf hyps nodes vertices labelsIn labelsOut freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP vidx inst edges*
 ⟨proof⟩

lemma *node-disjoint-fresh-vars:*

assumes $n \in \text{sset nodes}$

assumes $i < \text{length } (\text{inPorts}' n)$

assumes $i' < \text{length } (\text{inPorts}' n)$

shows $a\text{-fresh } (\text{inPorts}' n ! i) \cap a\text{-fresh } (\text{inPorts}' n ! i') = \{\} \vee i = i'$

⟨proof⟩

sublocale *Well-Scoped-Instantiation freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP inPorts outPorts nodeOf hyps nodes vertices labelsIn labelsOut vidx inst edges local-vars*
 ⟨proof⟩

sublocale *Scoped-Proof-Graph freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP inPorts outPorts nodeOf hyps nodes vertices labelsIn labelsOut vidx inst edges local-vars*⟨proof⟩

sublocale *tpg:Tasked-Proof-Graph freshenLC renameLCs lconsts closed subst subst-lconsts subst-renameLCs anyP antecedent consequent rules assumptions conclusions vertices nodeOf edges vidx inst*
 ⟨proof⟩

end

end

8 Instantiations

To ensure that our locale assumption are fulfillable, we instantiate them with small examples.

8.1 Propositional_Formulas

theory *Propositional-Formulas*

imports

Abstract-Formula

HOL-Library.Countable

HOL-Library.Infinite-Set

HOL-Library.Infinite-Typeclass

begin

lemma *countable-infinite-ex-bij*: $\exists f::('a::\{countable,infinite\}\Rightarrow'b::\{countable,infinite\})$. *bij f*
<proof>

Propositional formulas are either a variable from an infinite but countable set, or a function given by a name and the arguments.

datatype (*'var','cname*) *pform* =
 Var 'var::\{countable,infinite\}
 | *Fun (name:'cname) (params: ('var,'cname) pform list)*

Substitution on and closedness of propositional formulas is straight forward.

fun *subst* :: (*'var::\{countable,infinite\}*) \Rightarrow (*'var','cname*) *pform* \Rightarrow (*'var','cname*) *pform*
 where *subst s (Var v) = s v*
 | *subst s (Fun n ps) = Fun n (map (subst s) ps)*

fun *closed* :: (*'var::\{countable,infinite\},'cname*) *pform* \Rightarrow *bool*
 where *closed (Var v) \longleftrightarrow False*
 | *closed (Fun n ps) \longleftrightarrow list-all closed ps*

Now we can interpret *Abstract-Formulas*. As there are no locally fixed constants in propositional formulas, most of the locale parameters are dummy values

interpretation *propositional: Abstract-Formulas*

— No need to freshen locally fixed constants

curry (SOME f. bij f):: nat \Rightarrow 'var \Rightarrow 'var

— also no renaming needed as there are no locally fixed constants

λ -. id λ -. \}

— closedness and substitution as defined above

closed :: ('var::\{countable,infinite\},'cname) pform \Rightarrow bool subst

— no substitution and renaming of locally fixed constants

λ -. \} λ -. id

— most generic formula

Var undefined

<proof>

declare *propositional.subst-lconsts-empty-subst* [*simp del*]

end

8.2 Incredible_Propositional

theory *Incredible-Propositional* **imports**

*Abstract-Rules-To-Incredible
Propositional-Formulas*

begin

Our concrete interpretation with propositional logic will cover conjunction and implication as well as constant symbols. The type for variables will be *string*.

datatype *prop-funs* = *and* | *imp* | *Const string*

The rules are introduction and elimination of conjunction and implication.

datatype *prop-rule* = *andI* | *andE* | *impI* | *impE*

definition *prop-rules* :: *prop-rule stream*
where *prop-rules* = *cycle [andI, andE, impI, impE]*

lemma *iR-prop-rules [simp]: sset prop-rules = {andI, andE, impI, impE}*
<proof>

Just some short notation.

abbreviation *X* :: (*string, 'a*) *pform*
where *X* ≡ *Var "X"*

abbreviation *Y* :: (*string, 'a*) *pform*
where *Y* ≡ *Var "Y"*

Finally the right- and left-hand sides of the rules.

fun *consequent* :: *prop-rule* ⇒ (*string, prop-funs*) *pform list*
where *consequent andI* = [*Fun and [X, Y]*]
| *consequent andE* = [*X, Y*]
| *consequent impI* = [*Fun imp [X, Y]*]
| *consequent impE* = [*Y*]

fun *antecedent* :: *prop-rule* ⇒ ((*string, prop-funs*) *pform, string*) *antecedent list*
where *antecedent andI* = [*plain-ant X, plain-ant Y*]
| *antecedent andE* = [*plain-ant (Fun and [X, Y])*]
| *antecedent impI* = [*Antecedent {|X|} Y {|}*]
| *antecedent impE* = [*plain-ant (Fun imp [X, Y]), plain-ant X*]

interpretation *propositional: Abstract-Rules*
curry (SOME f. bij f):: nat ⇒ string ⇒ string
λ-. id
λ-. {}
closed :: (string, prop-funs) pform ⇒ bool
subst
λ-. {}
λ-. id
Var undefined
antecedent
consequent
prop-rules
<proof>

end

8.3 Incredible_Propositional_Tasks

theory *Incredible-Propositional-Tasks*

imports

Incredible-Completeness

Incredible-Propositional

begin

context *ND-Rules-Inst* **begin**

lemma *eff-NatRuleI*:

nat-rule rule c ants

$\implies \text{entail} = (\Gamma \vdash \text{subst } s \text{ (freshen } a \text{ } c))$

$\implies \text{hyps} = ((\lambda \text{ant. } ((\lambda p. \text{subst } s \text{ (freshen } a \text{ } p)) \mid^{\dagger} a\text{-hyps } \text{ant} \mid \cup \mid \Gamma \vdash \text{subst } s \text{ (freshen } a \text{ (} a\text{-conc } \text{ant})))) \mid^{\dagger} \text{ants})$

$\implies (\bigwedge \text{ant } f. \text{ant} \mid \in \mid \text{ants} \implies f \mid \in \mid \Gamma \implies \text{freshenLC } a \text{ ' (} a\text{-fresh } \text{ant} \text{) } \cap \text{lconsts } f = \{\})$

$\implies (\bigwedge \text{ant. } \text{ant} \mid \in \mid \text{ants} \implies \text{freshenLC } a \text{ ' (} a\text{-fresh } \text{ant} \text{) } \cap \text{subst-lconsts } s = \{\})$

$\implies \text{eff (NatRule rule) entail hyps}$

<proof>

end

context *Abstract-Task* **begin**

lemma *natEff-InstI*:

rule = (r,c)

$\implies c \in \text{set (consequent } r)$

$\implies \text{antec} = f\text{-antecedent } r$

$\implies \text{natEff-Inst rule } c \text{ antec}$

<proof>

end

context **begin**

8.3.1 Task 1.1

This is the very first task of the Incredible Proof Machine: $A \longrightarrow A$

abbreviation $A :: (\text{string,prop-funs}) \text{ pform}$

where $A \equiv \text{Fun (Const "A")} \square$

First the task is defined as an *Abstract-Task*.

interpretation *task1-1: Abstract-Task*

curry (SOME f. bij f):: nat \Rightarrow string \Rightarrow string

$\lambda\text{-. id}$

$\lambda\text{-. \{\}$

closed :: (string, prop-funs) pform \Rightarrow bool

subst

$\lambda\text{-. \{\}$

$\lambda\text{-. id}$

Var undefined

antecedent

consequent

prop-rules

[A]

[A]

<proof>

Then we show, that this task has a proof within our formalization of natural deduction by giving a concrete proof tree.

lemma *task1-1.solved*
 ⟨*proof*⟩

print-locale *Vertex-Graph*

interpretation *task1-1: Vertex-Graph* *task1-1.nodes* *task1-1.inPorts* *task1-1.outPorts* $\{|0::nat,1|\}$
undefined(*0* := *Assumption A*, *1* := *Conclusion A*)
 ⟨*proof*⟩

print-locale *Pre-Port-Graph*

interpretation *task1-1: Pre-Port-Graph* *task1-1.nodes* *task1-1.inPorts* *task1-1.outPorts* $\{|0::nat,1|\}$
undefined(*0* := *Assumption A*, *1* := *Conclusion A*)
 $\{((0,Reg\ A),(1,plain-ant\ A))\}$
 ⟨*proof*⟩

print-locale *Instantiation*

interpretation *task1-1: Instantiation*
task1-1.inPorts
task1-1.outPorts
undefined(*0* := *Assumption A*, *1* := *Conclusion A*)
task1-1.hyps
task1-1.nodes
 $\{((0,Reg\ A),(1,plain-ant\ A))\}$
 $\{|0::nat,1|\}$
task1-1.labelsIn
task1-1.labelsOut
curry (*SOME* *f. bij f*):: *nat* \Rightarrow *string* \Rightarrow *string*
 λ -. *id*
 λ -. $\{\}$
closed :: (*string*, *prop-funs*) *pform* \Rightarrow *bool*
subst
 λ -. $\{\}$
 λ -. *id*
Var *undefined*
id
undefined
 ⟨*proof*⟩

declare *One-nat-def* [*simp del*]

lemma *path-one-edge*[*simp*]:

task1-1.path *v1* *v2* *pth* \longleftrightarrow
 (*v1* = 0 \wedge *v2* = 1 \wedge *pth* = $[(0,Reg\ A),(1,plain-ant\ A)]$) \vee
pth = [] \wedge *v1* = *v2*)
 ⟨*proof*⟩

Finally we can also show that there is a proof graph for this task.

interpretation *Tasked-Proof-Graph*

curry (*SOME* *f. bij f*):: *nat* \Rightarrow *string* \Rightarrow *string*
 λ -. *id*
 λ -. $\{\}$
closed :: (*string*, *prop-funs*) *pform* \Rightarrow *bool*
subst
 λ -. $\{\}$
 λ -. *id*
Var *undefined*
antecedent

```

consequent
prop-rules
[A]
[A]
{|0::nat,1|}
undefined(0 := Assumption A, 1 := Conclusion A)
{((0,Reg A),(1,plain-ant A))}
id
undefined
⟨proof⟩

```

8.3.2 Task 2.11

This is a slightly more interesting task as it involves both our connectives: $P \wedge Q \longrightarrow R \implies P \longrightarrow Q \longrightarrow R$

```

abbreviation B :: (string,prop-funs) pform
  where B ≡ Fun (Const "B") []
abbreviation C :: (string,prop-funs) pform
  where C ≡ Fun (Const "C") []

```

```

interpretation task2-11: Abstract-Task
  curry (SOME f. bij f):: nat ⇒ string ⇒ string
  λ-. id
  λ-. {}
  closed :: (string, prop-funs) pform ⇒ bool
  subst
  λ-. {}
  λ-. id
  Var undefined
  antecedent
  consequent
  prop-rules
  [Fun imp [Fun and [A,B],C]]
  [Fun imp [A,Fun imp [B,C]]]
⟨proof⟩

```

```

abbreviation n-andI ≡ task2-11.n-rules !! 0
abbreviation n-andE1 ≡ task2-11.n-rules !! 1
abbreviation n-andE2 ≡ task2-11.n-rules !! 2
abbreviation n-impI ≡ task2-11.n-rules !! 3
abbreviation n-impE ≡ task2-11.n-rules !! 4

```

```

lemma n-andI [simp]: n-andI = (andI, Fun and [X,Y])
⟨proof⟩
lemma n-andE1 [simp]: n-andE1 = (andE, X)
⟨proof⟩
lemma n-andE2 [simp]: n-andE2 = (andE, Y)
⟨proof⟩
lemma n-impI [simp]: n-impI = (impI, Fun imp [X,Y])
⟨proof⟩
lemma n-impE [simp]: n-impE = (impE, Y)
⟨proof⟩

```

```

lemma subst-Var-eq-id [simp]: subst Var = id
⟨proof⟩

```

lemma *xy-update*: $f = \text{undefined}("X" := x, "Y" := y) \implies x = f "X" \wedge y = f "Y" \langle \text{proof} \rangle$

lemma *y-update*: $f = \text{undefined}("Y" := y) \implies y = f "Y" \langle \text{proof} \rangle$

declare *snth.simps*(1) [*simp del*]

By interpreting *Solved-Task* we show that there is a proof tree for the task. We get the existence of the proof graph for free by using the completeness theorem.

interpretation *task2-11: Solved-Task*

```
curry (SOME f. bij f):: nat  $\Rightarrow$  string  $\Rightarrow$  string
 $\lambda$ -. id
 $\lambda$ -. {}
closed :: (string, prop-funs) pform  $\Rightarrow$  bool
subst
 $\lambda$ -. {}
 $\lambda$ -. id
Var undefined
antecedent
consequent
prop-rules
[Fun imp [Fun and [A,B],C]]
[Fun imp [A, Fun imp [B,C]]]
 $\langle \text{proof} \rangle$ 
```

interpretation *Tasked-Proof-Graph*

```
curry (SOME f. bij f):: nat  $\Rightarrow$  string  $\Rightarrow$  string
 $\lambda$ -. id
 $\lambda$ -. {}
closed :: (string, prop-funs) pform  $\Rightarrow$  bool
subst
 $\lambda$ -. {}
 $\lambda$ -. id
Var undefined
antecedent
consequent
prop-rules
[Fun imp [Fun and [A,B],C]]
[Fun imp [A, Fun imp [B,C]]]
task2-11.vertices
task2-11.nodeOf
task2-11.edges
task2-11.vidx
task2-11.inst
 $\langle \text{proof} \rangle$ 
```

end

end

8.4 Predicate_Formulas

theory *Predicate-Formulas*

imports

HOL-Library.Countable

HOL-Library.Infinite-Set

begin

This theory contains an example instantiation of *Abstract-Formulas* with an formula type with local constants. It is a rather ad-hoc type that may not be very useful to work with, though.

type-synonym $var = nat$

type-synonym $lconst = nat$

We support higher order variables, in order to express $\forall x. ?P x$. But we stay first order, i.e. the parameters of such a variables will only be instantiated with ground terms.

datatype $form =$

$Var (var:var) (params: form list)$
 $| LC (var:lconst)$
 $| Op (name:string) (params: form list)$
 $| Quant (name:string) (var:nat) (body: form)$

type-synonym $schema = var list \times form$

type-synonym $subst = (nat \times schema) list$

fun $fv :: form \Rightarrow var set$ **where**

$fv (Var v xs) = insert v (Union (fv ' set xs))$
 $| fv (LC v) = \{\}$
 $| fv (Op n xs) = Union (fv ' set xs)$
 $| fv (Quant n v f) = fv f - \{v\}$

definition $fresh-for :: var set \Rightarrow var$ **where**

$fresh-for V = (SOME n. n \notin V)$

lemma $fresh-for-fresh: finite V \Longrightarrow fresh-for V \notin V$

$\langle proof \rangle$

Free variables

fun $fv-schema :: schema \Rightarrow var set$ **where**

$fv-schema (ps,f) = fv f - set ps$

definition $fv-subst :: subst \Rightarrow var set$ **where**

$fv-subst s = \bigcup (fv-schema ' ran (map-of s))$

definition $fv-subst1$ **where**

$fv-subst1 s = \bigcup (fv ' snd ' set s)$

lemma $fv-subst-Nil[simp]: fv-subst1 [] = \{\}$

$\langle proof \rangle$

Local constants, separate from free variables.

fun $lc :: form \Rightarrow lconst set$ **where**

$lc (Var v xs) = Union (lc ' set xs)$
 $| lc (LC c) = \{c\}$
 $| lc (Op n xs) = Union (lc ' set xs)$
 $| lc (Quant n v f) = lc f$

fun $lc-schema :: schema \Rightarrow lconst set$ **where**

$lc-schema (ps,f) = lc f$

definition *lc-subst1* **where**

$$lc\text{-}subst1\ s = \bigcup (lc\ 'snd\ 'set\ s)$$

fun *lc-subst* :: *subst* \Rightarrow *lconst set* **where**

$$lc\text{-}subst\ s = \bigcup (lc\text{-}schema\ 'snd\ 'set\ s)$$

fun *map-lc* :: (*lconst* \Rightarrow *lconst*) \Rightarrow *form* \Rightarrow *form* **where**

$$\begin{aligned} &map\text{-}lc\ f\ (Var\ v\ xs) = Var\ v\ (map\ (map\text{-}lc\ f)\ xs) \\ | &map\text{-}lc\ f\ (LC\ n) = LC\ (f\ n) \\ | &map\text{-}lc\ f\ (Op\ n\ xs) = Op\ n\ (map\ (map\text{-}lc\ f)\ xs) \\ | &map\text{-}lc\ f\ (Quant\ n\ v\ f') = Quant\ n\ v\ (map\text{-}lc\ f\ f') \end{aligned}$$

lemma *fv-map-lc[simp]*: $fv\ (map\text{-}lc\ p\ f) = fv\ f$

<proof>

lemma *lc-map-lc[simp]*: $lc\ (map\text{-}lc\ p\ f) = p\ 'lc\ f$

<proof>

lemma *map-lc-map-lc[simp]*: $map\text{-}lc\ p1\ (map\text{-}lc\ p2\ f) = map\text{-}lc\ (p1\ \circ\ p2)\ f$

<proof>

fun *map-lc-subst1* :: (*lconst* \Rightarrow *lconst*) \Rightarrow (*var* \times *form*) *list* \Rightarrow (*var* \times *form*) *list* **where**

$$map\text{-}lc\text{-}subst1\ f\ s = map\ (apsnd\ (map\text{-}lc\ f))\ s$$

fun *map-lc-subst* :: (*lconst* \Rightarrow *lconst*) \Rightarrow *subst* \Rightarrow *subst* **where**

$$map\text{-}lc\text{-}subst\ f\ s = map\ (apsnd\ (apsnd\ (map\text{-}lc\ f)))\ s$$

lemma *map-lc-noop[simp]*: $lc\ f = \{\} \Longrightarrow map\text{-}lc\ p\ f = f$

<proof>

lemma *map-lc-cong[cong]*: $(\bigwedge x. x \in lc\ f \Longrightarrow f1\ x = f2\ x) \Longrightarrow map\text{-}lc\ f1\ f = map\text{-}lc\ f2\ f$

<proof>

lemma *[simp]*: $fv\text{-}subst1\ (map\ (apsnd\ (map\text{-}lc\ p))\ s) = fv\text{-}subst1\ s$

<proof>

lemma *map-lc-subst-cong[cong]*:

assumes $(\bigwedge x. x \in lc\text{-}subst\ s \Longrightarrow f1\ x = f2\ x)$

shows $map\text{-}lc\text{-}subst\ f1\ s = map\text{-}lc\text{-}subst\ f2\ s$

<proof>

In order to make the termination checker happy, we define substitution in two stages: One that substitutes only ground terms for variables, and the real one that can substitute schematic terms (or lambda expression, if you want).

fun *subst1* :: (*var* \times *form*) *list* \Rightarrow *form* \Rightarrow *form* **where**

$$\begin{aligned} &subst1\ s\ (Var\ v\ []) = (case\ map\text{-}of\ s\ v\ of\ Some\ f \Rightarrow f\ | None \Rightarrow Var\ v\ []) \\ | &subst1\ s\ (Var\ v\ xs) = Var\ v\ xs \\ | &subst1\ s\ (LC\ n) = LC\ n \\ | &subst1\ s\ (Op\ n\ xs) = Op\ n\ (map\ (subst1\ s)\ xs) \\ | &subst1\ s\ (Quant\ n\ v\ f) = \\ &\quad (if\ v \in fv\text{-}subst1\ s\ then \\ &\quad (let\ v' = fresh\text{-}for\ (fv\text{-}subst1\ s) \\ &\quad in\ Quant\ n\ v'\ (subst1\ ((v,\ Var\ v'\ [])\#s)\ f)) \\ &\quad else\ Quant\ n\ v\ (subst1\ s\ f)) \end{aligned}$$

lemma *subst1-Nil[simp]*: $subst1\ []\ f = f$

$\langle \text{proof} \rangle$

lemma *lc-subst1*: $lc (subst1 s f) \subseteq lc f \cup \bigcup (lc \text{ ' } snd \text{ ' } set s)$
 $\langle \text{proof} \rangle$

lemma *apsnd-def'*: $apsnd f = (\lambda(k, v). (k, f v))$
 $\langle \text{proof} \rangle$

lemma *map-of-map-apsnd*:
 $map\text{-of} (map (apsnd f) xs) = map\text{-option} f \circ map\text{-of} xs$
 $\langle \text{proof} \rangle$

lemma *map-lc-subst1[simp]*: $map\text{-lc} p (subst1 s f) = subst1 (map\text{-lc}\text{-subst1} p s) (map\text{-lc} p f)$
 $\langle \text{proof} \rangle$

fun *subst'* :: $subst \Rightarrow form \Rightarrow form$ **where**
 $subst' s (Var v xs) =$
 $(case\ map\text{-of} s v\ of\ None \Rightarrow (Var v (map (subst' s) xs))$
 $| Some (ps, rhs) \Rightarrow$
 $if\ length\ ps = length\ xs$
 $then\ subst1 (zip\ ps (map (subst' s) xs))\ rhs$
 $else (Var v (map (subst' s) xs))$
 $| subst' s (LC n) = LC n$
 $| subst' s (Op n xs) = Op n (map (subst' s) xs)$
 $| subst' s (Quant n v f) =$
 $(if\ v \in fv\text{-subst} s\ then$
 $(let\ v' = fresh\text{-for} (fv\text{-subst} s)$
 $in\ Quant\ n\ v' (subst' ((v, [], Var v' []))\#s)\ f))$
 $else\ Quant\ n\ v (subst' s f)$

lemma *subst'-Nil[simp]*: $subst' [] f = f$
 $\langle \text{proof} \rangle$

lemma *lc-subst'*: $lc (subst' s f) \subseteq lc f \cup lc\text{-subst} s$
 $\langle \text{proof} \rangle$

lemma *ran-map-option-comp[simp]*:
 $ran (map\text{-option} f \circ m) = f \text{ ' } ran\ m$
 $\langle \text{proof} \rangle$

lemma *fv-schema-apsnd-map-lc[simp]*:
 $fv\text{-schema} (apsnd (map\text{-lc} p) a) = fv\text{-schema} a$
 $\langle \text{proof} \rangle$

lemma *fv-subst-map-apsnd-map-lc[simp]*:
 $fv\text{-subst} (map (apsnd (apsnd (map\text{-lc} p))) s) = fv\text{-subst} s$
 $\langle \text{proof} \rangle$

lemma *map-apsnd-zip[simp]*: $map (apsnd f) (zip a b) = zip a (map f b)$
 $\langle \text{proof} \rangle$

lemma *map-lc-subst'[simp]*: $map\text{-lc} p (subst' s f) = subst' (map\text{-lc}\text{-subst} p s) (map\text{-lc} p f)$
 $\langle \text{proof} \rangle$

Since *subst'* happily renames quantified variables, we have a simple wrapper that ensures that the substitution is minimal, and is empty if *f* is closed. This is a hack to support lemma *subst-noop*.

```

fun subst :: subst  $\Rightarrow$  form  $\Rightarrow$  form where
  subst s f = subst' (filter ( $\lambda$  (v,s). v  $\in$  fv f) s) f

lemma subst-Nil[simp]: subst [] f = f
  <proof>

lemma subst-noop[simp]: fv f = {}  $\implies$  subst s f = f
  <proof>

lemma lc-subst: lc (subst s f)  $\subseteq$  lc f  $\cup$  lc-subst s
  <proof>

lemma lc-subst-map-lc-subst[simp]: lc-subst (map-lc-subst p s) = p ' lc-subst s
  <proof>

lemma map-lc-subst[simp]: map-lc p (subst s f) = subst (map-lc-subst p s) (map-lc p f)
  <proof>

fun closed :: form  $\Rightarrow$  bool where
  closed f  $\longleftrightarrow$  fv f = {}  $\wedge$  lc f = {}

interpretation predicate: Abstract-Formulas
  curry to-nat :: nat  $\Rightarrow$  var  $\Rightarrow$  var
  map-lc
  lc
  closed
  subst
  lc-subst
  map-lc-subst
  Var 0 []
  <proof>

declare predicate.subst-lconsts-empty-subst [simp del]

end

```

8.5 Incredible_Predicate

```

theory Incredible-Predicate imports
  Abstract-Rules-To-Incredible
  Predicate-Formulas
begin

```

Our example interpretation with predicate logic will cover implication and the universal quantifier.

The rules are introduction and elimination of implication and universal quantifiers.

```

datatype prop-rule = allI | allE | impI | impE

```

```

definition prop-rules :: prop-rule stream
  where prop-rules = cycle [allI, allE, impI, impE]

```

```

lemma iR-prop-rules [simp]: sset prop-rules = {allI, allE, impI, impE}
  <proof>

```

Just some short notation.

```

abbreviation X :: form
  where X ≡ Var 10 []
abbreviation Y :: form
  where Y ≡ Var 11 []
abbreviation x :: form
  where x ≡ Var 9 []
abbreviation t :: form
  where t ≡ Var 13 []
abbreviation P :: form ⇒ form
  where P f ≡ Var 12 [f]
abbreviation Q :: form ⇒ form
  where Q f ≡ Op "Q" [f]
abbreviation imp :: form ⇒ form ⇒ form
  where imp f1 f2 ≡ Op "imp" [f1, f2]
abbreviation ForallX :: form ⇒ form
  where ForallX f ≡ Quant "all" 9 f

```

Finally the right- and left-hand sides of the rules.

```

fun consequent :: prop-rule ⇒ form list
  where consequent allI = [ForallX (P x)]
  | consequent allE = [P t]
  | consequent impI = [imp X Y]
  | consequent impE = [Y]

abbreviation allI-input where allI-input ≡ Antecedent {||} (P (LC 0)) {0}
abbreviation impI-input where impI-input ≡ Antecedent {|X|} Y {}

fun antecedent :: prop-rule ⇒ (form, lconst) antecedent list
  where antecedent allI = [allI-input]
  | antecedent allE = [plain-ant (ForallX (P x))]
  | antecedent impI = [impI-input]
  | antecedent impE = [plain-ant (imp X Y), plain-ant X]

interpretation predicate: Abstract-Rules
  curry to-nat :: nat ⇒ var ⇒ var
  map-lc
  lc
  closed
  subst
  lc-subst
  map-lc-subst
  Var 0 []
  antecedent
  consequent
  prop-rules
  ⟨proof⟩

end

```

8.6 Incredible_Predicate_Tasks

```

theory Incredible-Predicate-Tasks
imports
  Incredible-Completeness
  Incredible-Predicate
  HOL-Eisbach.Eisbach

```

begin

declare *One-nat-def* [*simp del*]

context *ND-Rules-Inst* **begin**

lemma *eff-NatRuleI*:

nat-rule rule c ants

$\implies \text{entail} = (\Gamma \vdash \text{subst } s \text{ (freshen } a \text{ } c))$

$\implies \text{hyps} = ((\lambda \text{ant. } ((\lambda p. \text{subst } s \text{ (freshen } a \text{ } p)) \mid^{\dagger} a\text{-hyps } \text{ant} \mid \cup \mid \Gamma \vdash \text{subst } s \text{ (freshen } a \text{ (} a\text{-conc } \text{ant})))) \mid^{\dagger}$
ants)

$\implies (\bigwedge \text{ant } f. \text{ant} \mid \in \mid \text{ants} \implies f \mid \in \mid \Gamma \implies \text{freshenLC } a \text{ ' (} a\text{-fresh } \text{ant} \text{) } \cap \text{lconsts } f = \{\})$

$\implies (\bigwedge \text{ant. ant} \mid \in \mid \text{ants} \implies \text{freshenLC } a \text{ ' (} a\text{-fresh } \text{ant} \text{) } \cap \text{subst-lconsts } s = \{\})$

$\implies \text{eff (NatRule rule) entail hyps}$

$\langle \text{proof} \rangle$

end

context *Abstract-Task* **begin**

lemma *natEff-InstI*:

rule = (r,c)

$\implies c \in \text{set (consequent } r)$

$\implies \text{antec} = f\text{-antecedent } r$

$\implies \text{natEff-Inst rule } c \text{ antec}$

$\langle \text{proof} \rangle$

end

context **begin**

A typical task with local constants:: $\forall x. Q \ x \longrightarrow Q \ x$

First the task is defined as an *Abstract-Task*.

interpretation *task: Abstract-Task*

curry to-nat :: nat \Rightarrow var \Rightarrow var

map-lc

lc

closed

subst

lc-subst

map-lc-subst

Var 0 []

antecedent

consequent

prop-rules

\square

$[ForallX (imp (Q \ x) (Q \ x))]$

$\langle \text{proof} \rangle$

Then we show, that this task has a proof within our formalization of natural deduction by giving a concrete proof tree.

abbreviation *lx :: nat* **where** *lx \equiv to-nat (1::nat,0::nat)*

abbreviation *base-tree :: ((form fset \times form) \times (prop-rule \times form) NatRule) tree* **where**

base-tree \equiv Node ($\{ \mid Q \ (LC \ lx) \} \vdash Q \ (LC \ lx), \text{Axiom} \ \{ \mid \})$

abbreviation *imp-tree :: ((form fset \times form) \times (prop-rule \times form) NatRule) tree* **where**

imp-tree \equiv Node ($\{ \mid \} \vdash \text{imp } (Q \ (LC \ lx)) \ (Q \ (LC \ lx)), \text{NatRule } (\text{impI}, \text{imp } X \ Y) \ \{ \mid \text{base-tree} \})$

abbreviation *solution-tree* :: ((form fset × form) × (prop-rule × form) NatRule) tree **where**
solution-tree ≡ Node ({}|{}|) ⊢ ForallX (imp (Q x) (Q x)), NatRule (allI, ForallX (P x)) {|imp-tree|}

abbreviation *s1* **where** *s1* ≡ [(12, ([9], imp (Q x) (Q x)))]

abbreviation *s2* **where** *s2* ≡ [(10, ([], Q (LC lx))), (11, ([], Q (LC lx)))]

lemma *fv-subst-s1*[simp]: *fv-subst s1* = {}
⟨proof⟩

lemma *subst1-simps*[simp]:
subst s1 (P (LC n)) = imp (Q (LC n)) (Q (LC n))
subst s1 (ForallX (P x)) = ForallX (imp (Q x) (Q x))
⟨proof⟩

lemma *subst2-simps*[simp]:
subst s2 X = Q (LC lx)
subst s2 Y = Q (LC lx)
subst s2 (imp X Y) = imp (subst s2 X) (subst s2 Y)
⟨proof⟩

lemma *substI1*: ForallX (imp (Q x) (Q x)) = subst s1 (predicate.freshen 1 (ForallX (P x)))
⟨proof⟩

lemma *substI2*: imp (Q (LC lx)) (Q (LC lx)) = subst s2 (predicate.freshen 2 (imp X Y))
⟨proof⟩

declare *subst.simps*[simp del]

lemma *task.solved*
⟨proof⟩

abbreviation *vertices* **where** *vertices* ≡ {|0::nat,1,2 |}

fun *nodeOf* **where**
nodeOf n = [Conclusion (ForallX (imp (Q x) (Q x))),
Rule allI,
Rule impI] ! n

fun *inst* **where**
inst n = [[], s1, s2] ! n

interpretation *task*: Vertex-Graph *task.nodes* *task.inPorts* *task.outPorts* *vertices* *nodeOf*⟨proof⟩

abbreviation *e1* :: (nat, form, nat) edge'
where *e1* ≡ ((1, Reg (ForallX (P x))), (0, plain-ant (ForallX (imp (Q x) (Q x)))))

abbreviation *e2* :: (nat, form, nat) edge'
where *e2* ≡ ((2, Reg (imp X Y)), (1, allI-input))

abbreviation *e3* :: (nat, form, nat) edge'
where *e3* ≡ ((2, Hyp X (impI-input)), (2, impI-input))

abbreviation *task-edges* :: (nat, form, nat) edge' set **where** *task-edges* ≡ {e1, e2, e3}

interpretation *task*: Scoped-Graph *task.nodes* *task.inPorts* *task.outPorts* *vertices* *nodeOf* *task-edges* *task.hyps*
⟨proof⟩

interpretation *task*: Instantiation
task.inPorts

```

task.outPorts
nodeOf
task.hyps
task.nodes
task-edges
vertices
task.labelsIn
task.labelsOut
curry to-nat :: nat ⇒ var ⇒ var
map-lc
lc
closed
subst
lc-subst
map-lc-subst
Var 0 []
id
inst
⟨proof⟩

```

Finally we can also show that there is a proof graph for this task.

interpretation *Well-Scoped-Graph*

```

task.nodes
task.inPorts
task.outPorts
vertices
nodeOf
task-edges
task.hyps
⟨proof⟩

```

lemma *no-path-01*[simp]: $task.path\ 0\ v\ pth \longleftrightarrow (pth = [] \wedge v = 0)$
 ⟨proof⟩

lemma *no-path-12*[simp]: $\neg task.path\ 1\ 2\ pth$
 ⟨proof⟩

interpretation *Acyclic-Graph*

```

task.nodes
task.inPorts
task.outPorts
vertices
nodeOf
task-edges
task.hyps
⟨proof⟩

```

interpretation *Saturated-Graph*

```

task.nodes
task.inPorts
task.outPorts
vertices
nodeOf
task-edges
⟨proof⟩

```

interpretation *Pruned-Port-Graph*

```

task.nodes

```

task.inPorts
task.outPorts
vertices
nodeOf
task-edges
(proof)

interpretation *Well-Shaped-Graph*

task.nodes
task.inPorts
task.outPorts
vertices
nodeOf task-edges
task.hyps
(proof)

interpretation *Solution*

task.inPorts
task.outPorts
nodeOf
task.hyps
task.nodes
vertices
task.labelsIn
task.labelsOut
curry to-nat :: nat ⇒ var ⇒ var
map-lc
lc
closed
subst
lc-subst
map-lc-subst
Var 0 []
id
inst
task-edges
(proof)

interpretation *Proof-Graph*

task.nodes
task.inPorts
task.outPorts
vertices
nodeOf
task-edges
task.hyps
task.labelsIn
task.labelsOut
curry to-nat :: nat ⇒ var ⇒ var
map-lc
lc
closed
subst
lc-subst
map-lc-subst
Var 0 []
id

inst
⟨*proof*⟩

lemma *path-20*:
 assumes *task.path 2 0 pth*
 shows $(1, \text{allI-input}) \in \text{snd } \text{'set pth}$
⟨*proof*⟩

lemma *scope-21*: $2 \in \text{task.scope } (1, \text{allI-input})$
⟨*proof*⟩

interpretation *Scoped-Proof-Graph*

curry to-nat :: $\text{nat} \Rightarrow \text{var} \Rightarrow \text{var}$
map-lc
lc
closed
subst
lc-subst
map-lc-subst
Var 0 []
task.inPorts
task.outPorts
nodeOf
task.hyps
task.nodes
vertices
task.labelsIn
task.labelsOut
id
inst
task-edges
task.local-vars
⟨*proof*⟩

interpretation *Tasked-Proof-Graph*

curry to-nat :: $\text{nat} \Rightarrow \text{var} \Rightarrow \text{var}$
map-lc
lc
closed
subst
lc-subst
map-lc-subst
Var 0 []
antecedent
consequent
prop-rules
[]
[*ForallX* (*imp* (*Q x*) (*Q x*))]
vertices
nodeOf
task-edges
id
inst
⟨*proof*⟩

end

end