T-Axi (declarative)

Wojciech Kołowski
Mateusz Pyzik

TODO

- Kinding.
- Polymorphism.
- Higher-order quantification.
- Totality checker.
- Computation.
- Inductives and records.
- Algorithmic system.
- Distinguish partial terms.

Quantities

Quantities:
$r ::= 0 \mid 1 \mid ? \mid + \mid *$

- 0 means a resource has been used up and is no longer available.
- 1 means a resource must be used exactly once.
- ? (pronounced "few") means a resource must be used at most once.
- $+$ (pronounced "many") means a resource must be used at least once.
- $*$ (pronounced "any") means no restrictions on usage.

$*$ is the default quantity, so when there's nothing to indicate quantity, it means it's $*$.

Subusage ordering

$r_1 \sqsubseteq r_2$ means that a resource with quantity r_1 may be used when quantity r_2 is expected. This ordering is called sub-usaging. The definition below is just the skeleton, the full ordering is the reflexive-transitive closure of it.

$$
\begin{gathered}
* \sqsubseteq ? \\
* \sqsubseteq + \\
+ \sqsubseteq 1 \\
? \sqsubseteq 1 \\
? \sqsubseteq 0
\end{gathered}
$$

We will denote the greatest lower bound in this order with $r_1 \sqcap r_2$ and the least upper bound (if it exists) with $r_1 \sqcup r_2$.

Addition of quantities

When we have two quantities of the same resource, we can sum the quantities.

$$
\begin{aligned}
0 + r &= r \\
r + 0 &= r \\
?+? &= * \\
? + * &= * \\
*+? &= * \\
* + * &= * \\
\_ + \_ &= +
\end{aligned}
$$

Multiplication of quantities

When we have a quantity r_1 of resource A that contains quantitty r_2 of resource B, then we in fact have quantity $r_1 \cdot r_2$ of resource B.

$$
\begin{aligned}
0 \cdot r &= 0 \\
r \cdot 0 &= 0 \\
1 \cdot r &= r \\
r \cdot 1 &= r \\
? \cdot ? &= ? \\
+ \cdot + &= + \\
\_ \cdot \_ &= *
\end{aligned}
$$

The algebra of quantities

Quantities $\mathcal{Q}$ form a positive ordered commutative semiring with no zero divisors, i.e.:

- $(\mathcal{Q}, +, 0)$ is a commutative monoid.
- $(\mathcal{Q}, \cdot, 1)$ is a commutative monoid.
- 0 annihilates multiplication.
- Multiplication distributes over addition.
- Addition and multiplication preserve the subusage ordering in both arguments.
- If $r_1 + r_2 = 0$, then $r_1 = 0$ and $r_2 = 0$.
- If $r_1 \cdot r_2 = 0$, then $r_1 = 0$ or $r_2 = 0$.

Subtraction of quantities

$r_1 - r_2$ is the least r' such that $r_1 \sqsubseteq r' + r_2$.

$r_1 - r_2$	0	1	?	$+$	$*$
0	0				
1	1	0			
?	?	0	0		
$+$	$+$	$*$	$+$	$*$	$+$
$*$	$*$	$*$	$*$	$*$	$*$

Division with remainder

$a/b = (q, r)$ when $a = b \cdot q + r$, with q as large as possible and r being as small as possible according to the order $0 \leq 1 \leq ? \leq + \leq *$. Note that $a/b = q$ means that $r = 0$.

r_1/r_2	0	1	$?$	$+$	$*$
0	$*$	0	0	0	0
1	$(*, 1)$	1	$(0, 1)$	$(0, 1)$	$(0, 1)$
$?$	$(*, ?)$	$?$	$?$	$(0, ?)$	$(0, ?)$
$+$	$(*, +)$	$+$	$(*, 1)$	$+$	$(*, 1)$
$*$	$(*, *)$	$*$	$*$	$*$	$*$

Types

Types:

$$A, B ::= r\, A \to B \mid \texttt{!}_r\, A \mid A \otimes B \mid A \oplus B \mid \texttt{Unit} \mid \texttt{Empty}$$

Terms

Terms:

$e ::=$

$x \mid \lambda_r\, x : A.\, e \mid e_1\ e_2 \mid$
$\texttt{box}_r\ e \mid \texttt{let box}\ x = e_1\ \texttt{in}\ e_2$
$(e_1, e_2) \mid \texttt{let}\ (x, y) = e_1\ \texttt{in}\ e_2 \mid$
$\texttt{inl}_A\ e \mid \texttt{inr}_A\ e \mid \texttt{case}\ e\ \texttt{of}\ (e_1, e_2) \mid$
$\texttt{unit} \mid \texttt{let}_A\ \texttt{unit} = e_1\ \texttt{in}\ e_2 \mid$
$\texttt{Empty-elim}_A\ e \mid$
$\texttt{let}_r\ x : A = e_1\ \texttt{in}\ e_2 \mid$
$\texttt{let noncomputable}\ x : A = e_1\ \texttt{in}\ e_2 \mid$
$\texttt{choose}_A\ p \mid \texttt{choose-witness}\ x\ h\ \texttt{for}\ p\ \texttt{in}\ e$

$\texttt{choose}_A\ p$ and $\texttt{choose-witness}\ x\ h\ \texttt{for}\ p\ \texttt{in}\ e$ are noncomputable terms, whereas all others are computable.

Propositions

Propositions:

$P, Q ::=$

$\quad \top \mid \bot \mid P \Rightarrow Q \mid P \wedge Q \mid P \vee Q \mid$

$\quad \forall x : A.\, P \mid \exists x : A.\, P \mid$

$\quad e_1 =_A e_2$

Notations:

$\neg P$ stands for $P \Rightarrow \bot$

$P \Leftrightarrow Q$ stands for $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

Proofterms

Proofterms (P, Q are propositions, e are terms, h are variables):

p, q ::=

h | **assumption** | **trivial** | **absurd** p
assume $h : P$ **in** q | **apply** $p_1\ p_2$ |
both $p_1\ p_2$ | **and-left** p | **and-right** p |
or-left p | **or-right** p | **cases** $p_1\ p_2\ p_3$ |
lemma $h : P$ **by** p **in** q | **proving** P **by** p |
suffices P **by** q **in** p |
pick-any $x : A$ **in** e | **instantiate** p **with** e |
witness e **such that** p | **pick-witness** $x\ h$ **for** p_1 **in** p_2 |
refl e | **rewrite** p_1 **in** p_2 | **funext** $x : A$ **in** p
by-contradiction $h : \neg P$ **in** q |
choose-spec p | **choose-witness** $x\ h$ **for** p **in** q

Contexts

Contexts:

$$\Gamma ::= \cdot \mid \Gamma, r\, x : A \mid \Gamma, r\, x : A := e \mid \Gamma, h : P$$

Judgements

Well-formed context judgement: $\Gamma\ \mathtt{ctx}_i$

Well-formed type judgement: $\Gamma \vdash A\ \mathtt{type}$
Typing judgement: $\Gamma \vdash_i e : A$

Well-formed proposition judgement: $\Gamma \vdash P\ \mathtt{prop}$
Proof judgement: $\Gamma \vdash p : P$

Sanity checks

We'll set up the system so that:

- If $\Gamma \vdash_i e : A$, then $|\Gamma| \vdash A\ \mathtt{type}$.
- If $\Gamma \vdash_i e : A$, then $\Gamma\ \mathtt{ctx}_i$.
- If $\Gamma \vdash p : P$, then $\Gamma \vdash P\ \mathtt{prop}$.
- If $\Gamma \vdash P\ \mathtt{prop}$, then $\Gamma\ \mathtt{ctx}_{\mathtt{nc}}$.
- If $\Gamma \vdash A\ \mathtt{type}$, then $\Gamma\ \mathtt{ctx}_{\mathtt{nc}}$.
- If $\Gamma\ \mathtt{ctx}_{\mathtt{nc}}$, then $\Gamma\ \mathtt{ctx}_{\mathtt{c}}$.

Operations on contexts

Operations on contexts:
$\Gamma_1 \sqsubseteq \Gamma_2$ – context subusaging
$\Gamma_1 + \Gamma_2$ – context addition
$r\,\Gamma$ – context scaling
Γ / r – context division (with remainder)
$|\Gamma|$ – cartesianization
$|\Gamma|_x$ – spotlight x

Context subusaging

$$\frac{}{\cdot \sqsubseteq \cdot}$$

$$\frac{\Gamma_1 \sqsubseteq \Gamma_2 \quad r_1 \sqsubseteq r_2}{\Gamma_1, r_1\, x : A \sqsubseteq \Gamma_2, r_2\, x : A}$$

$$\frac{\Gamma_1 \sqsubseteq \Gamma_2 \quad r_1 \sqsubseteq r_2}{\Gamma_1, r_1\, x : A := e \sqsubseteq \Gamma_2, r_2\, x : A := e}$$

$$\frac{\Gamma_1 \sqsubseteq \Gamma_2}{\Gamma_1, h : P \sqsubseteq \Gamma_2, h : P}$$

Context addition

$$\cdot + \cdot = \cdot$$
$$(\Gamma_1, r_1\, x : A) + (\Gamma_2, r_2\, x : A) = (\Gamma_1 + \Gamma_2), (r_1 + r_2)\, x : A$$
$$(\Gamma_1, r_1\, x : A := e) + (\Gamma_2, r_2\, x : A := e) = (\Gamma_1 + \Gamma_2), (r_1 + r_2)\, x : A := e$$
$$(\Gamma_1, p : P) + (\Gamma_2, h : P) = (\Gamma_1 + \Gamma_2), h : P$$

Context scaling

$$
\begin{aligned}
s\,\cdot &= \cdot \\
s\,(\Gamma, r\,x : A) &= s\,\Gamma, (s \cdot r)\,x : A \\
s\,(\Gamma, r\,x : A := e) &= s\,\Gamma, (s \cdot r)\,x : A := e \\
s\,(\Gamma, h : P) &= s\,\Gamma, h : P
\end{aligned}
$$

Spotlight

$$
\begin{aligned}
|\cdot|_x &= \cdot \\
|\Gamma, r\, x : A|_x &= 0\,\Gamma, 1\, x : A \\
|\Gamma, r\, y : A|_x &= |\Gamma|_x, 0\, y : A \\
|\Gamma, r\, x : A := e|_x &= 0\,\Gamma, 1\, x : A := e \\
|\Gamma, r\, y : A := e|_x &= |\Gamma|_x, 0\, y : A := e \\
|\Gamma, h : P|_x &= |\Gamma|_x, h : P
\end{aligned}
$$

Context division with remainder

$$\frac{}{\cdot/r = \cdot}$$

$$\frac{\Gamma/q = (\Gamma_1, \Gamma_2) \quad r/q = (r_1, r_2)}{(\Gamma, r\,x : A)/q = ((\Gamma_1, r_1\,x : A), (\Gamma_2, r_2\,x : A))}$$

$$\frac{\Gamma/q = (\Gamma_1, \Gamma_2) \quad r/q = (r_1, r_2)}{(\Gamma, r\,x : A := e)/q = ((\Gamma_1, r_1\,x : A := e), (\Gamma_2, r_2\,x : A := e))}$$

$$\frac{\Gamma/q = \Gamma'}{(\Gamma, h : P)/q = ((\Gamma', h : P), (\Gamma', h : P))}$$

Cartesianization

Cartesianization turns a context into a traditional context that doesn't mention any quantities.

$$
\begin{aligned}
|\cdot| &= \cdot \\
|\Gamma, r\, x : A| &= |\Gamma|, x : A \\
|\Gamma, r\, x : A := e| &= |\Gamma|, x : A := e \\
|\Gamma, h : P| &= |\Gamma|, h : P
\end{aligned}
$$

Well-formed contexts

$$\frac{}{\cdot\ \mathtt{ctx_c}}$$

$$\frac{\Gamma\ \mathtt{ctx_c} \quad |\Gamma| \vdash A\ \mathtt{type} \quad x \notin \Gamma}{\Gamma, r\, x : A\ \mathtt{ctx_c}}$$

$$\frac{\Gamma\ \mathtt{ctx_c} \quad |\Gamma| \vdash_{\mathtt{nc}} e : A \quad x \notin \Gamma}{\Gamma, r\, x : A := e\ \mathtt{ctx_c}}$$

$$\frac{\Gamma\ \mathtt{ctx_c} \quad |\Gamma| \vdash P\ \mathtt{prop} \quad h \notin \Gamma}{\Gamma, h : P\ \mathtt{ctx_c}}$$

Q: Do we really need to check type well-formedness in a cartesianized context?

Cartesian contexts

$$\frac{\Gamma\ \mathtt{ctx_c} \quad \Gamma = |\Gamma|}{\Gamma\ \mathtt{ctx_{nc}}}$$

Well-formed types

$$\frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}}}{\Gamma \vdash \mathtt{Unit}\ \mathtt{type}} \qquad \frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}}}{\Gamma \vdash \mathtt{Empty}\ \mathtt{type}}$$

$$\frac{\Gamma \vdash A\ \mathtt{type} \quad \Gamma \vdash B\ \mathtt{type}}{\Gamma \vdash r\,A \to B\ \mathtt{type}} \qquad \frac{\Gamma \vdash A\ \mathtt{type}}{\Gamma \vdash\ !_r\,A\ \mathtt{type}}$$

$$\frac{\Gamma \vdash A\ \mathtt{type} \quad \Gamma \vdash B\ \mathtt{type}}{\Gamma \vdash A \otimes B\ \mathtt{type}} \qquad \frac{\Gamma \vdash A\ \mathtt{type} \quad \Gamma \vdash B\ \mathtt{type}}{\Gamma \vdash A \oplus B\ \mathtt{type}}$$

The inherent quantity of a type

$$
\begin{aligned}
\mathtt{qty}(\mathtt{Unit}) &= * \\
\mathtt{qty}(\mathtt{Empty}) &= * \\
\mathtt{qty}(\mathtt{!}_0\, A) &= * \\
\mathtt{qty}(\mathtt{!}_r\, A) &= r \cdot \mathtt{qty}(A) \\
\mathtt{qty}(A \otimes B) &= \mathtt{qty}(A) \sqcup \mathtt{qty}(B) \\
\mathtt{qty}(A \oplus B) &= \mathtt{qty}(A) \sqcup \mathtt{qty}(B) \\
\mathtt{qty}(r\, A \to B) &= 1
\end{aligned}
$$

Total quantity added to context

$$r_A^{\mathtt{nc}} = *$$
$$r_A^{\mathtt{c}} = r \cdot \mathtt{qty}(A)$$

Using variables

$$\frac{\Gamma\ \texttt{ctx}_i \quad (x : A) \in \Gamma \quad \Gamma \sqsubseteq |\Gamma|_x}{\Gamma \vdash_i x : A}$$

Functions

$$\frac{\Gamma, r^i_A\, x : A \vdash_i e : B}{\Gamma \vdash_i \lambda_r\, x : A.\, e : r\, A \to B}$$

$$\frac{\Gamma \sqsubseteq \Gamma_1 + r\,\Gamma_2 \quad \Gamma_1 \vdash_i e_1 : r\, A \to B \quad \Gamma_2 \vdash_i e_2 : A}{\Gamma \vdash_i e_1\ e_2 : B}$$

Box

$$\frac{\Gamma \sqsubseteq r\,\Gamma' \quad \Gamma' \vdash_i e : A}{\Gamma \vdash_i \mathtt{box}_r\ e : !_r\, A}$$

$$\frac{\Gamma \sqsubseteq \Gamma_1 + \Gamma_2 \quad \Gamma_1 \vdash_i e_1 : !_r\, A \quad \Gamma_2, r^i_A\, x : A \vdash_i e_2 : B}{\Gamma \vdash_i \mathtt{let\ \ box}\ x = e_1\ \mathtt{in}\ e_2 : B}$$

Q: Notation for box intro and elim?

Empty

$$\frac{|\Gamma| \vdash A \; \texttt{type} \qquad \Gamma \vdash_i e : \texttt{Empty}}{\Gamma \vdash_i \texttt{Empty-elim}_A \; e : A}$$

Unit

$$\frac{\Gamma\ \mathtt{ctx}_i \quad \Gamma \sqsubseteq 0\,\Gamma}{\Gamma \vdash_i \mathtt{unit} : \mathtt{Unit}}$$

$$\frac{\Gamma \sqsubseteq \Gamma_1 + \Gamma_2 \quad \Gamma_1 \vdash_i e_1 : \mathtt{Unit} \quad \Gamma_2 \vdash_i e_2 : A}{\Gamma \vdash_i \mathtt{let}_A\ \mathtt{unit} = e_1\ \mathtt{in}\ e_2 : A}$$

Products

$$\frac{\Gamma \sqsubseteq \Gamma_1 + \Gamma_2 \quad \Gamma_1 \vdash_i a : A \quad \Gamma_2 \vdash_i b : B}{\Gamma \vdash_i (a, b) : A \otimes B}$$

$$\frac{\Gamma \sqsubseteq \Gamma_1 + \Gamma_2 \quad \Gamma_1 \vdash_i e_1 : A \otimes B \quad \Gamma_2, 1^i_A\, x : A, 1^i_B\, y : B \vdash_i e_2 : C}{\Gamma \vdash_i \mathtt{let}\ (x, y) = e_1\ \mathtt{in}\ e_2 : C}$$

Sums

$$\frac{\Gamma \vdash_i e : A \quad |\Gamma| \vdash B \ \mathtt{type}}{\Gamma \vdash_i \mathtt{inl}_B \ e : A \oplus B} \qquad \frac{|\Gamma| \vdash A \ \mathtt{type} \quad \Gamma \vdash_i e : B}{\Gamma \vdash_i \mathtt{inr}_A \ e : A \oplus B}$$

$$\frac{\Gamma \sqsubseteq \Gamma_1 + \Gamma_2 \quad \Gamma_1 \vdash_i e : A \oplus B \quad \Gamma_2 \vdash_i f : 1\, A \to C \quad \Gamma_2 \vdash_i g : 1\, B \to C}{\Gamma \vdash_i \mathtt{case} \ e \ \mathtt{of} \ (f, g) : C}$$

Q: Do we want first-order representation of the branches?
Probably yes.

Let

$$\frac{\Gamma \sqsubseteq r\,\Gamma_1 + \Gamma_2 \quad \Gamma_1 \vdash_i e_1 : A \quad \Gamma_2, r^i_A\, x : A := e_1 \vdash_i e_2 : B}{\Gamma \vdash_i \texttt{let}_r\ x : A = e_1\ \texttt{in}\ e_2 : B}$$

Well-formed propositions

$$\frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}}}{\Gamma \vdash \top\ \mathtt{prop}} \qquad \frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}}}{\Gamma \vdash \bot\ \mathtt{prop}}$$

$$\frac{\Gamma \vdash P\ \mathtt{prop} \quad \Gamma \vdash Q\ \mathtt{prop}}{\Gamma \vdash P \Rightarrow Q\ \mathtt{prop}}$$

$$\frac{\Gamma \vdash P\ \mathtt{prop} \quad \Gamma \vdash Q\ \mathtt{prop}}{\Gamma \vdash P \wedge Q\ \mathtt{prop}} \qquad \frac{\Gamma \vdash P\ \mathtt{prop} \quad \Gamma \vdash Q\ \mathtt{prop}}{\Gamma \vdash P \vee Q\ \mathtt{prop}}$$

$$\frac{\Gamma \vdash A\ \mathtt{type} \quad \Gamma, x : A \vdash P\ \mathtt{prop}}{\Gamma \vdash \forall x : A.\, P\ \mathtt{prop}}$$

$$\frac{\Gamma \vdash A\ \mathtt{type} \quad \Gamma, x : A \vdash P\ \mathtt{prop}}{\Gamma \vdash \exists x : A.\, P\ \mathtt{prop}}$$

$$\frac{\Gamma \vdash A\ \mathtt{type} \quad \Gamma \vdash_{\mathtt{nc}} e_1 : A \quad \Gamma \vdash_{\mathtt{nc}} e_2 : A}{\Gamma \vdash e_1 =_A e_2\ \mathtt{prop}}$$

Substitution

The notation is $P\,[x := e]$ for substitution in propositions.

Q: Do we need to check type well-formedness when checking proposition well-formedness? It should follow from the other sanity checks.

Type well-formedness checks are redundant.

Assumptions and implication

$$\frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}} \quad (h : P) \in \Gamma}{\Gamma \vdash h : P} \qquad \frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}} \quad (h : P) \in \Gamma}{\Gamma \vdash \textbf{assumption} : P}$$

$$\frac{\Gamma, h : P \vdash q : Q}{\Gamma \vdash \textbf{assume}\ h : P\ \textbf{in}\ q : P \Rightarrow Q}$$

$$\frac{\Gamma \vdash q : P \Rightarrow Q \quad \Gamma \vdash p : P}{\Gamma \vdash \textbf{apply}\ q\ p : Q}$$

Propositional logic

$$\frac{\Gamma\ \mathtt{ctx}_{\mathtt{nc}}}{\Gamma \vdash \textbf{trivial} : \top} \qquad \frac{\Gamma \vdash Q\ \mathtt{prop} \quad \Gamma \vdash p : \bot}{\Gamma \vdash \textbf{absurd}\ p : Q}$$

$$\frac{\Gamma \vdash p : P \quad \Gamma \vdash q : Q}{\Gamma \vdash \textbf{both}\ p\ q : P \wedge Q}$$

$$\frac{\Gamma \vdash pq : P \wedge Q}{\Gamma \vdash \textbf{and-left}\ pq : P} \qquad \frac{\Gamma \vdash pq : P \wedge Q}{\Gamma \vdash \textbf{and-right}\ pq : Q}$$

$$\frac{\Gamma \vdash p : P \quad \Gamma \vdash Q\ \mathtt{prop}}{\Gamma \vdash \textbf{or-left}\ p : P \vee Q} \qquad \frac{\Gamma \vdash P\ \mathtt{prop} \quad \Gamma \vdash q : Q}{\Gamma \vdash \textbf{or-right}\ q : P \vee Q}$$

$$\frac{\Gamma \vdash pq : P \vee Q \quad \Gamma \vdash r_1 : P \Rightarrow R \quad \Gamma \vdash r_2 : Q \Rightarrow R}{\Gamma \vdash \textbf{cases}\ pq\ r_1\ r_2 : R}$$

Utilities

$$\frac{\Gamma \vdash p : P \quad \Gamma, h : P \vdash q : Q}{\Gamma \vdash \textbf{lemma } h : P \textbf{ by } p \textbf{ in } q : Q}$$

$$\frac{\Gamma \vdash p : P}{\Gamma \vdash \textbf{proving } P \textbf{ by } p : P}$$

$$\frac{\Gamma \vdash pq : P \Rightarrow Q \quad \Gamma \vdash p : P}{\Gamma \vdash \textbf{suffices } P \textbf{ by } pq \textbf{ in } p : Q}$$

Quantifiers

$$\frac{\Gamma, x : A \vdash p : P}{\Gamma \vdash \textbf{pick-any } x : A \textbf{ in } p : \forall x : A.\, P}$$

$$\frac{\Gamma \vdash p : \forall x : A.\, P \quad \Gamma \vdash_{\mathtt{nc}} e : A}{\Gamma \vdash \textbf{instantiate } p \textbf{ with } e : P\,[x := e]}$$

$$\frac{\Gamma \vdash_{\mathtt{nc}} e : A \quad \Gamma, x : A \vdash P \ \mathtt{prop} \quad \Gamma \vdash p : P\,[x := e]}{\Gamma \vdash \textbf{witness } e \textbf{ such that } p : \exists x : A.\, P}$$

$$\frac{\Gamma \vdash p : \exists x : A.\, P \quad \Gamma \vdash Q \ \mathtt{prop} \quad \Gamma, x : A, h : P \vdash q : Q}{\Gamma \vdash \textbf{pick-witness } x \ h \textbf{ for } p \textbf{ in } q : Q}$$

Equality

$$\frac{\Gamma \vdash_{\mathtt{nc}} e : A}{\Gamma \vdash \mathbf{refl}\ e : e =_A e}$$

$$\frac{\Gamma \vdash q : e_1 =_A e_2 \quad \Gamma, x : A \vdash P\ \mathtt{prop} \quad \Gamma \vdash p : P\,[x := e_2]}{\Gamma \vdash \mathbf{rewrite}\ q\ \mathbf{in}\ p : P\,[x := e_1]}$$

$$\frac{\Gamma, x : A \vdash p : f\ x =_B g\ x}{\Gamma \vdash \mathbf{funext}\ x : A\ \mathbf{in}\ p : f =_{r\,A \to B} g}$$

Classical Logic

$$\frac{\Gamma, h : \neg P \vdash q : \bot}{\Gamma \vdash \textbf{by-contradiction } h : \neg P \textbf{ in } q : P}$$

$$\frac{|\Gamma| \vdash p : \exists x : A.\, P}{\Gamma \vdash_{\mathtt{nc}} \mathtt{choose}\ p : A}$$

$$\frac{\Gamma \vdash p : \exists x : A.\, P}{\Gamma \vdash \textbf{choose-spec } p : P\,[x := \mathtt{choose}\ p]}$$

$$\frac{\Gamma \vdash p : \exists x : A.\, P \quad \Gamma \vdash Q\ \mathtt{prop} \quad \Gamma, x : A := \mathtt{choose}\ p, h : P \vdash q : Q}{\Gamma \vdash \textbf{choose-witness } x\ h \textbf{ for } p \textbf{ in } q : Q}$$

$$\frac{|\Gamma| \vdash p : \exists x : A.\, P \quad |\Gamma| \vdash B\ \mathtt{type} \quad \Gamma, x : A := \mathtt{choose}\ p, h : P \vdash_{\mathtt{nc}} e : B}{\Gamma \vdash_{\mathtt{nc}} \mathtt{choose\text{-}witness}\ x\ h\ \mathtt{for}\ p\ \mathtt{in}\ e : B}$$

Environments

Global environments:

$$\Sigma ::= \\ \quad \emptyset \mid \Sigma, h : P := p \mid \Sigma, x : A := e \mid \\ \quad \Sigma, \texttt{partial}\ x : A := e \mid \Sigma, \texttt{totality}\ x\ p$$

Well-formed environments

$$\frac{}{\emptyset\ \texttt{env}}$$

$$\frac{\Sigma\ \texttt{env} \quad h \notin \Sigma \quad \Sigma \mid \cdot \vdash p : P}{\Sigma, h : P := p\ \texttt{env}}$$

$$\frac{\Sigma\ \texttt{env} \quad x \notin \Sigma \quad \Sigma \mid \cdot \vdash_{\mathsf{c}} e : A}{\Sigma, x : A := e\ \texttt{env}}$$

$$\frac{\Sigma\ \texttt{env} \quad x \notin \Sigma \quad \Sigma \mid \cdot \vdash_{\mathsf{c}} e : A \quad e\ \textbf{fails syntactic check}}{\Sigma, \texttt{partial}\ x : A := e\ \texttt{env}}$$

$$\frac{\Sigma\ \texttt{env} \quad \Sigma = \Sigma_1, \texttt{partial}\ x : A := e, \Sigma_2 \quad \Sigma \mid \cdot \vdash p : \exists r : A.\, e =?= r}{\Sigma, \texttt{totality}\ x\ p\ \texttt{env}}$$