Proof Irrelevance with Hereditary Substitution

Jason Reed

May 16, 2006

1 Language

Relevance	$\star, *$	$::=$	$: \mid \div$
Normal Terms	M, N	$::=$	$\lambda x.M \mid R$
Atomic Terms	R	$::=$	$H \cdot S$
Heads	H	$::=$	$x \mid c$
Spines	S	$::=$	$() \mid (M^\star; S)$
Types	A, B	$::=$	$a \cdot S \mid \Pi x \star A.B$
Kinds	K, L	$::=$	$\mathrm{type} \mid \Pi x \star A.K$
Classifiers	V, W	$::=$	$A \mid K$
Contexts	Γ	$::=$	$\cdot \mid \Gamma, x \star A$
Signatures	Σ	$::=$	$\cdot \mid \Sigma, c : A \mid \Sigma, a : K$
Simple Types	τ	$::=$	$o \mid \tau_1 \to \tau_2$

2 Syntactic Operations

2.1 Simplification

$$(a \cdot S)^- = o$$

$$(\Pi x \star A.B)^- = (A)^- \to (B)^-$$

2.2 Substitution and Reduction

Definitions adapted from [CLF paper *XXX cite*]. Substitution is a partial function $[M/x]^\tau N$ on two terms and a simple type; it is the substitution of the term M for the variable x at simple type τ in the term N, which may be undefined. The definition of substitution is mutually recursive with that of *reduction* $[M|S]^\tau$, which operates on a term M and list of arguments (a 'spine') S at simple type τ, and produces the term that is the result of applying the head M (presumed to be of simple type τ) to arguments S.

The important case of the definition of substitution is when we reach the variable, and invoke reduction (see below).

$$[M/x]^\tau(x \cdot S) = [M|[M/x]^\tau S]^\tau$$

The remainder of the definition consists of simple congruences. Let σ abbreviate $[M/x]^\tau$.

$$\begin{aligned}
\sigma(\lambda y.N) &= \lambda y.\sigma N \\
\sigma(y \cdot S) &= y \cdot (\sigma S) \qquad (y \neq x) \\
\sigma(c \cdot S) &= c \cdot (\sigma S) \\
\sigma() &= () \\
\sigma(N^\star; S) &= ((\sigma N)^\star; \sigma S) \\
\sigma(a \cdot S) &= a \cdot (\sigma S) \\
\sigma(\Pi y \star A.B) &= \Pi y \star (\sigma A).(\sigma B) \\
\sigma\, \mathrm{type} &= \mathrm{type} \\
\sigma(\Pi y \star A.K) &= \Pi y \star (\sigma A).(\sigma K) \\
\sigma\cdot &= \cdot \\
\sigma(\Gamma, x \star A) &= (\sigma\Gamma), x \star (\sigma A)
\end{aligned}$$

2.3 Reduction

Here we recursively use the definition of substitution, but only at strictly smaller simple types.

$$[\lambda x.M|(N^\star; S)]^{\tau_1 \to \tau_2} = [[N/x]^{\tau_1} M|S]^{\tau_2}$$

$$[R|()]^o = R$$

Any other reduction $[M|S]^\tau$ that doesn't match these two patterns is undefined.

2.4 Promotion

Promotion is an operation on contexts; written as $\Gamma^\star$, it outputs a context.

$$\cdot^{\div} = \cdot$$

$$(\Gamma, x \star A)^{\div} = \Gamma^{\div}, x : A$$

$$\Gamma^{:} = \Gamma$$

The purpose of promotion is to allow irrelevant arguments to functions to refer to irrelevant hypotheses. When irrelevant arguments are type-checked, they are checked in the 'promoted' context where all irrelevant hypotheses have been converted to genuine ones.

2.5 Equivalence

We tacitly identify all α-equivalent terms. If a metavariable is repeated, it implies a requirement of strict syntactic identity (up to α-equivalence). We write this same notion of syntactic identity as $=$. The definition of equivalence $\equiv$ is nearly the same as $=$, except that we accept as equal all terms M found at positions of the form $(M^{\div}; S)$. In other words the term identity of terms 'at irrelevant position' does not matter. A program that checks equivalence does strictly a subset of the work an ordinary syntactic equality check would have performed. In this way we have unique canonical forms *up to* the choice of irrelevant representatives.

$$\frac{M_1 \equiv M_2}{\lambda x.M_1 \equiv \lambda x.M_2}$$

$$\frac{S_1 \equiv S_2}{H \cdot S_1 \equiv H \cdot S_2}$$

$$\frac{}{() \equiv ()}$$

$$\frac{M_1 \equiv M_2 \qquad S_1 \equiv S_2}{(M_1^{\vdots}; S_1) \equiv (M_2^{\vdots}; S_2)} \qquad \frac{S_1 \equiv S_2}{(M_1^{\div}; S_1) \equiv (M_2^{\div}; S_2)}$$

$$\frac{S_1 \equiv S_2}{a \cdot S_1 \equiv a \cdot S_2}$$

$$\frac{A_1 \equiv A_2 \qquad V_1 \equiv V_2}{\Pi x \star A_1.V_1 \equiv \Pi x \star A_2.V_2}$$

$$\frac{}{\mathrm{type} \equiv \mathrm{type}}$$

3 Typing

We begin with signature validity — it is, however, mutually recursive with all the remaining typing rules. These are the only ones on which we explicitly index the judgement by a signature. All turnstiles that follow these three rules carry an implicit Σ subscript.

3.1 Signature Validity

$$\frac{}{\vdash \cdot : \mathrm{sgn}}$$

$$\frac{\cdot \vdash_\Sigma A : \mathrm{type} \qquad \vdash \Sigma : \mathrm{sgn}}{\vdash (\Sigma, c : A) : \mathrm{sgn}}$$

$$\frac{\cdot \vdash_\Sigma K : \mathrm{kind} \qquad \vdash \Sigma : \mathrm{sgn}}{\vdash (\Sigma, a : K) : \mathrm{sgn}}$$

Term typing is divided naturally into checking and synthesis.

3.2 Term Checking

$$\frac{\Gamma, x \star A \vdash M \Leftarrow B}{\Gamma \vdash \lambda x.M \Leftarrow \Pi x \star A.B}$$

In the following rule, the boundary between synthesis and checking, we check that the synthesized type is equal to the type the term is checked against, up to the choice of irrelevant representatives.

$$\frac{\Gamma \vdash R \Rightarrow A' \qquad A \equiv A'}{\Gamma \vdash R \Leftarrow A}$$

3.3 Term Synthesis

$$\frac{c : A \in \Sigma \qquad \Gamma \vdash S : A > B}{\Gamma \vdash c \cdot S \Rightarrow B}$$

$$\frac{x : A \in \Gamma \qquad \Gamma \vdash S : A > B}{\Gamma \vdash x \cdot S \Rightarrow B}$$

3.4 Spine Synthesis

In $\Gamma \vdash S : V > W$, the inputs are Γ, S, V, and W is output.

$$\frac{}{\Gamma \vdash () : a \cdot S > a \cdot S}$$

$$\frac{}{\Gamma \vdash () : \text{type} > \text{type}}$$

$$\frac{\Gamma \vdash M \Leftarrow^\star A \qquad \Gamma \vdash S : [M/x]^{A^-} V > W}{\Gamma \vdash (M^\star; S) : \Pi x \star A.V > W}$$

3.5 Promotion

$$\frac{\Gamma^\star \vdash M \Leftarrow B}{\Gamma \vdash M \Leftarrow^\star B}$$

3.6 Type Validity

$$\frac{a : K \in \Sigma \qquad \Gamma \vdash S : K > \text{type}}{\Gamma \vdash a \cdot S : \text{type}}$$

$$\frac{\Gamma \vdash A : \text{type} \qquad \Gamma, x \star A \vdash B : \text{type}}{\Gamma \vdash \Pi x \star A.B : \text{type}}$$

3.7 Kind Validity

$$\frac{}{\Gamma \vdash \mathrm{type} : \mathrm{kind}}$$

$$\frac{\Gamma \vdash A : \mathrm{type} \qquad \Gamma, x \star A \vdash K : \mathrm{kind}}{\Gamma \vdash \Pi x \star A.K : \mathrm{kind}}$$

3.8 Context Validity

$$\frac{}{\vdash \cdot : \mathrm{ctx}}$$

$$\frac{\Gamma \vdash A : \mathrm{type} \qquad \vdash \Gamma : \mathrm{ctx}}{\vdash (\Gamma, x \star A) : \mathrm{ctx}}$$

4 Properties

Lemma 4.1 *If $\Gamma \vdash R \Rightarrow A$, then A is of the form $a \cdot S$.*

Proof By induction on the structure of the typing derivation. ■

A note on the fact that substitution is partial: when we say two expressions are syntactically identical without any further qualification, (i.e. $M = N$) we mean that either both are undefined, or both are defined and syntactically identical.

Lemma 4.2 $([M/x]^\tau \Gamma)^{\div} = [M/x]^\tau (\Gamma^{\div})$.

Proof By induction on the structure of Γ. ■

Definition Defining $\Gamma \preceq \Gamma'$, "Γ is weaker than Γ'".

$$\frac{}{\cdot \preceq \cdot} \qquad \frac{\Gamma \preceq \Gamma'}{\Gamma, x \star A \preceq \Gamma, x \star A} \qquad \frac{\Gamma \preceq \Gamma'}{\Gamma, x \div A \preceq \Gamma, x : A}$$

Lemma 4.3 *Suppose $\Gamma \preceq \Gamma'$. If $\Gamma \vdash J$ then $\Gamma' \vdash J$, for any typing judgment J.*

Proof By induction on the structure of the typing derivation. Most cases are trivial. The only interesting cases are those that treat rules that significantly manipulate the context.

Case:

$$\mathcal{D} = \frac{\overset{\mathcal{D}'}{\Gamma, x \star A_0 \vdash M_0 \Leftarrow B}}{\Gamma \vdash \lambda x.M_0 \Leftarrow \Pi x \star A_0.B}$$

Observe that since $\Gamma \preceq \Gamma'$, also $\Gamma, x \star A_0 \preceq \Gamma', x \star A_0$. Use the induction hypothesis on this fact and the derivation $\mathcal{D}'$ to obtain $\Gamma', x \star A_0 \vdash M_0 \Leftarrow B$. Rule application gives $\Gamma' \vdash \lambda x.M_0 \Leftarrow \Pi x \star A_0.B$ as required.

Case:

$$\mathcal{D} = \cfrac{x : A \in \Gamma \qquad \overset{\mathcal{D}'}{\Gamma \vdash S : A > B}}{\Gamma \vdash x \cdot S \Rightarrow B}$$

Use the induction hypothesis on $\mathcal{D}'$ to get $\Gamma' \vdash S : A > B$. It follows from the definition of $\preceq$ that if $x : A \in \Gamma$ and $\Gamma \preceq \Gamma'$, then $x : A \in \Gamma'$. So by rule application we see $\Gamma' \vdash x \cdot S \Rightarrow B$ as required.

Case:

$$\mathcal{D} = \cfrac{\overset{\mathcal{D}'}{\Gamma^\star \vdash M \Leftarrow B}}{\Gamma \vdash M \Leftarrow^\star B}$$

It is easy to see from the definitions of $\preceq$ and promotion that if $\Gamma \preceq \Gamma'$, then $\Gamma^\star \preceq (\Gamma')^\star$ for either possible value of $\star$. Therefore use the induction hypothesis on $\mathcal{D}'$ to obtain $(\Gamma')^\star \vdash M \Leftarrow B$ and apply the rule to get $\Gamma' \vdash M \Leftarrow^\star B$ as required.

■

Corollary 4.4 *If $\Gamma \vdash M \Leftarrow^\star A$, then $\Gamma^\div \vdash M \Leftarrow A$.*

Proof If $\star$ is :, then apply the lemma to $\Gamma \vdash M \Leftarrow A$ (which we know by inversion) and the fact that $\Gamma \preceq \Gamma^\div$. If $\star$ is $\div$ then the result is immediate from inversion. ■

Lemma 4.5 *If $[M/x]^\tau A$ is well-defined, then $([M/x]^\tau A)^- = A^-$.*

Proof By induction on the structure of A. ■

Lemma 4.6 (Weakening) *If $\Gamma, \Gamma' \vdash J$ then $\Gamma, x \star A, \Gamma' \vdash J$.*

Proof By induction on the derivation of $\Gamma \vdash J$. ■

Lemma 4.7 *If X contains no free occurrence of x, then $[M/x]^\tau X = X$.*

Proof By induction on the structure of X. ■

Lemma 4.8 *If $X \equiv X'$ and both $[M/x]^\tau X$ and $[M/x]^\tau X'$ are defined, then $[M/x]^\tau X \equiv [M/x]^\tau X'$.*

Proof By induction over $\mathcal{D} :: X \equiv X'$. The only interesting case is when

$$\mathcal{D} = \cfrac{\overset{\mathcal{D}'}{S_1 \equiv S_2}}{(M_1^\div ; S_1) \equiv (M_2^\div ; S_2)}$$

Here the induction hypothesis on $\mathcal{D}'$ gives us that $[M/x]^\tau S_1 \equiv [M/x]^\tau S_2$. By rule application we get $(([M/x]^\tau M_1)^\div ; [M/x]^\tau S_1) \equiv (([M/x]^\tau M_2)^\div ; [M/x]^\tau S_2)$ as required. ■

Lemma 4.9 *Make the following abbreviations:* $\sigma_B = [N/z]^{B^-}$, $\sigma_A = [M/x]^{A^-}$, *and* $\sigma'_A = [\sigma_B M/x]^{A^-}$.

1. *Suppose* $\sigma_A V$, $\sigma_B V$, *and* $\sigma_B M$ *are defined. Suppose* x *does not occur free in* N. *Then* $\sigma_B \sigma_A V$ *and* $\sigma'_A \sigma_B V$ *are both defined, and* $\sigma_B \sigma_A V = \sigma'_A \sigma_B V$.

2. *Suppose* $[M|S]^{C^-}$, $\sigma_B M$, *and* $\sigma_B S$ *are defined. Then* $\sigma_B [M|S]^{C^-}$ *and* $[\sigma_B M|\sigma_B S]^{C^-}$ *are both defined, and* $\sigma_B [M|S]^{C^-} = [\sigma_B M|\sigma_B S]^{C^-}$.

Proof By lexicographic induction first on the simple type (either the larger of (A^-, B^-) in case 1 or C^- in case 2), and subsequently on the structure of the expression V.

1.

Case: $V = z \cdot S$.

$$\sigma'_A \sigma_B (z \cdot S) = \sigma'_A [N|\sigma_B S]^{B^-}$$

$$\sigma_B \sigma_A (z \cdot S) = [\sigma'_A N|\sigma_B \sigma_A S]^{B^-}$$

We know that $\sigma'_A N$ is defined because x does not occur in N. By the induction hypothesis part 1, we know that $\sigma'_A \sigma_B S$ and $\sigma_B \sigma_A S$ are defined and identical. From the induction hypothesis part 2 on N, $\sigma_B S$, B^-, and σ'_A, we get $\sigma'_A [N|\sigma_B S]^{B^-} = [\sigma'_A N|\sigma'_A \sigma_B S]^{B^-}$. It follows from the identity above that the latter is the same as $[\sigma'_A N|\sigma_B \sigma_A S]^{B^-}$, as required.

Case: $V = x \cdot S$.

$$\sigma'_A \sigma_B (x \cdot S) = [\sigma_B M|\sigma'_A \sigma_B S]^{A^-}$$

$$\sigma_B \sigma_A (x \cdot S) = \sigma_B [M|\sigma_A S]^{A^-}$$

We know that $\sigma_B M$ is defined by assumption. The remained of this case is symmetric to the previous one.

2.

Case: $M = \lambda w.M'$, $S = ((M'')^\star; S')$, and $C^- = C_1^- \to C_2^-$. Then by definition of reduction

$$\sigma_B [M|S]^{C^-} = \sigma_B [[M''/w]^{C_1^-} M'|S']^{C_2^-} \qquad (*)$$

$$[\sigma_B M|\sigma_B S]^{C^-} = [[\sigma_B M''/w]^{C_1^-} \sigma_B M'|\sigma_B S']^{C_2^-} \qquad (**)$$

We can see from the induction hypothesis (part 1, at a smaller type) that

$$\sigma_B [M''/w]^{C_1^-} M' = [\sigma_B M''/w]^{C_1^-} \sigma_B M'$$

and both are well-defined, since w can't appear in N. Thus we can use the induction hypothesis (part two, at C_2^-) to conclude the right-hand sides of $(*)$ and $(**)$ are equal, as required.

■

Lemma 4.10 (Substitution) *Suppose* $\Gamma \vdash N \Leftarrow^* B$. *Let* σ *be an abbreviation for* $[N/z]^{B^-}$, *with* z *being a variable that does not occur free in* Γ *or* B. *For cases 2-5, suppose* $\sigma\Gamma'$ *is well-defined.*

1. *If* $\Gamma \vdash S : B > A$ *and* $\Gamma \vdash M \Leftarrow B$ *then* $\Gamma \vdash [M|S]^{B^-} \Rightarrow A$.
2. *If* $\Gamma, z * B, \Gamma' \vdash M \Leftarrow^\star A$ *and* σA *is defined, then* $\Gamma, \sigma\Gamma' \vdash \sigma M \Leftarrow^\star \sigma A$.
3. *If* $\Gamma, z * B, \Gamma' \vdash M \Leftarrow A$ *and* σA *is defined, then* $\Gamma, \sigma\Gamma' \vdash \sigma M \Leftarrow \sigma A$.
4. *If* $\Gamma, z * B, \Gamma' \vdash R \Rightarrow A$, *then* $\Gamma, \sigma\Gamma' \vdash \sigma R \Rightarrow \sigma A$.
5. *If* $\Gamma, z * B, \Gamma' \vdash S : V > W$ *and* σV *is defined, then* $\Gamma, \sigma\Gamma' \vdash \sigma S : \sigma V > \sigma W$.

Proof By lexicographic induction on first the simple type B^-, next on the case (where case 1 is ordered less than all the remaining cases), and finally (for cases 2-5) on the structure of the typing derivation.

1.

Case: M is of the form $\lambda x.M_0$. Then the typing derivation of M must be of the form

$$\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, x \star B_1 \vdash M_0 \Leftarrow B_2\end{array}}{\Gamma \vdash \lambda x.M_0 \Leftarrow \Pi x \star B_1.B_2}$$

Since we know that B is $\Pi x \star B_1.B_2$, the typing derivation of S must look like

$$\dfrac{\begin{array}{cc}\mathcal{D}_2 & \mathcal{D}_3\\ \Gamma \vdash M_1 \Leftarrow^\star B_1 & \Gamma \vdash S_1 : [M_1/x]^{B_1^-} B_2 > A\end{array}}{\Gamma \vdash (M_1^\star; S_1) : \Pi x \star B_1.B_2 > A}$$

with S being $(M_1^\star; S_1)$. By the induction hypothesis (part 3) on the smaller simple type B_1^- and the derivations $\mathcal{D}_1$ and $\mathcal{D}_2$, (knowing that $[M_1/x]^{B_1^-} B_2$ is defined because we have $\mathcal{D}_3$ in our hands) we find that

$$\Gamma \vdash [M_1/x]^{B_1^-} M_0 \Leftarrow [M_1/x]^{B_1^-} B_2 \qquad (*)$$

Observe that by Lemma 4.5 we know $([M_1/x]^{B_1^-} B_2)^- = B_2^-$, and therefore (since B_2^- is a smaller simple type) we can apply the induction hypothesis (part 1) to $(*)$ and the derivation $\mathcal{D}_3$ to infer first that

$$\Gamma \vdash [[M_1/x]^{B_1^-} M_0|S_1]^{([M_1/x]^{B_1^-} B_2)^-} \Leftarrow A$$

and subsequently by the syntactic identity we just noted

$$\Gamma \vdash [[M_1/x]^{B_1^-} M_0|S_1]^{B_2^-} \Leftarrow A$$

But by definition of reduction we can read off that

$$[M|S]^{B^-} = [(\lambda x.M_0)|(M_1^\star; S_1)]^{B_1^- \to B_2^-} = [[M_1/x]^{B_1^-} M_0|S_1]^{B_2^-}$$

so we are done.

Case: M is atomic, i.e. of the form R. By inversion and Lemma 4.1 we have a typing derivation

$$\Gamma \vdash R \Leftarrow a \cdot S_0 \qquad (*)$$

That is, B is $a \cdot S_0$, and so $B^- = o$. The only typing rule that would conclude $S : B > A$ is

$$\frac{}{\Gamma \vdash () : a \cdot S_0 > a \cdot S_0}$$

so S must be empty, and A is also $a \cdot S_0$. Therefore

$$[M|S]^{B^-} = [R|()]^o = R$$

but we already have a derivation that $\Gamma \vdash R \Leftarrow a \cdot S_0$, namely $(*)$.

2.

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}' \\ \Gamma, z * B, \Gamma' \vdash M \Leftarrow A\end{array}}{\Gamma, z * B, \Gamma' \vdash M \Leftarrow^{:} A}$$

By the induction hypothesis on $\mathcal{D}'$ we obtain $\Gamma, \sigma\Gamma' \vdash \sigma M \Leftarrow \sigma A$. By rule application we have $\Gamma, \sigma\Gamma' \vdash \sigma M \Leftarrow^{:} \sigma A$ as required.

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}' \\ (\Gamma, z * B, \Gamma')^{\div} \vdash M \Leftarrow A\end{array}}{\Gamma, z * B, \Gamma' \vdash M \Leftarrow^{\div} A}$$

By Corollary 4.4 we know $\Gamma^{\div} \vdash N \Leftarrow B$, so we can apply the induction hypothesis to $\mathcal{D}'$ (which, unwinding the definition of promotion, is a derivation of $\Gamma^{\div}, z : B, (\Gamma')^{\div} \vdash M \Leftarrow A$) to obtain $\Gamma^{\div}, \sigma((\Gamma')^{\div}) \vdash \sigma M \Leftarrow \sigma A$. This is the same as $(\Gamma, \sigma\Gamma')^{\div} \vdash \sigma M \Leftarrow \sigma A$ by Lemma 4.2. By rule application we have $\Gamma, \sigma\Gamma' \vdash \sigma M \Leftarrow^{\div} \sigma A$ as required.

3.

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}' \\ \Gamma, z * B, \Gamma', x \star A_0 \vdash M_0 \Leftarrow B_0\end{array}}{\Gamma, z * B, \Gamma' \vdash \lambda x.M_0 \Leftarrow \Pi x \star A_0.B_0}$$

By the induction hypothesis on $\mathcal{D}'$ we know $\Gamma, \sigma\Gamma', x \star \sigma A_0 \vdash \sigma M_0 \Leftarrow \sigma B_0$. By rule application we obtain $\Gamma, \sigma\Gamma' \vdash \lambda x.\sigma M_0 \Leftarrow \Pi x \star \sigma A_0.\sigma B_0$ as required.

Case:

$$\mathcal{D} = \dfrac{\overset{\mathcal{D}'}{\Gamma, z * B, \Gamma' \vdash R \Rightarrow A'} \qquad A \equiv A'}{\Gamma, z * B, \Gamma' \vdash R \Leftarrow A}$$

By the induction hypothesis on $\mathcal{D}'$ we obtain $\Gamma, \sigma\Gamma' \vdash \sigma R \Rightarrow \sigma A'$. Since $A \equiv A'$, so too $\sigma A \equiv \sigma A'$ by Lemma 4.8. By rule application we obtain $\Gamma, \sigma\Gamma' \vdash \sigma R \Leftarrow \sigma A$ as required.

4.

Case:

$$\mathcal{D} = \dfrac{c : A_0 \in \Sigma \qquad \overset{\mathcal{D}'}{\Gamma, z * B, \Gamma' \vdash S : A_0 > A}}{\Gamma, z * B, \Gamma' \vdash c \cdot S \Rightarrow A}$$

By the induction hypothesis on $\mathcal{D}'$ we obtain $\Gamma, \sigma\Gamma' \vdash \sigma S : \sigma A_0 > \sigma A$. But A_0 can have no free occurrence of z, so $\sigma A_0 = A_0$ by Lemma 4.7. By rule application we get $\Gamma, \sigma\Gamma' \vdash c \cdot \sigma S \Rightarrow \sigma A$ as required.

Case:

$$\mathcal{D} = \dfrac{x : A_0 \in \Gamma, z * B, \Gamma' \qquad \overset{\mathcal{D}'}{\Gamma, z * B, \Gamma' \vdash S : A_0 > A}}{\Gamma, z * B, \Gamma' \vdash x \cdot S \Rightarrow A}$$

We split on three subcases depending on the location of $x \in \Gamma, z * B, \Gamma'$.

Subcase: $x \in \Gamma$. In this case z can have no occurrence in the type A_0 of x. Thus σA_0 is syntactically equal to A_0 by Lemma 4.7. By the induction hypothesis (part 5) on $\mathcal{D}'$ we obtain $\Gamma, \sigma\Gamma' \vdash \sigma S : A_0 > \sigma A$. By rule application we get $\Gamma, \sigma\Gamma' \vdash x \cdot \sigma S \Rightarrow \sigma A$ as required.

Subcase: x is in fact z. In this case A_0 and B are syntactically identical, the relevancy variable $*$ must be :, and the term $\sigma(x \cdot S)$ we aim to type is $[N|\sigma S]^{B^-}$. We know $\Gamma \vdash N \Leftarrow B$, and by using Lemma 4.6 repeatedly we can obtain $\Gamma, \sigma\Gamma' \vdash N \Leftarrow B$. By Lemma 4.7 and the induction hypothesis (part 5), we know $\Gamma, \sigma\Gamma' \vdash \sigma S : B > \sigma A$. Use the induction hypothesis (part 1: this is licensed because it is ordered as less than the other cases, and the simple type B^- has remained the same) to obtain the required derivation of $\Gamma, \sigma\Gamma' \vdash [N|\sigma S]^{B^-} \Rightarrow \sigma A$.

Subcase: $x \in \Gamma'$. By assumption on Γ', we have that σA_0 is defined. By the induction hypothesis (part 5) $\Gamma, \sigma\Gamma' \vdash \sigma S : \sigma A_0 > \sigma A$. Clearly $x : \sigma A_0 \in \Gamma, \sigma\Gamma'$ so it follows by rule application that $\Gamma, \sigma\Gamma' \vdash x \cdot \sigma S \Rightarrow \sigma A$.

5.

Case:

$$\mathcal{D} = \overline{\Gamma, z * B, \Gamma' \vdash () : a \cdot S > a \cdot S}$$

Since we know $a \cdot \sigma S$ is defined, by rule application we immediately have $\Gamma, \sigma\Gamma' \vdash () : a \cdot \sigma S > a \cdot \sigma S$.

Case:

$$\mathcal{D} = \overline{\Gamma, z * B, \Gamma' \vdash () : \text{type} > \text{type}}$$

By rule application, we immediately have $\Gamma, \sigma\Gamma' \vdash () : \text{type} > \text{type}$.

Case:

$$\mathcal{D} = \frac{\begin{array}{cc} \mathcal{D}_1 & \mathcal{D}_2 \\ \Gamma, z * B, \Gamma' \vdash M \Leftarrow^{\star} A & \Gamma, z * B, \Gamma' \vdash S : [M/x]^{A^-} V > W \end{array}}{\Gamma, z * B, \Gamma' \vdash (M^{\star}; S) : \Pi x \star A.V > W}$$

By the induction hypothesis (part 2) we know $\Gamma, \sigma\Gamma' \vdash \sigma M \Leftarrow^{\star} \sigma A$. Observe that M has no free occurrence of z, by assumption σV is well-defined, and from the existence of $\mathcal{D}_2$ we know that $[M/x]^{A^-} V$ is well-defined. Therefore we can use Lemma 4.9 to infer that both $[\sigma M/x]^{A^-} \sigma V$ and $\sigma[M/x]^{A^-} V$ are defined, and that they are syntatically identical. By the induction hypothesis (part 5) we know $\Gamma, \sigma\Gamma' \vdash \sigma S : \sigma[M/x]^{A^-} V > \sigma W$, which is the same thing as $\Gamma, \sigma\Gamma' \vdash \sigma S : [\sigma M/x]^{A^-} \sigma V > \sigma W$. By rule application we obtain $\Gamma, \sigma\Gamma' \vdash (\sigma M^{\star}; \sigma S) : \Pi x \star \sigma A.\sigma V > \sigma W$.

■

Lemma 4.11 (Validity) *Suppose* Γ *is well-formed.*

1. *If* $\Gamma \vdash R \Rightarrow A$ *then* $\Gamma \vdash A : \text{type}$.
2. *If* $\Gamma \vdash S : A > B$ *and* $\Gamma \vdash A : \text{type}$*, then* $\Gamma \vdash B : \text{type}$.

Proof By induction on the structure of the derivation. Requires the fact that if Γ valid, then $\Gamma^{\div}$ valid, which requires Corollary 4.4. ■