Type Theory and Formal Proof

An Introduction

Rob Nederpelt
Herman Geuvers

Published by
Cambridge University Press

Solutions to Selected Exercises and Errata

SOLUTIONS TO SELECTED EXERCISES

Chapter 1

1.3 $\lambda z \,.\, z(\lambda z \,.\, y) =_\alpha \lambda x \,.\, (z(\lambda z \,.\, y))^{z \to x}$, because $x \notin FV(z \,.\, (\lambda z \,.\, y))$ and x is not a binding variable in $z(\lambda z \,.\, y)$.

Since $\lambda x \,.\, (z(\lambda z \,.\, y))^{z \to x} \equiv \lambda x \,.\, x(\lambda z \,.\, y)$, by symmetry of $=_\alpha$, it follows that $\lambda x \,.\, x(\lambda z \,.\, y) =_\alpha \lambda z \,.\, z(\lambda z \,.\, y)$.

1.16 (a) Since M has a β-normal form, there is an L in β-nf such that $M =_\beta L$. By CR there is an N such that $M \twoheadrightarrow_\beta N$ and $L \twoheadrightarrow_\beta N$. The latter and Lemma 1.9.2 imply that $L \equiv N$, hence $M \twoheadrightarrow_\beta L$.

From $M \twoheadrightarrow_\beta M_i$ and $M \twoheadrightarrow_\beta L$ follows $M_i =_\beta L$. So, M_i *has* a β-normal form, since L is in β-nf.

1.16 (b) On the one hand, $(\lambda u \,.\, v)\Omega \to_\beta v$ (take the full term as the redex) and v is in β-nf, so $(\lambda u \,.\, v)\Omega$ has a β-normal form.

On the other hand, $(\lambda u \,.\, v)\Omega \to_\beta (\lambda u \,.\, v)\Omega \to_\beta (\lambda u \,.\, v)\Omega \ldots$ (take Ω as the redex).

Chapter 2

2.5 (a) Since x has two arguments in the subterm $x(\lambda z \,.\, y)y$, we start with $x : \sigma \to \tau \to \rho$. Then $\lambda z \,.\, y : \sigma$ and $y : \tau$.

Take $z : \zeta$, then $\lambda z : \zeta \,.\, y \;:\; \zeta \to \tau \equiv \sigma$. Hence $x : (\zeta \to \tau) \to \tau \to \rho$ and we get the legal term $\lambda x : (\zeta \to \tau) \to \tau \to \rho \,.\, \lambda y : \tau \,.\, x(\lambda z : \zeta \,.\, y)y$ of type $((\zeta \to \tau) \to \tau \to \rho) \to \tau \to \rho$.

2.5 (b) Again, take $x : \sigma \to \tau \to \rho$. Then $\lambda z \,.\, x : \sigma$ and $y : \tau$.

Take $z : \zeta$, then $\lambda z : \zeta \,.\, x \;:\; \zeta \to \sigma \to \tau \to \rho \equiv \sigma$, which is impossible. Hence, $\lambda x \,.\, \lambda y \,.\, x(\lambda z \,.\, x)y$ is not typable.

2.10 (d) Consider the subterm $y(x\,z)z$. Since $x : \alpha \to \beta$, we must have $z : \alpha$ and hence $x\,z : \beta$. So, $y : \beta \to \alpha \to \gamma$ for some type γ. Now we can derive:

(a)	$y : \beta \to \alpha \to \gamma$	
(b)	$\quad z : \alpha$	
(c)	$\quad\quad x : \alpha \to \beta$	
(1)	$\quad\quad\quad x\,z : \beta$	(*appl*) on (c) and (b)
(2)	$\quad\quad\quad y(x\,z) : \alpha \to \gamma$	(*appl*) on (a) and (1)
(3)	$\quad\quad\quad y(x\,z)z : \gamma$	(*appl*) on (2) and (b)

(4) $\quad | \quad | \quad \lambda x : \alpha \to \beta \,.\, y(x\,z)z \;:\; (\alpha \to \beta) \to \gamma \qquad (abst)$ on (3)

Hence, $\lambda x : \alpha \to \beta \,.\, y(x\,z)z$ is legal, since we have found a context Γ (namely $y : \beta \to \alpha \to \gamma,\; z : \alpha$) and a type τ (namely $(\alpha \to \beta) \to \gamma$) such that $\Gamma \vdash \lambda x : \alpha \to \beta \,.\, y(x\,z)z \;:\; \tau$.

2.12 (a)

$$
\begin{array}{l}
\boxed{x : (\alpha \to \beta) \to \alpha} \\
\quad \boxed{y : \alpha \to \alpha \to \beta} \\
\quad\quad \boxed{z : \alpha} \\
\quad\quad\quad y\,z : \alpha \to \beta \\
\quad\quad\quad y\,z\,z : \beta \\
\quad\quad \lambda z : \alpha \,.\, y\,z\,z \;:\; \alpha \to \beta \\
\quad\quad x(\lambda z : \alpha \,.\, y\,z\,z) \;:\; \alpha \quad (*) \\
\quad \lambda y : \alpha \to \alpha \to \beta \,.\, x(\lambda z : \alpha \,.\, y\,z\,z) \;:\; (\alpha \to \alpha \to \beta) \to \alpha \\
\lambda x : (\alpha \to \beta) \to \alpha \,.\, \lambda y : \alpha \to \alpha \to \beta \,.\, x(\lambda z : \alpha \,.\, y\,z\,z) \;: \\
\qquad ((\alpha \to \beta) \to \alpha) \to (\alpha \to \alpha \to \beta) \to \alpha
\end{array}
$$

2.12 (b)

$$
\begin{array}{l}
\boxed{x : (\alpha \to \beta) \to \alpha} \\
\quad \boxed{y : \alpha \to \alpha \to \beta} \\
\quad\quad x(\lambda z : \alpha \,.\, y\,z\,z) \;:\; \alpha \quad \text{(see } (*) \text{ in part (a))} \\
\quad\quad y(x(\lambda z : \alpha \,.\, y\,z\,z)) : \alpha \to \beta \\
\quad\quad y(x(\lambda z : \alpha \,.\, y\,z\,z))(x(\lambda z : \alpha \,.\, y\,z\,z)) : \beta \\
\quad \lambda y : \alpha \to \alpha \to \beta \,.\, y(x(\lambda z : \alpha \,.\, y\,z\,z))(x(\lambda z : \alpha \,.\, y\,z\,z)) \;: \\
\qquad\quad (\alpha \to \alpha \to \beta) \to \beta \\
\lambda x : (\alpha \to \beta) \to \alpha \,.\, \lambda y : \alpha \to \alpha \to \beta \,.\, y(--)(--) \;: \\
\qquad ((\alpha \to \beta) \to \alpha) \to (\alpha \to \alpha \to \beta) \to \beta
\end{array}
$$

2.18 Proof of the Compatibility cases of Lemma 2.11.5.

Induction: Subject Reduction holds for the assumption $M \to_\beta M'$; that is: for all Γ and σ, if $\Gamma \vdash M : \sigma$ and $M \to_\beta M'$, then $\Gamma \vdash M' : \sigma$.

(2.1) Case 1: $\Gamma \vdash MK : \rho$ and $MK \to_\beta M'K$. Then by Lemma 2.10.7 (2) there is a type σ such that $\Gamma \vdash M : \sigma \to \rho$ and $\Gamma \vdash K : \sigma$. By induction: $\Gamma \vdash M' : \sigma \to \rho$. Hence $\Gamma \vdash M'K : \rho$.

(2.2) Case 2: $\Gamma \vdash KM : \rho$ and $KM \to_\beta K'M$. Then by Lemma 2.10.7 (2) there is a type σ such that $\Gamma \vdash K : \sigma \to \rho$ and $\Gamma \vdash M : \sigma$. By induction: $\Gamma \vdash M' : \sigma$. Hence $\Gamma \vdash KM' : \rho$.

(2.3) Case 3: $\Gamma \vdash \lambda x : \tau \,.\, M : \rho$. Then by Lemma 2.10.7 (3) there is a type σ such that $\Gamma, x : \tau \vdash M : \sigma$ and $\rho \equiv \tau \to \sigma$. By induction: $\Gamma, x : \tau \vdash M' : \sigma$. Hence $\Gamma \vdash \lambda x : \tau \,.\, M' : \tau \to \sigma$, so $\Gamma \vdash \lambda x : \tau \,.\, M' : \rho$.

Chapter 3

3.6 (b)

> $\alpha : *$
>
> > $\beta : *$
> >
> > > $\gamma : *$
> > >
> > > > $\delta : *$
> > > >
> > > > > $x : (\alpha \to \gamma) \to \delta$
> > > > >
> > > > > > $y : \alpha \to \beta$
> > > > > >
> > > > > > > $z : \beta \to \gamma$
> > > > > > >
> > > > > > > > $u : \alpha$
> > > > > > > >
> > > > > > > > $y\,u : \beta$
> > > > > > > >
> > > > > > > > $z(y\,u) : \gamma$
> > > > > > >
> > > > > > > $\lambda u : \alpha \,.\, z(y\,u) : \alpha \to \gamma$
> > > > > > >
> > > > > > > $x(\lambda u : \alpha \,.\, z(y\,u)) : \delta$
> > > > > >
> > > > > > $\lambda z : \beta \to \gamma \,.\, x(\lambda u : \alpha \,.\, z(y\,u)) : (\beta \to \gamma) \to \delta$
> > > > >
> > > > > $\lambda y : \alpha \to \beta \,.\, \lambda z : \beta \to \gamma \,.\, x(\lambda u : \alpha \,.\, z(y\,u))$:
> > > > > $(\alpha \to \beta) \to (\beta \to \gamma) \to \delta$
> > > >
> > > > $\lambda x : (\alpha \to \gamma) \to \delta \,.\, \lambda y : \alpha \to \beta \,.\, \lambda z : \beta \to \gamma \,.\, x(\lambda u : \alpha \,.\, z(y\,u))$:
> > > > $((\alpha \to \gamma) \to \delta) \to (\alpha \to \beta) \to (\beta \to \gamma) \to \delta$
> > >
> > > $\lambda \delta : * \,.\, \lambda x : (\alpha \to \gamma) \to \delta \,.\, \lambda y : \alpha \to \beta \,.\, \lambda z : \beta \to \gamma \,.$
> > > $x(\lambda u : \alpha \,.\, z(y\,u))$:
> > > $\Pi \delta : * \,.\, ((\alpha \to \gamma) \to \delta) \to (\alpha \to \beta) \to (\beta \to \gamma) \to \delta$

3.6 (c)

$\alpha : *$

$\beta : *$

$\gamma : *$

$x : \alpha \to (\beta \to \alpha) \to \gamma$

$y : \alpha$

$x\,y : (\beta \to \alpha) \to \gamma$

$z : \beta$

$y : \alpha \quad (var)$

$\lambda z : \beta \,.\, y \;:\; \beta \to \alpha$

$x\,y(\lambda z : \beta \,.\, y) \;:\; \gamma$

and so on

So an inhabitant is:

– $\lambda\alpha : * \,.\, \lambda\beta : * \,.\, \lambda\gamma : * \,.\, \lambda x : \alpha \to (\beta \to \alpha) \to \gamma \,.\, \lambda y : \alpha \,.\, x\,y(\lambda z : \beta \,.\, y)$.

3.13 (b) $\mathit{Mult} \equiv \lambda m, n : \mathit{Nat} \,.\, \lambda\alpha : * \,.\, \lambda f : \alpha \to \alpha \,.\, \lambda x : \mathit{Nat} \,.\, m\,\alpha(n\,\alpha\,f)x$.

Example:

$\mathit{Mult}\ \mathit{One}\ \mathit{Two} \twoheadrightarrow_\beta \lambda\alpha : * \,.\, \lambda f : \alpha \to \alpha \,.\, \lambda x : \mathit{Nat} \,.\, \mathit{One}\ \alpha(\mathit{Two}\ \alpha\, f)x$.

Now we have:

(1) $\mathit{Two}\ \alpha\, f \equiv (\lambda\alpha : * \,.\, \lambda f : \alpha \to \alpha \,.\, \lambda x : \alpha \,.\, f(f\,x))\alpha\, f \twoheadrightarrow_\beta \lambda x : \alpha \,.\, f(f\,x)$,

(2) $\mathit{One}\ \alpha(\mathit{Two}\ \alpha\, f) \twoheadrightarrow_\beta (\lambda\alpha : * \,.\, \lambda f : \alpha \to \alpha \,.\, \lambda x : \alpha \,.\, f\,x)\alpha(\lambda x : \alpha \,.\, f(f\,x)) \twoheadrightarrow_\beta \lambda x : \alpha \,.\, (\lambda x : \alpha \,.\, f(f\,x))x \to_\beta \lambda x : \alpha \,.\, f(f\,x)$,

(3) $\mathit{One}\ \alpha(\mathit{Two}\ \alpha\, f)x \twoheadrightarrow_\beta f(f\,x)$.

So $\mathit{Mult}\ \mathit{One}\ \mathit{Two} \twoheadrightarrow_\beta \lambda\alpha : * \,.\, \lambda f : \alpha \to \alpha \,.\, \lambda x : \mathit{Nat} \,.\, f(f\,x) \equiv \mathit{Two}$.

3.17 We try to find a $\lambda 2$-term M such that $(\lambda u : \mathit{Nat} \,.\, M)\mathit{Zero} \twoheadrightarrow_\beta \mathit{True}$ and $(\lambda u : \mathit{Nat} \,.\, M)n \twoheadrightarrow_\beta \mathit{False}$ for polymorphic Church numerals n that are not *Zero*.

In the if–then–else term of Exercise 1.14, what we take for x in $x\,u\,v$ decides about the answer. Here the decision follows from what we take for u. Therefore we substitute $u\,X\,Y$ for M and try to find X and Y. We now have:

$(\lambda u : \mathit{Nat} \,.\, u\,X\,Y)\mathit{Zero} \to_\beta \mathit{Zero}\,X\,Y$, which should reduce to *True*,

and for other numbers (for example *One*):

$(\lambda u : \mathit{Nat} \,.\, u\,X\,Y)\mathit{One} \to_\beta \mathit{One}\,X\,Y$, which should reduce to *False*.

Now both *Zero* and *One* have not two, but three abstractions in their definitions, so $u\,X\,Y$ is not good enough. We should add one more argument to u.

Since *Zero* and *One* start with $\lambda\alpha : *. \ \dots$ and end in x or $f\,x$, both of type α, and since the answer must always be a Boolean (*True* or *False*), it is a good guess to take *Bool* for α.

So instead of $u\,X\,Y$ we try $u\,Bool\,X\,Y$ and we try to find X and Y such that $Zero\,Bool\,X\,Y \twoheadrightarrow_\beta True$ and $One\,Bool\,X\,Y \twoheadrightarrow_\beta False$. Now we can easily see that $Zero\,Bool\,X\,Y \twoheadrightarrow_\beta Y$ and $One\,Bool\,X\,Y \twoheadrightarrow_\beta X\,Y$. Hence, we can take *True* for Y and the function $\lambda x : Bool\,.\,False$ for X, since then $X\,Y \twoheadrightarrow_\beta False$.

Altogether, we get $Iszero \equiv \lambda u : Nat\,.\,u\,Bool\,(\lambda x : Bool\,.\,False)\,True$, and it is not hard to verify that this works not only for *Zero* and *One*, but also for the other polymorphic Church numerals.

Chapter 4

4.3 (a)

(1)	$* : \Box$	(*sort*)
	$\boxed{\alpha : *}$	
(2)	$* : \Box$	(*weak*) on (1) and (1)
(3)	$\alpha : *$	(*var*) on (1)
	$\boxed{\beta : *}$	
(4)	$* : \Box$	(*weak*) on (2) and (2)
(5)	$\alpha : *$	(*weak*) on (3) and (2)
(6)	$\beta : *$	(*var*) on (2)
	$\boxed{x : \alpha}$	
(7)	$x : \alpha$	(*var*) on (5)
(8)	$\alpha : *$	(*weak*) on (5) and (5)
(9)	$\beta : *$	(*weak*) on (6) and (5)
(10)	$\alpha \to \beta : *$	(*form*) on (8) and (9)
	$\boxed{y : \alpha \to \beta}$	
(11)	$y : \alpha \to \beta$	(*var*) on (10)
(12)	$x : \alpha$	(*weak*) on (7) and (10)
(13)	$y\,x : \beta$	(*appl*) on (11) and (12)

4.4 (a)

(a)	$\alpha : *$	
(b)	$\quad \beta : * \to *$	
(1)	$\quad \beta\,\alpha : *$	(*appl*) on (b) and (a)
(2)	$\quad \beta(\beta\,\alpha : *$	(*appl*) on (b) and (1)

4.5

(a)	$\alpha : *$	
(b)	$\quad x : \alpha$	
(c)	$\qquad y : \alpha$	
(1)	$\qquad x : \alpha$	(*weak*) on (b)
(2)	$\quad \lambda y : \alpha \,.\, x \,:\, \alpha \to \alpha$	(*abst*) on (1)
(d)	$\qquad \beta : *$	
(3)	$\qquad \beta \to \beta \,:\, *$	(*form*) on (d) and (d)
(4)	$\quad \lambda\beta : * \,.\, \beta \to \beta \,:\, * \to *$	(*abst*) on (3)
(5)	$\quad (\lambda\beta : * \,.\, \beta \to \beta)\alpha \,:\, *$	(*appl*) on (4) and (a)
(6)	$\quad \lambda y : \alpha \,.\, x \,:\, (\lambda\beta : * \,.\, \beta \to \beta)\alpha$	(*conv*) on (2) and (5)

4.6 (b) Proof by induction on the structure of the derivation tree of the judgement $\Gamma \vdash M \to \Box \,:\, N$.

The last step in the derivation can only have been (*weak*), (*form*) or (*cond*).
Case 1: (*weak*). First premiss must have been of the form $\Gamma' \vdash M \to \Box \,:\, N$. By induction this is not derivable.
Case 2: (*form*). Second premiss must have been $\Gamma \vdash \Box \,:\, N$. This is not derivable by Exercise 4.6 (a).
Case 3: (*cond*). First premiss must have been $\Gamma \vdash M \to \Box \,:\, L$. By induction this is not derivable.

Final conclusion: $\Gamma \vdash M \to \Box \,:\, N$ is not derivable.

Chapter 5

5.4

The kind $* \to *$ is actually $\Pi x : * \,.\, *$, which can only be constructed by means of (*form*). The first `premiss` then requires $\Gamma \vdash * : *$.

However, $\Gamma \vdash * : B$ is impossible for any B not being $\Box$ (which can be shown by induction on the length of the assumed derivation of such a judgement, by inspection of the derivation rules given in Figure 5.1). As a consequence, $\Gamma \vdash * : *$ is impossible, so $* \to * : \Box$ cannot be derived in any Γ.

A similar observation holds for all other kinds, except $*$ itself.

5.9 (b) Proof in natural deduction:

(a)	$\boxed{\forall_{x \in S}(P(x) \Rightarrow Q(x))}$	
(b)	$\quad \boxed{\forall_{y \in S}(P(y))}$	
(c)	$\quad\quad \boxed{z \in S}$	
(1)	$\quad\quad P(z) \Rightarrow Q(z)$	$\forall$-elimination on (a) and (c)
(2)	$\quad\quad P(z)$	$\forall$-elimination on (b) and (c)
(3)	$\quad\quad Q(z)$	$\Rightarrow$-elimination on (1) and (2)
(4)	$\quad \forall_{z \in S}(Q(z))$	$\forall$-introduction on (3)
(5)	$(\forall_{y \in S}(P(y))) \Rightarrow (\forall_{z \in S}(Q(z)))$	$\Rightarrow$-introduction on (4)
(6)	$(\forall_{x \in S}(P(x) \Rightarrow Q(x))) \Rightarrow ((\forall_{y \in S}(P(y))) \Rightarrow (\forall_{z \in S}(Q(z))))$	$\Rightarrow$-introduction on (5)

Proof by a λP-derivation:

$$\boxed{S : *}$$
$$\quad \boxed{P, Q : S \to *}$$
$$\quad\quad \boxed{u : \Pi x : S \,.\, (P\, x \to Q\, x)}$$
$$\quad\quad\quad \boxed{v : \Pi y : S \,.\, P\, y}$$
$$\quad\quad\quad\quad \boxed{z : S}$$
$$\quad\quad\quad\quad u\, z : P\, z \to Q\, z$$
$$\quad\quad\quad\quad v\, z : P\, z$$
$$\quad\quad\quad\quad u\, z\, (v\, z) : Q\, z$$
$$\quad\quad\quad \lambda z : S \,.\, u\, z\, (v\, z) : \Pi z : S \,.\, Q\, z$$
$$\quad\quad \lambda v : (\Pi y : S \,.\, P\, y) \,.\, \lambda z : S \,.\, u\, z\, (v\, z) : (\Pi y : S \,.\, P\, y) \to \Pi z : S \,.\, Q\, z$$
$$\quad \lambda u : (\Pi x : S \,.\, (P\, x \to Q\, x)) \,.\, \lambda v : (\Pi y : S \,.\, P\, y) \,.\, \lambda z : S \,.\, u\, z\, (v\, z) : (\Pi x : S \,.\, (P\, x \to Q\, x)) \to (\Pi y : S \,.\, P\, y) \to \Pi z : S \,.\, Q\, z$$

5.11 Note that $R(g(g\, x))(g\, x)$ can be obtained from the second assumption if we have $Q(g(g\,x))(f(g\,x))$, which in its turn follows from the first assumption and $Q(g\,x)(f(f(g\,x)))$. The last-mentioned expression is a consequence of the third assumption, as can be seen in the following derivation:

$$\boxed{S : *}$$

$$\boxed{Q, R \;:\; S \to S \to *}$$

$$\boxed{f, g \;:\; S \to S}$$

$$\boxed{u \;:\; \Pi x, y : S\,.\; Q\,x(f\,y) \to Q(g\,x)y}$$

$$\boxed{v \;:\; \Pi x, y : S\,.\; Q\,x(f\,y) \to R\,x\,y}$$

$$\boxed{w \;:\; \Pi x : S\,.\; Q\,x(f(f\,x))}$$

$$\boxed{x : S}$$

$$g\,x : S$$

$$w(g\,x) \;:\; Q(g\,x)(f(f(g\,x)))$$

$$f(g\,x) \;:\; S$$

$$u(g\,x)(f(g\,x)) \;:\; Q(g\,x)(f(f(g\,x))) \to Q(g(g\,x))(f(g\,x))$$

$$u(g\,x)(f(g\,x))(w(g\,x)) \;:\; Q(g(g\,x))(f(g\,x))$$

$$g(g\,x) : S$$

$$v(g(g\,x))(g\,x) \;:\; Q(g(g\,x))(f(g\,x)) \to R(g(g\,x))(g\,x)$$

$$v(g(g\,x))(g\,x)\,(u(g\,x)(f(g\,x))(w(g\,x))) \;:\; R(g(g\,x))(g\,x)$$

$$\lambda x : S\,.\; v(g(g\,x))(g\,x)\,(u(g\,x)(f(g\,x))(w(g\,x))) \;:\; \Pi x : S\,.\; R(g(g\,x))(g\,x)$$

Chapter 6

6.4 (a) Determine the (s_1, s_2)-combination of each Π-type occurring in M:

Π-type	(s_1, s_2)	because
$S \to *$	$(*, \square)$	
$S \to S \to *$	$(*, \square)$	$S \to * \ : \ \square$
$\bot$	$(\square, *)$	
$Q\,y\,x \to \bot$	$(*, *)$	$\bot : *$
$Q\,x\,y \to Q\,y\,x \to \bot$	$(*, *)$	$Q\,y\,x \to \bot \ : \ *$
$Q\,z\,z \to \bot$	$(*, *)$	$\bot : *$
$\Pi z : S\,.\,(Q\,z\,z \to \bot)$	$(*, *)$	
$\Pi y : S\,.\,(Q\,x\,y \to Q\,y\,x \to \bot)$	$(*, *)$	
$\Pi x, y : S\,.\,(Q\,x\,y \to Q\,y\,x \to \bot)$	$(*, *)$	
$(\Pi x, y : S\,.\ \ldots) \to (\Pi z : S\,.\ \ldots)$	$(*, *)$	

So the smallest system to which this judgement belongs is λP2.

6.4 (c) M can be interpreted as the proposition
$\forall_{x,y \in S}(Q(x,y) \Rightarrow \neg Q(y,x)) \Rightarrow \forall_{z \in S}(\neg Q(z,z))$.
The inhabiting term describes, in an abstract manner, the steps that can be made to achieve a natural deduction proof of this proposition, namely:

> $\forall_{x,y \in S}(Q(x,y) \Rightarrow \neg Q(y,x))$
>
> > $z \in S$
> >
> > > $Q(z,z)$
> > >
> > > $\forall_{y \in S}(Q(z,y) \Rightarrow \neg Q(y,z))$ $(\forall\!-\!elim)$
> > >
> > > $Q(z,z) \Rightarrow \neg Q(z,z))$ $(\forall\!-\!elim)$
> > >
> > > $\neg Q(z,z))$ $(\Rightarrow\!-\!elim)$
> > >
> > > $contradiction\ (i.e. :\bot)$ $(\Rightarrow\!-\!elim)$
> >
> > $\neg Q(z,z)$ $(\neg\!-\!intro)$
>
> $\forall_{z \in S}(\neg Q(z,z))$ $(\forall\!-\!intro)$

$(\forall_{x,y \in S}(Q(x,y) \Rightarrow \neg Q(y,x)) \Rightarrow \forall_{z \in S}(\neg Q(z,z))$ $(\Rightarrow\!-\!intro)$

For example, the subterm $u\,z$ of the inhabiting term describes how to apply $(\forall\!-\!elim)$ on $\forall_{x,y \in S}(Q(x,y) \Rightarrow \neg Q(y,x))$ (inhabitant: u) and $z \in S$, in order to obtain $\forall_{y \in S}(Q(z,y) \Rightarrow \neg Q(y,z))$.

6.6 (a) The smallest system is λC itself, since, for example:

- $\bot$ needs $(\Box, *)$,
- $\lambda x : S \,.\, (P\,x \to \bot)$ needs $(*, \Box)$, and
- $\lambda P : S \to * \,.\, \lambda x : S \,.\, (P\,x \to \bot)$ needs $(\Box, \Box)$.

6.6 (b)

$$\boxed{S : *}$$
$$\quad \boxed{P : S \to *}$$
$$\quad\quad \boxed{x : S}$$
$$\quad\quad\quad P\,x : *$$
$$\quad\quad\quad \bot : *$$
$$\quad\quad\quad P\,x \to \bot \;:\; *$$
$$\quad\quad \lambda x : S \,.\, (P\,x \to \bot) \;:\; S \to *$$
$$\quad \lambda P : S \to * \,.\, \lambda x : S \,.\, (P\,x \to \bot) \;:\; (S \to *) \to S \to *$$
$$\lambda S : * \,.\, \lambda P : S \to * \,.\, \lambda x : S \,.\, (P\,x \to \bot) \;:\; S \to (S \to *) \to S \to *$$

6.6 (c) M can be interpreted as the function that maps a set S and a predicate P on S to the 'complement' of P, that is: the predicate that is only true for x in S if P does *not* hold for x.

6.8 (a)

$$\boxed{S : *}$$
$$\quad \boxed{P : S \to *}$$
$$\quad\quad \boxed{u \;:\; \Pi\alpha : * \,.\, ((\Pi x : S \,.\, (P\,x \to \alpha)) \to \alpha)}$$
$$\quad\quad\quad \boxed{v \;:\; \Pi x : S \,.\, (P\,x \to \bot)}$$
$$\quad\quad\quad u\,\bot \;:\; ((\Pi x : S \,.\, (P\,x \to \bot)) \to \bot)$$
$$\quad\quad\quad u\,\bot\,v : \bot$$
$$\quad\quad \lambda v : (\Pi x : S \,.\, (P\,x \to \bot)) \,.\, u\,\bot\,v \;:\; (\Pi x : S \,.\, (P\,x \to \bot)) \to \bot$$
$$\quad\quad \lambda u : \Pi\alpha : * \,.\, ((\Pi x : S \,.\, (P\,x \to \alpha)) \to \alpha) \,.$$
$$\quad\quad\quad \lambda v : (\Pi x : S \,.\, (P\,x \to \bot)) \,.\, u\,\bot\,v \;:$$
$$\quad\quad\quad\quad (\Pi\alpha : * \,.\, ((\Pi x : S \,.\, (P\,x \to \alpha)) \to \alpha)) \;\to$$
$$\quad\quad\quad\quad\quad (\Pi x : S \,.\, (P\,x \to \bot)) \to \bot$$

6.8 (b) System λ2.

6.8 (c) N can be interpreted as the logical proposition:
$\exists_{x \in S}(P(x)) \Rightarrow \neg\forall_{x \in S}(\neg P(x))$.

Chapter 7

7.1 (d) Proof in natural deduction:

$\boxed{\neg(A \Rightarrow B)}$

- $\boxed{B}$
  - $\boxed{A}$
    - B $\quad$ (*repeat*)
  - $A \Rightarrow B$ $\quad$ ($\Rightarrow$–*intro*)
  - $\bot$ $\quad$ ($\neg$–*elim*)
- $\neg B$ $\quad$ ($\neg$–*intro*)

$\neg(A \Rightarrow B) \Rightarrow \neg B$ $\quad$ ($\Rightarrow$–*intro*)

A corresponding derivation is the following (for the 'condensed' first flag, see Notation 11.5.1):

$\boxed{A, B : *}$

- $\boxed{x : \neg(A \to B)}$
  - $\boxed{y : B}$
    - $\boxed{z : A}$ $\quad$ *(see Exercise 7.1 (a) for this flag and the next two lines)*
      - $y : B$ $\quad$ (*weak*)
    - $\lambda z : A \,.\, y \;:\; A \to B$ $\quad$ (*abst*)
    - $x(\lambda z : A \,.\, y) \;:\; \bot$ $\quad$ (*appl*)
  - $\lambda y : B \,.\, x(\lambda z : A \,.\, y) \;:\; \neg B$ $\quad$ (*abst*)
- $\lambda x : \neg(A \to B) \,.\, \lambda y : B \,.\, x(\lambda z : A \,.\, y) \;:\; \neg(A \to B) \to \neg B$ $\quad$ (*abst*)

7.2 (a)

$\boxed{\iota_{DN} \;:\; \Pi\beta : * \,.\, \neg\neg\beta \to \beta}$

7.4 (a)

$A, B : *$

$x \,:\, \Pi C : * \,.\, (A \to B \to C) \to C \quad (\equiv A \wedge B)$

$x\,A \,:\, (A \to B \to A) \to A$

$\lambda u : A \,.\, \lambda v : B \,.\, u \,:\, A \to B \to A \quad (cf.\ Exercise\ 7.1\ (a))$

$x\,A(\lambda u : A \,.\, \lambda v : B \,.\, u) \,:\, A$

7.5 (a)

$\iota_{DN} \,:\, \Pi\beta : * \,.\, \neg\neg\beta \to \beta$

$A, B : *$

$x : \neg(A \to B)$

$y : \neg A$

$\lambda u : \neg A \,.\, \lambda v : A \,.\, u\,v\,B \,:\, \neg A \to (A \to B)$

$(see\ Exercise\ 7.1\ (b))$

$(\lambda u : \neg A \,.\, \lambda v : A \,.\, u\,v\,B)y \,:\, A \to B \quad (appl)$

$\lambda v : A \,.\, y\,v\,B \,:\, A \to B \quad (Subject\ Reduction)$

$x(\lambda v : A \,.\, y\,v\,B) \,:\, \bot \quad (appl)$

$\lambda y : \neg A \,.\, x(\lambda v : A \,.\, y\,v\,B) \,:\, \neg\neg A \quad (abst)$

$\iota_{DN}\,A \,:\, \neg\neg A \to A \quad (appl)$

$\iota_{DN}\,A(\lambda y : \neg A \,.\, x(\lambda v : A \,.\, y\,v\,B)) \,:\, A \quad (appl) \quad (*)$

$\lambda x : \neg(A \to B) \,.\, \ldots \,:\, \neg(A \to B) \to A \quad (abst)$

7.5 (b)

$x : \neg(A \to B)$

$\lambda y : B \,.\, x(\lambda z : A \,.\, y) \,:\, \neg B \quad (see\ Exercise\ 7.1\ (d))$

$\lambda C : * \,.\, \lambda z : A \to \neg B \to C \,.$

$z(\iota_{DN}\,A(\lambda y : \neg A \,.\, x(\lambda v : A \,.\, y\,v\,B)))(\lambda y : B \,.\, x(\lambda z : A \,.\, y))$

$(see\ (*)\ in\ the\ solution\ to\ Exercise\ 7.5\ (a);$

$see\ also\ line\ (4)\ in\ the\ derivation\ in\ Section\ 7.2) \,:$

$\Pi C : * \,.\, (A \to \neg B \to C) \to C \quad (\equiv A \wedge \neg B)$

$\lambda x : \neg(A \to B) \, . \, \ldots \; : \; \neg(A \to B) \to (A \wedge \neg B) \quad (abst)$

7.11 (a)

$S : *$

$P, Q : S \to *$

$y \; : \; \Pi \alpha : * \, . \, ((\Pi x : S \, . \, (P\,x \to \alpha)) \to \alpha)$

$z \; : \; \Pi x : S \, . \, (P\,x \to Q\,x)$

$x : S$

$y (Q\,x) \;\; : \;\; (\Pi \mathbf{y} : S \, . \, (P\,\mathbf{y} \to Q\,x)) \to Q\,x$

Note: there is a 'new' x involved in $y(Q\,x)$ (the one in the last flag). Hence, for the calculation of its type, the binding variable x in $\Pi x : S \, . \, (P\,x \to \alpha)$ must be renamed, in order to avoid a 'variable clash'.

7.11 (b)

Incorrect, because z is not of type $(\Pi \mathbf{y} : S \, . \, (P\,\mathbf{y} \to Q\,x)) \to Q\,x$.

7.12 (b)

In Exercise 7.12 (a) we show that, when $P\,a$ is inhabited for some a in S, then we can derive $\exists x : S \, . \, P\,x$. In the derivation below we use a variant: since $\neg(P\,y)$ is inhabited (see the fifth flag), we can derive, similarly to Exercise 7.12 (a), that $\exists x : S \, . \, \neg(P\,x)$, which is
$\Pi \alpha : * \, . \, ((\Pi x : S \, . \, (\neg(P\,x) \to \alpha)) \to \alpha)$.
See (*) in the derivation below.

$S : *$

$P : S \to *$

$u : \neg \, \Pi \alpha : * \, . \, ((\Pi x : S \, . \, (\neg(P\,x) \to \alpha)) \to \alpha \quad [\equiv \neg \exists x : S \, . \, \neg(P\,x)\,]$

$y : S$

$v : \neg(P\,y)$

$\alpha : *$

$w \; : \; \Pi x : S \, . \, (\neg(P\,x) \to \alpha)$

$w\,y \; : \; \neg(P\,y) \to \alpha$

$w\,y\,v \; : \; \alpha$

$\lambda w : (\Pi x : S \, . \, (\neg P(\,x) \to \alpha)) \, . \, w\,y\,v \;\; :$

$$\begin{array}{l}
(\Pi x : S \,.\, (\neg(P\,x) \to \alpha)) \to \alpha \\
\lambda\alpha : *\,.\, \lambda w : (\Pi x : S\,.\, (\neg P(\,x) \to \alpha))\,.\, w\,y\,v \;: \\
\quad \Pi\alpha : *\,.\, ((\Pi x : S\,.\, (\neg(P\,x) \to \alpha)) \to \alpha) \\
\quad\quad [\equiv \exists x : S\,.\, \neg(P\,x)] \quad (^*) \\
u(\lambda\alpha : *\,.\, \ldots) \;:\; \bot \\
\lambda v : \neg(P\,y)\,.\, u(\lambda\alpha : *\,.\, \ldots) \;:\; \neg\neg(P\,y)) \\
\iota_{DN}(P\,y)(\lambda v : \neg(P\,y)\,.\, u(\lambda\alpha : *\,.\, \ldots)) \;:\; P\,y \\
\lambda y : S\,.\, \iota_{DN}\ldots \;:\; \Pi y : S\,.\, P\,y \quad [\equiv \forall y : S\,.\, P\,y] \\
\lambda u : (\neg\exists x : S\,.\, \neg P\,x)\,.\, \lambda y : S\,.\, \iota_{DN}\ldots \;: \\
\quad \neg\exists x : S\,.\, \neg(P\,x) \to \forall y : S\,.\, P\,y
\end{array}$$

7.14 (a)

$w \;:\; P\,y \wedge Q\,y \; [\equiv\; \Pi C : *\,.\, (P\,y \to Q\,y \to C) \to C]$

$P\,y : *$, so

$w(P\,y) \;:\; (P\,y \to Q\,y \to P\,y) \to P\,y$

$\lambda s : P\,y\,.\, \lambda t : Q\,y\,.\, s \;:\; P\,y \to Q\,y \to P\,y$, so

$w(P\,y)(\lambda s : P\,y\,.\, \lambda t : Q\,y\,.\, s) \;:\; P\,y$

$v : (\Pi x : S\,.\, (P\,x \to \alpha))$

$y : S$, so

$v\,y : P\,y \to \alpha$, and

$v\,y(w(P\,y)(\lambda s : P\,y\,.\, \ldots)) \;:\; \alpha$

$\lambda w : (P\,y \wedge Q\,y)\,.\, v\,y(w(P\,y)(\lambda s : P\,y\,.\, \ldots)) \;:\; (P\,y \wedge Q\,y) \to \alpha$

$\lambda y : S\,.\, \lambda w : (P\,y \wedge Q\,y)\,.\, v\,y(w(P\,y)(\lambda s : P\,y\,.\, \ldots)) \;:$
$\quad \Pi y : S\,.\, ((P\,y \wedge Q\,y) \to \alpha)$

$u : \exists x : S\,.\, (P\,x \wedge Q\,x) \; [\equiv\; \Pi\alpha : *((\Pi x : S\,.\, ((P\,x \wedge Q\,x) \to \alpha)) \to \alpha)]$

$\alpha : *$, so

$u\,\alpha \;:\; (\Pi x : S\,.\, ((P\,x \wedge Q\,x) \to \alpha)) \to \alpha$, and

$u\,\alpha(\lambda y : S\,.\, \ldots) \;:\; \alpha$

$\lambda v : (\Pi x : S\,.\, (P\,x \to \alpha))\,.\, u\,\alpha(\lambda y : S\,.\, \ldots) \;:\; (\Pi x : S\,.\, (P\,x \to \alpha)) \to \alpha$

$\lambda\alpha : *\,.\, \lambda v : (\Pi x : S\,.\, (P\,x \to \alpha))\,.\, u\,\alpha(\lambda y : S\,.\, \ldots) \;:$
$\quad \Pi\alpha : *\,.\, ((\Pi x : S\,.\, (P\,x \to \alpha)) \to \alpha) \; [\equiv\; \exists x : S\,.\, P\,x]$

$\lambda u : (\exists x : S\,.\, (P\,x \wedge Q\,x))\,.\, \lambda\alpha : *\,.\, \lambda v : \ldots \;:$
$\quad (\exists x : S\,.\, (P\,x \wedge Q\,x)) \to \exists x : S\,.\, P\,x$

7.14 (b) $\exists_{x \in S}(P(x) \wedge Q(x)) \Rightarrow \exists_{x \in S}(P(x))$

Chapter 8

8.1 $m : \mathbb{N}^+,\ n : \mathbb{N}^+,\ u : coprime(m,n) \rhd$

$p(m,n,u) := \texttt{formalproof} \ : \ \exists x, y : \mathbb{Z}\,.\ (m\,x + n\,y = 1)$

$m : \mathbb{N}^+,\ n : \mathbb{N}^+ \rhd$

$q(m,n) := \texttt{formalproof}_1 \ : \ coprime(m,n) \Rightarrow coprime(n,m)$

Then: $m : \mathbb{N}^+,\ n : \mathbb{N}^+,\ u : coprime(m,n) \rhd$

$r(m,n,u) := p(n,m,q(m,n)u) \ : \ \exists x, y : \mathbb{Z}\,.\ (n\,x + m\,y = 1)$

8.4 (a) Let S be a set and $\cdot$ a binary operation on S. We call $(S,\cdot)$ a *semigroup* if for all $x, y, z \in S$: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Let $(S,\cdot)$ be a semigroup. An element e in S is called a *unit* of $(S,\cdot)$ if, for all $x \in S$, $x \cdot e = e \cdot x = x$.

If both e_1 and e_2 are units of $(S,\cdot)$, then $e_1 = e_2$.

8.6 (a)

$k, l, m : \mathbb{Z}$

$\quad u : m > 0$

(1) $\quad congruent\text{-}modulo(k,l,m,u) \ := \ m \mid k - l \ : \ *_p$

(2) $\quad eqv(k, l.m.u) \ := \ congruent\text{-}modulo(k,l,m,u) \ : \ *_p$

(3) $v \ := \ \texttt{formalproof}_3 \ : \ 5 > 0$

(4) $a_4 \ := \ \texttt{formalproof}_4 \ : \ eqv(-3, 17, 5, v)$

(5) $a_5 \ := \ \texttt{formalproof}_5 \ : \ \neg eqv(-3, -17, 5, v)$

$k, l, m : \mathbb{Z}$

$\quad u : m > 0$

(6) $\quad a_6(k,l,m,u) \ := \ \texttt{formalproof}_6 \ : \ eqv(k,l,m,u) \Rightarrow eqv(l,k,m,u)$

(7) $\quad a_7(k,l,m,u) \ := \ \texttt{formalproof}_7 \ :$

$\qquad eqv(k,l,m,u) \Rightarrow \exists n : \mathbb{Z}\,.\ (k = l + n\,m)$

8.6 (c) Line (2), (k,l,m,u) in $congruent\text{-}modulo(k,l,m,u)$. Identity instantiation.

Line (4), $(-3, 17, 5, v)$. Type conditions: $-3 : \mathbb{Z}$, $17 : \mathbb{Z}$, $5 : \mathbb{Z}$, $v : 5 > 0$.

Line (5), $(-3, -17, 5, v)$. Type conditions: $-3 : \mathbb{Z}$, $-17 : \mathbb{Z}$, $5 : \mathbb{Z}$, $v : 5 > 0$.

Line (6), (k,l,m,u) in $eqv(k,l,m,u)$. Identity instantiation.

Line (6), (l,k,m,u) in $eqv(l,k,m,u)$. Type conditions: $l : \mathbb{Z}$, $k : \mathbb{Z}$, m : $\mathbb{Z}$, u : $m > 0$.

Line (7), (k,l,m,u) in $eqv(k,l,m,u)$. Identity instantiation.

Chapter 9

9.3 $\forall x : \mathbb{R} . [x \in \{z : \mathbb{R} \mid \exists n : \mathbb{R} . (n \in \mathbb{N} \wedge z = \frac{n}{n+1})\} \Rightarrow x \leq 1] \wedge$
$\forall x : \mathbb{R} . [x < 1 \Rightarrow$
$\neg \forall y : \mathbb{R} . (y \in \{z : \mathbb{R} \mid \exists n : \mathbb{R} . (n \in \mathbb{N} \wedge z = \frac{n}{n+1})\} \Rightarrow y \leq x)]$

9.5 We only treat the expression *least-upper-bound*$(S, p_6, 1)$ in line (8), with instantiated list $(S, p_6, 1)$ instead of the original list (V, u, s).

(1) $V \to S$. We have $V : *_s$ and $S : *_s$, so ✓.

(2) $u \to p_6$. Now $u : V \subseteq \mathbb{R}$, so we must have $p_6 : (V \subseteq \mathbb{R})[V := S] \equiv S \subseteq \mathbb{R}$, ✓.

(3) $s \to 1$. Now $s : \mathbb{R}$, so we must have $1 : \mathbb{R}[V := S, u := p_6] \equiv \mathbb{R}$, ✓.

9.6 (b) Arithmetic progression.

9.6 (c) $\Sigma_{i=0}^{100}((\lambda x : \mathbb{N} . 2x)i) = (100+1) \cdot (\lambda x : \mathbb{N} . 2x)0 + \frac{1}{2} \cdot 100 \cdot (100+1) \cdot 2$
(In 'words': $0 + 2 + \ldots + 200 = 101 \cdot 0 + \frac{1}{2} \cdot 100 \cdot 101 \cdot 2$, so $= 10100$.)

9.7 (b) $\mathcal{D}_1, \mathcal{D}_2 ; \emptyset \vdash * : \square$?

Conditions according to (*def*):

– $\mathcal{D}_1 ; \emptyset \vdash * : \square$ (see Exercise 9.7 (a)).
– $\mathcal{D}_1 ; f : \mathbb{N} \to \mathbb{R}, d : \mathbb{R} \vdash \forall n : \mathbb{N} . (f(n+1) - f\,n = d) : *_p$

9.10 (a) The final judgement $\mathcal{J}_n \equiv \Delta_n ; \Gamma_n \vdash M_n : N_n$ has been derived by means of (*weak*), so the last step was:

$$\frac{\Delta_n ; \Gamma'_n \vdash M_n : N_n \qquad \Delta_n ; \Gamma'_n \vdash C : s}{\Delta_n ; \Gamma_n \vdash M_n : N_n} ,$$

with $\Gamma_n \equiv \Gamma'_n, x : C$.

By the assumption, since $\Delta_n ; \Gamma'_n \vdash M_n : N_n$ has been derived earlier than $\mathcal{J}_n$, we have $\Delta_n ; \Gamma'_n \vdash * : \square$. Then (*weak*), again, gives:

$$\frac{\Delta_n ; \Gamma'_n \vdash * : \square \qquad \Delta_n ; \Gamma'_n \vdash C : s}{\Delta_n ; \Gamma'_n, x : C \vdash * : \square}$$

Hence, $\Delta_n ; \Gamma_n \vdash * : \square$.

Chapter 10

10.2 (a)

If we define $A, B : *_p \rhd k(A, B) := \perp\!\!\!\perp : (A \Rightarrow B) \Rightarrow A$, then
$k(\perp, \perp) : (\perp \Rightarrow \perp) \Rightarrow \perp$. We have: $\lambda x : \perp . x : \perp \Rightarrow \perp$, hence
$k(\perp, \perp)(\lambda x : \perp . x) : \perp$.

So $\perp$ is inhabited, otherwise said: a contradiction is derived.

10.2 (c) Suppose we define:

$P : \mathbb{N} \to *_p \rhd \mathit{ind\text{-}s}(P) \ := \ \forall n : \mathbb{N} \, . \, (P\,n \Rightarrow P(s\,n)) \Rightarrow \forall n : \mathbb{N} \, . \, P\,n \, .$

Now define the predicate $P_\perp$ by $\emptyset \ \rhd \ P_\perp \ := \ \lambda n : \mathbb{N} \, . \, \perp$. Then:

$\mathit{ind\text{-}s}(P_\perp) =_\delta \forall n : \mathbb{N} \, . \, (P_\perp\,n \Rightarrow P_\perp(s\,n)) \Rightarrow \forall n : \mathbb{N} \, . \, P_\perp\,n$

$=_\beta \forall n : \mathbb{N} \, . \, (\perp \Rightarrow \perp) \Rightarrow \forall n : \mathbb{N} \, . \, \perp.$

It is easy to see that $\lambda n : \mathbb{N} \, . \, \lambda u : \perp . \, u \ : \ \forall n : \mathbb{N} \, . \, (\perp \Rightarrow \perp)$, so:

$\mathit{ind\text{-}s}(P_\perp)(\lambda n : \mathbb{N} \, . \, \lambda u : \perp . \, u) \ : \ \forall n : \mathbb{N} \, . \, \perp \, .$

Since $0 : \mathbb{N}$, it follows that $\mathit{ind\text{-}s}(P_\perp)(\lambda n : \mathbb{N} \, . \, \lambda u : \perp . \, u)\, 0 \ : \ \perp \, .$

10.4 $\Delta \, ; \Gamma$ is a legal combination, so there are M, N such that $\Delta \, ; \Gamma \ \vdash \ M : N$.
To prove: $\Delta \, ; \Gamma \ \vdash \ * : \Box$.

We use induction on the structure of the derivation of $\Delta \, ; \Gamma \ \vdash \ M : N$. We only treat here three of the eleven cases, namely: the last step in the derivation was (*var*), (*weak*) or (*def*).

(*var*) Then $\Delta \, ; \Gamma \ \vdash \ M : N \ \equiv \ \Delta \, ; \Gamma', \, x : A \ \vdash \ x : A$, as a `conclusion` from `premiss` $\Delta \, ; \Gamma' \ \vdash \ A : s$.
By induction, the `premiss` gives us: $\Delta \, ; \Gamma' \ \vdash \ * : \Box$.
Then we can derive with (*weak*):

$$\frac{\Delta \ ; \ \Gamma' \ \vdash \ * : \Box \qquad \Delta \, ; \Gamma' \ \vdash \ A : s}{\Delta \ ; \ \Gamma', \, x : A \ \vdash \ * : \Box},$$

where the derived judgement is identical to $\Delta \ ; \ \Gamma \ \vdash \ * : \Box$.

(*weak*) Then $\Delta \, ; \Gamma \ \vdash \ M : N \ \equiv \ \Delta \, ; \Gamma', \, x : C \ \vdash \ A : B$, as a `conclusion` from `premisses` $\Delta \, ; \Gamma' \ \vdash \ A : B$ and $\Delta \, ; \Gamma' \ \vdash \ C : s$.
By induction, either of the `premisses` gives us: $\Delta \, ; \Gamma' \ \vdash \ * : \Box$.
Then we can derive with (*weak*):

$$\frac{\Delta \ ; \ \Gamma' \ \vdash \ * : \Box \qquad \Delta \, ; \Gamma' \ \vdash \ C : s}{\Delta \ ; \ \Gamma', \, x : C \ \vdash \ * : \Box},$$

where the derived judgement is identical to $\Delta \ ; \ \Gamma \ \vdash \ * : \Box$.

(*def*) Then $\Delta, \, \Gamma \ \vdash \ M : N \ \equiv \ \Delta', \, \overline{x} : \overline{A} \rhd a(\overline{x}) \ := \ M' : N' \ ; \ \Gamma \ \vdash \ K : L$, as a `conclusion` from `premisses` $\Delta' \, ; \Gamma \ \vdash \ K : L$ and $\Delta' \, ; \overline{x} : \overline{A} \ \vdash \ M' : N'$.
By induction, the first `premiss` gives us: $\Delta' \, ; \Gamma \ \vdash \ * : \Box$.
Then we can derive with (*def*):

$$\frac{\Delta' \ ; \ \Gamma \ \vdash \ * : \Box \qquad \Delta' \, ; \overline{x} : \overline{A} \ \vdash \ M' : N'}{\Delta', \, \overline{x} : \overline{A} \ \rhd \ a(\overline{x}) \ := \ M' : N' \ ; \ \Gamma \ \vdash \ * : \Box},$$

where the derived judgement is identical to $\Delta \ ; \ \Gamma \ \vdash \ * : \Box$.

10.5 Let $\Delta\,;\Gamma$ be a legal combination, where $x : A \in \Gamma$.
Then there are Γ_1 and Γ_2 such that $\Gamma \equiv \Gamma_1,\, x : A,\, \Gamma_2$, and there are M and N such that $\Delta : \Gamma \;\vdash\; M : N$, i.e., $\Delta\,; \Gamma_1,\, x : A,\, \Gamma_2 \;\vdash\; M : N$.

To prove: $\Delta\,; \Gamma_1,\, x : A,\, \Gamma_2 \;\vdash\; x : A$.

We proceed by induction on the structure of the derivation of $\Delta\,;\Gamma \vdash M : N$. See Figures 9.3 and 10.1.

First note that $\Delta;\Gamma$ does not change in the transition from (at least) one of the `premisses` to the `conclusion` of the derivation rules (*form*), (*appl*), (*abst*), (*conv*), (*inst*) and (*inst-prim*). This implies that in all these cases, induction immediately leads to the desired result.

Secondly, the case (*sort*) also gives the desired result, because the condition is not satisfied (since we suppose that $x : A \in \Gamma$).

What remains, are the four cases (*var*), (*weak*), (*def*) and (*def-prim*). For the first two of these cases, we distinguish between::
subcase a: $x : A$ is the final assumption in Γ, i.e., $\Gamma_2 \equiv \emptyset$,
subcase b: $x : A$ is *not* the final assumption, i.e., $\Gamma_2 \not\equiv \emptyset$.

Case 1: (*var*).

Subcase 1 a: $\Gamma_2 \equiv \emptyset$. Then for $\Delta\,;\Gamma \;\vdash\; M : N$ we have the `conclusion` $\Delta\,; \Gamma_1,\, x : A \;\vdash\; x : A$, so we are ready.

Subcase 1 b: $\Gamma_2 \not\equiv \emptyset$. Then for $\Delta\,;\Gamma \;\vdash\; M : N$ we have the `conclusion` $\Delta\,; \Gamma_1,\, x : A,\, \Gamma',\, y : B \;\vdash\; y : B$. The `premiss` is $\Delta\,; \Gamma_1,\, x : A,\, \Gamma' \;\vdash\; B : s$ $(*)$. By induction on $(*)$: $\Delta\,; \Gamma_1,\, x : A,\, \Gamma' \;\vdash\; x : A$ $(**)$. By (*weak*) on $(**)$ and $(*)$, we obtain: $\Delta\,; \Gamma_1,\, x : A,\, \Gamma',\, y : B \;\vdash\; x : A$, so we are ready.

Case 2: (*weak*).

Subcase 2 a: $\Gamma_2 \equiv \emptyset$. Then for $\Delta\,;\Gamma \;\vdash\; M : N$ we have the `conclusion` $\Delta\,; \Gamma_1,\, x : A \;\vdash\; B : C$. So `premiss`$_1$ is $\Delta\,; \Gamma_1 \;\vdash\; B : C$ and `premiss`$_2$ is $\Delta\,; \Gamma_1 \;\vdash\; A : s$ $(*)$. By (*var*) on $(*)$ we have $\Delta\,; \Gamma_1,\, x : A \;\vdash\; x : A$

Subcase 2 b: $\Gamma_2 \not\equiv \emptyset$. Then for $\Delta\,;\Gamma \;\vdash\; M : N$ we have the `conclusion` $\Delta\,; \Gamma_1,\, x : A,\, \Gamma',\, y : C \;\vdash\; D : E$. So `premiss`$_1$ is $\Delta\,; \Gamma_1,\, x : A,\, \Gamma' \;\vdash\; D : E$ and `premiss`$_2$ is $\Delta\,; \Gamma_1,\, x : A,\, \Gamma' \;\vdash\; C : s$ $(*)$.
By induction on either of the `premisses`: $\Delta\,; \Gamma_1,\, x : A,\, \Gamma' \;\vdash\; x : A$ $(**)$. By (*weak*) on $(**)$ and $(*)$ we obtain: $\Delta\,; \Gamma_1,\, x : A,\, \Gamma',\, y : C \;\vdash\; x : A$.

Case 3: (*def*).

Then for $\Delta\,;\Gamma \;\vdash\; M : N$ we have the `conclusion` $\Delta_1,\, d\,;\Gamma \;\vdash\; M : N$, where $d \equiv \overline{x} : \overline{A} \,\rhd\, a(\overline{x}) := S : T$. Now `premiss`$_1$ is $\Delta_1\,;\Gamma \;\vdash\; M : N$ $(*)$ and `premiss`$_2$ is $\Delta_1\,; \overline{x} : \overline{A} \;\vdash\; T : s$ $(**)$.
By induction on $(*)$: $\Delta_1\,;\Gamma \;\vdash\; x : A$ $(***)$. By (*def*) on $(***)$ and $(**)$ we obtain: $\Delta_1,\, d\,;\Gamma \;\vdash\; x : A$.

Case 4: (*def-prim*). Similar to case 3.

Chapter 11

11.3

(1) $\emptyset\,;\emptyset\ \vdash\ *:\square$ $\quad$ (*sort*)
(2) $\emptyset\,;S:*\ \vdash\ *:\square$ $\quad$ (*weak*) on (1) and (1)
(3) $\emptyset\,;S:*\ \vdash\ S:*$ $\quad$ (*var*) on (1)
(4) $\emptyset\,;S:*,\,x:S\ \vdash\ *:\square$ $\quad$ (*weak*) on (2) and (3)
(5) $\emptyset\,;S:*\ \vdash\ \Pi x:S\,.\,*\ (\equiv S\to *)\ :\ \square$ $\quad$ (*form*) on (3) and (4)
(6) $\emptyset\,;S:*,\,P\,:\,S\to *\ \vdash\ S:*$ $\quad$ (*weak*) on (3) and (5)
(7) $\emptyset\,;S:*,\,P\,:\,S\to *\ \vdash\ P\,:\,S\to *$ $\quad$ (*var*) on (5)
(8) $\emptyset\,;S:*,\,P\,:\,S\to *,\,x:S\ \vdash\ P\,:\,S\to *$ $\quad$ (*weak*) on (7) and (6)
(9) $\emptyset\,;S:*,\,P\,:\,S\to *,\,x:S\ \vdash\ x:S$ $\quad$ (*var*) on (6)
(10) $\emptyset\,;S:*,\,P\,:\,S\to *,\,x:S\ \vdash\ P\,x:*$ $\quad$ (*appl*) on (8) and (9)
(11) $\emptyset\,;S:*,\,P\,:\,S\to *\ \vdash\ \Pi x:S\,.\,P\,x\ :\ *$ $\quad$ (*form*) on (6) and (10)
(12) $\mathcal{D}_4\,;S:*,\,P\,:\,S\to *\ \vdash\ \forall(S,P)\ :\ *$ $\quad$ (*par*) on (11),
with $\mathcal{D}_4\ \equiv\ \Gamma\ \rhd\ \forall(S,P)\ :=\ \Pi x:S\,.\,P\,x\ :\ *$

11.6 (a)

Let $\Delta\ \equiv\ \mathcal{D}',\,\mathcal{D}''$.

(1) $\Delta\,;\emptyset\ \vdash\ *:\square$ $\quad$ (*assumption*)
(2) $\Delta\,;\alpha:*\ \vdash\ \alpha:*$ $\quad$ (*var*) on (1)
(3) $\Delta\,;\alpha:*\ \vdash\ \neg(\alpha):*$ $\quad$ (*inst*) on (2) and definition of $\neg$
(4) $\Delta\,;\alpha:*\ \vdash\ \vee(\alpha,\neg(\alpha)):*$ $\quad$ (*inst*) on (1), (2) and definition of $\vee$
(5) $\Delta\,;\emptyset\ \vdash\ \Pi\alpha:*\,.\ \vee(\alpha,\neg(\alpha))\ :\ *$ $\quad$ (*form*) on (1) and (4)

11.6 (b)

(6) $\Delta,\,i_{ET}\ :=\ \perp\!\!\!\perp\ :\ \Pi\alpha:*\,.\ \vee(\alpha,\neg(\alpha))\ ;\ \emptyset\ \vdash\ *:\square$ $\quad$ (*def-prim*) on (1) and (5)

11.9 (c)

For the derivation using the type-theoretic style, see below.

In the natural deduction style, the proof objects for a_2, a_3, a_5 and a_6 in the derivation should read:

$a_2(S,P,u,y,v)\ :=\ \neg\text{-}el(\exists x:S\,.\,\neg(P\,x),u,a_1(S,P,u,y,v))$

$a_3(S,P,u,y)\ :=\ \neg\text{-}in(\neg(P\,y),\lambda v:\neg(P\,y)\,.\,a_2(S,P,u,y,v))$

$a_5(S,P,u)\ :=\ \forall\text{-}in(S,P,\lambda y:S\,.\,a_4(S,P,u,y))$

$a_6(S,P)\ :=\ \Rightarrow\text{-}in(\neg\exists x:S\,.\,\neg(P\,x),\forall y:S\,.\,P\,y,$
$\lambda u:(\neg\exists x:S\,.\,\neg(P\,x))\,.\,a_5(S,P,u))$

$$\boxed{S : * \mid P : S \to *}$$

$$\boxed{u : \neg\exists x : S \,.\, \neg(P\,x)}$$

$$\boxed{y : S}$$

$$\boxed{v : \neg(P\,y)}$$

$$a_1(S, P, u, y, v) \;:=\; \exists\text{-}in(S, \lambda z : S \,.\, \neg(P\,z), y, v) \;:\; \exists y : S \,.\, \neg(P\,y)$$

$$a_2(S, P, u, y, v) \;:=\; u\,a_1(S, P, u, y, v) \;:\; \bot$$

$$a_3(S, P, u, y) \;:\; \lambda v : \neg(P\,y) \,.\, a_2(S, P, u, y, v) \;:\; \neg\neg(P\,y)$$

$$a_4(S, P, u, y) \;:=\; \neg\neg\text{-}el(P\,y, a_3(S, P, u, y)) \;:\; P\,y$$

$$a_5(S, P, u) \;:=\; \lambda y : S \,.\, a_4(S, P, u, y) \;:\; \forall y : S \,.\, P\,y$$

$$a_6(S, P) \;:=\; \lambda u : (\neg\exists x : S \,.\, \neg(P\,x)) \,.\, a_5(S, P, u) \;:$$
$$\neg\exists x : S \,.\, \neg(P\,x) \Rightarrow \forall y : S \,.\, P\,y$$

11.10

$$\boxed{A, B : *_p}$$

$$\boxed{u \;:\; (A \Rightarrow B) \Rightarrow A}$$

$$\boxed{v : \neg A}$$

$$\boxed{w : A}$$

$$a_1(A, B, u, v, w) \;:=\; v\,w \;:\; \bot$$

$$a_2(A, B, u, v, w) \;:=\; a_1(A, B, u, v, w)\,B \;:\; B$$

$$a_3(A, B, u, v) \;:=\; \lambda w : A \,.\, a_2(A, B, u, v, w) \;:\; A \Rightarrow B$$

$$a_4(A, B, u, v) \;:=\; u\,a_3(A, B, u, v) \;:\; A$$

$$a_5(A, B, u, v) \;:=\; v\,a_4(A, B, u, v) \;:\; \bot$$

$$a_6(A, B, u) \;:=\; \lambda v : \neg A \,.\, a_5(A, B, u, v) \;:\; \neg\neg A$$

$$a_7(A, B, u) \;:=\; \neg\neg\text{-}el(A, a_6(A, B, u)) \;:\; A$$

$$a_8(A, B) \;:=\; \lambda v : \neg A \,.\, a_7(A, B, u) \;:\; ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$$

11.13 (b)

$$DN \;:=\; \Pi A:*\,.\,(\neg\neg A \Rightarrow A) \;:\; *_p$$

$$ET \;:=\; \Pi A:*\,.\,(A \vee \neg A) \;:\; *_p$$

$$
\begin{array}{l}
\boxed{d : DN} \\
\quad \boxed{A : *} \\
\quad\quad \boxed{C : *} \\
\quad\quad\quad \boxed{u \;:\; A \Rightarrow C} \\
\quad\quad\quad\quad \boxed{v \;:\; \neg A \Rightarrow C} \\
\quad\quad\quad\quad\quad \boxed{w : \neg C} \\
\quad\quad\quad\quad\quad\quad \boxed{z : A} \\
\quad\quad\quad\quad\quad\quad\quad a_1(d,A,C,u,v,w,z) \;:=\; u\,z \;:\; C \\
\quad\quad\quad\quad\quad\quad\quad a_2(\ldots) \;:=\; w\,a_1(\ldots) \;:\; \bot \\
\quad\quad\quad\quad\quad\quad a_3(d,A,C,u,v,w) \;:=\; \lambda z : A\,.\,a_2(\ldots) \;:\; \neg A \\
\quad\quad\quad\quad\quad\quad a_4(\ldots) \;:=\; v\,a_3(\ldots) \;:\; C \\
\quad\quad\quad\quad\quad\quad a_5(\ldots) \;:=\; w\,a_4(\ldots) \;:\; \bot \\
\quad\quad\quad\quad\quad a_6(d,A,C,u,v) \;:=\; \lambda w : \neg C\,.\,a_5(\ldots) \;:\; \neg\neg C \\
\quad\quad\quad\quad\quad a_7(\ldots) \;:=\; d\,C\,a_6(\ldots) \;:\; C \\
\quad\quad\quad\quad a_8(d,A,C,u) \;:=\; \lambda v : (\neg A \Rightarrow C)\,.\,a_7(\ldots) \;:\; (\neg A \Rightarrow C) \Rightarrow C \\
\quad\quad\quad a_9(d,A,C) \;:=\; \lambda u : (A \Rightarrow C)\,.\,a_8(\ldots) \;: \\
\quad\quad\quad\quad\quad\quad (A \Rightarrow C) \Rightarrow (\neg A \Rightarrow C) \Rightarrow C \\
\quad\quad a_{10}(d,A) \;:=\; \lambda C : *\,.\,a_9(d,A,C) \;: \\
\quad\quad\quad\quad\quad \Pi C : *\,.\,(A \Rightarrow C) \Rightarrow (\neg A \Rightarrow C) \Rightarrow C \quad [=_\delta A \vee \neg A] \\
\quad a_{11}(d) \;:=\; \lambda A : *\,.\,a_{10}(d,A) \;:\; \Pi A : *\,.\,(A \vee \neg A) \quad [=_\delta ET] \\
a_{12} \;:=\; \lambda d : DN\,.\,a_{11}(d) \;:\; DN \Rightarrow ET
\end{array}
$$

11.16

$S : *_s \mid P : S \to *_p$

$u \; : \; \forall x : S \,.\, P\,x$

$v \; : \; \exists y : S \,.\, \neg(P\,y)$

(1) $a_1(S,P,u,v) \;:=\; a_{\ldots[Exercise\ 11.15\,(a)]}(S,P)\,v \;:=\; \neg\forall x : S \,.\, P\,x$

(2) $a_2(S,P,u,v) \;:=\; a_1(S,P,u,v)\,u \;:\; \bot$

(3) $a_3(S,P,u) \;:=\; \lambda v : (\exists y : S \,.\, \neg(P\,y)) \,.\, a_2(S,P,u,v) \;:$
$\neg\exists y : S \,.\, \neg(P\,y)$

(4) $a_4(S,P) \;:=\; \lambda u : (\forall x : S \,.\, P\,x) \,.\, a_3(S,P,u) \;:$
$\forall x : S \,.\, P\,x \Rightarrow \neg\exists y : S \,.\, \neg(P\,y)$

$u \; : \; \neg\exists y : S \,.\, \neg(P\,y)$

$x : S$

(5) $a_5(S,P,u,x) \;:=\; a_{5[Fig.\ 11.26]}(S, \lambda y : S \,.\, \neg(P\,y))\,u \;:$
$\forall y : S \,.\, \neg\neg(P\,y)$

(6) $a_6(S,P,u,x) \;:=\; a_5(S,P,u,x)\,x \;:\; \neg\neg(P\,x)$

(7) $a_7(S,P,u,x) \;:=\; \neg\neg\text{-}el(P\,x, a_6(S,P,u,x)) \;:\; P\,x$

(8) $a_8(S,P,u) \;:=\; \lambda x : S \,.\, a_7(S,P,u,x) \;:\; \forall x : S \,.\, P\,x$

(9) $a_9(S,P) \;:=\; \lambda u : (\neg\exists y : S \,.\, \neg(P\,y)) \,.\, a_8(S,P,u) \;:$
$\neg\exists y : S \,.\, \neg(P\,y) \Rightarrow \forall x : S \,.\, P\,x$

(10) $a_{10}(S,P) \;:=$
$\Leftrightarrow\text{-}in(\forall x : S \,.\, P\,x, \neg\exists y : S \,.\, \neg(P\,y), a_4(S,P), a_9(S,P)) \;:$
$\forall x : S \,.\, P\,x \;\Leftrightarrow\; \neg\exists y : S \,.\, \neg(P\,y)$

Notes:

(i) In line (1) we assume that Exercise 11.15 (a) has been worked out in a derivation, so that we can use its result. (The index of the final line of that derivation should yet be put in.) One can, of course, also construct the proof *here* to derive from $\exists y : S \,.\, \neg(P\,y)$ that $\neg\forall x : S \,.\, P\,x$.

(ii) In line (5) we use the final line of Figure 11.26. This is shorter – and more in line with what we advocate in the book – than to 'duplicate' the proof in the present situation, so with $\lambda y : S \,.\, \neg(P\,y)$ instead of P.

Chapter 12

12.4 (a)

$S : *_s \mid \; \leq : S \to S \to *_p \mid r : part\text{-}ord(S, \leq)$

$< (S, \leq, r) := \lambda m : S \,.\, \lambda n : S \,.\, (m \leq_S n \wedge \neg(m =_S n)) \; : \; S \to S \to *_p$

`Notation :` $x <_S y$ `for` $< (S, \leq, r)\, x\, y$

12.4 (c)

$m, n : S$

$u : m <_S n \wedge n <_S m$

$\ldots : m <_S n$

$\ldots : m \leq_S n$

$\ldots : \neg(m =_S n)$

$\ldots : n <_S m$

$\ldots : n \leq_S m$

$\ldots : antisymm(S, \leq)$

$\ldots : m \leq_S n \Rightarrow n \leq_S m \Rightarrow m =_S n$

$\ldots : n \leq_S m \Rightarrow m =_S n$

$\ldots : m =_S n$

$\ldots : \perp$

$\ldots : \neg(m <_S n \wedge n <_S m)$

$\ldots : \forall m, n : S \,.\, \neg(m <_S n \wedge n <_S m)$

12.4 (d)

$k, l.m : S$

$u : k <_S l$

$v : l <_S m$

$\ldots : k \leq_S l$

$\ldots : l \leq_S m$

$\ldots : k \leq_S m$ *(by transitivity of* $\leq$*)*

$w : k =_S m$

$\ldots : m =_S k$ (*by symmetry of* $=_S$)

$\ldots : l <_S k$ (*by substitutivity in* $l <_S m$)

$\ldots : k <_S l \wedge l <_S k$

$\ldots : \perp$ (*by part* (*c*))

$\ldots : \neg(k =_S m)$

$\ldots : k \leq_S m \wedge \neg(k =_S m)$

$\ldots : k <_S m$

$\ldots : l <_S m \Rightarrow k <_S m$

$\ldots : k <_S l \Rightarrow l <_S m \Rightarrow k <_S m$

$\ldots : \forall k, l, m : S \,.\, (k <_S l \Rightarrow l <_S m \Rightarrow k <_S m)$

12.5 (a) *Complete proof*:

$S : *_s \mid P : S \to *_p \mid n : S$

$u : P\,n \wedge \forall x : S \,.\, (P\,x \Rightarrow (x =_S n))$

$a_1(\ldots) := \wedge\text{-}el_1(P\,n, \forall x : S \,.\, (P\,x \Rightarrow (x =_S n)), u) : P\,n$

$a_2(\ldots) := \wedge\text{-}el_2(P\,n, \forall x : S \,.\, (P\,x \Rightarrow (x =_S n)), u) :$
$\quad \forall x : S \,.\, (P\,x \Rightarrow (x =_S n))$

$a_3(\ldots) := \exists\text{-}in(S, P, n, a_1(\ldots)) : \exists^{\geq 1} x : S \,.\, P\,x$

$y, z : S$

$v : P\,y \mid w : P\,z$

$a_4(\ldots) := a_2(\ldots)\, y\, v : y =_S n$

$a_5(\ldots) := a_2(\ldots)\, z\, w : z =_S n$

$a_6(\ldots) := a_{4[Fig.\ 12.10]}(S)\ z\ n\ a_5(\ldots) : n =_S z$

$a_7(\ldots) := a_{3[Fig.\ 12.13]}(S)\ y\ n\ z\ a_4(\ldots)\ a_6(\ldots) : y =_S z$

$a_8(\ldots) := \lambda y, z : S \,.\, \lambda v : P\,y \,.\, \lambda w : P\,z \,.\, a_7(\ldots) :$
$\quad \forall y, z : S \,.\, (P\,y \Rightarrow P\,z \Rightarrow (y =_S z))$

$a_9(\ldots) := a_8(\ldots) : \exists^{\leq 1} x : S \,.\, P\,x$

$a_{10}(\ldots) := \wedge\text{-}in(\exists^{\geq 1} x : S \,.\, P\,x, \exists^{\leq 1} x : S \,.\, P\,x, a_3(\ldots), a_9(\ldots)) :$
$\quad \exists^1 x : S \,.\, P\,x$

12.5 (b) *Complete proof*:

$$a_{11}(\ldots) \;:=\; a_{5[Fig.\ 12.17]}(S, P, a_{10}(\ldots)) \;:\; \forall z : S\,.\,(P\,z \Rightarrow (z =_S \iota^{a_{10}(\ldots)}_{x:S}(P\,x)))$$

$$a_{12}(\ldots) \;:=\; a_{11}(\ldots)\,n\,a_1(\ldots) \;:\; n =_S \iota^{a_{10}(\ldots)}_{x:S}(P\,x)$$

12.7 (a)

$S : *_s \mid \circ : S \to S \to *_p$

Notation : $x \circ y$ for $\circ\, x\, y$ (on S)

$$associative(S, \circ) \;:=\; \forall x, y, z : S\,.\,((x \circ y) \circ z =_S x \circ (y \circ z)) \;:\; *_p$$

$$monoid(S, \circ) \;:=\; associative(S, \circ) \;:\; *_p$$

$e : S$

$$unit(S, \circ, e) \;:=\; \forall x : S\,.\,(e \circ x =_S x \wedge x \circ e =_S x) \;:\; *_p$$

$u : monoid(S, \circ)$

$e : S \mid v : unit(S, \circ, e)$

12.7 (b)

$e' : S \mid w : unit(S, \circ, e')$

$$a_1(\ldots) \;:=\; unit(S, \circ, e)e' \;:\; e \circ e' =_S e' \wedge e' \circ e =_S e'$$

$$a_2(\ldots) \;:=\; unit(S, \circ, e')e \;:\; e' \circ e =_S e \wedge e \circ e' =_S e$$

$$a_3(\ldots) \;:=\; \wedge\text{-}el_1(e \circ e' =_S e', e' \circ e =_S e', a_1(\ldots) \;:\; e \circ e' =_S e'$$

$$a_4(\ldots) \;:=\; \wedge\text{-}el_2(e' \circ e =_S e, e \circ e' =_S e, a_2(\ldots) \;:\; e \circ e' =_S e$$

$$a_5(\ldots) \;:=\; eq\text{-}sym(S, e \circ e', e', a_3(\ldots)) \;:\; e' =_S e \circ e'$$

$$a_6(\ldots) \;:=\; eq\text{-}trans(S, e', e \circ e', e, a_5(\ldots), a_4(\ldots)) \;:\; e' =_S e$$

$$a_7(\ldots) \;:=\; \lambda e' : S\,.\,\lambda w : unit(S, \circ, e')\,.\,a_6(\ldots) \;:\; \forall e' : S\,.\,unit(S, \circ, e') \Rightarrow e' =_S e)$$

$$a_8(\ldots) \;:=\; a_{\ldots[Exercise\ 12.5]}(S, \lambda e' : S\,.\,unit(S, \circ, e'), e, v, a_7(\ldots)) \;:\; e =_S \iota_{x \in S}(unit(S, \circ, e'))$$

12.7 (c)

$x, y : S$

$inverse(S, \circ, u, e, v, x, y) \ := \ x \circ y =_S e \wedge y \circ x =_S e \ : \ *_p$

$w \ : \ \forall x : S \,.\, \exists y : S \,.\, inverse(S, \circ, u, e, v, x, y)$

$x : S$

$\ldots \ : \ \exists^{\geq 1} y : S \,.\, (inverse(\ldots, x, y))$

$k, l : S$

$p \ : \ inverse(\ldots, x, k) \mid q \ : \ inverse(\ldots, x, l)$

$\ldots \ : \ x \circ k =_S e \wedge k \circ x =_S e$

$\ldots \ : \ k \circ x =_S e$

$\ldots \ : \ x \circ l =_S e \wedge l \circ x =_S e$

$\ldots \ : \ x \circ l =_S e$

$\ldots \ : \ (k \circ x) \circ l =_S e \circ l$

$\ldots \ : \ e \circ l =_S l$

$\ldots \ : \ (k \circ x) \circ l =_S l$

$\ldots \ : \ (k \circ x) \circ l =_S k \circ (x \circ l)$

$\ldots \ : \ k \circ (x \circ l) =_S k \circ e$

$\ldots \ : \ (k \circ x) \circ l =_S k \circ e$

$\ldots \ : \ k \circ e =_S k$

$\ldots \ : \ (k \circ x) \circ l =_S k$

$\ldots \ : \ k =_S (k \circ x) \circ l$

$\ldots \ : \ k =_S l$

$\ldots \ : \ \forall k, l : S \,.\, (inverse(\ldots, x, k) \Rightarrow inverse(\ldots, x, l) \Rightarrow k =_S l)$

$\ldots \ : \ \exists^{\leq 1} y : S \,.\, (inverse(\ldots, x, y))$

$a_n(\ldots) \ := \ \ldots \ : \ \exists^1 y : S \,.\, (inverse(\ldots, x, y))$

12.7 (d)

$inv(S, \circ, u, e, v, w, x) \ : \ \iota_{y:S}^{a_{n[Exercise\ 12.7\,(c)]}}(inverse(\ldots, x, y)) \ : \ S$

12.8

$S : *_S \mid \; \leq : S \to S \to *_p \mid r : \textit{part-ord}(S, \leq)$

$w : \exists^{\geq 1} x : S \,.\, \textit{Least}(S, \leq, x)$

$x : S \mid u : (x =_S \textit{Min}(S, \leq, r, w))$

$a_1(\ldots) :=$
$\iota\text{-}\textit{prop}(S, \lambda m : S \,.\, \textit{Least}(S, \leq, m), a_{11[\textit{Fig. 12.16}]}(S, \leq, r, w)) \; :$
$\textit{Least}(S, \leq, \textit{Min}(S, \leq, r, w))$

$a_2(\ldots) := a_{4[\textit{Fig. 12.10}]}(S)\, x\, (\textit{Min}(S, \leq, r, w))\, u \; :$
$\textit{Min}(S, \leq, r, w) =_S x$

$a_3(\ldots) := \textit{eq-subs}(S, \lambda y : S \,.\, \textit{Least}(S, \leq, y), \textit{Min}(S, \leq, r, w), x,$
$a_2(\ldots), a_1(\ldots)) \; :$
$\textit{Least}(S, \leq, x)$

$a_4(\ldots) := \lambda x : S \,.\, \lambda u : (x =_S \textit{Min}(S, \leq, r, w)) \,.\, a_3(\ldots) \; :$
$\forall x : S \,.\, ((x =_S \textit{Min}(S, \leq, r, w)) \Rightarrow \textit{Least}(S, \leq, x))$

Chapter 13

13.1

$S : *_s \mid V, W : ps(S)$

$u : V \widehat{=}_{ps(S)} W \quad [=_\delta \Pi K : ps(S) \to *_p \,.\, (K\, V \Leftrightarrow K\, W)]$

$x : S$

$K := \lambda P : ps(S) \,.\, (x \;\varepsilon\; P) \; : \; ps(S) \to *_p$

$a_2 := u\, K \; : \; x \;\varepsilon\; V \Leftrightarrow x \;\varepsilon\; W$ —

$a_3 := \ldots$ `use` $\Leftrightarrow\text{-}el_1 \ldots \; : \; x \;\varepsilon\; V \Rightarrow x \;\varepsilon\; W$

$a_4 := \ldots$ `use` $\Leftrightarrow\text{-}el_2 \ldots \; : \; x \;\varepsilon\; W \Rightarrow x \;\varepsilon\; V$

$a_5 := \lambda x : S \,.\, a_3 \; : \; V \subseteq W$

$a_6 := \lambda x : S \,.\, a_4 \; : \; W \subseteq V$

$a_7 := \ldots$ `use` $\wedge\text{-}in \ldots \; : \; V = W$

$a_8 := \ldots$ `use` $\Rightarrow\text{-}in \ldots \; : \; (V \widehat{=}_{ps(S)} W) \Rightarrow (V = W)$

13.4 (c)

$S : *_s \mid V : ps(S)$

$x : S \mid u : x \,\varepsilon\, (V \cup \mathit{full\text{-}set}(S))$

$a_1 := \lambda x : \bot .\, x : \neg\bot$

$a_2 := a_1 : x \,\varepsilon\, \mathit{full\text{-}set}(S)$

$a_3 := \ldots$ use $\Rightarrow$-*in* and $\forall$-*in* $\ldots : V \cup \mathit{full\text{-}set}(S)) \subseteq \mathit{full\text{-}set}(S)$

$x : S \mid u : x \,\varepsilon\, \mathit{full\text{-}set}(S)$

$a_4 := \vee\text{-}in_2(x \,\varepsilon\, V, x \,\varepsilon\, \mathit{full\text{-}set}(S), u) : x \,\varepsilon\, V \vee x \,\varepsilon\, \mathit{full\text{-}set}(S)$

$a_5 := a_4 : x \,\varepsilon\, V \cup \mathit{full\text{-}set}(S)$

$a_6 := \ldots$ use $\Rightarrow$-*in* and $\forall$-*in* $\ldots : \mathit{full\text{-}set}(S)) \subseteq V \cup \mathit{full\text{-}set}(S)$

$a_7 := \ldots$ use $\wedge$-*in* $\ldots : V \cup \mathit{full\text{-}set}(S)) = \mathit{full\text{-}set}(S)$

13.7 (c)

$S : *_s \mid V, W : ps(S)$

$u : V \subseteq W$

$x : S \mid v : x \,\varepsilon\, V \backslash W$

$a_1 := v : x \,\varepsilon\, V \wedge \neg(x \,\varepsilon\, W)$

$a_2 := \ldots$ use $\wedge$-el_1 $\ldots : x \,\varepsilon\, V$

$a_3 := \ldots$ use $\wedge$-el_2 $\ldots : \neg(x \,\varepsilon\, W)$

$a_4 := u\, x\, a_2 : x \,\varepsilon\, W$

$a_5 := a_3\, a_4 : \bot$

$a_6 := a_5 : x \,\varepsilon\, \emptyset_S$

$a_7 := \ldots$ use $\Rightarrow$-*in* and $\forall$-*in* $\ldots : V \backslash W \subseteq \emptyset_S$

$a_8 := a_{5[Fig.13.7]}(S, V \backslash W) : \emptyset_S \subseteq V \backslash W$

$a_9 := \ldots$ use $\wedge$-*in* $\ldots : V \backslash W = \emptyset_S$

$a_{10} := \ldots$ use $\Rightarrow$-*in* $\ldots : (V \subseteq W) \Rightarrow (V \backslash W = \emptyset_S)$

$u : (V \backslash W = \emptyset_S)$

$a_{11} := \ldots$ use $\wedge$-el_1 $\ldots : V \backslash W \subseteq \emptyset_S$

$x : S \mid v : x \,\varepsilon\, V$

$w : \neg(x \,\varepsilon\, W)$

$a_{12} := \ldots$ use $\wedge$-in $\ldots : x \,\varepsilon\, V \backslash W$

$a_{13} := a_{11}\, x\, a_{12} : x \,\varepsilon\, \emptyset_S \; [=_\delta \bot]$

$a_{14} := \ldots$ use $\neg$-in and $\neg\neg$-el $\ldots : x \,\varepsilon\, W$

$a_{15} := \ldots$ use $\Rightarrow$-in and $\forall$-in $\ldots : V \subseteq W$

$a_{16} := \ldots$ use $\Rightarrow$-in $\ldots : (V \backslash W = \emptyset_S) \Rightarrow (V \subseteq W)$

$a_{17} := \ldots$ use $\Leftrightarrow$-in $\ldots : (V \subseteq W) \Leftrightarrow (V \backslash W = \emptyset_S)$

13.8

$S : *_s \mid R : S \to S \to *_p$

$u : \forall x, y : S \,.\, (R\,x\,y \Rightarrow R\,y\,x)$ [*i.e. R is symmetric*]

$v : \forall x, y, z : S \,.\, (R\,x\,y \Rightarrow R\,y\,z \Rightarrow R\,x\,z)$ [*i.e. R is transitive*]

$w : \forall x : S \,.\, \exists y : S \,.\, R\,x\,y$

$x : S$

$a_1 := w\,x : \exists y : S \,.\, R\,x\,y$

$y : S \mid t : R\,x\,y$

$a_2 := u\,x\,y\,t : R\,y\,x$

$a_3 := v\,x\,y\,x\,t\,a_2 : R\,x\,x$

$a_4 := \ldots$ use $\Rightarrow$-in and $\forall$-in $\ldots : \forall y : S \,.\, (R\,x\,y \Rightarrow R\,x\,x)$

$a_5 := \ldots$ use $\exists$-el $\ldots : R\,x\,x$

$a_6 := \ldots$ use $\forall$-in $\ldots : \forall x : S \,.\, R\,x\,x$ [*i.e. R is reflexive*]

13.10 (a)

$S : *_s \mid R : S \to S \to *_p \mid u : \textit{equivalence-relation}(S, R)$

$x : S$

$a_1 := \ldots$ `use reflexivity` $\ldots : R\,x\,x$

$a_2 := a_1 : x \;\varepsilon\; [x]_R$

$a_3 := \ldots$ `use` $\exists$-in $\ldots : \exists y : S\,.\,(y \;\varepsilon\; [x]_R)$

$a_4 := a_{12[Fig.13.8]}(S, [x]_R, a_3) : [x]_R \neq \emptyset$

$a_5 := \ldots$ `use` $\forall$-in $\ldots : \forall x : S\,.\,([x]_R \neq \emptyset)$

13.10 (b)

$x, y, z : S$

$u : y \;\varepsilon\; [x]_R \wedge z \;\varepsilon\; [x]_R$

$a_6 := \ldots$ `use` $\wedge$-el_1 $\ldots : y \;\varepsilon\; [x]_R \quad [=_\delta R\,x\,y]$

$a_7 := \ldots$ `use` $\wedge$-el_2 $\ldots : z \;\varepsilon\; [x]_R \quad [=_\delta R\,x\,z]$

$a_8 := \ldots$ `use symmetry on` a_6 $\ldots : R\,y\,x$

$a_9 := \ldots$ `use transitivity on` a_8 `and` a_7 $\ldots : R\,y\,z$

$a_{10} := \ldots$ `use` $\Rightarrow$-in `and` $\forall$-in $\ldots :$

$\forall x, y, z : S\,.\,((y \;\varepsilon\; [x]_R \wedge z \;\varepsilon\; [x]_R) \Rightarrow R\,y\,z)$

13.10 (c)

$y : S$

$a_{11} := \ldots$ `use reflexivity` $\ldots : R\,y\,y$

$a_{12} := \ldots$ `use` $\exists$-in $\ldots : \exists z : S\,.\,R\,z\,y$

$a_{13} := a_{12} : \exists z : S\,.\,(y \;\varepsilon\; [z]_R)$

$a_{14} := \ldots$ `use` $\forall$-in $\ldots : \forall y : S\,.\,\exists z : S\,.\,(y \;\varepsilon\; [z]_R)$

13.13 (b)

$S_1, S_2, S_3 : *_s \mid F : S_1 \to S_2 \mid G : S_2 \to S_3$

$u : surjective(S_1, S_2, F) \mid v : surjective(S_2, S_3, G)$

$z : S_3$

$a_1 := v : \forall z : S_3 \,.\, \exists y : S_2 \,.\, (G\,y =_{S_3} z)$

$a_2 := a_1\,z : \exists y : S_2 \,.\, (G\,y =_{S_3} z)$

$y : S_2 \mid w_1 : (G\,y =_{S_3} z)$

$a_3 := u : \forall y : S_2 \,.\, \exists x : S_1 \,.\, (F\,x =_{S_2} y)$

$a_4 := a_3\,y : \exists x : S_1 \,.\, (F\,x =_{S_2} y)$

$x : S_1 \mid w_2 : (F\,x =_{S_2} y)$

$a_5 :=$ ... `use symmetry of` $=_{S_2}$ ... $: y =_{S_2} F\,x$

$a_6 :=$ ... `use` *eq-subs** `on` w_1 `and` a_5 ... $: G(F\,x) =_{S_3} z$

$a_7 := a_6 : (G \circ F)x =_{S_3} z$

$a_8 :=$ ... `use` $\exists$-*in* ... $: \exists k : S_1 \,.\, ((G \circ F)k =_{S_3} z)$

$a_9 :=$ ... `use` $\exists$-*el* ... $: \exists k : S_1 \,.\, ((G \circ F)k =_{S_3} z)$

$a_{10} :=$ ... `use` $\exists$-*el* ... $: \exists k : S_1 \,.\, ((G \circ F)k =_{S_3} z)$

$a_{11} :=$ ... `use` $\forall$-*in* ... $: \forall z : S_3 \,.\, \exists k : S_1 \,.\, ((G \circ F)k =_{S_3} z)$

$a_{12} := a_{11} : surjective(S_1, S_3, G \circ F)$

* The predicate involved in *eq-subs* (see a_6) is $P \equiv \lambda k : S_2 \,.\, (G\,k =_{S_3} z)$.

13.15 (a)

$S, T, *_s \mid V : ps(S) \mid F : \Pi x : S \,.\, ((x \,\varepsilon\, V) \to T)$

$inj\text{-}subset(S, T, V, F)$ [see Figure 13.14] $:= \forall x, y : S \,.$

$\Pi p : (x \,\varepsilon\, V) \,.\, \Pi q : (y \,\varepsilon\, V) \,.\, ((F\,x\,p =_T F\,y\,q) \Rightarrow x =_S y) : *_p$

$surj\text{-}subset(S, T, V, F) :=$

$\forall y : T \,.\, \exists x : S \,.\, (x \,\varepsilon\, V \wedge \Pi p : (x \,\varepsilon\, V) \,.\, (F\,x\,p =_T y)) : *_p$

$bij\text{-}subset(S, T, V, F) :=$

$inj\text{-}subset(S, T, V, F) \wedge surj\text{-}subset(S, T, V, F) : *_p$

Chapter 14

14.2 (b)

$x : \mathbb{Z}$

$u \,:\, x \;\varepsilon\; \mathbb{N} \;\; [=_\delta \; \mathbb{N}\, x \;=_\delta\; \Pi P : \mathbb{Z} \to *_p \,.\, (\textit{nat-cond}(P) \Rightarrow P\, x)]$

[To prove: $s\,x \;\varepsilon\; \mathbb{N}$? I.e. $\Pi P : \mathbb{Z} \to *_p \,.\, (\textit{nat-cond}(P) \Rightarrow P(s\,x))$?]

$P \,:\, \mathbb{Z} \to *_p$

$v \,:\, \textit{nat-cond}(P) \;\; [=_\delta \; P\,0 \wedge \forall y : \mathbb{Z} \,.\, (P\,y \Rightarrow P(s\,y))]$

$a_1 \;:=\; \ldots$ `use` $\wedge\text{-}\textit{el}_2$ `on` $v \;\ldots \;:\; \forall y : \mathbb{Z} \,.\, (P\,y \Rightarrow P(s\,y))$

$a_2 \;:=\; u\,P\,v \;:\; P\,x$

$a_3 \;:=\; a_1\, x \;:\; P\,x \Rightarrow P(s\,x)$

$a_4 \;:=\; a_3\, a_2 \;:\; P(s\,x)$

$a_5 \;:=\; \ldots$ `use` $\Rightarrow\text{-}\textit{in} \;\ldots \;:\; \textit{nat-cond}(P) \Rightarrow P(s\,x)$

$a_6 \;:=\; \ldots$ `use` $(\textit{abst}) \;\ldots \;:\; \Pi P : \mathbb{Z} \to *_p \,.\, (\textit{nat-cond}(P) \Rightarrow P(s\,x))$

$a_7 \;:=\; a_6 \;:\; s\,x \;\varepsilon\; \mathbb{N}$

$a_8 \;:=\; \ldots$ `use` $\Rightarrow\text{-}\textit{in} \;\ldots \;:\; x \;\varepsilon\; \mathbb{N} \Rightarrow s\,x \;\varepsilon\; \mathbb{N}$

$a_9 \;:=\; \ldots$ `use` $\forall\text{-}\textit{in} \;\ldots \;:\; \forall x : \mathbb{Z} \,.\, (x \;\varepsilon\; \mathbb{N} \Rightarrow s\,x \;\varepsilon\; \mathbb{N})$

14.5

$P \;:=\; \lambda x : \mathbb{Z} \,.\, (x =_{\mathbb{Z}} 0 \vee p\,x \;\varepsilon\; \mathbb{N})$

[Step 1: to prove: $P\,0$? I.e. $0 =_{\mathbb{Z}} 0 \vee p\,0 \;\varepsilon\; \mathbb{N}$?]

$a_1 \;:=\; \textit{eq-refl}(\mathbb{Z}, 0) \;:\; 0 =_{\mathbb{Z}} 0$

$a_2 \;:=\; \ldots$ `use` $\vee\text{-}\textit{in}_1 \;\ldots \;:\; 0 =_{\mathbb{Z}} 0 \vee p\,0 \;\varepsilon\; \mathbb{N}$

$a_3 \;:=\; a_2 \;:\; P\,0$

[Step 2: to prove: $\forall x : \mathbb{Z} \,.\, (x \;\varepsilon\; \mathbb{N} \Rightarrow (P\,x \Rightarrow P(s\,x)))$?]

$x : \mathbb{Z} \mid u \,:\, x \;\varepsilon\; \mathbb{N} \mid v : P\,x \;\; [=_\delta \; x =_{\mathbb{Z}} 0 \vee p\,x \;\varepsilon\; \mathbb{N}]$

$w_1 \,:\, x =_{\mathbb{Z}} 0$

$a_4 \;:=\; \ldots$ `use` *zero-prop*, *eq-sym* `and` *eq-subs* $\ldots \;:\; x \in \mathbb{N}$

$a_5 \;:=\; \ldots$ `use` *p-s-ann*, *eq-sym* `and` *eq-subs* $\ldots \;:\; p(s\,x) \;\varepsilon\; \mathbb{N}$

$a_6 \;:=\; \ldots$ `use` $\vee\text{-}\textit{in}_2 \;\ldots \;:\; s\,x =_{\mathbb{Z}} 0 \vee p(s\,x) \;\varepsilon\; \mathbb{N}$

$a_7 \;:=\; a_6 \;:\; P(s\,x)$

$a_8 \;:=\; \ldots$ `use` $\Rightarrow\text{-}\textit{in} \;\ldots \;:\; (x =_{\mathbb{Z}} 0) \Rightarrow P(s\,x)$

$w_2 : p\,x\,\varepsilon\,\mathbb{N}$

$a_9 := \textit{clos-prop}(p\,x)w_2 : s(p\,x)\,\varepsilon\,\mathbb{N}$

$a_{10} := \ldots$ use *s-p-ann* and *eq-subs* $\ldots : x\,\varepsilon\,\mathbb{N}$

$a_{11} := \ldots$ use *p-s-ann*, *eq-sym* and *eq-subs* $\ldots : p(s\,x)\,\varepsilon\,\mathbb{N}$

$a_{12} := \ldots$ use $\vee$-in_2 $\ldots : s\,x =_{\mathbb{Z}} 0 \vee p(s\,x)\,\varepsilon\,\mathbb{N}$

$a_{13} := a_{12} : P(s\,x)$

$a_{14} := \ldots$ use $\Rightarrow$-*in* $\ldots : (p\,x\,\varepsilon\,\mathbb{N}) \Rightarrow P(s\,x)$

$a_{15} := \ldots$ use v, a_8, a_{14} and $\vee$-*el* $\ldots : P(s\,x)$

$a_{16} := \ldots$ use $\Rightarrow$-*in*, $\Rightarrow$-*in* and $\forall$-*in* :

$\forall x : \mathbb{Z}\,.\,(x\,\varepsilon\,\mathbb{N} \Rightarrow (P\,x \Rightarrow P(s\,x)))$

[Step 3:]

$a_{17} := \ldots$ use $\wedge$-*in* $\ldots : P\,0 \wedge \forall x : \mathbb{Z}\,.\,(x\,\varepsilon\,\mathbb{N} \Rightarrow (P\,x \Rightarrow P(s\,x)))$

$a_{18} := \textit{nat-ind}(P)a_{17} : \forall x : \mathbb{Z}\,.\,(x\,\varepsilon\,\mathbb{N} \Rightarrow P\,x)$

$a_{19} := a_{18} : \forall x : \mathbb{Z}\,.\,(x\,\varepsilon\,\mathbb{N} \Rightarrow (x =_{\mathbb{Z}} 0 \vee p\,x\,\varepsilon\,\mathbb{N}))$

14.7 *with respect to Lemma 14.3.2 (c)*:

$x : \mathbb{Z}$

$u : neg(p\,x)$

$a_1 := u : \neg(p\,x\,\varepsilon\,\mathbb{N})$

$a_2 := a_1 : \neg(pos(x))$

$a_3 := \ldots$ use logic $[(A \vee B) \Leftrightarrow (\neg B \Rightarrow \neg A)]$ on *nat-split-alt* $\ldots$:

$\neg(pos(x)) \Rightarrow (x =_{\mathbb{Z}} 0 \vee neg(x))$

$a_4 := a_3\,a_2 : x =_{\mathbb{Z}} 0 \vee neg(x)$

$a_5 := \ldots$ use $\Rightarrow$-*in* $\ldots : neg(p\,x) \Rightarrow (x =_{\mathbb{Z}} 0 \vee neg(x))$

$u : x =_{\mathbb{Z}} 0 \vee neg(x)$

$v_1 : x =_{\mathbb{Z}} 0$

$a_6 := \textit{ax-int}_3 : \neg(p\,0\,\varepsilon\,\mathbb{N})$

$a_7 := a_6 : neg(p\,0)$

$a_8 := \ldots$ use *eq-subs* $: neg(p\,x)$

$a_9 := \ldots$ use $\Rightarrow$-*in* $\ldots : (x =_{\mathbb{Z}} 0) \Rightarrow neg(p\,x))$

$v_2 : neg(x)$

$a_{10} := v_2 : \neg(x \,\varepsilon\, \mathbb{N})$

$w : p\,x \,\varepsilon\, \mathbb{N}$

$a_{11} := \textit{clos-prop}\,(p\,x)\,w : s(p\,x) \,\varepsilon\, \mathbb{N}$

$a_{12} := \ldots$ use *s-p-ann* and *eq-subs* $: x \,\varepsilon\, \mathbb{N}$

$a_{13} := a_{10}\,a_{12} : \bot$

$a_{14} := \ldots$ use $\neg$-*in* $\ldots : \neg(p\,x \,\varepsilon\, \mathbb{N})$

$a_{15} := a_{14} : neg(p\,x)$

$a_{16} := \ldots$ use $\Rightarrow$-*in* $\ldots : neg(x) \Rightarrow neg(p\,x))$

$a_{17} := \ldots$ use $\vee$-*el* $\ldots : neg(p\,x)$

$a_{18} := \ldots$ use $\Rightarrow$-*in* $\ldots : (x =_{\mathbb{Z}} 0 \vee neg(x)) \Rightarrow neg(p\,x)$

$a_{19} := := \ldots$ use $\Leftrightarrow$-*in* $\ldots : neg(p\,x) \Leftrightarrow (x =_{\mathbb{Z}} 0 \vee neg(x))$

$a_{20} := \ldots$ use $\forall$-*in* $\ldots : \forall x : \mathbb{Z}\,.\,(neg(p\,x) \Leftrightarrow (x =_{\mathbb{Z}} 0 \vee neg(x)))$

14.9 (a)

Take R such that $x \in \mathbb{Z}$ is related to $y \in \mathbb{Z}$ (which we write as $x\,R\,y$) iff $(y = s\,x \wedge pos(y)) \vee (y = p\,x \wedge neg(y))$.

Then we have on the one hand: $0\ R\ 1\ R\ 2\ R\ 3\ R\ \ldots$,
and on the other hand: $0\ R\ (-1)\ R\ (-2)\ R\ (-3)\ R\ \ldots$.

It will be clear that no chain $\ldots x_3\ R\ x_2\ R\ x_1\ R\ x_0$ can be infinitely expanded on the left.

14.9 (b)

Then we obtain for example

$g\,1 = f_1(g\,0) = f_1(f_2(g\,1)) = f_1(f_2(f_1(g\,0))) = \ldots$, ad infinitum.

The corresponding relation is now:

$x\,R\,y \Leftrightarrow ((y = s\,x) \vee (y = p\,x))$.

So, for example, $0\,R\,1$ since $1 = s\,0$ and $1\,R\,0$ since $0 = p\,1$. Consequently, we have the left-infinite (i.e. infinite descending) chain $\ldots 1\ R\ 0\ R\ 1\ R\ 0\ R\ 1$.

14.12 (c)

Lemma 14.6.5 (a): $\forall x, y, z : \mathbb{Z}\,.\,(x + z = y + z \Rightarrow x = y)$.

Proof Let x, y be fixed in $\mathbb{Z}$. Proceed by symmetric induction on z in $\mathbb{Z}$. Let $Q := \lambda z : \mathbb{Z}(x + z = y + z \Rightarrow x = y)$.

(1) $Q\,0$? I.e. $x + 0 = y + 0 \Rightarrow x = y$? Yes, by *eq-subs*, *plus-i* and $\Rightarrow$-*in*.

(2) Induction hypothesis: $Q\,z$, i.e. $x + z = y + z \Rightarrow x = y$.

(2a) $Q(s\,z)$?

| $x + s\,z = y + s\,z$
| $s(x + z) = s(y + z)$ by *plus-ii* (twice)
| $x + z = y + z$ since s is a bijection
| $x = y$ by induction hypothesis

$x + s\,z = y + s\,z \;\Rightarrow\; x = y$, so $Q(s\,z)$

(2b) $Q(p\,z)$?

| $x + p\,z = y + p\,z$
| $p(x + z) = p(y + z)$ by *plus-iii* (twice)
| $x + z = y + z$ since p is a bijection
| $x = y$ by induction hypothesis

$x + p\,z = y + p\,z \;\Rightarrow\; x = y$, so $Q(p\,z)$

Hence $\forall z : \mathbb{Z}\,.\,(Q\,z \Rightarrow (Q(s\,z) \wedge Q(p\,z)))$.

So by symmetric induction: $\forall z : \mathbb{Z}\,.\,Q\,z$.

Final conclusion by $\forall$-*in* (twice): $\forall x, y, z : \mathbb{Z}\,.\,(x + z = y + z \Rightarrow x = y)$. □

14.14

Lemma 14.8.6 (b): $\forall x, y : \mathbb{Z}\,.\,(x - p\,y = s(x - y))$.

Proof

| $x, y : \mathbb{Z}$
| a_1 := ... `use Lemma` 14.8.2 ... : $(x - p\,y) + p\,y = x$
| a_2 := ... `use Lemma` 14.6.3 (b) ... : $s(x - y) + p\,y = (x - y) + y$
| a_3 := ... `use Lemma` 14.8.2 ... : $(x - y) + y = x$
| a_4 := ... `use` *eq-trans* `on` a_2 `and` a_3 ... : $s(x - y) + p\,y = x$
| a_5 := ... `use properties of` *eq* `on` a_1 `and` a_4 ... :
| $(x - p\,y) + p\,y = s(x - y) + p\,y$
| a_6 := ... `use Lemma` 14.6.5 (*Right Cancellation*) ... :
| $x - p\,y = s(x - y)$

a_7 := `use` $\forall$-*in* ... : $\forall x, y : \mathbb{Z}\,.\,(x - p\,y = s(x - y))$ □

14.18

$u : \exists l : \mathbb{Z}\,.\,(P\,l) \wedge \forall x : \mathbb{Z}\,.\,(P\,x \Rightarrow (P(s\,x) \wedge P(p\,x)))$

$a_1 := \ldots$ use $\wedge$-el_1 $\ldots : \exists l : \mathbb{Z}\,.\,P\,l$

$a_2 := \ldots$ use $\wedge$-el_2 $\ldots : \forall x : \mathbb{Z}\,.\,(P\,x \Rightarrow (P(s\,x) \wedge P(p\,x)))$

$l : \mathbb{Z} \mid v : P\,l$

$Q := \lambda y : \mathbb{Z}\,.\,P(l + y)$

$a_3 := \ldots$ use u and *plus-i* $\ldots : Q\,0$

$x : \mathbb{Z} \mid w : Q\,x$

[To prove: $Q(s\,x) \wedge Q(p\,x)$? I.e. $P(l + s\,x) \wedge P(l + p\,x)$?]

$a_4 := w : P(l + x)$

$a_5 := a_2\,(l + x) : P(l + x) \Rightarrow (P(s(l + x)) \wedge P(p(l + x)))$

$a_6 := a_5\,a_4 : P(s(l + x)) \wedge P(p(l + x))$

$a_7 := \ldots$ use $\wedge$-el_1 $\ldots : P(s(l + x))$

$a_8 := \ldots$ use $\wedge$-el_2 $\ldots : P(p(l + x))$

$a_9 := \ldots$ use *plus-ii* $\ldots : P(l + s\,x)$

$a_{10} := \ldots$ use *plus-iii* $\ldots : P(l + p\,x)$

$a_{11} := \ldots$ use $\wedge$-in on a_9 and a_{10} $\ldots : Q(s\,x) \wedge Q(p\,x)$

$a_{12} := \ldots$ use $\Rightarrow$-in and $\forall$-in $\ldots :$
$\forall x : \mathbb{Z}\,.\,(Q\,x \Rightarrow (Q(s\,x) \wedge Q(p\,x)))$

$a_{13} := \ldots$ use $\wedge$-in $\ldots :$
$Q\,0 \wedge \forall x : \mathbb{Z}\,.\,(Q\,x \Rightarrow (Q(s\,x) \wedge Q(p\,x)))$

$a_{14} := ax\text{-}int_2\,a_{13} : \forall x : \mathbb{Z}\,.\,Q\,x$

$a_{15} := a_{14} : \forall x : \mathbb{Z}\,.\,P(l + x)$

$x : \mathbb{Z}$

$a_{16} := a_{15}\,(x - l) : P(l + (x - l))$

$a_{17} := \ldots$ use *subtr-prop*$_1$ $\ldots : P\,x$

$a_{18} := \ldots$ use $\forall$-in $\ldots : \forall x : \mathbb{Z}\,.\,P\,x$

$a_{19} := \ldots$ use $\exists$-el $\ldots : \forall x : \mathbb{Z}\,.\,P\,x$

$a_{20} := \ldots$ use $\Rightarrow$-in $\ldots :$
$(\exists l : \mathbb{Z}\,.\,(P\,l) \wedge \forall x : \mathbb{Z}\,.\,(P\,x \Rightarrow (P(s\,x) \wedge P(p\,x)))) \Rightarrow \forall x : \mathbb{Z}\,.\,P\,x$

14.21 (a)

$$P \;:=\; \lambda g : \mathbb{Z} \to \mathbb{Z} \,.\, [\, g\,0 = 0 \;\wedge$$
$$\forall x : \mathbb{Z} \,.\, [\,(pos(s\,x) \Rightarrow (g(s\,x) = s(g\,x))) \;\wedge$$
$$(neg(p\,x) \Rightarrow (g(p\,x) = s(g\,x)))\,]\,] \;:$$
$$\mathbb{Z} \to (\mathbb{Z} \to \mathbb{Z}) \to *_p$$

$$abs \;:=\; \lambda x : \mathbb{Z} \,.\, \iota(\mathbb{Z} \to \mathbb{Z}, P, \textit{spec-rec-th}(\mathbb{Z}, 0, s, s)) \;:\; \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$$

$$a_1 \;:=\; \iota\textit{-prop}(\mathbb{Z} \to \mathbb{Z}, P, \textit{spec-rec-th}(\mathbb{Z}, 0, s, s)) \;:$$
$$abs\,0 = 0 \;\wedge$$
$$\forall x : \mathbb{Z} \,.\, [\,(pos(s\,x) \Rightarrow (abs(s\,x) = s(abs\,x))) \;\wedge$$
$$(neg(p\,x) \Rightarrow (abs(p\,x) = s(abs\,x)))\,]$$

14.21 (c)

$Q \;:=\; \lambda x : \mathbb{Z} \,.\, (abs\,(-x) = x)$

a_2 := ... `use` $\wedge$-el_1 `on` a_1 `of Exercise` 14.21 (a) ... : $abs\,0 = 0$

a_3 := ... `use Lemma` 14.9.2 (a) ... : $abs\,(-0) = 0$

$x : \mathbb{Z} \mid u : x\,\varepsilon\,\mathbb{N} \mid v : Q\,x \quad [=_\delta abs\,(-x) = x]$

> a_4 := ... `use` $\wedge$-el_2 `and logic on` a_1 `of Exercise` 14.21 (a) ... :
> $\qquad \forall x : \mathbb{Z} \,.\, (neg(p\,x) \Rightarrow (abs(p\,x) = s(abs\,x)))$
>
> a_5 := ... `use Lemma` 14.3.2 (a) ... : $pos\,(s\,x)$
>
> a_6 := ... `use Lemma` 14.9.4 (a) ... : $neg\,(-(s\,x))$
>
> a_7 := ... `use Lemma` 14.9.3 (a) ... : $neg\,(p(-x))$
>
> a_8 := $a_4\,(-x)\,a_7$: $abs(p(-x)) = s(abs(-x))$
>
> a_9 := ... `use Lemma` 14.9.3 (a) `and` a_8 ... :
> $\qquad abs(-(s\,x)) = s(abs\,(-x))$
>
> a_{10} := ... `use` *eq*`-properties on` a_9 `and` v ... :
> $\qquad abs(-(s\,x)) = s\,x \quad [=_\delta Q(s\,x)]$

a_{11} := ... `use logic` ... : $\forall x : \mathbb{Z} \,.\, (x\,\varepsilon\,\mathbb{N} \Rightarrow (Q\,x \Rightarrow Q(s\,x)))$

a_{12} := ... `use` $\wedge$`-in and` $\textit{nat-ind}(Q)$ ... :
$\qquad \forall x : \mathbb{Z} \,.\, (x\,\varepsilon\,\mathbb{N} \Rightarrow (abs\,(-x) = x))$

14.24 (a)

$x, y : \mathbb{Z}$

$u : x < y$

$a_1 := u : y - x \,\varepsilon\, \mathbb{N} \wedge x \neq y$

$a_2 :=$ ... use $\wedge$-el_1 ... : $y - x \,\varepsilon\, \mathbb{N}$

$a_3 :=$ ... use $\wedge$-el_2 ... : $x \neq y$

$a_4 :=$ ... use Lemma 14.8.6 (a) ... : $s\,y - s\,x = p(s\,y - x)$

$a_5 :=$ ... use Lemma 14.8.7 (b) ... : $p(s\,y - x) = p(s\,y) - x$

$a_6 :=$ ... use p-s-ann ... : $p(s\,y) - x = y - x$

$a_7 :=$ ... use a_4 to a_6 and eq-properties on a_2 ... : $s\,y - s\,x \,\varepsilon\, \mathbb{N}$

$v : s\,x = s\,y$

$a_8 :=$ ... use eq-$congr$ ... : $p(s\,x) = p(s\,y)$

$a_9 :=$ ... use p-s-ann (twice) ... : $x = y$

$a_{10} := a_3\, a_9 : \perp$

$a_{11} :=$ ... use $\neg$-in ... : $s\,x \neq s\,y$

$a_{12} :=$ ... use $\wedge$-in ... : $s\,y - s\,x \,\varepsilon\, \mathbb{N} \wedge s\,x \neq s\,y$

$a_{13} := a_{12} : s\,x < s\,y$

$a_{14} :=$ ... use $\Rightarrow$-in ... : $x < y \Rightarrow s\,x < s\,y$

$u : s\,x < s\,y$

... Similar to the derivation above, from a_1 to a_{13} ... : $x < y$

$a_{15} :=$ ... use $\Rightarrow$-in ... : $s\,x < s\,y \Rightarrow x < y$

$a_{16} :=$ ... use $\Leftrightarrow$-in ... : $x < y \Leftrightarrow s\,x < s\,y$

$a_{17} :=$ ... use $\forall$-in ... : $\forall x : \mathbb{Z}\,.\,(x < y \Leftrightarrow s\,x < s\,y)$

14.27 *Lemma 14.10.2 (a)*: $\forall x : \mathbb{Z}\,.\,(pos(x) \Leftrightarrow x > 0)$.

Proof (1) $pos(x) \Leftrightarrow p\,x \,\varepsilon\, \mathbb{N}$,
(2) $x > 0 \Leftrightarrow (x - 0 \,\varepsilon\, \mathbb{N} \wedge x \neq 0) \Leftrightarrow (x \,\varepsilon\, \mathbb{N} \wedge x \neq 0) \Leftrightarrow (\neg neg(x) \wedge x \neq 0)$,
(3) $(p\,x \,\varepsilon\, \mathbb{N}) \Leftrightarrow (\neg neg(x) \wedge x \neq 0)$ by Lemma 14.3.3 (a). □

Lemma 14.10.2 (b): $\forall x : \mathbb{Z}\,.\,(neg(x) \Leftrightarrow x < 0)$.

Proof $neg(x) \overset{\textit{Lem. 14.9.4 (b)}}{\Longleftrightarrow} pos(-x) \overset{\textit{Lem. 14.10.2 (a)}}{\Longleftrightarrow} -x > 0 \overset{\textit{Lem. 14.10.1 (e)}}{\Longleftrightarrow}$
$(-x)+x > x \overset{\textit{Lem. 14.6.2}}{\Longleftrightarrow} x+(-x) > x \overset{\textit{Fig. 14.7, line (3))}}{\Longleftrightarrow} x-x > x \overset{\textit{Lem. 14.8.4}}{\Longleftrightarrow}$
$0 > x \overset{\textit{def.} >}{\Longleftrightarrow} x < 0$ □

14.29 (a)

$x, y : \mathbb{Z}$

$u : x \leq y \wedge y \leq x$

$a_1 := \ldots$ `use` $\wedge$-el_1 $\ldots : x \leq y$

$a_2 := \ldots$ `use` $\wedge$-el_2 $\ldots : y \leq x$

$v : x \neq y$

$a_3 := \ldots$ `use` $\wedge$-in `on` a_1 `and` v $\ldots : x < y$

$a_4 := \ldots$ `use` *Lemma* 14.10.1 (d) `on` a_3 `and` a_2 $\ldots : x < x$

$a_5 := \ldots$ `use` $\wedge$-el_2 `on` a_4 $\ldots : x \neq x$

$a_6 := a_5\ eq\text{-}refl(\mathbb{Z}, x) : \bot$

$a_7 := \ldots$ `use` $\neg$-in `and` $\neg\neg$-el $\ldots : x = y$

$a_8 := \ldots$ `use` $\Rightarrow$-in $\ldots : (x \leq y \wedge y \leq x) \Rightarrow x = y$

$a_9 := \ldots$ `use` $\forall$-in $\ldots : \forall x, y \in \mathbb{Z} . ((x \leq y \wedge y \leq x) \Rightarrow x = y)$

14.33 (part one) *Lemma 14.11.3 (a)*: $\forall x, y : \mathbb{Z} . (x \cdot y = y \cdot x)$.

Proof Let x be fixed in $\mathbb{Z}$.
To prove: $\forall y : \mathbb{Z} . (x \cdot y = y \cdot x)$. We apply symmetric induction.
Take $P(x) := \lambda y : \mathbb{Z} . (x \cdot y = y \cdot x)$.

(1) To prove: $P(x)\, 0$, i.e. $x \cdot 0 = 0 \cdot x$.

$$x \cdot 0 \stackrel{times\text{-}i}{=} 0 \stackrel{Lem.\ 14.11.1\,(a)}{=} 0 \cdot x.$$

(2) Let $y : \mathbb{Z}$. Assume (induction hypothesis): $P(x)\, y$, i.e. $x \cdot y = y \cdot x$.

(2a) To prove: $P(x)\,(s\, y)$, i.e. $x \cdot s\, y = s\, y \cdot x$.

$$x \cdot s\, y \stackrel{times\text{-}ii}{=} x \cdot y + x \stackrel{ind.\ hyp.}{=} y \cdot x + x \stackrel{Lem.\ 14.11.1\,(b)}{=} s\, y \cdot x.$$

(2b) To prove: $P(x)\,(p\, y)$, i.e, $x \cdot p\, y = p\, y \cdot x$.

$$x \cdot p\, y \stackrel{times\text{-}iii}{=} x \cdot y - x \stackrel{ind.\ hyp.}{=} y \cdot x - x \stackrel{Lem.\ 14.11.1\,(c)}{=} p\, y \cdot x.$$

(3) Hence $P(x)\, 0 \wedge \forall y : \mathbb{Z} . (P(x)\, y \Rightarrow (P(x)\,(s\, y) \wedge P(x)\,(p\, y)))$.
So, by symmetric induction: $\forall y : \mathbb{Z} . P(x)\, y$, i.e, $\forall y : \mathbb{Z} . (x \cdot y = y \cdot x)$.

Final conclusion: $\forall x, y : \mathbb{Z} . (x \cdot y = y \cdot x)$.

$\square$

14.36 *Lemma 14.11.5 (a)*: $\forall x, y : \mathbb{Z}\,.\,((x \,\varepsilon\, \mathbb{N} \wedge y \,\varepsilon\, \mathbb{N}) \Rightarrow x \cdot y \,\varepsilon\, \mathbb{N})$.

Proof We first prove: $\forall x : \mathbb{Z}\,.\,(x \,\varepsilon\, \mathbb{N} \Rightarrow \forall y : \mathbb{Z}\,.\,(y \,\varepsilon\, \mathbb{N} \Rightarrow x \cdot y \,\varepsilon\, \mathbb{N}))$. See a_8 below.

| $x : \mathbb{Z}$
| $P := \lambda y : \mathbb{Z}\,.\,(x \cdot y \,\varepsilon\, \mathbb{N})$
| | $u : x \,\varepsilon\, \mathbb{N}$
| | $a_1 := \mathit{times\text{-}i}(x) : x \cdot 0 = 0$
| | $a_2 :=$ ... `use` *zero-prop* ... $: P\,0$
| | | $y : \mathbb{Z} \mid v : y \,\varepsilon\, \mathbb{N}$
| | | | $w : P\,y \quad [=_\delta x \cdot y \,\varepsilon\, \mathbb{N}]$
| | | | *To prove* : $P(s\,y)$, *i.e.* $x \cdot s\,y \,\varepsilon\, \mathbb{N}$
| | | | $a_3 := \mathit{times\text{-}ii}(x, y) : x \cdot s\,y = x \cdot y + y$
| | | | $a_4 := \mathit{clos\text{-}nat}(x \cdot y, x, w, u) : x \cdot y + x \,\varepsilon\, \mathbb{N}$
| | | | $a_5 :=$ ... `use` *eq-properties* ... $: x \cdot s\,y \,\varepsilon\, \mathbb{N}$
| | $a_6 :=$ ... `use logic` ... $: \forall y : \mathbb{Z}\,.\,(y \,\varepsilon\, \mathbb{N} \Rightarrow (P\,y \Rightarrow P(s\,y)))$
| | $a_7 :=$ ... `use` $\wedge$-*in* `on` a_2 `and` a_6, `and` $\Rightarrow$-*in* `on` $\mathit{nat\text{-}ind}(P)$ ... :
| | $\forall y : \mathbb{Z}\,.\,(y \,\varepsilon\, \mathbb{N} \Rightarrow P\,y)$

$a_8 :=$ ... `use` $\Rightarrow$-*in* `and` $\forall$-*in* ... :
    $\forall x : \mathbb{Z}\,.\,(x \,\varepsilon\, \mathbb{N} \Rightarrow \forall y : \mathbb{Z}\,.\,(y \,\varepsilon\, \mathbb{N} \Rightarrow x \cdot y \,\varepsilon\, \mathbb{N}))$

| $x, y : \mathbb{Z} \mid u : x \,\varepsilon\, \mathbb{N} \wedge y \,\varepsilon\, \mathbb{N}$
| $a_9 :=$ ... `use` $\wedge$-el_1 ... $: x \,\varepsilon\, \mathbb{N}$
| $a_{10} :=$ ... `use` $\wedge$-el_2 ... $: y \,\varepsilon\, \mathbb{N}$
| *times-clos-nat* $:= a_8\,x\,a_9\,y\,a_{10} : x \cdot y \,\varepsilon\, \mathbb{N}$

$a_{11} :=$ ... `use` $\Rightarrow$-*in* `and` $\forall$-*in* ... :
    $\forall x, y : \mathbb{Z}\,.\,((x \,\varepsilon\, \mathbb{N} \wedge y \,\varepsilon\, \mathbb{N}) \Rightarrow x \cdot y \,\varepsilon\, \mathbb{N})$

□

14.40 (b) *Lemma 14.12.2 (a):* $\forall m : \mathbb{Z} . (l \,|\, m \Leftrightarrow -l \,|\, m)$.

Proof

$m : \mathbb{Z}$

$\quad u : l \,|\, m \quad [=_\delta \exists q : \mathbb{Z} . (l \cdot q = m)]$

$\quad\quad q : \mathbb{Z} \quad | \quad v : l \cdot q = m$

$\quad\quad\quad (-l) \cdot (-q) \stackrel{Lem.\ 14.11.4}{\Longleftrightarrow} ((-l) \cdot q) \stackrel{Lem.\ 14.11.3\,(a)}{\Longleftrightarrow}$

$\quad\quad\quad -(q \cdot (-l)) \stackrel{Lem.\ 14.11.4}{\Longleftrightarrow} -(-(q \cdot l)) \stackrel{Lem.\ 14.9.2\,(b)}{\Longleftrightarrow}$

$\quad\quad\quad q \cdot l \stackrel{Lem.\ 14.11.3\,(a)}{\Longleftrightarrow} l \cdot q \stackrel{v}{\Longleftrightarrow} m$

$\quad\quad\quad$ *Hence* : $\exists r : \mathbb{Z} . ((-l) \cdot r = m)$, *i.e.* $-l \,|\, m$

$\quad\quad \exists$-*el gives* $-l \,|\, m$

$\quad u : -l \,|\, m \quad [=_\delta \exists q : \mathbb{Z} . ((-l) \cdot q = m)]$

$\quad\quad q : \mathbb{Z} \quad | \quad v : (-l) \cdot q = m$

$\quad\quad\quad l \cdot (-q) \stackrel{Lem.\ 14.11.4}{\Longleftrightarrow} -(l \cdot q) \stackrel{see\ above}{\Longleftrightarrow}$

$\quad\quad\quad -((-l) \cdot (-q)) \stackrel{Lem.\ 14.11.4}{\Longleftrightarrow} (-l) \cdot (-(-q)) \stackrel{Lem.\ 14.9.2\,(b)}{\Longleftrightarrow}$

$\quad\quad\quad (-l) \cdot q \stackrel{v}{\Longleftrightarrow} m$

$\quad\quad\quad$ *Hence* : $\exists r : \mathbb{Z} . (l \cdot r = m)$, *i.e.* $l \,|\, m$

$\quad\quad \exists$-*el gives* $l \,|\, m$

$\quad \Rightarrow$-*in and* $\Leftrightarrow$-*in give*: $l \,|\, m \Leftrightarrow -l \,|\, m$

$\forall m : \mathbb{Z} . (l \,|\, m \Leftrightarrow -l \,|\, m)$

□

14.44

$k, m : \mathbb{Z} \;|\; u : k > 0 \;|\; v : m > 0 \;|\; w : k \,|\, m$

$a_1 :=$ ... use $\wedge$-el_1 on u ... : $k \,\varepsilon\, \mathbb{N}$

$a_2 :=$ ... use $\wedge$-el_2 on u ... : $k \neq 0$

$a_3 :=$ ... use $\wedge$-el_1 on v ... : $m \,\varepsilon\, \mathbb{N}$

$a_4 :=$ ... use $\wedge$-el_2 on v ... : $m \neq 0$

$a_5 := w : \exists q : \mathbb{Z} \,.\, (k \cdot q = m)$

> $q : \mathbb{Z} \;|\; z : k \cdot q = m$
>
> > $s : q < 0$
> >
> > $a_6 :=$ ... use *Lemma 14.11.5* (c) ... : $k \cdot q < 0$
> >
> > $a_7 :=$ ... use properties of eq on a_6 and z ... : $m < 0$
> >
> > $a_8 :=$ ... use *Lemma 14.10.2* (b) ... : $neg(m)$
> >
> > $a_9 :=$ ... use *Lemma 14.3.3* (b) ... : $\neg pos(m)$
> >
> > $a_{10} :=$ ... use *Lemma 14.10.2* (a) ... : $\neg(m > 0)$
> >
> > $a_{11} := v\, a_{10} : \perp$
>
> $a_{12} :=$ ... use $\neg$-in ... : $\neg(q < 0)$
>
> $a_{13} :=$ ... use *Lemma 14.10.2* (b) ... : $\neg neg(q)$
>
> $a_{14} :=$ ... use $\neg\neg$-el ... : $q \,\varepsilon\, \mathbb{N}$
>
> > $t : q = 0$
> >
> > $a_{15} :=$ ... use properties of eq on z and t ... : $k \cdot 0 = m$
> >
> > $a_{16} :=$ ... use properties of eq and $times$-i ... : $m = 0$
> >
> > $a_{17} := a_4\, a_{16} : \perp$
>
> $a_{18} :=$ ... use $\neg$-in ... : $\neg(q = 0)$
>
> $a_{19} :=$ ... use *Exercise 14.41* (a) on q, a_{14} and a_{18} ... : $q \geq 1$
>
> $a_{20} :=$ ... use *Exercise 14.39* (a) on a_{19} and a_1 ... : $q \cdot k \geq 1 \cdot k$
>
> $a_{21} :=$ ... use properties of eq, *Lemma 14.11.3* (a) and
> *Exercise 14.35* (a) on z and a_{20} ... : $m \geq k$

$a_{22} :=$ ... use $\exists$-el on a_5 ... : $k \leq m$

Chapter 15

15.1 (a)

$m, n : \mathbb{Z}$ | $u : m > 0$ | $v : n > 0$

$d \;:=\; gcd(m, n, u, v) \;:\; \mathbb{Z}$

$a_1 \;:=\; \iota\text{-}prop(\mathbb{Z}, \lambda k : \mathbb{Z} \,.\, gcd\text{-}prop(k, m, n), gcd\text{-}unq(m, n, u, v)) \;:$
$\quad gcd\text{-}prop(d, m, n)$

$a_2 \;:=\; \ldots$ `use` $\wedge\text{-}el_1$ `on` $a_1 \;\ldots\; : \; com\text{-}div(d, m, n)$

$a_3 \;:=\; \ldots$ `use` $\wedge\text{-}el_1$ `on` $a_2 \;\ldots\; : \; d \,|\, m$

$a_4 \;:=\; \ldots$ `use` $\wedge\text{-}el_2$ `on` $a_2 \;\ldots\; : \; d \,|\, n$

15.1 (b)

We first formulate two lemmas:

Lemma I Let $a, b, c : \mathbb{Z}$ such that $a \cdot b = c$. Assume $a > 0$ and $c > 0$. Then $b > 0$.

Proof

(1) Assume that $b < 0$.

Then $a \cdot b < 0$ by Lemma 14.11.5 (c), so $c < 0$. This implies $neg(c)$ by Lemma 14.10.2 (b), so $\neg pos(c)$ by Lemma 14.3.3 (b). But $pos(c)$ by assumption u (see part (a)) and Lemma 14.10.2 (a), so we have a contradiction. Hence, $\neg(b < 0)$.

(2) Assume that $b = 0$.

Then $a \cdot b = 0$ by Lemma 14.11.3 (a) and Lemma 14.11.1 (a), so $c = 0$. But by $\wedge$-el_2 on $c > 0$, we also have $c \neq 0$. Contradiction, again. So $b \neq 0$.

From Lemma 14.10.2 (c) follows that $b > 0$. □

Lemma II Let $a, b : \mathbb{Z}$ such that $a \cdot b \leq a$. Assume $a > 0$ and $b > 0$. Then $b = 1$.

Proof

(Left to the reader) □

We continue with the same context as in part (a). Then, by a_3 of part (a): $\exists k : \mathbb{Z} \,.\, (d \cdot k = m)$. So let $k : \mathbb{Z}$ such that $d \cdot k = m$.

Now $gcd\text{-}pos(m, n, u, v)$ (see Figure 14.23) proves that $d > 0$, so we can use Lemma I to derive that $k > 0$.

Also, by a_4 of part (a): $\exists l : \mathbb{Z} \,.\, (d \cdot l = n)$. It follows, in a similar manner as above, that we also have $l > 0$. (Note: in a formal λD-derivation we can easily conclude this from the derivation of $k > 0$, by an appropriate parameter substitution.)

Now define $g := gcd(k, l, exp_1, exp_2)$, with exp_1 the proof of $k > 0$ and exp_2 the proof of $l > 0$.

Moreover, $g \mid k$ and $g \mid l$, so $\exists a : \mathbb{Z} . (g \cdot a = k)$ and $\exists b : \mathbb{Z} . (g \cdot b = l)$. So let $a, b : \mathbb{Z}$ such that $ass_1 : g \cdot a = k$ and $ass_2 : g \cdot b = l$.

Then $m = d \cdot k = d \cdot (g \cdot a) = (d \cdot g) \cdot a$ and $n = d \cdot l = d \cdot (g \cdot b) = (d \cdot g) \cdot b$, both by properties of *eq* and Lemma 14.11.3 (b).

Use $\exists$-*in* (twice) to obtain $d \cdot g \mid m$ and $d \cdot g \mid n$, hence $com\text{-}div(d \cdot g, m, n)$.

From a_1 of part (a) follows that $\forall p : \mathbb{Z} . (com\text{-}div(p, m, n) \Rightarrow p \leq d)$. Combine this with the previous result, to obtain $d \cdot g \leq d$. Now Lemma II gives $g = 1$ (note that $g > 0$ by $gcd\text{-}pos(k, l, exp_1, exp_2)$), which is also the final result after an appropriate number of applications of the $\exists$-*el*-rule.

So we are ready.

15.3 To prove: $\exists x : \mathbb{Z} . lw\text{-}bnd_{\mathbb{Z}}(S^+, x)$.

$1 := s\,0 : \mathbb{Z}$

| $t : \mathbb{Z}$ \| $u : t \,\varepsilon\, S^+$

| a_1 := ... use $\wedge$-el_2 ... : $t \,\varepsilon\, \mathbb{N}^+$
| a_2 := a_1 : $t > 0$
| a_3 := ... use $\wedge$-el_1 on a_2 ... : $t - 0 \,\varepsilon\, \mathbb{N}$
| a_4 := ... use Lemma 14.8.5 ... : $t \,\varepsilon\, \mathbb{N}$
| a_5 := ... use $\wedge$-el_2 on a_2 ... : $t \neq 0$
| a_6 := ... use Lemma 14.3.1 ... : $t = 0 \vee p\,t \,\varepsilon\, \mathbb{N}$
| a_7 := ... use $\vee$-$el\text{-}alt_1$ ... : $p\,t \,\varepsilon\, \mathbb{N}$
| a_8 := ... use Lemma 14.8.8 (b) ... : $t - 1 \,\varepsilon\, \mathbb{N}$
| a_9 := a_8 : $1 \leq t$

a_{10} := ... use $\Rightarrow$-*in* and $\forall$-*in* ... : $\forall t : \mathbb{Z} . (t \,\varepsilon\, S^+ \Rightarrow 1 \leq t)$
a_{11} := a_{10} : $lw\text{-}bnd_{\mathbb{Z}}(S^+, 1)$
a_{12} := ... use $\exists$-*in* on 1 and a_{11} ... : $\exists x : \mathbb{Z} . lw\text{-}bnd_{\mathbb{Z}}(S^+, x)$

15.7 Minimum Theorem:

| $T : ps(\mathbb{Z})$ \| $u : T \neq \emptyset_{\mathbb{Z}}$ \| $v : \exists x : \mathbb{Z} . lw\text{-}bnd_{\mathbb{Z}}(T, x)$

| $min\text{-}the(T, u, v)$:= ... : $\exists y : \mathbb{Z} . least_{\mathbb{Z}}(T, y)$

Now we give a proof sketch of the Maximum Theorem:

$T : ps(\mathbb{Z}) \mid u : T \neq \emptyset_{\mathbb{Z}} \mid v : \exists x : \mathbb{Z} \,.\, up\text{-}bnd_{\mathbb{Z}}(T, x)$ [*see Fig. 15.19*]

[*To prove* : $\exists y : \mathbb{Z} \,.\, grtst_{\mathbb{Z}}(T, y)$]

$T' := \{x : \mathbb{Z} \mid -x \,\varepsilon\, T\}$

(1) $T' : ps(\mathbb{Z})$

$\exists x : \mathbb{Z} \,.\, x \,\varepsilon\, T$ by u and Figure 13.8. Use $\exists$-el on this :

$x : \mathbb{Z} \mid ass_1 : x \,\varepsilon\, T$

$-(-x) \,\varepsilon\, T$

$-x : \mathbb{Z}$

$-x \,\varepsilon\, T'$

$\exists y : \mathbb{Z} \,.\, y \,\varepsilon\, T'$

$T' \neq \emptyset_{\mathbb{Z}}$ by Figure 13.8

(2) $T' \neq \emptyset_{\mathbb{Z}}$ by $\exists$-el; inhabitant is (say) a

Now use $\exists$-el on v :

$x : \mathbb{Z} \mid ass_2 : up\text{-}bnd_{\mathbb{Z}}(T, x)$ $[=_\delta \forall t : \mathbb{Z} \,.\, (t \,\varepsilon\, T \Rightarrow t \leq x)]$

[We now show that $-x$ is a lower bound of T' :]

$t : S \mid ass_3 : t \,\varepsilon\, T'$

$-t \,\varepsilon\, T$

$-t : \mathbb{Z}$

$-t \leq x$ by ass_2

$x - (-t) \,\varepsilon\, \mathbb{N}$

$x + t \,\varepsilon\, \mathbb{N}$

$t - (-x) \,\varepsilon\, \mathbb{N}$

$-x \leq t$

$\forall t : S \,.\, (t \,\varepsilon\, T' \Rightarrow -x \leq t)$

$lw\text{-}bnd_{\mathbb{Z}}(T', -x)$

$\exists y : \mathbb{Z} \,.\, lw\text{-}bnd_{\mathbb{Z}}(T', y)$

(3) $\exists y : \mathbb{Z} \,.\, lw\text{-}bnd_{\mathbb{Z}}(T', y)$ by $\exists$-el; inhabitant is (say) b

Apply $min\text{-}the$ on (1), (2) and (3) :

$min\text{-}the(T', a, b) : \exists m : \mathbb{Z} \,.\, least_{\mathbb{Z}}(T', m)$

Use $\exists$-el on this; so let m be a least element of T',

we shall now show that $-m$ is a greatest element of T :

$m : \mathbb{Z} \mid ass_4 : least_{\mathbb{Z}}(T', m) \ [=_\delta m \,\varepsilon\, T' \wedge lw\text{-}bnd_{\mathbb{Z}}(T', m)]$

$m \,\varepsilon\, T'$

$t : S \mid ass_5 : t \,\varepsilon\, T$

$-(-t) \,\varepsilon\, T$

$-t : \mathbb{Z}$

$-t \,\varepsilon\, T'$

$m \leq -t$ `by` ass_4

$(-t) - m \,\varepsilon\, \mathbb{N}$

$-(t + m) \,\varepsilon\, \mathbb{N}$

$-(m + t) \,\varepsilon\, \mathbb{N}$

$(-m) - t \,\varepsilon\, \mathbb{N}$

$t \leq -m$

$\forall t : S \,.\, (t \,\varepsilon\, T \Rightarrow t \leq -m)$

$up\text{-}bnd(\mathbb{Z}, \leq, T, -m)$

$-m \,\varepsilon\, T$ `since` $m \,\varepsilon\, T'$

$grtst_{\mathbb{Z}}(T, -m)$

$\exists x : \mathbb{Z} \,.\, grtst_{\mathbb{Z}}(T, x)$

$\exists x : \mathbb{Z} \,.\, grtst_{\mathbb{Z}}(T, x)$ `by` $\exists\text{-}el$

ERRATA

Page 12, *Definition 1.6.1, (3):* ... such that $z \notin FV(N)$, *add:* and $z \not\equiv x$.

Page 15, *Lemma 1.7.1:*
Instead of $M_1 =_\alpha N_1$ and $M_2 =_\alpha N_2$, *read:* $M_1 =_\alpha M_2$ and $N_1 =_\alpha N_2$.

Page 21, *Example 1.9.7:*
Instead of Δ, *read:* $\Delta\,\Delta$.

Page 31, *Exercise 1.15:*
Instead of Δ, *read:* $\Delta\,\Delta$.

Page 46, *line 7, in (3'):*
Instead of y, *read:* $y\,z$.

Page 59, *Section 2.11, line 7, (3):* ... such that $z \notin FV(N)$, *add:* and $z \not\equiv x$.

Page 82, *Exercise 3.5 (a): The notion 'legality' has not yet been defined. Read this part of the exercise as:*
Show that there is a t such that $\bot : t$.

Page 87, *paragraph 3 from below: Replace the sentence*
By gluing things together, ... *by*
By gluing things together, we informally write *judgement chains* such as $t : \sigma : *$, or even $t : \sigma : * : \square$, expressing $t : \sigma$ and $\sigma : *$ and $* : \square$.

Page 198, *Definition 9.5.1, (2), (Compatibility) If ....*

Replace $\lambda x \,.\, M \overset{\Delta}{\to} \lambda x \,.\, M'$ *by*
$\lambda x : M \,.\, K \overset{\Delta}{\to} \lambda x : M' \,.\, K$, $\lambda x : K \,.\, M \overset{\Delta}{\to} \lambda x : K \,.\, M'$, $\Pi x : M \,.\, K \overset{\Delta}{\to} \Pi x : M' \,.\, K$ and $\Pi x : K \,.\, M \overset{\Delta}{\to} \Pi x : K \,.\, M'$.

Page 208, *Exercise 9.4:*
This exercise is practically unsolvable, as communicated by Iaroslav Baranov. (The number of δ-reductions required is 2102!)
Replace Exercise 9.4 by:
9.4. See Section 9.6. Add the following definition to $(\mathcal{D}_1) \ldots (\mathcal{D}_4)$:
$(\mathcal{D}_5) \quad x : \mathbb{Z}, y : \mathbb{Z} \;\rhd\; d(x, y) \;:=\; (x + y)^2.$

Let $\Delta \equiv \mathcal{D}_1, \ldots, \mathcal{D}_5$.
Give the full δ-reduction diagram of $d(a(u,v), b(w,w))$.

Page 217, *Lemma 10.4.6: Replace* $a(x)$ *by* $a(\overline{x})$.

Page 218, *Lemma 10.4.7: Replace (1a) by (2a) and (1b) by (2b).*

Lemma 10.4.8: $\Delta_1 \subseteq \Delta_2$ *has not been defined. Give the definition yourself. (Cf. Definition 2.10.1, (2).)*

Lemma 10.4.9, (5): Replace $|\Gamma|$ *by* $|\overline{x}|$ *(three times).*

Page 235, *below Figure 11.6:*
Replace ... since $\perp$-*in* is a special case of $\Rightarrow$-*in* ...
by ... since $\perp$-*in* is a special case of $\Rightarrow$-*el* ...

Page 242, *Figure 11.17:*
Replace Figure 11.17 by the figure on p. 394, displayed under the heading Double Negation.

Page 262, *first paragraph of Section 12.3: replace by:*
... predicates (which are functions with *the collection of all propositions* as co-domain)....

Page 282, *13.2, fourth line: omit the comma in*
... there are *only subsets,* which are formalised as predicates.

(Thanks to Erkki Luuk, Gun Pinyo, Bulmaro Jimenez, Andrew Myers, Mario Weitzer, Ziqi Fan, Marcelo Caro, Travis Allison, Lillian Ryan Uhl, Ming Gao, Borysław Paulewicz, Iaroslav Baranov.)