| left | | right | |
|---|---|---|---|
| impliesL | $H,f{:}A\Rightarrow B,H'\vdash C$ ev $=c[f(a)/b]$<br>$H,f{:}A\Rightarrow B,H'\vdash A$ ev $=a$<br>$H,b{:}B,H'\vdash C$ ev $=c$ | $H\vdash A\Rightarrow B$ ev $=\lambda a.b$<br>$H,a{:}A\vdash B$ ev $=b$ | impliesR |
| andL | $H,x{:}A\wedge B,H'\vdash C$ ev $=c[x_1,x_2/a,b]$<br>$H,a{:}A,b{:}B,H'\vdash C$ ev $=c$ | $H\vdash A\wedge B$ ev $=(a,b)$<br>$H\vdash A$ ev $=a$<br>$H\vdash B$ ev $=b$ | andR |
| orL | $H,x{:}A\vee B,H'\vdash C$ ev = case $x$ of inl$(a)\rightarrow c_1$ \| inr$(b)\rightarrow c_2$<br>$H,a{:}A,H'\vdash C$ ev $=c_1$<br>$H,b{:}B,H'\vdash C$ ev $=c_2$ | $H\vdash A\vee B$ ev = inl$(a)$<br>$H\vdash A$ ev $=a$<br><br>$H\vdash A\vee B$ ev = inr$(b)$<br>$H\vdash B$ ev $=b$ | orR1<br><br><br>orR2 |
| notL | $H,f{:}\neg A,H'\vdash C$ ev = any$(f(a))$<br>$H,f{:}\neg A,H'\vdash A$ ev $=a$ | $H\vdash\neg A$ ev $=\lambda a.b$<br>$H,a{:}A\vdash$ f ev $=b$ | notR |
| | | $H,a{:}A,H'\vdash A$ ev $=a$ | axiom |
| allL $a$ | $H,f{:}(\forall x)B,H'\vdash C$ ev $=c[f(a)/b]$<br>$H,f{:}(\forall x)B,b{:}B[a/x],H'\vdash C$ ev $=c$ | $H\vdash(\forall x)B$ ev $=\lambda a'.b$<br>$H\vdash B[a'/x]$ ev $=b$ | allR |
| exL | $H,z{:}(\exists x)B,H'\vdash C$ ev $=c[z_1,z_2/a'.b]$<br>$H,b{:}B[a'/x],H'\vdash C$ ev $=c$ | $H\vdash(\exists x)B$ ev $=(a,b)$<br>$H\vdash B[a/x]$ ev $=b$ | exR $a$ |
| *$a$ can be an arbitrary parameter while $a'$ must be new* | | | |

**Table 8.2** Rules of the first-order refinement calculus

## Exercises

As an exercise the following problems should be investigated in groups. For each of the formulas below the group should find a refinement proof and construct the evidence from the proof. In cases where no proof can be found, try to explain why the proof has to get stuck.

(1) $((\forall x)(Px\wedge Qx))\Rightarrow((\forall x)Px\wedge(\forall x)Qx)$:

$\vdash ((\forall x)(Px\wedge Qx))\Rightarrow((\forall x)Px\wedge(\forall x)Qx)$ by impliesR
1 $(\forall x)(Px\wedge Qx)\vdash((\forall x)Px\wedge(\forall x)Qx)$ by andR
1.1 $(\forall x)(Px\wedge Qx)\vdash(\forall x)Px$ by allR
1.1.1 $(\forall x)(Px\wedge Qx)\vdash Pa$ by allL $a$
1.1.1.1 $(\forall x)(Px\wedge Qx),Pa\wedge Qa\vdash Pa$ by andL
1.1.1.1.1 $(\forall x)(Px\wedge Qx),Pa,Qa\vdash Pa$ by axiom
1.2 $(\forall x)(Px\wedge Qx)\vdash(\forall x)Qx$ by allR
1.2.1 $(\forall x)(Px\wedge Qx)\vdash Qa$ by allL $a$
1.2.1.1 $(\forall x)(Px\wedge Qx),Pa\wedge Qa\vdash Qa$ by andL
1.2.1.1.1 $(\forall x)(Px\wedge Qx),Pa,Qa\vdash Qa$ by axiom

The evidence extracted from this proof is $\lambda f.(\lambda x.(f\,x)_1,\lambda x.(f\,x)_2)$

(2) $((\forall x)Px\wedge(\forall x)Qx)\Rightarrow((\forall x)(Px\wedge Qx))$:

$\vdash((\forall x)Px\wedge(\forall x)Qx)\Rightarrow((\forall x)(Px\wedge Qx))$ by impliesR
1 $(\forall x)Px\wedge(\forall x)Qx\vdash(\forall x)(Px\wedge Qx)$ by andL
1.1 $(\forall x)Px,(\forall x)Qx\vdash(\forall x)(Px\wedge Qx)$ by allR
1.1.1 $(\forall x)Px,(\forall x)Qx\vdash Pa\wedge Qa$ by andR
1.1.1.1 $(\forall x)Px,(\forall x)Qx\vdash Pa$ by allL $a$
1.1.1.1.1 $(\forall x)Px,(\forall x)Qx,Pa\vdash Pa$ by axiom
1.1.1.2 $(\forall x)Px,(\forall x)Qx\vdash Qa$ by allL $a$
1.1.1.2.1 $(\forall x)Px,(\forall x)Qx,Qa\vdash Qa$ by axiom

(3) $((\forall x)Px \vee (\forall x)Qx) \Rightarrow ((\forall x)(Px \vee Qx))$:

| | |
|---|---|
| $\vdash ((\forall x)Px \vee (\forall x)Qx) \Rightarrow ((\forall x)(Px \vee Qx))$ | by impliesR |
| 1 $(\forall x)Px \vee (\forall x)Qx \vdash (\forall x)(Px \vee Qx)$ | by orL |
| 1.1 $(\forall x)Px \vee (\forall x)Qx \vdash Pa \vee Qa$ | by allR |
| 1.1.1 $(\forall x)Px \vdash Pa \vee Qa$ | by allL $a$ |
| 1.1.1.1 $Pa \vdash Pa \vee Qa$ | by orR1 |
| 1.1.1.1.1 $Pa \vdash Pa$ | by axiom |
| 1.1.2 $(\forall x)Qx \vdash Pa \vee Qa$ | by |
| 1.1.2.1 $Qa \vdash Pa \vee Qa$ | by orR2 |
| 1.1.2.1.1 $Qa \vdash Qa$ | by axiom |

(4) $((\forall x)(Px \vee Qx)) \Rightarrow ((\forall x)Px \vee (\forall x)Qx)$: A proof attempt will get stuck

| | |
|---|---|
| $\vdash ((\forall x)(Px \vee Qx)) \Rightarrow ((\forall x)Px \vee (\forall x)Qx)$ | by impliesR |
| 1 $(\forall x)(Px \vee Qx) \vdash (\forall x)Px \vee (\forall x)Qx$ | by ??? |

At this point we have to prove either $(\forall x)Px$ or $(\forall x)Qx$ but there is no way to prove that.

(5) $((\exists x)(Px \wedge Qx)) \Rightarrow ((\exists x)Px \wedge (\exists x)Qx)$:

| | |
|---|---|
| $\vdash ((\exists x)(Px \wedge Qx)) \Rightarrow ((\exists x)Px \wedge (\exists x)Qx)$ | by impliesR |
| 1 $(\exists x)(Px \wedge Qx) \vdash (\exists x)Px \wedge (\exists x)Qx$ | by exL |
| 1.1 $Pa \wedge Qa \vdash (\exists x)Px \wedge (\exists x)Qx$ | by andL |
| 1.1.1 $Pa, Qa \vdash (\exists x)Px \wedge (\exists x)Qx$ | by andR |
| 1.1.1.1 $Pa, Qa \vdash (\exists x)Px$ | by exR $a$ |
| 1.1.1.1.1 $Pa, Qa \vdash Pa$ | by axiom |
| 1.1.1.2 $Pa, Qa \vdash (\exists x)Qx$ | by exR $a$ |
| 1.1.1.2.1 $Pa, Qa \vdash Qa$ | by axiom |

(6) $((\exists x)Px \wedge (\exists x)Qx) \Rightarrow ((\exists x)(Px \wedge Qx))$: Here is a proof attempt

$\vdash ((\exists x)Px \wedge (\exists x)Qx) \Rightarrow ((\exists x)(Px \wedge Qx))$ by `impliesR`
1 $(\exists x)Px \wedge (\exists x)Qx \vdash (\exists x)(Px \wedge Qx)$ by `andL`
1.1 $(\exists x)Px, (\exists x)Qx \vdash (\exists x)(Px \wedge Qx)$ by `exL`
1.1.1 $Pa, (\exists x)Qx \vdash (\exists x)(Px \wedge Qx)$ by `exL`
1.1.1 $Pa, Qb \vdash (\exists x)(Px \wedge Qx)$ by ???

The proof gets stuck because in the second application of `exL` we will have to use a *new* parameter instead of using $a$ again.

(7) $((\exists x)Px \vee (\exists x)Qx) \Rightarrow ((\exists x)(Px \vee Qx))$:

$\vdash ((\exists x)Px \vee (\exists x)Qx) \Rightarrow ((\exists x)(Px \vee Qx))$ by `impliesR`
1 $(\exists x)Px \vee (\exists x)Qx \vdash (\exists x)(Px \vee Qx)$ by `orL`
1.1 $(\exists x)Px \vdash (\exists x)(Px \vee Qx)$ by `exL`
1.1.1 $Pa \vdash (\exists x)(Px \vee Qx)$ by `exR` $a$
1.1.1.1 $Pa \vdash Pa \vee Qa$ by `orR1`
1.1.1.1.1 $Pa \vdash Pa$ by `axiom`
1.2 $(\exists x)Qx \vdash (\exists x)(Px \vee Qx)$ by `exL`
1.2.1 $Qa \vdash (\exists x)(Px \vee Qx)$ by `exR` $a$
1.2.1.1 $Qa \vdash Pa \vee Qa$ by `orR2`
1.2.1.1.1 $Qa \vdash Qa$ by `axiom`

(8) $((\exists x)(Px \vee Qx)) \Rightarrow ((\exists x)Px \vee (\exists x)Qx)$:

$\vdash ((\exists x)(Px \vee Qx)) \Rightarrow ((\exists x)Px \vee (\exists x)Qx)$ by `impliesR`
1 $(\exists x)(Px \vee Qx) \vdash (\exists x)Px \vee (\exists x)Qx$ by `exL`
1.1 $Pa \vee Qa \vdash (\exists x)Px \vee (\exists x)Qx$ by `orL`
1.1.1 $Pa \vdash (\exists x)Px \vee (\exists x)Qx$ by `orR1`
1.1.1.1 $Pa \vdash (\exists x)Px$ by `exR` $a$
1.1.1.1.1 $Pa \vdash Pa$ by `axiom`
1.1.2 $Pa \vdash (\exists x)Px \vee (\exists x)Qx$ by `orR1`
1.1.2.1 $Pa \vdash (\exists x)Px$ by `exR` $a$
1.1.2.1.1 $Pa \vdash Pa$ by `axiom`

(9) $(\exists x)(Px \Rightarrow (\forall y)Py)$: Here is a proof attempt

$\vdash (\exists x)(Px \Rightarrow (\forall y)Py)$ by `exR` $a$
1 $\vdash Pa \Rightarrow (\forall y)Py$ by `impliesR`
1.1 $Pa \vdash (\forall y)Py$ by `allR`
1.1.1 $Pa \vdash Pb$ by ???

The proof gets stuck because in the application of `allR` we will have to use a *new* parameter instead of using $a$ again.

(10) $(\forall x)((\forall y)Py \Rightarrow Px)$:

$\vdash (\forall x)((\forall y)Py \Rightarrow Px)$ by `allR`
1 $\vdash (\forall y)Py \Rightarrow Pa$ by `impliesR`
1.1 $(\forall y)Py \vdash Pa$ by `allL` $a$
1.1.1 $Pa \vdash Pa$ by `axiom`

(11) $(\exists x)((\exists y)Py \Rightarrow Px)$: Here is a proof attempt

$\vdash (\exists x)((\exists y)Py \Rightarrow Px)$ by `exR` $a$
1 $\vdash (\exists y)Py \Rightarrow Pa$ by `impliesR`
1.1 $(\exists y)Py \vdash Pa$ by `exL`
1.1.1 $Pb \vdash Pa$ by ???

The proof gets stuck because in the application of `exL` we will have to use a *new* parameter instead of using $a$ again.

(12) $\neg((\exists x)Px) \Rightarrow ((\forall x)(((\exists y)Py) \Rightarrow Px))$:

$\vdash \neg((\exists x)Px) \Rightarrow ((\forall x)(((\exists y)Py) \Rightarrow Px))$ by `impliesR`
1 $\neg((\exists x)Px) \vdash (\forall x)(((\exists y)Py) \Rightarrow Px)$ by `allR`

```
1.1  ¬((∃x)Px) ⊢ ((∃y)Py) ⇒ Pa          by impliesR
1.1.1  ¬((∃x)Px), (∃y)Py ⊢ Pa           by notL
1.1.1.1  ¬((∃x)Px), (∃y)Py ⊢ (∃x)Px by axiom
```

(13) $((\exists x)Px) \Rightarrow (((\forall x)(Px \Rightarrow Qx) \Rightarrow ((\exists y)Qy))$:

```
⊢ ((∃x)Px) ⇒ ((∀x)(Px ⇒ Qx) ⇒ ((∃y)Qy)) by impliesR
1  (∃x)Px ⊢ (∀x)(Px ⇒ Qx) ⇒ ((∃y)Qy) by impliesR
1.1  (∃x)Px, (∀x)(Px ⇒ Qx) ⊢ (∃y)Qy by exL
1.1.1  Pa, (∀x)(Px ⇒ Qx) ⊢ (∃y)Qy    by allL a
1.1.1.1  Pa, Pa ⇒ Qa ⊢ (∃y)Qy         by exR a
1.1.1.1.1  Pa, Pa ⇒ Qa ⊢ Qa           by impliesL
1.1.1.1.1.1  Pa, Pa ⇒ Qa ⊢ Pa         by axiom
1.1.1.1.1.2  Pa, Pa ⇒ Qa, Qa ⊢ Qa     by axiom
```

(14) $\neg((\exists x)Px) \Rightarrow ((\forall x)\neg(Px))$:

```
⊢ ¬((∃x)Px) ⇒ ((∀x)¬(Px))              by impliesR
1  ¬((∃x)Px) ⊢ (∀x)¬(Px)               by allR
1.1  ¬((∃x)Px) ⊢ ¬(Pa)                 by notR
1.1.1  ¬((∃x)Px), Pa ⊢ f               by notL
1.1.1.1  ¬((∃x)Px), Pa ⊢ (∃x)Px        by exR a
1.1.1.1.1  ¬((∃x)Px), Pa ⊢ Pa          by axiom
```

(15) $((\forall x)\neg(Px)) \Rightarrow \neg((\exists x)Px)$:

```
⊢ ((∀x)¬(Px)) ⇒ ¬((∃x)Px)              by impliesR
1  (∀x)¬(Px)) ⊢ ¬((∃x)Px)              by notR
1.1  (∀x)¬(Px)), (∃x)Px ⊢ f            by exL
1.1.1  (∀x)¬(Px)), Pa ⊢ f              by allL a
1.1.1.1  ¬(Pa), Pa ⊢ f                 by notL
1.1.1.1.1  ¬(Pa), Pa ⊢ Pa              by axiom
```

(16) $((\exists x)Px) \Rightarrow \neg((\forall x)\neg(Px))$:

```
⊢ ((∃x)Px) ⇒ ¬((∀x)¬(Px)               by impliesR
1  (∃x)Px ⊢ ¬((∀x)¬(Px)                by exL
1.1  Pa ⊢ ¬((∀x)¬(Px)                  by notR
1.1.1  Pa, (∀x)¬(Px) ⊢ f               by allL a
1.1.1.1  Pa, ¬(Pa) ⊢ f                 by notL
1.1.1.1.1  Pa, ¬(Pa) ⊢ Pa              by axiom
```

(17) $\neg((\forall x)Px) \Rightarrow ((\exists x)\neg(Px))$: Here is a proof attempt

```
⊢ ¬((∀x)Px) ⇒ ((∃x)¬(Px)))             by impliesR
1  ⊢  ¬((∀x)Px) ⊢ ((∃x)¬(Px)))         by ???
```

At this point we're stuck. If we apply `notL` we will lose the conclusion $((\exists x)\neg(Px)))$ and have to prove $(\forall x)Px$, which clearly won't work. But there are no other proof rule that can be applied here.