

14 RP Extended with an Application to $\#(S \times T)$

The following extends **14 RP** to the case of \star any operator.

Theorem 14 RP (Extended): For ρ a relation and provided x, y, z do not occur free in ρ and x, y do not occur free in P ,

$$\vdash (\star z \mid z \in \rho : P) = (\star x, y \mid \langle x, y \rangle \in \rho : P[z := \langle x, y \rangle]) .$$

Proof:

$$\begin{aligned} & (\star x, y \mid \langle x, y \rangle \in \rho : P[z := \langle x, y \rangle]) \\ = & \langle (8.14) \rangle \\ & (\star x, y \mid \langle x, y \rangle \in \rho : (\star z \mid z = \langle x, y \rangle : P[z := \langle x, y \rangle])) \\ = & \langle (8.20) \text{ for multiple quantifications, } z \text{ d.n.o.f. in } \langle x, y \rangle \in \rho \rangle \\ & (\star x, y, z \mid \langle x, y \rangle \in \rho \wedge z = \langle x, y \rangle : P[z := \langle x, y \rangle]) \\ = & \langle (3.84)(a), \vdash (\star x, y \mid R : P) = (\star y, x \mid R : P) \text{ for multiple quantifications} \rangle \\ & (\star z, x, y \mid z \in \rho \wedge z = \langle x, y \rangle : P[z := \langle x, y \rangle]) \\ = & \langle (8.20) \text{ for multiple quantifications, } x, y \text{ d.n.o.f. in } z \in \rho \rangle \\ & (\star z \mid z \in \rho : (\star x, y \mid z = \langle x, y \rangle : P[z := \langle x, y \rangle])) \\ = & \langle \textbf{Lemma: } \vdash z \in \rho \Rightarrow (\star x, y \mid z = \langle x, y \rangle : P[z := \langle x, y \rangle]) = P \rangle \\ & (\star z \mid z \in \rho : P) . \end{aligned}$$

Proof of Lemma: Note that as ρ is a relation,

$$\vdash z \in \rho \equiv z \in \rho \wedge (\exists x, y \mid : z = \langle x, y \rangle) .$$

We will prove

$$\vdash z \in \rho \wedge (\exists x, y \mid : z = \langle x, y \rangle) \Rightarrow (\star x, y \mid z = \langle x, y \rangle : P[z := \langle x, y \rangle]) = P .$$

Take u, v to be fresh variables. By (3.65), (9.30), and (3.65), it suffices to prove

$$\vdash z \in \rho \wedge z = \langle u, v \rangle \Rightarrow (\star x, y \mid z = \langle x, y \rangle : P[z := \langle x, y \rangle]) = P .$$

Assume $z \in \rho \wedge z = \langle u, v \rangle$.

$$\begin{aligned} & (\star x, y \mid z = \langle x, y \rangle : P[z := \langle x, y \rangle]) \\ = & \langle \text{Assumption gives } z = \langle u, v \rangle \rangle \\ & (\star x, y \mid \langle u, v \rangle = \langle x, y \rangle : P[z := \langle x, y \rangle]) \\ = & \langle (14.2) \rangle \\ & (\star x, y \mid u = x \wedge v = y : P[z := \langle x, y \rangle]) \\ = & \langle (8.20), y \text{ d.n.o.f. in } x = u, (1.3) \rangle \\ & (\star x \mid x = u : (\star y \mid y = v : P[z := \langle x, y \rangle])) \\ = & \langle (8.14), x \text{ d.n.o.f. in } u, \text{ definition of contextual substitution} \rangle \end{aligned}$$

$$\begin{aligned}
& (\star y \mid y = v : P[z := \langle x, y \rangle][x := u]) \\
= & \langle (8.14), y \text{ d.n.o.f. in } v \rangle \\
& P[z := \langle x, y \rangle][x := u][y := v] \\
= & \langle \text{Definition of contextual substitution} \rangle \\
& P[z := \langle u, v \rangle] \\
= & \langle \text{Assumption gives } z = \langle u, v \rangle, (3.83), \text{ Modus Ponens} \rangle \\
& P[z := z] \\
= & \langle \text{Definition of contextual substitution gives } P[z := z] \text{ is } P \rangle \\
& P
\end{aligned}$$

As an application, we will prove,

$$\vdash (\exists n : \mathbb{N} \mid : \#T = n) \Rightarrow \#(S \times T) = \#S \cdot \#T .$$

$(\exists n : \mathbb{N} \mid : \#T = n)$ is understood to be an abbreviation for “ T is finite”.

Lemma: Provided x does not occur free in S ,

$$\vdash (\forall n : \mathbb{N} \mid : (+x \mid x \in S : n) = n \cdot \#S) .$$

Proof: This follows easily by Mathematical Induction.

For $n = 0$ we have

$$\begin{aligned}
& (+x \mid x \in S : 0) \\
= & \langle (8.13) \rangle \\
& (+x \mid x \in S : (+y \mid false : 0)) \\
= & \langle (8.20), y \text{ d.n.o.f. in } x \in S \rangle \\
& (+x, y \mid false \wedge x \in S : 0) \\
= & \langle (8.20), y \text{ d.n.o.f. in } false \rangle \\
& (+x \mid false : (+y \mid x \in S : 0)) \\
= & \langle (8.13) \rangle \\
& 0 \\
= & \langle \text{Arithmetic} \rangle \\
& 0 \cdot \#S .
\end{aligned}$$

Assume $(+x \mid x \in S : n) = n \cdot \#S$.

$$\begin{aligned}
& (+x \mid x \in S : n + 1) \\
= & \langle (8.15) \rangle \\
& (+x \mid x \in S : n) + (+x \mid x \in S : 1) \\
= & \langle \text{Assumption, (11.12)} \rangle
\end{aligned}$$

$$\begin{aligned}
& n \cdot \#S + \#S \\
= & \langle \text{Algebra} \rangle \\
& (n + 1) \cdot \#S .
\end{aligned}$$

Theorem: Provided n does not occur free in T ,

$$\vdash (\exists n : \mathbb{N} \mid : \#T = n) \Rightarrow \#(S \times T) = \#S \cdot \#T .$$

Proof: Take k fresh, k of type \mathbb{N} . By (9.30) it suffices to prove

$$\vdash \#T = k \Rightarrow \#(S \times T) = \#S \cdot \#T .$$

Assume $\#T = k$. Take x, y, z to be fresh variables.

$$\begin{aligned}
& \#(S \times T) \\
= & \langle (11.12) \rangle \\
& (+z \mid z \in S \times T : 1) \\
= & \langle 14\text{RP (Extended)} \rangle \\
& (+x, y \mid \langle x, y \rangle \in S \times T : 1) \\
= & \langle (14.4) \rangle \\
& (+x, y \mid x \in S \wedge y \in T : 1) \\
= & \langle (8.20), y \text{ d.n.o.f. in } x \rangle \\
& (+x \mid x \in S : (+y \mid y \in T : 1)) \\
= & \langle (11.12), \text{Assumption} \rangle \\
& (+x \mid x \in S : k) \\
= & \langle \text{Lemma} \rangle \\
& k \cdot \#S \\
= & \langle \text{Assumption} \rangle \\
& \#T \cdot \#S \\
= & \langle \text{Algebra} \rangle \\
& \#S \cdot \#T .
\end{aligned}$$