305 (weakest prespecification, weakest postspecification) Given specifications P and Q, find the weakest specification S (in terms of P and Q) such that P is refined by

(a) $S.\ Q$

(b) $Q.\ S$

After trying the question, scroll down to the solution.

(a) $S.\,Q$

§ $\forall\sigma,\sigma'\cdot P \Leftarrow (S.Q)$ expand sequential composition

$= \forall\sigma,\sigma'\cdot P \Leftarrow (\exists\sigma''\cdot \langle\sigma'\cdot S\rangle\sigma'' \land \langle\sigma\cdot Q\rangle\sigma'')$

use distributive law to move $\exists\sigma''$ outward

$= \forall\sigma,\sigma',\sigma''\cdot P \Leftarrow \langle\sigma'\cdot S\rangle\sigma'' \land \langle\sigma\cdot Q\rangle\sigma''$ portation

$= \forall\sigma,\sigma',\sigma''\cdot (P \Leftarrow \langle\sigma\cdot Q\rangle\sigma'') \Leftarrow \langle\sigma'\cdot S\rangle\sigma''$

use distributive law to move $\forall\sigma'$ inward

$= \forall\sigma,\sigma''\cdot (\forall\sigma'\cdot P \Leftarrow \langle\sigma\cdot Q\rangle\sigma'') \Leftarrow \langle\sigma'\cdot S\rangle\sigma''$ rename σ' to σ'''

$= \forall\sigma,\sigma''\cdot\ (\forall\sigma'''\cdot \langle\sigma'\cdot P\rangle\sigma''' \Leftarrow \langle\sigma'\cdot \langle\sigma\cdot Q\rangle\sigma''\rangle\sigma''') \Leftarrow \langle\sigma'\cdot S\rangle\sigma''$ rename σ'' to σ'

$= \forall\sigma,\sigma'\cdot\ (\forall\sigma'''\cdot \langle\sigma'\cdot P\rangle\sigma''' \Leftarrow \langle\sigma\cdot \langle\sigma'\cdot Q\rangle\sigma'''\rangle\sigma') \Leftarrow S$

Hence $\forall\sigma'''\cdot \langle\sigma'\cdot P\rangle\sigma''' \Leftarrow \langle\sigma\cdot \langle\sigma'\cdot Q\rangle\sigma'''\rangle\sigma'$ is the desired weakest prespecification. Let $Q^{\cup}$ be the transpose of Q, defined as

$Q^{\cup} =$ (substitute σ for σ' and simultaneously σ' for σ in Q)

Then we can write the weakest prespecification as follows.

$\forall\sigma'''\cdot \langle\sigma'\cdot P\rangle\sigma''' \Leftarrow \langle\sigma\cdot \langle\sigma'\cdot Q\rangle\sigma'''\rangle\sigma'$

$= \forall\sigma'''\cdot \langle\sigma'\cdot P\rangle\sigma''' \Leftarrow \langle\sigma\cdot Q^{\cup}\rangle\sigma'''$

$= \neg\exists\sigma'''\cdot \neg\langle\sigma'\cdot P\rangle\sigma''' \land \langle\sigma\cdot Q^{\cup}\rangle\sigma'''$

$= \neg\exists\sigma'''\cdot\langle\sigma'\cdot \neg P\rangle\sigma''' \land \langle\sigma\cdot Q^{\cup}\rangle\sigma'''$

$= \neg(\neg P.\ Q^{\cup})$

(b) $Q.\,S$

§ $\forall\sigma,\sigma'\cdot P \Leftarrow (Q.S)$ expand sequential composition

$= \forall\sigma,\sigma'\cdot P \Leftarrow (\exists\sigma''\cdot \langle\sigma'\cdot Q\rangle\sigma'' \land \langle\sigma\cdot S\rangle\sigma'')$

use distributive law to move $\exists\sigma''$ outward

$= \forall\sigma,\sigma',\sigma''\cdot P \Leftarrow \langle\sigma'\cdot Q\rangle\sigma'' \land \langle\sigma\cdot S\rangle\sigma''$ portation

$= \forall\sigma,\sigma',\sigma''\cdot (P \Leftarrow \langle\sigma'\cdot Q\rangle\sigma'') \Leftarrow \langle\sigma\cdot S\rangle\sigma''$

use distributive law to move $\forall\sigma$ inward

$= \forall\sigma',\sigma''\cdot (\forall\sigma\cdot P \Leftarrow \langle\sigma'\cdot Q\rangle\sigma'') \Leftarrow \langle\sigma\cdot S\rangle\sigma''$ rename σ to σ'''

$= \forall\sigma',\sigma''\cdot\ (\forall\sigma'''\cdot \langle\sigma\cdot P\rangle\sigma''' \Leftarrow \langle\sigma'\cdot \langle\sigma\cdot Q\rangle\sigma'''\rangle\sigma'') \Leftarrow \langle\sigma\cdot S\rangle\sigma''$ rename σ'' to σ

$= \forall\sigma,\sigma'\cdot\ (\forall\sigma'''\cdot \langle\sigma\cdot P\rangle\sigma''' \Leftarrow \langle\sigma'\cdot \langle\sigma\cdot Q\rangle\sigma'''\rangle\sigma) \Leftarrow S$

Hence $\forall\sigma'''\cdot \langle\sigma\cdot P\rangle\sigma''' \Leftarrow \langle\sigma'\cdot \langle\sigma\cdot Q\rangle\sigma'''\rangle\sigma$ is the desired weakest postspecification. Let $Q^{\cup}$ be the transpose of Q, defined as

$Q^{\cup} =$ (substitute σ for σ' and simultaneously σ' for σ in Q)

Then we can write the weakest postspecification as follows.

$\forall\sigma'''\cdot \langle\sigma\cdot P\rangle\sigma''' \Leftarrow \langle\sigma'\cdot \langle\sigma\cdot Q\rangle\sigma'''\rangle\sigma$

$= \forall\sigma'''\cdot \langle\sigma\cdot P\rangle\sigma''' \Leftarrow \langle\sigma'\cdot Q^{\cup}\rangle\sigma'''$

$= \neg\exists\sigma'''\cdot \langle\sigma'\cdot Q^{\cup}\rangle\sigma''' \land \neg\langle\sigma\cdot P\rangle\sigma'''$

$= \neg\exists\sigma'''\cdot \langle\sigma'\cdot Q^{\cup}\rangle\sigma''' \land \langle\sigma\cdot \neg P\rangle\sigma'''$

$= \neg(Q^{\cup}.\ \neg P)$