Aufgabe 5b (Zusatz): Fundamentaltheorem

Beweisen Sie das

Fundamentaltheorem
Es sei Q bezüglich r eine vollständige, sichere, prompte, behinderungsfreie und schwach prozeßtreue Implementation von P. Weiter sei β ein aktiver Ablauf in P und $\mathrm{lf}_P(\beta) = \{g_1, ..., g_m\}$.
Dann existiert in Q ein aktiver Ablauf α und Aktionen $h_1, ...h_m$ derart, daß gilt

1. $r(\alpha) = \beta$ und $r(h_i) = g_i$ für $i = 1, ..., m$.
2. $\{h_1, ..., h_m\} = \mathrm{lf}_Q(\alpha)$.

Lösungsvorschlag Aufgabe 5b (Zusatz):

1. zeige: $r(\alpha) = \beta$ und $r(h_i) = g_i$ für $i = 1, ..., m$.

   vollständig $\Longrightarrow$ $\forall \beta \in P\ \exists \alpha \in Q : r(\alpha) = \beta$
   d.h. jeder spezifizierte Ablauf ist auch in der Implementation enthalten, damit wäre der erste Teil bereits erledigt.

   prompt $\Longrightarrow$ $\exists c > 0 : length(\alpha) \leq c(1 + length(\beta))$ und $r(\alpha) = \beta$
   d.h. α enthält endlich viele Buchhaltungsaktionen und damit gilt auch $length(\alpha) < \infty$

   Wähle nun α maximal lang, wobei aber immer noch $r(\alpha) = \beta$ sein muß.
   Dann gilt fur eine Aktion h:

   $$\alpha \bullet h \text{ aktiv in } Q \quad \Longrightarrow \quad h \text{ ist beobachtbar} \qquad (*)$$

   behinderungsfrei $\Longrightarrow$ $\forall g_i \in \mathrm{lf}_P(\beta)\ \exists h_i \in \mathrm{lf}_Q(\alpha) : r(h_i) = g_i$,
   d.h. ist ein Prozeß in P nach α fortsetzbar, so muß auch die entsprechende Aktion in Q lauffähig sein. Da von jedem Prozeß immer nur eine Aktion zur Ausführung anstehen kann, müssen die $h_1, ..., h_m$ von verschiedenen Prozessen stammen.

   Wegen $(*)$ sind alle Aktionen nach α (das sind die h_i) beobachtbar.

   sicher $\Longrightarrow$ $r(\{h_1, ..., h_m\}) \subseteq \{g_1, ..., g_m\}$,
   d.h. alle beobachtbaren Aktionen aus Q sind auch spezifiziert.

   schwach prozeßtreu $\Longrightarrow$ $\forall i \neq j : \neg \mathrm{proc}_Q(h_i, h_j) \Longrightarrow r(h_i) \neq r(h_j)$.
   Eine Aktion der Spezifikation kann nicht auf mehrere Prozesse in der Implementation aufgespalten werden. Umgekehrt heißt das dann (wie oben angegeben): Wenn zwei Aktionen aus der Implementation nicht vom gleichen Prozeß sind, dann können sie auch nicht auf ein und dieselbe Aktion der Spezifikation abgebildet werden.
   Effektiv bedeutet das, daß die $h_1, ..., h_m$ auf exakt m Aktionen, nämlich die $g_1, ...g_m$ abgebildet werden.
   Damit ist $r(\{h_1, ..., h_m\}) = \{g_1, ..., g_m\}$ und die Behauptung (1) ist gezeigt.

2. zeige: $\{h_1, ..., h_m\} = \mathrm{lf}_Q(\alpha)$.

   Widerspruchsbeweis:

   Wir wissen bereits, daß $\{h_1, ..., h_m\} \in \mathrm{lf}_Q(\alpha)$ ist. Bleibt nur noch zu zeigen, daß keine weiteren Aktionen in $\mathrm{lf}_Q(\alpha)$ sind.

   Sei $h \in \mathrm{lf}_Q(\alpha)\ \wedge\ h \notin \{h_1, ..., h_m\}$.
   Da die Implementation sicher, und h wegen $(*)$ beobachtbar ist, existiert eine Aktion g_i in P mit $r(h) = g_i$.
   Andererseits ist auch $r(h_i) = g_i$.
   Wegen der schwachen Prozeßtreue gilt somit $\mathrm{proc}_Q(h, h_i)$.
   Da h lauffähig sein soll und die Implementation behinderungsfrei ist, kann aber nur noch $h = h_i$ im Widerspruch zur Annahme sein.

   Also kann $\mathrm{lf}_Q(\alpha)$ keine weiteren Aktionen enthalten und die Behauptung (2) ist gezeigt.

$\square$