Ejercicio 9.11

$$[\text{repeat } 3_p] \quad \frac{\{P\}\ S\ \{(P \wedge \neg \mathcal{B}[\![b]\!]) \vee (Q \wedge \mathcal{B}[\![b]\!])\}}{\{P\}\ \text{repeat } S \text{ until } b\ \{Q\}}$$

(Ej. 9.18)

Corrección: $\vdash_p \{P\}$ repeat S until b $\{Q\} \Rightarrow \models_p \{P\}$ repeat S until b $\{Q\}$

Veamos que $(P\,s \wedge \langle \text{repeat } S \text{ until } b, s\rangle \to s') \Rightarrow Q\,s'$

Por inducción sobre la derivación de $\langle \text{repeat } S \text{ until } b, s\rangle \to s'$

- $\langle S, s\rangle \to s'$ con $\mathcal{B}[\![b]\!]\,s' \Rightarrow Q\,s'$.
- $(\langle S, s\rangle \to s'' \wedge \langle \text{repeat } S \text{ until } b, s''\rangle \to s' \wedge \neg\mathcal{B}[b]\,s'') \Rightarrow$ $P\,s''$ y por h.i. obtenemos $Q\,s'$.

Ejercicio 9.14 $\vdash_p \{P\}$ repeat S until b $\{Q\} \Leftrightarrow \vdash_p \{P\}$ S; while $\neg b$ do S $\{Q\}$

$\boxed{\Rightarrow}$ Trivialmente podemos "ignorar" posibles aplicaciones finales de [cons_p], asumiendo que derivamos la terna del repeat vía [repeat 3_p].
Bastaría entonces probar $\{(P \wedge \neg\mathcal{B}[\![b]\!]) \vee (Q \wedge \mathcal{B}[\![b]\!])\}$ while $\neg b$ do S $\{Q\}$

$$\underbrace{\{(P \wedge \neg\mathcal{B}[\![b]\!]) \vee (Q \wedge \mathcal{B}[\![b]\!])\}}_{\equiv\, P'}$$

Al aplicar la regla del while llegamos siempre a $P' \wedge \mathcal{B}[\![b]\!]$, pero en este caso tenemos $P' \wedge \mathcal{B}[\![b]\!] \equiv Q \wedge \mathcal{B}[\![b]\!] \Rightarrow Q$. De modo que sólo nos queda ver que la regla es aplicable, o sea que $\{\neg\mathcal{B}[\![b]\!] \wedge P'\}\ S\ \{P'\}$. Pero sabemos que $\{P\}\ S\ \{P'\}$, y $\neg\mathcal{B}[\![b]\!] \wedge P' \equiv \neg\mathcal{B}[\![b]\!] \wedge P \Longrightarrow P$, con lo que concluimos esta parte.

$\boxed{\Leftarrow}$ Tendremos $\vdash_p \{P\}\ S\ \{R\}$, $\{R\}$ while $\neg b$ do S $\{Q\}$, y es fácil ver que podemos asumir que la terna del while fue obtenida vía [while$_p$], lo que implica que $Q \equiv R \wedge \mathcal{B}[\![b]\!]$
Hemos de ver, pues $\vdash_p \{P\}$ repeat S until b $\{R \wedge \mathcal{B}[\![b]\!]\}$, lo que se derivaría vía [repeat 3_p] si tuviésemos $\{P\}\ S\ \{(P \wedge \neg\mathcal{B}[\![b]\!]) \vee \underbrace{(Q \wedge \mathcal{B}[\![b]\!])}_{\equiv\,(R \wedge \mathcal{B}[\![b]\!])}\}$

Pero si pudimos aplicar [while p] fue porque teníamos

$\vdash_p \{R \wedge \neg \mathcal{B}[\![b]\!]\}\ S\ \{R\}$, que podemos "juntar con" $\vdash_p \{P\}\ S\ \{R\}$

obteniendo $\{P \vee (R \wedge \neg \mathcal{B}[\![b]\!])\}\ S\ \{R\}$

Ahora utilizamos que $R \equiv (R \wedge \neg \mathcal{B}[\![b]\!]) \vee (R \wedge \mathcal{B}[\![b]\!])$, con

lo que $R \Rightarrow \underbrace{(P \wedge \neg \mathcal{B}[\![b]\!]) \vee (R \wedge \neg \mathcal{B}[\![b]\!])}_{\equiv\ (P \vee (R \wedge \neg \mathcal{B}[\![b]\!])) \wedge \neg \mathcal{B}[\![b]\!]} \vee (R \wedge \mathcal{B}[\![b]\!]))$

De modo que a lo que hemos podido llegar es a

$$\vdash_p \{\underbrace{P \vee (R \wedge \neg \mathcal{B}[\![b]\!])}_{\equiv\ P'}\}\ S\ \{(P' \wedge \neg \mathcal{B}[\![b]\!]) \vee (R \wedge \mathcal{B}[\![b]\!])\}$$

lo que nos permite aplicar [repeat 3 p] para derivar

$\vdash_p \{P'\}$ repeat S until b $\{R \wedge \mathcal{B}[\![b]\!]\}$

y como $P \Rightarrow P'$ obtenemos $\vdash_p \{P\}$ repeat S until b $\{Q\}$.

<u>Nota</u>: Aunque en un principio nos pareció que necesitábamos (y pensábamos que íbamos a poder probar "directamente")

$\vdash_p \{P\}\ S\ \{(P \wedge \neg \mathcal{B}[\![b]\!]) \vee (R \wedge \mathcal{B}[\![b]\!])\}$, a la postre

no hemos probado tal cosa, sino la "instanciación" de este aserto tomando en lugar de P un predicado (muy oportuno) P' <u>más débil</u>. Usando $P \Rightarrow P'$ pudimos "terminar" nuestra demostración, pero ya <u>después</u> de aplicar [repeat 3 p]. Sin embargo, de que para P' se cumpla la terna de arriba, <u>no se sigue</u> que P "también la cumpla" (lo mismo hasta es falso en ocasiones, pero afortunadamente, como no lo usamos, <u>nos trae sin cuidado</u>).
