Variable side-conditions in concurrent separation logic

CCR rule

$$\frac{\Gamma \vdash \{(P * R) \wedge B\}\ C\ \{Q * R\}}{\Gamma, r(X): R \vdash \{P\}\ \textbf{with}\ r\ \textbf{when}\ B\ \textbf{do}\ C\ \textbf{od}\ \{Q\}}$$

Owicki-Gries/O'Hearn:

— No variable free in P or Q is changed by any "other process"

Brookes:

— $r \notin \textbf{dom}(\Gamma)$
— $X \cap \textbf{owned}(\Gamma) = \varnothing$
— $\textbf{free}(R) \cap \textbf{owned}(\Gamma) = \varnothing$
— $\textbf{free}(P, Q) \cap X = \varnothing$

Unsoundness in Brookes's rules [Ian Wehrman]

```
x := a;
resource r(x) { x = a } in

{ true }                    ||   { true }
with r do t := x od ;       ||   with r do
{ t = a }                   ||      x := x + 1 ;
with r do x := t od         ||      a := a + 1
{ true }                    ||   od
                            ||   { true }

end
{ x = a }
```