

## Sheet 12 solution

a)  $P \equiv c1 \neq null \wedge c2 \neq null \wedge c1 \neq c2$

type information is optional:  $\dots \wedge \tau(c1) \preceq Cell \wedge \tau(c2) \preceq Cell$

b)  $cell(e, x) \equiv e \neq null \wedge (\tau(e) = StandardCell \wedge \$(e.x) = x \vee \tau(e) = PrevCell \wedge \$(e.f) = true \wedge \$(e.c1) = x \vee \$(e.f) = false \wedge \$(e.c2) = x)$

c) Note: To make the proof a bit shorter we ignore exceptions in the rules. For example we use the rule *seq – ok* which is similar to the *seq* rule but assumes that there is no exception.

Proof for the call:

$$\frac{\frac{\frac{\frac{\{this = C \wedge par = X\}Cell : set\{cell(C, X)\}}{\{c \neq null \wedge c = C \wedge x = X\}r = c.set(x)\{cell(C, X)\}} \text{invoc}}{\{c \neq null \wedge c = C \wedge x = x\}r = c.set(x)\{cell(C, x)\}} \text{invoc - var}}{\{c \neq null \wedge c = c \wedge x = x\}r = c.set(x)\{cell(c, x)\}} \text{invoc - var}}{\{c \neq null\}r = c.set(x)\{cell(c, x)\}} \text{strength}}$$

Proof for  $Cell : set$ :

$$\frac{\frac{\frac{\{this = C \wedge par = X\}StandardCell : set\{cell(C, X)\}}{\{\tau(this) \preceq StandardCell \wedge this = C \wedge par = X\}Cell : set\{cell(C, X)\}} \text{subtype}}{\{\tau(this) \preceq StandardCell \wedge this = C \wedge par = X \vee \tau(this) \preceq PrevCell \wedge this = C \wedge par = X\}Cell : set\{cell(C, X)\}} \text{strength}}{\frac{\frac{\{this = C \wedge par = X\}PrevCell : set\{cell(C, X)\}}{\{\tau(this) \preceq PrevCell \wedge this = C \wedge par = X\}Cell : set\{cell(C, X)\}} \text{subtype}}{\{\tau(this) \preceq StandardCell \wedge this = C \wedge par = X \vee \tau(this) \preceq PrevCell \wedge this = C \wedge par = X\}Cell : set\{cell(C, X)\}} \text{strength}} \text{disjunct}}$$

Proof for  $StandardCell : set$ :

$$\frac{\frac{\frac{\frac{\{C \neq null \wedge \tau(C) = StandardCell \wedge \$(this.x := par)(C.x) = X\}this.x = par; \{C \neq null \wedge \tau(C) = StandardCell \wedge \$(C.x) = X\}}{\{\tau(this) = StandardCell \wedge this = C \wedge par = X \wedge res = 0\}this.x = par; \{C \neq null \wedge \tau(C) = StandardCell \wedge \$(C.x) = X\}} \text{strength}}{\{\tau(this) = StandardCell \wedge this = C \wedge par = X \wedge res = 0\}this.x = par; \{cell(C, X)\}} \text{weak}}{\frac{\frac{\{\tau(this) = StandardCell \wedge this = C \wedge par = X\}StandardCell@set\{cell(C, X)\}}{\{\tau(this) = StandardCell \wedge this = C \wedge par = X\}StandardCell : set\{cell(C, X)\}} \text{class}}{\{\tau(this) = StandardCell \wedge this = C \wedge par = X\}StandardCell : set\{cell(C, X)\}} \text{impl}} \text{strength}}$$



Proof for (d):

$$\frac{\frac{(then - case)}{\{!t = true \wedge this = C \wedge par = X \wedge \$(C.f) \neq t\}x1 = \mathbf{par}\{cell(C, X)\}}{\quad} \quad \frac{(else - case)}{\{!t = false \wedge this = C \wedge par = X \wedge \$(C.f) \neq t\}x2 = \mathbf{par}\{cell(C, X)\}}}{\{this = C \wedge par = X \wedge \$(C.f) \neq t\} \mathbf{if} (!t) x1 = \mathbf{par}; \mathbf{else} x2 = \mathbf{par}; \{cell(C, X)\}} \textit{if}$$

Proof for (then - case):

$$\frac{\frac{\frac{\{C \neq null \wedge \tau(C) = PrevCell \wedge \$(\dots)(C.f) = true \wedge \$(this.x1 := par)(C.x1) = X\}x1 = \mathbf{par}; \{C \neq null \wedge \tau(C) = PrevCell \wedge \$(C.f) = true \wedge \$(C.x1) = X\}}{\quad} \textit{field - write}}{\frac{\{!t = true \wedge this = C \wedge par = X \wedge \$(C.f) \neq t\}x1 = \mathbf{par}; \{C \neq null \wedge \tau(C) = PrevCell \wedge \$(C.f) = true \wedge \$(C.x1) = X\}}{\quad} \textit{strength}}}{\{!t = true \wedge this = C \wedge par = X \wedge \$(C.f) \neq t\}x1 = \mathbf{par}; \{cell(C, X)\}} \textit{weak}$$

Proof for (else - case):

$$\frac{\frac{\frac{\{C \neq null \wedge \tau(C) = PrevCell \wedge \$(\dots)(C.f) = false \wedge \$(this.x2 := par)(C.x2) = X\}x2 = \mathbf{par}; \{C \neq null \wedge \tau(C) = PrevCell \wedge \$(C.f) = false \wedge \$(C.x2) = X\}}{\quad} \textit{field - write}}{\frac{\{!t = false \wedge this = C \wedge par = X \wedge \$(C.f) \neq t\}x1 = \mathbf{par}; \{C \neq null \wedge \tau(C) = PrevCell \wedge \$(C.f) = false \wedge \$(C.x2) = X\}}{\quad} \textit{strength}}}{\{!t = false \wedge this = C \wedge par = X \wedge \$(C.f) \neq t\}x2 = \mathbf{par}; \{cell(C, X)\}} \textit{weak}$$