Lecture 18

{true}

if (x ≥ 0) {

x := x + 1

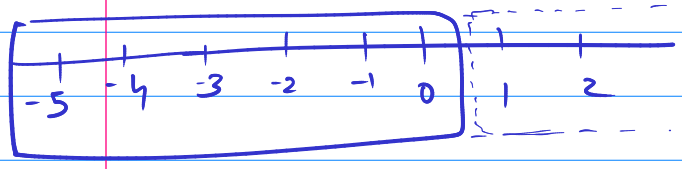
} else {

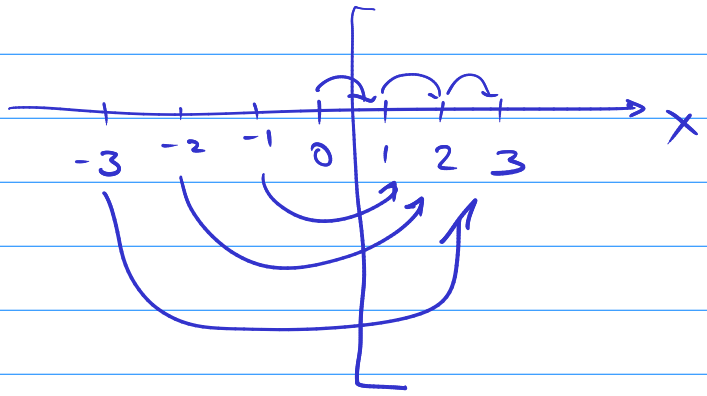
x := -x

{ {x ≥ 1}

#

{x ≥ -5} ←

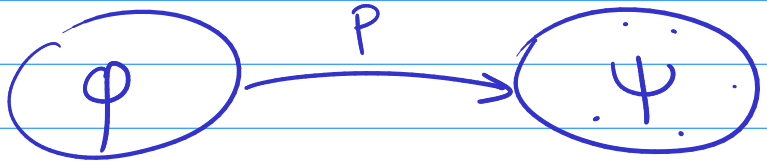




Claim: If ~~φ~~ is the wpre of ψ wrt P

then ~~ψ~~ is the spost of φ wrt P

Claim: If ψ is the spost of φ wrt P & P always terminates, then φ is the wpre of ψ wrt P



Axiom 1:

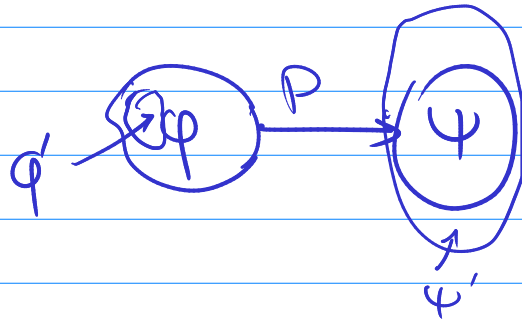
$$\frac{}{\{\varphi[e/x]\}\ x := e\ \{\varphi\}}$$

No assumptions needed

Axiom 2:

$$\frac{\varphi' \Rightarrow \varphi \qquad \{\varphi\}\ P\ \{\psi\}}{\{\varphi'\}\ P\ \{\psi\}}$$

stronger: φ' ; weaker: φ



Axiom 3

$$\frac{\{\varphi\}\ P\ \{\psi\} \qquad \psi \Rightarrow \psi'}{\{\varphi\}\ P\ \{\psi'\}}$$

$\{ x = 5 \}$

int $*y = \&x$

$*y = 3$

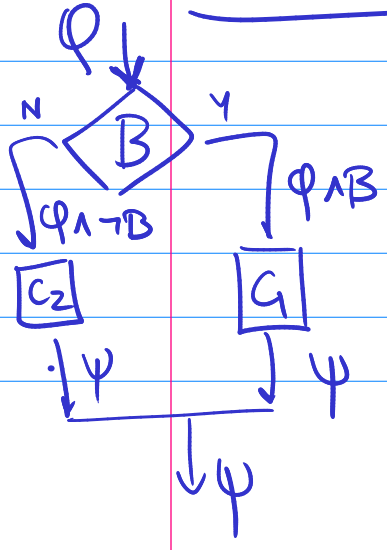
$\{ x = 3 \}$

Cmd ::= v := e
| $C_1 ; C_2$
| skip
| if (BExp) then C_1 else C_2
| while (BExp) do C

Axiom 4: $\dfrac{\{\varphi\}\ P\ \{\psi\} \qquad \{\psi\}\ Q\ \{\chi\}}{\{\varphi\}\ P ; Q\ \{\chi\}}$

Axiom 5: $\dfrac{}{\{\varphi\}\ \text{skip}\ \{\varphi\}}$

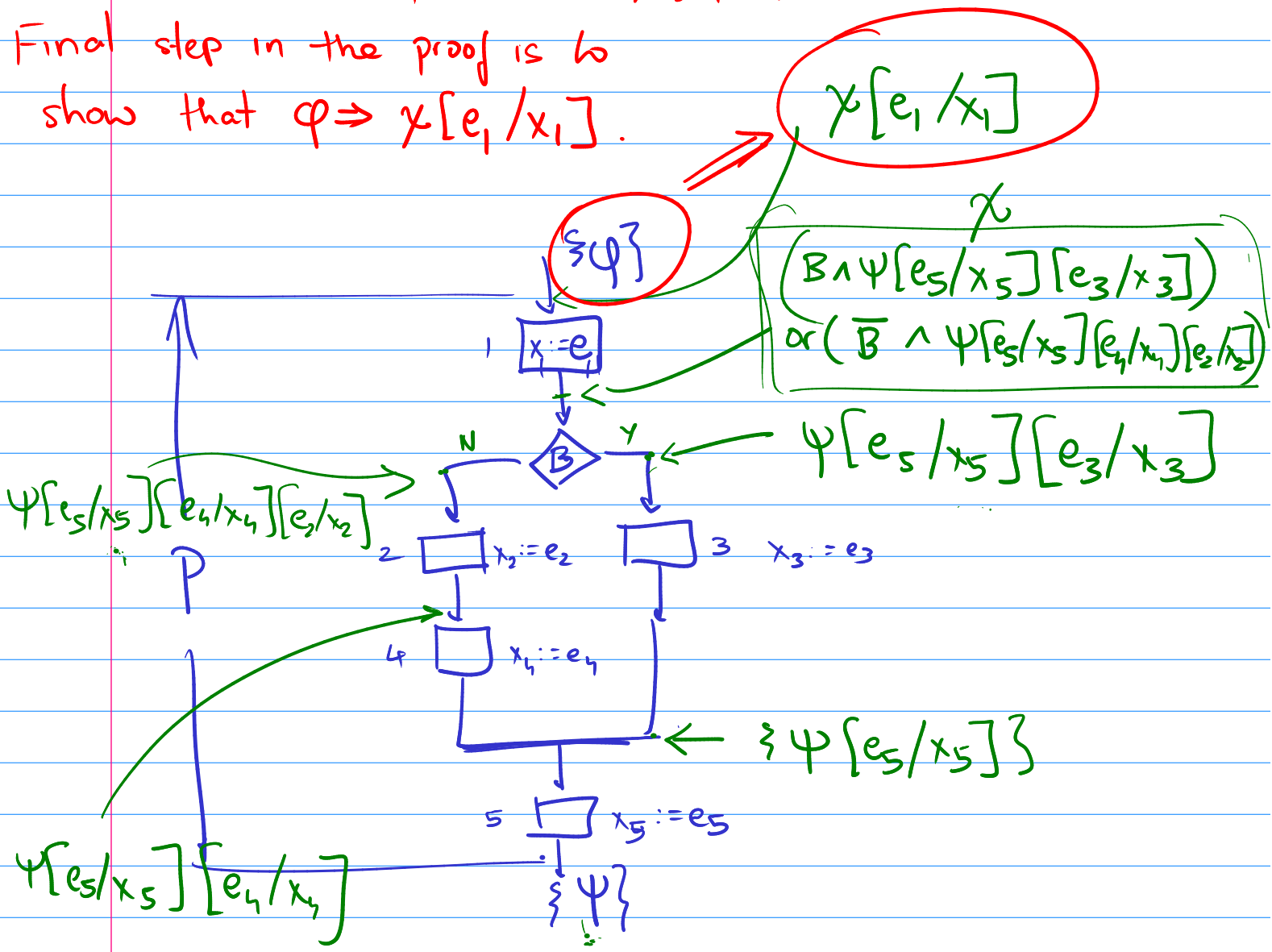
Axiom 6: $\dfrac{\{\varphi \wedge B\}\ C_1\ \{\psi\} \qquad \{\varphi \wedge \neg B\}\ C_2\ \{\psi\}}{\{\varphi\}\ \text{if}(B)\ \text{then}\ C_1\ \text{else}\ C_2\ \{\psi\}}$



We wanted to prove: $\{\varphi\}\ P\ \{\psi\}$

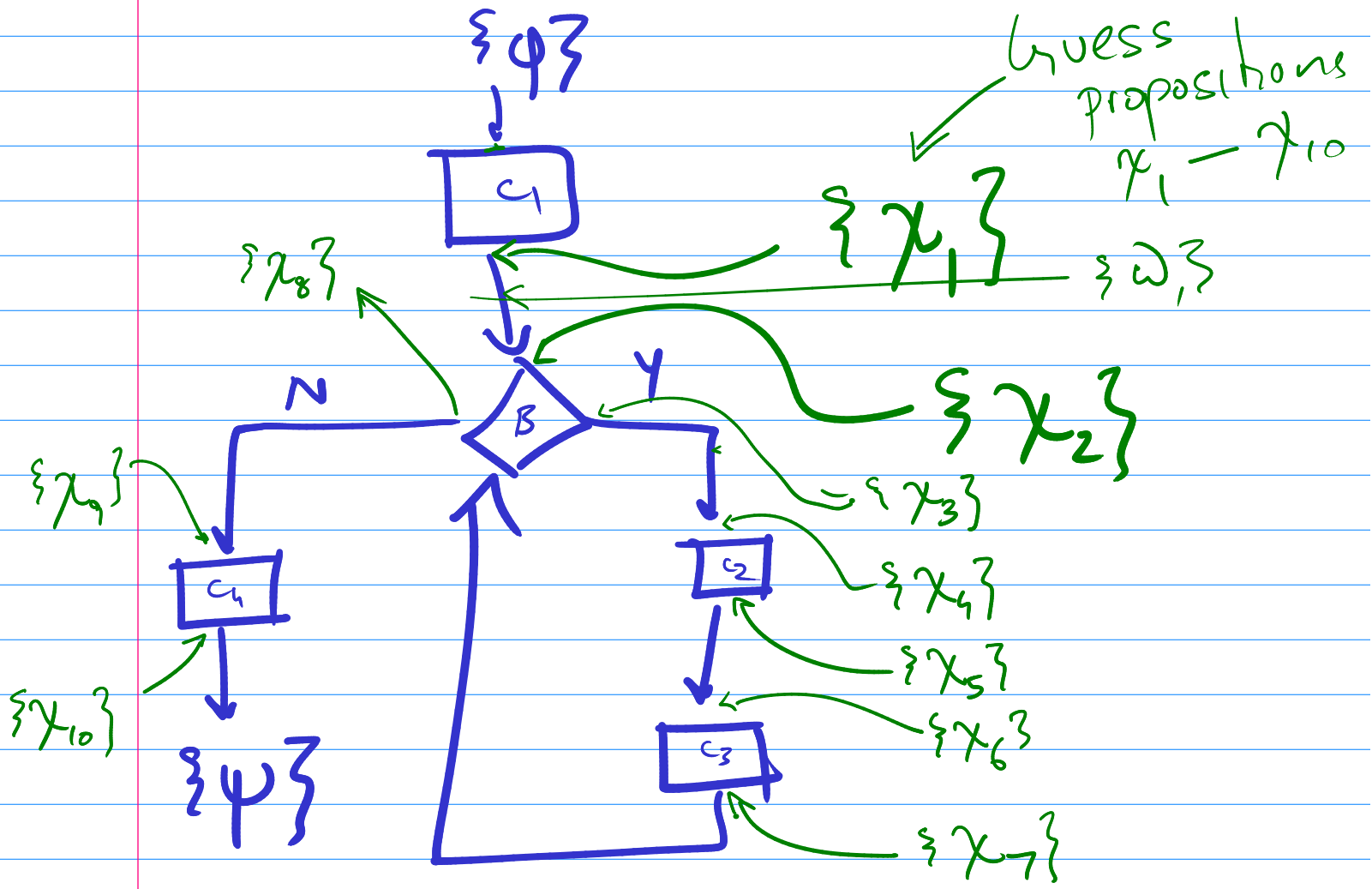
We have instead proved: $\{\chi[e_1/x_1]\}\ P\ \{\psi\}$

Final step in the proof is to show that $\varphi \Rightarrow \chi[e_1/x_1]$.



Proving properties of loops

Approach 1: (Using flowcharts) / Bob Floyd.



Verification conditions

(→ conditions)

$\chi_1 \Rightarrow \chi_2$ $\chi_3 \Rightarrow \chi_4$ $\chi_5 \Rightarrow \chi_6$

$\chi_7 \Rightarrow \chi_2$

$\chi_8 \Rightarrow \chi_9$ $\chi_{10} \Rightarrow \psi$

(Branch conditions)

$\psi_2 \wedge B \Rightarrow \psi_3 \qquad \psi_2 \wedge \overline{B} \Rightarrow \psi_8$

(Assignments)

$\{\varphi\}\, C_1\, \{\psi_1\} \qquad \{\psi_4\}\, C_2\, \{\psi_5\} \qquad \{\psi_6\}\, C_3\, \{\psi_7\}$

$\{\psi_9\}\, C_4\, \{\psi_{10}\}$