A VC GENERATOR

We define mapping $vcg : Stm \rightarrow A \times A \rightarrow A \times A$ so that $vcg[\![S]\!](post\_cond, vc) = (pre\_cond, new\_vc)$

$$vcg[\![skip]\!](P,Q) \stackrel{def}{=} (P,Q)$$

$$vcg[\![x := a]\!](P,Q) \stackrel{def}{=} (P[a/x], Q)$$

$$vcg[\![S_1; S_2]\!](P,Q) \stackrel{def}{=} vcg[\![S_1]\!](vcg[\![S_2]\!](P,Q))$$

$$\begin{aligned} vcg[\![\underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2]\!](P,Q) &\stackrel{def}{=} \\ \underline{\text{let}}\ (P_1, Q_1) &= vcg[\![S_1]\!](P,Q), \\ (P_2, Q_2) &= vcg[\![S_2]\!](P,Q) \\ \underline{\text{in}}\ ((b \Rightarrow P_1) \wedge (\neg b \Rightarrow P_2)&, Q_1 \wedge Q_2) \end{aligned}$$

$$\begin{aligned} vcg[\![\{I\}\ \underline{\text{while}}\ b\ \underline{\text{do}}\ S]\!](P,Q) &\stackrel{def}{=} \\ \underline{\text{let}}\ (P', Q') &= vcg[\![S]\!](I, true) \\ \underline{\text{in}}\ (I, Q \wedge Q' \wedge (I \wedge b \Rightarrow P') &\wedge (I \wedge \neg b) \Rightarrow P) \end{aligned}$$

Finally we define

$$\begin{aligned} VCG(\{P\}S\{Q\}) &\stackrel{def}{=} \\ \underline{\text{let}}\ (P', Q') &= vcg[\![S]\!](Q, true) \\ \underline{\text{in}}\ (P \Rightarrow P') &\wedge Q' \end{aligned}$$

VC GENERATION EXAMPLE

$$\mathrm{vcg}\,[\![p := 1 ; \{p * x^y = m^n\}\ \underline{\text{while}}\ \neg(y=0)\ \underline{\text{do}}\ p := p * x ; y := y - 1]\!]\,(p = m^n, \mathit{true})$$

$$= \mathrm{vcg}\,[\![p := 1]\!]\,(\mathrm{vcg}\,[\![\{p * x^y = m^n\}\ \underline{\text{while}}\ \neg(y=0)\ \underline{\text{do}}\ p := p * x ; y := y - 1]\!]\,(p = m^n, \mathit{true}))$$

$$= \mathrm{vcg}\,[\![p := 1]\!]\,(\underline{\text{Let}}\ (P', Q') = \mathrm{vcg}\,[\![p := p * x ; y := y - 1]\!]\,(p * x^y = m^n, \mathit{true})$$
$$\underline{\text{in}}\ (p * x^y = m^n, Q' \wedge (p * x^y = m^n \wedge \neg(y=0) \Rightarrow P')$$
$$\wedge\ (p * x^y = m^n \wedge \neg\neg(y=0) \Rightarrow p = m^n)))$$

$$= \mathrm{vcg}\,[\![p := 1]\!]\,(\underline{\text{Let}}\ (P', Q') = ((p * x) * x^{y-1} = m^n, \mathit{true})$$
$$\underline{\text{in}}\ \ldots)$$

$$= \mathrm{vcg}\,[\![p := 1]\!]\,(p * x^y = m^n, (p * x^y = m^n \wedge \neg(y=0) \Rightarrow (p * x) * x^{y-1} = m^n)$$
$$\wedge\ (p * x^y = m^n \wedge \neg\neg(y=0) \Rightarrow p = m^n))$$

$$= (1 * x^y = m^n, \ldots)$$

Finally we obtain (for Pow annotated with loop invariant $p * x^y = m^n$)

$$\mathrm{VCG}(\{x = m \wedge y = n\}\ \mathrm{Pow}\ \{p = m^n\}$$

$$= (x = m \wedge y = n \Rightarrow 1 * x^y = m^n)$$
$$\wedge\ (p * x^y = m^n \wedge \neg(y=0) \Rightarrow (p * x) * x^{y-1} = m^n)$$
$$\wedge\ (p * x^y = m^n \wedge \neg\neg(y=0) \Rightarrow p = m^n)$$