CS 357 D

Lecture 4

Preconditions and backward propagation

http://cs357d.stanford.edu/

April 12, 2007

SPL example

```
local x,y: integer where x=N ∧ y=0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

Φ: $< V , \Theta , \mathcal{T} >$ with

$V : \{ x{:}int , y{:}int , \pi{:}\{ l_1, l_2 , l_3 , l_4 \} \}$

$\Theta : x = N \wedge y = 0 \wedge \pi = l_1$

$\mathcal{T}: \{ \tau_1 , \tau_2 , \tau_3 , \tau_4 \}$ with

$\rho_{\tau 1} : \pi = l_1 \wedge ((x > 0 \wedge \pi' = l_2) \vee (x \leq 0 \wedge \pi' = l_4)) \wedge pres(\{ x , y \})$
$\rho_{\tau 2} : \pi = l_2 \wedge \pi' = l_3 \wedge x' = x - 1 \wedge y' = y$
$\rho_{\tau 3} : \pi = l_3 \wedge \pi' = l_1 \wedge y' = y + x \wedge x' = x$
$\rho_{\tau 4} : pres(\{ x , y , \pi \})$

Invariants: example

```
local x,y: integer where x=2 ∧ y=0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

reachable state space:

$\{ (2, 0, l_1) , (2, 0, l_2) , (1, 0, l_3) , (1, 1, l_1) , (1, 1, l_2) , (0, 1, l_3) , (0, 1, l_1) , (0, 1, l_4) \}$

some invariants:

$0 \leq x \leq 2$ $\quad (\pi = l_4) \rightarrow (y = 1)$ $\quad y \leq x + 1$

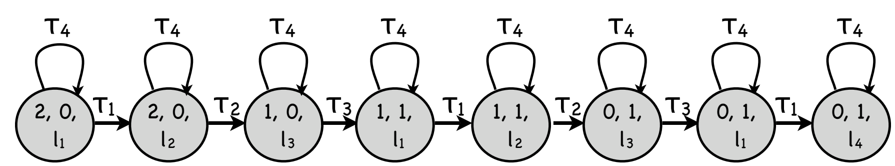
$0 \leq y \leq 1$ $\quad (\pi = l_4) \rightarrow (x = 0)$ $\quad (\pi = l_3) \rightarrow x + y = 1$

Proving invariants by model checking: example

To prove **$y \leq x + 2$** :

1. Construct the reachable state space

$\Theta : x = 2 \wedge y = 0 \wedge \pi = l_1$



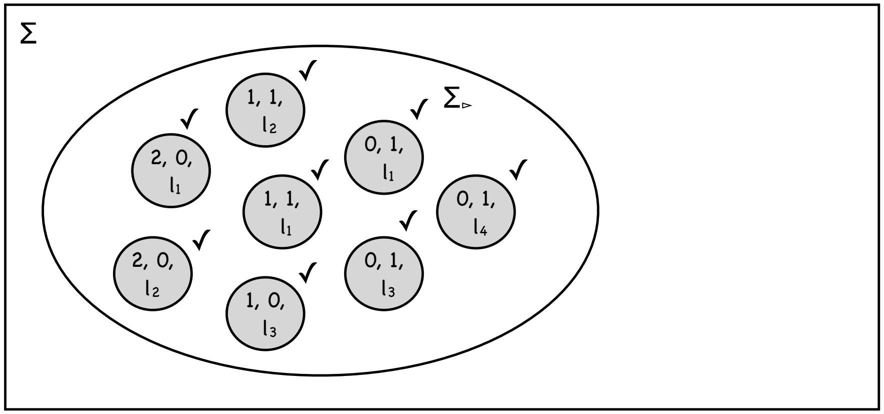
$\mathcal{T}: \{ \tau_1 , \tau_2 , \tau_3 , \tau_4 \}$ with

$\rho_{\tau 1} : \pi = l_1 \wedge ((x > 0 \wedge \pi' = l_2) \vee (x \leq 0 \wedge \pi' = l_4)) \wedge pres(\{ x , y \})$
$\rho_{\tau 2} : \pi = l_2 \wedge \pi' = l_3 \wedge x' = x - 1 \wedge y' = y$
$\rho_{\tau 3} : \pi = l_3 \wedge \pi' = l_1 \wedge y' = y + x \wedge x' = x$
$\rho_{\tau 4} : pres(\{ x , y , \pi \})$

Proving invariants by model checking: example

To prove $y \leq x + 2$:

2. Check that all reachable states satisfy $y \leq x + 2$



Invariants: example

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

invariants ?

$0 \leq x \leq 2$ $\quad$ $(\pi = l_4) \rightarrow (y = 1)$ $\quad$ $y \leq x + 1$

$0 \leq y \leq 1$ $\quad$ $(\pi = l_4) \rightarrow (x = 0)$ $\quad$ $(\pi = l_3) \rightarrow x + y = 1$

replace by N or N-1 ?

Invariants: example

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

invariants ?

$0 \leq x \leq N$ $\quad$ $(\pi = l_4) \rightarrow (y = N - 1)$ $\quad$ $y \leq x + (N - 1)$

$0 \leq y \leq N - 1$ $\quad$ $(\pi = l_4) \rightarrow (x = 0)$ $\quad$ $(\pi = l_3) \rightarrow x + y = 1$

How do we check?

Model checking for N = 1, N = 2, N = 3, N = 4, N = 5, ...

Proving invariance properties deductively

To prove that assertion p is an invariant of system Φ :

(every state of every run of Φ satisfies p)

it is sufficient to prove that (proof by induction on the run)

- p holds at the beginning of every run (base case)
- p is preserved by every transition τ (inductive step)

For assertion p — B-INV

B1. $\Theta \rightarrow p$

B2. $p \wedge \rho_\tau \rightarrow p'$ for all τ in $\mathcal{T}$

$\square p$ (p is an invariant of Φ)

Proving invariance properties deductively: example

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

$x \leq N$

is an invariant for all values of N > 0

Proof: (validity of 5 first-order formulas)

$x = N \wedge y = 0 \wedge N > 0 \wedge \pi = l_1 \rightarrow x \leq N$

$\tau_1 : x \leq N \wedge \ldots \wedge x' = x \wedge \ldots \rightarrow x' \leq N$

$\tau_2 : x \leq N \wedge \ldots \wedge x' = x - 1 \wedge \ldots \rightarrow x' \leq N$

$\tau_3 : x \leq N \wedge \ldots \wedge x' = x \wedge \ldots \rightarrow x' \leq N$

$\tau_4 : x \leq N \wedge \ldots \wedge x' = x \wedge \ldots \rightarrow x' \leq N$

Proving invariance properties deductively: example

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

invariant to prove:

$x \geq 0$

Not a proof:

$x = N \wedge y = 0 \wedge N > 0 \wedge \pi = l_1 \rightarrow x \geq 0$	valid
$\tau_1 : x \geq 0 \wedge \ldots \wedge x' = x \wedge \ldots \rightarrow x' \geq 0$	valid
$\tau_2 : x \geq 0 \wedge \ldots \wedge x' = x - 1 \wedge \ldots \rightarrow x' \geq 0$	**not valid**
$\tau_3 : x \geq 0 \wedge \ldots \wedge x' = x \wedge \ldots \rightarrow x' \geq 0$	valid
$\tau_4 : x \geq 0 \wedge \ldots \wedge x' = x \wedge \ldots \rightarrow x' \geq 0$	valid

what is the problem?

$\tau_2 : \boxed{x \geq 0} \wedge \ldots \wedge x' = x - 1 \wedge \ldots \rightarrow x' \geq 0$

inductive hypothesis is too weak

it is not preserved by all transitions

$x \geq 0$ is an invariant, but it is not **inductive**

it cannot be proven deductively directly

Solution: strengthen the inductive hypothesis

identify the problem states

$(0, 0, l_2), (0, 1, l_2), \ldots$

in general: $(0, y, l_2)$ for any value of y

remove them by strengthening the inductive hypothesis

$x \geq 0 \wedge \boxed{((\pi = l_2) \rightarrow x > 0)}$

Strengthening by backwards propagation

if $p(V) \wedge \rho_\tau(V,V') \rightarrow p(V')$ does not hold

identify the largest set of states for which it does hold

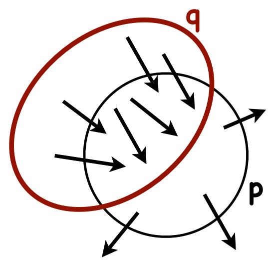
☛ find the **weakest** formula $q(V)$ such that

$$q(V) \wedge \rho_\tau(V,V') \rightarrow p(V')$$

holds for all values of V'

represented by the **weakest precondition**

$$\text{wpc}(\tau, p): \forall V' .\ \rho_\tau(V,V') \rightarrow p(V')$$



Strengthening by backwards propagation

represented by the **weakest precondition**

identify the largest set of states for which it does hold

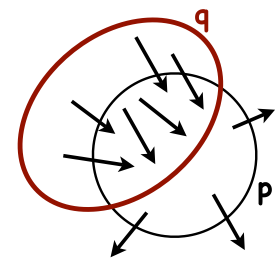
$$\text{wpc}(\tau, p): \forall V' .\ \rho_\tau(V,V') \rightarrow p(V')$$

all values (assignments, interpretations) of V

such that

for all values (assignments, interpretations) of V'

$$\rho_\tau(V,V') \rightarrow p(V') \quad \text{is true}$$



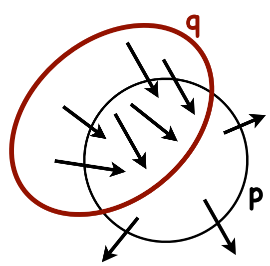
Strengthening by backwards propagation

largest set of states for which τ leads to p

$$\underbrace{(\forall V' .\ \rho_\tau(V,V') \rightarrow p(V'))}_{\text{wpc}(\tau,\ p)} \wedge \rho_\tau(V,V') \rightarrow p(V')$$

assertion over V

$$(\forall Z .\ \rho_\tau(V, Z) \rightarrow p(Z)) \wedge \rho_\tau(V, V') \rightarrow p(V')$$



Strengthening by backwards propagation

wpc $(\forall Z .\ \rho_\tau(V, Z) \rightarrow p(Z))$ set of states

verification condition valid or not valid

$$(\forall Z .\ \rho_\tau(V, Z) \rightarrow p(Z)) \wedge \rho_\tau(V, V') \rightarrow p(V')$$

validity of verification condition true or false

$$\forall V,V' \, [\, (\forall Z .\ \rho_\tau(V, Z) \rightarrow p(Z)) \wedge \rho_\tau(V, V') \rightarrow p(V') \,]$$

Strengthening by backwards propagation: example

failed verification condition: $x \geq 0 \wedge \rho_{\tau 2} \rightarrow x' \geq 0$

with $\rho_{\tau 2} : \pi = l_2 \wedge \pi' = l_3 \wedge x' = x - 1 \wedge y' = y$

$\text{wpc}(\tau_2 , x \geq 0) : \forall x', y', \pi' . \ \rho_{\tau 2}(x,y,\pi, x',y',\pi') \rightarrow x' \geq 0$

$\forall x',y'\pi' . (\pi = l_2 \wedge \pi' = l_3 \wedge x' = x - 1 \wedge y' = y) \rightarrow x' \geq 0$

can be simplified to $(\pi = l_2) \rightarrow x - 1 \geq 0$

Strengthening by backwards propagation

Two approaches

- Prove that **wpc(τ , p)** is invariant
  and use it as a supporting invariant in INC-INV

wpc(τ , p) may not be inductive

- Use **p ∧ wpc(τ , p)** as the strengthening in G-INV

In both cases the verification condition for τ is guaranteed to be valid, but verification conditions for other transitions may now fail

Note: if p is invariant
then wpc(τ , p) is also invariant for all $\tau \in \mathcal{T}$

Verification rule INC-INV (incremental invariance)

For assertion p, q_1 .... q_n

B0. $\square q_1$ ...... $\square q_n$

B1. $\Theta \rightarrow p$

B2. $p \wedge q_1 \wedge \ldots \wedge q_n \wedge \rho_\tau \rightarrow p'$ for all τ in $\mathcal{T}$

$\square p$ (p is an invariant of Φ)

Proving the supporting invariant

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

invariant to prove:

$(\pi = l_2) \rightarrow x > 0$

Proof:

$x = N \wedge y = 0 \wedge N > 0 \wedge \pi = l_1 \rightarrow ((\pi = l_2) \rightarrow x > 0)$ valid

τ_1 : .... $\wedge ((x > 0 \wedge \pi' = l_2) \vee (x \leq 0 \wedge \pi' = l_4)) \wedge x' = x \wedge$ .... $\rightarrow ((\pi' = l_2) \rightarrow x' > 0)$ valid

τ_2 : .... $\wedge \pi' = l_3 \wedge$ .... $\rightarrow ((\pi' = l_2) \rightarrow x' > 0)$ valid

τ_3 : .... $\wedge \pi' = l_1 \wedge$ .... $\rightarrow ((\pi' = l_2) \rightarrow x' > 0)$ valid

τ_4 : .... $\wedge \pi' = \pi \wedge x' = x \wedge$ ...... $\rightarrow ((\pi' = l_2) \rightarrow x' > 0)$ valid

Strengthening by backwards propagation

Two approaches

- Prove that **wpc(τ , p)** is invariant — wpc(τ , p) may not be inductive

  and use it as a supporting invariant in INC-INV

- Use **p ∧ wpc(τ , p)** as the strengthening in G-INV

In both cases the verification condition for τ is guaranteed to be valid, but verification conditions for other transitions may now fail

Note: if p is invariant

then wpc(τ , p) is also invariant for all $\tau \in \mathcal{T}$

Verification rule G-INV (general invariance)

For assertions φ, p

$$
\begin{array}{ll}
\text{I1.} & \varphi \rightarrow p \\
\text{I2.} & \Theta \rightarrow \varphi \\
\text{I3.} & \varphi \wedge \rho_\tau \rightarrow \varphi' \quad \text{for all } \tau \text{ in } \mathcal{T} \\
\hline
 & \Box p \quad (\text{ p is an invariant of } \Phi \text{ })
\end{array}
$$

Backward propagation does not always work

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
      l2: x := x - 1 ;
      l3: y := y + x ;
    ]
l4:
```

invariant to prove:

$$\frac{(\pi = l_4) \rightarrow y = (N^2 - N)/2}{\varphi}$$

not preserved by τ_1 :

$((\pi = l_4) \rightarrow y = (N^2 - N)/2) \wedge \rho_{\tau 1} \rightarrow ((\pi' = l_4) \rightarrow y' = (N^2 - N)/2)$ not valid

$$\text{wpc}(\tau_1, \varphi) : \underbrace{(\pi = l_1 \wedge x = 0) \rightarrow y = (N^2 - N)/2}_{\varphi_1}$$

Backward propagation does not always work

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
      l2: x := x - 1 ;
      l3: y := y + x ;
    ]
l4:
```

invariant to prove:

$$\frac{(\pi = l_4) \rightarrow y = (N^2 - N)/2}{\varphi}$$

$\varphi_1 : (\pi = l_1 \wedge x = 0) \rightarrow y = (N^2 - N)/2$

not preserved by τ_3 :

$((\pi = l_1 \wedge x = 0) \rightarrow y = (N^2 - N)/2) \wedge \rho_{\tau 3} \rightarrow (\pi' = l_1 \wedge x = 0) \rightarrow y' = (N^2 - N)/2$

not valid

wpc(τ_1 , φ_1) : φ_2 not preserved by τ_2

wpc(τ_1 , φ_2) : φ_3 not preserved by τ_1

General schema for backwards propagation

invariant we want to prove: φ

φ	not inductive	not preserved by τ
$\varphi_1 : \varphi \wedge wpc(\tau, \varphi)$	not inductive	not preserved by τ
$\varphi_2 : \varphi_1 \wedge wpc(\tau, \varphi_1)$	not inductive	not preserved by τ
$\varphi_3 : \varphi_2 \wedge wpc(\tau, \varphi_2)$	not inductive	not preserved by τ
$\varphi_4 : \varphi_3 \wedge wpc(\tau, \varphi_3)$	not inductive	not preserved by τ
⋮		
$\varphi_n : \varphi_{n-1} \wedge wpc(\tau, \varphi_{n-1})$	inductive	

Predicate transformers

φ	assertion (predicate)	set of states	domain
Example: $x > 0$		$\{ 1, 2, 3, 4, \ldots \}$	N
		$\{ \ldots 0.0001, \ldots 0.01, \ldots \}$	R
		$\{ 1, 2 \}$	$\Sigma_{\triangleright}$

A predicate transformer is a function that maps

predicates into predicates

sets of states into sets of states

Backwards propagation expressed as a predicate transformer

Given a predicate φ (and a transition system Φ)

Conjoin it with the wpc of all transitions that are not preserved

$$\mathcal{F}(\varphi) = \varphi \wedge wpc(\tau_{i1}, \varphi) \wedge wpc(\tau_{i2}, \varphi) \wedge \ldots \wedge wpc(\tau_{in}, \varphi)$$

To prove φ invariant keep applying $\mathcal{F}$ to φ until we get a predicate that is preserved by all transitions (that is inductive)

Weakest precondition

$wpc(\tau, \varphi)$ — largest set of states from which τ leads to a φ-state

What if φ is preserved by τ ?

Weakest precondition

if $p(V) \wedge \rho_\tau(V,V') \rightarrow p(V')$ does not hold

identify the largest set of states for which it does hold

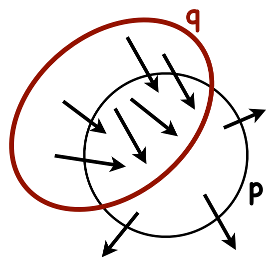
☛ find the **weakest** formula $q(V)$ such that

$$q(V) \wedge \rho_\tau(V,V') \rightarrow p(V')$$

holds for all values of V'

represented by the **weakest precondition**

$$\text{wpc}(\tau, p) : \forall V' .\ \rho_\tau(V,V') \rightarrow p(V')$$



Weakest precondition

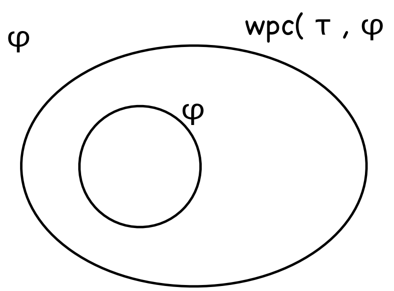
$\text{wpc}(\tau, \varphi)$ largest set of states from which τ leads to a φ-state

What if φ is preserved by τ ?

$\text{wpc}(\tau, \varphi)$ must be weaker than φ

$$\varphi \rightarrow \text{wpc}(\tau, \varphi)$$

$$\varphi \wedge \text{wpc}(\tau, \varphi) \rightarrow \varphi$$



Backwards propagation expressed as a predicate transformer

Given a predicate φ (and a transition system Φ)

Conjoin it with the wpc of all transitions ~~that are not preserved~~

$$\mathcal{F}(\varphi) = \varphi \wedge \bigwedge_{\tau \in \mathcal{T}} \text{wpc}(\tau, \varphi)$$

To prove φ invariant keep applying $\mathcal{F}$ to φ until we get a predicate that is preserved by all transitions (that is inductive)

To prove φ invariant keep applying $\mathcal{F}$ to φ until we reach a fixed point

$$\mathcal{F}(\varphi) = \varphi$$

Fixed points: examples

$f(x{:}\text{int}) = \lfloor x/2 \rfloor$ fixed point: $x = 0$

$f(0) = 0$

$f(x{:}\text{real}) = x/2$ fixed point: $x = 0$

$f(0) = 0$

Tarski's fixed point theorem (1955)

$\varphi_1 \subseteq \varphi_2 \rightarrow \mathcal{F}(\varphi_1) \subseteq \mathcal{F}(\varphi_2)$

or

$\varphi_1 \subseteq \varphi_2$ implies $\mathcal{F}(\varphi_1) \subseteq \mathcal{F}(\varphi_2)$

$\mathcal{F}(\varphi) \subseteq \varphi$

or

$\mathcal{F}(\varphi) \rightarrow \varphi$

if $\mathcal{F}(\varphi)$ is a monotone function and reductive

then $\mathcal{F}$ has a unique greatest fixed point (gfp)

that can be obtained by repeated application of $\mathcal{F}$:

$$\text{gfp}(\mathcal{F}) = \lim_{n\rightarrow\infty} \mathcal{F}^n(\text{true})$$

Fixed points: examples

f(x:int) = $\lfloor x/2 \rfloor$ fixed point: x = 0

f (0) = 0

fixed point is reached in finitely many function applications, starting from any value of x

f(x:real) = x/2 fixed point: x = 0

f (0) = 0

reaching the fixed point from any value x > 0 takes infinitely many function applications

Backwards propagation expressed as a predicate transformer

Given a predicate φ

Conjoin it with the wpc of all transitions

$$\mathcal{F}(\varphi) = \varphi \wedge \bigwedge_{\tau\in\mathcal{T}} \text{wpc}(\tau, \varphi)$$

To prove φ invariant keep applying $\mathcal{F}$ to φ until we reach a fixed point

$$\mathcal{F}(\varphi) = \varphi$$

Note: $\mathcal{F}$(true) = true

true is the greatest fixed point of $\mathcal{F}$

Backwards propagation expressed as a predicate transformer

Assertion φ is an invariant of system $\Phi : \langle V, \Theta, \mathcal{T} \rangle$ if the greatest fixed point of

$$\mathcal{F}(X) = \varphi \wedge X \wedge \bigwedge_{\tau\in\mathcal{T}} \text{wpc}(\tau, X)$$

contains Θ

Backward propagation does not always work

```
local x,y: integer where x = N ∧ y=0 ∧ N > 0
l1: while x > 0 do [
    l2: x := x - 1 ;
    l3: y := y + x ;
    ]
l4:
```

invariant to prove:

$$(\pi = l_4) \rightarrow y = (N^2 - N) / 2$$

φ

wpc(τ_1 , φ_1) : φ_2 not preserved by τ_2

wpc(τ_1 , φ_2) : φ_3 not preserved by τ_1

⋮

does not terminate