


III. SPECIFICATION AND VERIFICATION

Systems + temporal logic: state validity

- for a state formula q

$\models q$

q holds in all states
q is state-valid

Example: $\models x=1 \rightarrow x>0$

Given a system Φ

- for a state formula q

$\Phi \models q$

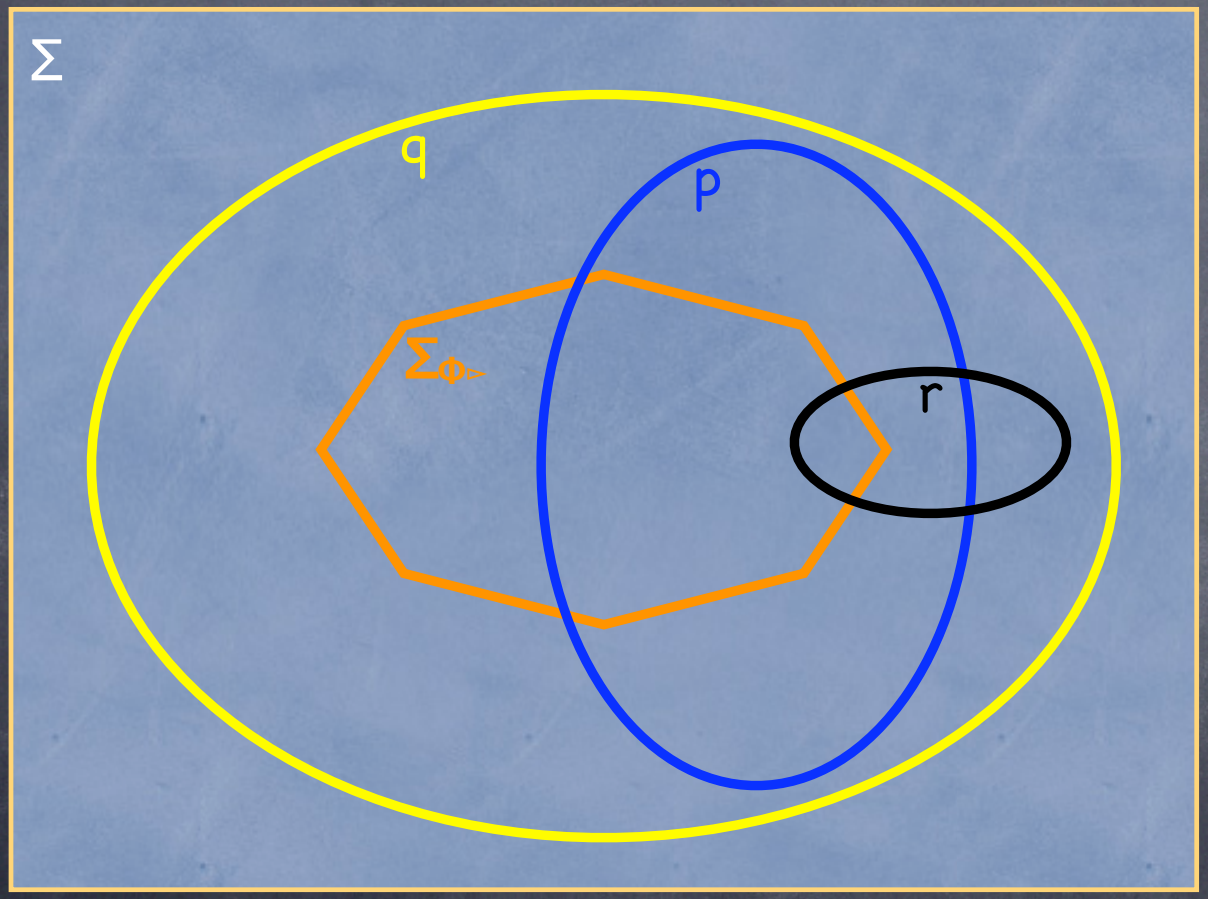
q holds in all Φ-reachable states
q is Φ-state-valid

Example: $\Phi = \langle V,\Theta,\mathcal{T},\mathcal{F}\rangle$

V: {x}
Θ: x=0
$\mathcal{T}$: {τ} with ρ_τ: $x'=x+2$

$\Phi \models x \geq 0 \wedge even(x)$

State validity



$\not\models p$

$\not\models q$

$\not\models r$

$\Phi \not\models p$

$\Phi \models q$

$\Phi \not\models r$

$\models p \rightarrow q$

$\Phi \models r \rightarrow p$

Systems + temporal logic : temporal validity

- for a temporal formula φ

$$\models \varphi$$

φ holds over all sequences states

φ is valid

Example: $\models \Box p \vee \Diamond \neg p$

Given a system Φ

- for a temporal formula φ

$$\Phi \models \varphi$$

φ holds over all computations of Φ

φ is Φ-valid

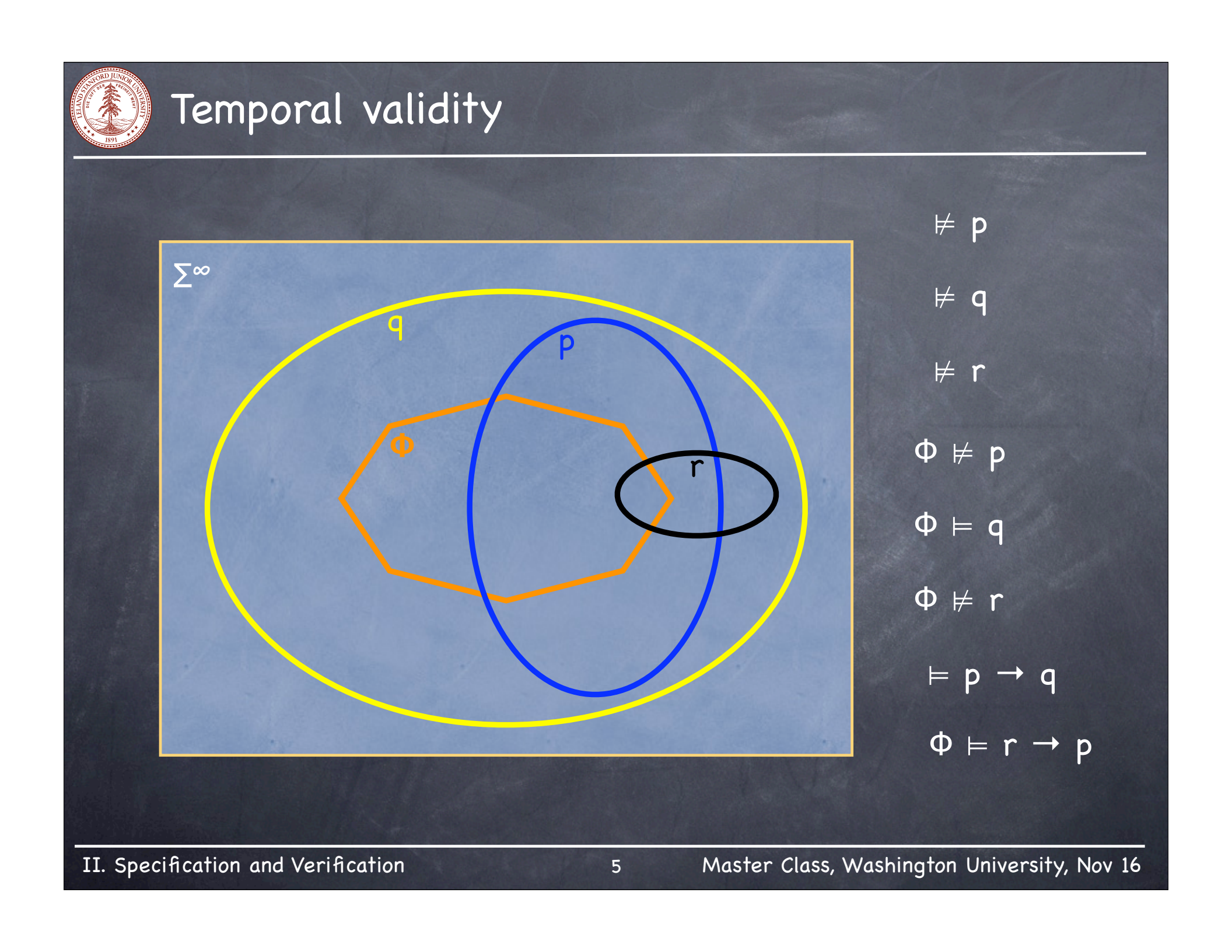
Example: $\Phi = \langle V, \Theta, \mathcal{T}, \mathcal{F} \rangle$

V: {x}

Θ: x=0

$\mathcal{T}$: {τ} with ρ_τ: $x' = x+2$

$$\Phi \models (x<6)\,\mathcal{U}\,(x=6) \wedge \Diamond\Box(x>6)$$



Temporal validity

$\not\models p$

$\not\models q$

$\not\models r$

$\Phi \not\models p$

$\Phi \models q$

$\Phi \not\models r$

$\models p \rightarrow q$

$\Phi \models r \rightarrow p$

System-validity: summary

	general	system Φ
state formula q	$\models q$ **state valid** q holds in all states $x=1 \rightarrow x>0$	$\Phi \models q$ **Φ-state valid** q holds in all Φ-reachable states
temporal formula φ	$\models \varphi$ **valid** φ holds over all sequences of states $\models \Box p \vee \Diamond \neg p$	$\Phi \models \varphi$ **Φ-valid** φ holds over all computations of Φ

System validity: summary

Note:

$\models q$ iff $\models \Box q$

$\Phi \models q$ iff $\Phi \models \Box q$

Specification of properties

- Property P is a set of sequences of states
- Property is specified by a temporal formula φ:
  for every sequence of states σ:

$$\sigma \in P \quad \text{iff} \quad \sigma \models \varphi$$

or $\mathcal{L}(\varphi) = P$

- System Φ has property P if
  for every computation σ of Φ:

$$\sigma \in P$$

or $\mathcal{L}(\Phi) \subseteq P$

Classification of properties

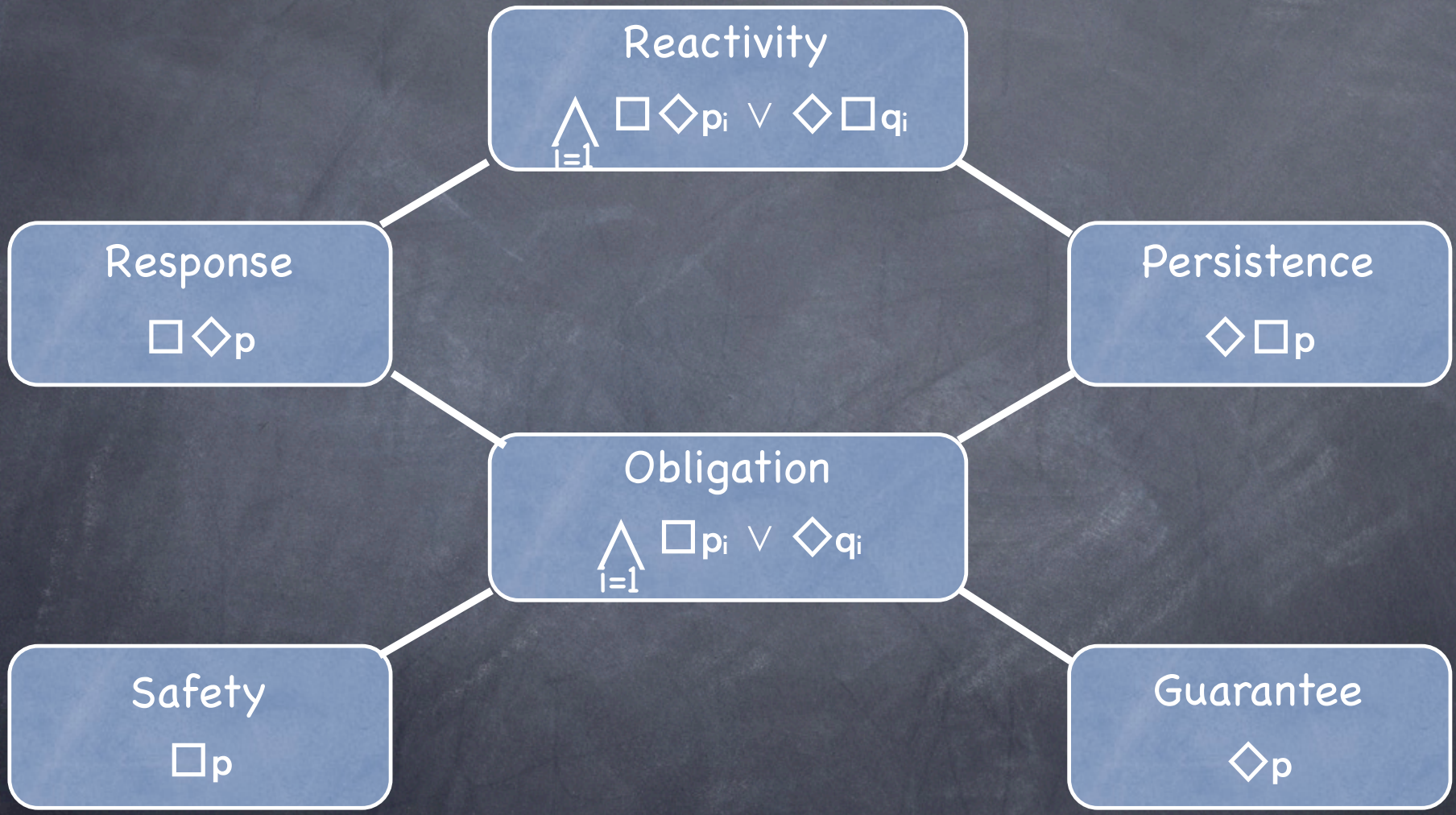
Safety

- no bad things will happen
- all finite prefixes of a computation satisfy a certain requirement
- violation can be detected in finite time
- fairness is not relevant
- proofs by induction

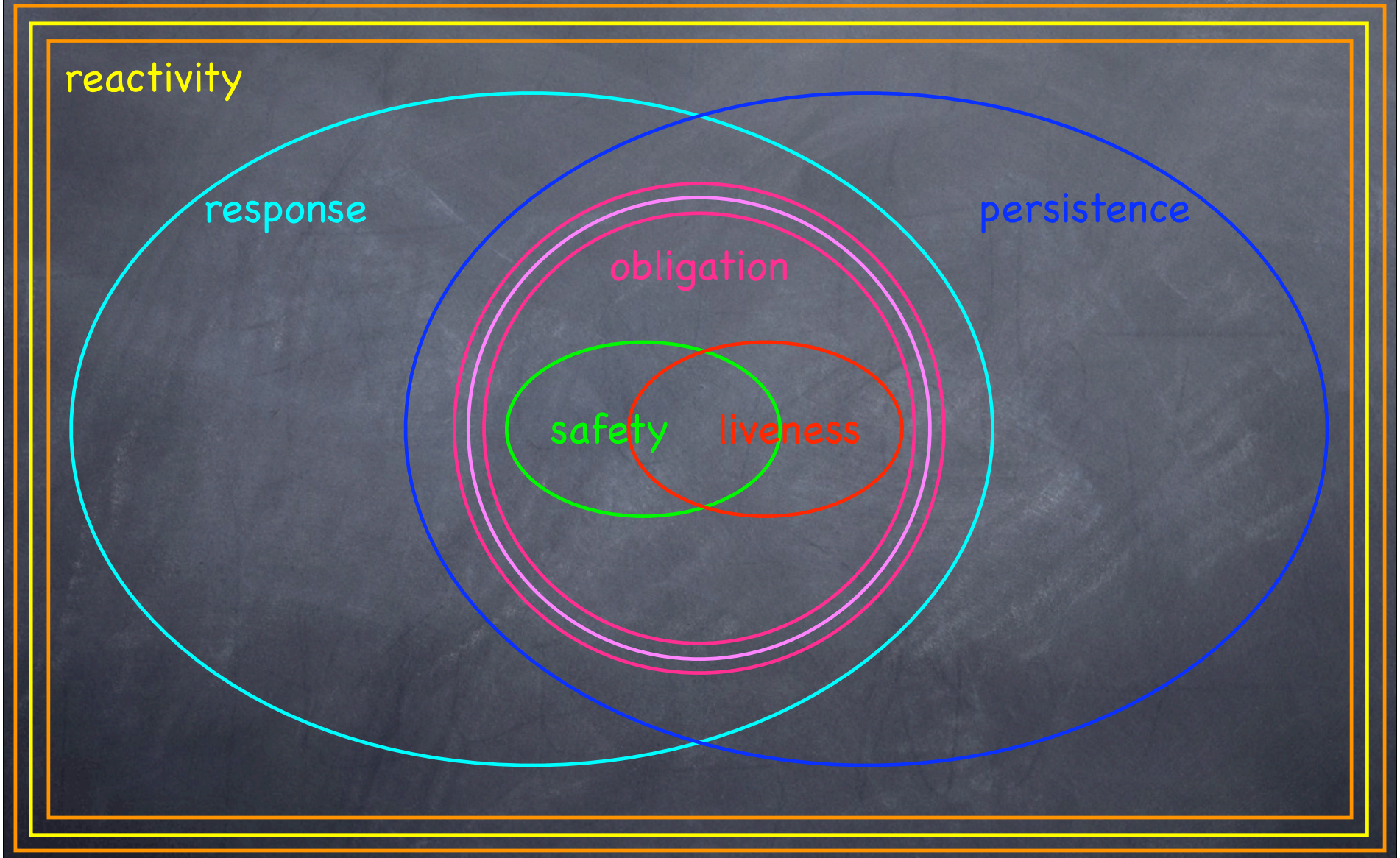
Liveness

- some good thing will happen
- violation cannot be detected in finite time
- satisfaction can be detected in finite time
- proofs use measure functions or appeal to fairness

Classification of properties



Classification of properties




III. SPECIFICATION AND VERIFICATION

Proving temporal properties

$\Phi \models \varphi$

Deductively

Algorithmically
(Model checking)
(finite-state only)

represent Φ by a temporal formula ψ and prover $\psi \rightarrow \varphi$

Temporal-logic prover

TLA

transform all to first-order logic theorems

First-order or higher-order prover

PVS,ACL2

transform to first-order verification conditions through verification rules or verification diagrams

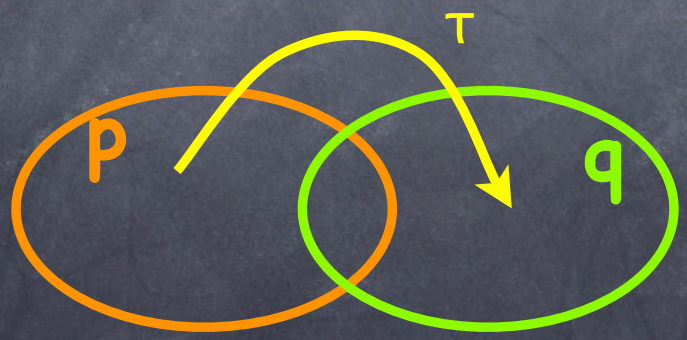
STeP

Verification condition

$$p \wedge \rho_\tau \rightarrow q'$$

Starting from a state that satisfies p, transition τ leads to a state that satisfies q

aka "Hoare triple" $\{p\}\ \tau\ \{q\}$



Verification conditions: examples

$$p \wedge \rho_\tau \rightarrow q'$$

$$\{p\}\ \tau\ \{q\}$$

$\{x>0\}\ x'=x+1\ \{x>1\}$ $\qquad$ $x>0 \wedge x'=x+1 \rightarrow x'>1$

substitute $x+1$ for x': $\quad x>0 \rightarrow (x+1) > 1$

$\{x>0\}\ x'=x+1\ \{true\}$ $\qquad$ $x>0 \wedge x'=x+1 \rightarrow true$

$\{x\geq 0\}\ x>0 \wedge x'=x-1\ \{x\geq 0\}$

$\{true\}\ x>0 \wedge x'=x-1\ \{x\geq 0\}$

Proving invariance properties

Invariant: $\Box p$ for state formula p

We want to prove $\Phi \models \Box p$

every state of every computation of Φ satisfies p

A sequence of states σ: $s_0, s_1, s_2 \ldots$

is a computation of Φ: $\langle V, \Theta, \mathcal{T}, \mathcal{F} \rangle$ if

- Initiality: $s_0 \models \Theta$
- Consecution: for each $j \geq 0$, s_{j+1} is a τ-successor of s_j, for some $\tau \in \mathcal{T}$
- Justice

Proving invariance properties

Proving $\Phi \models \Box p$

means proving that every state of every sequence of states that satisfies

- Initiality: $s_0 \models \Theta$
- Consecution: for each $j \geq 0$, s_{j+1} is a τ-successor of s_j, for some $\tau \in \mathcal{T}$

also satisfies p

Proof by induction:

Base case: $\Theta \rightarrow p$ ensures that every initial state satisfies p

Inductive step: $p \wedge \rho_\tau \rightarrow p'$ for every $\tau \in \mathcal{T}$

ensures that p is preserved by all transitions

Verification rule B-INV (basic invariance)

For assertion q

B1. $\Phi \models \Theta \rightarrow q$

B2. $\Phi \models \{q\}\ \mathcal{T}\ \{q\}$

$\Phi \models \Box q$

$\{q\}\ \mathcal{T}\ \{q\}$ stands for $\{q\}\ \tau\ \{q\}$ for all $\tau \in \mathcal{T}$

B-INV : example

Φ: to prove $\Phi \models \Box(x \geq 0)$

V: $\{x\}$

Θ: $x=0$

$\mathcal{T}$: $\{\tau_1, \tau_2\}$ with $\rho_{\tau 1}$: $x' = x+1$

$\rho_{\tau 2}$: $x>0 \wedge x' = x-1$

B1: $x=0 \rightarrow x \geq 0$ ✓

B2: $x \geq 0 \wedge x' = x+1 \rightarrow x' \geq 0$ ✓

$x \geq 0 \wedge x>0 \wedge x' = x-1 \rightarrow x' \geq 0$ ✓

B-INV : example

Φ: to prove $\Phi \models \Box(x \geq 0)$

V: $\{x,y\}$

Θ: $x=0 \wedge y=0$

$\mathcal{T}$: $\{\tau_1,\tau_2\}$ with $\rho_{\tau 1}$: $x'=x+y \wedge y'=y+1$

$\rho_{\tau 2}$: $x>0 \wedge x'=x-1$

B1: $x=0 \wedge y=0 \rightarrow x \geq 0$ ✓

B2: $x \geq 0 \wedge x'=x+y \wedge y'=y+1 \rightarrow x' \geq 0$ ×

$x \geq 0 \wedge x>0 \wedge x'=x-1 \rightarrow x' \geq 0$ ✓

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

Verification rule B-INV (basic invariance)

For assertion q

B1. $\Phi \models \Theta \rightarrow q$

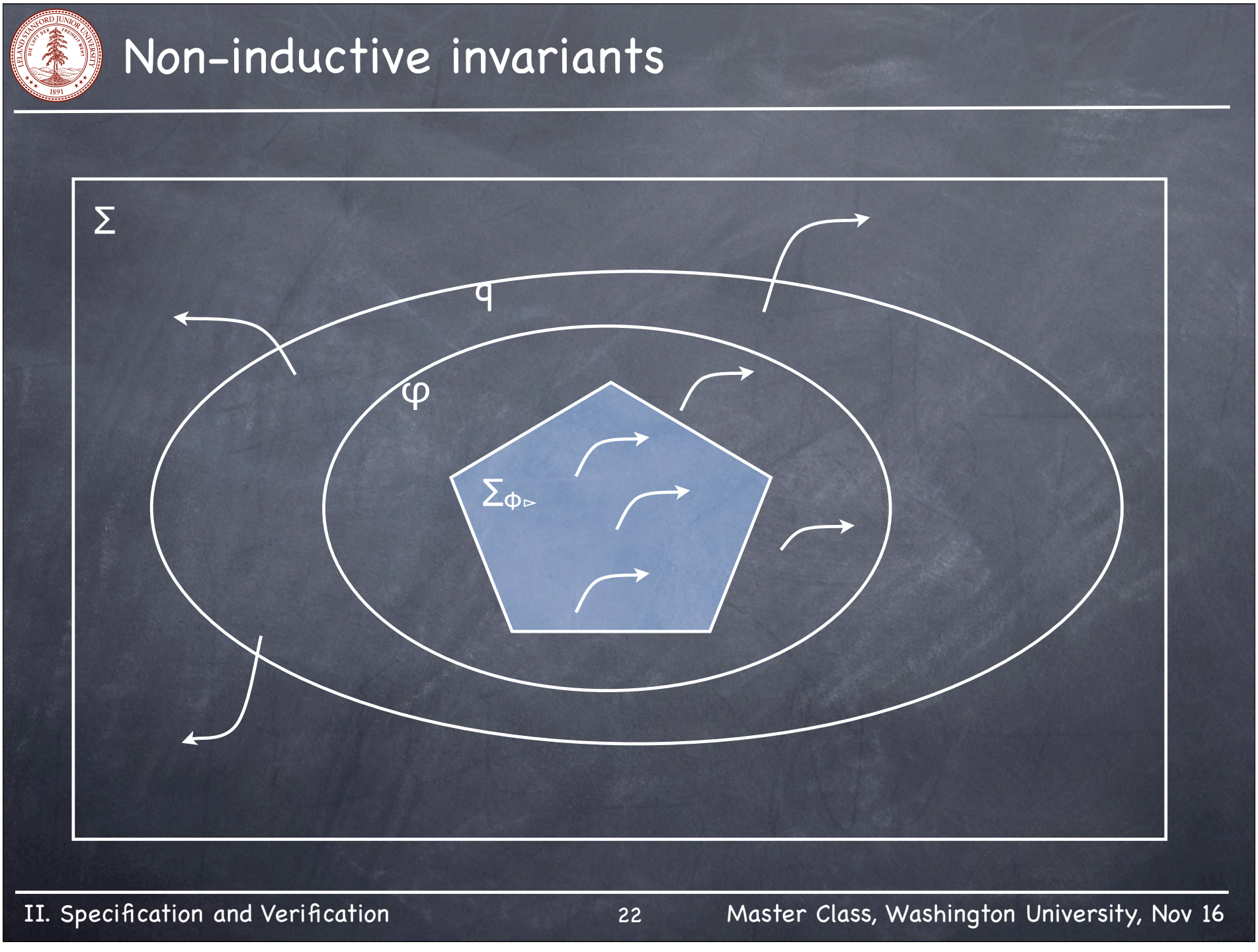
B2. $\Phi \models \{q\}\ \mathcal{T}\ \{q\}$

$\Phi \models \Box q$

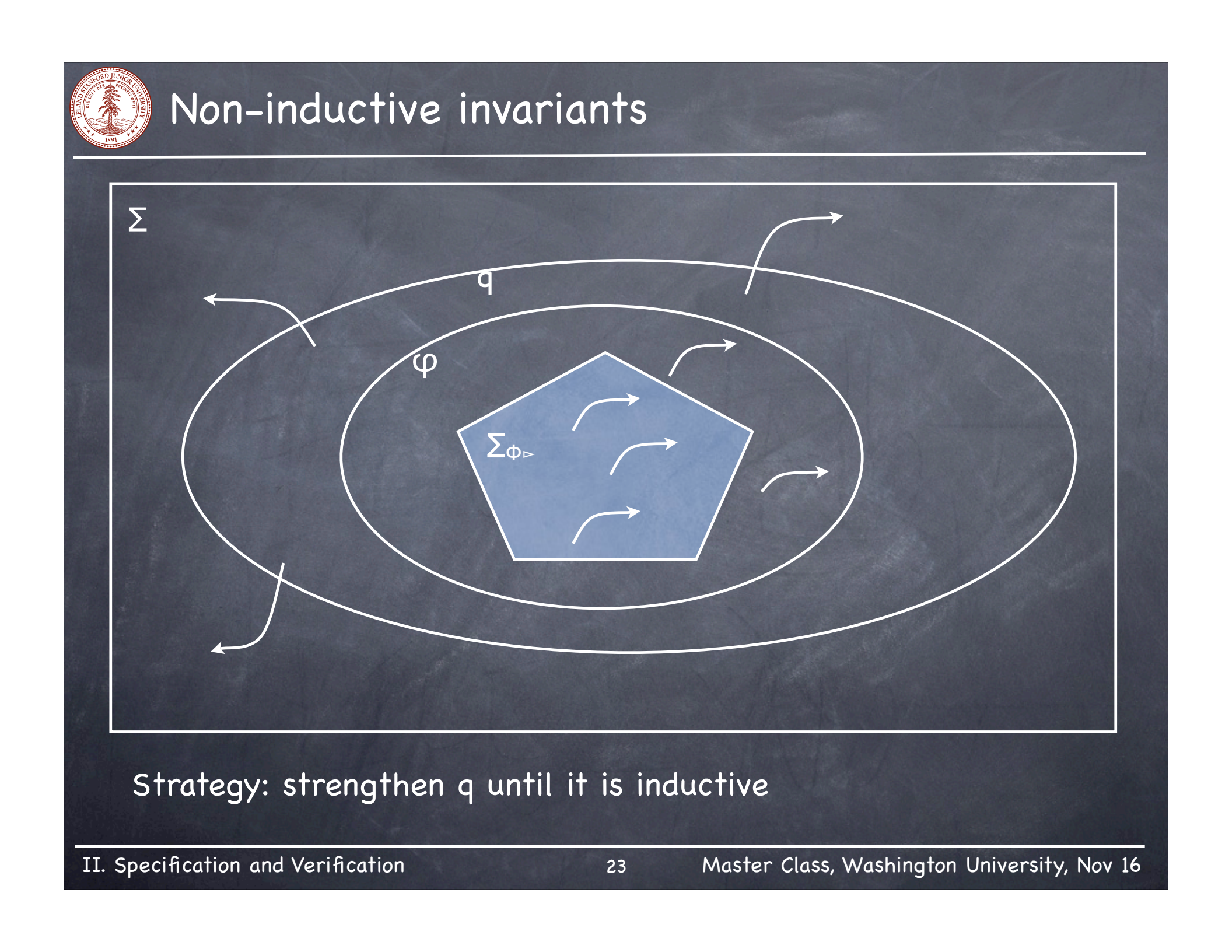
if B1 and B2 are (state) valid then q is inductive

every inductive assertion is an invariant

the converse is not true: not every invariant is inductive



Non-inductive invariants



Non-inductive invariants

Strategy: strengthen q until it is inductive

Strategy 1: Strengthening

Φ:

V: {x,y}

Θ: $x=0 \wedge y=0$

$\mathcal{T}$: $\{\tau_1,\tau_2\}$ with $\rho_{\tau 1}$: $x'=x+y \wedge y'=y+1$

$\rho_{\tau 2}$: $x>0 \wedge x'=x-1 \wedge y'=y$

to prove $\Phi \models \Box(x\geq 0)$

strengthen it to

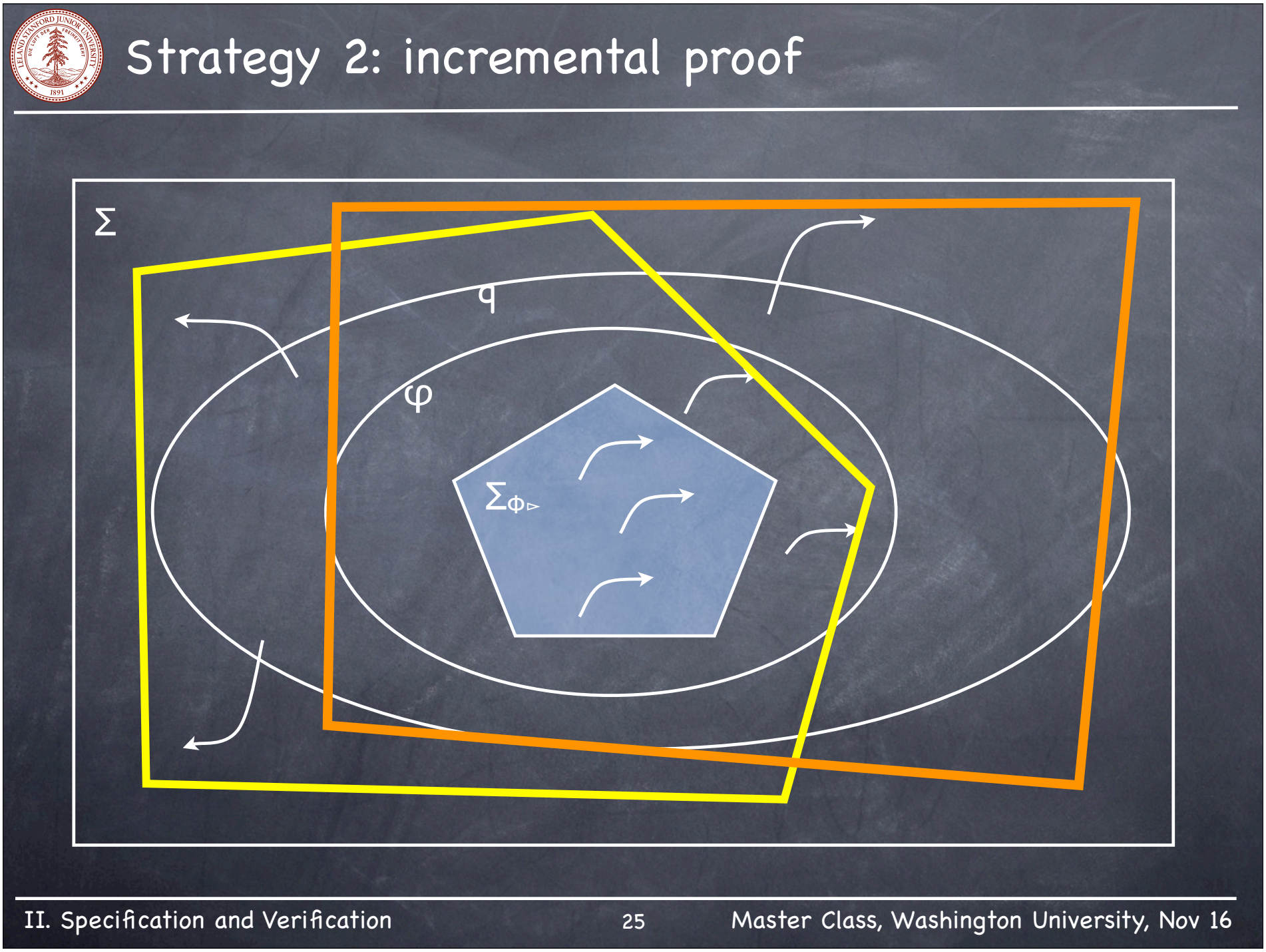
$\Phi \models \Box(x\geq 0 \wedge y\geq 0)$

B1: $x=0 \wedge y=0 \rightarrow x\geq 0 \wedge y\geq 0$ ✓

B2: $x\geq 0 \wedge y\geq 0 \wedge x'=x+y \wedge y'=y+1 \rightarrow x'\geq 0 \wedge y'\geq 0$ ✓

$x\geq 0 \wedge x>0 \wedge x'=x-1 \wedge y'=y \rightarrow x'\geq 0 \wedge y'\geq 0$ ✓

$x\geq 0 \wedge y\geq 0$ is an invariant and is inductive



Strategy 2: incremental proof

Strategy 2: Incremental Proof

Φ:

V: $\{x,y\}$

Θ: $x=0 \wedge y=0$

$\mathcal{T}$: $\{\tau_1,\tau_2\}$ with $\rho_{\tau 1}$: $x'=x+y \wedge y'=y+1$

$\rho_{\tau 2}$: $x>0 \wedge x'=x-1 \wedge y'=y$

to prove $\Phi \models \Box(x\geq 0)$

first prove $\Phi \models \Box(y\geq 0)$

and then prove $\Phi \models \Box(x\geq 0)$ relative to $\Box(y\geq 0)$

B1: $x=0 \wedge y=0 \rightarrow x\geq 0$ ✓

B2: $x\geq 0 \wedge y\geq 0 \wedge x'=x+y \wedge y'=y+1 \rightarrow x'\geq 0$ ✓

$x\geq 0 \wedge x>0 \wedge x'=x-1 \wedge y'=y \rightarrow x'\geq 0$ ✓

$x\geq 0$ is an invariant and is inductive relative to $y\geq 0$