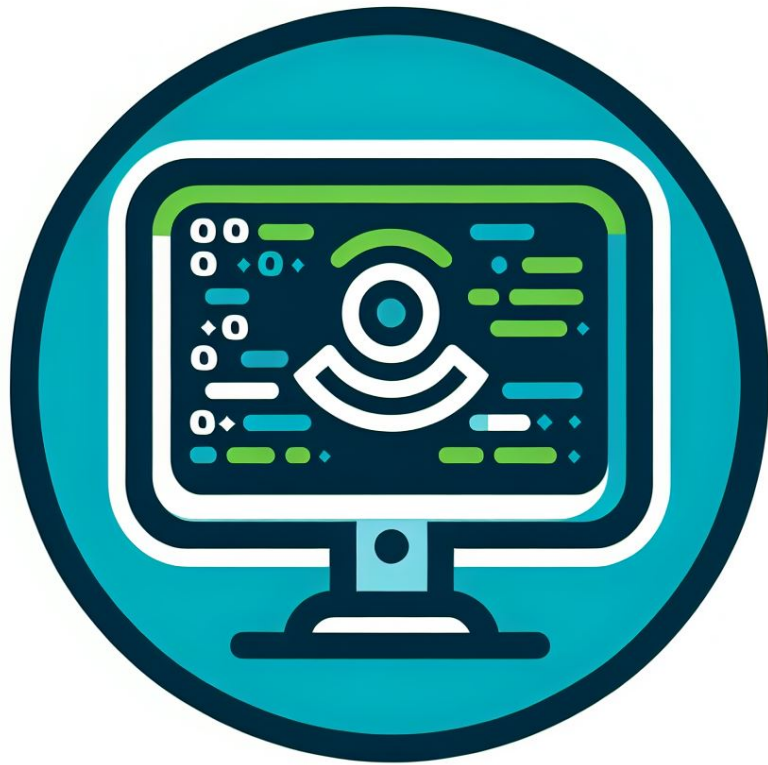




PSC 2024/25 (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni

<http://www.di.unipi.it/~bruni/>

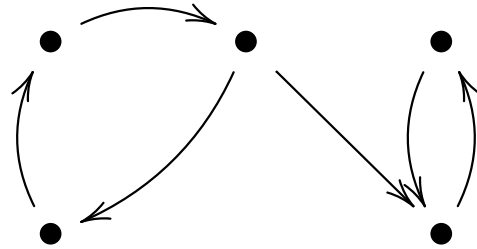
[http://didawiki.di.unipi.it/doku.php/
magistraleinformatica/psc/start](http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/start)

22b - Mu-calculus

μ -calculus

mu-calculus

models



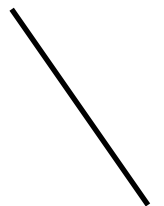
syntax

ψ	$::=$	$\mathbf{tt} \mid \mathbf{ff} \mid \psi_0 \wedge \psi_1 \mid \psi_0 \vee \psi_1$	classical ops
	$ $	$p \mid \neg p$	atomic propositions
	$ $	$\Diamond \psi$	there is a next state where ψ holds
	$ $	$\Box \psi$	ψ holds at every next state
	$ $	x	predicate variable, for recursive def
	$ $	$\mu x. \psi$	LEAST FIXPOINT of $x =_{\min} \psi$
	$ $	$\nu x. \psi$	GREATEST FIXPOINT of $x =_{\max} \psi$

mu-calculus: semantics

$$G = (V, \rightarrow)$$

$[[\psi]]_\rho$ set of nodes where ψ holds


$$\rho : P \cup X \rightarrow \wp(V)$$

assignment

$(\wp(V), \subseteq)$ is a complete lattice

for monotone functions: least / greatest fixpoint exist
for this reason negation is not present in the syntax
the formulas we consider: *positive normal form*

otherwise:

even number of negations before each variable occurrence

Positive normal form

$$\neg \Diamond \psi \equiv \Box \neg \psi$$

$$\neg \Box \psi \equiv \Diamond \neg \psi$$

$$\neg \mu x. \psi \equiv \nu x. \neg \psi[\neg^x / x]$$

$$\neg \nu x. \psi \equiv \mu x. \neg \psi[\neg^x / x]$$

$$\neg \neg \psi \equiv \psi$$

plus usual De Morgan's laws

mu-calculus: semantics

$$\llbracket \cdot \rrbracket : \mathcal{F} \rightarrow (P \cup X \rightarrow \wp(V)) \rightarrow \wp(V)$$

defined by structural induction

$$\llbracket \mathbf{tt} \rrbracket \rho \triangleq V$$

$$\llbracket \psi_0 \wedge \psi_1 \rrbracket \rho \triangleq \llbracket \psi_0 \rrbracket \rho \cap \llbracket \psi_1 \rrbracket \rho$$

$$\llbracket \mathbf{ff} \rrbracket \rho \triangleq \emptyset$$

$$\llbracket \psi_0 \vee \psi_1 \rrbracket \rho \triangleq \llbracket \psi_0 \rrbracket \rho \cup \llbracket \psi_1 \rrbracket \rho$$

$$\llbracket p \rrbracket \rho \triangleq \rho(p)$$

$$\llbracket \Diamond \psi \rrbracket \rho \triangleq \{v \mid \exists w \in \llbracket \psi \rrbracket \rho. v \rightarrow w\}$$

$$\llbracket \neg p \rrbracket \rho \triangleq V \setminus \rho(p)$$

$$\llbracket \Box \psi \rrbracket \rho \triangleq \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \llbracket \psi \rrbracket \rho\}$$

$$\llbracket x \rrbracket \rho \triangleq \rho(x)$$

$$\llbracket \mu x. \psi \rrbracket \rho \triangleq \text{fix } \lambda S. \llbracket \psi \rrbracket \rho [^S / x]$$

$$\llbracket \nu x. \psi \rrbracket \rho \triangleq \text{FIX } \lambda S. \llbracket \psi \rrbracket \rho [^S / x]$$

mu-calculus: fixpoint

V finite

$f : \wp(V) \rightarrow \wp(V)$ monotone (hence continuous)

we can compute the least fixpoint by

$$\text{fix } f = \bigcup_{n \in \mathbb{N}} f^n(\emptyset)$$

we can compute the greatest fixpoint by

$$\text{FIX } f = \bigcap_{n \in \mathbb{N}} f^n(V)$$

Examples

$$\begin{aligned} \llbracket \Diamond \mathbf{tt} \rrbracket \rho &\triangleq \{v \mid \exists w \in \llbracket \mathbf{tt} \rrbracket \rho. v \rightarrow w\} \\ &= \{v \mid \exists w \in V. v \rightarrow w\} \end{aligned}$$

$\Diamond \mathbf{tt}$

non deadlocked states

$$\begin{aligned} \llbracket \Box \mathbf{ff} \rrbracket \rho &\triangleq \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \llbracket \mathbf{ff} \rrbracket \rho\} \\ &= \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \emptyset\} \\ &= \{v \mid v \nrightarrow\} \end{aligned}$$

$\Box \mathbf{ff}$

deadlocks

Examples

$$\begin{aligned} \llbracket \Diamond \mathbf{ff} \rrbracket \rho &\triangleq \{v \mid \exists w \in \llbracket \mathbf{ff} \rrbracket \rho. v \rightarrow w\} \\ &= \{v \mid \exists w \in \emptyset. v \rightarrow w\} \\ &= \emptyset \end{aligned}$$

$\Diamond \mathbf{ff}$
false

$$\begin{aligned} \llbracket \Box \mathbf{tt} \rrbracket \rho &\triangleq \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \llbracket \mathbf{tt} \rrbracket \rho\} \\ &= \{v \mid \forall w. v \rightarrow w \Rightarrow w \in V\} \\ &= V \end{aligned}$$

$\Box \mathbf{tt}$
true

Examples

$$\begin{aligned} \llbracket \mu x. x \rrbracket \rho &\triangleq \text{fix } \lambda S. \llbracket x \rrbracket \rho [^S / _x] \\ &= \text{fix } \lambda S. S \\ &= \emptyset \end{aligned}$$

$\mu x. x$

false

$$\begin{aligned} \llbracket \nu x. x \rrbracket \rho &\triangleq \text{FIX } \lambda S. \llbracket x \rrbracket \rho [^S / _x] \\ &= \text{FIX } \lambda S. S \\ &= V \end{aligned}$$

$\nu x. x$

true

Examples

$$\begin{aligned} \llbracket \mu x. \Diamond x \rrbracket \rho &\triangleq \text{fix } \lambda S. \llbracket \Diamond x \rrbracket \rho [^S / x] \\ &= \text{fix } \lambda S. \{v \mid \exists w \in \llbracket x \rrbracket \rho [^S / x]. v \rightarrow w\} \\ &= \text{fix } \lambda S. \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = \emptyset$$

$$\begin{aligned} S_1 &= \{v \mid \exists w \in S_0. v \rightarrow w\} \\ &= \{v \mid \exists w \in \emptyset. v \rightarrow w\} \\ &= \emptyset \end{aligned}$$

$\mu x. \Diamond x$

false

Examples

how to represent?

EO ψ $\Diamond\psi$

AO ψ $\Box\psi$

EF p

$p \vee \dots$

$p \vee \Diamond(p \vee \dots)$

$p \vee \Diamond(p \vee \Diamond(p \vee \dots))$

$x = p \vee \Diamond x$

$\mu x. p \vee \Diamond x$

$\nu x. p \vee \Diamond x$

?

EF p ?

Example

$$\begin{aligned} \llbracket \nu x. p \vee \Diamond x \rrbracket \rho &\triangleq FIX \ \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \llbracket p \rrbracket \rho[S/x] \cup \llbracket \Diamond x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \rho(p) \cup \{v \mid \exists w \in \llbracket x \rrbracket \rho[S/x]. v \rightarrow w\} \\ &= FIX \ \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = V$$

$$\begin{aligned} S_1 &= \rho(p) \cup \{v \mid \exists w \in S_0. v \rightarrow w\} \\ &= \rho(p) \cup \{v \mid \exists w \in V. v \rightarrow w\} \\ &= \rho(p) \cup \{v \text{ can move}\} \end{aligned}$$

EF p ?

Example

$$\begin{aligned} \llbracket \nu x. p \vee \Diamond x \rrbracket \rho &\triangleq FIX \ \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \llbracket p \rrbracket \rho[S/x] \cup \llbracket \Diamond x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \rho(p) \cup \{v \mid \exists w \in \llbracket x \rrbracket \rho[S/x]. v \rightarrow w\} \\ &= FIX \ \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = V$$

$$S_1 = \rho(p) \cup \{v \text{ can move}\}$$

$$S_2 = \rho(p) \cup \{v \mid \exists w \in S_1. v \rightarrow w\}$$

$$= \rho(p) \cup \{v \mid \exists w \in \rho(p). v \rightarrow w\} \cup \{v \text{ can make 2 moves}\}$$

EF p ?

Examples

$$\begin{aligned} \llbracket \nu x. p \vee \Diamond x \rrbracket \rho &\triangleq \text{FIX } \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= \text{FIX } \lambda S. \llbracket p \rrbracket \rho[S/x] \cup \llbracket \Diamond x \rrbracket \rho[S/x] \\ &= \text{FIX } \lambda S. \rho(p) \cup \{v \mid \exists w \in \llbracket x \rrbracket \rho[S/x]. v \rightarrow w\} \\ &= \text{FIX } \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = V$$

$$S_1 = \rho(p) \cup \{v \text{ can move}\}$$

$$S_2 = \rho(p) \cup \{v \mid \exists w \in \rho(p). v \rightarrow w\} \cup \{v \text{ can make 2 moves}\}$$

$$\begin{aligned} S_n &= \{v \text{ can reach a state in } \rho(p) \text{ in less than } n \text{ moves}\} \\ &\quad \cup \{v \text{ can make } n \text{ moves}\} \end{aligned}$$

EF p ?

Example

$$\begin{aligned} \llbracket \nu x. p \vee \Diamond x \rrbracket \rho &\triangleq \text{FIX } \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= \text{FIX } \lambda S. \llbracket p \rrbracket \rho[S/x] \cup \llbracket \Diamond x \rrbracket \rho[S/x] \\ &= \text{FIX } \lambda S. \rho(p) \cup \{v \mid \exists w \in \llbracket x \rrbracket \rho[S/x]. v \rightarrow w\} \\ &= \text{FIX } \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$\begin{aligned} S_n &= \{v \text{ can reach a state in } \rho(p) \text{ in less than } n \text{ moves}\} \\ &\cup \{v \text{ can make } n \text{ moves}\} \end{aligned}$$

$$\bigcap_{n \in \mathbb{N}} S_n = \{v \text{ can reach a state in } \rho(p) \text{ or has an infinite path}\}$$

EF p ?

Example

$$\begin{aligned} \llbracket \mu x. p \vee \Diamond x \rrbracket \rho &\triangleq \text{fix } \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= \text{fix } \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = \emptyset$$

$$\begin{aligned} S_1 &= \rho(p) \cup \{v \mid \exists w \in S_0. v \rightarrow w\} \\ &= \rho(p) \cup \{v \mid \exists w \in \emptyset. v \rightarrow w\} \\ &= \rho(p) \end{aligned}$$

EF p ?

Example

$$\begin{aligned} \llbracket \mu x. p \vee \Diamond x \rrbracket \rho &\triangleq \text{fix } \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= \text{fix } \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = \emptyset$$

$$S_1 = \rho(p)$$

$$S_2 = \rho(p) \cup \{v \mid \exists w \in S_1. v \rightarrow w\}$$

$$= \rho(p) \cup \{v \mid \exists w \in \rho(p). v \rightarrow w\}$$

$$= \{v \text{ can reach a state in } \rho(p) \text{ in less than 2 moves}\}$$

EF p ?

Example

$$\begin{aligned} \llbracket \mu x. p \vee \Diamond x \rrbracket \rho &\triangleq \text{fix } \lambda S. \llbracket p \vee \Diamond x \rrbracket \rho[S/x] \\ &= \text{fix } \lambda S. \rho(p) \cup \{v \mid \exists w \in S. v \rightarrow w\} \end{aligned}$$

$$S_0 = \emptyset$$

$$S_1 = \rho(p)$$

$$S_2 = \{v \text{ can reach a state in } \rho(p) \text{ in less than 2 moves}\}$$

$$S_n = \{v \text{ can reach a state in } \rho(p) \text{ in less than } n \text{ moves}\}$$

$$\bigcup_{n \in \mathbb{N}} S_n = \{v \text{ can reach a state in } \rho(p)\}$$

$\mu x. p \vee \Diamond x$

EF p

Example

which formula for
“*some deadlock is reachable*”?

$\Box \mathbf{ff}$

deadlocks

$\mu x. \Box \mathbf{ff} \vee \Diamond x$

$\mu x. p \vee \Diamond x$

$\text{EF } p$

which formula for
“*deadlock free*”?

$$\begin{aligned}\neg(\mu x. \Box \mathbf{ff} \vee \Diamond x) &= \nu x. \neg(\Box \mathbf{ff} \vee \Diamond \neg x) \\ &= \nu x. \neg(\Box \mathbf{ff}) \wedge \neg(\Diamond \neg x) \\ &= \nu x. \Diamond \mathbf{tt} \wedge \Box x\end{aligned}$$

Example

$$\begin{aligned} \llbracket \nu x. p \wedge \Box x \rrbracket \rho &\triangleq FIX \ \lambda S. \llbracket p \wedge \Box x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \llbracket p \rrbracket \rho[S/x] \cap \llbracket \Box x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \llbracket x \rrbracket \rho[S/x]\} \\ &= FIX \ \lambda S. \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in S\} \end{aligned}$$

$$S_0 = V$$

$$\begin{aligned} S_1 &= \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in S_0\} \\ &= \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in V\} \\ &= \rho(p) \cap V \\ &= \rho(p) \end{aligned}$$

Example

$$\begin{aligned} \llbracket \nu x. p \wedge \Box x \rrbracket \rho &\triangleq FIX \ \lambda S. \llbracket p \wedge \Box x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \llbracket p \rrbracket \rho[S/x] \cap \llbracket \Box x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \llbracket x \rrbracket \rho[S/x]\} \\ &= FIX \ \lambda S. \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in S\} \end{aligned}$$

$$S_0 = V$$

$$S_1 = \rho(p)$$

$$\begin{aligned} S_2 &= \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in S_1\} \\ &= \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \rho(p)\} \\ &= \{v \text{ s.t. all nodes reachable in less than 2 moves are in } \rho(p)\} \end{aligned}$$

Example

$$\begin{aligned} \llbracket \nu x. p \wedge \Box x \rrbracket \rho &\triangleq FIX \ \lambda S. \llbracket p \wedge \Box x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \llbracket p \rrbracket \rho[S/x] \cap \llbracket \Box x \rrbracket \rho[S/x] \\ &= FIX \ \lambda S. \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in \llbracket x \rrbracket \rho[S/x]\} \\ &= FIX \ \lambda S. \rho(p) \cap \{v \mid \forall w. v \rightarrow w \Rightarrow w \in S\} \end{aligned}$$

$$S_0 = V$$

$$S_1 = \rho(p)$$

$$\nu x. p \wedge \Box x$$

$$AG \ p$$

$$S_2 = \{v \text{ s.t. all nodes reachable in less than 2 moves are in } \rho(p)\}$$

$$S_n = \{v \text{ s.t. all nodes reachable in less than } n \text{ moves are in } \rho(p)\}$$

$$\bigcap_{n \in \mathbb{N}} S_n = \{v \text{ can only reach states in } \rho(p)\}$$

Invariants & possibly

Invariants $Inv(\psi) \triangleq \nu x. \psi \wedge \Box x$

Possibly $Pos(\psi) \triangleq \mu x. \psi \vee \Diamond x$

Example

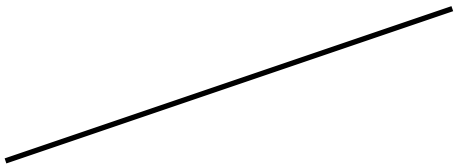
which temporal formula?

$$\mu x. q \vee (p \wedge \Diamond x)$$

$$E(p \text{ U } q) \quad (\text{CTL})$$

$$\mu x. q \vee (p \wedge \Diamond x \wedge \Box x)$$

$$A(p \text{ U } q) \quad (\text{LTL / CTL})$$

$$\nu x. \underbrace{\mu y. (p \wedge \Diamond x) \vee \Diamond y}$$


$$E \text{ G F } p \quad (\text{CTL}^*)$$

after a finite number of steps you reach a state where

1) p holds

2) there is a next step where the property holds recursively

Alternation depth

Fixed points *alternate* if a least fixed point influences the greatest fixed point, and vice-versa.

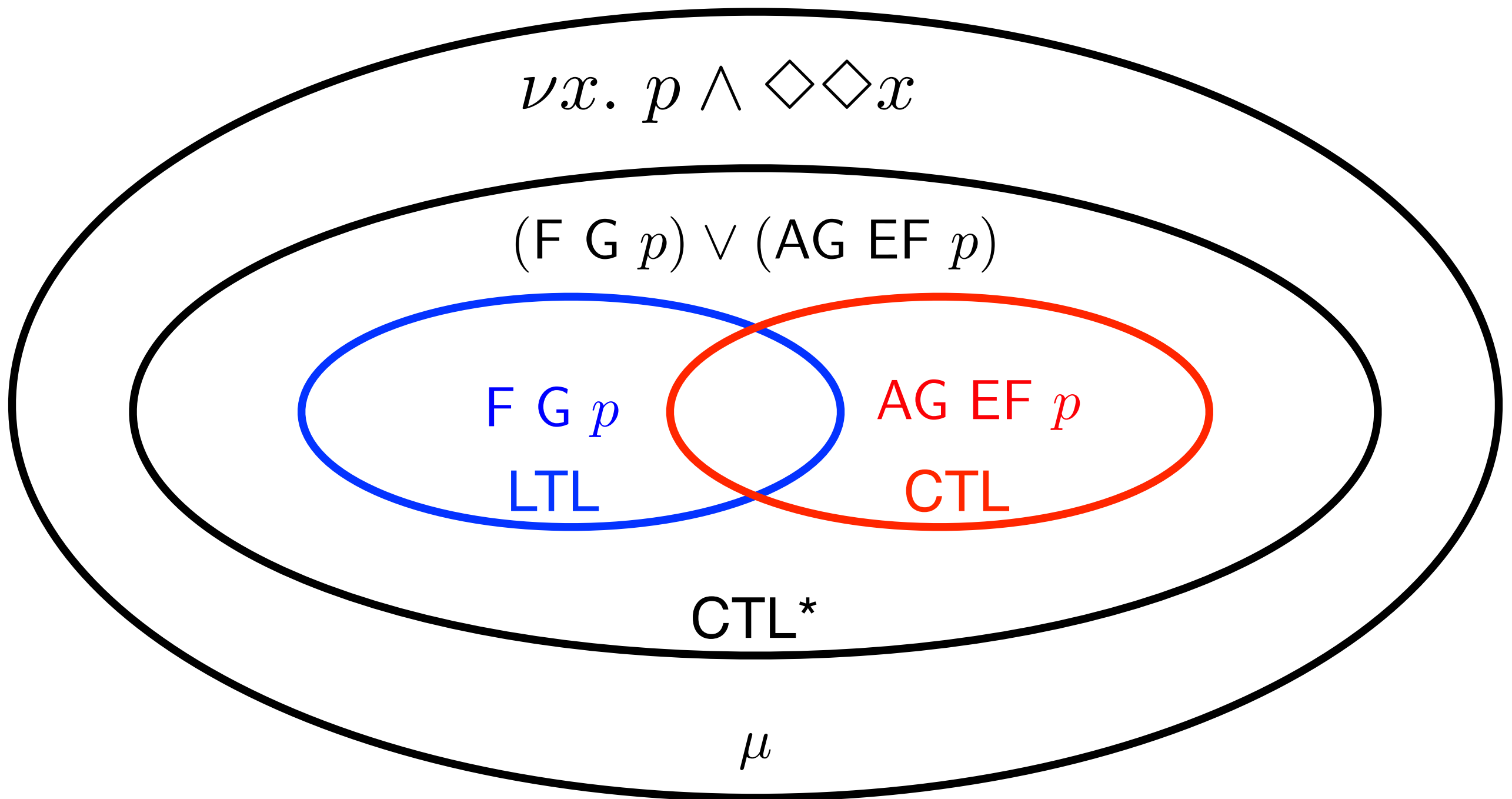
The *alternation depth* counts the number of alternations.

The alternation hierarchy of the μ -calculus is strict: strictly more properties are expressible as the alternation depth increases.

CTL can be encoded in μ -calculus with alternation depth 1

CTL* and LTL can be encoded in μ -calculus with alternation depth at most 2

Expressiveness



mu-calculus with labels

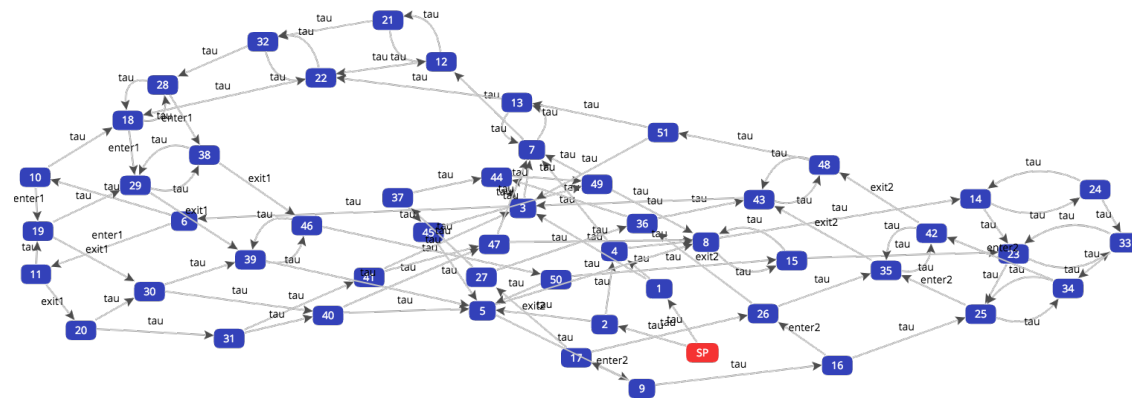
$$\psi ::= \dots$$

|

|

$\diamond_L \psi$
 $\square_L \psi$

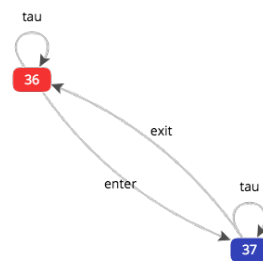
Space reduction



?
 $\models \psi$

identify
bisimilar
states

$\Leftrightarrow$



?
 $\models \psi$