

Computer-Aided Reasoning for Software

CSE 507 Finite Model Finding

courses.cs.washington.edu/courses/cse507/17wi/

Emina Torlak

emina@cs.washington.edu

Today

Last lecture

- The DPPL(T) framework for deciding quantifier-free SMT formulas

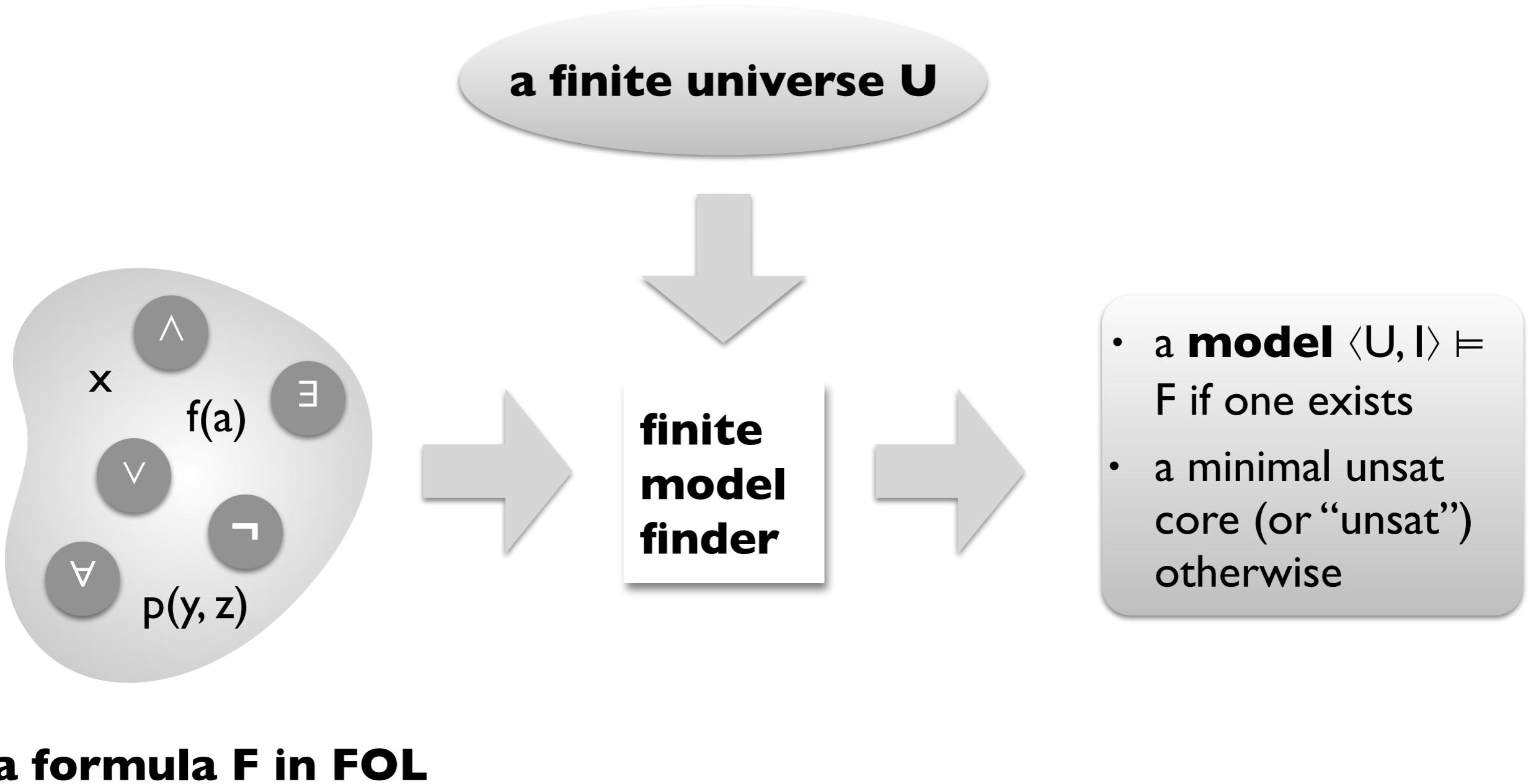
Today

- Finite model finding for quantified FOL and beyond

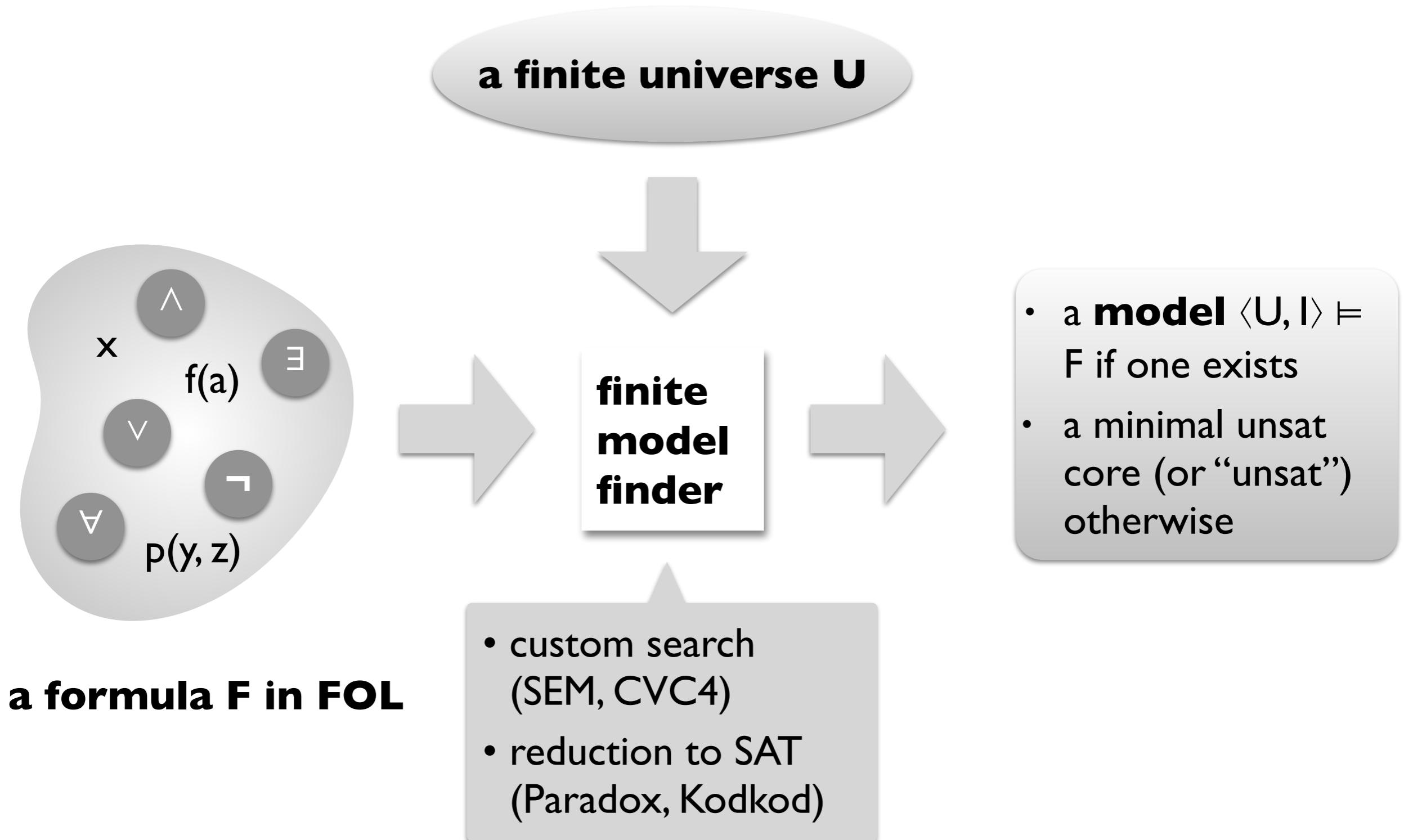
Reminders

- HWI is due tonight!

Finite model finding



Finite model finding



Some applications of finite model finding

Proving theorems in finite algebras (Finder, SEM, MACE)

Some applications of finite model finding

Proving theorems in finite algebras (Finder, SEM, MACE)



Checking lightweight formal specifications (Alloy, ProB, ExUML)



Some applications of finite model finding

Proving theorems in finite algebras (Finder, SEM, MACE)



Checking lightweight formal specifications (Alloy, ProB, ExUML)



Counterexamples to tentative theorems in interactive proof assistants (Nitpick/Isabelle)

Some applications of finite model finding

Proving theorems in finite algebras (Finder, SEM, MACE)



Checking lightweight formal specifications (Alloy, ProB, ExUML)



Counterexamples to tentative theorems in interactive proof assistants (Nitpick/Isabelle)

TACO

MemSAT

Bounded verification of code and memory models (Forge, Miniatur, TACO, MemSAT)

FORGE

Some applications of finite model finding

Proving theorems in finite algebras (Finder, SEM, MACE)



Checking lightweight formal specifications (Alloy, ProB, ExUML)



Counterexamples to tentative theorems in interactive proof assistants (Nitpick/Isabelle)



Bounded verification of code and memory models (Forge, Miniatur, TACO, MemSAT)



Declarative configuration and execution (ConfigAssure, Margrave, Squander, PBnJ)



Some applications of finite model finding

Checking lightweight formal specifications
(Alloy, ProB, ExUML)

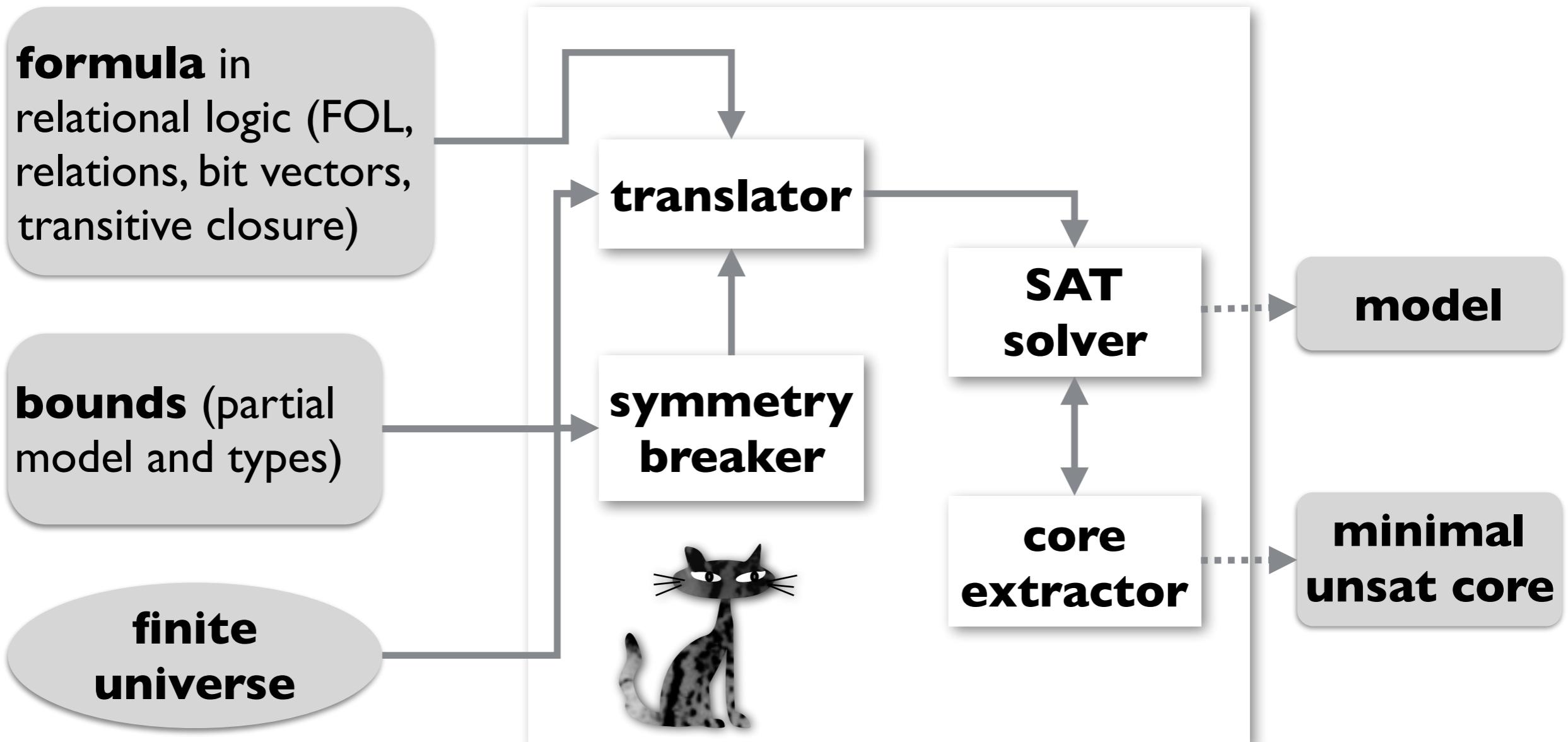
Counterexamples to tentative theorems in
interactive proof assistants (Nitpick/Isabelle)

Bounded verification of code and memory
models (Forge, Miniatur, TACO, MemSAT)

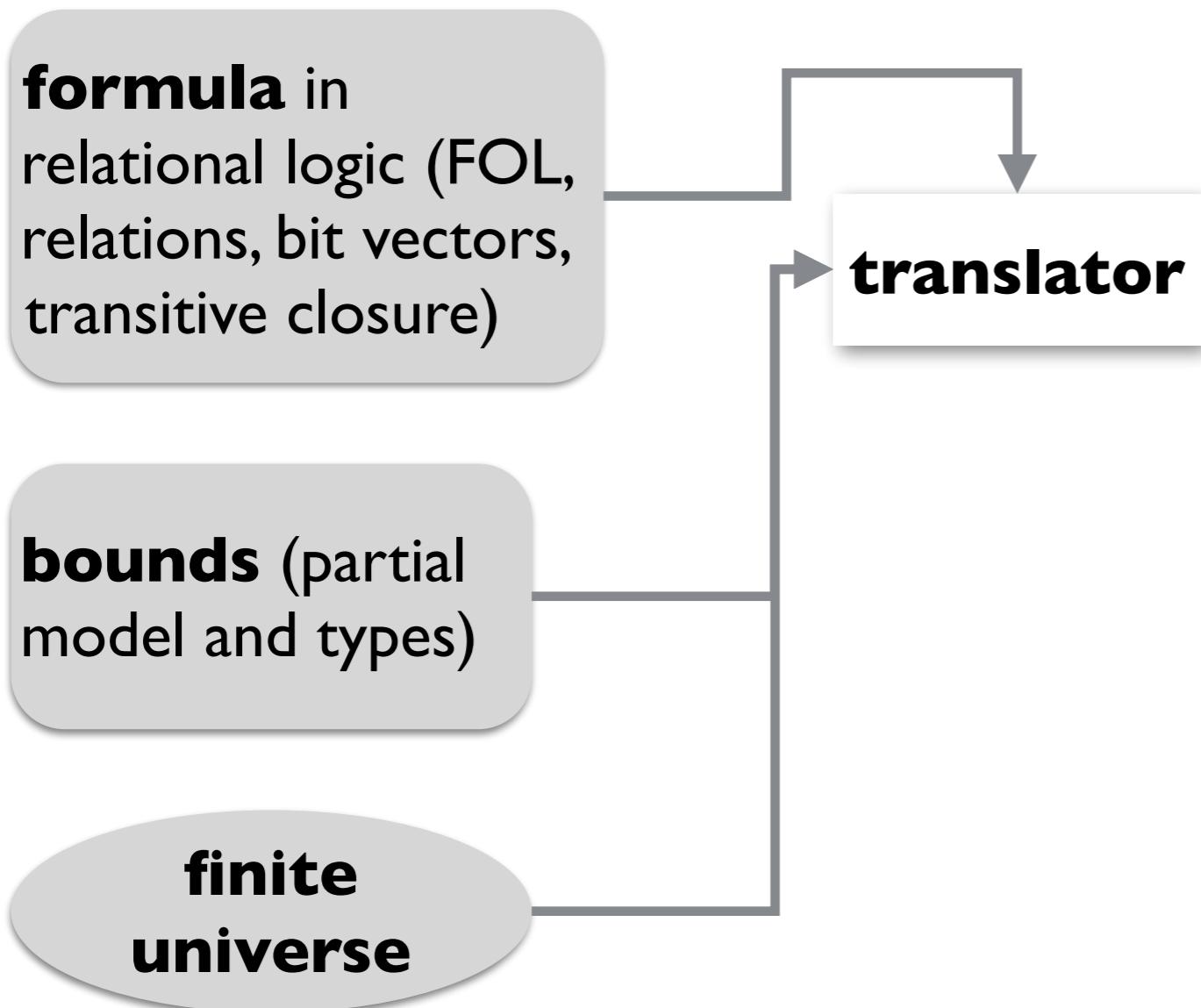
Declarative configuration and execution
(ConfigAssure, Margrave, Squander, PBnJ)



Overview of Kodkod



Overview of Kodkod



Relational logic by example

**a minimalistic
formal specification
of a filesystem**

Relational logic by example

$\text{Root} \subseteq \text{Dir}$

- The root of a filesystem hierarchy is a directory.

Relational logic by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

- The root of a filesystem hierarchy is a directory.
- Directories may contain files or directories.

Relational logic by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

- The root of a filesystem hierarchy is a directory.
- Directories may contain files or directories.
- All directories and files are reachable from the root.

Relational logic by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\text{*contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.^{\wedge}\text{contents})$

- The root of a filesystem hierarchy is a directory.
- Directories may contain files or directories.
- All directories and files are reachable from the root.
- The contents relation is acyclic.

Bounded relational logic by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.*\text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.^{\wedge}\text{contents})$

{ **R**, **D₁**, **D₂**, **F₁**, **F₂** }



Finite universe of interpretation.

Bounded relational logic by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\text{*contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.^{\wedge}\text{contents})$

{ **R**, **D₁**, **D₂**, **F₁**, **F₂** }

Finite universe of interpretation.

{⟨R⟩} ⊆ Root ⊆ {⟨R⟩}

{ } ⊆ Dir ⊆ {⟨R⟩, ⟨D₁⟩, ⟨D₂⟩}

{ } ⊆ File ⊆ {⟨F₁⟩, ⟨F₂⟩}

{ } ⊆ contents ⊆ {R, D₁, D₂} × {R, D₁, D₂, F₁, F₂}

Bounds for each relation:

- Tuples it *must* contain (partial model).
- Tuples it *may* contain (type).

Bounded relational logic by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.*\text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.^{\wedge}\text{contents})$

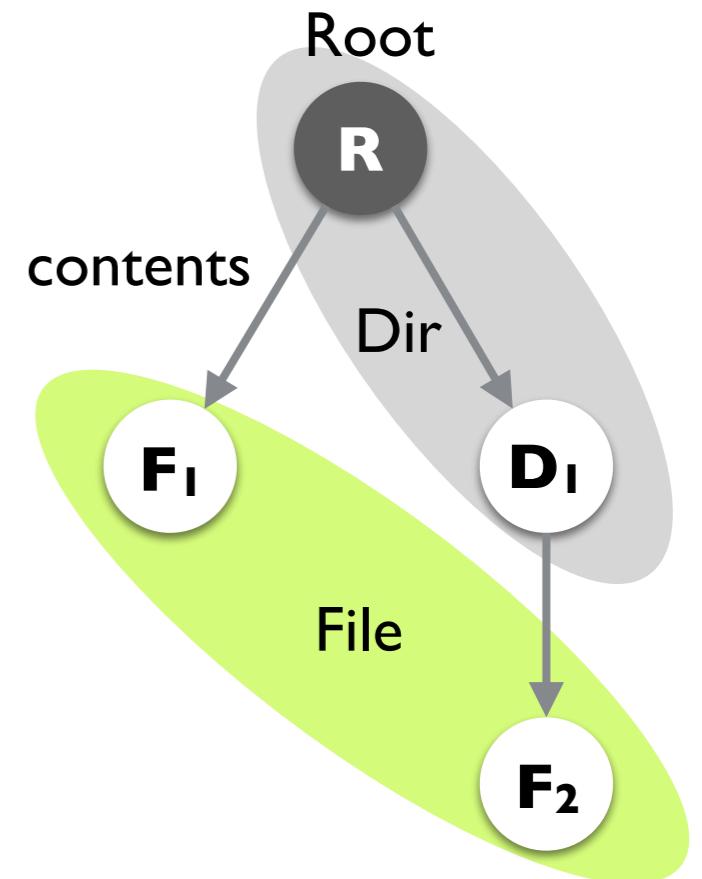
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Translation by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

$\forall d: \text{Dir} \mid \neg(d \subseteq d.\wedge\text{contents})$

$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$

Translation by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge\text{contents})$

$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$

Encode

- relational constants as boolean matrices
- relational expressions as matrix operations
- formulas as constraints over matrix entries

Relational constants as boolean matrices

Relational constants as boolean matrices

R	D ₁	D ₂	F ₁	F ₂
I	0	0	0	0

$$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$$

Relational constants as boolean matrices

R	D ₁	D ₂	F ₁	F ₂
I	0	0	0	0
d ₀	d ₁	d ₂	0	0

{⟨R⟩} ⊆ Root ⊆ {⟨R⟩}

{ } ⊆ Dir ⊆ {⟨R⟩, ⟨D₁⟩, ⟨D₂⟩}

Relational constants as boolean matrices

R	D ₁	D ₂	F ₁	F ₂
I	0	0	0	0
d ₀	d ₁	d ₂	0	0
0	0	0	f ₀	f ₁

{⟨R⟩} ⊆ Root ⊆ {⟨R⟩}

{ } ⊆ Dir ⊆ {⟨R⟩, ⟨D₁⟩, ⟨D₂⟩}

{ } ⊆ File ⊆ {⟨F₁⟩, ⟨F₂⟩}

Relational constants as boolean matrices

R D₁ D₂ F₁ F₂

I	0	0	0	0
---	---	---	---	---

d ₀	d ₁	d ₂	0	0
----------------	----------------	----------------	---	---

0	0	0	f ₀	f ₁
---	---	---	----------------	----------------

R	c ₀	c ₁	c ₂	c ₃	c ₄
D ₁	c ₅	c ₆	c ₇	c ₈	c ₉
D ₂	c ₁₀	c ₁₁	c ₁₂	c ₁₃	c ₁₄
F ₁	0	0	0	0	0
F ₂	0	0	0	0	0

{⟨R⟩} ⊆ Root ⊆ {⟨R⟩}

{ } ⊆ Dir ⊆ {⟨R⟩, ⟨D₁⟩, ⟨D₂⟩}

{ } ⊆ File ⊆ {⟨F₁⟩, ⟨F₂⟩}

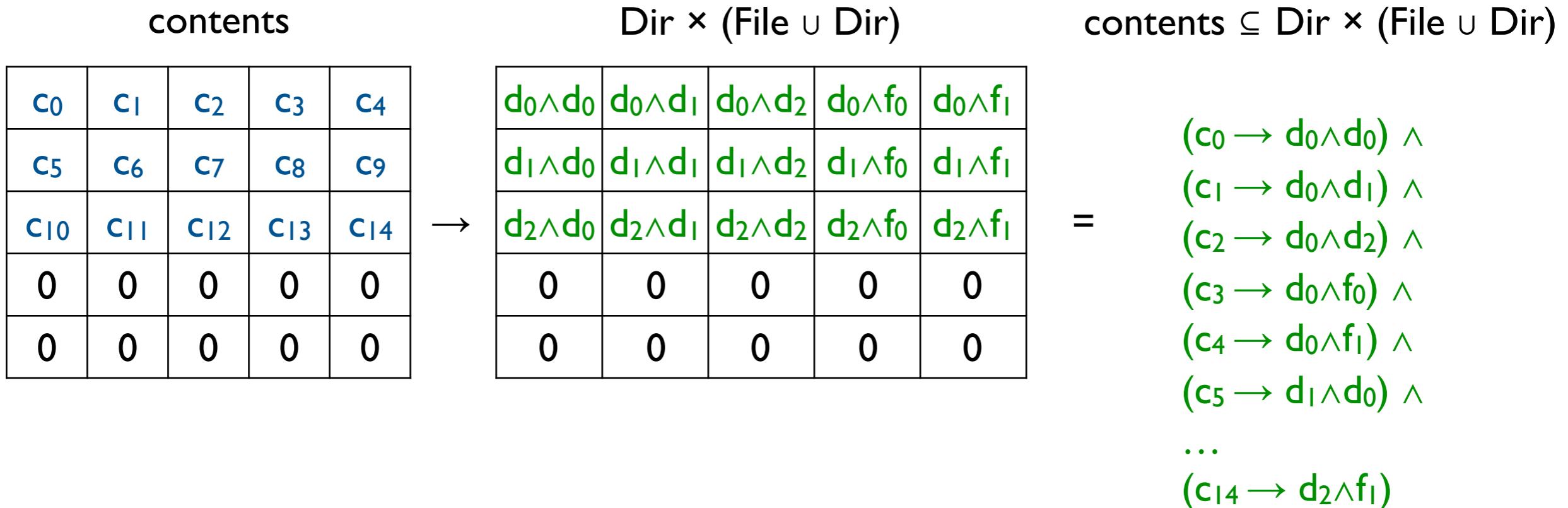
{ } ⊆ contents ⊆ {R, D₁, D₂} × {R, D₁, D₂, F₁, F₂}

Relational expressions as matrix operations

$$\begin{array}{c}
 \text{File} \\
 \boxed{0 \ 0 \ 0 \ f_0 \ f_1} \quad \vee \quad \boxed{d_0 \ d_1 \ d_2 \ 0 \ 0} \quad = \quad \boxed{d_0 \ d_1 \ d_2 \ f_0 \ f_1}
 \end{array}$$

$$\begin{array}{c}
 \text{Dir} \\
 \begin{array}{c} d_0 \\ d_1 \\ d_2 \\ 0 \\ 0 \end{array} \times \begin{array}{c} \text{File} \cup \text{Dir} \\ \boxed{d_0 \ d_1 \ d_2 \ f_0 \ f_1} \end{array} = \begin{array}{c} \text{Dir} \times (\text{File} \cup \text{Dir}) \\ \begin{array}{ccccc} d_0 \wedge d_0 & d_0 \wedge d_1 & d_0 \wedge d_2 & d_0 \wedge f_0 & d_0 \wedge f_1 \\ d_1 \wedge d_0 & d_1 \wedge d_1 & d_1 \wedge d_2 & d_1 \wedge f_0 & d_1 \wedge f_1 \\ d_2 \wedge d_0 & d_2 \wedge d_1 & d_2 \wedge d_2 & d_2 \wedge f_0 & d_2 \wedge f_1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \end{array}
 \end{array}$$

Formulas as constraints over matrix entries



Dealing with sparseness and redundancy

$\text{Dir} \times (\text{File} \cup \text{Dir})$

$d_0 \wedge d_0$	$d_0 \wedge d_1$	$d_0 \wedge d_2$	$d_0 \wedge f_0$	$d_0 \wedge f_1$
$d_1 \wedge d_0$	$d_1 \wedge d_1$	$d_1 \wedge d_2$	$d_1 \wedge f_0$	$d_1 \wedge f_1$
$d_2 \wedge d_0$	$d_2 \wedge d_1$	$d_2 \wedge d_2$	$d_2 \wedge f_0$	$d_2 \wedge f_1$
0	0	0	0	0
0	0	0	0	0

Dealing with sparseness and redundancy

$\text{Dir} \times (\text{File} \cup \text{Dir})$

$d_0 \wedge d_0$	$d_0 \wedge d_1$	$d_0 \wedge d_2$	$d_0 \wedge f_0$	$d_0 \wedge f_1$
$d_1 \wedge d_0$	$d_1 \wedge d_1$	$d_1 \wedge d_2$	$d_1 \wedge f_0$	$d_1 \wedge f_1$
$d_2 \wedge d_0$	$d_2 \wedge d_1$	$d_2 \wedge d_2$	$d_2 \wedge f_0$	$d_2 \wedge f_1$
0	0	0	0	0
0	0	0	0	0

Empty regions in matrices
(exponential w.r.t. relation arity).

Dealing with sparseness and redundancy

Different circuits for
the same formula.

$\text{Dir} \times (\text{File} \cup \text{Dir})$

$d_0 \wedge d_0$	$d_0 \wedge d_1$	$d_0 \wedge d_2$	$d_0 \wedge f_0$	$d_0 \wedge f_1$
$d_1 \wedge d_0$	$d_1 \wedge d_1$	$d_1 \wedge d_2$	$d_1 \wedge f_0$	$d_1 \wedge f_1$
$d_2 \wedge d_0$	$d_2 \wedge d_1$	$d_2 \wedge d_2$	$d_2 \wedge f_0$	$d_2 \wedge f_1$
0	0	0	0	0
0	0	0	0	0

Empty regions in matrices
(exponential w.r.t. relation arity).

Dealing with sparseness and redundancy

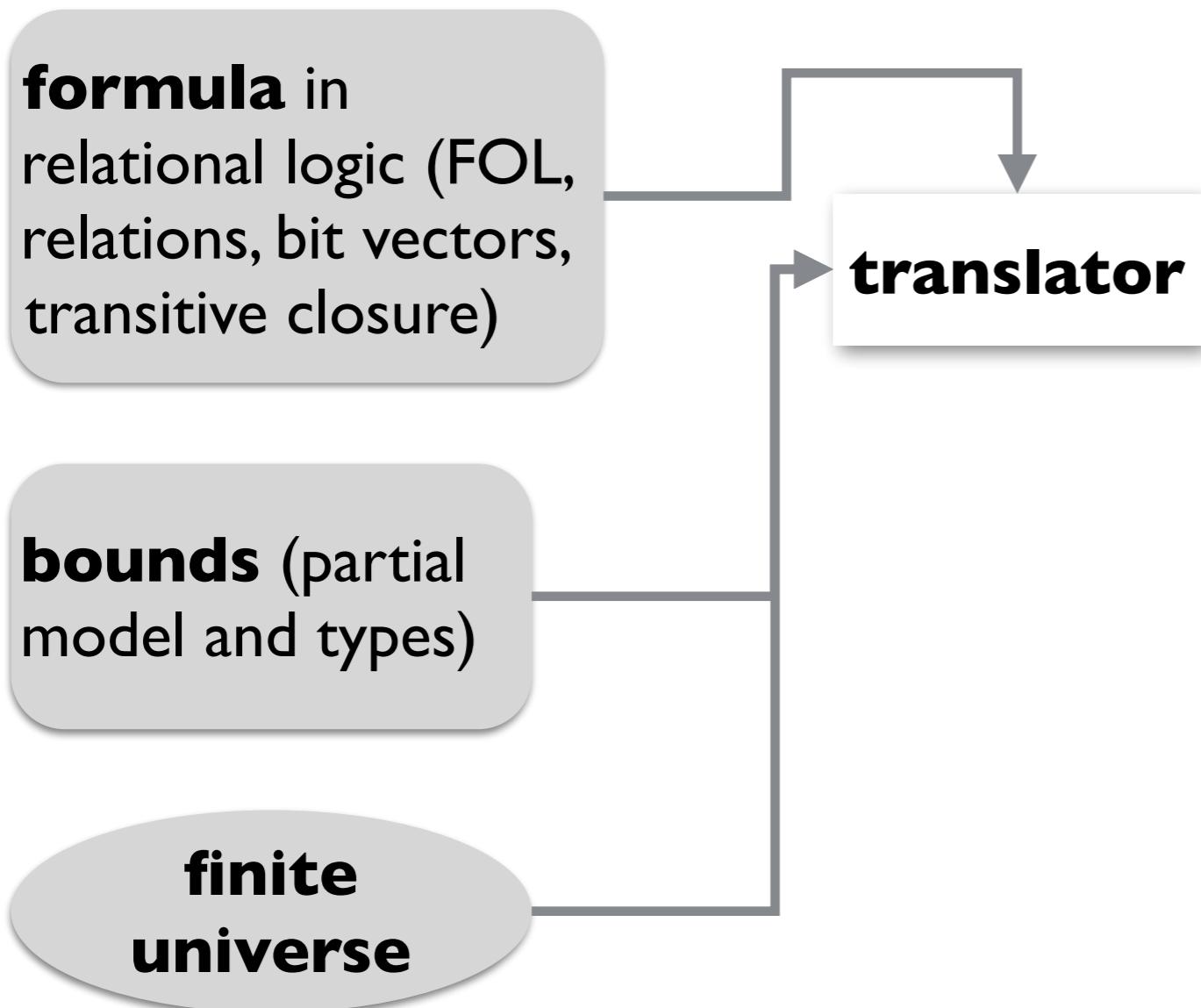
Compact Boolean Circuits (CBCs).

$\text{Dir} \times (\text{File} \cup \text{Dir})$

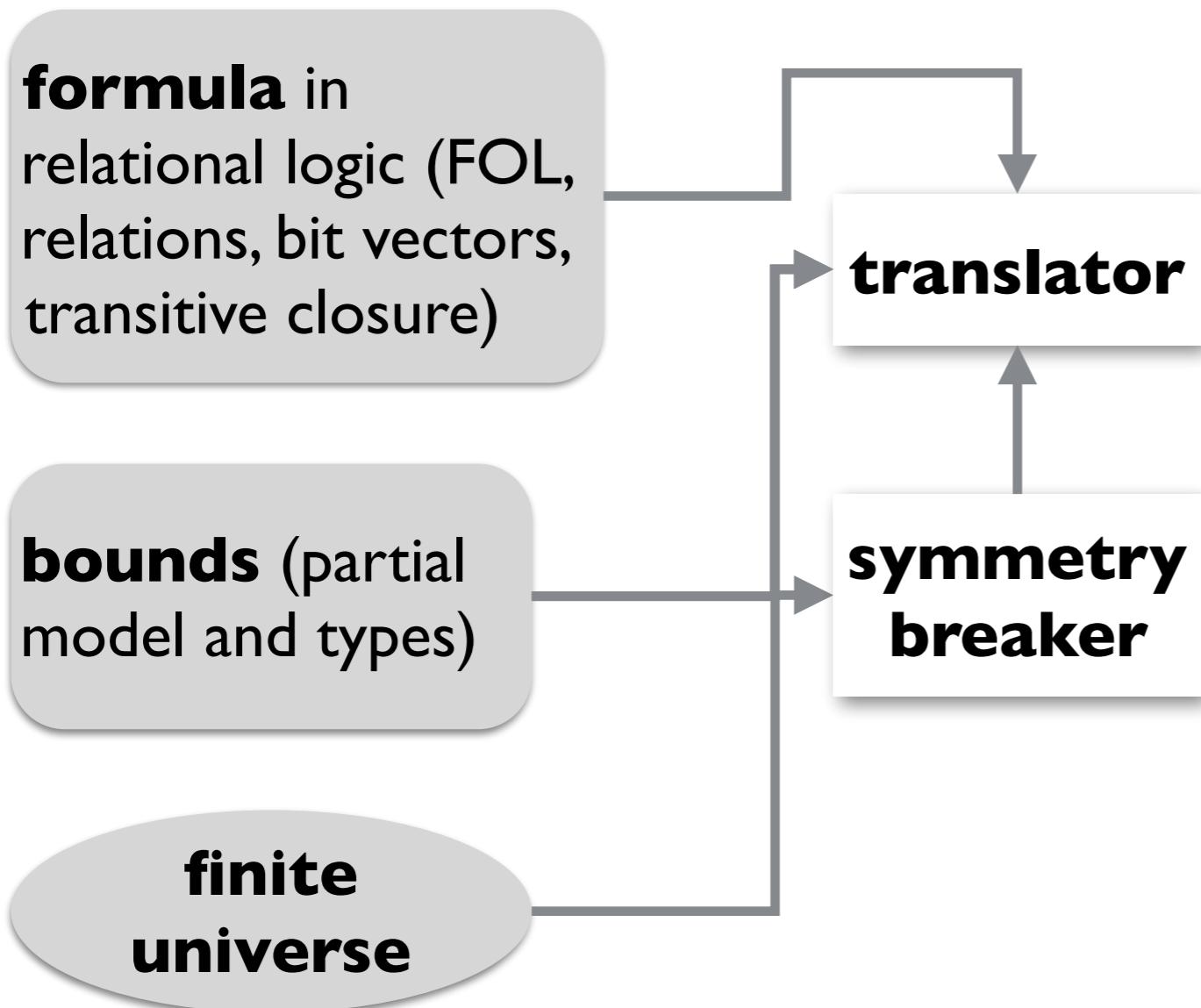
$d_0 \wedge d_0$	$d_0 \wedge d_1$	$d_0 \wedge d_2$	$d_0 \wedge f_0$	$d_0 \wedge f_1$
$d_1 \wedge d_0$	$d_1 \wedge d_1$	$d_1 \wedge d_2$	$d_1 \wedge f_0$	$d_1 \wedge f_1$
$d_2 \wedge d_0$	$d_2 \wedge d_1$	$d_2 \wedge d_2$	$d_2 \wedge f_0$	$d_2 \wedge f_1$
0	0	0	0	0
0	0	0	0	0

Sparse matrices represented as interval trees.

Overview of Kodkod



Overview of Kodkod



Symmetry by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

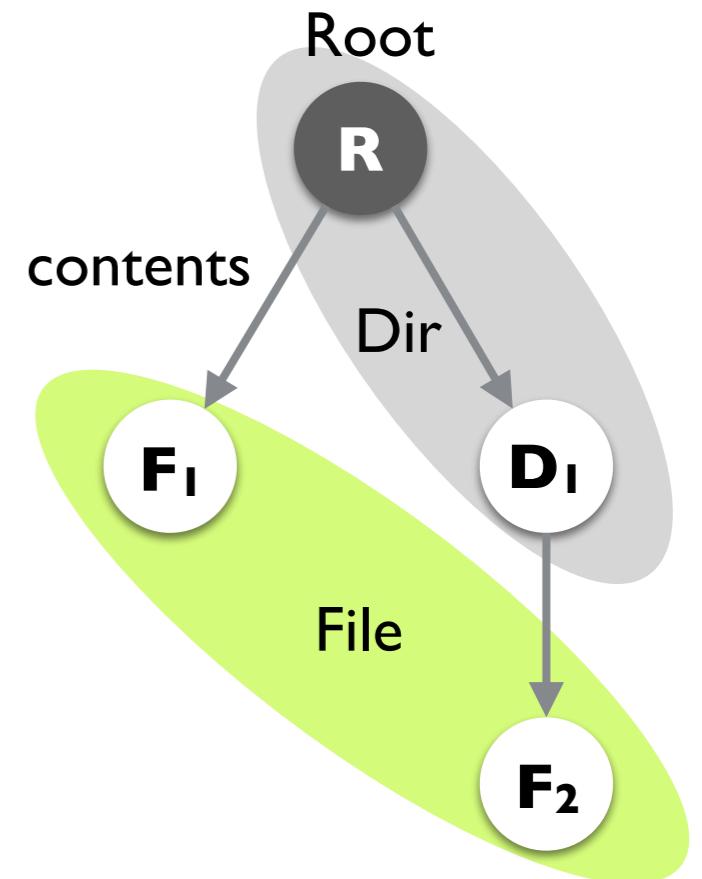
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Symmetry by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge\text{contents})$

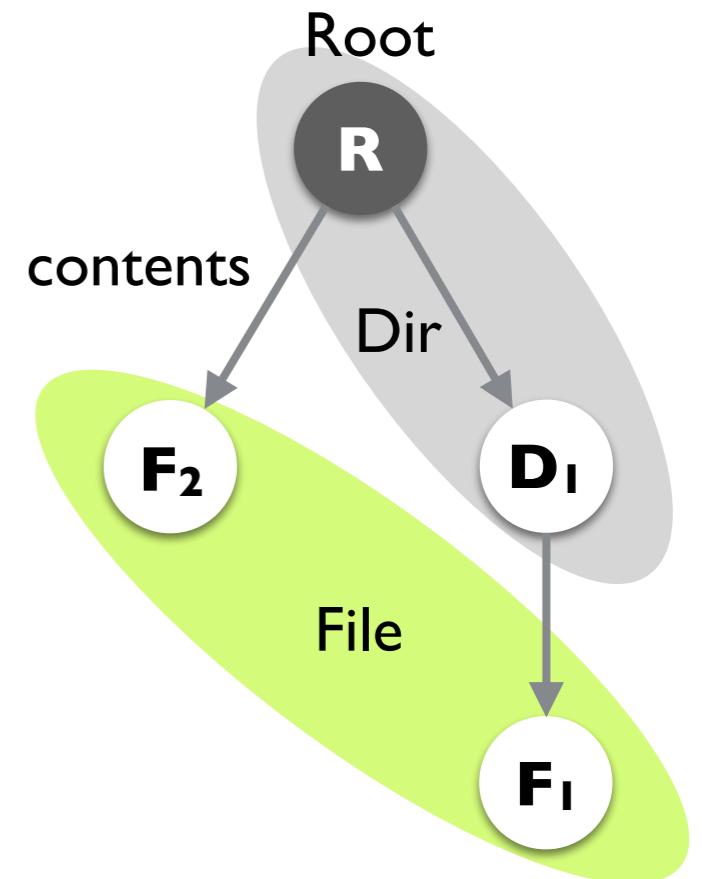
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Symmetry by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge\text{contents})$

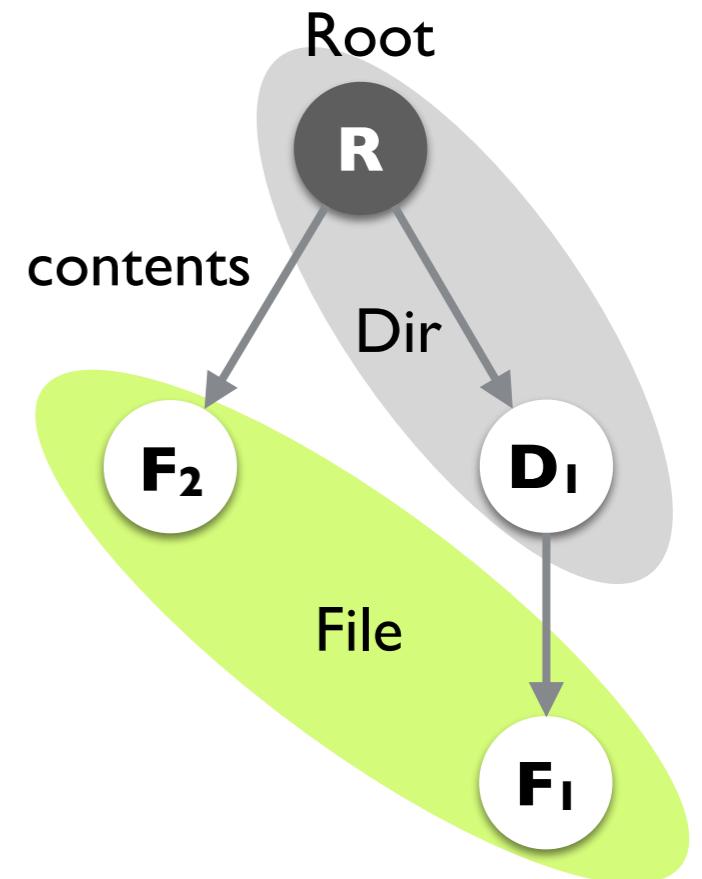
{ **R**, **D₁**, **D₂**, **F₁**, **F₂** }

{⟨**R**⟩} ⊆ Root ⊆ {⟨**R**⟩}

{ } ⊆ Dir ⊆ {⟨**R**⟩, ⟨**D₁**⟩, ⟨**D₂**⟩}

{ } ⊆ File ⊆ {⟨**F₁**⟩, ⟨**F₂**⟩}

{ } ⊆ contents ⊆ {**R**, **D₁**, **D₂**} × {**R**, **D₁**, **D₂**, **F₁**, **F₂**}



Symmetry by example

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge\text{contents})$

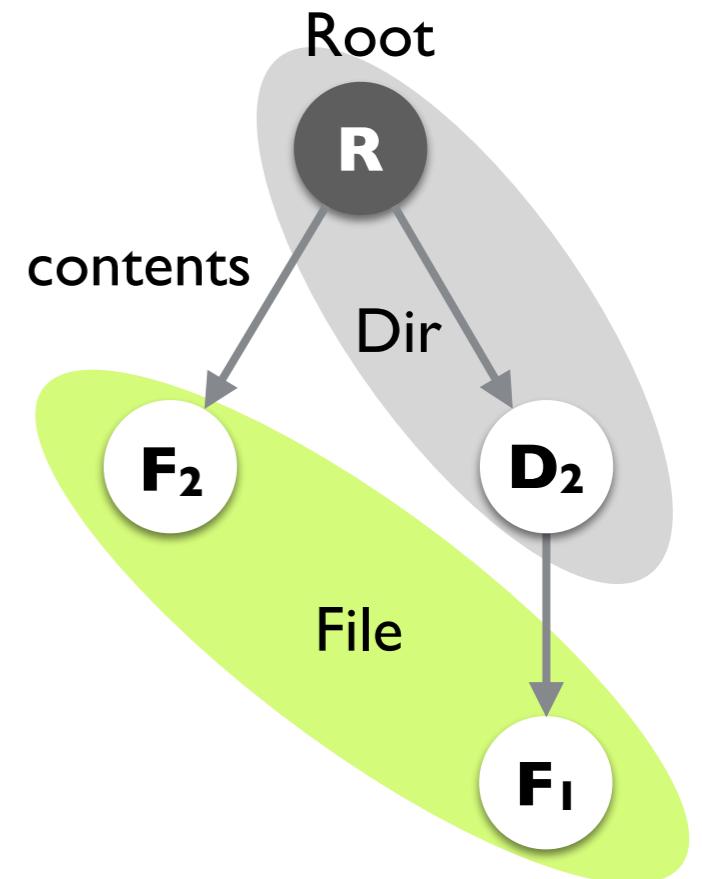
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Symmetries between models

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

{ **R**, **D₁**, **D₂**, **F₁**, **F₂** }

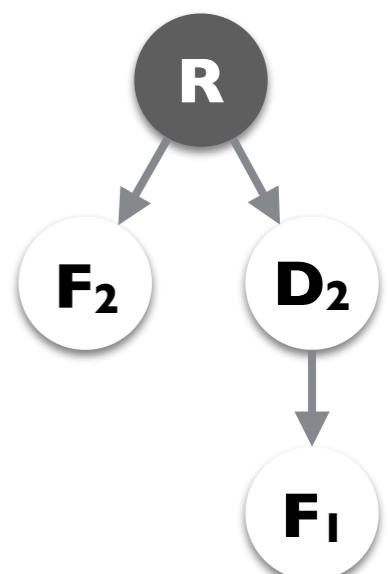
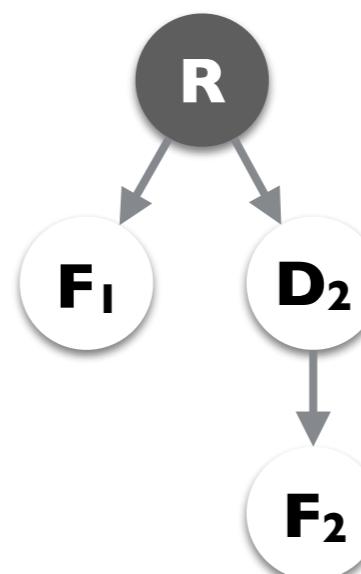
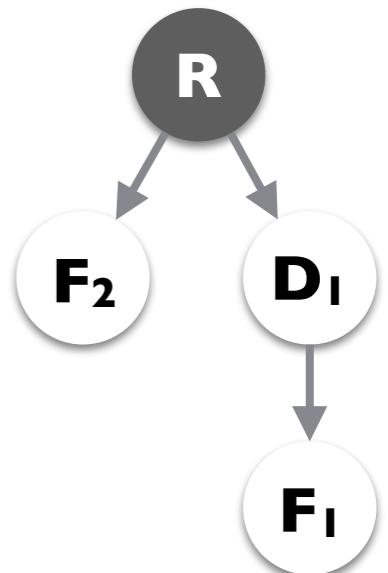
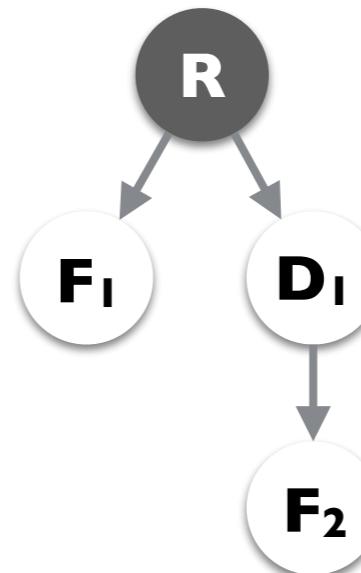


$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Symmetries between non-models

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

{ **R**, **D₁**, **D₂**, **F₁**, **F₂** }

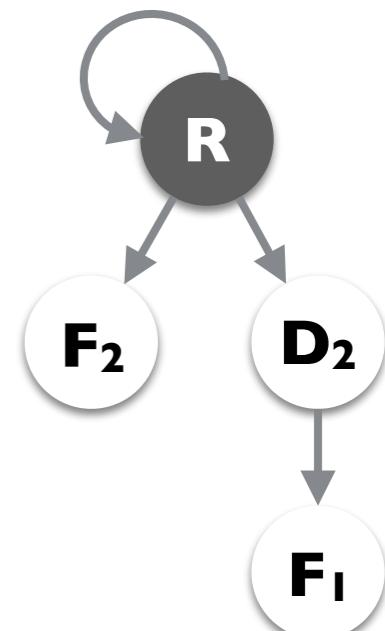
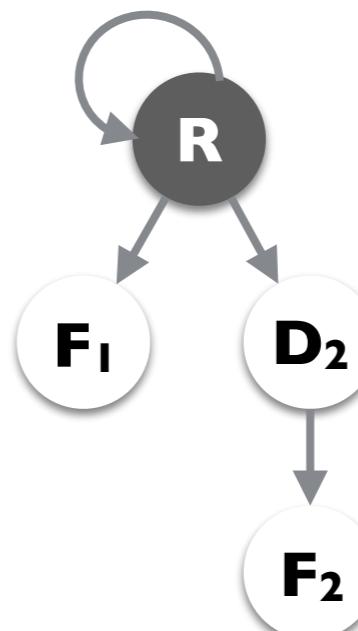
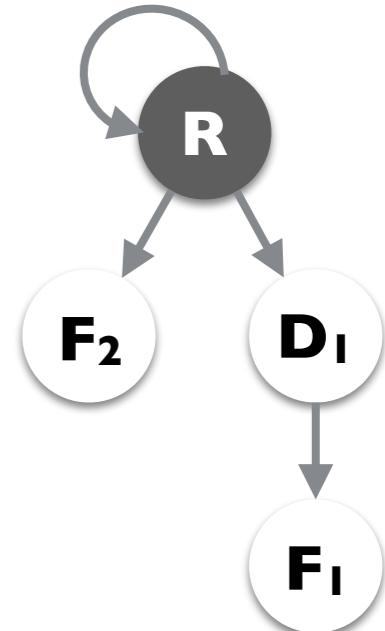
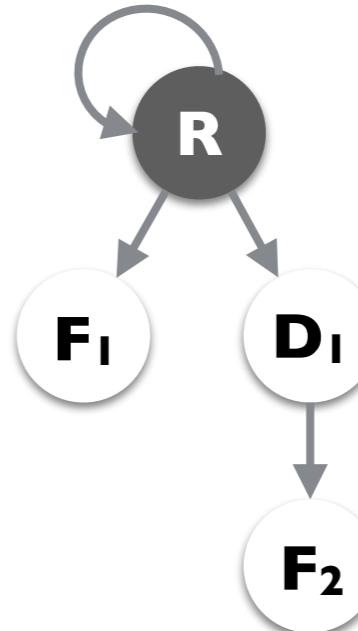


$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Symmetries induce equivalence classes

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

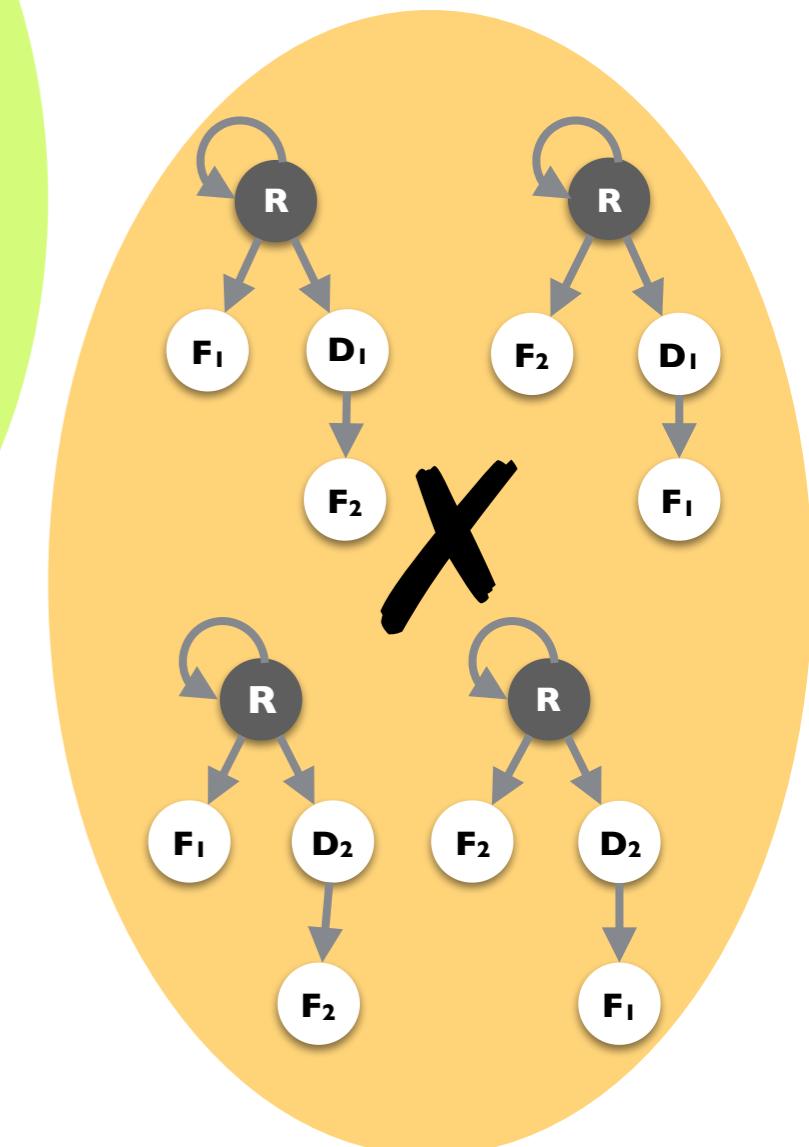
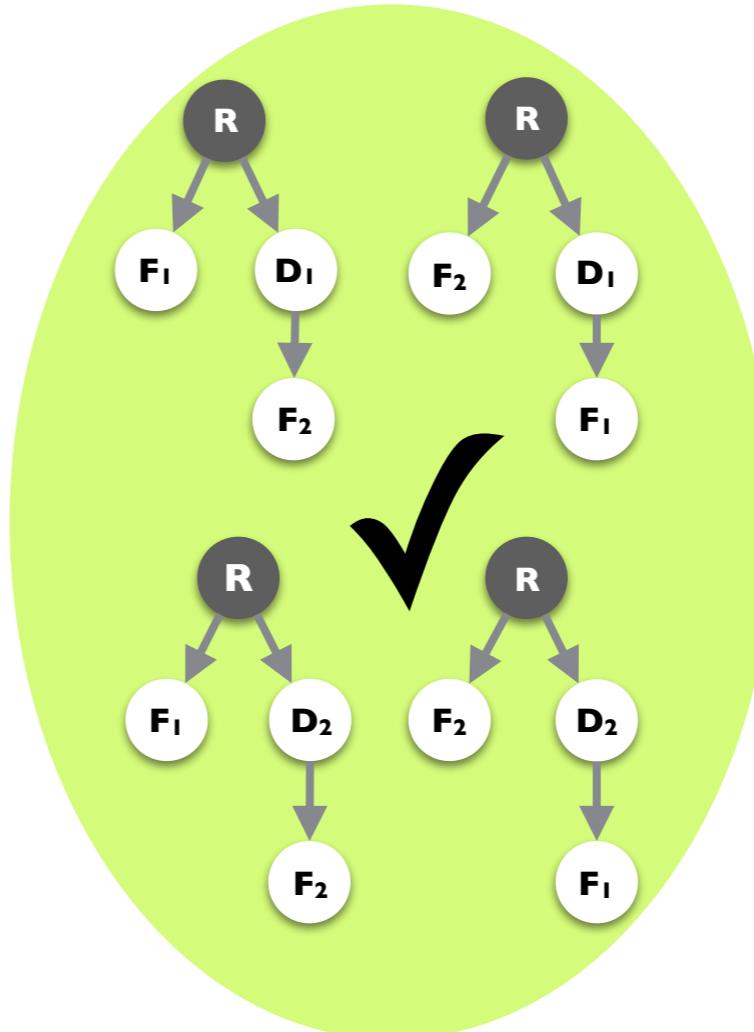
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Symmetries induce equivalence classes

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\text{*contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

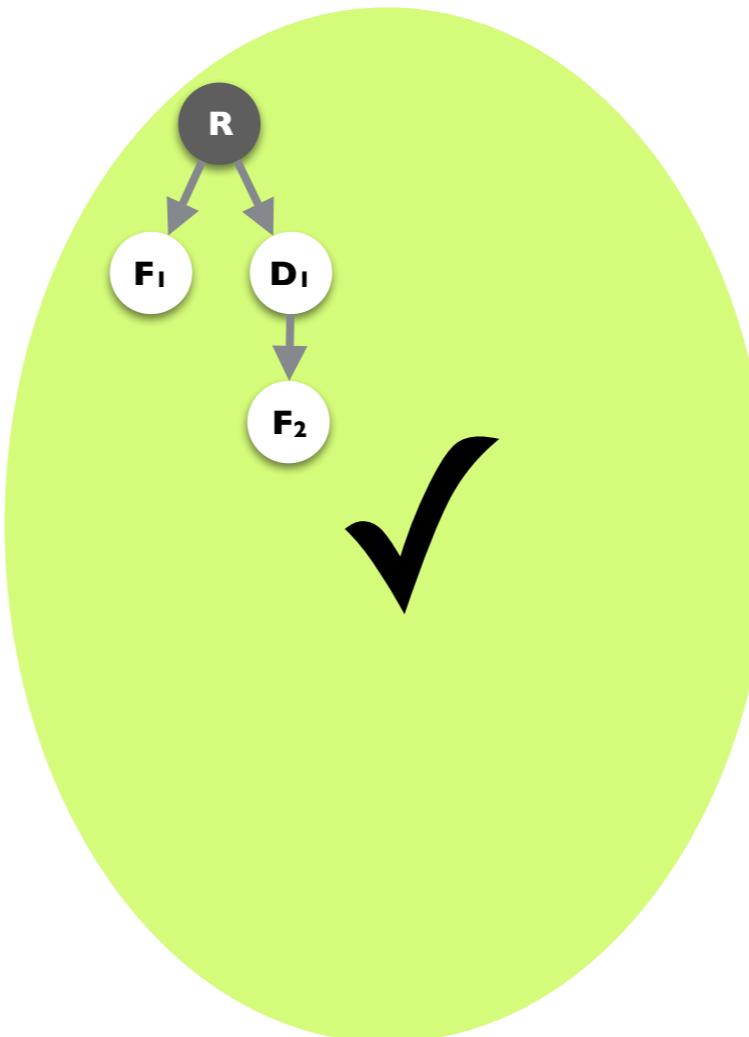
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

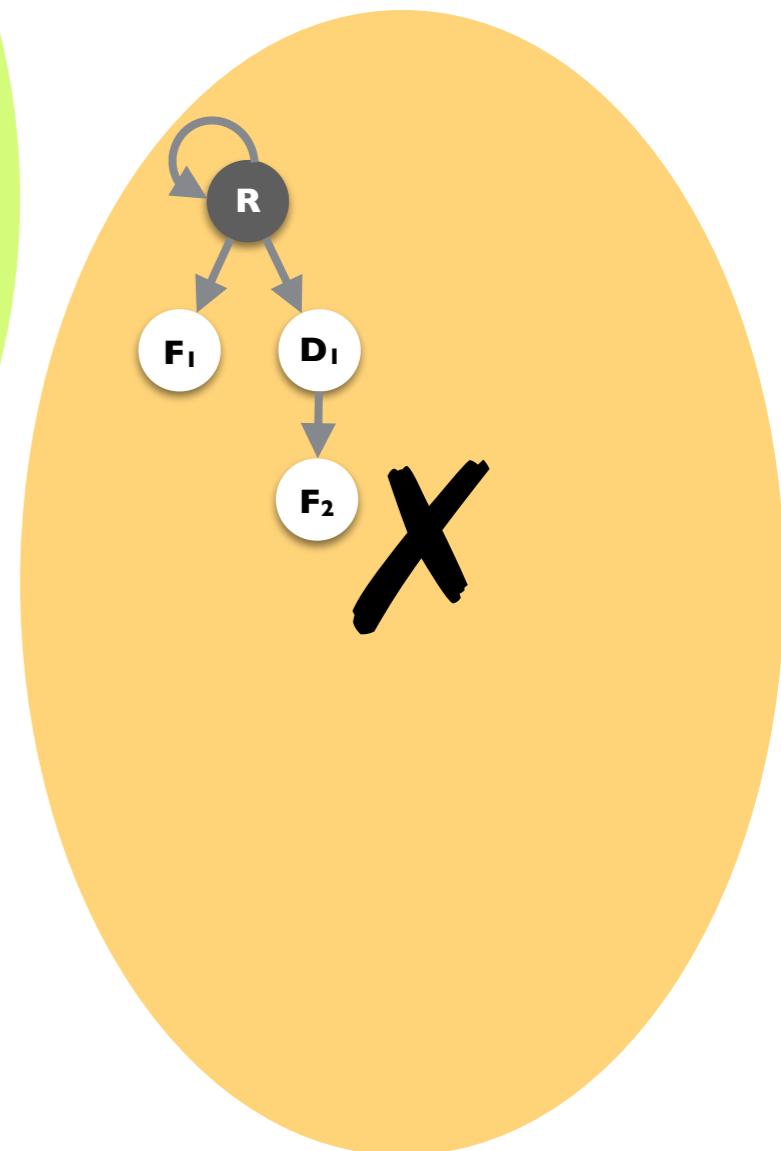
$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



Sufficient to check
one interpretation
per equivalence class.



Symmetry detection

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

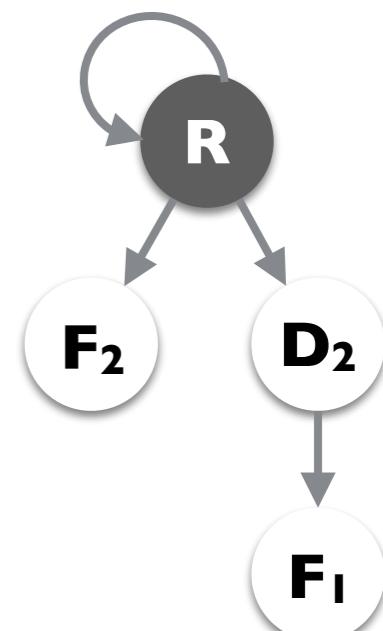
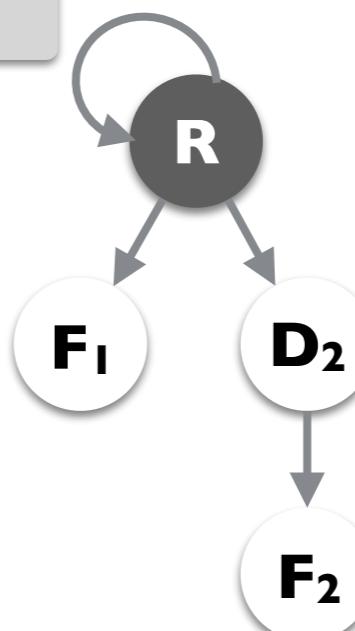
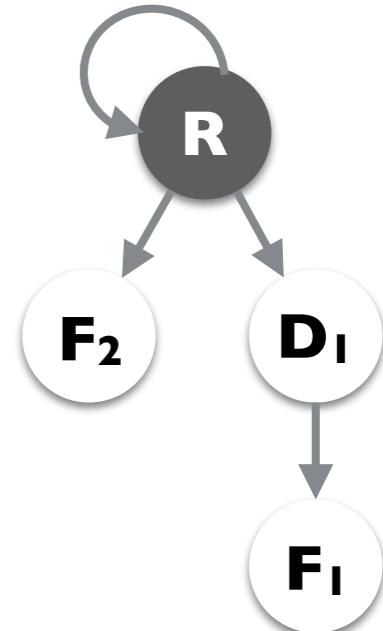
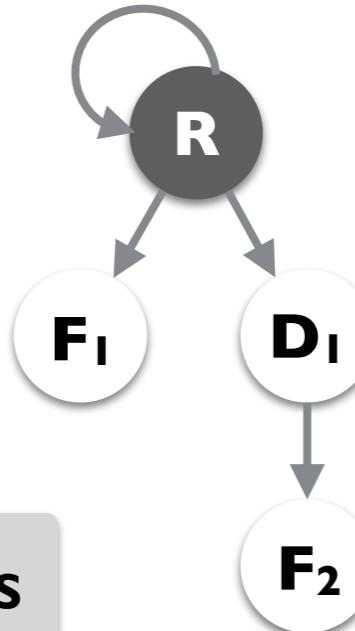
Interpretation symmetries
= bound symmetries

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$

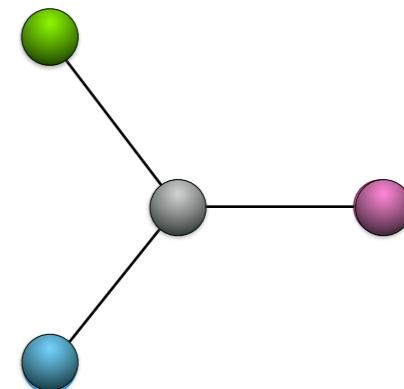


Detecting symmetries is hard ...

Interpretation symmetries
= bound symmetries



Graph automorphism
detection

$$\{ \langle \text{green}, \text{grey} \rangle \langle \text{grey}, \text{green} \rangle, \\ \langle \text{grey}, \text{pink} \rangle \langle \text{pink}, \text{grey} \rangle, \\ \langle \text{grey}, \text{blue} \rangle \langle \text{blue}, \text{grey} \rangle \}$$


But only a few symmetries needed in practice

Greedy algorithm that partitions the universe into equivalence classes



Graph automorphism detection



Base partitioning: practical symmetry detection

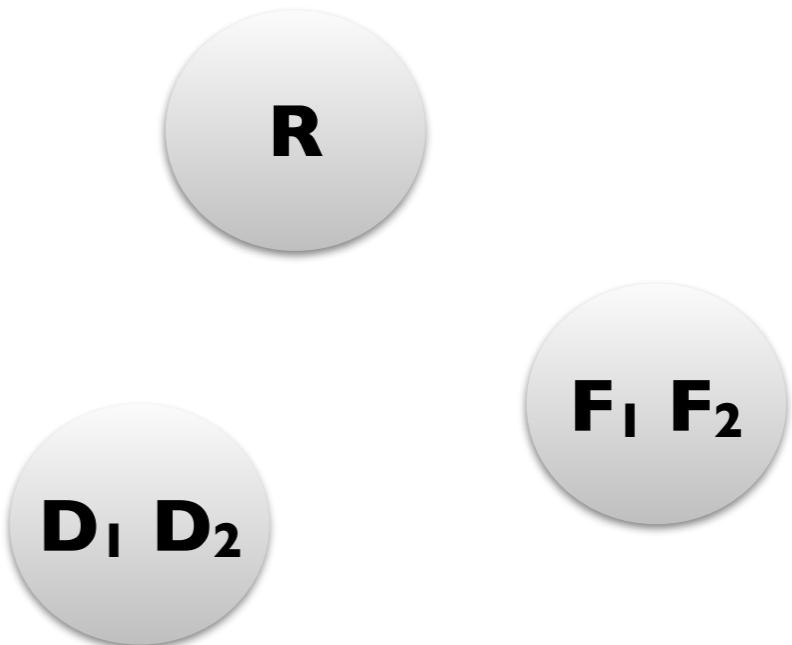
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



The coarsest partition of the universe such that each non-empty bound is expressible as a union of products of parts.

Finding the base partitioning

R D₁ D₂ F₁ F₂

start with a single partition
and refine minimally for
each non-empty lower and
upper bound

Finding base partitioning

R D₁ D₂ F₁ F₂

Finding base partitioning

R D₁ D₂ F₁ F₂

$$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$$

Finding base partitioning



$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

Finding base partitioning


$$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$$
$$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$$

Finding base partitioning



$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

Finding base partitioning



$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

Finding base partitioning



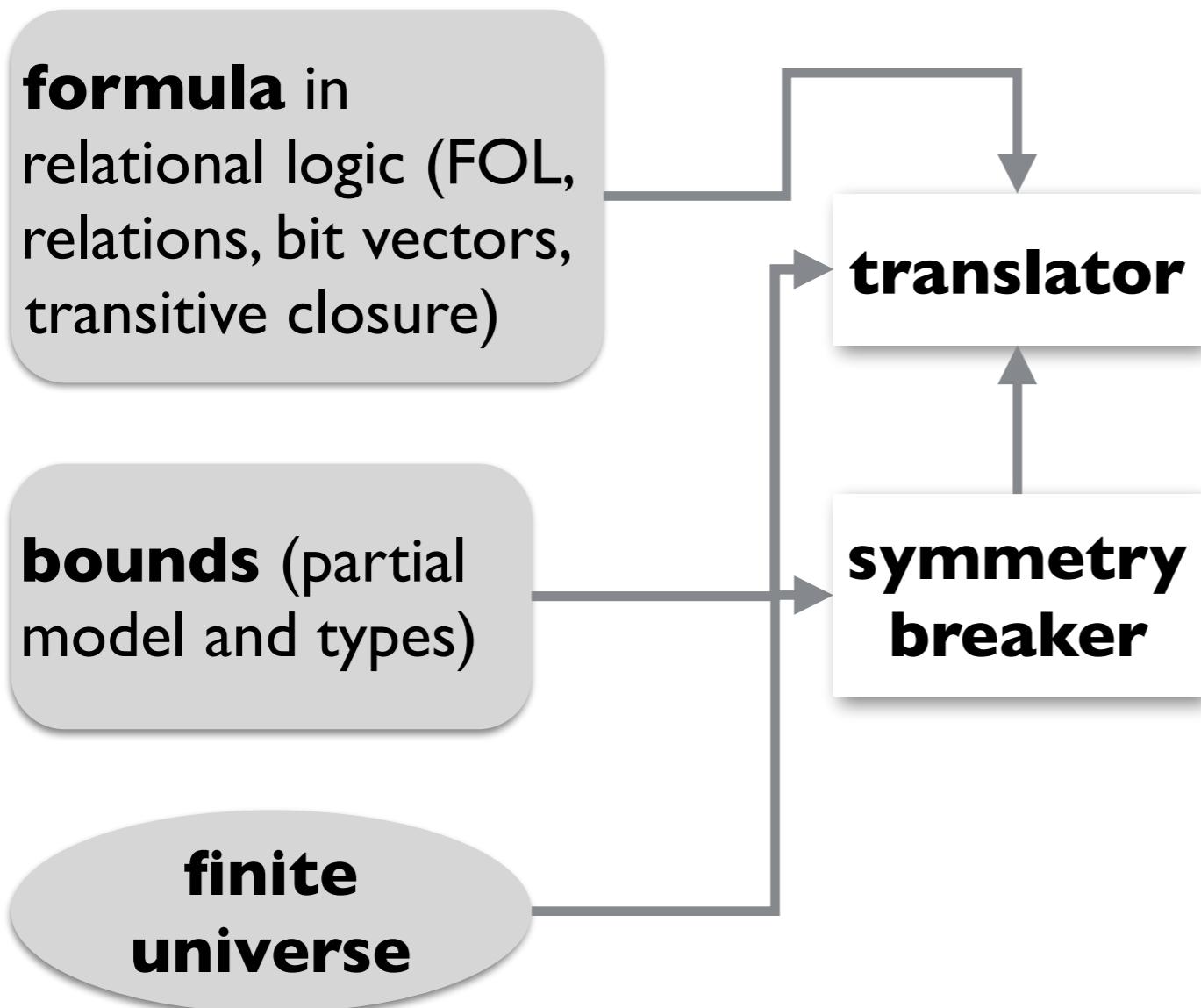
$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

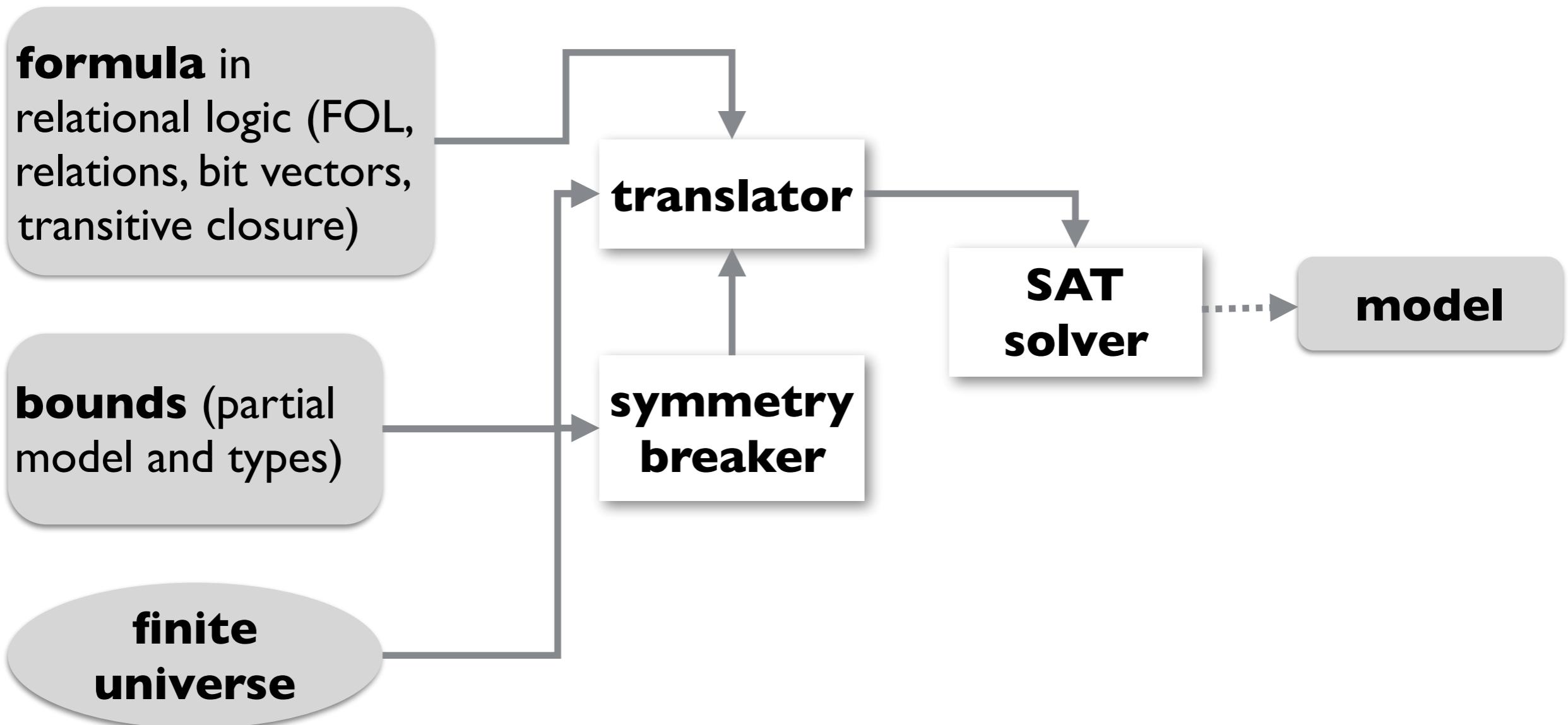
$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$

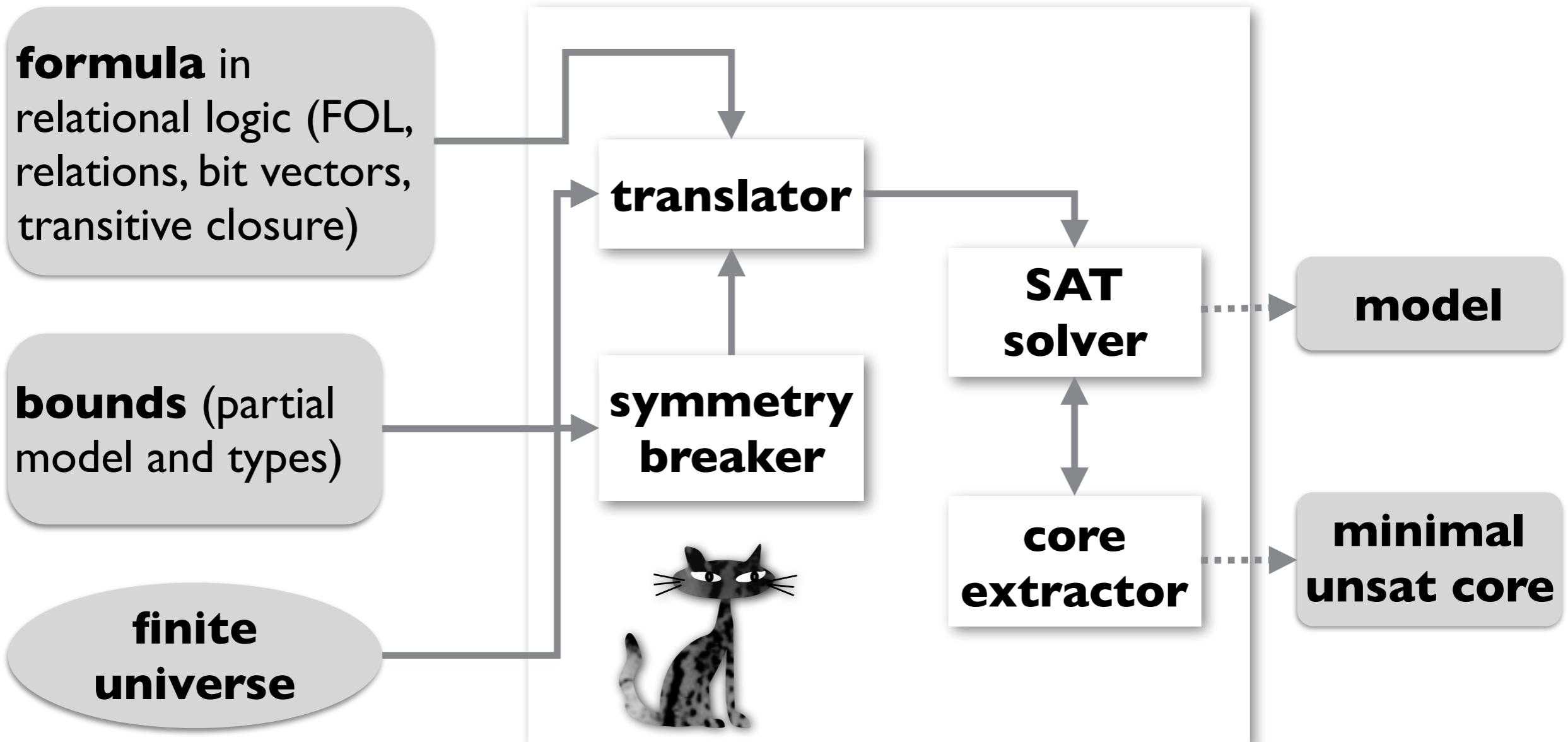
Overview of Kodkod



Overview of Kodkod



Overview of Kodkod



A bug in the tiny filesystem

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

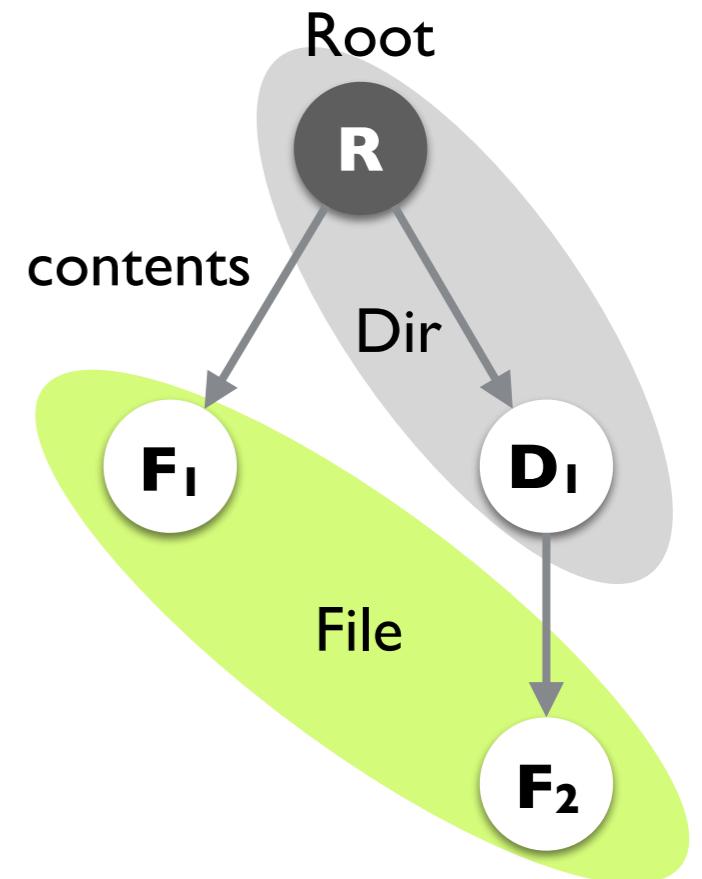
$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$



A bug in the tiny filesystem

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast \text{contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

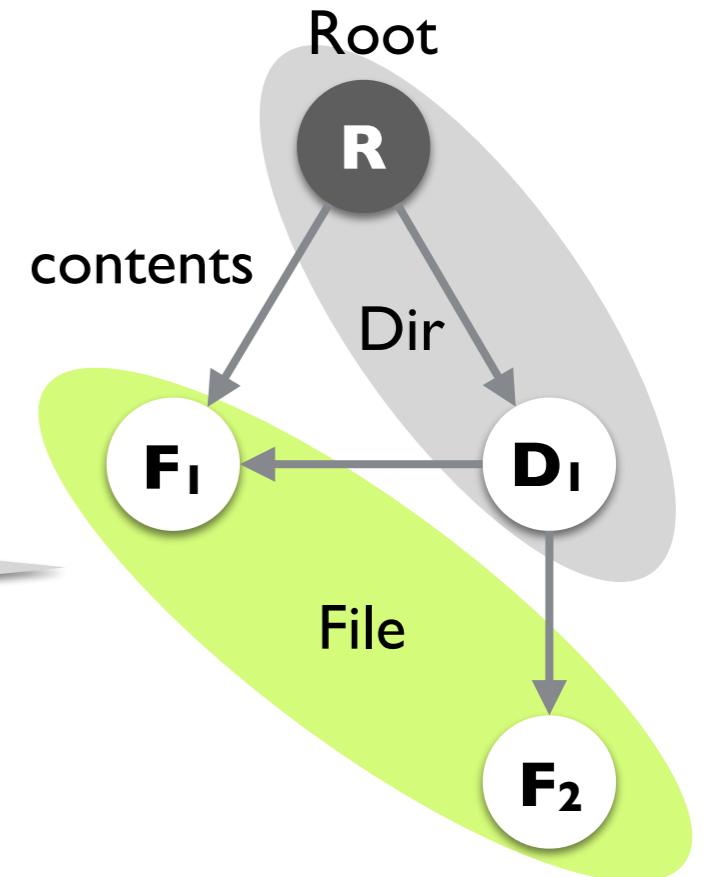
$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$

The spec allows multiple parents.



Fixing the tiny filesystem

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\text{*contents}$

$\forall d: \text{Dir} \mid \neg (d \subseteq d.^{\wedge}\text{contents})$

$\forall f: \text{File} \mid \text{one contents}.f$

$\forall d: \text{Dir} \mid \text{one contents}.d$

$\{ \mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2} \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D_1} \rangle, \langle \mathbf{D_2} \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F_1} \rangle, \langle \mathbf{F_2} \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D_1}, \mathbf{D_2}\} \times \{\mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\}$

Fixing the tiny filesystem

$\text{Root} \subseteq \text{Dir}$

$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\ast\text{contents}$

$\forall d: \text{Dir} \mid \neg(d \subseteq d.\wedge\text{contents})$

$\forall f: \text{File} \mid \text{one contents}.f$

$\forall d: \text{Dir} \mid \text{one contents}.d$

$\{ \mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2 \}$

$\{\langle \mathbf{R} \rangle\} \subseteq \text{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

$\{\} \subseteq \text{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D}_1 \rangle, \langle \mathbf{D}_2 \rangle\}$

$\{\} \subseteq \text{File} \subseteq \{\langle \mathbf{F}_1 \rangle, \langle \mathbf{F}_2 \rangle\}$

$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2\} \times \{\mathbf{R}, \mathbf{D}_1, \mathbf{D}_2, \mathbf{F}_1, \mathbf{F}_2\}$

Minimal unsatisfiable core:
an unsatisfiable subset of a formula that becomes satisfiable if any of its members are removed.

Resolution-based core extraction

$\text{Root} \subseteq \text{Dir}$

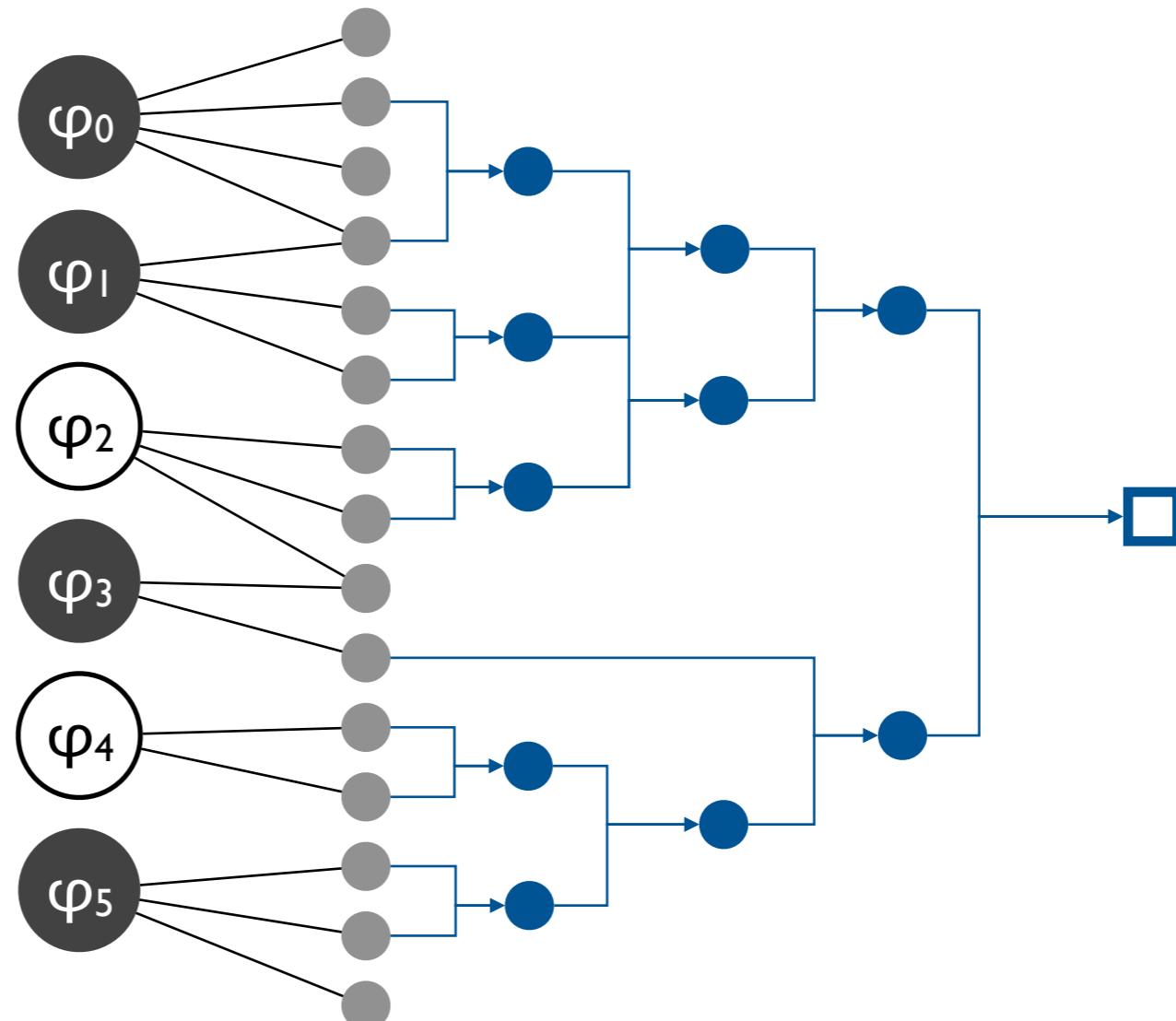
$\text{contents} \subseteq \text{Dir} \times (\text{File} \cup \text{Dir})$

$(\text{File} \cup \text{Dir}) \subseteq \text{Root}.\text{*contents}$

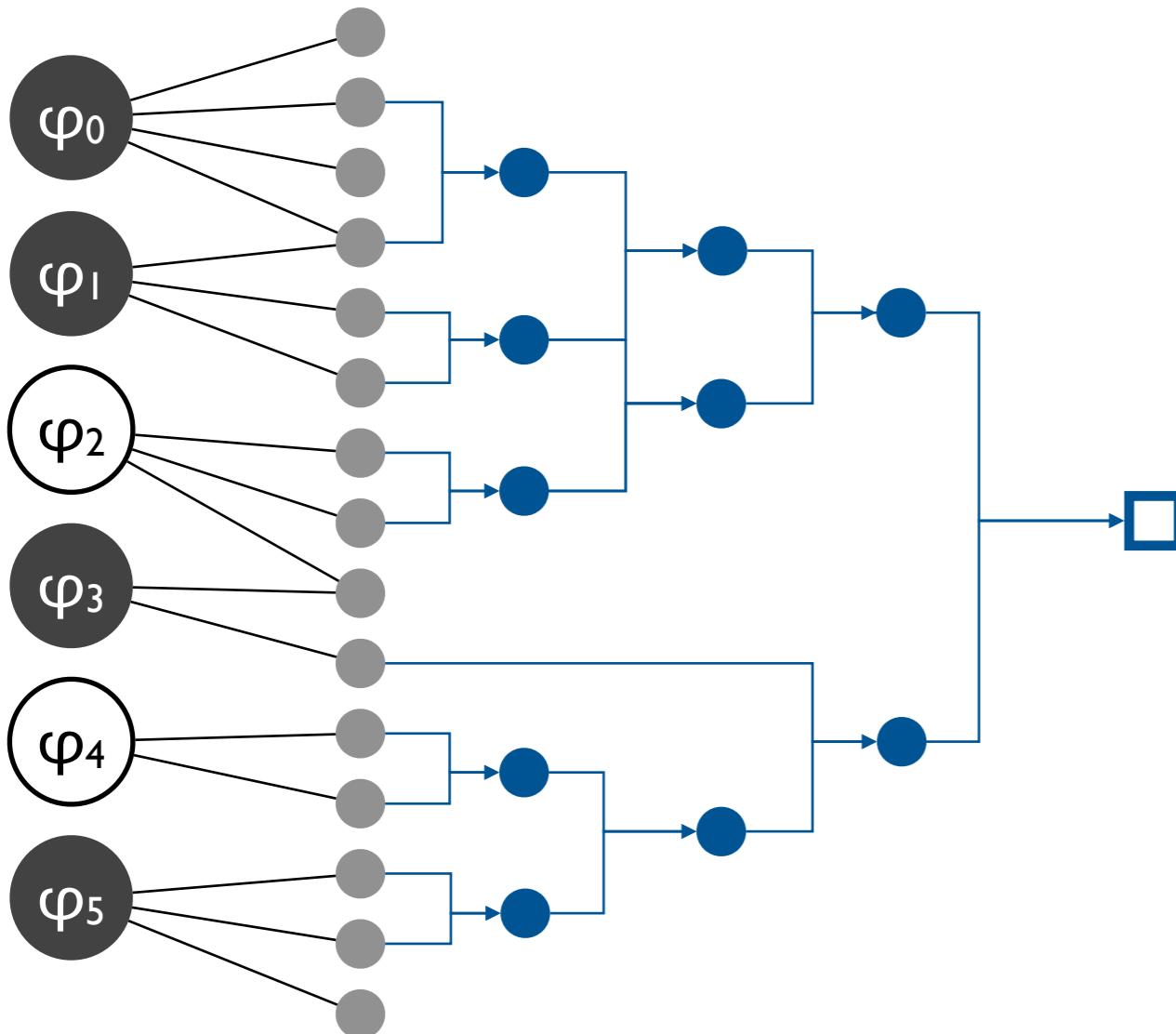
$\forall d: \text{Dir} \mid \neg (d \subseteq d.\wedge \text{contents})$

$\forall f: \text{File} \mid \text{one contents}.f$

$\forall d: \text{Dir} \mid \text{one contents}.d$



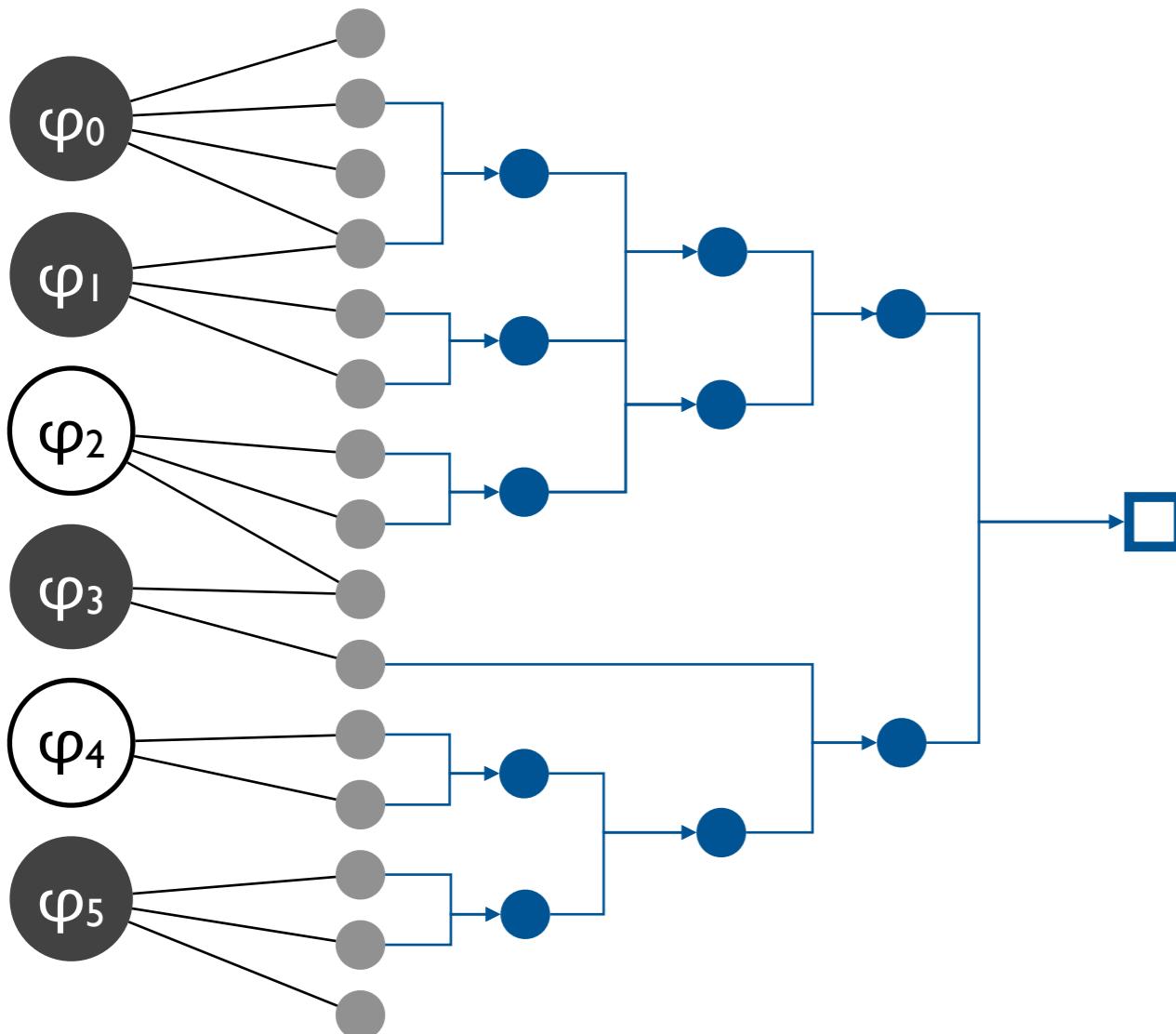
High-level minimal cores from low-level proofs



How to use the proof at the SAT level to find a minimal core at the specification level when

- SAT proof is not minimal
- minimal SAT core may map to a large specification core?

Recycling core extraction



Key idea: minimize core by removing constraints at the specification level but re-use valid resolvents from the previous step so that the solver doesn't have to re-derive them.

Summary

Today

- Finite model finding for first-order logic with quantifiers, relations, and transitive closure

Next lecture

- Reasoning about program correctness