Computer-Aided Reasoning for Software

CSE507

Finite Model Finding

Emina Torlak
emina@cs.washington.edu

Today

Last lecture

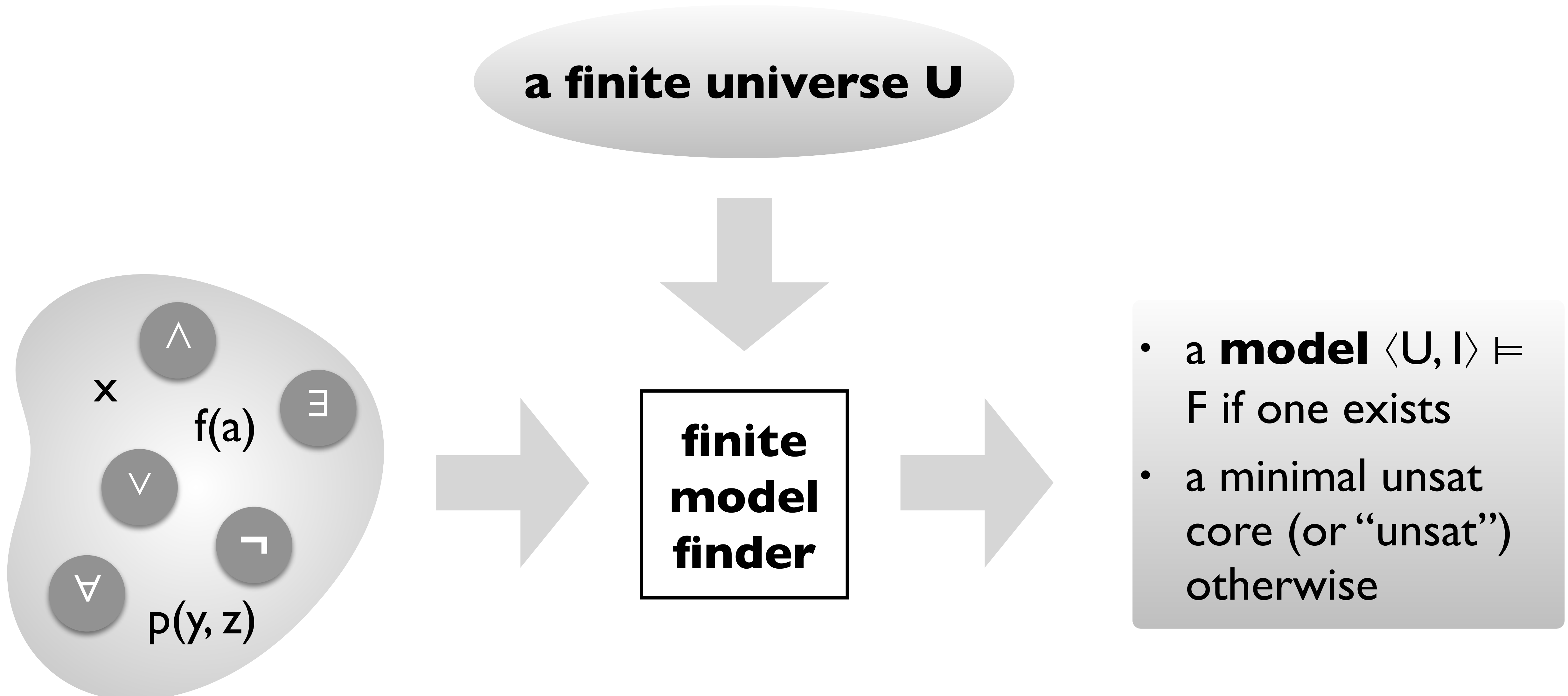
- The DPPL(T) framework for deciding quantifier-free SMT formulas

Today

- Finite model finding for quantified FOL and beyond

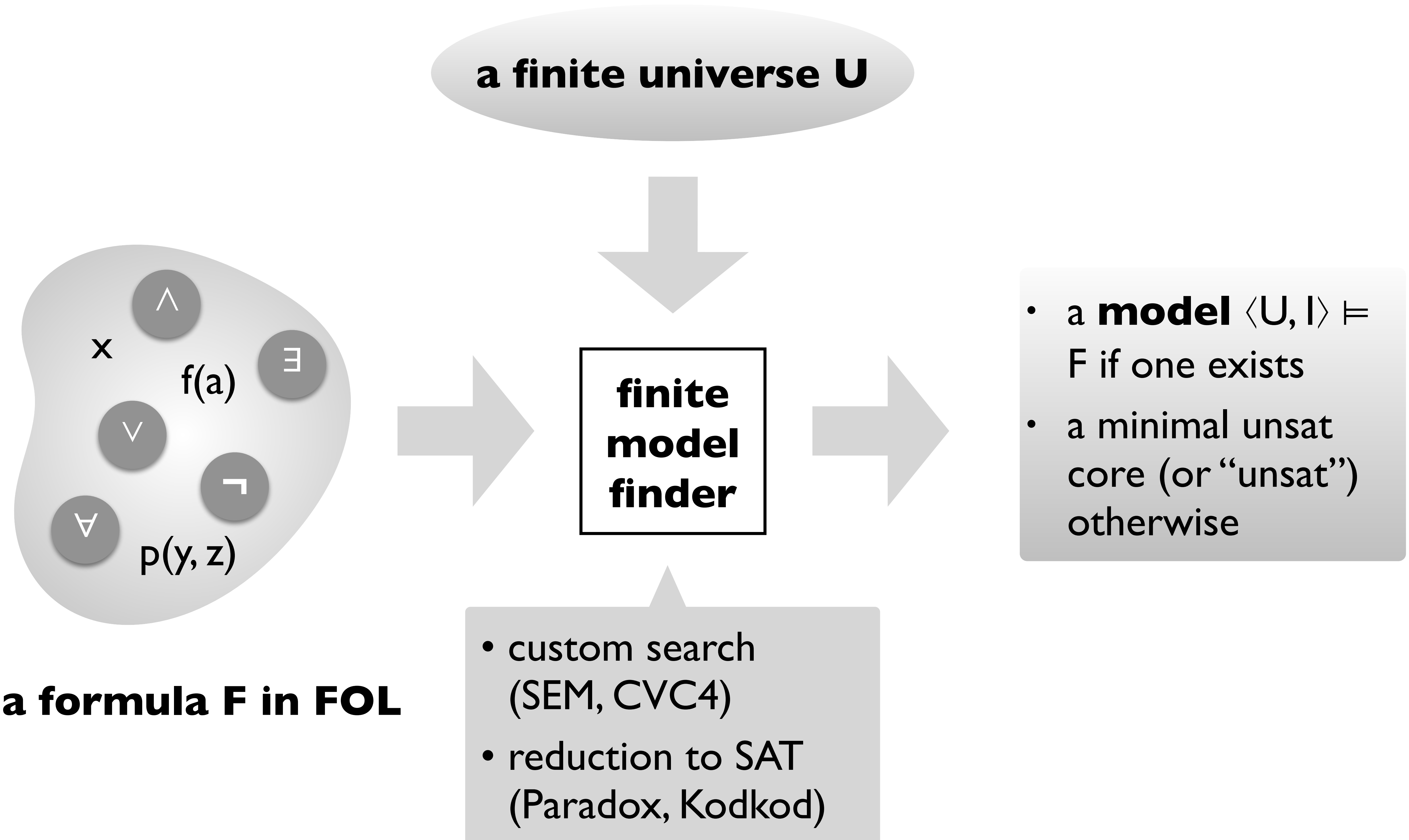
topics

Finite model finding



a formula F in FOL

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)

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

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)

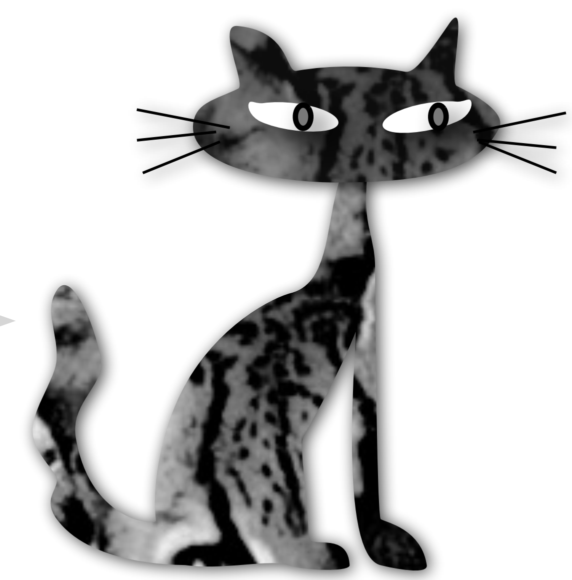
Some applications of finite model finding

Checking lightweight formal specifications (Alloy, ProB, ExUML)

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

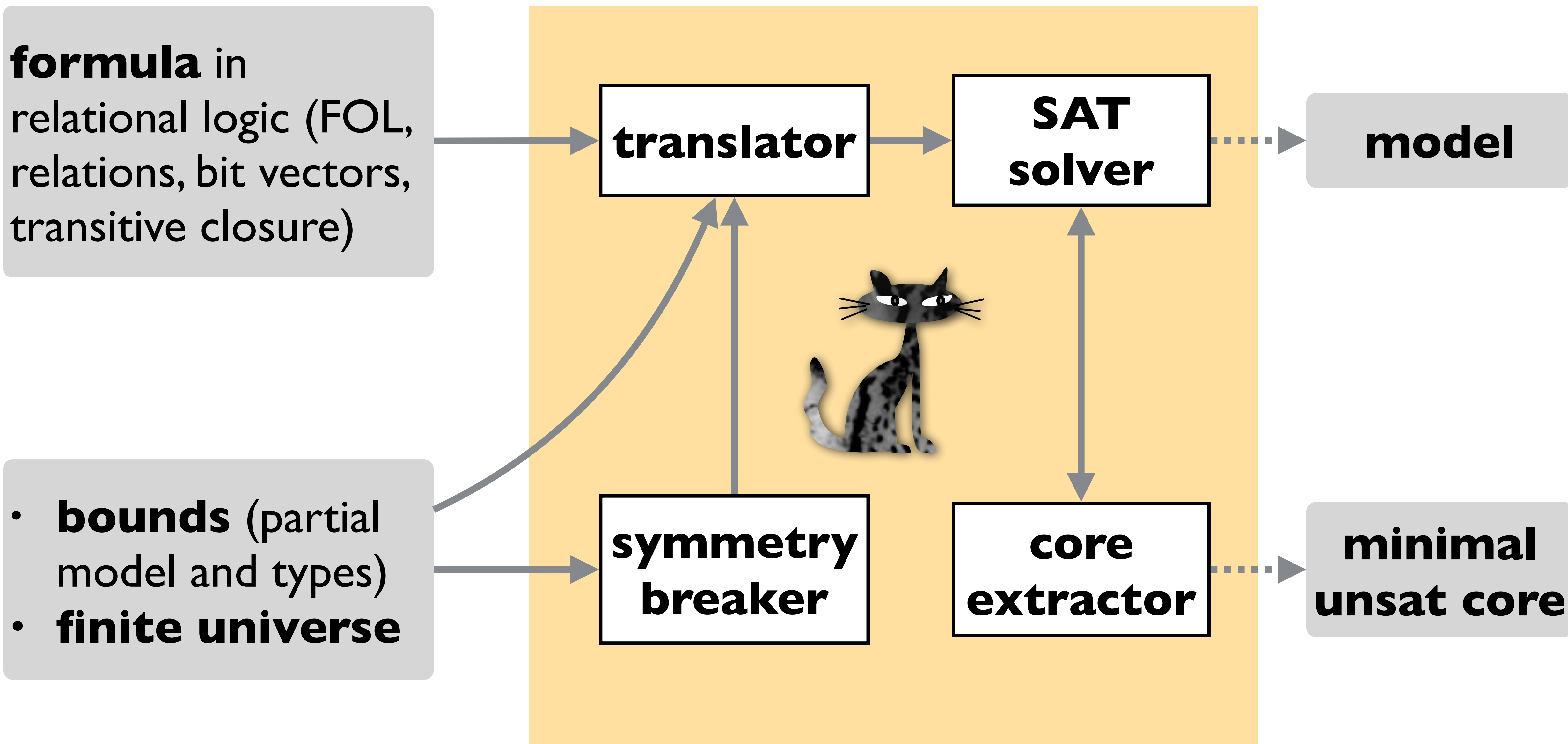
Bounded verification of code and memory models (Forge, Miniatur, TACO, MemSAT)

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

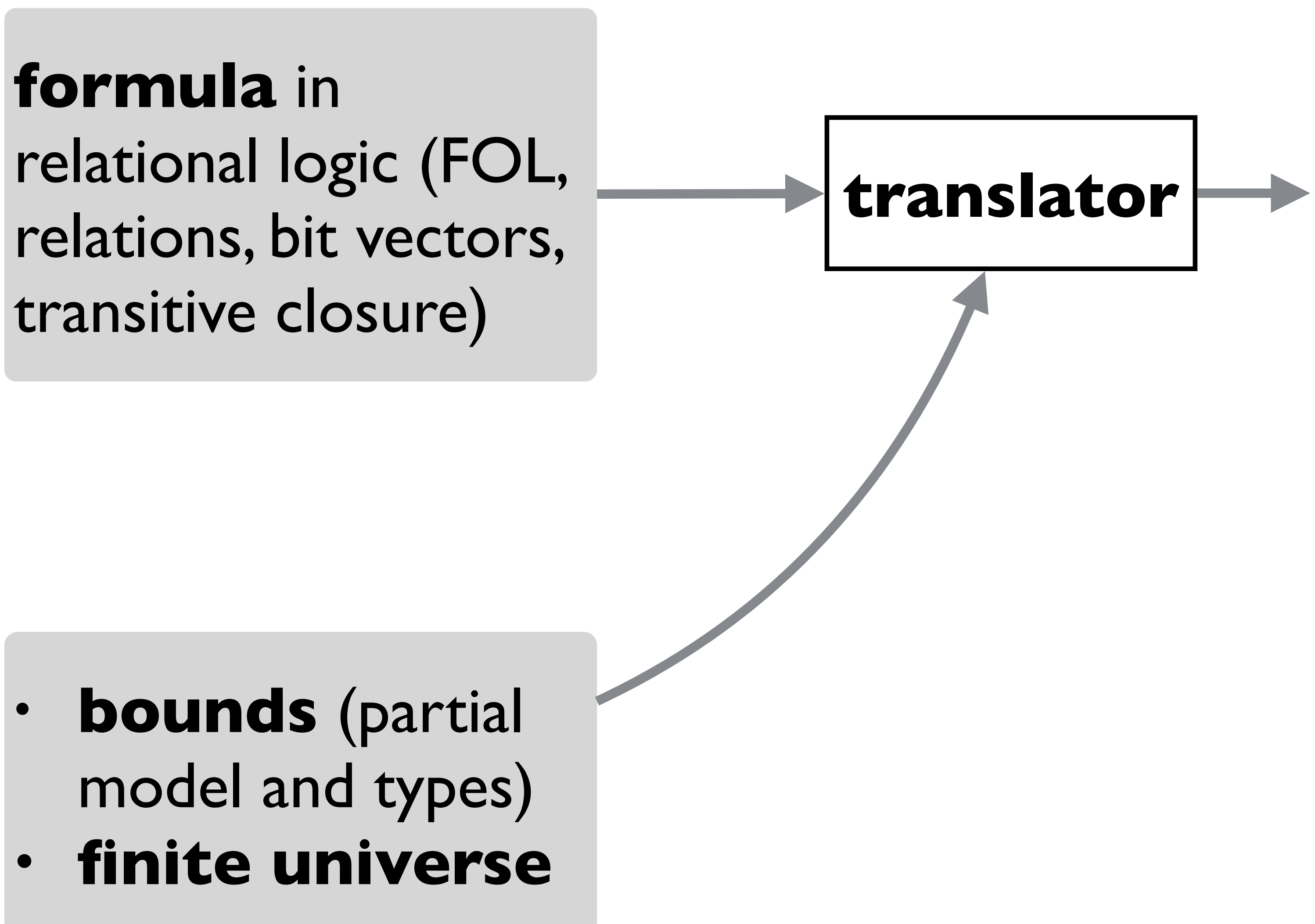


KODKOD

Overview of Kodkod



Overview of Kodkod



Relational logic by example

a minimalistic formal specification of a filesystem

Relational logic by example

$Root \subseteq Dir$

- The root of a filesystem hierarchy is a directory.

Relational logic by example

Root ⊆ Dir

contents ⊆ Dir × (File ∪ Dir)

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

Relational logic by example

$Root \subseteq Dir$

$contents \subseteq Dir \times (File \cup Dir)$

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

- 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

$Root \subseteq Dir$

$contents \subseteq Dir \times (File \cup Dir)$

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

$\forall\, d: Dir \mid \neg\, (d \subseteq d.\hat{}contents)$

- 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

$Root \subseteq Dir$

$contents \subseteq Dir \times (File \cup Dir)$

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

$\forall\, d: Dir \mid \neg\, (d \subseteq d.\hat{}contents)$

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

Finite universe of interpretation.

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

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

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

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

Bounded relational logic by example

Root ⊆ Dir

contents ⊆ Dir × (File ∪ Dir)

(File ∪ Dir) ⊆ Root.*contents

∀ d: Dir | ¬ (d ⊆ d.^contents)

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

Finite universe of interpretation.

{⟨**R**⟩} ⊆ Root ⊆ {⟨**R**⟩}

{} ⊆ Dir ⊆ {⟨**R**⟩, ⟨$\mathbf{D_1}$⟩, ⟨$\mathbf{D_2}$⟩}

{} ⊆ File ⊆ {⟨$\mathbf{F_1}$⟩, ⟨$\mathbf{F_2}$⟩}

{} ⊆ contents ⊆ {**R**, $\mathbf{D_1}$, $\mathbf{D_2}$} × {**R**, $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{F_1}$, $\mathbf{F_2}$}

Bounds for each relation:

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

Bounded relational logic by example

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

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

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

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

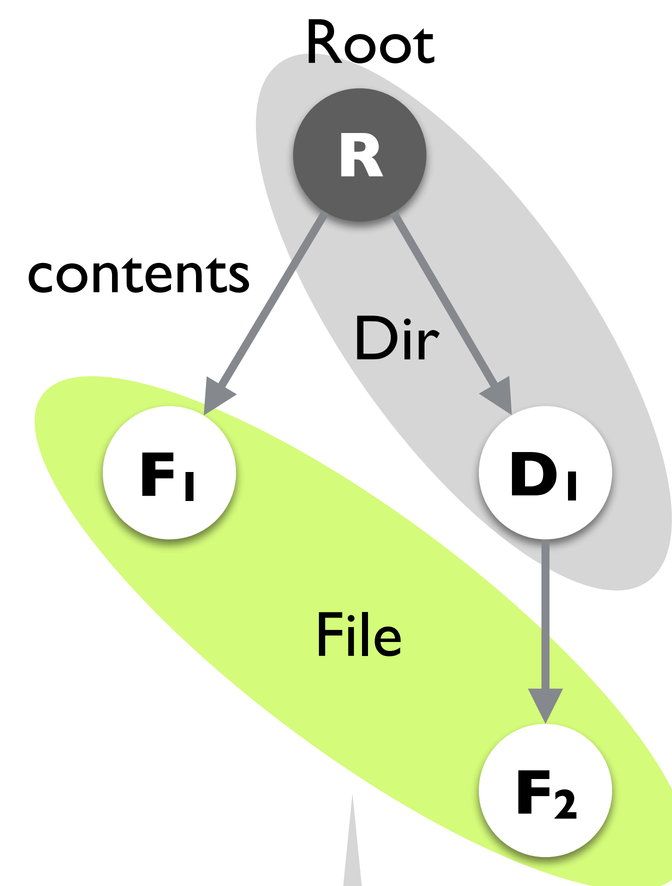
$\{\ \mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\ \}$

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

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

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

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



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

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

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

$\text{contents} = \{\langle \mathbf{R}, \mathbf{F_1} \rangle, \langle \mathbf{R}, \mathbf{D_1} \rangle, \langle \mathbf{D_1}, \mathbf{F_2} \rangle\}$

Translation by example

$\mathrm{Root} \subseteq \mathrm{Dir}$

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

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

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

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

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

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

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

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

Translation by example

Root ⊆ Dir

contents ⊆ Dir × (File ∪ Dir)

(File ∪ Dir) ⊆ Root.*contents

∀ d: Dir | ¬ (d ⊆ d.^contents)

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

{⟨$\mathbf{R}$⟩} ⊆ Root ⊆ {⟨$\mathbf{R}$⟩}

{} ⊆ Dir ⊆ {⟨$\mathbf{R}$⟩, ⟨$\mathbf{D_1}$⟩, ⟨$\mathbf{D_2}$⟩}

{} ⊆ File ⊆ {⟨$\mathbf{F_1}$⟩, ⟨$\mathbf{F_2}$⟩}

{} ⊆ contents ⊆ {$\mathbf{R}$, $\mathbf{D_1}$, $\mathbf{D_2}$} × {$\mathbf{R}$, $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{F_1}$, $\mathbf{F_2}$}

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**
1	0	0	0	0

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

Relational constants as boolean matrices

R	$\mathbf{D_1}$	$\mathbf{D_2}$	$\mathbf{F_1}$	$\mathbf{F_2}$
1	0	0	0	0

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

d_0	d_1	d_2	0	0

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

Relational constants as boolean matrices

R	$\mathbf{D_1}$	$\mathbf{D_2}$	$\mathbf{F_1}$	$\mathbf{F_2}$
1	0	0	0	0

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

d_0	d_1	d_2	0	0

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

0	0	0	f_0	f_1

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

Relational constants as boolean matrices

R	D_1	D_2	F_1	F_2
1	0	0	0	0

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

R	D_1	D_2	F_1	F_2
d_0	d_1	d_2	0	0

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

R	D_1	D_2	F_1	F_2
0	0	0	f_0	f_1

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

	R	D_1	D_2	F_1	F_2
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

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

Relational expressions as matrix operations

$$\overset{\text{File}}{\begin{bmatrix}0 & 0 & 0 & f_0 & f_1\end{bmatrix}} \vee \overset{\text{Dir}}{\begin{bmatrix}d_0 & d_1 & d_2 & 0 & 0\end{bmatrix}} = \overset{\text{File} \cup \text{Dir}}{\begin{bmatrix}d_0 & d_1 & d_2 & f_0 & f_1\end{bmatrix}}$$

$$\overset{\text{Dir}}{\begin{bmatrix}d_0 \\ d_1 \\ d_2 \\ 0 \\ 0\end{bmatrix}} \times \overset{\text{File} \cup \text{Dir}}{\begin{bmatrix}d_0 & d_1 & d_2 & f_0 & f_1\end{bmatrix}} = \overset{\text{Dir} \times (\text{File} \cup \text{Dir})}{\begin{bmatrix}d_0 \wedge d_0 & d_0 \wedge d_1 & d_0 \wedge d_2 & d_0 \wedge f_0 & d_0 \wedge f_1 \\ d_1 \wedge d_0 & d_1 \wedge d_1 & d_1 \wedge d_2 & d_1 \wedge f_0 & d_1 \wedge f_1 \\ d_2 \wedge d_0 & d_2 \wedge d_1 & d_2 \wedge d_2 & d_2 \wedge f_0 & d_2 \wedge f_1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0\end{bmatrix}}$$

Formulas as constraints over matrix entries

contents

c_0	c_1	c_2	c_3	c_4
c_5	c_6	c_7	c_8	c_9
c_{10}	c_{11}	c_{12}	c_{13}	c_{14}
0	0	0	0	0
0	0	0	0	0

$\rightarrow$

Dir × (File ∪ 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

=

contents ⊆ Dir × (File ∪ Dir)

$$
\begin{aligned}
&(c_0 \longrightarrow d_0 \wedge d_0) \wedge \\
&(c_1 \longrightarrow d_0 \wedge d_1) \wedge \\
&(c_2 \longrightarrow d_0 \wedge d_2) \wedge \\
&(c_3 \longrightarrow d_0 \wedge f_0) \wedge \\
&(c_4 \longrightarrow d_0 \wedge f_1) \wedge \\
&(c_5 \longrightarrow d_1 \wedge d_0) \wedge \\
&\ldots \\
&(c_{14} \longrightarrow d_2 \wedge f_1)
\end{aligned}
$$

Dealing with sparseness and redundancy

Dir × (File ∪ 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

Dir × (File ∪ 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.

Dir × (File ∪ 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

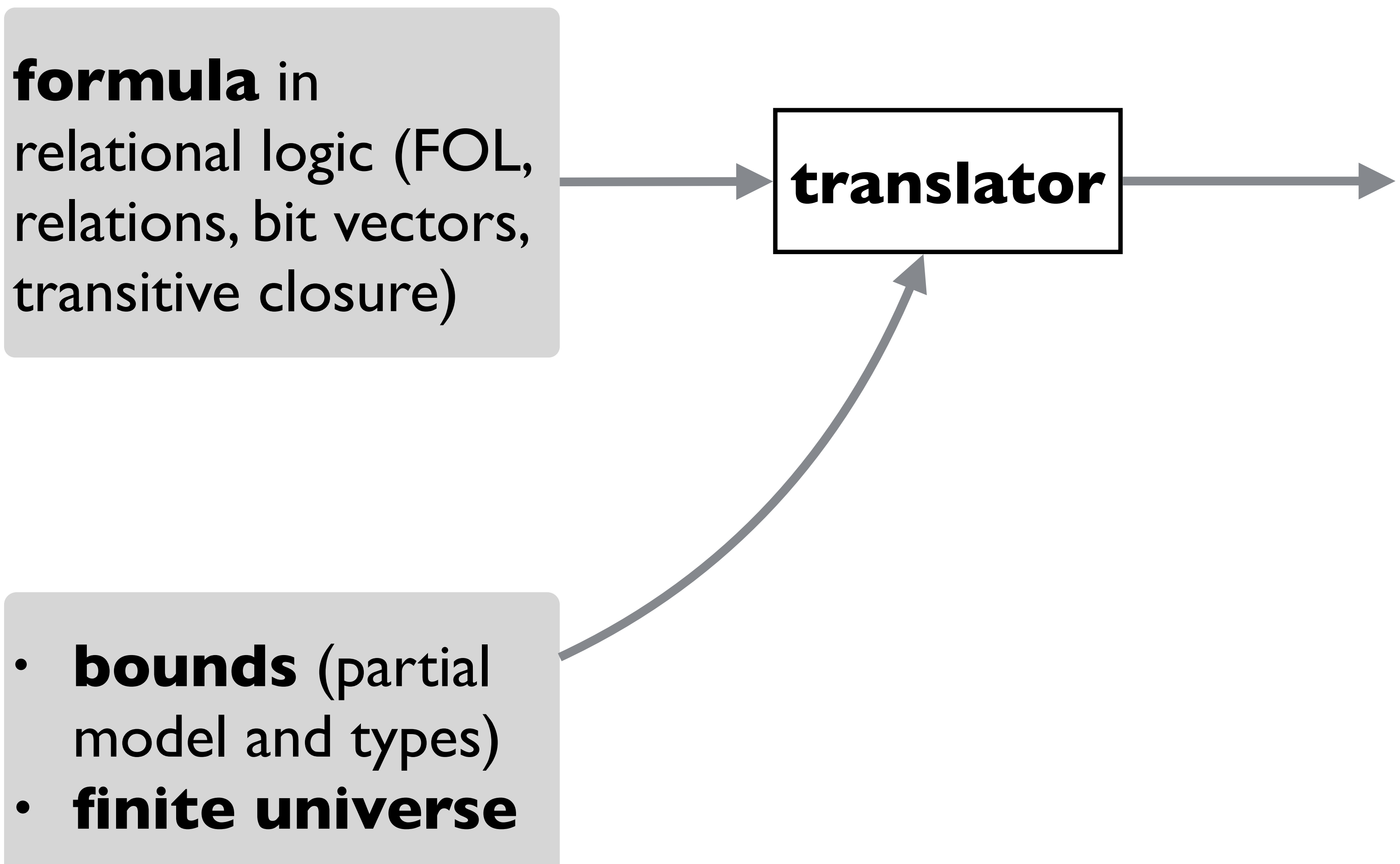
Dir × (File ∪ Dir)

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

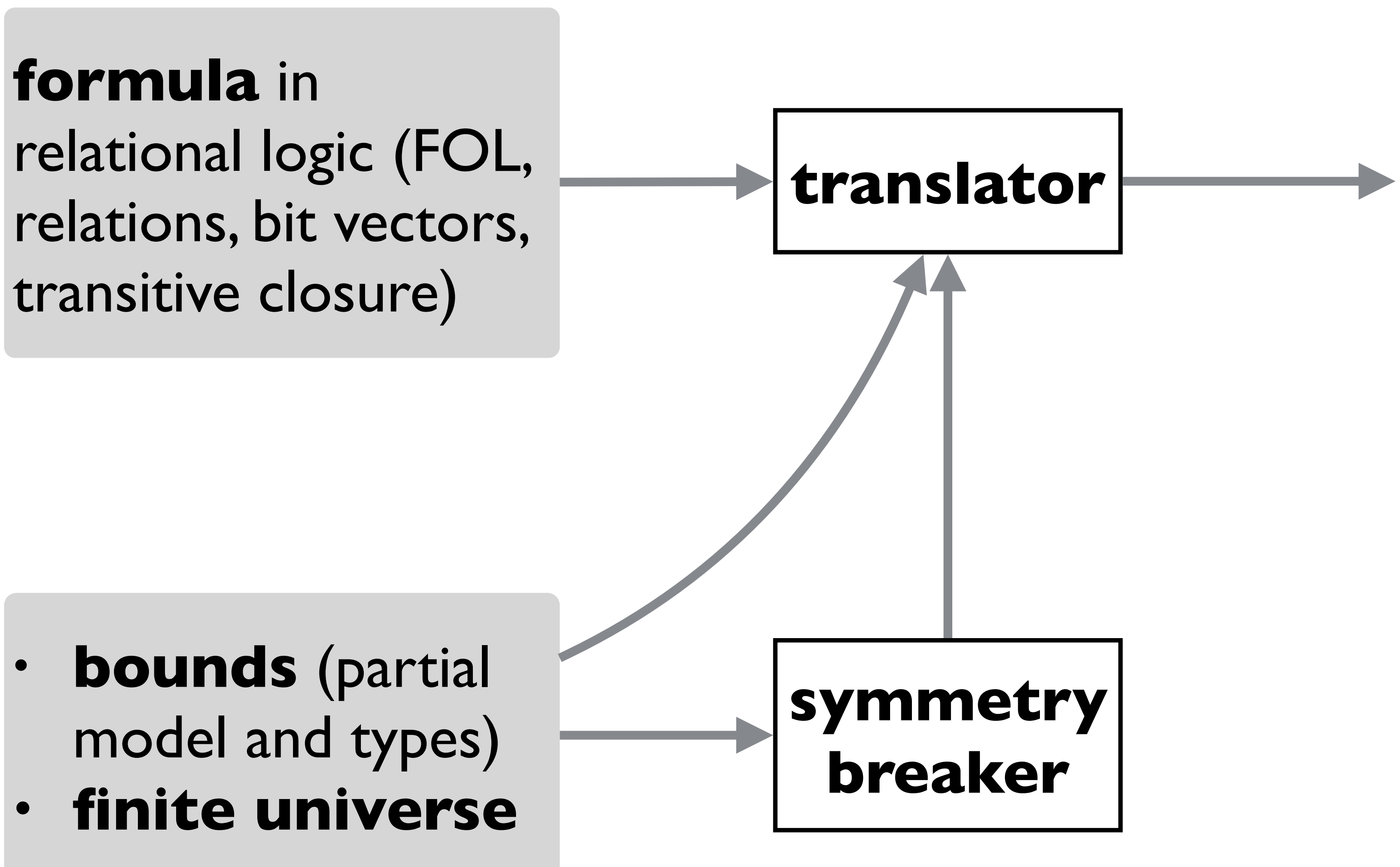
Compact Boolean Circuits (CBCs).

Sparse matrices represented as interval trees.

Overview of Kodkod



Overview of Kodkod



Symmetry by example

Root ⊆ Dir

contents ⊆ Dir × (File ∪ Dir)

(File ∪ Dir) ⊆ Root.*contents

∀ d: Dir | ¬ (d ⊆ d.^contents)

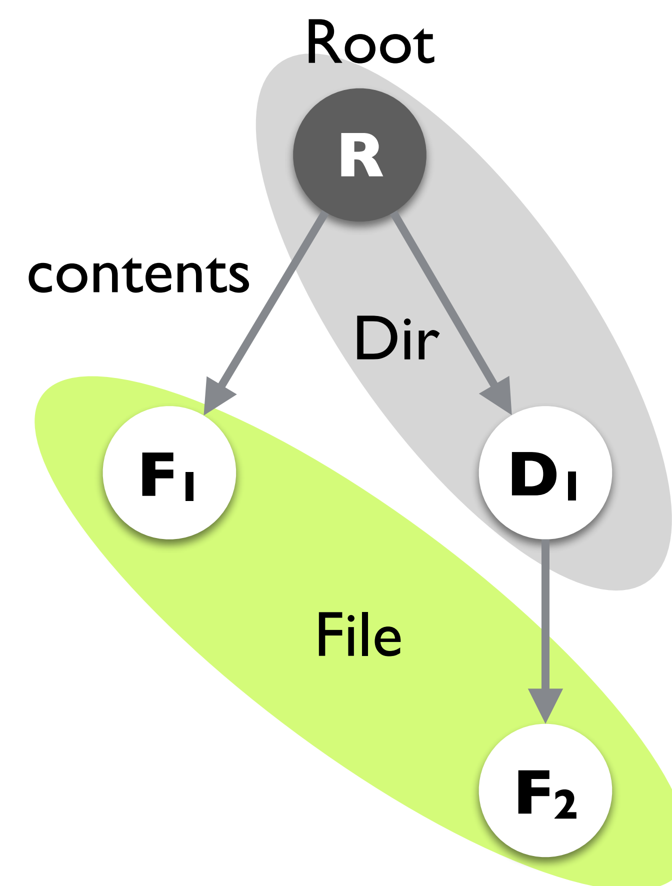
{ $\mathbf{R}$, $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{F_1}$, $\mathbf{F_2}$ }

{⟨$\mathbf{R}$⟩} ⊆ Root ⊆ {⟨$\mathbf{R}$⟩}

{} ⊆ Dir ⊆ {⟨$\mathbf{R}$⟩, ⟨$\mathbf{D_1}$⟩, ⟨$\mathbf{D_2}$⟩}

{} ⊆ File ⊆ {⟨$\mathbf{F_1}$⟩, ⟨$\mathbf{F_2}$⟩}

{} ⊆ contents ⊆ {$\mathbf{R}$, $\mathbf{D_1}$, $\mathbf{D_2}$} × {$\mathbf{R}$, $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{F_1}$, $\mathbf{F_2}$}



Symmetry by example

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

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

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

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

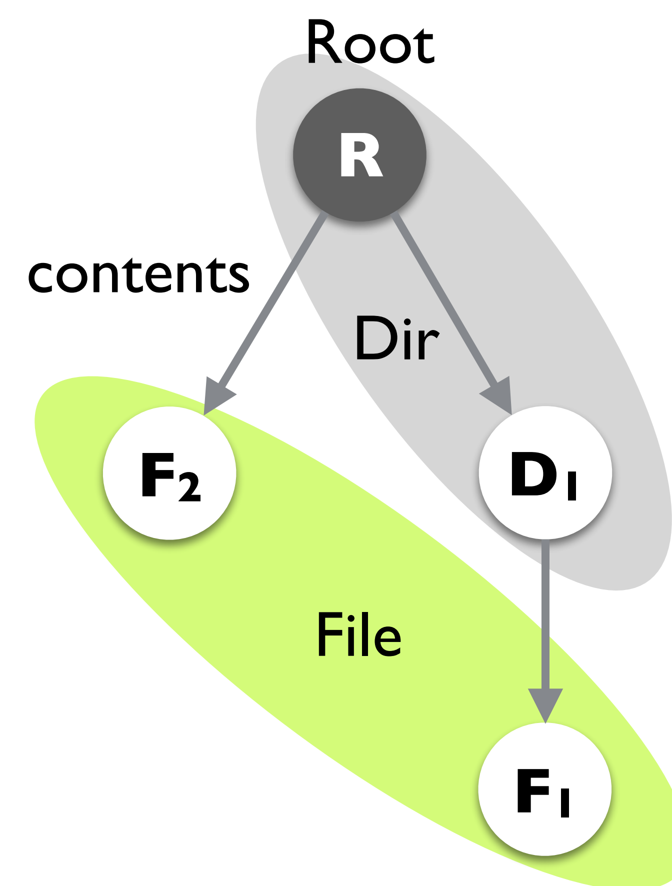
$\{\ \mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\ \}$

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

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

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

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



Symmetry by example

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

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

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

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

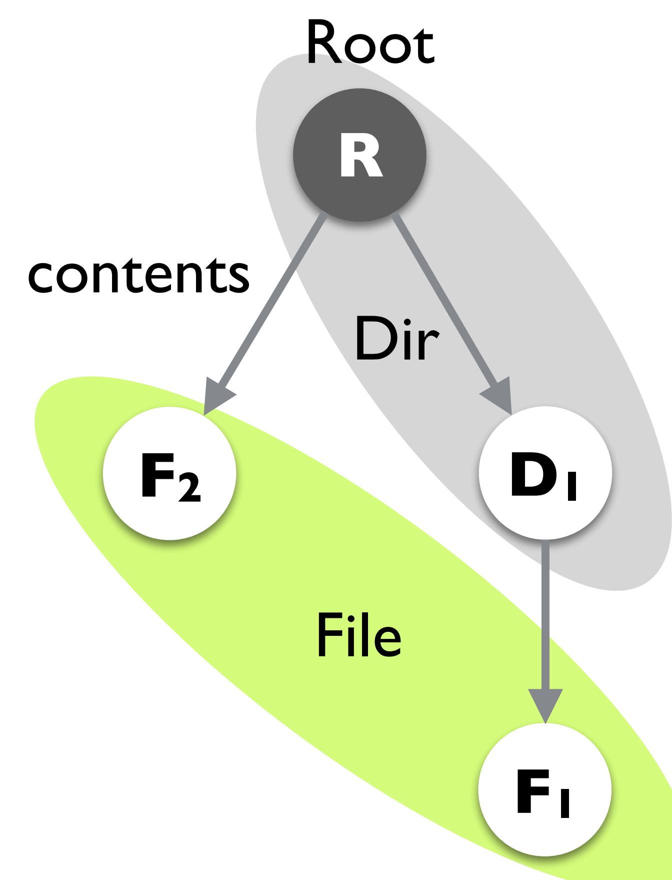
$\{\ \mathbf{R}, \mathbf{D}\ \mathbf{D_2}\ \mathbf{F_1}, \mathbf{F_2}\ \}$

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

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

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

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



Symmetry by example

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

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

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

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

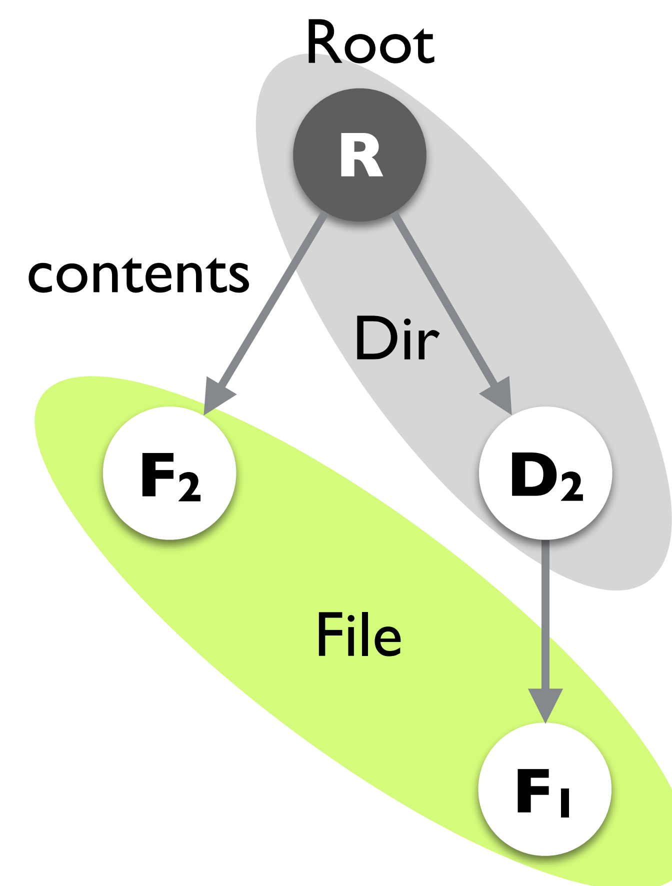
$\{\ \mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\ \}$

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

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

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

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



Symmetries between models

Root ⊆ Dir

contents ⊆ Dir × (File ∪ Dir)

(File ∪ Dir) ⊆ Root.*contents

∀ d: Dir | ¬ (d ⊆ d.^contents)

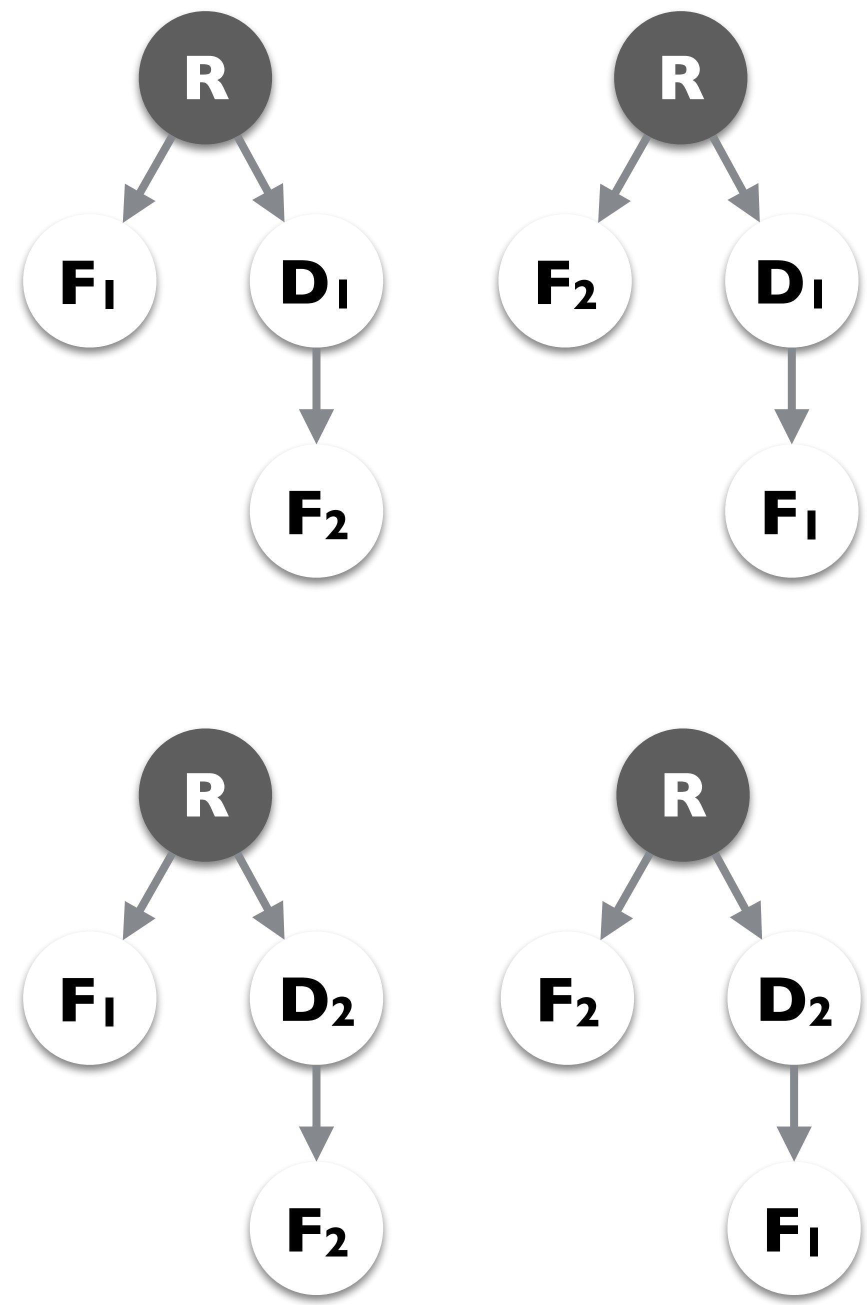
{ **R**, **D₁**, **D₂**, **F₁**, **F₂** }

{⟨**R**⟩} ⊆ Root ⊆ {⟨**R**⟩}

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

{} ⊆ File ⊆ {⟨**F₁**⟩, ⟨**F₂**⟩}

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



Symmetries between non-models

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

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

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

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

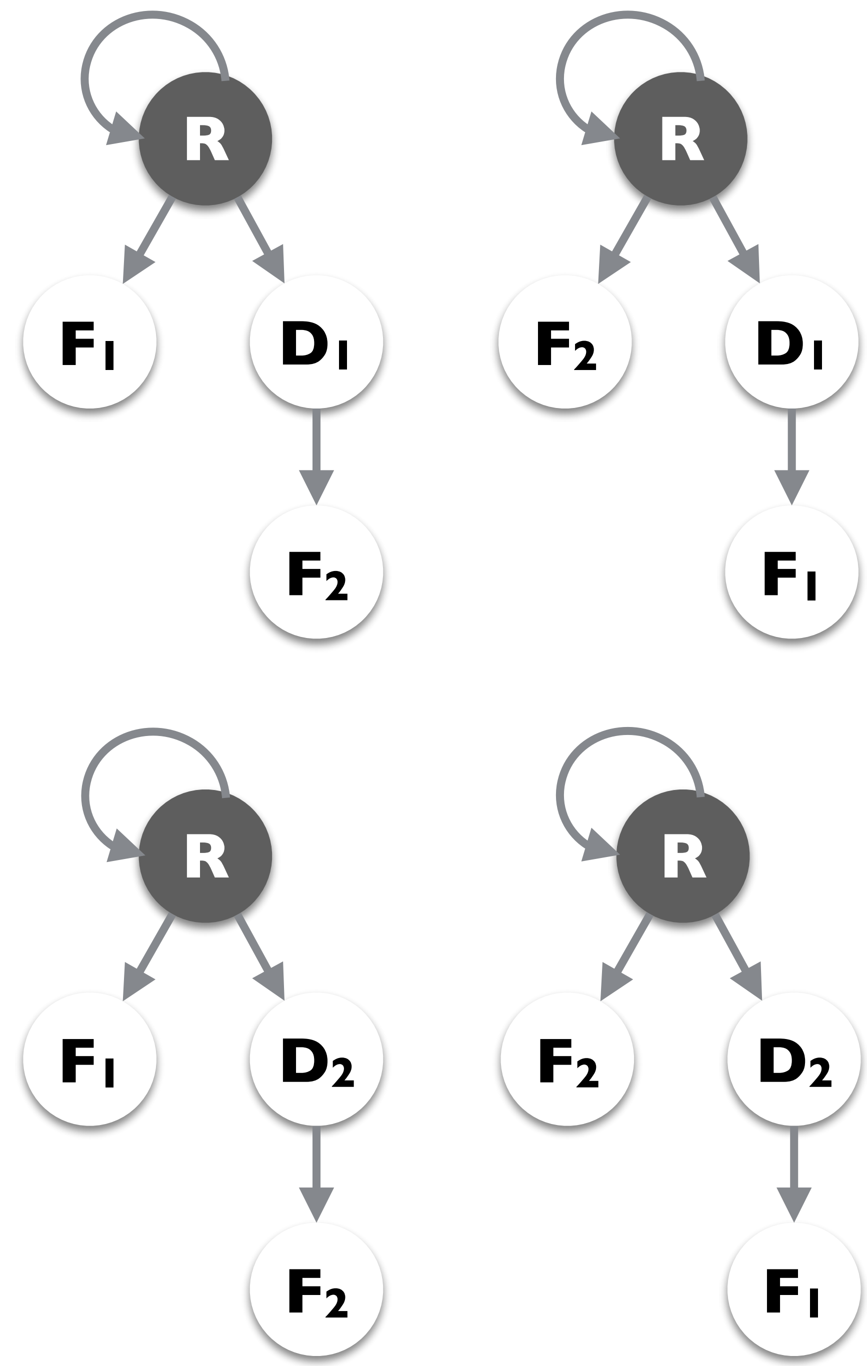
$\{\ \mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\ \}$

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

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

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

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



Symmetries induce equivalence classes

Root $\subseteq$ Dir

contents $\subseteq$ Dir $\times$ (File $\cup$ Dir)

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

$\forall$ d: Dir | $\neg$ (d $\subseteq$ d.^contents)

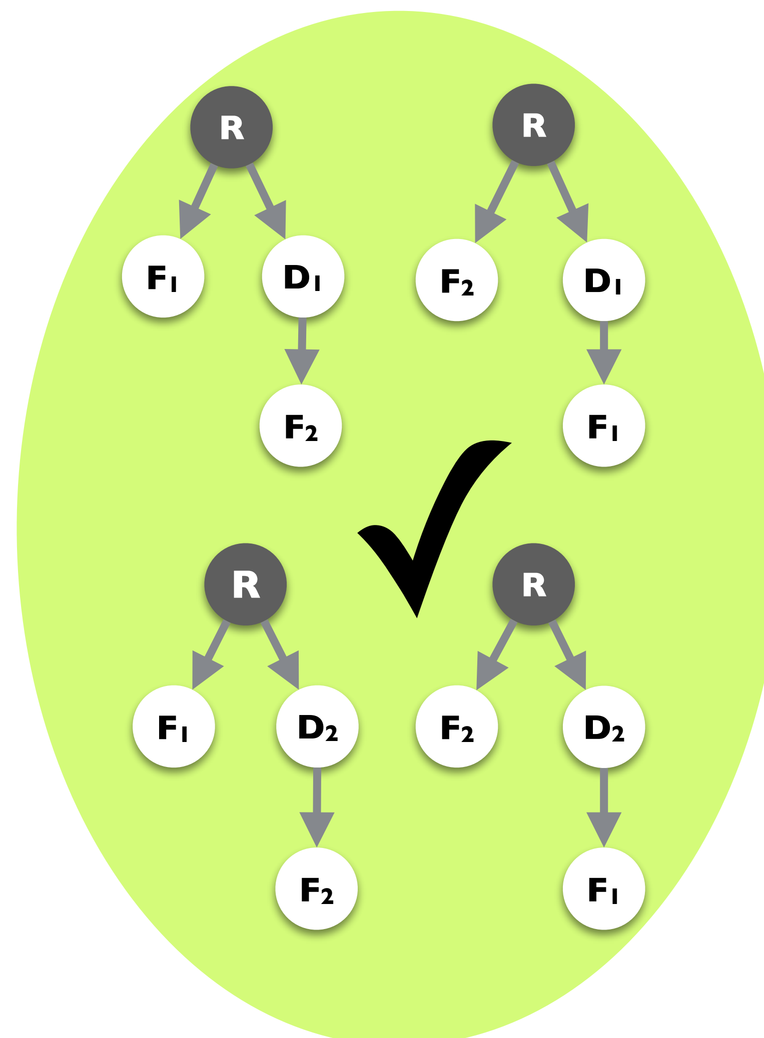
{ **R**, **D$_1$**, **D$_2$**, **F$_1$**, **F$_2$** }

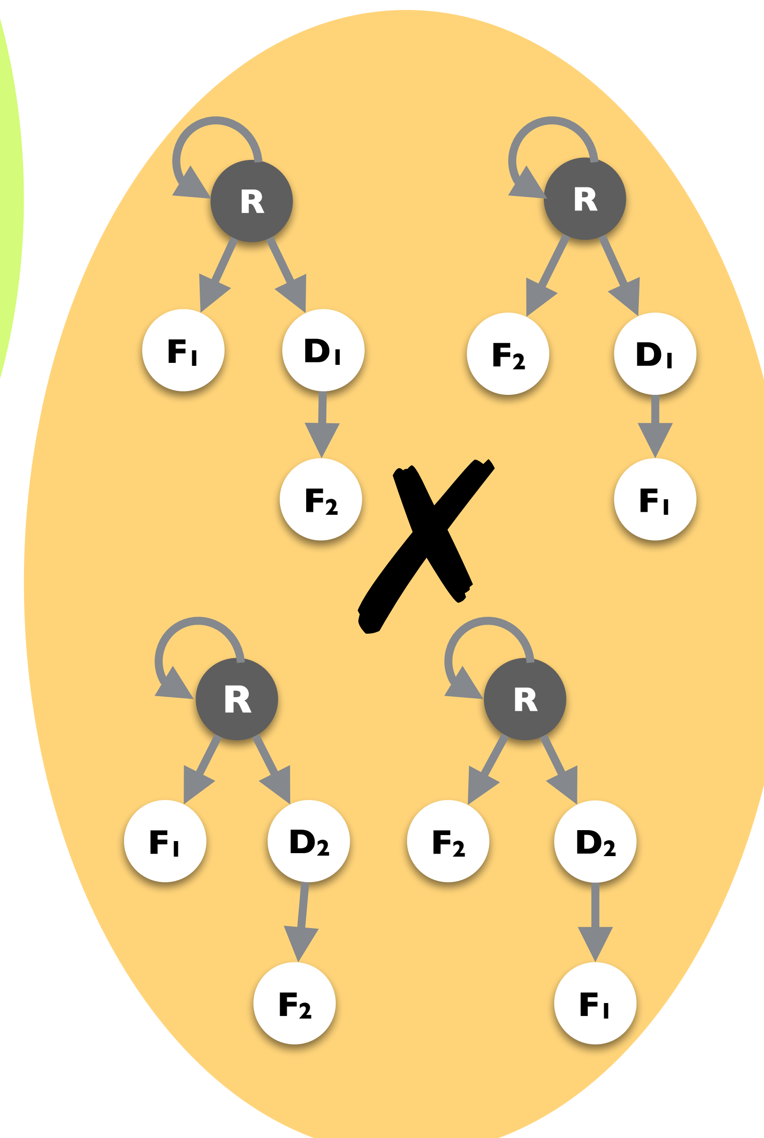
{⟨**R**⟩} $\subseteq$ Root $\subseteq$ {⟨**R**⟩}

{} $\subseteq$ Dir $\subseteq$ {⟨**R**⟩, ⟨**D$_1$**⟩, ⟨**D$_2$**⟩}

{} $\subseteq$ File $\subseteq$ {⟨**F$_1$**⟩, ⟨**F$_2$**⟩}

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





Symmetries induce equivalence classes

Root ⊆ Dir

contents ⊆ Dir × (File ∪ Dir)

(File ∪ Dir) ⊆ Root.*contents

∀ d: Dir | ¬ (d ⊆ d.^contents)

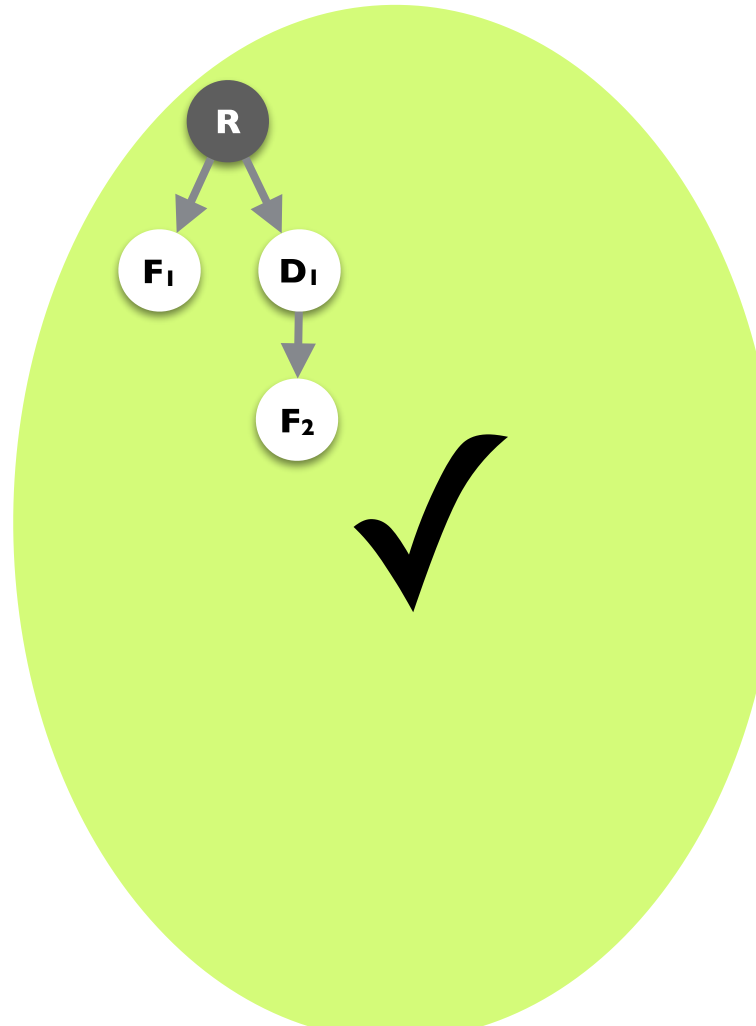
$\{\ \mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\ \}$

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

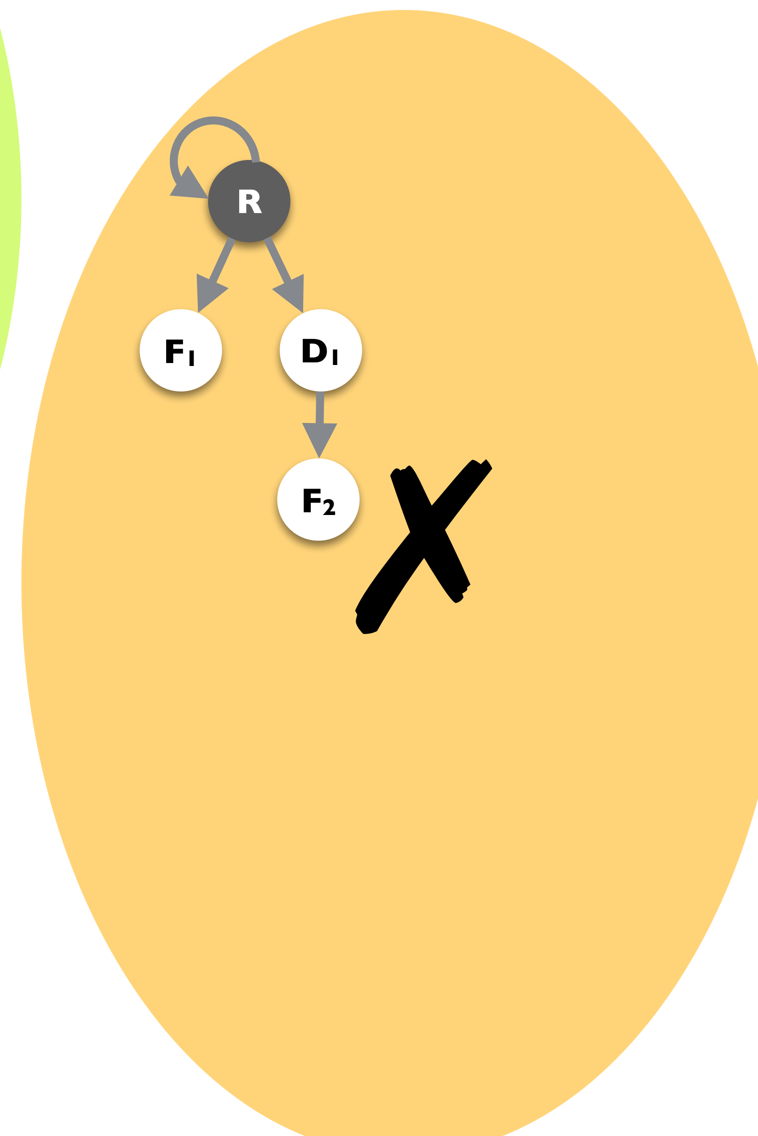
$\{\} \subseteq \text{Dir} \subseteq \{\langle\mathbf{R}\rangle, \langle\mathbf{D_1}\rangle, \langle\mathbf{D_2}\rangle\}$

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

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



Sufficient to check one interpretation per equivalence class.



Symmetry detection

Root $\subseteq$ Dir

contents $\subseteq$ Dir × (File $\cup$ Dir)

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

$\forall$ d: Dir | $\neg$ (d $\subseteq$ d.^contents)

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

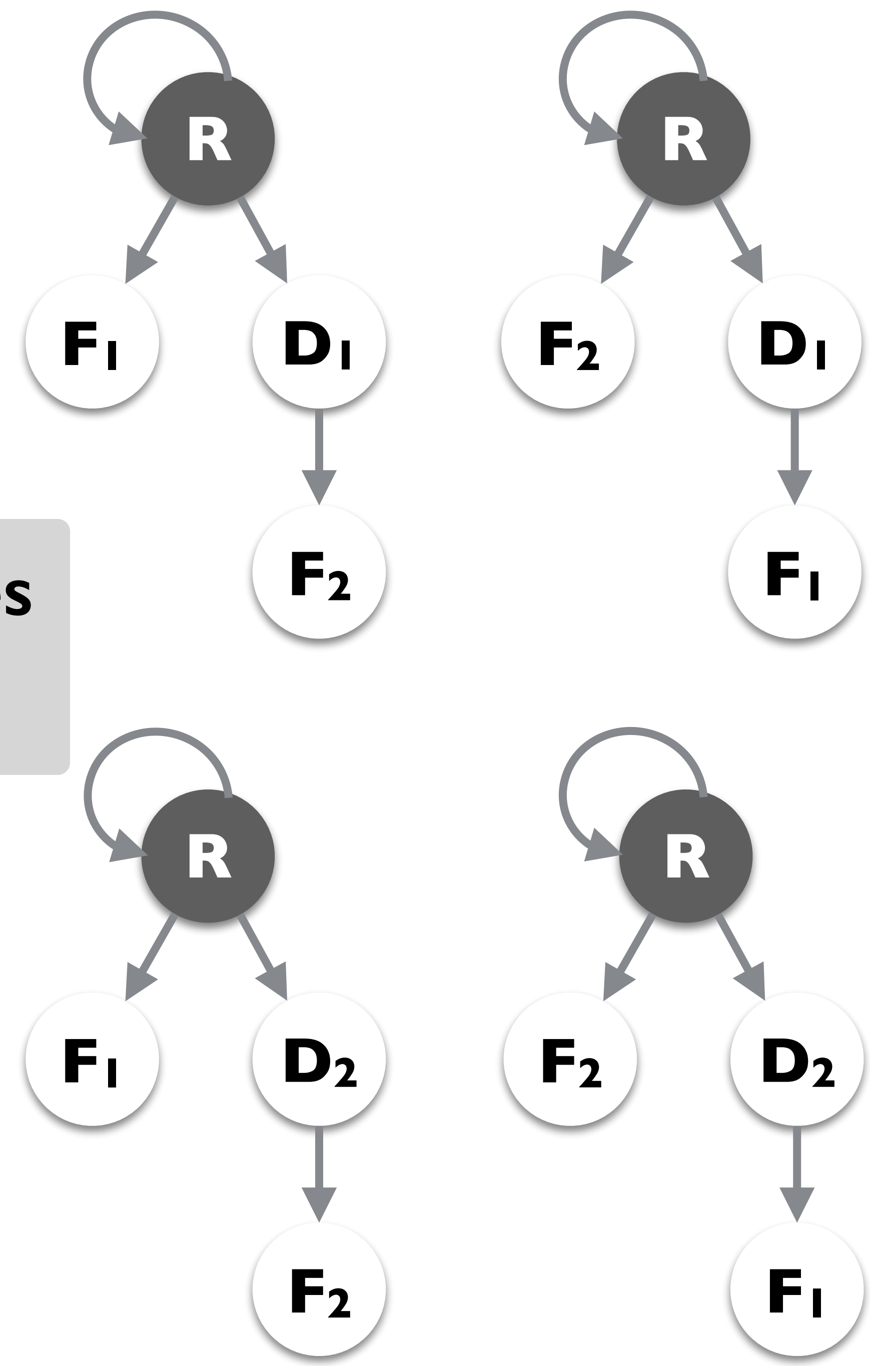
Interpretation symmetries
= bound symmetries

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

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

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

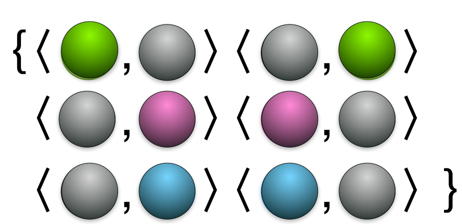
$\{\} \subseteq \text{contents} \subseteq \{\mathbf{R}, \mathbf{D_1}, \mathbf{D_2}\} \times \{\mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\}$

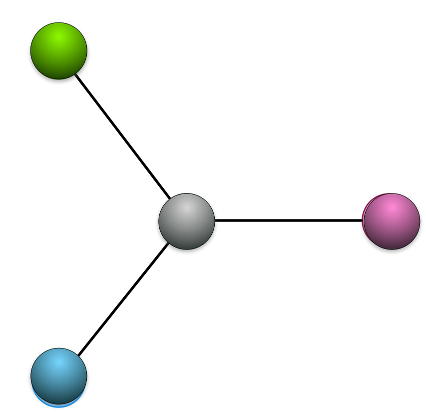


Detecting symmetries is hard …

Interpretation symmetries
= bound symmetries

Graph automorphism
detection





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

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

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

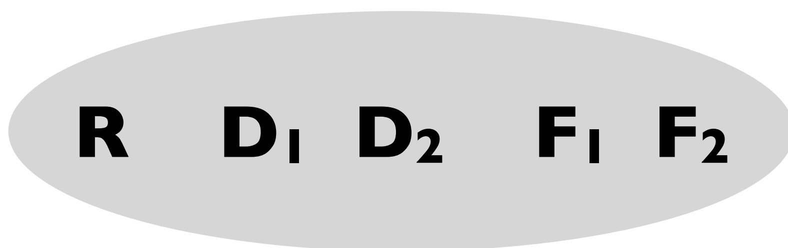
$\{\} \subseteq \text{Dir} \subseteq \{\langle\mathbf{R}\rangle, \langle\mathbf{D_1}\rangle, \langle\mathbf{D_2}\rangle\}$

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

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

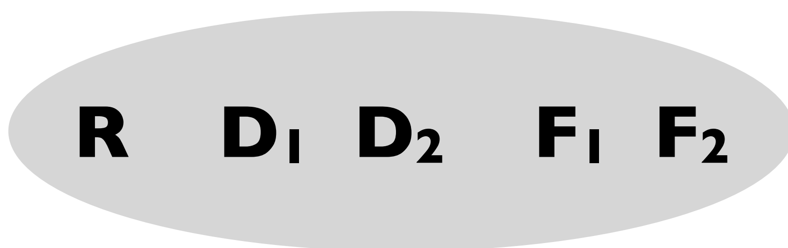
The coarsest partition of the universe such that each non-empty bound is expressible as a union of products of parts.

Finding the base partitioning



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

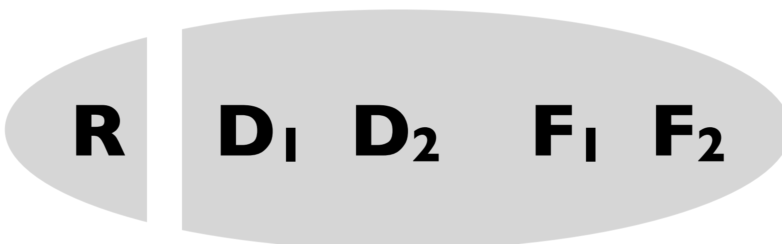
Finding the base partitioning



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

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

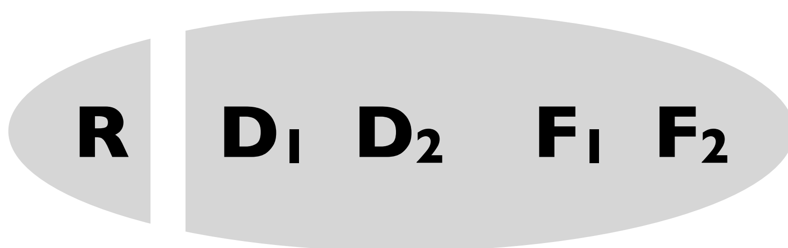
Finding the base partitioning



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

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

Finding the base partitioning



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

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

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

Finding the base partitioning

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

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

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

Finding the base partitioning

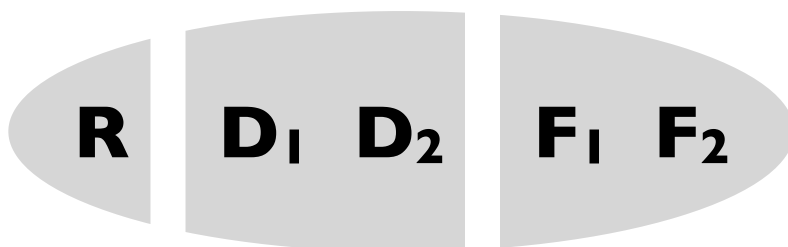
$\{\langle \mathbf{R} \rangle\} \subseteq \mathrm{Root} \subseteq \{\langle \mathbf{R} \rangle\}$

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

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

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

Finding the base partitioning



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

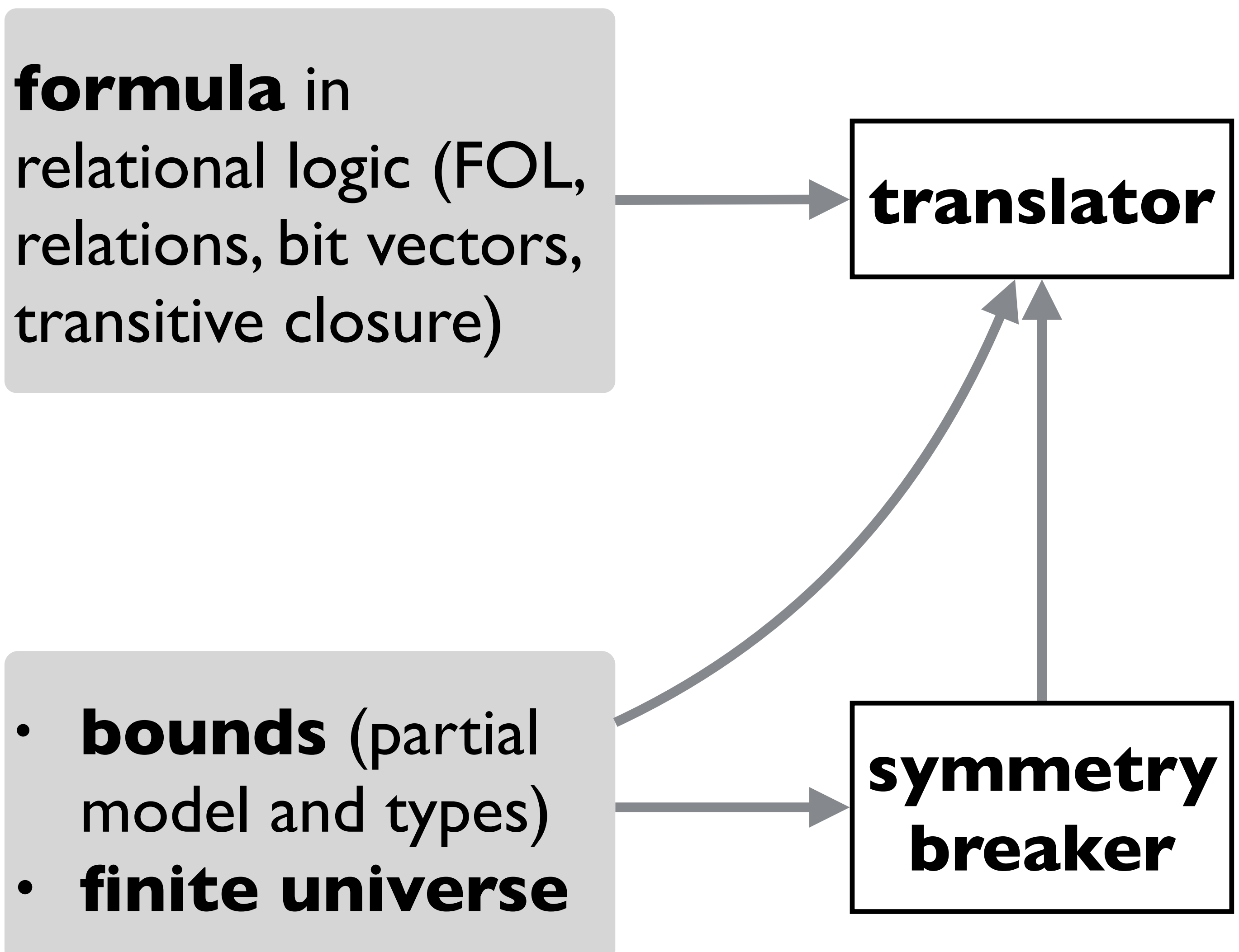
$\{\} \subseteq \mathrm{Dir} \subseteq \{\langle \mathbf{R} \rangle, \langle \mathbf{D_1} \rangle, \langle \mathbf{D_2} \rangle\}$

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

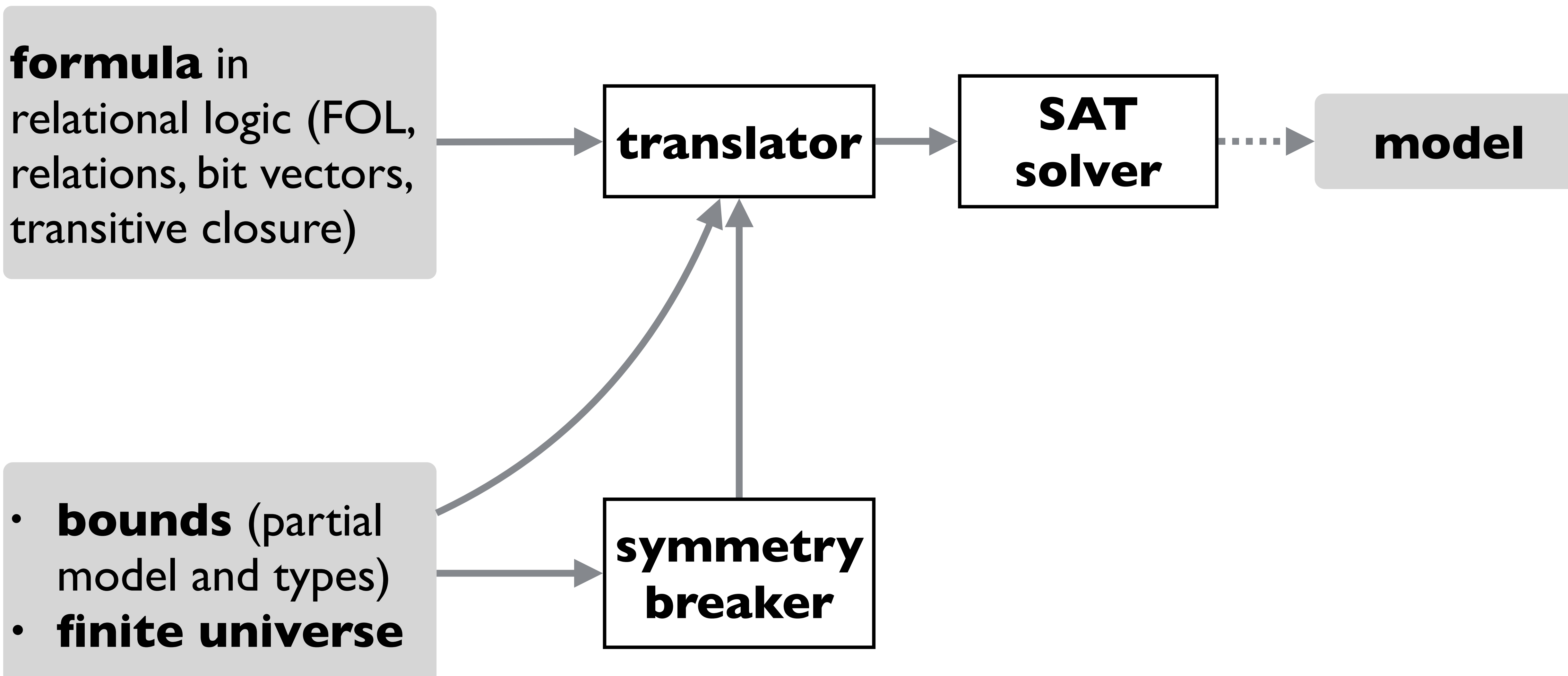
$\{\} \subseteq \mathrm{contents} \subseteq \{\mathbf{R}, \mathbf{D_1}, \mathbf{D_2}\} \times \{\mathbf{R}, \mathbf{D_1}, \mathbf{D_2}, \mathbf{F_1}, \mathbf{F_2}\}$

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

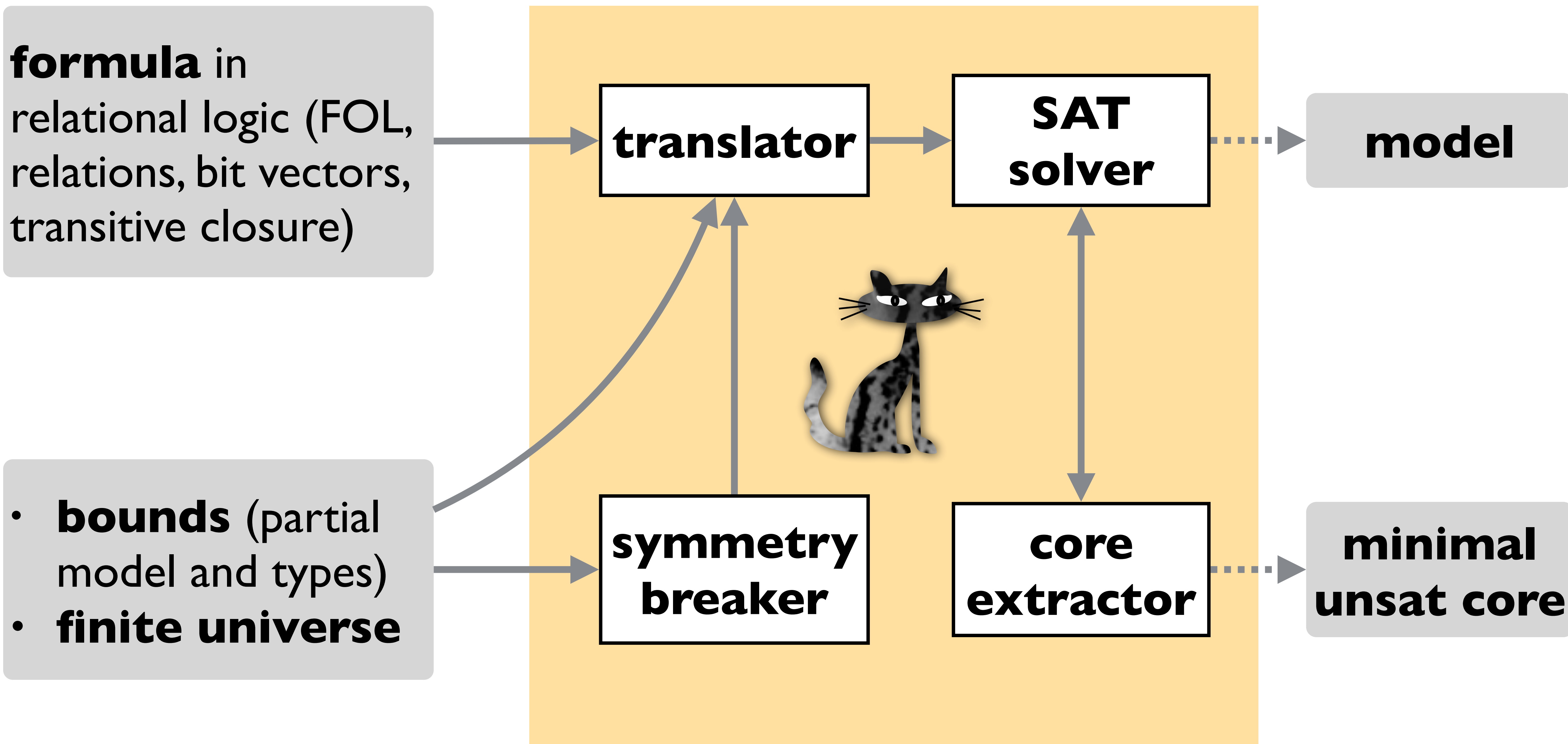
Overview of Kodkod



Overview of Kodkod



Overview of Kodkod



A bug in the tiny filesystem

Root $\subseteq$ Dir

contents $\subseteq$ Dir × (File $\cup$ Dir)

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

$\forall$ d: Dir | $\neg$ (d $\subseteq$ d.^contents)

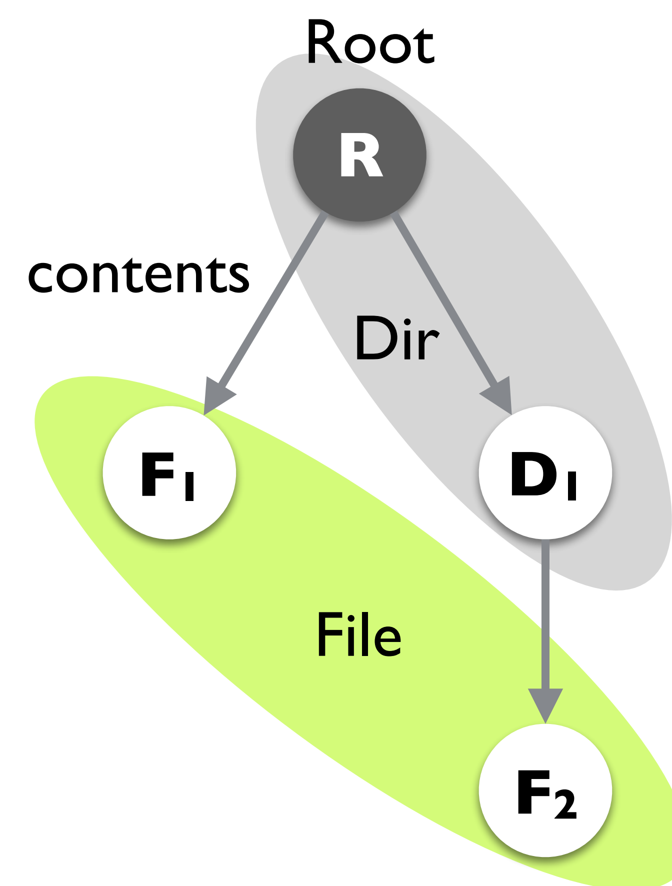
{ $\mathbf{R}$, $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{F_1}$, $\mathbf{F_2}$ }

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

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

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

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



A bug in the tiny filesystem

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

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

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

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

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

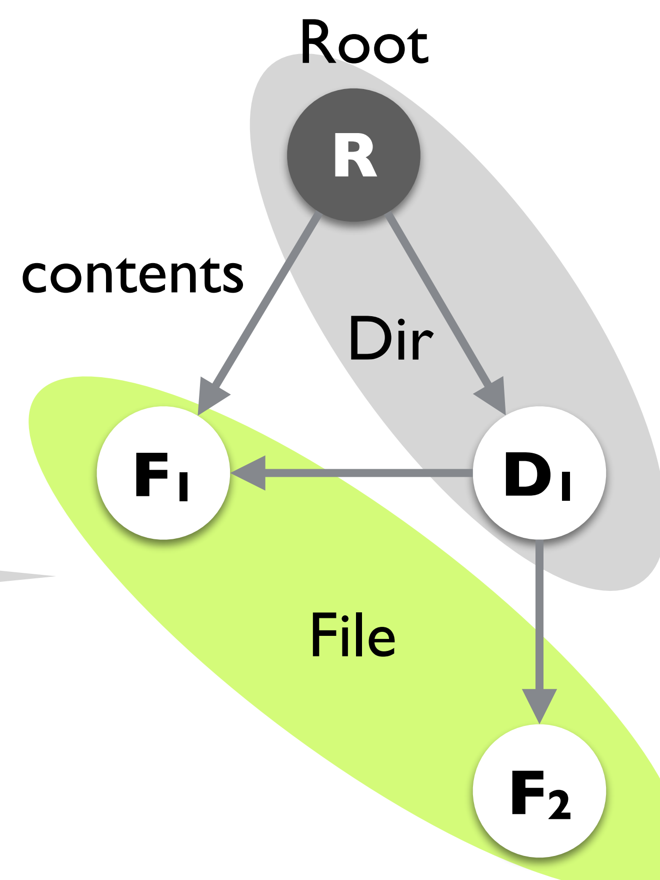
$\{\langle\mathbf{R}\rangle\} \subseteq \text{Root} \subseteq \{\langle\mathbf{R}\rangle\}$

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

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

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

The spec allows multiple parents.



Fixing the tiny filesystem

$Root \subseteq Dir$

$contents \subseteq Dir \times (File \cup Dir)$

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

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

$\forall\ f: File \mid one\ contents.f$

$\forall\ d: Dir \mid one\ contents.d$

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

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

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

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

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

Fixing the tiny filesystem

$Root \subseteq Dir$

$contents \subseteq Dir \times (File \cup Dir)$

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

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

$\forall\ f: File \mid one\ contents.f$

$\forall\ d: Dir \mid one\ contents.d$

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

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

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

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

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

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

Resolution-based core extraction

Root ⊆ Dir

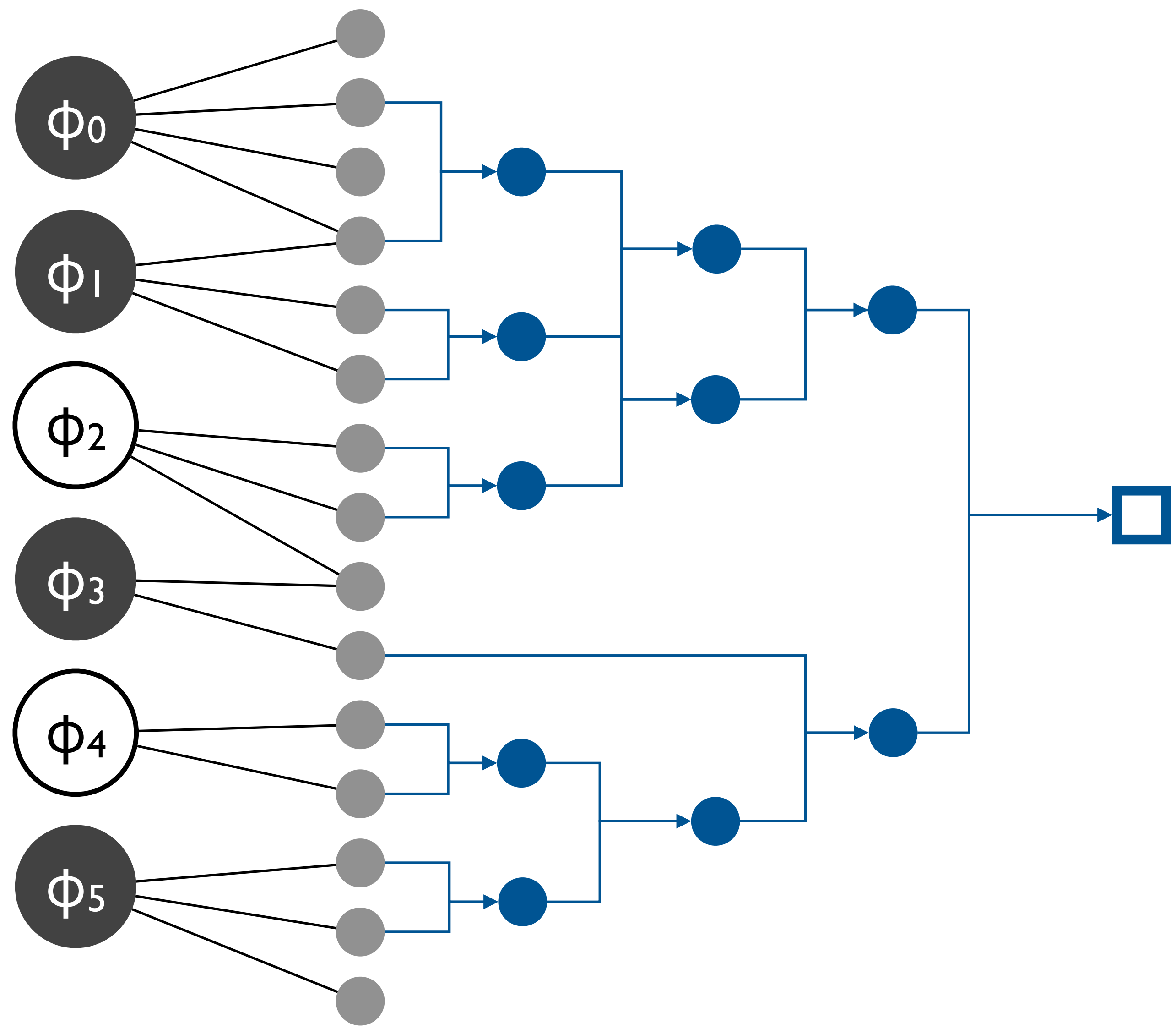
contents ⊆ Dir × (File ∪ Dir)

(File ∪ Dir) ⊆ Root.*contents

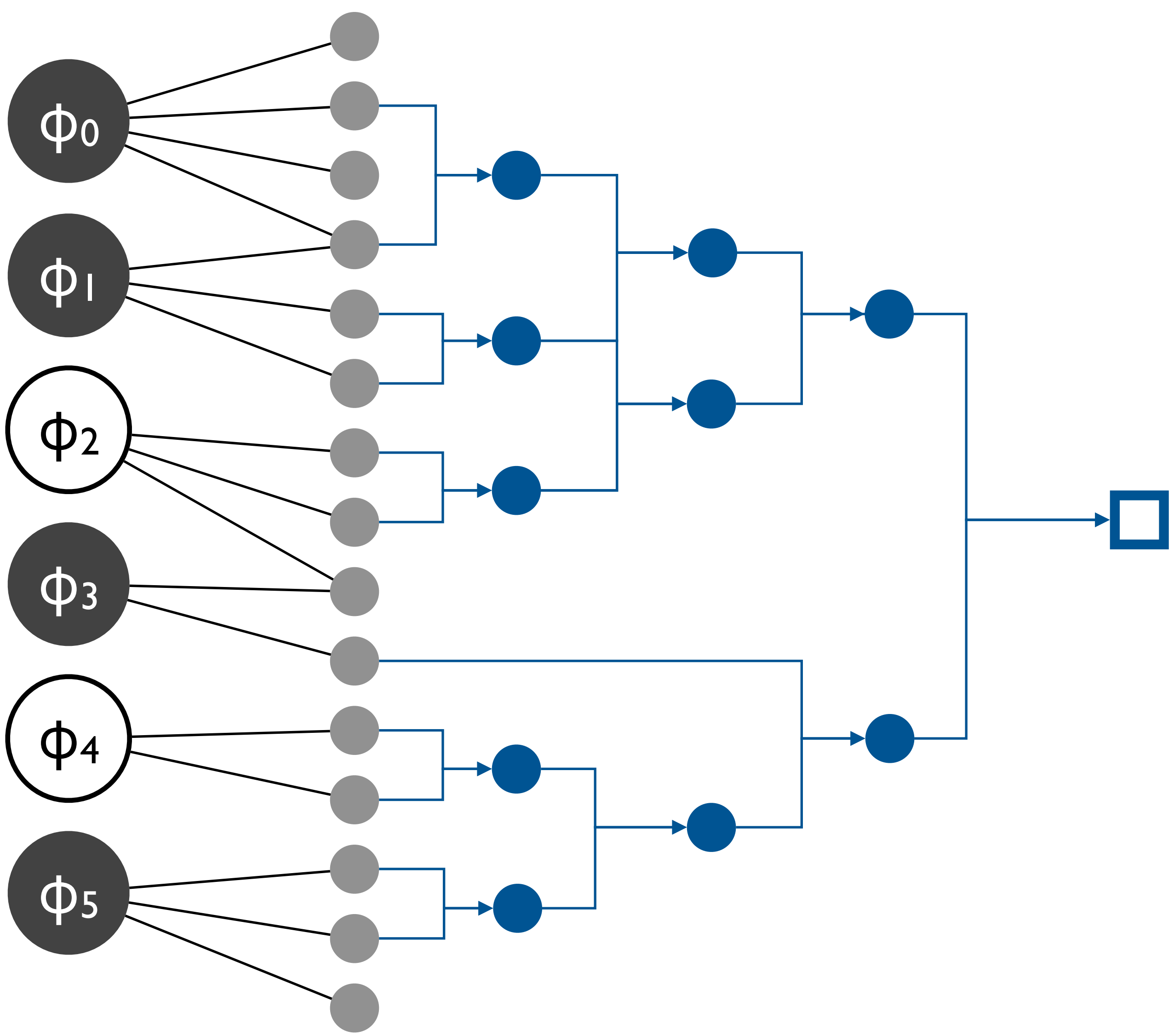
∀ d: Dir | ¬ (d ⊆ d.^contents)

∀ f: File | one contents.f

∀ d: Dir | one contents.d



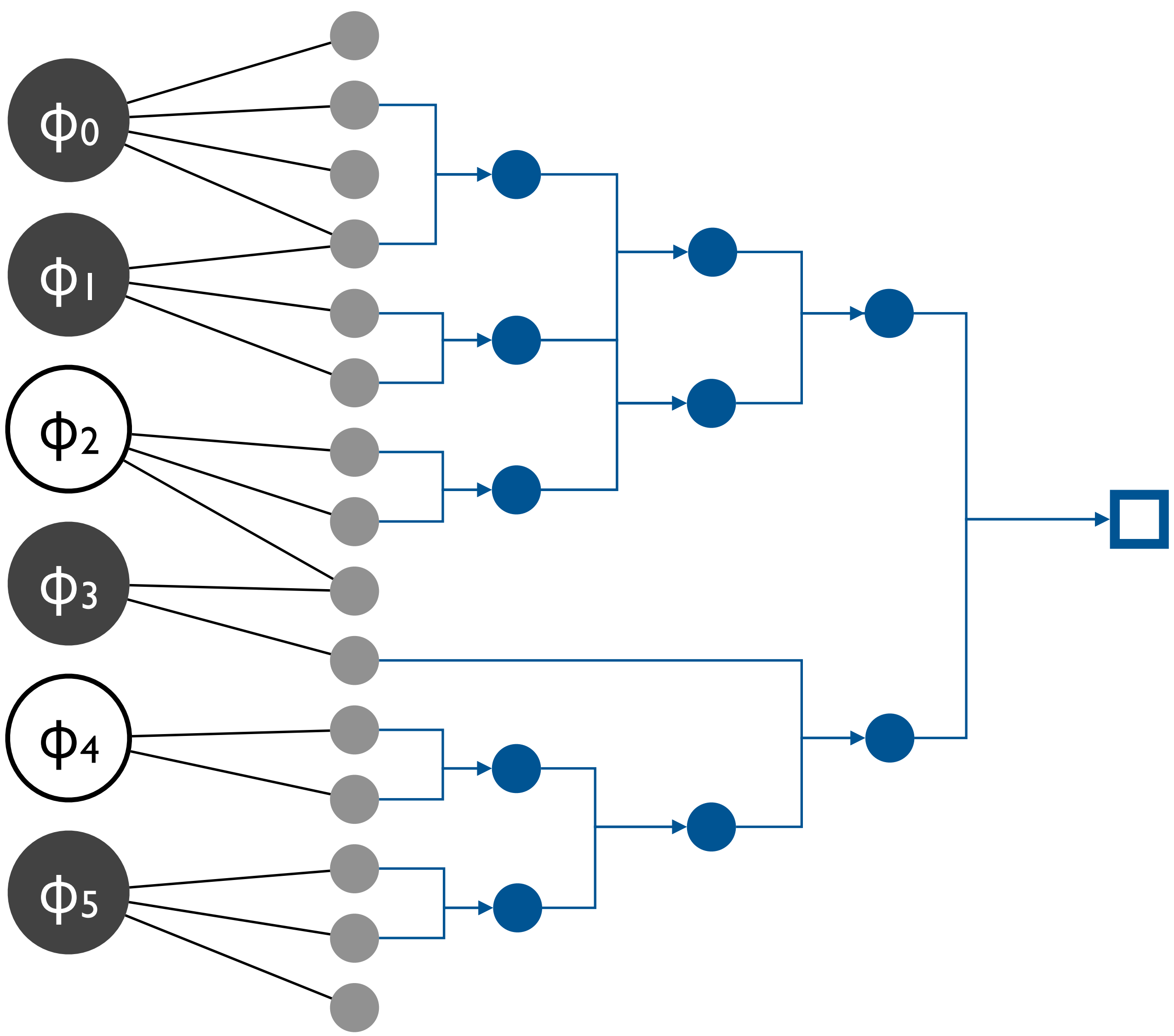
High-level minimal cores from low-level proofs



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