Symbolic Execution with Separating Decision Diagrams

Josh Berdine

O'Hearn Fest
14 January 2024
London

From an old talk...

The Spatial Assertion Workbench

Josh Berdine

Queen Mary, University of London

Email: berdine@dcs.qmul.ac.uk

(Joint work with Cristiano Calcagno, Peter O'Hearn, and Hongseok Yang)

AVoCS'02 16 April 2002

...a long-standing TODO item

SAW: Improvements

SAW is a "proof of concept" prototype

Improvements include

- a model checker better than enumerate all the states!

  BDDs, symbolic MC, compact representation of sets of states (heaps) which supports splitting
- pointer arithmetic
- GUI

...a long-standing TODO item

SAW: Improvements

SAW is a "proof of concept" prototype

Improvements include

- a model checker better than enumerate all the states!

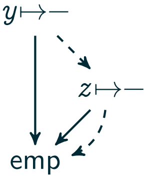
  BDDs, symbolic MC, compact representation of sets of states (heaps) which supports splitting

- pointer arithmetic

- GUI

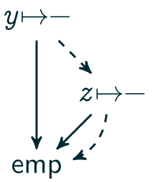
∗DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x{\mapsto}{-} \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$



∗DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x{\mapsto}- \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$

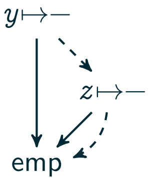


Semantics:

- consider each path from root to emp
- take atoms preceding solid “then” edges
- ∗-conjoin them all with emp
- disjoin ∗-conjunctions for all paths

$*$DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x \mapsto - \mid \cdots \mid x = y \mid x \neq y \mid \cdots$



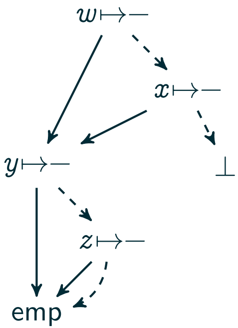
Semantics:

- consider each path from root to emp
- take atoms preceding solid “then” edges
- $*$-conjoin them all with emp
- disjoin $*$-conjunctions for all paths

Paths	DNF
$y \mapsto - \longrightarrow \mathsf{emp}$	$y \mapsto - * \mathsf{emp}$
$y \mapsto - \dashrightarrow z \mapsto - \longrightarrow \mathsf{emp}$	$\vee\ z \mapsto - * \mathsf{emp}$
$y \mapsto - \dashrightarrow z \mapsto - \dashrightarrow \mathsf{emp}$	$\vee\ \mathsf{emp}$

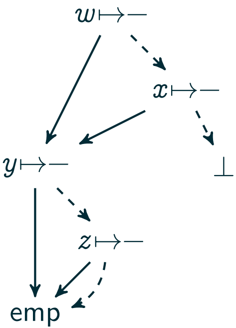
$*$DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A$ $\qquad$ $\mathbf{A} ::= x {\mapsto} - \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$



$*$DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x {\mapsto} - \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$

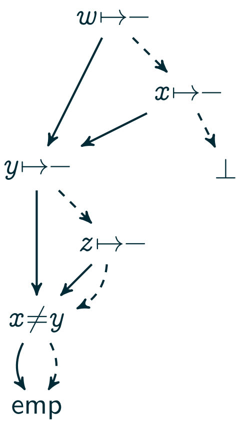


DNF

$$
\begin{aligned}
& w{\mapsto}- * y{\mapsto}- \\
\vee\ & w{\mapsto}- * z{\mapsto}- \\
\vee\ & w{\mapsto}- \\
\vee\ & x{\mapsto}- * y{\mapsto}- \\
\vee\ & x{\mapsto}- * z{\mapsto}- \\
\vee\ & x{\mapsto}-
\end{aligned}
$$

$*$DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x{\mapsto}{-} \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$

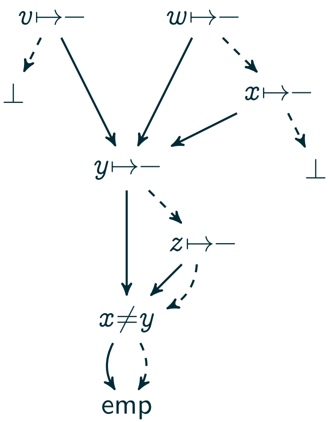


DNF

$$
\begin{aligned}
& w{\mapsto}{-} * y{\mapsto}{-} * x{\neq}y \\
\vee\ & w{\mapsto}{-} * y{\mapsto}{-} \\
\vee\ & w{\mapsto}{-} * z{\mapsto}{-} * x{\neq}y \\
\vee\ & w{\mapsto}{-} * z{\mapsto}{-} \\
\vee\ & w{\mapsto}{-} * x{\neq}y \\
\vee\ & w{\mapsto}{-} \\
\vee\ & x{\mapsto}{-} * y{\mapsto}{-} * x{\neq}y \\
\vee\ & x{\mapsto}{-} * y{\mapsto}{-} \\
\vee\ & x{\mapsto}{-} * z{\mapsto}{-} * x{\neq}y \\
\vee\ & x{\mapsto}{-} * z{\mapsto}{-} \\
\vee\ & x{\mapsto}{-} * x{\neq}y \\
\vee\ & x{\mapsto}{-}
\end{aligned}
$$

$*$DDs: Separating Decision Diagrams

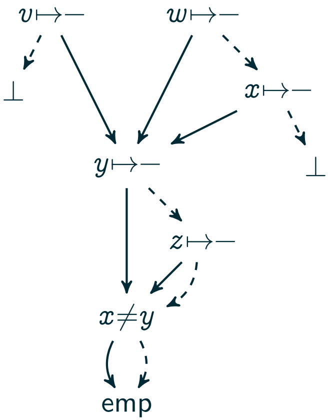
$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x{\mapsto}- \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$



- One DAG for all formulas
  - Multiple roots
  - Diagram rooted by each node represents a (sub)formula
  - Share subformulas between all formulas

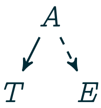
$*$DDs: Separating Decision Diagrams

$\mathbf{F} ::= \bot \mid \mathsf{emp} \mid F \vee F \mid F * F \mid A \qquad \mathbf{A} ::= x{\mapsto}- \mid \cdots \mid x{=}y \mid x{\neq}y \mid \cdots$



- Diagrams subject to several invariants (later)
- Ignoring sharing and invariants, diagram nodes as formulas:

$$\mathbf{Q} ::= \bot \mid \mathsf{emp} \mid A{*}Q \vee Q$$



$$\equiv \quad A{*}T \vee E$$

BDDs: Binary Decision Diagrams

- Randal E. Bryant: Graph-Based Algorithms for Boolean Function Manipulation. IEEE Trans. Computers 35(8): 677-691 (1986)
  - Donald Knuth: "one of the only really fundamental data structures that came out in the last twenty-five years"
- Propose to use BDDs in a way inspired by symbolic model checking
  - Kenneth L. McMillan: Symbolic Model Checking: An Approach to the State Explosion Problem. Ph.D. Thesis, Carnegie Mellon University (1992)
- ZDDs: variant of BDDs with modified core data structure invariants
  - Shin-ichi Minato: Zero-Suppressed BDDs for Set Manipulation in Combinatorial Problems. DAC 1993: 272-277

ZDDs: Zero-Suppressed BDDs

- Key: can't say "if a, b, and c then false"
  - instead phrase positively, express ways to achieve included cases, everything else excluded
- Well-suited to sparse combinatorial problems
  - BDDs omit "don't care" elements
  - ZDDs need not mention absent elements
- Naturally viewed as representing "families" (i.e. sets) of sets of elements

ZDDs: Zero-Suppressed BDDs

- Key: can't say "if a, b, and c then false"
  - instead phrase positively, express ways to achieve included cases, everything else excluded
- Well-suited to sparse combinatorial problems
  - BDDs omit "don't care" elements
  - ZDDs need not mention absent elements
- Naturally viewed as representing "families" (i.e. sets) of sets of elements

- Pro: size can be exponentially smaller than enumerating all the possibilities (DNF)
- Con: size sometimes (necessarily) blows up
  - but worst case no worse than DNF
- State of the art for precise heap analyzers is DNF
  - relied on for relational constraints
  - there are some abstractions with Cartesian aspects
- Intuition: analogues of cases where BDDs blow up in traditional SMC are not natural

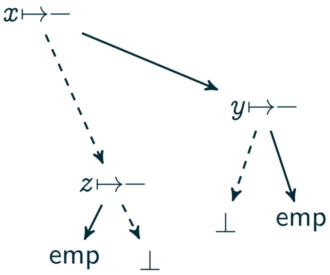
$*$DDs: Separating Decision Diagrams

- A $*$DD is a ZDD where elements are atomic SL formulas
  - family of sets of elements $\equiv$ disjunctions of starjunctions of atoms
  - i.e., a more compact representation of DNF
- Same core data structure invariants as (RO)ZDDs
  - $\exists$ total order on atoms, atoms appear in strictly decreasing order along every path
  - $\nexists$ duplicate subdiagrams, sharing must be introduced whenever possible
  - no "then" edge leads directly to $\perp$
- Guarantee the representation is canonical
  - any formulas equivalent when leaving atoms uninterpreted have same diagram
  - makes checking equality easy
  - enables detecting when to introduce, and capitalize on, sharing
- Define operations to account for spatial vs pure atomic formulas
  - do not represent starjunctions directly as *sets* since $A * A \iff \perp$ not $A * A \iff A$

Disjunction of $*$DDs

$$(w \mapsto - \vee ((x \mapsto - * z \mapsto -) \vee y \mapsto -))$$

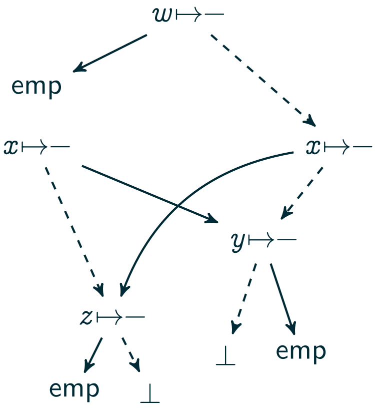
$$\bigvee ((x \mapsto - * y \mapsto -) \vee z \mapsto -)$$



Disjunction of $*$DDs

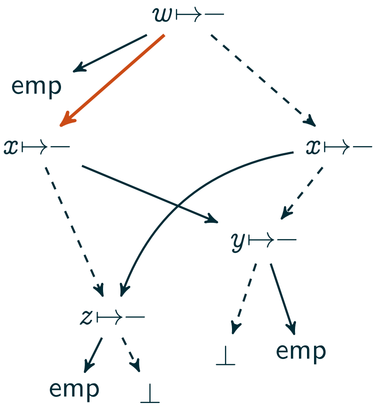
$$(w{\mapsto}- \vee ((x{\mapsto}- * z{\mapsto}-) \vee y{\mapsto}-))$$

$$\bigvee ((x{\mapsto}- * y{\mapsto}-) \vee z{\mapsto}-)$$



Disjunction of $*$DDs

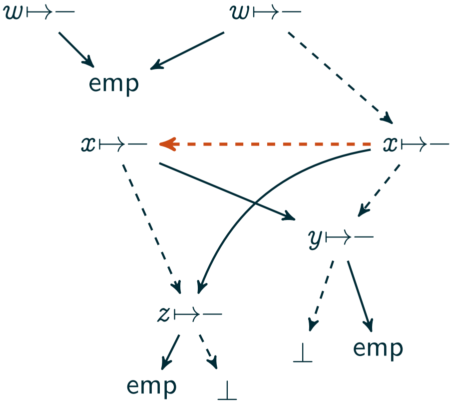
$$\big(w \mapsto - \vee ((x \mapsto - * z \mapsto -) \vee y \mapsto -)\big)$$
$$\bigvee \big((x \mapsto - * y \mapsto -) \vee z \mapsto -\big)$$



$$(a * t \vee e) \bigvee (a' * t' \vee e') \qquad \text{if } a > a'$$
$$= a * t \vee \big(e \bigvee (a' * t' \vee e')\big)$$

Disjunction of $*$DDs

$$(w \mapsto - \vee ((x \mapsto - * z \mapsto -) \vee y \mapsto -))$$
$$\bigvee ((x \mapsto - * y \mapsto -) \vee z \mapsto -)$$

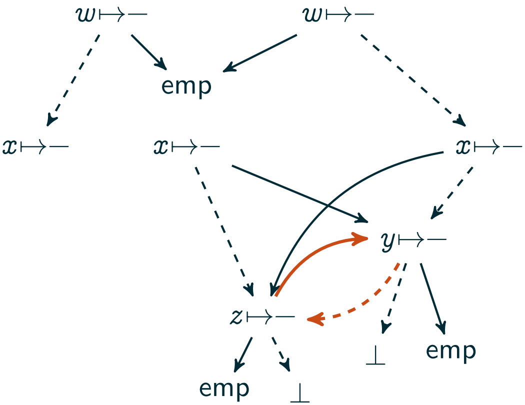


$$(a * t \vee e) \bigvee (a' * t' \vee e') \qquad \text{if } a > a'$$
$$= a * t \vee \left(e \bigvee (a' * t' \vee e')\right)$$

$$(a * t \vee e) \bigvee (a * t' \vee e')$$
$$= a * (t \bigvee t') \vee (e \bigvee e')$$

Disjunction of $*$DDs

$$(w\mapsto - \vee ((x\mapsto - * z\mapsto -) \vee y\mapsto -))$$
$$\bigvee ((x\mapsto - * y\mapsto -) \vee z\mapsto -)$$



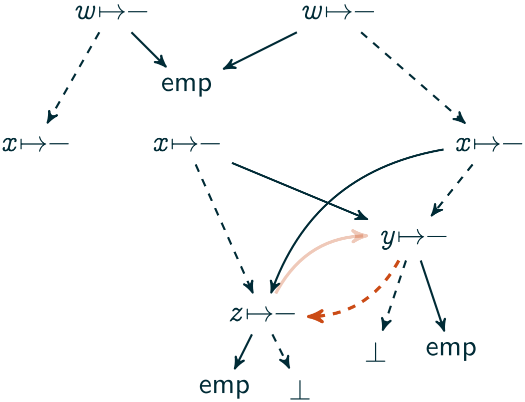
$$(a*t \vee e) \bigvee (a'*t' \vee e') \qquad \text{if } a > a'$$
$$= a*t \vee \big(e \bigvee (a'*t' \vee e')\big)$$

$$(a*t \vee e) \bigvee (a*t' \vee e')$$
$$= a*(t \bigvee t') \vee (e \bigvee e')$$

Disjunction of $*$DDs

$$(w\mapsto - \vee ((x\mapsto - * z\mapsto -) \vee y\mapsto -))$$

$$\bigvee ((x\mapsto - * y\mapsto -) \vee z\mapsto -)$$

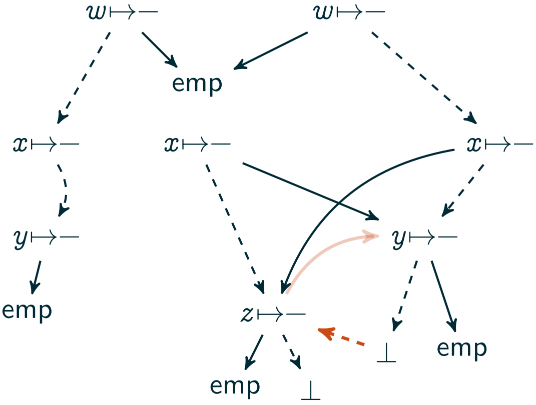


$$(a{*}t \vee e) \bigvee (a'{*}t' \vee e') \qquad \text{if } a > a'$$
$$= a{*}t \vee \big(e \bigvee (a'{*}t' \vee e')\big)$$

$$(a{*}t \vee e) \bigvee (a{*}t' \vee e')$$
$$= a{*}(t \bigvee t') \vee (e \bigvee e')$$

Disjunction of $*$DDs

$$\begin{aligned} & (w{\mapsto}- \vee ((x{\mapsto}- * z{\mapsto}-) \vee y{\mapsto}-)) \\ \bigvee\ & ((x{\mapsto}- * y{\mapsto}-) \vee z{\mapsto}-) \end{aligned}$$



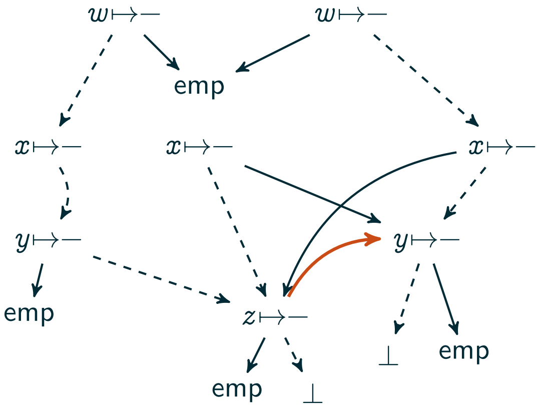
$$(a{*}t \vee e) \bigvee (a'{*}t' \vee e') \qquad \text{if } a > a'$$
$$= a{*}t \vee \left(e \bigvee (a'{*}t' \vee e')\right)$$

$$(a{*}t \vee e) \bigvee (a{*}t' \vee e')$$
$$= a{*}(t \bigvee t') \vee (e \bigvee e')$$

$$\perp \bigvee q \;=\; q$$

Disjunction of $*$DDs

$$
\begin{aligned}
& (w \mapsto - \vee ((x \mapsto - * z \mapsto -) \vee y \mapsto -)) \\
\bigvee\ & ((x \mapsto - * y \mapsto -) \vee z \mapsto -)
\end{aligned}
$$



memoize recursive calls

$$
\begin{aligned}
(a*t \vee e) \bigvee (a'*t' \vee e') & \qquad \text{if } a > a' \\
= a*t \vee \big(e \bigvee (a'*t' \vee e')\big) &
\end{aligned}
$$

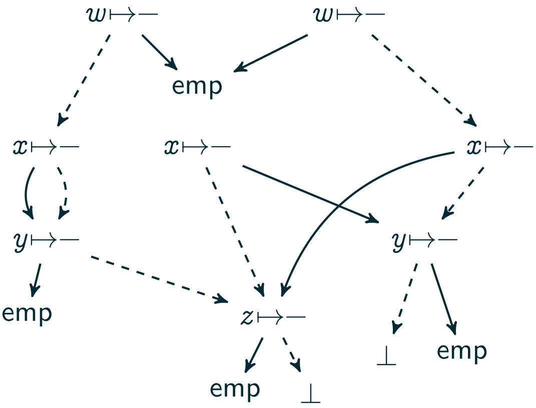
$$
\begin{aligned}
& (a*t \vee e) \bigvee (a*t' \vee e') \\
& \quad = a*(t \bigvee t') \vee (e \bigvee e')
\end{aligned}
$$

$$\bot \bigvee q \ = \ q$$

$$p \bigvee q \ = \ q \bigvee p$$

Disjunction of $*$DDs

$$(w\mapsto - \vee ((x\mapsto - * z\mapsto -) \vee y\mapsto -))$$
$$\bigvee\ ((x\mapsto - * y\mapsto -) \vee z\mapsto -)$$



memoize recursive calls

$$(a*t \vee e) \bigvee (a'*t' \vee e') \qquad \text{if } a > a'$$
$$= a*t \vee \left(e \bigvee (a'*t' \vee e')\right)$$

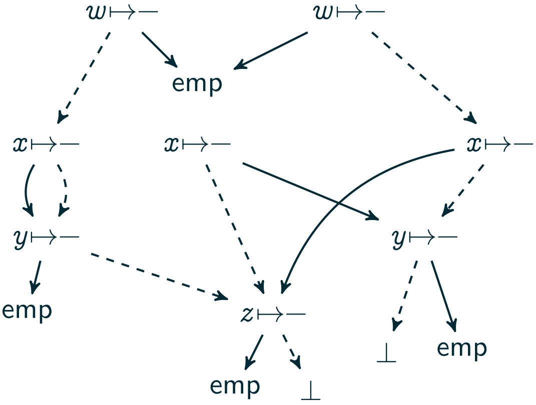
$$(a*t \vee e) \bigvee (a*t' \vee e')$$
$$= a*(t \bigvee t') \vee (e \bigvee e')$$

$$\perp \bigvee q \ = \ q$$

$$p \bigvee q \ = \ q \bigvee p$$

Disjunction of $*$DDs

$$(w{\mapsto}- \vee ((x{\mapsto}- * z{\mapsto}-) \vee y{\mapsto}-))$$
$$\bigvee ((x{\mapsto}- * y{\mapsto}-) \vee z{\mapsto}-)$$



memoize recursive calls

$$(a{*}t \vee e) \bigvee \text{emp}$$
$$= a{*}e \vee (e \bigvee \text{emp})$$

$$(a{*}t \vee e) \bigvee (a'{*}t' \vee e') \qquad \text{if } a > a'$$
$$= a{*}t \vee (e \bigvee (a'{*}t' \vee e'))$$

$$(a{*}t \vee e) \bigvee (a{*}t' \vee e')$$
$$= a{*}(t \bigvee t') \vee (e \bigvee e')$$

$$\perp \bigvee q = q$$

$$p \bigvee q = q \bigvee p$$

$$q \bigvee q = q$$

Separating Conjunction of $*$DDs

$$\mathsf{emp} * q = q$$

$$\bot * q = \bot$$

$$p * q = q * p$$

Separating Conjunction of $*$DDs

$$\mathsf{emp} \ast q = q$$

$$\bot \ast q = \bot$$

$$p \ast q = q \ast p$$

$$\begin{aligned}(a{*}t \vee e) \ast (a'{*}t' \vee e') & \qquad \text{if } a > a' \\ = a{*}\big(t \ast (a'{*}t' \vee e')\big) \vee \big(e \ast (a'{*}t' \vee e')\big) &\end{aligned}$$

Separating Conjunction of $*$DDs

$$\mathsf{emp} \ast q = q$$

$$\bot \ast q = \bot$$

$$p \ast q = q \ast p$$

$$\begin{aligned}&(a{*}t \vee e) \ast (a'{*}t' \vee e') && \text{if } a > a'\\ &= a{*}\big(t \ast (a'{*}t' \vee e')\big) \vee \big(e \ast (a'{*}t' \vee e')\big)\end{aligned}$$

$$\begin{aligned}&(a{*}t \vee e) \ast (a{*}t' \vee e') && \text{if } a \text{ pure}\\ &= a{*}\big((t \ast t') \bigvee (t \ast e') \bigvee (e \ast t')\big) \vee (e \ast e')\end{aligned}$$

$$\begin{aligned}&(a{*}t \vee e) \ast (a{*}t' \vee e') && \text{if } a \text{ spatial}\\ &= a{*}\big((t \ast e') \bigvee (e \ast t')\big) \vee (e \ast e')\end{aligned}$$

Separating Conjunction of $*$DDs

$$\mathsf{emp} \circledast q = q$$

$$\bot \circledast q = \bot$$

$$p \circledast q = q \circledast p$$

$$(a{*}t \vee e) \circledast (a'{*}t' \vee e') \qquad \text{if } a > a'$$
$$= a{*}\big(t \circledast (a'{*}t' \vee e')\big) \vee \big(e \circledast (a'{*}t' \vee e')\big)$$

$$(a{*}t \vee e) \circledast (a{*}t' \vee e') \qquad \text{if } a \text{ pure}$$
$$= a{*}\big((t \circledast t') \bigvee (t \circledast e') \bigvee (e \circledast t')\big) \vee (e \circledast e')$$

$$(a{*}t \vee e) \circledast (a{*}t' \vee e') \qquad \text{if } a \text{ spatial}$$
$$= a{*}\big((t \circledast e') \bigvee (e \circledast t')\big) \vee (e \circledast e')$$

$$(z{=}0 * x{\mapsto}{-}) \circledast (x{\mapsto}{-} \vee y{\mapsto}{-} \vee (z{=}0 * z{\mapsto}{-}))$$
$$= \ z{=}0 * x{\mapsto}{-} \ * \ (y{\mapsto}{-} \vee z{\mapsto}{-})$$

Symbolic Execution

- Small axioms determine execution of instructions on their footprints:

$$\frac{}{\{x \mapsto -\}\ \mathsf{free}(x)\ \{\mathsf{emp}\}}$$

- Apply small axiom to general precondition using Frame:

$$\frac{P \vdash x \mapsto - * Q \qquad \dfrac{\overline{\{x \mapsto -\}\ \mathsf{free}(x)\ \{\mathsf{emp}\}}}{\{x \mapsto - * Q\}\ \mathsf{free}(x)\ \{\mathsf{emp} * Q\}}}{\{P\}\ \mathsf{free}(x)\ \{Q\}}$$

- Need solver for "Frame Inference" problem:

$$P \vdash x \mapsto - * ?Q$$

- *Could* enumerate DNF expansion of P and accumulate a frame for each, *or…*

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \qquad \vee$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on ∗DD structure)

precondition $\vdash$ footprint $\ast$?frame $\vee$?remainder

$$\frac{p_t \vdash a \ast q_t \vee r_t \qquad p_e \vdash a \ast q_e \vee r_e}{p_a{\ast}p_t \vee p_e \vdash a \ast (p_a{\ast}q_t \vee q_e) \vee (p_a{\ast}r_t \vee r_e)}\; p_a > a$$

$$\overline{w{\mapsto}- \ast \varphi_0 \vee (x{\mapsto}- \ast y{\mapsto}- \vee \varphi_0) \vdash z{\mapsto}- \ast \qquad\qquad \vee}$$

where $\varphi_0 = y{\mapsto}- \ast z{\mapsto}-$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a{*}p_t \vee p_e \vdash a * (p_a{*}q_t \vee q_e) \vee (p_a{*}r_t \vee r_e)}\ p_a > a$$

$$\frac{}{\underbrace{y{\mapsto}- * z{\mapsto}-}_{\varphi_0} \vdash z{\mapsto}- * \qquad \vee}$$

$$\frac{}{w{\mapsto}- * \varphi_0 \vee (x{\mapsto}- * y{\mapsto}- \vee \varphi_0) \vdash z{\mapsto}- * \qquad \vee}$$

where $\varphi_0 = y{\mapsto}- * z{\mapsto}-$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\bigvee$?remainder

$$\frac{p_t \vdash a * q_t \bigvee r_t \qquad p_e \vdash a * q_e \bigvee r_e}{p_a{*}p_t \vee p_e \vdash a * (p_a{*}q_t \vee q_e) \bigvee (p_a{*}r_t \vee r_e)}\ p_a > a$$

$$\frac{}{z{\mapsto}- \vdash z{\mapsto}- \ * \qquad \bigvee}$$

$$\frac{}{\underbrace{y{\mapsto}- * z{\mapsto}-}_{\varphi_0} \vdash z{\mapsto}- \ * \qquad \bigvee}$$

$$\frac{}{w{\mapsto}- * \varphi_0 \vee (x{\mapsto}- * y{\mapsto}- \vee \varphi_0) \vdash z{\mapsto}- \ * \qquad \bigvee}$$

where $\varphi_0 = y{\mapsto}- * z{\mapsto}-$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\dfrac{}{a * p_t \vee p_e \vdash a * p_t \vee p_e}$$

$$\dfrac{}{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot}$$

$$\dfrac{}{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * \quad \vee}$$

$$\dfrac{}{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \quad \vee}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} \ast \text{?frame} \vee \text{?remainder}$$

$$\frac{p_t \vdash a \ast q_t \vee r_t \qquad p_e \vdash a \ast q_e \vee r_e}{p_a * p_t \vee p_e \vdash a \ast (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\; p_a > a$$

$$\overline{z \mapsto - \vdash z \mapsto - \ast \mathsf{emp} \vee \bot} \qquad \overline{\bot \vdash z \mapsto - \ast \quad \vee \quad}$$

$$\overline{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - \ast \qquad \vee \qquad}$$

$$\overline{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - \ast \qquad\qquad \vee \qquad}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\dfrac{}{\bot \vdash a * \bot \vee \bot}$$

$$\dfrac{\dfrac{}{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \dfrac{}{\bot \vdash z \mapsto - * \bot \vee \bot}}{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * \quad \vee}$$

$$\dfrac{}{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \quad \vee}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\; p_a > a$$

$$\frac{}{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \frac{}{\bot \vdash z \mapsto - * \bot \vee \bot}$$

$$\frac{}{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * y \mapsto - \vee \bot}$$

$$\frac{}{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \qquad\qquad \vee}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} \ast \,?\text{frame} \bigvee ?\text{remainder}$$

$$\frac{p_t \vdash a \ast q_t \bigvee r_t \qquad p_e \vdash a \ast q_e \bigvee r_e}{p_a{*}p_t \vee p_e \vdash a \ast (p_a{*}q_t \vee q_e) \bigvee (p_a{*}r_t \vee r_e)}\; p_a > a$$

$$\frac{}{z{\mapsto}- \vdash z{\mapsto}- \ast \mathsf{emp} \bigvee \bot} \qquad \frac{}{\bot \vdash z{\mapsto}- \ast \bot \bigvee \bot}$$

$$\frac{}{\underbrace{y{\mapsto}- * z{\mapsto}-}_{\varphi_0} \vdash z{\mapsto}- \ast y{\mapsto}- \bigvee \bot}$$

$$\frac{}{x{\mapsto}- * y{\mapsto}- \vee \varphi_0 \vdash z{\mapsto}- \ast \qquad \bigvee}$$

$$\frac{}{w{\mapsto}- * \varphi_0 \vee (x{\mapsto}- * y{\mapsto}- \vee \varphi_0) \vdash z{\mapsto}- \ast \qquad \bigvee}$$

where $\varphi_0 = y{\mapsto}- * z{\mapsto}-$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\ p_a > a$$

$$\overline{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \overline{\bot \vdash z \mapsto - * \bot \vee \bot}$$

$$\overline{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * y \mapsto - \vee \bot} \qquad \overline{y \mapsto - \vdash z \mapsto - * \quad \vee}$$

$$\overline{x \mapsto - * y \mapsto - \vee \varphi_0 \vdash z \mapsto - * \quad \vee}$$

$$\overline{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \quad \vee}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\ p_a > a$$

$$\overline{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \overline{\bot \vdash z \mapsto - * \bot \vee \bot} \qquad \overline{\mathsf{emp} \vdash z \mapsto - * \quad \vee \quad}$$

$$\overline{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * y \mapsto - \vee \bot} \qquad \overline{y \mapsto - \vdash z \mapsto - * \quad \vee \quad}$$

$$\overline{x \mapsto - * y \mapsto - \vee \varphi_0 \vdash z \mapsto - * \quad \vee \quad}$$

$$\overline{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \quad \vee \quad}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} \mathbin{*} ?\text{frame} \vee ?\text{remainder}$$

$$\overline{\mathsf{emp} \vdash a \mathbin{*} \bot \vee \mathsf{emp}}$$

$$\overline{z \mapsto - \vdash z \mapsto - \mathbin{*} \mathsf{emp} \vee \bot} \qquad \overline{\bot \vdash z \mapsto - \mathbin{*} \bot \vee \bot} \qquad \overline{\mathsf{emp} \vdash z \mapsto - \mathbin{*} \bot \vee \mathsf{emp}}$$

$$\overline{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - \mathbin{*} y \mapsto - \vee \bot} \qquad \overline{y \mapsto - \vdash z \mapsto - \mathbin{*} \quad \vee \quad}$$

$$\overline{x \mapsto - * y \mapsto - \vee \varphi_0 \vdash z \mapsto - \mathbin{*} \quad \vee \quad}$$

$$\overline{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - \mathbin{*} \quad \vee \quad}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\; p_a > a$$

$$\frac{}{z\mapsto - \vdash z\mapsto - * \mathsf{emp} \vee \bot} \qquad \frac{}{\bot \vdash z\mapsto - * \bot \vee \bot} \qquad \frac{}{\mathsf{emp} \vdash z\mapsto - * \bot \vee \mathsf{emp}}$$

$$\frac{}{\underbrace{y\mapsto - * z\mapsto -}_{\varphi_0} \vdash z\mapsto - * y\mapsto - \vee \bot} \qquad \frac{}{y\mapsto - \vdash z\mapsto - * \qquad \vee \qquad}$$

$$\frac{}{x\mapsto - * y\mapsto - \vee \varphi_0 \vdash z\mapsto - * \qquad \vee \qquad}$$

$$\frac{}{w\mapsto - * \varphi_0 \vee (x\mapsto - * y\mapsto - \vee \varphi_0) \vdash z\mapsto - * \qquad \vee \qquad}$$

where $\varphi_0 = y\mapsto - * z\mapsto -$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\; p_a > a$$

$$\overline{z\mapsto - \vdash z\mapsto - * \mathrm{emp} \vee \bot} \qquad \overline{\bot \vdash z\mapsto - * \bot \vee \bot} \qquad \overline{\mathrm{emp} \vdash z\mapsto - * \bot \vee \mathrm{emp}}$$

$$\overline{\underbrace{y\mapsto - * z\mapsto -}_{\varphi_0} \vdash z\mapsto - * y\mapsto - \vee \bot} \qquad \overline{y\mapsto - \vdash z\mapsto - * \bot \vee y\mapsto -}$$

$$\overline{x\mapsto - * y\mapsto - \vee \varphi_0 \vdash z\mapsto - * \qquad \vee}$$

$$\overline{w\mapsto - * \varphi_0 \vee (x\mapsto - * y\mapsto - \vee \varphi_0) \vdash z\mapsto - * \qquad \vee}$$

where $\varphi_0 = y\mapsto - * z\mapsto -$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} * \,?\text{frame} \vee \,?\text{remainder}$$

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\; p_a > a$$

$$\frac{}{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \frac{}{\bot \vdash z \mapsto - * \bot \vee \bot} \qquad \frac{}{\mathsf{emp} \vdash z \mapsto - * \bot \vee \mathsf{emp}}$$

$$\frac{}{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * y \mapsto - \vee \bot} \qquad \frac{}{y \mapsto - \vdash z \mapsto - * \bot \vee y \mapsto -}$$

$$\frac{}{x \mapsto - * y \mapsto - \vee \varphi_0 \vdash z \mapsto - * \qquad \vee}$$

$$\frac{}{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \qquad\qquad \vee}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

precondition $\vdash$ footprint $*$?frame $\vee$?remainder

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a{*}p_t \vee p_e \vdash a * (p_a{*}q_t \vee q_e) \vee (p_a{*}r_t \vee r_e)}\ p_a > a$$

$$\overline{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \overline{\bot \vdash z \mapsto - * \bot \vee \bot} \qquad \overline{\mathsf{emp} \vdash z \mapsto - * \bot \vee \mathsf{emp}}$$

$$\overline{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * y \mapsto - \vee \bot} \qquad \overline{y \mapsto - \vdash z \mapsto - * \bot \vee y \mapsto -}$$

$$\overline{x \mapsto - * y \mapsto - \vee \varphi_0 \vdash z \mapsto - * y \mapsto - \vee x \mapsto - * y \mapsto -}$$

$$\overline{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * \qquad\qquad \vee}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} * ?\text{frame} \vee ?\text{remainder}$$

$$\frac{p_t \vdash a * q_t \vee r_t \qquad p_e \vdash a * q_e \vee r_e}{p_a * p_t \vee p_e \vdash a * (p_a * q_t \vee q_e) \vee (p_a * r_t \vee r_e)}\ p_a > a$$

$$\overline{z \mapsto - \vdash z \mapsto - * \mathsf{emp} \vee \bot} \qquad \overline{\bot \vdash z \mapsto - * \bot \vee \bot} \qquad \overline{\mathsf{emp} \vdash z \mapsto - * \bot \vee \mathsf{emp}}$$

$$\overline{\underbrace{y \mapsto - * z \mapsto -}_{\varphi_0} \vdash z \mapsto - * y \mapsto - \vee \bot} \qquad \overline{y \mapsto - \vdash z \mapsto - * \bot \vee y \mapsto -}$$

$$\overline{x \mapsto - * y \mapsto - \vee \varphi_0 \vdash z \mapsto - * y \mapsto - \vee x \mapsto - * y \mapsto -}$$

$$\overline{w \mapsto - * \varphi_0 \vee (x \mapsto - * y \mapsto - \vee \varphi_0) \vdash z \mapsto - * (w \mapsto - * y \mapsto - \vee y \mapsto -) \vee x \mapsto - * y \mapsto -}$$

where $\varphi_0 = y \mapsto - * z \mapsto -$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} \ast \text{?frame} \bigvee \text{?remainder}$$

$$\frac{}{\bot \vdash a \ast \bot \bigvee \bot} \qquad \frac{}{\mathsf{emp} \vdash a \ast \bot \bigvee \mathsf{emp}}$$

$$\frac{}{a{*}p_t \vee p_e \vdash a \ast p_t \bigvee p_e}$$

$$\frac{p_t \vdash a \ast q_t \bigvee r_t \qquad p_e \vdash a \ast q_e \bigvee r_e}{p_a{*}p_t \vee p_e \vdash a \ast (p_a{*}q_t \vee q_e) \bigvee (p_a{*}r_t \vee r_e)}\ p_a > a$$

$$\frac{}{p_a{*}p_t \vee p_e \vdash a \ast \bot \bigvee (p_a{*}p_t \vee p_e)}\ p_a < a$$

Frame Inference (directly on $*$DD structure)

$$\text{precondition} \vdash \text{footprint} \ast \text{?frame} \bigvee \text{?remainder}$$

$$\frac{}{\bot \vdash a \ast \bot \bigvee \bot} \qquad \frac{}{\mathsf{emp} \vdash a \ast \bot \bigvee \mathsf{emp}}$$

$$\frac{}{a{*}p_t \lor p_e \vdash a \ast p_t \bigvee p_e}$$

$$\frac{p_t \vdash a \ast q_t \bigvee r_t \qquad p_e \vdash a \ast q_e \bigvee r_e}{p_a{*}p_t \lor p_e \vdash a \ast (p_a{*}q_t \lor q_e) \bigvee (p_a{*}r_t \lor r_e)}\ p_a > a$$

$$\frac{}{p_a{*}p_t \lor p_e \vdash a \ast \bot \bigvee (p_a{*}p_t \lor p_e)}\ p_a < a$$

Generalizing to footprints that are starjunctions of atoms is easy
Generalizing to arbitrary footprints *could* be done by DNF expanding the footprint, *or…*

Frame Inference (directly on $*$DD structure)

$$\frac{}{p \vdash \bot \circledast \bot \bigvee p} \qquad \frac{}{p \vdash \mathsf{emp} \circledast p \bigvee \bot} \qquad \frac{}{p \vdash p \circledast \mathsf{emp} \bigvee \bot}$$

$$\frac{}{\bot \vdash s \circledast \bot \bigvee \bot} \qquad \frac{}{\mathsf{emp} \vdash (a{*}t \vee e) \circledast \bot \bigvee \mathsf{emp}}$$

$$\frac{p_t \vdash s_t \circledast q_1 \bigvee r_1 \qquad p_e \vdash a{*}s_t \circledast q_2 \bigvee r_2 \qquad a{*}r_1 \vee r_2 \vdash s_e \circledast q_3 \bigvee r_3}{a{*}p_t \vee p_e \vdash (a{*}s_t \vee s_e) \circledast (q_1 \vee q_2 \vee q_3) \bigvee r_3}$$

$$\frac{p_t \vdash s_a{*}s_t \circledast q_1 \bigvee r_1 \qquad p_e \vdash s_a{*}s_t \circledast q_2 \bigvee r_2 \qquad p_a{*}r_1 \vee r_2 \vdash s_e \circledast q_3 \bigvee r_3}{p_a{*}p_t \vee p_e \vdash (s_a{*}s_t \vee s_e) \circledast (p_a{*}q_1 \vee q_2 \vee q_3) \bigvee r_3}\ p_a > s_a$$

$$\frac{p_a{*}p_t \vee p_e \vdash s_e \circledast q \bigvee r}{p_a{*}p_t \vee p_e \vdash (s_a{*}s_t \vee s_e) \circledast q \bigvee r}\ p_a < s_a$$

Nondeterminism

Results not uniquely determined:

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \vdash (x \mapsto - \vee y \mapsto -) \ast (y \mapsto - \vee \mathsf{emp}) \bigvee \bot$$

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \vdash (x \mapsto - \vee y \mapsto -) \ast (x \mapsto - \vee \mathsf{emp}) \bigvee \bot$$

Nondeterminism, Incompleteness

Results not uniquely determined:

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \vdash (x \mapsto - \vee y \mapsto -) \circledast (y \mapsto - \vee \mathsf{emp}) \bigvee \bot$$

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \vdash (x \mapsto - \vee y \mapsto -) \circledast (x \mapsto - \vee \mathsf{emp}) \bigvee \bot$$

Analogue of Euclid's Division Lemma fails:

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \not\vdash (x \mapsto - \vee y \mapsto -) \circledast (y \mapsto - \vee \mathsf{emp}) \bigvee \bot$$

$$\overset{\text{dividend}}{\cancel{\text{precondition}}} \neq \overset{\text{divisor}}{\cancel{\text{footprint}}} \circledast \overset{\text{quotient}}{\cancel{\text{frame}}} \bigvee \text{remainder}$$

Nondeterminism, Incompleteness and Junk

Results not uniquely determined:

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \vdash (x \mapsto - \vee y \mapsto -) \mathbin{\ast} (y \mapsto - \vee \mathsf{emp}) \bigvee \perp$$

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \vdash (x \mapsto - \vee y \mapsto -) \mathbin{\ast} (x \mapsto - \vee \mathsf{emp}) \bigvee \perp$$

Analogue of Euclid's Division Lemma fails:

$$x \mapsto - * (y \mapsto - \vee \mathsf{emp}) \nvdash (x \mapsto - \vee y \mapsto -) \mathbin{\ast} (y \mapsto - \vee \mathsf{emp}) \bigvee \perp$$

$$\underset{\cancel{\text{precondition}}}{\text{dividend}} \neq \underset{\cancel{\text{footprint}}}{\text{divisor}} \mathbin{\ast} \underset{\cancel{\text{frame}}}{\text{quotient}} \bigvee \text{remainder}$$

Excess expressiveness:

$x \mapsto - \vee y \mapsto -$ not minimal safe pre of *any* local action

Unknown how to syntactically characterize "good" footprints

Unknown if incomplete when restricted to "good" footprints

Conclusion

- $*\vee$ Separation Logic formulas can be represented compactly using a form of ZDDs
  - Perhaps other connectives could be handled like atoms
- Shared subformulas arise when configs of heap parts independent of each other
  - Similar to when particular Cartesian abstractions would be precise
- Sharing yields
  - Reused subcomputations of formula manipulation operations
  - Proof DAGs rather than proof trees for theorem proving algorithms
- Frame inference
  - Starjunctive footprints: "done"
  - Disjunctive footprints: some questions remain open
- Future
  - Good combination with pure first-order reasoning is in progress
  - Use remainders for incorrectness reasoning?