# A NEW DECISION PROCEDURE FOR FINITE SETS AND CARDINALITY IN SMT

K. Bansal* and C. Barrett* and A. Reynolds+ and C. Tinelli+

June 30, 2016

*New York University +The University of Iowa

# THIS WORK

New tableaux-style calculus for many-sorted quantifier-free theory of finite sets with cardinality constraints

# THIS WORK

New tableaux-style calculus for many-sorted quantifier-free

theory of finite sets with cardinality constraints

**Motivation:** formalizes modular, incremental *T*-solver that can be integrated into SMT solvers

# THIS WORK

New tableaux-style calculus for many-sorted quantifier-free

theory of finite sets with cardinality constraints

**Motivation:** formalizes modular, incremental *T*-solver that can be integrated into SMT solvers

**Target use:** static analysis tools (Leon, LiquidHaskell, ...)

# THIS WORK

New tableaux-style calculus for many-sorted quantifier-free

theory of finite sets with cardinality constraints

**Motivation:** formalizes modular, incremental *T*-solver that can be integrated into SMT solvers

**Target use:** static analysis tools (Leon, LiquidHaskell, ...)

**Current restriction:** Element sort must be infinite

# THIS WORK

New tableaux-style calculus for many-sorted quantifier-free

theory of finite sets with cardinality constraints

**Motivation:** formalizes modular, incremental *T*-solver that can be integrated into SMT solvers

**Target use:** static analysis tools (Leon, LiquidHaskell, ...)

**Current restriction:** Element sort must be infinite

**Implementation:** initial version, fully integrated in CVC4

# CLOSELY RELATED WORK

(Cantone and Zarba, FTP 1998)

Finite sets with $\{\_\}$, $\cup$, $\cap$, $\setminus$, $\in$, $\subseteq$. Tableaux-based procedure.

(Zarba, FroCoS 2002)

As above plus $|\_|$ and LIA constraints. Theoretical results. Highly inefficient in practice.

(Suter et al., VMCAI 2011)

Boolean Algebras and Presburger Arithmetic, no $\{\_\}$ and $\in$. Based on Venn-region computation. Relatively inefficient in practice.

# OUR CONTRIBUTION

- A more efficient, decision procedure for sets of literals
- incremental and modular
- Capitalizes on separate solvers for CC and for LIA
- Reasons modulo equality (over elements and over sets)
- Tries to minimize number of Venn regions that need to be considered
- Introduces Venn regions lazily

# CALCULUS: MAIN IDEA

Try to build a model for input constraint set

# CALCULUS: MAIN IDEA

Try to build a model for input constraint set

1. Build (partial) candidate model while ignoring cardinality constraints
   - For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
   - Work modulo equality
   - Propagate equalities

# CALCULUS: MAIN IDEA

Try to build a model for input constraint set

1. Build (partial) candidate model while ignoring cardinality constraints
   - For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
   - Work modulo equality
   - Propagate equalities

2. Adjust candidate model to accommodate cardinality constraints
   - Decompose each set into a partition of non-empty regions
   - Propagate cardinality constraints over these decompositions

# THEORY SIGNATURE

$\{\_\} : \text{Elem} \to \text{Set}$  $\sqcup, \sqcap, \setminus : \text{Set} \times \text{Set} \to \text{Set}$  $\emptyset : \text{Set}$

$\sqsubseteq : \text{Set} \times \text{Set}$  $\sqsubset\!\!\!- : \text{Elem} \times \text{Set}$

$|\_| : \text{Set} \to \text{Card}$  $n : \text{Card}$ for all $n \in \mathbb{N}$

$\texttt{-} : \text{Card} \to \text{Card}$  $\texttt{+} : \text{Card} \times \text{Card} \to \text{Card}$

$\texttt{<} : \text{Card} \times \text{Card}$  $\texttt{>=} : \text{Card} \times \text{Card}$

$\approx : \alpha \times \alpha$ for $\alpha \in \{\text{Set}, \text{Elem}, \text{Card}\}$

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \mathrel{\underline{\in}} C$
4. $x \mathrel{\underline{\in}} E \sqcup F$
5. $x \not\mathrel{\underline{\in}} D$
6. $y \not\mathrel{\underline{\in}} C \sqcap D$
7. $y \mathrel{\underline{\in}} A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| | | $A$ |
| | | $B$ |
| | | $C$ |
| | | $D$, $E$ |
| | | $F$ |
| | | $A \sqcup B$, $C \sqcap D$ |
| | | $E \sqcup F$ |
| | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$ ➡
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| | | $A$ |
| | | $B$ |
| ✓ | | $C$ |
| | | $D$, $E$ |
| | | $F$ |
| | | $A \sqcup B$, $C \sqcap D$ |
| | | $E \sqcup F$ |
| | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$

➡ 4. $x \sqsubseteq E \sqcup F$

5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| | | $A$ |
| | | $B$ |
| ✓ | | $C$ |
| | | $D$, $E$ |
| | | $F$ |
| | | $A \sqcup B$, $C \sqcap D$ |
| ✓ | | $E \sqcup F$ |
| | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$

➡ 5. $x \not\sqsubseteq D$

6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| | | $A$ |
| | | $B$ |
| ✓ | | $C$ |
| ✗ | | $D$, $E$ |
| | | $F$ |
| | | $A \sqcup B$, $C \sqcap D$ |
| ✓ | | $E \sqcup F$ |
| | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| | $x$ | $y$ | |
|---|---|---|---|
| | | | $A$ |
| | | | $B$ |
| | ✓ | | $C$ |
| ➡ | ✗ | | $D$, $E$ |
| | ✓ | | $F$ |
| | | | $A \sqcup B$, $C \sqcap D$ |
| ➡ | ✓ | | $E \sqcup F$ |
| | | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term *e* and *relevant* set term *s*, determine if *e* is in *t* or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| | | $A$ |
| | | $B$ |
| ✓ | | $C$ |
| ➡ ✗ | | $D$, $E$ |
| ✓ | | $F$ |
| ✗ | | $A \sqcup B$, $C \sqcap D$ |
| ✓ | | $E \sqcup F$ |
| | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term *e* and *relevant* set term *s*, determine if *e* is in *t* or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| | $x$ | $y$ | |
|---|---|---|---|
| | ✗ | | $A$ |
| | ✗ | | $B$ |
| | ✓ | | $C$ |
| | ✗ | | $D$, $E$ |
| | ✓ | | $F$ |
| ➡ | ✗ | | $A \sqcup B$, $C \sqcap D$ |
| | ✓ | | $E \sqcup F$ |
| | | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x ⋿ C$
4. $x ⋿ E \sqcup F$
5. $x \not⋿ D$
6. $y \not⋿ C \sqcap D$
7. $y ⋿ A \sqcup D$

| | $x$ | $y$ | |
|---|---|---|---|
| ➡ | ✗ | | $A$ |
| | ✗ | | $B$ |
| | ✓ | | $C$ |
| ➡ | ✗ | | $D$, $E$ |
| | ✓ | | $F$ |
| | ✗ | | $A \sqcup B$, $C \sqcap D$ |
| | ✓ | | $E \sqcup F$ |
| | ✗ | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x ⋿ C$
4. $x ⋿ E \sqcup F$
5. $x \not⋿ D$
6. ➡ $y \not⋿ C \sqcap D$
7. $y ⋿ A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| ✗ | | $A$ |
| ✗ | | $B$ |
| ✓ | | $C$ |
| ✗ | | $D, E$ |
| ✓ | | $F$ |
| ✗ | ✗ | $A \sqcup B, C \sqcap D$ |
| ✓ | | $E \sqcup F$ |
| ✗ | | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$

➡ 7. $y \sqsubseteq A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| ✗ | | $A$ |
| ✗ | | $B$ |
| ✓ | | $C$ |
| ✗ | | $D$, $E$ |
| ✓ | | $F$ |
| ✗ | ✗ | $A \sqcup B$, $C \sqcap D$ |
| ✓ | | $E \sqcup F$ |
| ✗ | ✓ | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| | $x$ | $y$ | |
|---|---|---|---|
| | ✗ | ✗ | $A$ |
| | ✗ | ✗ | $B$ |
| | ✓ | | $C$ |
| | ✗ | | $D$, $E$ |
| | ✓ | | $F$ |
| ➡ | ✗ | ✗ | $A \sqcup B$, $C \sqcap D$ |
| | ✓ | | $E \sqcup F$ |
| | ✗ | ✓ | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| | $x$ | $y$ | |
|---|---|---|---|
| ➡ | ✗ | ✗ | $A$ |
| | ✗ | ✗ | $B$ |
| | ✓ | | $C$ |
| | ✗ | ✓ | $D, E$ |
| | ✓ | | $F$ |
| | ✗ | ✗ | $A \sqcup B, C \sqcap D$ |
| | ✓ | | $E \sqcup F$ |
| ➡ | ✗ | ✓ | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x ⋿ C$
4. $x ⋿ E \sqcup F$
5. $x \not⋿ D$
6. $y \not⋿ C \sqcap D$
7. $y ⋿ A \sqcup D$

|  | $x$ | $y$ |  |
|---|---|---|---|
|  | ✗ | ✗ | $A$ |
|  | ✗ | ✗ | $B$ |
|  | ✓ |  | $C$ |
| ➡ | ✗ | ✓ | $D$, $E$ |
|  | ✓ |  | $F$ |
|  | ✗ | ✗ | $A \sqcup B$, $C \sqcap D$ |
|  | ✓ | ✓ | $E \sqcup F$ |
|  | ✗ | ✓ | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x \sqsubseteq C$
4. $x \sqsubseteq E \sqcup F$
5. $x \not\sqsubseteq D$
6. $y \not\sqsubseteq C \sqcap D$
7. $y \sqsubseteq A \sqcup D$

| | $x$ | $y$ | |
|---|---|---|---|
| | ✗ | ✗ | $A$ |
| | ✗ | ✗ | $B$ |
| | ✓ | ✗ | $C$ |
| ➡ | ✗ | ✓ | $D$, $E$ |
| | ✓ | | $F$ |
| ➡ | ✗ | ✗ | $A \sqcup B$, $C \sqcap D$ |
| | ✓ | ✓ | $E \sqcup F$ |
| | ✗ | ✓ | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 1

1. $A \sqcup B \approx C \sqcap D$
2. $D \approx E$
3. $x ⋿ C$
4. $x ⋿ E \sqcup F$
5. $x \not⋿ D$
6. $y \not⋿ C \sqcap D$
7. $y ⋿ A \sqcup D$

| $x$ | $y$ | |
|---|---|---|
| ✗ | ✗ | $A$ |
| ✗ | ✗ | $B$ |
| ✓ | ✗ | $C$ |
| ✗ | ✓ | $D$, $E$ |
| ✓ | | $F$ |
| ✗ | ✗ | $A \sqcup B$, $C \sqcap D$ |
| ✓ | ✓ | $E \sqcup F$ |
| ✗ | ✓ | $A \sqcup D$ |

# PROCESSING SET CONSTRAINTS

- For each element term *e* and *relevant* set term *s*, determine if *e* is in *t* or not
- Work modulo equality

## Example 2

1. $x \not⋿ A \sqcup B$
2. $x ⋿ A \sqcap C$

| $x$ | |
|---|---|
| | $A$ |
| | $B$ |
| | $C$ |
| ✗ | $A \sqcup B$ |
| ✓ | $A \sqcap C$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 2

1. $x \not\sqsubseteq A \sqcup B$
2. $x \sqsubseteq A \sqcap C$

| | $x$ | |
|---|---|---|
| | ✗ | $A$ |
| | ✗ | $B$ |
| | | $C$ |
| ➡ | ✗ | $A \sqcup B$ |
| | ✓ | $A \sqcap C$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 2

1. $x \not\mathrel{⋿} A \sqcup B$
2. $x \mathrel{⋿} A \sqcap C$

| | $x$ | |
|---|---|---|
| | ✗ ✓ | $A$ |
| | ✗ | $B$ |
| | ✓ | $C$ |
| | ✗ | $A \sqcup B$ |
| ➡ | ✓ | $A \sqcap C$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 2

1. $x \not\sqsubseteq A \sqcup B$
2. $x \sqsubseteq A \sqcap C$

| $x$ | |
|---|---|
| ✗ ✓ | $A$ |
| ✗ | $B$ |
| ✓ | $C$ |
| ✗ | $A \sqcup B$ |
| ✓ | $A \sqcap C$ |

Contradiction!

## PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

### Example 3

$$\begin{array}{c} \dots \\ x \approx y \\ \dots \end{array}$$

| $x$ | $y$ | |
|---|---|---|
| | ✓ | $A$ |
| ✗ | | $B$ |
| ✓ | | $C$ |
| | ✗ | $D$ |
| $\dots$ | $\dots$ | $\dots$ |

# PROCESSING SET CONSTRAINTS

- For each element term $e$ and *relevant* set term $s$, determine if $e$ is in $t$ or not
- Work modulo equality

## Example 3

$\dots$

➡ $x \approx y$

$\dots$

| $x, y$ | |
|---|---|
| ✓ | $A$ |
| ✗ | $B$ |
| ✓ | $C$ |
| ✗ | $D$ |
| $\dots$ | $\dots$ |

# PROCESSING SET CONSTRAINTS

- Propagate equalities

## Example 4

$$\begin{gathered}\dots\\ A \approx \{y\}\\ A \approx B\\ x \sqsubseteq A\\ x \sqsubseteq A \sqcup C\\ y \sqsubseteq B \sqcup C\\ \dots\end{gathered}$$

| $x$ | $y$ | |
|---|---|---|
| ✓ | ✓ | $A$, $B$, $\{y\}$ |
| $\dots$ | $\dots$ | $A \sqcup C$ |
| $\dots$ | $\dots$ | $B \sqcup C$ |
| $\dots$ | $\dots$ | $\dots$ |

# PROCESSING SET CONSTRAINTS

- Propagate equalities

## Example 4

$\dots$

$A \approx \{y\}$

$A \approx B$

➡ $x \sqsubseteq A$

$x \sqsubseteq A \sqcup C$

$y \sqsubseteq B \sqcup C$

$\dots$

| $x, y$ | |
|---|---|
| ✓ | $A, B, \{y\}$ |
| $\dots$ | $A \sqcup C$ |
| $\dots$ | $B \sqcup C$ |
| $\dots$ | $\dots$ |

# PROCESSING SET CONSTRAINTS

- Propagate equalities

## Example 4

$\dots$

$A \approx \{y\}$

➡ $A \approx B$

$x \sqsubseteq A$

$x \sqsubseteq A \sqcup C$

$y \sqsubseteq B \sqcup C$

$\dots$

| $x, y$ | |
|---|---|
| ✓ | $A, B, \{y\}$ |
| $\dots$ | $A \sqcup C, B \sqcup C$ |
| $\dots$ | $\dots$ |

# PROCESSING CARDINALITY CONSTRAINTS

## Simplifying requirements:

- Only variables for elements
- No applications of $\sqsubseteq$
- All constraints in *flat form* ( $x \sqsubset\!\!\!- A \text{ op } B,\ A \text{ op } B \approx C \text{ op } D$ )
- Each set variable occurs at most once in non-variable terms

# PROCESSING CARDINALITY CONSTRAINTS

Simplifying requirements:

- Only variables for elements
- No applications of $\sqsubseteq$
- All constraints in *flat form* ( $x \sqsubset A$ op $B$, $A$ op $B \approx C$ op $D$ )
- Each set variable occurs at most once in non-variable terms

No loss of generality

# AUXILIARY DATA STRUCTURE

*Cardinality graph* $G = (N, E)$

$N$, selected terms in or constructed from input problem

$E$, s.t. the leaves of each subtree form a partition of its root

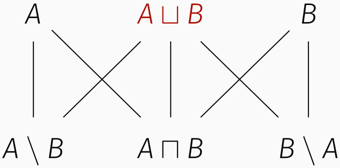
# AUXILIARY DATA STRUCTURE

*Cardinality graph* $G = (N, E)$

$N$, selected terms in or constructed from input problem

$E$, s.t. the leaves of each subtree form a partition of its root

**Example**



**Note:** $|A \sqcup B| = |A \setminus B| + |A \sqcap B| + |B \setminus A| \quad |A| = |A \setminus B| + |A \sqcap B|$

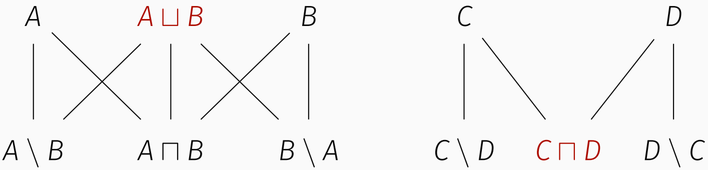
# AUXILIARY DATA STRUCTURE

*Cardinality graph* $G = (N, E)$

$N$, selected terms in or constructed from input problem

$E$, s.t. the leaves of each subtree form a partition of its root

**Example**



**Note:** $|A \sqcup B| = |A \setminus B| + |A \sqcap B| + |B \setminus A| \quad |A| = |A \setminus B| + |A \sqcap B|$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D$

$y \not\sqsubseteq A \sqcup B$

$x \sqsubseteq E \sqcup F$

$x \sqsubseteq C$

$y \sqsubseteq D$

$A \sqcup B \approx C \sqcap D$

$D \approx E$

$|A \sqcup B| \geq 4$

$|C| + |D| \leq 10$

$|E \sqcup F| \geq 100$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D$

$y \not\sqsubseteq A \sqcup B$

$x \sqsubseteq E \sqcup F$

$x \sqsubseteq C$

$y \sqsubseteq D$

$A \sqcup B \approx C \sqcap D$

$D \approx E$

$|A \sqcup B| \geq 4$

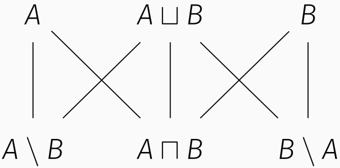
$|C| + |D| \leq 10$

$|E \sqcup F| \geq 100$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ \ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 10,\ |E \sqcup F| \geq 100$



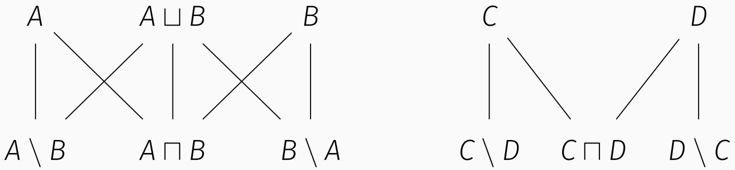
$A$ $A \sqcup B$ $B$

$A \setminus B$ $A \sqcap B$ $B \setminus A$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 10,\ |E \sqcup F| \geq 100$



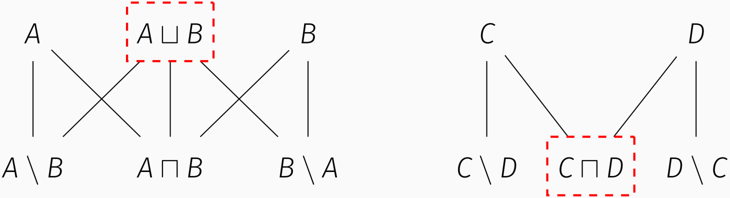
$A$ $A \sqcup B$ $B$ $C$ $D$

$A \setminus B$ $A \sqcap B$ $B \setminus A$ $C \setminus D$ $C \sqcap D$ $D \setminus C$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 10,\ |E \sqcup F| \geq 100$



$A$ $\boxed{A \sqcup B}$ $B$ $C$ $D$

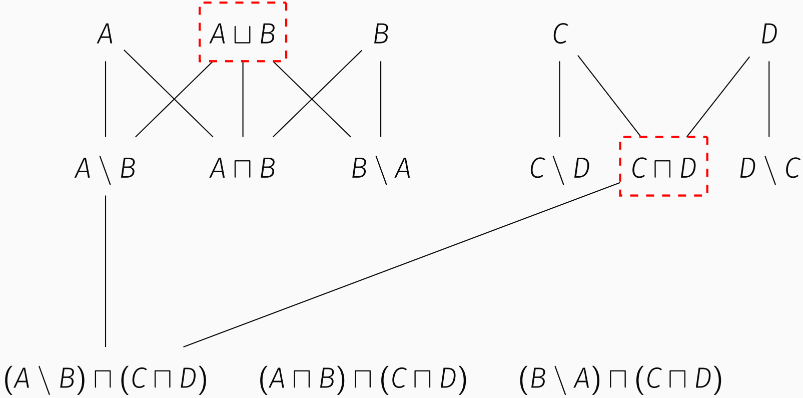
$A \setminus B$ $A \sqcap B$ $B \setminus A$ $C \setminus D$ $\boxed{C \sqcap D}$ $D \setminus C$

$(A \setminus B) \sqcap (C \sqcap D)$ $(A \sqcap B) \sqcap (C \sqcap D)$ $(B \setminus A) \sqcap (C \sqcap D)$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

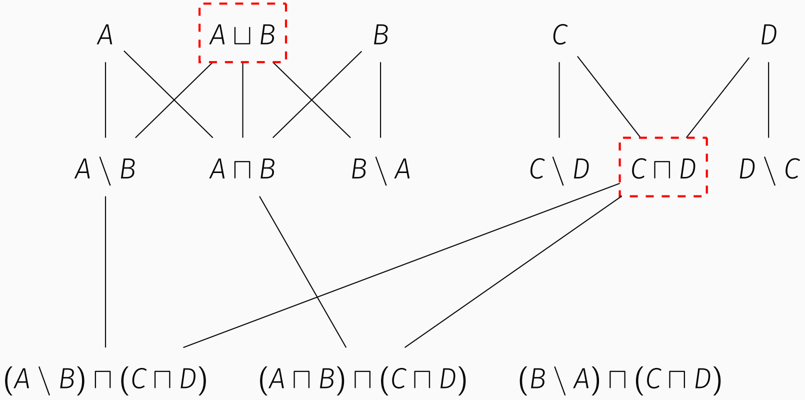
$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 10,\ |E \sqcup F| \geq 100$


$A$
$A \sqcup B$
$B$
$C$
$D$
$A \setminus B$
$A \sqcap B$
$B \setminus A$
$C \setminus D$
$C \sqcap D$
$D \setminus C$
$(A \setminus B) \sqcap (C \sqcap D)$
$(A \sqcap B) \sqcap (C \sqcap D)$
$(B \setminus A) \sqcap (C \sqcap D)$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 10,\ |E \sqcup F| \geq 100$$



$A$ $\boxed{A \sqcup B}$ $B$ $C$ $D$

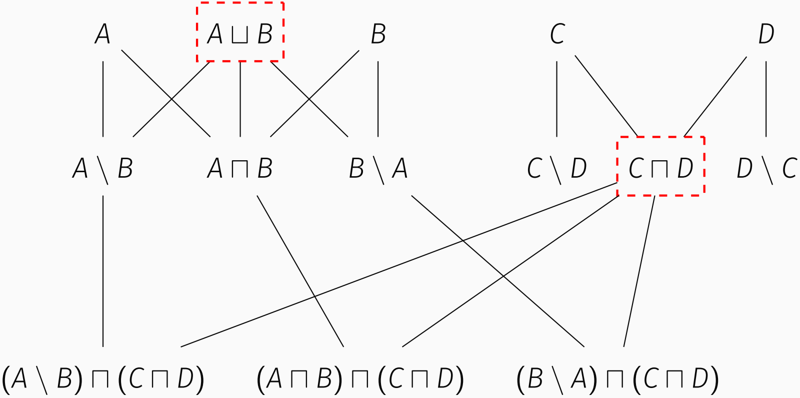
$A \setminus B$ $A \sqcap B$ $B \setminus A$ $C \setminus D$ $\boxed{C \sqcap D}$ $D \setminus C$

$(A \setminus B) \sqcap (C \sqcap D)$ $(A \sqcap B) \sqcap (C \sqcap D)$ $(B \setminus A) \sqcap (C \sqcap D)$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 10,\ |E \sqcup F| \geq 100$



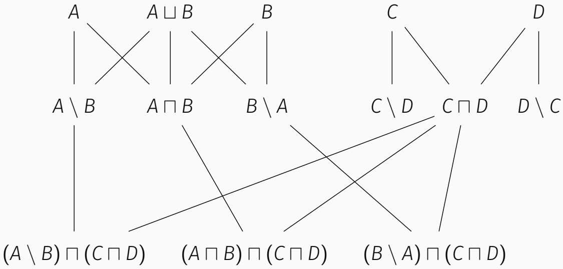
$A$ $A \sqcup B$ $B$ $C$ $D$

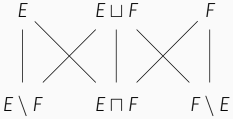
$A \setminus B$ $A \sqcap B$ $B \setminus A$ $C \setminus D$ $C \sqcap D$ $D \setminus C$

$(A \setminus B) \sqcap (C \sqcap D)$ $(A \sqcap B) \sqcap (C \sqcap D)$ $(B \setminus A) \sqcap (C \sqcap D)$

$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

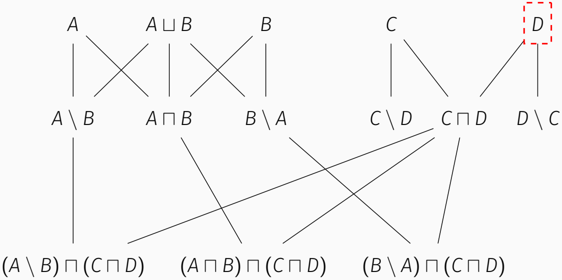
$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$


$A$
$A \sqcup B$
$B$
$C$
$D$
$A \setminus B$
$A \sqcap B$
$B \setminus A$
$C \setminus D$
$C \sqcap D$
$D \setminus C$
$(A \setminus B) \sqcap (C \sqcap D)$
$(A \sqcap B) \sqcap (C \sqcap D)$
$(B \setminus A) \sqcap (C \sqcap D)$

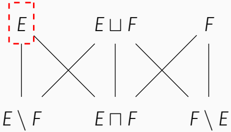


$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ \ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$

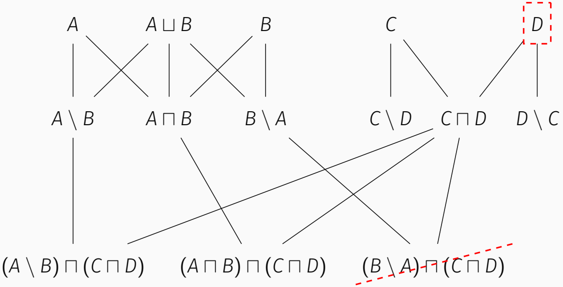


$A$
$A \sqcup B$
$B$
$C$
$D$
$A \setminus B$
$A \sqcap B$
$B \setminus A$
$C \setminus D$
$C \sqcap D$
$D \setminus C$
$(A \setminus B) \sqcap (C \sqcap D)$
$(A \sqcap B) \sqcap (C \sqcap D)$
$(B \setminus A) \sqcap (C \sqcap D)$



$x \not\sqsubseteq D$, $y \not\sqsubseteq A \sqcup B$ $x \sqsubseteq E \sqcup F$, $x \sqsubseteq C$, $y \sqsubseteq D$

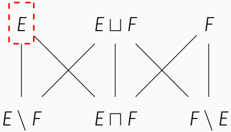
$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$



$A$ $A \sqcup B$ $B$ $C$ $\boxed{D}$

$A \setminus B$ $A \sqcap B$ $B \setminus A$ $C \setminus D$ $C \sqcap D$ $D \setminus C$

$(A \setminus B) \sqcap (C \sqcap D)$ $(A \sqcap B) \sqcap (C \sqcap D)$ $\cancel{(B \setminus A) \sqcap (C \sqcap D)}$

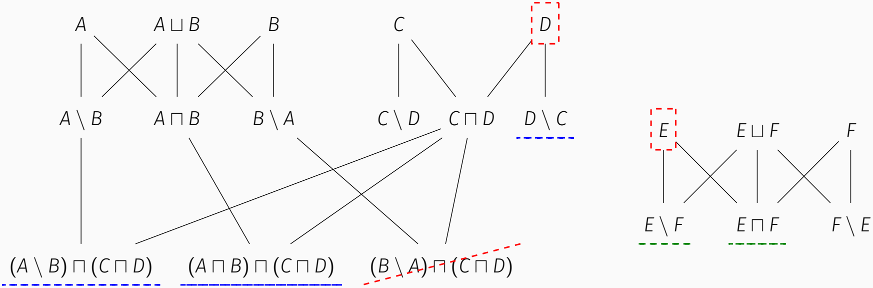


$\boxed{E}$ $E \sqcup F$ $F$

$E \setminus F$ $E \sqcap F$ $F \setminus E$

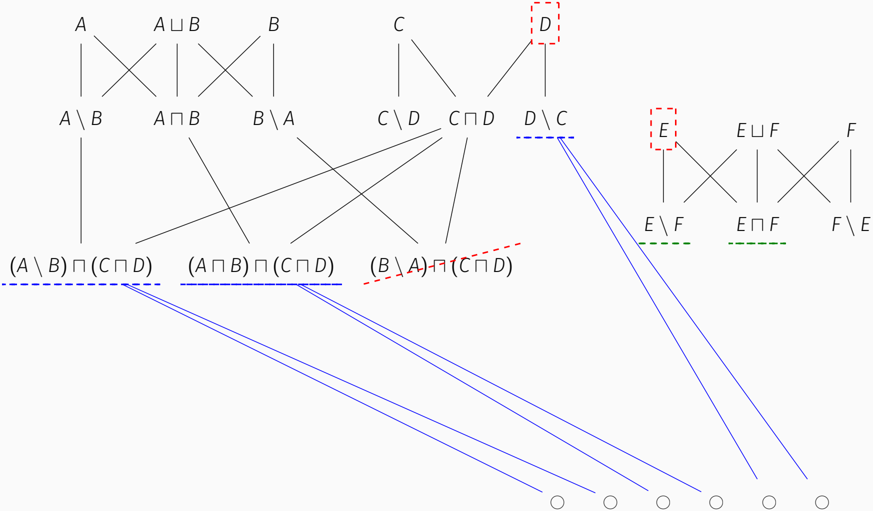
$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$



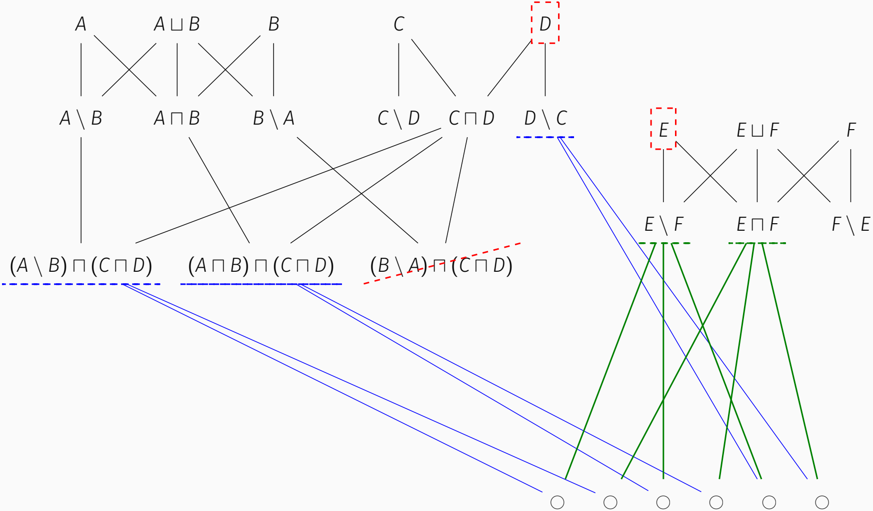
$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$



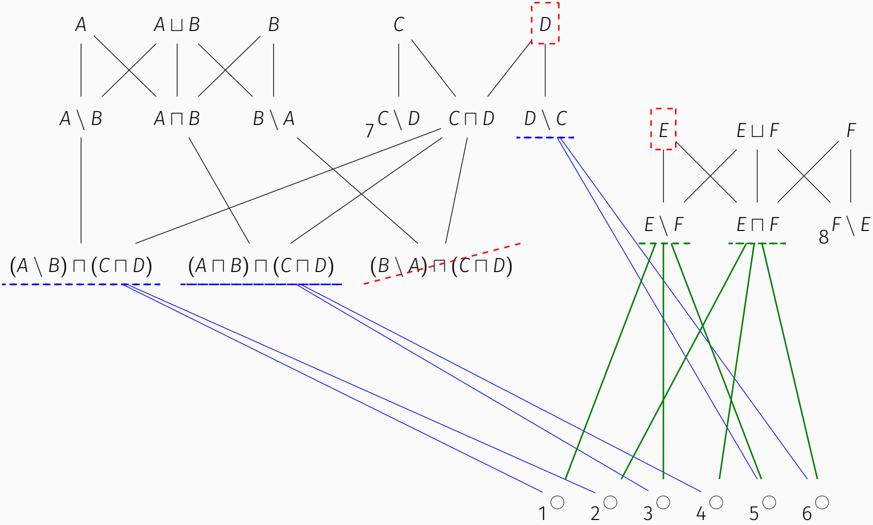
$x \not\sqsubseteq D,\ y \not\sqsubseteq A \sqcup B\ x \sqsubseteq E \sqcup F,\ x \sqsubseteq C,\ y \sqsubseteq D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$



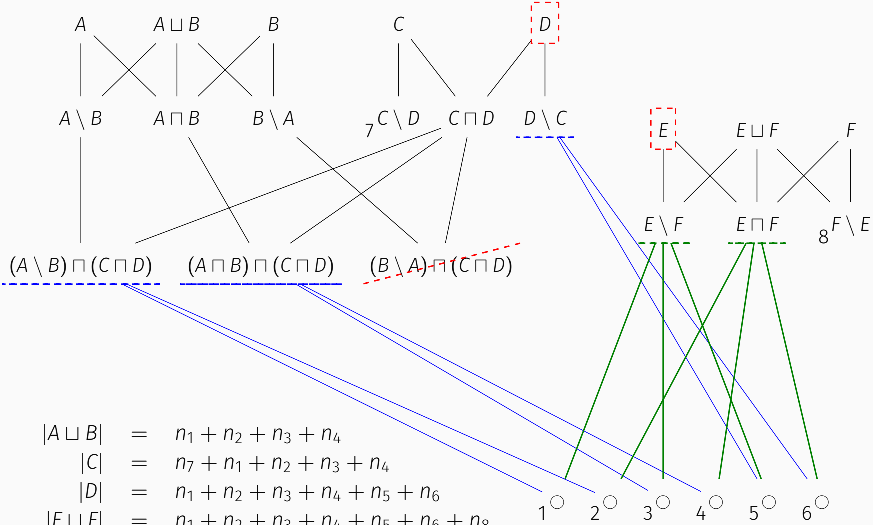
$x \not\sqsubseteq D$, $y \not\sqsubseteq A \sqcup B$ $x \sqsubseteq E \sqcup F$, $x \sqsubseteq C$, $y \sqsubseteq D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$



$x \not⋿ D,\ y \not⋿ A \sqcup B\ x ⋿ E \sqcup F,\ x ⋿ C,\ y ⋿ D$

$$A \sqcup B \approx C \sqcap D,\ D \approx E,\ |A \sqcup B| \geq 4,\ |C| + |D| \leq 9,\ |E \sqcup F| \geq 100$$



$$
\begin{aligned}
|A \sqcup B| &= n_1 + n_2 + n_3 + n_4 \\
|C| &= n_7 + n_1 + n_2 + n_3 + n_4 \\
|D| &= n_1 + n_2 + n_3 + n_4 + n_5 + n_6 \\
|E \sqcup F| &= n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_8
\end{aligned}
$$

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

Reasoning about cardinality is reduced to solving:

$$\begin{cases} n_1 + n_2 + n_3 + n_4 \geq 4 \\ n_7 + n_1 + n_2 + n_3 + n_4 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 \leq 10 \\ n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_8 \geq 100 \\ n_i \geq 0 \quad \text{for} \;\; i \in \{1, \ldots 8\} \end{cases}$$

(which is satisfiable)

# PROCESSING CARDINALITY CONSTRAINTS: EXAMPLE

Reasoning about cardinality is reduced to solving:

$$\begin{cases} n_1 + n_2 + n_3 + n_4 \geq 4 \\ n_7 + n_1 + n_2 + n_3 + n_4 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 \leq 10 \\ n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_8 \geq 100 \\ n_i \geq 0 \quad \text{for } \; i \in \{1, \ldots 8\} \end{cases}$$

(which is satisfiable)

However, we must also consider lower bounds on region cardinalities imposed by membership constraints:

$x \sqsubseteq C, \; x \not\sqsubseteq D \quad \models \quad x \sqsubseteq C \setminus D \quad \models \quad n_7 \geq 1$

...

Then, arithmetic reasoning can give:

$$n_1 = n_2 = 2 \quad n_3 = n_4 = n_6 = 0 \quad n_5 = n_7 = 1 \quad n_8 = 100$$

Set reasoning can give:

$$r_5 = \{y\} \qquad r_7 = \{x\} \qquad r_8 = \{x\}$$

Then, arithmetic reasoning can give:

$$n_1 = n_2 = 2 \quad n_3 = n_4 = n_6 = 0 \quad n_5 = n_7 = 1 \quad n_8 = 100$$

Set reasoning can give:

$$r_5 = \{y\} \qquad r_7 = \{x\} \qquad r_8 = \{x\}$$

We can just add elements to the other regions to match cardinalities:

$$\begin{aligned} r_1 &= \{e_1, e_2\} & r_2 &= \{e_3, e_4\} \\ r_3 &= \emptyset & r_4 &= \emptyset \\ r_5 &= \{e_y\} & r_6 &= \emptyset \\ r_7 &= \{e_x\} & r_8 &= \{e_x, e_5, \ldots, e_{103}\} \end{aligned}$$

Satisfying assignment:

$$\begin{array}{lclcl}
A & = & r_1 \cup r_2 \cup r_3 \cup r_4 & = & \{e_1, e_2, e_3, e_4\} \\
B & = & r_3 \cup r_4 & = & \emptyset \\
C & = & r_1 \cup r_2 \cup r_3 \cup r_4 \cup r_7 & = & \{e_x, e_1, e_2, e_3, e_4\} \\
D & = & r_1 \cup r_2 \cup r_3 \cup r_4 \cup r_5 \cup r_6 & = & \{e_y, e_1, e_2, e_3, e_4\} \\
E & = & r_1 \cup r_2 \cup r_3 \cup r_4 \cup r_5 \cup r_6 & = & \{e_y, e_1, e_2, e_3, e_4\} \\
F & = & r_2 \cup r_4 \cup r_6 \cup r_8 & = & \{e_x, e_5, \ldots, e_{103}\}
\end{array}$$

Original problem:

$x \not\sqsubseteq D,\; y \not\sqsubseteq A \sqcup B \;\; x \sqsubseteq E \sqcup F,\; x \sqsubseteq C,\; y \sqsubseteq D,$

$A \sqcup B \approx C \sqcap D,\; D \approx E,\; |A \sqcup B| \geq 4,\; |C| + |D| \leq 10,\; |E \sqcup F| \geq 100$

# THEORETICAL RESULTS

Our calculus is

- terminating
- refutation sound & complete
- solution sound & complete

for any derivation strategy

# EXPERIMENTAL EVALUATION 1

| file | output | time (s.) | # N | # L |
|---|---|---|---|---|
| vc1 | unsat | 0.00 | 3 | 3 |
| vc2a | unsat | 0.01 | 17 | 8 |
| vc2b | sat | 0.01 | 15 | 7 |
| vc2 | unsat | 0.00 | 8 | 5 |
| vc3a | unsat | 0.00 | 6 | 0 |
| vc3b | sat | 0.01 | 17 | 8 |
| vc3 | unsat | 0.00 | 6 | 0 |
| vc4b | sat | 0.22 | 45 | 16 |
| vc4 | unsat | 0.07 | 57 | 18 |
| vc5b | sat | 1.71 | 71 | 22 |
| vc5 | unsat | 0.36 | 68 | 21 |
| vc6a | unsat | 0.02 | 34 | 14 |
| vc6b | sat | 0.14 | 31 | 13 |
| vc6c | sat | 0.06 | 34 | 14 |
| vc6 | sat | 0.02 | 38 | 18 |

- single query benchmarks
- generated by the Jahob system
- from verifying programs with pointer-based data structures

# EXPERIMENTAL EVALUATION 2

| file | output | time (s.) | # N | # L |
|---|---|---|---|---|
| vc1 | 1 sat/4 unsat | 0.02 | 12 | 6 |
| vc2 | 1 sat/3 unsat | 0.07 | 39 | 23 |
| vc3 | 2 sat/2 unsat | 0.09 | 54 | 21 |
| vc4 | 1 sat/3 unsat | 0.02 | 0 | 0 |
| vc5 | 2 sat/2 unsat | 0.08 | 27 | 13 |
| vc6 | 1 sat/3 unsat | 0.01 | 0 | 0 |
| vc7 | 2 sat/4 unsat | 0.34 | 56 | 33 |
| vc8 | 1 sat/3 unsat | 0.01 | 0 | 0 |
| vc9 | 2 sat/2 unsat | 0.09 | 39 | 19 |
| vc10 | 2 sat/2 unsat | 0.32 | 94 | 32 |

- incremental (i.e., multiple-query) verification conditions
- generated by Leon verification system
- from Scala programs
- mixed constrains over sets, datatypes and bitvectors
- only CVC4 can handle this combination of theories

# Thank you