Model-Driven Computation of Disjunctive Normal Forms

Christoph Lüders

University of Kassel

Symbiont Workshop, 16.03.22, Bonn

SYMBIONT PROJECT

Overview

Preliminaries

Preliminaries: Satisfiability Modulo Theories

- SMT solving tests a first-order formula for satisfiability
- The formula can contain *free constants*
- It allows to produce a witness, called a *model*
- It requires a theory
- We use `QF_LRA`

Preliminaries: Satisfiability Modulo Theories, Example

Example

$\varphi = x > 0 \wedge x < 1$ is satisfiable in `QF_LRA`
$x = \frac{1}{2}$ is a witness

Preliminaries: Satisfiability Modulo Theories, Example

Example

$\varphi = x > 0 \land x < 1$ is satisfiable in QF_LRA
$x = \frac{1}{2}$ is a witness

Example

$\varphi = x > 0 \land x < 1$ is not satisfiable in QF_LIA

Preliminaries: Distributive Normal Form

Definitions:

- Given a set P of *constraints*
- For $p \in P$, we call p and $\neg p$ *literals*
- For literals $\ell_1, \ldots, \ell_r$, we call $\ell_1 \wedge \cdots \wedge \ell_r$ a *conjunction*
- The empty conjunction is **true**
- For conjunctions $\gamma_1, \ldots, \gamma_s$, we call $\gamma_1 \vee \cdots \vee \gamma_s$ a *disjunctive normal form (DNF)*
- The empty disjunction is **false**
- A conjunction of disjunctions is called a *CDC-form*

Preliminaries: Tropical Equilibria

- Tropical polynomials are piecewise linear functions
- Operations are:
  - $a \oplus b := \min(a, b)$
  - $a \otimes b := a + b$
- Tropical polynomials can be interpreted as (convex) polyhedra, possibly unbounded
- Tropical equilibrium of a polynomial:
  - Sort monomials by sign into $\mathcal{P}$ and $\mathcal{N}$
  - Tropicalize $\mathcal{P}$ and $\mathcal{N}$
- Tropical equilibrium of a set of polynomials: intersection of tropical equilibria of polynomials

Preliminaries: Tropical Equilibria, Example

Example

$$x_1^2 + 3x_2 - x_2^3 - x_1 x_2 = 0$$
$$x_1^2 + 3x_2 = x_2^3 + x_1 x_2$$
$$\Downarrow$$
$$\min(2a_1, 3 + a_2) = \min(3a_2, a_1 + a_2)$$

Preliminaries: Tropical Equilibria, Example, cont'd

Example

$$\min(2a_1, 3 + a_2) = \min(3a_2, a_1 + a_2)$$

$$\Updownarrow$$

$$(2a_1 = 3a_2 \ \wedge \ 2a_1 \le 3 + a_2 \ \wedge \ 3a_2 \le a_1 + a_2) \ \vee$$
$$(2a_1 = a_1 + a_2 \ \wedge \ 2a_1 \le 3 + a_2 \ \wedge \ a_1 + a_2 \le 3a_2) \ \vee$$
$$(3 + a_2 = 3a_2 \ \wedge \ 3 + a_2 \le 2a_1 \ \wedge \ 3a_2 \le a_1 + a_2) \ \vee$$
$$(3 + a_2 = a_1 + a_2 \ \wedge \ 3 + a_2 \le 2a_1 \ \wedge \ a_1 + a_2 \le 3a_2)$$

Preliminaries: Tropical Equilibria, Example, cont'd

Example

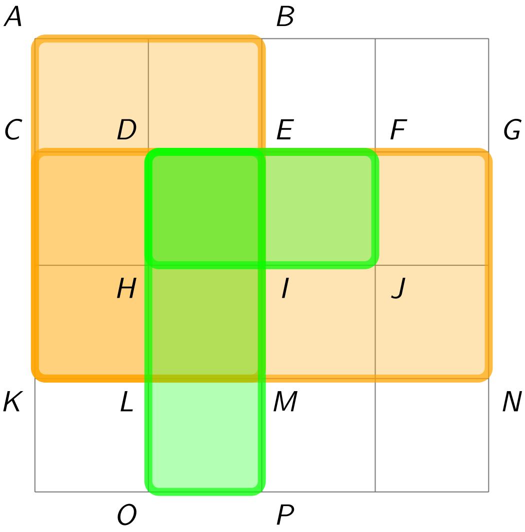
$$\min(2a_1, 3 + a_2) = \min(3a_2, a_1 + a_2)$$
$$\Updownarrow$$
$$(2a_1 = 3a_2 \ \wedge\ 2a_1 \leq 3 + a_2 \ \wedge\ 3a_2 \leq a_1 + a_2) \ \vee$$
$$(2a_1 = a_1 + a_2 \ \wedge\ 2a_1 \leq 3 + a_2 \ \wedge\ a_1 + a_2 \leq 3a_2) \ \vee$$
$$(3 + a_2 = 3a_2 \ \wedge\ 3 + a_2 \leq 2a_1 \ \wedge\ 3a_2 \leq a_1 + a_2) \ \vee$$
$$(3 + a_2 = a_1 + a_2 \ \wedge\ 3 + a_2 \leq 2a_1 \ \wedge\ a_1 + a_2 \leq 3a_2)$$

- The tropical equilibrium of a polynomial is a DNF
- The tropical equilibrium of a set of polynomials is a CDC-form

Example

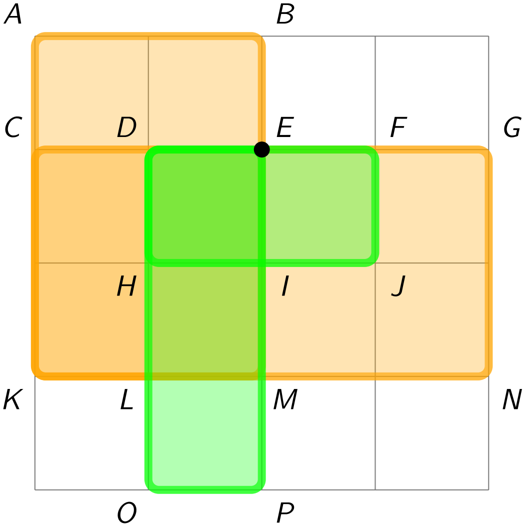
Example

Task: Compute the intersection of the orange and green sections



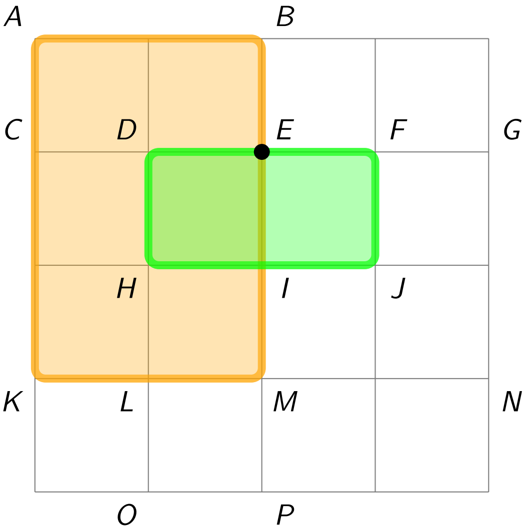
Example

Step 1: SMT solver produces a witness: point E



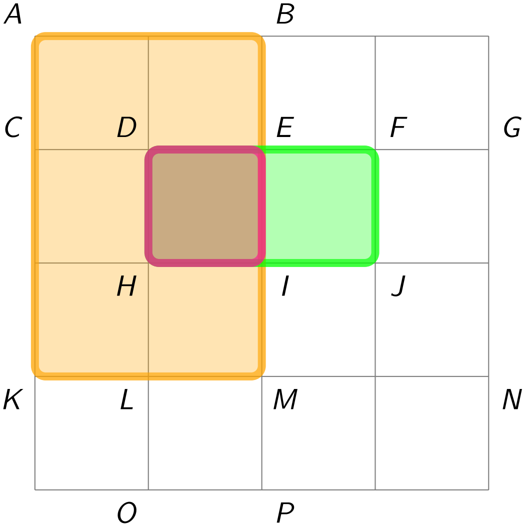
Example

Step 2: For each color, find a DNF that contains the point



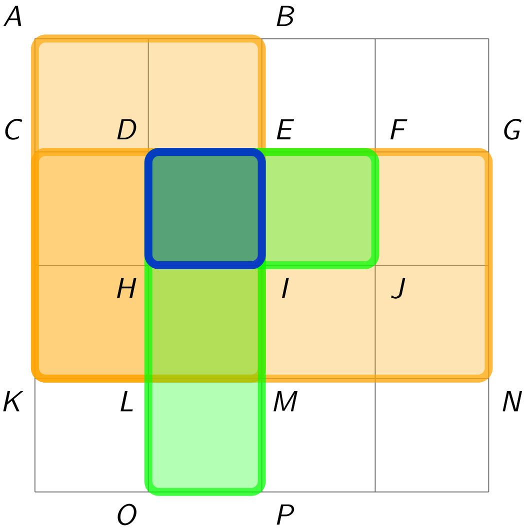
Example

Step 3: Intersect the found DNFs



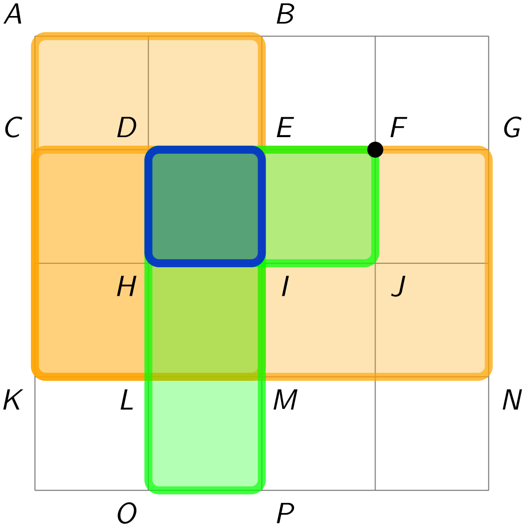
Example

Step 4: Exclude the intersection of DNFs



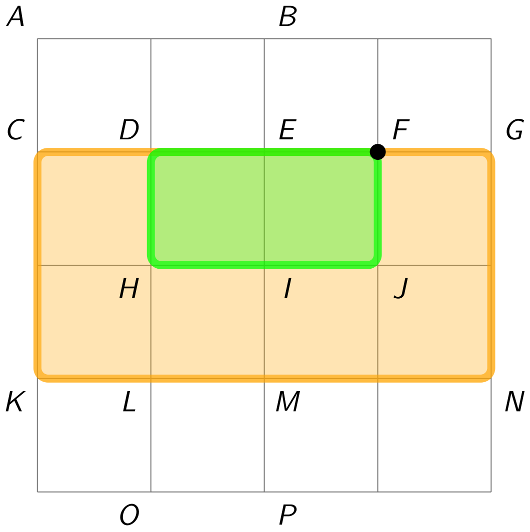
Example

Step 1, pass 2: SMT solver produces a witness: point F



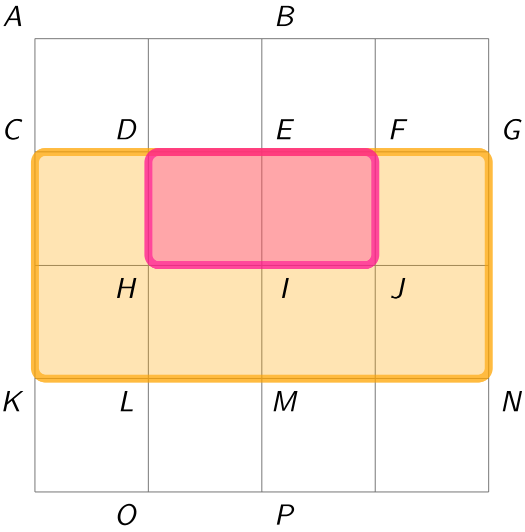
Example

Step 2, pass 2: For each color, find a DNF that contains the point



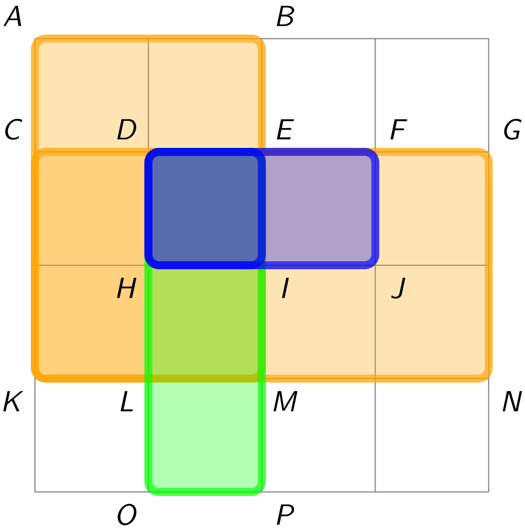
Example

Step 3, pass 2: Intersect the found DNFs



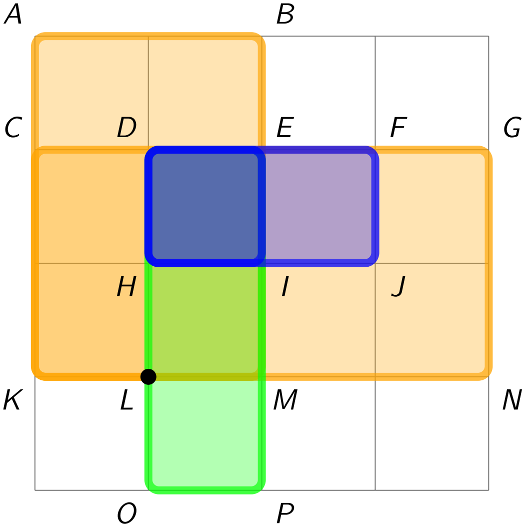
Example

Step 4, pass 2: Exclude the intersection of DNFs



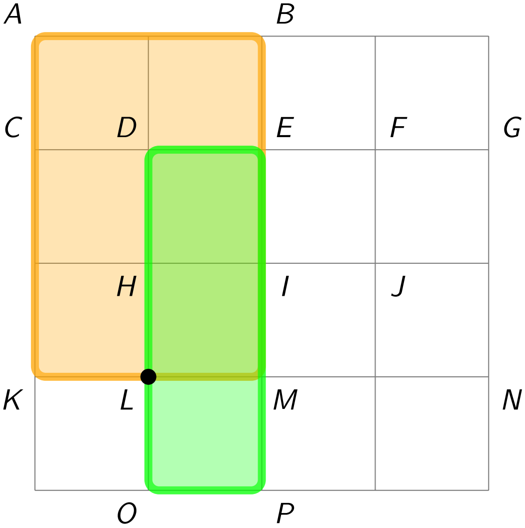
Example

Step 1, pass 3: SMT solver produces a witness: point L



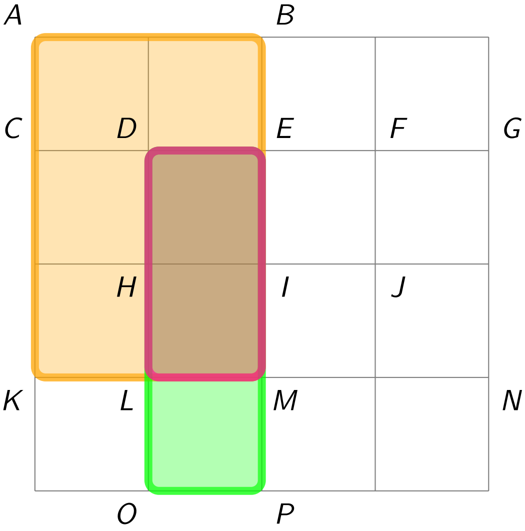
Example

Step 2, pass 3: For each color, find a DNF that contains the point



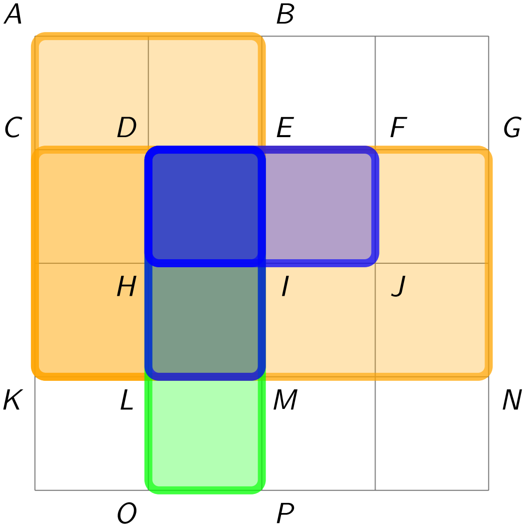
Example

Step 3, pass 3: Intersect the found DNFs



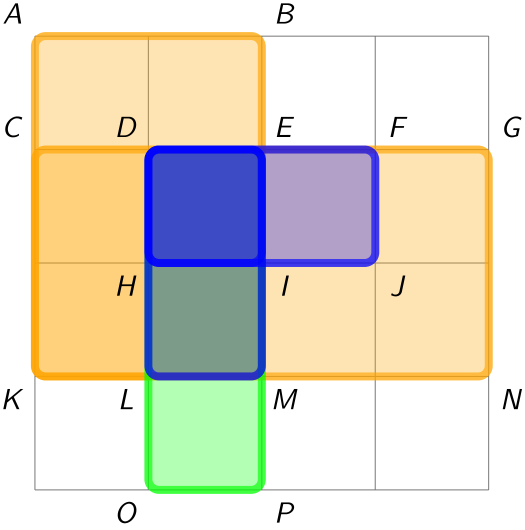
Example

Step 4, pass 3: Exclude the intersection of DNFs



Example

Step 1, pass 4: SMT solver cannot produce a witness: **unsat**!



The Calculus

The Calculus

- A *state* is a 4-tuple $(\varphi, \delta, \psi, \zeta)$, where φ is a formula, δ is a DNF, ψ is a formula or $\perp$, and ζ is a DNF or $\perp$
- The input is the CDC-form

$$\varphi = \bigwedge_{i \in \mathcal{I}} \bigvee_{j \in \mathcal{J}_i} \gamma_{i,j}$$

- The initial state is

$$S_0 := (\varphi_0, \text{false}, \perp, \perp)$$

- If no rules are applicable, an end state $(\varphi, \delta_{\text{end}}, \psi, \zeta)$ is reached with δ_{end} as the output

The Calculus, cont'd

Filter:

$$(\varphi,\,\delta,\,\bot,\,\bot) \implies (\varphi,\,\delta,\,\psi_0,\,\text{false})$$

where $\varphi = \varphi_0 \wedge \varphi_*$, $\psi_0 = \bigwedge_{i\in\mathcal{I}} \bigvee_{j\in\mathcal{S}(\varphi_0,M,i)} \gamma_{i,j}$

if φ is sat with $M \models \varphi$

Add Clause:

$$(\varphi,\,\delta,\,\psi,\,\zeta) \implies (\varphi,\,\delta,\,\psi \wedge \neg\gamma',\,\zeta \vee \gamma')$$

where $\psi = \psi_0 \wedge \psi^*$, $\psi_0 = \bigwedge_{i\in\mathcal{I}} \bigvee_{j\in\mathcal{S}(\varphi_0,M,i)} \gamma_{i,j}$, $\gamma' = \bigwedge_{i\in\mathcal{I}} \gamma_{i,\mathsf{S}(\psi_0,N,i)}$

if $\psi \neq \bot$, $\zeta \neq \bot$, and ψ is sat with $N \models \psi$

Entailment:

$$(\varphi,\,\delta,\,\psi,\,\zeta) \implies (\varphi,\,\delta,\,\psi,\,\zeta')$$

where $\zeta = \gamma_1 \vee \cdots \vee \gamma_s \vee \gamma'$, $\zeta' = \gamma_1 \vee \cdots \vee \gamma_{k-1} \vee \gamma_{k+1} \vee \cdots \vee \gamma_s \vee \gamma'$

if $\psi \neq \bot$, $\zeta \neq \bot$, and $\gamma_k \longrightarrow \gamma'$ is sat

Combine:

$$(\varphi,\,\delta,\,\psi,\,\zeta) \implies (\varphi \wedge \neg\zeta,\,\delta \vee \zeta,\,\bot,\,\bot)$$

if $\psi \neq \bot$, $\zeta \neq \bot$, and ψ is unsat

Theorems

The Calculus: Termination

Theorem (Termination)

The calculus terminates. In other words, there are no infinite derivations

$$S_0 \vdash S_1 \vdash \dots$$

The Calculus: Invariant

Proposition (Invariant of the calculus)

Consider a derivation

$$S_0 \vdash^* T.$$

$S_0 = (\varphi_0, \text{false}, \cdot, \cdot)$ is the initial state, where φ_0 is the input formula.
$T = (\varphi, \delta, \cdot, \cdot)$ is a state. Then

$$\varphi \vee \delta \equiv \varphi_0.$$

The Calculus: Soundness

Theorem (Soundness)

The calculus is sound. In other words, let φ_0 be an input CDC-form and let δ_{end} be an output DNF. Consider a terminating derivation

$$S_0 \vdash^* T,$$

where $S_0 = (\varphi_0, \cdot, \cdot, \cdot)$ is the initial state and $T = (\cdot, \delta_{\mathrm{end}}, \cdot, \cdot)$ is a terminating state. Then

$$\varphi_0 \equiv \delta_{\mathrm{end}}.$$

The Calculus: Minimality

Proposition (Minimality)

Consider a derivation

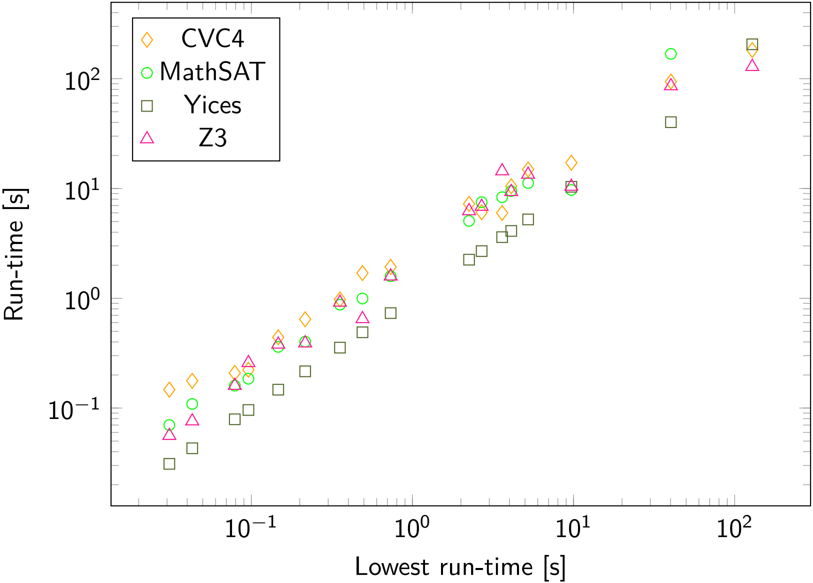
$$S_0 \vdash^* V,$$

where **Entailment** is applied whenever applicable. S_0 denotes the initial state. $V = (\cdot, \delta, \cdot, \cdot)$ is a state. δ is a DNF and has the form $\bigvee_k \gamma_k$. Let ℓ, $m \in \mathbb{N}$ such that $\ell \neq m$. Then

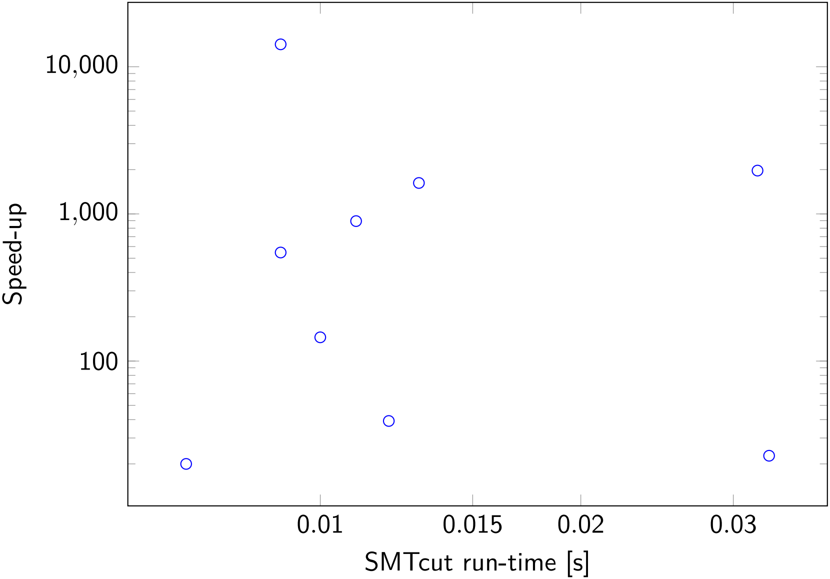
$$\gamma_\ell \nVdash \gamma_m.$$

Benchmarks

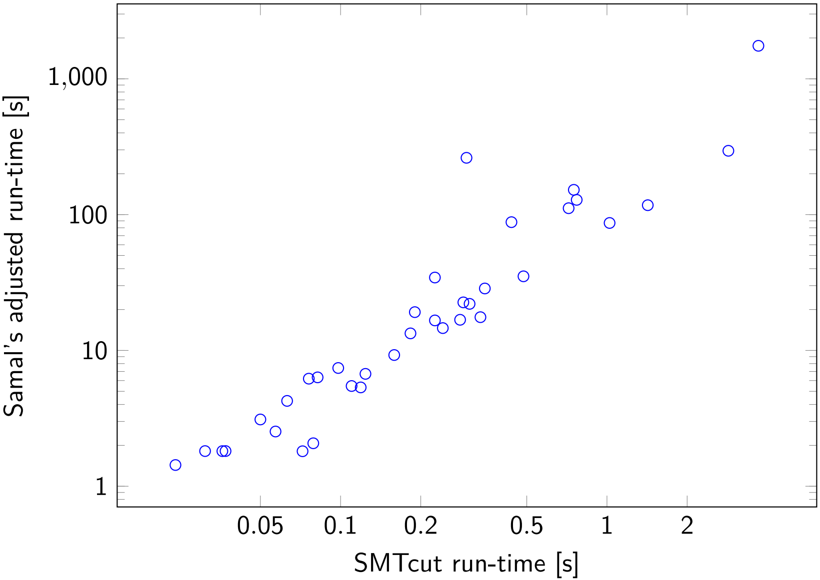
Benchmarks: Different Solvers



Benchmarks: SMTcut vs. Redlog



Benchmarks: SMTcut vs. Samal 2016



End credits

Thank you for your attention!

Thanks to Thomas Sturm.

This work has been supported by ANR-17-CE40-0036 / DFG-391322026 SYMBIONT.

SYMBIONT PROJECT