Comparing Different Projection Operators in the Cylindrical Algebraic Decomposition for SMT Solving

Tarik Viehmann, **Gereon Kremer**, Erika Ábrahám

SC^2 Workshop July 29th

Outline

1. Preliminaries
2. CAD
3. Experiments
   - Projections
   - SMT solving
   - Incompleteness of McCallum / Brown
   - Effects of squarefree basis
4. Conclusion

Nonlinear arithmetic QF_NRA

Definition (Nonlinear arithmetic)

Boolean combinations of **polynomial** constraints over reals

Nonlinear arithmetic QF_NRA

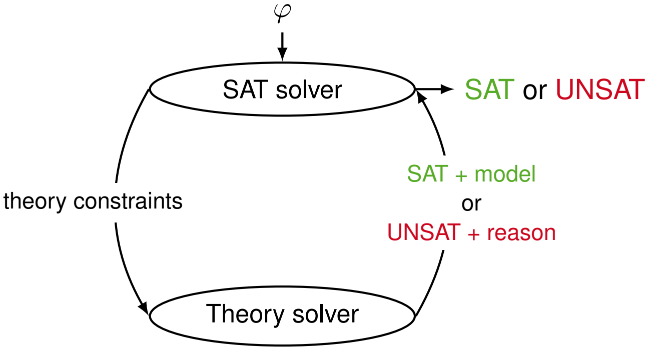
Definition (Nonlinear arithmetic)

Boolean combinations of **polynomial** constraints over reals

Example

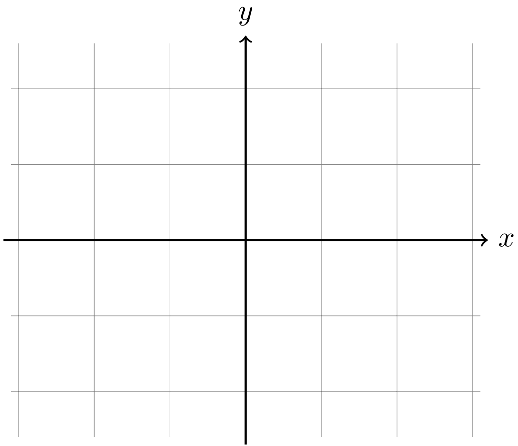
$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$

SMT Solving


φ
SAT solver
SAT or UNSAT
theory constraints
SAT + model
or
UNSAT + reason
Theory solver

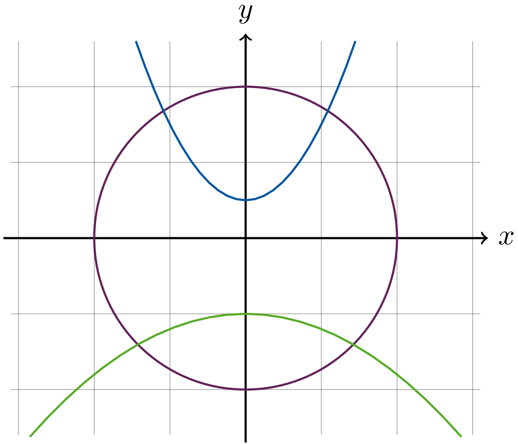
Cylindrical Algebraic Decomposition

$$\exists x, y. \quad x^2 + y^2 - 4 \leq 0 \land (x^2 - y + 0.5 < 0 \lor x^2 + 5 \cdot y + 5 < 0)$$



Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$

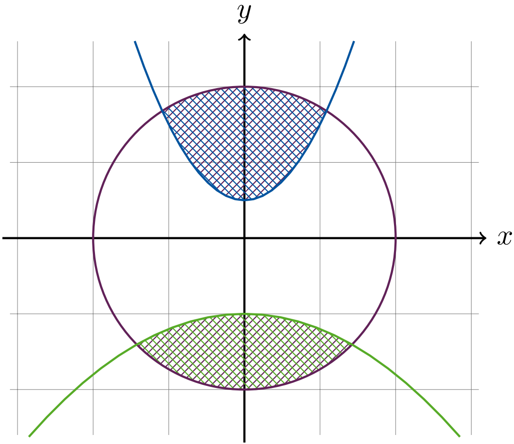


- Where are solutions?

$\rightarrow$ Sign-invariant regions

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$

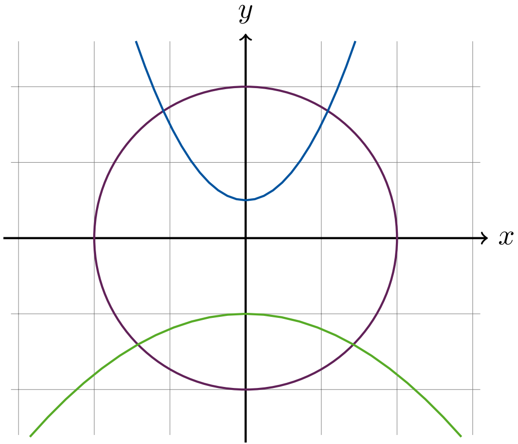


- Where are solutions?

$\rightarrow$ Sign-invariant regions

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \land (x^2 - y + 0.5 < 0 \lor x^2 + 5 \cdot y + 5 < 0)$$



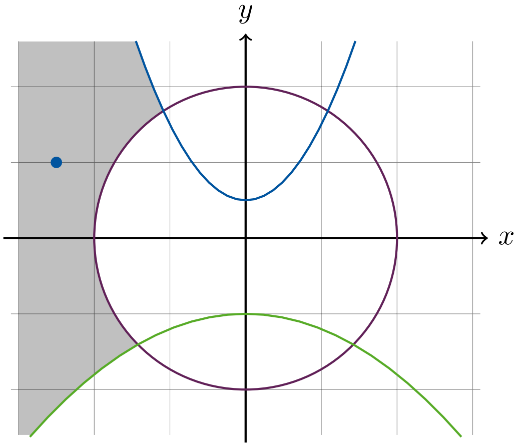
- Where are solutions?

→ Sign-invariant regions

- What would a human do?

Cylindrical Algebraic Decomposition

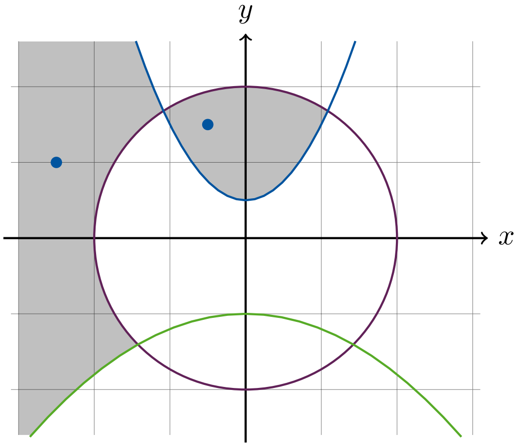
$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \land (x^2 - y + 0.5 < 0 \lor x^2 + 5 \cdot y + 5 < 0)$$



- Where are solutions?
- → Sign-invariant regions
- What would a human do?

Cylindrical Algebraic Decomposition

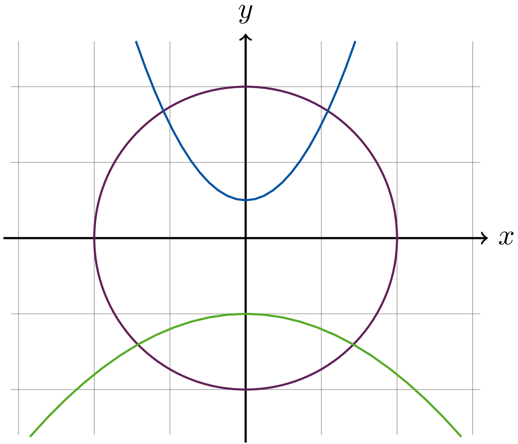
$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



- ▶ Where are solutions?
- → Sign-invariant regions
- ▶ What would a human do?

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \land (x^2 - y + 0.5 < 0 \lor x^2 + 5 \cdot y + 5 < 0)$$



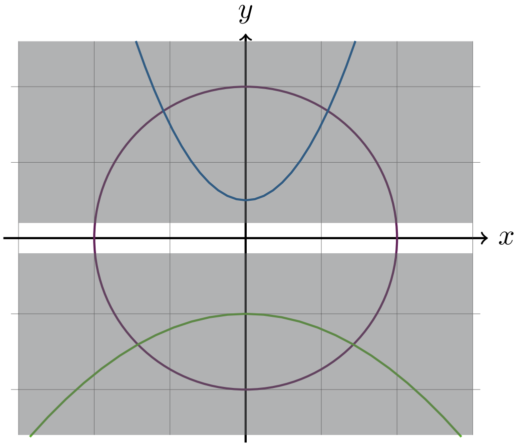
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



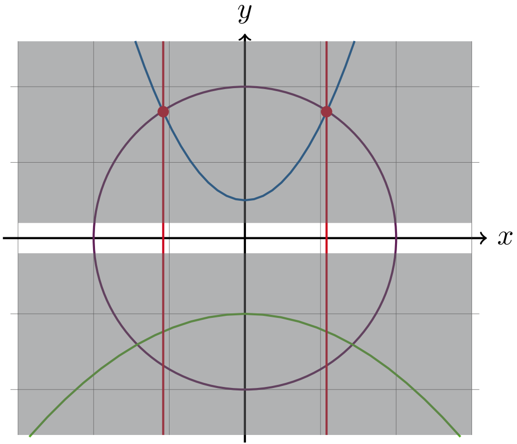
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x

Cylindrical Algebraic Decomposition

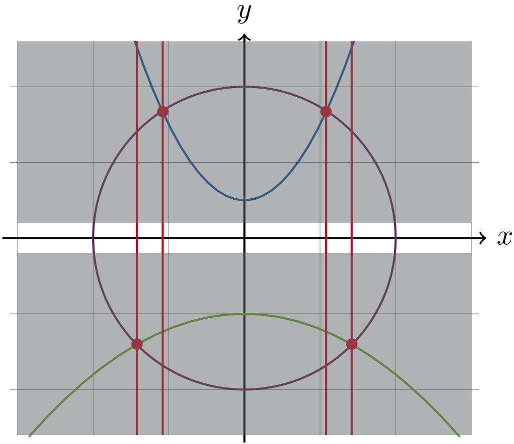
$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



- Where are solutions?
- → Sign-invariant regions
- What would a human do?
- What would CAD do?
  - First dimension x

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



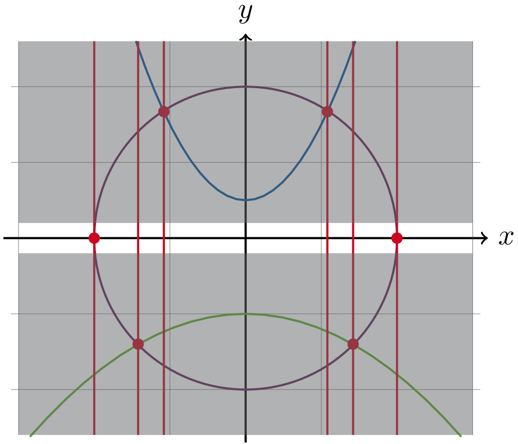
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



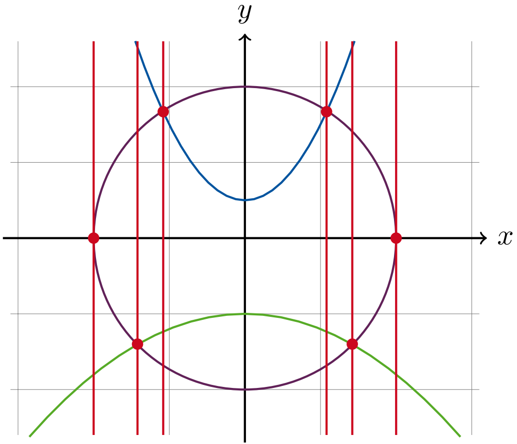
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



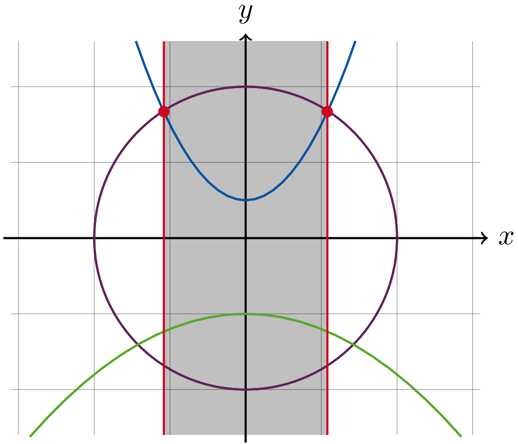
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \land (x^2 - y + 0.5 < 0 \lor x^2 + 5 \cdot y + 5 < 0)$$



- Where are solutions?

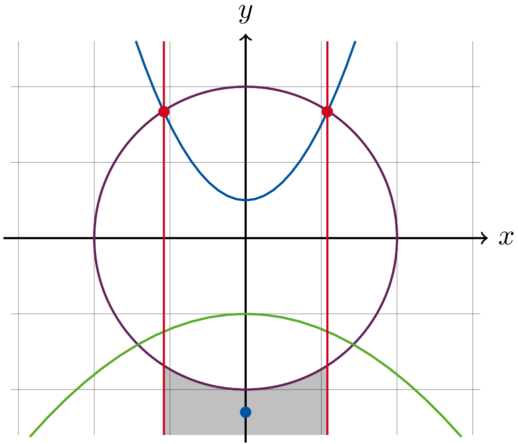
→ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y

RWTH AACHEN UNIVERSITY

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



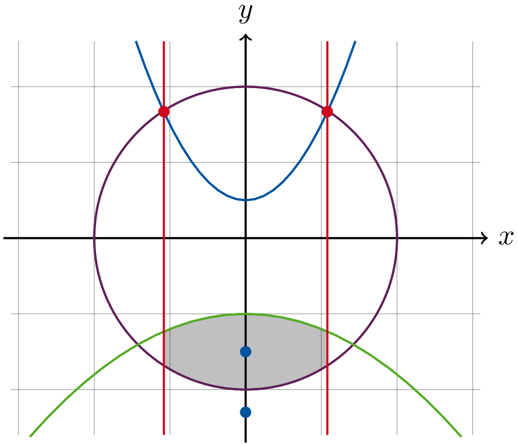
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y
  - Test sample points

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



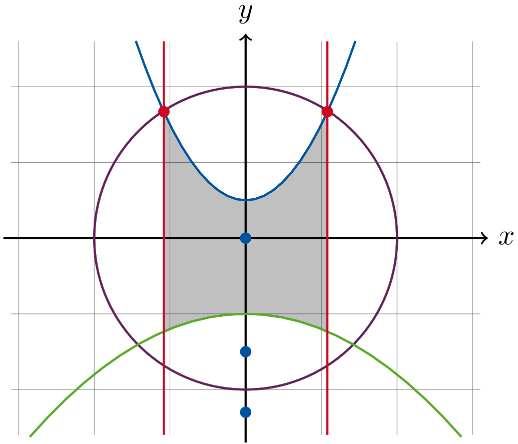
- Where are solutions?

→ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y
  - Test sample points

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



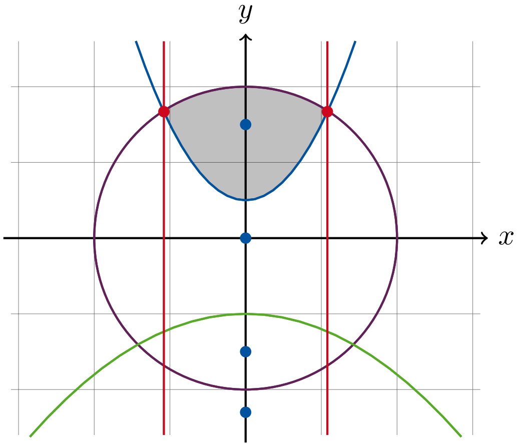
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y
  - Test sample points

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



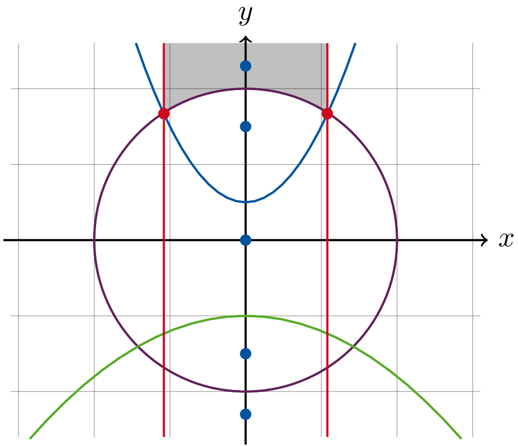
- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y
  - Test sample points

Cylindrical Algebraic Decomposition

$$\exists x, y. \qquad x^2 + y^2 - 4 \leq 0 \wedge (x^2 - y + 0.5 < 0 \vee x^2 + 5 \cdot y + 5 < 0)$$



- Where are solutions?

$\rightarrow$ Sign-invariant regions

- What would a human do?
- What would CAD do?
  - First dimension x
  - Second dimension y
  - Test sample points

Cylindrical Algebraic Decomposition

$$
\begin{array}{c}
P_n \subseteq \mathbb{Z}[x_1, \ldots, x_n] \\
\text{project} \big\downarrow \\
P_{n-1} \subseteq \mathbb{Z}[x_1, \ldots, x_{n-1}] \\
\text{project} \big\downarrow \\
\vdots \\
\text{project} \big\downarrow \\
P_1 \subseteq \mathbb{Z}[x_1]
\end{array}
$$

Cylindrical Algebraic Decomposition

$$
\begin{tikzcd}
P_n \subseteq \mathbb{Z}[x_1, \ldots, x_n] \arrow[d, "\text{project}"'] & Z_n \subseteq Z_{n-1} \times \mathbb{R} \\
P_{n-1} \subseteq \mathbb{Z}[x_1, \ldots, x_{n-1}] \arrow[d, "\text{project}"'] & \vdots \arrow[u, "\mathit{roots}(P_n \text{ at } Z_{n-1})"'] \\
\vdots \arrow[d, "\text{project}"'] & Z_2 \subseteq Z_1 \times \mathbb{R} \arrow[u, "\mathit{roots}(P_3 \text{ at } Z_2)"'] \\
P_1 \subseteq \mathbb{Z}[x_1] \arrow[r, bend right, "\mathit{roots}(P_1)"'] & Z_1 \subseteq \mathbb{R} \arrow[u, "\mathit{roots}(P_2 \text{ at } Z_1)"']
\end{tikzcd}
$$

RWTH AACHEN UNIVERSITY

Cylindrical Algebraic Decomposition

Projection

$$P_n \subseteq \mathbb{Z}[x_1, \dots, x_n]$$

project $\downarrow$

$$P_{n-1} \subseteq \mathbb{Z}[x_1, \dots, x_{n-1}]$$

project $\downarrow$

$$\vdots$$

project $\downarrow$

$$P_1 \subseteq \mathbb{Z}[x_1]$$

$$P_1 \xrightarrow{roots(P_1)} Z_1$$

$$Z_1 \subseteq \mathbb{R}$$

$\uparrow$ $roots(P_2 \text{ at } Z_1)$

$$Z_2 \subseteq Z_1 \times \mathbb{R}$$

$\uparrow$ $roots(P_3 \text{ at } Z_2)$

$$\vdots$$

$\uparrow$ $roots(P_n \text{ at } Z_{n-1})$

$$Z_n \subseteq Z_{n-1} \times \mathbb{R}$$

Projection Operators

We consider:

- Collins
- Hong
- McCallum
- Brown

Projection Operators

We consider:

- Collins
- Hong
- McCallum
- Brown

Not considered:

- Lazard
- Seidl & Sturm
- Strzeboński
- Brown & Košta
- ...

Collins & Hong

Definition (Collins' operator [Collins75])

$$proj_C^1 := \bigcup_{p \in P} \left(coeffs(p) \cup \bigcup_{r \in RED(p)} PSC(r, r') \right)$$

$$proj_C^2 := \bigcup_{p,q \in P} \bigcup_{\substack{r_p \in RED(p) \\ r_q \in RED(q)}} PSC(r_p, r_q)$$

$$proj_C := proj_C^1 \cup proj_C^2$$

Collins & Hong

Definition (Hong's operator [Hong90])

$$proj_C^1 := \bigcup_{p \in P} \left(coeffs(p) \cup \bigcup_{r \in RED(p)} PSC(r, r') \right)$$

$$proj_H^2 := \bigcup_{p,q \in P} \bigcup_{r_p \in RED(p)} PSC(r_p, q)$$

$$proj_H := proj_C^1 \cup proj_H^2$$

McCallum & Brown

Definition (McCallum's operator [McCallum84])

Let P be a squarefree basis.

$$proj_M^1 := \bigcup_{p \in P} \{disc(p)\} \cup coeffs(p)$$

$$proj_M^2 := \bigcup_{p,q \in P} \{res(p, q)\}$$

$$proj_M := proj_M^1 \cup proj_M^2$$

Incomplete!

RWTH AACHEN UNIVERSITY

McCallum & Brown

Definition (Brown's operator [Brown01])

Let P be a squarefree basis.

$$proj_B^1 := \bigcup_{p \in P} \{disc(p)\} \cup \{lcf(p)\}$$

$$proj_M^2 := \bigcup_{p,q \in P} \{res(p,q)\}$$

$$proj_B := proj_B^1 \cup proj_M^2$$

Incomplete!

Experiments

- SMT-RAT
  - Projections: CAD only
  - SMT solving: SAT + VS + CAD

Experiments

- SMT-RAT
  - Projections: CAD only
  - SMT solving: SAT + VS + CAD
  - No squarefree basis, no delineating polynomials (McCallum), no additional points (Brown)
  - But: fully incremental, early abort

RWTH AACHEN UNIVERSITY

Experiments

- SMT-RAT
  - Projections: CAD only
  - SMT solving: SAT + VS + CAD
  - No squarefree basis, no delineating polynomials (McCallum), no additional points (Brown)
  - But: fully incremental, early abort
- QF_NRA from SMT-COMP 2014
- Timeout 60s

Experiments

- SMT-RAT
  - Projections: CAD only
  - SMT solving: SAT + VS + CAD
  - No squarefree basis, no delineating polynomials (McCallum), no additional points (Brown)
  - But: fully incremental, early abort
- QF_NRA from SMT-COMP 2014
- Timeout 60s
- Analyzed:
  - Different projection operators
  - Different projection orders

Experiments

- SMT-RAT
  - Projections: CAD only
  - SMT solving: SAT + VS + CAD
  - No squarefree basis, no delineating polynomials (McCallum), no additional points (Brown)
  - But: fully incremental, early abort
- QF_NRA from SMT-COMP 2014
- Timeout 60s

- Analyzed:
  - Different projection operators
  - Different projection orders
- Not analyzed yet:
  - Different variable orderings
  - Different lifting orders

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated

RWTH AACHEN UNIVERSITY

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

RWTH AACHEN UNIVERSITY

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

	Level 1	Level 2	Level 3	Level 4
Collins	10.9 / 7.8			
Hong	8.6 / 7.8			
McCallum	6.1 / 6.7			
Brown	5.3 / 6.7			

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

	Level 1	Level 2	Level 3	Level 4
Collins	10.9 / 7.8	783.1 / 26.4		
Hong	8.6 / 7.8	158.8 / 26.2		
McCallum	6.1 / 6.7	16.7 / 13.3		
Brown	5.3 / 6.7	11.6 / 13.5		

RWTH AACHEN UNIVERSITY

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

	Level 1	Level 2	Level 3	Level 4
Collins	10.9 / 7.8	783.1 / 26.4	117.0 / 11.9	
Hong	8.6 / 7.8	158.8 / 26.2	20.2 / 11.7	
McCallum	6.1 / 6.7	16.7 / 13.3	5.1 / 5.3	
Brown	5.3 / 6.7	11.6 / 13.5	4.7 / 5.1	

RWTH AACHEN UNIVERSITY

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

	Level 1	Level 2	Level 3	Level 4
Collins	10.9 / 7.8	783.1 / 26.4	117.0 / 11.9	15.6 / 5.3
Hong	8.6 / 7.8	158.8 / 26.2	20.2 / 11.7	10.3 / 5.1
McCallum	6.1 / 6.7	16.7 / 13.3	5.1 / 5.3	7.9 / 3.8
Brown	5.3 / 6.7	11.6 / 13.5	4.7 / 5.1	5.5 / 3.5

RWTH AACHEN UNIVERSITY

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

	Level 1	Level 2	Level 3	Level 4
Collins	10.9 / 7.8	783.1 / 26.4	117.0 / 11.9	15.6 / 5.3
Hong	8.6 / 7.8	158.8 / 26.2	20.2 / 11.7	10.3 / 5.1
McCallum	6.1 / 6.7	16.7 / 13.3	5.1 / 5.3	7.9 / 3.8
Brown	5.3 / 6.7	11.6 / 13.5	4.7 / 5.1	5.5 / 3.5

- Theory: $proj_B \subseteq proj_M \subseteq proj_H \subseteq proj_C$

RWTH AACHEN UNIVERSITY

Projection sizes

- Project **all polynomials**, ignore boolean structure
- 5698 benchmarks such that all projections terminated
- On average 6.4 **polynomials** of degree 5.2 (**total degree** 6.1)
- Rarely more than 5 variables

	Level 1	Level 2	Level 3	Level 4
Collins	10.9 / 7.8	783.1 / 26.4	117.0 / 11.9	15.6 / 5.3
Hong	8.6 / 7.8	158.8 / 26.2	20.2 / 11.7	10.3 / 5.1
McCallum	6.1 / 6.7	16.7 / 13.3	5.1 / 5.3	7.9 / 3.8
Brown	5.3 / 6.7	11.6 / 13.5	4.7 / 5.1	5.5 / 3.5

- Theory: $proj_B \subseteq proj_M \subseteq proj_H \subseteq proj_C$
- Hong may be viable if **incompleteness** of McCallum is an issue

RWTH AACHEN UNIVERSITY

SMT solving performance

- 5698 benchmarks from before
- Incremental calls from SAT module
- **Incremental projection**, early abort if **satisfying solution** is found

SMT solving performance

- 5698 benchmarks from before
- Incremental calls from SAT module
- **Incremental projection**, early abort if **satisfying solution** is found
- $\Rightarrow$ Size of projection may not be that crucial

SMT solving performance

- 5698 benchmarks from before
- Incremental calls from SAT module
- **Incremental projection**, early abort if **satisfying solution** is found
- $\Rightarrow$ Size of projection may not be that crucial

Operator	Solved	Timeout
Collins	5041	657
Hong	5125	573
McCallum	5284	414
Brown	5299	399

McCallum vs. Brown

- Similar behaviour, but some outliers in **both directions**

RWTH AACHEN UNIVERSITY

McCallum vs. Brown

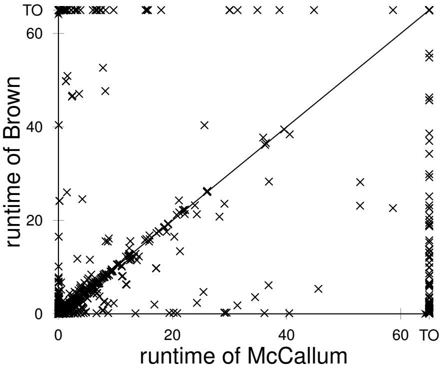
- Similar behaviour, but some outliers in **both directions**
- Make behaviour different

McCallum vs. Brown

- Similar behaviour, but some outliers in **both directions**
- Make behaviour different
- Modify Brown: Consider **resultants last** for projection

McCallum vs. Brown

- Similar behaviour, but some outliers in **both directions**
- Make behaviour different
- Modify Brown: Consider **resultants last** for projection



Incompleteness of McCallum / Brown

- McCallum and Brown are **incomplete**
- Is this a problem in **practice**?

Incompleteness of McCallum / Brown

- McCallum and Brown are **incomplete**
- Is this a problem in **practice**?

- 510 out of 5889 benchmarks

  (may be fixed by delineating polynomials or additional points)

Incompleteness of McCallum / Brown

- McCallum and Brown are **incomplete**
- Is this a problem in **practice**?

- 510 out of 5889 benchmarks
  (may be fixed by delineating polynomials or additional points)
- 353 were found to be satisfiable
- 157 were found to be unsatisfiable

Incompleteness of McCallum / Brown

- McCallum and Brown are **incomplete**
- Is this a problem in **practice**?

- 510 out of 5889 benchmarks

  (may be fixed by delineating polynomials or additional points)
- 353 were found to be satisfiable
- 157 were found to be unsatisfiable

- **All are correct!**

Incompleteness of McCallum / Brown

- McCallum and Brown are **incomplete**
- Is this a problem in **practice**?

- 510 out of 5889 benchmarks
  (may be fixed by delineating polynomials or additional points)
- 353 were found to be satisfiable
- 157 were found to be unsatisfiable

- **All are correct!**

- $\Rightarrow$ not a pressing issue **on our SMT benchmarks**

Effects of squarefree basis

- McCallum / Brown require P_k to be a **squarefree basis**
- **Difficult** to compute ignored until now

Effects of squarefree basis

- McCallum / Brown require P_k to be a **squarefree basis**
- **Difficult** to compute ignored until now

- Using CoCoALib

Effects of squarefree basis

- McCallum / Brown require P_k to be a **squarefree basis**
- **Difficult** to compute ignored until now

- Using CoCoALib
- Overall solving is about 10% **slower**
- But **less timeouts!** McCallum: $889 \to 739$, Brown: $842 \to 739$
- McCallum closes in on Brown!

RWTH AACHEN UNIVERSITY

Effects of squarefree basis

- McCallum / Brown require P_k to be a **squarefree basis**
- **Difficult** to compute ignored until now

- Using CoCoALib
- Overall solving is about 10% **slower**
- But **less timeouts!** McCallum: $889 \to 739$, Brown: $842 \to 739$
- McCallum closes in on Brown!

- $\Rightarrow$ usually detrimental, sometimes essential
  required for correctness!

Conclusion

- Overall trend matches theoretical expectation
- Individual examples **may vary wildly**
- $\Rightarrow$ Portfolio?

RWTH AACHEN UNIVERSITY

Conclusion

- Overall trend matches theoretical expectation
- Individual examples **may vary wildly**
- $\Rightarrow$ Portfolio?

- **Incompleteness** is not a pressing issue (for us)
- Computing squarefree basis is rather **expensive**

RWTH AACHEN UNIVERSITY

Conclusion

- Overall trend matches theoretical expectation
- Individual examples **may vary wildly**
- $\Rightarrow$ Portfolio?

- **Incompleteness** is not a pressing issue (for us)
- Computing squarefree basis is rather **expensive**

- Adapt variable ordering?
- Effects of delineating polynomials and additional points?

RWTH AACHEN UNIVERSITY

References

- Chistopher W. Brown, **Improved projection for cylindrical algebraic decomposition**, JSC **32** (2001).
- George E. Collins, **Quantifier elimination for real closed fields by cylindrical algebraic decompostion**, ATFL'75.
- Hoon Hong, **An improvement of the projection operator in cylindrical algebraic decomposition**, ISSAC '90.
- Scott McCallum, **An improved projection operation for cylindrical algebraic decomposition**, Ph.D. thesis, 1984.

RWTH AACHEN UNIVERSITY

Notation

Definition (Polynomials)

$p = \sum_{i=0}^{m} a_i \cdot x_n^i$ in **main variable** x_n and $a_i \in \mathbb{R}[x_1, ..., x_{n-1}]$.

Definition (Simple properties)

$$coeffs(p) := \{a_0, ..., a_m\} \qquad lcf(p) := a_m$$

$$red_k(p) := \sum_{i=0}^{m-k} a_i \cdot x_n^i \qquad red(p) := \{red_k(p) \mid k = 0 \ldots m\}$$

Building blocks

$$Syl(p, q) := \begin{pmatrix} a_k & \cdots & a_0 & & & \\ & a_k & \cdots & a_0 & & \\ & & \ddots & & \ddots & \\ & & & a_k & \cdots & a_0 \\ b_l & \cdots & b_0 & & & \\ & b_l & \cdots & b_0 & & \\ & & \ddots & & \ddots & \\ & & & b_l & \cdots & b_0 \end{pmatrix} \begin{array}{l} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} l \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} k \end{array}$$

Building blocks

$$M_j(p,q) := \begin{pmatrix} a_k & & \cdots & & a_0 & & & \\ & a_k & & \cdots & & a_0 & & \\ & & \ddots & & & & \ddots & \\ & & & a_k & & \cdots & & a_0 \\ b_l & & \cdots & & b_0 & & & \\ & b_l & & \cdots & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & b_l & & \cdots & & b_0 \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} l-j \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} k-j \end{matrix}$$

Building blocks

$$M_j(p,q) := \begin{pmatrix} a_k & \cdots & a_0 & & & & \\ & a_k & \cdots & a_0 & & & \\ & & \ddots & & \ddots & & \\ & & & a_k & \cdots & a_0 & \\ b_l & \cdots & b_0 & & & & \\ & b_l & \cdots & b_0 & & & \\ & & \ddots & & \ddots & & \\ & & & b_l & \cdots & b_0 & \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ \ddots \\ a \end{matrix}}\right\} l-j \\ \left.\vphantom{\begin{matrix} b \\ b \\ \ddots \\ b \end{matrix}}\right\} k-j \end{matrix}$$

Definition (Principal subresultant coefficients)

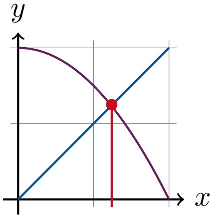
$$psc_i(p,q) := \det(M_i)$$
$$PSC(p,q) := \{psc_i \mid i = 0 \ldots \min(k,l)\}$$

Building blocks

Definition (Resultant)

$$res(p, q) := \det(Syl(p, q))$$

p, q have a **common root** $\Leftrightarrow$ $res(p, q)$ has a root



Definition (Discriminant)

$$disc(p) := res(p, p')$$

p has a **multiple root** $\Leftrightarrow$ $disc(p)$ has a root