Towards Efficient Quantifier Elimination in Mathematica

Katherine Cordwell

15824

December 11, 2018

What is quantifier elimination (QE)?

- Example: $\forall x_1 \exists x_2 (x_1 + x_2 = 0)$ becomes "True"

[1] Adapted from Pablo Parillo's lecture notes

What is quantifier elimination (QE)?

- Example: $\forall x_1 \exists x_2 (x_1 + x_2 = 0)$ becomes "True"
- Example: $\forall x_1 \forall x_2 (x_1^2 + a x_2^2 \leq 1) \rightarrow a x_1^2 - a^2 x_1 x_2 + 2 \geq 0$ becomes $(a \geq 0) \wedge (a^3 - 8a - 16) \leq 0$[1]

[1] Adapted from Pablo Parillo's lecture notes

Two seminal results

- Quantifier elimination is decidable (Tarski, 1930).
- Cylindrical algebraic decomposition (CAD) algorithm (Collins, 1975)

Why is QE important in theorem proving?

- Safety proofs of hybrid systems reduce to real arithmetic questions.
- Efficient QE is key for efficient proofs.

Why is QE important in theorem proving?

- Safety proofs of hybrid systems reduce to real arithmetic questions.
- Efficient QE is key for efficient proofs.
- KeYmaera X outsources QE calls to Mathematica.

Our Goal

Improve quantifier elimination in Mathematica, with a view towards increasing the efficiency of KeYmaera X.

Our Approach

- Focus on the universal fragment of decision problems

$$\forall x_1, \forall x_2, \ldots, \forall x_k \; \phi(x_1, \ldots, x_k)$$

Our Approach

- Focus on the universal fragment of decision problems

$$\forall x_1, \forall x_2, \ldots, \forall x_k \ \phi(x_1, \ldots, x_k)$$

- Because we can put formulas into CNF, we focus on disjunctions.

$$\forall x_1, \ldots, x_n (\phi_1 \wedge \phi_2)$$

$$\forall x_1, \ldots, x_n \ \phi_1 \qquad \forall x_1, \ldots, x_n \ \phi_2$$

Our Approach

Two sub-approaches:

- Analyze the structures of the input polynomials.
- Analyze the structures of the polynomials computed during CAD.

Our Approach

Two sub-approaches:

- Analyze the structures of the input polynomials.
- Analyze the structures of the polynomials computed during CAD.

Odd Degree Variables

Example 1

$$\forall v, w, x, y, z(-6 - 7v^2w^3x + 9v^2w^3xyz + 6v^3w^2z^2 > 0 \vee$$
$$6 - 5v^2w^2xy + 7v^3wx^3yz + vy^3z > 0)$$

Odd Degree Variables

Example 1

$\forall v, w, x, y, z(-6 - 7v^2w^3x + 9v^2w^3xyz + 6v^3w^2z^2 > 0 \vee$
$6 - 5v^2w^2xy + 7v^3wx^3yz + vy^3z > 0)$

- Notice that v has odd degree in both polynomials.

Odd Degree Variables

Example 1

$\forall v, w, x, y, z(-6 - 7v^2w^3x + 9v^2w^3xyz + 6v^3w^2z^2 > 0 \vee$
$6 - 5v^2w^2xy + 7v^3wx^3yz + vy^3z > 0)$

- Notice that v has odd degree in both polynomials.
- Find values of w, x, y, z so that $6w^2z^2$ and $7wx^3yz$ are either both positive or both negative. (E.g. $w = x = y = z = 1$.)

Odd Degree Variables

Example 1

$\forall v, w, x, y, z(-6 - 7v^2w^3x + 9v^2w^3xyz + 6v^3w^2z^2 > 0 \vee$
$6 - 5v^2w^2xy + 7v^3wx^3yz + vy^3z > 0)$

- Notice that v has odd degree in both polynomials.
- Find values of w, x, y, z so that $6w^2z^2$ and $7wx^3yz$ are either both positive or both negative. (E.g. $w = x = y = z = 1$.)
- Return FALSE with "v is $-\infty$, all other variables are 1" as a witness.

Set a Variable to 0

Example 2

$\forall v, w, x, y, z\ (1 - 10vw^2y - v^3x^3yz^2 - v^3wx^2yz^3 > 0 \vee$
$-7 + 9w^2xy^3z + 8v^2w^3xz^2 > 0)$

Set a Variable to 0

Example 2

$\forall v, w, x, y, z\ (1 - 10vw^2y - v^3x^3yz^2 - v^3wx^2yz^3 > 0 \vee$
$-7 + 9w^2xy^3z + 8v^2w^3xz^2 > 0)$

- Notice that if we set $w = 0$ in each polynomial, we get $1 - v^3x^3yz^2$ and -7.

Set a Variable to 0

Example 2

$\forall v, w, x, y, z\ (1 - 10vw^2y - v^3x^3yz^2 - v^3wx^2yz^3 > 0 \vee$
$-7 + 9w^2xy^3z + 8v^2w^3xz^2 > 0)$

- Notice that if we set $w = 0$ in each polynomial, we get $1 - v^3x^3yz^2$ and -7.
- Notice that we can find values of v, x, y, and z so that $-7 \leq 0$ and $1 - v^3x^3yz^2 \leq 0$. (E.g. $v = x = y = z = 1$.)

Set a Variable to 0

Example 2

$\forall v, w, x, y, z\ (1 - 10vw^2y - v^3x^3yz^2 - v^3wx^2yz^3 > 0 \vee$
$-7 + 9w^2xy^3z + 8v^2w^3xz^2 > 0)$

- Notice that if we set $w = 0$ in each polynomial, we get $1 - v^3x^3yz^2$ and -7.
- Notice that we can find values of v, x, y, and z so that $-7 \leq 0$ and $1 - v^3x^3yz^2 \leq 0$. (E.g. $v = x = y = z = 1$.)
- Return FALSE with "w is 0, all other variables are 1" as a witness.

Set all Variables Equal

Example 3

$$\forall v, w, x, y, z - 10 - 5v^2w^3y^2z - 10vxyz^3 > 0 \vee$$
$$8 + 2v^3wy^2z + 4v^3x^2z^2 - 4v^2wxy^3z^3 > 0$$

Set all Variables Equal

Example 3

$\forall v, w, x, y, z - 10 - 5v^2w^3y^2z - 10vxyz^3 > 0 \vee$
$8 + 2v^3wy^2z + 4v^3x^2z^2 - 4v^2wxy^3z^3 > 0$

- Notice that the highest degree monomial in the first polynomial is $-5v^2w^3y^2z$ and the highest degree monomial in the second polynomial is $-4v^2wxy^3z^3$.

Set all Variables Equal

Example 3

$\forall v, w, x, y, z - 10 - 5v^2w^3y^2z - 10vxyz^3 > 0 \vee$
$8 + 2v^3wy^2z + 4v^3x^2z^2 - 4v^2wxy^3z^3 > 0$

- Notice that the highest degree monomial in the first polynomial is $-5v^2w^3y^2z$ and the highest degree monomial in the second polynomial is $-4v^2wxy^3z^3$.
- Notice that both have negative real coefficients.

Set all Variables Equal

Example 3

$\forall v, w, x, y, z - 10 -5v^2w^3y^2z - 10vxyz^3 > 0 \vee$
$8 + 2v^3wy^2z + 4v^3x^2z^2 -4v^2wxy^3z^3 > 0$

- Notice that the highest degree monomial in the first polynomial is $-5v^2w^3y^2z$ and the highest degree monomial in the second polynomial is $-4v^2wxy^3z^3$.
- Notice that both have negative real coefficients.
- Return FALSE with "All variables are ∞ (i.e. set all variables equal and sufficiently large)" as a witness.

Analyze Leading Coefficients

Example 4

$$\forall v, w, z, w, y\ (-8 + 8v^2w^3z + 6v^2w^3y^2z - 7vx^3yz^2 > 0 \vee$$
$$-5 - 10v^2w^2x^2 + 7vwx^3yz - 7v^3wxz^2 > 0)$$

Analyze Leading Coefficients

Example 4

$\forall v, w, z, w, y\ (-8 + 8v^2w^3z + 6v^2w^3y^2z - 7vx^3yz^2 > 0 \vee$
$-5 - 10v^2w^2x^2 + 7vwx^3yz - 7v^3wxz^2 > 0)$

- Notice that the leading coefficients of z are $-7vx^3y$ and $-7v^3wx$.

Analyze Leading Coefficients

Example 4

$\forall v, w, z, w, y\ (-8 + 8v^2w^3z + 6v^2w^3y^2z - 7vx^3yz^2 > 0 \vee$
$-5 - 10v^2w^2x^2 + 7vwx^3yz - 7v^3wxz^2 > 0)$

- Notice that the leading coefficients of z are $-7vx^3y$ and $-7v^3wx$.
- Notice that we can find values of v, x, y, and x to make both of these negative. (E.g. $y = x = w = v = 1$.)

Analyze Leading Coefficients

Example 4

$\forall v, w, z, w, y\ (-8 + 8v^2w^3z + 6v^2w^3y^2z - 7vx^3yz^2 > 0 \vee$
$-5 - 10v^2w^2x^2 + 7vwx^3yz - 7v^3wxz^2 > 0)$

- Notice that the leading coefficients of z are $-7vx^3y$ and $-7v^3wx$.
- Notice that we can find values of v, x, y, and x to make both of these negative. (E.g. $y = x = w = v = 1$.)
- Return FALSE with "$z = \infty$, all other variables are 1" as a witness.

Polynomial Properties

- For each of these examples, we have a corresponding theorem.
- We implemented an algorithm for each theorem in Mathematica.

Benchmarks

We tested on several sets of benchmarks.

- 328 decision problems from KeYmaera 3.[2]

[2] Thanks to Stefan Mitsch.

[3] Mulligan et. al. *Quantifier elimination for reasoning in economics*, arXiv preprint (2018)

Benchmarks

We tested on several sets of benchmarks.

- 328 decision problems from KeYmaera 3.[2]
- 44 decision problems from Mulligan et. al.[3]

[2] Thanks to Stefan Mitsch.

[3] Mulligan et. al. *Quantifier elimination for reasoning in economics*, arXiv preprint (2018)

Benchmarks

We tested on several sets of benchmarks.

- 328 decision problems from KeYmaera 3.[2]
- 44 decision problems from Mulligan et. al.[3]
- Decision problems we generate ourselves.

[2] Thanks to Stefan Mitsch.

[3] Mulligan et. al. *Quantifier elimination for reasoning in economics*, arXiv preprint (2018)

Performance

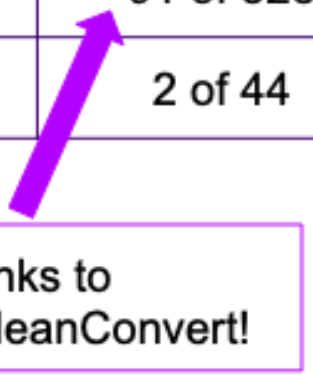
	Avg Runtime	Max Runtime	# decided	# with ==
KeYmaera 3	0.12 s			
Mulligan et. al.	0.35 s			

Performance

	Avg Runtime	Max Runtime	# decided	# with ==
KeYmaera 3	0.12 s	5.32 s		
Mulligan et. al.	0.35 s	5.29 s		

Performance

	Avg Runtime	Max Runtime	# decided	# with ==
KeYmaera 3	0.12 s	5.32 s	91 of 328	
Mulligan et. al.	0.35 s	5.29 s	2 of 44	



Performance

Our algorithms do not apply

	Avg Runtime	Max Runtime	# decided	# with ==
KeYmaera 3	0.12 s	5.32 s	91 of 328	120 of 328
Mulligan et. al.	0.35 s	5.29 s	2 of 44	19 of 44

Performance

- The third set of benchmarks is not fixed.
- Set of polynomials pseudorandomly generated each time our testing method is called.
- Generates many examples which our heuristics very quickly determine are false and on which Mathematica runs slowly.

Performance

In fact, **all of** Examples 1–4 were generated by running our testing method and finding an example where our algorithms return almost instantly but Mathematica stalls.

Conclusion

GOAL: Develop a set of algorithms to improve QE in Mathematica (for the universal fragment of decision procedures)

Exploit algebraic structure

Use properties of polynomials to immediately resolve queries

Encouraging experimental results, can admit witness generation

Conclusion

GOAL: Develop a set of algorithms to improve QE in Mathematica (for the universal fragment of decision procedures)

Exploit algebraic structure

Use properties of polynomials to immediately resolve queries

Encouraging experimental results, can admit witness generation

Use properties of discriminants and resultants to stop CAD in the projection phase

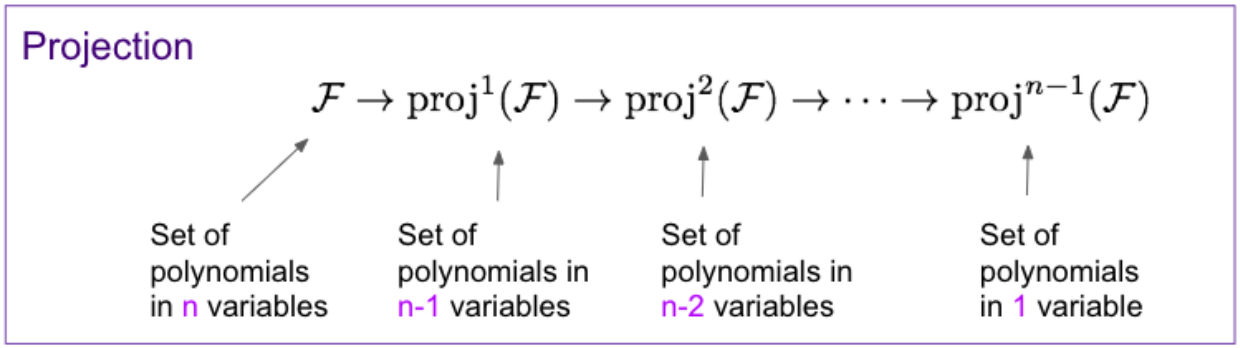
Interesting in theory, but does not seem to generalize easily to the full fragment

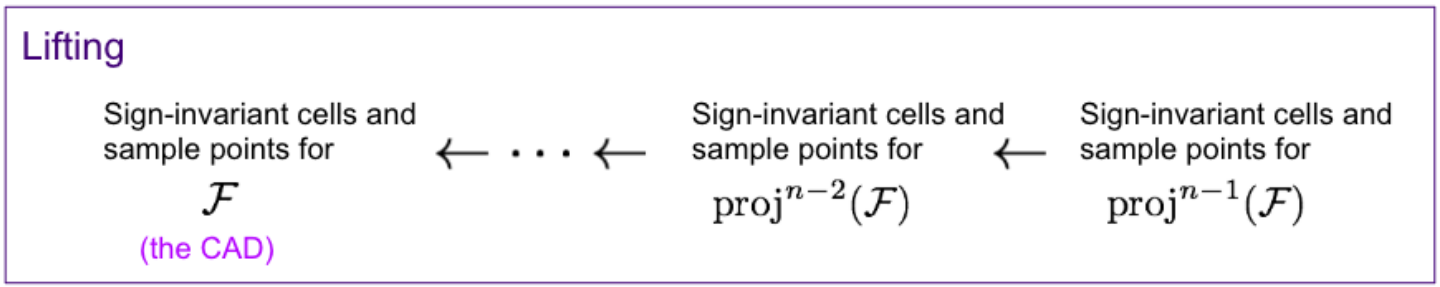
CAD

- Input: A set of polynomials in n variables
- Output: A sign-invariant decomposition of $\mathbb{R}^n$ composed of **cells** and a **sample point** for each cell (called a CAD)
- The signs of the polynomials at the (finitely many) sample points are representative of the signs of the polynomials on the entirety of $\mathbb{R}^n$

CAD

- Two phases: projection and lifting





CAD

- The projection operator is designed so that the projections of different cells are either disjoint or identical
- So if CAD A is lifted from CAD B, the cells in CAD A are cylindrically arranged over the cells in CAD B

[4] Jirstrand, *Algebraic methods for inequality constraints in control*, Ph.D. thesis (1998)

CAD

- The projection operator is designed so that the projections of different cells are either disjoint or identical
- So if CAD A is lifted from CAD B, the cells in CAD A are cylindrically arranged over the cells in CAD B

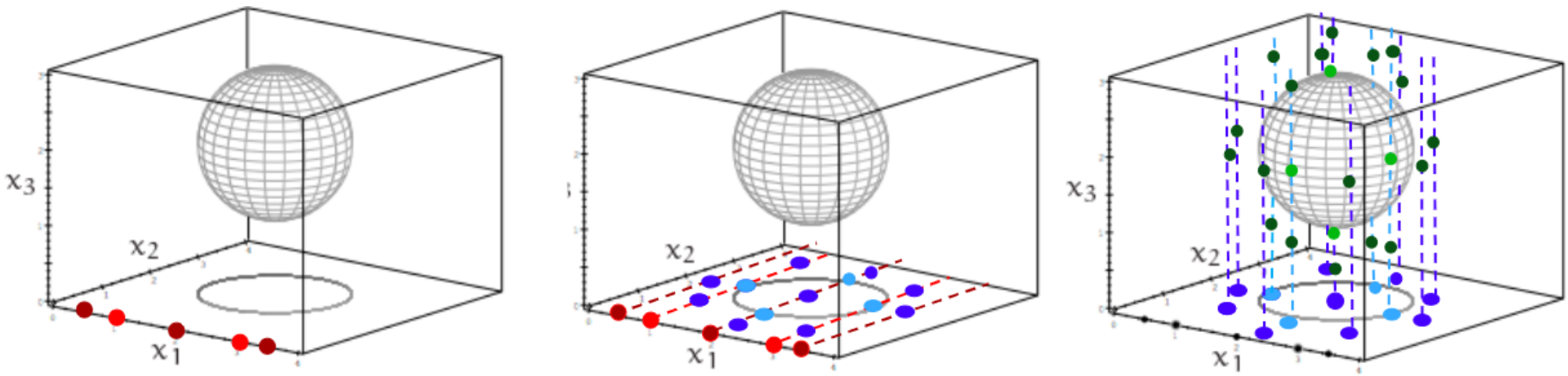


Figure 1: Modified from Jirstrand[4]

[4] Jirstrand, *Algebraic methods for inequality constraints in control*, Ph.D. thesis (1998)

CAD over the years

Many people have worked to improve CAD.

- Brown, McCallum: Improved projection operator
- Collins, Hong: Partial CAD
- McCallum: Full dimensional CAD
- Strzeboński: GCAD

Properties of Discriminants and Resultants

Multiple Zeros of f

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, if $\text{Disc}(f, x_1)(q) = 0$ for some point $q \in \mathbb{R}^{n-1}$ and the leading coefficient of x_1 in f (which is a polynomial in $\mathbb{R}[x_2, \ldots, x_n]$) evaluated at q is nonzero, then the decision problem $\forall x_1, \ldots, x_n \ f(x_1, \ldots, x_n) > 0$ is false.

Common Roots of f and g

Given $f, g \in \mathbb{R}[x_1, \ldots, x_n]$, if there exists a point $q \in \mathbb{R}^{n-1}$ where $\text{Res}(f, g, x_1)(q) = 0$ and the leading coefficients of x_1 in f and g (which are polynomials in $\mathbb{R}[x_2, \ldots, x_n]$) are nonzero when evaluated at q, then the decision problem
$\forall x_1, \ldots, x_n \ (f(x_1, \ldots, x_n) > 0 \vee g(x_1, \ldots, x_n) > 0$ is false.

Properties of Discriminants and Resultants

Discriminant Lemma

Take a polynomial $f = a_{2n}x^{2n} + \cdots + a_0$ with real coefficients and $a_{2n} \neq 0$ (i.e., an even-degree polynomial). If n is even and the discriminant of f is ≤ 0, then f has real roots, and if n is odd and the discriminant of f is ≥ 0, then f has real roots.

Discriminant Algorithm