The Complexity of Quantifier Elimination and Cylindrical Algebraic Decomposition

Christopher W. Brown / U.S. Naval Academy
James H. Davenport / University of Bath

ISSAC 2007
University of Waterloo
1 August 2007

The big picture

The big picture

Our paper is about ...

- a **problem** — real quantifier elimination (QE), and
- a **geometric object** – cylindrical algebraic decomposition (CAD).

The big picture

Our paper is about ...

- a **problem** — real quantifier elimination (QE), and
- a **geometric object** – cylindrical algebraic decomposition (CAD).

It presents proofs ...

- that in the worst case, the problem of real QE is **very hard** $\longleftarrow$ not new
- that in the worst case, CADs are **very big** even for QE problems that are not **very hard** $\longleftarrow$ new!
- that "variable ordering" can make the difference between **very hard** and **very easy** CAD construction problems in some cases, while in others all orderings lead to **very hard** CAD construction problems $\longleftarrow$ new!

Talk Outline

1. Define QE problem

2. Describe result complexity of QE

3. Describe CAD

4. Describe result on complexity (size) of CAD

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?
  - Rabinowitch's trick forces us to allow $\neq$.

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?
  - Rabinowitch's trick forces us to allow $\neq$.
  - Over $\mathbb{R}$ we are similarly forced to allow $\vee$ and $<, >, \leq, \geq$.

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?
  - Rabinowitch's trick forces us to allow $\neq$.
  - Over $\mathbb{R}$ we are similarly forced to allow $\vee$ and $<, >, \leq, \geq$.
- **Satisfiability of parametric Tarski formulas**
  - If F is a Tarski formula in $x_1, \ldots, x_n$,

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?
  - Rabinowitch's trick forces us to allow $\neq$.
  - Over $\mathbb{R}$ we are similarly forced to allow $\vee$ and $<, >, \leq, \geq$.

- **Satisfiability of parametric Tarski formulas**
  - If F is a Tarski formula in $x_1, \ldots, x_n$,
  - where coefficients are polynomials in parameters $s_1, \ldots, s_k$,

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?
  - Rabinowitch's trick forces us to allow $\neq$.
  - Over $\mathbb{R}$ we are similarly forced to allow $\vee$ and $<, >, \leq, \geq$.

- **Satisfiability of parametric Tarski formulas**
  - If F is a Tarski formula in $x_1, \ldots, x_n$,
  - where coefficients are polynomials in parameters $s_1, \ldots, s_k$,
  - then $\exists x_1, \ldots, x_n [F]$ is equivalent to a Tarski formula in $s_1, \ldots, s_k$.

- **Satisfiability of polynomial systems**
  - Is $\exists x_1, \ldots, x_n [P_1 = 0 \wedge \cdots \wedge P_m = 0]$ satisfiable?
  - Rabinowitch's trick forces us to allow $\neq$.
  - Over $\mathbb{R}$ we are similarly forced to allow $\vee$ and $<, >, \leq, \geq$.

- **Satisfiability of parametric Tarski formulas**
  - If F is a Tarski formula in $x_1, \ldots, x_n$,
  - where coefficients are polynomials in parameters $s_1, \ldots, s_k$,
  - then $\exists x_1, \ldots, x_n [F]$ is equivalent to a Tarski formula in $s_1, \ldots, s_k$.

- **Quantifier elimination**
  Given a quantified Tarski formula with parameters, find a Tarski formula defining necessary and sufficient conditions on the parameters for the satisfiability of the input formula.

A Simple Example

Consider the polynomial family $P_s(x,y) = s(x^2+y^2-1)+(1-s)(xy-1)$. For which values of s is the curve $P_s = 0$ bounded?

A Simple Example

Consider the polynomial family $P_s(x, y) = s(x^2 + y^2 - 1) + (1 - s)(xy - 1)$.
For which values of s is the curve $P_s = 0$ bounded?

$$\exists R \forall x, y [P_s(x, y) = 0 \Rightarrow x^2 + y^2 < R^2]$$

A Simple Example

Consider the polynomial family $P_s(x, y) = s(x^2 + y^2 - 1) + (1 - s)(xy - 1)$. For which values of s is the curve $P_s = 0$ bounded?

$$\exists R \forall x, y [P_s(x, y) = 0 \Rightarrow x^2 + y^2 < R^2] \iff s \leq -1 \vee s > 1/3$$

The Complexity of Quantifier Elimination

- Davenport-Heinz (1988)
  - Family of non-linear formulas, n variables, 2 parameters
  - Any equivalent formula has length $\Omega(2^{2^{n/5}})$ assuming dense representation

- Weispfenning (1988) — Based on a construction from Fischer-Rabin (1974)
  - Family of linear formulas in n quantified variables, 1 parameter
  - Any equivalent formula has length $\Omega(2^{2^{n/5}})$ assuming each equality/inequality is linear.

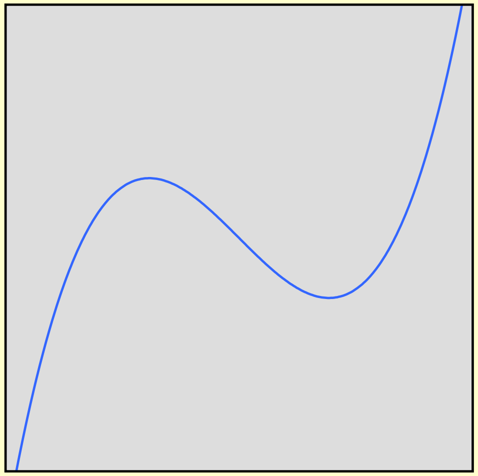
- Our result
  - Family of linear formulas in n quantified variables, 1 parameter
  - Any equivalent formula has length $\Omega(2^{2^{n/3}})$ assuming ...

Cylindrical Algebraic Decomposition (CAD)

- Invented by George Collins in the early 1970s to do QE.
- Defined by a set of polynomials and a variable order.

Cylindrical Algebraic Decomposition (CAD)

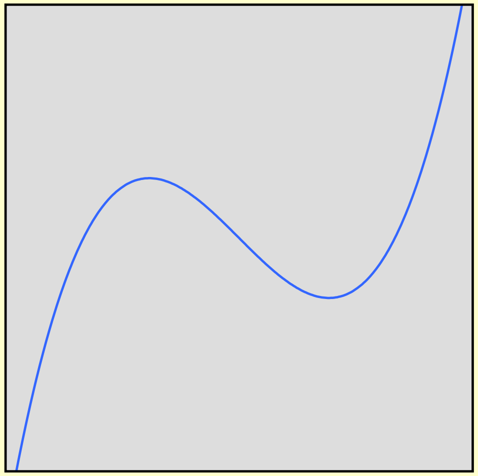
- Invented by George Collins in the early 1970s to do QE.
- Defined by a set of polynomials and a variable order.



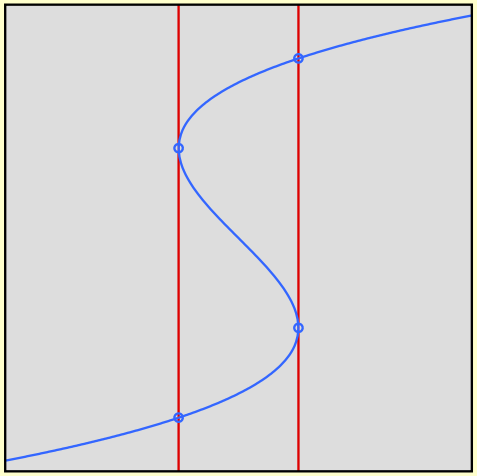
$\{y - x^3 + x\}$, order x, y

Cylindrical Algebraic Decomposition (CAD)

- Invented by George Collins in the early 1970s to do QE.
- Defined by a set of polynomials and a variable order.



$\{y - x^3 + x\}$, order x, y



$\{y - x^3 + x\}$, order y, x

Complexity of CAD

Complexity of CAD

- Worst case is $\Omega\left(2^{2^{n/5}}\right)$, constrained variable order, $\leftarrow$ Davenport-Heintz '88

Complexity of CAD

- Worst case is $\Omega\left(2^{2^{n/5}}\right)$, constrained variable order, $\leftarrow$ Davenport-Heintz '88
- There is a polynomial p_k in $3k+3$ variables such that w.r.t. one variable order there is a CAD of $\mathbb{R}^{3k+3}$ for $\{p_k\}$ consisting of 3 cells, while w.r.t. another order any CAD for $\{p_k\}$ has at least 2^{2^k} cells. $\leftarrow$ new

Complexity of CAD

- Worst case is $\Omega\left(2^{2^{n/5}}\right)$, constrained variable order, $\leftarrow$ Davenport-Heintz '88
- There is a polynomial p_k in $3k+3$ variables such that w.r.t. one variable order there is a CAD of $\mathbb{R}^{3k+3}$ for $\{p_k\}$ consisting of 3 cells, while w.r.t. another order any CAD for $\{p_k\}$ has at least 2^{2^k} cells. $\leftarrow$ new
- There is a set S_k of $(3k^2-k)/2$ linear polynomials in $3k$-variables, each of 2 or 3 terms, such that a CAD of $\mathbb{R}^{3k}$ for S_k has at least 2^{2^k} cells regardless of variable order. $\leftarrow$ new

Complexity of CAD

- Worst case is $\Omega\left(2^{2^{n/5}}\right)$, constrained variable order, $\leftarrow$ Davenport-Heintz '88
- There is a polynomial p_k in $3k+3$ variables such that w.r.t. one variable order there is a CAD of $\mathbb{R}^{3k+3}$ for $\{p_k\}$ consisting of 3 cells, while w.r.t. another order any CAD for $\{p_k\}$ has at least 2^{2^k} cells. $\leftarrow$ new
- There is a set S_k of $(3k^2-k)/2$ linear polynomials in $3k$-variables, each of 2 or 3 terms, such that a CAD of $\mathbb{R}^{3k}$ for S_k has at least 2^{2^k} cells regardless of variable order. $\leftarrow$ new

  Implies worst case is $\Omega\left(2^{2^{\sqrt{2/3n}}}\right)$, unconstrained variable order $\leftarrow$ new

Conclusions

Conclusions

- Quantifier elimination is still hard.

Conclusions

- Quantifier elimination is still hard.
- Variable order in CAD *can be* crucially important.

Conclusions

- Quantifier elimination is still hard.
- Variable order in CAD *can be* crucially important.
- There is a true gap between CAD-based QE and several more modern QE algorithms on QE problems with few alternations.