Formulating Problems in Real Algebra/Geometry

James Davenport
Hebron & Medlock Professor of Information Technology ¹

University of Bath (U.K.)

30 January 2014

¹Thanks to Russell Bradford, Matthew England, David Wilson (Bath); Chris Brown (USNA), Scott McCallum (Macquarie)
Throughout, $Q_i \in \{\exists, \forall\}$. Given

$$\Phi := Q_{k+1}x_{k+1} \ldots Q_nx_n\phi(x_1, \ldots, x_n),$$

where $\phi$ is in some (quantifier-free, generally Boolean-valued) language $L$, produce an equivalent

$$\Psi := \psi(x_1, \ldots, x_k) : \psi \in L$$

In particular, $k = 0$ is a decision problem: is $\Phi$ true?
\[ \forall n : n > 1 \Rightarrow \exists p_1 \exists p_2 \ (p_1 \in P \land p_2 \in P \land 2n = p_1 + p_2) \]

\[ [m \in P \equiv \forall p \forall q \ (m = pq \Rightarrow p = 1 \lor q = 1)] \]

is a statement of Goldbach’s conjecture with, naively, seven quantifiers (five will do)

In fact, quantifier elimination is impossible over \( \mathbb{N} \). [Mat70]

However, it is possible for semi-algebraic (polynomials and inequalities) \( L \) over \( \mathbb{R} \) [Tar51]

Unfortunately, the complexity of Tarski’s method is indescribable
Collins’ method [Col75]

1. Let \( S_n \) be the polynomials in \( \phi \) (\( m \) polynomials, degree \( d \), \( n \) variables)
2. Compute \( S_{n-1} \) (\( \Theta(m^2) \) polys, degree \( \Theta(d^2) \), \( n-1 \) variables)
3. and \( S_{n-2} \) (\( \Theta((m^2)^2) \) polys, degree \( \Theta((d^2)^2) \), \( n-2 \) variables)
   : continue
   \( n \) and \( S_1 \) (\( \Theta(m^{2n-1}) \) polys, degree \( \Theta(d^{2n-1}) \), 1 variable)
4. \( n+1 \) Isolate roots of \( S_1 \)
5. \( n+2 \) Over each root, or interval between roots, isolate roots of \( S_2 \)
   : continue
6. \( 2n \) \( S_n \) has invariant signs on each region of \( \mathbb{R}^n \), so \( \phi(x_1, \ldots, x_n) \) has invariant truth on each region
7. \( 2n + 1 \) So evaluate truth of \( \Phi \) on each region of \( (x_1, \ldots, x_k) \)-space

Clearly complexity \( (md)^{2O(n)} \): in fact \( O \left( (2m)^{2^{2n+8}} d^{2^{n+6}} \right) \) [Col75]
Well, at least that’s describable, even if worrying

A better analysis of step $n + 1$ [Dav85] gives $O \left( (2k)^{2^{n+8/6}} d^{2^{n+64}} \right)$

which doesn’t look very impressive until you realise it’s $Z^4 \rightarrow Z$

In fact, it largely affects the analysis, not the actual running time

[DH88] showed QE is $\Omega \left( 2^{2^{(n-2)/6}} \right)$, or (harder) $\Omega \left( 2^{2^{(n-2)/5}} \right)$

(at least in the dense model, i.e. storing all $d + 1$ coefficients of a polynomial of degree $d$).

So we’re in $\left( 2^{2^{\Theta(n)}} \right)$-land:

doesn’t look very impressive until you realise it’s $Z^4 \rightarrow Z$

In fact, it largely affects the analysis, not the actual running time

[DH88] showed QE is $\Omega \left( 2^{2^{(n-2)/6}} \right)$, or (harder) $\Omega \left( 2^{2^{(n-2)/5}} \right)$

(at least in the dense model, i.e. storing all $d + 1$ coefficients of a polynomial of degree $d$).

So we’re in $\left( 2^{2^{\Theta(n)}} \right)$-land:

doesn’t look very impressive until you realise it’s $Z^4 \rightarrow Z$

In fact, it largely affects the analysis, not the actual running time

[DH88] showed QE is $\Omega \left( 2^{2^{(n-2)/6}} \right)$, or (harder) $\Omega \left( 2^{2^{(n-2)/5}} \right)$

(at least in the dense model, i.e. storing all $d + 1$ coefficients of a polynomial of degree $d$).

So we’re in $\left( 2^{2^{\Theta(n)}} \right)$-land:

doesn’t look very impressive until you realise it’s $Z^4 \rightarrow Z$
More lower bounds [BD07]

The key idea [Hei83]: suppose \( \Phi_n \) is \( y_n = f_n(x_n) \). Then

\[
\Phi_{n+1}(x_{n+1}, y_{n+1}) := \exists z_n \forall x_n \forall y_n \\
[(y_n = y_{n+1} \land x_n = z_{n+1}) \lor (y_n = z_{n+1} \land x_n = x_{n+1})] \Rightarrow \Phi_n(x_n, y_n)
\]

is \( y_{n+1} = f_n(f_n(x_{n+1})) \). Apply this to

\[
f_0(x_0) = \begin{cases} 
2x & x \leq 1/2 \\
2 - 2x & x > 1/2 
\end{cases}
\]

Then \( \Phi_n(x_n, \frac{1}{2}) \) defines a set with \( 2^{2^n} \) isolated points. [BD07] shows this set needs doubly exponential space to encode, in dense, sparse or factored form.
The Heintz construction of [BD07] is $\exists \forall \exists \forall \exists \forall \ldots \exists \forall$, with two alternations of quantifiers for every three quantifiers. Let $a$ be the number of alternations. Then [FGM90] the (sequential) cost is $(md)^{n^{O(a)}}$. The doubly-exponential nature is really only for the number of alternations, and it’s singly-exponential for the number of variables. I know of no implementation of this method. But it means that cylindrical algebraic decomposition is not always (asymptotically!) best.
Consider the polynomial [BD07, Theorem 7]
\[
\left(\left(\frac{y_{n-1}}{2} + z_{n-1}\right)^2 + \left(x_{n-1} - z_n\right)^2\right) \left(\left(y_{n-1} - z_n\right)^2 + \left(x_{n-1} - x_n\right)^2\right) x^{n+1} \\
+ \sum_{i=1}^{n-1} \left(\left(y_{i-1} - y_i\right)^2 + \left(x_{i-1} - z_i\right)^2\right) \left(\left(y_{i-1} - z_i\right)^2 + \left(x_{i-1} - x_i\right)^2\right) x^{i+1} \\
+ \left(\hat{y}_0 - 2\hat{x}_0\right)^2 + \left(\hat{\alpha}^2 + \left(\hat{x}_0 - \frac{1}{2}\right)^2\right) \times \\
\left(\hat{y}_0 - 2 + 2\hat{x}_0\right)^2 + \left(\hat{\alpha}^2 - \left(\hat{x}_0 - \frac{1}{2}\right)^2\right) x + a
\]

Eliminating \(a, x_n, z_n, x_{n-1}, y_{n-1}, z_{n-1}, \ldots, z_1, x_0, \alpha, y_0, \hat{x}\) gives a CAD (in fact a polynomial in \(a\)) with at least \(2^{2^n}\) cells, whereas the opposite order has three cells.
Conversely [BD07, Theorem 8] there are problems that are doubly exponential for all orders.
If we can choose the order, how?

Various heuristics:

- **sotd** For all $n!$ orders, perform steps 1-$n$, measure sotd (sum of total degrees) and do $n+1, \ldots$ for the least

- **Greedy sotd** [DSS04] Do step 1 for each variable, choose the best (sotd) and repeat: often ties

- **ndrr** [BDEW13] For all $n!$ orders, perform steps 1-$n$, count number of distinct real roots

- **Brown** [Bro04, 5.2] Eliminate lowest degree variable first (with tie-breaking rules): quite effective

- **Machine Learning** metaheuristic: very preliminary results from Zongyan Huang (Cambridge) are encouraging
Lazard’s quartic: \( \forall x : px^2 + qx + r + x^4 \geq 0 \)
6 possible orders for \((p, q, r)\)

<table>
<thead>
<tr>
<th>order</th>
<th>sotd</th>
<th>#cells</th>
<th>CAD</th>
<th>#true</th>
<th>QE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>54</td>
<td>445</td>
<td>4.71</td>
<td>251</td>
<td>7.04</td>
</tr>
<tr>
<td>2</td>
<td>54</td>
<td>445</td>
<td>83.39</td>
<td>251</td>
<td>138.18</td>
</tr>
<tr>
<td>3</td>
<td>50</td>
<td>417</td>
<td>0.54</td>
<td>235</td>
<td>0.89</td>
</tr>
<tr>
<td>4</td>
<td>50</td>
<td>417</td>
<td>1.64</td>
<td>239</td>
<td>2.55</td>
</tr>
<tr>
<td>5</td>
<td>66</td>
<td>—</td>
<td>&gt;600</td>
<td>—</td>
<td>&gt;600</td>
</tr>
<tr>
<td>6</td>
<td>66</td>
<td>—</td>
<td>&gt;600</td>
<td>—</td>
<td>&gt;600</td>
</tr>
</tbody>
</table>
If $\phi$ is $f = 0 \land \hat{\phi}$, we need only consider the cells when $f = 0$ is true. This means the first projection step produces $O(m)$ polynomials rather than $O(m^2)$, and the complexity is $O \left( (2m)^{2n+6} d^{2n+6} \right)$.

This gives an interesting formulation problem: given

$$(f_1 = 0 \land g_1 < 0) \lor (f_2 = 0 \land g_2 < 0)$$

we are better off solving the equivalent

$$f_1 f_2 = 0 \land [(f_1 = 0 \land g_1 < 0) \lor (f_2 = 0 \land g_2 < 0)]$$

even though the degree goes up: $O \left( (2m)^{2n+6} d^{2n+6} \right)$

[There is a technical side-condition well-orientedness]
In

\[(f_1 = 0 \land g_1 < 0) \lor (f_2 = 0 \land g_2 < 0)\]  \hspace{1cm} (3)

during the first projection set need only be Disc\((f_1)\), Disc\((f_2)\), Res\((f_1, f_2)\), Res\((f_1, g_1)\), Res\((f_2, g_2)\) (and omits Disc\((g_1)\), Disc\((g_2)\), Res\((g_1, g_2)\), Res\((f_1, g_2)\), Res\((f_1, g_2)\)). Essentially all the advantages of

equational constraints.

There is still the technical side-condition well-orientedness,

removed (with many other improvements) in [BCD\(^+\)14]

There are still issues of formulation: e.g. in

\[(f_1 = 0 \land f_2 = 0 \land g_1 < 0) \lor \ldots, \text{ which equation do we prefer?}\]
<table>
<thead>
<tr>
<th>Cells</th>
<th>Time</th>
<th>S</th>
<th>N</th>
<th>Cells</th>
<th>Time</th>
<th>S</th>
<th>N</th>
<th>Cells</th>
<th>Time</th>
<th>S</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>657</td>
<td>5.6</td>
<td>61</td>
<td>7</td>
<td>463</td>
<td>5.1</td>
<td>64</td>
<td>8</td>
<td>269</td>
<td>1.3</td>
<td>42</td>
<td>4</td>
</tr>
<tr>
<td>463</td>
<td>5.1</td>
<td>64</td>
<td>8</td>
<td>471</td>
<td>5.4</td>
<td>71</td>
<td>6</td>
<td>303</td>
<td>1.1</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>435</td>
<td>3.6</td>
<td>73</td>
<td>8</td>
<td>303</td>
<td>1.1</td>
<td>40</td>
<td>5</td>
<td>425</td>
<td>2.8</td>
<td>80</td>
<td>8</td>
</tr>
<tr>
<td>375</td>
<td>2.7</td>
<td>81</td>
<td>9</td>
<td>1295</td>
<td>21.4</td>
<td>140</td>
<td>13</td>
<td>1437</td>
<td>23.9</td>
<td>158</td>
<td>14</td>
</tr>
<tr>
<td>1295</td>
<td>21.4</td>
<td>140</td>
<td>13</td>
<td>477</td>
<td>3.8</td>
<td>84</td>
<td>9</td>
<td>1437</td>
<td>23.9</td>
<td>158</td>
<td>14</td>
</tr>
<tr>
<td>285</td>
<td>2.0</td>
<td>61</td>
<td>7</td>
<td>169</td>
<td>1.0</td>
<td>59</td>
<td>5</td>
<td>117</td>
<td>0.7</td>
<td>35</td>
<td>3</td>
</tr>
<tr>
<td>39</td>
<td>0.1</td>
<td>54</td>
<td>5</td>
<td>9</td>
<td>0.0</td>
<td>47</td>
<td>1</td>
<td>39</td>
<td>0.1</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>F</td>
<td>-</td>
<td>14</td>
<td>0</td>
<td>F</td>
<td>-</td>
<td>14</td>
<td>0</td>
<td>27</td>
<td>0.1</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>57</td>
<td>0.3</td>
<td>32</td>
<td>3</td>
<td>117</td>
<td>0.7</td>
<td>35</td>
<td>3</td>
<td>119</td>
<td>0.6</td>
<td>36</td>
<td>4</td>
</tr>
</tbody>
</table>

**Table:** Comparing the choice of equational constraint for a selection of problems. The lowest cell count for each problem is highlighted and the minimal values of the heuristics emboldened.
We assume $x \prec y$ and consider $\{\phi_1, \phi_2\}$:

\[
\begin{align*}
    f_1 & := x^2 + y^2 - 1, \quad h := y^2 - \frac{x}{2}, \quad g_1 := xy - \frac{1}{4} \\
    f_2 & := (x - 4)^2 + (y - 1)^2 - 1 \quad g_2 := (x - 4)(y - 1) - \frac{1}{4}, \\
    \phi_1 & := h = 0 \land f_1 = 0 \land g_1 < 0, \quad \phi_2 := f_2 = 0 \land g_2 < 0. \quad (1)
\end{align*}
\]
RC-TTICAD with $f_1 \rightarrow h \rightarrow f_2$ (57 cells).
RC-TTICAD with $h \rightarrow f_1 \rightarrow f_2$ (75 cells). This is the default and the same as with $f_2, h, f_1$. 
RC-TTICAD with $f_2 \rightarrow f_1 \rightarrow h$ (77 cells).
PL-TTICAD with $f_1$ identified (117 cells).
RC-TTICAD with $h$ identified (163 cells).
Gröbner Reduction as well [BDEW13]

<table>
<thead>
<tr>
<th>Order</th>
<th>Full CAD</th>
<th>TTI CAD</th>
<th>TTI+Grö CAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Eq Const</td>
<td>Cells</td>
<td>Time</td>
</tr>
<tr>
<td>y ≺ x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f₁,₁, f₂,₁</td>
<td>153</td>
<td>0.818</td>
</tr>
<tr>
<td></td>
<td>f₁,₁, f₂,₂</td>
<td>111</td>
<td>0.752</td>
</tr>
<tr>
<td></td>
<td>f₁,₂, f₂,₁</td>
<td>121</td>
<td>0.732</td>
</tr>
<tr>
<td></td>
<td>f₁,₂, f₂,₂</td>
<td>75</td>
<td>0.840</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x ≺ y</td>
<td>f₁,₁, f₂,₁</td>
<td>125</td>
<td>0.676</td>
</tr>
<tr>
<td></td>
<td>f₁,₁, f₂,₂</td>
<td>117</td>
<td>0.792</td>
</tr>
<tr>
<td></td>
<td>f₁,₂, f₂,₁</td>
<td>117</td>
<td>0.728</td>
</tr>
<tr>
<td></td>
<td>f₁,₂, f₂,₂</td>
<td>85</td>
<td>0.650</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Experimental results relating to Example 7. The lowest cell counts are highlighted.
Reduces to CAD [SS83]. But can we move ladder 1 to position 2?

Insoluble in 1986 [Dav86], insoluble today by [SS83, and today’s hardware and CAD advances]
A different formulation [WBDE13]

Figure: Four canonical invalid positions of the ladder. Note from the algebraic descriptions that for positions A–C only one end need be outside the corridor.

\[ \text{length} \wedge \neg (A \lor B \lor C \lor D) : \text{Soluble (5 hours CPU, 285419 cells)} \]
The solution:

\[
x \leq 0 \land y \geq 0 \land w \leq 0 \land z \geq 0 \land (y - z)^2 + (x - w)^2 = 9
\land \left[ x + 1 \geq 0 \land w + 1 \geq 0 \right] \lor \left[ y - 1 \leq 0 \land w + 1 \geq 0 \right]
\land y^2w^2 - 2yw^2 + x^2w^2 + 2xw^2 + 2w^2 - 2xy^2w
\quad + 4xyw - 2x^3w - 4x^2w - 4xw + x^2y^2 - 2x^2y
\quad + x^4 + 2x^3 - 7x^2 - 18x - 9 \geq 0
\lor \left[ x + 1 \geq 0 \land yw - w + y + x \geq 0 \land w^2 - 2xw + y^2
\quad - 2y + x^2 - 8 > 0 \land z - 1 \leq 0 \right] \lor \left[ x + 1 \geq 0 \land yw - w + y + x \geq 0 \land y^2w^2 - 2yw^2
\quad + x^2w^2 + 2xw^2 + 2w^2 - 2xy^2w + 4xyw - 2x^3w
\quad - 4x^2w - 4xw + x^2y^2 - 2x^2y + x^4 + 2x^3 - 7x^2
\quad - 18x - 9 \leq 0 \land z - 1 \leq 0 \right]
\lor \left[ y - 1 \leq 0 \land z - 1 \leq 0 \right].
\]
The more I learn, the less I know, but

- There’s more than one way to state a problem
- Clearly equivalent in terms of **decidability**, but not **practical computability**
- The differences are vast in practice
- We have some reasonable heuristics
- But much more work needs to be done, theoretically, experimentally, and on the “software packaging” side
- We need practical work on alternative methods for quantifier elimination
Truth Table Invariant Cylindrical Algebraic Decomposition by Regular Chains.

The Complexity of Quantifier Elimination and Cylindrical Algebraic Decomposition.
Cylindrical Algebraic Decompositions for Boolean Combinations.

Optimising Problem Formulation for Cylindrical Algebraic Decomposition.

C.W. Brown.
Tutorial handout.
G.E. Collins.
Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.

J.H. Davenport.
Computer Algebra for Cylindrical Algebraic Decomposition.

J.H. Davenport.
On a ”Piano Movers” Problem.
J.H. Davenport and J. Heintz.
Real Quantifier Elimination is Doubly Exponential.

A. Dolzmann, A. Seidl, and Th. Sturm.
Efficient Projection Orders for CAD.

N. Fitchas, A. Galligo, and J. Morgenstern.
Precise sequential and parallel complexity bounds for the quantifier elimination over algebraic closed fields.
J. Heintz.
Definability and Fast Quantifier Elimination in Algebraically Closed Fields.

Yu.V. Matiyasevich.
Enumerable sets are Diophantine.

S. McCallum.
On Projection in CAD-Based Quantifier Elimination with Equational Constraints.
J.T. Schwartz and M. Sharir.


A. Tarski.
*A Decision Method for Elementary Algebra and Geometry.*

A "Piano Movers" Problem Reformulated.
http://opus.bath.ac.uk/36795/, 2013.