ISSAC’04

Tutorial

Cylindrical Algebraic Decomposition

Christopher W. Brown
U.S. Naval Academy
http://www.cs.usna.edu/~wcbrown

Work supported in part by the National Science Foundation grant CCR-0306440.
Preface

Goal: To compute symbolically with semi-algebraic sets in practice.

Definition: The semi-algebraic sets in $\mathbb{R}^n$ are defined recursively by:

1. the set of points satisfying $p \sigma 0$, where $p \in \mathbb{R}[x_1, \ldots, x_n]$ and $\sigma \in \{=, \neq, <, \leq, >, \geq\}$, is semi-algebraic

2. the complement of a semi-algebraic set, and the union or intersection of finitely many semi-algebraic sets are semi-algebraic.
Preface

Semi-algebraic sets are usually represented by Tarski Formulas.

Definition: A Tarski Formula is boolean combination of polynomial equalities and inequalities.

Tarski formulas map directly to the definition of semi-algebraic sets:

\[ x_1 \neq 0 \land x_2^2 - 4x_1x_3 > 0 \quad \rightarrow \quad x_1 \neq 0 \land x_2^2 - 4x_1x_3 > 0 \]

\[ x_1^2 + x_2^2 - 1 \leq 0 \quad \Rightarrow \quad x_1 + x_2 \geq 0 \quad \rightarrow \quad \overline{x_1^2 + x_2^2 - 1 \leq 0} \cup x_1 + x_2 \geq 0 \]

So we may view semi-algebraic sets from the standpoint of geometry or of logic. One viewpoint: the objects are geometric, the representations are logical.
Introduction

What is “Cylindrical Algebraic Decomposition”? 

*Cylindrical Algebraic Decomposition* (CAD) provides an *explicit* representation for semi-algebraic sets, in which many operations and queries can be carried out easily.
Tutorial Outline

• Motivate

• Develop intuition

• Present CAD fundamentals more rigorously

• Present what you need to use and adapt CAD effectively

• Analyze some case studies
Problems

1. An application from epidemiology

2. Triangles and Euclidean geometry

3. The role of Rolle’s theorem
An Epidemiological Problem

• Andreas Weber and colleagues have applied symbolic tools to epidemiological models.

• We consider the SEIT model, used to model tuberculosis in van den Driessche & Watmough, 2002.

• Uses system of ODEs to model movement of disease through population. Model contains many parameters.

• Question: For what parameters is there an endemic equilibrium, i.e. an equilibrium that doesn’t have the disease dying out.
An Epidemiological Model

\[ S' = d - dS - \beta_1 IS \]
\[ E' = \beta_1 IS + \beta_2 IT - (d + \nu + r_1)E + (1 - q)r_2I \]
\[ I' = \nu E - (d + r_2)I \]
\[ T' = -dT + r_1 E + qr_2 I - \beta_2 TI \]

\textbf{S} susceptibles \hspace{2cm} \beta_1, \beta_2 \text{ transmission parameters for } S \text{ and } T
\textbf{E} exposed (not yet infectious) \hspace{2cm} d \text{ birth and death rate (assumed equal)}
\textbf{I} infectious \hspace{2cm} \nu \text{ rate of change from exposed to infectious}
\textbf{T} under treatment \hspace{2cm} r_1, r_2 \text{ treatment rates for } E \text{ and } I
\text{} \hspace{2cm} q \text{ fraction of infectious successfully treated}
Endemic equilibrium

• an endemic equilibrium satisfies $0 = S', E', I', T'$ and $0 < S, E, I, T$

• for what parameter values is there a solution satisfying $0 < S, E, I, T$ for:

\[
\begin{align*}
0 &= d - dS - \beta_1 IS \\
0 &= \beta_1 IS + \beta_2 IT - (d + \nu + r_1)E + (1 - q)r_2 I \\
0 &= \nu E - (d + r_2)I \\
0 &= -dT + r_1 E + qr_2 I - \beta_2 TI
\end{align*}
\]

assuming all parameters positive?
**Endemic equilibrium problem**

- It’s easy to solve for $E, I$ and $T$ in terms of $S$ three of the equations. Substituting the results into the fourth gives $P = 0$, where

$$P = -\nu S^2 \beta_1^2 + \beta_1 \nu S^2 \beta_2 + d\beta_1 Sr_2 - d^2 \beta_2 S + d^2 \beta_1 S + \beta_1 Sr_1 r_2 - d\nu S\beta_2$$

$$+ \nu\beta_1 Sqr_2 - d\beta_2 r_2 S + d\nu S\beta_1 - \beta_1 S\nu\beta_2 + \beta_1 Sr_1 d + \beta_2 d^2 + \nu\beta_2 d + \beta_2 dr_2$$

- The condition $0 < S, E, I, T$ is easily seen to be equivalent to $0 < S < 1$.

- So there is an endemic equilibrium for any assignment of positive parameter values for which there is a a real value $S$ such that $P(S) = 0 \land 0 < S < 1$, i.e.

$$\exists S \ [P(S) = 0 \land 0 < S < 1]$$
Given triangle $ABC$, consider the “external trisector of $B$ with respect to $A$” as defined in the figure.

Clearly, the trisectors exist if and only if $(\pi - \phi)/3 < \theta$.

**Problem:** Characterize the existence of the external trisector of $B$ with respect to $A$ in terms of the side lengths $a, b, c$. 
Converting from angles to side lengths

Using standard trig identities we see that $(\pi - \phi)/3 < \theta$ is equivalent to

\[
\cos \theta \leq \cos \frac{\pi}{3} \lor \cos \theta > \cos \frac{\pi}{3} \land \cos \phi < -4 \cos^3 \theta + 3 \cos \theta
\]

Using the law of cosines to describe $\cos \theta$ and $\cos \phi$ in terms of the side lengths $a$, $b$ and $c$, and clearing denominators, we get

\[
a^2 + b^2 - c^2 < ab \lor a^2 + b^2 - c^2 \geq ab \land -c \left(a^2 + b^2 - c^2\right)^3 + 3a^2b^2c \left(a^2 + b^2 - c^2\right)
\]
The External Trisector Problem

In the triangle with side lengths $a, b, c$, the external trisector of $B$ w.r.t. $A$ exists if and only if:

$$a^2 + b^2 - c^2 < ab \lor a^2 + b^2 - c^2 \geq ab \land -c \left(a^2 + b^2 - c^2\right)^3 + 3a^2b^2c\left(a^2 + b^2 - c^2\right)$$

**Problem:** Is there a simpler characterization?
Rolle’s Theorem


• Rolle’s theorem: between any two zeros of $f(x)$ there is a zero of $f'(x)$.

• Generically: from $x = -\infty$ to $x = +\infty$ the signs of $f$ and $f'$ can be

\[
\begin{array}{c}
 f \\
 f' \end{array} \begin{array}{c}
 + \\
 - \\
 + \\
 + \\
 \ldots \\
 - \\
 + \\
 - \\
 - \\
 \ldots \\
 \end{array}
\]

but cannot be

\[
\begin{array}{c}
 f \\
 f' \end{array} \begin{array}{c}
 + \\
 - \\
 - \\
 + \\
 - \\
 - \\
 - \\
 \ldots \\
 \end{array}
\]

according to Rolle’s theorem.
Sequence of “Sign-Stacks”
Sign-stack sequence restrictions

Consider the sign-stack sequence of a generic, monic, univariate polynomial.

1. *monic* implies: the bottom entry is always +, the first sign-stack is alternating +’s and −’s, and the last sign-stack is all +’s

2. *generic* implies: consecutive sign-stacks differ in only one entry

3. *Rolle’s theorem* implies: from one sign-sequence to the next, an entry may only be changed to equal the entry below it

A sequence satisfying these requirements is called *legal*. 
Problem: is every legal sign-stack sequence realizable by a polynomial?

There are lots of legal sign-stack sequences!

<table>
<thead>
<tr>
<th>degree of $f$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td># legal sequences</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>42</td>
<td>1000</td>
<td>114650</td>
<td>77740200</td>
</tr>
</tbody>
</table>
Questions?