FASTER REAL FEASIBILITY AND DISCRIMINANT COMPLEXITY

*Partially supported by NSF CAREER grant DMS-0349309.
Can one compute, in time polynomial in the \textit{sparse} size, an integer that is, with high probability, the number of connected components of the real zero set of a random input polynomial?
MAIN QUESTION

Can one compute, in time polynomial in the \textit{sparse} size, an integer that is, with high probability, the number of connected components of the real zero set of a random input polynomial?

We take a step toward a positive answer through our results...
WARM-UP...

Suppose you want to find the exact number of positive roots of

\[ 1 - 2x^{196418} + x^{317811} \ldots \]
THE RIGHT TOOL?

Suppose you want to find the exact number of positive roots of

\[ 1 - 2x^{196418} + x^{317811} \ldots \]

Let’s compare

Sturms Sequences and Discriminant Chambers...
$f_0 := 1 - 2x^{196418} + x^{317811}$
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]

\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := -\text{rem}(f_0/f_1) = -317811 + 242786x^{196418} \]

©J. Maurice Rojas
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := \text{rem}(f_0/f_1) = -317811 + 242786x^{196418} \]
\[ f_3 := \text{rem}(f_1/f_2) = -101003831721x^{121392} + 95375081096x^{196417} \]
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := -\text{rem}(f_0 / f_1) = -317811 + 242786x^{196418} \]
\[ f_3 := -\text{rem}(f_1 / f_2) = -101003831721x^{121392} + 95375081096x^{196417} \]
\[ \vdots \]
\[ f_{26} := [674206 \text{ digit number}] + [674209 \text{ digit number}]x^{610} \]
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := -\text{rem}(f_0/f_1) = -317811 + 242786x^{196418} \]
\[ f_3 := -\text{rem}(f_1/f_2) = -101003831721x^{121392} + 95375081096x^{196417} \]
\[ \vdots \]
\[ f_{26} := \left[674206\text{ digit number}\right] + \left[674209\text{ digit number}\right]x^{610} \]
\[ \vdots \]
\[ f_{37} := \text{Out of Memory Error!} \]
\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := -\text{rem}(f_0/f_1) = -317811 + 242786x^{196418} \]
\[ f_3 := -\text{rem}(f_1/f_2) = -101003831721x^{121392} + 95375081096x^{196417} \]
\[ \vdots \]
\[ f_{26} := [674206 \ \text{digit number}] + [674209 \ \text{digit number}]x^{610} \]
\[ \vdots \]
\[ f_{37} := \text{Out of Memory Error!} \]
\[ \vdots \]
\[ f_{58} := 0 \]
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := -\text{rem}(f_0/f_1) = -317811 + 242786x^{196418} \]
\[ f_3 := -\text{rem}(f_1/f_2) = -101003831721x^{121392} + 95375081096x^{196417} \]

\[ f_26 := [674206 \text{ digit number}] + [674209 \text{ digit number}]x^{610} \]
\[ f_{37} := \text{Out of Memory Error!} \]
\[ f_{58} := 0 \]

...now count sign alternations in \((f_0(t), f_1(t), \ldots, f_{57}(t))\) for \(t=0\) and \(t=+\infty\), and then subtract. (Should get 2 here.)
STURM SEQUENCES...

\[ f_0 := 1 - 2x^{196418} + x^{317811} \]
\[ f_1 := f'_0 = -392836x^{196417} + 317811x^{317810} \]
\[ f_2 := -\text{rem}(f_0/f_1) = -317811 + 242786x^{196418} \]
\[ f_3 := -\text{rem}(f_1/f_2) = -101003831721x^{121392} + 95375081096x^{196417} \]
\[ \vdots \]
\[ f_{26} := [674206 \text{ digit number}] + [674209 \text{ digit number}]x^{610} \]
\[ \vdots \]
\[ f_{37} := \text{Out of Memory Error!} \]
\[ \vdots \]
\[ f_{58} := 0 \]

Can we attain complexity polynomial in \( \log(\text{degree}) \)?

©J. Maurice Rojas
YES!
THEOREM 1

[Bihan-Rojas-Stella] Fix $n$. Then for any “honest” $n$-variate $(n + 2)$-nomial $f$, one can decide $Z_+(f) \neq \emptyset$ in $\mathbb{P}$. 
THEOREM 1

[Bihan-Rojas-Stella] Fix $n$. Then for any “honest” $n$-variate $(n + 2)$-nomial $f$, one can decide $Z_+(f) = \emptyset$ in $P$.

Note:
Input size: $\#$ of bits needed to write monomial term expansion.
e.g., $\text{Size}(a + b + c x_1^D x_2^D) = O(\log(a) + \log(b) + \log(c) + \log(D))$
[Bihan-Rojas-Stella] Fix $n$. Then for any “honest” $n$-variate $(n + 2)$-nomial $f$, one can decide $Z_+(f) \neq \emptyset$ in $\text{P}$.

**Note:** All earlier algorithms (even much more general results of Basu, Gabrielov, and Zell) yield singly exponential time at best.
KEY TRICK FOR $n = 1$

Look at the graph of

$$f(x_1) := 1 - cx_1^d + x_1^D \quad (0 < d < D)$$...
KEY TRICK FOR $n = 1$

Look at the graph of

$$f(x_1) := 1 - cx_1^d + x_1^D \quad (0 < d < D)$$

$c > 0$ small

$c > 0$ BIG
Look at the graph of

\[ f(x_1) := 1 - cx_1^d + x_1^D \quad (0 < d < D) \]

\(f = f' = 0\) has a root \(\zeta \in \mathbb{C} \setminus \{0\} \iff [1, c\zeta^d, \zeta^D]^T\) is a right-null vector for

\[
\begin{bmatrix}
1 & 1 & 1 \\
0 & d & D
\end{bmatrix}
\]
Look at the graph of
\[ f(x_1) := 1 - cx_1^d + x_1^D \quad (0 < d < D) \]

\[ f = f' = 0 \text{ has a root } \zeta \in \mathbb{C} \setminus \{0\} \iff \Delta_{\{0,d,D\}}(f) := \left( \frac{1}{D-d} \right)^{D-d} \left( \frac{-c}{-D} \right)^{-D} \left( \frac{1}{d} \right)^d - 1 \text{ vanishes!} \]
We call any connected component of the complement of
\[
\{c \in \mathbb{R} \setminus \{0\} \mid \bar{\Delta}_{\{0,d,D\}}(c) = 0\}
\]
a (reduced) discriminant chamber.

\[
c = \frac{317811}{196418^{196418/317811}121393^{121393/317811}} \approx 1.944526275\ldots
\]
$b^2 - 4ac \text{ ON STEROIDS}$

So you can decide whether

$$1 - cx^{196418} + x^{317811}$$

has 0, 1, or 2 positive roots, just by checking whether

$$196418^{196418}121393^{121393}c^{317811} - 317811^{317811}$$

is $<0$, $=0$, or $>0$...
So you can decide whether

\[ 1 - cx^{196418} + x^{317811} \]

has 0, 1, or 2 positive roots, just by checking whether

\[ 196418^{196418} 121393^{121393} c^{317811} - 317811^{317811} \]

is < 0, = 0, or > 0.

...and the preceding condition = checking the sign of

\[ 196418 \log(196418) + 121393 \log(121393) + 317811 \log(c) - 317811 \log(317811). \]
DIOPHANTINE SIDE

So you can decide whether

$$1 - cx^{196418} + x^{317811}$$

has 0, 1, or 2 positive roots, just by checking whether

$$196418^{196418} 121393^{121393} c^{317811} - 317811^{317811}$$

is < 0, = 0, or > 0.

...and the preceding condition = checking the sign of

$$196418 \log(196418) + 121393 \log(121393) + 317811 \log(c) - 317811 \log(317811),$$

which can be done in polynomial time via Baker’s Theorem on Linear Forms in Logarithms!
So you can decide whether

\[ 1 - cx^{196418} + x^{317811} \]

has 0, 1, or 2 positive roots, just by checking whether

\[ 196418^{196418} 121393^{121393} c^{317811} - 317811^{317811} \]

is < 0, = 0, or > 0.

...and the preceding condition = checking the sign of

\[ 196418 \log(196418) + 121393 \log(121393) + 317811 \log(c) - 317811 \log(317811), \]

which can be done in polynomial time via Baker’s Theorem on Linear Forms in Logarithms!

...and, availing to Morse Theory, this generalizes to arbitrary \( n \)...
TRIVARIATE EXAMPLE

Consider

\[ c_1 + c_2 x_1^{999} + c_3 x_1^{73} x_3 + c_4 x_2^{2009} + c_5 x_1^{2009} x_2^{6027} x_3^{18081} \ldots \]
TRIVARIATE EXAMPLE

Consider

\[ f(x) := c_1 + c_2 x_1^{999} + c_3 x_1^{73} x_3 + c_4 x_2^{2009} + c_5 x_1^{2009} x_2^{6027} x_3^{18081} \]

Then \( Z_+(f) \) has topology varying according to...
TRIVARIATE EXAMPLE

Consider

$$f(x) := c_1 + c_2 x_1^{999} + c_3 x_1^{73} x_3 + c_4 x_2^{2009} + c_5 x_1^{2009} x_2^{6027} x_3^{18081}$$

Then $Z_+(f)$ has topology varying according to

$$16747013 \log(16747013) + 1317904 \log(1317904) + 999 \log(999) + 18062919 \log(c_3) + 2997 \log(c_4)$$
$$- 18062919 \log(18062919) - 2997 \log(2997) - 16747013 \log(c_1) - 1317904 \log(c_2) - 999 \log(c_5)$$

being positive...
TRIVARIATE EXAMPLE

Consider

\[ f(x) := c_1 + c_2 x_1^{999} + c_3 x_1^{73} x_3 + c_4 x_2^{2009} + c_5 x_1^{2009} x_2^{6027} x_3^{18081} \]

Then \( Z_+(f) \) has topology varying according to

\[
16747013 \log(16747013) + 1317904 \log(1317904) + 999 \log(999) + 18062919 \log(c_3) + 2997 \log(c_4) \\
-18062919 \log(18062919) - 2997 \log(2997) - 16747013 \log(c_1) - 1317904 \log(c_2) - 999 \log(c_5)
\]

being positive... zero...
TRIVARIATE EXAMPLE

Consider

\[ f(x) := c_1 + c_2 x_1^{999} + c_3 x_1^{73} x_3 + c_4 x_2^{2009} + c_5 x_1^{2009} x_2^{6027} x_3^{18081} \]

Then \( Z_+(f) \) has topology varying according to

\[
16747013 \log(16747013) + 1317904 \log(1317904) + 999 \log(999) + 18062919 \log(c_3) + 2997 \log(c_4) \\
-18062919 \log(18062919) - 2997 \log(2997) - 16747013 \log(c_1) - 1317904 \log(c_2) - 999 \log(c_5)
\]

being positive... zero... or negative.

© J. Maurice Rojas
THE ALGORITHM

Given $f(x) := \sum_{i=1}^{n+2} c_i x^{a_i}$ with $\mathcal{A} := \{a_1, \ldots, a_{n+2}\}$ of cardinality $n + 2$ and

$$\begin{bmatrix} 1 & \cdots & 1 \\ \mathcal{A} & \end{bmatrix}$$

of rank $n$...
THE ALGORITHM

Given $f(x) := \sum_{i=1}^{n+2} c_i x^{a_i}$ with $A := \{a_1, \ldots, a_{n+2}\}$ of cardinality $n + 2$ and $\begin{bmatrix} 1 & \cdots & 1 \\ A \end{bmatrix}$ of rank $n$...

0. If the $c_i$ all have the same sign then say ‘‘Empty!’’ and STOP...
THE ALGORITHM

Given $f(x) := \sum_{i=1}^{n+2} c_i x^{a_i}$ with $A := \{a_1, \ldots, a_{n+2}\}$ of cardinality $n + 2$ and $\begin{bmatrix} 1 & \cdots & 1 \\ A \end{bmatrix}$ of rank $n$...

0. If the $c_i$ all have the same sign then say ‘‘Empty!’’ and STOP.

1. Let $P := \text{Conv} A$...
THE ALGORITHM

Given \( f(x) := \sum_{i=1}^{n+2} c_i x^{a_i} \) with \( A := \{a_1, \ldots, a_{n+2}\} \) of cardinality \( n + 2 \) and \( \begin{bmatrix} 1 & \cdots & 1 \\ A \end{bmatrix} \) of rank \( n \)...

0. If the \( c_i \) all have the same sign then say ‘‘Empty!’’ and STOP.

1. Let \( P := \text{Conv} A \).

2. If \( A \cap \text{RelInt} P = \emptyset \) and the \( c_i \) do not all have the same sign, then say ‘‘Non-empty!’’ and STOP...
THE ALGORITHM

Given \( f(x) := \sum_{i=1}^{n+2} c_i x^{a_i} \) with \( A := \{a_1, \ldots, a_{n+2}\} \) of cardinality \( n + 2 \) and \( \begin{bmatrix} 1 & \cdots & 1 \\ A & \end{bmatrix} \) of rank \( n \)

0. If the \( c_i \) all have the same sign then say ‘‘Empty!’’ and STOP.
1. Let \( P := \text{Conv} A \).
2. If \( A \cap \text{RelInt} P = \emptyset \) and the \( c_i \) do not all have the same sign, then say ‘‘Non-empty!’’ and STOP.
3. If there is an \((i, j)\) with \( c_i c_j < 0 \) and \( a_i, a_j \in \partial P \) then say ‘‘Non-empty!’’ and STOP...
THE ALGORITHM

Given \( f(x) := \sum_{i=1}^{n+2} c_i x^{a_i} \) with \( A := \{ a_1, \ldots, a_{n+2} \} \) of cardinality \( n + 2 \) and \( \begin{bmatrix} 1 & \cdots & 1 \\ A \end{bmatrix} \) of rank \( n \)...  

0. If the \( c_i \) all have the same sign then say ‘‘Empty!’’ and STOP.

1. Let \( P := \text{Conv}(A) \).

2. If \( A \cap \text{RelInt}P = \emptyset \) and the \( c_i \) do not all have the same sign, then say ‘‘Non-empty!’’ and STOP.

3. If there is an \((i, j)\) with \( c_i c_j < 0 \) and \( a_i, a_j \in \partial P \) then say ‘‘Non-empty!’’ and STOP.

4. Check if \( \Delta_A(f) \neq 0 \)...
THE ALGORITHM
Given $f(x) := \sum_{i=1}^{n+2} c_i x^{a_i}$ with $A := \{a_1, \ldots, a_{n+2}\}$ of cardinality $n + 2$ and $\begin{bmatrix} 1 & \cdots & 1 \\ A \end{bmatrix}$ of rank $n$...
0. If the $c_i$ all have the same sign then say ‘‘Empty!’’ and STOP.
1. Let $P := \text{Conv} A$.
2. If $A \cap \text{RelInt} P = \emptyset$ and the $c_i$ do not all have the same sign, then say ‘‘Non-empty!’’ and STOP.
3. If there is an $(i, j)$ with $c_i c_j < 0$ and $a_i, a_j \in \partial P$ then say ‘‘Non-empty!’’ and STOP.
4. Check if $\Delta_A(f) = 0$...
5. Check if $s_f \Delta_A(f) > 0$...

©J. Maurice Rojas
Corollary 1 For uniformly distributed sign, you can decide $Z_+(f) \neq \emptyset$ in $\text{NC}^2$ on a fraction of $1 - \frac{1}{2n+2}$ of the inputs, even if $n$ is not fixed a priori!
Corollary 1 For uniformly distributed sign, you can decide $Z_+(f) = \emptyset$ in $\text{NC}^2$ on a fraction of $1 - \frac{1}{2n+2}$ of the inputs, even if $n$ is not fixed a priori!
DIOPHANTINE REFINEMENT

[Bihan-Rojas-Stella] Fix $n$. Then for any “honest” $n$-variate $(n + 2)$-nomial $f$, one can decide $Z_+(f) \neq \emptyset$ in $P$.

Corollary 2 [Rojas, 2008] Assuming Baker’s refinement of the abc-Conjecture, we have polynomiality in $n$ as well!
Corollary 2 [Rojas, 2008] Assume Baker’s refinement of the abc-Conjecture. Then for any $n$ and any “honest” $n$-variate $(n+2)$-nomial $f$, one can decide $Z_+(f) \neq \emptyset$ in $\mathbb{P}$.

Baker’s Refined abc-Conjecture (1998)
Let $N(s) := \prod_{p|s \text{ and } p \text{ prime}} p$ for any integer $s$...
Corollary 2 [Rojas, 2008] Assume Baker’s refinement of the abc-Conjecture. Then for any \( n \) and any “honest” \( n \)-variate \((n+2)\)-nomial \( f \), one can decide \( \mathbb{Z}^+ (f) \neq \emptyset \) in \( \mathbb{P} \).

Baker’s Refined abc-Conjecture (1998)
Let \( N(s) := \prod_{p \mid s \text{ and } p \text{ prime}} p \) for any integer \( s \) and define
\[
\omega(s) := \# \{ p : p \mid s \text{ and } p \text{ prime} \} ...
\]
Corollary 2 [Rojas, 2008] Assume Baker’s refinement of the abc-Conjecture. Then for any \( n \) and any “honest” \( n \)-variate \((n + 2)\)-nomial \( f \), one can decide \( Z_+(f) \neq \emptyset \) in \( \mathbb{P} \).

Baker’s Refined abc-Conjecture (1998)

Let \( N(s) := \prod_{p \mid s \text{ and } p \text{ prime}} p \) for any integer \( s \) and define \( \omega(s) := \# \{ p : p \mid s \text{ and } p \text{ prime} \} \). Then for any \( a, b, c \in \mathbb{N} \) with \( a + b = c \) and no common factor, we have

\[
c = O\left( \frac{\log^{\omega(abc)} N(abc)}{\omega(abc)!} N(abc) \right).
\]
Corollary 2 [Rojas, 2008] Assume Baker’s refinement of the abc-Conjecture. Then... ...one can decide \( Z_+(f) = \emptyset \) in \( P \).

Baker’s Refined abc-Conjecture (1998)

Let \( N(s) := \prod_{p|s \text{ and } p \text{ prime}} p \) and define \( \omega(s) := \#\{p : p|s \text{ and } p \text{ prime}\} \). Then for any \( a, b, c \in \mathbb{N} \) with \( a + b = c \) and no common factor, we have

\[
c = O\left( \frac{\log \omega(abc) N(abc)}{\omega(abc)!} N(abc) \right).
\]

Note: Baker’s Refined abc-Conjecture implies: (1) Effective Falting’s Theorem [Elkies ’91], (2) Effective Roth’s Theorem [Bombieri ’94, Surroca ’07], (3) non-existence of Siegel zeroes for certain \( L \)-functions [Granville ’00]. Conversely, suitably sharp versions of (1) or (2) imply variants of abc! [Surroca ’07, van Frankenhuiysen ’07]
$n$-VARIATE $(n + 3)$-NOMIALS?

Obstruction #1:
Thank you for listening!

Please see...

www.math.tamu.edu/~rojas

for on-line papers and further information.