Counting Numbers of Solutions of Systems of Polynomial Equations

John B. Little

Department of Mathematics and Computer Science

College of the Holy Cross

Worcester, MA 01610

email: little@mathcs.holycross.edu

SIMU Colloquium

June 21, 2002

Outline of Talk

1. Applied problems to polynomial systems, an example: conformations of cyclohexane

2. Solving polynomial systems numerically – why counting solutions is important

3. Algebraic techniques 1: The fundamental theorem of algebra

4. Algebraic techniques 2: Bézout's theorem

5. Algebraic techniques 3: The BKK bound

An Applied Problem

Many organic molecules exist in different *conformations* or 3D geometric forms.

Identifying possible forms is of importance, for instance, in design of drugs, insectides, herbicides, etc. because the 3D structure influences functional properties of the molecules (how well they link to receptor sites in cells, for example).

In the Gröbner Bases seminar at SIMU 1999, I supervised Carlos Guillén (then at UC Riverside), Everilis Santana-Vega (now at Cornell U.), and Omar Zuñiga (now at U. Arizona), who studied the conformations of 6-element ring structures such as carbon ring in *cyclohexane* (C_6H_{12}).

Reducing the Problem

Determining molecular conformations is essentially an *energy minimization problem*. In the 1970's, however, chemists developed an approximate theory showing that energy depends only on the *dihedral angles* between certain planes defined by sets of atoms. Bond lengths and angles may be considered as *rigid*. This means that the conformations problem can be treated in *purely geometric* terms. Possible conformations are solutions of a system of equations for sines and cosines of the dihedral angles, denoted θ_i.

(Interestingly enough, the mathematics turns out to be quite similar to that used in robot kinematics questions.)

Polynomial Equations

The trigonometric equations can be converted to algebraic equations by means of *half-angle* formulas. Let $t_i = \tan(\theta_i/2)$. Then

$$\begin{aligned} \sin\theta_i &= \frac{2t_i}{1+t_i^2} \\ \cos\theta_i &= \frac{1-t_i^2}{1+t_i^2} \end{aligned}$$

Substituting and clearing denominators yields:

$$\begin{aligned} 0 &= \beta_{11} + \beta_{12}t_2^2 + \beta_{13}t_3^2 + \beta_{14}t_2t_3 + \beta_{15}t_2^2t_3^2 \\ 0 &= \beta_{21} + \beta_{22}t_3^2 + \beta_{23}t_1^2 + \beta_{24}t_1t_3 + \beta_{25}t_1^2t_3^2 \\ 0 &= \beta_{31} + \beta_{32}t_1^2 + \beta_{33}t_2^2 + \beta_{34}t_1t_2 + \beta_{35}t_1^2t_2^2 \end{aligned}$$

where β_{ij} are constants depending on the bond lengths and angles. The problem is then to find all solutions (t_1, t_2, t_3) in $\mathbf{R}^3$.

Solving Polynomial Systems

There are a number of approaches to solving polynomial systems used in practice:

- *numerical* methods, often iterative, for deriving approximations to solutions. For instance, for polynomial equations in one variable $f(x) = 0$, can use *Newton's Method*: x_0 chosen,

  $$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, n \geq 0$$

  Generalizes easily to systems $F(\vec{x}) = \vec{0}$:

  $$\vec{x}_{n+1} = \vec{x}_n - F'(\vec{x}_n)^{-1} F(\vec{x}_n)$$

- *algebraic* methods such as resultants (analogs of Cramer's Rule for linear systems), elimination via Gröbner bases (analogs of Gaussian Elimination for linear systems), and others

Maple demo

The Problem With Iterative Methods

One difficulty with iterative methods – If we want to find all the solutions of a system, *how do we ever know we have them all?* Of course,

- In some cases, we might be able to apply some cleverness (say inequalities) to bound the region to search for solutions, or

- There might be symmetries of the problem that could be exploited in some useful way, etc.

But it would be extremely useful to have some information about how many solutions to expect, given the "shape" of the polynomials in the system.

Some Polynomial Terminology

- A polynomial in one variable:

  $$p(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0$$

  The *coefficients* $c_i \in \mathbf{R}$ or $\mathbf{C}$ for us today.

- A polynomial in several variables $x_1, \ldots, x_n$: $\sum_\alpha c_\alpha x^\alpha$, only now $\alpha = (\alpha_1, \ldots, \alpha_n)$ and x^α means $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $c_\alpha \in \mathbf{R}$ or $\mathbf{C}$.

- The *degree* of a monomial x^α is the *sum* $\alpha_1 + \cdots + \alpha_n$.

- The *total degree* of a polynomial is the *largest* degree of the monomials appearing (with non-zero coefficients)

- Example:

  $$p(x_1, x_2, x_3) = 4x_1^3 x_2 - 7x_1 x_2^8 x_3 + 5x_3^5$$

Roots of Polynomials in One Variable

Recall the following basic facts from high school algebra

- $x = a$ is a root of the polynomial equation
$$p(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0 = 0$$
if and only if $x - a$ divides $p(x)$; that is $p(x) = (x - a)q(x)$ for some polynomial $q(x)$.

- If so, the degree of $q(x)$ is $d - 1$, so by induction we see that $p(x) = 0$ has *at most* d roots.

These are valid for polynomials with coefficients in any field.

Over the Complex Numbers

The most fundamental result on counting solutions of polynomial equations is based on

Theorem 1 *(Fundamental Theorem of Algebra) Every polynomial equation*

$$p(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0 = 0 \quad (1)$$

with $c_i \in \mathbf{C}$ has a root in $\mathbf{C}$.

Since $x - a$ divides $p(x)$ for each root a of (1), it follows that (1) has exactly d solutions in $\mathbf{C}$, provided we count roots with their multiplicities (i.e. a double root counts as two roots, a triple root counts as three roots, etc.)

More Than One Variable

- In several variables, answers this tidy are not always available

- We'll focus on a special case where we can at least hope for good information

- We'll assume that we have a system of polynomial equations with real or complex coefficients, with the *same number* n *of equations as variables*

- We'll also assume that the number of solutions in $\mathbf{C}^n$ is finite. (This amounts to assuming that the equations in the system are "independent" in a certain sense.)

Two Equations in Two Unknowns

Geometric approach to two polynomial equations in two variables:

$$(2) \qquad \begin{cases} p(x,y) = 0 \\ q(x,y) = 0 \end{cases}$$

- Separately, $p(x,y) = 0$ defines a curve C, and $q(x,y) = 0$ defines a curve D.

- Solutions of the simultaneous system (2) are *intersections* of the curves C and D.

- If $p(x,y)$ has total degree m we say C is a curve of degree m; similarly for q and D.

- The number of solutions is finite in this case, unless $p(x,y)$ and $q(x,y)$ have a non-constant *common factor*.

An Example

Consider the equations

$$\begin{aligned} p(x,y) &= x^2 - 4\,xy + 2\,y^2 - 3\,x \\ q(x,y) &= x^3 - 5\,yx^2 + 40\,x - y^2 + 4\,y - 1/2 \end{aligned}$$

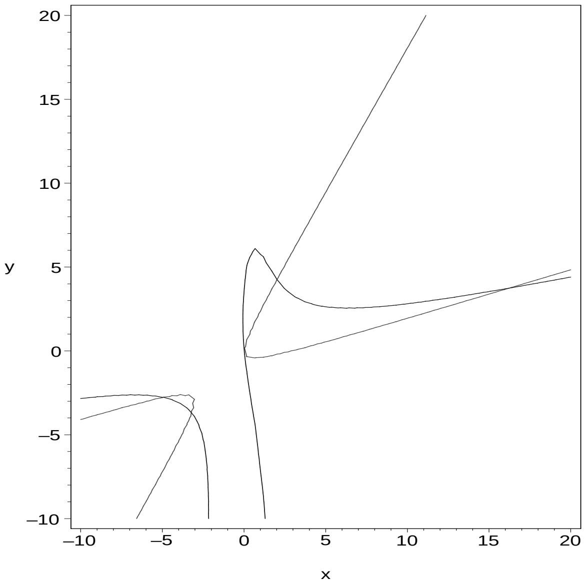
- The curve C defined by $p(x,y) = 0$ is a curve of degree 2, or *conic section* – by examining the discriminant of the quadratic terms, we can see that it is a *hyperbola*.

- The curve D defined by $q(x,y) = 0$ is a degree 3, or *cubic*, curve.

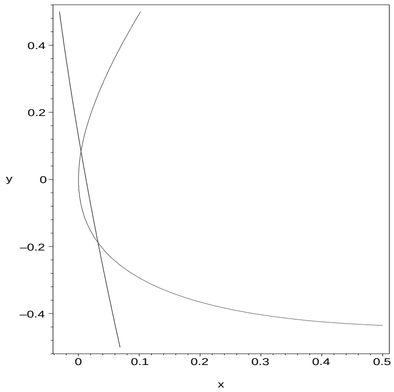
Let's plot the points on C, D with real coordinates:

Plots

"Wide-angle" view:



Zooming in near the origin:



A Pattern

In our example we see $6 = 2 \cdot 3$ (real) intersection points. Could there be others? Are there other non-real intersections? Should any of these count as multiple roots?

The answer in each case is *no* for these equations because of:

Theorem 2 *(***Bézout's Theorem***, weak form.) Let C be a curve $p(x, y) = 0$ of degree m and D be a curve $q(x, y) = 0$ of degree n, defined by polynomials with complex coefficients. Assume that $p(x, y)$ and $q(x, y)$ have no common nonconstant factors. Then, counting multiplicities, C and D have at most $m \cdot n$ intersections in $\mathbf{C}^2$.*

An "Easy Case" of Bézout

Consider the case $m = 1$ first. C is a line defined $\alpha x + \beta y + \gamma = 0$, where $\alpha \neq 0$ or $\beta \neq 0$. Say $\beta \neq 0$. Then use the equation of the line to solve for y in terms of x on the line: $y = -(\alpha/\beta)x - (\gamma/\beta)$. Substituting into $q(x, y) = 0$, we get that the x-coordinates of the intersections of C and D satisfy

$$q(x, -(\alpha/\beta)x - (\gamma/\beta)) = 0$$

Since the total degree of D is n, this is a polynomial of degree at most n in x, which has at most n roots by the FTA. Each x-value solving this equation corresponds to only one y solving the equation of the line, so the total number of solutions is at most n. (Note: $< n$ solutions is possible.)

Heuristic “Proof”

A stronger statement of Bézout’s theorem is true if we consider the closures of the two curves in the *projective plane* (where we add *a point at infinity* for each asymptotic direction, so that every two lines intersect somewhere). In the projective plane, $\overline{C}$ and $\overline{D}$ will always meet in exactly $m \cdot n$ points.

Intuitively, we can deform $\overline{C}$ continuously into a union of m lines – think of deforming the hyperbola above to its two asymptote lines – and similarly deform $\overline{D}$ into a union of n lines.

A union of m lines meets a union of n lines in exactly $m \cdot n$ points (some possibly at infinity, and not necessarily distinct).

Why This Is Not A Proof

- To make this argument precise requires justification for the implicit claim that the number of intersections stays constant in the deformation.

- This takes a continuity argument for the intersections as we deform (or some algebraic topology to determine the cohomology of the complex projective plane and the intersection, or "cup", product)

- There is also a more elementary argument using *resultants* ("19th century algebra").

A Generalized Bézout Theorem

For systems with more equations and variables, we have

Theorem 3 *(**Generalized Bézout's Theorem**) Let*

$$\begin{aligned} F_1(x_1, \ldots, x_n) &= 0 \\ F_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ F_n(x_1, \ldots, x_n) &= 0 \end{aligned}$$

be a system of n polynomial equations in n unknowns, and let the total degree of F_i be m_i. If the number of solutions (including any solutions "at infinity") is finite, then there are at most $m_1 \cdot m_2 \cdot \cdots \cdot m_n$ solutions in $\mathbf{C}^n$.

An Example

For instance, consider the system of equations we had before from the cyclohexane conformations problem:

$$
\begin{aligned}
0 &= \beta_{11} + \beta_{12}t_2^2 + \beta_{13}t_3^2 + \beta_{14}t_2t_3 + \beta_{15}t_2^2t_3^2 \\
0 &= \beta_{21} + \beta_{22}t_3^2 + \beta_{23}t_1^2 + \beta_{24}t_1t_3 + \beta_{25}t_1^2t_3^2 \\
0 &= \beta_{31} + \beta_{32}t_1^2 + \beta_{33}t_2^2 + \beta_{34}t_1t_2 + \beta_{35}t_1^2t_2^2
\end{aligned}
$$

The generalized Bézout theorem would say: Since each equation has total degree 4, provided the number of solutions is finite (which it is for “generic” choices of β_{ij}), then that number is $\leq 4 \cdot 4 \cdot 4 = 64$.

In fact, there are *far fewer*, generically(!)

The “Shape” of the Polynomials Matters!

The generalized Bézout upper bound is valid for *any* three polynomials of total degree 4, and in effect *includes* solutions “at infinity”.

But, our polynomials in this example are “sparse” – each has only a small fraction of the total possible number of terms (most of the terms have *zero coefficients*).

To get better bounds on the number of possible solutions, we must take the actual “shape” of the polynomials into account. This was done in a very interesting way by Bernstein, Kushnirenko, and Khovanskii in the late 1970’s – result is called the *BKK bound*.

BKK Ingredients

- To each monomial $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ associate the integer lattice point

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{R}^n$$

- If $p = \sum_\alpha c_\alpha x^\alpha$, then we can define the *Newton polytope* of p to be

$$NP(p) = \text{conv}(\{\alpha : c_\alpha \neq 0\})$$

(conv means *convex hull*).

- E.g., for $p(x, y) = x^2 - 4\,xy + 2\,y^2 - 3x$,

$$NP(p) = \text{conv}(\{(2,0), (1,1), (0,2), (1,0)\})$$

which is a triangle with vertices at $(2,0), (0,2)$, $(1,0)$ in $\mathbf{R}^2$.

BKK Ingredients, cont.

- For the cubic from our previous example, $q = x^3 - 5\,yx^2 + 40\,x - y^2 + 4\,y - 1/2$,

$$\begin{aligned} NP(q) &= \text{conv}(\{(3,0),(2,1),(1,0),\\ &\qquad (0,2),(0,1),(0,0)\}) \end{aligned}$$

  which is a quadrilateral.

- In general Newton polytopes are examples of convex polytopes in $\mathbf{R}^n$ (e.g. polygons if $n = 2$, polyhedra if $n = 3$, etc.)

BKK Ingredients, cont.

- Let P and Q be any two convex polytopes in $\mathbf{R}^n$. The *Minkowski sum* of P and Q is

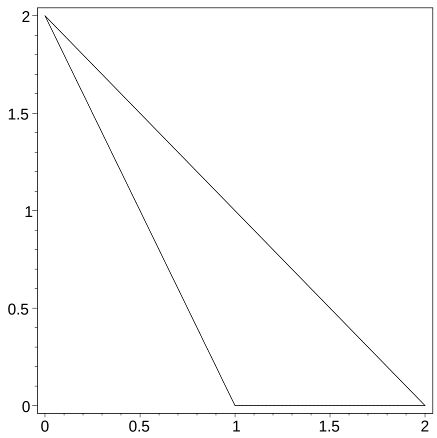
$$P + Q = \{p + q : p \in P, q \in Q\}$$

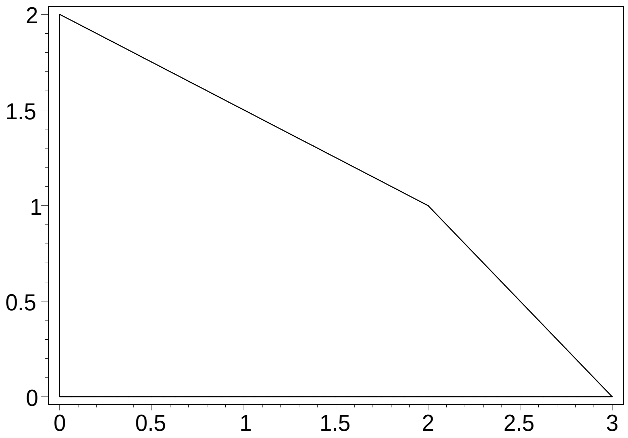
- It can be shown that this is also a convex polytope in $\mathbf{R}^n$.

- For instance, if $P = NP(p)$, $Q = NP(q)$ for the conic and cubic in our previous example, then here is a picture of P, Q, and $P + Q$:

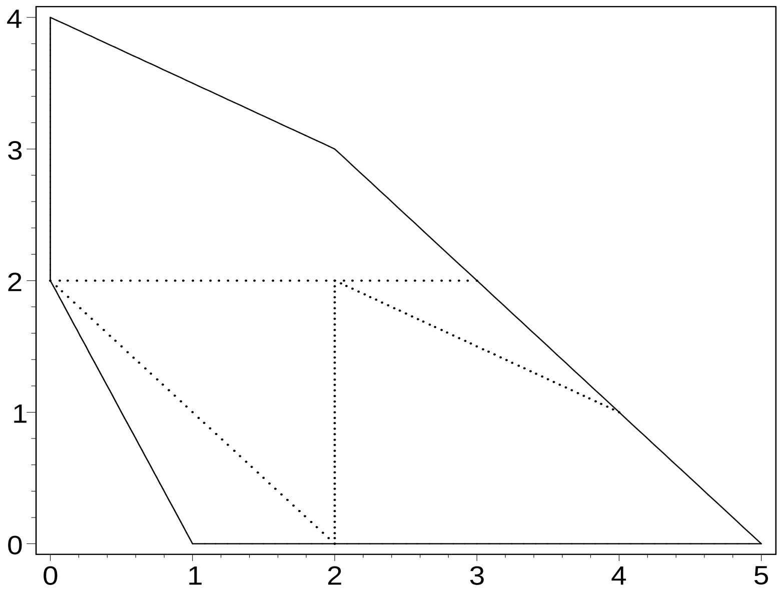
Minkowski Sum Example

Newton polytopes P and Q:





Minkowski sum:



BKK Ingredients, concluded

The final ingredient we need to state the BKK bound is the definition of the *mixed volume* of a collection $P_1, \ldots, P_n$ of polytopes in $\mathbf{R}^n$:

$$MV(P_1, \ldots, P_n) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{|I|=k} \mathrm{Vol}(\sum_{i \in I} P_i)$$

The notation $|I| = k$ on the middle summation sign means that we sum over all subsets $I \subseteq \{1, \ldots, n\}$ of size k; the innermost sum is the Minkowski sum of the subset of the polytopes with indices in I. Vol is n-dimensional volume in $\mathbf{R}^n$ (area in $\mathbf{R}^2$, ordinary volume in $\mathbf{R}^3$, etc.)

For Instance, ...

With two polygons in $\mathbf{R}^2$, the mixed volume ("mixed area"?) is just

$$MV(P,Q) = -\text{Vol}(P) - \text{Vol}(Q) + \text{Vol}(P+Q)$$

For our Newton polytopes P, Q from earlier, we have $\text{Vol}(P) = 1$, $\text{Vol}(Q) = 7/2$, and $\text{Vol}(P+Q) = 21/2$, so

$$MV(P,Q) = -1 - 7/2 + 21/2 = 6$$

Recall that the corresponding set of equations $p = q = 0$ *had 6 solutions!*

The BKK Theorem

We let $\mathbf{C}^*$ be the set of nonzero complex numbers.

Theorem 4 *(BKK) Let p_i be polynomials in n variables such that the system of equations $p_1 = \cdots = p_n = 0$ has finitely many common zeroes in $(\mathbf{C}^*)^n$. Let P_i be the Newton polytope of p_i. Then counting with multiplicities, the number of solutions in $(\mathbf{C}^*)^n$ is bounded above by $MV(P_1, \ldots, P_n)$. Moreover, for generic choices of the coefficients in the p_i, the number will be exactly $MV(P_1, \ldots, P_n)$.*

The theorem is also valid more generally for *Laurent polynomial* equations – each equation a sum of monomials with integer exponents (positive or negative).

BKK Implies Bézout

The BKK bound contains the Bézout bound as a special case.

- For completely "dense" polynomials $p(x, y)$, $q(x, y)$ of total degrees m and n, the Newton polytopes $NP(p)$ and $NP(q)$ will be isosceles right triangles with legs of lengths m, n along the two axes.

- the Minkowski sum will be an isosceles right triangle with legs $m + n$,

- the mixed volume is
$$MV(P, Q) = \frac{(m+n)^2}{2} - \frac{m^2}{2} - \frac{n^2}{2} = mn(!)$$

- Nice exercise – Show that BKK also implies generalized Bézout for more than 2 variables.

Returning to our first example

Recall the form of the cyclohexane equations:

$$
\begin{aligned}
0 &= \beta_{11} + \beta_{12}t_2^2 + \beta_{13}t_3^2 + \beta_{14}t_2t_3 + \beta_{15}t_2^2t_3^2 \\
0 &= \beta_{21} + \beta_{22}t_3^2 + \beta_{23}t_1^2 + \beta_{24}t_1t_3 + \beta_{25}t_1^2t_3^2 \\
0 &= \beta_{31} + \beta_{32}t_1^2 + \beta_{33}t_2^2 + \beta_{34}t_1t_2 + \beta_{35}t_1^2t_2^2
\end{aligned}
$$

What does the BKK bound tell us?

The actual number of solutions

In fact in the problem for

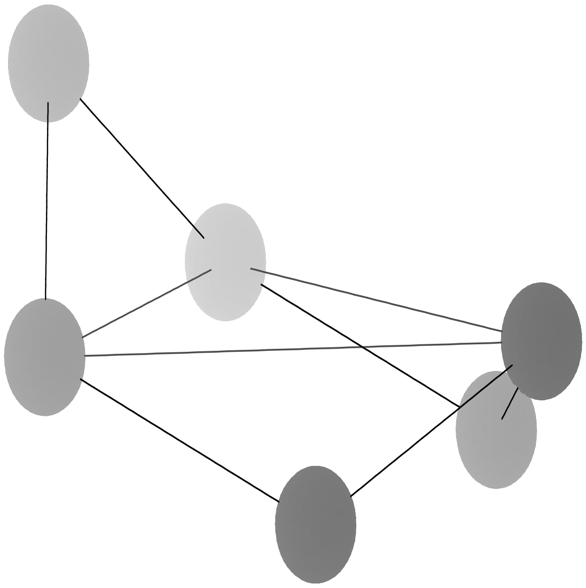
- equal bond lengths and
- the *exact* tetrahedral bond angle

$$= \arccos(-1/3),$$

the coefficients β_{ij} are all of the form $a + b\sqrt{6}$. If you take a rational approximation of $\sqrt{6}$ and substitute, there are actually only 16 solutions (and 8 real ones – 2 "boat" and 6 "chair" conformations).

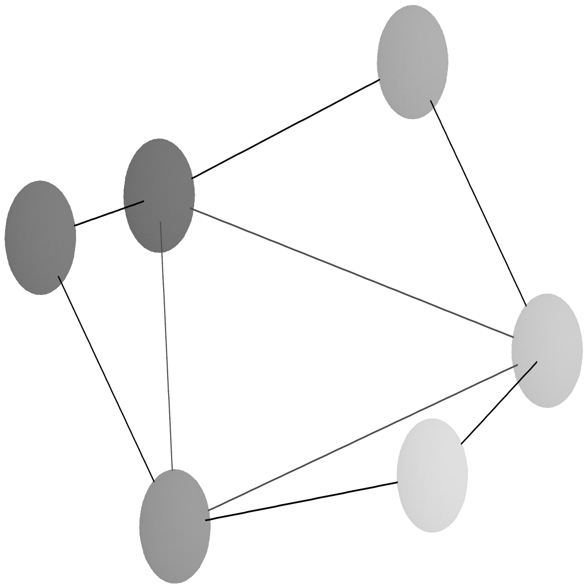
Boat Conformation of Cyclohexane Carbons

A “boat”:



Chair Conformation of Cyclohexane Carbons

A "chair":



A "Wrinkle"

If you don't approximate $\sqrt{6}$, there is actually a 1-dimensional parametrized family of conformations in the case of the exact tetrahedral bond angle(!) – the "boat" conformation is *flexible* and can be deformed in a continuous family(!)

The approximation of $\sqrt{6}$ (which is what Carlos, Everilis, and Omar did) can be thought of as adding some "noise" to the exact coefficients, which is enough to perturb the system of equations into one with only finitely many solutions.

Polynomial equations are often "perverse" in this way – any possible bad behavior can and does occur for some choices of coefficients!

Conclusions

- Bézout can be used to bound the number of solutions of a polynomial system
- The BKK bound is often tighter when the polynomials have some special "sparsity structure"
- The BKK bound also serves as an ingredient in a very promising "new generation" of numerical techniques for polynomial system solving called *homotopy continuation methods*. But that's another story, ...
- *¡Muchas gracias por su atención!*