Numerical Approximations: sometimes close is good enough

August 15, 2019

Overview

- A few comments on ideals
- Continued Fractions
- LLL

Ideals with generators in $\mathbb{Q}[x_0, \ldots, x_n]$

Call an ideal $\mathbb{Q}$-generated if the ideal has a set of generators in $\mathbb{Q}[x_0, \ldots, x_n]$.

If I is $\mathbb{Q}$-generated, what can we say about various ideals associated to I?

If J is $\mathbb{Q}$-generated then $I : J$ is $\mathbb{Q}$-generated.

The saturation, radical, $\mathbb{Q}$-projections, singular locus of I are all $\mathbb{Q}$-generated.

If the associated primes of the radical of I are partitioned into sets $S_1, \ldots, S_p$ based on their Hilbert function then the intersection of the prime ideals in S_i is $\mathbb{Q}$-generated.

Punchline: In many cases, most of the irreducible components of a $\mathbb{Q}$-generated ideal are either $\mathbb{Q}$-generated or are $\mathbb{Q}(\alpha)$-generated for a "small" field extension.

Numerical approximations of generic points

Let $V(I) \subset \mathbb{C}^n$ be the variety defined by I

Let J be an associated prime of $\sqrt{I}$

Given points almost on $V(J)$, can we recover J?

Why consider such a problem?

Homotopy continuation is a tool in algebraic geometry that utilizes numerical algorithms.

It produces numerical data instead of exact data.

The goal is to recover the exactness that is lost in a numerical algorithm but keep its computational advantages.

Homotopy Continuation:

In homotopy continuation, a polynomial ideal, I, is cast as a member of a parameterized family of polynomial ideals one of which has known isolated solutions.

Each of the known isolated solutions is tracked, using a predictor/corrector method, to a point which lies numerically close to the algebraic set $V(I)$ determined by I.

The basic algorithms of numerical algebraic geometry can be parallelized.

What will be assumed:

Let $V_1, V_2, \ldots, V_r$ denote the irreducible components of $V(I)$. The algorithms of numerical algebraic geometry can be used to produce sets of points $S_1, S_2, \ldots, S_r$ such that

- The points in S_i lie within any prescribed tolerance of V_i.
- The points in S_i approximate generic points on V_i.
- The number of points in S_i can be increased.
- Points in S_i can be "sharpened" to be arbitrarily close to V_i.
- Each V_i is labelled with its dimension and degree.

Basic Varieties

The simplest algebraic varieties are individual points.

A more general class of simple varieties are linear spaces.

The equations defining a linear space are linear polynomials.

What can we say about a linear space from points on or nearly on the linear space?

Some Questions:

Question 1: If you know enough points on a linear space, what can you say about the linear space?

Question 2: If you know enough points almost on a linear space, what can you say about the linear space?

Question 3: If a linear space is spanned by vectors with integer entries, does the answer to question 2 change?

Question 1 can be solved with basic linear algebra.

You can exactly determine the linear space.

Question 2 can be partially answered with tools from advanced linear algebra (Singular Value Decomposition).

You can determine the dimension of the linear space and can get a very good approximation for the space.

Question 3 is what we would like to answer.

But first, let's go to a seemingly unrelated topic:

Continued Fractions

A continued fraction will be taken to mean an expression of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i > 0$.

Sometimes this is written in the form $[a_0; a_1, a_2, a_3, \ldots]$.

For instance $[4; 3, 7, 2, \ldots] = 4 + \cfrac{1}{3 + \cfrac{1}{7 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}$.

Algorithm for continued fraction expansion

For $\alpha \in \mathbb{R}$, let $\lfloor \alpha \rfloor$ = greatest integer less than or equal to α.

Algorithm:
Given $\alpha \in \mathbb{R}$
Set $a_0 = \lfloor \alpha \rfloor$, $b_0 = \alpha - a_0$, $i = 0$
While $b_i \neq 0$
  $a_{i+1} = \lfloor \frac{1}{b_i} \rfloor$
  $b_{i+1} = \frac{1}{b_i} - \lfloor \frac{1}{b_i} \rfloor$
  Set $i \to i + 1$

Output: $\alpha = [a_0; a_1, a_2, \ldots]$

Example

Let $\alpha = \frac{18}{7}$

$a_0 = \lfloor \frac{18}{7} \rfloor = 2 \qquad \frac{18}{7} - 2 = \frac{4}{7}$

$a_1 = \lfloor \frac{7}{4} \rfloor = 1 \qquad \frac{7}{4} - 1 = \frac{3}{4}$

$a_2 = \lfloor \frac{4}{3} \rfloor = 1 \qquad \frac{4}{3} - 1 = \frac{1}{3}$

$a_3 = \lfloor 3 \rfloor = 3 \qquad 3 - 3 = 0 \qquad \text{STOP}$

$\frac{18}{7} = [2; 1, 1, 3]$

So $\frac{18}{7} = [2; 1, 1, 3] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}$

Note that $\frac{18}{7}$ is also equal to $[2; 1, 1, 2, 1]$.

I.e. $\frac{18}{7} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}}}$

Remarks

1) Irrational numbers are in 1-1 correspondence with infinite continued fractions $[a_0; a_1, a_2, a_3, \dots]$.

2) Rational numbers can be expressed in exactly *two ways* as a finite continued fraction.

For example, we saw that $\frac{18}{7} = [2; 1, 1, 3] = [2; 1, 1, 2, 1]$.

Convergents

Given a continued fraction expansion $\alpha = [a_0; a_1, a_2, a_3, \dots]$, the n^{th} convergent is the rational number $[a_0; a_1, a_2, \dots, a_n] = \frac{h_n}{k_n}$.

So we obtain a sequence of convergents:
$[a_0], \quad [a_0; a_1], \quad [a_0; a_1, a_2], \quad [a_0; a_1, a_2, a_3], \quad \dots$

For example, the convergents to $[2; 3, 4, 5, 6]$ are
$[2], \quad [2; 3], \quad [2; 3, 4], \quad [2; 3, 4, 5], \quad [2; 3, 4, 5, 6]$.

This gives a sequence of fractions $2, \quad \frac{7}{3}, \quad \frac{30}{13}, \quad \frac{157}{68}, \quad \frac{972}{421}$.

The decimal approximations:
2, 2.333333, 2.307692, 2.308824, 2.308789

The sequence of convergents of $\alpha = [a_0; a_1, a_2, \dots]$ converge to α.

If the n^{th} convergent of α is $\frac{h_n}{k_n}$, then a theorem states that

$$\frac{1}{k_n(k_{n+1} + k_n)} < |\alpha - \frac{h_n}{k_n}| < \frac{1}{k_n k_{n+1}}.$$

A corollary is that a convergent is nearer to α than any other fraction whose denominator is less than that of the convergent.

The rate at which a sequence of convergents approaches a number is exponential.

For instance,

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \dots]$$

and its first few convergents are

$$3, \ \frac{22}{7}, \ \frac{333}{106}, \ \frac{355}{113}, \ \frac{103993}{33102}, \ \dots$$

No fraction with denominator less than 33102 gets closer to π than the 4^{th} convergent

$$\frac{103993}{33102} = 3.14159265...$$

Remarks

1) We can encode any infinite sequence of positive integers $a_0, a_1, a_2, \ldots$ as an irrational number $\alpha = [a_0; a_1, a_2, \ldots]$.

2) We can encode any finite sequence of positive integers $a_0, a_1, a_2, \ldots, a_k$ as a rational number $\alpha = [a_0; a_1, a_2, \ldots, a_k, 1]$.

3) Other encodings are possible. For example, we could map a binary string to a string of $2's$ and $3's$:

$$011010110 \to 233232332 \to [0, 2, 3, 3, 2, 3, 2, 3, 3, 2, 1, 1]$$

$$= \frac{11479}{26446} \cong .434054299326930...$$

In this example, we use 0 as a start signal and 1,1 as a stop signal. In decoding, an error has occurred if we see a strange number.

$$.434054289326930 \to [0; 2, 3, 3, 2, 3, 2, 3, 3, 7, 6, ...]$$

$$.434054299326930 \to [0; 2, 3, 3, 2, 3, 2, 3, 3, 2, 1, 1, 4101181, 1, 4, 2, ...]$$

Gauss-Kuzmin Distribution

Let r be a random real number with continued fraction expansion $[a_0; a_1, a_2, a_3, \ldots]$. For large n,

$$Pr(a_n = k) = -\log_2[1 - \frac{1}{(k+1)^2}]$$

and

$$Pr(a_n \leq k) = 1 - \log_2[\frac{k+2}{k+1}]$$

and

$$Pr(a_n > k) = \log_2[\frac{k+2}{k+1}]$$

Big numbers are rare

The formulas show that

$Pr(\alpha_n > 1,000) \approx \frac{1}{693}$

$Pr(\alpha_n > 10,000) \approx \frac{1}{6930}$

$Pr(\alpha_n > 1,000,000) \approx \frac{1}{693000}$

Punchline: If you see a big number in a continued fraction, it typically is a signal

Example: Recovery of a rational number from an approximation

$\frac{97}{184} = [0; 1, 1, 8, 1, 2, 3] = [0; 1, 1, 8, 1, 2, 2, 1]$

$\frac{97}{184} = .527173913043478260869565 2...$

$.5271739130 = [0; 1, 1, 8, 1, 2, 2, 1, 679347, 8]$

$.527173913043478 = [0; 1, 1, 8, 1, 2, 2, 1, 113224637680, 2, 5, 2]$

$.527173913043479 = [0; 1, 1, 8, 1, 2, 3, 39961636828, 2, 5, 2]$

Example:

$$\frac{23571113}{17192329} = [1; 2, 1, 2, 3, 1, 1, 3, 1, 44, 1, 1326]$$

$$= [1; 2, 1, 2, 3, 1, 1, 3, 1, 44, 1, 1325, 1]$$

$$= 1.37102500772292107718506317555 9\ldots$$

$$1.37102500772292107718506317555 9 =$$
$$[1; 2, 1, 2, 3, 1, 1, 3, 1, 44, 1, 1326, 1183888099924070 2, 4, 8, \ldots]$$

$$1.37102500772292107718506317556 0 =$$
$$[1; 2, 1, 2, 3, 1, 1, 3, 1, 44, 1, 1325, 1, 473689544382864 8, 4, 1, \ldots]$$

Example:

$$\frac{45319752357111317192327293157593522194531975235711131719232729315759352219}{74637293741434753596167717356473829678673486763478638686028646777669234698}$$

$=$

.607199833827202950876327865772656460412150218662285387338148795427613851889934191081637550889404413076695461583000053768177202914703360582047917844144884055506617734383126831639994890011256870851O741 ...

[0, 1, 1, 1, 1, 4, 1, 21, 1, 1, 3, 2, 1, 15, 2, 16, 6, 1, 1, 2, 1, 26, 2, 14, 2, 1, 1, 89, 20, 1, 4, 27, 3, 1, 2, 1, 1, 4, 3, 2, 5, 199, 3, 2, 303, 5, 1, 2, 3, 4, 1, 2, 2, 6, 2, 1, 2, 1, 11, 2, 1, 8, 3, 6, 3, 9, 1, 1, 2, 7, 1, 3, 12, 2, 2, 1, 8, 1, 65, 1, 4, 1, 1, 1, 1, 2, 12, 3, 1, 2, 262, 2, 25, 1, 2, 1, 1, 6, 1, 26, 7, 2, 1, 1, 6, 2, 1, 1, 1, 1, 2, 1, 1, 1, 6, 7, 1, 6, 1, 1, 2, 2, 2, 2, 1, 3, 22, 13, 93, 1, 2, 3, 1, 1, 1, 8, 1, 4, 1, 2, 2, 660329530346930625231497653447220983821669790574780 86, 7, 1, 1, 4, ...]

Now let's work our way back to ideals.

Consider a line spanned by a vector with rational coordinates.

Given the first 13 digits of a random point on the line, we will use continued fractions to recover the line.

Example: Recovery of a line from a generic point

Consider the line, L, spanned by the vector $< 117\ 223\ 97 >$

Here is an approximation for a generic point on L:
$(367.5663404700058, 700.5751617505238, 304.7344873982099)$

Dividing by the first term we get the point:
$(1, \frac{700.5751617505238}{367.5663404700058}, \frac{304.7344873982099}{367.5663404700058}) = (1, \alpha, \beta)$

We find that $\alpha = [1; 1, 9, 1, 1, 1, 3, 4273504273504]$
and $\beta = [0; 1, 4, 1, 5, 1, 1, 1, 1221001221000, 1, 1, 3]$

We find $[1; 1, 9, 1, 1, 1, 3] = \frac{223}{117}$ and $[0; 1, 4, 1, 5, 1, 1, 1] = \frac{97}{117}$

Thus $(1, \alpha, \beta) \approx (1, \frac{223}{117}, \frac{97}{117})$

Four key facts about RREF

1) If $B \in \mathbb{Q}^{a \times b}$ then $RREF(B) \in \mathbb{Q}^{a \times b}$

2) Let $\mathbb{F}$ be any field containing $\mathbb{Q}$. If $A \in GL_{\mathbb{F}}(a)$ then $RREF(AB) = RREF(B)$

3) If B has a basis with entries from $\mathbb{Q}$ then the null space of B has a basis with entries from $\mathbb{Q}$

4) Small perturbations of B lead to small perturbations of RREF(B) (on the big cell)

Example:

Consider the twisted cubic in $\mathbb{R}^3$. The ideal of the twisted cubic has three linearly independent quadrics.

Consider the matrix $M \in \mathbb{R}^{Big \times 3}$ whose rows consist of random points on the twisted cubic.

What is the rank of M?

The 2-Veronese map of the rows of M gives a matrix $N \in \mathbb{R}^{Big \times 10}$. What is the rank of N?

The null space of N corresponds to the three quadric generators.

Why is this useful?

Let $I = (f_1, \ldots, f_k)$ be an ideal where $f_1, \ldots, f_k \in \mathbb{Q}[x_0, \ldots, x_9]$.
Let J_1 be the ideal of a twisted cubic in $\mathbb{R}^9$. Suppose $I = J_1 \cap J_2$.

Finding J_1 using only Grobner basis techniques can be difficult.

However, confirming that $I \subset J_1$ is a cheap computation.

Punchline: Using Grobner bases, we can prove that our "guess" is correct.

Almost orthogonality in the plane

If $|\alpha - \frac{h_n}{k_n}|$ is small then we can write this as

$$\alpha \approx \frac{h_n}{k_n}$$

or as

$$\alpha k_n - h_n \approx 0.$$

This can be thought of as saying

$$[\alpha \quad 1] \cdot [k_n \quad -h_n] \approx 0.$$

From the continued fraction expansion of a real number α there is an algorithm for finding all best rational approximations for α.

Consequence: Given a vector $v \in \mathbb{R}^2$ and an $\epsilon > 0$ there is an algorithm for finding a "smallest vector" $w \in \mathbb{Z}^2$ such that $v \cdot w < \epsilon$.

Thus, given a vector $v \in \mathbb{R}^2$, we have a method for finding vectors in $\mathbb{Z}^2$ which are almost orthogonal to v and are "small".

Almost Orthogonality in general

Let v be a vector in $\mathbb{C}^n$ and let $\epsilon > 0$.

Let $F(v, \epsilon) = min\{|w| \;\big|\; w \in \mathbb{Z}^n \;\text{ and }\; |w \cdot v| < \epsilon\}$

Problem: Find $F(v, \epsilon)$ and a w that realizes this minimum.

Lattices

Let $B = \{b_1, b_2, \ldots, b_m\}$ be a set of linearly independent vectors.

Let L be the lattice formed as the $\mathbb{Z}$-span of the elements of B.

In other words: $L = \mathbb{Z}b_1 + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_m$

Two sets of vectors generate the same lattice if and only if they are related by a unimodular integer transformation.

LLL Algorithm

The LLL algorithm starts with a basis B for a lattice L then uses a Gram-Schmidt type process to attempt to produce an orthogonal basis for the lattice.

In polynomial time it produces an *almost orthogonal* basis, B', called an LLL-reduced basis for L together with bounds $C_1, C_2, \ldots$ such that:

The first basis vector, b'_1, is no more than C_1 times as long as the shortest vector in the lattice.

The second basis vector, b'_2, is within C_2 of the shortest vector independent of b'_1, etc.

Note: An LLL-reduced basis is the basis output by the LLL algorithm.

Due to properties of an LLL-reduced basis, short vectors in the lattice typically appear among the elements of the reduced basis.

In particular, the bounds C_1 can lead to proofs that there are no integer relations up to a certain size.

How to use LLL to find almost orthogonal integral vectors

Starting with a vector $v \in \mathbb{C}^n$, we pick an M that is "large".

A basis for a lattice $L \in \mathbb{C}^{n+1}$ is built by stacking an $n \times n$ identity matrix on Mv.

Applying the LLL algorithm to this lattice gives us the information needed to build w such that $|w \cdot v|$ is small.

Example: Let $r = (7 + \sqrt{5})/2$.

The minimal polynomial of r is $11 - 7x + x^2$.

This implies that $[11,\ -7,\ 1] \cdot [1,\ r,\ r^2] = 0$.

With M large, we use the lattice generated by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ M & Mr & Mr^2 \end{pmatrix}$$

continued

The small lattice vector found by the LLL algorithm is:

$$\begin{pmatrix} 11 \\ -7 \\ 1 \\ M(11 - 7r + r^2) \end{pmatrix}$$

Remember that $11 - 7r + r^2 = 0$ so this vector is pretty small.

If we use an approximation s for r then $M(11 - 7s + s^2)$ will also be small.

In other words, it is enough to use a numerical approximation for r!

Summary:
Given a vector $v \in \mathbb{C}^n$ and an $\epsilon > 0$, there is a polynomial time algorithm for producing short vectors $w \in \mathbb{Z}^n$ such that $|w \cdot v| < \epsilon$.

The w that is produced is within a known multiple of the shortest possible integral vector.

If v is a random vector and if ϵ is very small, then the expected value for $|w|$ is large.

When $|w|$ is much smaller than the expected value for a random vector, then this provides evidence that v is not random.

Application: Minimal polynomials

Problem: Find the minimal polynomial of an algebraic number $r \in \mathbb{C}$.

Solution: Form successively the vectors $v_t = [1 \ r \ r^2 \ \ldots \ r^t]$ (for larger and larger values of t) and see if there exist small vectors in the associated lattices.

Example: Let $s = 1.38583026\ ...\ 77183810$ be the first fifty digits of $r = \sqrt{7} - \sqrt[3]{2}$. We use s to find the minimal polynomial of r.

If we apply the LLL algorithm to $v = [1 \quad s \quad s^2 \quad s^3 \quad s^4 \quad s^5]$ we obtain a vector, w, which is almost orthogonal to v but whose entries are 9 digit numbers. Increasing s to 100 digits, we obtain a w whose entries are 17 digit numbers.

These are not small vectors! This suggests the minimal polynomial has degree greater than 5.

continued

Now let s be the first 50 digits of r and apply the LLL algorithm to the vector $[1,\ s,\ \ldots,\ s^6]$. We obtain

$$w = [-339, 84, 147, 4, -21, 0, 1].$$

Increasing s to 100 digits leads to the same w.

This suggests the minimal polynomial has degree 6 and is equal to

$$P(x) = -339 + 84x + 147x^2 + 4x^3 - 21x^4 + x^6.$$

Through an exact computation, we can check the answer.

Application 2: Factoring over $\mathbb{Z}[x]$

Problem 1: Factor $F \in \mathbb{Z}[x]$ as a product of irreducibles in $\mathbb{Z}[x]$.

Solution: Find a root r of F then find its minimal polynomial. Pull off this factor of F and repeat.

Application 3: Generic point on a hyperplane

Problem: Let $L = c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n \in \mathbb{Z}[x_1, \ldots, x_n]$. Given a generic point $p = (p_1, p_2, \ldots, p_n) \in V(L) \subset \mathbb{C}^n$, find $V(L)$.

Partial Solution: Note that
$p \in V(L) \iff [c_0\ c_1\ c_2\ \ldots\ c_n] \cdot [1\ p_1\ p_2\ \ldots\ p_n] = 0.$

Pick ϵ then apply the LLL algorithm to the vector $v = [1\ p_1\ p_2\ \ldots\ p_n]$ to find a vector w with $v \cdot w < \epsilon$. If $v \cdot w = 0$ then you can use w to make L.

If $v \cdot w \neq 0$ then you know p is not a generic point on any $L \in \mathbb{Z}[x_1, \ldots, x_n]$ with coefficients less than $G(\epsilon)$ (G is known).

Application 4: Generic point on a hypersurface

Problem: Let $F = a + bx + cy + dx^2 + exy + fy^2 \in \mathbb{Z}[x, y]$. Given a generic point $(p, q) \in V(F) \subset \mathbb{C}^n$, find $V(F)$.

Solution: Note that
$p \in V(F) \iff [a\ b\ c\ d\ e\ f] \cdot [1\ p\ q\ p^2\ pq\ q^2] = 0.$

Secant example

Let V be the the 2-uple embedding of $\mathbb{P}^2$ into $\mathbb{P}^5$ given by the map $[a : b : c] \to [a^2 : ab : ac : b^2 : bc : c^2]$.

It is very easy to produce a generic point, P, on the secant variety of V. Applying the LLL algorithm to the 3-uple embedding of P we obtain the polynomial

$$C^2D + AE^2 + B^2F - ADF - 2BCE.$$

This is the generator of the principal ideal corresponding to the secant variety of the Veronese variety. It is the determinant of a generic 3×3 symmetric matrix.

Why is this useful?

Mixed with RREF and generic point sampling, one can find equations for components over number fields.

Mixed with RREF and generic point sampling, one can determine the number field needed to carry out a primary decomposition.

One can, theoretically, test if a set of complex numbers, $c_1, \ldots, c_k$ are $\mathbb{Q}$-linearly independent

Exact equations for a variety can, theoretically, be recovered from knowing a numerical approximation for a single generic point on the variety.