

# Solving System of Polynomial Equations

Carlos Osco Huaricapcha

Summer 2017, Mathematics Science Research Institute

Notes written from Maurice Rojas' lectures.

---

I'd love to hear your feedback. Feel free to email me at [coscohua@mail.sfsu.edu](mailto:coscohua@mail.sfsu.edu).  
See [git:icarlitoss/msri-up](https://github.com/icarlitoss/msri-up) for updates.

# Contents

<b>1</b>	<b>Introduction, Algebraic Geometry</b>	<b>3</b>
1.1	What is it? . . . . .	3
1.2	Euler's Formula . . . . .	3
1.3	ArchNewt and Newt . . . . .	4
1.4	Backup . . . . .	4
1.4.1	Convex . . . . .	4
1.4.2	Convex Hull . . . . .	4
1.4.3	Polytope . . . . .	4
1.4.4	Correct definitions for Newt and Archnewt . . . . .	4
1.5	Univariate Trinomials . . . . .	5
<b>2</b>	<b>Archimedean Tropical Variety</b>	<b>5</b>
2.1	ArchTrop and Amoeba . . . . .	5
2.2	Vertex, Edge, and Lower Edge . . . . .	6
2.2.1	Vertex . . . . .	6
2.2.2	Edge . . . . .	6
2.2.3	Lower Edge . . . . .	6
<b>3</b>	<b>ArchTrop and Amoeba in multivariable functions</b>	<b>6</b>

# 1 Introduction, Algebraic Geometry

← June 26, 2017

## 1.1 What is it?

Ideally, Algebraic Geometry occurs over rings other than  $\mathbb{C}$ . Let's see some examples of polynomial solving.

**Example 1.1.** Let  $N = pq$  where  $N$  is a positive integer and  $p, q > 1$ . (Factoring.) Usually, we are given  $N$ , so we can find  $p$  and  $q$ .

The security of the R.S.A. Crypto-system is based on this *hardness*.

**Example 1.2.** Equilibria in Chemical Analysis systems (reaction networks).

$$\begin{array}{ll} \text{linear ordinary differential equation} \rightarrow & \dot{x} = 3x + 7 \\ \text{non-linear ordinary differential equation} \rightarrow & \dot{x} = \text{polynomial}(x) (\deg \geq 2) \end{array}$$

Differential equations govern chemical reaction rates. So, when the reaction settles down the concentrations reactions an *equilibrium*, and the concentrations wind up being *real* solutions to a system of polynomial equations. It is fair to say that *real solving* in fact makes up to more than 30% of electrical engineering.

**Example 1.3.**  $\mathbb{F}_1$ : Finite field with  $q$  elements in coding theory and cryptography. You often do arithmetic over  $\mathbb{F}_q$ , and polynomial system solving occurs very often. ( $q$ =prime power).

**Example 1.4.**  $\mathbb{Q}_p$  ( $p$ -acid reactions): This field is related to the solution of Weil-conjectures around the mid-20th century. Multiple fields medals were ensued.

Fun fact: 40% of the field medals are awarded to Algebraic Geometry.

Let's start with easy equations (1 equation, 1 variable, 2 terms,  $\mathbb{C}$ ).

**Example 1.5.** Given  $c_1, c_2 \in \mathbb{C}; a_1, a_2 \in \mathbb{Z}$ . How do we solve

$$c_1 x_1^{a_1} + c_2 x_1^{a_2} = 0$$

? Notice that it is easy to reduce to the case

$$x^d = c \quad \text{where} \quad d \in \mathbb{Z}; c \in \mathbb{C}.$$

In fact if you throw-out  $x_1 = 0$ , then we may assume  $c \neq 0$ .

## 1.2 Euler's Formula

It is easy to take  $d^{\text{th}}$  roots.

$$\exp^{\sqrt{-1}\tau} = \cos \tau + \sqrt{-1} \sin \tau.$$

**Exercise 1.** What is a simple formula for the roots of  $x_1^d = c$  using Euler's formula?

Important observation: Polynomials and polytopes are long lost siblings.

### 1.3 ArchNewt and Newt

**Definition.**  $ArchNewt(c_1x_1^{a_1} + c_2x_2^{a_2}) :=$

*Picgoeshere*

Consider the slope of this line segment (assuming  $a_1 \neq a_2$ ).

$$\frac{\log |c_2| - (-\log |c_1|)}{a_2 - a_1} = \log |\text{all the roots of } c_1x_1^{a_1} + c_2x_2^{a_2}|.$$

**Exercise 2.** Prove it.

Here is another connection: If  $f(x) = c_0 + c_1x_1 + \dots + c_dx_1^d$ , where  $d \geq 1$  is the degree then  $f$  has exactly  $d$  roots counting multiplicity. (A version of the Fundamental Theorem of Algebra “F.T.A”). This fact goes back to 1609 “P. Roth,” and 1629 “Argand.”

**Definition.**  $Newt(c_0 + c_1x_1 + \dots + c_dx_1^d) := [0, d]$ .

Ray pic goes here.

Observe:  $d = Length(Newt(...))$ .

### 1.4 Backup

#### 1.4.1 Convex

**Definition.** Given any  $S \subseteq \mathbb{R}^n$ . We say  $S$  is convex  $\iff$  for all  $x, y \in S$  the line segment connecting  $x$  and  $y$  also lies in  $S$ .

$$\{\lambda x + (1 - \lambda)y \mid \lambda \in [0, 1]\}.$$

#### 1.4.2 Convex Hull

**Definition.** Given points  $a_1, \dots, a_\tau \in \mathbb{R}^n$  their convex hull is

$$Conv(\{a_1, \dots, a_\tau\}) := \text{smallest convex set containing } a_1, \dots, a_\tau.$$

**Example 1.6.**  $Conv(\{\cdot\}) = \text{Line}$ .

In  $\mathbb{R}^3$  it is the wrapping ribbons around one point to another (?).

#### 1.4.3 Polytope

**Definition.** A polytope (in  $\mathbb{R}^n$ ) is just the convex hull of any finite point set in  $\mathbb{R}^n$ .

#### 1.4.4 Correct definitions for Newt and Archnewt

Let's think about column vectors. If  $c_1x^{a_1} + \dots + c_\tau x^{a_\tau}$  ( $c_1, \dots, c_\tau \in \mathbb{C}^*$ ) where  $X = (x_1, \dots, x_n)$  and  $X^{a_J} = x_1^{a_{1,J}}, \dots, x_n^{a_{n,J}}$ . Then,

$$\begin{aligned} Newt(f) &:= Conv(\{a_1, \dots, a_\tau\}) \\ ArchNewt(f) &:= Conv(\{(a_J, -\log |c_J|) \mid J \in \{1, \dots, \tau\}\}). \end{aligned}$$

**Exercise 3.** Find each of following:  $\text{Newt}(0)$ ,  $\text{Newt}(1 - x_1)$ ,  $\text{Newt}(1 - x_1 + x_2 + x_1x_2)$ , and  $\text{ArchNewt}(1 + 1000x_1 + x_1^3)$ .

Note:

$$\begin{aligned} \mathcal{A} &:= [a_1, \dots, a_\tau] \\ &= \begin{bmatrix} a_{1,1} & \dots & a_{1,\tau} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,\tau} \end{bmatrix} \in \mathbb{Z}^{n \times \tau} \end{aligned}$$

is called the support of  $f$ .

## 1.5 Univariate Trinomials

Let  $f(x_1) = 1 - 1000x_1^{18} + x_1^{51}$ . What can we say about the  $(\mathbb{C})$  roots?

“Physicists Approach...”:  $|x_1| \begin{cases} \text{small} \\ \text{big} \end{cases}$

When  $|x_1|$  is *small*:  $|x_1|^{18} \gg |x_1|^{51}$ . Perhaps, the roots of  $1 - 1000x_1^{18}$  are close to the roots of  $1 - 1000x_1^{18} + x_1^{51} \Rightarrow$  maybe (?) there are 18 roots of  $f$  with norm  $\sqrt[18]{\frac{1}{1000}}$  (small radius). Also, when  $|x_1|$  is *big*:  $|x_1|^{51} \gg |x_1|^{18} \Rightarrow$  maybe(?) the nonzero roots of  $1 - 1000x_1^{18} + x_1^{51}$  are near the nonzero roots of  $f$ . Perhaps,  $f$  has 33 roots of norm near  $\sqrt[33]{1000}$  (big radius).

Truth: 18 roots near inner orbit and 33 in the bigger orbit.

pic goes here of the orbits

**Exercise 4.** How close are the norms of the roots of  $f$  to the 2 approximations?

Observe:  $\text{Archnewt}(f)$  is the following graph closed by the points  $(0, 0)$ ,  $(51, 0)$ , and  $(18, -\log 1000)$ .

Graph of the triangle goes here

slope “s” of the lowets segments are close to the  $\log |\text{roots of } f|$ .

## 2 Archimedean Tropical Variety

### 2.1 ArchTrop and Amoeba

The connection between polynomials and polytopes is closely related to Tropical Geometry. Historically, the roots of the connection go back to Newton around 1676, I. Newton wrote

a letter describing how to extract power series solutions  $y = y(x)$  to polynomial equations like  $f(x, y) = 0$ .

Also, J. Hadamard around 1896, derived a version of *ArcNewt* for the power series, and observed a connection between slopes of edges and location of roots.

**Definition.** For one variable:

$$\text{ArchTrop}(f) = \text{slopes of lower edges of } \text{ArchNewt}(f).$$

**Definition.**

$$\text{Amoeba}(f) = \{\log |J| \mid J \in \mathbb{C}, f(J) = 0, J \neq 0\}.$$

**Theorem** (Avendaño, Kogan, Nisse, Rojas.(2013)). *If  $f(x_1) = c_1x^{a_1} + \dots + c_Tx^{a_T}$  then, for any  $u \in \text{Amoeba}(f)$  there is a  $v \in \text{ArchTrop}(f)$  with  $|u - v| \leq \log 3$ .*

I.e. These sets approximate each other.

**Example 2.1.** Given:  $T = 2$ (binomials). Then,  $\text{Amoeba} = 1$  point and  $\text{ArchTrop} = 1$  point.

**Example 2.2.** Given:  $T = 3$ (trinomials). Then,  $\text{Amoeba} =$  up to the degree many points.  $1 - 1000x^{18} + x^{51}$  has  $\approx 26$  points (?) . Also,  $\text{ArchTrop}(f) = 2$  points. (Include graph of numb line).

**Exercise 5.** Figure out how many points.

## 2.2 Vertex, Edge, and Lower Edge

### 2.2.1 Vertex

**Definition.** Consider minimizing  $\alpha x + \beta y$  for  $(x, y) \in P$ . If this minimum is attained at a unique point  $v$  then we call  $v$  a *vertex* of  $P$  with inner normal  $(\alpha, \beta)$ .

### 2.2.2 Edge

**Definition.** Consider minimizing  $\alpha x + \beta y$  for  $(x, y) \in P$ . If this minimum is attained at a proper subset of  $P$ (with  $\geq 2$  points) then this set is called an *edge* with inner normal  $(\alpha, \beta)$ . (Include graph of norms).

### 2.2.3 Lower Edge

**Definition.** If  $P \in \mathbb{R}^2$  is a polygon then  $E \subset P$  is a lower edge if and only if  $E$  is an edge with inner normal  $(\alpha, \beta)$  for some  $(\beta > 0)$ . (Include graph of polygon).

## 3 ArchTrop and Amoeba in multivariable functions

Consider  $f(x_1, x_2) = 1 + x_1 + x_2$ .

**Definition.** If  $f$  is any polynomial in  $x = (x_1, \dots, x_n)$  then

$$\text{Amoeba}(f) := \{(\log |J_1|, \dots, \log |J_n|) \mid f(J_1, \dots, J_n) = 0; J_1, \dots, J_n \in \mathbb{C}^*\}.$$

**Definition.**

$ArchTrop(f) := \{v \in \mathbb{R}^n \mid \text{is an inner normal to a face of } ArchNewt(f) \text{ of positive dimension}\}.$

Note: We will clarify faces and dimension in complete generality next time. For now, let's consider the *Amoeba*.

*Enterpicof Amoebahere*

Amoebae are useful because they give some intuition to begin higher dimensional zero sets.

Note:  $f(x_1, x_2)$  where  $x_1, x_2 \in \mathbb{C}$  has 2 manifold in  $\mathbb{R}^+$ .

Let's analyze why is that picture true.

$$\text{If } 1 + x_1 + x_2 = 0 \text{ then } \begin{cases} x_1 + x_2 = -1 & \Rightarrow |x_1 + x_2| = 1 & (i) \\ x_1 = -1 - x_2 & \Rightarrow |x_1| = |1 - x_2| & (ii) \\ x_2 = -1 - x_1 & \Rightarrow |x_2| = |1 + x_1| & (iii) \end{cases}$$

So  $u := |x_1|, v := |x_2|$  implies that

$$\begin{aligned} 1 &\leq u + v \\ u &\leq 1 + v \\ v &\leq 1 + u. \end{aligned}$$

So  $(u, v) \in$

Show graph of the rect in diag

then by taking the log of the figure, we would obtain the  $Amoeba(1+x_1+x_2) = (\log |J_1|, \log |J_2|).$

Show graph of Amoeba

Q&A: What is the relation of the product  $fg$  with  $Newt(fg)$  and  $ArchNewt(fg)$ .

$$\begin{aligned} Newt(fg) &= Newt(f) + Newt(g) \\ ArchNewt(fg) &= \dots :: \text{mess} :: \dots \end{aligned}$$

It is a mess because  $ArchNewt((1+x)^3) \neq 3ArchNewt(1+x).$