

CS 829

Polynomial systems: geometry and algorithms

Lecture 8: Univariate root-finding

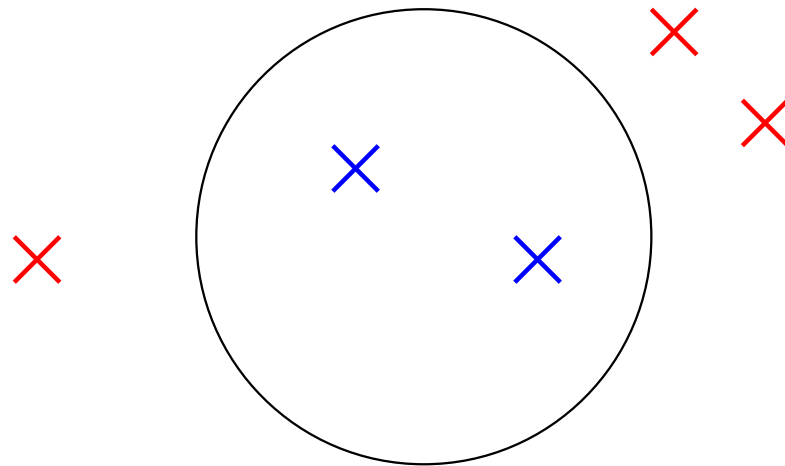
Éric Schost

eschost@uwo.ca

The main idea

Basic idea: split the polynomial F into two factors $F = PQ$ and continue on P and Q , until all factors are linear.

How: find a circle that contains some roots (but not all of them) and split the polynomial along this circle.



Basic tools: residue theorem, Gräffe iteration and Newton iteration.

Preamble on precision

Real numbers will be approximated by floating-point numbers of the form

$$\pm a \cdot 2^e,$$

with $a \geq 0$ and e an integer. Complex numbers use two floating-point numbers.

Remark. If a, b satisfy

$$|a - b \cdot 2^f| \leq \frac{1}{2^s} |a|,$$

then b should have approximately s bits.

Input / output

Input.

- Let F be of degree n in $\mathbb{C}[X]$, and let s_0 be our target precision.
- The norm $|A|$ of a polynomial A is the sum of the sum of the norm of its coefficients.

The algorithm computes **linear factors** L_1, \dots, L_n such that

$$|F - L_1 \cdots L_n| \leq 2^{-s_0} |F|.$$

Input / output

Input.

- Let F be of degree n in $\mathbb{C}[X]$, and let s_0 be our target precision.
- The norm $|A|$ of a polynomial A is the sum of the sum of the norm of its coefficients.

The algorithm computes **linear factors** L_1, \dots, L_n such that

$$|F - L_1 \cdots L_n| \leq 2^{-s_0} |F|.$$

Remark: from this, one can deduce approximations of the roots as well, but this is not straightforward!

- If F has all its root of norm ≤ 1 and has been factored with error 2^{-s_0} , then the roots of the L_i approximate those of F with error $\simeq 2^{-s_0/n}$.
- So we should take a precision $\simeq s_0 n$ in the factoring if we want roots with error s_0 .

Overview of the algorithm

Suppose that we know a factorization

$$|F - F_1 \cdots F_k| \leq \frac{k}{n} 2^{-s_0} |F|.$$

The main task will be to factor any polynomial F_i into **two** factors P, Q such that

$$|F_i - PQ| \leq \frac{1}{n} 2^{-s_0 - n} |F_i|.$$

Then

$$|F - PQF_2 \cdots F_k| \leq \frac{k+1}{n} 2^{-s_0} |F|.$$

We are left with the problem of factoring a polynomial into two factors, with relative precision $s_0 + n + \lceil \log n \rceil$.

Costs

0. The $O\tilde{}$ notation means that we neglect logarithmic factors.
1. Polynomials of degree n and norm ≤ 1 can be multiplied or divided with error $\leq 2^{-s}$ in $O\tilde{}(ns)$ word operations.
2. The cost of factoring into **two** factors at precision $s \simeq s_0 + n$ will be in $O\tilde{}(n^3 + ns_0)$.
3. Hence the cost of factoring into **linear** factors at precision s_0 will be in $O\tilde{}(n^4 + n^2s_0)$.

Basic formulas

Roots and coefficients

1. Let

$$F = f_n X^n + \cdots + f_1 X + f_0 = f_n (X - a_1) \cdots (X - a_n).$$

Then

$$\frac{f_{n-1}}{f_n} = -(a_1 + \cdots + a_n), \quad \dots, \quad \frac{f_0}{f_n} = (-1)^n a_1 \cdots a_n.$$

Roots and coefficients

1. Let

$$F = f_n X^n + \cdots + f_1 X + f_0 = f_n (X - a_1) \cdots (X - a_n).$$

Then

$$\frac{f_{n-1}}{f_n} = -(a_1 + \cdots + a_n), \quad \dots, \quad \frac{f_0}{f_n} = (-1)^n a_1 \cdots a_n.$$

2. Suppose $f_0 \neq 0$. The **reciprocal polynomial** of F is

$$\text{rec}(F) = X^n F\left(\frac{1}{X}\right) = f_0 X^n + \cdots + f_{n-1} X + f_n.$$

Its roots are

$$\frac{1}{a_1}, \quad \dots, \quad \frac{1}{a_n}.$$

Bounds and norms

1. We write

$$R_n(F) \geq R_{n-1}(F) \geq \cdots \geq R_1(F)$$

for the norms of the roots of F .

Bounds and norms

1. We write

$$R_n(F) \geq R_{n-1}(F) \geq \cdots \geq R_1(F)$$

for the norms of the roots of F .

2. The **norm** of the polynomial F is

$$|F| = |f_0| + \cdots + |f_n|.$$

The norm is **not** multiplicative:

$$|PQ| \leq |P| |Q| \quad \text{but} \quad |P| |Q| \leq 2^{\deg(P)+\deg(Q)} |PQ|.$$

Finding the roots' norms

Graeffe's iteration

Let $F = f_d \prod_{i=1}^d (X - a_i)$. The Graeffe transform of F is

$$G(F) = f_d^2 \prod_{i=1}^d (X - a_i^2),$$

i.e., the roots are squared.

Graeffe's iteration

Let $F = f_d \prod_{i=1}^d (X - a_i)$. The Graeffe transform of F is

$$G(F) = f_d^2 \prod_{i=1}^d (X - a_i^2),$$

i.e., the roots are squared.

Prop.

$$\begin{aligned} F(X)F(-X) &= f_d^2 \prod_{i=1}^d (X - a_i)(-X - a_i) \\ &= (-1)^d f_d^2 \prod_{i=1}^d (X - a_i)(X + a_i) \\ &= (-1)^d f_d^2 \prod_{i=1}^d (X^2 - a_i^2) \\ &= (-1)^d G_F(X^2) \end{aligned}$$

Corollary: cost $M(d) + O(d)$ operations in the base ring.

When taking precision into account, this becomes $O^\sim(ds)$ **word** operations.

Finding the roots' norms

Suppose as in the demo that

$$F = X^3 + f_2X^2 + f_1X + f_0 = (X - a_1)(X - a_2)(X - a_3),$$

with $|a_1| > |a_2| > |a_3|$. Then the m th iterate of Graeffe's transform gives

$$X^3 + f_2^{(m)}X^2 + f_1^{(m)}X + f_0^{(m)} = (X - a_1^{2^m})(X - a_2^{2^m})(X - a_3^{2^m}).$$

Finding the roots' norms

Suppose as in the demo that

$$F = X^3 + f_2 X^2 + f_1 X + f_0 = (X - a_1)(X - a_2)(X - a_3),$$

with $|a_1| > |a_2| > |a_3|$. Then the m th iterate of Graeffe's transform gives

$$X^3 + f_2^{(m)} X^2 + f_1^{(m)} X + f_0^{(m)} = (X - a_1^{2^m})(X - a_2^{2^m})(X - a_3^{2^m}).$$

So we get

$$f_2^{(m)} = a_1^{2^m} + a_2^{2^m} + a_3^{2^m} \simeq a_1^{2^m}.$$

Next,

$$f_1^{(m)} = a_1^{2^m} a_2^{2^m} + a_1^{2^m} a_3^{2^m} + a_2^{2^m} a_3^{2^m} \simeq a_1^{2^m} a_2^{2^m},$$

so

$$f_1^{(m)} / f_2^{(m)} \simeq a_2^{2^m}.$$

Finally,

$$f_0^{(m)} = a_1^{2^m} a_2^{2^m} a_3^{2^m} \quad \text{so} \quad f_0^{(m)} / f_1^{(m)} \simeq a_3^{2^m}.$$

Finding the roots' norms

There are issues:

- the speed of convergence is hard to control,
- the formulas break down when several roots have the same norm.

We use a similar scheme that makes convergence guaranteed.

Basic tool: Given a polynomial F , compute a real ρ such that

$$a \leq R_k(F(\rho X)) \leq b$$

for some constants a, b .

Details later; we first see how to use it.

A better Graeffe

0. $P_0 = P$

$$Q_0 = P_0(\rho_0 X)$$

1. $P_1 = G(Q_0)$

$$Q_1 = P_1(\rho_1 X)$$

...

t. $Q_r = P_t(\rho_r X)$

$$R_k(P) = R_k(P_0)$$

$$R_k(P) = \rho_0 R_k(Q_0)$$

$$R_k(P) = \rho_0 R_k(P_1)^{1/2}$$

$$R_k(P) = \rho_0 \rho_1^{1/2} R_k(Q_1)^{1/2}$$

...

$$R_k(P) = \rho_0 \rho_1^{1/2} \cdots \rho_r^{1/2^t} R_k(Q_r)^{1/2^t}$$

A better Graeffe

$$0. P_0 = P$$

$$R_k(P) = R_k(P_0)$$

$$Q_0 = P_0(\rho_0 X)$$

$$R_k(P) = \rho_0 R_k(Q_0)$$

$$1. P_1 = G(Q_0)$$

$$R_k(P) = \rho_0 R_k(P_1)^{1/2}$$

$$Q_1 = P_1(\rho_1 X)$$

$$R_k(P) = \rho_0 \rho_1^{1/2} R_k(Q_1)^{1/2}$$

...

...

$$t. Q_r = P_t(\rho_r X)$$

$$R_k(P) = \rho_0 \rho_1^{1/2} \cdots \rho_r^{1/2^t} R_k(Q_r)^{1/2^t}$$

Since $R_k(Q_t)$ is in $[a, b]$, we can choose t such that $(b - a)^{1/2^t}$ is close to 1.

Suppose that we want r such that $re^{-\tau} \leq R_k(P) \leq re^{\tau}$, for some $\tau \in [0, 1]$. We expect $t \simeq \log 1/\tau$.

For $\tau \simeq 1/n$, taking all precisions into account leads to a cost of $\tilde{O}(n^2)$ word operations, whence $\tilde{O}(n^3)$ for all R_k .

Root bounds

1. Upper bound. Let $F = f_n X^n + \cdots + f_1 X + f_0$ be such that for all m ,

$$|f_{n-m}| \leq 2^{nm} |f_n|.$$

Then $R_n(F) \leq 4n$.

This is true in particular if $|f_{n-m}| \leq 2^m \binom{n}{m} |f_n|$.

Root bounds

1. Upper bound. Let $F = f_n X^n + \cdots + f_1 X + f_0$ be such that for all m ,

$$|f_{n-m}| \leq 2^{nm} |f_n|.$$

Then $R_n(F) \leq 4n$.

This is true in particular if $|f_{n-m}| \leq 2^m \binom{n}{m} |f_n|$.

2. Lower bound. Let $F = f_n X^n + \cdots + f_1 X + f_0$ be such that for some m ,

$$|f_{n-m}| \geq \binom{n}{m} |f_n|.$$

Then $R_n(F) \geq 1$.

Proof. f_{n-m}/f_n is the sum of $\binom{n}{m}$ terms, each of which is a product of $n - m$ roots.

Hence, $|f_{n-m}| \leq \binom{n}{m} R_n(F)^{n-m} |f_n|$.

Using the root bounds

For $F = f_n X^n + \cdots + f_1 X + f_0$, we define an integer β by

$$\beta = \log \max_m \left[\frac{1}{m} \left| \frac{a_{n-m}}{a_n} \frac{1}{\binom{n}{m}} \right| \right]. \quad (1)$$

Write

$$G = F(2^\beta X) = g_n X^n + \cdots + g_1 X + g_0.$$

Then:

$$|g_{n-m}| \leq 2^m \binom{n}{m} |g_n| \quad \text{and} \quad |g_{n-m_0}| \geq \binom{n}{m_0} |g_n|$$

for the m_0 that reaches the max in (2).

Using the root bounds

For $F = f_n X^n + \cdots + f_1 X + f_0$, we define an integer β by

$$\beta = \log \max_m \left[\frac{1}{m} \left| \frac{a_{n-m}}{a_n} \frac{1}{\binom{n}{m}} \right| \right]. \quad (2)$$

Write

$$G = F(2^\beta X) = g_n X^n + \cdots + g_1 X + g_0.$$

Then:

$$|g_{n-m}| \leq 2^m \binom{n}{m} |g_n| \quad \text{and} \quad |g_{n-m_0}| \geq \binom{n}{m_0} |g_n|$$

for the m_0 that reaches the max in (2).

Hence (upper / lower bounds):

$$1 \leq R_n(G) \leq 4n.$$

More complicated techniques work for all R_k .

The easy case

Basic case distinction

Let F have degree n . We distinguish three cases:

1. The roots are all **small**, *i.e.*

$$R_n(F) \leq 2.$$

2. The roots are all **large**, *i.e.*

$$R_1(F) \geq \frac{1}{2}.$$

This says that the roots of the reciprocal polynomial $\text{rec}(F)$ are all small, so this is similar to case **1**.

3. Some roots are **small** and some are **large**, *i.e.*

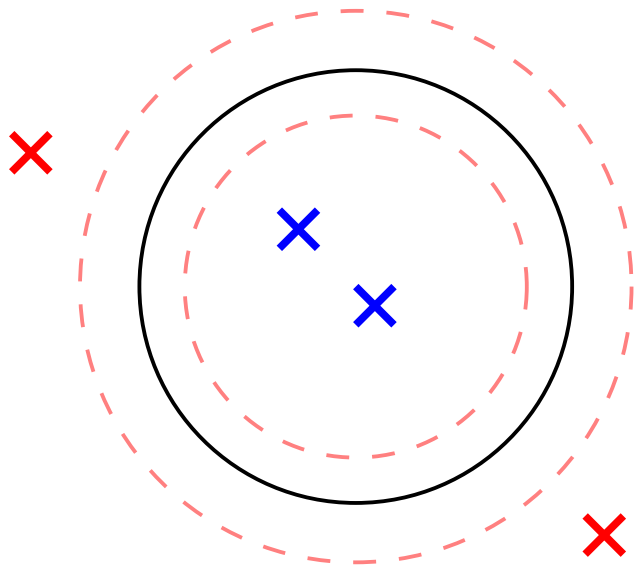
$$R_1(F) \leq \frac{1}{2} \quad \text{and} \quad R_n(F) \geq 2.$$

The roots are well-spread, this is the **nice case**.

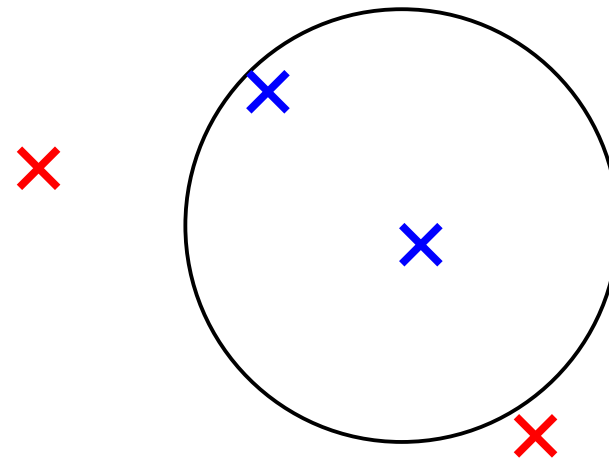
Requirements

We want to find an area of the complex plane that contains some, but not all of the roots, of the input polynomial F .

For numerical stability, we also want this circle to **separate** the roots.



GOOD



BAD

The case of well-spread roots

1. Compute the norms $r_1 \leq \dots \leq r_n$ of all the roots.

Remark: Computing them with error $e^{1/10n}$ would be enough.

2. Compute all ratios $h_i = r_i/r_{i-1}$. One of them (of index i_0) has to be at least $4^{1/(n-1)}$.

Proof. The product $h_2 \cdots h_n = r_n/r_1$ is at least 4.

3. Define $\rho = \sqrt{r_{i_0-1}r_{i_0}}$. Then there is no zero in the annulus

$$\left\{ z \mid \frac{\rho}{4^{1/(2n-2)}} \leq |z| \leq \rho 4^{1/(2n-2)} \right\}.$$

The circle $|z| = \rho$ is our **splitting circle**.

Remark: If the r_i are known up to some error we get similar results with factors of the form $4^{9/10(2n-2)}$.

The case of well-spread roots

By replacing $F(X)$ by $F(\rho X)$, we can assume that the splitting circle is the unit circle $|z| = 1$.

The separation bounds remain the same, up to a constant factor.

Next steps:

- Compute a rough factorization $F = PQ$, where P gathers the roots of norm < 1 and Q those of norm > 1 .

Residue theorem, Newton formulas.

- Refine the factorization to higher precision.

Newton iteration.

Newton sums

A review of Newton sums

Let F in $\mathbb{K}[X]$ (monic for simplicity). There are close connexions between:

- the **coefficients** of F :

$$F = T^d + f_{d-1}X^{d-1} + \cdots + f_0.$$

- the **Newton sums** S_1, S_2, \dots of F :

$$S_i = \sum_{F(x)=0} x^i, \quad \text{summing on all roots of } F \text{ (with multiplicities).}$$

Theorem. Let $\text{rec}(F)$ be the reciprocal polynomial of F :

$$\text{rec}(F) = 1 + f_{d-1}X + \cdots + f_0X^d.$$

Then the Taylor expansion of

$$\frac{\text{rec}(F)'}{\text{rec}(F)} \text{ is } - \sum_{i \geq 0} S_{i+1} X^i.$$

Conversion algorithms

Suppose that $1, 2, \dots, d$ can be inverted in \mathbb{K} .

Corollary (slow). Given **the first d Newton sums**, the coefficients can be computed using Newton relations:

$$if_{d-i} + S_1 f_{d-i+1} + \cdots + S_i = 0.$$

Complexity: $O(d^2)$.

Corollary (fast). Given **the first d Newton sums**, the coefficients can be computed using power series exponentiation:

$$\text{rec}(F) = \exp \left(- \int \sum_{i \geq 0} S_{i+1} X^i \right).$$

Complexity: $O(M(d))$.

The initial factorization

Residues

Let $F(X) = P(X)/Q(X)$ be in $\mathbb{C}(X)$. Around 0, F can be written

$$F(X) = \frac{f_{-d}}{X^d} + \cdots + \frac{f_{-1}}{X} + f_0 + f_1X + \cdots$$

The **residue** of F at 0 is f_{-1} .

More generally:

- a **pole** of F is a root of Q ;
- the **residue** of F at a pole c is the coefficient of $1/(X - c)$ in the expansion around c .

Example:

- The residue of $X^i/(X - c)$ at c is c^i .

Proof: $X^i/(X - c) = P(X) + c^i/(X - c)$.

The residue theorem

Theorem. Let $F(X) = P(X)/Q(X)$, and let γ be a curve (with no self-intersection). Then

$$\frac{1}{2i\pi} \int_{\gamma} F(z) dz = \sum_j \text{residue}(F, a_j),$$

where a_j are the poles of F **inside** the region delimited by γ .

The residue theorem

Theorem. Let $F(X) = P(X)/Q(X)$, and let γ be a curve (with no self-intersection). Then

$$\frac{1}{2i\pi} \int_{\gamma} F(z) dz = \sum_j \text{residue}(F, a_j),$$

where a_j are the poles of F **inside** the region delimited by γ .

Particular case: $F(X) = X^m P'(X)/P(X)$, for some $P = \prod (X - a_i)$. Then

$$X^m \frac{P'(X)}{P(X)} = \sum_i \frac{X^m}{X - a_i}$$

So the integral $\frac{1}{2i\pi} \int_{\gamma} F(z) dz$ is the sum

$$\sum_j a_j^m,$$

for all a_j inside the region delimited by γ .

Application to factoring

Let $F = PQ$, where P has its roots in the **unit circle** γ , and Q has its roots out of it.

The integrals

$$S_m = \frac{1}{2i\pi} \int_{\gamma} z^m \frac{F'(z)}{F(z)} dz$$

are the **Newton sums** of P .

Application to factoring

Let $F = PQ$, where P has its roots in the **unit circle** γ , and Q has its roots out of it.

The integrals

$$S_m = \frac{1}{2i\pi} \int_{\gamma} z^m \frac{F'(z)}{F(z)} dz$$

are the **Newton sums** of P .

These integrals will be **discretized**:

$$S_m \simeq \frac{1}{N} \sum_{k=0}^{N-1} e^{\frac{2i\pi k(m+1)}{N}} \frac{P'(e^{\frac{2i\pi k}{N}})}{P(e^{\frac{2i\pi k}{N}})} = \mathfrak{S}_{N,m},$$

which can be computed by Discrete Fourier Transform.

How large should we take N ?

Norm estimates

Suppose (we can!) that $|F| = 1$ and let $\mu = \min_{z \in \gamma} |F(z)|$. For the subsequent lifting, we need an estimate of the form

$$|F - P_0 Q_0| \leq \varepsilon = \frac{\mu^4}{n^4 16^n}. \quad (3)$$

Prop. Suppose that we find P_0 such that

$$|P_0 - P| \leq \frac{1}{2} \frac{\mu^5}{n^5 32^n}.$$

Let Q_0 be the quotient in the Euclidean division of F by P_0 . Then we have

$$|F - P_0 Q_0| \leq \varepsilon,$$

and P_0 has all its roots inside γ .

Precision

1. Suppose that P has no root in the annulus

$$\{z \mid e^{-\delta} \leq |z| \leq e^{\delta}\},$$

Then one has

$$|\mathfrak{S}_{N,m} - S_m| \leq n \frac{e^{-\delta N - \delta m} + e^{-\delta N + \delta m}}{1 - e^{-\delta N}}.$$

2. If we reconstruct P_0 from the $\mathfrak{S}_{N,m}$, it suffices to take

$$N \simeq \frac{n + \log 1/\mu}{\delta}$$

to ensure that the inequality in (3) holds.

Complexity

0. One shows that doing the computations with a precision of approximately

$$n + \log \frac{1}{\mu} \text{ bits}$$

is sufficient.

1. Remember that

$$\delta \simeq \frac{1}{n}.$$

2. The minimum μ satisfies

$$\log \frac{1}{\mu} \lesssim n \log n$$

We deduce that $N \simeq n^2 \log n$ suffices. Using Fast Fourier Transform, this gives a cost of $O^\sim(n^3)$.

Lifting techniques for factorization

p -adic factorization

Let $F = X^4 - 2X^3 + 9X^2 - 8X + 20$ be in $\mathbb{Z}[X]$.

Factorization mod 5. Modulo $p = 5$, we have

$$F \equiv X(X + 1)(X + 3)(X + 4) \pmod{5}.$$

Lifting. Lifting modulo the powers of 5, we successively get

- $F \equiv (X + 10)(X + 11)(X + 13)(X + 14) \pmod{5^2}$
- $F \equiv (X + 260)(X + 261)(X + 363)(X + 364) \pmod{5^4}$
- $F \equiv (X + 220885)(X + 220886)(X + 169738)(X + 169739) \pmod{5^8}$

p -adic factorization

Let $F = X^4 - 2X^3 + 9X^2 - 8X + 20$ be in $\mathbb{Z}[X]$.

Factorization mod 5. Modulo $p = 5$, we have

$$F \equiv X(X + 1)(X + 3)(X + 4) \pmod{5}.$$

Lifting. Lifting modulo the powers of 5, we successively get

- $F \equiv (X + 10)(X + 11)(X + 13)(X + 14) \pmod{5^2}$
- $F \equiv (X + 260)(X + 261)(X + 363)(X + 364) \pmod{5^4}$
- $F \equiv (X + 220885)(X + 220886)(X + 169738)(X + 169739) \pmod{5^8}$

Factorization in $\mathbb{C}[X]$ is similar (finding low-precision factors / refining them).

- The low-precision factorization are completely different in the p -adic / complex approaches.
- The lifting works similarly.

Lifting a factorization

let F be monic in $\mathbb{Z}[X]$, let p be a prime and let $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ (this is a field!).

Suppose that one knows a factorization

$$F \bmod p = PQ,$$

with P, Q coprime in $\mathbb{K}[X]$. Then one can deduce a factorization of F modulo any power of p that refines the previous one.

Another example. From the factorization

$$(X^2 + X + 1) = (X + 3)(X + 5) \bmod 7,$$

one can deduce

$$(X^2 + X + 1) = (X + 22143577275619761)(X + 57648689021992241) \bmod 7^{20}.$$

The basic lifting step $p \rightarrow p^2$

We can see all the previous objects in $\mathbb{Z}/p^2\mathbb{Z}[X]$, so that

$$F - PQ = R \quad \text{in } \mathbb{Z}/p^2\mathbb{Z}[X],$$

where R has all its coefficients multiple of p .

We look for

$$P^+ = P + \delta P \quad \text{and} \quad Q^+ = Q + \delta Q$$

with $\delta P, \delta Q$ unknown, having all their coefficients multiple of p .

The basic lifting step $p \rightarrow p^2$

We can see all the previous objects in $\mathbb{Z}/p^2\mathbb{Z}[X]$, so that

$$F - PQ = R \quad \text{in } \mathbb{Z}/p^2\mathbb{Z}[X],$$

where R has all its coefficients multiple of p .

We look for

$$P^+ = P + \delta P \quad \text{and} \quad Q^+ = Q + \delta Q$$

with $\delta P, \delta Q$ unknown, having all their coefficients multiple of p .

Then

$$F - P^+Q^+ = F - (P + \delta P)(Q + \delta Q) = R - Q\delta Q - Q\delta P \quad \text{mod } p^2.$$

So we need to solve

$$P\delta Q + Q\delta P = R.$$

Solvability of linear equations

Prop. Let A be of degree less than $\deg(P) + \deg(Q)$ such that $A = 0 \pmod{P}$ and $A = 0 \pmod{Q}$ in $\mathbb{Z}/p^2\mathbb{Z}[X]$. Then $A = 0$.

Lemma. The Sylvester matrix of P, Q is invertible modulo p^2 .

Proof. It is invertible modulo p , so it is also invertible modulo p^2 (lifting of inverses).

Proof.

- $A = 0 \pmod{P} \implies A = \alpha P, \deg(\alpha) < \deg(Q)$.
- $A = 0 \pmod{Q} \implies A = \beta Q, \deg(\beta) < \deg(P)$.

So $\alpha P - \beta Q = 0$, and since the Sylvester matrix of P, Q is invertible, $\alpha = \beta = 0$.

Solving our linear equations

Let U, V in $\mathbb{Z}/p\mathbb{Z}[X]$ be such that $UP + VQ = 1$. Hence,

$$UP + VQ = 1 + S \quad \text{in} \quad \mathbb{Z}/p^2\mathbb{Z}[X],$$

where S is a multiple of p . Define

$$\delta Q = UR \bmod Q \quad \text{and} \quad \delta P = VR \bmod P.$$

Solving our linear equations

Let U, V in $\mathbb{Z}/p\mathbb{Z}[X]$ be such that $UP + VQ = 1$. Hence,

$$UP + VQ = 1 + S \quad \text{in} \quad \mathbb{Z}/p^2\mathbb{Z}[X],$$

where S is a multiple of p . Define

$$\delta Q = UR \bmod Q \quad \text{and} \quad \delta P = VR \bmod P.$$

Then $P\delta Q + Q\delta P - R \bmod P$ is given by

$$Q\delta P - R = QVR - R = (1 + S)R - R = 0,$$

where the last identity follows from $RS = 0$ modulo p^2 . Similarly, $P\delta Q + Q\delta P - R \bmod Q = 0$, so $P\delta Q + Q\delta P - R = 0$.

Solving our linear equations

Let U, V in $\mathbb{Z}/p\mathbb{Z}[X]$ be such that $UP + VQ = 1$. Hence,

$$UP + VQ = 1 + S \quad \text{in} \quad \mathbb{Z}/p^2\mathbb{Z}[X],$$

where S is a multiple of p . Define

$$\delta Q = UR \bmod Q \quad \text{and} \quad \delta P = VR \bmod P.$$

Then $P\delta Q + Q\delta P - R \bmod P$ is given by

$$Q\delta P - R = QVR - R = (1 + S)R - R = 0,$$

where the last identity follows from $RS = 0$ modulo p^2 . Similarly, $P\delta Q + Q\delta P - R \bmod Q = 0$, so $P\delta Q + Q\delta P - R = 0$.

This gives us P^+ and Q^+ . To conclude, we need to compute U^+ and V^+ such that $U^+P^+ + V^+Q^+ = 1$. This is done by lifting inverses, as usual.

Refining the factorization

In the numerical world

Suppose that we know a factorization $F \simeq PQ$, for $F, P, Q \in \mathbb{C}[X]$ as before. We want to refine it to arbitrary precision.

Input. We suppose that P has all its roots inside γ and that

$$|F - PQ| \leq \varepsilon,$$

where ε satisfies

$$\varepsilon = \frac{\mu^4}{16^n n^4}, \quad \text{with} \quad \mu = \min_{z \in \gamma} |F(z)|.$$

Algorithm: the same as before:

- compute (and update) the inverse of P modulo Q (and conversely);
- replace $F \simeq PQ$ by $F \simeq P^+Q^+$, computed by the same formulas:

$$P^+ = P + \delta P \quad \text{and} \quad Q^+ = Q + \delta Q \quad \text{s.t.} \quad F - P^+Q^+ = \delta P\delta Q.$$

Locating the roots

Rouché's Theorem. If two polynomials $A(X), B(X)$ satisfy

$$|A(z)| < |B(z)|$$

for all $z \in \gamma$, then A and $A + B$ have the same number of roots inside γ .

Corollary. With $A = PQ - F$ and $B = F$, we get that PQ and F have the same number of roots inside γ .

Corollary. Q has all its roots outside of γ , and in particular, P and Q are coprime.

Convergence analysis

1. δP is small. From the integral formula

$$\delta P(z) = \frac{1}{2i\pi} \int_{\gamma} \frac{F(t) - P(t)Q(t)}{P(t)Q(t)} \frac{P(t) - P(z)}{t - z} dt,$$

we get $|\delta P| \leq \frac{8}{7} \frac{\varepsilon}{\mu} n |P|$.

2. δQ is small. From the equation $F - PQ = P\delta Q + Q\delta P$, we get bounds on $|P|^2 |\delta Q|$.

$$|P^2 \delta Q| \leq \varepsilon |P| \left(1 + \frac{9}{7} \frac{n}{\mu}\right).$$

3. $\delta Q \delta Q$ is small. We deduce an upper bound on $|P^2| |\delta Q|$ (introducing a factor 4^n) and simplify to get

$$|\delta P \delta Q| \leq |\delta P| |\delta Q| \leq \varepsilon^2 \frac{n^2 4^n}{\mu^2} \leq \varepsilon^{1.5}.$$

4. **Bonus.** Applying Rouché's theorem to $Q(P + \delta P)$ and QP , we deduce that $P + \delta P$ has all its roots inside γ .

Complexity analysis

0. We start from a factorization having precision $\log \frac{1}{\varepsilon} \simeq n + \log \frac{1}{\mu}$.
1. We iterate the process until $\varepsilon^{1.5t} = 2^{-s}$, so $t \simeq s$.
2. As before, we need extra precision to deal with rounding errors: we replace s by $s + n + \log \frac{1}{\mu}$.
This does not affect the complexity much!
3. The ℓ th lifting step involves multiplications of polynomials in degree n , having coefficients of precision $2^\ell (n + \log \frac{1}{\mu})$.

Putting things together, we get a complexity of $O^\sim(n^2 + ns)$ word operations.

The hard case

Scaling and shifting

Let $F(X) = f_d X^d + \dots + f_1 X + f_0$.

Shifting: $F(X) \rightarrow F(X + c)$. $F(X + c) = \sum_{i \leq d} f_i (X + c)^i$. Naive cost: $O(d^2)$.

The coefficient of X^k in $(X + c)^i$ is $\frac{i!}{k!(i-k)!} c^{i-k}$, so

$$F(X + c) = \sum_{k \leq d} \sum_{i \leq k} f_i \frac{i!}{k!(i-k)!} c^{i-k} X^k = \sum_{k \leq d} \sum_{i=k}^d f_i i! c^i \frac{1}{(i-k)!} \frac{X^k}{c^k k!}.$$

$\sum_{i=k}^d f_i i! c^i \frac{1}{(i-k)!}$ is the coefficient of X^{d-k} in the product

$$\sum_{i=0}^d f_{d-i} (d-i)! c^{d-i} X^i \times \sum_{i=0}^d \frac{1}{i!} X^i \quad (\star)$$

so the total cost is $M(d)$ (for (\star)) $+O(d)$ (for computing the $c^k, k!, \dots$)

A first center

1. **Scaling.** Reduce the maximal root norm to $\leq 1/2$.

2. **Moving the center.** Given $F = f_n X^n + \cdots + f_0$, we move the **barycenter** of the roots to the origin:

$$G(X) = F\left(X - \frac{1}{n} \frac{f_{n-1}}{f_n}\right).$$

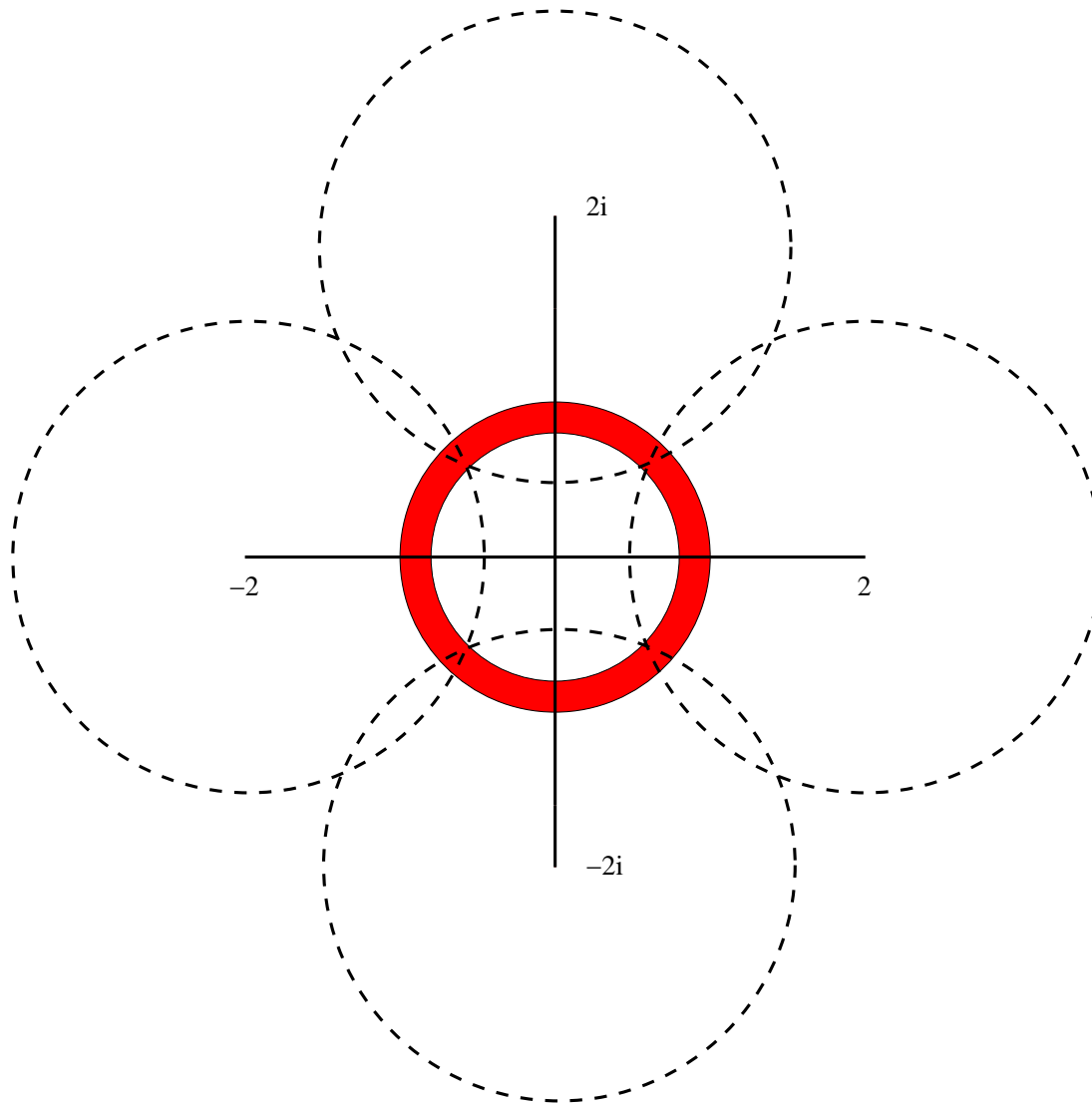
Then,

$$G(X) = g_n X^n + g_{n-2} X^{n-2} + \cdots + g_0,$$

with $g_n = f_n$. Hence, the sum of the roots of G is 0.

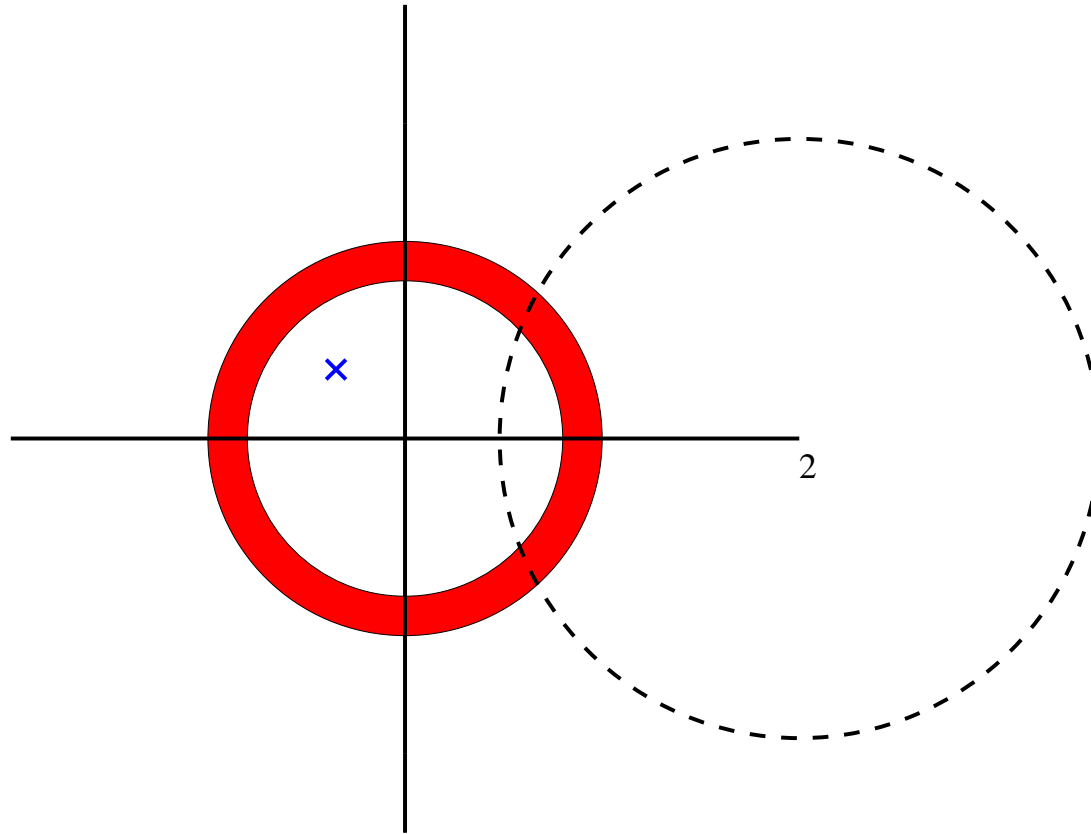
3. **Scaling.** Increase the maximal root norm to $0.99 \leq R_n(G) \leq 1$.

Four candidates



The red annulus $0.99 \leq |z| \leq 1$ contains a root, so one of the large circle does.

The good candidate



Suppose this is the one centered at 2. Then there **has to be** a root of abscissa < 0 .

Shifting the origin at 2, this tells us that there is a root of norm < 1.48 and another one of form > 2 .

So we are back to the nice case!