Efficiently finding roots of univariate polynomials over $\mathbb{C}$.

Polynomial $P(x)$ of degree d, coefficients in $\mathbb{Z}$, each coefficient is at most t bits.

Goal: find all roots $\alpha \in \mathbb{C}$ within n bits of precision. (within $\pm 2^{-n}$ error).

Ideal Running time: poly (d, n, t).

Schönhage '85: Can do it.

First How big can the roots be?

If $P(x) = \sum_{i=0}^{d} a_i x^i$

and each $a_i \in \mathbb{Z}$

with $|a_i| \le 2^t$, and

$P(\alpha) = 0$, then

$$|\alpha| \le \quad .$$

If $\alpha > 1$,

$$|a_0 \alpha^d| \le \sum_{i=0}^{d-1} a_i \alpha^i$$

$$\alpha^d \le \frac{|\sum a_i \alpha^i|}{|a_0|}$$

$$\le \frac{\sum |a_i| |\alpha|^i}{|a_0|}$$

$$\le \left(\frac{\sum |a_i|}{|a_0|}\right) \cdot \left(d\, |\alpha|^{d-1}\right)$$

$$|\alpha| \le d \cdot \frac{\sum |a_i|}{|a_0|} \le d \cdot \sum |a_i| .$$

Lemma Suppose $\prod (X - \alpha_i) = X^d - s_1 X^{d-1} + s_2 X^{d-2}$

$\pm s_d$

then $\max_i |\alpha_i| = \Theta_d\left(\max_j |s_j|^{1/j}\right)$

$\leq O(d \cdot \downarrow)$

$\geq \Omega\left(\frac{1}{d} \cdot \downarrow\right)$

Let $\alpha_1, \ldots \alpha_d$ be the roots.

Then if $a = \max_i |\alpha_i|$

then $|s_j| \leq \binom{d}{j} a^j$

$$|s_j|^{1/j} \leq \frac{ed}{j} \cdot a$$

$$\leq ed \cdot a.$$

So $\max_i |\alpha_i| \geq \Omega\left(\frac{1}{d} \cdot \max_j |s_j|^{1/j}\right)$

For any root α

$$\alpha^d - s_1 \alpha^{d-1} + s_2 \alpha^{d-2} \cdots = 0.$$

Want to show:

$$|\alpha| \le \max_j |s_j|^{1/j}$$

—

$$|\alpha|^d \le \sum_j |s_j| \, |\alpha|^{d-j}$$

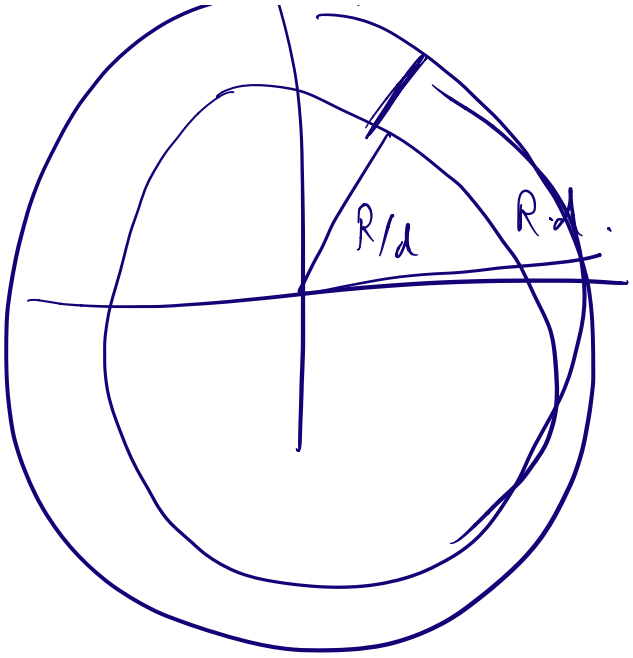
$$1 \le \left(\max_j \frac{|s_j|}{|\alpha|^j} \right) \cdot d$$

$\exists j_0$ s.t. $\frac{|s_{j_0}|}{|\alpha|^{j_0}} \ge \frac{1}{d}$.

$$|s_{j_0}|^{1/j_0} \ge \frac{|\alpha|}{d^{1/j_0}} \ge \frac{|\alpha|}{d}$$

So $|\alpha| \le \left(d \cdot \max_j |s_j|^{1/j} \right)$

—



Start with $P(X)$. Let roots be $\alpha_1, \ldots \alpha_d$

$a_0 \neq 0$, $a_d \neq 0$

$$P(X) = \sum_{i=0}^{d} a_i X^i$$

$$\tilde{P}(X) = \sum_{i=0}^{d} a_{d-i} X^i$$ (reciprocal poly).

Roots of $\tilde{P}(X)$ are $\frac{1}{\alpha_1}, \ldots \frac{1}{\alpha_d}$

Estimate largest abs. value of a root of $\tilde{P}$.

This gives an upper bound ($\leq$ factor $O(d^2)$ of truth) on the

smallest abs. value of a root of P.

Given $Q(x)$ and $\beta \in \mathbb{C}$,
estimating smallest root of
$Q(x+\beta)$ gives an upper bound
on the distance of β to
the nearest root of Q.
(that is $\leq O(d)$ × the true dist)

Gives a procedure to chase down the roots.

① Start with $\beta_0 = 0$ and a scale $u_0 \in \mathbb{R}$ s.t.
we are guaranteed that
there is a root in the square

$$\beta_0 + \left([-u_0, u_0] \times [-u_0, u_0] \right)$$
$$\subseteq \mathbb{R}^2 = \mathbb{C}.$$

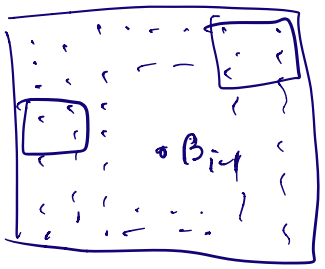
② Successively produce β_i, u_i

so that we are guaranteed a root in $\beta_i + \left([-u_i, u_i] \times [-u_i, u_i]\right)$

and $u_i \leq u_{i-1}/2$.

Details of (2)

Consider a $(1000d^2) \times (1000d^2)$ grid of points inside $\beta_{i-1} + \left([-u_{i-1}, u_{i-1}] \times [-u_{i-1}, u_{i-1}]\right)$



One point of this grid is within distance $\leq (u_{i-1})/50d^2$ from a root of Q.

If we run the root-distance estimator

on Q and that particular point on the then it will guarantee that the point is within distance $u_{i-1}/10$ from that point.

Alg for step 2

For each point r in this grid, run root distance estimator between Q and r.

If root-dist is guaranteed to be $< u_{i-1}/2$, set β_i = that r and $u_i = u_{i-1}/2$.

This finds one root.

To find all roots need 2 additional ideas.

① $\mathrm{GCD}\left(Q, \frac{\partial Q}{\partial x}\right)$ catches all

repeated roots.

② Roots are separated.

$$Q(x) = \prod (x - \alpha_i)$$

$$\text{disc}(Q) = \prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_{i=1}^{d} Q'(\alpha_i)$$

$$= \det \begin{bmatrix} a_d & a_{d-1} & \cdots & a_0 & 0 & \cdots & 0 \\ & a_d & \cdots & a_0 & & & \\ 0 & & & & & & \\ & & a_d & \cdots & a_0 & & \\ d \cdot a_d & (d-1) a_{d-1} & \cdots & a_0 & & & \\ & \ddots & & & & & \end{bmatrix}$$

(some expression, which is an integer).

$\text{Res}(f, g)$ $\quad f = \sum a_i x^i$ $\quad \deg d$

$\quad g = \sum b_j x^j$ $\quad \deg e$

$d + e$

$$\det \begin{bmatrix} a_0 & a_1 & \cdots & a_d & & 0 \\ & a_0 & a_1 & \cdots & a_d & \\ & & \ddots & & & \ddots \\ & & & a_0 & \cdots & a_d \\ b_0 & \cdots & b_e & & & \\ & b_0 & \cdots & b_e & & 0 \\ 0 & & & & & \end{bmatrix}$$

$$R \cdot f + S \cdot g$$

$\deg R < e$

$\deg S < d$.

$L \cup$ $b_0 \dots b_e$

If $\gcd(f,g)=1$, $Rf+Sg \neq 0$ $\Rightarrow$ matrix is invertible

$$\mathrm{Res}\left(Q, \frac{\partial Q}{\partial x}\right) = \mathrm{disc}(Q)$$

$$\mathrm{Res}(f,g) = a_0^e b_0^d \prod_{i,j} (\alpha_i - \beta_j)$$

α_i: roots of f; β_j: roots of g.

$$\mathbb{C}^e \times \mathbb{C}^d \to \mathbb{C}^{d+e}$$

$$(R(x), S(x)) \mapsto R \cdot f + S \cdot g$$

$\deg R < e$, $\deg S < d$, $\deg(Rf+Sg) < d+e$