Real Algebraic Numbers

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}_{alg} \subseteq \mathbb{R}$$

$$x^2 - 2 = 0 \wedge x > 0$$

Real Closed Fields (RCFs)

- ordered field
- $\forall x \; x > 0 \Rightarrow \exists y . \; x = y^2$
- for each odd n

  $\forall a_0 \ldots a_n . \; a_n \neq 0 \Rightarrow \exists x \; a_n X^n + \cdots + a_1 X + a_0 = 0$

- Upper/Lower Bounds
- Root Isolation
- Tower of field Extensions
- Improvements

Positive Root Upper bound

$$a_n x^n + \dots + a_1 x + a_0 \qquad a_n > 0$$

$$B = \max\left\{ \sqrt[k]{\frac{|a_{n-k}|}{a_n}} \;\middle|\; 1 \leq k \leq n \,,\; a_{n-k} < 0 \right\}$$

$2B$ is a bound for the positive roots

$$\sqrt[k]{\frac{|a_{n-k}|}{a_n}} \rightsquigarrow \frac{\log_2 |a_{n-k}| + 1 - \log_2 a_n}{k} + 1$$

$$\log_2 \underbrace{00001101}_{13} = 3$$

$$2^{\log_2 c} \leq c < 2^{\log_2 c + 1}$$

Compute 2B as a power of TWO

Square free Polynomials

$$f = p_1^{k_1} \, p_2^{k_2} \cdots p_n^{k_n}$$

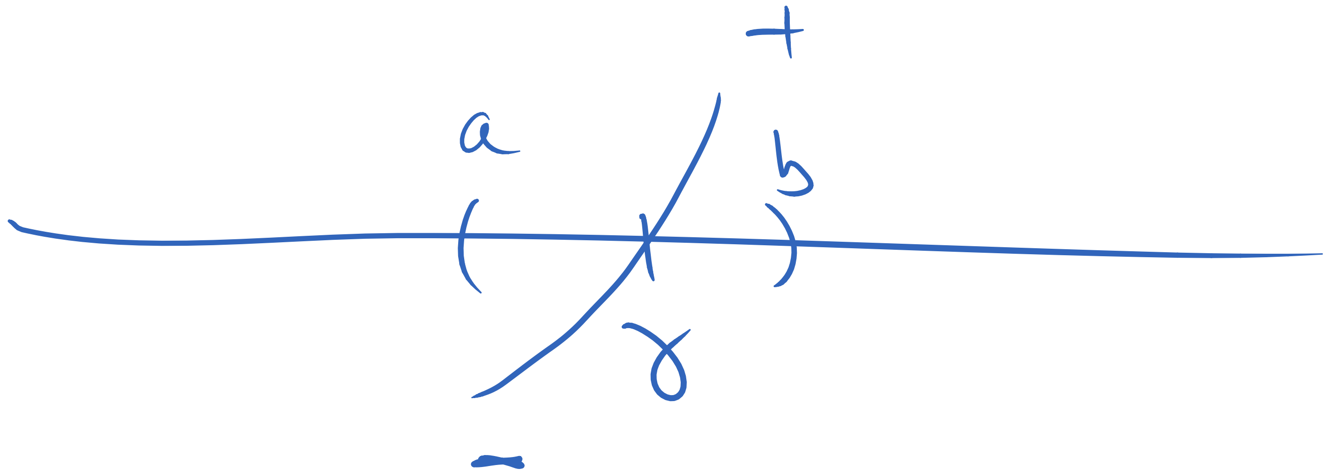
$$\mathrm{SQf}(f) = p_1 \, p_2 \cdots p_n$$

$$\mathrm{SQf}(f) = \frac{f}{\mathrm{GCD}(f, f')}$$

h_m in the Sturm seq.

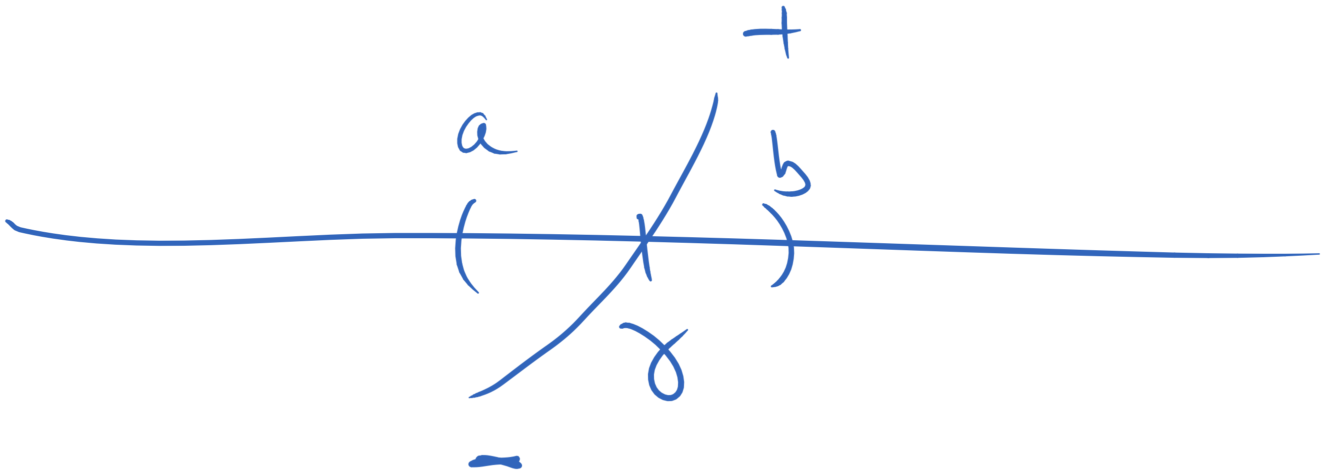
Square free Polynomials

Why?



Square free Polynomials

Why?



Refine Root using Bisection.

Field Extension $K(\gamma)$

- Given K
  - ordered field $+, -, \cdot, INV$
  - $approx(a) = (l, u)$ $\quad a = 0 \vee 0 \notin (l, u)$

    $l, u \in \mathbb{Q}$ $\quad$ improvement $l, u \in \mathbb{Q}_B$ $\quad \frac{a}{2^k}$
  - $sign(a) = \begin{cases} -1 & a < 0 \\ 0 & a = 0 \\ 1 & a > 0 \end{cases}$
- Polynomial $P = a_n x^n + \cdots + a_1 x_1 + a_0, \quad a_i\text{'s} \in K$
- Return new ordered field $K(\gamma)$ where γ is root of P.

Isolate Roots of $a_n x^n + \dots + a_1 x_1 + a_0$

1) Remove zero root

$$a_n x^n + \dots + a_k x^k$$

$$\Downarrow$$

$$a_n x^{n-k} + \dots + a_k$$

Isolate Roots of $a_n x^n + \dots + a_1 x_1 + a_0$

1) Remove zero root

$$P = a_n x^n + \dots + a_k x^k$$

$$\Downarrow$$

$$P_1 = a_n x^{n-k} + \dots + a_k$$

Isolate Roots of $a_n x^n + \cdots + a_1 x_1 + a_0$

2) Compute SQF

$$P_2 = \frac{P_1}{GCD(P_1, P_1')}$$

3) Compute Sturm(P_2, P_2')

IF P_2 has zero roots, return

Isolate Roots of $a_n x^n + \dots + a_1 x_1 + a_0$

4) Handle positive and negative roots separately

$P_2(x)$ $\qquad\qquad$ $P_2(-x)$

if γ is a positive root of $P_2(-x)$

Then $-\gamma$ is a negative root of $P_2(x)$

Example $P_2(x) = x^4 + x^3 - 2x^2 - 6x + 1$

$\Downarrow$

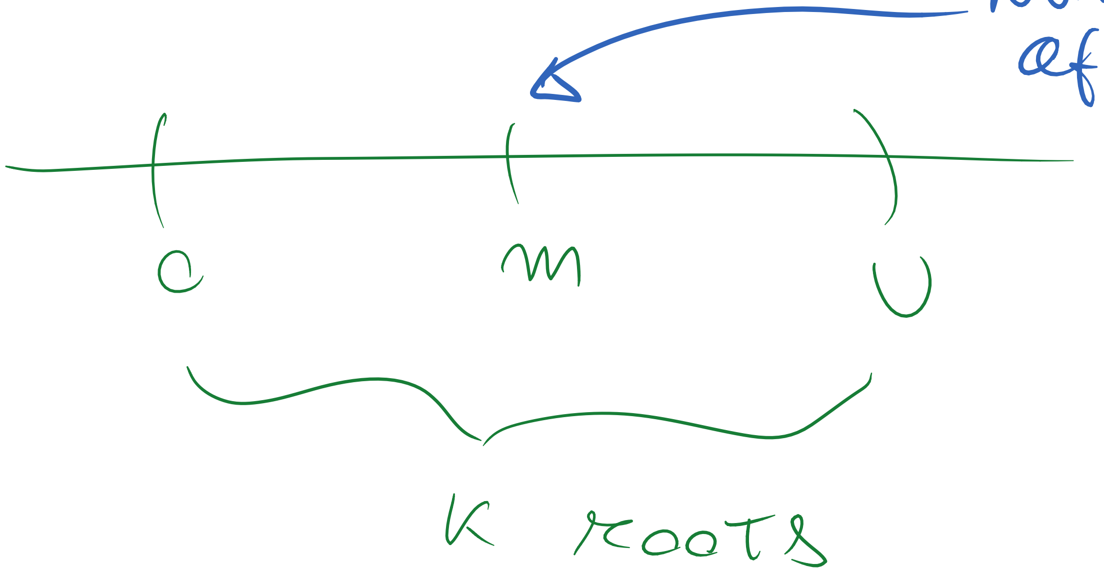
$P_2(-x) = x^4 - x^3 - 2x^2 + 6x + 1$

Isolate Roots of $a_n x^n + \dots + a_1 x_1 + a_0$

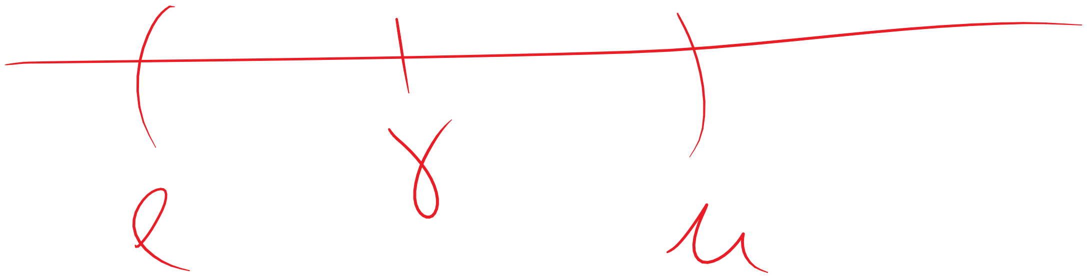
5) Compute upper bound U

6) Use interval bisection for looking for isolating interval

Number of variations of the sturm sequence



Assume interval (ℓ, u)



has only one root.

$\Rightarrow$ use $(P_2, (\ell, u))$ to represent γ

Remark: Only works for Archimedian RCFs.

How to represent elements of $K(\gamma)$?

How to represent elements of $K(\gamma)$?

Idea: Polynomials in γ.

Example: $\gamma = (x^2 - 2, (0, 2))$

$a = 3\gamma + 1$

How to represent elements of $K(\gamma)$?

Idea: Polynomials in γ.

Example: $\gamma = (x^2 - 2, (0, 2))$

$$a = 3\gamma + 1$$

Implement $+, -, \cdot$ using polynomial arithmetic.

Example: $(\gamma + 1)(3\gamma + 1) = 3\gamma^2 + 4\gamma + 1$

Normalizing values of $K(\gamma)$

$\gamma = (f, (l, u))$

$a = g(\gamma)$

Polynomial division again

$g(\gamma) = q(\gamma) \cdot f(\gamma) + r(\gamma)$

Example: $\gamma = (x^2 - 2, (0, 2))$

$a = \gamma^3 + 1 = 2\gamma + 1$

$x^3 + 1 = x(x^2 - 2) + (2x + 1)$

Computing (l,u) for $a = g(\gamma)$

1) use interval arithmetic

2) Refine intervals (l,u) and intervals for coefficients of $g(x) = a_n x^n + \dots + a_1 x_1 + a_0$

3) Until $0 \notin (l,u)$ or threshold is reached

If Threshold is reached

$$\gamma(f, (l, u))$$

$$a = g(\gamma)$$

$$TaQ(g, f; (l, u)) =$$

$$\#\{\gamma \mid f(\gamma) = 0,\ g(\gamma) > 0,\ l < \gamma < u\}$$

$$- \#\{\gamma \mid f(\gamma) = 0,\ g(\gamma) < 0,\ l < \gamma < u\}$$

If Threshold is reached

$\gamma(f, (l, u))$

$a = g(\gamma)$

There is one and only one root of f in (l, u)

$TaQ(g, f; (l, u)) =$

$\#\{\gamma \mid f(\gamma)=0,\ g(\gamma)>0,\ l<\gamma<u\}$

$-\ \#\{\gamma \mid f(\gamma)=0,\ g(\gamma)<0,\ l<\gamma<u\}$

$$TaQ(g, f; (l, u)) = \begin{cases} -1 & g(\gamma) < 0 \\ 0 & g(\gamma) = 0 \\ 1 & g(\gamma) > 0 \end{cases}$$

Comparing $a, b \in K(\gamma)$

1) Compare intervals

2) If intervals overlap

a) refine

b) Compute $a - b$

Multiplicative Inverse

$a = g(\gamma)$ $\qquad \frac{1}{a} = \frac{1}{g(\gamma)}$ ← This is not a polynomial

Idea: Compute $h(\gamma)$ such that

$$g(\gamma) \cdot h(\gamma) = 1$$

Given $\gamma = (f, (\ell, u))$ $a = g(\gamma)$

$p := g$

$h := 1$

Loop

INVARIANT $g(\gamma) \cdot h(\gamma) = p(\gamma)$

IF p is the constant polynomial a_0

return $\frac{1}{a_0} h(\gamma)$

ELSE

(q, r) s.t. $f = q \cdot p + r$

IF $r \neq 0$

$h = q h$

$p = -r$

ELSE

refine γ using q or p

$\underbrace{f(\gamma)}_{0} = q(\gamma) p(\gamma) + r(\gamma)$

$-r(\gamma) = q(\gamma) p(\gamma)$

f is not minimal

Tower of extensions

$$\mathbb{Q}(\gamma_1)(\gamma_2)\ldots(\gamma_k)$$

$$\gamma_1 = \left(x^5 - x - 1,\ \left(-2, -\tfrac{1}{2}\right)\right)$$

$$\gamma_2 = \left(x^2 + \gamma_1,\ \left(\tfrac{1}{2}, 2\right)\right)$$

$$a = (\gamma_1^3 + 2)\gamma_2 + (\gamma_1^2 + 3)$$

Refinements

- Use Descartes Rule of Signs for isolating intervals.
- Use GCD for checking whether f, g have a common root

Computable Transcendentals

$\mathbb{Q}(\pi)(e)$

$\mathrm{Approx}_\pi(n) \rightsquigarrow$ approximating interval.

Remark: $\sqrt{\pi}$ is transcendental with respect to $\mathbb{Q}$, but it is not with respect to $\mathbb{Q}(\pi)$

$P(\pi)$ is zero iff P is the zero polynomial

Elements of $K(\mathbb{T})$ are rational functions.

$$\frac{p(\mathbb{T})}{q(\mathbb{T})}$$

We can easily implement the API using polynomial arithmetic and interval arithmetic.

Periodic Functions

$\sin x = 0$ iff $x = \pi n$

$\sin y = 0 \wedge 0 < y < 4$ iff $y = \pi$

Periodic Functions

$\sin x = 0$ iff $x = \pi n$

$\sin y = 0 \wedge 0 < y < 4$ iff $y = \pi$

$\text{Integer}(z)$ iff

$$\exists x\, y.\ \sin x = 0 \wedge \sin y = 0 \wedge 0 < y < 4 \wedge z \cdot y = x$$

Resources

http://tinyurl.com/ksb32xw