Root finding and evaluation of univariate polynomials with low-precision arithmetic

Guillaume Moroz

December 16, 2021

Problems

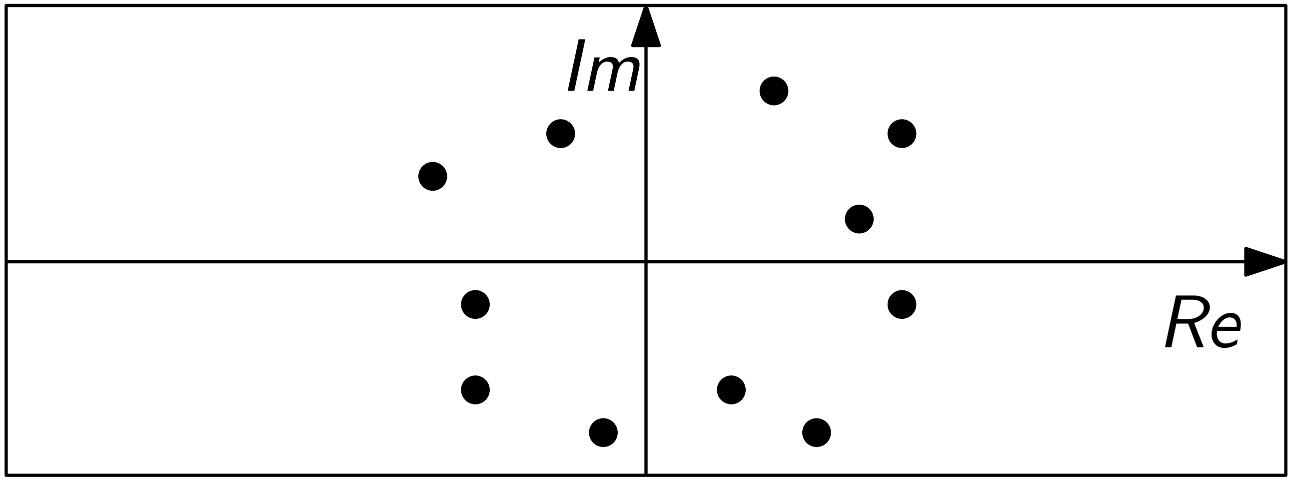
$$f(z) = a_0 + \cdots + a_d z^d \qquad a_k \in \mathbb{C}$$

Multipoint evaluation

Given d complex numbers z_k, evaluate all the $f(z_k)$.

Root finding

Find all the complex solutions ζ_k of $f(z) = 0$.



$\mathbb{C} \simeq \mathbb{R}^2$

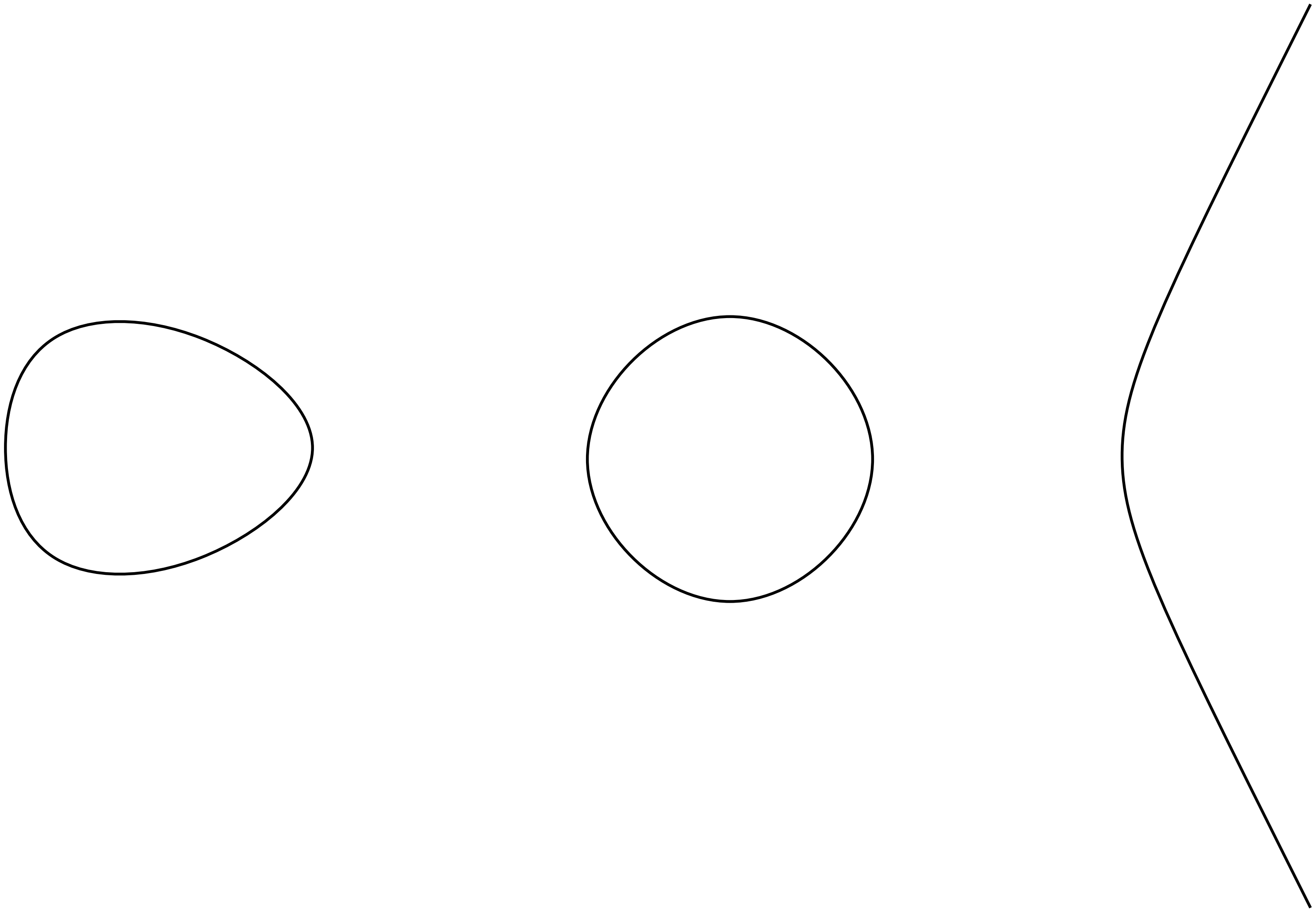
Problems

Discrete data

```
           /*         EPI CARAMEL        */                 C,A,
           /*  Cryptologie, Arithmétique :  */             R,a,
           /*     Matériel et Logiciel      */            M,E,
                                                          L,i=
                                                         5,e,
    d[5],Q[999                     ]={0};main(N           ){for
  (;i--;e=scanf("%"              "d",d+i));for(A          =*d;
 ++i<A         ;++Q[         i*i%          A],R=         i[Q]?
R:i);            for(;i     --;)            for(M        =A;M
--;N             +=!M*Q     [E%A            ],e+=        Q[(A
+E*E-           R*L*         L%A)           %A])          for(
  E=i,L=M,a=4;a;C=             i*E+R*M*L,L=(M*E          +i*L)
    %A,E=C%A+a                  --[d]);printf             ("%d"
                                                         "\n",
                                                          (e+N*
                                                            N)/2
     /* cc caramel.c; echo f3 f2 f1 f0 p | ./a.out */      -A);}
```

Problems

Continuous data



Problems

Evaluation output

- Arbitrary precision
- Finite precision

$$\text{Light-year: } 9\,460\,730\,472\,580\,800 \text{ m}$$
$$9.460 \cdot 10^{15} \text{ m}$$

Root finding output

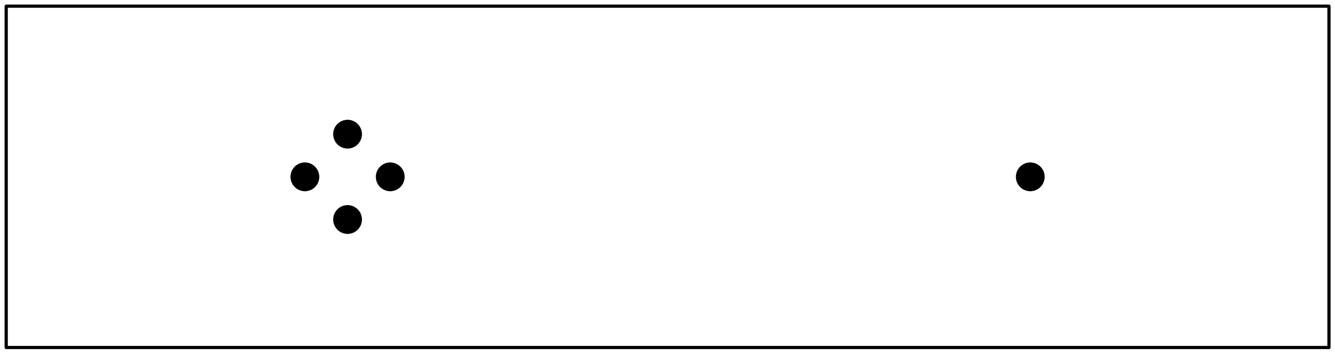
- Initial point and program for convergence

$$\text{Newton: } x_0 = z$$
$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}$$

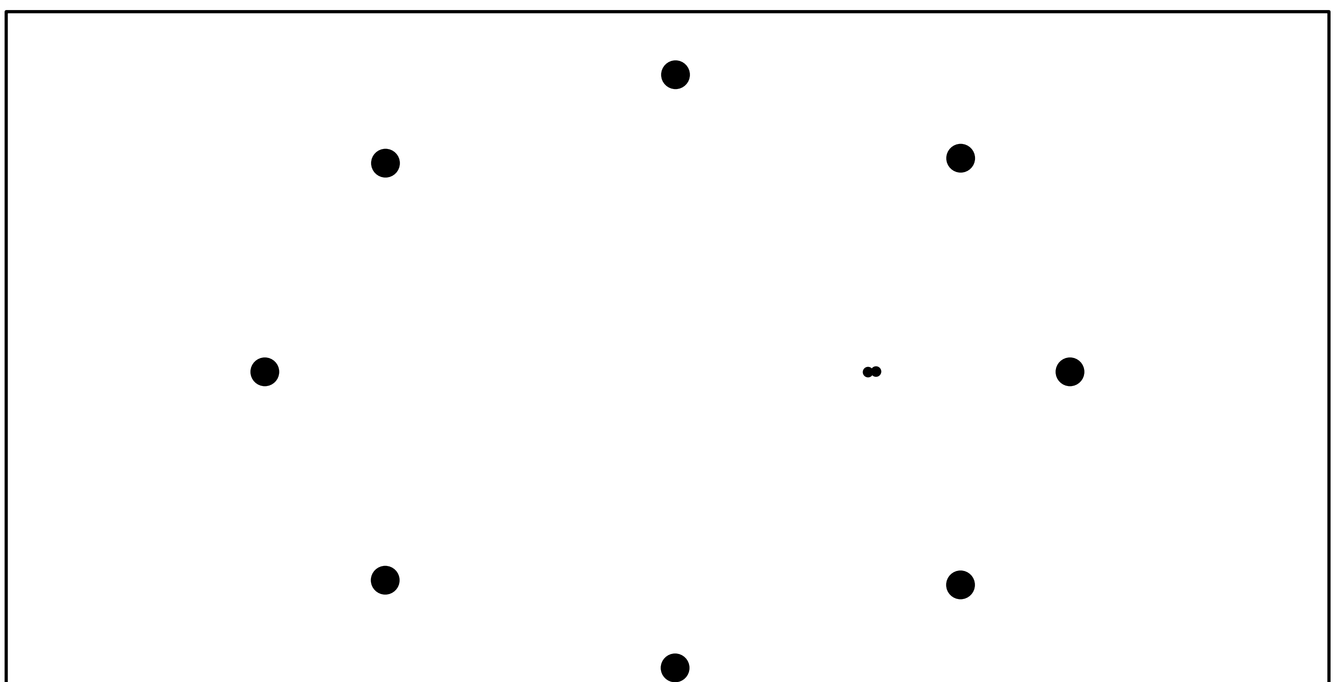
- Isolating disk

Numerically ill-conditioned root finding

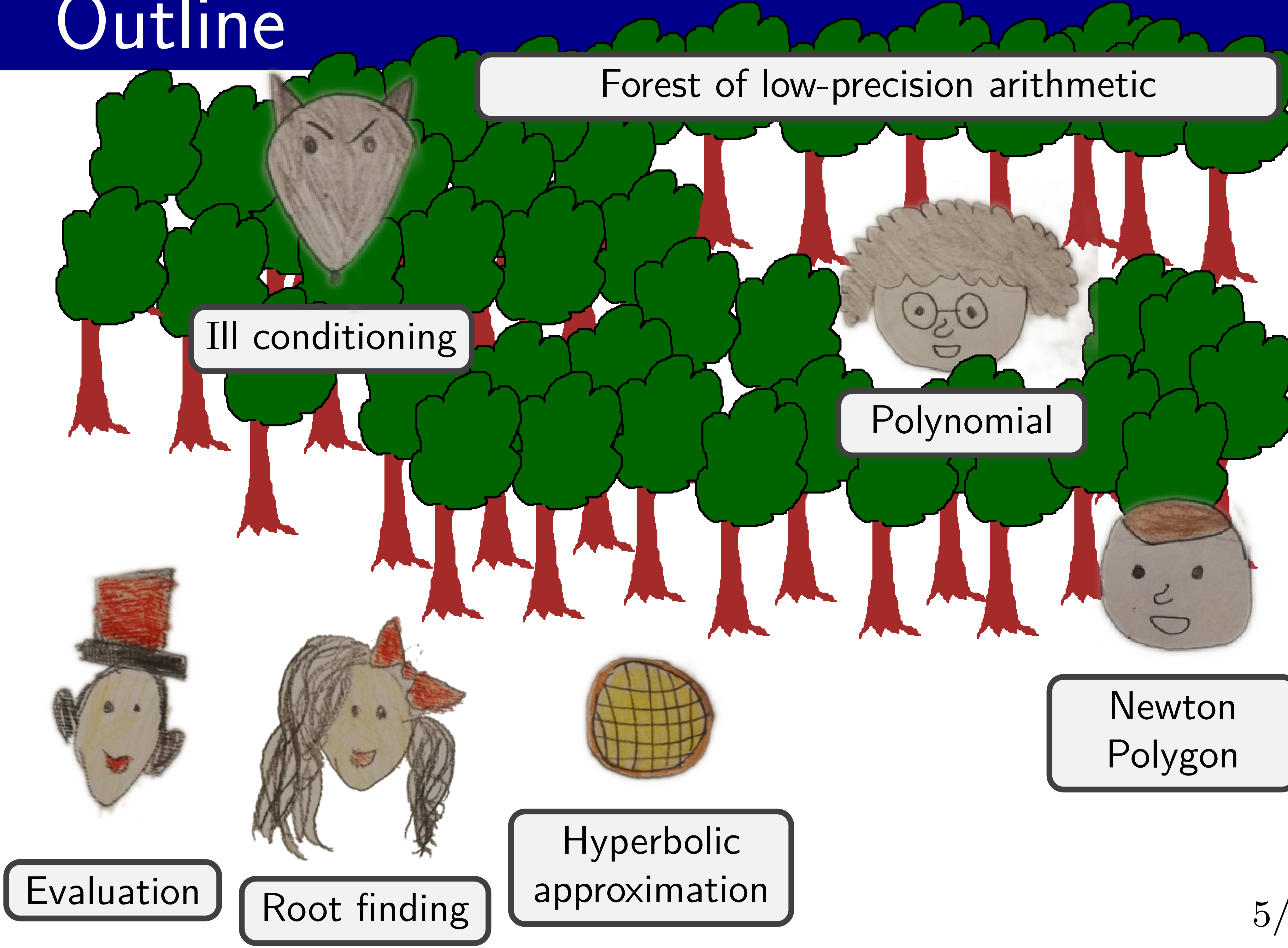
$$(z^4 - \epsilon)(z - 1) = 0$$



$$z^{10} - 2(2z^2 - 1)^2 = 0$$ [Mignotte 82]



Outline


Forest of low-precision arithmetic
Ill conditioning
Polynomial
Newton
Polygon
Evaluation
Root finding
Hyperbolic
approximation

Conditioning of root finding

$$f(z) = a_0 + \cdots + a_d z^d \qquad a_k \in \mathbb{C}$$

$$h(z) = h_0 + \cdots + h_d z^d \qquad \textstyle\sum_k |h_k| \le \varepsilon$$

$\psi(a_0 + h_0, \ldots, a_d + h_d) =$ unique root of $f + h$ in U

ζ simple root of f in the unit disk

$\zeta \in U \subset \mathbb{C}$ neighborhood of ζ

Condition number [Bürgisser 2013]

$$\kappa_\zeta = \lim_{\varepsilon \to 0} \max_{\|h\| \le \varepsilon} \frac{|\psi(f+h) - \psi(f)|}{\varepsilon} = \frac{1}{|f'(\zeta)|}$$

Proof: $\quad 0 = (f + h)(\psi(f + h)) - f(\psi(f))$

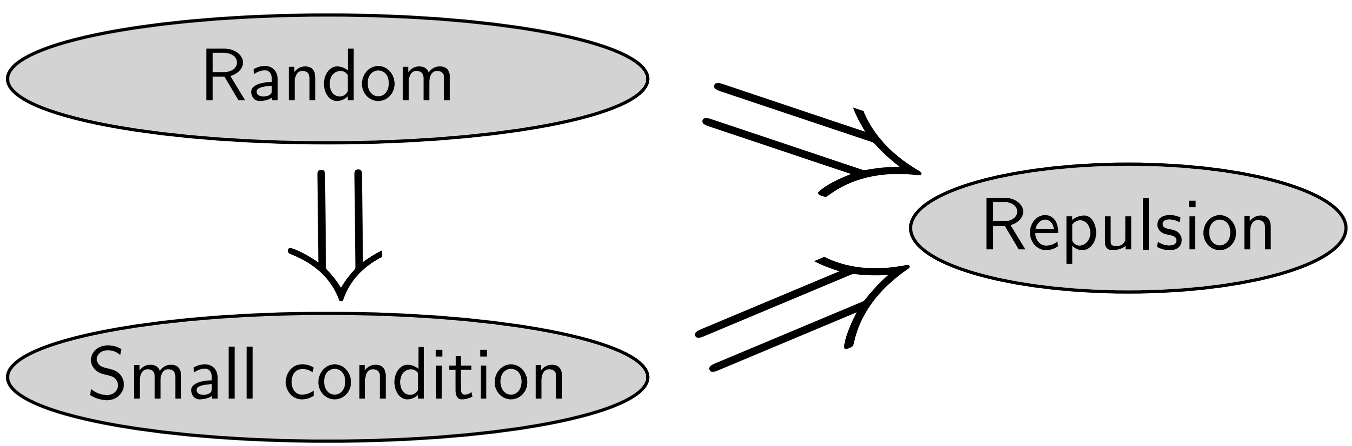
$$\approx h(\zeta) + f'(\zeta)(\psi(f + h) - \psi(f))$$

Properties of polynomials

- Small condition number $\Rightarrow$ large isolating disks
  [Kantorovitch 1948]

- Random coefficients $\Rightarrow$ small condition number
  [Cucker, Krick, Malajovich, Wshebor 2012]

- Random coefficients $\Rightarrow$ large isolating disks
  [Hough, Krishnapour, Peres, Virág 2009]



State of the art: multipoint evaluation

Evaluate $f(z)$ on d points with error in 2^{-m} $|a_k| < 2^m$

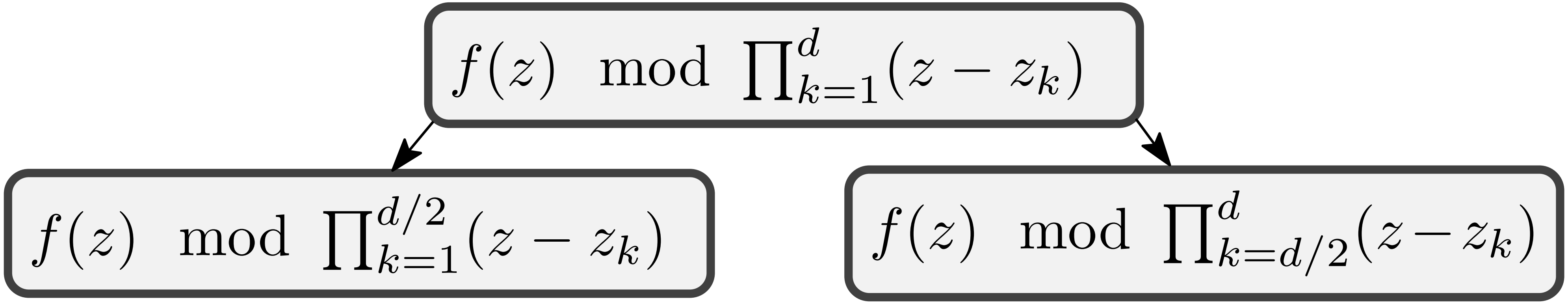
Hörner

$$a_0 + z(a_1 + z(\cdots + z(a_{d-1} + za_d)\cdots))$$

$\rightarrow$ multipoint evaluation in $\widetilde{O}(d^2 m)$ bit operations

Divide and conquer

- $f(z_k) = f(z) \mod (z - z_k)$

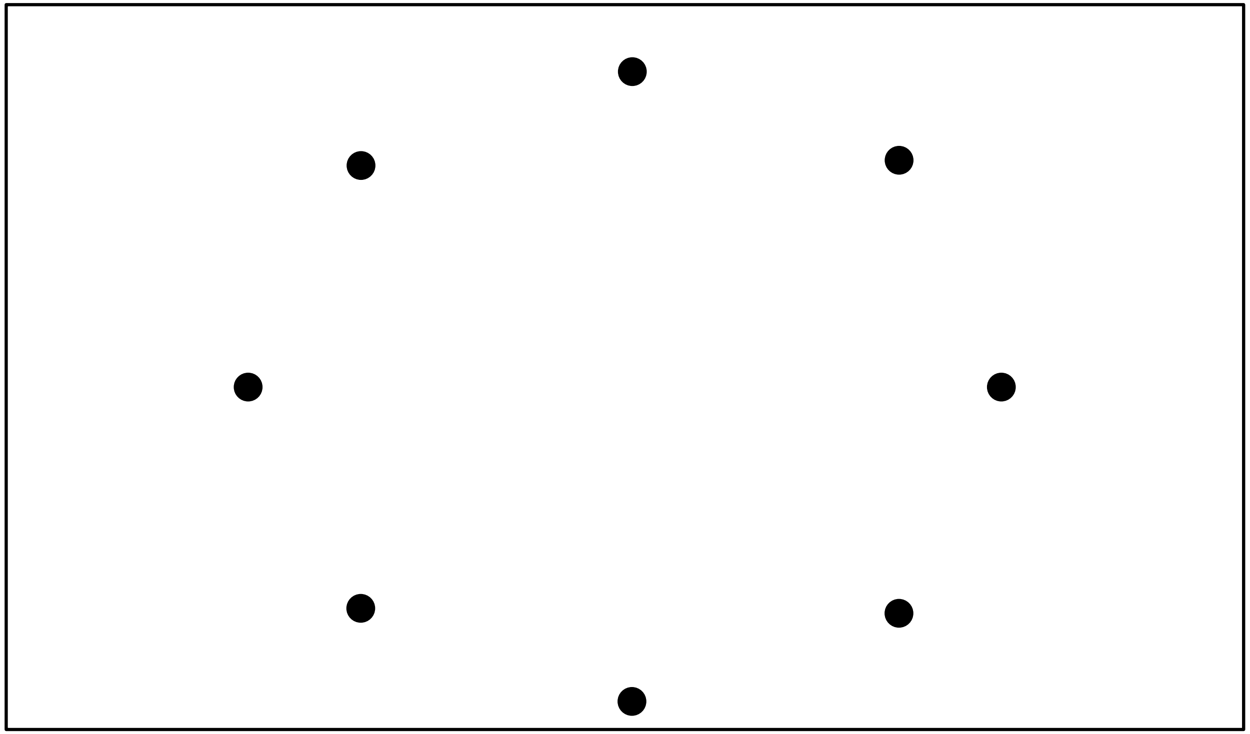


$\rightarrow$ multipoint evaluation in:

- $\widetilde{O}(d)$ arithmetic operations [Fiduccia 1972]
- $\widetilde{O}(d(d+m))$ bit operations [van der Hoeven 2008]

State of the art: multipoint evaluation

Evaluation on the roots of unity $w_k = e^{i\pi k/d}$



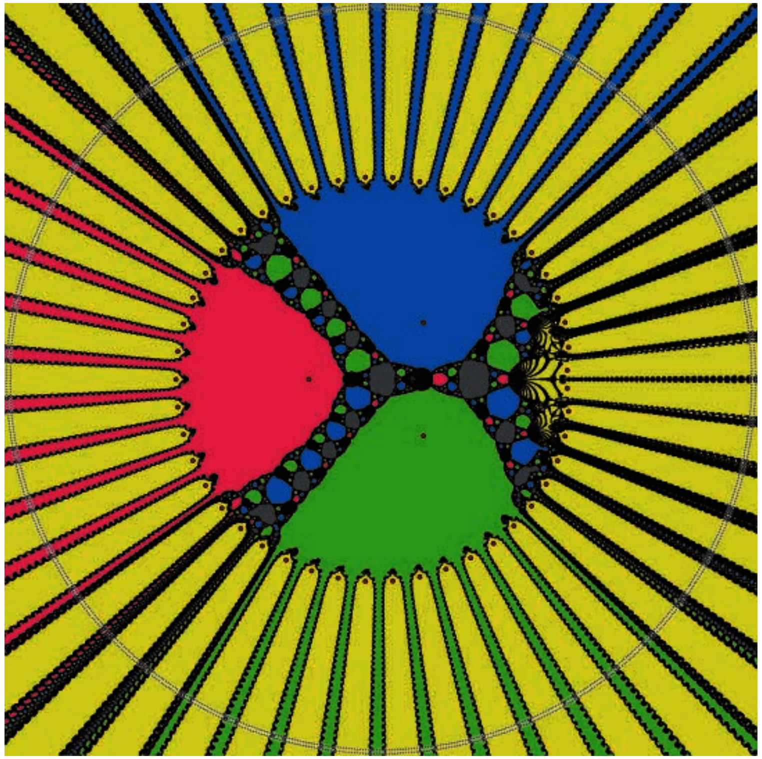
$\rightarrow$ evaluation on w_k in $\widetilde{O}(dm)$ using Fast Fourier Transform
[Gauss 1805, Cooley, Tukey 1965, Schönhage 1982]

$\rightarrow$ multipoint evaluation in $\widetilde{O}(d^{3/2}m^{3/2})$ bit operations
[van der Hoeven 2008]

State of the art: root finding

Newton

[Hubbard, Schleicher, Sutherland 2001]



$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Aberth-Ehrlich variant (1967)

$$F(z) = \frac{f(z)}{(z-z_2)\cdots(z-z_d)}$$

Approximate factorization

$$\|\prod(z - z_k) - f(z)\| \leq 2^{-m}\|f\|$$

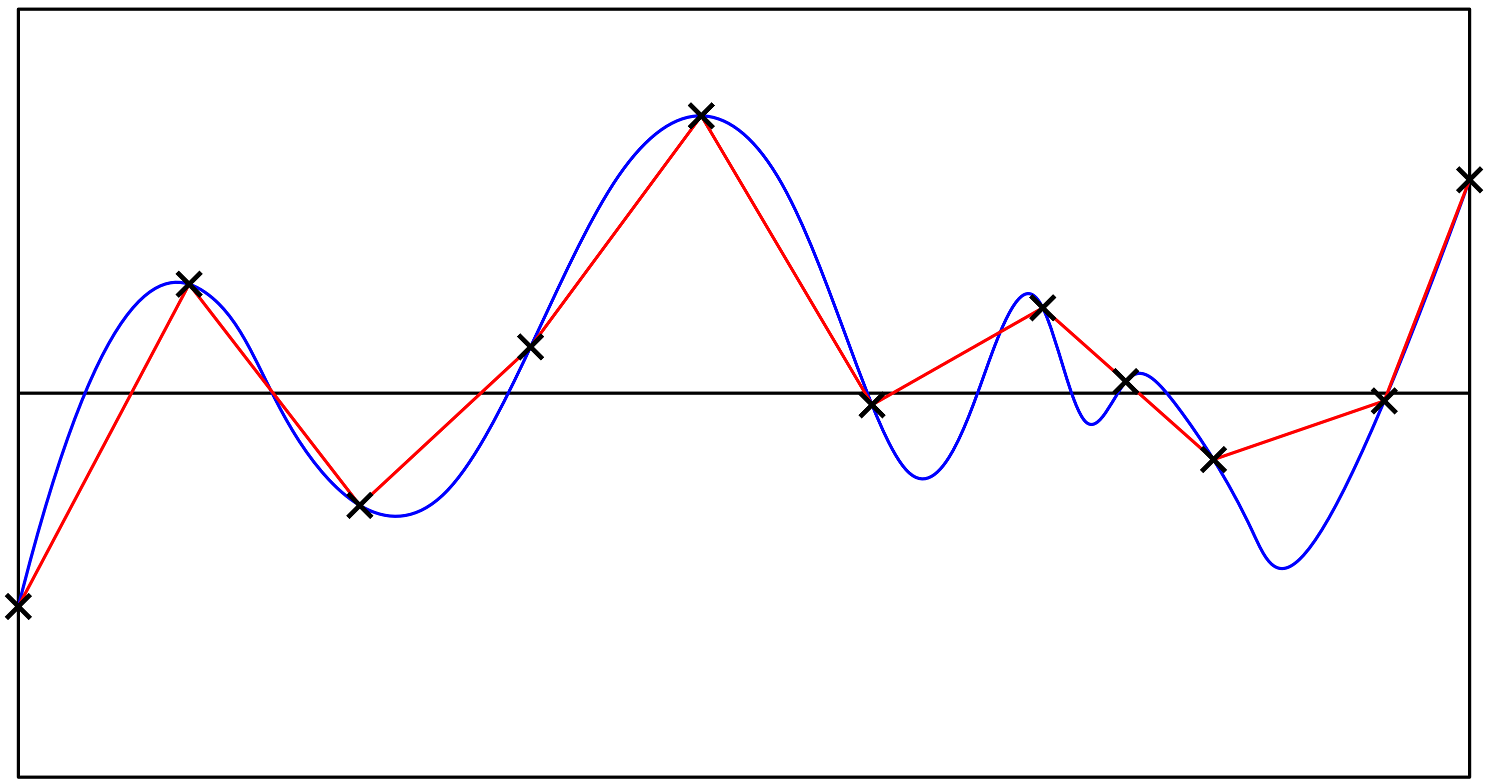
$\rightarrow$ approximation in $\widetilde{O}(d(d+m))$ bit operations
[Schönhage 1982, Pan 2002]

Other methods

Subdivision, Weierstrass, eigenvalue of companion matrix, . . .

State of the art: root finding

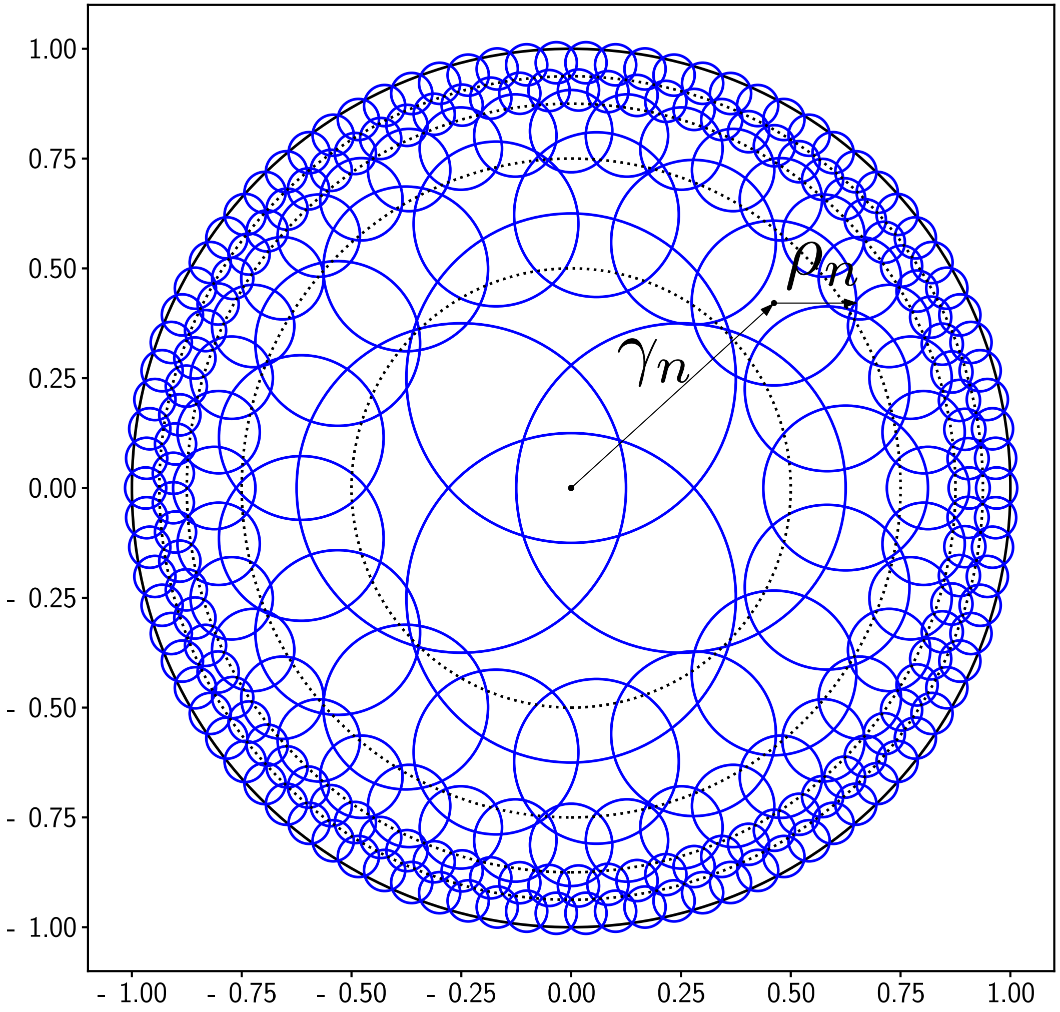
Piecewise linear approximation



$\rightarrow$ piecewise linear or polynomial with constant degrees

[Boyd 2006, etc.]

Hyperbolic approximation



$$0 \le n < N - 1 = O\left(\log \frac{d}{m}\right)$$

$$\begin{cases} \gamma_n = 1 - \frac{3}{4}\frac{1}{2^n} \\ \rho_n = \frac{3}{8}\frac{1}{2^n} \end{cases}$$

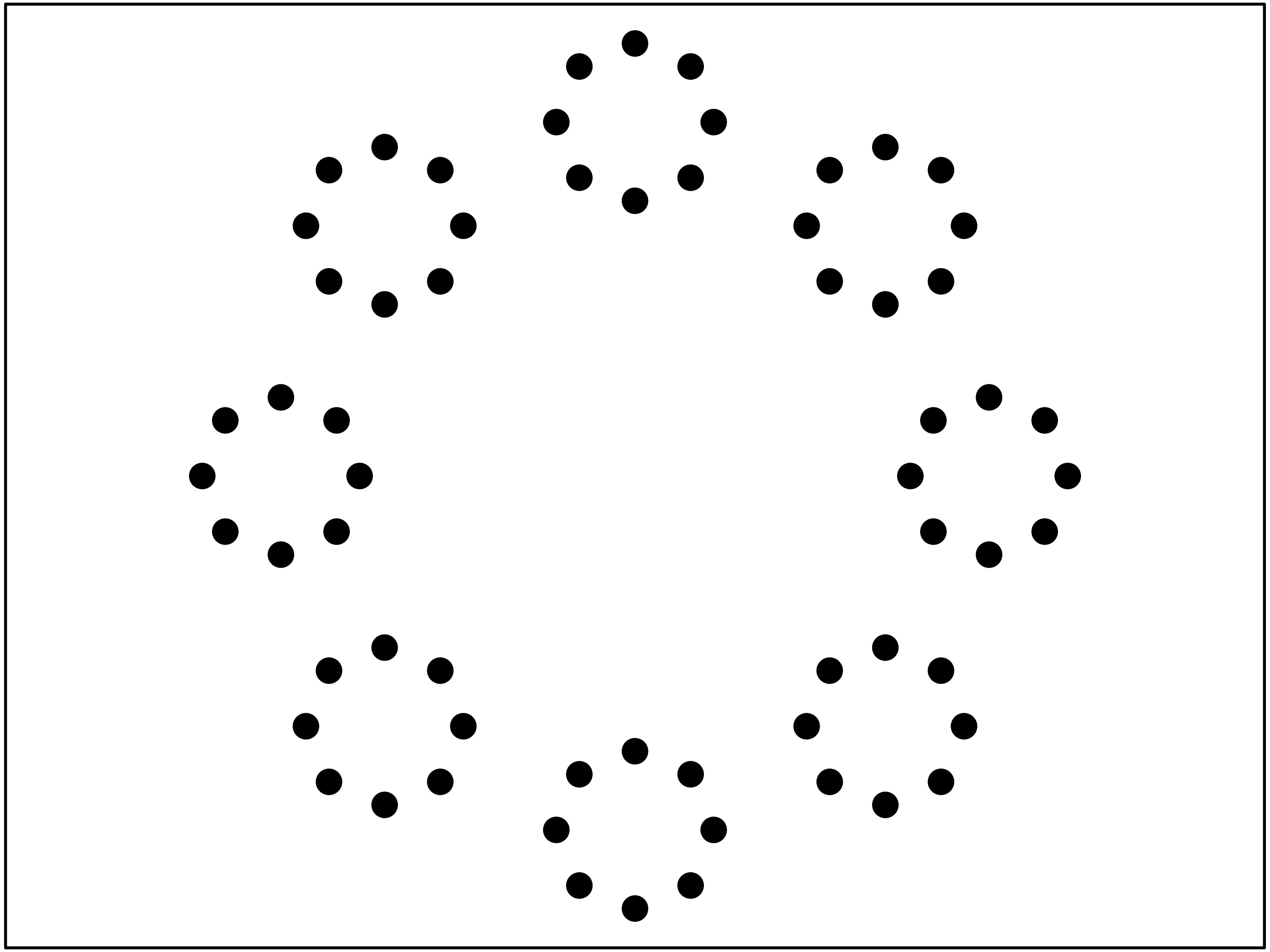
$$g(z) = f(\gamma + \rho z) \mod z^m$$

$\widetilde{O}(\frac{d}{m})$ polynomials of degree m

Approximation bound [New]

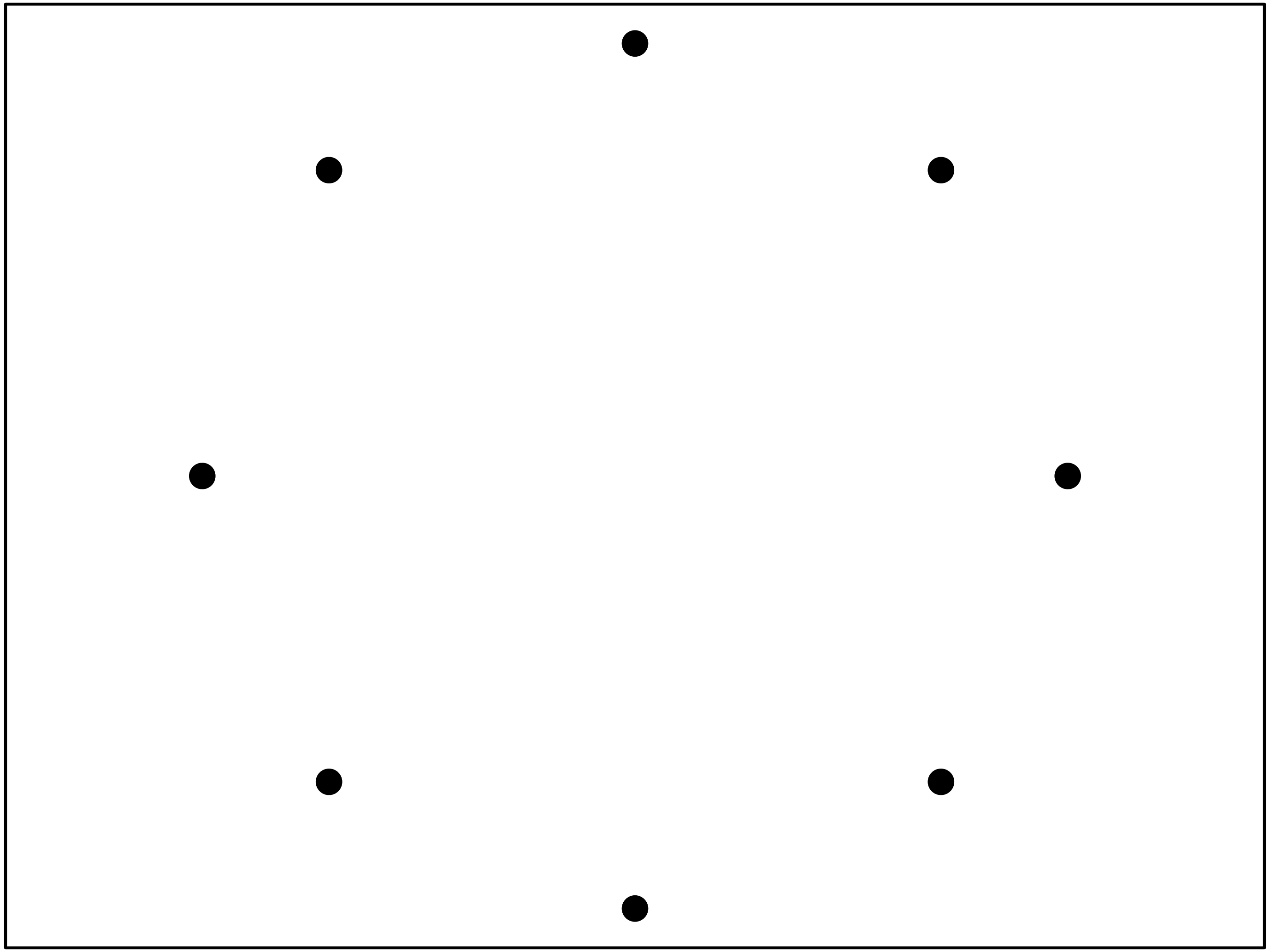
$$\|f(\gamma + \rho z) - g(z)\| \le 2^{-m}\|f\|$$

Hyperbolic approximation computation



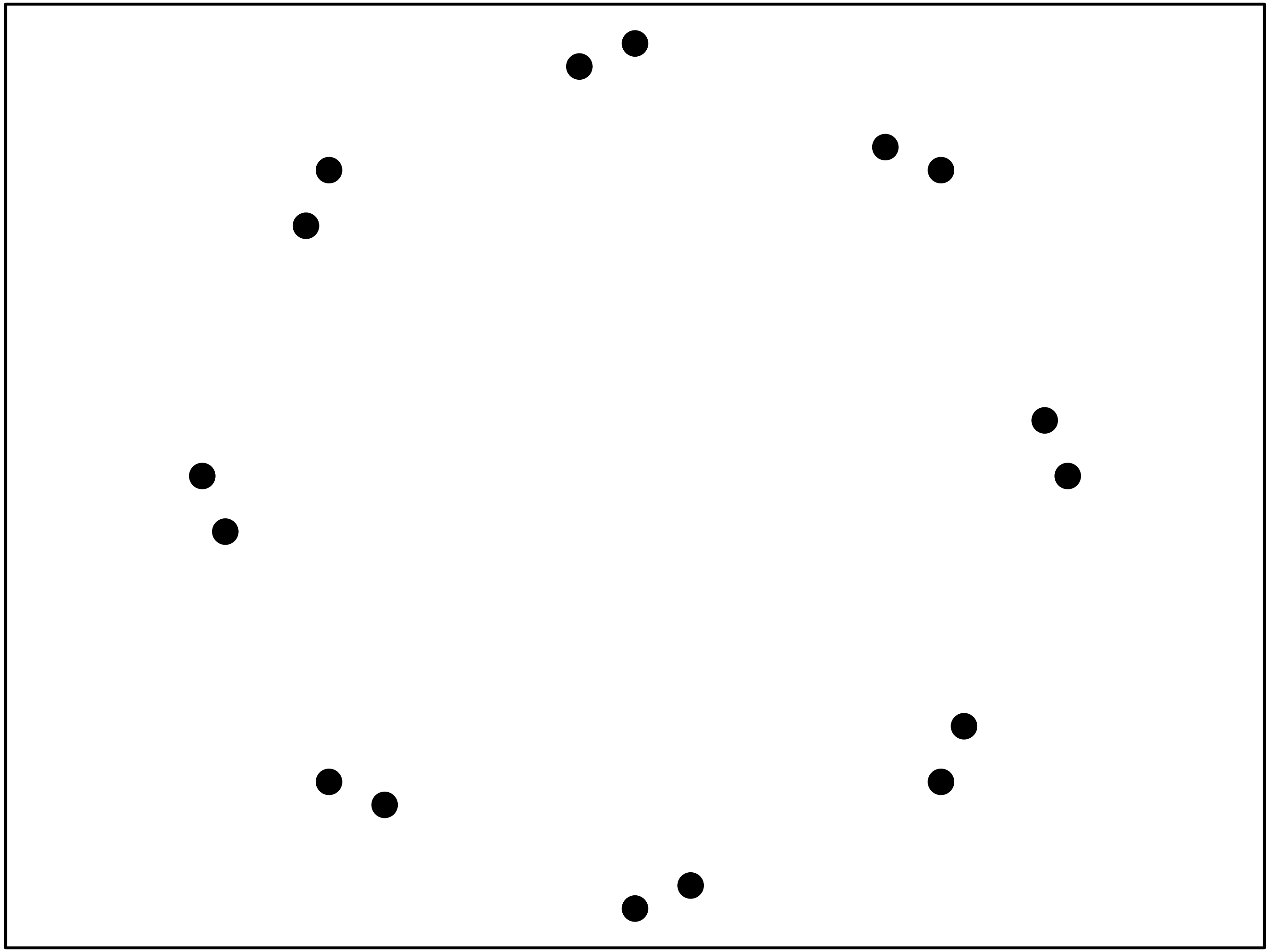
Do m times
  SCALE d coefficients
  FFT on d/m roots of unity

Hyperbolic approximation computation



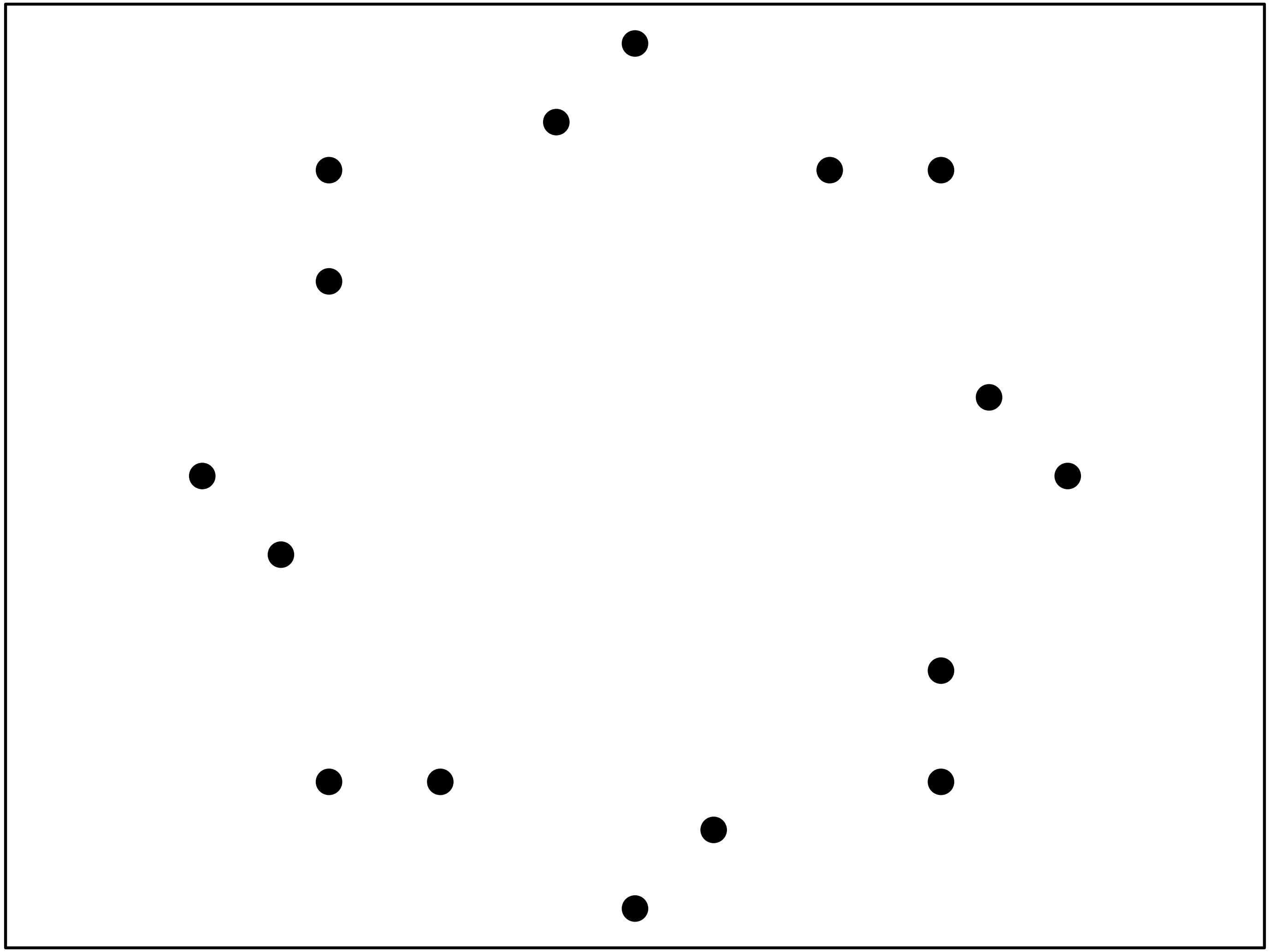
Do m times
  SCALE d coefficients
  FFT on d/m roots of unity

Hyperbolic approximation computation



Do m times
    SCALE d coefficients
    FFT on d/m roots of unity

Hyperbolic approximation computation

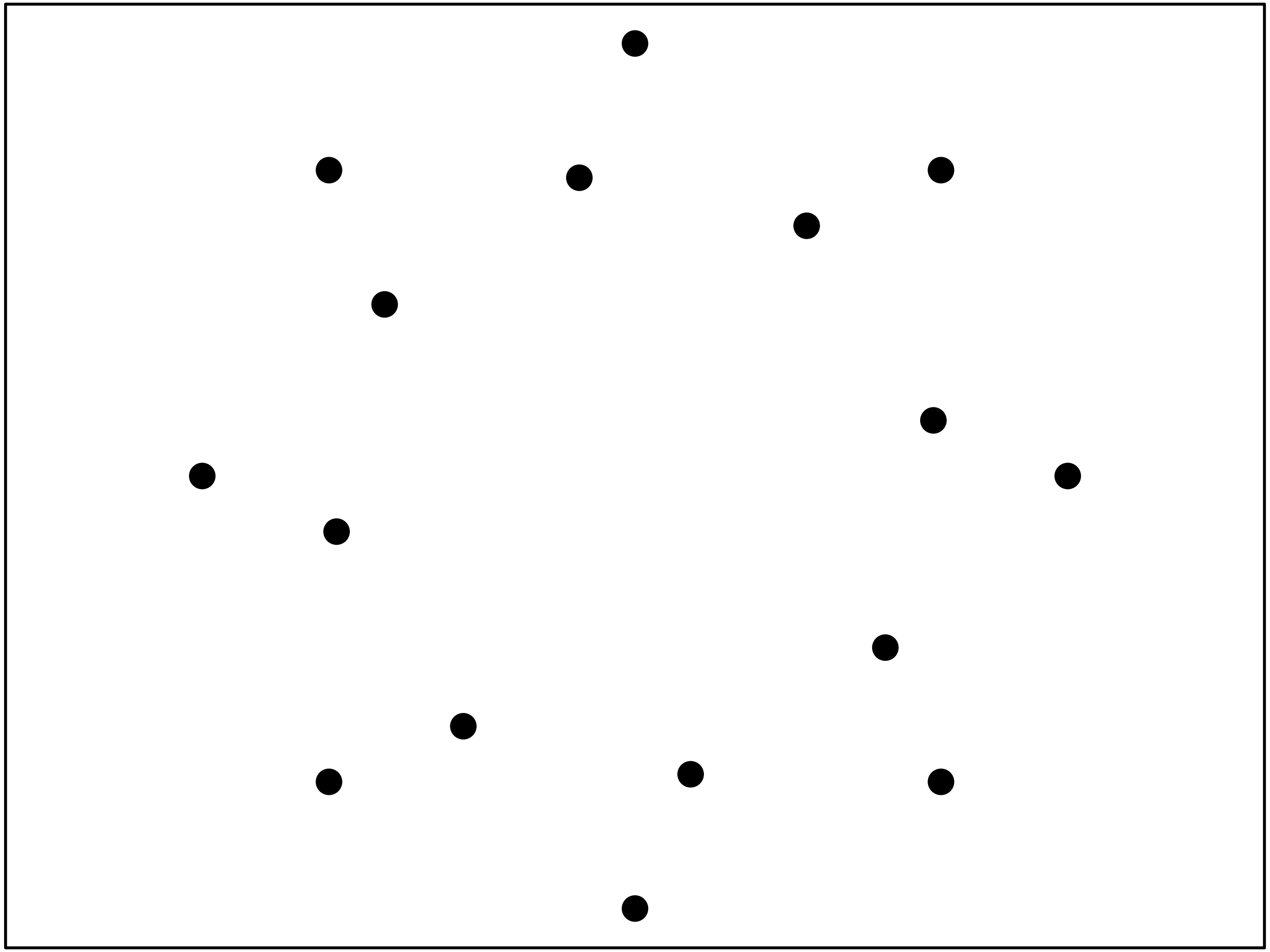


Do m times

  SCALE d coefficients

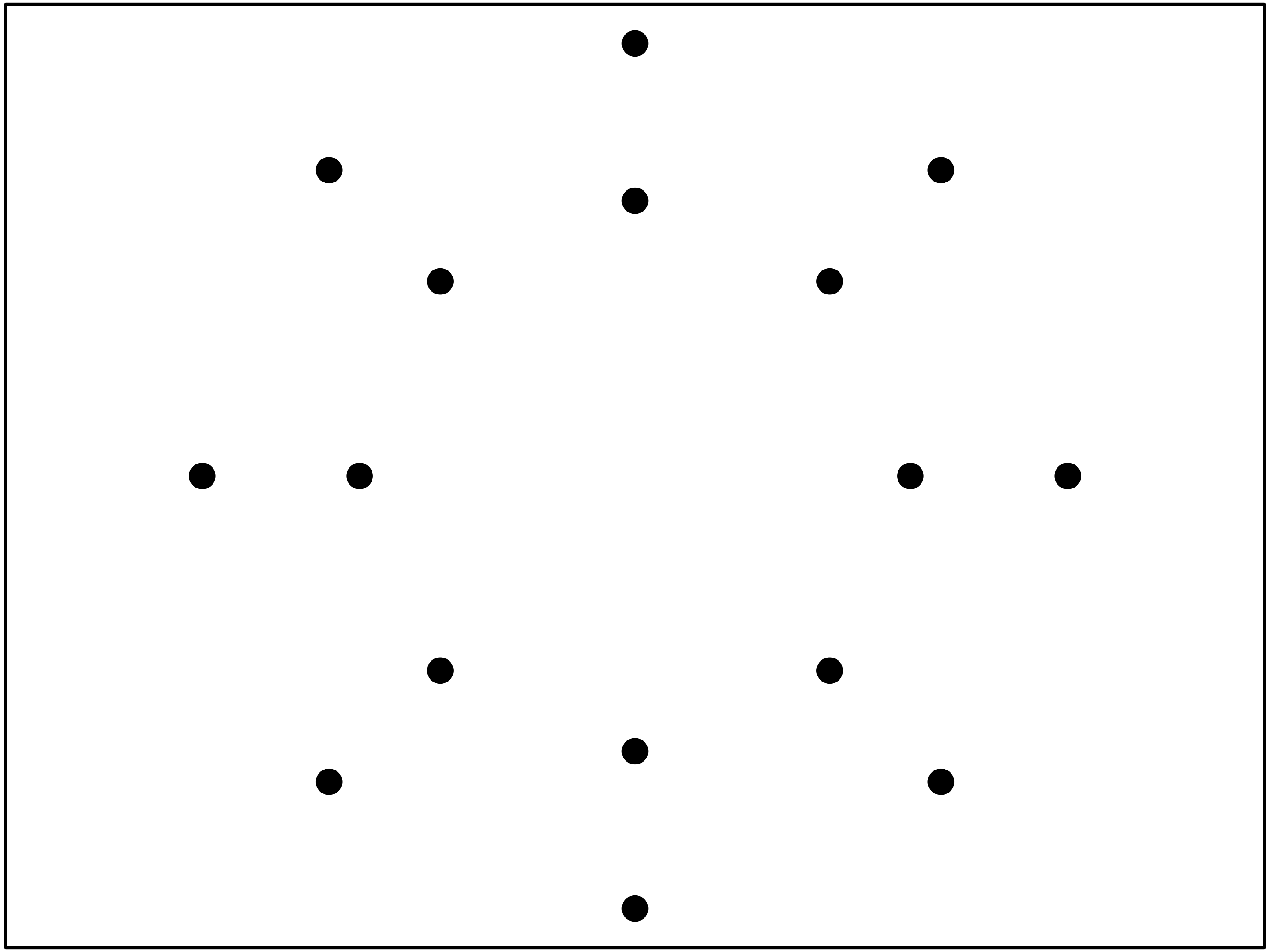
  FFT on d/m roots of unity

Hyperbolic approximation computation



Do m times
$\textsc{Scale}$ d coefficients
FFT on d/m roots of unity

Hyperbolic approximation computation

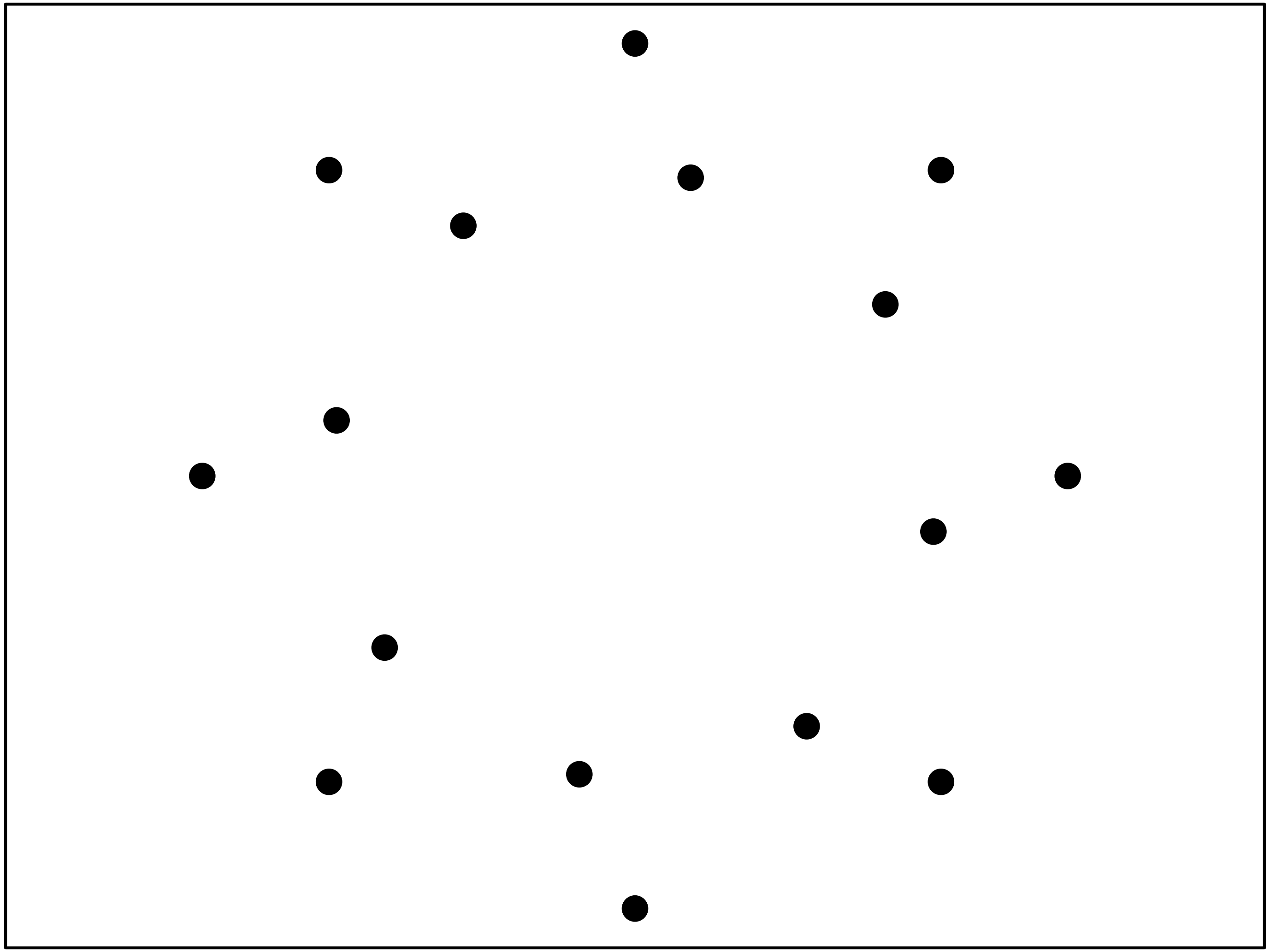


Do m times

$\quad$ SCALE d coefficients

$\quad$ FFT on d/m roots of unity

Hyperbolic approximation computation

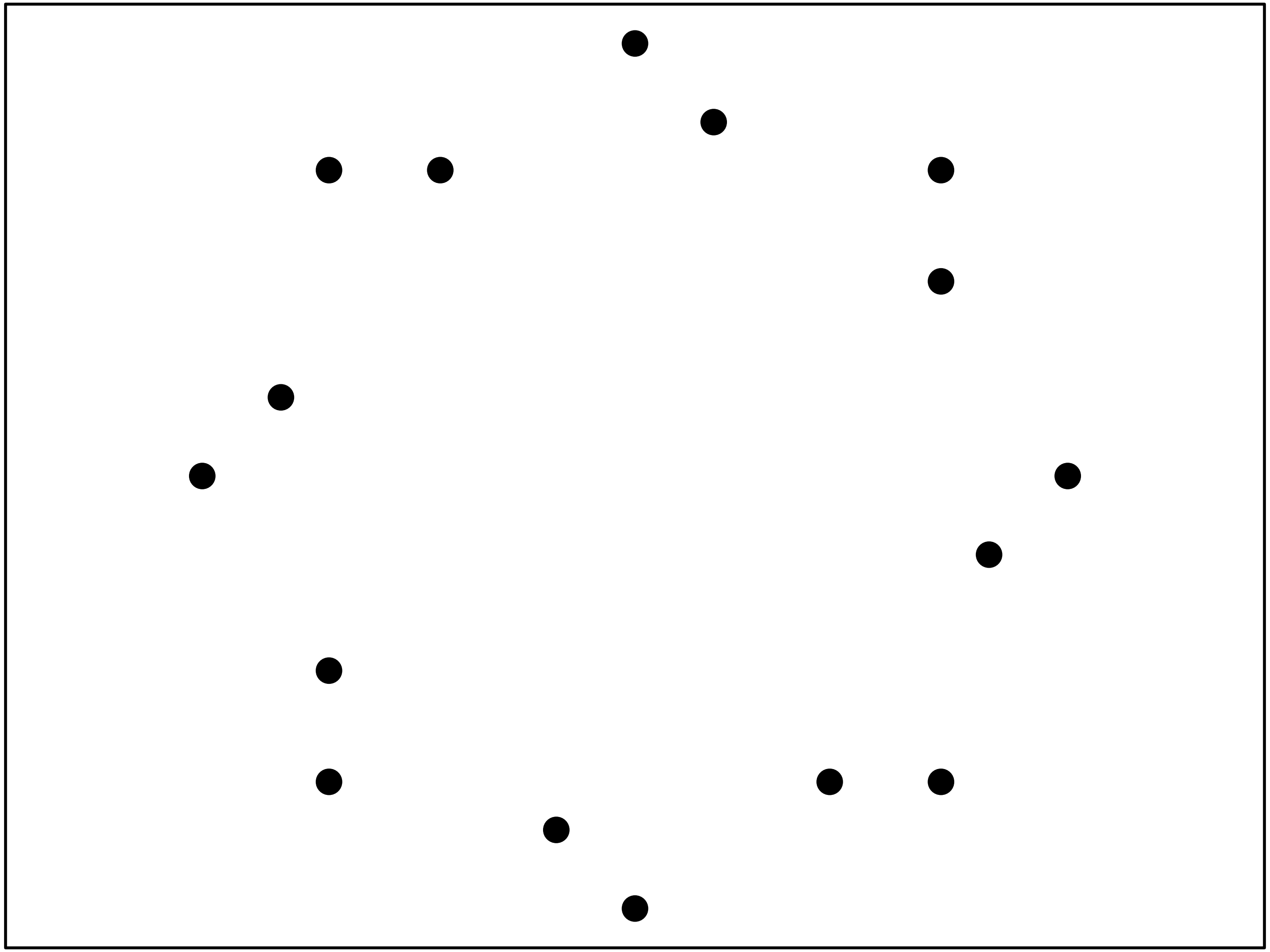


Do m times

Scale d coefficients

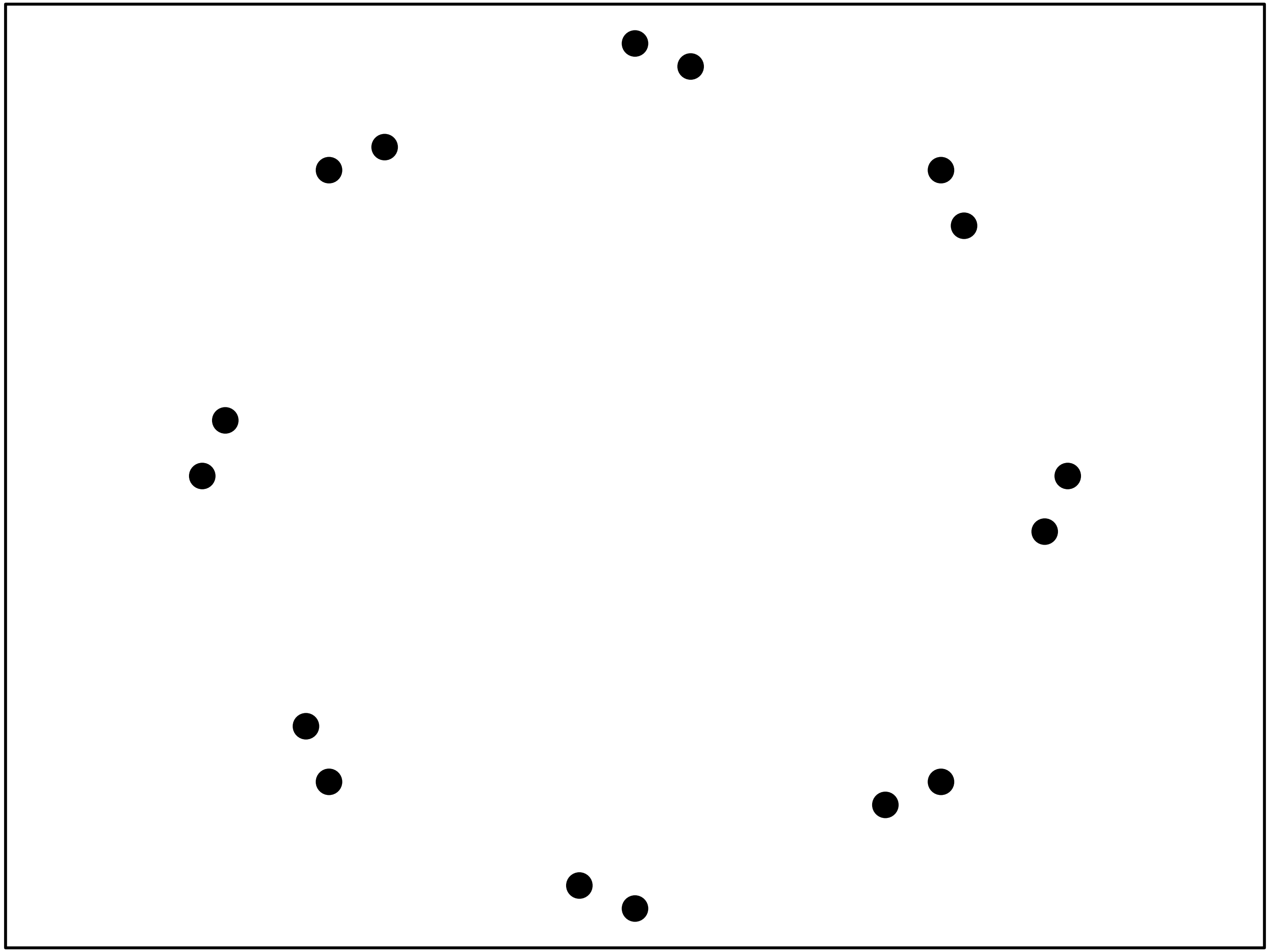
FFT on d/m roots of unity

Hyperbolic approximation computation



Do m times
  $\textsc{Scale}$ d coefficients
  FFT on d/m roots of unity

Hyperbolic approximation computation

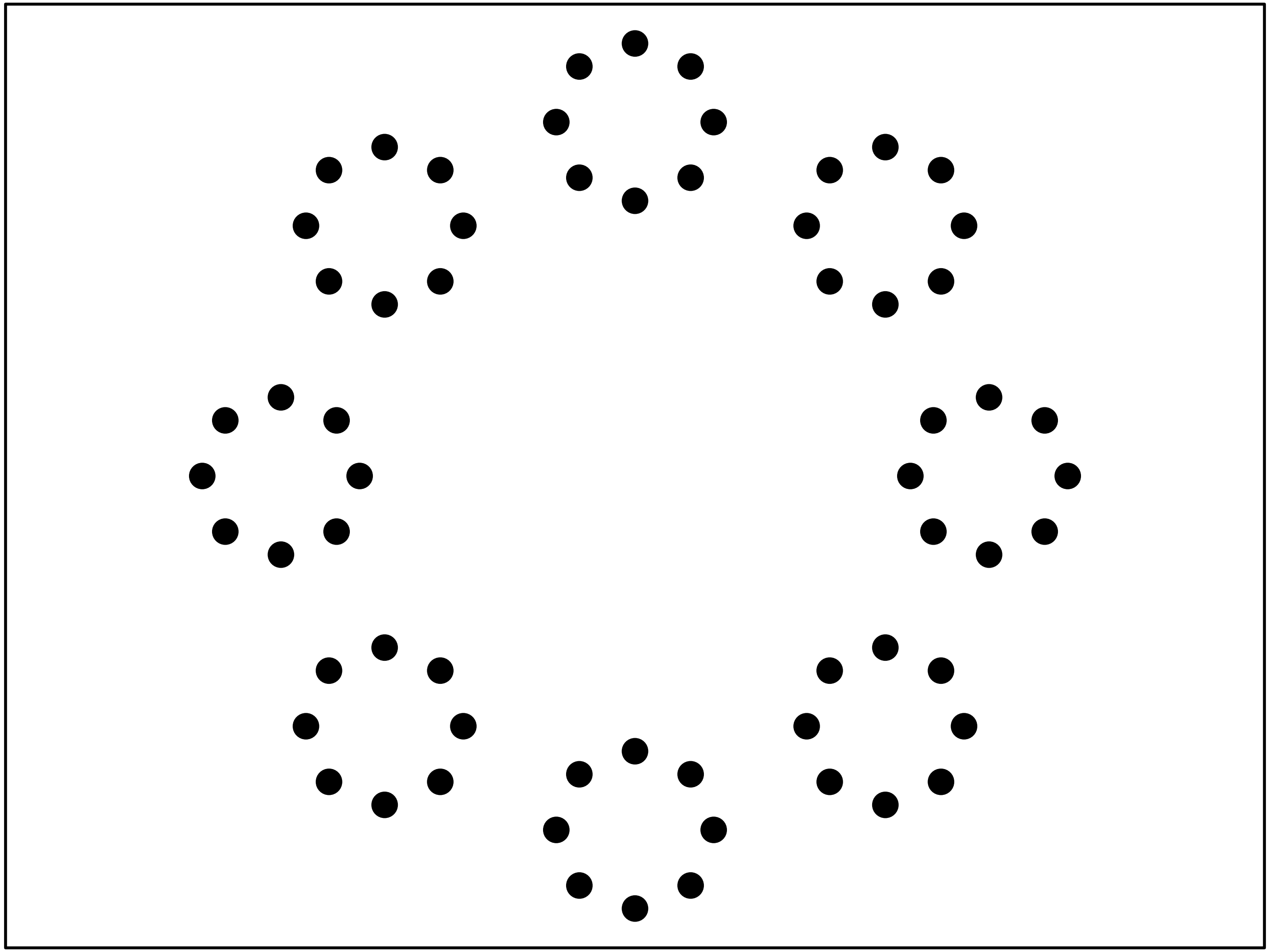


Do m times

  SCALE d coefficients

  FFT on d/m roots of unity

Hyperbolic approximation computation



Do m times

  SCALE d coefficients

  FFT on d/m roots of unity

Hyperbolic approximation complexity

Do m times
  $\textsc{Scale}$ d coefficients
  FFT on d/m roots of unity

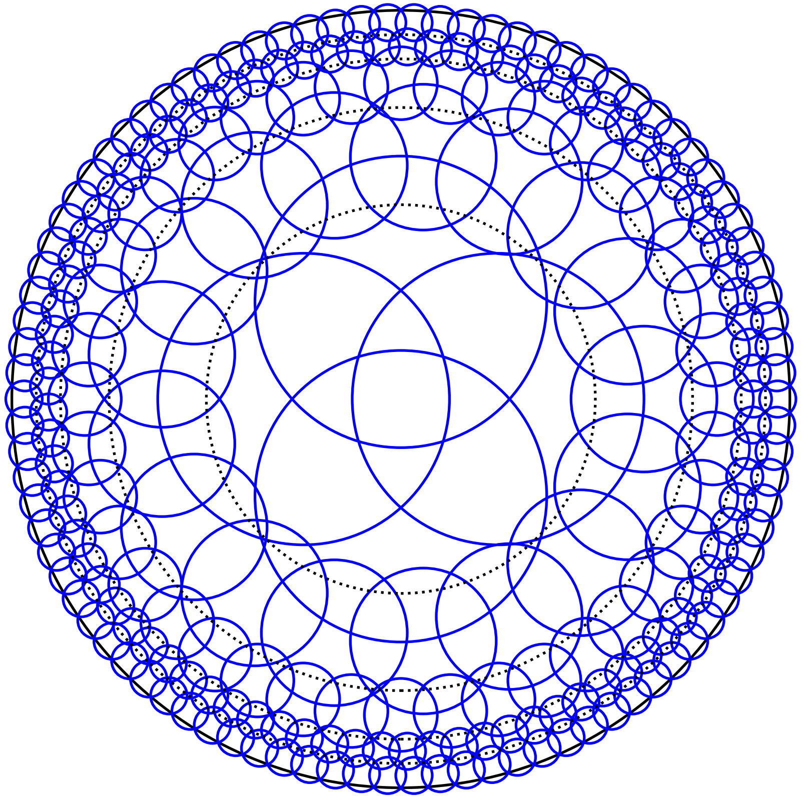
Scale

- Each: $O(dm)$ bit operations
- Total: $O(dm^2)$ bit operations
  $\rightarrow$ Good enough if m is constant
- Total amortized : $\widetilde{O}(dm)$ bit operations
  $\rightarrow$ with fast multipoint evaluation or numerical composition

FFT

- Each: $\widetilde{O}(\frac{d}{m}m)$
- Total: $\widetilde{O}(dm)$

Multipoint evaluation in $\widetilde{O}(dm)$ [New]



INPUT:

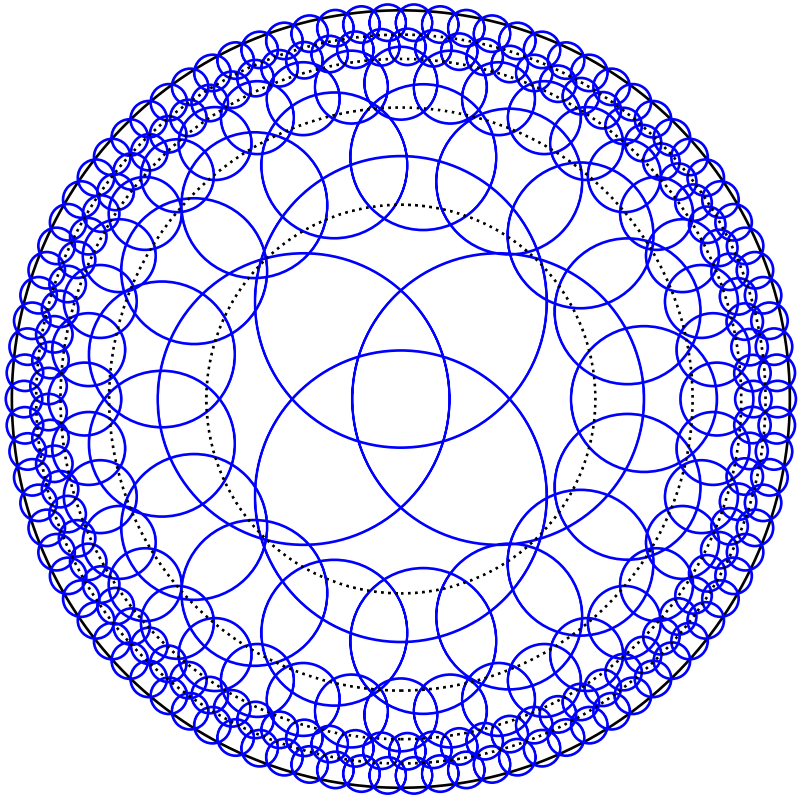
- f polynomial of degree d
- d points z_k
- precision m

OUTPUT:

- y_k such that $|y_k - f(z_k)| < 2^{-m}\|f\|$

Compute m-hyperbolic approximation of f	$\widetilde{O}(dm)$
For each pair of disk D and polynomial g:	$O(d/m)$
QUERY the n_k points in D	$\widetilde{O}(n_k)$
EVALUATE g on the n_k points	$\widetilde{O}(m(n_k + m))$

Root finding in $\widetilde{O}(d \log(\|f\|\kappa))$ [New]



INPUT:

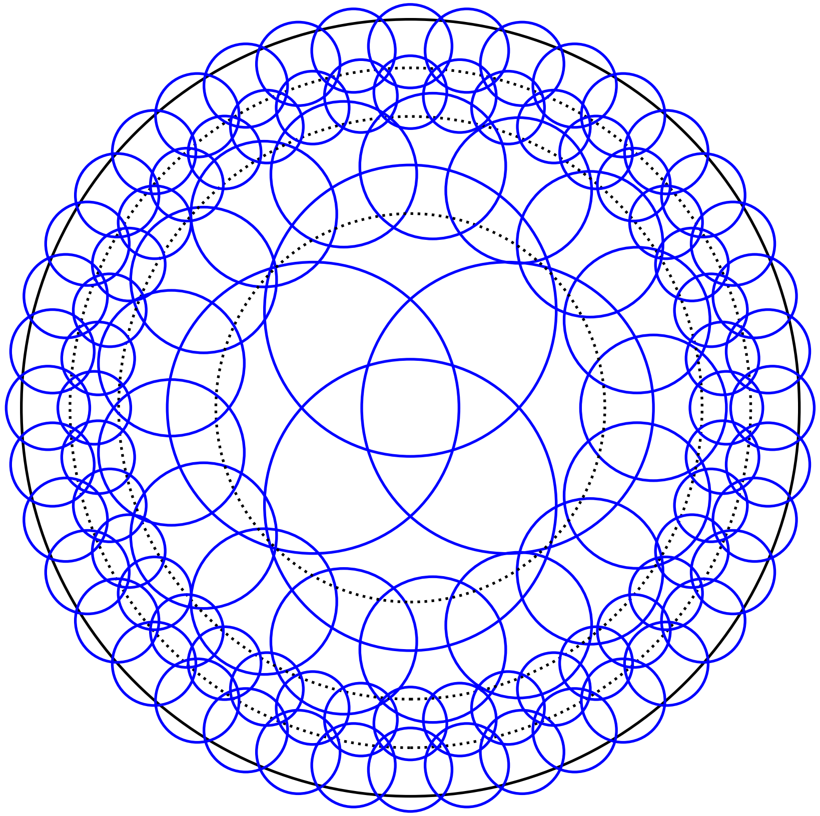
- f squarefree polynomial

OUTPUT:

- d root-isolating disks

Compute 1-hyperbolic approximation of f	$\widetilde{O}(d)$
For each polynomial g:	$O(d)$
APPROXIMATE roots of g	$\widetilde{O}(1)$
COMPUTE enclosing disks	$\widetilde{O}(1)$
Check if we have d isolating disks	$\widetilde{O}(d)$

Root finding in $\widetilde{O}(d \log(\|f\|\kappa))$ [New]



INPUT:

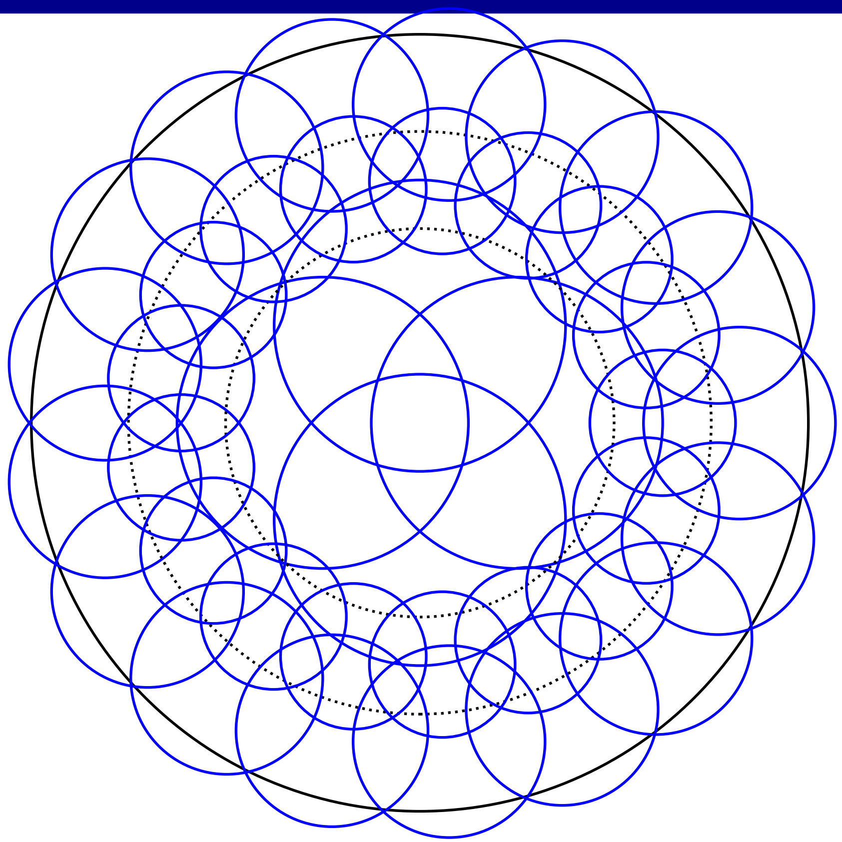
- f squarefree polynomial

OUTPUT:

- d root-isolating disks

Compute 2-hyperbolic approximation of f	$\widetilde{O}(d)$
For each polynomial g:	$O(d)$
APPROXIMATE roots of g	$\widetilde{O}(1)$
COMPUTE enclosing disks	$\widetilde{O}(1)$
Check if we have d isolating disks	$\widetilde{O}(d)$

Root finding in $\widetilde{O}(d\log(\|f\|\kappa))$ [New]



INPUT:

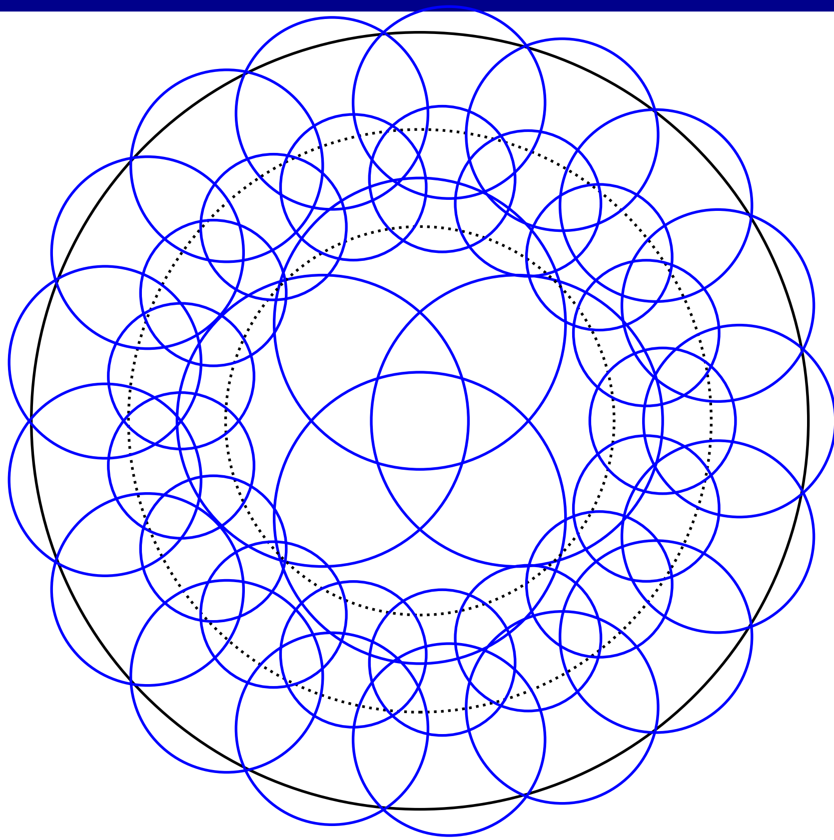
- f squarefree polynomial

OUTPUT:

- d root-isolating disks

Compute m-hyperbolic approximation of f	$\widetilde{O}(dm)$
For each polynomial g:	$O(d/m)$
APPROXIMATE roots of g	$\widetilde{O}(m^2)$
COMPUTE enclosing disks	$\widetilde{O}(m^2)$
Check if we have d isolating disks	$\widetilde{O}(dm)$

Root finding in $\widetilde{O}(d\log(\|f\|\kappa))$ [New]



INPUT:

- f squarefree polynomial

OUTPUT:

- d root-isolating disks

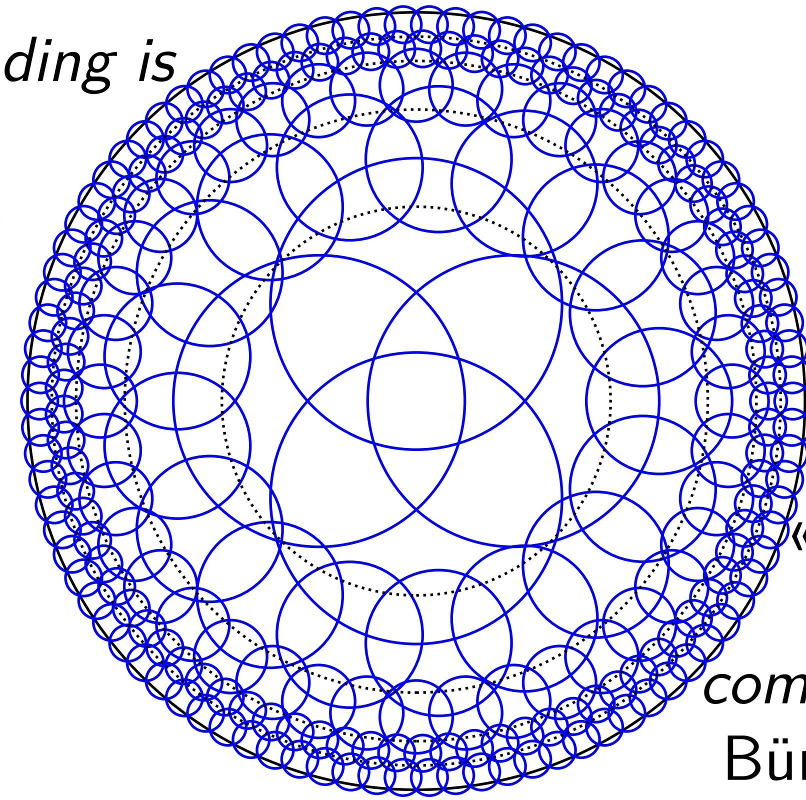
COMPLEXITY:

- $\widetilde{O}(dm)$ bit operations
- m in $\widetilde{O}\left(\log(\|f\|\kappa)\right)$

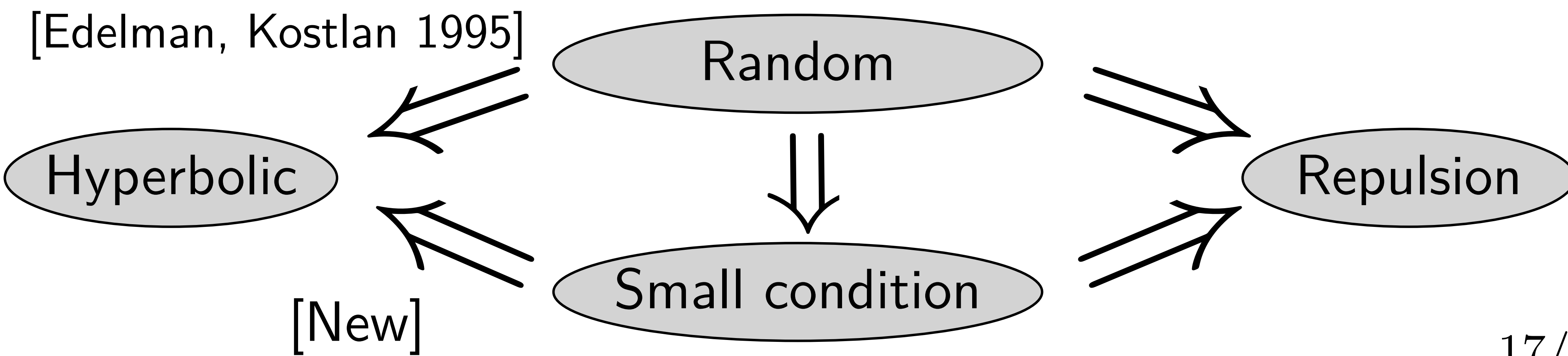
Compute m-hyperbolic approximation of f	$\widetilde{O}(dm)$
For each polynomial g:	$O(d/m)$
APPROXIMATE roots of g	$\widetilde{O}(m^2)$
COMPUTE enclosing disks	$\widetilde{O}(m^2)$
Check if we have d isolating disks	$\widetilde{O}(dm)$

Roots distribution

«Polynomial rootfinding is an ill-conditioned problem in general»
Trefethen and Bau



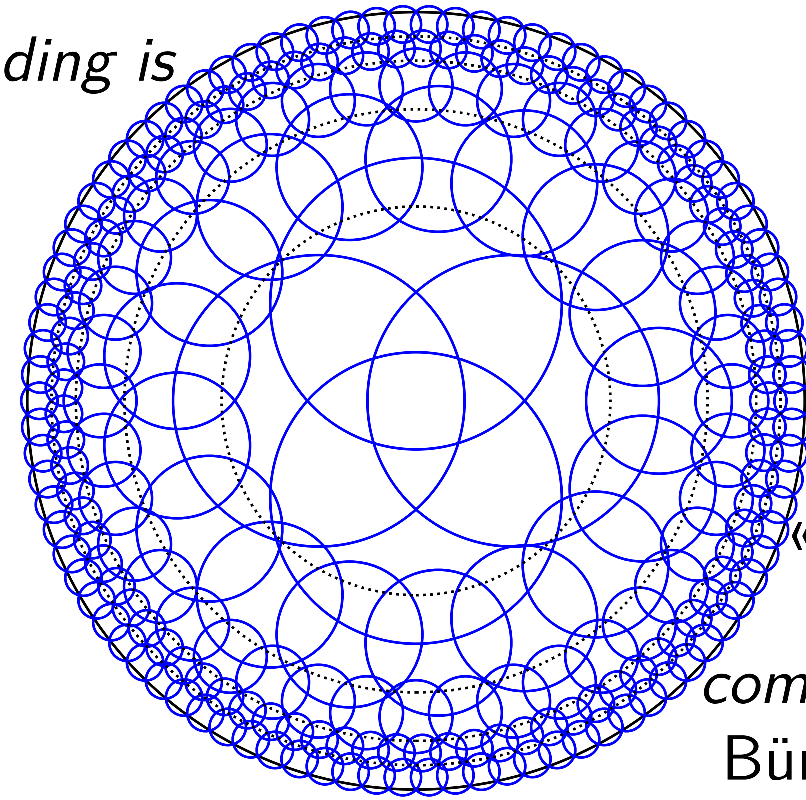
«Typical polynomials are well-conditioned for the computation of their zeros»
Bürgisser, Cucker, Cardozo



Roots distribution

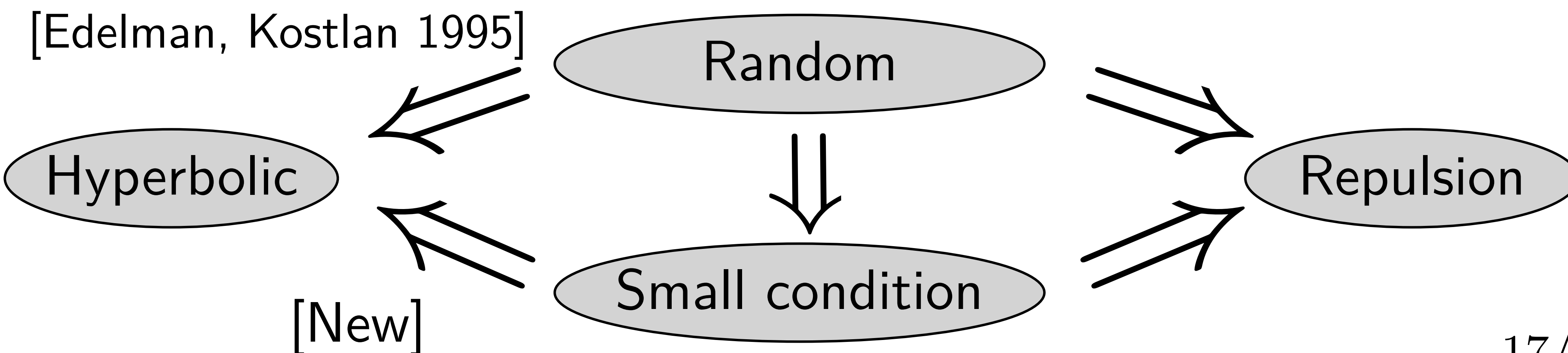
«*Polynomial rootfinding is an ill-conditioned problem in general*»
Trefethen and Bau

For uniform distribution of roots



For uniform distribution of coefficients

«*Typical polynomials are well-conditioned for the computation of their zeros*»
Bürgisser, Cucker, Cardozo



End of the story?

Ongoing work

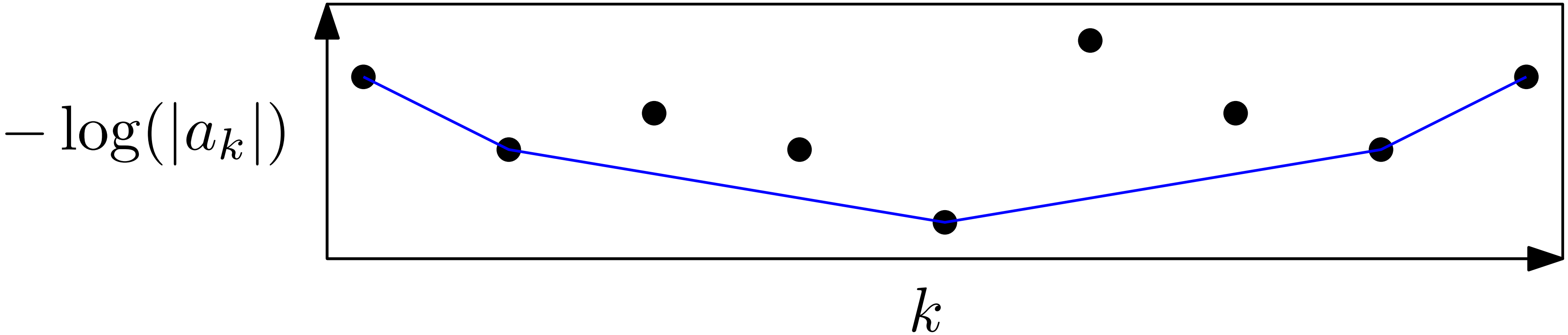
$$f^+(z) = |a_0| + \cdots + |a_d||z|^d$$

Adaptive approximation

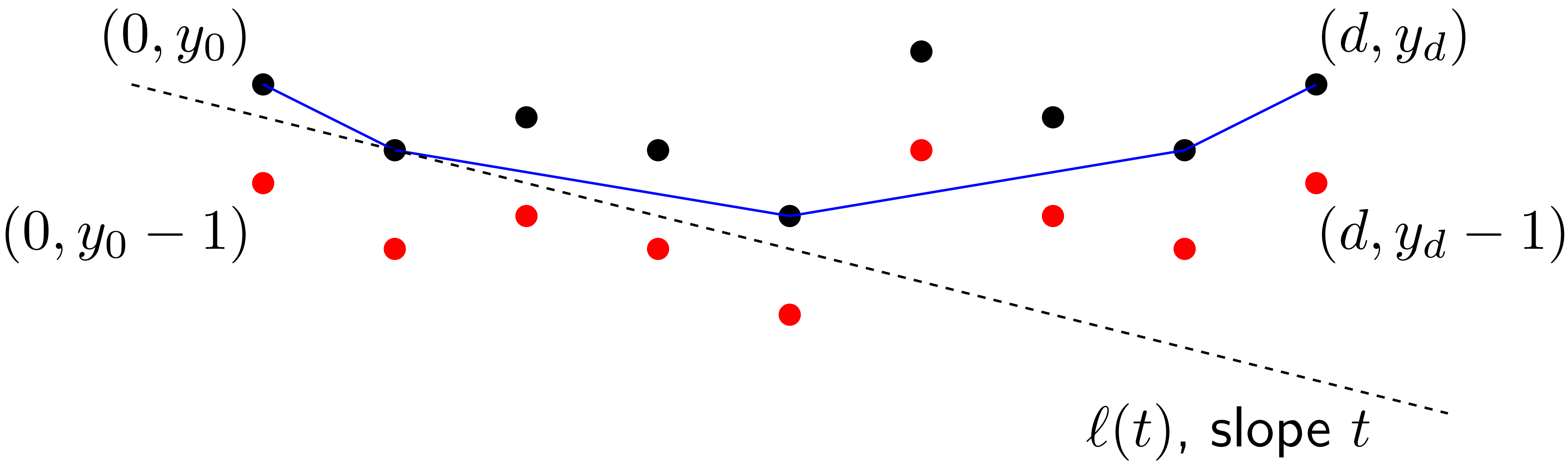
$$\|f(\gamma + \rho z) - g(z)\| \leq 2^{-m} f^+(z)$$

Based on Newton polygon

- Used in MPSolve for initial root module estimation
- Can be used for adaptive repartition of disks



Complexity: a geometric problem



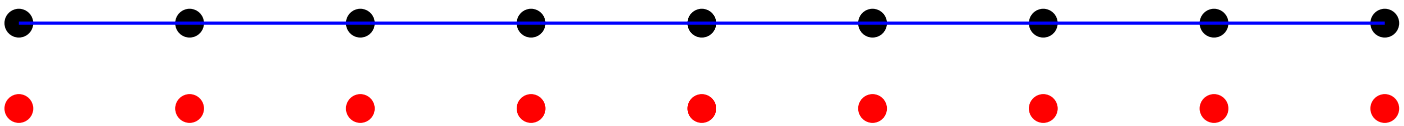
Open question

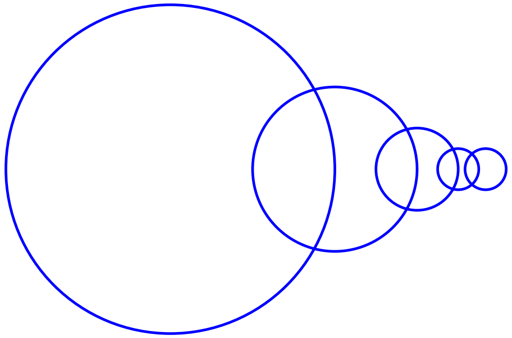
Let $n(t)$ be the number of red points below $\ell(t)$.

$$\int_{t=-1}^{1} n^2(t)\, dt = \widetilde{O}(d) \ ?$$

Complexity: a geometric problem

Case $|a_k| = 1$



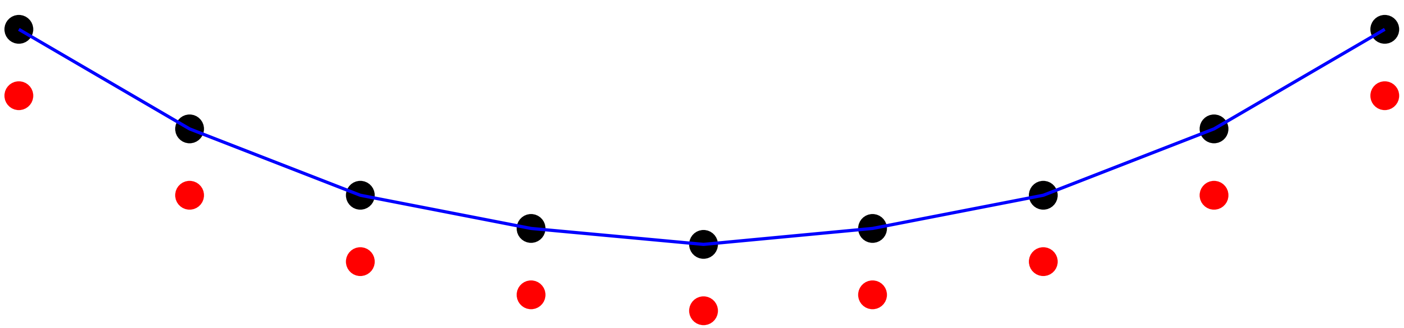


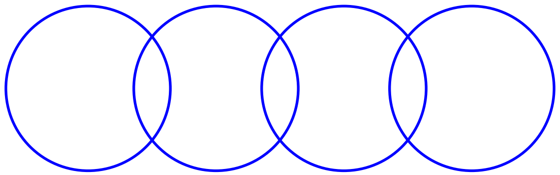
$$n(t) \leq \min(\tfrac{1}{t}, d) \Rightarrow \widetilde{O}(d)$$

artanh(γ) uniform

Case $|a_k| = \sqrt{\binom{d}{k}}$

[M. 2021]





$$n(t) = O(\sqrt{d}) \Rightarrow \widetilde{O}(d)$$

arctan(γ) uniform

Thank you!