Random Polynomial Dilations

January 28, 2022 12:24 PM

Let $f \in K[x,y,z]$ be non-zero, K is a field e.g. $K = \mathbb{Z}_p$.

Let $\alpha, \beta, \gamma \in K$ be non-zero.

Let $\hat{f} = f(\alpha x, \beta y, \gamma z)$ a "dilation" of f.

This mapping $\hat{f} : K[x,y,z] \to K[x,y,z]$ is invertible.

The inverse is $\hat{f}(x/\alpha, y/\beta, z/\gamma) = f$.

Let $f = \sum_{i=1}^{t} a_i M_i(x,y,z)$ where $a_i \in K \backslash \{0\}$ and M_i are monomials.

Let $M = x^i y^j z^k$

$$\hat{M} = M(\alpha x, \beta y, \gamma z) = (\alpha x)^i (\beta y)^j (\gamma z)^k$$
$$= \alpha^i \beta^j \gamma^k x^i y^j z^k$$
$$= M(\alpha, \beta, \gamma) \cdot M(x,y,z).$$

$$\hat{f} = \sum_{i=1}^{t} [a_i \underbrace{M_i(\alpha,\beta,\gamma)}_{\neq 0}] M_i(x,y,z)$$

The support does not change.

$\Rightarrow$ t doesn't change

$\Rightarrow$ f is sparse $\Rightarrow$ $\hat{f}$ is sparse.

$\Rightarrow$ degrees don't change.

Theorem. f is irreducible over K $\Leftrightarrow$ $\hat{f}$ is irreducible over K.

Theorem Let $a, b \in K[x,y,z]$, $g = \gcd(a,b)$ and let $\hat{h} = \gcd(\hat{a}, \hat{b})$ $\hat{g}$

Then $\hat{h} \sim \hat{g}$ $\Rightarrow$ $\hat{h} \mid \hat{g}$ and $\hat{g} \mid \hat{h}$.

Idea: Use a random dilation (pick $\alpha, \beta, \gamma \in K \setminus \{0\}$ at random) to deal with unlucky/bad/problem evaluation points in a modular gcd algorithm.

2 terms $\Rightarrow \geq 4$ evaluation points.

Example. Let $g = 1 \cdot x^2 + (2y^2 + 5 \cdot y^0)$

$\bar{a} = x^2 + yx + z$

$\bar{b} = x^2 + (y-4)x + yx + z$

$a = g\bar{a}$

$b = g\bar{b}$

$\gcd(a, b) = g$.

$y = 4$ is an unlucky evaluation point.

Let $r = \mathrm{res}(\bar{a}, \bar{b}, x) = 2(y-4)^2 \Rightarrow y = 4$ is the only unlucky one.

In Ben-Or/Tiwari the evaluation points would be

$y = \boxed{\boxed{2^0, 2^1, 2^2, 2^3}, 2^4, 2^5}, \ldots$

...

Consider $\hat{a} = a(x, \beta y)$ random dilation.

$\hat{b} = b(x, \beta y)$

$\hat{h} = \gcd(\hat{a}, \hat{b})$

$\bar{a} = x^2 + yx + z$

$\bar{b} = x^2 + (y-4)x + yx + z$

$\hat{a} = x^2 + \beta y + z$

$\hat{b} = x^2 + (\beta y - 4) + \beta y x + z$

$= 0$

We moved the unlucky $y = 4$ to $y = 4 \cdot \beta^{-1}$

If $\beta \in [1, p-1]$ at random then $\beta^{-1} \in [1, p-1]$ is random.

In Ben-Or/Tiwari, instead of using

$$v_j = f(2^j, 3^j, 5^j) \quad \text{for } j = 0, 1, \dots, 2T-1$$

Let $g(x,y,z) = f(\alpha x, \beta y, \gamma z)$ Then use

$$\hat{v}_j = g(2^j, 3^j, 5^j) = f(\alpha 2^j, \beta 3^j, \gamma 5^j) \quad \text{for } 0 \le j < 2T.$$

Evaluating $\hat{f}$.

Case f is a Black Box. Assume $\alpha, \beta, \gamma \in K \setminus \{0\}$ are random.

```
g := proc(x, y, z, p)
    f(α·x mod p, β·y mod p, γ·z mod p, p);
end;
```

n multiplications per evaluation of f.

Case: $\displaystyle = \sum_{i=1}^{t} a_i \cdot M_i(x,y,z)$

Compute $d_i = M_i(\alpha, \beta, \gamma)$

$m_i = M_i(2, 3, 5)$.

$$\hat{v}_j = f(\alpha 2^j, \beta 3^j, \gamma 5^j) = \sum_{i=1}^{t} a_i M_i(\alpha 2^j, \beta 3^j, \gamma 5^j) = \sum_{i=1}^{t} a_i d_i m_i^j$$

$j = 0, 1, \dots$

Initialize

$C := \boxed{a_1 d_1 \mid a_2 d_2 \mid \cdots \mid a_t d_t}$

$M := \boxed{m_1 \mid m_2 \mid \cdots \mid m_t}$

Extra Cost is to compute $d_i = M_i(\alpha, \beta, \gamma)$ and t mults

$$\hat{v}_0 = f(\alpha \cdot 1, \beta \cdot 1, \gamma \cdot 1) = \sum_{i=1}^{t} C_i$$

$C := \boxed{C_i \cdot M_i = a_i d_i m_i \ : \ 1 \le i \le t}$

$$\hat{V}_1 = f(\alpha\cdot 2, \beta\cdot 3, \gamma\cdot 5) = \sum_{i=1}^{t} c_i$$

$$C := \boxed{c_i \cdot M_i \;:\; 1 \le i \le t.}$$

$$\hat{V}_2 := \sum_{i=1}^{t} c_i .$$

Reference: Mark Giesbrecht and Daniel Roche.
"Diversification Improves Interpolation" ISSAC 2011.

Let $f \in K[x]$, $d = \deg(f)$. $f = \sum_{i=1}^{t} a_i x^{e_i}$

Choose $\alpha \in S \subset K \setminus \{0\}$ at random.

Theorem: $f(\alpha x)$ has distinct coefficients with prob. $\geq \frac{\binom{t}{2} d}{|S|}$

For $f = \sum_{i=1}^{t} \underline{a_i} x^{e_i}$ $f(\alpha x) = \sum_{i=1}^{t} a_i \alpha^{e_i} x^{e_i}$

not distinct.   distinct w.h.p.

Proof. Suppose $a_i \alpha^{e_i} = a_j \alpha^{e_j}$

$\Rightarrow$ $h(\alpha) = 0$ where $h(x) = a_i x^{e_i} - a_j x^{e_j}$.

$$\text{Prob}[\,h(\alpha) = 0\,] \le \frac{\max(e_i, e_j)}{|S|} \le \frac{d}{|S|}.$$

pairs of coefficients.

$$\text{Prob}\left[\begin{array}{c} a_i \alpha^i = a_j \alpha^j \text{ for} \\ \text{some } 1 \le i < j \le t \end{array}\right] \le \frac{\binom{t}{2} d}{|S|}$$