The Total Degree

November 23, 2023 10:44 AM

Lemma (Schwartz–Zippel 1978).

Let $f \in D[x_1, \dots, x_n]$, D an integral domain, $f \neq 0$.

Let S be a finite subset of D ($|S| > 10^9$).

If $\alpha_1, \alpha_2, \dots, \alpha_n$ are chosen at random from S then

$$\text{Prob}[\, f(\alpha_1, \dots, \alpha_n) = 0 \,] \leq \frac{\deg(f)}{|S|}.$$

Equivalently, the # of roots of $f \leq \deg(f) \cdot |S|^{n-1}$.

Ex. Find $f \in \mathbb{Z}_p[x,y]$ s.t. $\deg(f) = d$ and ($S = \mathbb{Z}_p$). f has $d \cdot p$. Assume p is large.

NB: D must be an integral domain.

For $n=1$ S-Z says # roots $\leq \deg(f)$.

Consider $D = \mathbb{Z}_8$ and $f = x(x-2)$. roots $= 0, 2, 4, 6$.

Let $B : D^n \to D$ be a black-box for $f \in D[x_1, \dots, x_n]$.

Let $d_i = \deg(f, x_i)$. How can we compute d_i?

E.g. $f = 3x_1^2 x_2^2 + 2x_1^2 x_2 x_3 - 3x_2 x_3^2 + 5x_3 \in \mathbb{Z}[x_1, x_2, x_3]$.

For $i=1$ $d_1 = \deg(f, x_1) = 2$.

$$f = \sum_{i=0}^{d_1} f_i(x_2, x_3) \cdot x^i = \underbrace{(3x_2^2 + 2x_2 x_3)}_{f_2} \cdot x_1^2 + \overbrace{}^{f_1 = 0} \underbrace{(-3x_2 x_3^2 + 5x_3)}_{f_0} \cdot x_1^0$$

$\uparrow$ $f_2(\beta_2, \beta_3) = 0$.

① Let S be a large subset of $\mathbb{Z}$.

Pick $\beta_2, \beta_3 \in S$ at random.

Let $g(x) = f(x, \beta_2, \beta_3)$.

$$\Pr[\deg(g) \neq \deg(f, x_1)] = \Pr[f_2(\beta_2, \beta_3) = 0] \leq \frac{\deg(f_2)}{|S|} \leq \frac{\deg(f)}{|S|}.$$

② Let B_g be a black-box for $g(x)$.

```
Bg := proc( alpha :: [integer] )
        B([alpha[1], β2, β3])
end;
return GetDegree( Bg ).
```

Let $B : D^n \to D$ be a black-box for $f \in D[x_1, \ldots, x_n]$.

Let $d = \deg(f)$ be the total degree of f.

How can we compute d?

E.g. $f = 3x_1^3 + 2x_1x_2^2x_3 + 4x_2^2x_3^2 + 7x_1^1x_3^4 - 7x_2^3x_3^2 \in \mathbb{Z}[x_1, x_2, x_3]$.

Consider $g(z) = f(z, z, z) = z^3(3) + z^4(2+4) + z^5(7-7)$.

Notice $\deg(g) \neq \deg(f) = 5$.

① Let S be a large finite subset of $\mathbb{Z}$.

Pick $\beta_1, \beta_2, \ldots, \beta_n$ from S at random.

② Let B_h be a black box for

$$h(z) = f(\beta_1 z, \beta_2 z, \ldots, \beta_n z) \doteq z^3(3\beta_1^3) + z^4(2\beta_1\beta_2^2\beta_3 + 4\beta_2^2\beta_3^2) + z^5(7\beta_1\beta_3^4 - 7\beta_2^3\beta_3^2)$$

return GetDegree(B_h).

Let $f = \sum_{i=0}^{d=\deg(f)} f_i(x_1, \ldots, x_n)$ where each term in f_i has degree i.

$f_0 = f_1 = f_2 = 0 = \underbrace{3x_1^3}_{f_3} + \underbrace{(2x_1x_2^2x_3 + 4x_2^2x_3^2)}_{f_4} + \underbrace{(7x_1x_3^4 - 7x_2^3x_3^2)}_{f_5}$

We have $\deg(h) \neq \deg(f) = d \iff f_d(\beta) = 0$.

$$\text{Prob}[f_d(\beta) = 0] \leq \frac{\deg(f_d)}{|S|} = \frac{d}{|S|}.$$

We would like to have a numerical bound $D \geq \deg(f) = d$.