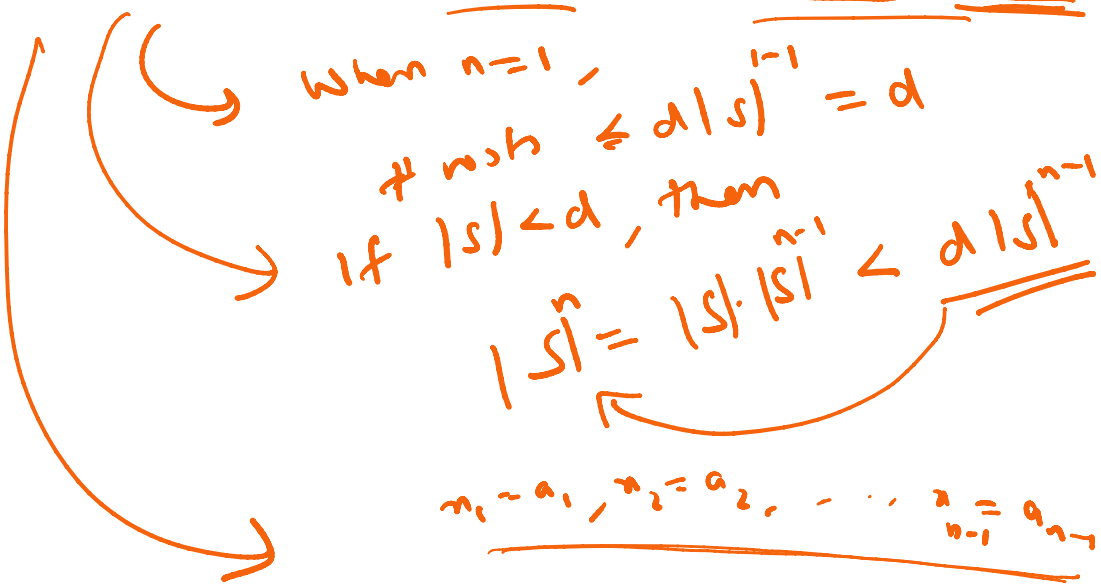
04 December 2020 14:07

We know, for single variable polynomials, a non-zero polynomial of degree d has at most d roots.

↓ Generalizing

Lemma [DeMillo–Lipton–Schwartz–Zippel lemma] (1978, 79, 80)

For every field $S \subseteq \mathbb{F}$ of $|S| \geq d$ field elements, every non-zero polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d can have at most $d|S|^{n-1}$ roots in S^n.



Proof by induction on n.

Base Case: $n=1$. We know.

Induction Step: We re-write $f(x)$ as

Induction step: We re-write $f(x)$ as

$3x_1^3 x_2^{n_2} \cdots x_n^{n_n}$

$x = (x_1, x_2, \ldots, x_n)$

$$f(x) = f_0 + f_1 x_n + f_2 x_n^2 + \cdots + f_t x_n^t$$

where (i) f_t is not identically zero

(means f_t does not evaluate to zero on all $a \in S^{n-1}$)

(ii) Every $f_i \in \mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$

The question now is: For how many $(a,b) \in S^{n-1} \times S$, does $f(a,b) = 0$?

($S^n = S \times S \times S \times \cdots \times S$, n times)

Proof by splitting into two cases:

Case 1: $f_t(a) = 0$

First of all, for how many $a \in S^{n-1}$ is $f_t(a) = 0$? $a \in S^{n-1}$

Ans: (by Ind hyp) $(d-t)|S|^{n-2}$

Therefore, no. of $(a,b) \in S^{n-1} \times S$ for which $f_t(a) = 0$ and $f(a,b) = 0$ is at most $(d-t)|S|^{n-2} \times |S| = (d-t)|S|^{n-1}$ (1)

$\cdots \quad (d-1)|S|^{n-1} \quad \cdots \quad (d-t)|S|^{n-1}$ → (1)

Case 2: $f_t(a) \neq 0$.

For each $a \in S^{n-1}$, we have a polynomial in one variable (which is x_n)

$$f_0(a) + f_1(a)\, x_1 + \cdots + f_t(a)\, x_n^t$$

By induction hyp, this polynomial has at most t roots in S. Therefore, in this case, no. of $(a,b) \in S^{n-1} \times S$ for which $f(a,b) = 0$ is at most

$$|S|^{n-1} \times t = t|S|^{n-1} \quad \text{→ (2)}$$

Total no. of $(a,b) \in S^{n-1} \times S$ for which $f(a,b) = 0$ is at most

$$(1) + (2) = (d-t)|S|^{n-1} + t|S|^{n-1}$$

$$= d|S|^{n-1}$$

Applications in polynomial identity testing

Given a multivariate polynomial $f \in \mathbb{F}[x_1, x_2 \ldots, x_n]$ of degree d,

Q. Is f a zero polynomial?

Can be used to answer whether $f_1(x_1, x_2, \ldots, x_n) = f_2(x_1, x_2 \ldots, x_n)$

$$(c_1 + c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n)(c_2 + c_{21}x_1 + \cdots + c_{2n}x_n)$$

$$(\quad . \quad) \cdots (c_d + c_{d1}x_1 + \cdots + c_{dn}x_n)$$

simplification

$$O\binom{n+d}{d} \text{ time.}$$

No good deterministic algo known.

What about a randomized algo?

Lemma [Recurring DeMillo-Lipton-Schwartz-]

Lemma [Rewriting DeMillo-Lipton-Schwartz-Zippel lemma in a different form]

Suppose that $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a non-zero polynomial of degree d and $S \subseteq \mathbb{F}$ is non-empty. Then,

$$\Pr\left[f(\overbrace{r_1, r_2, \ldots, r_n}^{\in S^n}) = 0 \right] \leq \frac{d}{|S|} = \frac{d|S|^{n-1}}{|S|^n}$$

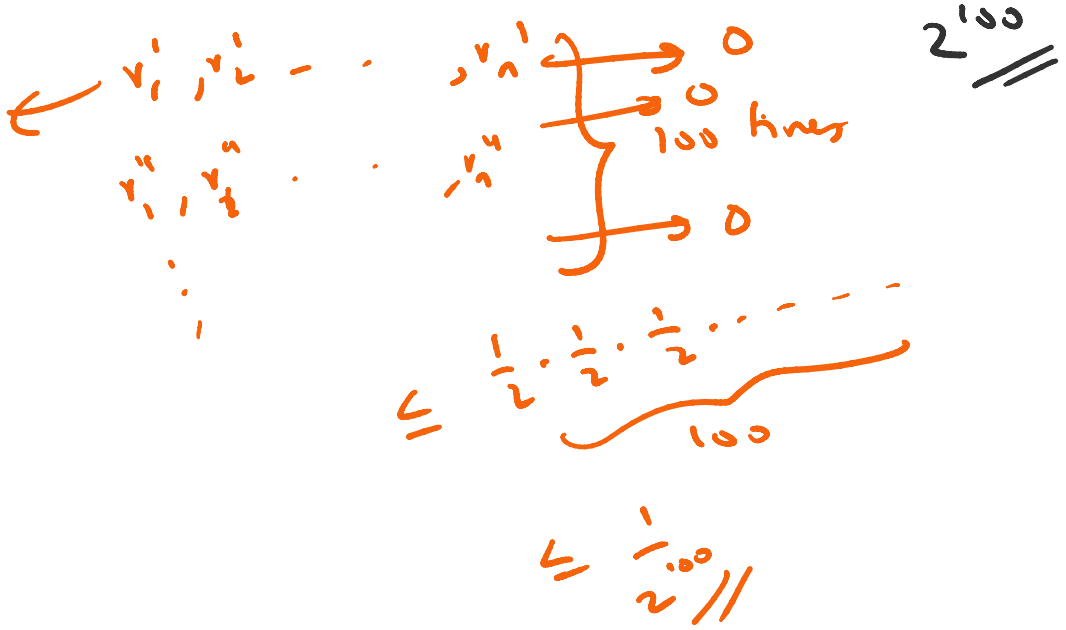
where every r_i is independently and uniformly at random chosen from S.

□

Take S s.t. $|S| = 2d$. Suppose $f \in \mathbb{F}[x_1, x_2, \ldots, x_n)$ is not a zero polynomial. Indep and uniformly at random chosen $r_1, r_2, \ldots, r_n$ from S.

$$\Pr\left[f(r_1, r_2, \ldots, r_n) = 0 \right] \leq \frac{d}{|S|} = \frac{d}{2d} = \frac{1}{2}$$

Repeating the above experiment say 100 times, our error probability $\leq \frac{1}{2^{100}}$



$$\leq \underbrace{\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots}_{100}$$

$$\leq \frac{1}{2^{100}}$$