Part II polyn. Methods

§1 Schwartz-Zippel Lemma

Recall

Lem 1. f non-zero, deg $< p$, polyn. on $\mathbb{F}_p^n$

$\Rightarrow$ f does NOT vanish on $\mathbb{F}_p^n$.

- S-Z says multivar. low-deg polyn. cannot have too many roots.
- Useful for polyn identity testing.

Lem [Schwartz-Zippel] $f \in \mathbb{F}_p[x_1, \cdots, x_n]$

f n-var., non-zero, deg-d polyn. on $\mathbb{F}_p^n$, $d < p$

$\Rightarrow$ f has $\leq dp^{n-1}$ roots.

Pf: • $\forall\, a, z \in \mathbb{F}_p^n$, $z \neq 0$ line $L = \{at + z : t \in \mathbb{F}_p\}$

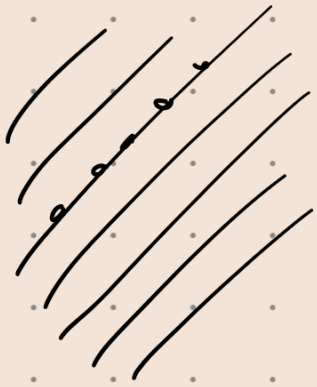
Consider the restriction of f on L, denoted by f_L

FACT $\Rightarrow$ f_L: deg-d univar. (in t) w./ leading coeff. $f_d(z)$, where f_d = deg-d part of f.

- As f_d is non-zero, and $d < p$,

Lem 1 $\Rightarrow$ $\exists\, z \neq 0$ s.t. $f_d(z) \neq 0$.

$\Rightarrow$ f_L is non-zero, deg-d



$\Rightarrow \leq d$ roots on L.

- $\mathbb{F}_p^n$ can be partitioned into p^{n-1} lines in direction z (parallel to L).

$\Rightarrow \leq d \cdot p^{n-1}$ roots in $\mathbb{F}_p^n$ ▨

Rmk: • Sharp: e.g. f depends only on x_1.

• Can also bound # roots in a finite subset.

Lem [S-Z, prob. version]

- f n-var. non-zero deg-d polyn over a field K.
- $S \subseteq K$ a finite subset.
- $r_1, \dots, r_n$ unif indep. ele^t. of S.

$\Rightarrow \Pr(f(r_1, \dots, r_n) = 0) \leq \frac{d}{|S|}$

Pf: • Induct on n:

base case $n=1$, univar. poly deg-d $\Rightarrow \leq d$ roots

• Write f as a polyn in x_1:

$$f(x_1, \dots, x_n) = \sum_{i=0}^{d} x_1^i \cdot f_i(x_2, \dots, x_n)$$

• f non-zero $\Rightarrow$ Take max i, f_i is non-zero

$\deg f_i \le d - i$

- Let $r_1, \dots, r_n \sim S$ indep.

  Def events $\begin{cases} A = \{ f(r_1, \dots, r_n) = 0 \} \\ B = \{ f_i(r_2, \dots, r_n) = 0 \} \end{cases}$

- $\Pr(A) = \Pr(A \cap B) + \Pr(A \cap B^c)$

  $= \Pr(A|B)\Pr(B) + \Pr(A|B^c)\Pr(B^c)$

  $\le \Pr(B) + \Pr(A|B^c)$ b/c $B^c \equiv f_i(x_2, \dots, x_n) \neq 0$

  $\le \frac{d-i}{|S|} + \frac{i}{|S|}$ $f(x_1, r_2, \dots, r_n)$ non-zero w/ deg $= i$

  (IH) $\uparrow$ on f_i

  $\le d/|S|$ ▨.

§2 Testing polyn. identity & existence of perfect matching

§2.1 Polyn. id. testing.

Q: How do we test whether two given polyn. on $\mathbb{F}_p^n$ are the same, i.e. $f = g$?

- One can check the coeff. of all monomials.

but too many term (n^d if deg is d)

Probabilistic Alg Suppose $f \neq g \Rightarrow f-g$ is nonzero, $\deg \leq d$

Want to tell $f-g \not\equiv 0$

- Pick $r = (r_1, \dots, r_n)$ w/ r_i unif in $\mathbb{F}_p$ indep.

$$[S\text{-}Z] \Rightarrow \Pr\left((f-g)(r)=0\right) \leq d/p$$

- Repeat k times $\Rightarrow \Pr\left((f-g) \text{ vanishes on all } k \text{ choices}\right) \leq \left(\frac{d}{p}\right)^k \leq \varepsilon$

So if say $d/p < 1/2$, need $k = O(\log 1/\varepsilon)$

- Only need test $O(\log 1/\varepsilon)$ to have prob $\geq 1-\varepsilon$ to test it correctly.

  - if some outcome $\neq 0$ $\Rightarrow f \neq g$
  - if all outcomes $= 0$ ← { $f = g$ ✓ ; $f \neq g$ $\Pr \leq \varepsilon$ }

∎

§2.2 Testing existence of PM.

Q: How to test whether a given bipartite graph

has a perfect matching (PM)?

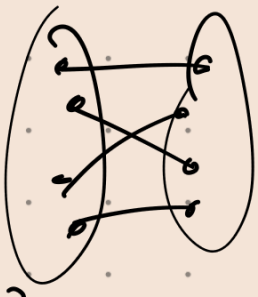
Shall see: G has NO PM $\iff$ certain polyn is 0-polyn (determ. of a matrix)

Def: (Edmonds matrix) Given an $n \times n$-vertex bipartite graph G w/ vxs $u_1, \dots, u_n, v_1, \dots, v_n$.

its Edmonds matrix A is the $n \times n$ matrix w/ variables ↑ entries correp. to edges of G.

i.e. $A = (a_{ij})$, $a_{ij} = \begin{cases} x_{ij} & \text{if } u_i v_j \in E(G) \\ 0 & \text{o.w.} \end{cases}$

- $\det(A)$ is a polyn in $e(G)$ many variables w/ deg $\leq n$



- Identify PM of G w/ perm. in S_n: $\{(u_1, v_{\pi(1)}), \dots, (u_n, v_{\pi(n)})\}$

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi(1)} \cdots a_{n,\pi(n)}$$

↑ non-zero only when π is a PM

$$(*) \cdots = \sum_{\pi \in PM(G)} \operatorname{sgn}(\pi)\, x_{1,\pi(1)} \cdots x_{n,\pi(n)}.$$

Lem G has no PM $\Leftrightarrow$ $\det(A)$ is 0-polyn.

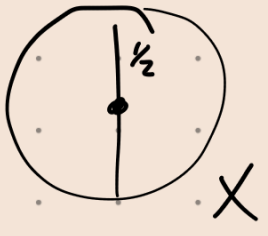
Pf: ($\Rightarrow$) by $(*)$

($\Leftarrow$) Exer. (try to prove contrapositive) ▨

§3. Discrete Kakeya problem

Motivation Rotating a needle 360°, how much space needed.

- necessary cond. for turning a unit-length needle inside a set X.



is: X contains a unit-length segment of every direction.

Such set is called a Kakeya set.

- [Besicovitch]: $\exists$ a Kakeya set of measure 0.

Q: How large is a Kakeya set in finite field setting?

Def. $K \subseteq \mathbb{F}_p^n$ is a Kakeya set if it contains a line in every direction.

i.e. $\forall$ direction $z \neq 0$, $z \in \mathbb{F}_p^n$, $\exists\, a \in \mathbb{F}_p^n$ s.t.

$$\{a + tz : t \in \mathbb{F}_p\} \subseteq K.$$