Today
- Polynomial Identity Testing
- Perfect Matching in bipartite graphs

CS.413.1
Pseudorandomness
Lecture 02 (2021-08-26)
Instructor: Prahladh Harsha.

Power of Randomness

Field – $\mathbb{Q}$ (rationals)
– $\mathbb{R}$ (reals)
– $\mathbb{C}$ (complexes)

$(\mathbb{F}, +, \cdot)$

$+$ ↳ addition

$\cdot$ multiplication.

$(\mathbb{F}, +)$ – group (under addition) / commutative $a+b = b+a$

- additive identity 0
  $\exists$ an elt $0 \in \mathbb{F}$, $\forall a \in \mathbb{F}$
  $a+0 = 0+a = a$.
- additive inverse
  $\forall a \in \mathbb{F}$, $\exists b \in \mathbb{F}$
  $a+b = b+a = 0$ $\Big\}$ $b = -a$

$(\mathbb{F}\setminus\{0\}, \cdot)$ – group (under multiplication) (commutative) $a\cdot b = b \cdot a$

- mult. identity 1

- mult inverse a^{-1} or $1/a$

$0 \cdot a = a \cdot 0 \hat{=} 0$

Distributive Property $\forall a, b, c \in \mathbb{F}$

$a \cdot (b+c) = a \cdot b + ac$

—

Finite fields: p - prime number

$\mathbb{Z}/p\mathbb{Z}$ - Integers mod p

$= \{0, 1, 2, \ldots\ p-1\}$.

Non-trivial fact to check.

- multiplicative inverse.

$\forall a \in \mathbb{F} \setminus \{0\}$, $\exists\, b \in \mathbb{F}^*$, s.t $a \cdot b = 1$

$\overset{\shortparallel}{\mathbb{F}^*}$

<u>Euclid's GCD Algorithm:</u>

Greatest Common Divisor

$a, \quad b \longrightarrow d$

there exist two other integers m & n

s.t $\quad am + bn = d$.

<u>Fact:</u>

$\forall a \in \{1 \ldots p-1\}$, $\exists\, b \in \{1 \ldots p-1\}$, $a \cdot b = 1 \pmod{p}$

Pf: Use Euclid's alg. on a & p

$GCD(a,p) = 1$

$\exists\ m, n \quad am + pn = 1$

$\Rightarrow \quad am \equiv 1 \pmod{p}$

$m =$ mul inverse of a. $\boxtimes$

$\mathbb{Z}/p\mathbb{Z}$ - field of size p (p-prime).

$\mathbb{F}_p$ - $GF(p)$.

More finite fields:

For $q = p^k$ (p-prime & k-positive integer) there is "a" finite field $\mathbb{F}_q = GF(q)$ of size exactly q.

$\mathbb{F}_p$ - field of size p

$\mathbb{F}_p[z]$ - Ring of polynomials

$$= \{ a_0 + a_1 z + \ldots + a_k z^k \mid k \in \mathbb{N} \cup \{0\},\ a_0 \ldots a_k \in \mathbb{F}_p \}.$$

$\mathbb{F}_p[z]$ - addition (group), $\underbrace{\text{multiplication}}_{\text{not a group.}}$

$f(z) = a_0 + a_1 z + \quad + z^k$ (monic-irreducible polynomial. (leading coeff is 1).

$$S = \frac{\mathbb{F}_p[z]}{f\,\mathbb{F}_p[z]} = \text{Set of polynomials modulo } f(z).$$

$|S| = p^k$ $\quad S - \mathbb{F}_q$ finite field.

Inherits addition & mult from the ring $\mathbb{F}_p[z]$.

Non-trivial fact to be checked.
S is a group under mult.

$\forall\, a \in S, \quad \exists\, b \in S, \quad a \cdot b = 1$

or

$\forall\, a(z) \in S, \quad \exists\, b(z) \in S, \quad a(z) \cdot b(z) \equiv 1 \pmod{f(z)}$

Pf: Use Euclid's GCD algorithm for polynomials instead.

$a(z), \quad b(z). \longrightarrow d(z)$ greatest common divisor

Euclid: $\exists$ poly $m(z)$ & $n(z)$ s.t

$$a(z) \cdot m(z) + b(z) \cdot n(z) = d(z).$$

—

Find the mult inverse of $a(z)$ in S.

$GCD(a(z), f(z)) = 1$

Euclid's alg: $\exists\, m, n,$ $a \cdot m + bf = 1$

$$a(z) \cdot m(z) \equiv 1 \pmod{f(z)}$$

—

<u>Concl:</u> S^* is a group under multiplication

—

Repn of $\mathbb{F}_q$ — prime p
$(q = p^k)$ — irreducible poly $f(z) \in \mathbb{F}_p[z]$ of deg k.

—

Only 3 properties of finite fields that we will use.

1. Degree Mantra:

$g(z) \in \mathbb{F}_q[z]$ $\deg(g) = d$.

then g has at most d roots.

2. Solving Linear Systems

$$\left.\begin{array}{l} a_{11}x_1 + \dots + a_{n1}x_n = 0 \\ a_{21}x_1 + \dots + a_{n2}x_n = 0 \\ \vdots \\ a_{m1}x_1 + \dots + a_{nm}x_n = 0 \end{array}\right\}$$

System of m eqns in n vars $(x_1 \dots x_n)$

Coeffts $- a_{ij} \in \mathbb{F}_q$.

$n \geq m \Rightarrow$ there is a soln to the above linear system.

(in fact the space of solns is a vector space of dim at least $n-m$.

3. $\mathbb{F}_q$ - finite field.

then every $a \in \mathbb{F}_q$ satisfies

$$x^q - x = 0.$$

The set of roots of $x^q - x = 0$ are exactly the field $\mathbb{F}_q$.

Resuming, Power of Randomness

Application 7: Polynomial Identity Testing

Problem: Let $\mathbb{F}$ - field.

"Given" 2 multivariate polynomials

$P, Q \in \mathbb{F}[x_1 \dots x_m]$

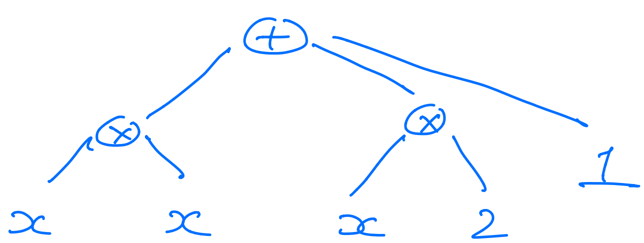
check $P \equiv Q$?

"Given": (1) List of coefficients (trivial)

(2) Oracle

(2b) Arithmetic formula that computes P, Q.

$x^2 + 2x + 1$



Restrict to univariate setting

Degree Mantra. # roots of a deg d non-zero poly $\leq d$.

$P \equiv Q$, $P - Q$ – Zero poly

$P \not\equiv Q$, $P - Q$ – non-zero poly of

$$P \not\equiv Q \quad \begin{cases} \Pr_{a \leftarrow S} [P(a) = Q(a)] \le \frac{d}{|S|} & \deg \le d. \\ \Pr_{a \leftarrow S} [(P-Q)(a) = 0] \le \frac{d}{|S|} \end{cases}$$

where $S \subseteq \mathbb{F}$

$$P \equiv Q \quad . \Pr_{a \leftarrow \mathbb{F}} [P(a) = Q(a)] = 1$$

What about the multivariate setting?

Obs: Degree Mantra is not true in the multivariate setting.

But the following is true.

Schwartz-Zippel Lemma:

P - non-zero multivariate poly of deg $\le d$

$P \in \mathbb{F}[X_1 \ldots X_m]$, $S \subseteq \mathbb{F}$

$$\Pr_{(a_1 \ldots a_m) \leftarrow S \times \ldots \times S} [P(a_1 \ldots a_m) = 0] \le \frac{d}{|S|}.$$

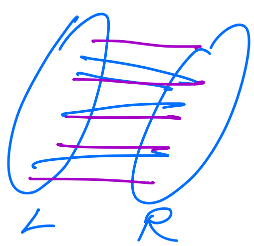
Even in multivariate setting

$$P \equiv Q, \quad \Pr_{\bar{a} \leftarrow S^m} [P(\bar{a}) = Q(\bar{a})] = 1$$

$$P \not\equiv Q \quad \Pr [P(\bar{a}) = Q(\bar{a})] \le d/|S|$$

Application 8: Bipartite Matching

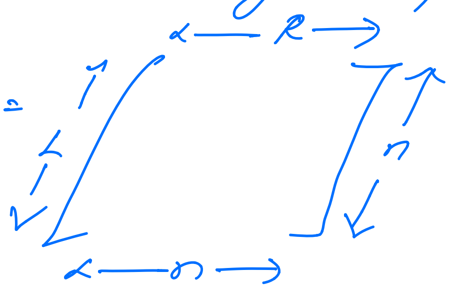
<u>Problem:</u> Given a simple bipartite graph $G = (L, R, E)$, does there exist a perfect matching in G?



(Assume, $|L| = |R| = n$)

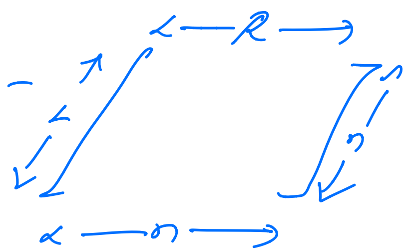
Bipartite Adjacency Matrix

$A =$



$$A(i,j) = \begin{cases} 1 & \text{if } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

$A(z) =$



$$A(z)(i,j) = \begin{cases} z_{ij} & \text{if } (i,j) \in E \\ 0 & \text{if } (i,j) \notin E \end{cases}$$

$\det(A(z))$

$$M: \quad \det(M) = \sum_{\sigma \in S_n} (-1)^{\mathrm{sign}(\sigma)} \prod_{i \in [n]} M_{i,\sigma(i)}$$

<u>Obs:</u> (1) G has no perfect matching

then $\det(A(z)) \equiv 0$

② G has a perfect matching

then $\det(A(z)) \not\equiv 0$

$\geq \deg(\det(A(z))) = n$

To check existence of perfect matching

$\Updownarrow$

$\det(A(z)) \not\equiv 0$

$S \subseteq \mathbb{F}$. $|S| = 100n$.

G has a perfect matching

$$\Pr_{\bar{a} \leftarrow S^E}\left[\det(A(\bar{a})) = 0\right] \leq \frac{n}{|S|} \leq \frac{1}{100}$$

G has no perfect matching

$$\Pr\left[\qquad\right] = 1$$

$\boxtimes$