Lecture 9 - Fields & Polynomials

[SCRIBE] - Refs: Sheup book, Forney notes, Madhu & Venkat's notes

rec. Field F: # system w/ $+, -, \cdot, (\div)$

Ring.

Polynomial over F: eg: $c_1 X_1^3 + c_2 X_2 X_3^5 + c_3 X_1^2 X_2^2 X_3^2 \in F[X_1, X_2, X_3]$

(c_1, c_2, c_3: #'s in F)

[Can think of it formally, as symbols, or as a map.]

put up before

TLDR:

- p prime $\Rightarrow$ {integers mod p} is a field, $\mathbb{F}_p$
- for $\ell \in \mathbb{N}$, also $\exists$ field w/ p^ℓ elts., $\mathbb{F}_{p^\ell}$ } unique ([isomorph] & no more
- can construct, work with $\mathbb{F}_q$ in $\text{poly}(\log(q))$ time* ([poly in rep size])

(*randomization...)

- deg-d univariate poly has $\le d$ roots [zeros]
- More generally: Let $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ have total deg $\le d$. Then $\Pr_{a_1, \ldots, a_n \sim \mathbb{F}_q} [P(a_1, \ldots, a_n) = 0] \le \frac{d}{q}$.

"Schwartz-Zippel Thm" [Tangled naming history].

[Today: we'll amplify on this, do some applications in TCS.]

Q: Why is $\mathbb{Z}_p$ [ints mod p; we say $\mathbb{F}_p$ to emph. it's a field] a field?

[knowing p prime, basically why do elts. have inverses? Actually, how to get them?]

A: Given $a \in \mathbb{Z}_p \setminus \{0\}$, can find a^{-1} using Extended GCD Alg. [Euclid's alg...]

(100, 45): $100 - 2\times 45 = 10$
$45 - 4\times 10 = 5$
$10 = 2\times 5$.

(polylog(p) time)
OPEN: In "NC"? polylog(log(p)) time parallel?

Finds $c, d \in \mathbb{Z}$ s.t.

$$c \cdot a + d \cdot p = \gcd(a, p) = 1 \quad [\text{if } p \text{ prime}]$$
$$\Rightarrow ca \equiv 1 \ (p)$$
$$c = a^{-1}.$$

[Why $\mathbb{Z}_n$ not field for n not prime? b/c $\exists$ elem with non-1 gcd. → zero divisors]

$\therefore$ $\mathbb{F}_p$ arithmetic is efficient.

[Wait. Yeah, if you know p, a prime. How to get it? Often want a prime around a certain value. How to get it, and check it?]

To get an m-bit prime:
- Repeat:
  - Pick rand. m-bit #
  - Check if it's prime. ← $\exists$ deterministic, poly(m) alg [AKS '02]

[!] [Rem: no efficient deterministic alg. known.
Can't just try $2^m, 2^m+1, 2^m+2, \ldots$ ← believed to req. $\sqrt{m}$ time.
$\exists$ an eff. det alg which is believed to work — demand thy.

[Not so bad — sometimes you actually want a unif. rand prime]

Prime # Theorem [cf Hmwk 1]: frac. of m-bit # which are prime $\sim \frac{1}{\ln 2 \cdot m}$.

[[So in poly(m) time, w.v.h.p., (like 2^{-m}) you get a # which is def. prime]]

Zero-sided error: expected poly time, answer always correct.

recall Miller-Rabin primality test: one-sided error
- poly(m) time [[Much faster: $\tilde{O}(m^3)$ vs. AKS $\tilde{O}(m^{7.5})$]]
- prime ⇒ always says "prime"
  composite ⇒ says "composite" w.h.p. [[eg. $\frac{1}{2}$, can be boosted]]

[[What abt. non-prime fields...]]

ex: $\{a+bi : a,b \in \mathbb{F}_3\} \cong \mathbb{F}_9$. $\{a+bi : a,b \in \mathbb{F}_5\}$: not a field

[[as we'll see, you get other fields by taking a field, "adjoining" a # satisfying a certain eq^n...]]

Polys $F[X_1, \dots, X_n]$ — coeffs in F
→ formal expressions like $c_1 X_1^3 X_2^4 + c_2 X_1^2 X_3 X_5^2 + \dots$ (A ring)
↖ 7

def: · total degree: max deg. of all monoms
· individual deg of X_i: [[eg: X_1: 3, X_2: 4, X_4: 0]]

skip for time

fact: ∃ univariate poly. division: $A(X) \overline{)\, B(X)}$ with quotient $Q(X)$, remainder $R(X)$ (or 0)

$B(X) = A(X)Q(X) + R(X)$, $\deg(R) < \deg(A)$

cor: ∃ Euclid's alg. [[for univ polys]]

Skip for time

~~Degree Monday~~

def: $P(X)$ irreducible (prime): $\Rightarrow$ can't be factored
[deg ≥ 2] $\Leftarrow$ $\gcd(P(X), Q(X)) = 1$
(or any deg-0 #)

$\Downarrow$

fact: $\{F[X] \bmod P(X)\}$ a field of size $|F|^{\deg(P)}$.
Pf: same as $\mathbb{Z} \bmod p$. !

$\|$

all polys of deg $<$ deg(P). e.g. $\mathbb{F}_q = \{\mathbb{F}_3[X] \bmod X^2+1\}$.
$a+bX$ with "rule" $X^2+1=0$.

cor: Given irred. of deg ℓ, arithmetic in $\mathbb{F}_q$, $q=p^\ell$
is poly$(\log(q)) =$ poly$(\ell \log p)$ time.

rem: $\mathbb{F}_{p^\ell}$ is vector space over $\mathbb{F}_p$ [elts. are like vecs, addition is vec add.]

[How to get the irred?]

"Prime # Thm for Ireds": [elementary!]
- Pick $P(X) = X^\ell + c_{\ell-1}X^{\ell-1} + \cdots + c_1X_1 + c_0$ unif $\in$ rand. ($c_i \in \mathbb{F}_p$)
- $\Pr[P(X)$ irred.$]$ between $\frac{1}{2\ell}$ & $\frac{1}{\ell}$ $(\sim \frac{1}{\ell})$.

$\Rightarrow \exists$ for all ℓ, findable in expected $O(\ell)$ trials.

(fact: irred. checkable in poly$(\ell, \log p)$ det. time.)
[~~Write more stuff here to check irreducibility~~]
[derand. is kinda known] For p const.:

Sharp: poly(ℓ, p) time det. alg. ~~for p=2~~

van Lint: x^2+x+1, x^6+x^3+1, $x^{16}+x^9+1$, ... are irred. over $\mathbb{F}_2$
[so for $\frac{1}{3}$ of ℓ's you're done.]

(Berlekamp: ∃ randomized 0-sided err, poly-time alg. for factoring elts of $\mathbb{F}_q[X]$!)

[Polys not just formal: you can evaluate them @ field pts.]
["Root" an input where the polynomial is 0.]

"Degree Mantra": Nonzero deg.-d univ. poly has $\le d$ roots.

Pf: Facto to irreds:

$$P(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X^{n-2}+\cdots \text{ irred})\ (\text{irred})$$

(1 root; 0 roots)

[Why? α root $\Rightarrow X-\alpha$ divides. Why? Poly div alg.]

[Seems so trivial. What's it good for?]

Communication Complexity of Equality.

Goal: $a=b$? Min # bits comm'd.

ex: Any det. alg req's $\ge n$ bits. [Nothing nontriv.]

prop: Allowing 1-sided error of $\frac{1}{n}$ ... $O(\log n)$ bits. [!!] [Optimal]

pf: • Alice fixes $\mathbb{F}_q$, $q \in [n^2, 2n^2]$, tells Bob $\log q = O(\log n)$
[e.g., chooses a prime (exp. time, or poly time with error) Bob can check. Or can use von Lint, $q \in [n^2, n^6]$]

• Alice forms $P_A(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X \in \mathbb{F}_q[X]$

Bob $P_B(X) = b_n X^n$ — — —

· Goal: $P_A(X) \stackrel{?}{=} P_B(X) \iff P_A - P_B \equiv 0$.

· Alice: chooses $\alpha \in \mathbb{F}_q$ at rand, sends α, $P_A(\alpha)$ to Bob. $O(\log n)$ bits

· Bob computes $P_B(\alpha)$, says "YES" if $= P_A(\alpha)$ $\iff (P_A - P_B)(\alpha) = 0$.

Now: $a = b \Rightarrow \Pr[\text{YES}] = 1$.

$a \neq b \Rightarrow P_A - P_B \not\equiv 0$, deg $\leq n$

$\Rightarrow \leq n$ roots.

$\Rightarrow \Pr[\text{YES}] \leq \frac{n}{q} \leq \frac{1}{n^2}$. ☺ . □

[Polys vs. fcns]

· Every poly $P(X_1, \ldots, X_n)$ computes a fcn $f: \mathbb{F}_q^n \to \mathbb{F}_q$.

fact: · Every $f: \mathbb{F}_q^n \to \mathbb{F}_q$ computable by some poly, deg $\leq q-1$ in each var. Why? [Interpolation. Do for point indicators.]

· q^{q^n} fcns, ∞'ly many polys.

∴ ∃ nonzero polys (formally) computing the everywhere-0 fcn!

e.g.: $X^q - X \in \mathbb{F}_q[X]$. pf: F.L.T. → same pf in general.

says $\alpha^q = \alpha$ $\forall \alpha \in \mathbb{F}_q$.

cor: Can reduce any poly so each individ. deg $\leq q-1$, w/o changing fcn it computes [$q=2$: multilinear].

fact: # reduced monomials $= q^n$ ⇒ # reduced polys $= q^{q^n}$

⇒ every fcn $\mathbb{F}_q^n \to \mathbb{F}_q$ has unique reduced poly. rep^n.

[⇒ reduced poly is 0-fcn ⟺ is 0-poly.]

[Generalization of Degree Mantra to multivariate polys.]

(Super) Schwartz-Zippel [-De-Dellillo-Lipton]:

Let $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ be (reduced) nonzero poly, total deg. $\leq d$.

Then $\Pr_{\alpha_1, \ldots, \alpha_n \sim \mathbb{F}_q}[P(\alpha_1, \ldots, \alpha_n) \neq 0] \geq \frac{1}{q^{\lfloor \frac{d}{q-1} \rfloor}} \left(1 - \frac{d \bmod (q-1)}{q}\right)$.

Huh? Case 1: $q=2$: $\geq \frac{1}{2^d}$.

(*) Case 2: $d < q$: $\geq 1 - \frac{d}{q}$ $\Rightarrow \Pr[=0] \leq \frac{d}{q}$.

Rem: also $\leq \frac{d}{|S|}$ for $\alpha_1, \ldots, \alpha_n \sim S \subseteq \mathbb{F}_q$ [eg, $\mathbb{R}$]

$n=1$ case: Degree Mantra

$n \to 1$: boring induction on n (hmwk)

[App:] Perfect Matchings in Bipartite Graphs:

Old: testable/findable in $O(mn)$ time [basically, repeated BFSs] (m = #edges)

Open: In "NC"? i.e.: polylog(n) parallel time?

Thm [Lovász 79]: Yes, allowing randomness. ("RNC")

Testing $\exists$ PM.

[finding also doable, but never mind.]

Vj: Karp-Upfal-Wig / Mulm Vaz².

Let $A = \left[\{ x_{ij} \text{ if } (i,j) \in E \text{ else } 0 \} \right]$

$$\det(A) = \sum_{\pi \in S_n} \underbrace{\operatorname{sgn}(\pi)}_{\pm 1} \prod_{i \in [n]} X_{i\pi(i)}$$

$= \neq$ a deg-n poly in, say, $\mathbb{Q}[(X_{ij})]$

$= 0$ iff no perfect matching !

[Can't compute directly – expon many terms.]

- Evaluate on random choice of X_{ij}'s $\in \{1, 2, \ldots, n^2\}$. ($|S|$)
  - no perf matching → always 0
  - $\exists$ perf matching → $\Pr[=0] \leq \frac{n}{n^2} \leq \frac{1}{n^{\alpha}}$. (☺)

[Csanky '76]: numerical det. computable over $\mathbb{Q}$ in NC (= polylog(n) parallel time).