Factoring polynomials over $\mathbb{F}_q$.

Given $f(x) \in \mathbb{F}_q[x]$ of degree d, we want to factor it into irreducible factors in time $\text{poly}(d, \log q)$.

OPEN!

Thm: Can do this in randomized $\text{poly}(d, \log q)$ time.

Thm — — — — — — deterministic $\text{poly}(d, q)$ time.

Algorithm for factoring in randomized $\text{poly}(d, \log q)$ time.

1. Get rid of repeated factors:

Replace $f(x)$ with

$\frac{f(x)}{g(x)}$, $g(x)$

where $g(x) = GCD(f(x), f'(x))$

$g(x)$ contains all repeated factors of $f(x)$.

2. Now we may assume $f(x)$ has no repeated factors in $\mathbb{F}_q[x]$.

For $i = 1$ to d,

Let $f_i(x) = GCD(f(x), x^{q^i} - x)$

$f(x) = f(x) / f_i(x)$

Then $f_i(x) =$ Π of irreducible factors of $f(x)$ of degree exactly i

3. Focus on each $f_i(x)$ one at a time.

Let $d_i = \deg f_i(X)$

Note $f_i(X)$ splits as a product of linear polynomials in $\mathbb{F}_{q^i}$. (with distinct roots).

Because irreducible polys of degree i have all their roots in $\mathbb{F}_{q^i}$.

FIRST Construct $\mathbb{F}_{q^i}$ using randomness

NEXT we find roots in $\mathbb{F}_{q^i}$ using Berlekamp's root finding trick.

compute

(Namely, $GCD\left(X^{\frac{q^i-1}{2}} - 1, f_i(\alpha X + \beta)\right)$

where $\alpha, \beta \in \mathbb{F}_{q^i}$, uniformly at random).

From this, we get all roots

$$\alpha_1, \alpha_2, \ldots, \alpha_{d_i} \in \mathbb{F}_{q^i} \text{ of } f_i(X).$$

These roots come in bundles of size i

$$\left\{\alpha_1, \alpha_1^q, \alpha_1^{q^2}, \ldots, \alpha_1^{q^{i-1}}\right\}$$

Find $\prod (X - \alpha_1^{q^i})$ etc. for each bundle, these are irred factors of $f_i(X)$.

Runtime of all this is $\text{poly}(d_i, \log(q^i))$

$= \text{poly}(d, \log q)$.

End of algorithm.

Deterministic factoring in poly(d, q) time.

Take $f(x) \in \mathbb{F}_q[X]$. $\deg(f) = d$

Let $R = \mathbb{F}_q[X]/f(x)$ = { polys of deg $< d$, with $+, \cdot$ mod $f(x)$ }.

$\mathbb{F}_2$-algebra ISOMORPHISM ||?

$$\left(\bigoplus_{i=1}^{l} \mathbb{F}_q[X]/(a_i(x))^{e_i} \right)$$

where $f(x) = \prod a_i(x)^{e_i}$

is their factorization into irreducible..

Algorithm for factoring

1. Reduce to the case that f is square free, as before. So all $e_i = 1$.
2. Look at $R = \mathbb{F}_q[x]/f(x)$.

$$R \simeq \mathbb{F}_{q^{u_1}} \oplus \mathbb{F}_{q^{u_2}} \oplus \cdots \oplus \mathbb{F}_{q^{u_\ell}}$$

↑ where $u_i = \deg(a_i(x))$

$\mathbb{F}_q$-algebra isomorphism

Find all solutions $y \in R$ s.t.

$$y^q - y = 0.$$

There are q^ℓ solutions to this, namely any $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ where $\alpha_i \in \mathbb{F}_q \subseteq \mathbb{F}_{q^{u_i}}$

and they form an $\mathbb{F}_2$-linear space of

dimension d. Call this space V.

VERY EXPLICITLY

Start with a basis $w_1, w_2, \ldots, w_d$ for R.

Compute $w_1^q, w_2^q, \ldots, w_d^q$

and write them in the basis $\{w_i\}$.

$$w_i^q = \sum a_{ij} w_j \qquad a_{ij} \in \mathbb{F}_q$$

Solve the system for $\beta_1, \ldots, \beta_d \in \mathbb{F}_q$:

$$\left(\sum_i \beta_i w_i\right)^q - \sum \beta_i w_i = 0$$

$$\Updownarrow$$

$$\sum_i \beta_i \sum_j a_{ij} w_j - \sum \beta_i w_i = 0.$$

$$\Updownarrow$$

$$\sum \beta_i a_{ij} - \beta_j = 0 \quad \forall j$$

$\langle r_R(m_i) = p_i$ for all $i \in [a]$

Inside V, there is a copy of $\mathbb{F}_q$ which is $\{(\beta, \beta, \beta, \ldots, \beta) : \beta \in \mathbb{F}_q\}$

Take any element $v \in V$ that is not from that copy of $\mathbb{F}_q$.

v is a polynomial of degree $\leq d-1$

s.t. $f(X) \mid v(X)^q - v(X)$

$\prod_{i=1}^{l} g_i(X) = f(X) \mid \prod_{\beta \in \mathbb{F}_q} (v(X) - \beta)$

If $V_\beta(X) = GCD(f(X), v(X) - \beta)$

then some $V_\beta(X)$ has deg ≥ 1,

but deg $< d$.

So this is a factor that is nontrivial.

Takes $\text{poly}(d, q)$ time, since we have to try all $\beta \in \mathbb{F}_q$ and look at $v_\beta(X)$.