Berlekamp as a reduction method

- Berlekamp's algorithm can be used to reduce polynomial factoring over $\mathbb{F}_q$ to that over $\mathbb{F}_p$, in det. poly-time.

- This requires a nice algebraic tool — Resultant.

Defn: • Let $a, b \in \mathbb{F}[x]$ be polys. Euclid's gcd algo. proved the existence of polys $u, v \in \mathbb{F}[x]$, with $(\deg u, \deg v) < (\deg b, \deg a)$, s.t. $ua + vb = \gcd(a, b)$.

[Exercise: Such u, v are unique iff $\gcd(a, b) = 1$.]

- Related to this is a system of linear equations in (deg a·b)-many unknowns:

$$\left(u_0 + u_1 x + \dots + u_{\deg b - 1} \cdot x^{\deg b - 1}\right) \cdot a(x) +$$

$$\left(v_0 + v_1 x + \dots + v_{\deg a - 1} \cdot x^{\deg a - 1}\right) \cdot b(x)$$

$$= \gcd(a, b) .$$

[u_i, v_j are unknowns and the eqns. are obtained by comparing the coefficients of x^m on both the sides, $\forall m$.]

- This gives us a matrix $\underline{M_{a,b}}$, over $\mathbb{F}$, of deg a·b order. Its entries are the coefficients of $a(x)$, $b(x)$ or zeroes.

$$M_{a,b} \cdot \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ v_0 \\ v_1 \\ \vdots \end{pmatrix} = \begin{pmatrix} \\ \\ \\ \\ \\ \end{pmatrix} \nwarrow \text{coeffs. in } \gcd(a,b)$$

- Resultant of $a(x)$, $b(x)$ is defined as

$$\underline{\mathrm{Res}(a,b)} := |M_{a,b}| .$$

Lemma: $\mathrm{Res}(a,b) \neq 0$ iff $\gcd(a,b) = 1$.

Pf:

- Referring to the previous system of eqns. $(ua+vb=(a,b))$:

$$|M_{a,b}| \neq 0$$
$$\iff u,v \text{ exist \& are unique}$$
$$\iff a,b \text{ are coprime.} \qquad \square$$

— Resultant is a very useful tool in computational algebra.

Mainly, because when a,b are multivariates, say in $\mathbb{F}[x_1,x_2]$,

Variable elimination → then we can consider $\mathrm{Res}_{x_2}(a,b)$.

It is now a polynomial in $\mathbb{F}[x_1]$.

(It captures those x_1-pts. at which a,b have a common zero.)

Proof by looking at the matrix equation. ▷

▷ If $\gcd_{x_2}(a,b)=1$ then $\exists\, u,v \in \mathbb{F}[x_1,x_2]$, with $(\deg_{x_2} u, \deg_{x_2} v) < (\deg_{x_2} b, \deg_{x_2} a)$ s.t.

$$ua + vb = \mathrm{Res}_{x_2}(a,b).$$

Pf: • By extended Euclid's gcd (or (Bézout's identity): $\exists\, u', v' \in \underbrace{\mathbb{F}(x_1)}_{\uparrow\ \text{field of rational functions}}[x_2]$ s.t. $u'a + v'b = 1$

• By clearing away the denominator, we get $u, v \in \mathbb{F}[x_1, x_2]$ & $w \in \mathbb{F}[x_1]$ s.t.

$$ua + vb = w(x_1).$$

• Also the matrix equation: $M_{a,b} \cdot \underset{\text{unknown } u_i', v_j'\text{'s}}{\overline{C}} = \underset{\uparrow \begin{pmatrix}1\\0\\0\\\vdots\end{pmatrix}}{\overline{B}}$

gives us $\overline{C} = \dfrac{\operatorname{adj}(M_{a,b}) \cdot \overline{B}}{|M_{a,b}|}$.

$\Rightarrow$ $w(x_1)$ can be set to $\mathrm{Res}_{x_2}(a,b)$ to get u, v s.t.

$$\deg_{x_2} u < \deg_{x_2} b \quad \& \quad \deg_{x_2} v < \deg_{x_2} a.$$

□

▷ $\mathrm{Res}_{x_2}(a,b) \in \langle a,b \rangle \cap \mathbb{F}[x_1]$

▷ For $a, b \in \mathbb{F}[x]$, $\mathrm{Res}(a,b) \in \langle a,b \rangle \cap \mathbb{F}$.

- Also, we have an easy degree bound:

▷ $\deg_{x_1} \mathrm{Res}_{x_2}(a,b) \leq \deg_{x_2} b \cdot \deg_{x_1} a + \deg_{x_2} a \cdot \deg_{x_1} b$

$\leq 2 \cdot (\deg a) \cdot (\deg b)$.

Reduction from $\mathbb{F}_q$ to $\mathbb{F}_p$ —

- We move back to univariate factoring over $\mathbb{F}_q$.

Using resultant we could show:

Theorem: Factoring over $\mathbb{F}_q \leq_p$ Factoring over $\mathbb{F}_p$.

Pf:

- Say, $f(x) \in \mathbb{F}_q[x]$ factors into k equi-degree coprime irreducible polynomials over $\mathbb{F}_q$.
- Using linear-algebra, compute a $g(x) \in \mathbb{F}_q[x]$, with $0 < \deg g < d$ & $g^p \equiv g \pmod f$.

- Compute $h(y) := res_x(f(x), g(x)-y)$.
  [We deduce $\deg h \leq d$.]

- By the properties of the resultant, we know that an $\mathbb{F}_p$-root α of h satisfies:
  $$\gcd(f, g-\alpha) \neq 1.$$

- So, instead of searching for such an α, we could simply factor
  $$h_1(y) := \gcd(h, y^p - y).$$
  [Note: $\deg h_1 \leq d$ & $h_1 \in \mathbb{F}_p[y]$.]

- Each of the steps above are polynomial in $d \cdot \lg q$.

□

$\mathbb{F}_p$-root-finding

Corollary: For polynomial factoring over $\mathbb{F}_q$, it suffices to factor a polynomial $f \in \mathbb{F}_p[x]$, that completely splits & has distinct $\mathbb{F}_p$-roots.