Lecture 9: Univariate Polynomial Factoring over Finite Fields

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 8, 2021

Overview

- Review from last lecture: Cantor-Zassenhaus
- Today's algorithm: Berlekamp's algorithm (1967)
- Properties of Irreducible Polynomials
- Conclusion
- Acknowledgements

Square roots over $\mathbb{F}_p$

$x^2 - a = (x-\alpha)(x+\alpha)$

- α is a root of f_1 and $-\alpha$ is a root of f_2 iff

$$\alpha^{(p-1)/2} \equiv 1 \quad \text{and} \quad (-\alpha)^{(p-1)/2} \equiv -1$$

$f_1(x) = x^{\frac{p-1}{2}} - 1$ $\qquad$ $f_2(x) = x^{\frac{p-1}{2}} + 1$

Square roots over $\mathbb{F}_p$

- α is a root of f_1 and $-\alpha$ is a root of f_2 iff

$$\alpha^{(p-1)/2} \equiv 1 \quad \text{and} \quad (-\alpha)^{(p-1)/2} \equiv -1$$

- If $p \equiv 3 \mod 4$ we know that f_1, f_2 <u>split the roots</u> of $x^2 - a$ and thus we are good!
- How do we make this work in general?

Square roots over $\mathbb{F}_p$

- α is a root of f_1 and $-\alpha$ is a root of f_2 iff

$$\alpha^{(p-1)/2} \equiv 1 \quad \text{and} \quad (-\alpha)^{(p-1)/2} \equiv -1$$

- If $p \equiv 3 \mod 4$ we know that f_1, f_2 split the roots of $x^2 - a$ and thus we are good!
- How do we make this work in general?
- Factoring $g(x) = x^2 - a$ equivalent to factoring

$$h(x) = (x-d)^2 - c^2 a$$

Square roots over $\mathbb{F}_p$

- α is a root of f_1 and $-\alpha$ is a root of f_2 iff

$$\alpha^{(p-1)/2} \equiv 1 \quad \text{and} \quad (-\alpha)^{(p-1)/2} \equiv -1$$

- If $p \equiv 3 \mod 4$ we know that f_1, f_2 split the roots of $x^2 - a$ and thus we are good!
- How do we make this work in general?
- Factoring $g(x) = x^2 - a$ equivalent to factoring

$$h(x) = (x-d)^2 - c^2 a$$

- $g(x) = (x-\alpha)(x+\alpha)$ if, and only if,

$$h(x) = (x - d - c\alpha)(x - d + c\alpha)$$

Square roots over $\mathbb{F}_p$

- α is a root of f_1 and $-\alpha$ is a root of f_2 iff

$$\alpha^{(p-1)/2} \equiv 1 \quad \text{and} \quad (-\alpha)^{(p-1)/2} \equiv -1$$

- If $p \equiv 3 \mod 4$ we know that f_1, f_2 split the roots of $x^2 - a$ and thus we are good!
- How do we make this work in general?
- Factoring $g(x) = x^2 - a$ equivalent to factoring

$$h(x) = (x - d)^2 - c^2 a$$

- $g(x) = (x - \alpha)(x + \alpha)$ if, and only if,

$$h(x) = (x - d - c\alpha)(x - d + c\alpha)$$

- So, if g factors, we can try to find "good" (c, d) so that $f_1(x), f_2(x)$ "split" the factors of h

Square roots over $\mathbb{F}_p$

- What if we pick $c, d \in \mathbb{F}_p$ at random? What is the probability that $f_1(x)$ has only one of the roots of h as a factor?

Square roots over $\mathbb{F}_p$

- What if we pick $c, d \in \mathbb{F}_p$ at random? What is the probability that $f_1(x)$ has only one of the roots of h as a factor?
- If $a_1 \neq a_2$ and $b_1 \neq b_2$ over $\mathbb{F}_p$:

$$\Pr_{c,d}[c \cdot a_1 + d = b_1 \text{ and } c \cdot a_2 + d = b_2] = \frac{1}{p^2}$$

Square roots over $\mathbb{F}_p$

- What if we pick $c, d \in \mathbb{F}_p$ at random? What is the probability that $f_1(x)$ has only one of the roots of h as a factor?
- If $a_1 \neq a_2$ and $b_1 \neq b_2$ over $\mathbb{F}_p$:

$$\Pr_{c,d}[c \cdot a_1 + d = b_1 \text{ and } c \cdot a_2 + d = b_2] = \frac{1}{p^2}$$

- On the other hand:

$$\Pr_{b_1}[b_1 \text{ is root of } x^{(p-1)/2}] = \frac{1}{2}$$

$$\Pr_{b_2}[b_2 \text{ is not root of } x^{(p-1)/2}] = \frac{1}{2}$$

Square roots over $\mathbb{F}_p$

- What if we pick $c, d \in \mathbb{F}_p$ at random? What is the probability that $f_1(x)$ has only one of the roots of h as a factor?
- If $a_1 \neq a_2$ and $b_1 \neq b_2$ over $\mathbb{F}_p$:

$$\Pr_{c,d}[c \cdot a_1 + d = b_1 \text{ and } c \cdot a_2 + d = b_2] = \frac{1}{p^2}$$

- On the other hand:

$$\Pr_{b_1}[b_1 \text{ is root of } x^{(p-1)/2}] = \frac{1}{2}$$

$$\Pr_{b_2}[b_2 \text{ is not root of } x^{(p-1)/2}] = \frac{1}{2}$$

- Thus, with probability $\approx 1/2$, uniform random choice of c, d gives us that $f_1(x)$ splits $h(x)$

Square Root Algorithm

1. Pick random $c, d \in \mathbb{F}_p$ and compute $h(x)$

Square Root Algorithm

1. Pick random $c, d \in \mathbb{F}_p$ and compute $h(x)$
2. Compute $\ell(x) \equiv f_1(x) \mod h(x)$

Square Root Algorithm

1. Pick random $c, d \in \mathbb{F}_p$ and compute $h(x)$
2. Compute $\ell(x) \equiv f_1(x) \mod h(x)$
3. Compute $r(x) = \gcd(h(x), \ell(x))$

Square Root Algorithm

1. Pick random $c, d \in \mathbb{F}_p$ and compute $h(x)$
2. Compute $\ell(x) \equiv f_1(x) \mod h(x)$
3. Compute $r(x) = \gcd(h(x), \ell(x))$
4. If $r(x) = 1$ or $r(x) = h(x)$, go back to step 1

Square Root Algorithm

1. Pick random $c, d \in \mathbb{F}_p$ and compute $h(x)$
2. Compute $\ell(x) \equiv f_1(x) \mod h(x)$
3. Compute $r(x) = \gcd(h(x), \ell(x))$
4. If $r(x) = 1$ or $r(x) = h(x)$, go back to step 1
5. Otherwise we found a root of $h(x)$

Cantor-Zassenhaus Factoring Algorithm (1981)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$ with (unknown) factorization

$$f(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$$

- **Output:** irreducible factors $f_1(x), \ldots, f_k(x)$

Cantor-Zassenhaus Factoring Algorithm (1981)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$ with (unknown) factorization

$$f(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$$

- **Output:** irreducible factors $f_1(x), \ldots, f_k(x)$
- Algorithm:
  1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$

Cantor-Zassenhaus Factoring Algorithm (1981)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$ with (unknown) factorization

$$f(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$$

- **Output:** irreducible factors $f_1(x), \ldots, f_k(x)$
- Algorithm:

1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
2. If

$$\underline{h_d(x)} := \prod_{\deg(f_i)=d} f_i(x)$$

only has deg. d factors of f

obtain $h_d(x)$ for each $1 \leq d \leq \deg(f)$ by taking $\gcd(f(x), \underbrace{x^{q^d} - x}_{\prod \text{ all irred. deg } d \text{ polynomials}})$

Cantor-Zassenhaus Factoring Algorithm (1981)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$ with (unknown) factorization

$$f(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$$

- **Output:** irreducible factors $f_1(x), \ldots, f_k(x)$
- Algorithm:
  1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
  2. If

$$h_d(x) := \prod_{\deg(f_i)=d} f_i(x)$$

     obtain $h_d(x)$ for each $1 \le d \le \deg(f)$ by taking $\gcd(f(x), x^{q^d} - x)$
  3. Take a random $T(x) \in \mathbb{F}_q[x]$ such that $d < \deg(T) < 2 \cdot d$ and output

$$a(x) := \gcd(h_d, T(x)^{(q^d-1)/2} - 1)$$

     if it is not equal to $h_d(x)$

Cantor-Zassenhaus Factoring Algorithm (1981)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$ with (unknown) factorization

$$f(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$$

- **Output:** irreducible factors $f_1(x), \ldots, f_k(x)$
- Algorithm:
  1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
  2. If
  $$h_d(x) := \prod_{\deg(f_i)=d} f_i(x)$$
  obtain $h_d(x)$ for each $1 \leq d \leq \deg(f)$ by taking $\gcd(f(x), x^{q^d} - x)$
  3. Take a random $T(x) \in \mathbb{F}_q[x]$ such that $d < \deg(T) < 2 \cdot d$ and output
  $$a(x) := \gcd(h_d, T(x)^{(q^d-1)/2} - 1)$$
  if it is not equal to $h_d(x)$
  4. Recurse on $h_d(x)/a(x)$

- Review from last lecture: Cantor-Zassenhaus
- Today's algorithm: Berlekamp's algorithm (1967)
- Properties of Irreducible Polynomials
- Conclusion
- Acknowledgements

Berlekamp's Algorithm: Main Idea

- We will be working over $\mathbb{F}_q$ where $q = p^m$ for some prime p
- As in the previous lecture, we can assume that input polynomial $f(x)$ is square-free and its factors have same degree
- For simplicity, let's just stick to the case $f(x) = f_1(x) \cdot f_2(x)$ both irreducible factors f_1, f_2 having same degree

Berlekamp's Algorithm: Main Idea

- We will be working over $\mathbb{F}_q$ where $q = p^m$ for some prime p
- As in the previous lecture, we can assume that input polynomial $f(x)$ is square-free and its factors have same degree
- For simplicity, let's just stick to the case $f(x) = f_1(x) \cdot f_2(x)$ both irreducible factors f_1, f_2 having same degree
- *Key idea*: find a polynomial $g(x) \in \mathbb{F}_q[x]$ such that

$$g(x)^q \equiv g(x) \bmod f(x) \quad \text{and} \quad \underline{0 < \deg(g) < \deg(f)}$$

$\alpha^q - \alpha \equiv 0$ in $\mathbb{F}_q$ for any $\alpha \in \mathbb{F}_q$

$(\deg g = 0)$

$\deg(g) = \deg(f)$ $\quad g = f$

Berlekamp's Algorithm: Main Idea

- We will be working over $\mathbb{F}_q$ where $q = p^m$ for some prime p
- As in the previous lecture, we can assume that input polynomial $f(x)$ is square-free and its factors have same degree
- For simplicity, let's just stick to the case $f(x) = f_1(x) \cdot f_2(x)$ both irreducible factors f_1, f_2 having same degree
- *Key idea*: find a polynomial $g(x) \in \mathbb{F}_q[x]$ such that

$$g(x)^q \equiv g(x) \bmod f(x) \quad \text{and} \quad 0 < \deg(g) < \deg(f)$$

- Questions:
  1. Why is it useful?
  2. Does such a polynomial always exist?
  3. If is exists, how do we find it?

Usefulness

- Let us look at $z^q - z$ once again:

$$z^q - z = \prod_{\alpha \in \mathbb{F}_q} (z - \alpha)$$

Usefulness

- Let us look at $z^q - z$ once again:
$$z^q - z = \prod_{\alpha \in \mathbb{F}_q} (z - \alpha)$$
- If $g(x)^q - g(x) \equiv 0 \bmod f(x)$, then we know that
$$f(x) \ \text{ divides } \ \prod_{\alpha \in \mathbb{F}_q} (g(x) - \alpha) = g(x)^q - g(x)$$

Usefulness

- Let us look at $z^q - z$ once again:

$$z^q - z = \prod_{\alpha \in \mathbb{F}_q} (z - \alpha)$$

- If $g(x)^q - g(x) \equiv 0 \mod f(x)$, then we know that

$$f(x) \text{ divides } \prod_{\alpha \in \mathbb{F}_q} (g(x) - \alpha)$$

- If $0 < \deg(g) < \deg(f)$, then there exists $\alpha \in \mathbb{F}_q$ such that

$$\gcd(g(x) - \alpha, f(x)) \neq 1$$

get a factor of $f(x)$.

Usefulness

- Let us look at $z^q - z$ once again:

$$z^q - z = \prod_{\alpha \in \mathbb{F}_q} (z - \alpha)$$

- If $g(x)^q - g(x) \equiv 0 \bmod f(x)$, then we know that

$$f(x) \;\text{ divides }\; \prod_{\alpha \in \mathbb{F}_q} (g(x) - \alpha)$$

- If $0 < \deg(g) < \deg(f)$, then there exists $\alpha \in \mathbb{F}_q$ such that

$$\underline{\gcd(g(x) - \alpha, f(x)) \neq 1}$$

  get a factor of $f(x)$.
- Degree condition of g is very important:
  - If $g(x)$ was a constant, then $g^q - g = 0$
  - If $\deg(d) = \deg(f)$, then $g(x) = f(x)$ would satisfy our condition, but that is not useful

Existence

- Chinese Remainder Theorem: since $f(x) = f_1(x) \cdot f_2(x)$

$$\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(f_1(x)) \times \mathbb{F}_q[x]/(f_2(x))$$

Existence

- Chinese Remainder Theorem: since $f(x) = f_1(x) \cdot f_2(x)$

$$\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(f_1(x)) \times \mathbb{F}_q[x]/(f_2(x))$$

- If $g(x) \equiv \alpha_1 \bmod f_1(x)$ and $g(x) \equiv \alpha_2 \bmod f_2(x)$, where $\underline{\alpha_1}, \underline{\alpha_2} \in \underline{\mathbb{F}_q}$, then

$$g(x)^q - g(x) \equiv \alpha_i^q - \alpha_i \equiv 0 \bmod f_i(x) \qquad i \in \{1, 2\}$$

so $g(x)^q - g(x) \equiv 0 \bmod f(x)$

Existence

- Chinese Remainder Theorem: since $f(x) = f_1(x) \cdot f_2(x)$

$$\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(f_1(x)) \times \mathbb{F}_q[x]/(f_2(x))$$

- If $g(x) \equiv \alpha_1 \bmod f_1(x)$ and $g(x) \equiv \alpha_2 \bmod f_2(x)$, where $\alpha_1, \alpha_2 \in \mathbb{F}_q$, then

$$g(x)^q - g(x) \equiv \alpha_i^q - \alpha_i \equiv 0 \bmod f_i(x)$$

  so $g(x)^q - g(x) \equiv 0 \bmod f(x)$
- CRT tells us that there is unique $g(x) \in \mathbb{F}_q[x]/(f(x))$ such that

$$g(x) \equiv \alpha_i \bmod f_i(x)$$

Existence

- Chinese Remainder Theorem: since $f(x) = f_1(x) \cdot f_2(x)$

$$\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(f_1(x)) \times \mathbb{F}_q[x]/(f_2(x))$$

- If $g(x) \equiv \alpha_1 \bmod f_1(x)$ and $g(x) \equiv \alpha_2 \bmod f_2(x)$, where $\alpha_1, \alpha_2 \in \mathbb{F}_q$, then

$$g(x)^q - g(x) \equiv \alpha_i^q - \alpha_i \equiv 0 \bmod f_i(x)$$

  so $g(x)^q - g(x) \equiv 0 \bmod f(x)$
- CRT tells us that there is unique $g(x) \in \mathbb{F}_q[x]/(f(x))$ such that

$$g(x) \equiv \alpha_i \bmod f_i(x)$$

- Need to show that we have a non-constant $g(x)$ satisfying it!
  - Only q elements of $\mathbb{F}_q[x]/(f(x))$ are constants - these correspond to

$$\alpha \longleftrightarrow (\alpha, \alpha) \in \mathbb{F}_q[x]/(f_1(x)) \times \mathbb{F}_q[x]/(f_2(x))$$

  - So all we need is to take $\alpha_1 \neq \alpha_2$ $\quad (\alpha_1, \alpha_2) \longleftrightarrow g(x)$

Constructing $g(x)$

- **Lemma:** the space of all polynomials $g(x)$ such that

$$g(x)^q \equiv g(x) \bmod f(x)$$

is a *linear space*

Constructing $g(x)$

$q = p^m$

- **Lemma:** the space of all polynomials $g(x)$ such that

$$\underline{g(x)^q \equiv g(x) \bmod f(x)}$$

  is a *linear space*
- Proof

$$(g_1(x) + g_2(x))^q = \underline{g_1(x)}^q + \underline{g_2(x)}^q \equiv g_1(x) + g_2(x) \bmod f(x)$$

$$\parallel$$

$$g_1(x)^q + p\,\underbrace{\cancel{(\ldots)}}_{\sum_{i=1}^{q-1} \underbrace{\binom{q}{i}}_{p \mid} \cdot g_1^{q-i} g_2^i} + g_2(x)^q$$

$$= 0 \text{ over } \mathbb{F}_q$$

Constructing $g(x)$

- **Lemma:** the space of all polynomials $g(x)$ such that
$$g(x)^q \equiv g(x) \bmod f(x)$$
is a *linear space*
- Proof
$$(g_1(x) + g_2(x))^q = g_1(x)^q + g_2(x)^q \equiv g_1(x) + g_2(x) \bmod f(x)$$
- Since we have a linear space, we might as well construct a basis for this linear space. If $g(x) = g_0 + g_1 x + \cdots + g_\ell x^\ell$ then
$$g(x)^q = g(x^q) = g_0 + g_1 x^q + \cdots + g_\ell x^{\ell q}$$

Constructing $g(x)$

- **Lemma:** the space of all polynomials $g(x)$ such that
$$g(x)^q \equiv g(x) \bmod f(x)$$
is a *linear space*
- Proof
$$(g_1(x) + g_2(x))^q = g_1(x)^q + g_2(x)^q \equiv g_1(x) + g_2(x) \bmod f(x)$$
- Since we have a linear space, we might as well construct a basis for this linear space. If $g(x) = g_0 + g_1 x + \cdots + g_\ell x^\ell$ then
$$g(x)^q = g(x^q) = g_0 + g_1 x^q + \cdots + g_\ell x^{\ell q}$$
- Find coefficients $\underline{\beta_{ij}}$ such that
$$x^{iq} \equiv \underline{\beta_{i0}} + \underline{\beta_{i1}} x + \cdots + \underline{\beta_{i(d-1)}} x^{d-1}$$

$x^{iq} \bmod f(x)$

Constructing $g(x)$

- **Lemma:** the space of all polynomials $g(x)$ such that
$$\underline{g(x)^q \equiv g(x) \bmod f(x)}$$
is a *linear space*
- Proof
$$(g_1(x) + g_2(x))^q = g_1(x)^q + g_2(x)^q \equiv g_1(x) + g_2(x) \bmod f(x)$$
- Since we have a linear space, we might as well construct a basis for this linear space. If $g(x) = g_0 + g_1 x + \cdots + g_\ell x^\ell$ then
$$g(x)^q = g(x^q) = g_0 + g_1 x^q + \cdots + g_\ell x^{\ell q}$$
- Find coefficients β_{ij} such that
$$x^{iq} \equiv \beta_{i0} + \beta_{i1} x + \cdots + \beta_{i(d-1)} x^{d-1}$$
- Solve linear system:
$$g(x^q) = g(x)^q = \sum_{i=1}^{\ell} \underline{g_i} \cdot \overbrace{\left(\sum_{j=0}^{d-1} \underline{\beta_{ij}} x^j \right)}^{x^{iq}} = \sum_{i=0}^{\ell} \underline{g_i} x^i = g(x)$$

Constructing $g(x)$ - Example

$\mathbb{Z}_5[x]$

$$f(x) = (x^2+x+1)(x^2-2)$$

$q = 5$

$$= x^4 + x^3 - x^2 - 2x - 2$$

$$g(x) = g_0 + g_1 x + g_2 x^2 + g_3 x^3$$

$(\alpha x+\beta)^5 \equiv (\alpha x + \beta) \bmod f$

$\alpha = 0 \quad \beta \in \mathbb{Z}_5$

$$g(x^5) = g_0 + g_1 x^5$$

$$x^5 = x^5 - xf = -x^4 + x^3 + 2x + 2$$

$$g_0 + g_1(-x^4 + x^3 + 2x + 2) \equiv g_0 + g_1 x$$

$$\Leftrightarrow (2g_1) + g_1 x + g_1 x^3 - g_1 x^4 = 0$$

$$\Leftrightarrow g_1 = 0$$

Berlekamp's Factoring Algorithm (1967)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$
- **Output:** non-trivial factor of $f(x)$

Berlekamp's Factoring Algorithm (1967)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$
- **Output:** non-trivial factor of $f(x)$
- Algorithm:
    1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$

Berlekamp's Factoring Algorithm (1967)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$
- **Output:** non-trivial factor of $f(x)$
- Algorithm:
  1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
  2. If
$$h_d(x) := \prod_{\deg(f_i)=d} f_i(x)$$
obtain $h_d(x)$ for each $1 \leq d \leq \deg(f)$ by taking $\gcd(f(x), x^{q^d} - x)$

Berlekamp's Factoring Algorithm (1967)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$
- **Output:** non-trivial factor of $f(x)$
- Algorithm:

1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
2. If
$$h_d(x) := \prod_{\deg(f_i)=d} f_i(x)$$
obtain $h_d(x)$ for each $1 \le d \le \deg(f)$ by taking $\gcd(f(x), x^{q^d} - x)$
3. Compute a $g(x) \in \mathbb{F}_q[x]$ such that $0 < \deg(g) < d$ and
$$g(x)^q \equiv g(x) \bmod f(x)$$

Berlekamp's Factoring Algorithm (1967)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$
- **Output:** non-trivial factor of $f(x)$
- Algorithm:
  1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
  2. If
  $$h_d(x) := \prod_{\deg(f_i)=d} f_i(x)$$
  obtain $h_d(x)$ for each $1 \leq d \leq \deg(f)$ by taking $\gcd(f(x), x^{q^d} - x)$
  3. Compute a $g(x) \in \mathbb{F}_q[x]$ such that $0 < \deg(g) < d$ and
  $$g(x)^q \equiv g(x) \bmod f(x)$$
  4. For all $\underline{\alpha \in \mathbb{F}_q,}$ compute
  $$r_\alpha(x) := \gcd(g(x) - \alpha, f(x))$$

for some $\alpha \in \mathbb{F}_q$ $\gcd(g(x) - \alpha, f(x)) \neq 1$

Berlekamp's Factoring Algorithm (1967)

- **Input**: polynomial $f \in \mathbb{F}_q[x]$
- **Output:** non-trivial factor of $f(x)$
- Algorithm:
  1. Get square-free part of $f(x)$ by computing $\dfrac{f}{\gcd(f, f')}$
  2. If

     $$h_d(x) := \prod_{\deg(f_i)=d} f_i(x)$$

     obtain $h_d(x)$ for each $1 \leq d \leq \deg(f)$ by taking $\gcd(f(x), x^{q^d} - x)$
  3. Compute a $g(x) \in \mathbb{F}_q[x]$ such that $0 < \deg(g) < d$ and

     $$g(x)^q \equiv g(x) \bmod f(x)$$

  4. For all $\alpha \in \mathbb{F}_q$, compute

     $$r_\alpha(x) := \gcd(g(x) - \alpha, f(x))$$

  5. If $r_\alpha(x) \neq 1$, return $r_\alpha(x)$.

$\mathbb{Z}_5[x]$

$f(x) = (x^2+x+1)^2(x^2-2)^2$

$\gcd(f, f') = (x^2+x+1)(x^2-2)$

$f! = f/\gcd(f,f')$ square-free

$f = (x^2+x+1)(x^2-2)$

$h_1 = \gcd(f, x^5-x) = 1$

$h_2 = \gcd(f, x^{5^2}-x) = f$

$\to f$ has only deg 2 irreducible factors

$$f(x) = (x^2 + x + 1)(x^2 - 2)$$

Pick random polynomial

$$T(x) \quad 2 < \deg(T) < 4$$

$$T(x) = x^3 + 3x^2 + x + 1$$

compute $T(x)^{\frac{5^2-1}{2}} - 1 = T(x)^{12} - 1$

mod $f(x) \longrightarrow g(x)$

$$\gcd(f(x), \underset{T(x)^{12}-1}{g(x)}) \neq 1$$

Finite Fields and Field Extensions

- Now that we saw two algorithms to factor univariate polynomials over finite fields, let's see in more depth properties of polynomials over finite fields that we went over quickly

Finite Fields and Field Extensions

- Now that we saw two algorithms to factor univariate polynomials over finite fields, let's see in more depth properties of polynomials over finite fields that we went over quickly
- Explore irreducible polynomials of degree d over $\mathbb{F}_q[x]$
  1. For every $q = p^k$ and every integer $d > 0$, there is *irreducible* polynomial of degree d in $\mathbb{F}_q[x]$
  2. The probability of *monic* polynomial of degree d to be *irreducible* is equal to $1/d$

Finite Fields and Field Extensions

- Now that we saw two algorithms to factor univariate polynomials over finite fields, let's see in more depth properties of polynomials over finite fields that we went over quickly
- Explore irreducible polynomials of degree d over $\mathbb{F}_q[x]$
  1. For every $q = p^k$ and every integer $d > 0$, there is *irreducible* polynomial of degree d in $\mathbb{F}_q[x]$
  2. The probability of *monic* polynomial of degree d to be *irreducible* is equal to $1/d$
- Which irreducible polynomials divide $x^{q^d} - x$

Finite Fields and Field Extensions

- Now that we saw two algorithms to factor univariate polynomials over finite fields, let's see in more depth properties of polynomials over finite fields that we went over quickly
- Explore irreducible polynomials of degree d over $\mathbb{F}_q[x]$
  1. For every $q = p^k$ and every integer $d > 0$, there is *irreducible* polynomial of degree d in $\mathbb{F}_q[x]$
  2. The probability of *monic* polynomial of degree d to be *irreducible* is equal to $1/d$
- Which irreducible polynomials divide $x^{q^d} - x$
- For that, we need properties of finite fields and field extensions

Field Extensions

- We know that $\mathbb{Z}_3$ is a field. How do we know that there exists field with $9 = 3^2$ elements? Can we construct one?

Field Extensions

- We know that $\mathbb{Z}_3$ is a field. How do we know that there exists field with $9 = 3^2$ elements? Can we construct one?
- Let $f(x) = x^2 + 1$ over $\mathbb{Z}_3[x]$. Let's prove that this is irreducible polynomial:

$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 2$$

Field Extensions

- We know that $\mathbb{Z}_3$ is a field. How do we know that there exists field with $9 = 3^2$ elements? Can we construct one?
- Let $f(x) = x^2 + 1$ over $\mathbb{Z}_3[x]$. Let's prove that this is irreducible polynomial:
- Now, let's look at the ring $\boxed{\mathbb{Z}_3[x]/(f(x))}$. This has only *9 elements*! Moreover, it is a field!

$\alpha x + \beta$ in $\mathbb{Z}_3[x]/(f(x))$ has inverse $s(x)$

$\Updownarrow$

$s(\alpha x + \beta) \equiv 1 \mod f(x)$

$\Longleftrightarrow s(\alpha x + \beta) = 1 + f(x) \cdot t(x)$

$\Longleftrightarrow s(x)(\alpha x + \beta) - f(x)t(x) = 1 \Longleftrightarrow \gcd(\alpha x + \beta, f) = 1$

$\Updownarrow$

f irreducible!

Field Extensions

- We know that $\mathbb{Z}_3$ is a field. How do we know that there exists field with $9 = 3^2$ elements? Can we construct one?
- Let $f(x) = x^2 + 1$ over $\mathbb{Z}_3[x]$. Let's prove that this is irreducible polynomial:
- Now, let's look at the ring $\mathbb{Z}_3[x]/(f(x))$. This has only *9 elements*! Moreover, it is a field!
- This is how we can construct fields with p^k elements for some prime p
- The *characteristic* of a field $\mathbb{F}$ is the minimum positive element $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ over $\mathbb{F}$ (if no such n exists, we say $\mathbb{F}$ has characteristic zero)

$\mathrm{char}(\mathbb{Q}) = 0$

$\mathrm{char}(\mathbb{Z}_3) = 3$

$\mathrm{char}(\mathbb{F}_q) = 3$

$\mathrm{char}(\mathbb{F}_q) = p$

$q = p^k$

Field Extensions

- We know that $\mathbb{Z}_3$ is a field. How do we know that there exists field with $9 = 3^2$ elements? Can we construct one?
- Let $f(x) = x^2 + 1$ over $\mathbb{Z}_3[x]$. Let's prove that this is irreducible polynomial:
- Now, let's look at the ring $\mathbb{Z}_3[x]/(f(x))$. This has only *9 elements*! Moreover, it is a field!
- This is how we can construct fields with p^k elements for some prime p
- The *characteristic* of a field $\mathbb{F}$ is the minimum positive element $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ over $\mathbb{F}$ (if no such n exists, we say $\mathbb{F}$ has characteristic zero)
- If $\mathbb{K}$ is a field with subfield $\mathbb{F} \subset \mathbb{K}$, we say that $\mathbb{K}$ is a *field extension* of $\mathbb{F}$ and we can see $\mathbb{K}$ as a *vector space* over $\mathbb{F}$

Field Extensions

- We know that $\mathbb{Z}_3$ is a field. How do we know that there exists field with $9 = 3^2$ elements? Can we construct one?
- Let $f(x) = x^2 + 1$ over $\mathbb{Z}_3[x]$. Let's prove that this is irreducible polynomial:
- Now, let's look at the ring $\mathbb{Z}_3[x]/(f(x))$. This has only *9 elements*! Moreover, it is a field!
- This is how we can construct fields with p^k elements for some prime p
- The *characteristic* of a field $\mathbb{F}$ is the minimum positive element $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ over $\mathbb{F}$ (if no such n exists, we say $\mathbb{F}$ has characteristic zero)
- If $\mathbb{K}$ is a field with subfield $\mathbb{F} \subset \mathbb{K}$, we say that $\mathbb{K}$ is a *field extension* of $\mathbb{F}$ and we can see $\mathbb{K}$ as a *vector space* over $\mathbb{F}$
- Example: $\mathbb{K} = \mathbb{F}_9$ and $\mathbb{F} = \mathbb{F}_3$

$$ax + b \leftrightarrow (a, b)$$

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$

$\mathbb{Z}_3 \qquad f(x) = x^2+1$

$\mathbb{F}_9 = \mathbb{Z}_3[x]/(f(x)) \qquad \mathbb{F}_9[y]$

$y^2+1 = (y-x)(y+x)$
$= y^2 - x^2 = y^2+1$

$\mathbb{F}_9$ splits x^2+1.

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1
- Roots are x and $-x$

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1
- Roots are x and $-x$
- Every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field.
  1. If $f(x)$ does not split over $\mathbb{F}$, f must have irreducible factor of degree > 1. Call it $f_1(x)$

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1
- Roots are x and $-x$
- Every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field.
  1. If $f(x)$ does not split over $\mathbb{F}$, f must have irreducible factor of degree > 1. Call it $f_1(x)$
  2. Let $\mathbb{K}_1 = \mathbb{F}[x]/(f_1(x))$. The element $x \in \mathbb{K}_1$ is a *root* of $f_1(y) \in \mathbb{K}_1[y]$. Thus, $f_1(y)$ factors over $\mathbb{K}_1[y]$

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1
- Roots are x and $-x$
- Every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field.
  1. If $f(x)$ does not split over $\mathbb{F}$, f must have irreducible factor of degree > 1. Call it $f_1(x)$
  2. Let $\mathbb{K}_1 = \mathbb{F}[x]/(f_1(x))$. The element $x \in \mathbb{K}_1$ is a *root* of $f_1(y) \in \mathbb{K}_1[y]$. Thus, $f_1(y)$ factors over $\mathbb{K}_1[y]$
  3. In particular, f also has extra linear factor over $\mathbb{K}_1$

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1
- Roots are x and $-x$
- Every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field.
  1. If $f(x)$ does not split over $\mathbb{F}$, f must have irreducible factor of degree > 1. Call it $f_1(x)$
  2. Let $\mathbb{K}_1 = \mathbb{F}[x]/(f_1(x))$. The element $x \in \mathbb{K}_1$ is a *root* of $f_1(y) \in \mathbb{K}_1[y]$. Thus, $f_1(y)$ factors over $\mathbb{K}_1[y]$
  3. In particular, f also has extra linear factor over $\mathbb{K}_1$
  4. Can iterate this construction until f *only has linear factors*

$\deg(f) = d \implies f$ has $\leq d$ factors

Splitting Fields

- Given a polynomial $f(x) \in \mathbb{F}[x]$ a field extension $\mathbb{K}$ of $\mathbb{F}$ is a *splitting field* of $f(x)$ if $f(x)$ *splits into linear factors* over $\mathbb{K}$
- Example: $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ is a splitting field of x^2+1
- Roots are x and $-x$
- Every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field.
  1. If $f(x)$ does not split over $\mathbb{F}$, f must have irreducible factor of degree > 1. Call it $f_1(x)$
  2. Let $\mathbb{K}_1 = \mathbb{F}[x]/(f_1(x))$. The element $x \in \mathbb{K}_1$ is a *root* of $f_1(y) \in \mathbb{K}_1[y]$. Thus, $f_1(y)$ factors over $\mathbb{K}_1[y]$
  3. In particular, f also has extra linear factor over $\mathbb{K}_1$
  4. Can iterate this construction until f *only has linear factors*
- For a polynomial $f(x) \in \mathbb{F}[x]$, we usually call a field $\mathbb{K}$ *the* splitting field of f if $\mathbb{K}$ is the "smallest" field that fully splits f into linear factors

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d
- Let $\mathbb{K}$ be the splitting field of $x^{q^d} - x$

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d
- Let $\mathbb{K}$ be the splitting field of $x^{q^d} - x$
- Let

$$S = \{\alpha \in \mathbb{K} \mid \underline{\alpha^{q^d} - \alpha} = 0\}$$

we claim that S is our desired extension field.

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d
- Let $\mathbb{K}$ be the splitting field of $x^{q^d} - x$
- Let

$$S = \{\alpha \in \mathbb{K} \mid \alpha^{q^d} - \alpha = 0\}$$

we claim that S is our desired extension field.

- S is a field

$$(\alpha+\beta)^{q^d} = \alpha^{q^d} + \beta^{q^d} + \cancel{p(\cdot)} \to 0$$

$$= \alpha^{q^d} + \beta^{q^d} = \alpha + \beta$$

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d
- Let $\mathbb{K}$ be the splitting field of $x^{q^d} - x$
- Let

$$S = \{\alpha \in \mathbb{K} \mid \alpha^{q^d} - \alpha = 0\}$$

  we claim that S is our desired extension field.
- S is a field
- $|S| = q^d$
  1. Note that $x^{q^d} - x$ has no repeated root (since $\gcd(f, f') = 1$)

$$\frac{d}{dx}\left(x^{q^d} - x\right) = \underbrace{q^d}_{0} \cdot x^{q^d - 1} - 1 = -1$$

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d
- Let $\mathbb{K}$ be the splitting field of $x^{q^d} - x$
- Let
$$S = \{\alpha \in \mathbb{K} \mid \alpha^{q^d} - \alpha = 0\}$$
we claim that S is our desired extension field.
- S is a field
- $|S| = q^d$
  1. Note that $x^{q^d} - x$ has no repeated root (since $\gcd(f, f') = 1$)
  2. S can have at most q^d roots over $\mathbb{K}$, since it has degree q^d

Existence of Extension Fields of size q^d Extending $\mathbb{F}_q$

- We will use the splitting field of $f(x) = x^{q^d} - x$ over $\mathbb{F}_q$ to construct an extension field of $\mathbb{F}_q$ of size q^d
- Let $\mathbb{K}$ be the splitting field of $x^{q^d} - x$
- Let
$$S = \{\alpha \in \mathbb{K} \mid \alpha^{q^d} - \alpha = 0\}$$
we claim that S is our desired extension field.
- S is a field
- $|S| = q^d$
  1. Note that $x^{q^d} - x$ has no repeated root (since $\gcd(f, f') = 1$)
  2. S can have at most q^d roots over $\mathbb{K}$, since it has degree q^d
  3. Since we know that all roots of $f(x)$ are in $\mathbb{K}$, we have that $|S| = q^d$

$\alpha \in \mathbb{F}_q \quad \alpha^q = \alpha = \alpha^{q^2} = \cdots$

Number of Monic Irreducible Polynomials of Degree d

- There are at least $\frac{q^d - 1}{d}$ monic irreducible polynomials of degree $\leq d$ over $\mathbb{F}_q$

Number of Monic Irreducible Polynomials of Degree d

- There are at least $\dfrac{q^d - 1}{d}$ monic irreducible polynomials of degree $\leq d$ over $\mathbb{F}_q$
- Take a field extension of $\mathbb{F}_q$ with exactly q^d elements. Call it $\mathbb{K}$

Number of Monic Irreducible Polynomials of Degree d

$$\sum_{i=0}^{d-1} \beta_i \alpha^i = 0$$

$$\underbrace{1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{d-1}}_{d \text{ elements}}$$

if they are Linearly independent then $e_i = \sum_{j=0}^{d-1} \gamma_{ij} \alpha^j$

- There are at least $\dfrac{q^d - 1}{d}$ monic irreducible polynomials of degree $\leq d$ over $\mathbb{F}_q$
- Take a field extension of $\mathbb{F}_q$ with exactly q^d elements. Call it $\mathbb{K}$
- We can consider the smallest degree polynomial in $\mathbb{K}[x]$ that vanishes on $\alpha \in \mathbb{K}$

$\alpha \in \mathbb{K}$

$$\boxed{\alpha = \sum_{i=1}^{d} \beta_i e_i} = \sum_{i=1}^{d} \beta_i \sum_{k=0}^{d-1} \gamma_{ik} \alpha^k$$

$d-1$

$$\underbrace{\alpha, \alpha^2, \dots, \alpha^{d-1}}_{\mathbb{F}_q^d}, \alpha^d$$

$d+1$ vectors over $\mathbb{F}_q^d$ must be Linearly Dependent!

$\implies \exists f(x) \in \mathbb{F}_q[x]$ s.t. $f(\alpha) = 0$, $\deg(f) < d$

Number of Monic Irreducible Polynomials of Degree d

$|\mathbb{K}| = q^d$ $\quad \alpha \leftrightarrow (1, a_{d-2}, \ldots, a_0) = f_\alpha \quad d-1$

f_α has at most d roots over $\mathbb{K}$ $\quad \geq \frac{q^d - 1}{d}$

- There are at least $\boxed{\frac{q^d - 1}{d}}$ monic irreducible polynomials of degree $\leq d$ over $\mathbb{F}_q$
- Take a field extension of $\mathbb{F}_q$ with exactly q^d elements. Call it $\mathbb{K}$
- We can consider the smallest degree polynomial in $\mathbb{K}[x]$ $\mathbb{F}_q$ that vanishes on $\alpha \in \mathbb{K}$
- Has degree $\cancel{\leq}$ $<$ d since $\mathbb{K}$ is a vector space of dimension d over $\mathbb{F}$

smallest deg polynomial $f \in \mathbb{F}_q[x]$
has deg $< d$ and it is irreducible

suppose not : $f(x) = g(x) \cdot h(x)$

$f(\alpha) = 0 \iff g(\alpha) = 0$ or $h(\alpha) = 0$

Properties of $x^{q^d} - x$

Lemma: $f(x)$ irreducible $\mathbb{F}_q[x]$

$f(x) \mid x^{q^d} - x$ iff $\deg(f) \mid d$.

Lemma: $$x^{q^d} - x = \prod_{\substack{f \text{ irreducible} \\ \deg(f) \mid d}} f(x)$$

Madhu's notes.

- Review from last lecture: Cantor-Zassenhaus
- Today's algorithm: Berlekamp's algorithm (1967)
- Properties of Irreducible Polynomials
- **Conclusion**
- Acknowledgements

Conclusion

In today's lecture, we learned

- Berlekamp's Factoring Algorithm
- Properties of irreducible polynomials over finite fields
  1. Field Extensions
  2. Splitting fields
  3. Irreducible polynomials of degree d
  4. Properties of $x^{q^d} - x$ and how they help us in previous tasks

Acknowledgement

Based entirely on

- Lecture 6 from Madhu's notes
  http://people.csail.mit.edu/madhu/FT98/