Extensiones de cuerpos finitos $\mathbb{F}_p$ de grado $n > 1$ y el algoritmo Berlekamp

Joel Barraza Nava

Colorado State University

November 2024

Introduction

- En esta platica exploraremos las extensiones de cuerpos de caracteristica $p > 0$ y primo. Dado un cuerpo finito $\mathbb{F}_p$, quisieramos saber como construir el cuerpo $\mathbb{F}_{p^n}$. Vearemos que la extension $\mathbb{F}_{p^n}$ se puede construir si obtenemos un polinomio irreducible de un variable sobre $\mathbb{F}_p$. Es decir, si $p(x) \in \mathbb{F}_p[x]$ es irreducible de grado n tenemos $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/\langle p(x) \rangle$. Con este hecho, existe un algoritmo "ligero" para determinar si un polinomio es irreducible sobre un cuerpo finito $\mathbb{F}_p$? Resulta que todavia no existe un algoritmo para determinar si un polinomio es irreducible en tiempo polinomio $O(n^k)$. A pesar de esto, terminaremos con un ejemplo del algoritmo Berlekamp cual esta en uso hoy para ver como funciona.

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- Sea $\mathbb{F}$ un cuerpo, la *caracteristica* de $\mathbb{F}$ es el numero entero positivo mas pequeño p tal que $p \cdot 1_{\mathbb{F}} = 0$.
- Siendo p el numero mas pequeño implica que p debe ser 0 o un numero primo.
- Supone que $p = (ab)$, entonces

$$0 = p \cdot 1 = (ab) \cdot 1 = (a \cdot 1)(b \cdot 1)$$

debe ser que $0 = a \cdot 1$ o $0 = b \cdot 1$.

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- Definimos la mapa,

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{F} \\ p &\mapsto p \cdot 1_{\mathbb{F}} \end{aligned}$$

  con $\ker(\varphi) = p\mathbb{Z}$ de modo que $\mathbb{Z}/\ker(\varphi)$ nos da una inyeccion a $\mathbb{F}$.

- Obtenemos un subcuerpo generado por $1_{\mathbb{F}}$.

- Dado que la caracteristica de $\mathbb{F}$ es p un numero primo (o cero), el cuerpo contiene un subcuerpo cual es isomorfico a $\mathbb{F}_p$ (o $\mathbb{Q}$).

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- El cuerpo $\mathbb{K}$ es una *extension* del cuerpo $\mathbb{F}$ si contiene $\mathbb{F}$ como un subcuerpo. Es decir, $\mathbb{F} \leq \mathbb{K}$ y denotado $\mathbb{K}/\mathbb{F}$.
- Dado una extension $\mathbb{K}/\mathbb{F}$ la operacion de multiplicacion hace que $\mathbb{K}$ sea un *espacio vectorial* sobre $\mathbb{F}$.
- El *grado* de $\mathbb{K}/\mathbb{F}$ cual denotamos $[\mathbb{K} : \mathbb{F}]$ es la dimension de $\mathbb{K}$ como un espacio vectorial sobre $\mathbb{F}$.
- Siendo un espacio vectorial, queremos un base para representar los elementos de $\mathbb{K}/\mathbb{F}$.

Cuerpos finitos, $\mathbb{F}_{p^n}$

- En esta platica, restringimos nuestra consideracion a cuerpos de caracteristica $p > 0$.

- Sea $p(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado n sobre $\mathbb{F}_p$. La irreducibilidad de $p(x)$ es equivalente al ideal $\langle p(x) \rangle$ siendo maximal. En consecuencia, $\mathbb{K}$, el cociente dado por $\mathbb{F}_p[x]/\langle p(x) \rangle$ es un cuerpo.

- Deja $\alpha = x \mod p(x) \in \mathbb{K}$, los elementos

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

forman un base para $\mathbb{K}$ como un espacio vectorial sobre $\mathbb{F}_p$ tal que $[\mathbb{K} : \mathbb{F}_p] = n$.

$$\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} |\; a_0, a_1, a_2, \ldots, a_{n-1} \in \mathbb{F}_p\}$$

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- **Ejemplo:** El polinomio $p(x) = x^2 + x + 2$ es irreducible sobre $\mathbb{F}_3$. Existe una extension $\mathbb{F}_3/\langle p(x)\rangle$ conteniendo la raiz α de $p(x)$.

- El conjunto $\{1, \alpha\}$ es un base para la extension. Es decir,

$$\mathbb{F}_3[x]/\langle p(x)\rangle = \{a + b\alpha |\ a, b \in \mathbb{F}_3,\ \alpha^2 = 2\alpha + 1\}.$$

- Sumar:

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$$

- Multiplicacion:

$$\begin{aligned}(a + b\alpha)\cdot(c + d\alpha) &= ac + (ad + bc)\alpha + bc\alpha^2\\ &= ac + (ad + bc)\alpha + bc(2\alpha + 1)\end{aligned}$$

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- **Ejemplo:** El polinomio $p(x) = x^4 + x + 1$ es irreducible sobre $\mathbb{F}_2$. Existe una extension $\mathbb{F}_2[x]/\langle p(x) \rangle$ conteniendo la raiz α of $p(x)$.

- El conjunto $\{1, \alpha, \alpha^2, \alpha^3\}$ es un base para la extension.

$$\{a + b\alpha + c\alpha^2 + d\alpha^3 | \; a, b, c, d \in \mathbb{F}_2, \; \alpha^4 = \alpha + 1\}$$

- De hecho, si el polinomio $p(x) \in \mathbb{F}_p[x]$ es irreducible, el grado del polinomio va indicar el tamaño del cuerpo finito. Es decir, si el grado de $p(x)$ es n la extension contiene p^n elementos. Denotamos la extension del cuerpo finito con $\mathbb{F}_{p^n}$

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- Sea $f(x) \in \mathbb{F}_p[x]$ de grado n y $\mathbb{F}_{p^n}$ una extension de caracteristica $p \neq 0$, se dice que f se *descompone* en $\mathbb{F}_{p^n}$, si se puede escribir como un producto de factores lineales en $\mathbb{F}_{p^n}[x]$. Es decir, existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{p^n}$ tales que

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

  donde $a \in \mathbb{F}_p$ es el coeficiente líder de p.

- Al cuerpo $\mathbb{F}_{p^n}$ se le llama *cuerpo de descomposicion* de caracteristica p si se descompone sobre $\mathbb{F}_{p^n}$ y $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ donde α es una raiz de f.

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- Siendo $\mathbb{F}_{p^n}^{\times}$ generado por α implica que grupo es ciclico y el orden de la raiz es $p^n - 1$. Entonces,

$$\alpha^{p^n - 1} = 1 \Rightarrow \alpha^{p^n} = \alpha \Rightarrow \alpha^{p^n} - \alpha = 0$$

  y resulta que α es una raiz del polinomio $x^{p^n} - x$. Ademas, las raizes del polinomio $x^{p^n} - x$ son todo el cuerpo $\mathbb{F}_{p^n}$.
- Veamos que $\mathbb{F}_{p^n}$ es el cuerpo de descomposicion del polinomio $x^{p^n} - x$.
- Recordamos que α es un raiz de f. Entonces f resulta ser divisor de $x^{p^n} - x$.
- Este hecho motiva el resultado que el polinomio $x^{p^n} - x$ es el producto de polinomios distintos y irreducibles de grado $d > 1$ junto con factores lineales.

Cuerpos Finitos, $\mathbb{F}_{p^n}$

- **Ejemplo:** La factorizacion del polinomio $x^9 - x$ en polinomios de grado 2 sobre $\mathbb{F}_3$.

$$\frac{x^9 - x}{x(x-1)(x-2)} = (x^2 + x + 2)(x^2 + 2x + 2)(x^2 + 1)$$

- Si dos polinomios irreducibles de grado 2 sobre $\mathbb{F}_3$ forman cuerpos con el mismo numero de elementos, son isomorfos?
- Si! En general, todos los cuerpos $\mathbb{F}_{p^n}$ de grado $n \geq 1$ y caracteristica $p > 0$ primo son isomorfos.

Algoritmo Berlekamp

Ejemplo: Factorizamos el polinomio $f(x) = x^4 + x^2 + x + 1$ sobre $\mathbb{F}_2$ con el algoritmo Berlekamp.

- Resolvamos la derivada, $f'(x) = 4x^3 + 2x + 1 \equiv 1 \mod 2$ y calculamos el maximo comun divisor cual es $\gcd(f(x), f'(x)) = 1$. Siendo primos relativos implica que las raizes de $f(x)$ son unicos (multiplicidad 1).
- Calculamos los exponentes $x^{qi} \mod f(x)$ para todo $i = 0, 1, \ldots, n-1$ (dado que $q = 2$ y $n = 4$).

$$x^0 \equiv 1 \mod f$$
$$x^2 \equiv x^2 \mod f$$
$$x^4 \equiv 1 + x + x^2 \mod f$$
$$x^6 \equiv 1 + x + x^3 \mod f$$

Algoritmo Berlekamp

- Los monomios $\{1, x, \ldots, x^{n-1}\}$ forman el base para un espacio vectorial sobre $\mathbb{F}_2$. Los exponentes $1, x^2, x^4, x^6$ son las filas de una matriz (4×4).

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \Rightarrow B - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

- Reducimos $B - I$ con el metodo de eliminacion Gaussiana para calcular el rango del matriz cual es $r = 2$. Por lo tanto, el polinomio $f(x)$ se factoriza en $k = 4 - 2$ polinomios distintos, monicos, y irreducibles.

Algoritmo Berlekamp

- Calculamos el espacio nulo de $B - I$,

$$\mathrm{nul}(B - I) = \{(1,0,0,0),(0,0,1,1)\}$$

cuales vectores coresponden a los polinomios $h_1(x) = 1$ y $h_2(x) = x^2 + x^3$.

- Sea $h_i(x) = c$ para todos $c \in \mathbb{F}_2$, calculamos el maxino comun divisor por cada $(h_i(x) - c, f(x))$.

$$\gcd(f(x), h_2(x) - 0) = x + 1$$
$$\gcd(f(x), h_2(x) - 1) = x^3 + x^2 + 1$$

- El polinomio $f(x)$ se factoriza en dos polinomios monicos, distintos, y irreducibles. El algoritmo termina por la razon de que $k = 2$.

Algoritmo Berlekamp

Ejemplo: Factorizamos el polinomio $f(x) = x^8 + x^7 + x^4 + x^3 + x + 1$ sobre $\mathbb{F}_3$ con el algoritmo Berlekamp.

- Resolvamos la derivada, $f'(x) = 8x^7 + 7x^6 + 4x^3 + 3x^2 + 1 \equiv 2x^7 + x^6 + x^3 + 1 \mod 3$ y $\gcd(f(x), f'(x)) = 1$ implica que las raizes de $f(x)$ son unicos.

- Dado que $q = 3$ y $n = 8$, los exponentes $x^{3i} \mod f(x)$ para todo $i = 0, 1, \ldots, 7$.

Algoritmo Berlekamp

$$
\begin{aligned}
x^0 &\equiv 1 \mod f \\
x^3 &\equiv x^3 \mod f \\
x^6 &\equiv x^6 \mod f \\
x^9 &\equiv 1 + 2x^2 + x^3 + 2x^5 + x^7 \mod f \\
x^{12} &\equiv x + x^4 + 2x^5 \\
x^{15} &\equiv 1 + x + x^3 + 2x^4 + 2x^7 \mod f \\
x^{18} &\equiv 1 + x^4 + 2x^6 \mod f \\
x^{21} &\equiv 2 + x^2 + x^5 \mod f
\end{aligned}
$$

Algoritmo Berlekamp

- Las congruencias forman las filas de un martiz (8×8),

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Algoritmo Berlekamp

- $$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \end{pmatrix}$$

  El rango del matriz $B - I$ es $r = 5$, entonces $f(x)$ se factorizara en $k = 8 - 5 = 3$ polinomios distintos, monicos, y irreducibles.

Algoritmo Berlekamp

- Calculamos el espacio nulo,

$$\begin{aligned}\mathrm{nul}(B - I) = \{&(1,0,0,0,0,0,0,0),\\ &(0,0,0,1,0,0,0,1),(0,2,2,1,1,1,1,0)\}\end{aligned}$$

  cuales coresponden a los polinomios

$$\begin{aligned}h_1(x) &= 1\\ h_2(x) &= x^3 + x^7\\ h_3(x) &= 2x + 2x^2 + x^3 + x^4 + x^5 + x^6\end{aligned}$$

- Calculamos cada maximo comun divisor de $(h_i(x) - c, f(x))$ por todo $c \in \mathbb{F}_3$.

Algoritmo Berlekamp

- Tomamos $h_2(x)$,

$$\gcd(f(x), h_2(x) - 0) = 1$$
$$\gcd(f(x), h_2(x) - 1) = 1 + x$$
$$\gcd(f(x), h_2(x) - 2) = 1 + x^3 + x^7$$

- Entonces $f(x)$ se factoriza en $k = 3$ polinomios pero en este caso solo tenemos dos.

$$f(x) = (1 + x)(1 + x^3 + x^7)$$

Por este caso, applicamos el proceso otra vez al polinomio $1 + x^3 + x^7$ y obtenemos

$$1 + x^3 + x^7 = (2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x).$$

Algoritmo Berlekamp

- Ahora tenemos que,

$$f(x) = (1+x)(2+2x+2x^2+x^3+x^4+x^5+x^6)(2+x)$$

  y para $2+2x+2x^2+x^3+x^4+x^5+x^6$, applicando el proceso una vez mas nos da que $k=1$ entonces el polinomio ya es irreducible.

- Hacemos el proceso una vez mas con $h_3(x)$.

$$\gcd(f(x), h_3(x)-0) = 1+x$$
$$\gcd(f(x), h_3(x)-1) = 2+2x+2x^2+x^3+x^4+x^5+x^6$$
$$\gcd(f(x), h_3(x)-2) = 2+x$$

- La factorizacion de f es,

$$f(x) = (1+x)(2+2x+2x^2+x^3+x^4+x^5+x^6)(2+x).$$