Tópicos Avançados em Ciência da Computação I: Introdução à Teoria de Códigos para Criptografia Pós-quântica

Daniel Panario
School of Mathematics and Statistics
Carleton University

IC - Unicamp, Sala 351 do IC-3
das 13:30 as 18:30 em 16-17 de janeiro de 2020,
das 13:30 as 17:30 em 20-24 de janeiro de 2020

Introdução aos Corpos Finitos: Part II

Daniel Panario
School of Mathematics and Statistics
Carleton University

16-24 de janeiro de 2020

Conteúdo da aula

- Polinômios irredutíveis: definição, função de Möbius, número de polinômios irredutíveis. Propriedades. Testes de irredutibilidade.
- Polinômios minimais: definição, propriedades, exemplos; classes laterais ciclotômicas. Aplicação aos códigos cíclicos.
- Polinômios primitivos: definição, número de polinômios primitivos. Aplicação: LFSRs.
- Fatoração de polinômios: definição, método baseado na eliminação de fatores repetidos, fatoração em graus distintos, e fatoração em graus iguais. Achando raízes de polinômios.

Texto: Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos, Ariane M. Masuda e Daniel Panario. Publicações Matemáticas do IMPA, 26 Colóquio Brasileiro de Matemática, 2007.

Definição e exemplos

Definição

Um polinômio $f \in \mathbb{F}_q[x]$ é irredutível sobre $\mathbb{F}_q$ sempre que $f = gh$, com $g, h \in \mathbb{F}_q[x]$, implicar que g ou h esteja em $\mathbb{F}_q$. Caso contrário, f é redutível sobre $\mathbb{F}_q$.

Exemplos.

1. $ax + b$ com $a \neq 0$ é irredutível sobre $\mathbb{F}_q$.
2. $f(x) = x^6 + 5x^5 + 2x^4 + 10x^3 + x^2 + 2$ é redutível sobre $\mathbb{F}_{11}$, pois $f(x) = (x^2 + 2)(x^4 + 5x^3 + 1)$.
3. Um polinômio f de grau 2 ou 3 é redutível sobre $\mathbb{F}_q$ se e somente se f possui pelo menos uma raiz em $\mathbb{F}_q$.

Definição e exemplos

Definição

Um polinômio $f \in \mathbb{F}_q[x]$ é irredutível sobre $\mathbb{F}_q$ sempre que $f = gh$, com $g, h \in \mathbb{F}_q[x]$, implicar que g ou h esteja em $\mathbb{F}_q$. Caso contrário, f é redutível sobre $\mathbb{F}_q$.

Exemplos.

1. $ax + b$ com $a \neq 0$ é irredutível sobre $\mathbb{F}_q$.
2. $f(x) = x^6 + 5x^5 + 2x^4 + 10x^3 + x^2 + 2$ é redutível sobre $\mathbb{F}_{11}$, pois $f(x) = (x^2 + 2)(x^4 + 5x^3 + 1)$.
3. Um polinômio f de grau 2 ou 3 é redutível sobre $\mathbb{F}_q$ se e somente se f possui pelo menos uma raiz em $\mathbb{F}_q$.

Definição e exemplos

Definição

Um polinômio $f \in \mathbb{F}_q[x]$ é irredutível sobre $\mathbb{F}_q$ sempre que $f = gh$, com $g, h \in \mathbb{F}_q[x]$, implicar que g ou h esteja em $\mathbb{F}_q$. Caso contrário, f é redutível sobre $\mathbb{F}_q$.

Exemplos.

1. $ax + b$ com $a \neq 0$ é irredutível sobre $\mathbb{F}_q$.
2. $f(x) = x^6 + 5x^5 + 2x^4 + 10x^3 + x^2 + 2$ é redutível sobre $\mathbb{F}_{11}$, pois $f(x) = (x^2 + 2)(x^4 + 5x^3 + 1)$.
3. Um polinômio f de grau 2 ou 3 é redutível sobre $\mathbb{F}_q$ se e somente se f possui pelo menos uma raiz em $\mathbb{F}_q$.

Definição e exemplos

Definição

Um polinômio $f \in \mathbb{F}_q[x]$ é irredutível sobre $\mathbb{F}_q$ sempre que $f = gh$, com $g, h \in \mathbb{F}_q[x]$, implicar que g ou h esteja em $\mathbb{F}_q$. Caso contrário, f é redutível sobre $\mathbb{F}_q$.

Exemplos.

1. $ax + b$ com $a \neq 0$ é irredutível sobre $\mathbb{F}_q$.
2. $f(x) = x^6 + 5x^5 + 2x^4 + 10x^3 + x^2 + 2$ é redutível sobre $\mathbb{F}_{11}$, pois $f(x) = (x^2 + 2)(x^4 + 5x^3 + 1)$.
3. Um polinômio f de grau 2 ou 3 é redutível sobre $\mathbb{F}_q$ se e somente se f possui pelo menos uma raiz em $\mathbb{F}_q$.

Função de Möbius

Definição

A função μ de Möbius é a função $\mu\colon \mathbb{N} \to \mathbb{N}$ definida por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ (-1)^k & \text{se } n \text{ é um produto de } k \text{ primos distintos}, \\ 0 & \text{caso contrário.} \end{cases}$$

Exemplos.

$\mu(7) = -1$, $\mu(6) = (-1)^2 = 1$, $\mu(12) = 0$.

Propriedades da função de Möbius

Apresentamos duas propriedades importantes da função de Möbius.

Lema

Para todo $n \in \mathbb{N}$, temos que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

Demonstração.

O caso $n = 1$ é trivial, uma vez que $\sum_{d|n} \mu(d) = \mu(1) = 1$.

Se $n > 1$, é suficiente considerar a soma $\sum_{d|n} \mu(d)$ para os valores $d = 1$, e os divisores d de n que têm uma fatoração em números primos distintos, dado que $\mu(d) = 0$ para todos os outros valores de d. Suponhamos que $p_1, p_2, \ldots, p_k$ sejam os divisores primos distintos de n. Temos que

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \le i_1 < i_2 \le k} \mu(p_{i_1} p_{i_2}) \\ &\quad + \sum_{1 \le i_1 < i_2 < i_3 \le k} \mu(p_{i_1} p_{i_2} p_{i_3}) + \cdots + \mu(p_1 p_2 \cdots p_k) \\ &= 1 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= \left(1 + (-1)\right)^k = 0. \end{aligned}$$

□

Fórmula de inversão de Möbius

O teorema seguinte é importante para achar o número de polinômios irredutíveis de um corpo finito com q elementos.

Teorema

Sejam f e g funções de $\mathbb{N}$ num grupo abeliano aditivo. Então, para todo $n \in \mathbb{N}$, temos que

$$f(n) = \sum_{d|n} g(d) \quad \textit{se e somente se} \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Demonstração. Suponhamos que $f(n) = \sum_{d|n} g(d)$. Se c e d são divisores de n, então c divide n/d se e somente se d divide n/c. Portanto,

$$\begin{aligned}
\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} g(c) \\
&= \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) g(c) \\
&= \sum_{c|n} g(c) \sum_{d|\frac{n}{c}} \mu(d) \\
&= g(n),
\end{aligned}$$

onde o último passo se deve ao fato de que, pelo lema anterior, é suficiente considerar o caso $c = n$. A recíproca é provada de maneira similar. □

Número de polinômios irredutíveis

Para estabelecer o número de polinômios irredutíveis de grau n no corpo finito de q elementos, necessitamos do seguinte teorema.

Esse teorema é fundamental para derivar não só a fórmula do número de polinômios irredutíveis, mas também para projetar algoritmos rápidos para testar a irredutibilidade de polinômios e para fatorar polinômios (como veremos depois).

Teorema

O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

Teorema

O número de polinômios mônicos irredutíveis de grau n sobre $\mathbb{F}_q$ é

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

onde μ é a função de Möbius.

Demonstração.

Comparando os graus dos polinômios no teorema anterior, obtemos que $q^n = \sum_{d|n} d I_d$. Pela fórmula de inversão de Möbius, temos que $n I_n = \sum_{d|n} \mu(d) q^{n/d}$. □

Teorema

O número de polinômios mônicos irredutíveis de grau n sobre $\mathbb{F}_q$ é

$$I_n = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

onde μ é a função de Möbius.

Demonstração.

Comparando os graus dos polinômios no teorema anterior, obtemos que $q^n = \sum_{d|n} dI_d$. Pela fórmula de inversão de Möbius, temos que $nI_n = \sum_{d|n}\mu(d)q^{n/d}$. □

Exemplo.

Há q^{24} polinômios mônicos de grau 24 em $\mathbb{F}_q[x]$, enquanto que o número de polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ de grau 24 é

$$\begin{aligned} I_{24} &= \frac{1}{24}\left(\mu(1)q^{24} + \mu(2)q^{12} + \mu(3)q^8 + \mu(4)q^6 + \mu(6)q^4\right. \\ &\quad \left. + \mu(8)q^3 + \mu(12)q^2 + \mu(24)q\right) \\ &= \frac{1}{24}\left(q^{24} - q^{12} - q^8 + q^4\right). \end{aligned}$$

Assim, a probabilidade de que um polinômio mônico de grau 24 seja irredutível sobre $\mathbb{F}_q$ é

$$\frac{I_{24}}{q^{24}} = \frac{1}{24}\left(1 - \frac{1}{q^{12}} - \frac{1}{q^{16}} + \frac{1}{q^{20}}\right) \approx \frac{1}{24}.$$

Outro exemplo: em $\mathbb{F}_2$ o número de polinômios de grau 100 é (verifique!):

$$\frac{1}{100}\left(2^{100} - 2^{50} - 2^{20} + 2^{10}\right),$$

e a probabilidade de um polinômio de grau 100 ser irredutível é perto de $1/100$. Em geral, se o grau do polinômio é n, esta probabilidade é aproximadamente $1/n$.

Podemos deduzir que o número de polinômios irredutíveis I_n é positivo para todas as potências q de um número primo e todos os inteiros $n > 1$:

$$I_n = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \geq \frac{1}{n}\left(q^n - q^{n-1} - q^{n-2} - \cdots - q\right) > 0.$$

Esse teorema também dá um algoritmo probabilístico para encontrar polinômios irredutíveis, como veremos a seguir.

Um resultado fundamental

O seguinte teorema pode ser usado para testar a irredutibilidade de um polinômio sobre $\mathbb{F}_q$.

Teorema

O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

Primeiramente calculamos $\mathrm{mdc}(f, x^q - x)$. Se esse mdc não é 1, então f tem fatores lineares e, portanto, é redutível.

Caso contrário, calculamos o $\mathrm{mdc}(f, x^{q^2} - x)$ para verificar se f tem fatores irredutíveis cujos graus dividem 2. Como f não tem nenhum fator linear, estamos testando se f tem algum fator irredutível de grau exatamente igual a 2, e assim sucessivamente.

Um resultado fundamental: prova

Teorema

O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

Demonstração.
Temos que $x^{q^n} - x$ é um produto de polinômios irredutíveis distintos sobre $\mathbb{F}_q$. Seja f um desses fatores irredutíveis de grau m. Segue que $\mathbb{F}_{q^n}$ contém uma raiz θ de f e, portanto, $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_{q^n}$. Portanto, $[\mathbb{F}_q(\theta) : \mathbb{F}_q] = m$ divide $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Reciprocamente, seja f um polinômio irredutível sobre $\mathbb{F}_q$ de grau m onde $m \mid n$. Se θ é uma raiz de f no corpo de decomposição, concluímos que $\mathbb{F}_q(\theta) \cong \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ e $\theta^{q^n} - \theta = 0$. Logo, f é o polinômio minimal de θ e, assim, divide $x^{q^n} - x$. □

Um resultado fundamental: prova

Teorema

O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

Demonstração.
Temos que $x^{q^n} - x$ é um produto de polinômios irredutíveis distintos sobre $\mathbb{F}_q$. Seja f um desses fatores irredutíveis de grau m. Segue que $\mathbb{F}_{q^n}$ contém uma raiz θ de f e, portanto, $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_{q^n}$. Portanto, $[\mathbb{F}_q(\theta) : \mathbb{F}_q] = m$ divide $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Reciprocamente, seja f um polinômio irredutível sobre $\mathbb{F}_q$ de grau m onde $m \mid n$. Se θ é uma raiz de f no corpo de decomposição, concluímos que $\mathbb{F}_q(\theta) \cong \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ e $\theta^{q^n} - \theta = 0$. Logo, f é o polinômio minimal de θ e, assim, divide $x^{q^n} - x$. □

Um resultado fundamental: prova

Teorema

O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

Demonstração.
Temos que $x^{q^n} - x$ é um produto de polinômios irredutíveis distintos sobre $\mathbb{F}_q$. Seja f um desses fatores irredutíveis de grau m. Segue que $\mathbb{F}_{q^n}$ contém uma raiz θ de f e, portanto, $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_{q^n}$. Portanto, $[\mathbb{F}_q(\theta) : \mathbb{F}_q] = m$ divide $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Reciprocamente, seja f um polinômio irredutível sobre $\mathbb{F}_q$ de grau m onde $m \mid n$. Se θ é uma raiz de f no corpo de decomposição, concluímos que $\mathbb{F}_q(\theta) \cong \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ e $\theta^{q^n} - \theta = 0$. Logo, f é o polinômio minimal de θ e, assim, divide $x^{q^n} - x$. □

Um resultado fundamental: exemplos

Exemplo. Consideremos $q = 2$:

- $n = 2$: $x^{q^n} - x = x^4 - x = x(x+1)(x^2+x+1)$
- $n = 3$: $x^{q^n} - x = x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$
- $n = 4$: $x^{q^n} - x = x^{16} - x =$
  $x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

Um resultado fundamental: exemplos

Exemplo. Consideremos $q = 2$:

- $n = 2$: $x^{q^n} - x = x^4 - x = x(x+1)(x^2+x+1)$
- $n = 3$: $x^{q^n} - x = x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$
- $n = 4$: $x^{q^n} - x = x^{16} - x =$
  $x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

Um resultado fundamental: exemplos

Exemplo. Consideremos $q = 2$:

- $n = 2$: $x^{q^n} - x = x^4 - x = x(x+1)(x^2+x+1)$
- $n = 3$: $x^{q^n} - x = x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$
- $n = 4$: $x^{q^n} - x = x^{16} - x =$
  $x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

Algoritmo de teste de irredutibilidade

Entrada: $f \in \mathbb{F}_q[x]$ de grau n.
Saída: "f irredutível" ou "f redutível".

Idéia: Se $\mathrm{mdc}(f, x^q - x) \neq 1$, então f tem fatores lineares. Caso contrário, calcule $\mathrm{mdc}(f, x^{q^2} - x)$. Se tal mdc não é 1, então f tem um fator irredutível de grau 2. Continue calculando $\mathrm{mdc}(f, x^{q^i} - x)$, enquanto $i \leq \mathrm{grau}(f)/2$ e $\mathrm{mdc} \neq 1$.

```
para i = 1 até ⌊n/2⌋ faça
   se mdc(f, x^{q^i} − x) ≠ 1 então
      { retorne ''f redutível'' e pare; }
retorne ''f irredutível'';
```


Algoritmo de teste de irredutibilidade

Entrada: $f \in \mathbb{F}_q[x]$ de grau n.
Saída: "f irredutível" ou "f redutível".

Idéia: Se $\mathrm{mdc}(f, x^q - x) \neq 1$, então f tem fatores lineares. Caso contrário, calcule $\mathrm{mdc}(f, x^{q^2} - x)$. Se tal mdc não é 1, então f tem um fator irredutível de grau 2. Continue calculando $\mathrm{mdc}(f, x^{q^i} - x)$, enquanto $i \leq \mathrm{grau}(f)/2$ e $\mathrm{mdc} \neq 1$.

```
para i = 1 até ⌊n/2⌋ faça
   se mdc(f, x^{q^i} − x) ≠ 1 então
      { retorne ''f redutível'' e pare; }
retorne ''f irredutível'';
```

Daniel Panario | Introdução aos Corpos Finitos: Part II | 16-24 de janeiro de 2020 | 17 / 68

Algoritmo de teste de irredutibilidade

Entrada: $f \in \mathbb{F}_q[x]$ de grau n.
Saída: "f irredutível" ou "f redutível".

Idéia: Se $\mathrm{mdc}(f, x^q - x) \neq 1$, então f tem fatores lineares. Caso contrário, calcule $\mathrm{mdc}(f, x^{q^2} - x)$. Se tal mdc não é 1, então f tem um fator irredutível de grau 2. Continue calculando $\mathrm{mdc}(f, x^{q^i} - x)$, enquanto $i \leq \mathrm{grau}(f)/2$ e $\mathrm{mdc} \neq 1$.

```
para i = 1 até ⌊n/2⌋ faça
   se mdc(f, x^{q^i} − x) ≠ 1 então
      { retorne ‘‘f redutível’’ e pare; }
retorne ‘‘f irredutível’’;
```


Exemplos

1. Como $\mathrm{mdc}(x^{15} - 1, x^{11} - x) = x^5 - 1$, o polinômio $x^{15} - 1$ é redutível sobre $\mathbb{F}_{11}$. Em particular, esse mdc mostra que $x^{15} - 1$ tem cinco fatores lineares: $x - 1$, $x - 3$, $x - 4$, $x - 5$ e $x - 9$.

2. Seja $f(x) = x^6 + 10x^5 + x^4 + 14x^3 + 13x^2 + x + 3$ em $\mathbb{F}_{17}[x]$. Temos que $\mathrm{mdc}(x^{17} - x, f) = 1$ e $\mathrm{mdc}(x^{17^2} - x, f) = 1$; portanto, f não tem fatores lineares, nem quadráticos. No entanto, temos que $\mathrm{mdc}(x^{17^3} - x, f) = f$, o que mostra que f não só é redutível sobre $\mathbb{F}_{17}$, mas também é o produto de dois fatores irredutíveis de grau 3. De fato, $f(x) = (x^3 + x + 3)(x^3 + 10x^2 + 1)$.

Exemplos

1. Como $\mathrm{mdc}(x^{15}-1, x^{11}-x) = x^5 - 1$, o polinômio $x^{15}-1$ é redutível sobre $\mathbb{F}_{11}$. Em particular, esse mdc mostra que $x^{15}-1$ tem cinco fatores lineares: $x-1$, $x-3$, $x-4$, $x-5$ e $x-9$.

2. Seja $f(x) = x^6 + 10x^5 + x^4 + 14x^3 + 13x^2 + x + 3$ em $\mathbb{F}_{17}[x]$. Temos que $\mathrm{mdc}(x^{17} - x, f) = 1$ e $\mathrm{mdc}(x^{17^2} - x, f) = 1$; portanto, f não tem fatores lineares, nem quadráticos. No entanto, temos que $\mathrm{mdc}(x^{17^3} - x, f) = f$, o que mostra que f não só é redutível sobre $\mathbb{F}_{17}$, mas também é o produto de dois fatores irredutíveis de grau 3. De fato, $f(x) = (x^3 + x + 3)(x^3 + 10x^2 + 1)$.

Polinômios Minimais

Definição e motivação

Definição

Seja K uma extensão do corpo F. Um elemento $\theta \in K$ é algébrico sobre F, se existe $f \in F[x]$ tal que $f(\theta) = 0$.

Suponhamos que θ seja algébrico sobre F. Seja M um polinômio mônico de menor grau dentre todos os polinômios f em $F[x]$ tais que $f(\theta) = 0$. Então M divide qualquer polinômio f com tal propriedade. De fato, escrevendo $f = qM + r$ onde $\text{grau}(r) < \text{grau}(M)$, obtemos que $r(\theta) = 0$. Pela minimalidade do grau de M, concluímos que $r = 0$ e M divide f.

M é também único e dizemos que M é o polinômio minimal de θ.

Polinômios minimais estão diretamente relacionados com códigos cíclicos e polinômios primitivos, por exemplo.

Seja $q = p^\ell$, $K = \mathbb{F}_q$ e $F = \mathbb{F}_p$. O polinômio minimal de $\alpha \in \mathbb{F}_q$ é definido sobre $\mathbb{F}_p$ e, portanto, se escreve com coeficientes em $\mathbb{F}_p$.

Temos que $\alpha^q = \alpha$ e, portanto, α é raiz do polinômio $x^q - x$.
Então, α é algébrico sobre $\mathbb{F}_p$ e, portanto, tem um polinômio minimal $M \in \mathbb{F}_p[x]$.

É claro que o polinômio minimal de $\alpha \in \mathbb{F}_p$ é $x - \alpha$.
Qual é o polinômio minimal de $\alpha \in \mathbb{F}_q$?

Exemplo

Sejam $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3+x+1)$ *e* α *raiz de* x^3+x+1.

elemento	*polinômio minimal*
0	x
1	$x+1$
α	x^3+x+1
α^2	x^3+x+1
α^3	x^3+x^2+1
α^4	x^3+x+1
α^5	x^3+x^2+1
α^6	x^3+x^2+1

Temos que $x^3+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$; *e se* $\beta=\alpha^3$, $x^3+x^2+1=(x-\beta)(x-\beta^2)(x-\beta^4)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^5)$ *(verifique!).*

Exemplo

Sejam $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3+x+1)$ *e* α *raiz de* x^3+x+1.

elemento	*polinômio minimal*
0	x
1	$x+1$
α	x^3+x+1
α^2	x^3+x+1
α^3	x^3+x^2+1
α^4	x^3+x+1
α^5	x^3+x^2+1
α^6	x^3+x^2+1

Temos que $x^3+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$; *e se* $\beta=\alpha^3$, $x^3+x^2+1=(x-\beta)(x-\beta^2)(x-\beta^4)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^5)$ *(verifique!).*

Daniel Panario | Introdução aos Corpos Finitos: Part II | 16-24 de janeiro de 2020 | 22 / 68

Propriedades

Proposition

Seja $\alpha \in \mathbb{F}_{p^m}$ com polinômio minimal M sobre $\mathbb{F}_p$. Então:

1. *M é irredutível sobre $\mathbb{F}_p$;*
2. *se $f \in \mathbb{F}_p[x]$ com $f(\alpha) = 0$, então $M \mid f$;*
3. *$M \mid (x^{p^m} - x)$;*
4. *$\text{grau}(M) \leq m$;*
5. *se α é um elemento primitivo de $\mathbb{F}_{p^m}$, então $\text{grau}(M) = m$ e M é um polinômio primitivo.*

Proposition

Sejam $\alpha \in \mathbb{F}_q$ e $p = \text{car}(\mathbb{F}_q)$. Então, α e α^p têm o mesmo polinômio minimal sobre $\mathbb{F}_p$.

Exemplo

Para $\alpha \in \mathbb{F}_{2^3}$, temos que

$$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8 = \alpha$$

têm o mesmo polinômio minimal. O mesmo acontece com

$$\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^6)^2 = \alpha^{12} = \alpha^5, (\alpha^5)^2 = \alpha^{10} = \alpha^3.$$

Vimos que se α é raiz de $x^3 + x + 1$, então
$x^3 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$ e
$x^3 + x^2 + 1 = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5)$. Temos que

$$x^{2^3-1} - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Proposition

Sejam $\alpha \in \mathbb{F}_q$ e $p = \mathrm{car}(\mathbb{F}_q)$. Então, α e α^p têm o mesmo polinômio minimal sobre $\mathbb{F}_p$.

Exemplo

Para $\alpha \in \mathbb{F}_{2^3}$, temos que

$$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8 = \alpha$$

têm o mesmo polinômio minimal. O mesmo acontece com

$$\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^6)^2 = \alpha^{12} = \alpha^5, (\alpha^5)^2 = \alpha^{10} = \alpha^3.$$

Vimos que se α é raiz de $x^3 + x + 1$, então
$x^3 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$ *e*
$x^3 + x^2 + 1 = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5)$. *Temos que*

$$x^{2^3-1} - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Exemplo

Para $\alpha \in \mathbb{F}_{2^4}$, temos que

$$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8, (\alpha^8)^2 = \alpha^{16} = \alpha$$

têm o mesmo polinômio minimal. O mesmo acontece com

$$\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^6)^2 = \alpha^{12}, (\alpha^{12})^2 = \alpha^{24} = \alpha^9, (\alpha^9)^2 = \alpha^{18} = \alpha^3;$$

com

$$\alpha^5, (\alpha^5)^2 = \alpha^{10}, (\alpha^{10})^2 = \alpha^{20} = \alpha^5;$$

e com

$$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}.$$

Se $\alpha \in \mathbb{F}_{2^4}$ é um elemento primitivo raiz de x^4+x+1, todos os elementos de $\mathbb{F}_{2^4}^*$ se escrevem como uma potência de α. E temos

$$\begin{aligned}\prod_{\beta\in\mathbb{F}_{2^4}^*}(x-\beta) &= (x-1)\,[(x-\alpha^5)(x-\alpha^{10})] \\ &\quad [(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)] \\ &\quad [(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)] \\ &\quad [(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})]\end{aligned}$$

O produto da direita é

$$(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1) = x^{15}-1,$$

e, portanto, são os polinômios irredutíveis de grau dividindo 4:

$$\prod_{\alpha\in\mathbb{F}_{2^4}^*}(x-\alpha) = x^{15}-1.$$

Porém $x^4+x^3+x^2+x+1$ não é primitivo (por que?).

Classes laterais ciclotômicas

A operação de multiplicar por p particiona $\mathbb{Z}_{p^m-1}$ em certos conjuntos módulo p^m-1.

Definição

Seja m_s o menor inteiro positivo tal que $p^{m_s}s \equiv s \pmod{p^m-1}$. A classe lateral ciclotômica de s é

$$\{s, ps, p^2s, \ldots, p^{m_s-1}s\}.$$

Exemplo: Para $p=2$, $m=3$ e $p^m-1=7$, as classes laterais ciclotômicas módulo 7 são

$$C_0=\{0\},\ C_1=\{1,2,4\},\ C_3=\{3,6,5\}.$$

Estas classes correspondem aos expoentes de α que têm o mesmo polinômio minimal!

Classes laterais ciclotômicas

A operação de multiplicar por p particiona $\mathbb{Z}_{p^m-1}$ em certos conjuntos módulo $p^m - 1$.

Definição

Seja m_s o menor inteiro positivo tal que $p^{m_s} s \equiv s \pmod{p^m - 1}$. A classe lateral ciclotômica de s é

$$\{s, ps, p^2 s, \ldots, p^{m_s - 1} s\}.$$

Exemplo: Para $p = 2$, $m = 3$ e $p^m - 1 = 7$, as classes laterais ciclotômicas módulo 7 são

$$C_0 = \{0\}, \ C_1 = \{1, 2, 4\}, \ C_3 = \{3, 6, 5\}.$$

Estas classes correspondem aos expoentes de α que têm o mesmo polinômio minimal!

Teorema

Sejam $q = p^m$ e β um elemento primitivo em $\mathbb{F}_q$. Então, para $0 \leq s \leq p^m - 1$ e $i \in C_s$, temos que

$$M^{(i)}(x) = \prod_{j \in C_s} (x - \beta^j),$$

onde $M^{(i)}$ é o polinômio minimal de β^i sobre $\mathbb{F}_p$. Além disso, como

$$x^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^*} (x - \alpha) = \prod_{0 \leq j \leq q-1} (x - \beta^j),$$

temos que $x^{q-1} - 1 = \prod_s M^{(s)}(x)$, onde s varia sobre os representantes das classes laterais ciclotômicas módulo $p^m - 1$.

Polinômios Primitivos

Polinômios primitivos

Polinômios primitivos formam uma classe particular importante de polinômios irredutíveis.

Definição

Um polinômio $f \in \mathbb{F}_q[x]$ de grau m é primitivo, se f é o polinômio minimal sobre $\mathbb{F}_q$ de algum elemento primitivo em $\mathbb{F}_{q^m}$.

Definição

Seja p a característica de $\mathbb{F}_q$. Um polinômio $g \in \mathbb{F}_p[x]$ é o polinômio minimal de $\alpha \in \mathbb{F}_q$, se é mônico e tem o menor grau dentre os polinômios com α como raiz.

Polinômios minimais são irredutíveis (como veremos), e possuem a propriedade de que qualquer outro polinômio não nulo h satisfazendo $h(\alpha) = 0$ é um múltiplo de g.

Polinômios primitivos (cont)

Em outras palavras, um polinômio primitivo de grau m é um polinômio mônico e irredutível, com a propriedade adicional de que, se $\alpha \in \mathbb{F}_{q^m}$ é uma raiz de f, então a ordem de α é $q^m - 1$. Portanto, as raízes de um polinômio primitivo são geradores do grupo multiplicativo $\mathbb{F}_{q^m}^*$.

Uma definição alternativa é a seguinte:

Um polinômio irredutível $f \in \mathbb{F}_q[x]$ de grau m é um polinômio primitivo se o menor inteiro positivo n tal que $f(x) \mid x^n - 1$ é $n = q^m - 1$.

Número de polinômios primitivos

Vimos que o número de elementos primitivos em $\mathbb{F}_{p^m}$ é $\phi(p^m - 1)$, onde ϕ é a função de Euler.

O número de polinômios primitivos em $\mathbb{F}_{p^m}[x]$ é $\phi(p^m - 1)/m$.

De fato, se f é um polinômio primitivo e α é uma de suas raízes, então os conjugados de α têm o mesmo polinômio primitivo f.

Exemplo

Seja $p = 2$, $m = 2$. Em $\mathbb{F}_{2^2}$ temos

$$\phi(p^m - 1)/m = \phi(3)/2 = 1$$

polinômio primitivo: $x^2 + x + 1$.
(Verifique que uma raiz α de $x^2 + x + 1$ é um elemento primitivo.)

Temos que $x^{2^2} - x = x(x + 1)(x^2 + x + 1)$.

Exemplo

Seja $p = 2$, $m = 3$. Em $\mathbb{F}_{2^3}$ temos

$$\phi(p^m - 1)/m = \phi(7)/3 = 6/3 = 2$$

polinômios primitivos: $x^3 + x + 1$ e $x^3 + x^2 + 1$ (verifique!!).
Temos que $x^{2^3} - x = x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Exemplo

Seja $p = 2$, $m = 4$. Em $\mathbb{F}_{2^4}$ temos

$$\phi(p^m - 1)/m = \phi(15)/4 = 8/4 = 2.$$

Exercício: ache os dois polinômios primitivos (dentre os três irredutíveis) em $\mathbb{F}_{2^4}$ e a decomposição de $x^{2^4} - x$.

Uma aplicação: LFSR

As sequências em corpos finitos são usadas numa variedade de aplicações, nas áreas de engenharia e criptografia. Por exemplo, elas aparecem na comunicação digital, na construção de geradores de números pseudo-aleatórios e nas cifras de fluxo.

Normalmente, representamos uma seqüência usando um registrador de deslocamento com realimentação linear. Neste curso, denotaremos este registrador por LFSR, que é a abreviação das iniciais em inglês (Linear Feedback Shift Register).

Cada registrador do LFSR contém um valor em $\mathbb{F}_q$. Chamamos de estado do LFSR a n-upla de valores contida no LFSR. Há, então, q^n estados no LFSR. Denotaremos os estados do LFSR por vetores em $\mathbb{F}_q^n$, onde n é o número de registradores do LFSR.

O LFSR muda de estado de acordo com uma função linear. A saída do LFSR é usada como realimentação do LFSR para gerar o estado seguinte. O estado inicial $\overrightarrow{\mathbf{S_0}}$ do LFSR é chamado de semente do registrador. O LFSR resulta deterministicamente num elemento em $\mathbb{F}_q$ de cada vez. Logo, a sequência de valores do LFSR é completamente determinada pela sua semente.

Na maioria das aplicações práticas, o corpo finito usado é $\mathbb{F}_2$ e o LFSR computa, assim, um bit. Porém, não há necessidade de considerar somente $\mathbb{F}_2$ e consideraremos um corpo finito de q elementos.

Dizemos que uma sequência $s_0, s_1, s_2, \ldots$ em $\mathbb{F}_q$ satisfaz uma recorrência linear (homogênea) de ordem n se, para $k = 0, 1, \ldots$

$$s_{k+n} = a_{n-1}s_{k+n-1} + a_{n-2}s_{k+n-2} + \cdots + a_0 s_k. \tag{1}$$

Para cada sequência, existe um LFSR que a calcula.

Seja a sequência $\{s_k\}$ em $\mathbb{F}_2$ definida por

$$s_{k+4} = s_{k+1} + s_k, \quad k \geq 0, \quad s_0 = s_1 = s_2 = 0, \ s_3 = 1.$$

O LFSR correspondente tem 4 registradores. Sejam x_0, x_1, x_2 e x_3 os valores atuais dos 4 registradores do LFSR, onde x_0 é o valor mais à direita e x_3 é o valor mais à esquerda do LFSR. Então, o estado atual do LFSR é o vetor (x_3, x_2, x_1, x_0). É claro que a função linear (1) correspondente é $x_0 + x_1$ e a mudança de estado é dada por

$$(x_3, x_2, x_1, x_0) \mapsto (x_0 + x_1, x_3, x_2, x_1).$$

A semente é o vetor consistindo dos valores iniciais da sequência, ou seja, $\overrightarrow{\mathbf{S_0}} = (s_3, s_2, s_1, s_0) = (1, 0, 0, 0)$; veja a figura seguinte.

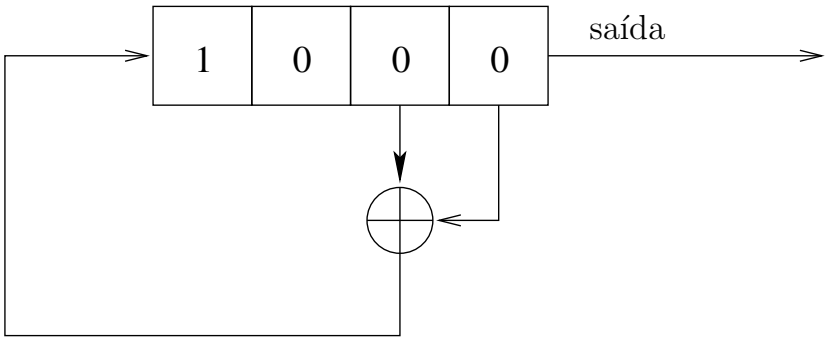


Figura: LFSR de $s_{k+4} = s_{k+1} + s_k$.

A saída, a cada vez, é o valor do último registrador; portanto, 0 é a primeira saída. Em seguida, aplica-se a função (1) ao vetor $(1, 0, 0, 0)$ para obter $(0, 1, 0, 0)$ nos registradores. A segunda saída é, então, novamente 0. No próximo passo, os registradores contêm $(0, 0, 1, 0)$ e a saída é 0.

Mais uma aplicação de (1) produz $(1, 0, 0, 1)$ nos registradores e uma saída igual a 1. Continuando assim, vemos que os primeiros 15 termos da sequência são 000100110101111.

A cada LFSR, ou seja, a cada sequência satisfazendo uma recorrência da forma (1), associamos um polinômio em $\mathbb{F}_q[x]$, chamado polinômio característico do LFSR, da seguinte maneira. Se o comprimento (ou o número de registradores) do LFSR é n, o polinômio característico tem grau n. Além disso, seus coeficientes em $\mathbb{F}_q$ preenchem as portas lógicas do LFSR de tal maneira que, se (1) é satisfeita, então

$$f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0 \tag{2}$$

é o polinômio característico do LFSR. Reciprocamente, dado o polinômio (2), podemos construir o LFSR correspondente. A função linear associada é dada pela matriz

$$A = \begin{pmatrix} a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

que é essencialmente a matriz companheira de f. Se $\overrightarrow{\mathbf{S_0}}$ é a semente, então o próximo estado é $\overrightarrow{\mathbf{S_1}} = A\overrightarrow{\mathbf{S_0}}$.

Em geral, temos que $\overrightarrow{\mathbf{S_k}} = A\overrightarrow{\mathbf{S_{k-1}}} = A^k\overrightarrow{\mathbf{S_0}}$. Portanto, após k passos, o LFSR terá $\overrightarrow{\mathbf{S_k}}$ nos seus registradores. A k-ésima saída será a última entrada de $\overrightarrow{\mathbf{S_k}}$.

Exemplo

Consideremos a seqüência do exemplo anterior. O polinômio característico é $x^4 + x + 1$, *a matriz companheira é*

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

e a semente é $\overrightarrow{\mathbf{S_0}} = (1, 0, 0, 0)$.

O LFSR tem um número finito de estados: se o LFSR tem n registradores, então tem no máximo q^n estados. Assim, deve repetir estado e, depois daquele momento, a sequência de saídas será repetida. O comprimento do ciclo é o período do LFSR.

Nas aplicações práticas, estamos interessados nos LFSR's com períodos maximais. Ciclos LFSR's maximais visitam todos os possíveis $q^n - 1$ estados do registrador de deslocamentos com a exceção do estado em que todas as entradas dos registradores são nulas. A propriedade mais importante de um LFSR é dada pelo próximo teorema.

Teorema

Uma condição necessária e suficiente para a seqüência gerada por um LFSR, com semente não nula, ter comprimento maximal é que seu polinômio característico seja primitivo.

Uma demonstração deste resultado pode ser encontrada no livro de Golomb e Gong, por exemplo. O LFSR do exemplo anterior tem comprimento maximal. Nesse livro se encontram também as propriedades que uma seqüência tem que ter para parecer aleatória (balance, distribuição de tuplas e "runs", complexidade linear, etc).

Exemplo.

Considere o LFSR da figura anterior. O polinômio característico é $f(x) = x^4 + x + 1$. Como f é um polinômio primitivo, o LFSR tem comprimento maximal.

Como já vimos, se usarmos a semente 1000, a seqüência de período maximal 15 é 000100110101111. Se usarmos a semente 1111, por exemplo, a seqüência gerada será 111100010011010 (exercício).

De fato, cada uma das 15 possíveis sementes não nulas gera uma seqüência de período maximal 15. A semente 0000 gera a seqüência 00000000000000, que não é interessante. □

A literatura sobre LFSR é bem vasta; veja, por exemplo, os livros de Golomb; Golomb e Gong; Berlekamp; Lidl e Niederreiter; e Jungnickel.

Fatoração de Polinômios

O problema

Seja $\mathbb{F}_q$ um corpo finito:

Dado um polinômio mônico $f \in \mathbb{F}_q[x]$, achar a fatoração completa $f = f_1^{e_1} \cdots f_r^{e_r}$, onde os polinômios irredutíveis $f_1, \ldots, f_r$, são dois a dois distintos e $e_i > 0$, $1 \leq i \leq r$.

Aplicações

- Teoria algébrica de códigos (Berlekamp 1968);
- Álgebra computacional (Collins 1979, Knuth 1981, Geddes, Czapor e Labahn 1992);
- Criptografia (Chor e Rivest 1984, Odlyzko 1985, Lenstra 1991);
- Teoria computacional de números (Buchmann 1990).
- Criptografia Pós-Quântica (seculo XXI).

Método geral para fatorar polinômios

ERF Eliminação de fatores repetidos substitui um polinômio por um polinômio livre de quadrados que contém todos os fatores irredutíveis do polinômio original.

DDF Fatoração em graus distintos fatora um polinômio livre de quadrados no produto de polinômios contendo todos os fatores de grau 1, grau 2, etc.

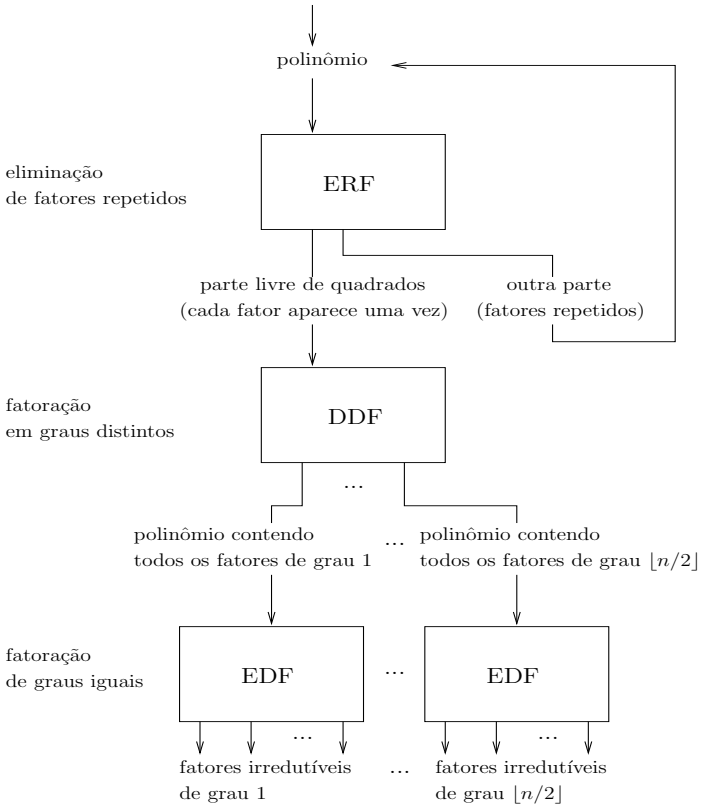
EDF Fatoração de graus iguais fatora um polinômio de tal maneira que todos os seus fatores irredutíveis tenham o mesmo grau.

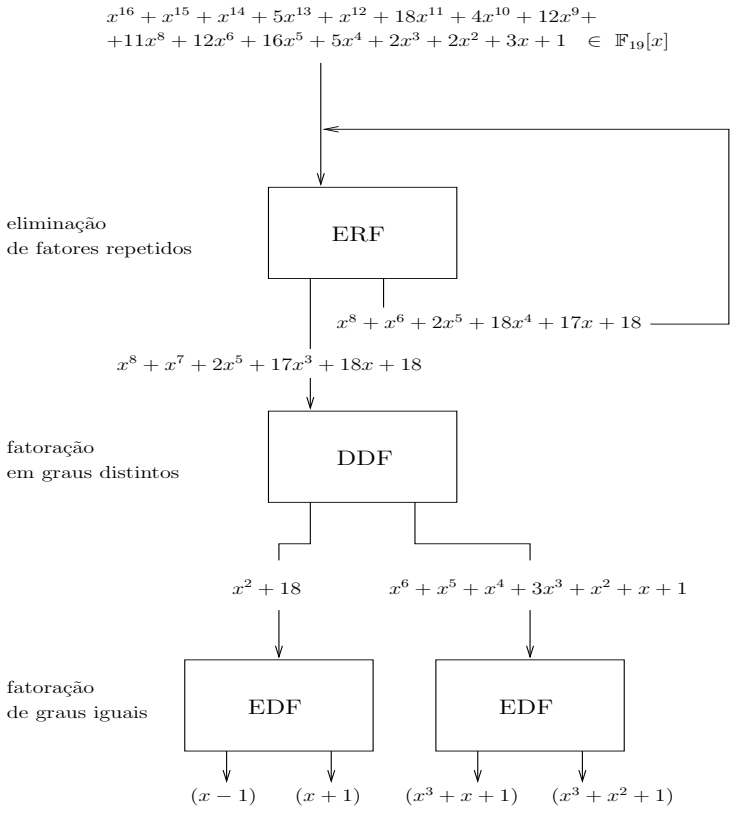
Factor (f)

Entrada: Polinômio mônico $f \in \mathbb{F}_q[x]$ de grau n.

Saída: Polinômios irredutíveis f_i e inteiros e_i, $1 \leq j \leq r$, tais que $f = f_1^{e_1} \cdots f_r^{e_r}$.

```
se f = 1 retorne 1;
a := ERF(f);
b := DDF(a);
F := 1;
para k := 1 ate n faca
      F := F· EDF(b[k], k);
c := Factor(f/a);
retorne F · c;
```


polinômio
eliminação
de fatores repetidos
ERF
parte livre de quadrados
(cada fator aparece uma vez)
outra parte
(fatores repetidos)
fatoração
em graus distintos
DDF
...
polinômio contendo
todos os fatores de grau 1
...
polinômio contendo
todos os fatores de grau $\lfloor n/2 \rfloor$
fatoração
de graus iguais
EDF
...
EDF
fatores irredutíveis
de grau 1
...
fatores irredutíveis
de grau $\lfloor n/2 \rfloor$


$x^{16} + x^{15} + x^{14} + 5x^{13} + x^{12} + 18x^{11} + 4x^{10} + 12x^9 +$
$+11x^8 + 12x^6 + 16x^5 + 5x^4 + 2x^3 + 2x^2 + 3x + 1 \quad \in \quad \mathbb{F}_{19}[x]$
eliminação
de fatores repetidos
ERF
$x^8 + x^6 + 2x^5 + 18x^4 + 17x + 18$
$x^8 + x^7 + 2x^5 + 17x^3 + 18x + 18$
fatoração
em graus distintos
DDF
$x^2 + 18$
$x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1$
fatoração
de graus iguais
EDF
EDF
$(x - 1)$
$(x + 1)$
$(x^3 + x + 1)$
$(x^3 + x^2 + 1)$

Eliminação de fatores repetidos (ERF)

O primeiro passo no processo de fatoração de um polinômio é a *eliminação de fatores repetidos* (ERF).

Idéia: usar o mdc entre o polinômio f e a sua derivada f'.

Exemplo: consideremos o polinômio $f = AB^3$, onde A é o produto dos fatores irredutíveis de f que aparecem somente uma vez e B é o produto dos fatores irredutíveis de f que aparecem três vezes. Temos que

$$f' = A'B^3 + 3AB^2B' = B^2(A'B + 3AB'),$$

e assim, $\mathrm{mdc}(f, f') = B^2$. Então, o polinômio $f/\mathrm{mdc}(f, f') = AB$ não contém fatores repetidos.

Em corpos finitos, onde a característica é diferente de zero, deve-se ter cuidado. Se $p = \mathrm{car}(\mathbb{F}_q)$ e $f = \sum_{i=0}^{n/p} f_{ip}x^{ip}$, temos que

$$f' = \sum_{i=1}^{n/p} ipf_{ip}x^{ip-1} = 0,$$

e, assim, $f/\mathrm{mdc}(f, f') = 1$. No entanto, o polinômio f contém fatores repetidos, pois

$$f = \left(\sum_{i=0}^{n/p} f_{ip}^{q/p} x^i \right)^p.$$

De qualquer forma, o ERF envolve essencialmente o mdc entre o polinômio f e sua derivada f'. O seu custo é negligível quando comparado com os outros passos do algoritmo.

Algoritmo ERF

ERF (f)
Entrada: $f \in \mathbb{F}_q[x]$ mônico de grau n.
Saída: a parte de f livre de quadrados.

$g := \mathrm{mdc}(f, f')$; $h := f/g$; $k := \mathrm{mdc}(g, h)$;
enquanto $k \neq 1$ faca
$g := g/k$; $k := \mathrm{mdc}(g, h)$
se $g \neq 1$, entao $h := h * \mathtt{ERF}(g^{1/p})$;
retorne h;

Exemplos: ERF

Exemplo

1. $p \neq 3$: *se* $f = AB^3$, *então* $f' = A'B^3 + 3AB^2B' = B^2(A'B + 3AB')$, $g = \mathrm{mdc}(f, f') = B^2$, $h = f/g = AB$ *e* $k = \mathrm{mdc}(g, h) = B$. *Então,* $k \neq 1$, $g = g/k = B$ *e* $k = B$. *Finalmente,* $g = g/k = 1$ *e* $k = 1$, *retornando* $h = AB$.

2. $p = 3$: *se* $f = (AB)^3$, *então* $f' = 3(AB)^2(AB)' = 0$, $g = \mathrm{mdc}(f, f') = (f, 0) = f$, $h = f/g = 1$ *e* $k = \mathrm{mdc}(g, h) = 1$. *Então, como* $g \neq 1$, $h = ERF(g^{1/p}) = ERF(((AB)^3)^{1/3}) = ERF(AB)$.

Fatoração em graus distintos (DDF)

Teorema. O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

DDF (a)
Entrada: um polinômio $a \in \mathbb{F}_q[x]$ de grau n, livre de quadrados.
Saída: polinômios $(b[1], b[2], \ldots, b[n])$ tais que cada $b[j]$ é o produto de todos os fatores irredutíveis de a de grau j.

```
g := a; h := x;
para k := 1 ate n faca {
      h := h^q mod g; b[k] := mdc(h − x, g);
      g := g/b[k]; [a sem fatores de grau ≤ k]
      se b[k] ≠ 1, entao h := h mod g; }
retorne (b[1], b[2], ..., b[n]);
```


Fatoração em graus distintos (DDF)

Teorema. O produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.

DDF (a)
Entrada: um polinômio $a \in \mathbb{F}_q[x]$ de grau n, livre de quadrados.
Saída: polinômios $(b[1], b[2], \ldots, b[n])$ tais que cada $b[j]$ é o produto de todos os fatores irredutíveis de a de grau j.

```
g := a; h := x;
para k := 1 ate n faca {
      h := h^q mod g; b[k] := mdc(h − x, g);
      g := g/b[k]; [a sem fatores de grau ≤ k]
      se b[k] ≠ 1, entao h := h mod g; }
retorne (b[1], b[2], ..., b[n]);
```

É claro que não é necessario o "para" até n e podemos parar ao chegar a $n/2$:

$h_0 \leftarrow x$; $f_0 \leftarrow f$;
para $i = 1$ até $\lfloor n/2 \rfloor$ faça {
    calcule $h_i \equiv h_{i-1}^q \pmod f$ em $\mathbb{F}_q[x]$;
    calcule $g_i = \mathrm{mdc}(h_i - x, f_{i-1})$ em $\mathbb{F}_q[x]$;
    $f_i = f_{i-1}/g_i$; }
para $i = \lfloor n/2 \rfloor + 1$ até n faça $g_i \leftarrow 1$;
$k \leftarrow \mathrm{grau}(f_{\lfloor n/2 \rfloor})$;
se $k > \lfloor n/2 \rfloor$ então $g_k \leftarrow f_{\lfloor n/2 \rfloor}$;
retorne $(g_1, g_2, \ldots, g_n)$.

Exemplos: DDF

Exemplo

1. *Seja* $f(x) = x^{15} - 1 \in \mathbb{F}_{11}[x]$. *Temos que*

$$\mathrm{mdc}(x^{15} - 1, x^{11} - x) = x^5 - 1 \quad \text{e}$$

$$\mathrm{mdc}(x^{11^2} - 1, x^{10} + x^5 + 1) = x^{10} + x^5 + 1.$$

A DDF é $(x^5 - 1, x^{10} + x^5 + 1, 1, \ldots, 1)$ *e, assim, há* 5 *fatores irredutíveis lineares cujo produto é* $x^5 - 1$ *e há* 5 *fatores irredutíveis quadráticos cujo produto é* $x^{10} + x^5 + 1$.

No algoritmo DDF apresentado, o "loop" principal pára quando $i = \lfloor n/2 \rfloor$. De fato, poderíamos parar antes de $\lfloor n/2 \rfloor$ usando a estratégia de abortar antes.

Exemplo

Seja f um polinômio de grau 28 formado pelo produto de 20 fatores lineares e um fator de grau 8. A execução de DDF(f) dá:

$i = 1$: g_1 tem grau 20 (20 fatores lineares) e f_1 tem grau 8;
$i = 2$: f_2 tem grau 8;
$i = 3$: f_3 tem grau 8;
$i = 4$: f_4 tem grau 8;
$i = 5$: e como $5 > 8/2$, pára com um fator irredutível de grau 8.

Este exemplo mostra que não precisamos considerar todos os graus até $\lfloor n/2 \rfloor$ (14 no último exemplo), mas até o grau dos fatores restantes divididos por 2. Isto acelera consideravelmente os cálculos sem nenhum custo extra.

O gargalo da execução do algoritmo de fatoração é o DDF e muitas variantes têm sido apresentadas.

A fatoração em graus distintos fornece um método para decompor f em polinômios contendo todos os fatores de grau 1, grau 2, etc. Se todos os fatores de f têm graus distintos, então temos a fatoração completa de f.

Para um polinômio escolhido aleatoriamente de maneira uniforme, isso acontece mais da metade das vezes! De fato, em $\mathbb{F}_2[x]$, a probabilidade é 0.6656 e, num corpo finito muito grande, a probabilidade cai para $e^{-\gamma} = 0.5614\ldots$. Para mais informação ver The complete analysis of a polynomial factorization algorithm over finite fields, Flajolet, Gourdon e Panario, Journal of Algorithms, 37–81, 2001.

Outros resultados sobre polinômios aleatórios são também conhecidos; ver What do random polynomials over finite fields look like?", D. Panario, LNCS 2948, 89–108, 2004.

Fatoração de graus iguais (EDF)

O terceiro passo é a fatoração de graus iguais (EDF) que requer fatorar um polinômio b_k que tem todos os fatores irredutíveis do mesmo grau k. A referência clássica é o algoritmo probabilístico de Cantor-Zassenhaus.

Suponhamos que q seja ímpar, $r \geq 2$ e $f = f_1 \cdots f_r$, onde $\mathrm{grau}(f_i) = k$ para cada i, $1 \leq i \leq r$, e $\mathrm{grau}(f) = n = kr$.

Pelo teorema chinês dos restos, temos que

$$\mathbb{F}_q[x]/(b_k) \cong \mathbb{F}_q[x]/(f_1) \times \cdots \times \mathbb{F}_q[x]/(f_r).$$

Idéia: se $c \in \mathbb{F}_q[x]$ é tal que $c \equiv 0 \pmod{f_i}$ e $c \not\equiv 0 \pmod{f_j}$, para certos i e j distintos, então o $\mathrm{mdc}(c, f)$ decompõe f.

Para qualquer $1 \leq i \leq r$, temos

$$\mathbb{F}_q \subseteq \mathbb{F}_q[x]/(f_i) \cong \mathbb{F}_{q^k}.$$

Tomamos q ímpar e $m = (q^k - 1)/2$. Escolha aleatoriamente um elemento $h \in \mathbb{F}_q[x]/(f)$ não nulo de grau menor que $\mathrm{grau}(f)$ com $h \mapsto (h_1, \ldots, h_r)$, usando o teorema chinês dos restos. Os elementos h_i, $1 \leq i \leq r$, são independentes e uniformemente distribuídos em $\mathbb{F}_{q^k}^*$. Temos que $h_i^m = \pm 1$ com probabilidade $1/2$.

As únicas duas r-uplas que não contribuem na fatoração de f são $(0, \ldots, 0)$ e $(-2, \ldots, -2)$. Logo, o $\mathrm{mdc}(h^m - 1, f)$ não decompõe f com probabilidade $2(\frac{1}{2})^r \leq \frac{1}{2}$; isto é, o $\mathrm{mdc}(h^m - 1, f)$ fatora f com probabilidade igual a $1 - (\frac{1}{2})^r$, ou seja, pelo menos $1/2$.

Algoritmo EDF: q odd

EDF (b, k)

Entrada: q uma potência de um primo ímpar, um polinômio mônico $b_k \in \mathbb{F}_q[x]$ de grau $n = kr$ livre de quadrados com $r \geq 2$ fatores irredutíveis, cada um de grau k.

Saída: os fatores mônicos irredutíveis de b_k.

```
se deg(b_k) ≤ k, entao retorne b_k;
h := randpoly(deg(b_k) − 1);
a := h^((q^k − 1)/2) − 1 mod b_k;
d := gcd(a, b_k);
retorne EDF(d, k)·EDF(b_k/d, k);
```

EDF tem custo menor que DDF usando algoritmos probabilísticos.

EDF em característica 2

Para $q = 2^\ell$, usamos um método baseado no cálculo do traço de elementos aleatórios em $R = \mathbb{F}_q[x]/(f)$.

Escolhemos $h \in R$ aleatoriamente, e calculamos seu traço:

$$g = \sum_{i=0}^{k-1} h^{q^i}.$$

Calculando $\sum_{i=0}^{\ell-1} g^{2^i}$ leva a uma fatoração não trivial de f de maneira análoga, com probabilidades similares, como no algoritmo acima para q ímpar.

Achando raízes de um polinômio

Um problema de interesse independente e' achar as raízes de um polinômio sobre um corpo finito. Esse problema é usado em criptografia, por exemplo no método de Chor e Rivest (1984).

Na área de criptografia pós-quântica, vários ataques de canal lateral existem para os sistemas criptográficos baseados em códigos. Esses ataques tentam achar as posições dos erros que são as raízes do polinômio localizador de erros ("error locator polynomial") e assim quebrar o sistema.

Um método para achar raízes é usar a eliminação de fatores repetidos seguida por uma rodada do algoritmo de fatoração de graus distintos para grau 1, e a rodada do algoritmo de graus iguais para esses fatores de grau 1. Esse algoritmo é aleatório. Outros algoritmos existem para essa tarefa que são determinísticos, como: buscas exaustivas, usar polinômios linearizados, o algoritmo do traço de Berlekamp, o algoritmo baseado em computar resultantes sucessivas, etc.

Tempos de execução

Os tempos de execução dos algoritmos de fatoração dependem da aritmética usada e da variante considerada em cada estágio. O gargalo da execução do algoritmo é o DDF.

Nos anos 1990 apareceram variantes do método básico anterior: von zur Gathen e Shoup (1992), Shoup (1996), Kaltofen e Shoup (1998).

Kaltofen e Shoup têm um algoritmo com tempo de execução essencialmente $O(n^{1.815}(\log q)^{0.407})$ operações em $\mathbb{F}_q$. Este é o primeiro algoritmo de tempo subquadrático em n. O algoritmo usa multiplicação rápida de matrizes e sua praticidade não é clara.

Experimentos computacionais

Shoup (1995) dá uma versão prática do algoritmo anterior com tempo de execução essencialmente $O(n^{2.5} + n^{1+o(1)} \log q)$ operações em $\mathbb{F}_q$, usando um espaço de $O(n^{1.5})$ elementos em $\mathbb{F}_q$.

As variantes anteriores levaram à fatoração de um polinômio de grau um milhão (Bonorden, von zur Gathen, Gerhard, Müller e Nöcker 2000).

A seguir apresentamos dados de von zur Gathen e Gerhard (2002) para a fatoração de polinômios sobre $\mathbb{F}_2$.

n	tempo	grau de parada	padrão de fatoração
65 535	14′	4776	1^2, 1^4, 2, 33, 143, 319, 551, 2772, 61 709
65 535	19′	6602	1^3, 1, 10, 31, 590, 824, 1037, 1898, 3831, 57 310
65 535	20′	7098	1^5, 6, 10, 11, 99, 653, 2355, 3364, 5413, 53 619
65 535	24′	9082	1, 1, 3^2, 42, 71, 205, 607, 852, 2197, 3066, 3165, 7891, 47 431
65 535	27′	9610	1^2, 5, 18, 29, 56, 80, 94, 259, 643, 1476, 3294, 8328, 51 251

n	tempo	grau de parada	padrão de fatoração
131 071	$41'$	7736	1^2, 1^2, 2, 14, 20, 23, 331, 1187, 3696, 125 794
131 071	$46'$	8824	1, 1^2, 27, 164, 612, 5402, 124 863
131 071	$1^h40'$	20 526	1, 1^3, 3, 449, 483, 1274, 18 136, 110 722
131 071	$2^h04'$	27 378	1, 1^4, 14, 67, 203, 631, 3546, 3580, 3877, 3924, 10 400, 23 894, 26 057, 27 069, 27 804
131 071	$2^h18'$	29 996	1^2, 1^3, 2, 5, 8, 68, 111, 359, 1048, 1607, 12 758, 15 699, 28 780, 70 621

n	tempo	grau de parada	padrão de fatoração
262 143	$4^h14'$	23 794	1, 1, 9, 33, 41, 96, 291, 336, 795, 1860, 2906, 18 555, 237 219
262 143	$7^h43'$	47 560	1, 3, 215, 781, 16 881, 29 207, 29 819, 43 371, 45 887, 95 978
262 143	$7^h59'$	47 844	2, 56, 110, 174, 1096, 1876, 13 616, 29 823, 44 413, 170 977
262 143	$10^h40'$	65 412	1, 2^2, 3, 11, 109, 259, 416, 1170, 1519, 1937, 2488, 3125, 7247, 33 587, 62 673, 147 594
262 143	$15^h47'$	95 922	4, 7, 37, 96, 103, 177, 738, 1268, 1649, 1796, 6283, 7015, 95 459, 147 520

n	tempo	grau de parada	padrão de fatoração
524 287	$16^h15'$	42 839	1, 1^2, 20, 830, 1443, 1538, 2054, 3175, 33 369, 34 852, 447 003
524 287	$20^h17'$	53 792	1, 1^2, 15, 41, 132, 188, 1097, 4480, 7436, 14 419, 17 159, 44 788, 434 529
524 287	$43^h48'$	125 352	2, 12, 14, 14, 85, 113, 148, 296, 343, 345, 6338, 31 278, 48 200, 119 622, 317 477
524 287	$44^h06'$	126 310	3, 25, 338, 1532, 12 564, 33 055, 98 748, 122 164, 255 858
524 287	$64^h25'$	183 618	1, 1^3, 5, 52, 62, 67, 403, 561, 569, 1566, 1776, 20 384, 183 268, 315 570