

Dále se budeme zabývat tím, jak hledat f -redukující polynomy. Použijeme čínskou větu o zbytcích.

Předpokládejme, že $f = f_1 \cdots f_k$ pro navzájem různé ireducibilní polynomy $f_1, \dots, f_k$ a nechť $\deg f = n$. Zvolíme uspořádanou k -tici $(c_1, \dots, c_k)$ prvků $\mathbf{F}_q$. Podle čínské věty o zbytcích existuje právě jeden polynom $h(x) \in \mathbf{F}_q[x]$ stupně menšího než n takový, že $h(x) \equiv c_i \pmod{f_i(x)}$ pro všechna $i = 1, \dots, k$. Pak $h^q(x) \equiv c_i^q = c_i \equiv h(x) \pmod{f_i(x)}$ pro všechna $i = 1, \dots, k$, tedy $f_i(x) | h^q(x) - h(x)$ pro všechna $i = 1, \dots, k$. Protože jsou $f_1, \dots, f_k$ po dvou nesoudělné, platí $f(x) = f_1(x) \cdots f_k(x) | h^q(x) - h(x)$.

Je-li $h(x)$ libovolný polynom stupně menšího než n , pak podle Věty 7.1 platí $f(x) = \prod_{c \in \mathbf{F}_q} \text{NSD}(f(x), h(x) - c)$. Pro libovolné $i = 1, \dots, k$ platí $f_i(x) | f(x) = \prod_{c \in \mathbf{F}_q} \text{NSD}(f(x), h(x) - c)$. Protože $f_i(x)$ je ireducibilní v $\mathbf{F}_q[x]$, existuje $c_i \in \mathbf{F}_q$ takový, že $f_i(x) | \text{NSD}(f(x), h(x) - c_i)$. Tedy $f_i(x) | h(x) - c_i$ a proto $h(x) \equiv c_i \pmod{f_i(x)}$. Z jednoznačnosti existence takového polynomu $h(x)$ (t.j. stupně menšího než n a kongruentního s konstantou c_i modulo $f_i(x)$ pro $i = 1, \dots, k$), která je dána čínskou větou o zbytcích, pak plyne, že počet polynomů $h(x)$, pro které platí $h^q(x) \equiv h(x) \pmod{f(x)}$ a $\deg h < n$, je přesně q^k .

Jak tedy budeme postupovat? Předchozí odstavec a následující tvrzení nám dávají návod na algoritmus, který se nazývá Berlekampův algoritmus. Nejprve spočítáme $x^{jq} \pmod{f(x)}$ pro $j = 0, \dots, n-1$. Platí $x^{jq} \pmod{f(x)} = \sum_{i=0}^{n-1} b_{ij} x^i$, kde $b_{ij} \in \mathbf{F}_q$. Označme $B = (b_{ij})$ (čtvercová matice řádu n).

Lemma 7.2. *Polynom $h(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ je řešením rovnice $h^q(x) \equiv h(x) \pmod{f(x)}$ právě když platí*

$$B \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix},$$

$$\text{neboli } (B - I) \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0.$$

$$\text{Důkaz. Platí } B \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \text{ právě tehdy, když } a_i = \sum_{j=0}^{n-1} b_{ij} \cdot a_j$$

pro každé $i = 0, \dots, n-1$ (z násobení matic). To je právě tehdy, když $h(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} (\sum_{j=0}^{n-1} b_{ij} a_j) \cdot x^i = \sum_{j=0}^{n-1} a_j \sum_{i=0}^{n-1} b_{ij} x^i \equiv \sum_{j=0}^{n-1} a_j x^{jq} = \sum_{j=0}^{n-1} a_j^q x^{jq} = (\sum_{j=0}^{n-1} a_j x^j)^q = h^q(x) \pmod{f(x)}$ $\square$

Stačí nám pak najít nějakou bázi nulového prostoru matice $(B - I)$. Jeden prvek je $(1, 0, \dots, 0)$, tomu odpovídá $h_1(x) = 1$. Doplňme ho do báze nulového prostoru a dostaneme tak další polynomy $h_2(x), \dots, h_k(x)$.

Lemma 7.3. *Jsou-li f_1, f_2 dva různé ireducibilní faktory $f(x)$, pak existuje polynom $h_j(x)$ pro $j = 2, \dots, k$ takový, že v součinu $\prod_{c \in \mathbf{F}_q} \text{NSD}(f(x), h_j(x) - c)$ polynomy $f_1(x)$ a $f_2(x)$ dělí různé činitele.*

Důkaz. Platí, že $h_1(x) = 1$, tj. $h_1(x) \equiv 1 \pmod{f_1(x)}$ a také $h_1(x) \equiv \text{mod } f_2(x)$. Předpokládejme dále, že $h_j(x) \equiv c_{j1} \pmod{f_1(x)}$, $h_j(x) \equiv c_{j2} \pmod{f_2(x)}$ a $c_{j1} = c_{j2}$ pro každé $j = 2, \dots, k$. Pak libovolný polynom $h(x) \in \mathbf{F}_q[x]$ stupně menšího než n , pro který platí $h(x)^q \equiv h(x) \pmod{f(x)}$ lze vyjádřit jako lineární kombinaci

$$h(x) = \sum_{j=1}^k a_j h_j(x)$$

pro nějaké koeficienty $a_j \in \mathbf{F}_q$. Pak ale platí $h(x) \equiv \sum_{j=1}^k a_j c_{j1} \pmod{f_1(x)}$ a $h(x) \equiv \sum_{j=1}^k a_j c_{j2} \pmod{f_2(x)}$. Označíme-li $c = \sum_{j=1}^k a_j c_{j1} \in \mathbf{F}_q$ pak $h(x) \equiv c \pmod{f_1(x)}$ a $h(x) \equiv c \pmod{f_2(x)}$. To je ale ve sporu s tím, že podle čínské věty o zbytcích existuje polynom $h(x) \in \mathbf{F}_q[x]$ stupně menšího než n , pro který platí $h(x) \equiv 0 \pmod{f_1(x)}$, $h(x) \equiv 1 \pmod{f_2(x)}$ a $h(x)^q \equiv h(x) \pmod{f(x)}$. $\square$

Příklad. Rozložte polynom $f(x) = x^8 + x^6 + x^4 + x^3 + 1 \in \mathbf{F}_2[x]$ pomocí Berlekampova algoritmu.

Řešení:

Máme $q = 2$ a $n = \deg f = 8$. Platí $f' = 8x^7 + 6x^5 + 4x^3 + 3x^2 = x^2$ a $\text{NSD}(f, f') = 1$. Tedy $f(x)$ nemá vícenásobné činitele.

Spočteme x^{jq} pro $j = 0, \dots, n-1$.

$$\begin{aligned} x^0 &\equiv 1 \pmod{f(x)} \\ x^2 &\equiv x^2 \pmod{f(x)} \\ x^4 &\equiv x^4 \pmod{f(x)} \\ x^6 &\equiv x^6 \pmod{f(x)} \\ x^8 &\equiv x^6 + x^4 + x^3 + 1 \pmod{f(x)} \\ x^{10} &\equiv x^6 + x^4 + x^3 + 1 + x^6 + x^5 + x^2 = x^5 + x^4 + x^3 + x^2 + 1 \pmod{f(x)} \\ x^{12} &\equiv x^7 + x^6 + x^5 + x^4 + x^2 \pmod{f(x)} \\ x^{14} &\equiv x^5 + x^4 + x^3 + x + 1 \pmod{f(x)} \end{aligned}$$

Z toho dostáváme matici

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

Dále spočteme

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

$$\sim \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Báze nulového prostoru je tedy $(1, 0, 0, 0, 0, 0, 0, 0, 0), (0, 1, 1, 0, 0, 1, 1, 1, 1)$.

Tedy $h_2(x) = x + x^2 + x^5 + x^6 + x^7$. Platí $\text{NSD}(f(x), h_2(x)) = x^6 + x^5 + x^4 + x + 1$
a $\text{NSD}(f(x), h_2(x) - 1) = x^2 + x + 1$.