Berlekampův algoritmus

Konečná tělesa

5. června 2020

Obsah přednášky

Podsekce 6.1: V poslední sekci popíšme algoritmy rozkládající polynomy nad konečnými tělesy.

Obsah přednášky

Podsekce 6.1: V poslední sekci popíšme algoritmy rozkládající polynomy nad konečnými tělesy. Nejprve rozložíme polynom v součin bezčtevercových polynomů.

Obsah přednášky

Podsekce 6.1: V poslední sekci popíšme algoritmy rozkládající polynomy nad konečnými tělesy. Nejprve rozložíme polynom v součin bezčtevercových polynomů.

Podsekce 6.2: Bezčtvercové polynomy dále rozložíme pomocí Berlekampova algoritmu.

Definice

Polynom $f(x)$ nazýváme bezčtvercový, pokud není dělitelný druhou mocninou nekonstantního (ireducibilního) polynomu.

Definice

Polynom $f(x)$ nazýváme bezčtvercový, pokud není dělitelný druhou mocninou nekonstantního (ireducibilního) polynomu.

Tvrzení (6.1)

Nechť $f(x)$ a $g(x)$ jsou polynomy nad libovolným tělesem $\boldsymbol{F}$. Pro každé $k \in \mathbb{N}$ platí, že

$$f^k(x) \mid g(x) \implies f^{k-1}(x) \mid g'(x),$$

kde $g'(x)$ značí formální derivaci polynomu $g(x)$.

Definice

Polynom $f(x)$ nazýváme bezčtvercový, pokud není dělitelný druhou mocninou nekonstantního (ireducibilního) polynomu.

Tvrzení (6.1)

Nechť $f(x)$ a $g(x)$ jsou polynomy nad libovolným tělesem $\boldsymbol{F}$. Pro každé $k \in \mathbb{N}$ platí, že

$$f^k(x) \mid g(x) \implies f^{k-1}(x) \mid g'(x),$$

kde $g'(x)$ značí formální derivaci polynomu $g(x)$.

Cvičení 6.1(2,3)

Definice

Polynom $f(x)$ nazýváme bezčtvercový, pokud není dělitelný druhou mocninou nekonstantního (ireducibilního) polynomu.

Tvrzení (6.1)

Nechť $f(x)$ a $g(x)$ jsou polynomy nad libovolným tělesem $\boldsymbol{F}$. Pro každé $k \in \mathbb{N}$ platí, že

$$f^k(x) \mid g(x) \implies f^{k-1}(x) \mid g'(x),$$

kde $g'(x)$ značí formální derivaci polynomu $g(x)$.

Cvičení 6.1(2,3)

(2) Buď $f(x)$ nenulový polynom nad daným tělesem. Označme $d(x) = \mathrm{NSD}(f'(x), f(x))$. Polynom $\frac{f(x)}{d(x)}$ je bezčtvercový.

Definice

Polynom $f(x)$ nazýváme bezčtvercový, pokud není dělitelný druhou mocninou nekonstantního (ireducibilního) polynomu.

Tvrzení (6.1)

Nechť $f(x)$ a $g(x)$ jsou polynomy nad libovolným tělesem $\boldsymbol{F}$. Pro každé $k \in \mathbb{N}$ platí, že

$$f^k(x) \mid g(x) \implies f^{k-1}(x) \mid g'(x),$$

kde $g'(x)$ značí formální derivaci polynomu $g(x)$.

Cvičení 6.1(2,3)

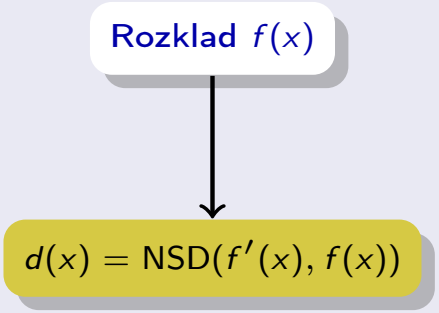
(2) Buď $f(x)$ nenulový polynom nad daným tělesem. Označme $d(x) = \mathrm{NSD}(f'(x), f(x))$. Polynom $\frac{f(x)}{d(x)}$ je bezčtvercový.

(3) Nechť $f(x)$ je nekonstantní polynom nad tělesem $\boldsymbol{F}$ kladné charakteristiky p. Je-li $f'(x) = 0$, existuje polynom $g(x) \in \boldsymbol{F}[x]$ takový, že $f(x) = g(x)^p$.

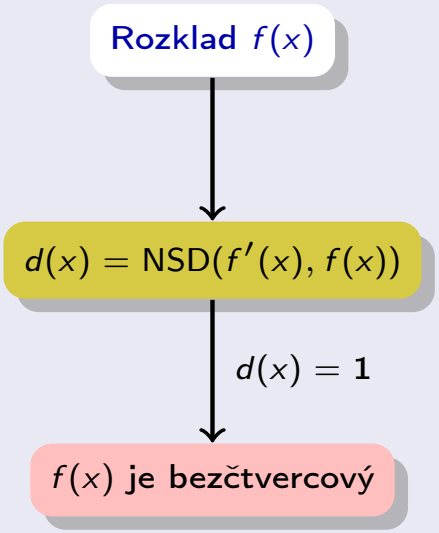
Algoritmus: - rozklad polynomu v součin bezčtvercových

Rozklad $f(x)$

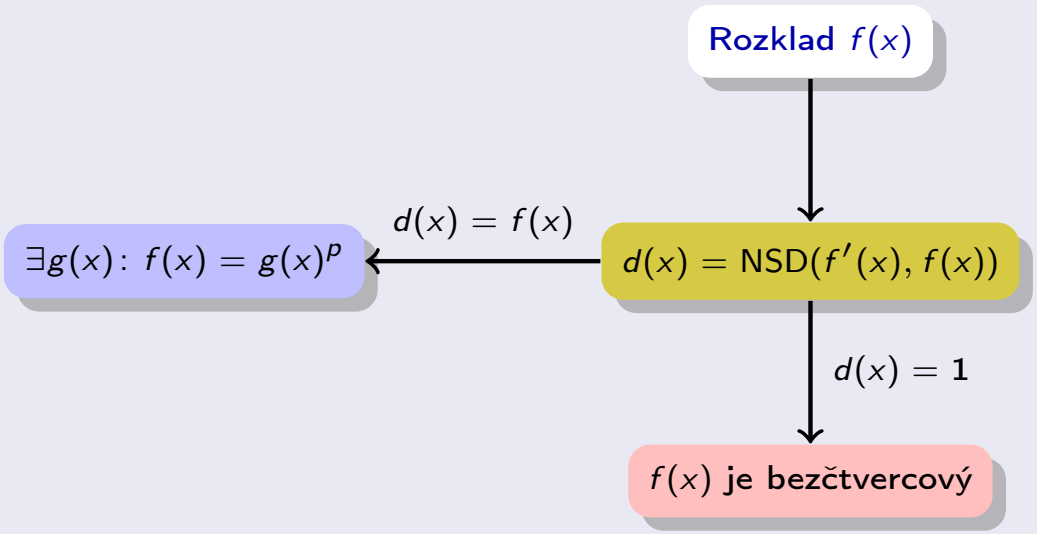
Algoritmus: - rozklad polynomu v součin bezčtvercových



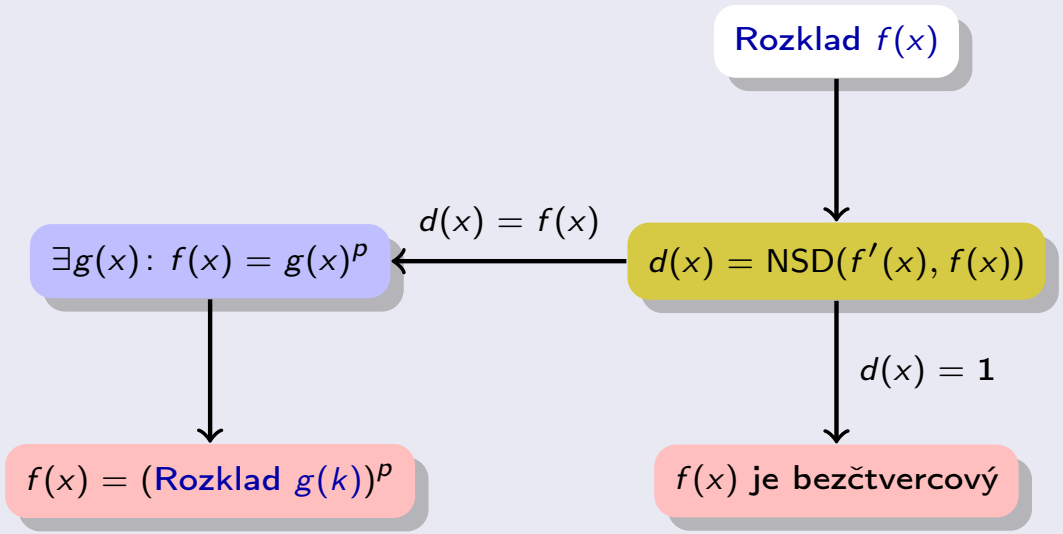
Algoritmus: - rozklad polynomu v součin bezčtvercových



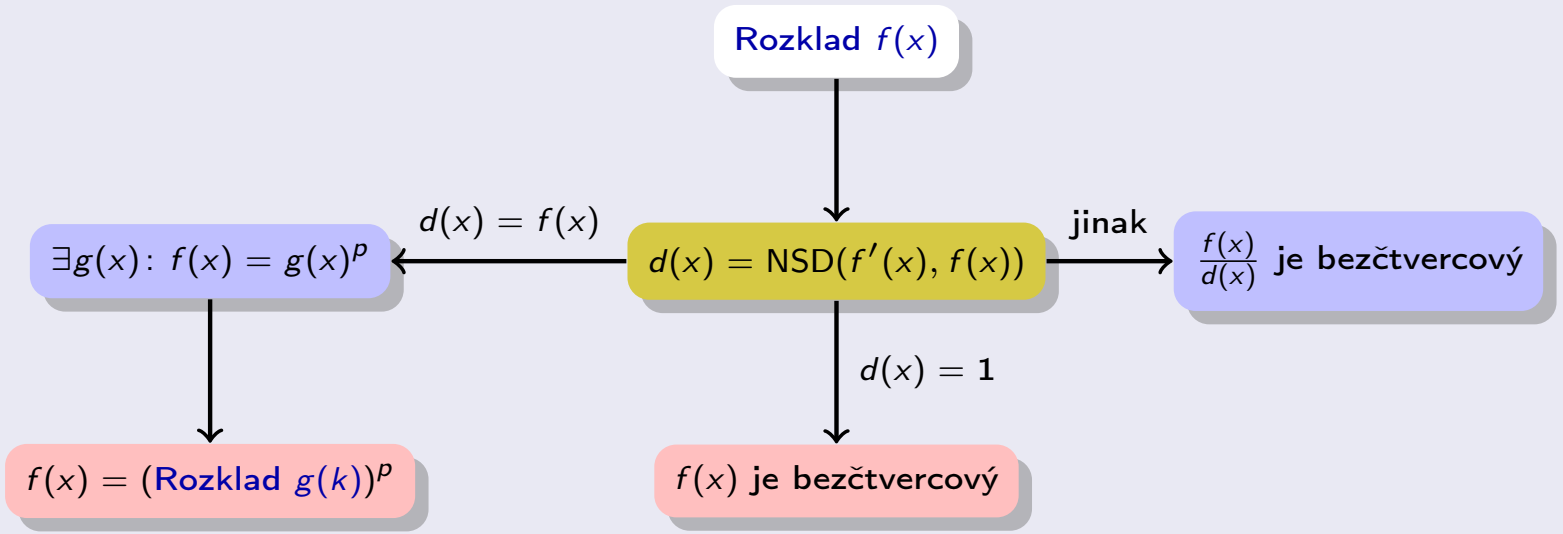
Algoritmus: - rozklad polynomu v součin bezčtvercových



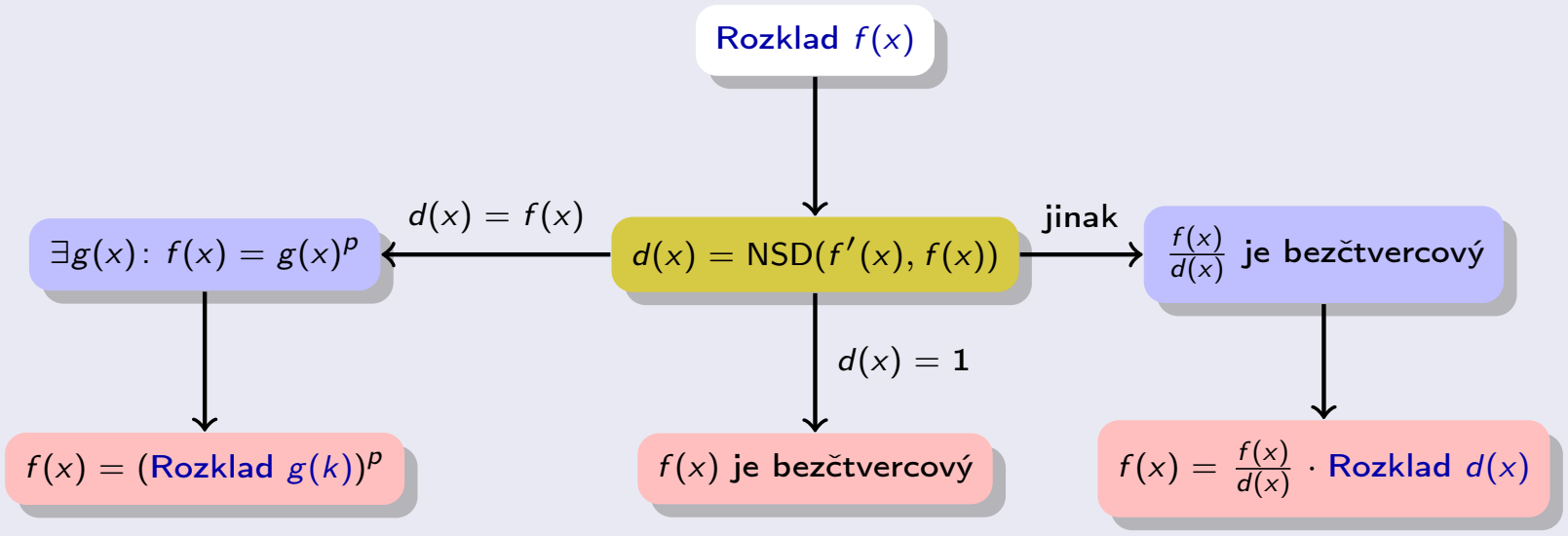
Algoritmus: - rozklad polynomu v součin bezčtvercových



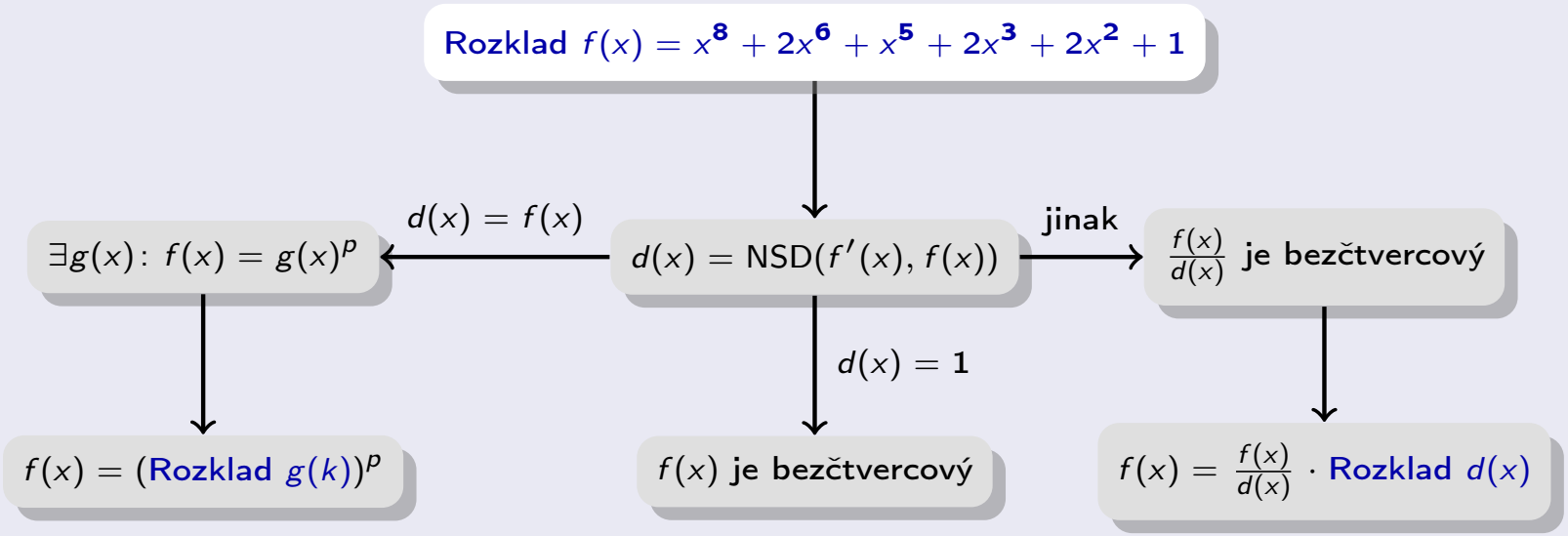
Algoritmus: - rozklad polynomu v součin bezčtvercových



Algoritmus: - rozklad polynomu v součin bezčtvercových



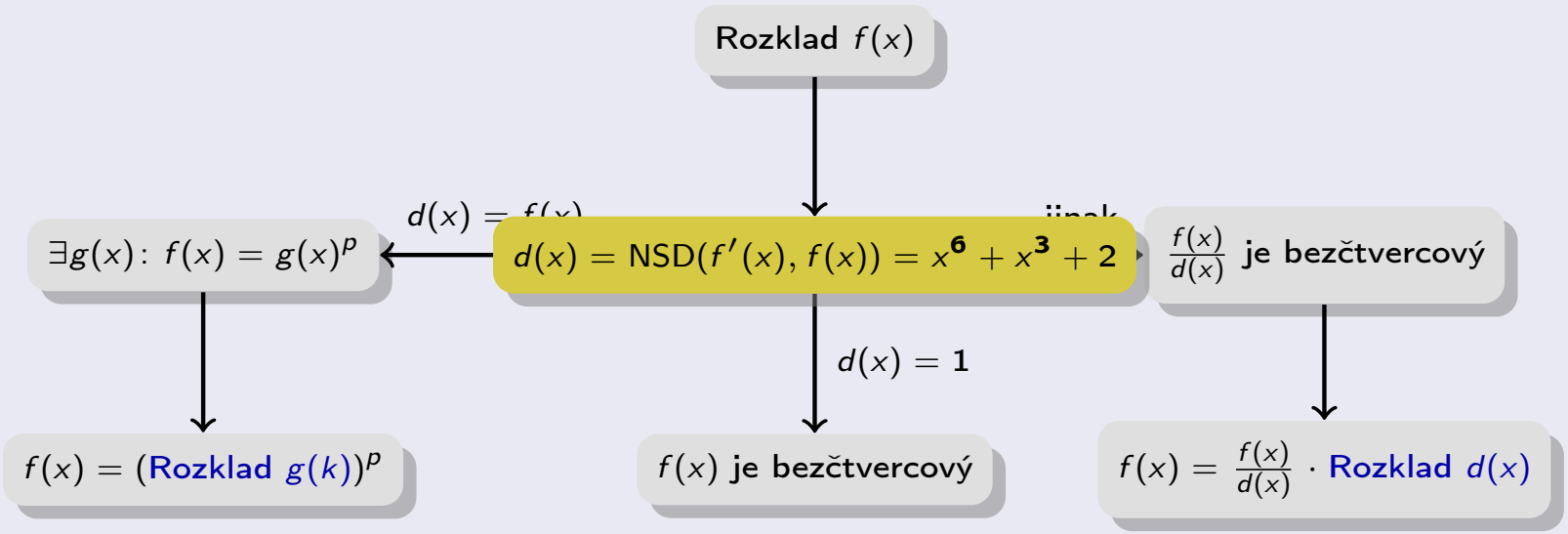
Algoritmus: - rozklad polynomu v součin bezčtvercových



Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

Algoritmus: - rozklad polynomu v součin bezčtvercových

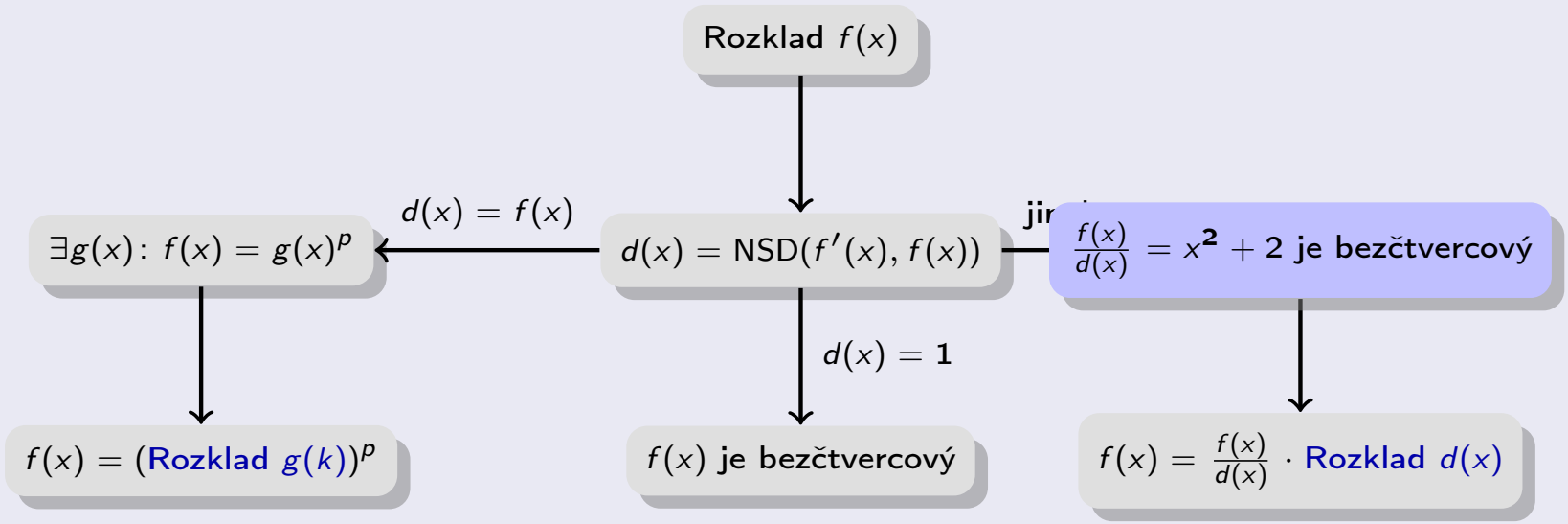


Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$f'(x) = 2x^7 + 2x^4 + x,\ d(x) = x^6 + x^3 + 2$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



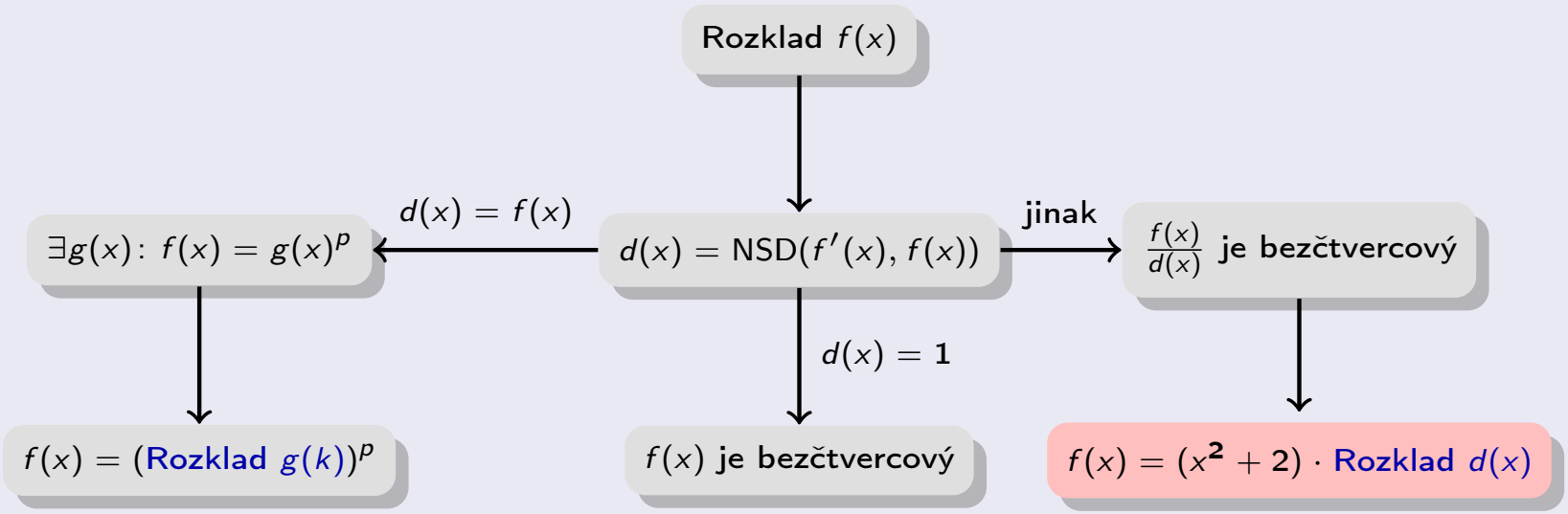
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$f'(x) = 2x^7 + 2x^4 + x,\ d(x) = x^6 + x^3 + 2$$

$$\frac{f(x)}{d(x)} = x^2 + 2$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



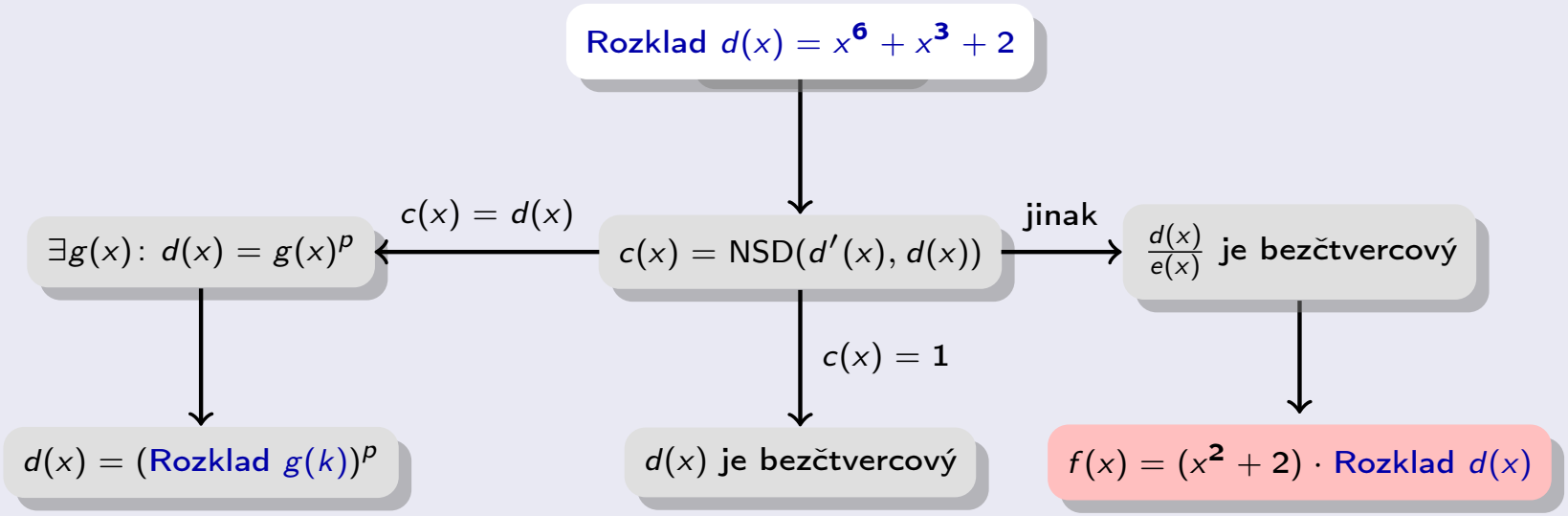
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$f'(x) = 2x^7 + 2x^4 + x,\ d(x) = x^6 + x^3 + 2$$

$$\frac{f(x)}{d(x)} = x^2 + 2$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



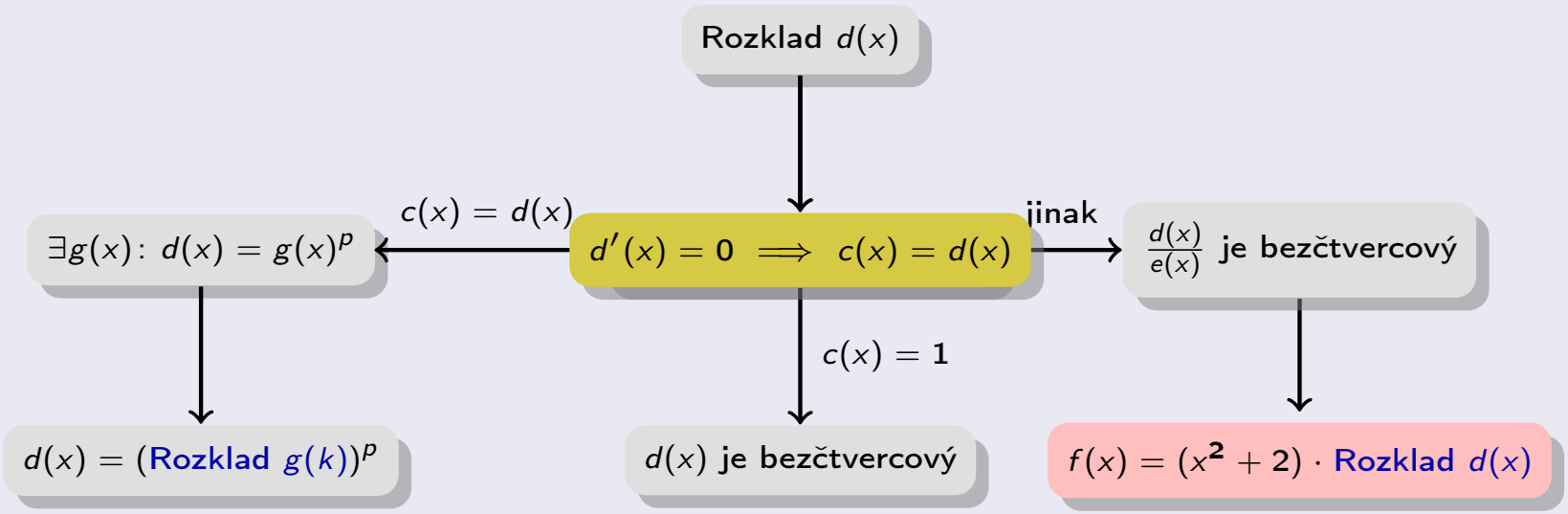
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$f'(x) = 2x^7 + 2x^4 + x,\ d(x) = x^6 + x^3 + 2$$

$$\frac{f(x)}{d(x)} = x^2 + 2$$

Algoritmus: - rozklad polynomu v součin bezčtvercových

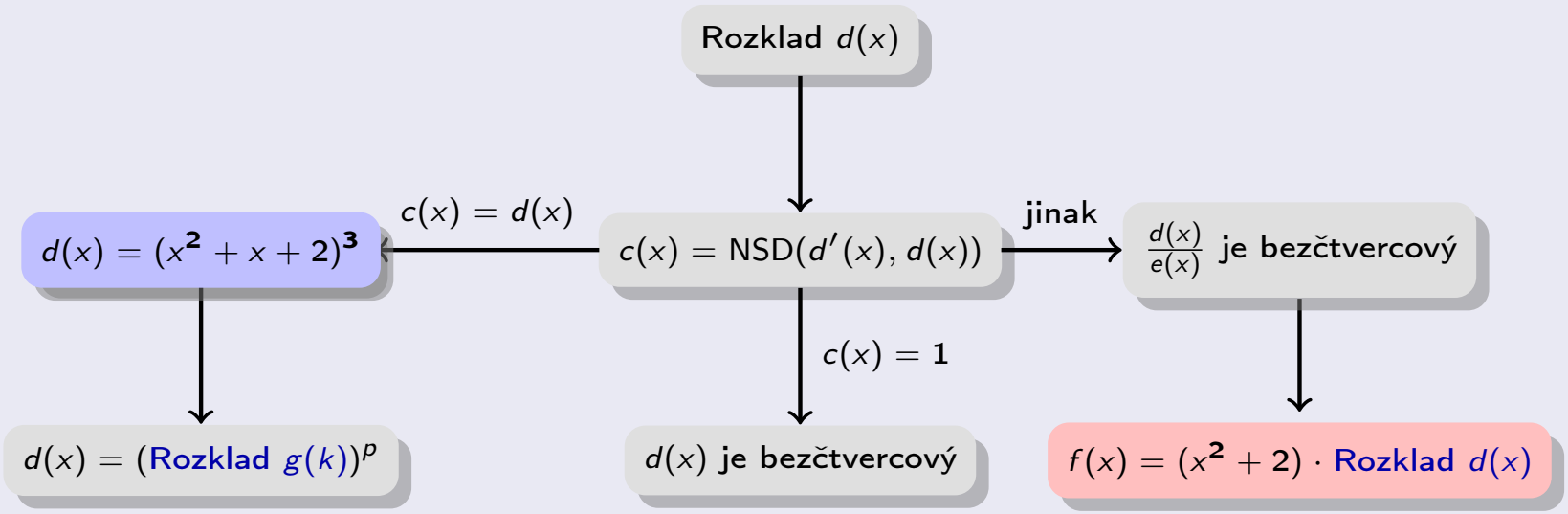


Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$d(x) = x^6 + x^3 + 2,\ d'(x) = 0,\ c(x) = d(x)$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



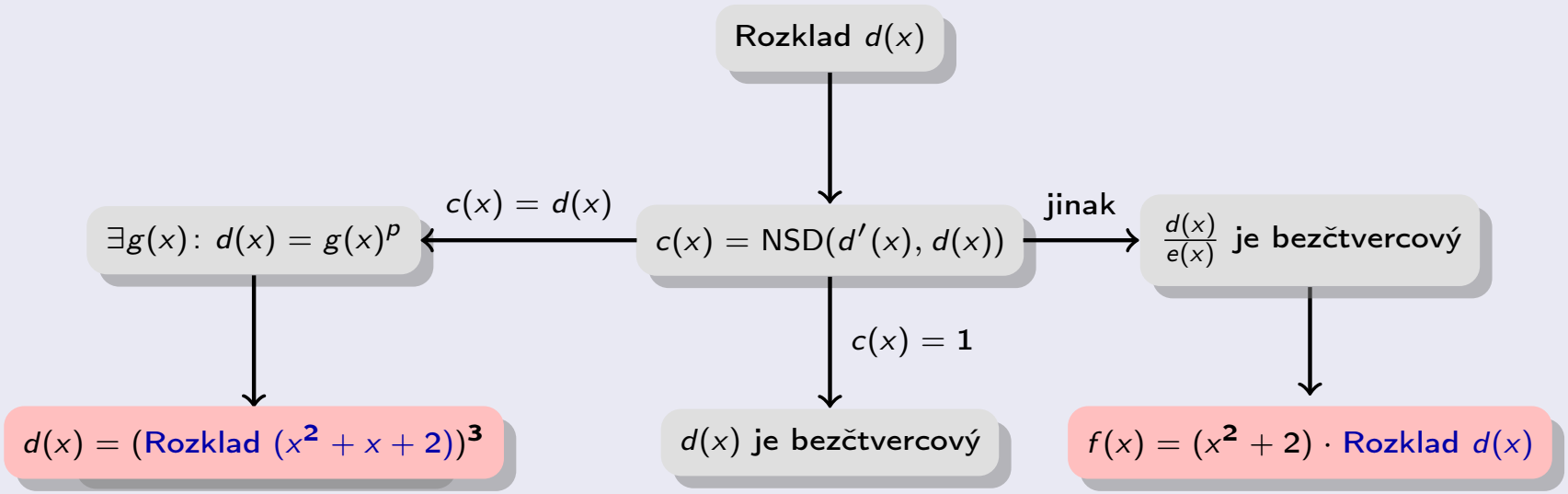
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$d(x) = x^6 + x^3 + 2,\ d'(x) = 0,\ c(x) = d(x)$$

$$d(x) = (x^2 + x + 2)^3$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



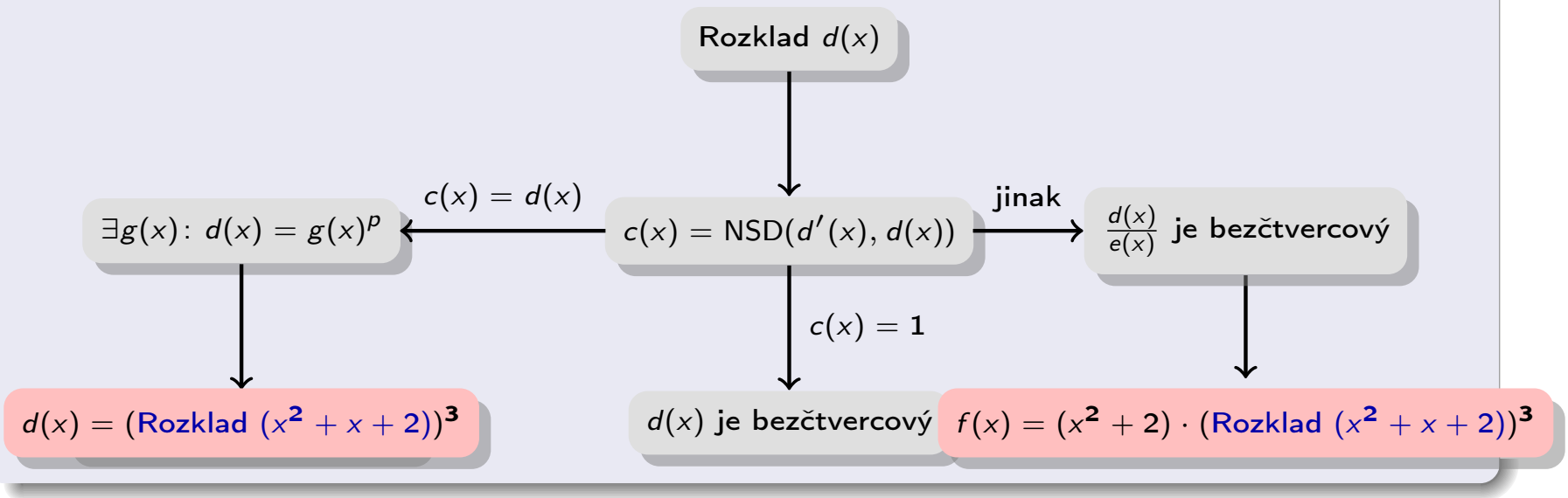
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$d(x) = x^6 + x^3 + 2,\ d'(x) = 0,\ c(x) = d(x)$$

$$d(x) = (x^2 + x + 2)^3$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



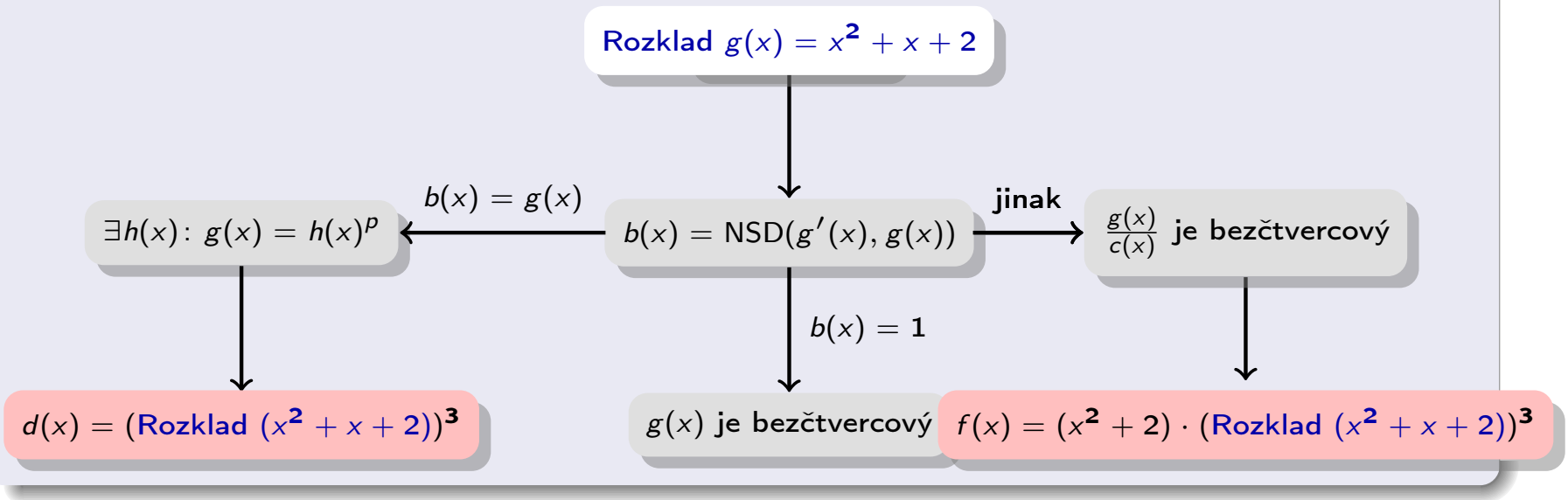
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$d(x) = x^6 + x^3 + 2,\ d'(x) = 0,\ c(x) = d(x)$$

$$d(x) = (x^2 + x + 2)^3$$

Algoritmus: - rozklad polynomu v součin bezčtvercových



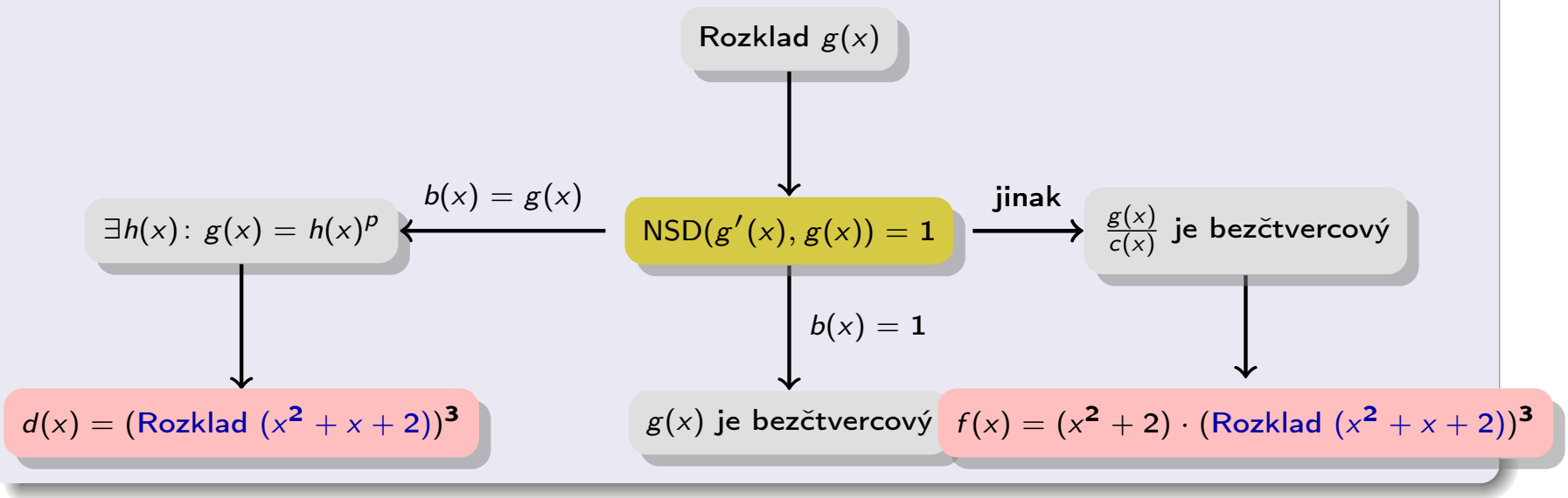
Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$$d(x) = x^6 + x^3 + 2,\ d'(x) = 0,\ c(x) = d(x)$$

$$d(x) = (x^2 + x + 2)^3$$

Algoritmus: - rozklad polynomu v součin bezčtvercových

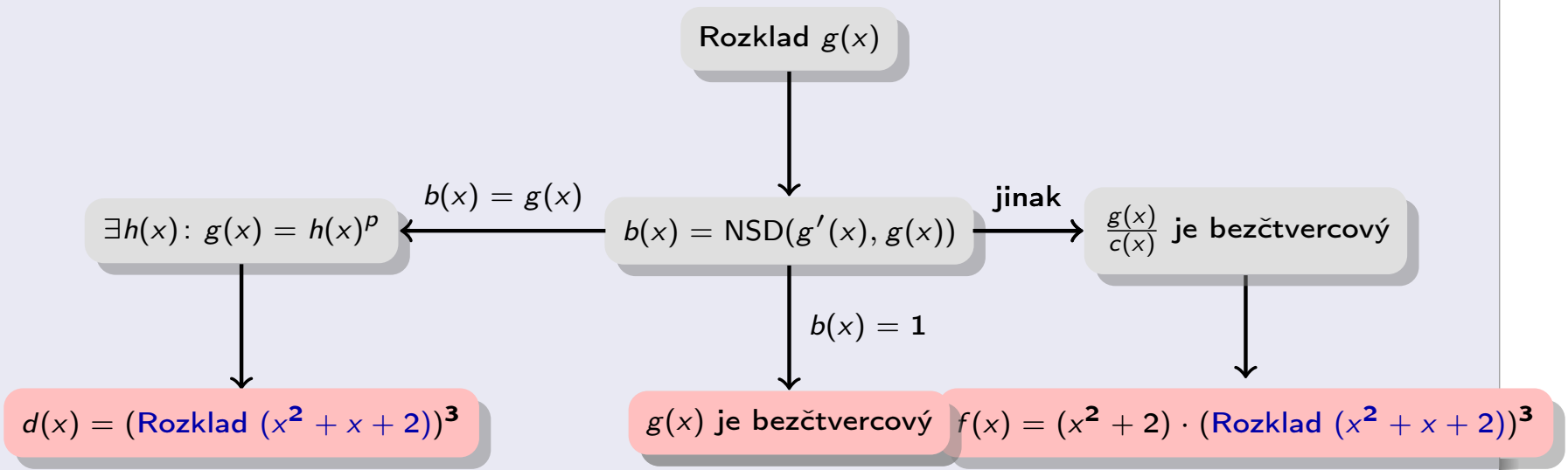


Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$g(x) = x^2 + x + 2,\ g'(x) = 2x + 1,\ \mathrm{NSD}(g'(x), g(x)) = 1$

Algoritmus: - rozklad polynomu v součin bezčtvercových

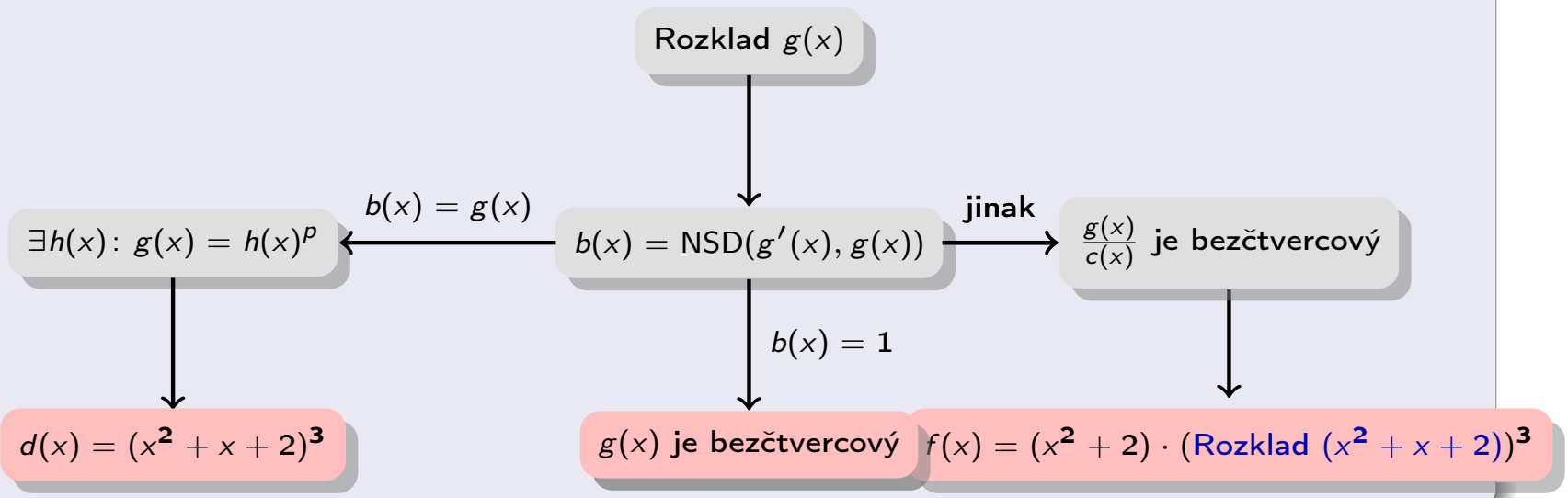


Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$g(x) = x^2 + x + 2,\ g'(x) = 2x + 1,\ \mathrm{NSD}(g'(x), g(x)) = 1$

Algoritmus: - rozklad polynomu v součin bezčtvercových

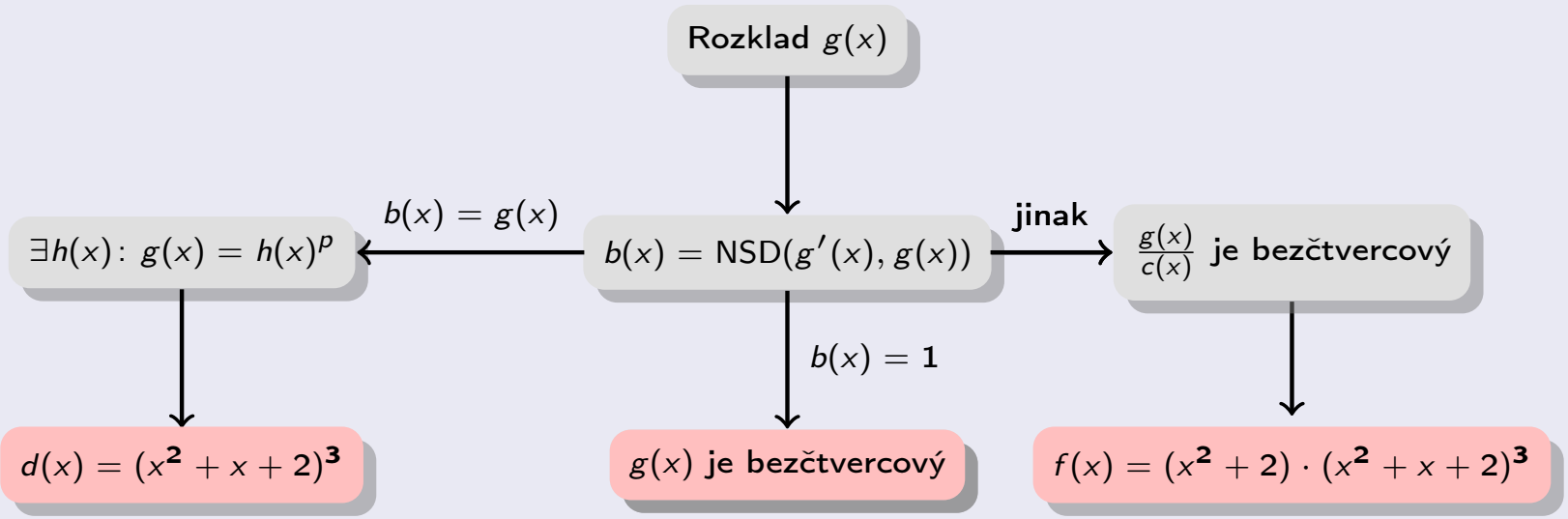


Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

$g(x) = x^2 + x + 2,\ g'(x) = 2x + 1,\ \mathrm{NSD}(g'(x), g(x)) = 1$

Algoritmus: - rozklad polynomu v součin bezčtvercových



Příklad

Vstup: $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$

Výstup: $f(x) = (x^2 + 2)(x^2 + x + 2)^3$

Tvrzení (6.2)

Nechť $f(x)$ je bezčtvercový polynom nad tělesem $\mathbb{F}_q$. Pro každý polynom $h(x) \in \mathbb{F}_q[x]$ splňující $h^q(x) \equiv h(x) \pmod{f(x)}$ platí, že

$$f(x) = \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a). \tag{6.1}$$

Tvrzení (6.2)

Nechť $f(x)$ je bezčtvercový polynom nad tělesem $\mathbb{F}_q$. Pro každý polynom $h(x) \in \mathbb{F}_q[x]$ splňující $h^q(x) \equiv h(x) \pmod{f(x)}$ platí, že

$$f(x) = \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a). \tag{6.1}$$

Poznámka

Je-li $0 < \deg h(x) < \deg f(x)$, pak rovnost (6.2) dává netriviální rozklad polynomu $f(x)$.

Důkaz.

□

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

$\mathrm{NSD}(h(x) - a, h(x) - b) = \mathrm{NSD}(h(x) - a, a - b) = 1$

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

Pro $a \neq b$ jsou $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - b)$ nesoudělné.

Jejich společný dělitel by byl i společným dělitelem $h(x) - a$ a $h(x) - b$

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

Pro $a \neq b$ jsou $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - b)$ nesoudělné.

Proto $\prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a) \mid f(x)$

$\mathbb{F}_q[x]$ je Gaussův obor. Nad Gausovým oborem platí, pro po dvou nesodělné $a_1, a_2, \ldots, a_n$ a b takové, že $a_i \mid b$ pro všechna $i \leq n$, vztah $\prod_{i=1}^{n} a_i \mid b$

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

Pro $a \neq b$ jsou $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - b)$ nesoudělné.

Proto $\prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a) \mid f(x)$

Naopak: Platí, že $h(x)^q - h(x) = \prod_{a \in \mathbb{F}_q} (h(x) - a)$

V konečném tělese $y^q - y = \prod_{a \in \mathbb{F}_q} (y - a)$. Dosadíme $h(x) \mapsto y$

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

Pro $a \neq b$ jsou $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - b)$ nesoudělné.

Proto $\prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a) \mid f(x)$

Naopak: Platí, že $h(x)^q - h(x) = \prod_{a \in \mathbb{F}_q} (h(x) - a)$

Proto $f(x) \mid \prod_{a \in \mathbb{F}_q} (h(x) - a)$

Použijem předpoklad $h(x)^q \equiv h(x) \pmod{f(x)}$

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

Pro $a \neq b$ jsou $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - b)$ nesoudělné.

Proto $\prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a) \mid f(x)$

Naopak: Platí, že $h(x)^q - h(x) = \prod_{a \in \mathbb{F}_q} (h(x) - a)$

Proto $f(x) \mid \prod_{a \in \mathbb{F}_q} (h(x) - a)$

Odtud $f(x) = \mathrm{NSD}(f(x), \prod_{a \in \mathbb{F}_q} (h(x) - a) = \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a)$.

Nad Gaussovým oborem platí: jsou-li $b_1, b_2, \ldots, b_n$ po dvou nesoudělné, je

$$\mathrm{NSD}(a, \prod_{i=1}^{n} b_i) = \prod_{i=1}^{n} \mathrm{NSD}(a, b_i)$$

Důkaz.

Pro $a \neq b$ jsou polynomy $h(x) - a$ a $h(x) - b$ nesoudělné.

Pro $a \neq b$ jsou $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - b)$ nesoudělné.

Proto $\prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a) \mid f(x)$

Naopak: Platí, že $h(x)^q - h(x) = \prod_{a \in \mathbb{F}_q} (h(x) - a)$

Proto $f(x) \mid \prod_{a \in \mathbb{F}_q} (h(x) - a)$

Odtud $f(x) = \mathrm{NSD}(f(x), \prod_{a \in \mathbb{F}_q} (h(x) - a) = \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a)$.

Proto $f(x) \mid \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h(x) - a)$

Tvrzení (6.3)

Nechť $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ *je rozklad polynomu* $f(x) \in \mathbb{F}_q[x]$ *na ireducibilní faktory. Označme* W *množinu všech polynomů* $h(x) \in \mathbb{F}_q[x]$ *takových, že*

$$\deg h(x) < \deg f(x) \text{ a zároveň } \quad h(x)^q \equiv h(x) \pmod{f(x)}.$$

Množina W *je vektorovým prostorem nad* $\mathbb{F}_q$ *a platí*

Tvrzení (6.3)

Nechť $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ *je rozklad polynomu* $f(x) \in \mathbb{F}_q[x]$ *na ireducibilní faktory. Označme* W *množinu všech polynomů* $h(x) \in \mathbb{F}_q[x]$ *takových, že*

$$\deg h(x) < \deg f(x) \text{ a zároveň } \quad h(x)^q \equiv h(x) \pmod{f(x)}.$$

Množina W *je vektorovým prostorem nad* $\mathbb{F}_q$ *a platí*

- *pro každé* $h(x) \in W$ *a každý ireducibilní faktor* $f_i(x)$ *polynomu* $f(x)$ *je*

$$h(x) \bmod f_i(x) \in \mathbb{F}_q;$$

Tvrzení (6.3)

Nechť $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ *je rozklad polynomu* $f(x) \in \mathbb{F}_q[x]$ *na ireducibilní faktory. Označme* W *množinu všech polynomů* $h(x) \in \mathbb{F}_q[x]$ *takových, že*

$$\deg h(x) < \deg f(x) \text{ a zároveň } \quad h(x)^q \equiv h(x) \pmod{f(x)}.$$

Množina W *je vektorovým prostorem nad* $\mathbb{F}_q$ *a platí*

- *pro každé* $h(x) \in W$ *a každý ireducibilní faktor* $f_i(x)$ *polynomu* $f(x)$ *je*

$$h(x) \bmod f_i(x) \in \mathbb{F}_q;$$

- *Zobrazení* $\phi\colon W \to \mathbb{F}_q^n$ *dané předpisem*

$$h(x) \mapsto (h(x) \bmod f_1(x), h(x) \bmod f_2(x), \ldots, h(x) \bmod f_n(x))$$

je izomorfismem vektorových prostorů.

Důkaz.

□

Důkaz.

Snadno ověříme, že je množina W uzavřena na sčítání a násobení prvky tělesa $\mathbb{F}_q$.

□

Pro uzavřenost na sčítání využijeme vztahu $h_1(x)^q + h_2(x)^q = (h_1 + h_2)(x)^q$.

Důkaz.

Snadno ověříme, že je množina W uzavřena na sčítání a násobení prvky tělesa $\mathbb{F}_q$.

Proto je W vektorovým prostorem nad tělesem $\mathbb{F}_q$.

Pro uzavřenost na sčítání využijeme vztahu $h_1(x)^q + h_2(x)^q = (h_1 + h_2)(x)^q$.

Důkaz.

Snadno ověříme, že je množina W uzavřena na sčítání a násobení prvky tělesa $\mathbb{F}_q$.

Proto je W vektorovým prostorem nad tělesem $\mathbb{F}_q$.

Pro každý polynom $h(x) \in W$ a kařdé $i \leq k$ existuje právě jedno $a \in \mathbb{F}_q$ takové, že $f_i(x) \mid h(x) - a$. Proto $h(x) \bmod f_i(x) = a \in \mathbb{F}_q$.

□

Podle Tvrzení 6.2 je $f_i(x) \mid f(x)$ a $f(x) \mid \prod_{a \in \mathbb{F}_q} (h(x) - a)$.

Protože jsou polynomy $f_i(x)$ nerozložitelné a tedy prvočinitele, existuje $a \in \mathbb{F}_q$ tak, že $f_i(x) \mid h(x) - a$. Protože jsou polynomy $h(x) - a$ po dvou nesoudělné, je takové a právě jedno.

Důkaz.

Snadno ověříme, že je množina W uzavřena na sčítání a násobení prvky tělesa $\mathbb{F}_q$.

Proto je W vektorovým prostorem nad tělesem $\mathbb{F}_q$.

Pro každý polynom $h(x) \in W$ a kařdé $i \leq k$ existuje právě jedno $a \in \mathbb{F}_q$ takové, že $f_i(x) \mid h(x) - a$. Proto $h(x) \bmod f_i(x) = a \in \mathbb{F}_q$.

Podle **Čínské věty o zbytcích** existuje pro každou n-tici $a_1, a_2, \ldots, a_n$ právě jeden polynom $h(x)$ takový, že $\deg h(x) < \deg f(x)$ a $h(x) \equiv a_i \pmod{f_i(x)}$ pro všechna i.

□

Čínská věta o zbytcích pro okruh $\boldsymbol{F}[x]$: Pro každé n-tice po dvou nesoudělných polynomů $f_1(x), f_2(x), \ldots f_n(x)$ a polynomů $g_1(x), g_2(x), \ldots, g_n(x)$ existuje právě jedno řešení $h(x)$ soustavy kongruencí $h(x) \equiv g_i(x) \pmod{f_i(x)}$, $i \leq n$ takové, že $\deg h(x) < \deg(f_1(x) \cdot f_2(x) \cdots f_n(x))$.

Důkaz.

Snadno ověříme, že je množina W uzavřena na sčítání a násobení prvky tělesa $\mathbb{F}_q$.

Proto je W vektorovým prostorem nad tělesem $\mathbb{F}_q$.

Pro každý polynom $h(x) \in W$ a kařdé $i \leq k$ existuje právě jedno $a \in \mathbb{F}_q$ takové, že $f_i(x) \mid h(x) - a$. Proto $h(x) \bmod f_i(x) = a \in \mathbb{F}_q$.

Podle **Čínské věty o zbytcích** existuje pro každou n-tici $a_1, a_2, \ldots, a_n$ právě jeden polynom $h(x)$ takový, že $\deg h(x) < \deg f(x)$ a $h(x) \equiv a_i \pmod{f_i(x)}$ pro všechna i.

Z jednoznačnosti polynomu $h(x)$ plyne, že je zobrazení Φ prosté.

□

Čínská věta o zbytcích pro okruh $\boldsymbol{F}[x]$: Pro každé n-tice po dvou nesoudělných polynomů $f_1(x), f_2(x), \ldots f_n(x)$ a polynomů $g_1(x), g_2(x), \ldots, g_n(x)$ existuje právě jedno řešení $h(x)$ soustavy kongruencí $h(x) \equiv g_i(x) \pmod{f_i(x)}$, $i \leq n$ takové, že $\deg h(x) < \deg(f_1(x) \cdot f_2(x) \cdots f_n(x))$.

Důkaz.

Pro každé $i \leq n$ je $h^q(x) \equiv a^q = a \pmod{f_i(x)}$.

Podle Lemmatu 2.6 je $a^q = a$ pro každé $a \in \mathbb{F}_q$.

Důkaz.

Pro každé $i \leq n$ je $h^q(x) \equiv a^q = a \pmod{f_i(x)}$.

Z jednoznačnosti řešení v Čínské větě zbytcích plyne, že $h^q(x) \equiv h(x) \pmod{f(x)}$.

□

Polynom $h^q(x) \bmod f(x) \equiv a_i \pmod{f_i(x)}$ pro všechna $i \leq n$.

Stupeň tohoto polynomu je $< \deg f(x)$ a tedy je roven polynomu $h(x)$.

Důkaz.

Pro každé $i \leq n$ je $h^q(x) \equiv a^q = a \pmod{f_i(x)}$.

Z jednoznačnosti řešení v Čínské větě zbytcích plyne, že $h^q(x) \equiv h(x) \pmod{f(x)}$.

Proto platí, že $h(x) \in W$. Odtud plyne, že ϕ je na. □

Důkaz.

Pro každé $i \leq n$ je $h^q(x) \equiv a^q = a \pmod{f_i(x)}$.

Z jednoznačnosti řešení v Čínské větě zbytcích plyne, že $h^q(x) \equiv h(x) \pmod{f(x)}$.

Proto platí, že $h(x) \in W$. Odtud plyne, že ϕ je na.

Ukázali jsme, že $\phi\colon W \to \mathbb{F}_q^n$ je izomorfismus vektorových prostorů

Důsledek

Protože je $\phi\colon W \to \mathbb{F}_q^n$ *izomorfismus a* n *je počet ireducibilních faktorů polynomu* $f(x)$ *platí, že*

$$\dim W = \text{ počet ireducibiních faktorů polynomu } f(x).$$

Důsledek

Protože je $\phi\colon W \to \mathbb{F}_q^n$ *izomorfismus a* n *je počet ireducibilních faktorů polynomu* $f(x)$ *platí, že*

$$\dim W = \text{ počet ireducibiních faktorů polynomu } f(x).$$

Důsledek

Protože je $\phi\colon W \to \mathbb{F}_q^n$ *izomorfismus a* n *je počet ireducibilních faktorů polynomu* $f(x)$ *platí, že*

$$\dim W = \text{ počet ireducibiních faktorů polynomu } f(x).$$

Speciálně je polynom $f(x)$ *ireducibilní právě když* $\dim W = 1$.

Výpočet polynomu $h(x)$.

Výpočet polynomu $h(x)$.

Položme $k = \deg f(x)$. Hledáme polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Výpočet polynomu $h(x)$.

Položme $k = \deg f(x)$. Hledáme polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Po umocnění $h^q(x) = b_{k-1}x^{q(k-1)} + \cdots + b_1 x^q + b_0$.

Výpočet polynomu $h(x)$.

Položme $k = \deg f(x)$. Hledáme polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Po umocnění $h^q(x) = b_{k-1}x^{q(k-1)} + \cdots + b_1 x^q + b_0$.

Nechť $s_{i,j}$ jsou takové, že

$$\begin{aligned}
x^0 \bmod f(x) &= s_{k-1,0}x^{k-1} + \cdots + s_{1,0}x + s_{0,0},\\
x^q \bmod f(x) &= s_{k-1,1}x^{k-1} + \cdots + s_{1,1}x + s_{0,1},\\
&\cdots\\
x^{q(k-1)} \bmod f(x) &= s_{k-1,k-1}x^{k-1} + \cdots + s_{1,k-1}x + s_{0,k-1}.
\end{aligned}$$

Výpočet polynomu $h(x)$.

Položme $k = \deg f(x)$. Hledáme polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Po umocnění $h^q(x) = b_{k-1}x^{q(k-1)} + \cdots + b_1 x^q + b_0$.

Nechť $s_{i,j}$ jsou takové, že

$$\begin{aligned} x^0 \bmod f(x) &= s_{k-1,0}x^{k-1} + \cdots + s_{1,0}x + s_{0,0}, \\ x^q \bmod f(x) &= s_{k-1,1}x^{k-1} + \cdots + s_{1,1}x + s_{0,1}, \\ &\cdots \\ x^{q(k-1)} \bmod f(x) &= s_{k-1,k-1}x^{k-1} + \cdots + s_{1,k-1}x + s_{0,k-1}. \end{aligned}$$

Položme

$$S_f := \begin{pmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,k-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{k-1,0} & s_{k-1,1} & \cdots & s_{k-1,k-1} \end{pmatrix}$$

Výpočet polynomu $h(x)$.

Výpočet polynomu $h(x)$.

Pro polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ položme

$$\boldsymbol{v}_h := (b_0, b_1, \ldots, b_{k-1}).$$

Výpočet polynomu $h(x)$.

Pro polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ položme

$$\boldsymbol{v}_h := (b_0, b_1, \ldots, b_{k-1}).$$

Je-li $h^q(x) \bmod f(x) = c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ spočteme, že

$$\underbrace{\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{k-1} \end{pmatrix}}_{\boldsymbol{v}_{h^q \bmod f}^T} = \underbrace{\begin{pmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,k-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{k-1,0} & s_{k-1,1} & \cdots & s_{k-1,k-1} \end{pmatrix}}_{\boldsymbol{S}_f} \cdot \underbrace{\begin{pmatrix} b_0 \\ b_1 \\ \cdots \\ b_{k-1} \end{pmatrix}}_{\boldsymbol{v}_h^T} .$$

Výpočet polynomu $h(x)$.

Pro polynom $h(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ položme

$$\boldsymbol{v}_h := (b_0, b_1, \ldots, b_{k-1}).$$

Je-li $h^q(x) \bmod f(x) = c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ spočteme, že

$$\underbrace{\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{k-1} \end{pmatrix}}_{\boldsymbol{v}_{h^q \bmod f}^T} = \underbrace{\begin{pmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,k-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{k-1,0} & s_{k-1,1} & \cdots & s_{k-1,k-1} \end{pmatrix}}_{\boldsymbol{S}_f} \cdot \underbrace{\begin{pmatrix} b_0 \\ b_1 \\ \cdots \\ b_{k-1} \end{pmatrix}}_{\boldsymbol{v}_h^T} .$$

Dostáváme tak rovnost

$$\boldsymbol{v}_{h^q \bmod f}^T = \boldsymbol{S}_f \cdot \boldsymbol{v}_h^T$$

Tvrzení (6.4)

Polynom $h(x)$ stupně $< k$ leží ve W právě když

$$(\boldsymbol{S}_f - \boldsymbol{I}) \cdot \boldsymbol{v}_h = \boldsymbol{0}, \qquad (6.2)$$

kde $\boldsymbol{I}$ značí jednotkovou matici.

Tvrzení (6.4)

Polynom $h(x)$ stupně $< k$ leží ve W právě když

$$(\boldsymbol{S}_f - \boldsymbol{I}) \cdot \boldsymbol{v}_h = \boldsymbol{0}, \qquad (6.2)$$

kde $\boldsymbol{I}$ značí jednotkovou matici.

Poznámka

Všimněme si, že $x^0 \bmod f(x) = 1$ a tedy první sloupec matice $\boldsymbol{S}_f$ odpovídá vektoru $(1, 0, \ldots, 0)^T$. Proto je první sloupec matice $\boldsymbol{S}_f - \boldsymbol{I}$ nulový a vektory $(a, 0, \ldots, 0)^T$ jsou řešením rovnice (6.2). Tato řešení budeme nazývat *triviální*, zbylá řešení *netriviální*. Triviální řešení reflektují fakt, že konstantní polynomy leží vždy v množině W.

Berlekampův algoritmus

Rozkládáme bezčtvercový polynom $f(x)$

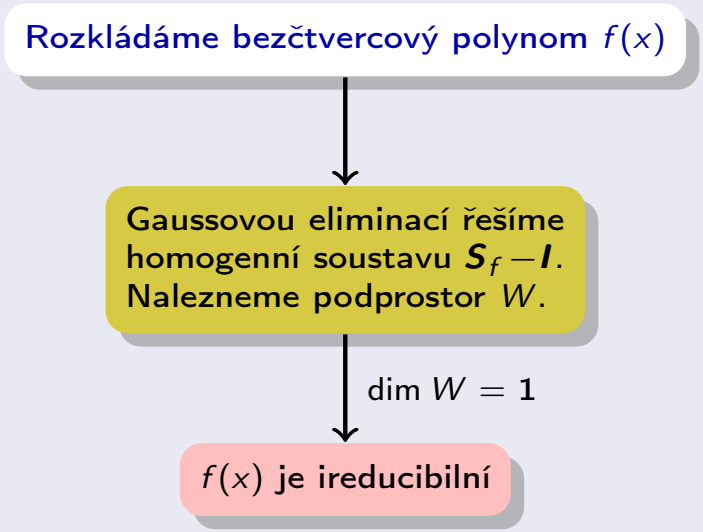
Berlekampův algoritmus

Rozkládáme bezčtvercový polynom $f(x)$

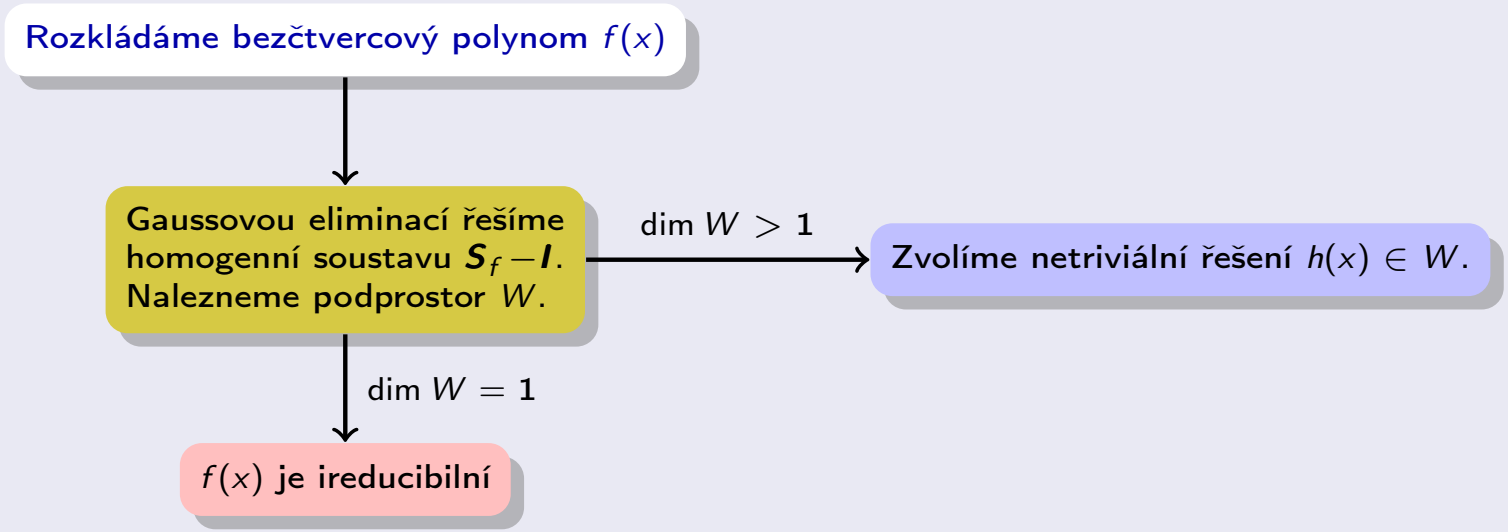
↓

Gaussovou eliminací řešíme homogenní soustavu $\boldsymbol{S}_f - \boldsymbol{I}$. Nalezneme podprostor W.

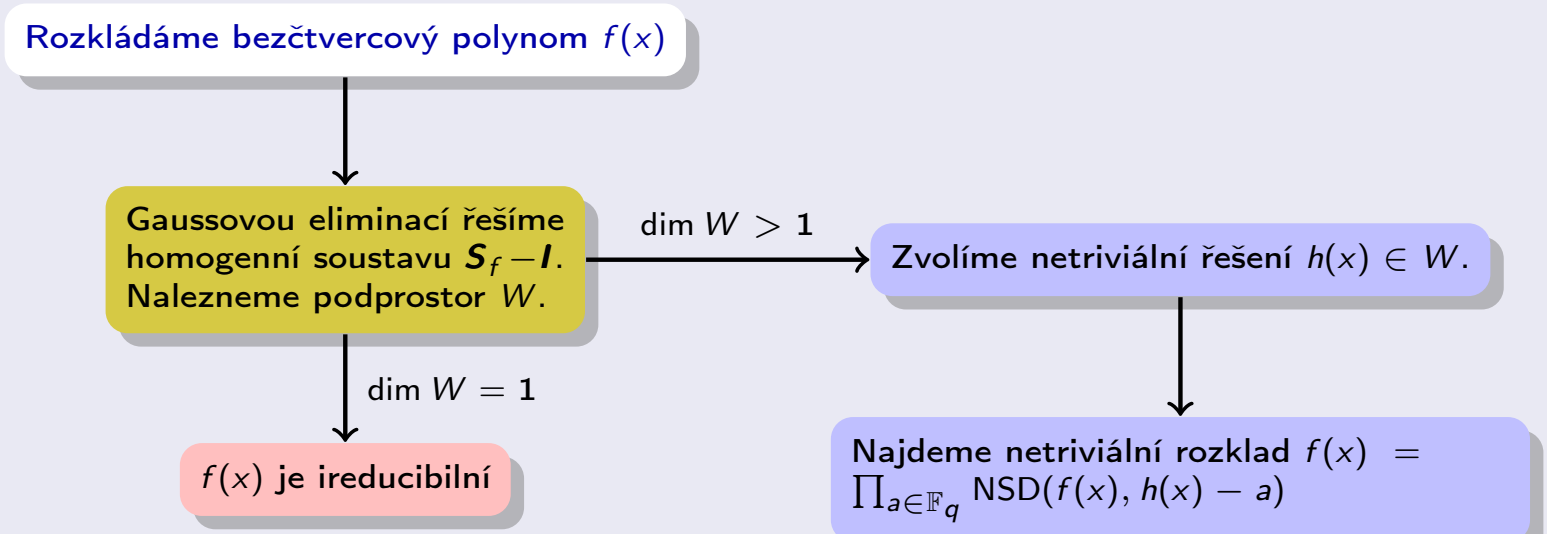
Berlekampův algoritmus



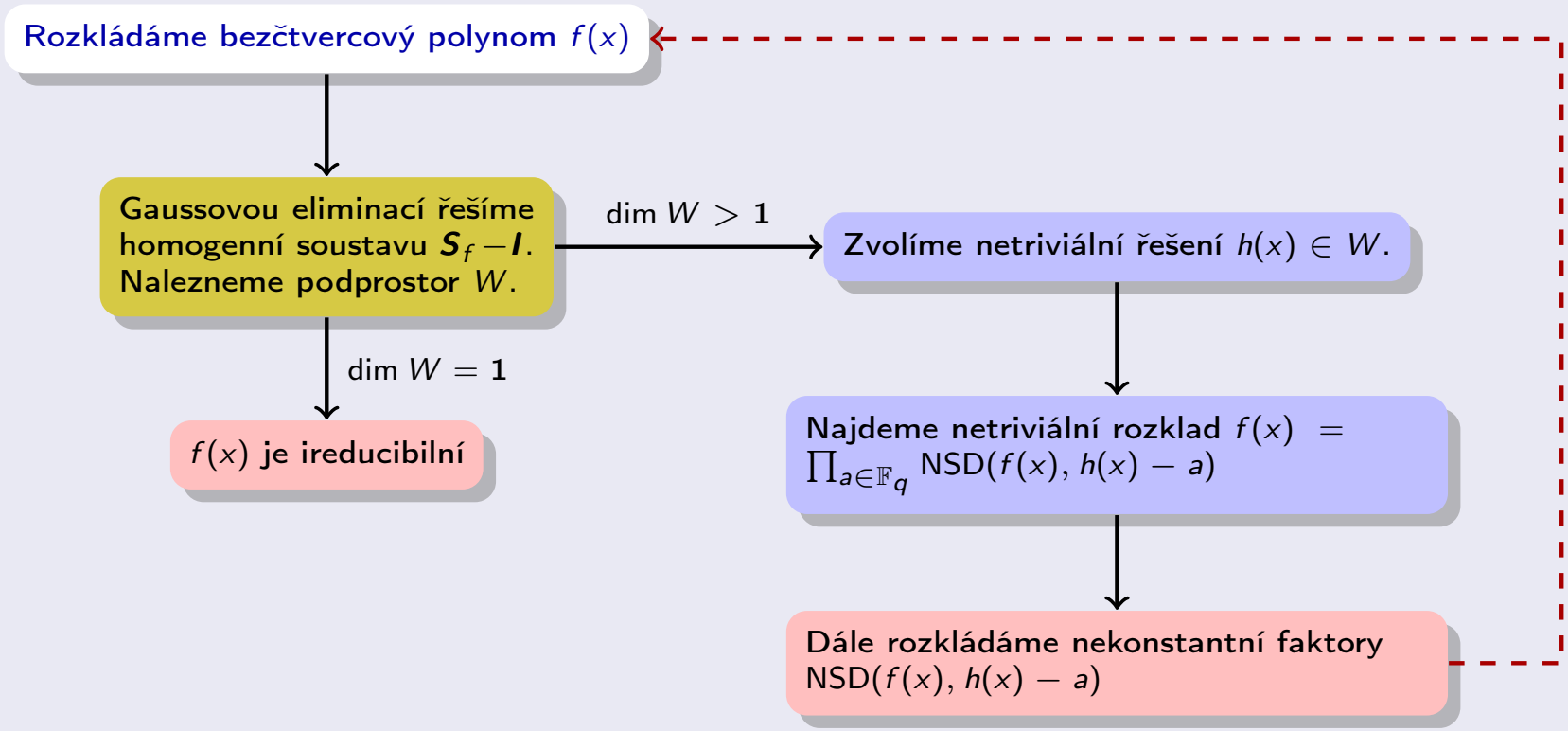
Berlekampův algoritmus



Berlekampův algoritmus



Berlekampův algoritmus



Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Spočteme $f'(x) = 4x^3$ a $\mathrm{NSD}(f'(x), f(x)) = 1$. Odtud odvodíme, že je polynom $f(x)$ bezčtvercový.

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Spočteme $f'(x) = 4x^3$ a $\mathrm{NSD}(f'(x), f(x)) = 1$. Odtud odvodíme, že je polynom $f(x)$ bezčtvercový.

Dále spočítáme, že

$$x^0 \bmod f(x) = 1,$$
$$x^3 \bmod f(x) = x^3,$$
$$x^6 \bmod f(x) = 2x^2,$$
$$x^9 \bmod f(x) = x.$$

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Spočteme $f'(x) = 4x^3$ a $\mathrm{NSD}(f'(x), f(x)) = 1$. Odtud odvodíme, že je polynom $f(x)$ bezčtvercový.

Dále spočítáme, že

$$x^0 \bmod f(x) = 1,$$
$$x^3 \bmod f(x) = x^3,$$
$$x^6 \bmod f(x) = 2x^2,$$
$$x^9 \bmod f(x) = x.$$

Odtud dostaneme, že

$$\boldsymbol{S}_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Gausovou eliminací upravíme matici $\boldsymbol{S}_f - \boldsymbol{I}$:

$$\boldsymbol{S}_f - \boldsymbol{I} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Gausovou eliminací upravíme matici $\boldsymbol{S}_f - \boldsymbol{I}$:

$$\boldsymbol{S}_f - \boldsymbol{I} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Odtud dostaneme $W = \langle (1,0,0,0), (0,1,0,1) \rangle$. To odpovídá polynomům $h_1(x) = 1$ a $h_2(x) = x^3 + x$.

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Gausovou eliminací upravíme matici $\boldsymbol{S}_f - \boldsymbol{I}$:

$$\boldsymbol{S}_f - \boldsymbol{I} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Odtud dostaneme $W = \langle (1,0,0,0), (0,1,0,1) \rangle$. To odpovídá polynomům $h_1(x) = 1$ a $h_2(x) = x^3 + x$.

Spočteme

$$\begin{aligned} \mathrm{NSD}(f(x), h_2(x) - 0) &= \mathrm{NSD}(x^4 + 1, x^3 + x) = 1, \\ \mathrm{NSD}(f(x), h_2(x) - 1) &= \mathrm{NSD}(x^4 + 1, x^3 + x + 2) = x^2 + 2x + 2, \\ \mathrm{NSD}(f(x), h_2(X) - 2) &= \mathrm{NSD}(x^4 + 1, x^3 + x + 1) = x^2 + x + 2, \end{aligned}$$

Příklad

Hledáme rozklad polynomu $f(x) = x^4 + 1$ nad tělesem $\mathbb{F}_3$.

Gausovou eliminací upravíme matici $\boldsymbol{S}_f - \boldsymbol{I}$:

$$\boldsymbol{S}_f - \boldsymbol{I} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Odtud dostaneme $W = \langle (1,0,0,0), (0,1,0,1) \rangle$. To odpovídá polynomům $h_1(x) = 1$ a $h_2(x) = x^3 + x$.

Spočteme

$$\begin{aligned} \mathrm{NSD}(f(x), h_2(x) - 0) &= \mathrm{NSD}(x^4 + 1, x^3 + x) = 1, \\ \mathrm{NSD}(f(x), h_2(x) - 1) &= \mathrm{NSD}(x^4 + 1, x^3 + x + 2) = x^2 + 2x + 2, \\ \mathrm{NSD}(f(x), h_2(X) - 2) &= \mathrm{NSD}(x^4 + 1, x^3 + x + 1) = x^2 + x + 2, \end{aligned}$$

Polynomy $x^2 + 2x + 2$ a $x^2 + x + 2$ jsou nad $\mathbb{Z}_3$ ireducibilní (nemají kořen). Hledaný rozklad je tedy $f(x) = (x^2 + 2x + 2)(x^2 + x + 2)$.

Tvrzení (6.5)

Nechť $f_1(x)$ a $f_2(x)$ jsou dva různé ireducibilní faktory polynomu $f(x)$. Potom existuje $i \leq n$ takové, že $f_1(x)$ a $f_2(x)$ dělí různé členy rozkladu

$$f(x) = \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h_i(x) - a).$$

Tvrzení (6.5)

Nechť $f_1(x)$ a $f_2(x)$ jsou dva různé ireducibilní faktory polynomu $f(x)$. Potom existuje $i \leq n$ takové, že $f_1(x)$ a $f_2(x)$ dělí různé členy rozkladu

$$f(x) = \prod_{a \in \mathbb{F}_q} \mathrm{NSD}(f(x), h_i(x) - a).$$

Poznámka

Poznamenejme, že polynom $h_i(x)$ z předchozího tvrzení je nutně nekonstantní. Pokud totiž $\deg h_i(x) = 0$, tak platí, že

$$f_j(x) \mid h_i(x) - a \iff h_i(x) = a,$$

pro všechna j.

Důkaz.

Důkaz.

Buď $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ rozklad polynomu $f(x)$ v součin ireducibilních polynomů.

Důkaz.

Buď $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ rozklad polynomu $f(x)$ v součin ireducibilních polynomů.

Protože $f_i(x)$ dělí polynom $f(x)$ platí, že

$$f_i(x) \mid \mathrm{NSD}(f(x), h_i(x) - a) \iff f_i(x) \mid h_i(x) - a \iff h_i(x) \bmod f_i(x) = a.$$

Důkaz.

Buď $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ rozklad polynomu $f(x)$ v součin ireducibilních polynomů.

Protože $f_i(x)$ dělí polynom $f(x)$ platí, že

$$f_i(x) \mid \mathrm{NSD}(f(x), h_i(x) - a) \iff f_i(x) \mid h_i(x) - a \iff h_i(x) \bmod f_i(x) = a.$$

Podle Tvrzení 6.3 je zobrazení $\phi\colon W \to \mathbb{F}_q^n$ dané předpisem

$$h(x) \mapsto (h(x) \bmod f_1(x), h(x) \bmod f_2(x), \ldots, h(x) f_n(x))$$

izomorfismus vektorových prostorů nad tělesem $\mathbb{F}_q$.

Důkaz.

Buď $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$ rozklad polynomu $f(x)$ v součin ireducibilních polynomů.

Protože $f_i(x)$ dělí polynom $f(x)$ platí, že

$$f_i(x) \mid \mathrm{NSD}(f(x), h_i(x) - a) \iff f_i(x) \mid h_i(x) - a \iff h_i(x) \bmod f_i(x) = a.$$

Podle Tvrzení 6.3 je zobrazení $\phi\colon W \to \mathbb{F}_q^n$ dané předpisem

$$h(x) \mapsto (h(x) \bmod f_1(x), h(x) \bmod f_2(x), \ldots, h(x) f_n(x))$$

izomorfismus vektorových prostorů nad tělesem $\mathbb{F}_q$.

Obrazy $\phi(h_1(x)), \phi(h_2(x)), \ldots, \phi(h_n(x))$ tvoří bázi $\mathbb{F}_q^n$ a proto existuje $i \leq n$ takové, že vektor obrazu $\phi(h_i(x))$ má různé první dvě složky. Pro toto i pak

$$h_i(x) \bmod f_1(x) \neq h_i(x) \bmod f_2(x).$$

Upravený Berlekampův algoritmus

Rozkládáme bezčtvercový polynom $f(x)$

Upravený Berlekampův algoritmus

Rozkládáme bezčtvercový polynom $f(x)$

↓

Gaussovou eliminací řešíme homogenní soustavu $\boldsymbol{S}_f - \boldsymbol{I}$. Najdeme bázi $h_{\mathbf{1}}(x), h_{\mathbf{2}}(x), \ldots, h_n(x)$ prostoru W.

Upravený Berlekampův algoritmus

Rozkládáme bezčtvercový polynom $f(x)$

↓

Gaussovou eliminací řešíme homogenní soustavu $\boldsymbol{S}_f - \boldsymbol{I}$. Najdeme bázi $h_{\mathbf{1}}(x), h_{\mathbf{2}}(x), \ldots, h_n(x)$ prostoru W.

Upravený Berlekampův algoritmus

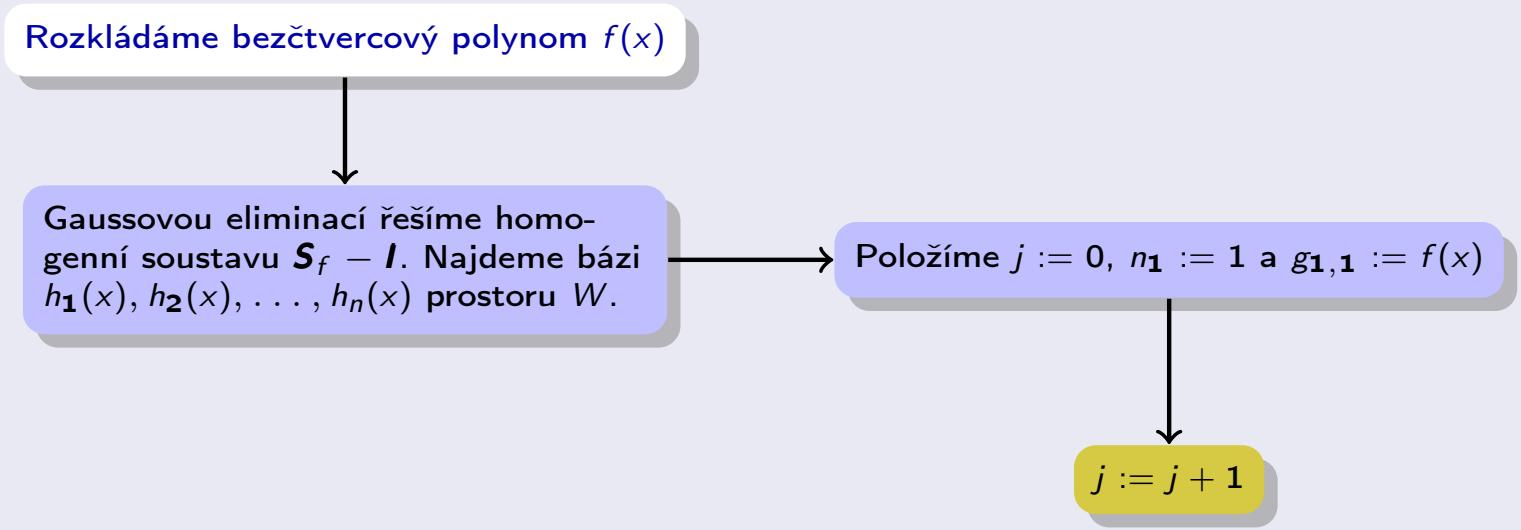
Rozkládáme bezčtvercový polynom $f(x)$

↓

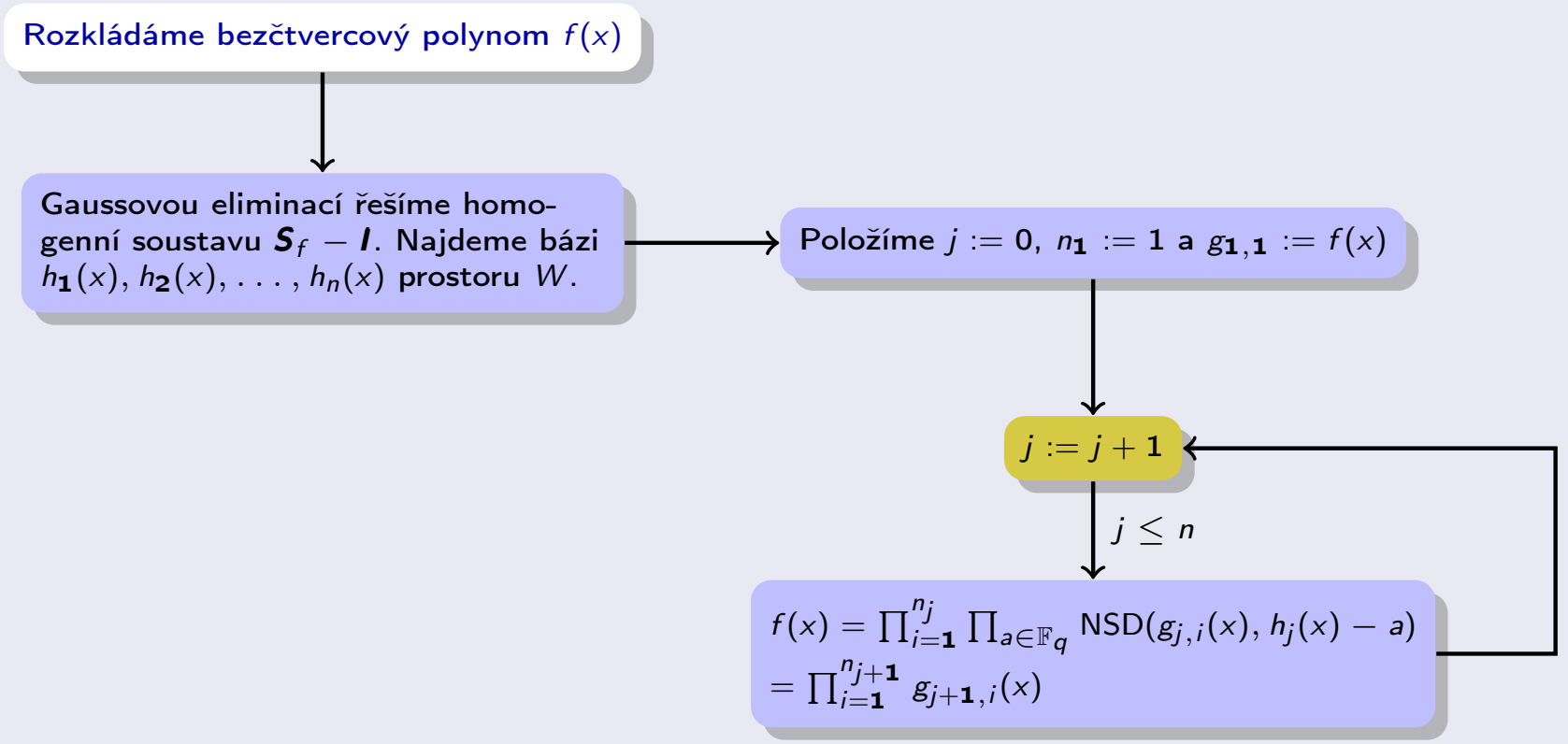
Gaussovou eliminací řešíme homogenní soustavu $\boldsymbol{S}_f - \boldsymbol{I}$. Najdeme bázi $h_{\mathbf{1}}(x), h_{\mathbf{2}}(x), \ldots, h_n(x)$ prostoru W.

→ Položíme $j := 0$, $n_{\mathbf{1}} := 1$ a $g_{\mathbf{1},\mathbf{1}} := f(x)$

Upravený Berlekampův algoritmus



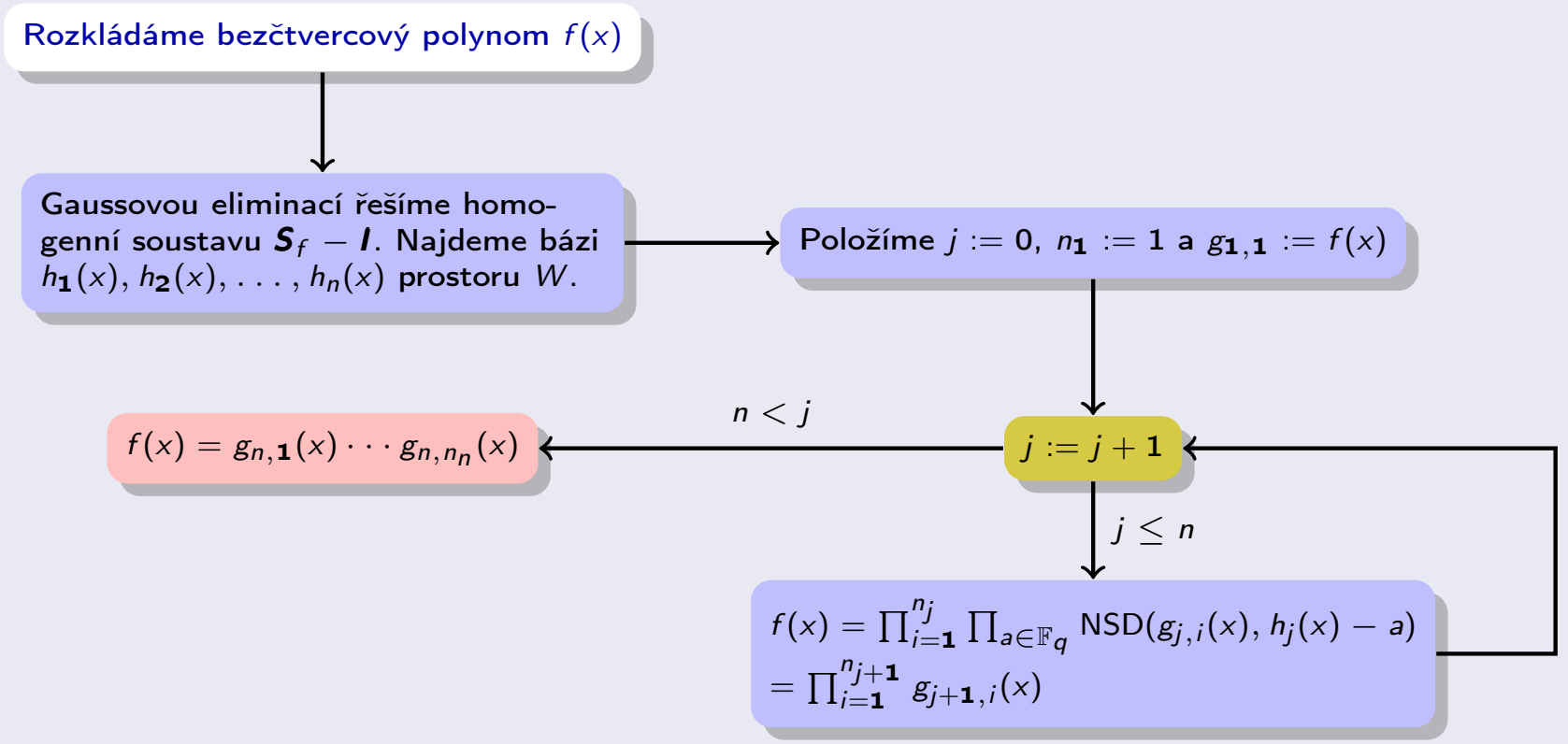
Upravený Berlekampův algoritmus



Postupně zjemňujeme rozklad

$$f(x) = g_{1,1}(x) = g_{2,1}(x) \cdot g_{2,2}(x) \cdots g_{2,n_{\mathbf{2}}}(x) = \cdots = g_{n,1}(x) \cdot g_{n,2}(x) \cdots g_{n,n_n}(x).$$

Upravený Berlekampův algoritmus



Postupně zjemňujeme rozklad

$$f(x) = g_{1,1}(x) = g_{2,1}(x) \cdot g_{2,2}(x) \cdots g_{2,n_{\mathbf{2}}}(x) = \cdots = g_{n,1}(x) \cdot g_{n,2}(x) \cdots g_{n,n_n}(x).$$

Vzhledem k Tvrzení 6.5 je $n_n = n$ a výsledný rozklad je na ireducibilní faktory.

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Spočteme $f'(x) = 3x^2$ a $\mathrm{NSD}(f'(x), f(x)) = 1$. Odtud odvodíme, že je polynom $f(x)$ bezčtvercový.

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Spočteme $f'(x) = 3x^2$ a $\mathrm{NSD}(f'(x), f(x)) = 1$. Odtud odvodíme, že je polynom $f(x)$ bezčtvercový.

Dále spočítáme, že

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

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Odtud dostaneme, že

$$S_f = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Odtud dostaneme, že

$$S_f = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

A proto

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

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Odtud dostaneme, že

$$S_f = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

A proto

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

Řešením je podprostor $W = \langle (1,0,0,0,0,0,0,0), (0,1,1,0,0,1,1,1) \rangle$.

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Vektory báze odpovídají polynomům $h_1(x) = 1$ a $h_2(x) = x^7 + x^6 + x^5 + x^2 + x$.
Vidíme, že polynom $f(x)$ se nad tělesem $\mathbb{F}_2$ rozkládá v součin dvou ireducibilních faktorů.

Příklad

Hledáme rozklad polynomu $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ nad tělesem $\mathbb{F}_2$.

Vektory báze odpovídají polynomům $h_1(x) = 1$ a $h_2(x) = x^7 + x^6 + x^5 + x^2 + x$.
Vidíme, že polynom $f(x)$ se nad tělesem $\mathbb{F}_2$ rozkládá v součin dvou ireducibilních faktorů.

Spočteme

$$\mathrm{NSD}(f(x), h_2(x) - 0) = \mathrm{NSD}(x^8 + x^6 + x^4 + x^3 + 1, x^7 + x^6 + x^5 + x^2 + x) = x^6 + x^5 + x^4 + x + 1,$$
$$\mathrm{NSD}(f(x), h_2(x) - 1) = \mathrm{NSD}(x^8 + x^6 + x^4 + x^3 + 1, x^7 + x^6 + x^5 + x^2 + x + 1) = x^2 + x + 1.$$

Dostaneme rozklad

$$x^8 + x^6 + x^4 + x^3 + 1 = (x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1)$$

polynomu $f(x)$ na ireducibilní faktory.