Zassenhausův algoritmus

Konečná tělesa

12. června 2020

Obsah přednášky

Obsah přednášky

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Buď $h(x)$ nekonstantní polynom takový, že $0 < \deg h(x) < \deg f(x)$ a

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

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Buď $h(x)$ nekonstantní polynom takový, že $0 < \deg h(x) < \deg f(x)$ a

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

Ukázali jsme (Tvrzení 6.2), že

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

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Buď $h(x)$ nekonstantní polynom takový, že $0 < \deg h(x) < \deg f(x)$ a

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

Ukázali jsme (Tvrzení 6.2), že

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

V případě, že $\deg f(x) \ll q$, bude výhodné určit ty prvky $a \in \mathbb{F}_q$, pro které jsou polynomy $f(x)$ a $h(x) - a$ soudělné.

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Buď $h(x)$ nekonstantní polynom takový, že $0 < \deg h(x) < \deg f(x)$ a

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

Ukázali jsme (Tvrzení 6.2), že

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

V případě, že $\deg f(x) \ll q$, bude výhodné určit ty prvky $a \in \mathbb{F}_q$, pro které jsou polynomy $f(x)$ a $h(x) - a$ soudělné.

Položme

$$A := \{a \in \mathbb{F}_q \mid \mathrm{NSD}(f(x), h(x) - a) \neq 1\}.$$

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Buď $h(x)$ nekonstantní polynom takový, že $0 < \deg h(x) < \deg f(x)$ a

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

Ukázali jsme (Tvrzení 6.2), že

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

V případě, že $\deg f(x) \ll q$, bude výhodné určit ty prvky $a \in \mathbb{F}_q$, pro které jsou polynomy $f(x)$ a $h(x) - a$ soudělné.

Položme

$$A := \{a \in \mathbb{F}_q \mid \mathrm{NSD}(f(x), h(x) - a) \neq 1\}.$$

Je jasné, že

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

Uvažme polynom $f(x) \in \mathbb{F}_q[x]$.

Buď $h(x)$ nekonstantní polynom takový, že $0 < \deg h(x) < \deg f(x)$ a

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

Ukázali jsme (Tvrzení 6.2), že

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

V případě, že $\deg f(x) \ll q$, bude výhodné určit ty prvky $a \in \mathbb{F}_q$, pro které jsou polynomy $f(x)$ a $h(x) - a$ soudělné.

Položme

$$A := \{a \in \mathbb{F}_q \mid \mathrm{NSD}(f(x), h(x) - a) \neq 1\}.$$

Je jasné, že

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

V tomto případě nelze žádný z členů v součinu vynechat.

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

- Z rovnosti (6.1) plyne, že $f(x) \mid G(h(x))$.

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

- Z rovnosti (6.1) plyne, že $f(x) \mid G(h(x))$.

Věta (6.6)

Položme

$$J = \{g(y) \in \mathbb{F}_q[y] \mid f(x) \mid g(h(x))\}.$$

Potom je J hlavní udeál okruhu $\mathbb{F}_q[y]$ generovaný polynomem $G(y)$.

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

- Z rovnosti (6.1) plyne, že $f(x) \mid G(h(x))$.

Věta (6.6)

Položme

$$J = \{g(y) \in \mathbb{F}_q[y] \mid f(x) \mid g(h(x))\}.$$

Potom je J hlavní udeál okruhu $\mathbb{F}_q[y]$ generovaný polynomem $G(y)$.

Důkaz -1

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

- Z rovnosti (6.1) plyne, že $f(x) \mid G(h(x))$.

Věta (6.6)

Položme

$$J = \{g(y) \in \mathbb{F}_q[y] \mid f(x) \mid g(h(x))\}.$$

Potom je J hlavní udeál okruhu $\mathbb{F}_q[y]$ generovaný polynomem $G(y)$.

Důkaz -1

Nejprve ukážeme, že J je ideál (tj. že je uzavřen na sčítání a násobení skaláry, t.j., prvky z okruhu $\mathbb{F}_q[x]$.)

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

- Z rovnosti (6.1) plyne, že $f(x) \mid G(h(x))$.

Věta (6.6)

Položme

$$J = \{g(y) \in \mathbb{F}_q[y] \mid f(x) \mid g(h(x))\}.$$

Potom je J hlavní udeál okruhu $\mathbb{F}_q[y]$ generovaný polynomem $G(y)$.

Důkaz -1

Nejprve ukážeme, že J je ideál (tj. že je uzavřen na sčítání a násobení skaláry, t.j., prvky z okruhu $\mathbb{F}_q[x]$.)

Uzavřenost na sčítání: Nechť $g_1(y), g_2(y) \in J$. Potom $f(x) \mid g_i(h(x))$, $i = 1, 2$, odkud

$$f(x) \mid (g_1(h(x)) + g_2(h(x))) = (g_1 + g_2)(h(x)),$$

a tedy $(g_1 + g_2)(y) \in J$.

Uvažme polynom

$$G(y) := \prod_{a \in A} (y - a).$$

- Z rovnosti (6.1) plyne, že $f(x) \mid G(h(x))$.

Věta (6.6)

Položme

$$J = \{g(y) \in \mathbb{F}_q[y] \mid f(x) \mid g(h(x))\}.$$

Potom je J hlavní udeál okruhu $\mathbb{F}_q[y]$ generovaný polynomem $G(y)$.

Důkaz -1

Nejprve ukážeme, že J je ideál (tj. že je uzavřen na sčítání a násobení skaláry, t.j., prvky z okruhu $\mathbb{F}_q[x]$.)

Uzavřenost na sčítání: Nechť $g_1(y), g_2(y) \in J$. Potom $f(x) \mid g_i(h(x))$, $i = 1, 2$, odkud

$$f(x) \mid (g_1(h(x)) + g_2(h(x))) = (g_1 + g_2)(h(x)),$$

a tedy $(g_1 + g_2)(y) \in J$.

Uzavřenost na násobení skaláry: Pokud $f(x) \mid g(h(x))$, tak zřejmě $f(x) \mid s(h(x)) \cdot g(h(x))$ pro každé $h(y) \in \mathbb{F}_q[y]$.

Důkaz Věty 6.6 -2

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Protože $f(x) \mid G(h(x))$ (viz. úvaha výše), $G(y) \in J$, a proto $G_0(y) \mid G(y)$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Protože $f(x) \mid G(h(x))$ (viz. úvaha výše), $G(y) \in J$, a proto $G_0(y) \mid G(y)$.

Odtud plyne, že existuje $B \subseteq A$ taková, že $G_0(y) = \prod_{a \in B}(y - a)$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Protože $f(x) \mid G(h(x))$ (viz. úvaha výše), $G(y) \in J$, a proto $G_0(y) \mid G(y)$.

Odtud plyne, že existuje $B \subseteq A$ taková, že $G_0(y) = \prod_{a \in B}(y - a)$. (Polynomy $y - a$, $a \in \mathbb{F}_q$, jsou po dvou nesoudělné prvočinitele v $\mathbb{F}_q[y]$ a $\mathbb{F}_q[y]$ je Gaussův obor.)

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Protože $f(x) \mid G(h(x))$ (viz. úvaha výše), $G(y) \in J$, a proto $G_0(y) \mid G(y)$.

Odtud plyne, že existuje $B \subseteq A$ taková, že $G_0(y) = \prod_{a \in B}(y - a)$. (Polynomy $y - a$, $a \in \mathbb{F}_q$, jsou po dvou nesoudělné prvočinitele v $\mathbb{F}_q[y]$ a $\mathbb{F}_q[y]$ je Gaussův obor.)

Protože $G_0(y) \in J$, platí, že $f(x) \mid G_0(h(x))$ a tedy

$$f(x) = \mathrm{NSD}(f(x), g(h(x))) = \prod_{a \in B} \mathrm{NSD}(f(x), h(x) - a).$$

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Protože $f(x) \mid G(h(x))$ (viz. úvaha výše), $G(y) \in J$, a proto $G_0(y) \mid G(y)$.

Odtud plyne, že existuje $B \subseteq A$ taková, že $G_0(y) = \prod_{a \in B}(y - a)$. (Polynomy $y - a$, $a \in \mathbb{F}_q$, jsou po dvou nesoudělné prvočinitele v $\mathbb{F}_q[y]$ a $\mathbb{F}_q[y]$ je Gaussův obor.)

Protože $G_0(y) \in J$, platí, že $f(x) \mid G_0(h(x))$ a tedy

$$f(x) = \mathrm{NSD}(f(x), g(h(x))) = \prod_{a \in B} \mathrm{NSD}(f(x), h(x) - a).$$

Vzhledem k tomu, že v rovnosti (6.1) nelze žádný z členů vynechat (t.j., že rovnost (6.1) neplatí pro žádnou vlastní podmnožinu množiny A), je $B = A$.

Důkaz Věty 6.6 -2

Ukážeme, že J je hlavní ideál generovaný polynomem $G(y)$.

Protože je $\mathbb{F}_q[y]$ oborem hlavních ideálů (je to okruh polynomů v jedné neurčité nad tělesem), je ideál J generován jedním polynomem; označme jej $G_0(y)$.

To znamená, že $J = \{s(y) \in \mathbb{F}_q(x) \mid G_0(y) \mid s(y)\}$.

Ukážeme, že $G_0(y) = G(y)$.

Protože $f(x) \mid G(h(x))$ (viz. úvaha výše), $G(y) \in J$, a proto $G_0(y) \mid G(y)$.

Odtud plyne, že existuje $B \subseteq A$ taková, že $G_0(y) = \prod_{a \in B}(y - a)$. (Polynomy $y - a$, $a \in \mathbb{F}_q$, jsou po dvou nesoudělné prvočinitele v $\mathbb{F}_q[y]$ a $\mathbb{F}_q[y]$ je Gaussův obor.)

Protože $G_0(y) \in J$, platí, že $f(x) \mid G_0(h(x))$ a tedy

$$f(x) = \mathrm{NSD}(f(x), g(h(x))) = \prod_{a \in B} \mathrm{NSD}(f(x), h(x) - a).$$

Vzhledem k tomu, že v rovnosti (6.1) nelze žádný z členů vynechat (t.j., že rovnost (6.1) neplatí pro žádnou vlastní podmnožinu množiny A), je $B = A$.

Odtud dostáváme, že $G_0(y) = G(y)$. □

Nalezení polynomu $G(y)$ a množiny A

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$.

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$. (Tyto podmnínky polynom $G(y)$ jednoznačně určují.)

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$. (Tyto podmnínky polynom $G(y)$ jednoznačně určují.)

Všimněme si, že $f(x) \mid G(h(x)) \iff G(h(x)) \equiv 0 \pmod{f(x)}$.

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$. (Tyto podmnínky polynom $G(y)$ jednoznačně určují.)

Všimněme si, že $f(x) \mid G(h(x)) \iff G(h(x)) \equiv 0 \pmod{f(x)}$.

Proto

$$0 = b_m(h^m(x) \bmod f(x)) + \cdots + b_1(h(x) \bmod f(x)) + b_0.$$

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$. (Tyto podmnínky polynom $G(y)$ jednoznačně určují.)

Všimněme si, že $f(x) \mid G(h(x)) \iff G(h(x)) \equiv 0 \pmod{f(x)}$.

Proto

$$0 = b_m(h^m(x) \bmod f(x)) + \cdots + b_1(h(x) \bmod f(x)) + b_0.$$

Spočteme $h^i(x) \bmod f(x)$ pro všechna $i = 1, 2, \ldots, m$.

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$. (Tyto podmnínky polynom $G(y)$ jednoznačně určují.)

Všimněme si, že $f(x) \mid G(h(x)) \iff G(h(x)) \equiv 0 \pmod{f(x)}$.

Proto

$$0 = b_m(h^m(x) \bmod f(x)) + \cdots + b_1(h(x) \bmod f(x)) + b_0.$$

Spočteme $h^i(x) \bmod f(x)$ pro všechna $i = 1, 2, \ldots, m$.

Položíme $b_m = 1$ (polynom $G(y)$ je monický) a řešením homogenní soustavy rovnic určíme zbývající koeficienty $b_0, b_1, \ldots, b_{m-1}$ polynomu $G(y)$.

Nalezení polynomu $G(y)$ a množiny A

Buď m počet ireducibilních faktorů polynomu $f(x)$ ($= \dim W$). Všimněme si, že $\deg G(y) = |A| = m$.

Hledáme monický polynom $G(y)$ tvaru

$$G(y) = b_m y^m + \cdots + b_1 y + b_0,$$

pro nějaké $b_0, b_1 \ldots b_m \in \mathbb{F}_q$.

Víme, že $G(y)$ je monický polynom nejmenšího stupně takový, že $f(x) \mid G(h(x))$. (Tyto podmnínky polynom $G(y)$ jednoznačně určují.)

Všimněme si, že $f(x) \mid G(h(x)) \iff G(h(x)) \equiv 0 \pmod{f(x)}$.

Proto

$$0 = b_m(h^m(x) \bmod f(x)) + \cdots + b_1(h(x) \bmod f(x)) + b_0.$$

Spočteme $h^i(x) \bmod f(x)$ pro všechna $i = 1, 2, \ldots, m$.

Položíme $b_m = 1$ (polynom $G(y)$ je monický) a řešením homogenní soustavy rovnic určíme zbývající koeficienty $b_0, b_1, \ldots, b_{m-1}$ polynomu $G(y)$.

Spočteme kořeny polynomu $G(y)$ a tak dostaneme množinu A.