Počítačová algebra

Alexandr Kazda

Univerzita Karlova

17. dubna 2020

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

NSD polynomů

- Polynomy jedné proměnné nad tělesy: Euklidův algoritmus
- Problém: Nad $\mathbb{Q}$ nám začnou během dělení se zbytkem ~~exponenciálně~~ velmi růst délky koeficientů
- [Příklad v Sage]
- A nešlo by NSD nad $\mathbb{Z}$ počítat bez výletu do $\mathbb{Q}$?
- A jak počítat NSD polynomů více proměnných?
- To vše bude obsahem dnešní hodiny
- Model složitosti: Počet operací na jedné cifře R

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Primitivní polynomy

- Připomínám $\mathrm{cont}(f)$ je obsah polynomu f; je to NSD všech koeficientů
- Primitivní polynom má obsah 1
- Primitivní část polynomu f, značená $\mathrm{pp}(f)$ je $f / \mathrm{cont}(f)$
- Algebra I: Pokud R je gaussovský obor integrity, tak $R[x]$ je gaussovský.
- Platí $f, g \in R[x]$

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_R(\mathrm{cont}(f), \mathrm{cont}(g)) \cdot \mathrm{NSD}_{R[x]}(\mathrm{pp}(f), \mathrm{pp}(g)),$$

tedy stačí počítat NSD pro primitivní polynomy

- Příklad ze $\mathbb{Z}[x]$:

$$\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2 - 8, 10x + 20) = 2\,\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 4, x + 2) = 2(x + 2)$$

Gaussovo lemma

- Pro primitivní polynomy z gaussovského oboru integrity R platí

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_{Q[x]}(f,g),$$

  kde Q je podílové těleso R (např. $R = \mathbb{Z}$ a $Q = \mathbb{Q}$)
- Tady $\mathrm{NSD}_{Q[x]}$ volíme tak, aby ležel v $R[x]$ a byl primitivní
- Příklad $\mathrm{NSD}_{\mathbb{Z}[x]}(x^2-1, x^2-2x+1) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2-1, x^2-2x+1)$
- Jsme zvyklí, že tělesa jsou „lepší“, než jenom gaussovské obory, ale výpočty v $\mathbb{Q}$ jsou pomalé
- Proto praktické použití Gaussova lemmatu je překvapivě na výpočet $\mathrm{NSD}_{\mathbb{Q}[x]}$ pomocí $\mathrm{NSD}_{\mathbb{Z}[x]}$

Gaussovo lemma

- Pro primitivní polynomy z gaussovského oboru integrity R platí

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_{Q[x]}(f,g),$$

  kde Q je podílové těleso R (např. $R = \mathbb{Z}$ a $Q = \mathbb{Q}$)
- Tady $\mathrm{NSD}_{Q[x]}$ volíme tak, aby ležel v $R[x]$ a byl primitivní
- Příklad $\mathrm{NSD}_{\mathbb{Z}[x]}(x^2-1, x^2-2x+1) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2-1, x^2-2x+1)$
- Jsme zvyklí, že tělesa jsou „lepší“, než jenom gaussovské obory, ale výpočty v $\mathbb{Q}$ jsou pomalé
- Proto praktické použití Gaussova lemmatu je překvapivě na výpočet $\mathrm{NSD}_{\mathbb{Q}[x]}$ pomocí $\mathrm{NSD}_{\mathbb{Z}[x]}$

Gaussovo lemma

- Pro primitivní polynomy z gaussovského oboru integrity R platí

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_{Q[x]}(f,g),$$

  kde Q je podílové těleso R (např. $R = \mathbb{Z}$ a $Q = \mathbb{Q}$)
- Tady $\mathrm{NSD}_{Q[x]}$ volíme tak, aby ležel v $R[x]$ a byl primitivní
- Příklad $\mathrm{NSD}_{\mathbb{Z}[x]}(x^2-1, x^2-2x+1) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2-1, x^2-2x+1)$
- Jsme zvyklí, že tělesa jsou „lepší“, než jenom gaussovské obory, ale výpočty v $\mathbb{Q}$ jsou pomalé
- Proto praktické použití Gaussova lemmatu je překvapivě na výpočet $\mathrm{NSD}_{\mathbb{Q}[x]}$ pomocí $\mathrm{NSD}_{\mathbb{Z}[x]}$

Gaussovo lemma

- Pro primitivní polynomy z gaussovského oboru integrity R platí

$$\mathrm{NSD}_{R[x]}(f, g) = \mathrm{NSD}_{Q[x]}(f, g),$$

  kde Q je podílové těleso R (např. $R = \mathbb{Z}$ a $Q = \mathbb{Q}$)
- Tady $\mathrm{NSD}_{Q[x]}$ volíme tak, aby ležel v $R[x]$ a byl primitivní
- Příklad $\mathrm{NSD}_{\mathbb{Z}[x]}(x^2 - 1, x^2 - 2x + 1) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2 - 1, x^2 - 2x + 1)$
- Jsme zvyklí, že tělesa jsou „lepší“, než jenom gaussovské obory, ale výpočty v $\mathbb{Q}$ jsou pomalé
- Proto praktické použití Gaussova lemmatu je překvapivě na výpočet $\mathrm{NSD}_{\mathbb{Q}[x]}$ pomocí $\mathrm{NSD}_{\mathbb{Z}[x]}$

Gaussovo lemma

- Pro primitivní polynomy z gaussovského oboru integrity R platí

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_{Q[x]}(f,g),$$

  kde Q je podílové těleso R (např. $R = \mathbb{Z}$ a $Q = \mathbb{Q}$)
- Tady $\mathrm{NSD}_{Q[x]}$ volíme tak, aby ležel v $R[x]$ a byl primitivní
- Příklad $\mathrm{NSD}_{\mathbb{Z}[x]}(x^2-1, x^2-2x+1) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2-1, x^2-2x+1)$
- Jsme zvyklí, že tělesa jsou „lepší“, než jenom gaussovské obory, ale výpočty v $\mathbb{Q}$ jsou pomalé
- Proto praktické použití Gaussova lemmatu je překvapivě na výpočet $\mathrm{NSD}_{\mathbb{Q}[x]}$ pomocí $\mathrm{NSD}_{\mathbb{Z}[x]}$

Gaussovo lemma

- Pro primitivní polynomy z gaussovského oboru integrity R platí

$$\mathrm{NSD}_{R[x]}(f,g) = \mathrm{NSD}_{Q[x]}(f,g),$$

  kde Q je podílové těleso R (např. $R = \mathbb{Z}$ a $Q = \mathbb{Q}$)
- Tady $\mathrm{NSD}_{Q[x]}$ volíme tak, aby ležel v $R[x]$ a byl primitivní
- Příklad $\mathrm{NSD}_{\mathbb{Z}[x]}(x^2-1, x^2-2x+1) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2-1, x^2-2x+1)$
- Jsme zvyklí, že tělesa jsou „lepší“, než jenom gaussovské obory, ale výpočty v $\mathbb{Q}$ jsou pomalé
- Proto praktické použití Gaussova lemmatu je překvapivě na výpočet $\mathrm{NSD}_{\mathbb{Q}[x]}$ pomocí $\mathrm{NSD}_{\mathbb{Z}[x]}$

Pseudodělení

- Bylo: dělení $f \operatorname{div} g$, $f \mod g$ v okruhu $R[x]$ funguje jenom když umíme dělit vedoucím členem g
- Pseudodělení: Počítejme

$$f \operatorname{pdiv} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \operatorname{div} g$$
$$f \operatorname{pmod} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \mod g$$

- Výhoda: Funguje v každém euklidovském oboru
- Nevýhoda: Narůstá velikost koeficientů
- Nápad: Co během Euklidova algoritmu koeficienty polynomů dělit nějakým společným dělitelem

Pseudodělení

- Bylo: dělení $f \operatorname{div} g$, $f \mod g$ v okruhu $R[x]$ funguje jenom když umíme dělit vedoucím členem g
- Pseudodělení: Počítejme

$$f \operatorname{pdiv} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \operatorname{div} g$$
$$f \operatorname{pmod} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \mod g$$

- Výhoda: Funguje v každém euklidovském oboru
- Nevýhoda: Narůstá velikost koeficientů
- Nápad: Co během Euklidova algoritmu koeficienty polynomů dělit nějakým společným dělitelem

Pseudodělení

- Bylo: dělení $f \operatorname{div} g$, $f \mod g$ v okruhu $R[x]$ funguje jenom když umíme dělit vedoucím členem g
- Pseudodělení: Počítejme

$$f \operatorname{pdiv} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \operatorname{div} g$$
$$f \operatorname{pmod} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \mod g$$

- Výhoda: Funguje v každém euklidovském oboru
- Nevýhoda: Narůstá velikost koeficientů
- Nápad: Co během Euklidova algoritmu koeficienty polynomů dělit nějakým společným dělitelem

Pseudodělení

- Bylo: dělení $f \operatorname{div} g$, $f \mod g$ v okruhu $R[x]$ funguje jenom když umíme dělit vedoucím členem g
- Pseudodělení: Počítejme

$$f \operatorname{pdiv} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \operatorname{div} g$$
$$f \operatorname{pmod} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \mod g$$

- Výhoda: Funguje v každém euklidovském oboru
- Nevýhoda: Narůstá velikost koeficientů
- Nápad: Co během Euklidova algoritmu koeficienty polynomů dělit nějakým společným dělitelem

Pseudodělení

- Bylo: dělení $f \operatorname{div} g$, $f \mod g$ v okruhu $R[x]$ funguje jenom když umíme dělit vedoucím členem g
- Pseudodělení: Počítejme

$$f \operatorname{pdiv} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \operatorname{div} g$$
$$f \operatorname{pmod} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \mod g$$

- Výhoda: Funguje v každém euklidovském oboru
- Nevýhoda: Narůstá velikost koeficientů
- Nápad: Co během Euklidova algoritmu koeficienty polynomů dělit nějakým společným dělitelem

Pseudodělení

- Bylo: dělení $f \operatorname{div} g$, $f \mod g$ v okruhu $R[x]$ funguje jenom když umíme dělit vedoucím členem g
- Pseudodělení: Počítejme

$$f \operatorname{pdiv} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \operatorname{div} g$$
$$f \operatorname{pmod} g = (\operatorname{lc}(g)^{\deg f - \deg g + 1} f) \mod g$$

- Výhoda: Funguje v každém euklidovském oboru
- Nevýhoda: Narůstá velikost koeficientů
- Nápad: Co během Euklidova algoritmu koeficienty polynomů dělit nějakým společným dělitelem

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0,\ f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

Posloupnost polynomiálních zbytků

- Polynomial remainder sequence – PRS
- $f, g \in R[x]$ jsou si podobné, pokud existují nenulové $k, l \in R$, že $kf = lg$; značíme $f \sim g$
- PRS je posloupnost $f_1, f_2, \ldots, f_k \in R[x]$ taková, že
  1. $f_1, \ldots, f_{k-1} \neq 0$, $f_k = 0$
  2. $\deg f_1 \geq \deg f_2$
  3. $f_{i+1} \sim (f_{i-1} \operatorname{pmod} f_i)$
- PRS jsou polynomy z Euklida modulo $\sim$
- Pozorování: R gaussovský, $f_1, \ldots, f_k$ PRS v $R[x]$. Pak $f_k \sim \mathrm{NSD}(f_1, f_2)$

NSD pomocí PRS

- Kostra algoritmu pro $R = \mathbb{Z}[x]$, $R = \mathbb{Q}[y, z][x]$ a podobně

  Data: f, g primitivní polynomy, $\deg f \geq \deg g$
  Result: $\mathrm{NSD}(f, g)$
  $f_1 := f$;
  $f_2 := g$;
  while $f_i \neq 0$ **do**
  $\quad f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$;
  $\quad i := i + 1$;
  end
  return $\mathrm{pp}(f_{i-1})$;

- Jak volit α_{i+1}? Různé strategie...

NSD pomocí PRS

- Kostra algoritmu pro $R = \mathbb{Z}[x]$, $R = \mathbb{Q}[y, z][x]$ a podobně

  Data: f, g primitivní polynomy, $\deg f \geq \deg g$
  Result: $\mathrm{NSD}(f, g)$
  $f_1 := f$;
  $f_2 := g$;
  while $f_i \neq 0$ **do**
  $\quad f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$;
  $\quad i := i + 1$;
  end
  return $\mathrm{pp}(f_{i-1})$;

- Jak volit α_{i+1}? Různé strategie...

NSD pomocí PRS

- Kostra algoritmu pro $R = \mathbb{Z}[x]$, $R = \mathbb{Q}[y, z][x]$ a podobně

  Data: f, g primitivní polynomy, $\deg f \geq \deg g$
  Result: $\mathrm{NSD}(f, g)$
  $f_1 := f$;
  $f_2 := g$;
  while $f_i \neq 0$ **do**
  $\quad f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$;
  $\quad i := i + 1$;
  end
  return $\mathrm{pp}(f_{i-1})$;

- Jak volit α_{i+1}? Různé strategie...

NSD pomocí PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Euklidovská PRS: $\alpha_{i+1} = 1$
- Primitivní PRS: $\alpha_{i+1} = \operatorname{cont}(f_{i-1} \operatorname{pmod} f_i)$
- Primitivní PRS je pomalá např. pro $R[x] = T[y, z][x]$

NSD pomocí PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Euklidovská PRS: $\alpha_{i+1} = 1$
- Primitivní PRS: $\alpha_{i+1} = \operatorname{cont}(f_{i-1} \operatorname{pmod} f_i)$
- Primitivní PRS je pomalá např. pro $R[x] = T[y, z][x]$

NSD pomocí PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Euklidovská PRS: $\alpha_{i+1} = 1$
- Primitivní PRS: $\alpha_{i+1} = \operatorname{cont}(f_{i-1} \operatorname{pmod} f_i)$
- Primitivní PRS je pomalá např. pro $R[x] = T[y, z][x]$

NSD pomocí PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Euklidovská PRS: $\alpha_{i+1} = 1$
- Primitivní PRS: $\alpha_{i+1} = \operatorname{cont}(f_{i-1} \operatorname{pmod} f_i)$
- Primitivní PRS je pomalá např. pro $R[x] = T[y, z][x]$

NSD pomocí PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Euklidovská PRS: $\alpha_{i+1} = 1$
- Primitivní PRS: $\alpha_{i+1} = \operatorname{cont}(f_{i-1} \operatorname{pmod} f_i)$
- Primitivní PRS je pomalá např. pro $R[x] = T[y, z][x]$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS

- Jednoduchá na implementaci
- Délka koeficientů roste zhruba exponenciálně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Pro náhodné polynomy bude typicky $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = \mathrm{lc}(f_i)^2 f_{i-1} - (ax + b) f_i$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1}$

Euklidovská PRS, II

- Máme rekurenci $\ell_{i+1} = 2\ell_i + \ell_{i-1}$
- Zkusíme dosadit $\ell_i = \lambda^i$
- Pak $\lambda^2 = 2\lambda + 1$;
- to má řešení $\lambda = 1 \pm \sqrt{2}$
- [Numerické experimenty v Sage]

Euklidovská PRS, II

- Máme rekurenci $\ell_{i+1} = 2\ell_i + \ell_{i-1}$
- Zkusíme dosadit $\ell_i = \lambda^i$
- Pak $\lambda^2 = 2\lambda + 1$;
- to má řešení $\lambda = 1 \pm \sqrt{2}$
- [Numerické experimenty v Sage]

Euklidovská PRS, II

- Máme rekurenci $\ell_{i+1} = 2\ell_i + \ell_{i-1}$
- Zkusíme dosadit $\ell_i = \lambda^i$
- Pak $\lambda^2 = 2\lambda + 1$;
- to má řešení $\lambda = 1 \pm \sqrt{2}$
- [Numerické experimenty v Sage]

Euklidovská PRS, II

- Máme rekurenci $\ell_{i+1} = 2\ell_i + \ell_{i-1}$
- Zkusíme dosadit $\ell_i = \lambda^i$
- Pak $\lambda^2 = 2\lambda + 1$;
- to má řešení $\lambda = 1 \pm \sqrt{2}$
- [Numerické experimenty v Sage]

Euklidovská PRS, II

- Máme rekurenci $\ell_{i+1} = 2\ell_i + \ell_{i-1}$
- Zkusíme dosadit $\ell_i = \lambda^i$
- Pak $\lambda^2 = 2\lambda + 1$;
- to má řešení $\lambda = 1 \pm \sqrt{2}$
- [Numerické experimenty v Sage]

Euklidovská PRS, II

- Máme rekurenci $\ell_{i+1} = 2\ell_i + \ell_{i-1}$
- Zkusíme dosadit $\ell_i = \lambda^i$
- Pak $\lambda^2 = 2\lambda + 1$;
- to má řešení $\lambda = 1 \pm \sqrt{2}$
- [Numerické experimenty v Sage]

Primitivní PRS

- Lineární nárůst délky koeficientů (to dokazovat nebudeme)
- [Příklad v Sage]

Primitivní PRS

- Lineární nárůst délky koeficientů (to dokazovat nebudeme)
- [Příklad v Sage]

Primitivní PRS

- Lineární nárůst délky koeficientů (to dokazovat nebudeme)
- [Příklad v Sage]

Redukovaná PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_i - \deg f_{i+1}$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Vlastně dělíme multiplikátorem pro pseudodělení z předchozího kroku
- Není jasné, proč α_{i+1} dělí $f_{i-1} \operatorname{pmod} f_i$

Redukovaná PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_i - \deg f_{i+1}$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Vlastně dělíme multiplikátorem pro pseudodělení z předchozího kroku
- Není jasné, proč α_{i+1} dělí $f_{i-1} \operatorname{pmod} f_i$

Redukovaná PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_i - \deg f_{i+1}$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Vlastně dělíme multiplikátorem pro pseudodělení z předchozího kroku
- Není jasné, proč α_{i+1} dělí $f_{i-1} \operatorname{pmod} f_i$

Redukovaná PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_i - \deg f_{i+1}$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Vlastně dělíme multiplikátorem pro pseudodělení z předchozího kroku
- Není jasné, proč α_{i+1} dělí $f_{i-1} \operatorname{pmod} f_i$

Redukovaná PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_i - \deg f_{i+1}$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Vlastně dělíme multiplikátorem pro pseudodělení z předchozího kroku
- Není jasné, proč α_{i+1} dělí $f_{i-1} \operatorname{pmod} f_i$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b) f_i) / \operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b) f_i) / \operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b) f_i) / \operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b) f_i) / \operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b)f_i)/\operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b)f_i)/\operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b)f_i)/\operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, II

- Délka koeficientů typicky roste lineárně
- Heuristický argument: Nechť f_i má koeficienty délky ℓ_i
- Zase předpokládejme $\deg f_i = \deg f_{i-1} - 1$
- Potom $f_{i+1} = (\operatorname{lc}(f_i)^2 f_{i-1} - (ax+b)f_i)/\operatorname{lc}(f_{i-1})^2$
- Pak zhruba $\ell_{i+1} = 2\ell_i + \ell_{i-1} - 2\ell_{i-1} = 2\ell_i - \ell_{i-1}$
- Tedy $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$
-

$$\ell_{i+1} - \ell_1 = (\ell_{i+1} - \ell_i) + (\ell_i - \ell_{i-1}) + \cdots + (\ell_3 - \ell_2) + (\ell_2 - \ell_1)$$

Redukovaná PRS, III

- $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$,
- To popisuje lineární růst!
- [Příklad v Sage]
- Redukovaná PRS běhá v praxi o něco málo rychleji než primitivní PRS

Redukovaná PRS, III

- $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$,
- To popisuje lineární růst!
- [Příklad v Sage]
- Redukovaná PRS běhá v praxi o něco málo rychleji než primitivní PRS

Redukovaná PRS, III

- $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$,
- To popisuje lineární růst!
- [Příklad v Sage]
- Redukovaná PRS běhá v praxi o něco málo rychleji než primitivní PRS

Redukovaná PRS, III

- $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$,
- To popisuje lineární růst!
- [Příklad v Sage]
- Redukovaná PRS běhá v praxi o něco málo rychleji než primitivní PRS

Redukovaná PRS, III

- $\ell_{i+1} - \ell_i = \ell_i - \ell_{i-1}$,
- To popisuje lineární růst!
- [Příklad v Sage]
- Redukovaná PRS běhá v praxi o něco málo rychleji než primitivní PRS

Redukovaná PRS, IV

- Asymptotické chování
- Nechť $\deg f = n$, $\deg g = n-1$,
- Předpokládejme $\deg f_i = n+1-i$ pro všechna i a $\ell_i = ci$ pro nějaké c
- $f_{i-1} \bmod f_i$ má složitost $O((n-i+1)(ci)^2)$
- Složitost $O(\sum_{i=1}^{n}(n-i+1)c^2i^2) = O(c^2 n \sum_{i=1}^{n} i^2) = O(c^2 n^4)$

Redukovaná PRS, IV

- Asymptotické chování
- Nechť $\deg f = n$, $\deg g = n-1$,
- Předpokládejme $\deg f_i = n+1-i$ pro všechna i a $\ell_i = ci$ pro nějaké c
- $f_{i-1} \bmod f_i$ má složitost $O((n-i+1)(ci)^2)$
- Složitost $O(\sum_{i=1}^{n}(n-i+1)c^2i^2) = O(c^2 n \sum_{i=1}^{n} i^2) = O(c^2 n^4)$

Redukovaná PRS, IV

- Asymptotické chování
- Nechť $\deg f = n$, $\deg g = n-1$,
- Předpokládejme $\deg f_i = n+1-i$ pro všechna i a $\ell_i = ci$ pro nějaké c
- $f_{i-1} \bmod f_i$ má složitost $O((n-i+1)(ci)^2)$
- Složitost $O(\sum_{i=1}^{n}(n-i+1)c^2i^2) = O(c^2 n \sum_{i=1}^{n} i^2) = O(c^2 n^4)$

Redukovaná PRS, IV

- Asymptotické chování
- Nechť $\deg f = n$, $\deg g = n-1$,
- Předpokládejme $\deg f_i = n+1-i$ pro všechna i a $\ell_i = ci$ pro nějaké c
- $f_{i-1} \bmod f_i$ má složitost $O((n-i+1)(ci)^2)$
- Složitost $O(\sum_{i=1}^{n}(n-i+1)c^2i^2) = O(c^2 n \sum_{i=1}^{n} i^2) = O(c^2 n^4)$

Redukovaná PRS, IV

- Asymptotické chování
- Nechť $\deg f = n$, $\deg g = n-1$,
- Předpokládejme $\deg f_i = n+1-i$ pro všechna i a $\ell_i = ci$ pro nějaké c
- $f_{i-1} \bmod f_i$ má složitost $O((n-i+1)(ci)^2)$
- Složitost $O(\sum_{i=1}^{n}(n-i+1)c^2i^2) = O(c^2 n \sum_{i=1}^{n} i^2) = O(c^2 n^4)$

Redukovaná PRS, IV

- Asymptotické chování
- Nechť $\deg f = n$, $\deg g = n-1$,
- Předpokládejme $\deg f_i = n+1-i$ pro všechna i a $\ell_i = ci$ pro nějaké c
- $f_{i-1} \bmod f_i$ má složitost $O((n-i+1)(ci)^2)$
- Složitost $O(\sum_{i=1}^{n}(n-i+1)c^2i^2) = O(c^2 n \sum_{i=1}^{n} i^2) = O(c^2 n^4)$

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

Subrezultantová PRS

- $f_{i+1} := \frac{1}{\alpha_{i+1}}(f_{i-1} \operatorname{pmod} f_i)$
- Značme $\delta_i = \deg f_{i-1} - \deg f_i$
- Nechť $\beta_2 = \operatorname{lc}(f_2)^{\delta_1}$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^{\delta_i} \beta_i^{1-\delta_i}$
- Pak $\alpha_3 = 1$; $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^{\delta_{i-1}}$
- Uff. Pro $\delta_i = 1$ to je redukovaná PRS:
- $\beta_2 = \operatorname{lc}(f_2)^1$; $\beta_{i+1} = \operatorname{lc}(f_{i+1})^1 \beta_i^{1-1} = \operatorname{lc}(f_{i+1})$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1}) \beta_{i-1}^1 = \operatorname{lc}(f_{i-1})^2$
- Redukovaná PRS (J. J. Sylvester, cca 1850): $\alpha_3 = 1$;
  $\alpha_{i+1} = \operatorname{lc}(f_{i-1})^{\deg f_{i-2} - \deg f_{i-1} + 1}$
- Rezultanty budou...
- Lze dokázat, že délka koeficientů roste vždy lineárně a výpočet α_{i+1} je rychlý

13. Rezultant a Sylvestrovo kritérium nesoudělnosti

Theorem

Buď R gaussovský, Q jeho podílové těleso, $\overline{Q}$ algebraický uzávěr Q. Buďte $f, g \in R[x]$, $\deg f, g \geq 1$. PNTJE:

1. $\mathrm{NSD}_{Q[x]}(f, g) \neq 1$
2. $\deg \mathrm{NSD}_{R[x]}(f, g) > 0$
3. $\exists u, v \in R[x] \setminus \{0\}$, *že*

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

4. *f, g mají společný kořen v $\overline{Q}$*

13. Rezultant a Sylvestrovo kritérium nesoudělnosti

Theorem

Buď R gaussovský, Q jeho podílové těleso, $\overline{Q}$ algebraický uzávěr Q. Buďte $f, g \in R[x]$, $\deg f, g \geq 1$. PNTJE:

1. $\mathrm{NSD}_{Q[x]}(f, g) \neq 1$
2. $\deg \mathrm{NSD}_{R[x]}(f, g) > 0$
3. $\exists u, v \in R[x] \setminus \{0\}$, *že*

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

4. f, g *mají společný kořen v* $\overline{Q}$

Důkaz

- Gaussovo lemma: $\mathrm{NSD}_{Q[x]}(f,g) \neq 1 \Leftrightarrow \deg \mathrm{NSD}_{R[x]}(f,g) > 0$p
- Nechť

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

- Pak $f | vg$ a $\deg f > \deg v$, tedy f, g mají společný ireducibilní faktor
- Nechď $d = \mathrm{NSD}_{R[x]}(f,g)$. Pak volba $u = g/d$, $v = -f/d$ nám dá (3)

$$uf + vg = (g/d)f + (-f/d)g = gf/d - gf/d = 0$$

Důkaz

- Gaussovo lemma: $\mathrm{NSD}_{Q[x]}(f,g) \neq 1 \Leftrightarrow \deg \mathrm{NSD}_{R[x]}(f,g) > 0$p
- Nechť

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

- Pak $f | vg$ a $\deg f > \deg v$, tedy f, g mají společný ireducibilní faktor
- Nechď $d = \mathrm{NSD}_{R[x]}(f,g)$. Pak volba $u = g/d$, $v = -f/d$ nám dá (3)

$$uf + vg = (g/d)f + (-f/d)g = gf/d - gf/d = 0$$

Důkaz

- Gaussovo lemma: $\mathrm{NSD}_{Q[x]}(f,g) \neq 1 \Leftrightarrow \deg \mathrm{NSD}_{R[x]}(f,g) > 0$p
- Nechť

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

- Pak $f | vg$ a $\deg f > \deg v$, tedy f, g mají společný ireducibilní faktor
- Nechď $d = \mathrm{NSD}_{R[x]}(f,g)$. Pak volba $u = g/d$, $v = -f/d$ nám dá (3)

$$uf + vg = (g/d)f + (-f/d)g = gf/d - gf/d = 0$$

Důkaz

- Gaussovo lemma: $\mathrm{NSD}_{Q[x]}(f,g) \neq 1 \Leftrightarrow \deg \mathrm{NSD}_{R[x]}(f,g) > 0$p
- Nechť

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

- Pak $f | vg$ a $\deg f > \deg v$, tedy f, g mají společný ireducibilní faktor
- Nechď $d = \mathrm{NSD}_{R[x]}(f,g)$. Pak volba $u = g/d$, $v = -f/d$ nám dá (3)

$$uf + vg = (g/d)f + (-f/d)g = gf/d - gf/d = 0$$

Důkaz

- Gaussovo lemma: $\mathrm{NSD}_{Q[x]}(f,g) \neq 1 \Leftrightarrow \deg \mathrm{NSD}_{R[x]}(f,g) > 0$p
- Nechť

$$\deg u < \deg g$$
$$\deg v < \deg f$$
$$uf + vg = 0$$

- Pak $f | vg$ a $\deg f > \deg v$, tedy f, g mají společný ireducibilní faktor
- Nechď $d = \mathrm{NSD}_{R[x]}(f,g)$. Pak volba $u = g/d$, $v = -f/d$ nám dá (3)

$$uf + vg = (g/d)f + (-f/d)g = gf/d - gf/d = 0$$

Důkaz II

- Rozmyslete si, že Euklidův algoritmus v Q a $\overline{Q}$ běží zcela stejně
- Nechť $\mathrm{NSD}_{Q[x]}(f,g) \neq 1$. Pak $\mathrm{NSD}_{\overline{Q}[x]}(f,g) \neq 1$.
- Tedy f, g mají společný lineární faktor v $\overline{Q}[x]$
- $x - \alpha | f, g$ znamená, že $f(\alpha) = g(\alpha) = 0$

Důkaz II

- Rozmyslete si, že Euklidův algoritmus v Q a $\overline{Q}$ běží zcela stejně
- Nechť $\mathrm{NSD}_{Q[x]}(f,g) \neq 1$. Pak $\mathrm{NSD}_{\overline{Q}[x]}(f,g) \neq 1$.
- Tedy f, g mají společný lineární faktor v $\overline{Q}[x]$
- $x - \alpha | f, g$ znamená, že $f(\alpha) = g(\alpha) = 0$

Důkaz II

- Rozmyslete si, že Euklidův algoritmus v Q a $\overline{Q}$ běží zcela stejně
- Nechť $\mathrm{NSD}_{Q[x]}(f,g) \neq 1$. Pak $\mathrm{NSD}_{\overline{Q}[x]}(f,g) \neq 1$.
- Tedy f, g mají společný lineární faktor v $\overline{Q}[x]$
- $x - \alpha | f, g$ znamená, že $f(\alpha) = g(\alpha) = 0$

Důkaz II

- Rozmyslete si, že Euklidův algoritmus v Q a $\overline{Q}$ běží zcela stejně
- Nechť $\mathrm{NSD}_{Q[x]}(f,g) \neq 1$. Pak $\mathrm{NSD}_{\overline{Q}[x]}(f,g) \neq 1$.
- Tedy f, g mají společný lineární faktor v $\overline{Q}[x]$
- $x - \alpha | f, g$ znamená, že $f(\alpha) = g(\alpha) = 0$

Důkaz II

- Rozmyslete si, že Euklidův algoritmus v Q a $\overline{Q}$ běží zcela stejně
- Nechť $\mathrm{NSD}_{Q[x]}(f,g) \neq 1$. Pak $\mathrm{NSD}_{\overline{Q}[x]}(f,g) \neq 1$.
- Tedy f, g mají společný lineární faktor v $\overline{Q}[x]$
- $x - \alpha | f, g$ znamená, že $f(\alpha) = g(\alpha) = 0$

Polynomy u, v

- Vraťme se k bodu (3)
- Berme $m \geq n$

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$
$$g = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0$$

- Hledaní koeficientů polynomů u, v omezených stupňů, že $fu + gv = 0$ je soustava lineárních rovnic
- Rovnice:

$$\begin{aligned} f_n u_{m-1} + g_m v_{n-1} &= 0 \\ f_{n-1} u_{m-1} + f_n u_{m-2} + g_{m-1} v_{n-1} + g_m v_{n-2} &= 0 \\ &\vdots \\ f_0 u_0 + g_0 v_0 &= 0 \end{aligned}$$

Polynomy u, v

- Vraťme se k bodu (3)
- Berme $m \geq n$

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$
$$g = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0$$

- Hledaní koeficientů polynomů u, v omezených stupňů, že $fu + gv = 0$ je soustava lineárních rovnic
- Rovnice:

$$\begin{aligned} f_n u_{m-1} + g_m v_{n-1} &= 0 \\ f_{n-1} u_{m-1} + f_n u_{m-2} + g_{m-1} v_{n-1} + g_m v_{n-2} &= 0 \\ &\vdots \\ f_0 u_0 + g_0 v_0 &= 0 \end{aligned}$$

Polynomy u, v

- Vraťme se k bodu (3)
- Berme $m \geq n$

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$
$$g = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0$$

- Hledaní koeficientů polynomů u, v omezených stupňů, že $fu + gv = 0$ je soustava lineárních rovnic
- Rovnice:

$$f_n u_{m-1} + g_m v_{n-1} = 0$$
$$f_{n-1} u_{m-1} + f_n u_{m-2} + g_{m-1} v_{n-1} + g_m v_{n-2} = 0$$
$$\vdots$$
$$f_0 u_0 + g_0 v_0 = 0$$

Polynomy u, v

- Vraťme se k bodu (3)
- Berme $m \geq n$

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$
$$g = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0$$

- Hledaní koeficientů polynomů u, v omezených stupňů, že $fu + gv = 0$ je soustava lineárních rovnic
- Rovnice:

$$f_n u_{m-1} + g_m v_{n-1} = 0$$
$$f_{n-1} u_{m-1} + f_n u_{m-2} + g_{m-1} v_{n-1} + g_m v_{n-2} = 0$$
$$\vdots$$
$$f_0 u_0 + g_0 v_0 = 0$$

Polynomy u, v

- Vraťme se k bodu (3)
- Berme $m \geq n$

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$
$$g = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0$$

- Hledaní koeficientů polynomů u, v omezených stupňů, že $fu + gv = 0$ je soustava lineárních rovnic
- Rovnice:

$$\begin{aligned} f_n u_{m-1} + g_m v_{n-1} &= 0 \\ f_{n-1} u_{m-1} + f_n u_{m-2} + g_{m-1} v_{n-1} + g_m v_{n-2} &= 0 \\ &\vdots \\ f_0 u_0 + g_0 v_0 &= 0 \end{aligned}$$

- Matice soustavy $fu + gv = 0$

$$M(f,g)^T = \begin{pmatrix}
f_n & 0 & 0 & \dots & g_m & 0 & 0 & \dots & 0 \\
f_{n-1} & f_n & 0 & \dots & g_{m-1} & g_m & 0 & \dots & 0 \\
f_{n-2} & f_{n-1} & f_n & \dots & g_{m-2} & g_{m-1} & g_m & \dots & 0 \\
 & & & \ddots & & & & & \\
f_0 & f_1 & f_2 & \ddots & \ddots & & & & \\
0 & f_0 & f_1 & \ddots & & \ddots & & & \\
0 & 0 & & \dots & g_0 & g_1 & g_2 & \dots & g_{n-1} \\
0 & 0 & & \dots & 0 & g_0 & g_1 & \dots & g_{n-2} \\
 & & \ddots & & & \ddots & & & \\
0 & 0 & 0 & f_0 & 0 & 0 & 0 & \dots & g_0
\end{pmatrix}$$

- Netriviální řešení u, v právě když $\det(M(f,g)) = 0$

- Matice soustavy $fu + gv = 0$

$$M(f,g)^T = \begin{pmatrix}
f_n & 0 & 0 & \dots & g_m & 0 & 0 & \dots & 0 \\
f_{n-1} & f_n & 0 & \dots & g_{m-1} & g_m & 0 & \dots & 0 \\
f_{n-2} & f_{n-1} & f_n & \dots & g_{m-2} & g_{m-1} & g_m & \dots & 0 \\
 & & & \ddots & & & & & \\
f_0 & f_1 & f_2 & \ddots & \ddots & & & & \\
0 & f_0 & f_1 & \ddots & & \ddots & & & \\
0 & 0 & & \dots & g_0 & g_1 & g_2 & \dots & g_{n-1} \\
0 & 0 & & \dots & 0 & g_0 & g_1 & \dots & g_{n-2} \\
 & & \ddots & & & \ddots & & & \\
0 & 0 & 0 & f_0 & 0 & 0 & 0 & \dots & g_0
\end{pmatrix}$$

- Netriviální řešení u, v právě když $\det(M(f,g)) = 0$

- Matice soustavy $fu + gv = 0$

$$M(f,g)^T = \begin{pmatrix}
f_n & 0 & 0 & \dots & g_m & 0 & 0 & \dots & 0 \\
f_{n-1} & f_n & 0 & \dots & g_{m-1} & g_m & 0 & \dots & 0 \\
f_{n-2} & f_{n-1} & f_n & \dots & g_{m-2} & g_{m-1} & g_m & \dots & 0 \\
 & & & \ddots & & & & & \\
f_0 & f_1 & f_2 & \ddots & \ddots & & & & \\
0 & f_0 & f_1 & \ddots & & \ddots & & & \\
0 & 0 & & \dots & g_0 & g_1 & g_2 & \dots & g_{n-1} \\
0 & 0 & & \dots & 0 & g_0 & g_1 & \dots & g_{n-2} \\
 & & \ddots & & & \ddots & & & \\
0 & 0 & 0 & f_0 & 0 & 0 & 0 & \dots & g_0
\end{pmatrix}$$

- Netriviální řešení u, v právě když $\det(M(f,g)) = 0$

Rezultant I

- $\deg f = n$, $\deg g = m$; berme $m \geq n$
- Sylvesterova matice je $(n+m) \times (n+m)$ matice $M(f,g)$, jejíž prvních m řádků má tvar

$$(\ldots, 0, f_n, f_{n-1}, \ldots, f_0, 0, \ldots)$$

- a zbylých n řádků tvar

$$(\ldots, 0, g_m, g_{m-1}, \ldots, g_0, 0, \ldots)$$

- Rezultant polynomů f, g je $\operatorname{res}(f,g) = \det M(f,g)$

Rezultant I

- $\deg f = n$, $\deg g = m$; berme $m \geq n$
- Sylvesterova matice je $(n+m) \times (n+m)$ matice $M(f,g)$, jejíž prvních m řádků má tvar

$$(\ldots, 0, f_n, f_{n-1}, \ldots, f_0, 0, \ldots)$$

- a zbylých n řádků tvar

$$(\ldots, 0, g_m, g_{m-1}, \ldots, g_0, 0, \ldots)$$

- Rezultant polynomů f, g je $\operatorname{res}(f,g) = \det M(f,g)$

Rezultant I

- $\deg f = n$, $\deg g = m$; berme $m \geq n$
- Sylvesterova matice je $(n+m) \times (n+m)$ matice $M(f,g)$, jejíž prvních m řádků má tvar

$$(\ldots, 0, f_n, f_{n-1}, \ldots, f_0, 0, \ldots)$$

- a zbylých n řádků tvar

$$(\ldots, 0, g_m, g_{m-1}, \ldots, g_0, 0, \ldots)$$

- Rezultant polynomů f, g je $\operatorname{res}(f,g) = \det M(f,g)$

Rezultant I

- $\deg f = n$, $\deg g = m$; berme $m \geq n$
- Sylvesterova matice je $(n+m) \times (n+m)$ matice $M(f,g)$, jejíž prvních m řádků má tvar

$$(\ldots, 0, f_n, f_{n-1}, \ldots, f_0, 0, \ldots)$$

- a zbylých n řádků tvar

$$(\ldots, 0, g_m, g_{m-1}, \ldots, g_0, 0, \ldots)$$

- Rezultant polynomů f, g je $\operatorname{res}(f,g) = \det M(f,g)$

Rezultant I

- $\deg f = n$, $\deg g = m$; berme $m \geq n$
- Sylvesterova matice je $(n+m) \times (n+m)$ matice $M(f,g)$, jejíž prvních m řádků má tvar

$$(\ldots, 0, f_n, f_{n-1}, \ldots, f_0, 0, \ldots)$$

- a zbylých n řádků tvar

$$(\ldots, 0, g_m, g_{m-1}, \ldots, g_0, 0, \ldots)$$

- Rezultant polynomů f, g je $\operatorname{res}(f,g) = \det M(f,g)$

Rezultant II

Příklad: $\mathrm{res}(x^2 - 5x + 6, x - 6)$ v $\mathbb{Z}[x]$

$$\det \begin{pmatrix} 1 & -5 & 6 \\ 1 & -6 & 0 \\ 0 & 1 & -6 \end{pmatrix} = 36 + 6 - 30 = 12$$

Theorem (Sylvesterovo kritérium)

Buď R gaussovský, Q jeho podílové těleso, f, g stupně > 1 nad R. PNTJE

1. *f, g jsou soudělné v $Q[x]$*
2. $\mathrm{res}(f, g) = 0$

Rezultant II

Příklad: $\mathrm{res}(x^2 - 5x + 6, x - 6)$ v $\mathbb{Z}[x]$

$$\det \begin{pmatrix} 1 & -5 & 6 \\ 1 & -6 & 0 \\ 0 & 1 & -6 \end{pmatrix} = 36 + 6 - 30 = 12$$

Theorem (Sylvesterovo kritérium)

Buď R gaussovský, Q jeho podílové těleso, f, g stupně > 1 nad R. PNTJE

1. *f, g jsou soudělné v $Q[x]$*
2. $\mathrm{res}(f, g) = 0$

Rezultant II

Příklad: $\mathrm{res}(x^2 - 5x + 6, x - 6)$ v $\mathbb{Z}[x]$

$$\det \begin{pmatrix} 1 & -5 & 6 \\ 1 & -6 & 0 \\ 0 & 1 & -6 \end{pmatrix} = 36 + 6 - 30 = 12$$

Theorem (Sylvesterovo kritérium)

Buď R gaussovský, Q jeho podílové těleso, f, g stupně > 1 nad R. PNTJE

1. *f, g jsou soudělné v $Q[x]$*
2. $\mathrm{res}(f, g) = 0$

Rezultant II

Příklad: $\mathrm{res}(x^2 - 5x + 6, x - 6)$ v $\mathbb{Z}[x]$

$$\det \begin{pmatrix} 1 & -5 & 6 \\ 1 & -6 & 0 \\ 0 & 1 & -6 \end{pmatrix} = 36 + 6 - 30 = 12$$

Theorem (Sylvesterovo kritérium)

Buď R gaussovský, Q jeho podílové těleso, f, g stupně > 1 nad R. PNTJE

1. *f, g jsou soudělné v $Q[x]$*
2. $\mathrm{res}(f, g) = 0$