

Soustavy polynomiálních rovnic s konečným počtem řešení

Gröbnerova báze a Buchbergerův algoritmus

Základní definice

Definice 9.1. • *Monomem* rozumíme polynom s jediným členem, u něhož je koeficient 1.

- Pro *lexikografické uspořádání*, kde $x_1 > x_2 > \dots > x_n$ klademe

$$x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} > x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \Leftrightarrow \exists i \in \{1, 2, \dots, n\} \forall j < i: (a_j = b_j \wedge a_i > b_i).$$

- Vedoucím monomem polynomu f rozumíme monom, který se v f vyskytuje (s nenulovým koeficientem) a je největší v daném uspořádání. Značíme $\text{LM } f$.
- Vedoucím koeficientem rozumíme (nenulový) koeficient u vedoucího monomu. Značíme $\text{LC } f$.
- Vedoucím členem rozumíme součin vedoucího monomu s vedoucím koeficientem. Značíme $\text{LT } f$.
- Necht' f, g jsou polynomy. *S-polynomem* polynomů f, g rozumíme polynom daný předpisem

$$S(f, g) = \frac{[\text{LM } f, \text{LM } g]}{\text{LT } f} \cdot f - \frac{[\text{LM } f, \text{LM } g]}{\text{LT } g} \cdot g,$$

kde monom $[\text{LM } f, \text{LM } g]$ je nejmenší společný násobek vedoucích monomů polynomů f a g .

Algoritmus

Vstup: $f_1, \dots, f_r$

Výstup: Gröbnerova báze

1. Pro $i < j$ spočítáme $S(f_i, f_j)$.
2. Pokud dostaneme nenulový polynom, budeme od něj postupně odečítat vhodné násobky báзовých polynomů tak, abychom při každém odečtení přesně zrušili vedoucí člen. Pokud další odečtení není možné (tj. žádný vedoucí monom báзовých polynomů nedělí vedoucí monom redukovaného polynomu) a vzniklý polynom je nenulový, přidáme jej do báze.
3. Provádíme postupně pro všechny dvojice $i < j$ (tedy počítáme S -polynomy i pro ty nově přidané). Skončíme ve chvíli, kdy všechny S -polynomy jsme schopni pomocí báзовých zredukovat na nulu.

Definice 9.2. Výsledné množině polynomů budeme říkat *Gröbnerova báze*. Řekneme navíc, že tato báze je *redukováná*, jestliže žádný monom libovolného polynomu není dělitelný vedoucím monomem jiného polynomu.

Usnadnění výpočtu

V rámci provádění algoritmu si můžeme práci usnadnit následujícím způsobem

- Pro každou dvojici (i, j) stačí počítat polynom $S(f_i, f_j)$ pouze jednou.
- Pořadí, ve kterém počítáme S -polynomy není fixní. Volíme proto nejprve takové dvojice, aby byl příslušný S -polynom co možná nejmenší v našem uspořádání (můžeme ušetřit desítky zbytečných polynomů v nereduované bázi, čemuž odpovídá i několik hodin práce, pokud počítáme pouze na papíře).
- Mají-li polynomy nesoudělné vedoucí koeficienty, nemusíme počítat příslušný S -polynom. Po redukci pomocí polynomů, ze kterých byl S -polynom tvořen, nám vždy vyjde nula.
- Pokud mají dva polynomy stejný vedoucí monom (tj. S -polynom vznikne jen jako jejich rozdíl s případným vynásobením číselnou konstantou) a některý z nich jsme ještě nepoužili při žádné redukci, můžeme tento polynom z báze zcela vyřadit a dát místo něj příslušný S -polynom (respektive ten, který dostaneme po jeho redukci).
- Pokud nám jde pouze o hledání řešení soustavy, nepotřebujeme nutně (redukovanou) Gröbnerovu bázi, ale stačí nám, když obdržíme nějaký polynom o jedné proměnné. Je-li množina řešení soustavy konečná, vždy po nějaké době dostaneme dostatečně malý polynom v lexikografickém uspořádání, který bude polynomem o jedné (té nejmenší) proměnné.

Příklady

Příklad 9.1. Nalezněte (redukovanou) Gröbnerovu bázi a pomocí ní vyřešte soustavu

$$\begin{aligned}x^3 - 2xy &= 0, \\ x^2y + x - 2y^2 &= 0.\end{aligned}$$

Příklad 9.2. Řešte soustavu

$$\begin{aligned}x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1\end{aligned}$$

Příklad 9.3. Řešte soustavu

$$\begin{aligned}x^2 + y^2 + z &= 2 \\ x + y^2 + z^2 &= 2 \\ x^2 + y + z^2 &= 2\end{aligned}$$

Příklad 9.4. Dokažte, že nulové body původních (zadaných) polynomů a polynomů Gröbnerovy (respektive redukované Gröbnerovy) báze jsou stejné. Tedy soustava vzniklá z nalezené báze je ekvivalentní soustavě původní.

***Příklad 9.5.** Řešte soustavu

$$\begin{aligned}xy + yz &= 1, \\ yz + zw &= 1, \\ zw + wx &= 1, \\ wx + xy &= 1\end{aligned}$$