Algoritmy na polynomech, cvičení 4

borysek@karlin.mff.cuni.cz
https://karlin.mff.cuni.cz/~borysek/

14. listopadu 2024

1. Nechť R je Gröbnerova báze ideálu $I < T[x_1, \ldots, x_k]$ vůči $<_{LEX}$ $x_1 < \ldots < x_k$. Eliminační lemma říká, že pro každé $i = 1, \ldots, k$ je

$$I \cap T[x_1, \ldots, x_i] = \langle R \cap T[x_1, \ldots, x_i] \rangle_{T[x_1, \ldots, x_i]}.$$

   Dokažte, že $R \cap T[x_1, \ldots, x_i]$ je navíc Gröbnerova báze ideálu $I \cap T[x_1, \ldots, x_i]$.

2. Nechť T je algebraicky uzavřené těleso, $R \subset T[x_1, \ldots, x_k]$ Gröbnerova báze vzhledem k $<_{LEX}$ s $x_1 < \cdots < x_k$. Dokažte, že pak $V(R)$ je konečná $\iff$ pro každé $i = 1, \ldots, k$ existuje polynom $f_i \in R$ tak, že $\mathrm{lt}(f_i) = x_i^n$ pro nějaké $n \in \mathbb{N}_0$ (speciálně $f \in T[x_1, \ldots, x_i]$).

   Poznámka. Uvědomte si, jak lze pomocí tohoto tvrzení rozhodnout, zda je $V(R)$ konečná, a poté spočítat všechny její prvky, máme-li po ruce orákulum, které umí spočítat kořeny polynomů v jedné proměnné.

3. Kolik řešení má následující soustava v $\mathbb{Q}$ a v $\mathbb{C}$? Řešte pomocí Gröberových bazí. Můžete si pomoci `SageMath`.

   (a)

$$\begin{aligned} 1 + 2x^2 + y^2 + 4x^2y^2 + 2x^2y^4 &= 0 \\ xy^2 + xy^4 &= 0. \end{aligned}$$

   (b)

$$\begin{aligned} x^2 - 2xy^2 + 1 &= 0 \\ xy - 2y^2 + x &= 0. \end{aligned}$$

4. Nalezněte všechna řešení nad $\mathbb{Q}$ následující soustavy. Řešte pomocí Gröberových bazí s $<_{LEX}$ $x < y < z$. Můžete si pomoci `SageMath`.

$$\begin{aligned} xy^2 - y^2 - xy + y + x^2 - x &= 0 \\ yz + xy^2 - y^2 - xy + y - 1 &= 0 \\ yz - 1 &= 0 \end{aligned}$$

5. Nechť $T \leq S$ jsou tělesa. Nechť $g, f_1, \ldots, f_n \in T[x_1, \ldots, x_k]$ a nechť existují $h_1, \ldots, h_n \in S[x_1, \ldots, x_k]$ tak, že $\sum_{i=1}^n h_i f_i = g$. S pomocí Gröbnerových bazí dokažte, že pak existují $c_1 \ldots, c_n \in T[x_1, \ldots, x_k]$ tak, že $\sum_{i=1}^n c_i f_i = g$. Tedy že pokud $g \in \langle f_1, \ldots, f_n \rangle_{S[x_1, \ldots, x_k]}$, pak i $g \in \langle f_1, \ldots, f_n \rangle_{T[x_1, \ldots, x_k]}$.
   Speciálně $1 \in \langle f_1, \ldots, f_n \rangle_{S[x_1, \ldots, x_k]} \iff 1 \in \langle f_1, \ldots, f_n \rangle_{T[x_1, \ldots, x_k]}$.

6. Ukažte, že problém určit zda polynom $p(\overline{x})$ náleží danému ideálu $I \leq \mathbb{Q}[\overline{x}]$ je NP-těžký, pomocí redukce SATu na tento problém. Nápověda: Nejprve si to rozmyslete pro situaci v $\mathbb{C}[\overline{x}]$. Může se hodit Důsledek 22.3 ze skript.

   Poznámka. Poznamenejme, že problém náležení ideálu je dokonce EXPSPACE-úplný, a proto neleží v NP.

7. Nechť $T \leq S$ jsou tělesa a nechť navíc T je algebraicky uzavřené. Mějme $f_1, \ldots, f_n \in T[x_1, \ldots, x_k]$. Ukažte, že je-li $V(f_1, \ldots, f_n)_T = \emptyset$, pak i $V(f_1, \ldots, f_n)_S = \emptyset$. Tedy pokud soustava nemá řešení v algebraicky uzavřeném tělese, pak nemá řešení v žádném jiném nadtělese.

8. Nechť T je těleso a $A \subset T^k$ konečná. Ukažte, že pak existují polynomy $f_1, \ldots, f_k$ tak, že $f_i \in T[x_1, \ldots, x_i]$ a $A = V(f_1, \ldots, f_k)$. Tedy A lze popsat jako řešení soustavy rovnic

$$\begin{aligned} f_1(x_1) &= 0 \\ f_2(x_1, x_2) &= 0 \\ &\vdots \\ f_k(x_1, x_2, \ldots, x_k) &= 0 \end{aligned}$$

   Nápověda: interpolace ve více proměnných.

9. Vyřešte následující nelineární optimalizační problém pomocí Lagrangeových multiplikátorů: Najděte všechna maxima a minima polynomu $f = x^2y - 2xy + y + 1$ na jednotkové kružnici $S = \{(u, v) \in \mathbb{R}^2 : \ g(u, v) = 0\}$, kde $g(u, v) = x^2 + y^2 - 1$. Nápověda: Vytvořte systém polynomiálních rovnic

$$g = 0 \quad \text{a} \quad \nabla f - z\nabla g = 0,$$

   kde z je nová proměnná. Spočtěte Gröbnerovu bázi ideálu generovaného těmito rovnicemi vzhledem k $< LEX$ s $z > x > y$. Z toho již nalezněte body extrémů na S. Můžete si pomoci `Sagemath`.

10. Nechť $T \leq S$ jsou tělesa, $M \in T^{m \times n}$, $b \in T^m$ a nechť má soustava lineárních rovnic $Mx = b$ řešení nad S. Ukažte, že pak má řešení i nad T.

11. Nechť $f_1, \ldots, f_k \in T[x_1, \ldots, x_m]$, $T \leq S$ tělesa a $s_1, \ldots, s_k \in S$ tak, že $\sum_{i=1}^{k} s_i f_i = 1$. Platí potom, že existují $\{t_1, \ldots, t_k\} \in T$ tak, že:

$$\sum_{i=1}^{k} t_i f_i = 1?$$

12. * Dokažte cvičení 5 bez použití znalosti Gröbnerových bazí, pouze ve stylu předchozího cvičení.

13. Nechť T je algebraicky uzavřené těleso a nechť $f \in T[x, y]$. Ukažte, že pak $V(f)$ je buď prázdná, nebo nekonečná.

14. Nechť $f, g \in T[x, y]$ jsou nesoudělné polynomy. Ukažte, že pak $V(f, g)$ je konečná. Nápověda:

    (a) Uvědomte si, že pomocí ireducibilního rozkladu f a g stačí úlohu vyřešit jen pro f, g ireducibilní a nekonstatní (pro konstatní je to zřejmé.) Navíc si uvědomte, že případ, kdy $f, g \in K[x]$ nebo $f, g \in K[y]$ je také zřejmý. Tedy dále můžete předpokládat, že $\deg_x(f) > 0$ nebo $\deg_x(g) > 0$ a zároveň $\deg_y(f) > 0$ nebo $\deg_y(g) > 0$ (tedy objeví se obě dvě proměnné).

    (b) Dále bez újmy na obecnosti předpokládejte, že $\deg_y(f) > 0$. Uvědomte si, že pak z ireducibility f v $K[x][y]$ plyne ireducibilita i v $K(x)[y]$.

    (c) Dále ukažte, že v $K(x)[y]$ jsou f, g stále nesoudělné. Díky ireducibilitě f stačí ukázat, že f nedělí g.

    (d) Dále využijte toho, že $K(x)[y]$ je již Eukleidovský obor (narozdíl od $K[x, y]$, který není ani obor hlavních ideálů). Využijte Bezoutovy rovnosti a ukažte, že pokud $(x_0, y_0) \in V(f, g)$, pak x_0 může nabývat jen konečně mnoha hodnot.

    (e) Použijte analogický postup pro druhou proměnnou. Pomocí toho dokončete důkaz.

15. * Buď ABC rovnoramenný trojúhelník, kde |AB| = |AC|, nechť H je pata výšky na stranu BC, E kolmý průmět bodu H stranu AB a M střed strany EH. Dokažte, že přímka EC je kolmá na přímku AM. (Pozn. řešení viz skripta).

16. * Dokažte pomocí metody Gröbnerových bází *Simson-Wallaceovu větu*: Buď ABC trojúhelník a P bod na kružnici opsané. Nechť K, L, M značí paty kolmic z bodu P na přímky AB, AC, BC. Pak body K, L, M leží na přímce.