

APLIKACE GEOMETRIE 2

Pomocný učební text

Bohumír Bastl

18. října 2007

Obsah

1	Abstraktní algebraické struktury	3
1.1	Relace, ekvivalence, uspořádání	3
1.2	Grupoid, pologrupa, grupa	7
1.3	Okruh, těleso	10
1.4	Ideály v okruhu	12
2	Voroného diagramy	16
2.1	Úvod	16
2.2	Definice a základní vlastnosti	17
2.3	Algoritmy konstrukce Voroného diagramů	22
2.3.1	Naivní algoritmus	22
2.3.2	Inkrementální algoritmus	23
2.3.3	Algoritmus „rozděl a panuj“	23
2.3.4	Zametací „Fortuneho“ algoritmus	24
2.3.5	Metoda zdvihu	28
2.4	Delaunayho triangulace	28
2.5	Zobecnění Voroného diagramů	29
2.5.1	Změna dimenze	29
2.5.2	Změna metriky	30
2.5.3	Přidání váhy	31
2.6	Aplikace	32
3	Afinní variety a ideály	33
3.1	Polynomy a afinní prostor	33
3.2	Afinní variety	34
3.3	Parametrizace afinních variet	36
3.4	Ideály	37
3.5	Polynomy v jedné proměnné	40
4	Gröbnerovy báze	44
4.1	Úvod	44
4.2	Uspořádání monomů v $k[x_1, \dots, x_n]$	46
4.3	Algoritmus dělení v $k[x_1, \dots, x_n]$	49

4.4	Monomické ideály a Dicksonovo lemma	52
4.5	Věta o Hilbertově bázi a Gröbnerovy báze	53
4.6	Vlastnosti Gröbnerovýchází	56
4.7	Buchbergerův algoritmus	58
4.8	Vylepšení Buchbergerova algoritmu	62
5	Teorie eliminací	68
5.1	Základní věty teorie eliminací	68
5.2	Geometrická interpretace eliminace proměnných	73
6	Aplikace metody Gröbnerovýchází	76
6.1	Řešitelnost soustavy polynomiálních rovnic	76
6.2	Převod parametrického vyjádření afinní variety na implicitní	79
6.3	Automatické dokazování v geometrii	85
6.4	Kótování a variační geometrie	92
6.5	Robotika	98
7	Rezultanty	102
7.1	Rezultanty pro polynomy v jedné proměnné	102
7.1.1	Sylvesterův resultant, dialytická metoda	104
7.1.2	Bézoutův resultant	105
7.2	Rezultanty pro polynomy ve více proměnných	108
7.2.1	Resultant a projekční operátor	109
7.2.2	Sylvesterův resultant pro polynomy ve dvou proměnných	110
7.2.3	Dixonův resultant pro polynomy ve dvou proměnných	112
7.2.4	Matice Sylvesterova typu	117
7.2.5	Macaulayho matice	118
7.2.6	Dixonova matice	119
7.2.7	Dixonova dialytická matice	120
8	Implicitizace křivek a ploch	123
8.1	Implicitizace pomocí Gröbnerovýchází a resultantů	124
8.2	Implicitizace pomocí moving curves a moving surfaces	127
8.3	Implicitizace pomocí polynomiální interpolace	133
8.4	Přímá metoda implicitizace	137

Kapitola 1

Abstraktní algebraické struktury

1.1 Relace, ekvivalence, uspořádání

Pojmy týkající se teorie množin, jako je identické zobrazení, prosté zobrazení, vzájemně jednoznačné zobrazení, inverzní zobrazení atd. jsou dostatečně dobře známy, proto se jimi v tomto textu nebudeme zabývat. Začneme pojmem binární relace.

Definice 1.1.1 *Nechť M je množina, $M \times M$ je množina všech uspořádaných dvojic (a, b) , kde $a, b \in M$. Nechť R je libovolná podmnožina $M \times M$. Potom R definuje na množině M binární relaci takto: jsou-li $a, b \in M$, říkáme, že prvek a je v relaci R s prvkem b a zapisujeme aRb nebo $(a, b) \in R$.*

Studium binárních relací na množině M se tedy neliší od studia podmnožin množiny $M \times M$. Lze tedy mluvit o průniku a sjednocení binárních relací, komplementu $\bar{R}$ k binární relaci R ($\bar{R} = (M \times M) \setminus R$), součinu binárních relací R a S ($(RS)b \iff \exists c \in M : aRc \wedge cSb$) apod. Násobení binárních relací je *asociativní*, tzn.

$$(RS)T = R(ST);$$

obecně ale není *komutativní*.

Jednotková relace E : $aEb \iff a = b$ (jinak řečeno, relace E je dána množinou všech dvojic (a, a) , kde $a \in M$). Zřejmě $E^{-1} = E$ a pro libovolnou relaci R je

$$ER = RE = R.$$

Prázdná relace O : definována prázdnou podmnožinou množiny $M \times M$. Zřejmě pro libovolnou binární relaci R na M platí

$$O \subseteq R \quad \text{a} \quad RO = OR = O.$$

Vlastnosti binárních relací:

1. reflexivita: $aRa, \forall a \in M$ (jinak řečeno $E \subseteq R$),

2. tranzitivita: je-li aRb a bRc , potom aRc (jinak řečeno $RR \subseteq R$),
3. symetrie: je-li aRb , potom bRa (jinak řečeno $R^{-1} = R$),
4. antisymetrie: je-li $aRb \wedge bRa$, potom $a = b$ (jinak řečeno $R \cap R^{-1} \subseteq E$).

Má-li binární relace R libovolnou z těchto vlastností, má inverzí relace R^{-1} tutéž vlastnost.

Pojem binární relace je možné zobecnit. Vezměme n -tou mocninu M^n množiny M , tj. množinu všech uspořádaných n -tic $(a_1, a_2, \dots, a_n)$ prvků množiny M . Každá podmnožina R množiny M^n definuje n -ární relaci (např. ternární relaci).

Definice 1.1.2 *Binární relace, které jsou reflexivní, tranzitivní a symetrické se nazývají ekvivalence (např. rovnost zlomků, kongruence celých čísel podle určitého modulu). Ekvivalence obvykle značíme $\sim$ nebo $\equiv$.*

Ekvivalence definované na množině M velmi úzce souvisejí s rozkladem množiny M na disjunktní třídy. Rozkladem množiny rozumíme soustavu podmnožin M vybraných tak, aby každý prvek M patřil do právě jedné z těchto podmnožin.

Věta 1.1.1 *Každý rozklad Π množiny M definuje na M ekvivalenci.*

Důkaz: (náznak) Jsou-li $a, b \in M$ a položíme-li $a \sim b \iff a$ i b patří do téže třídy rozkladu Π , dostaneme na M binární relaci, která zřejmě vyhovuje všem požadavkům uvedeným v definici ekvivalence. $\square$

Věta 1.1.2 *Každá ekvivalence R na množině M definuje rozklad této množiny.*

Důkaz: Nechť K_a (třída prvku a) je množina všech $x \in M$, pro které aRx . Z vlastností ekvivalence vyplývá:

- reflexivita: $a \in K_a$, tj. množina tříd K_a , $a \in M$ pokrývá celou množinu M .
- symetrie: jestliže $b \in K_a$, potom $a \in K_b$.
- tranzitivita: je-li $b \in K_a \wedge c \in K_b$, potom $c \in K_a$, tj. $K_b \subseteq K_a$. Odtud plyne, že je-li $b \in K_a$, pak $K_b = K_a$, tj. třída je definována libovolným prvkem.

Jsou-li K_a a K_b dvě libovolné třídy s neprázdným průnikem obsahujícím např. prvek c , potom $K_a = K_c$ i $K_b = K_c$, tj. $K_a = K_b$. $\square$

$\implies$ mezi ekvivalencemi na množině M a rozklady množiny M na disjunktní třídy existuje tedy vzájemně jednoznačné zobrazení.

Definice 1.1.3 *Množinu tříd rozkladu, odpovídající dané ekvivalenci R na množině M , budeme označovat M/R a nazývat faktorová množina množiny M podle ekvivalence R . Zobrazení množiny M na faktorovou množinu M/R , v němž obrazem každého prvku $a \in M$ je třída rozkladu, do níž prvek a patří, nazveme přirozené zobrazení M na M/R .*

Definice 1.1.4 *Binární relace, která je reflexivní, tranzitivní a antisymetrická, se nazývá uspořádání. Obvykle se značí $\leq$, je-li $a, b \in M$ a $a \leq b$, říkáme, že a je menší nebo rovno než b , a je před b .*

Je-li $a \leq b$ a $a \neq b$, píšeme $a < b$ a říkáme, že a je menší než b . Binární relace $<$ už není reflexivní.

Je-li na množině M definováno uspořádání, říkáme, že prvky a, b této množiny jsou *srovnatelné*, je-li $a \leq b$ nebo $b \leq a$. Libovolné dva prvky množiny M však *nemusejí* být vůbec srovnatelné — hovoříme pak o *částečném uspořádání*. Např. položíme-li $a \leq b \Leftrightarrow a = b$, dostáváme triviální uspořádání množiny M , v němž různé prvky nejsou srovnatelné.

Uspořádaná množina, jejíž každé dva prvky jsou srovnatelné, se nazývá *úplně uspořádaná množina* nebo *řetězec*.

Příklady úplně uspořádaných množin:

- množina přirozených čísel s přirozeným uspořádáním,
- množina bodů přímky (množina reálných čísel) s přirozeným uspořádáním.

Příklady částečně uspořádaných množin:

- množina všech podmnožin nějaké množiny M s uspořádáním definovaným množinovou inkluzí $\subseteq$,
- množina všech spojitých reálných funkcí definovaných na $\langle 0, 1 \rangle$, jestliže $f \leq g \Leftrightarrow \forall x \in \langle 0, 1 \rangle : f(x) \leq g(x)$,
- množina všech přirozených čísel, jestliže $a \leq b \Leftrightarrow a \perp b$.

Věta 1.1.3 *Každé uspořádání dané množiny M lze rozšířit na úplné uspořádání této množiny, tj. lze najít úplné uspořádání, v němž je dané uspořádání obsaženo (ve smyslu inkluze binárních relací).*

Definice 1.1.5 *Nechť $f : M \rightarrow M'$ je vzájemně jednoznačné zobrazení dvou uspořádaných množin, tzn. pro $a \in M$, $a' \in M'$ je $f(a) = a'$. Jestliže z $a \leq b$, $a, b \in M$ VŽDY plyne $f(a) \leq f(b)$ a obráceně, nazývá se f izomorfismem množin M a M' a o množinách M a M' říkáme, že jsou to izomorfní uspořádané množiny.*

V případech, kdy studujeme jen uspořádání a povaha prvků, z nichž se obě zkoumané množiny skládají, nás nezajímá, lze zřejmě izomorfní množiny ztotožnit.

Definice 1.1.6 *Prvek a uspořádané množiny M nazveme minimálním prvkem této množiny, není-li v M ani jeden prvek x , pro který $x < a$.*

Množina M může zřejmě obsahovat mnoho různých minimálních prvků, nemusí však obsahovat ani jeden takový prvek. Např. množina všech podmnožin množiny M obsahuje jediný minimální prvek — prázdnou množinu. V množině všech neprázdných podmnožin

množiny M jsou minimálními prvky všechny podmnožiny obsahující jediný prvek. Je-li M nekonečná množina, nemá množina všech nekonečných podmnožin žádný minimální prvek.

Pojem minimálního prvku lze využít k zavedení speciální třídy uspořádaných množin. Tato třída je bohatší než třída konečných uspořádaných množin a platí v ní následující věta:

Věta 1.1.4 *Následující tři podmínky jsou ekvivalentní:*

1. Minimální podmínka: *Každá neprázdná podmnožina N uspořádané množiny M obsahuje alespoň jeden (v N) minimální prvek.*
2. Podmínka konečnosti klesajících řetězců: *Každý klesající řetězec prvků uspořádané množiny M*

$$a_1 > a_2 > \dots > a_n > \dots$$

má jen konečný počet prvků. Jinak řečeno, pro každý nerostoucí řetězec

$$a_1 \geq a_2 \geq \dots \geq a_n \geq \dots$$

existuje index n tak, že

$$a_n = a_{n+1} = \dots$$

3. Indukční podmínka: *Všechny prvky uspořádané množiny M mají vlastnost ε , mají-li tuto vlastnost všechny minimální prvky množiny M (pokud existují) a je-li možno dokázat, že prvek a má vlastnost ε z předpokladu, že tuto vlastnost mají všechny prvky menší než a .*

Důkaz: Minimální podmínka $\Rightarrow$ indukční podmínka $\Rightarrow$ podmínka konečnosti klesajících řetězců $\Rightarrow$ minimální podmínka. Podrobněji viz [14], str. 20-21. $\square$

Definice 1.1.7 *Úplně uspořádaná množina, v níž platí minimální podmínka a ovšem též obě ekvivalentní podmínky, se nazývá dobře uspořádaná množina.*

Příkladem dobře uspořádané množiny je množina všech přirozených čísel s přirozeným uspořádáním.

Každá podmnožina dobře uspořádané množiny je dobře uspořádanou množinou. Z definice dobře uspořádané množiny plyne, že obsahuje *jediný* minimální prvek.

Ke každému prvku a dobře uspořádané množiny M existuje *následovník*, tj. prvek, který za a bezprostředně následuje. K prvku a však nemusí existovat bezprostředně předcházející prvek — prvek a pak nazveme *limitním prvkem*.

Věta 1.1.5 *V uspořádané množině platí minimální podmínka právě tehdy, když všechny řetězce (tj. úplně uspořádané množiny) jsou dobře uspořádány.*

Důkaz: Platí-li v uspořádané množině M minimální podmínka, platí i v každé její podmnožině a speciálně v každém řetězci. Obrácené tvrzení plyne z toho, že při formulaci podmínky konečnosti klesajících řetězců, která je s minimální podmínkou ekvivalentní, se mluví jen o řetězcích množiny M . $\square$

V uspořádané množině M lze přejít k *inverznímu* uspořádání. Minimální prvky tohoto inverzního uspořádání jsou potom *maximálními prvky* množiny M v původním uspořádání. Podobně klesající řetězec v inverzním uspořádání nazýváme v původním uspořádání *rostoucí řetězec*. Obecně lze takto z každého pojmu (nebo tvrzení) souvisejícího s uspořádáním odvodit *duální pojem (tvrzení)*.

Jestliže v uspořádané množině M platí minimální podmínka a vezmeme-li v M inverzní uspořádání, dostaneme uspořádanou množinu, v níž platí maximální podmínka. Pro tyto množiny zůstanou správná všechna tvrzení dokázaná o množinách, v nichž platí minimální podmínka, zaměníme-li ovšem relaci $\leq$ za $\geq$ a obráceně.

1.2 Grupoid, pologrupa, grupa

Základem všech pojmů, které studujeme v různých partiích algebry, je pojem *algebraické operace*, přičemž nejprve se omezíme na *binární operace* — v nejširším slova smyslu je to zákon, který některým uspořádaným dvojicím prvků dané množiny M přiřazuje jeden nebo několik prvků množiny M . Nazveme-li tuto operaci *násobení* a uijeme-li obvyklý multiplikativní zápis, vyjadřuje rovnost

$$ab = c,$$

že pro dvojici prvků $a, b \in M$ je součin definován a že jednou z hodnot tohoto součinu je c . Pojem binární algebraické operace je, v tomto širokém slova smyslu, ekvivalentní s pojmem ternární relace na množině M .

Binární algebraickou operaci běžně chápeme v užším slova smyslu — násobení musí být definováno pro *každou* uspořádanou dvojici prvků z M a musí být *jednoznačné*.

Definice 1.2.1 *Každá množina, v níž je dána binární algebraická operace uvedeného typu, se nazývá grupoid.*

Tento pojem je stále příliš široký. Užší je již pojem pologrupy, který již má různé aplikace.

Definice 1.2.2 *Grupoid, v němž platí asociativní zákon, se nazývá pologrupa.*

V pologrupě tedy pro libovolné prvky a, b, c platí

$$(ab)c = a(bc).$$

Odtud plyne, že součin abc tří libovolných prvků pologrupy je určen jednoznačně. Z toho ihned plyne, že pro všechna přirozená n je součin $a_1 \cdot a_2 \cdot \dots \cdot a_n$ libovolných n prvků pologrupy (v uvedeném pořadí) také jednoznačně určeným prvkem pologrupy.

Ještě užší je jeden z nejdůležitějších algebraických pojmů — grupa.

Definice 1.2.3 *Pologrupa, v níž existují inverzní operace, tj. v níž pro libovolné prvky a, b má každá z rovnic*

$$ax = b, ya = b \quad (1.1)$$

jednoznačné řešení, se nazývá grupa.

Protože rovnice (1.1) mají jednoznačné řešení, lze v grupě *krátit zleva nebo zprava*. Je-li

$$ab_1 = ab_2 \quad \text{nebo} \quad b_1a = b_2a,$$

je $b_1 = b_2$.

Řešení x a y rovnic (1.1) nemusí být v libovolné grupě identická. O uvažované operaci totiž nepředpokládáme, že je komutativní, takže součin může záviset na pořadí faktorů.

Definice 1.2.4 *Grupa (pologrupa, grupoid), pro jejíž každé dva prvky a, b platí komutativní zákon*

$$ab = ba,$$

se nazývá Abelova nebo komutativní.

Věta 1.2.1 *V každé grupě G existuje právě jeden prvek e tak, že*

$$ae = ea = a$$

pro všechna $a \in G$. Prvek e se nazývá jednotkový prvek grupy G a obvykle se označuje symbolem 1 .

Důkaz: Z definice grupy plyne, že pro každý prvek $a \in G$ existuje v G právě jeden prvek e'_a tak, že $ae'_a = a$. Je-li b libovolný jiný prvek grupy G a y řešení rovnice $ya = b$, plyne z asociativního zákona

$$be'_a = (ya)e'_a = y(ae'_a) = ya = b,$$

takže $e'_b = e'_a$. Prvek e'_a tedy nezávisí na volbě prvku a a můžeme ho označit e' . Je tudíž

$$ae' = a \quad \text{pro všechna} \quad a \in G. \quad (1.2)$$

Analogicky dokážeme existenci a jednoznačnost takového prvku e'' , že

$$e''a = a \quad \text{pro všechna} \quad a \in G. \quad (1.3)$$

Aplikujeme-li identity (1.2) a (1.3) na součin $e''e'$, dostaneme $e''e' = e''$ i $e''e' = e'$, z čehož plyne $e'' = e'$. Tím je věta dokázána. $\square$

Lemma 1.2.2 *Ke každému prvku a grupy G existuje právě jeden prvek a^{-1} tak, že*

$$aa^{-1} = a^{-1}a = 1.$$

Prvek a^{-1} se nazývá inverzní prvek k prvku a .

Důkaz: Z definice grupy plyne, že existují jednoznačně definované prvky a' a a'' tak, že

$$aa' = 1, \quad a''a = 1.$$

Užitím asociativního zákona dostaneme

$$\begin{aligned} a''aa' &= a''(aa') = a'' \cdot 1 = a'', \\ a''aa' &= (a''a)a' = 1 \cdot a' = a', \end{aligned}$$

takže $a'' = a'$. ■

Ověření, že daná pologrupa je grupou, často usnadňuje následující věta.

Věta 1.2.3 *Pologrupa G je grupou právě tehdy, když v G existuje alespoň jeden pravý jednotkový prvek e tak, že*

$$ae = a \quad \text{pro všechna } a \in G,$$

přičemž e lze vybrat tak, že ke každému $a \in G$ existuje alespoň jeden pravý inverzní prvek a^{-1} , pro který

$$aa^{-1} = e.$$

Důkaz: Viz [14], str. 28-29. □

Poznámka 1.2.4 *Někdy, zvláště při studiu Abelových grup, užíváme aditivní zápis místo multiplikativního. Grupové operaci pak říkáme sčítání a součet zapisujeme $a + b$, jednotkovému prvku grupy říkáme nulový prvek a označujeme jej symbolem 0 . Místo o inverzním prvku mluvíme o opačném prvku a značíme jej $-a$. Inverzní operace se v aditivním zápise Abelových grup nazývá odečítání.*

Příklady:

1. celá čísla s operací sčítání — Abelova grupa,
2. racionální čísla s operací sčítání — Abelova grupa,
3. reálná (komplexní) čísla s operací sčítání — Abelova grupa,
4. přirozená čísla s operací sčítání — pologrupa (nelze odečítat),
5. multiplikativní grupy čísel — nutno vynechat 0 , protože nulou nelze dělit, např. nenulová racionální čísla, kladná racionální čísla — Abelova grupa,
6. množina všech celých čísel s operací násobení, množina všech celých nezáporných čísel s operací násobení, přirozená čísla s operací násobení — pologrupy.

Příklady nekomutativních grup a pologrup:

1. regulární čtvercové matice n -tého stupně ($n \geq 2$) s reálnými prvky vzhledem k operaci násobení matic — nekomutativní grupa.

1.3 Okruh, těleso

Druhým nejdůležitějším algebraickým pojmem je, vedle pojmu grupy, okruh.

Definice 1.3.1 Okruhem nazýváme množinu R , v níž jsou definovány dvě binární algebraické operace — sčítání a násobení, přičemž vzhledem ke sčítání je R Abelovou grupou — je to tzv. aditivní grupa okruhu R , a vzhledem k násobení je R grupoidem — je to tzv. multiplikativní grupoid okruhu R . Násobení souvisí se sčítáním distributivními zákony

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca.$$

Je-li násobení v okruhu R asociativní, hovoříme o asociativním okruhu a jeho multiplikativní pologrupě.

Je-li násobení v okruhu R asociativní i komutativní, říkáme, že okruh je asociativní a komutativní.

V každém okruhu platí distributivní zákony i pro rozdíl, tj. platí

$$a(b - c) = ab - ac, \quad (b - c)a = ba - ca.$$

Příklady okruhů:

1. celá čísla — asociativní a komutativní okruh,
2. čtvercové matice n -tého stupně ($n \geq 2$) s reálnými prvky — asociativní okruh, nekomutativní,
3. vektory v $\mathbb{E}_3$ s operacemi skládání vektorů a vektorový součin — neasociativní a nekomutativní okruh.

Definice 1.3.2 Nenulové prvky a, b , jejichž součin je roven nulovému prvku, tzn.

$$ab = 0,$$

se nazývají dělitelé nuly.

Některé okruhy obsahují dělitele nuly, jsou to např. okruhy matic. Je-li R libovolný okruh, lze obecně studovat všechny možné čtvercové matice n -tého stupně s prvky z okruhu R . Definujeme-li obvyklým způsobem sčítání a násobení matic, dostaneme okruh, který je asociativní, pokud je asociativní okruh R . Nulovým prvkem je nulová matice sestavená z nulových prvků. Tento okruh se nazývá *úplný okruh matic n -tého stupně nad okruhem R* a označujeme ho R_n .

Lemma 1.3.1 Je-li $n \geq 2$ a okruh R neobsahuje pouze nulový prvek, existují v úplném okruhu matic R_n dělitelé nuly.

Důkaz: Je-li totiž a nenulový prvek z okruhu R , nerovná se žádná z matic

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix}$$

nulové matici, ale jejich součin je nulovou maticí. ■

Dalším příkladem okruhů obsahujících dělitele nuly jsou *úplně okruhy funkcí*. Mějme libovolnou množinu M a libovolný okruh R . Utvořme množinu všech možných funkcí na M , jejichž hodnoty jsou v R , tj. všech možných zobrazení f množiny M do okruhu R . Definujeme-li násobení a sčítání funkcí jako obvykle vzorci

$$\begin{aligned} (f+g)(x) &= f(x) + g(x), \\ (fg)(x) &= f(x)g(x), \end{aligned}$$

stane se tato množina funkcí okruhem, který je asociativní nebo komutativní, pokud je výchozí okruh R asociativní nebo komutativní. Tento okruh se nazývá *úplný okruh funkcí nad M s hodnotami v okruhu R* . Je-li M množina bodů číselné osy a R množina všech reálných čísel, je náš okruh obyčejným okruhem všech reálných funkcí reálné proměnné.

Lemma 1.3.2 *Každý úplný okruh funkcí s hodnotami v okruhu R nad množinou M obsahující alespoň dva prvky, má dělitele nuly, jestliže R obsahuje alespoň jeden nenulový prvek.*

Důkaz: Nulovým prvkem je v tomto okruhu nulová funkce, identicky rovná nulové nulovému prvku ve všech bodech M . Rozložíme-li množinu M na dvě neprázdné disjunktní množiny A a B , existují zřejmě dvě takové nenulové funkce f a g , že f je rovna nulové funkci na A a g na B . Součin fg je potom zřejmě nulovou funkcí. ■

Definice 1.3.3 *Asociativní a komutativní okruh, který neobsahuje dělitele nuly, se nazývá obor integrity.*

Mezi obory integrity patří speciálně všechny číselné okruhy.

Je-li R libovolný asociativní a komutativní okruh, je možné studovat všechny polynomy

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad n \geq 0$$

proměnné x s koeficienty $a_0, a_1, \dots, a_n \in R, a_n \neq 0$, n je stupeň polynomu. Definujeme-li sčítání a násobení standardně, dostaneme okruh, který se nazývá *okruh polynomů $R[x]$* . Tento okruh je asociativní a komutativní.

Analogicky definujeme okruh $R[x_1, \dots, x_n]$ libovolného konečného počtu proměnných. Je to vlastně okruh polynomů proměnné x_n nad okruhem $R[x_1, \dots, x_{n-1}]$.

Lze mluvit i o okruhu polynomů libovolné nekonečné množiny proměnných nad R , předpokládáme-li, že každý konkrétní polynom závisí jen na konečně mnoha z těchto proměnných.

Věta 1.3.3 *Je-li R oborem integrity, je každý okruh polynomů nad R také oborem integrity.*

Důkaz: Tvrzení plyne z toho, že jsou-li f a g nenulové polynomy nad okruhem R , který nemá dělitele nuly, je stupeň součinu fg roven součtu stupňů obou faktorů, takže součin nemůže být nulovým polynomem. K okruhům polynomů libovolného konečného počtu proměnných přejdeme jednoduše indukcí a u okruhů polynomů s nekonečnou množinou proměnných stačí uvážit, že každý polynom je polynomem jen v konečně mnoha proměnných. $\square$

Definice 1.3.4 *Okruh, jehož nenulové prvky tvoří grupu vzhledem k násobení, je nutně asociativní a nazývá se těleso.*

Grupa jeho nenulových prvků je multiplikativní grupou tohoto tělesa.

Těleso s komutativním násobením se nazývá komutativní těleso, těleso s nekomutativním násobením se nazývá nekomutativní těleso.

Příklady těles: těleso racionálních čísel, reálných čísel, komplexních čísel.

Z definice tělesa přímo plyne, že těleso neobsahuje dělitele nuly. V každém tělese je jednotkový prvek, neboť jednotkový prvek multiplikativní grupy je jednotkovým prvkem tělesa.

Konečně v každém tělese má každá z rovnic

$$ax = b, \quad ya = b, \quad \text{kde } a \neq 0$$

právě jedno řešení.

1.4 Ideály v okruhu

Definice 1.4.1 *Neprázdňá podmnožina I okruhu R je ideálem, jestliže:*

1. $\forall a, b \in I$ platí, že $a - b \in I$,
2. je-li $a \in I$ a $r \in R$, potom $ar \in I$.

Ideály každého okruhu jsou: sám okruh R a nulový ideál O , obsahující jen nulový prvek. Okruh, který nemá jiné ideály, se nazývá *jednoduchý*. Příklady jednoduchých okruhů jsou:

1. každé těleso,
2. okruh s dělením (může obsahovat dělitele nuly),
3. úplný okruh matic R_n libovolného stupně n nad každým okruhem s dělením R .

Nevyžadujeme-li v definici ideálu, aby pro každé $a \in I$ a každé $r \in R$ patřily do I oba součiny ar i ra , ale požadujeme-li jen, aby do I patřil buď součin ar nebo ra , dojdeme k pojmu *jednostranného ideálu*, konkrétně k *pravému ideálu*, když $ra \in I$, a k *levému ideálu*,

když $ar \in I$. V komutativních okruzích je ale každý jednostranný ideál ideálem (nebo, jak se také někdy říká, oboustranným ideálem).

Příklady ideálů:

1. násobky celého čísla: $\langle 2 \rangle$, $\langle 7 \rangle$, $\langle 9 \rangle$,
2. násobky daného polynomu: $\langle x + 1 \rangle$.

Definice 1.4.2 *Nechť R je obor integrity s jednotkovým prvkem. Je-li $a \in R$, je množina*

$$\langle a \rangle = \{ar; r \in R\},$$

tj. množina prvků tvaru $ar, r \in R$, ideálem okruhu R a nazývá se hlavní ideál generovaný prvkem a .

Definice 1.4.3 *Jsou-li všechny ideály okruhu R hlavní, tj. každý z nich je generovaný některým prvkem, říkáme, že R je okruhem hlavních ideálů.*

Definice 1.4.4 *Řekneme, že obor integrity R s jednotkovým prvkem je Eukleidovým okruhem, lze-li každému nenulovému prvků $a \in R$ přiřadit nezáporné celé číslo $n(a)$ a kromě toho k libovolným prvkům $a, b \in R, b \neq 0$ lze v okruhu R najít prvky q a r tak, že*

$$a = bq + r,$$

přičemž buď $r = 0$, nebo $n(r) < n(b)$.

Příkladem Eukleidova okruhu je např. $\mathbb{R}[x], \mathbb{Z}$.

Věta 1.4.1 *Každý Eukleidův okruh je okruhem hlavních ideálů.*

Důkaz: Zvolme v R ideál I . Je-li $I = O$, je $I = \langle 0 \rangle$. Je-li $I \neq O$, označme a_0 jeden z těch nenulových prvků z I , jemuž je přiřazeno $n(a_0)$ tak, že $n(a_0) \leq n(a)$ pro všechny nenulové prvky z I . Podle předpokladu lze pro každé $a \in I$ najít v R takové prvky q a r , že

$$a = a_0q + r.$$

Je-li $r \neq 0$, je $n(r) < n(a_0)$, ale

$$r = a - a_0q \in I,$$

což je ve sporu s tím, jak jsme vybrali prvek a_0 . Proto je $r = 0$, takže $a = a_0q$ a I je hlavní ideál generovaný prvkem a_0 . $\square$

Eukleidovým okruhem je tedy okruh celých čísel $\mathbb{Z}$, úlohu $n(a)$ v něm hraje absolutní hodnota $|a|$ čísla a , a také okruh polynomů $P[x]$ nad tělesem P , ve kterém hraje úlohu $n(a)$ stupeň polynomu. Okruhy $\mathbb{Z}$ a $P[x]$ jsou tedy okruhy hlavních ideálů. V každém Eukleidově okruhu je možné najít největšího společného dělitele dvou prvků známým Eukleidovým algoritmem.

Definice 1.4.5 Ideál I je konečně generovaný, jestliže existují $a_1, \dots, a_t \in I$ takové, že

$$I = \langle a_1, \dots, a_t \rangle = \left\{ \sum_{i=1}^t h_i a_i : h_1, \dots, h_t \in R \right\}.$$

Definice 1.4.6 Součinem IJ ideálů $I, J \subseteq R$ nazveme ideál generovaný všemi možnými součiny tvaru ab , kde $a \in I$ a $b \in J$.

Poznamenejme, že samotné součiny netvoří výsledný ideál, jsou pouze generátory výsledného ideálu, který tvoří součin těchto ideálů.

Lemma 1.4.2 Necht' $I = \langle a_1, \dots, a_t \rangle$ a $J = \langle b_1, \dots, b_s \rangle$. Potom IJ je generováno množinou všech součinů generátorů ideálů I a J , tj.

$$IJ = \langle f_i g_j : 1 \leq i \leq t, 1 \leq j \leq s \rangle.$$

Důkaz: Zřejmé. ■

Jednou z možných aplikací součinu ideálů je, pokud se omezíme na polynomiální ideály, úzká souvislost mezi součinem ideálů a sjednocením afinních variet (pojem afinní variety, viz část věnovaná afinním varietám).

Definice 1.4.7 Ideál L je prvoideálem právě tehdy, když pro libovolné ideály I, J z inkluze $IJ \subseteq L$ plyne buď $I \subseteq L$ nebo $J \subseteq L$. Jinak řečeno, jestliže $a \cdot b \in L$, potom $a \in L \vee b \in L$.

Pro příklad můžeme opět uvést vztah k afinním varietám. Prvoideál v tomto případě odpovídá ireducibilní varietě V (vyjádříme-li ireducibilní varietu V ve tvaru $V = V_1 \cup V_2$, kde V_1 a V_2 jsou opět afinní variety, potom $V_1 = V$ nebo $V_2 = V$). Podobným příkladem prvoideálů, uvažujeme-li tentokrát ideály nad číselnými okruhy, mohou být ideály generované prvočíslly.

Definice 1.4.8 Maximálním ideálem I je vlastní ideál v okruhu R (tj. ideál různý od R), který přidáním libovolného prvku z $R \setminus I$ přejde na celý okruh R .

Maximální ideál I je tedy největším možným vlastním ideálem v okruhu R . Příkladem maximálního ideálu, položíme-li $R = k[x_1, \dots, x_n]$ a k je těleso, je ideál

$$I = \langle x_1 - a_1, \dots, x_n - a_n \rangle,$$

kde $a_1, \dots, a_n \in k$.

Věta 1.4.3 Každý maximální ideál je prvoideálem.

Důkaz: Předpokládejme, že I je vlastní ideál, který není prvoideálem a že $ab \in I$, přičemž $a \notin I$ a $b \notin I$. Uvažujme ideál $\langle a \rangle + I$. Potom $I \subsetneq \langle a \rangle + I$, protože $a \notin I$. Navíc, jestliže by platilo, že $\langle a \rangle + I = R$, potom $1 = ca + h$ pro nějaké $c \in R$ a $h \in I$. Vynásobením

b dostaneme $b = cfb + hb \in I$, což je ve sporu s volbou b . Tedy, $I + \langle a \rangle$ je vlastní ideál obsahující I a tedy I není maximální. $\square$

V okruhu hlavních ideálů jsou prvoideály právě ty ideály, které mají tvar $\langle p \rangle$, kde p je prvočinitel.

V dalším stručně zmíníme rozkladové věty pro ideály, které popisují strukturu ideálů.

Definice 1.4.9 Primární ideál je takový ideál, ve kterém platí:

$$a \cdot b \in I \wedge a \notin I \Rightarrow \exists q : b^q \in I.$$

Je zřejmé, že prvoideály jsou také primárními ideály, naopak to ale samozřejmě neplatí.

Definice 1.4.10 Prvoideál asociovaný k primárnímu ideálu je definován vztahem

$$\bar{I} = \{a \in R : \exists q : a^q \in I\}.$$

Definice 1.4.11 Dělitel ideálu A je „nadmnožina“, která je ideálem, tj. $B \supseteq A$. Pravým dělitelem ideálu A je potom ideál B takový, že $B \supset A$.

Např. $\langle 2 \rangle \mid \langle 4 \rangle$, $\langle x+1 \rangle \mid \langle x^2-1 \rangle$.

Definice 1.4.12 Ireducibilní ideál je ideál, který nelze vyjádřit jako průnik pravých dělitelů.

Např. ideál $\langle x^2-1 \rangle = \langle x-1 \rangle \cap \langle x+1 \rangle$ není ireducibilním ideálem, zatímco ideály $\langle x-1 \rangle$ a $\langle x+1 \rangle$ jsou ireducibilní ideály.

Věta 1.4.4 (1. rozkladová) Každý ideál lze vyjádřit jako průnik konečného počtu ireducibilních ideálů.

Věta 1.4.5 Každý ireducibilní ideál je primární.

Pozor, obecně neplatí opak! Např. ideál $\langle x^2, xy, y^k \rangle$ je reducibilní a primární ideál, což vyplývá z toho, že prvky ideálu nemají absolutní členy a z toho, že lze tento ideál přepsat do tvaru

$$\langle x^2, xy, y^k \rangle = \langle x^2, y \rangle \cap \langle x, y^k \rangle.$$

Poznámka 1.4.6 Rozklad lze „optimalizovat“ eliminací skupin primárních ideálů se stejným přidruženým prvoideálem, tzn. rozklady nejsou jednoznačné.

Věta 1.4.7 (2. rozkladová) Každý ideál lze vyjádřit jako průnik maximálních primárních ideálů, tzn. $I = \bigcap P_i$, kde P_i jsou maximální primární ideály.

Věta 1.4.8 (O jednoznačnosti) Mějme dva rozklady $[P_1, \dots, P_n]$ a $[Q_1, \dots, Q_m]$ téhož ideálu maximálními primárními ideály. Potom $m = n$ a existuje oindexování (uspořádání) takové, že $\bar{P}_i = \bar{Q}_i$, tj. splývají asociované prvoideály.

Kapitola 2

Voroného diagramy

2.1 Úvod

Předpokládejme, že máte naplánovat umístění nového supermarketu. Musíte zjistit, pro kolik zákazníků bude supermarket atraktivní, aby se dalo odhadnout, zda bude supermarket vydělávat. Pro toto rozhodnutí je nezbytné modelovat chování lidí, potenciálních zákazníků: jak se tedy chovají, kde budou nakupovat?

Obecněji se samozřejmě nemusí jednat jen o supermarkety, ale i o jiná místa (střediska), poskytující různé služby či zboží, přičemž chceme zjistit množství lidí, kteří budou toto středisko využívat. Ve výpočtové geometrii se tato střediska tradičně reprezentují poštovními úřady, proto se tento problém typicky označuje jako *poštovní problém*.

V dalším budeme uvažovat následující zjednodušující předpoklady:

1. Cena služby nebo zboží je stejná ve všech střediscích.
2. Náklady na získání zboží nebo služby = cena zboží či služby + cena dopravy do střediska.
3. Cena dopravy do střediska = Eukleidovská vzdálenost do střediska $\times$ pevná cena za jednotku vzdálenosti.
4. Zákazníci se snaží minimalizovat náklady na získání zboží nebo služby.

Obvykle samozřejmě nejsou všechny tyto předpoklady splněny. Později si ukážeme, jak některá tato zjednodušení odstranit a přiblížit se více reálné situaci. Je zřejmé, že zboží může být v některých střediscích levnější a cena dopravy ve městě nemusí růst lineárně s Eukleidovskou vzdáleností. Nicméně tento model může poskytnout alespoň hrubou aproximaci oblastí příslušných k daným střediskům.

Nyní si uvedeme je geometrickou interpretaci předchozího modelu. Z předpokladů vyplývá, že model indukují rozdělení roviny na určité podoblasti (regiony) takové, že lidé bydlící v této oblasti budou nakupovat zboží, příp. využívat služeb střediska umístěného v této

podoblasti. Z předpokladů potom dále vyplývá, že lidé nakupují ve střediscích, která mají nejbližší, a proto každá podoblast daného střediska obsahuje všechny body, ze kterých je k tomuto středisku *blíže* než k jakémukoliv jinému středisku.

Toto rozdělení, indukované daným modelem, se nazývá *Voroného diagram* dané množiny středisek. Z Voroného diagramu se dají odvodit různé informace o oblastech příslušných k daným střediskům a o vztazích mezi nimi, např. jestliže oblasti dvou středisek mají společnou hranici, potom si tato dvě střediska přímo konkurují o zákazníky, žijící na (resp. okolo) této hranice.

Voroného diagramy mají různé aplikace v mnoha různorodých oblastech, např. ve fyzice, astronomii, robotice a dalších. Jsou také úzce svázány s další důležitou geometrickou strukturou, tzv. *Delaunayho triangulací*.

2.2 Definice a základní vlastnosti

Definice 2.2.1 Eukleidovská vzdálenost *mezi dvěma body* $P = [p_x, p_y]$ a $Q = [q_x, q_y]$ je definována vztahem

$$|PQ| = \text{dist}(P, Q) = \sqrt{(p_x - q_x)^2 + (p_y - q_y)^2}.$$

Definice 2.2.2 Necht $\mathbb{P} = \{P_1, \dots, P_n\}$ je množina n různých bodů v rovině, které nazýváme *generující body*. Voroného diagram množiny bodů $\mathbb{P}$ je rozdělení roviny na n buněk příslušných k jednotlivým bodům P_i takových, že libovolný bod Q leží v buňce příslušné k bodu P_i právě tehdy, když

$$|QP_i| < |QP_j| \quad \forall P_j \in \mathbb{P}, j \neq i.$$

Voroného diagram množiny $\mathbb{P}$ označíme $\text{Vor}(\mathbb{P})$. Buňku $\text{Vor}(\mathbb{P})$, patřící k bodu P_i , označíme $\nu(P_i)$ a nazveme ji Voroného buňkou bodu P_i .

Nyní se budeme podrobněji zabývat strukturou Voroného buňky. Pro dva body P, Q v rovině definujeme osu P, Q jako osu úsečky PQ . Tato osa dělí rovinu na 2 poloroviny. Označení (viz obr. 2.1(a)):

$h(P, Q)$... otevřená polorovina obsahující bod P ,

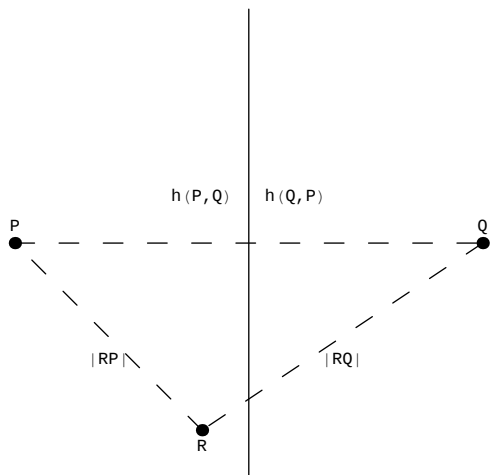
$h(Q, P)$... otevřená polorovina obsahující bod Q .

Poznámka 2.2.1 $R \in h(P, Q) \iff |RP| < |RQ|$.

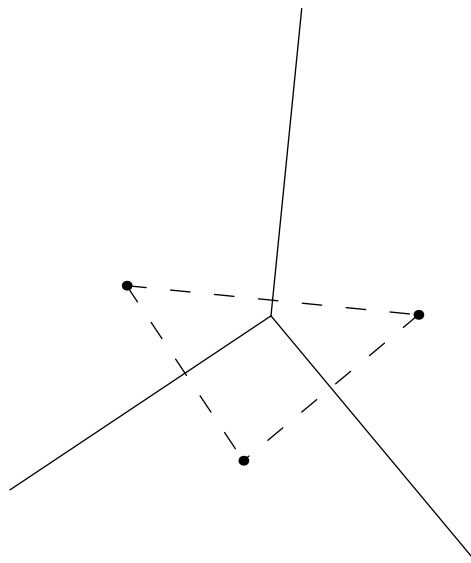
Poznámka 2.2.2

$$\nu(P_i) = \bigcap_{\substack{1 \leq j \leq n \\ j \neq i}} h(P_i, P_j),$$

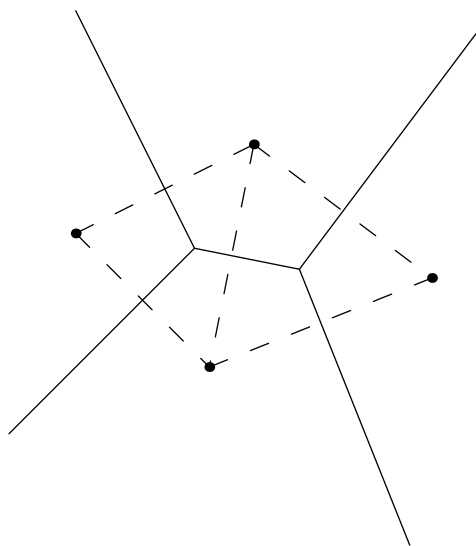
tedy Voroného buňka $\nu(P_i)$ je průnikem $n - 1$ polorovin a je to tedy otevřená konvexní polygonální oblast, ohraničená nejvýše $n - 1$ body (vrcholy) a nejvýše $n - 1$ hranami (může být i neohraničená).



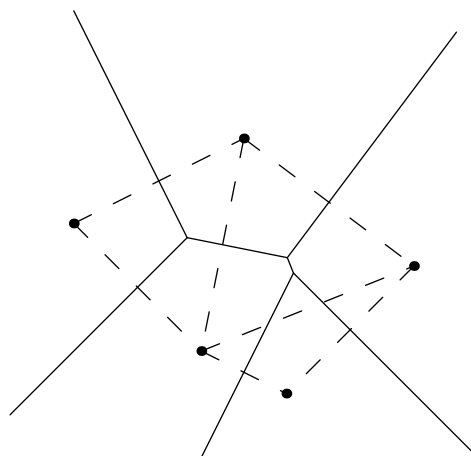
(a) Voroného diagram pro dva body, ukázka otevřených polorovin $h(P, Q)$ a $h(Q, P)$.



(b) Voroného diagram pro tři body.

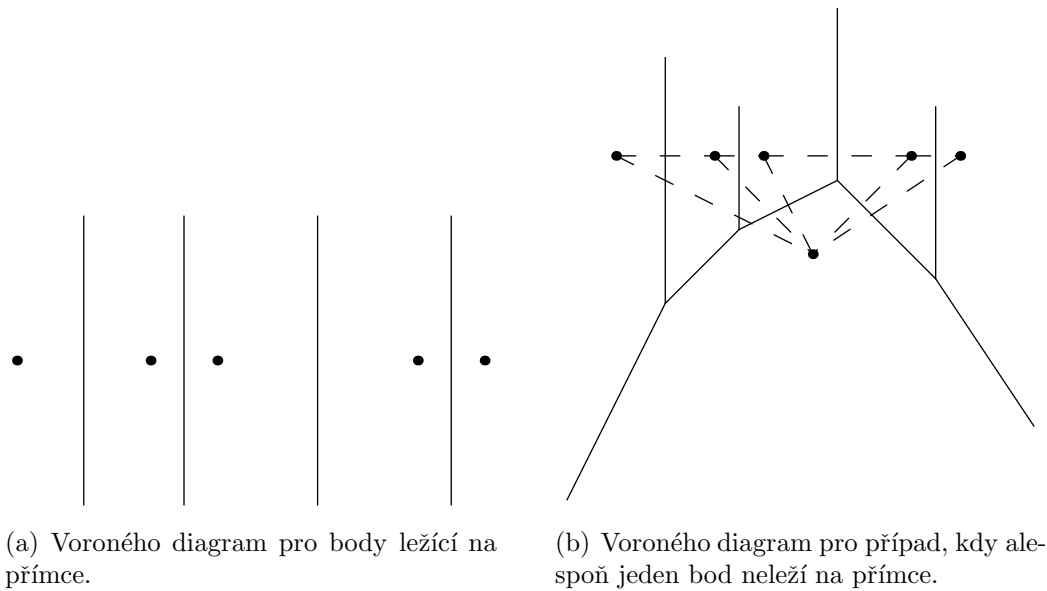


(c) Voroného diagram pro čtyři body.



(d) Voroného diagram pro pět bodů.

Obrázek 2.1: Příklady Voroného diagramů.

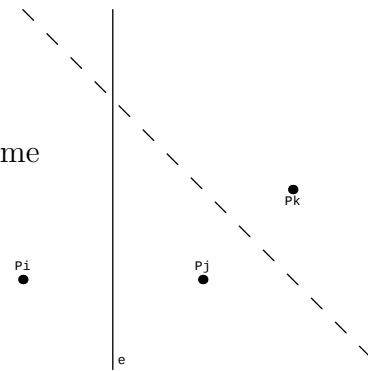


Obrázek 2.2: Příklady Voroného diagramů.

Voroného diagram je tedy rozdělení roviny, jehož hrany jsou úsečky, polopřímky a ve speciálním případě i přímky. Pokud leží všechny generující body na jedné přímce, potom všechny hrany Voroného diagramu jsou rovnoběžné přímky (viz obr. 2.2(a)). V opačném případě Voroného diagram neobsahuje žádnou přímku, pouze úsečky a polopřímky (viz obr. 2.2(b)).

Věta 2.2.3 *Nechť $\mathbb{P}$ je množina n generujících bodů v rovině. Jestliže všechny generující body jsou kolineární, potom $\text{Vor}(\mathbb{P})$ obsahuje $n - 1$ rovnoběžných přímek. Jinak, $\text{Vor}(\mathbb{P})$ je souvislý a jeho hrany jsou úsečky nebo polopřímky.*

Důkaz: První část je zřejmá, zaměříme se proto pouze na druhou část. Předpokládejme tedy, že všechny generující body nejsou kolineární. Nejprve ukážeme, že hrany $\text{Vor}(\mathbb{P})$ jsou úsečky nebo polopřímky. Víme, že hrany $\text{Vor}(\mathbb{P})$ jsou části os mezi dvojicemi generujících bodů. Nyní předpokládejme pro spor, že existuje hrana e Voroného diagramu $\text{Vor}(\mathbb{P})$, která je přímkou. Nechť e je na hranici buněk $\nu(P_i)$ a $\nu(P_j)$. Nechť $P_k \in \mathbb{P}$ je bod, který není kolineární s body P_i a P_j . Osa P_j, P_k není rovnoběžná s e a tedy protíná e . Ale potom tedy část e , která leží uvnitř $h(P_k, P_j)$ nemůže být na hranici $\nu(P_j)$, protože body této části jsou blíže k P_k než k P_j , což vede ke sporu s předpokladem.



Zbývá ukázat, že $\text{Vor}(\mathbb{P})$ je souvislý. Pokud by to tak nebylo, potom by existovala Voroného buňka $\nu(P_i)$, která rozděluje rovinu na dvě části. Protože jsou Voroného buňky

konvexní, $\nu(P_i)$ by se skládalo z pruhu, ohraničeného dvěma rovnoběžnými přímkami. Ale právě jsme dokázali, že hrany Voroného diagramu nemohou být přímky $\Rightarrow$ SPOR. ■

Nyní se budeme zabývat celkovým počtem vrcholů a hran Voroného diagramu, odtud potom plynou vztahy pro očekávanou složitost algoritmu sestavení Voroného diagramu. Jelikož máme n generujících bodů a každá Voroného buňka má nejvýše $n - 1$ vrcholů a hran, složitost nalezení Voroného diagramu $\text{Vor}(\mathbb{P})$ je nejvýše kvadratická.

Věta 2.2.4 *Nechť $n \geq 3$. Potom počet vrcholů Voroného diagramu množiny n generujících bodů v rovině je nejvýše $2n - 5$ a počet hran je nejvýše $3n - 6$.*

Důkaz: Jsou-li všechny generující body kolineární, potom důkaz vyplývá z předchozí věty. Pokud ne, použije se k důkazu Eulerova věta, která říká, že vztah

$$V - E + F = 2$$

platí pro libovolný souvislý rovinný graf s V vrcholy, E hranami a F stěnami. Eulerovu větu nelze použít přímo, protože $\text{Vor}(\mathbb{P})$ může obsahovat hrany tvořené polopřímkami a tedy není grafem. Proto přidáme nevlastní vrchol v_∞ v „nekonečnu“ do množiny vrcholů a všechny tyto polopřímky ve $\text{Vor}(\mathbb{P})$ spojíme s tímto bodem v_∞ . Nyní již můžeme aplikovat Eulerovu větu. Nechť:

- $n_V \dots$ počet vrcholů $\text{Vor}(\mathbb{P})$,
- $n_E \dots$ počet hran $\text{Vor}(\mathbb{P})$,
- $n \dots$ počet generujících bodů a jelikož každý generující bod leží uvnitř jedné stěny, odpovídá také počtu stěn grafu.

Potom

$$(n_V + 1) - n_E + n = 2.$$

Nechť dále d_i je stupeň i -tého vrcholu $\text{Vor}(\mathbb{P})$. Jelikož každá hrana daného grafu má právě dva vrcholy, platí

$$\sum_i d_i = 2n_E.$$

Protože každý vrchol (včetně vrcholu v_∞) má stupeň nejméně 3, platí

$$2n_E \geq 3(n_V + 1).$$

Potom

$$\begin{array}{rclcl} (n_V + 1) & = & n_E - n + 2 & n_E & = & (n_V + 1) + n - 2 \\ 2n_E \geq 3(n_V + 1) & = & 3(n_E - n + 2) & 2n_E & = & 2(n_V + 1) + 2n - 4 \\ 2n_E & \geq & 3(n_E - n + 2) & 2(n_V + 1) + 2n - 4 & \geq & 3(n_V + 1) \\ 3n - 6 & \geq & n_E & 2n - 5 & \geq & n_V \end{array}$$

Nyní tedy víme, že hrany jsou části os dvojic generujících bodů a vrcholy jsou průsečíky těchto os. Počet os odpovídá kvadrátu počtu generujících bodů, ale složitost $\text{Vor}(\mathbb{P})$ je lineární. Zřejmě tedy, ne všechny osy definují hrany $\text{Vor}(\mathbb{P})$ a ne všechny průsečíky jsou vrcholy $\text{Vor}(\mathbb{P})$. Abychom charakterizovali, které osy a které průsečíky budou hranami a vrcholy $\text{Vor}(\mathbb{P})$, je třeba uvést následující definici.

Definice 2.2.3 *Nechť Q je bod v rovině. Největší prázdnou kružnicí bodu Q vzhledem k $\mathbb{P}$ je největší kružnice se středem v bodě Q , která neobsahuje uvnitř žádný bod z $\mathbb{P}$. Tuto kružnici označíme $C_{\mathbb{P}}(Q)$.*

Následující věta potom charakterizuje vrcholy a hrany Voroného diagramu.

Věta 2.2.5 *Pro Voroného diagram $\text{Vor}(\mathbb{P})$ množiny bodů $\mathbb{P}$ platí:*

1. *Bod Q je vrcholem $\text{Vor}(\mathbb{P})$ právě tehdy, když kružnice $C_{\mathbb{P}}(Q)$ obsahuje tři nebo více bodů z množiny $\mathbb{P}$ na své hranici.*
2. *Osa generujících bodů P_i a P_j definuje hranu $\text{Vor}(\mathbb{P})$ právě tehdy, když existuje bod Q na ose P_i, P_j takový, že generující body P_i, P_j leží na hranici kružnice $C_{\mathbb{P}}(Q)$ a žádný další generující bod na ní neleží.*

Důkaz:

1. Předpokládejme, že Q je střed kružnice, na které leží alespoň 3 generující body. Označme tyto body P_i, P_j, P_k . Vnitřek kružnice je prázdný a tedy Q musí ležet na hranici buněk $\nu(P_i), \nu(P_j), \nu(P_k)$, protože Q je stejně vzdálený k bodu P_i i k P_j , z čehož vyplývá, že leží na hranici buněk $\nu(P_i)$ a $\nu(P_j)$ (podobně pro P_i, P_k a P_j, P_k). Odtud potom plyne, že Q musí být vrchol.

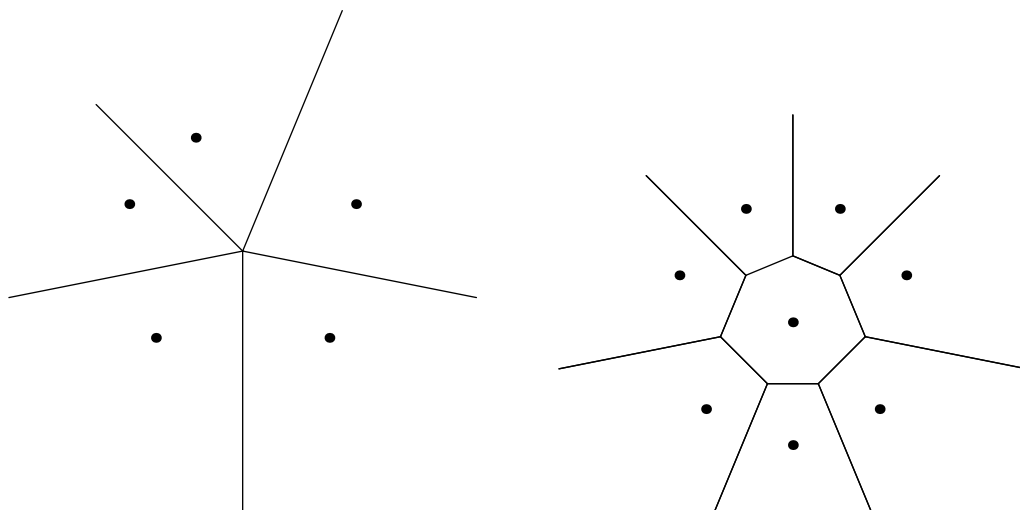
Obráceně: Q je vrchol $\Rightarrow Q$ je průsečíkem alespoň tří hran $\Rightarrow Q$ náleží alespoň třem buňkám $\nu(P_i), \nu(P_j), \nu(P_k)$ Voroného diagramu. Platí

$$|QP_i| = |QP_j| = |QP_k|,$$

protože Q leží v průsečíku os úseček P_iP_j, P_iP_k, P_jP_k a je tedy středem kružnice opsané trojúhelníku $\triangle P_iP_jP_k$. Žádný další bod nemůže být blíž k bodu Q než body P_i, P_j, P_k , protože jinak by Q neleželo v průsečíku os úseček P_iP_j, P_iP_k, P_jP_k a odpovídající Voroného buňky $\nu(P_i), \nu(P_j), \nu(P_k)$ by se v tomto bodě nesetkaly $\Rightarrow$ kružnice je prázdná.

2. Předpokládejme, že existuje bod Q na ose úsečky P_iP_j takový, že body P_i, P_j leží na hranici kružnice $C_{\mathbb{P}}(Q)$ a žádný jiný bod $\mathbb{P}$ uvnitř této kružnice, tedy platí

$$|QP_i| = |QP_j| < |QP_k| \quad \forall k : 1 \leq k \leq n, k \neq i, j.$$



Obrázek 2.3: Voroného diagramy pro množiny bodů, obsahující alespoň čtyři body ležící na kružnici.

Odtud vyplývá, že Q leží na hraně $\text{Vor}(\mathbb{P})$ (nemůže ležet ve vrcholu, body jsou jen dva).

Obráceně: necht' osa úsečky $P_i P_j$ definuje Voroného hranu. Potom největší prázdná kružnice pro libovolný bod z *vnitřku hrany* musí na hranici obsahovat body P_i, P_j a žádné další body (musí obsahovat oba body, protože pro libovolný bod hrany je $|QP_i| = |QP_j|$ a bude obsahovat pouze tyto dva body, protože jinak by se jednalo o vrchol, který jsme ale zde vyloučily). ■

Věta 2.2.6 *Voroného buňka $\nu(P_i)$ je neohraničená právě tehdy, když bod P_i patří hraně konvexního obalu množiny $\mathbb{P}$.*

V případě, že množina bodů $\mathbb{P}$ obsahuje čtyři nebo více bodů, které leží na jedné kružnici, přestane platit, že vrchol Voroného diagramu je tvořen průsečíkem tří os, resp. Voroného hran (viz obr. 2.3(a)). V takovém případě se hovoří o Voroného diagramu jako o *degenerovaném* a existuje vrchol Voroného diagramu $\text{Vor}(\mathbb{P})$ tvořený průsečíkem tolika Voroného hran, kolik bodů leží na odpovídající kružnici.

2.3 Algoritmy konstrukce Voroného diagramů

Existuje několik možností, jak zkonstruovat Voroného diagram, které se liší složitostí a efektivností výpočtu. Obecně lze ukázat, že sestavení Voroného diagramu pro n bodů zabere čas nejméně $O(n \log n)$, jelikož je to úloha ekvivalentní s tříděním. To tedy znamená, že každý algoritmus s touto složitostí je optimální. Klasické algoritmy pro sestavení Voroného diagramu jsou následující:

1. naivní algoritmus,
2. inkrementální algoritmus,
3. algoritmus „rozděl a panuj“,
4. zametací „Fortuneho“ algoritmus,
5. metoda zdvihu.

Nyní se budeme věnovat každému z těchto algoritmů podrobněji.

2.3.1 Naivní algoritmus

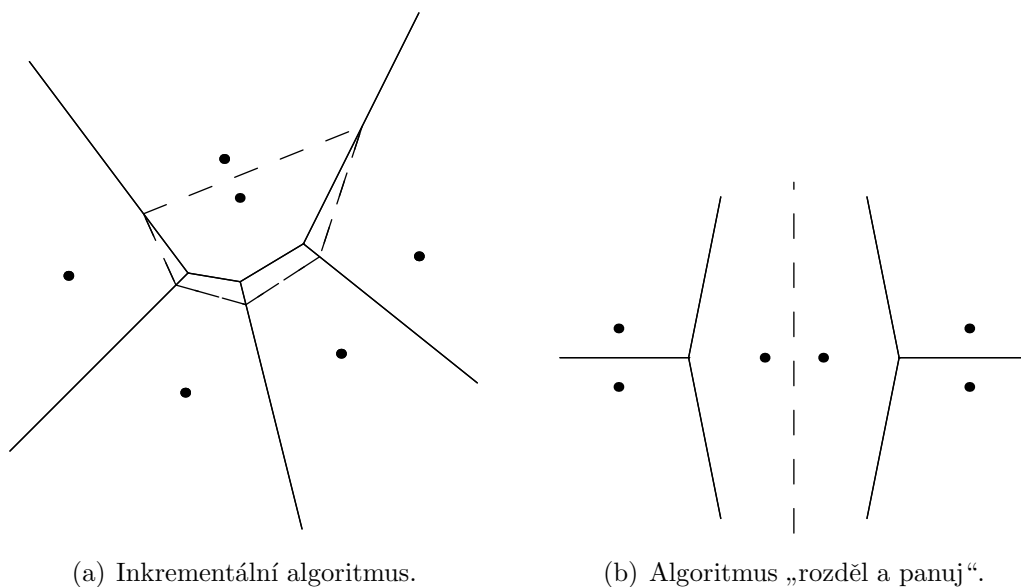
Nejjednodušší a nejpřímější algoritmus, založený na přímé aplikaci definice Voroného diagramu, kdy každá oblast $\nu(P_i)$ Voroného diagramu je získána jako průnik polorovin $h(P_i, P_j)$, $\forall j \neq i$. Složitost tohoto algoritmu není zdaleka optimální, protože je $O(n^2 \log n)$.

2.3.2 Inkrementální algoritmus

Jeden z klasických přístupů používaných ve výpočtové geometrii — inkrementální algoritmus — lze použít i v případě Voroného diagramů. Nejprve provedeme výpočet Voroného diagramu pro jednoduchý a snadno zvládnutelný případ, např. náhodně vybereme dva nebo tři z množiny generujících bodů a najdeme pro ně Voroného diagram. Poté postupně přidáváme po jednom zbylé body z generující množiny a vždy modifikujeme stávající strukturu (Voroného diagram pro do té doby použité body).

Postup modifikace stávající struktury při přidání $(i + 1)$ -ního bodu je následující (viz obr. 2.4(a)):

1. Lokalizace — v prvním kroku určíme, v jaké Voroného buňce stávajícího Voroného diagramu se nově přidávaný bod P_{i+1} nachází. Generující bod Voroného buňky, ve které se bod P_{i+1} nachází, označíme P_{i_1} .
2. Najdeme osu úsečky $P_{i+1}P_{i_1}$.
3. Najdeme průsečíky osy úsečky $P_{i+1}P_{i_1}$ s hranicí Voroného buňky, ve které se bod P_{i+1} nachází.
4. Vybereme si jeden z průsečíků, čímž určíme Voroného buňku, do které budeme pokračovat v dalším kroku algoritmu. Označme generující bod této buňky P_{i_2} .
5. Najdeme osu úsečky $P_{i+1}P_{i_2}$ a její průsečíky s hranicí buňky, ve které se nachází bod P_{i_2} . Vybereme průsečík, který neleží na společné hraně Voroného buněk $\nu(P_{i_1})$ a $\nu(P_{i_2})$ a pokračujeme dále.
6. Opakujeme krok 5, dokud se nedostaneme do druhého průsečíku osy úsečky $P_{i+1}P_{i_1}$ s hranicí Voroného buňky $\nu(P_{i_1})$.



Obrázek 2.4: Algoritmy nalezení Voroného diagramu.

Na konci je nezbytné provést tzv. „začištění“ — tzn. vyrušit hrany uvnitř nově vzniklé Voroného buňky.

Složitost inkrementálního algoritmu je obecně $O(n^2)$, ve speciálních případech ale může být i $O(n)$.

2.3.3 Algoritmus „rozděl a panuj“

Další z klasických přístupů používaných ve výpočtové geometrii, který lze i v tomto případě aplikovat na nalezení Voroného diagramu dané množiny bodů.

Algoritmus funguje následovně: zadanou generující množinu bodů dělíme rekurzivně na dvě části až do té úrovně, dokud nedostaneme množinu pouze tří bodů, pro které už lze sestavit Voroného diagram jednoduše. Následuje „zpětný chod“, při kterém jsou jednotlivé části — Voroného diagramy pro tři body — opět postupně spojovány do jednoho Voroného diagramu, což je nejsložitější část tohoto algoritmu.

Nevýhodou tohoto algoritmu je náchylnost na numerické chyby a z toho plynoucí numerická nestabilita. Výhodou potom je to, že algoritmus dosahuje optimální složitosti $O(n \log n)$.

2.3.4 Zametací „Fortuneho“ algoritmus

I v tomto případě se v principu jedná o klasický přístup používaný ve výpočtové geometrii — použití zametací přímk. Nicméně pro nalezení Voroného diagramu je nezbytné klasický algoritmus mírně modifikovat.

Základem je tzv. zametací přímka — horizont, který se postupně pohybuje od shora dolů a během pohybu jsou uchovávány všechny informace potřebné pro výpočet a vytváření hledané struktury, v tomto případě Voroného diagramu. Klasickým přístupem by bylo zkoumat průsečíky zametací přímky s Voroného diagramem. To ale bohužel není možné, jelikož Voroného diagram nad zametací přímkou l závisí nejen na bodech nad přímkou l , ale také na bodech pod ní. Jinak řečeno, pokud se zametací přímkou l dojdeme do nejvyššího bodu Voroného buňky $\nu(P_i)$, bod P_i ještě stále není mezi zpracovávanými body, protože je pod zametací přímkou l a algoritmus o něm ještě stále „neví“ – nejsou tedy k dispozici ještě všechny potřebné informace.

Proto je nutné modifikovat tento klasický přístup následujícím způsobem — místo udržování informací o průsečících Voroného diagramu se zametací přímkou l budeme uchovávat informace o té části Voroného diagramu nad l , která již nemůže být změněna, resp. která již nemůže být ovlivněna body pod zametací přímkou l .

Označme uzavřenou polorovinu nad zametací přímkou l symbolem l^+ . Nyní nás tedy zajímá, která část Voroného diagramu $\text{Vor}(\mathbb{P})$ již nemůže být modifikována, neboli pro které body $Q \in l^+$ již víme, který generující bod je k nim nejblíže? Je zřejmé, že vzdálenost libovolného bodu $Q \in l^+$ k libovolnému generujícímu bodu pod zametací přímkou l je větší než vzdálenost Q od přímky l a tedy nejblíže generující bod k bodu $Q \in l^+$ nemůže ležet pod zametací přímkou l , jestliže existuje generující bod $P_i \in l^+$ takový, že $|QP_i| \leq |Ql|$.

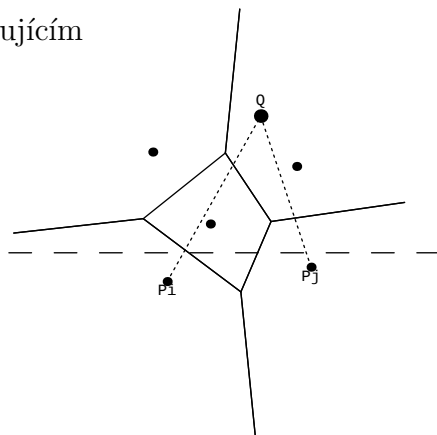
Dále víme, že množina všech bodů v rovině, které mají stejnou vzdálenost od pevně daného bodu a od pevně dané přímky tvoří *parabolu*. Proto množina bodů, které jsou blíže k danému generujícímu bodu $P_i \in l^+$ než k zametací přímce l je ohraničena právě parabolou. To samozřejmě platí pro libovolný generující bod nad přímkou l , a proto množina všech bodů $Q \in l^+$, které mají blíže k některému z generujících bodů ležících v l^+ je ohraničena parabolickými oblouky. Tato posloupnost parabolických oblouků se nazývá *beach line*.

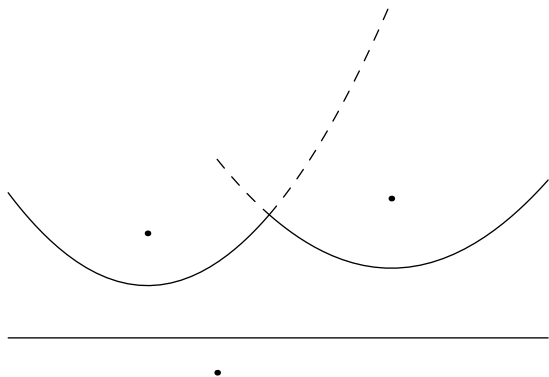
Poznámka 2.3.1 *Beach line je x -monotónní, tzn. že každá vertikální přímka protíná beach line právě v jednom bodě.*

Zřejmě jedna parabola může do beach line přispět několikrát různými částmi (viz např. obr. 2.5(c)). Průsečíky parabolických oblouků, které leží na beach line, leží na hranách Voroného diagramu a s pohybem zametací přímky l tyto průsečíky vytvářejí hrany Voroného diagramu $\text{Vor}(\mathbb{P})$ pro danou množinu generujících bodů $\mathbb{P}$.

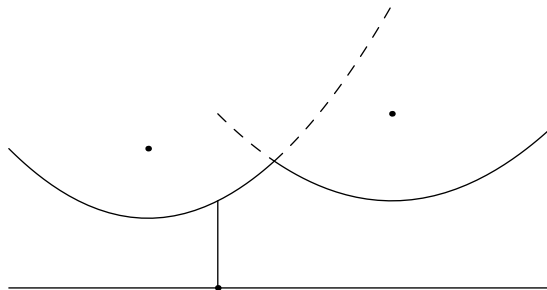
V průběhu provádění algoritmu jsou nejdůležitějšími operacemi následující dvě akce:

- *site event* — na beach line se objeví nový generující bod, je nutné ho přidat do struktury,

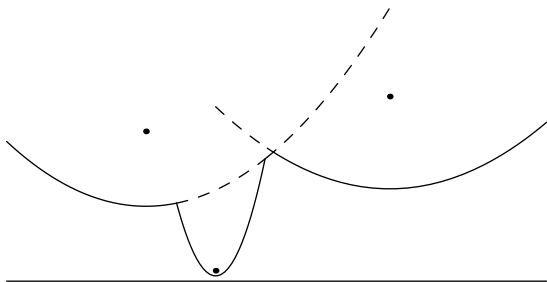




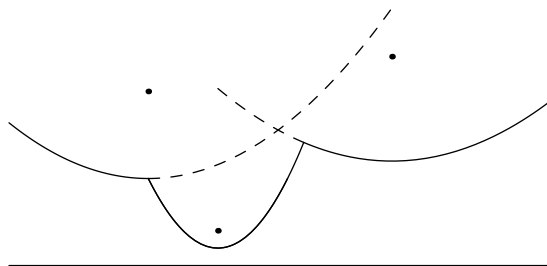
(a) První krok – jsou uvažovány jen dva body nad přímkou l , o bodu pod l algoritmus „neví“.



(b) Druhý krok – přímka narazí na další generující bod, dojde k vytvoření nové degenerované paraboly nulové šířky.



(c) Třetí krok — s posunem přímky l dojde k rozšíření paraboly.



(d) Pokud stále posouváme s přímkou l , nově vzniklá parabola se stále rozšiřuje.

Obrázek 2.5: Průběh jedné ze základních událostí, nastávajících v průběhu zametacího „Fortuneho“ algoritmu — *site event*.

- *circle event* — dojde k zániku jednoho z parabolických oblouků.

Site event (viz obr. 2.5) tedy nastává v případě, že se na beach line objeví nový, dosud nepoužitý generující bod. Tím zároveň vzniká nový parabolický oblouk, na počátku ve své degenerované formě jako parabola nulové šířky. Jelikož průsečíky parabol, tvořících beach line, sledují hrany Voroného diagramu, přidáním nového bodu do stávající struktury dojde ke vzniku dvou nových průsečíků (na počátku totožných), které se s pohybem beach line od sebe vzdalují a vytvářejí novou hranu Voroného diagramu. Zpočátku tato hrana není napojena na zbytek Voroného diagramu, později ale k tomu napojení dojde v nějakém vrcholu. Beach line se tedy skládá nejvýše z $2n - 1$ parabolických oblouků, protože každý generující bod představuje vznik jedné paraboly a rozdělení nejvýše jednoho parabolického oblouku na dvě části.

Circle event (viz obr. 2.6) nastává v případě, že dochází k zániku některého parabolického oblouku. Oblouk paraboly vymizí v případě, že tři paraboly příslušné třem generujícím bodům P_i, P_j, P_k procházejí společným bodem Q , pro který tedy platí

$$|QP_i| = |QP_j| = |QP_k| = |Ql|.$$

Zřejmě tedy kružnice se středem Q procházející body P_i, P_j, P_k se dotýká l a má nejnižší bod právě na l . Žádný další generující bod nemůže ležet uvnitř této kružnice, protože v takovém případě by vzdálenost od bodu Q k tomuto bodu byla menší než vzdálenost Q od zametací přímky l , což je ale ve sporu s tím, že bod Q leží na beach line. Odtud potom vyplývá, že bod Q musí být vrcholem Voroného diagramu. Shrnutí — zánikem některého z oblouků beach line vzniká vrchol Voroného diagramu $\text{Vor}(\mathbb{P})$.

Složitost je stejně jako v případě algoritmu „rozděl a panuj“ i u tohoto algoritmu optimální, tedy $O(n \log n)$.

2.3.5 Metoda zdvihu

Uvažujme transformaci, která libovolnému bodu $P = [p_x, p_y] \in \mathbb{E}^2$ přiřadí rovinu

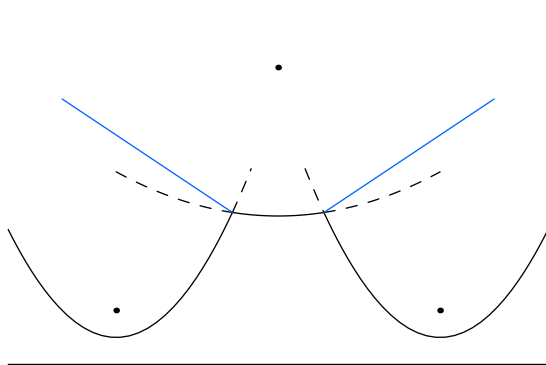
$$h(p) : z = 2p_x x + 2p_y y - (p_x^2 + p_y^2) \in \mathbb{E}^3.$$

Geometricky, $h(P)$ je tečná rovina k paraboloidu $z = x^2 + y^2$ v bodě $\bar{P} = [p_x, p_y, p_x^2 + p_y^2]$, tzn. v bodě odpovídajícím kolmému průmětu bodu P na paraboloid $z = x^2 + y^2$.

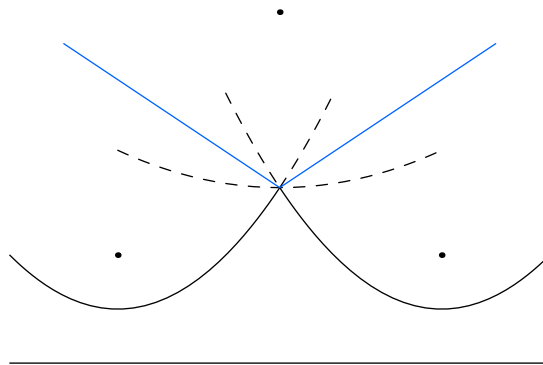
Nechť $\mathbb{P} = \{P_i : 1 \leq i \leq n\}$ je množina generujících bodů Voroného diagramu a nechť $H(\mathbb{P})$ je množina tečných rovin $h(P_i)$, $\forall i$. Průnikem všech kladných poloprostorů, definovaných rovinami z $H(\mathbb{P})$, vznikne konvexní mnohostěn $\mathcal{P}$, tedy

$$\mathcal{P} = \bigcap_{h(P_i) \in H(\mathbb{P})} h(P_i)^+,$$

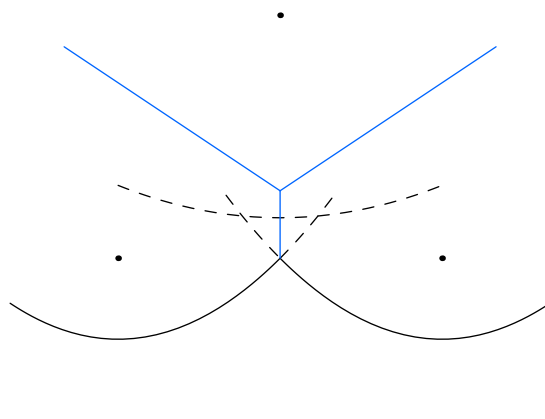
kde $h(P_i)^+$ označuje poloprostor nad $h(P_i)$. Pokud provedeme projekci hran a vrcholů tohoto vzniklého mnohostěnu zpět do roviny xy , dostaneme Voroného diagram množiny $\mathbb{P}$.



(a) První krok — beach line složena ze tří oblouků, průsečíky oblouků vytváří hrany Voroného diagramu, zametací přímka se pohybuje směrem dolů.

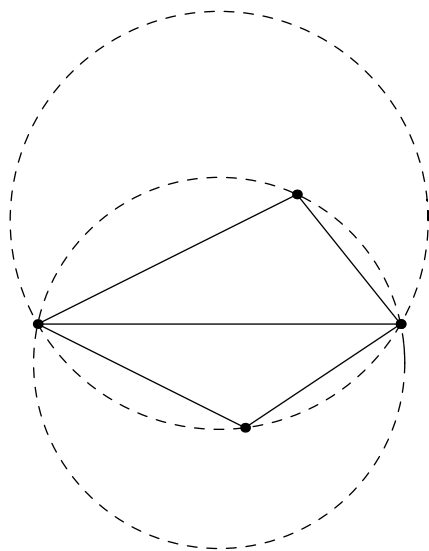


(b) Druhý krok — dochází k zániku jednoho z oblouků, resp. přestane tento oblouk přispívat do beach line, vzniká vrchol Voroného diagramu.

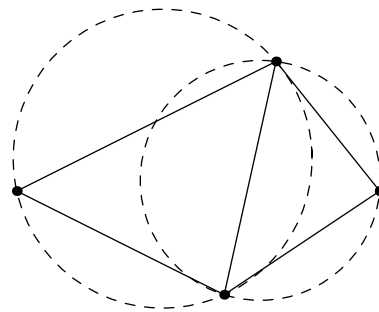


(c) Třetí krok — beach line už má jen dva oblouky, ze vzniklého vrcholu pokračuje dále hrana Voroného diagramu.

Obrázek 2.6: Průběh další ze základních událostí, nastávajících v průběhu zametacího „Fortuneho“ algoritmu — *circle event*.



(a) Triangulace, která není Delaunayova.



(b) Triangulace, která je Delaunayova.

Obrázek 2.7: Triangulace na čtyřech bodech.

2.4 Delaunayho triangulace

Duální strukturou k Voroného diagramu je Delaunayho triangulace (triangulace = pokrytí nepřekrývajícími se trojúhelníky). Tedy, pro daný Voroného diagram $\text{Vor}(\mathbb{P})$ dostaneme Delaunayho triangulaci bodů množiny $\mathbb{P}$ tak, že hrana $P_i P_j$ je v Delaunayho triangulaci právě tehdy, když Voroného buňky $\nu(P_i)$ a $\nu(P_j)$ sousedí, tzn. mají společnou hranu.

Pokud je množina bodů $\mathbb{P}$ degenerovaná, tzn. obsahuje čtyři a více bodů, které leží na jedné kružnici, potom dualizací nemusí vzniknout triangulace, ale může se objevit polygon o více hranách. Nicméně i tento polygon je možné dodatečně rozdělit na trojúhelníky přidáním hran.

Existuje vzájemně jednoznačné zobrazení mezi Voroného body (body generující množiny) a Delaunayho polygony, podobně existuje také vzájemně jednoznačné zobrazení mezi Voroného hranami a Delaunayho hranami — dvojice odpovídajících hran je tvořena vzájemně kolmými hranami. Navíc víme, že Delaunayho polygon je konvexní obálka generujících bodů, jejichž Voroného buňky incidují s daným Voroného vrcholem.

Důležitou vlastností Delaunayho triangulace v $\mathbb{E}^2$ je, že poskytuje *optimální triangulaci* v tom smyslu, že maximalizuje minimální úhel v trojúhelníku.

Věta 2.4.1 (Kritérium prázdného kruhu) *Triangulace množiny bodů $\mathbb{P}$ je Delaunayova právě tehdy, když opsaná kružnice každého trojúhelníka, tvořícího Delaunayho triangulaci, neobsahuje žádný další bod z množiny $\mathbb{P}$.*

Věta 2.4.2 (Max-min lokální kritérium) *Delaunayho triangulace maximalizuje lokálně minimální úhel.*

Na větách 2.4.1 a 2.4.2 je založen tzv. *překlápěcí algoritmus*, který z libovolné triangulace, která není Delaunayova, dokáže vytvořit Delaunayho triangulaci překlápěním hran ve smyslu obr. 2.7. Stačí tedy postupně brát čtyřúhelníky a zkoumat, jestli je splněno kritérium prázdného kruhu. Pokud není, zamění se úhlopříčka uvnitř tohoto čtyřúhelníka.

Vlivem vlastnosti uvedené ve větě 2.4.2 Delaunayho triangulace neobsahuje (pokud to jde) protáhlé trojúhelníky, resp. dává nejlepší možné výsledky v tomto směru, což je důležité zejména v aplikacích, jako je MKP, interpolace apod.

Existuje samozřejmě celá řada jiných typů triangulací, resp. algoritmů pro nalezení triangulace dané množiny bodů, jako je např. žravá triangulace, nejkratší triangulace, triangulace, která splňuje min-max kritérium (minimalizuje maximální úhel, což obecně nedává stejné triangulace jako Delaunayho triangulace).

2.5 Zobecnění Voroného diagramů

Zobecnění je možné provést v zásadě několika způsoby:

- změnou dimenze,
- změnou metriky,
- přidáním váhy generujícím bodům.

2.5.1 Změna dimenze

Předpokládejme, že máme množinu generujících bodů $\mathbb{P} = \{P_1, \dots, P_n\} \subset \mathbb{E}^d$. Pro každé P_i potom zcela analogicky definujeme Voroného buňky vztahem

$$\nu(P_i) = \{Q \in \mathbb{E}^d : \|Q - P_i\| < \|Q - P_j\| \ \forall j \neq i\},$$

kde $\|Q - P\|$ je Eukleidovská vzdálenost bodů P a Q . Tedy, $\nu(P_i)$ obsahuje body $Q \in \mathbb{E}^d$, které jsou blíže k P_i než k libovolnému jinému bodu $P_j \in \mathbb{P}$. Opět analogicky, $\nu(P_i)$ je průnikem všech poloprostorů ohraničených nadrovinami $\|Q - P_i\| = \|Q - P_j\|$, tedy platí

$$\nu(P_i) = \bigcap_{j \neq i} \{Q \in \mathbb{E}^d : \|Q - P_i\| < \|Q - P_j\|\}.$$

Odtud plyne, že Voroného buňka (oblast) je konvexní polyhedron (mnohostěn). Rozdělení prostoru $\mathbb{E}^d$ na buňky $\nu(P_1), \dots, \nu(P_n)$ představuje Voroného diagram pro danou množinu bodů $\mathbb{P}$.

Obecně Voroného vrchol inciduje s $d+1$ Voroného oblastmi. Degenerovanost se objeví v případech, že $d+2$ nebo více generujících bodů leží na kouli dimenze $d-1$ a žádné generující

body neleží uvnitř této koule. Potom Voroného oblasti těchto kosférických generujících bodů incidují se společným Voroného vrcholem.

Souvislost mezi Voroného vrcholy a Delaunayho polygony je možné také zobecnit do prostoru vyšší dimenze. Pro každý Voroného vrchol se konvexní obal generujících bodů, jejichž Voroného oblasti incidují s Voroného vrcholem, nazývá *Delaunayho mnohostěn*. Delaunayho mnohostěny odpovídající všem Voroného vrcholům dávají rozdělení konvexního obalu množiny generujících bodů. Pro každý Delaunayho mnohostěn dále platí, že všechny jeho vrcholy leží na kouli dimenze $d - 1$ a uvnitř této koule není žádný jiný generující bod. Jestliže množina generujících bodů $\mathbb{P}$ není degenerovaná, Delaunayho mnohostěn je d -*dimensionálním simplexem*. V takovém případě se pro Delaunayho diagram používá název *Delaunayho triangulace* (v $\mathbb{E}^3$ se používá termín *Delaunayho tetrahedronizace*).

Do vyšší dimenze lze také zobecnit *metodu zdvihu*. Necht' $\mathbb{P} = \{P_1, \dots, P_n\} \subset \mathbb{E}^d$. Definujme množinu $\mathbb{P}^* = \{P_1^*, \dots, P_n^*\}$ tak, že bod P_i^* dostaneme vytažením P_i ve směru nově přidané proměnné x_{d+1} na plochu

$$x_{d+1} = x_1^2 + x_2^2 + \dots + x_d^2.$$

Potom kolmá projekce $(d+1)$ -dimensionálního konvexního obalu množiny $\mathbb{P}^*$ dává Delaunayho triangulaci.

2.5.2 Změna metriky

Voroného diagram je rozdělení prostoru vzhledem k vzdálenostem definovaným metrikou. Doposud jsme používali klasickou Eukleidovskou vzdálenost (metriku). Nicméně pojem vzdálenosti (metriky) lze samozřejmě chápat obecněji a i v případě Voroného diagramů můžeme nahradit Eukleidovskou vzdálenost libovolnou jinou metrikou. Tím dostáváme tzv. *zobecněné Voroného diagramy*, kde pro každou Voroného buňku platí

$$\nu(P_i) = \bigcap_{j \neq i} \{Q \in \mathbb{E}^d : \text{dist}(Q, P_i) < \text{dist}(Q, P_j)\}$$

a tedy místo Eukleidovské vzdálenosti je použita libovolná metrika dist .

Standardním příkladem jiných metrik, které je možné použít, jsou tzv. L_p -metriky (mezi které patří i Eukleidovská metrika jako L_2 -metrika):

L_1 -metrika ... definována vztahem

$$\text{dist}_1(P, Q) = \|PQ\|_1 = \sum_{i=1}^d |P_{x_i} - Q_{x_i}|.$$

Všechny hrany v této metrice jsou složeny z horizontálních, vertikálních nebo diagonálních (pod úhlem $\pi/4$) úseček.

L_p -metrika ... definována vztahem

$$\text{dist}_p(P, Q) = \|PQ\|_p = \left(\sum_{i=1}^d |P_{x_i} - Q_{x_i}|^p \right)^{\frac{1}{p}}.$$

L_∞ – metrika ... definována vztahem

$$\text{dist}_\infty(P, Q) = \|PQ\|_\infty = \max\{|P_{x_1} - Q_{x_1}|, \dots, |P_{x_d} - Q_{x_d}|\}.$$

V jistém smyslu podobné L_1 -metrice — Voroného diagramy vzhledem k L_∞ -metrice jsou opět složeny pouze z úseček.

2.5.3 Přidání váhy

Další možností jak zobecnit Voroného diagramy je přidat váhy jednotlivým generujícím bodům, což může odpovídat např. různým cenám v supermarketech, kdy nižší cena je zohledněna vyšší váhou generujících bodu, protože lidé budou více chodit do tohoto supermarketu. Potom dostáváme tzv. *vážené Voroného diagramy*, které můžeme rozdělit ještě na dvě podskupiny:

Aditivní vážené Voroného diagramy — nechť bodu P_i přísluší váha $w_i \in \mathbb{R}$. Potom můžeme definovat metriku vztahem

$$\text{dist}_a(P, Q) = \text{dist}(P, Q) - w_i,$$

kde dist je opět libovolná metrika. Pokud zvyšujeme váhu daného bodu, příslušná Voroného buňka (oblast) se zvětšuje (vyplývá přímo z definované metriky). Jestliže $\text{dist}(P, Q)$ je Eukleidovská vzdálenost, potom $\text{dist}_a(P, P_i)$ lze interpretovat jako Eukleidovskou vzdálenost bodu P od kružnice se středem v P_i a poloměrem w_i — množina bodů, které mají stejnou vzdálenost od dvou kružnic tvoří hyperbolu a tedy Voroného hrany jsou v tomto případě části hyperbol.

Multiplikativní vážené Voroného diagramy — podobně můžeme definovat metriku vztahem

$$\text{dist}_m(P, Q) = \frac{1}{w_i} \text{dist}(P, Q).$$

Množina bodů, pro něž je poměr Eukleidovských vzdáleností ke dvěma bodům P_i a P_j konstantní, tvoří kružnici, která se nazývá Apolloniova kružnice. Tedy Voroného hrany multiplikativního váženého Voroného diagramu jsou kruhové oblouky.

2.6 Aplikace

Na závěr této kapitoly si uvedeme několik možných aplikací Voroného diagramů, a to jak klasických, tak zobecněných i vážených:

- dopravní problém — v podstatě přímo vyplývá z poštovního problému, zmíněného na začátku kapitoly. Příkladem může být např. určení spádových oblastí Záchrané služby, příp. určení nejbližší nemocnice, do které má sanitka jet.

- osa objektu — množina $\mathbb{P}$ bude tvořena body na hranici daného objektu, které musí být rozmístěny dostatečně hustě. Poté se sestaví Voroného diagram a spojnice Voroného vrcholů odpovídá ose objektu.
- ekvidistanty — použití např. při plánování cesty frézy při obrábění.
- interpolace.

Kapitola 3

Afinní variety a ideály

Tato kapitola bude věnována seznámení se základními pojmy, se kterými se bude dále pracovat. Půjde zejména o afinní variety, což jsou objekty definované polynomiálními rovnicemi. S pojmem afinní variety úzce souvisí pojem ideálu v okruhu polynomů $k[x_1, \dots, x_n]$. Formální aparát popsaný v této kapitole může mít mnoho aplikací všude, kde se pracuje s objekty a ději popsatenými polynomy, resp. systémy polynomiálních rovnic. Jedná se například o:

- hledání extrémů na ploše,
- analýzu pohybů součástí nějakého stroje,
- hledání příslušnosti bodu k nějakému tělesu.

3.1 Polynomy a afinní prostor

Tato část bude věnována studiu polynomů nad jistým číselným tělesem. Těleso je množina, kde jsou definovány operace sčítání, odčítání, násobení a dělení s obvyklými vlastnostmi (viz kapitola 1). Typickým příkladem jsou reálná čísla $\mathbb{R}$ (naproti tomu množina celých čísel $\mathbb{Z}$ není tělesem).

Definice 3.1.1 Monomem v proměnných $x_1, \dots, x_n$ se nazývá výraz tvaru

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

kde $\alpha_i \in \mathbb{N}$. Celkový stupeň monomu je součet $\alpha_1 + \alpha_2 + \dots + \alpha_n$.

Zápis monomu lze zjednodušit pomocí pojmu *multiindexu*, kde pro každou n -tici $\alpha = (\alpha_1, \dots, \alpha_n)$ položíme $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Celkový stupeň je potom $|\alpha| = \alpha_1 + \dots + \alpha_n$.

Definice 3.1.2 Polynomem v proměnných $x_1, \dots, x_n$ s koeficienty z tělesa k je konečná lineární kombinace monomů, která se zapisuje ve tvaru

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha}, \quad a_{\alpha} \in k,$$

kde se sčítá přes konečný počet n -tic $\alpha = (\alpha_1, \dots, \alpha_n)$. Množina všech polynomů s koeficienty v k se značí $k[x_1, \dots, x_n]$.

Příkladem polynomu z $\mathbb{Q}[x, y, z]$ je $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ (je to polynom tří proměnných x, y, z s koeficienty z tělesa racionálních čísel $\mathbb{Q}$).

Věta 3.1.1 Množina $k[x_1, \dots, x_n]$ všech polynomů v proměnných $x_1, \dots, x_n$ s koeficienty z tělesa k tvoří komutativní okruh.

Důkaz: Viz [14]. □

Jelikož z věty 3.1.1 vyplývá, že $k[x_1, \dots, x_n]$ tvoří komutativní okruh, nazývá se *okruhem polynomů*.

Definice 3.1.3 Je dáno těleso k a kladné celé číslo n . Afinním prostorem nad tělesem k se rozumí množina

$$k^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in k\}.$$

Ukažme, jaká je souvislost mezi polynomy a afinním prostorem. Klíčem je myšlenka, že polynom $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ lze chápat jako zobrazení

$$f : k^n \rightarrow k$$

definované následujícím způsobem: pro dané $(a_1, \dots, a_n) \in k^n$ se ve vyjádření f nahradí všechna x_i hodnotami a_i . Protože koeficienty také leží v k , je $f(a_1, \dots, a_n) \in k$.

Věta 3.1.2 Nechť k je nekonečné těleso a nechť $f \in k[x_1, \dots, x_n]$. Potom $f = 0$ tehdy a jen tehdy, když $f : k^n \rightarrow k$ je nulové zobrazení, tzn. pro libovolnou n -tici $(a_1, \dots, a_n) \in k^n$ je $f(a_1, \dots, a_n) = 0$.

Důkaz: Indukcí podle n . Podrobně viz [27], str. 2. □

Požadavek nekonečného tělesa je v tomto případě důležitý, protože např. pro $k = \mathbb{Z}_2$ a $f = x^2 - x$ je $f(x) = x(x - 1) = 0$ pro každé $x \in \mathbb{Z}_2$, ale f není nulový polynom.

Důsledek 3.1.3 Nechť k je nekonečné těleso a nechť $f, g \in k[x_1, \dots, x_n]$. Potom $f = g$ v $k[x_1, \dots, x_n]$ tehdy a jen tehdy, když $f : k^n \rightarrow k$ a $g : k^n \rightarrow k$ jsou stejná zobrazení, tzn. pro libovolnou n -tici $(a_1, \dots, a_n) \in k^n$ je $f(a_1, \dots, a_n) = g(a_1, \dots, a_n)$.

3.2 Afinní variety

Definice 3.2.1 Nechť k je těleso a nechť $f_1, \dots, f_s$ jsou polynomy z $k[x_1, \dots, x_n]$. Potom množina

$$V(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \text{ pro všechna } 1 \leq i \leq s\}$$

se nazývá afinní varieta určená polynomy $f_1, \dots, f_s$.

Afinní varieta $\mathbf{V}(f_1, \dots, f_s) \subset k^n$ je tedy množina všech řešení soustavy nelineárních algebraických rovnic $f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0$. Afinními varietami jsou tedy grafy všech funkcí daných polynomy nebo racionálními funkcemi, například kružnice $\mathbf{V}(x^2 + y^2 - 1)$ je varietou v $\mathbb{R}^2$, paraboloid $\mathbf{V}(z - x^2 - y^2)$ je varietou v $\mathbb{R}^3$.

Jedna rovnice v $\mathbb{R}^2$ obvykle určuje křivku. Podobně jedna rovnice v $\mathbb{R}^3$ obvykle dává plochu, která má dimenzi 2, dimenze se tedy opět snížila o jedna. Dvě rovnice v $\mathbb{R}^3$ obvykle určují křivku. Intuitivně se zdá, že každá rovnice sníží dimenzi o jedna. Bohužel to ale neplatí vždy, např. $\mathbf{V}(xz, yz)$ odpovídá varietě ve tvaru sjednocení roviny xy s osou z .

Zbývá uvést několik příkladů variet ve vyšších dimenzích. Řešení soustavy m lineárních rovnic pro n neznámých $x_1, \dots, x_n$

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m. \end{aligned} \tag{3.1}$$

s koeficienty v k tvoří afinní varietu v k^n , která se nazývá *lineární varieta*. Z lineární algebry je známa metoda pro řešení takové soustavy rovnic (Gaussova eliminace). V kapitole 4 bude uvedeno zobecnění tohoto algoritmu pro řešení obecné soustavy polynomiálních rovnic. Dimenze lineární variety je rovna $n - r$, kde r je hodnost matice (a_{ij}) . Tedy dimenze je dána počtem nezávislých rovnic.

Dalším příkladem afinní variety je Lagrangeova úloha, tzn. úloha hledání minima nebo maxima funkce (v tomto případě pouze funkce dané polynomem) na dané oblasti, které je také určena polynomiálními podmínkami. Například pro nalezení minima nebo maxima funkce $f(x, y, z) = x^3 + 2xyz - z^2$ na oblasti dané vztahem $g(x, y, z) = x^2 + y^2 + z^2 = 1$ je třeba řešit soustavu rovnic

$$\begin{aligned} 3x^2 + 2yz &= 2x\lambda, \\ 2xz &= 2y\lambda, \\ 2xy - 2z &= 2z\lambda, \\ x^2 + y^2 + z^2 &= 1, \end{aligned} \tag{3.2}$$

která definuje afinní varietu v $\mathbb{R}^4$.

Další možné aplikace afinních variet lze nalézt v robotice. Většinu sériových robotů i manipulátorů lze popsat pomocí soustavy polynomiálních rovnic. Pro nalezení řešení přímé i obrácené úlohy je potom nutné řešit tuto soustavu rovnic. Podrobněji se této problematice věnuje část 6.5.

Lemma 3.2.1 *Nechť $V, W \subset k^n$ jsou afinní variety. Potom také $V \cup W$ a $V \cap W$ jsou afinní variety a platí*

$$\begin{aligned} V \cap W &= \mathbf{V}(f_1, \dots, f_s, g_1, \dots, g_t), \\ V \cup W &= \mathbf{V}(f_i g_j) \text{ pro } 1 \leq i \leq s, 1 \leq j \leq t. \end{aligned}$$

Důkaz: Je zřejmé, podrobně viz [3], str. 11. □

Z lemmatu 3.2.1 pro výše uvedený příklad vyplývá, že

$$\mathbf{V}(zx, zy) = \mathbf{V}(z) \cup \mathbf{V}(x, y).$$

Obecně lze říci, že průnik konečného počtu afinních variet, resp. sjednocení konečného počtu afinních variet je opět afinní varietou.

3.3 Parametrizace afinních variet

Tato část bude věnována problému popisu bodů afinní variety. Pokud existuje nekonečně mnoho řešení soustavy obecně nelineárních algebraických rovnic $f_1 = \dots = f_s = 0$, potom je nutné danou afinní varietu parametrizovat.

Jednoduchým příkladem z lineární algebry může být soustava dvou lineárních rovnic pro tři neznámé

$$\begin{aligned} x + y + z &= 1, \\ x + 2y - z &= 3. \end{aligned}$$

Geometricky je řešení této soustavy reprezentováno přímkou v $\mathbb{R}^3$ danou jako průnik rovin $x + y + z = 1$ a $x + 2y - z = 3$. Soustava má nekonečně mnoho řešení a ze základních kurzů matematiky je zřejmé, že příslušná parametrizace bude

$$\begin{aligned} x &= -1 - 3t, \\ y &= 2 + 2t, \\ z &= t. \end{aligned}$$

Definice 3.3.1 *Nechť k je těleso. Racionální funkcí v proměnných $t_1, \dots, t_m$ s koeficienty v k se rozumí podíl f/g dvou polynomů $f, g \in k[t_1, \dots, t_m]$, kde g není nulový polynom. Navíc dvě racionální funkce f/g a h/k jsou si rovny, jestliže $kf = gh$ v $k[t_1, \dots, t_m]$. Množina všech racionálních funkcí v proměnných $t_1, \dots, t_m$ s koeficienty v k se značí $k(t_1, \dots, t_m)$.*

Snadno se definují operace sčítání a násobení, existuje inverzní prvek a tedy $k(t_1, \dots, t_m)$ je těleso.

Racionální parametrickou reprezentací variety $V = \mathbf{V}(f_1, \dots, f_s) \subset k^n$ se rozumí racionální funkce $r_1, \dots, r_n \in k(t_1, \dots, t_m)$ takové, že body dané vztahy

$$\begin{aligned} x_1 &= r_1(t_1, \dots, t_m), \\ &\vdots \\ x_n &= r_n(t_1, \dots, t_m) \end{aligned}$$

leží na V . Požaduje se také, aby V byla „nejmenší“ varieta obsahující tyto body.

Často je varieta V parametrizována polynomy místo racionálními funkcemi, což se nazývá *polynomiální parametrická reprezentace* variety V .

Naproti tomu původní soustava rovnic $f_1 = \dots = f_s = 0$, určující varietu V , se nazývá *implicitní reprezentace*.

Často je výhodné mít k dispozici jak parametrické tak implicitní vyjádření variety. Zatímco např. pro zobrazení variety pomocí počítače je výhodné parametrické vyjádření (a implicitní je naprosto nevhodné), pro zjištění, zda daný bod leží na varietě, je výhodné implicitní vyjádření (do kterého se pouze dosadí příslušné souřadnice a okamžitě je vidět výsledek) a parametrické je zde nevhodné, jelikož vede na řešení soustavy rovnic pro parametry variety. Potřeba mít k dispozici parametrické i implicitní vyjádření vede k následujícím otázkám:

- Existuje racionální parametrická reprezentace pro každou afinní varietu a lze ji nalézt?
- Existuje k parametricky zadané varietě implicitní popis a lze ho nalézt?

Obecná odpověď na první otázku je záporná. V podstatě lze říci, že většinu afinních variet parametrizovat nelze. Ty, u kterých se to podaří, nazýváme *neiracionální*. Obecně je obtížné říci, zda je varieta neiracionální nebo ne. Naproti tomu odpověď na druhou otázku je kladná. Existuje algoritmus, kterým k dané parametrizaci lze vždy nalézt implicitní popis. Tento algoritmus bude popsán v části 6.2.

3.4 Ideály

Tato část bude věnována seznámení s pojmem ideálu a naznačení souvislosti mezi ideály a afinními varietami. Důležitost ideálů je dána tím, že umožňují provádět výpočty na afinních varietách.

Definice 3.4.1 *Množina $I \subset k[x_1, \dots, x_n]$ se nazývá ideál v $k[x_1, \dots, x_n]$, jestliže platí:*

1. $0 \in I$,
2. *jestliže $f, g \in I$, potom $f + g \in I$,*
3. *jestliže $f \in I$ a $h \in k[x_1, \dots, x_n]$, potom $hf \in I$.*

Prvním příkladem ideálu v okruhu polynomů je ideál generovaný konečným počtem polynomů. Pro libovolnou s-tici polynomů $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ označme

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i f_i : h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\}. \quad (3.3)$$

Jak se ukáže v následujícím lemmatu, množina $\langle f_1, \dots, f_s \rangle$ je ideál.

Lemma 3.4.1 *Jestliže $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, potom $\langle f_1, \dots, f_s \rangle$ je ideál na množině $k[x_1, \dots, x_n]$.*

Důkaz: $0 \in \langle f_1, \dots, f_s \rangle$, protože $0 = \sum_{i=1}^s 0 \cdot f_i$. Dále nechť $f = \sum_{i=1}^s p_i f_i$ a $g = \sum_{i=1}^s q_i f_i$ a nechť $h \in k[x_1, \dots, x_n]$. Potom

$$\begin{aligned} f + g &= \sum_{i=1}^s (p_i + q_i) f_i, \\ hf &= \sum_{i=1}^s (hp_i) f_i, \end{aligned}$$

čímž je důkaz proveden. □

Definice 3.4.2 *Nechť $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Ideál $\langle f_1, \dots, f_s \rangle$, definovaný vztahem (3.3), se nazývá ideál generovaný polynomy $f_1, \dots, f_s$.*

Ideál $I \subset k[x_1, \dots, x_n]$ je *konečně generovaný*, jestliže existují $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ takové, že $I = \langle f_1, \dots, f_s \rangle$ a $f_1, \dots, f_s$ tvoří bázi I . Takových bází je pro každý ideál mnoho. V části 4.5 bude ukázáno, že každý ideál v $k[x_1, \dots, x_n]$ je konečně generovaný (Hilbertova věta o bázi) a že existuje jedna speciální a užitečná báze, která se nazývá Gröbnerova báze.

Věta 3.4.2 (Souvislost ideálů a afinních variet) *Jestliže $f_1, \dots, f_s$ a $g_1, \dots, g_t$ generují stejný ideál v $k[x_1, \dots, x_n]$, tedy $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$, potom se rovnají příslušné afinní variety, tj. platí*

$$\mathbf{V}(f_1, \dots, f_s) = \mathbf{V}(g_1, \dots, g_t).$$

Důkaz: Uvažujme libovolný $(a_1, \dots, a_n) \in \mathbf{V}(f_1, \dots, f_s)$. Pro něj platí, že

$$f_i(a_1, \dots, a_n) = 0 \quad \text{pro } i = 1, 2, \dots, s.$$

Protože $g_1, \dots, g_t \in \langle f_1, \dots, f_s \rangle$, existují nějaké polynomy $h_{1,1}, \dots, h_{t,s}$ v n proměnných tak, že

$$g_j = \sum_{i=1}^s h_{j,i} \cdot f_i \quad \text{pro } j = 1, 2, \dots, t.$$

Odtud plyne, že $g_j(a_1, \dots, a_n) = 0$ pro $j = 1, 2, \dots, t$. Máme tedy

$$\mathbf{V}(f_1, \dots, f_s) \subseteq \mathbf{V}(g_1, \dots, g_t).$$

Opačná inkluze se dokáže zcela analogicky. □

Příklad 3.1 Uvažujme afinní varietu $\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$. Jelikož platí

$$\begin{aligned} 2x^2 + 3y^2 - 11 &= 2(x^2 - 4) + 3(y^2 - 1), \\ x^2 - y^2 - 3 &= 1(x^2 - 4) - 1(y^2 - 1), \end{aligned}$$

lze psát, že $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ a tedy podle věty 3.4.2 platí

$$\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}.$$

Změnou báze ideálu je tedy možné snáze určit, jak daná varieta vypadá. ■

Věta 3.4.2 ve spojení s tzv. Gröbnerovou bází ideálu dává mocný nástroj pro hledání přesného řešení soustav rovnic definujících afinní variety.

Pro libovolnou afinní varietu $V \subset k^n$ označme

$$\mathbf{I}(V) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ pro všechna } (a_1, \dots, a_n) \in V\}. \quad (3.4)$$

Tato množina zahrnuje všechny polynomy, které nabývají nulové hodnoty ve všech bodech afinní variety, např. pro varietu $\mathbf{V}(y - x^2, z - x^3)$ patří do $\mathbf{I}(V)$ také polynomy $z - xy$ a $y^2 - xz$. To lze snadno ověřit, protože parametrizace řešení afinní variety může být např. $x = t, y = t^2, z = t^3$.

Lemma 3.4.3 *Jestliže $V \subset k^n$ je afinní varieta, potom $\mathbf{I}(V) \subset k[x_1, \dots, x_n]$ je ideál.*

Důkaz: Je zřejmé, že $0 \in \mathbf{I}(V)$. Nechť $f, g \in \mathbf{I}(V)$ a $h \in k[x_1, \dots, x_n]$. Nechť $(a_1, \dots, a_n)$ je libovolný bod z V . Potom

$$f(a_1, \dots, a_n) + g(a_1, \dots, a_n) = 0 \quad \text{a} \quad h(a_1, \dots, a_n)f(a_1, \dots, a_n) = 0.$$

Odtud potom plyne, že $\mathbf{I}(V)$ je ideál. □

Definice 3.4.3 *Nechť $V \subset k^n$ je afinní varieta. Ideál $\mathbf{I}(V)$, definovaný vztahem (3.4), se nazývá ideál variety V .*

Příkladem může být např. ideál variety $\mathbf{I}((0, 0, \dots, 0)) = \langle x_1, \dots, x_n \rangle$, tzn. v počátku se nulují všechny polynomy, patřící do ideálu $\langle x_1, \dots, x_n \rangle$. Dalším příkladem je $\mathbf{I}(k^n) = 0$ pro libovolné nekonečné těleso k , tzn. jediný polynom, který nabývá nuly ve všech bodech daného prostoru je nulový polynom.

Lemma 3.4.4 *Jestliže $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ a $V = \mathbf{V}(f_1, \dots, f_s)$, potom je $\langle f_1, \dots, f_s \rangle \subset \mathbf{I}(V)$, přičemž rovnost nemusí nastat.*

Důkaz: Uvažujme libovolný $f \in \langle f_1, \dots, f_s \rangle$. Ten lze psát jako

$$f = \sum_{i=1}^s h_i f_i \quad \text{pro nějaká } h_1, \dots, h_s \in k[x_1, \dots, x_n].$$

Pro $(a_1, \dots, a_n) \in V$ je tedy $f(a_1, \dots, a_n) = 0$. Proto platí $\langle f_1, \dots, f_s \rangle \subseteq \mathbf{I}(V)$. Dá se ale ukázat, že nemusí nastat rovnost. Například varieta $\mathbf{V}(x^2, y^2)$ má jediný bod $(0, 0)$. Potom je ale $\mathbf{I}(V) = \langle x, y \rangle$ a je zřejmé, že $\langle x^2, y^2 \rangle \subsetneq \langle x, y \rangle$ ($x \notin \langle x^2, y^2 \rangle$). □

Ačkoliv pro obecné těleso se $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ nemusí rovnat $\langle f_1, \dots, f_s \rangle$, ideál variety vždy obsahuje dostatek informací pro jednoznačné určení variety.

Věta 3.4.5 *Jsou-li V a W afinní variety v k^n , platí:*

1. $V \subset W$ právě tehdy, když $\mathbf{I}(V) \supset \mathbf{I}(W)$,

2. $V = W$ právě tehdy, když $\mathbf{I}(V) = \mathbf{I}(W)$.

Důkaz: Viz [3], str. 34. □

Základní otázky týkající se ideálů v $k[x_1, \dots, x_n]$ lze formulovat následujícím způsobem:

- Lze každý ideál $I \subset k[x_1, \dots, x_n]$ napsat jako $I = \langle f_1, \dots, f_s \rangle$ pro nějaké polynomy $f_1, \dots, f_s \in k[x_1, \dots, x_n]$?
- Mějme dány polynomy $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Existuje algoritmus, pomocí kterého lze rozhodnout, zda dané $f \in k[x_1, \dots, x_n]$ náleží ideálu $\langle f_1, \dots, f_s \rangle$?

Řešení těchto otázek pro polynomy z $k[x_1, \dots, x_n]$ bude provedeno v kapitole 4, pro speciální případ polynomů z $k[x]$ v části 3.5.

3.5 Polynomy v jedné proměnné

Tato část je věnována polynomům v jedné proměnné a známému algoritmu dělení polynomů. Tento jednoduchý algoritmus má některé překvapivě hluboké důsledky. Lze jej použít např. k určení struktury ideálu z $k[x]$ a k vysvětlení myšlenky největšího společného dělitele.

Definice 3.5.1 *Mějme dán nenulový polynom $f \in k[x]$. Nechť*

$$f = a_0x^m + a_1x^{m-1} + \dots + a_m,$$

kde $a_i \in k$ a $a_0 \neq 0$ (tedy $m = \deg(f)$). Potom a_0x^m je hlavní člen f a značí se $\text{LT}(f) = a_0x^m$.

Například pro polynom $f = 2x^3 - 4x + 3$ je hlavní člen $\text{LT}(f) = 2x^3$. Jestliže f a g jsou nenulové polynomy, potom

$$\deg(f) \leq \deg(g) \Leftrightarrow \text{LT}(f) \text{ dělí } \text{LT}(g).$$

Věta 3.5.1 (Algoritmus dělení polynomů) *Nechť k je těleso a nechť g je nenulový polynom v $k[x]$. Potom každé $f \in k[x]$ lze zapsat ve tvaru*

$$f = qg + r,$$

kde $q, r \in k[x]$ a buď $r = 0$ nebo $\deg(r) < \deg(g)$. Navíc q a r jsou jednoznačně určeny a existuje algoritmus pro jejich nalezení.

Důkaz: Je konstrukční, z důkazu plyne algoritmus pro nalezení q a r . Podrobně viz [3], str. 38. □

Důsledek 3.5.2 *Jestliže k je těleso a $f \in k[x]$ je nenulový polynom, potom f má nejvýše $\deg(f)$ kořenů v k .*

Důsledek 3.5.3 *Jestliže k je těleso, potom každý ideál z $k[x]$ je možné napsat ve tvaru $\langle f \rangle$ pro nějaké $f \in k[x]$. Navíc f je jednoznačně určeno vzhledem k násobení nenulovou konstantou z k .*

Generátor ideálu je nenulový polynom minimálního stupně obsažený v ideálu. Tento popis ale není vhodný k praktickému určení generátoru ideálu, jelikož by bylo nutné testovat stupně všech polynomů v ideálu, kterých je ale nekonečně mnoho. Existuje ale lepší cesta, jak najít generátor ideálu. Nástrojem potřebným k řešení tohoto problému je největší společný dělitel.

Definice 3.5.2 *Největším společným dělitelem polynomů $f, g \in k[x]$ je takový polynom h , pro který platí:*

1. h dělí f, g ,
2. *jestliže p je jiný polynom, který dělí f a g , potom p dělí h .*

Pokud h splňuje obě tyto vlastnosti, lze psát $h = \text{GCD}(f, g)$.

Věta 3.5.4 (Vlastnosti největšího společného dělitele) *Nechť $f, g \in k[x]$. Potom:*

1. $\text{GCD}(f, g)$ *existuje a je jediný vzhledem k násobení nenulovou konstantou z k ,*
2. $\text{GCD}(f, g)$ *je generátor ideálu $\langle f, g \rangle$,*
3. *existuje algoritmus pro nalezení $\text{GCD}(f, g)$.*

Důkaz: Podrobně viz [3], str. 41. Algoritmus pro nalezení největšího společného dělitele je založen na myšlence popsané v poznámce 3.5.5 a nazývá se Euklidův algoritmus. $\square$

Poznámka 3.5.5 *Použije-li se zápis $f = qg + r$, potom platí*

$$\text{GCD}(f, g) = \text{GCD}(f - qg, g) = \text{GCD}(r, g),$$

protože ideály $\langle f, g \rangle$ a $\langle f - qg, g \rangle$ jsou stejné. Jestliže $r \neq 0$, je možné proces opakovat. Lze psát, že $g = q'r + r'$, a podobnou úvahou se dostane, že

$$\text{GCD}(g, r) = \text{GCD}(r, r'),$$

kde $\deg(r) > \deg(r')$ nebo $r' = 0$. Opakováním tohoto procesu se dospěje k zápisu

$$\text{GCD}(f, g) = \text{GCD}(g, r) = \text{GCD}(r, r') = \text{GCD}(r', r'') = \dots,$$

kde stupně polynomů $g, r', r'', \dots$ postupně klesají nebo proces končí, když některý polynom $r, r', r'', \dots$ je nulový.

Příklad 3.2 Euklidův algoritmus demonstrujme na příkladě stanovení největšího společného dělitele polynomů $x^4 - 1$ a $x^6 - 1$. Pomocí algoritmu dělení polynomů se dostane

$$\begin{aligned}x^4 - 1 &= 0 \cdot (x^6 - 1) + x^4 - 1, \\x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1, \\x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0,\end{aligned}$$

což odpovídá zápisu

$$\begin{aligned}\text{GCD}(x^4 - 1, x^6 - 1) &= \text{GCD}(x^6 - 1, x^4 - 1) = \text{GCD}(x^4 - 1, x^2 - 1) = \\&= \text{GCD}(x^2 - 1, 0) = x^2 - 1.\end{aligned}$$

Poznamenejme, že výpočet GCD dává odpověď na otázku, jak najít generátor pro ideál $\langle x^4 - 1, x^6 - 1 \rangle$. Vzhledem k vlastnostem GCD a tomu, že $\text{GCD}(x^4 - 1, x^6 - 1) = x^2 - 1$ lze psát

$$\langle x^4 - 1, x^6 - 1 \rangle = \langle x^2 - 1 \rangle.$$

Tím byl nalezen generátor uvedeného ideálu. ■

Nyní je přirozené se ptát, co se stane, bude-li ideál generovaný třemi nebo více polynomy. Odpověď dává rozšíření definice pojmu GCD pro více než dva polynomy.

Definice 3.5.3 Největší společný dělitel polynomů $f_1, \dots, f_s \in k[x]$ je takový polynom h , pro který platí:

1. h dělí $f_1, \dots, f_s$,
2. jestliže p je jiný polynom, který dělí $f_1, \dots, f_s$, potom p dělí h .

Pokud má h tyto vlastnosti, lze psát $h = \text{GCD}(f_1, \dots, f_s)$.

Věta 3.5.6 (Vlastnosti největšího společného dělitele) Necht' $f_1, \dots, f_s$ jsou polynomy z $k[x]$ a $s \geq 2$. Potom:

1. $\text{GCD}(f_1, \dots, f_s)$ existuje a je jediný vzhledem k násobení nenulovou konstantou z k ,
2. $\text{GCD}(f_1, \dots, f_s)$ je generátor ideálu $\langle f_1, \dots, f_s \rangle$,
3. jestliže $s \geq 3$, potom $\text{GCD}(f_1, \dots, f_s) = \text{GCD}(f_1, \text{GCD}(f_2, \dots, f_s))$,
4. existuje algoritmus nalezení $\text{GCD}(f_1, \dots, f_s)$.

Důkaz: Viz [3], str. 43. □

Poznámka 3.5.7 K určení největšího společného dělitele více polynomů lze použít opakovaně Euklidův algoritmus.

Příklad 3.3 Uvažujme ideál $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle \subset k[x]$. Z věty 3.5.6 víme, že $\text{GCD}(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$ je generátor ideálu. Dá se ukázat, že platí

$$\begin{aligned} \text{GCD}(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \text{GCD}(x^3 - 3x + 2, \text{GCD}(x^4 - 1, x^6 - 1)) = \\ &= \text{GCD}(x^3 - 3x + 2, x^2 - 1) = x - 1. \end{aligned}$$

Odtud potom plyne, že

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle = \langle x - 1 \rangle.$$

Tím byl nalezen generátor uvedeného ideálu. ■

Závěr této části bude věnován řešení *problému příslušnosti k ideálu*, tzn. nalezení algoritmu pro ověření, zda polynom $f \in k[x]$ náleží ideálu $\langle f_1, \dots, f_s \rangle$. Prvním krokem algoritmu je nalezení generátoru h ideálu $\langle f_1, \dots, f_s \rangle$ pomocí největšího společného dělitele a úloha $f \in \langle f_1, \dots, f_s \rangle$ je potom ekvivalentní s úlohou $f \in \langle h \rangle$. Užitím algoritmu dělení polynomů lze f vyjádřit ve tvaru $f = qh + r$, kde $\deg(r) < \deg(h)$. Je zřejmé, že f náleží ideálu právě tehdy, když $r = 0$.

Příklad 3.4 Chtějme určit, zda

$$x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle.$$

Z příkladu 3.3 plyne, že generátor uvedeného ideálu je $x - 1$ a zbývá tedy určit, zda

$$x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle.$$

Pomocí algoritmu dělení lze $x^3 + 4x^2 + 3x - 7$ zapsat ve tvaru

$$x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$$

a tedy $x^3 + 4x^2 + 3x - 7$ nenáleží ideálu $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$. ■

Kapitola 4

Gröbnerovy báze

4.1 Úvod

Tato kapitola je věnována Gröbnerovým bázím, které umožňují řešit problémy spojené s polynomiálními ideály. V kapitole 3 bylo nastíněno několik problémů, které budou nyní probrány podrobněji.

Problémy:

1. Problém popisu ideálu: Je každý ideál $I \subset k[x_1, \dots, x_n]$ generovaný konečnou množinou polynomů? Neboli lze psát $I = \langle f_1, \dots, f_s \rangle$ pro nějaká $f_i \in k[x_1, \dots, x_n]$?
2. Problém příslušnosti k ideálu: Mějme dán polynom $f \in k[x_1, \dots, x_n]$ a ideál $I = \langle f_1, \dots, f_s \rangle$ a chtějme vědět, jestli $f \in I$. Geometricky tento problém úzce souvisí s problémem určení, zda $\mathbf{V}(f_1, \dots, f_s)$ leží na varietě $\mathbf{V}(f)$.
3. Problém řešení soustav nelineárních algebraických rovnic: Chtějme najít v k^n všechna řešení soustavy nelineárních algebraických rovnic

$$f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0.$$

Tento problém je shodný s hledáním bodů afinní variety $\mathbf{V}(f_1, \dots, f_s)$.

4. Problém převodu parametrického vyjádření na implicitní: Necht' V je podmnožina k^n daná parametricky vztahy

$$\begin{aligned} x_1 &= g_1(t_1, \dots, t_m), \\ &\vdots \\ x_n &= g_n(t_1, \dots, t_m). \end{aligned}$$

Jestliže jsou g_i polynomy (nebo racionální funkce) v proměnných t_j , potom V bude afinní varieta nebo její část. Chtějme najít soustavu nelineárních algebraických rovnic (v proměnných x_i), které definují tuto varietu.

Pro nalezení odpovědi na otázku (1) lze říci, že pro každý ideál definovaný na množině polynomů v konečně mnoha proměnných existuje konečná generující množina. Pouze v případě polynomů v nekonečně mnoha proměnných je odpověď záporná. Dále je zřejmé, že problémy (3) a (4) jsou vlastně vzájemně inverzní. V problému (3) se hledá řešení dané soustavy nelineárních algebraických rovnic. Naopak v problému (4) jsou dána řešení a úkolem je najít soustavu rovnic, která má tato řešení.

Příklad 4.1 Uvažujme afinní lineární podprostor $V \subset k^4$ definovaný vztahy

$$\begin{aligned}x_1 &= t_1 + t_2 + 1, \\x_2 &= t_1 - t_2 + 3, \\x_3 &= 2t_1 - 2, \\x_4 &= t_1 + 2t_2 - 3\end{aligned}$$

a hledejme soustavu lineárních rovnic, jejímž řešením jsou body V . Odečtením x_i od obou stran i -té rovnice lze rozšířenou matici soustavy zapsat ve tvaru

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{pmatrix},$$

kde první dva sloupce odpovídají t_j , další x_i a poslední sloupec je pravá strana. Matici lze převést na trojúhelníkový tvar

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{pmatrix}.$$

Poslední dva řádky této matice představují rovnice

$$x_1 - \frac{1}{4}x_3 - \frac{1}{2}x_4 - 3 = 0,$$

$$x_2 - \frac{3}{4}x_3 + \frac{1}{2}x_4 - 3 = 0,$$

které už neobsahují t_j a definují varietu V v k^4 . ■

Zbývající část této kapitoly bude věnována rozšíření metody užité v předchozím příkladě pro soustavy nelineárních algebraických rovnic libovolného stupně a libovolného počtu proměnných. K tomu je třeba zavést uspořádání monomů.

4.2 Uspořádání monomů v $k[x_1, \dots, x_n]$

Podrobným studiem algoritmu dělení polynomů v $k[x]$ a algoritmu Gaussovy eliminace pro soustavy lineárních rovnic lze dojít k závěru, že v obou těchto algoritmech hraje důležitou roli uspořádání členů v polynomech. V algoritmu dělení polynomů v jedné proměnné jsou jednotlivé členy řazeny sestupně podle jejich stupně, tzn.

$$\dots > x^{m+1} > x^m > \dots > x^2 > x > 1.$$

Funkčnost algoritmu závisí na tom, zda jsou systematicky brány vždy hlavní členy polynomů f a g .

Podobně při Gaussově eliminaci se pracuje v řádce vždy postupně s členy zleva. Uspořádání proměnných $x_1, \dots, x_n$ je tedy následující:

$$x_1 > x_2 > \dots > x_n.$$

Odtud lze usoudit, že důležitou součástí jakéhokoliv zobecnění algoritmu dělení pro polynomy ve více proměnných bude opět uspořádání členů v polynomech z $k[x_1, \dots, x_n]$. Tato část bude věnována studiu vlastností, které musí uspořádání mít a příkladům několika uspořádání, které tyto vlastnosti mají.

Nejdříve připomeňme, že existuje vzájemně jednoznačné přiřazení mezi monomy $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n} \in k[x_1, \dots, x_n]$ a n -ticemi $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Navíc každé uspořádání $>$ vytvořené na prostoru $\mathbb{Z}_{\geq 0}^n$ dává uspořádání monomů: jestliže $\alpha > \beta$ vzhledem k tomuto uspořádání, potom lze říci, že $x^\alpha > x^\beta$.

Jelikož polynom je suma monomů, je nutné uspořádat členy polynomů v sestupném (resp. vzestupném) pořadí. K tomu je třeba porovnat každé dva monomy a stanovit jejich vzájemnou pozici. Proto je nezbytné požadovat, aby naše uspořádání bylo *lineární* neboli *úplné*, tzn. že pro každou dvojici monomů x^α a x^β platí právě jeden ze vztahů

$$x^\alpha > x^\beta, \quad x^\alpha = x^\beta, \quad x^\beta > x^\alpha.$$

Každé uspořádání členů musí mít také následující vlastnost: jestliže $x^\alpha > x^\beta$ a x^γ je libovolný monom, potom $x^\alpha x^\gamma > x^\beta x^\gamma$. Pro odpovídající vektory exponentů a operace nad nimi to znamená, že jestliže $\alpha > \beta$ v uspořádání na $\mathbb{Z}_{\geq 0}^n$, potom pro všechna $\gamma \in \mathbb{Z}_{\geq 0}^n$ je $\alpha + \gamma > \beta + \gamma$.

Definice 4.2.1 Uspořádání monomů na $k[x_1, \dots, x_n]$ je libovolná relace $>$ na $\mathbb{Z}_{\geq 0}^n$ nebo ekvivalentně libovolná relace na množině monomů x^α , $\alpha \in \mathbb{Z}_{\geq 0}^n$, která splňuje:

1. $>$ je úplné (neboli lineární) uspořádání na $\mathbb{Z}_{\geq 0}^n$,
2. jestliže $\alpha > \beta$ a $\gamma \in \mathbb{Z}_{\geq 0}^n$, potom $\alpha + \gamma > \beta + \gamma$,
3. $>$ je dobré uspořádání na $\mathbb{Z}_{\geq 0}^n$. To znamená, že v každé neprázdné podmnožině $\mathcal{B} \subset \mathbb{Z}_{\geq 0}^n$ existuje prvek $m \in \mathcal{B}$ takový, že pro každé $\alpha \in \mathcal{B}$ platí $\alpha \geq m$.

Lemma 4.2.1 *Relace uspořádání $>$ na $\mathbb{Z}_{\geq 0}^n$ je dobré uspořádání právě tehdy, když každá ostře klesající posloupnost v $\mathbb{Z}_{\geq 0}^n$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

je konečná.

Důkaz: Viz [3], str. 54. □

Důležitost tohoto lemmatu se ukáže až dále. Některé algoritmy musí skončit po určité době právě proto, že členy ostře klesají (vzhledem k danému uspořádání monomů) v každém kroku algoritmu.

Nyní bude uvedeno několik možných způsobů uspořádání monomů, které budou dále používány.

Definice 4.2.2 (Lexikografické uspořádání) *Nechť $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Potom $\alpha >_{lex} \beta$, jestliže ve vektoru $\alpha - \beta \in \mathbb{Z}^n$ je první nenulová složka vektoru kladná a lze psát, že $x^\alpha >_{lex} x^\beta$.*

Uveďme několik příkladů:

- $(3, 2, 3) >_{lex} (1, 3, 6)$, jelikož $\alpha - \beta = (2, -1, -3)$,
- $(1, 4, 3) >_{lex} (1, 4, 2)$, jelikož $\alpha - \beta = (0, 0, 1)$,
- proměnné $x_1, \dots, x_n$ jsou uspořádány obvyklým způsobem při lexikografickém uspořádání:

$$(1, 0, \dots, 0) >_{lex} (0, 1, \dots, 0) >_{lex} \dots >_{lex} (0, \dots, 0, 1)$$

a tedy $x_1 >_{lex} x_2 >_{lex} \dots >_{lex} x_n$.

Existuje mnoho **lex** uspořádání pro daný polynom, vždy záleží na tom, jak jsou seřazeny proměnné, např. pro $x > y > z$ je **lex** uspořádání jiné než pro $z > y > x$. To znamená, že pro n proměnných existuje $n!$ různých **lex** uspořádání.

Při lexikografickém uspořádání hraje rozhodující roli uspořádání proměnných bez ohledu na celkový stupeň monomu. To znamená, že např. pro uspořádání $x > y > z$ je $x >_{lex} y^5 z^3$. Pro některé účely je ale třeba vzít v úvahu i celkový stupeň monomu a uspořádání monomů provést podle vyššího stupně monomu. Jednou z možných cest je *stupňované lexikografické uspořádání*.

Definice 4.2.3 (Stupňované lexikografické uspořádání) *Nechť $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Označme*

$$|\alpha| = \sum_{i=1}^n \alpha_i, \quad |\beta| = \sum_{i=1}^n \beta_i.$$

Potom $\alpha >_{grlex} \beta$, jestliže platí

$$|\alpha| > |\beta| \quad \text{nebo} \quad |\alpha| = |\beta| \wedge \alpha >_{lex} \beta.$$

Je vidět, že při tomto uspořádání se nejdříve uvažuje celkový stupeň monomu a až následně pro stejný stupeň monomů lexikografické uspořádání, např.

- $(1, 2, 3) >_{grlex} (3, 2, 0)$, jelikož $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$,
- $(1, 2, 4) >_{grlex} (1, 1, 5)$, jelikož $|(1, 2, 4)| = |(1, 1, 5)|$ a $(1, 2, 4) >_{lex} (1, 1, 5)$,
- proměnné jsou uspořádány podle lexikografického uspořádání $x_1 >_{grlex} \cdots >_{grlex} x_n$.

Podobně jako u **lex** uspořádání existuje $n!$ různých **grlex** uspořádání na n proměnných, záviselých na seřazení daných proměnných.

Dalším příkladem uspořádání monomů je *stupňované inverzní lexikografické* uspořádání.

Definice 4.2.4 (Stupňované inverzní lexikografické uspořádání) *Nechť $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Označme*

$$|\alpha| = \sum_{i=1}^n \alpha_i, \quad |\beta| = \sum_{i=1}^n \beta_i.$$

Potom $\alpha >_{grelex} \beta$, jestliže platí

$$|\alpha| > |\beta|$$

nebo $|\alpha| = |\beta|$ a v rozdílu $\alpha - \beta \in \mathbb{Z}^n$ je poslední nenulová složka vektoru záporná.

Jednoduché příklady:

- $(4, 7, 1) >_{grelex} (4, 2, 3)$, jelikož $|(4, 7, 1)| = 12 > |(4, 2, 3)| = 9$,
- $(1, 5, 2) >_{grelex} (4, 1, 3)$, jelikož $|(1, 5, 2)| = |(4, 1, 3)|$ a $\alpha - \beta = (-3, 4, -1)$,
- proměnné jsou uspořádány standardním způsobem, tzn. $x_1 >_{grelex} x_2 >_{grelex} \cdots >_{grelex} x_n$.

Rozdíly mezi **grlex** a **grelex** uspořádáním nastanou v případě rovnosti celkových stupňů monomů. Uspořádání **grlex** používá v takovém případě **lex** uspořádání a upřednostňuje vyšší mocninu největší proměnné. Naproti tomu uspořádání **grelex** dává přednost nižší mocnině nejmenší proměnné.

Jestliže $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ je polynom v $k[x_1, \dots, x_n]$, potom každé uspořádání monomů jednoznačně určuje pořadí monomů.

Příklad 4.2 Vezměme polynom $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$. Potom

- pro **lex** uspořádání dostaneme $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$
- pro **grlex** uspořádání dostaneme $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$
- pro **grelex** uspořádání dostaneme $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$ ■

V následující definici zavedeme některá označení, která budou používána v dalších částech textu.

Definice 4.2.5 *Nechť $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ je nenulový polynom v $k[x_1, \dots, x_n]$ a nechť $>$ je uspořádání monomů. Potom:*

1. Maximální stupeň polynomu f je $\text{multideg}(f) = \max(\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0)$.
2. Hlavní koeficient polynomu f je $\text{LC}(f) = a_{\text{multideg}(f)} \in k$.
3. Hlavní monom polynomu f je $\text{LM}(f) = x^{\text{multideg}(f)}$.
4. Hlavní člen polynomu f je $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$.

Například pro $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ s uvažováním lexikografického uspořádání je $\text{multideg}(f) = (3, 0, 0)$, $\text{LC}(f) = -5$, $\text{LM}(f) = x^3$, $\text{LT}(f) = -5x^3$.

4.3 Algoritmus dělení v $k[x_1, \dots, x_n]$

V této části bude uvedeno rozšíření klasického algoritmu dělení v $k[x]$ pro polynomy v $k[x_1, \dots, x_n]$. V obecném případě je cílem vydělení polynomu $f \in k[x_1, \dots, x_n]$ s-ticí polynomů $f_1, \dots, f_s \in k[x_1, \dots, x_n]$.

Základní myšlenka algoritmu je stejná jako v případě jedné proměnné: je nutné anulovat hlavní člen f (s ohledem na uspořádání monomů) vynásobením některého f_i vhodným monomem a odečtením. Potom tento monom odpovídá a_i . Nejdříve bude uveden příklad.

Příklad 4.3 V tomto příkladě budou demonstrovány problémy, které mohou vznikat pouze v souvislosti s dělením polynomů ve více než jedné proměnné. Úkolem je vydělit $f = x^2y + xy^2 + y^2$ polynomy $f_1 = xy - 1$ a $f_2 = y^2 - 1$ s použitím lexikografického uspořádání s $x > y$. První dva kroky algoritmu jsou standardní, přičemž dostaneme

$$\begin{array}{rcl}
 x^2y + xy^2 + y^2 & : & \begin{array}{l} f_1 \\ xy - 1 \\ y^2 - 1 \end{array} = \begin{array}{l} a_i \\ x + y \end{array} \\
 \hline
 x^2y - x & & \\
 xy^2 + x + y^2 & & \\
 \hline
 xy^2 - y & & \\
 x + y^2 + y & &
 \end{array}$$

Je vidět, že ani $\text{LT}(f_1) = xy$ ani $\text{LT}(f_2) = y^2$ nedělí $\text{LT}(x + y^2 + y) = x$. Ale $x + y^2 + y$ není zbytek po dělení, protože $\text{LT}(f_2)$ dělí y^2 . Proto se x přesune do zbytku a dělení pokračuje dále. Pro zbytek r je vytvořen zvláštní sloupec, kam budou zařazovány členy patřící do zbytku.

Obecněji lze říci, že pokud nelze dělit ani $\text{LT}(f_1)$ ani $\text{LT}(f_2)$, přesune se hlavní člen do zbytku a dělení pokračuje dále. Celé dělení lze zapsat ve tvaru:

$$\begin{array}{rcl}
x^2y + xy^2 + y^2 & : & \begin{array}{l} f_i \\ xy - 1 \\ y^2 - 1 \end{array} = \begin{array}{l} a_i \\ x + y \\ 1 \end{array} r \\
\hline
x^2y - x & & \\
xy^2 + x + y^2 & & \\
\hline
xy^2 - y & & \\
x + y^2 + y & & \\
\hline
y^2 + y & \longrightarrow & x \\
y^2 - 1 & & \\
\hline
y + 1 & & \\
1 & \longrightarrow & x + y \\
\hline
0 & \longrightarrow & x + y + 1
\end{array}$$

Lze tedy psát $x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$. ■

Věta 4.3.1 (Algoritmus dělení v $k[x_1, \dots, x_n]$) *Nechť $>$ je uspořádání monomů na $\mathbb{Z}_{\geq 0}^n$ a nechť $F = (f_1, \dots, f_s)$ je uspořádaná s -tice polynomů z $k[x_1, \dots, x_n]$. Potom každý polynom $f \in k[x_1, \dots, x_n]$ je možné vyjádřit ve tvaru*

$$f = a_1 f_1 + \dots + a_s f_s + r,$$

kde $a_i, r \in k[x_1, \dots, x_n]$ a buď $r = 0$ nebo r je lineární kombinace monomů s koeficienty z k , z nichž žádný není dělitelný $\text{LT}(f_1), \dots, \text{LT}(f_s)$. Člen r se nazývá zbytek f po dělení F . Navíc jestliže $a_i f_i \neq 0$, potom platí $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$.

Důkaz: Existence koeficientů a_i a zbytku r se dokáže sestavením algoritmu pro jejich nalezení. Algoritmus pro dělení polynomů ve více proměnných má následující podobu:

```

INPUT:  $f_1, \dots, f_s, f$ 
OUTPUT:  $a_1, \dots, a_s, r$ 
 $a_1 := 0; \dots; a_s := 0; r := 0$ 
 $p := f$ 
WHILE  $p \neq 0$  DO
     $i := 1$ 
    PROVEDENO DĚLENÍ := FALSE
    WHILE  $i \leq s$  AND PROVEDENO DĚLENÍ = FALSE DO
        IF  $\text{LT}(f_i)$  DĚLÍ  $\text{LT}(p)$  THEN
             $a_i := a_i + \text{LT}(p)/\text{LT}(f_i)$ 
             $p := p - (\text{LT}(p)/\text{LT}(f_i)) f_i$ 
            PROVEDENO DĚLENÍ := TRUE
        ELSE
             $i := i + 1$ 
    IF PROVEDENO DĚLENÍ = FALSE THEN
         $r := r + \text{LT}(p)$ 
         $p := p - \text{LT}(p)$ 

```

Při každém průchodu vnějším cyklem se provede právě jeden z příkazů $p := p - \text{LT}(p)$, $p := p - (\text{LT}(p)/\text{LT}(f_i))f_i$ a tedy stupeň p klesne. Proto algoritmus skončí.

Platí invariant $f = a_1f_1 + \dots + p + r$, a přitom každý člen každého a_i je podílem $\text{LT}(p)/\text{LT}(f_i)$ z nějakého okamžiku. Proto stupeň těchto členů je menší než stupeň p v daném okamžiku a ten je nejvýše roven stupni f . Dohromady stupeň každého a_if_i je menší nebo roven stupni f . $\square$

Tato část bude uzavřena posouzením vlastností algoritmu dělení polynomů ve více proměnných. Důležitou vlastností algoritmu dělení v $k[x]$ je jednoznačné určení zbytku. Z příkladu 4.4 ale vyplývá, že to už neplatí pro algoritmus dělení ve více proměnných. Nejlépe uvedený algoritmus funguje ve spojení s tzv. Gröbnerovou bází.

Příklad 4.4 Polynom $f = x^2y + xy^2 + y^2$ má být vydělen polynomy $f_1 = y^2 - 1$ a $f_2 = xy - 1$ s použitím lexikografického uspořádání s $x > y$. Jedná se tedy o obdobu příkladu 4.3, pouze je zaměněno pořadí dělitelů. Provedení dělení podle uvedeného algoritmu vede k zápisu

$$\begin{array}{rcl}
 x^2y + xy^2 + y^2 & : & \begin{array}{l} f_i \\ y^2 - 1 \\ xy - 1 \end{array} = \begin{array}{l} a_i \\ x + 1 \\ x \end{array} r \\
 \hline
 x^2y - x & & \\
 xy^2 + x + y^2 & & \\
 \hline
 xy^2 - x & & \\
 2x + y^2 & & \\
 \hline
 y^2 & \longrightarrow & 2x \\
 y^2 - 1 & & \\
 \hline
 1 & & \\
 0 & \longrightarrow & 2x + 1
 \end{array}$$

Potom tedy

$$x^2y + xy^2 + y^2 = (x + 1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1.$$

Srovnáním s příkladem 4.3 je zřejmé, že zbytek je při záměně pořadí dělitelů jiný. $\blacksquare$

Zbytek r tedy není jednoznačně určený vzhledem k požadavku, aby žádný z členů r nebyl dělitelný $\text{LT}(f_1), \dots, \text{LT}(f_s)$. Příklady 4.3 a 4.4 ukazují, že $a_1, \dots, a_s, r$ závisí na uspořádání s -tice polynomů $(f_1, \dots, f_s)$.

Algoritmus dělení polynomů ve více proměnných úzce souvisí s řešením problému příslušnosti k ideálu. Jestliže po dělení polynomu f s -ticí $F = (f_1, \dots, f_s)$ je zbytek $r = 0$, potom

$$f = a_1f_1 + \dots + a_sf_s$$

a $f \in \langle f_1, \dots, f_s \rangle$. Je tedy vidět, že $r = 0$ je *postačující* podmínkou pro příslušnost k ideálu. Následující příklad demonstruje, že to ale není podmínka *nutná*.

Příklad 4.5 Necht $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x]$ s **lex** uspořádáním. Úkolem je vydělit polynom $f = xy^2 - x$ dvojicí polynomů $F = (f_1, f_2)$. Provedením algoritmu dělení je možné f vyjádřit ve tvaru

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Dělení dvojicí polynomů $F = (f_2, f_1)$ vede k zápisu

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Odtud je vidět, že $f \in \langle f_1, f_2 \rangle$, a přesto při dělení $F = (f_1, f_2)$ je zbytek nenulový. ■

Další části budou věnovány hledání vhodné generující množiny, pro kterou dává algoritmus dělení polynomů ve více proměnných jednoznačné výsledky. Ukáže se, že touto vhodnou generující množinou ideálu je tzv. Gröbnerova báze daného ideálu.

4.4 Monomické ideály a Dicksonovo lemma

Tato část se bude zabývat speciálním případem ideálů, tzv. monomickými ideály.

Definice 4.4.1 Ideál $I \subset k[x_1, \dots, x_n]$ se nazývá monomický ideál, jestliže existuje podmnožina $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^n$ (i nekonečná) taková, že I obsahuje všechny polynomy ve tvaru konečné sumy $\sum_{\alpha \in \mathcal{A}} h_{\alpha} x^{\alpha}$, kde $h_{\alpha} \in k[x_1, \dots, x_n]$. Potom $I = \langle x^{\alpha} : \alpha \in \mathcal{A} \rangle$.

Příkladem monomického ideálu je ideál $I = \langle x^4 y^2, x^3 y^4, x^2 y^5 \rangle \subset k[x, y]$. Naopak příkladem ideálu, který není monomický, je ideál $J = \langle xy^2 - y^3, x^2 y^3 + xy^4 \rangle$.

Lemma 4.4.1 Necht $I = \langle x^{\alpha} : \alpha \in \mathcal{A} \rangle$ je monomický ideál. Potom monom x^{β} náleží I právě tehdy, když x^{β} je dělitelné x^{α} pro nějaké $\alpha \in \mathcal{A}$.

Důkaz: Je technický, podrobně viz [3], str. 69. □

Lemma 4.4.2 Necht I je monomický ideál a necht $f \in k[x_1, \dots, x_n]$. Potom jsou následující tvrzení ekvivalentní:

1. $f \in I$,
2. každý člen f leží v I ,
3. f je lineární kombinací monomů z I s koeficienty z k .

Důkaz: Implikace $3 \Rightarrow 2 \Rightarrow 1$ jsou triviální. Zbývá tedy ukázat, že $1 \Rightarrow 3$. Platí, že $f = \sum_{\alpha} a_{\alpha} x^{\alpha} \in I$, kde $a_{\alpha} \in k$. Z předpokladu vyplývá, že lze vyjádřit $f = \sum_{\beta \in \mathcal{A}} h_{\beta} x^{\beta}$, kde $h_{\beta} \in k[x_1, \dots, x_n]$. Každý člen $a_{\alpha} x^{\alpha}$ se musí rovnat některému členu z druhé rovnosti, tedy existují taková $d \in k, \delta \in \mathbb{Z}_{\geq 0}^n$ tak, že $a_{\alpha} x^{\alpha} = d x^{\beta + \delta}$. Proto $x^{\alpha} \in I$ a tedy platí 3. □

Důsledek 4.4.3 *Dva monomické ideály splývají právě tehdy, když obsahují stejné monomy.*

Hlavním výsledkem této části je tvrzení, že každý monomický ideál z $k[x_1, \dots, x_n]$ je konečně generovaný.

Věta 4.4.4 (Dicksonovo lemma) *Každý monomický ideál $I = \langle x^\alpha : \alpha \in \mathcal{A} \rangle \subset k[x_1, \dots, x_n]$ lze napsat ve tvaru*

$$I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle,$$

kde $\alpha(1), \dots, \alpha(s) \in \mathcal{A}$. Ideál I má konečnou bázi.

Důkaz: Provádí se indukcí podle počtu proměnných, podrobně viz [3], str. 70. □

Důsledek 4.4.5 *Nechť $>$ je relace na $\mathbb{Z}_{\geq 0}^n$ splňující:*

1. *$>$ je úplné uspořádání na $\mathbb{Z}_{\geq 0}^n$,*
2. *jestliže $\alpha > \beta$ a $\gamma \in \mathbb{Z}_{\geq 0}^n$, potom $\alpha + \gamma > \beta + \gamma$. Potom $>$ je dobré uspořádání právě tehdy, když $\alpha \geq 0 \ \forall \alpha \in \mathbb{Z}_{\geq 0}^n$.*

Užitím důsledku 4.4.5 lze zjednodušit definici 4.2.1. Podmínky 1 a 2 zůstanou beze změn, pouze podmínka 3 se nahradí jednodušší podmínkou $\alpha \geq 0 \ \forall \alpha \in \mathbb{Z}_{\geq 0}^n$. Ověření této podmínky (a tedy zjištění, zda uspořádání je uspořádáním monomů) je mnohem snazší.

4.5 Věta o Hilbertově bázi a Gröbnerovy báze

V této části bude provedeno kompletní řešení problému popisu ideálu, přičemž bude zaměřena na báze ideálu, které mají jisté dobré vlastnosti vzhledem k algoritmu dělení popsanému v 4.3. Klíčem je myšlenka, že pro dané uspořádání monomů odpovídá každému polynomu $f \in k[x_1, \dots, x_n]$ jednoznačně určený hlavní člen $\text{LT}(f)$.

Definice 4.5.1 *Nechť $I \subset k[x_1, \dots, x_n]$ je ideál různý od $\{0\}$, tzn. obsahuje alespoň jeden polynom různý od nuly.*

1. *Označme $\text{LT}(I)$ množinu hlavních členů prvků I . Tedy*

$$\text{LT}(I) = \{cx^\alpha : \text{existuje } f \in I \text{ takové, že } \text{LT}(f) = cx^\alpha\}.$$

2. *Označme $\langle \text{LT}(I) \rangle$ ideál generovaný prvky $\text{LT}(I)$.*

Hlavní členy hrály důležitou roli v algoritmu dělení popsanému v 4.3. Pro danou konečnou generující množinu ideálu $I = \langle f_1, \dots, f_s \rangle$, mohou být $\langle \text{LT}(I) \rangle$ a $\langle \text{LT}(f_1), \dots, \text{LT}(f_s) \rangle$ různé ideály. Je pravda, že $\text{LT}(f_i) \in \text{LT}(I) \subset \langle \text{LT}(I) \rangle$, z čehož plyne $\langle \text{LT}(f_1), \dots, \text{LT}(f_s) \rangle \subset \langle \text{LT}(I) \rangle$. Avšak $\langle \text{LT}(I) \rangle$ může být i ostře větší. To bude ukázáno v následujícím příkladě.

Příklad 4.6 Necht $I = \langle f_1, f_2 \rangle$, kde $f_1 = x^3 - 2xy$ a $f_2 = x^2y - 2y^2 + x$ a použijme **grlex** uspořádání monomů v $k[x, y]$. Potom

$$x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2$$

a tedy $x^2 \in I$. Tudíž $x^2 = \text{LT}(x^2) \in \langle \text{LT}(I) \rangle$. Ale x^2 není dělitelné $\text{LT}(f_1) = x^3$ nebo $\text{LT}(f_2) = x^2y$ a tedy $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$. ■

Věta 4.5.1 *Necht $I \subset k[x_1, \dots, x_n]$ je ideál. Potom*

1. $\langle \text{LT}(I) \rangle$ je monomický ideál,
2. existuje $g_1, \dots, g_t \in I$ takové, že $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$.

Důkaz: Podrobně viz [3], str. 75. □

Jelikož je $\langle \text{LT}(I) \rangle$ monomický ideál, je možné aplikovat poznatky z části 4.4, zejména Dicksonovo lemma k důkazu druhé části věty 4.5.1. Tato věta může být potom společně s algoritmem dělení polynomů použita k důkazu existence konečné generující množiny pro každý polynomiální ideál.

Věta 4.5.2 (Hilbertova věta o bázi) *Každý ideál $I \subset k[x_1, \dots, x_n]$ má konečnou generující množinu. Proto $I = \langle g_1, \dots, g_t \rangle$ pro nějaké $g_1, \dots, g_t \in I$.*

Důkaz: Pokud by $I = \{0\}$, za generující množinu lze vzít $\{0\}$, která je jistě konečná. Pokud I obsahuje nějaký nenulový polynom, potom podle předchozí věty (a podle Dicksonova lemmatu) existují $g_1, \dots, g_t$ takové, že $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$. Předpokládejme, že $I = \langle g_1, \dots, g_t \rangle$.

Je zřejmé, že $\langle g_1, \dots, g_t \rangle \subset I$, protože každé $g_i \in I$. Vezměme nyní libovolný polynom $f \in I$ a vydělme ho polynomy $g_1, \dots, g_t$. Potom lze psát

$$f = a_1g_1 + \dots + a_tg_t + r,$$

kde žádný člen r není dělitelný $\text{LT}(g_1), \dots, \text{LT}(g_t)$. Je vidět, že

$$r = f - a_1g_1 - \dots - a_tg_t \in I.$$

Pokud by $r \neq 0$, potom nutně $\text{LT}(r) \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$, a protože je $\langle \text{LT}(I) \rangle$ monomiální, musí být $\text{LT}(r)$ dělitelný některým z jeho generátorů $\text{LT}(g_i)$. To je ale ve sporu s tím, že r je zbytek po dělení. Proto $r = 0$. Potom

$$f = a_1g_1 + \dots + a_tg_t + 0 \in \langle g_1, \dots, g_t \rangle.$$

Odtud plyne, že $I \subset \langle g_1, \dots, g_t \rangle$, čímž je důkaz ukončen. □

Věta 4.5.2 dává odpověď na problém popisu ideálu. Navíc speciální vlastností báze popsané ve větě 4.5.2 je, že

$$\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle.$$

Taková báze bude speciálně označena.

Definice 4.5.2 Zvolme uspořádání monomů. Řekneme, že konečná množina $G = \{g_1, \dots, g_t\}$ ideálu I je Gröbnerovou bází (nebo standardní bází), jestliže

$$\langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle.$$

Ekvivalentně lze říci, že množina $\{g_1, \dots, g_t\} \subset I$ je Gröbnerovou bází I právě tehdy, když hlavní člen libovolného prvku I je dělitelný $\text{LT}(g_i)$ pro nějaké i .

Důsledek 4.5.3 Zvolme uspořádání monomů. Potom každý ideál $I \subseteq k[x_1, \dots, x_n]$ má Gröbnerovu bází. Naopak každá množina polynomů $g_1, \dots, g_t \in I$, pro kterou platí $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$, je Gröbnerovou bází ideálu I .

Například pro bází $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$ z příkladu 4.6 je vidět, že vzhledem ke **grlex** uspořádání není Gröbnerovou bází, jelikož $x^2 \in \langle \text{LT}(I) \rangle$, ale $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$. Podrobněji bude problematika určování, zda je daná báze Gröbnerovou bází, zmíněna později.

Tato část bude zakončena dvěma aplikacemi Hilbertovy věty o bázi. První je tvrzení o ideálech v $k[x_1, \dots, x_n]$. Vzestupná řada ideálu je posloupnost

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

Například posloupnost $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \dots \subset \langle x_1, \dots, x_n \rangle$ tvoří konečnou vzestupnou řadu ideálů.

Věta 4.5.4 (Podmínka vzestupné řady) Nechť $I_1 \subset I_2 \subset I_3 \subset \dots$ tvoří vzestupnou řadu ideálů v $k[x_1, \dots, x_n]$. Potom existuje $N \geq 1$ takové, že

$$I_N = I_{N+1} = I_{N+2} = \dots$$

Důkaz: Označme $I = \bigcup_{i=1}^{\infty} I_i$. Zřejmě I je ideál. Podle Hilbertovy věty existují $f_1, \dots, f_s$ tak, že $I = \langle f_1, \dots, f_s \rangle$. Ale každý generátor je obsažen v nějakém I_j , tedy $f_i \in I_{j_i}$ pro nějaké j_i . Vezměme N jako maximum z těchto j_i . Potom tedy $f_i \in I_N$ pro všechna i . Lze tedy psát

$$I = \langle f_1, \dots, f_s \rangle \subset I_N \subset I_{N+1} \subset \dots \subset I$$

a všechny tyto ideály jsou si rovny. □

Tvrzení, že každá vzestupná řada ideálu v $k[x_1, \dots, x_n]$ se stabilizuje, se zkráceně nazývá ACC (*Ascending Chain Condition*) a je ekvivalentní důsledku Hilbertovy věty o bázi.

Druhý důsledek Hilbertovy věty o bázi je geometrický. Afinní variety byly dosud uvažovány jako množiny řešení konečné soustavy polynomiálních rovnic

$$\mathbf{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \ \forall i\}.$$

Hilbertova věta o bázi ukazuje, že má také smysl hovořit o afinních varietách definovaných ideálem $I \subset k[x_1, \dots, x_n]$.

Definice 4.5.3 *Nechť $I \subset k[x_1, \dots, x_n]$ je ideál. Označme $V(I)$ množinu*

$$V(I) = \{(a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \forall f \in I\}.$$

Přestože nenulový ideál I vždy obsahuje nekonečně mnoho různých polynomů, množinu $V(I)$ lze vždy definovat pomocí konečné soustavy polynomiálních rovnic.

Věta 4.5.5 *Jestliže $I = \langle f_1, \dots, f_s \rangle$, potom $V(I) = V(f_1, \dots, f_s)$ a tedy $V(I)$ je afinní varieta.*

Nejdůležitějším důsledkem věty 4.5.5 je, že **variety jsou určeny ideály**.

4.6 Vlastnosti Gröbnerovýchází

Tato část bude věnována vlastnostem Gröbnerovýchází a možnostem určení, zda daná báze ideálu je Gröbnerovouází.

Věta 4.6.1 *Nechť $G = \{g_1, \dots, g_t\}$ je Gröbnerova báze ideálu $I \subset k[x_1, \dots, x_n]$ a $f \in k[x_1, \dots, x_n]$. Potom existuje jediné $r \in k[x_1, \dots, x_n]$ s následujícími vlastnostmi:*

1. žádný člen r není dělitelný žádným z hlavních členů $LT(g_1), \dots, LT(g_t)$,
2. existuje $g \in I$ takové, že $f = g + r$.

Důkaz: Viz [27], str. 17. □

Ačkoliv zbytek r je určený jednoznačně, koeficienty a_i získané algoritmem dělení (dostaneme $f = a_1g_1 + \dots + a_tg_t + r$) se mohou měnit v závislosti na pořadí $g_1, \dots, g_t$.

Důsledek 4.6.2 *Nechť $f \in k[x_1, \dots, x_n]$ a nechť $G = \{g_1, \dots, g_t\}$ je Gröbnerova báze pro ideál $I \subset k[x_1, \dots, x_n]$. Potom $f \in I$ právě tehdy, když zbytek po dělení f prvky báze G je nula.*

Tato vlastnost se také někdy bere jako definice Gröbnerovy báze, protože je ekvivalentní s podmínkou $\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$. Užití důsledku 4.6.2 vede k algoritmu pro řešení příslušnosti k ideálu. Za předpokladu, že je známa Gröbnerova báze G ideálu, je potřeba pouze spočítat zbytek po dělení f prvky báze G .

Zbývá ukázat, jak lze najít Gröbnerovuází. K tomu je nutné zavést nejprve některé další pojmy a označení.

Definice 4.6.1 *Označíme $\bar{f}^F$ zbytek po dělení f uspořádanou s -ticí $F = (f_1, \dots, f_s)$.*

Definice 4.6.2 *Nechť $f, g \in k[x_1, \dots, x_n]$ jsou nenulové polynomy.*

1. Necht $\text{multideg}(f) = \alpha$, $\text{multideg}(g) = \beta$ a necht $\gamma = (\gamma_1, \dots, \gamma_n)$, kde $\gamma_i = \max(\alpha_i, \beta_i)$ pro každé i . Monom x^γ se nazývá nejmenší společný násobek $\text{LM}(f)$ a $\text{LM}(g)$ a značí se $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$.

2. S-polynom polynomů f a g je kombinace

$$S(f, g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g.$$

Například necht $f = x^3y^2 - x^2y^3 + x$ a $g = 3x^4y + y^2$ v $\mathbb{R}[x, y]$ a uvažujme **grlex** uspořádání. Potom $\gamma = (4, 2)$ a

$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x \cdot f - \frac{1}{3}y \cdot g = -x^3y^3 + x^2 - \frac{1}{3}y^3.$$

Lemma 4.6.3 *Mějme součet tvaru $\sum_{i=1}^t c_i x^{\alpha(i)} g_i$, kde $c_1, \dots, c_t$ jsou konstanty a $\alpha(i) + \text{multideg}(g_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ pro $c_i \neq 0$. Jestliže*

$$\text{multideg}\left(\sum_{i=1}^t c_i x^{\alpha(i)} g_i\right) < \delta,$$

potom existují konstanty c_{jk} takové, že

$$\sum_{i=1}^t c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k),$$

kde $x^{\gamma_{jk}} = \text{LCM}(\text{LM}(g_j), \text{LM}(g_k))$. Navíc každé $x^{\delta - \gamma_{jk}} S(g_j, g_k)$ má maximální stupeň menší než δ .

Důkaz: Podrobně viz [3], str.83. □

Pomocí S-polynomu a lemmatu 4.6.3 lze formulovat následující kritérium, ze kterého vyplývá algoritmus pro ověření, kdy je báze ideálu Gröbnerovou bází.

Věta 4.6.4 (Nutná a postačující podmínka Gröbnerovy báze) *Necht I je polynomiální ideál. Potom báze $G = \{g_1, \dots, g_t\}$ je Gröbnerovou bází pro ideál I právě tehdy, když pro všechny dvojice $i, j, i \neq j$ je zbytek po dělení $S(g_i, g_j)$ prvky báze G (seřazené v jistém pořadí) roven nule.*

Důkaz: Viz [27], str. 19. □

Příklad 4.7 Uvažujme ideál $I = \langle y - x^2, z - x^3 \rangle$ a ukažme, že $G = \{y - x^2, z - x^3\}$ je Gröbnerova báze vzhledem k **lex** uspořádání pro $y > z > x$. K důkazu lze užít větu 4.6.4. Báze G má pouze dva členy a tedy stačí ověřit, že zbytek po dělení S-polynomu

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = yx^3 - zx^2$$

prvky báze G je nula. Provedením algoritmu dělení lze dostat

$$yx^3 - zx^2 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0$$

a tedy $\overline{S(y - x^2, z - x^3)}^G = 0$. Podle předchozí věty je tedy G Gröbnerovou bází. Podobně by bylo možné ověřit, že G není Gröbnerovou bází vzhledem k **lex** uspořádání pro $x > y > z$. ■

4.7 Buchbergerův algoritmus

Tato část bude věnována zejména algoritmu nalezení Gröbnerovy báze pro ideál $I \subset k[x_1, \dots, x_n]$.

Příklad 4.8 Uvažujme $k[x, y]$ s **grlex** uspořádáním a necht' $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Podle věty 4.6.4 lze snadno ověřit, že $\{f_1, f_2\}$ není Gröbnerovou bází ideálu I , jelikož $\text{LT}(S(f_1, f_2)) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$.

První přirozenou myšlenkou, jak vytvořit Gröbnerovu bází, je rozšířit původní generující množinu na Gröbnerovu bází přidáním polynomů do generující množiny ideálu I . V jistém smyslu to nepřináší nic nového a pouze to vnáší redundanci do báze I . Avšak další informace, které lze získat z Gröbnerovy báze, to vynahradí.

Které další generátory je nutné přidat? Pro S-polynom $S(f_1, f_2) = -x^2 \in I$ je zbytek po dělení $F = \{f_1, f_2\}$ roven $-x^2$, je tedy nenulový a měl by být přidán do generující množiny jako nový generátor $f_3 = -x^2$. Potom $F = \{f_1, f_2, f_3\}$ a pomocí věty 4.6.4 lze ověřit, zda je to Gröbnerova báze. Tedy

$$\begin{aligned} S(f_1, f_2) &= f_3 & \text{tedy } \overline{S(f_1, f_2)}^F &= 0, \\ S(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy & \text{ale } \overline{S(f_1, f_3)}^F &= -2xy \neq 0. \end{aligned}$$

Do generující množiny se tedy přidá $f_4 = -2xy$. Potom $F = \{f_1, f_2, f_3, f_4\}$ a lze psát

$$\begin{aligned} \overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0, \\ S(f_1, f_4) &= -2xy^2 = yf_4 & \text{tedy } \overline{S(f_1, f_4)}^F &= 0, \\ S(f_2, f_3) &= -2y^2 + x & \text{ale } \overline{S(f_2, f_3)}^F &= -2y^2 + x \neq 0. \end{aligned}$$

Rozšířením generující množiny o $f_5 = -2y^2 + x$ je $F = \{f_1, f_2, f_3, f_4, f_5\}$. Snadno lze ověřit, že platí

$$\overline{S(f_i, f_j)}^F = 0 \quad \text{pro všechna } 1 \leq i < j \leq 5.$$

Z věty 4.6.4 potom plyne, že

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

je Gröbnerovou bází pro ideál I . ■

Postup, předvedený v příkladě 4.8, lze zapsat jako algoritmus pro sestavení Gröbnerovy báze. Verze, která zde bude uvedena, je pouze základní. V 70. a 80. letech 20. století byla provedena mnohá vylepšení tohoto algoritmu vedoucí ke zvýšení efektivity výpočtu. Některá z těchto vylepšení budou uvedena v části 4.8.

Věta 4.7.1 (Buchbergerův algoritmus) *Nechť $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$ je polynomiální ideál. Potom lze Gröbnerovu bázi sestavit konečným počtem kroků následujícího algoritmu:*

```

INPUT:  $F = (f_1, \dots, f_s)$ 
OUTPUT: GRÖBNEROVA BÁZE  $G = (g_1, \dots, g_t)$  PRO IDEÁL  $I$ ,  $F \subset G$ 
 $G := F$ 
REPEAT
     $G' := G$ 
    FOR KAŽDOU DVOJICI  $\{p, q\}$ ,  $p \neq q$  V  $G'$  DO
         $S := \overline{S(p, q)}^{G'}$ 
        IF  $S \neq 0$  THEN  $G := G \cup \{S\}$ 
UNTIL  $G = G'$ 

```

Důkaz: Nejdříve se ukáže, že $G \subset I$ platí v každé fázi algoritmu. Kdykoliv dojde k rozšíření G , přidá se zbytek $S = \overline{S(p, q)}^{G'}$ pro $p, q \in G$. A tedy, jestliže $G \subset I$, potom i p, q a také $S(p, q)$ jsou v I , a protože se dělilo prvky $G' \subset I$, je $G \cup S \subset I$. G také obsahuje danou bázi F a tedy G je báze I .

Algoritmus končí, když $G = G'$, což znamená, že $\overline{S(p, q)}^G = 0$ pro všechna $p, q \in G$. Proto podle věty 4.6.4 je G Gröbnerovou bází I .

Zbývá ukázat, že algoritmus skončí. K tomu je nutné podrobněji zkoumat, co se stane po každém průchodu hlavním cyklem algoritmu. Množina G se skládá z G' (G z minulého průchodu cyklem) a z nenulových zbytků S -polynomů prvků množiny G' . Potom tedy

$$\langle \text{LT}(G') \rangle \subset \langle \text{LT}(G) \rangle,$$

protože $G' \subset G$. Navíc je-li $G' \neq G$, předpokládá se, že $\langle \text{LT}(G') \rangle$ je ostře menší než $\langle \text{LT}(G) \rangle$. Pro důkaz předpokládejme, že do G' byl přidán nenulový zbytek r po dělení S -polynomu prvky báze. Jelikož r je zbytek po dělení prvky G' , $\text{LT}(r)$ není dělitelný žádným z hlavních členů prvků G' , a tedy $\text{LT}(r) \notin \langle \text{LT}(G') \rangle$. Ale $\text{LT}(r) \in \langle \text{LT}(G) \rangle$, což dokazuje předpoklad.

Z předchozího je vidět, že ideály $\langle \text{LT}(G') \rangle$ tvoří vzestupnou řadu ideálů v $k[x_1, \dots, x_n]$. Z ACC potom plyne, že po konečném počtu iterací se řada stabilizuje a bude $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle$. Z předchozího odstavce potom plyne, že $G' = G$ a algoritmus skončí po konečném počtu kroků. □

Ihned je nutné upozornit, že algoritmus uvedený ve větě 4.7.1 byl vybrán hlavně pro svoji názornost. Není to příliš vhodná cesta, jak opravdu realizovat výpočet, jelikož se přímo nabízí zřejmé vylepšení tohoto algoritmu. Pokud je jednou vypočten zbytek $\overline{S(p, q)}^{G'} = 0$, potom bude tento zbytek stále nula i po přidání členů na konec uspořádané generující množiny G' . Není tedy nutné tento zbytek znovu počítat. Ve skutečnosti je po přidání nového generátoru f_j nezbytné spočítat pouze zbytky $\overline{S(f_i, f_j)}^{G'}$, kde $i \leq j - 1$. Další možná vylepšení algoritmu budou uvedena v části 4.8.

Gröbnerova báze vypočtená uvedeným algoritmem je často větší než je nezbytné. Nepotřebné generátory lze eliminovat užitím následujícího faktu.

Lemma 4.7.2 *Nechť G je Gröbnerova báze pro polynomiální ideál I . Nechť $p \in G$ je takový polynom, že $\text{LT}(p) \in \langle \text{LT}(G - \{p\}) \rangle$. Potom $G - \{p\}$ je také Gröbnerova báze ideálu I .*

Důkaz: Víme, že $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$. Je-li $\text{LT}(p) \in \langle \text{LT}(G - p) \rangle$, potom $\langle \text{LT}(G - p) \rangle = \langle \text{LT}(G) \rangle$. Odtud již podle definice plyne, že $G - p$ je také Gröbnerova báze I . $\square$

Definice 4.7.1 Minimální Gröbnerova báze pro polynomiální ideál I je Gröbnerova báze G taková, že:

1. $\text{LC}(p) = 1$ pro všechny $p \in G$,
2. pro všechny $p \in G$ je $\text{LT}(p) \notin \langle \text{LT}(G - \{p\}) \rangle$.

Minimální Gröbnerovu bázi pro daný nenulový ideál lze sestavit užitím algoritmu uvedeném ve větě 4.7.1 a následně lemmatu 4.7.2.

Příklad 4.9 V příkladě 4.8 byla vzhledem ke **grlex** uspořádání vypočtena Gröbnerova báze

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

Jelikož jsou některé hlavní koeficienty různé od 1, nejdříve se vynásobí generátory vhodnými konstantami, aby byly všechny hlavní koeficienty 1. Vzhledem k lemmatu 4.7.2 se nezařadí f_1 do minimální Gröbnerovy báze, jelikož platí $\text{LT}(f_1) = x^3 = -x \cdot \text{LT}(f_3)$. Podobně, jelikož $\text{LT}(f_2) = x^2y = -\frac{1}{2}x\text{LT}(f_4)$, je možné eliminovat f_2 . Dále již nelze nalézt žádný další případ, kdy hlavní člen generátoru dělí hlavní člen jiného generátoru a tedy

$$\tilde{f}_3 = x^2, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - \frac{1}{2}x$$

je minimální Gröbnerova báze ideálu I . ■

Bohužel ideál uvedený v příkladě 4.9 může mít více minimálních Gröbnerovýchází, jelikož také

$$\hat{f}_3 = x^2 + axy, \quad \hat{f}_4 = xy, \quad \hat{f}_5 = y^2 - \frac{1}{2}x$$

je minimální Gröbnerova báze pro $a \in k$ (libovolná konstanta). Pro k nekonečné tedy existuje nekonečně mnoho minimálních Gröbnerovýchází. Naštěstí lze vybrat minimální Gröbnerovu bázi, která je v jistém smyslu lepší než ostatní.

Definice 4.7.2 Redukovaná Gröbnerova báze pro polynomiální ideál I je Gröbnerova báze G pro ideál I taková, že:

1. $\text{LC}(p) = 1$ pro všechna $p \in G$,
2. pro všechna $p \in G$ žádný monom p nenáleží $\langle \text{LT}(G - \{p\}) \rangle$.

Věta 4.7.3 Necht $I \neq \{0\}$ je polynomiální ideál. Potom pro dané uspořádání monomů má I jedinou redukovanou Gröbnerovu bázi.

Důkaz: Předpokládejme, že G je minimální Gröbnerova báze I . Algoritmus minimalizace je zřejmý, stačí testovat pouze dělitelnost hlavních členů.

Necht $g \in G$ není redukovaný, tzn. obsahuje monom, který náleží v $\langle \text{LT}(G - \{g\}) \rangle$. Při dělení $g/(G - g)$ se tedy $\text{LT}(g)$ nutně dostane do zbytku, protože nemá čím být dělitelný (báze je minimální). Tedy $\text{LT}(\overline{g}^{G-g}) = \text{LT}(g)$, protože nic jiného už nemůže být vedoucím členem zbytku. Označme

$$g' = \overline{g}^{G-g} \quad \text{a} \quad G' = (G - g) \cup g'.$$

G' je opět minimální Gröbnerovouází ideálu I , protože $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle$, tj. také platí $\langle \text{LT}(G') \rangle = \langle \text{LT}(I) \rangle$. Polynom g' je zřejmě redukovaný pro G' díky vlastnostem algoritmu dělení. Byl-li nějaký $h \neq g$ redukovaný pro G , zůstává podle předchozího lemmatu redukovaný i pro G' . Tím je dán algoritmus pro redukci Gröbnerovy báze.

Zbývá dokázat jednoznačnost. Předpokládejme dvě redukované Gröbnerovy báze $G, \tilde{G}$ nenulového ideálu I . Platí tedy $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle = \langle \text{LT}(\tilde{G}) \rangle$. Protože tento ideál je monomiální, lze pro něj aplikovat Dicksonovo lemma. S odvoláním na konstrukci báze v jeho důkazu (podrobně viz [3], str. 70) lze tvrdit, že existuje právě jedna monomiální báze monomiálního ideálu tak, že koeficienty jejích členů jsou rovny jedné a žádný z členů této báze nedělí jiný.

Podle definice minimality musí být $\text{LT}(G)$ i $\text{LT}(\tilde{G})$ právě takovouází. Tedy $\text{LT}(G) = \text{LT}(\tilde{G})$. Ke každému $g \in G$ tedy existuje právě jedno $\tilde{g} \in \tilde{G}$ takové, že $\text{LT}(g) = \text{LT}(\tilde{g})$.

Platí $g - \tilde{g} \in I$. Protože G je Gröbnerova báze, platí $\overline{g - \tilde{g}}^G = 0$. Členy $\text{LT}(g), \text{LT}(\tilde{g})$ se odečtou už v $g - \tilde{g}$. Protože obě báze jsou redukované, nemůže být žádný ze zbývajících členů $g - \tilde{g}$ dělitelný kterýmkoliv z $\text{LT}(G) = \text{LT}(\tilde{G})$ a musí se tedy dostat do zbytku. Platí tedy

$$g - \tilde{g} = \overline{g - \tilde{g}}^G = 0.$$

Tím je jednoznačnost dokázána. □

Důsledkem věty 4.7.3 je algoritmus pro ověření, zda množiny polynomů $\{f_1, \dots, f_s\}$ a $\{g_1, \dots, g_t\}$ generují stejný ideál: pro dané uspořádání monomů se najdou redukované

Gröbnerovy báze pro $\langle f_1, \dots, f_s \rangle$ a $\langle g_1, \dots, g_t \rangle$ a ideály jsou si rovny právě tehdy, když jejich redukované Gröbnerovy báze jsou stejné.

Závěr této části bude věnován příkladu, který demonstruje souvislost Buchbergerova algoritmu a Gaussovy eliminace.

Příklad 4.10 Uvažujme soustavu lineárních rovnic

$$\begin{array}{cccccc} 3x & - & 6y & - & 2z & & = & 0 \\ 2x & - & 4y & & & + & 4w & = & 0 \\ x & - & 2y & - & z & - & w & = & 0. \end{array}$$

Užitím Gaussovy eliminaci na matici koeficientů soustavy lze původní matici převést do tvaru

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (4.1)$$

Pro získání redukované matice musí být každá hlavní 1 jedinou nenulovou hodnotou v daném sloupci, tedy

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (4.2)$$

Nechť I je ideál

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle \subset k[x, y, z, w]$$

odpovídající původní soustavě rovnic. Minimální Gröbnerova báze vzhledem k **lex** uspořádání pro $x > y > z > w$ je

$$I = \langle x - 2y - z - w, z + 3w \rangle,$$

což odpovídá lineární formě dané maticí (4.1). Redukovaná Gröbnerova báze pro ideál I je

$$I = \langle x - 2y + 2w, z + 3w \rangle,$$

což odpovídá matici (4.2). ■

Na základě příkladu 4.10 lze říci, že Gaussova eliminace je speciálním případem obecného Buchbergerova algoritmu pro soustavu lineárních rovnic.

4.8 Vylepšení Buchbergerova algoritmu

Základní Buchbergerův algoritmus je značně výpočetně náročný. Nejnáročnější částí algoritmu je výpočet S-polynomu a zejména následné dělení, při kterém se zjišťuje zbytek po dělení prvky báze. Proto bude tato část věnována jednomu z možných způsobů, jak vylepšit algoritmus uvedený ve větě 4.7.1 a podstatně tak zkrátit výpočetní dobu. Zejména

v poslední době se objevují zcela nové přístupy, jak najít Gröbnerovu bázi. Nejedná se už ale jen o vylepšení uvedeného algoritmu a jejich rozbor přesahuje možnosti tohoto textu.

Snahou je najít takové S-polynomy, které není třeba při dělení uvažovat. K tomu potřebujeme obecnější náhled na pojem nulového zbytku, uvedený v následující definici.

Definice 4.8.1 *Zvolme uspořádání monomů. Nechť $G = \{g_1, \dots, g_t\} \subset k[x_1, \dots, x_n]$. Pro libovolné $f \in k[x_1, \dots, x_n]$ lze říci, že f se redukuje na nulu modulo G a označit $f \rightarrow_G 0$, jestliže existují $a_1, \dots, a_t \in k[x_1, \dots, x_n]$ taková, že lze psát*

$$f = a_1 g_1 + \dots + a_t g_t$$

a je-li $a_i g_i \neq 0$, pak $\text{multideg}(f) \geq \text{multideg}(a_i g_i)$.

Vztah mezi redukcí na nulu modulo G a algoritmem dělení množinou polynomů G popisuje následující lemma.

Lemma 4.8.1 *Nechť $G = \{g_1, \dots, g_t\}$ a $f \in k[x_1, \dots, x_n]$. Potom platí implikace*

$$\bar{f}^G = 0 \implies f \rightarrow_G 0.$$

Obrácené tvrzení obecně neplatí.

Důkaz: První část plyne ihned z algoritmu dělení. Zbývá ukázat, že obrácené tvrzení nemusí platit, což lze předvést na příkladě. Vezměme $f = xy^2 - x$ a $G = \{xy + 1, y^2 - 1\}$. Pomocí algoritmu dělení lze f vyjádřit ve tvaru $xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$. Lze ale také psát $xy^2 - x = 0 \cdot (xy + 1) + x \cdot (y^2 - 1)$ a jelikož $\text{multideg}(xy^2 - x) \geq \text{multideg}(x \cdot (y^2 - 1))$, je $f \rightarrow_G 0$. $\square$

Věta 4.8.2 *Báze $G = \{g_1, \dots, g_t\}$ pro ideál I je Gröbnerovou bází právě tehdy, když platí $S(g_i, g_j) \rightarrow_G 0$ pro všechna $i \neq j$.*

Důkaz: Plyne okamžitě z důkazu věty 4.6.4, podrobně viz [3], str. 103. $\square$

Z lemmatu 4.8.1 vyplývá, že věta 4.6.4 je speciálním případem věty 4.8.2. Postačující podmínka redukce S-polynomu na nulu je formulována v následující větě.

Věta 4.8.3 *Mějme konečnou množinu $G \subset k[x_1, \dots, x_n]$ a předpokládejme, že existují $f, g \in G$ takové, že*

$$\text{LCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g).$$

Potom $S(f, g) \rightarrow_G 0$.

Důkaz: Viz [3], str. 103. $\square$

Příklad 4.11 Uvažujme $G = \langle yz + y, x^3 + y, z^4 \rangle$ s **grlex** uspořádáním na $k[x, y, z]$. Potom

$$S(x^3 + y, z^4) \rightarrow_G 0$$

podle věty 4.8.3. Algoritmem dělení se ale dostane

$$S(x^3 + y, z^4) = yz^4 = (z^3 - z^2 + z - 1)(yz + y) + y$$

a tedy $\overline{S(x^3 + y, z^4)}^G = y \neq 0$. ■

Věta 4.8.3 ve spojení s větou 4.8.2 umožňuje výrazně zefektivnit algoritmus pro výpočet Gröbnerovy báze. Stačí ověřit podmínku $S(g_i, g_j) \rightarrow_G 0$ pro $i < j$ taková, že $\text{LM}(g_i)$ a $\text{LM}(g_j)$ nesplňují podmínku z věty 4.8.3.

K zavedení dalšího možného vylepšení věty 4.8.2 je nutné nejdříve definovat některé nové pojmy.

Definice 4.8.2 *Nechť $F = \{f_1, \dots, f_s\}$. Syzygy¹ hlavních členů $\text{LT}(f_1), \dots, \text{LT}(f_s)$ se nazývají s -tice polynomů $S = (h_1, \dots, h_s)$ taková, že*

$$\sum_{i=1}^s h_i \cdot \text{LT}(f_i) = 0.$$

Množina $S(F)$ obsahuje všechny syzygy hlavních členů F .

Například pro $F = (x, x^2 + z, y + z)$ definuje trojice $S = (-x + y, 1, -x)$ jedno možné syzygy z $S(F)$, jelikož platí

$$(-x + y) \cdot \text{LT}(x) + 1 \cdot \text{LT}(x^2 + z) + (-x) \cdot \text{LT}(y + z) = 0.$$

Nechť $\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$ jsou vektory s jedničkou na i -tém místě. Potom syzygy $S \in S(F)$ lze napsat ve tvaru $S = \sum_{i=1}^s h_i \mathbf{e}_i$. Jako příklad je možné uvažovat syzygy pro S -polynomy. Pro každý pár $\{f_i, f_j\} \subset F$, kde $i < j$ a x^γ je nejmenší společný násobek hlavních členů polynomů f_i a f_j , označme

$$S_{ij} = \frac{x^\gamma}{\text{LT}(f_i)} \mathbf{e}_i - \frac{x^\gamma}{\text{LT}(f_j)} \mathbf{e}_j. \quad (4.3)$$

Potom S_{ij} patří do $S(F)$. Jelikož $S(F)$ má konečnou bázi, každé $S \in S(F)$ lze vyjádřit jako lineární kombinaci bázevých syzygy s polynomiálními koeficienty.

Definice 4.8.3 *Syzygy $S \in S(F)$ je homogenní stupně $\alpha \in \mathbb{Z}_{\geq 0}^n$, jestliže*

$$S = (c_1 x^{\alpha(1)}, \dots, c_s x^{\alpha(s)}),$$

kde $c_i \in k$ a $\alpha_i + \text{multideg}(f_i) = \alpha$ pro i taková, že $c_i \neq 0$.

Lemma 4.8.4 *Každé syzygy $S \in S(F)$ lze vyjádřit jednoznačně jako součet homogenních syzygy.*

¹česky „sprázení“

Důkaz: Podrobně viz [3], str. 105. □

Věta 4.8.5 *Nechť $F = (f_1, \dots, f_s)$. Potom každé syzygy $S \in S(F)$ lze vyjádřit ve tvaru*

$$S = \sum_{i < j} u_{ij} S_{ij},$$

kde $u_{ij} \in k[x_1, \dots, x_n]$ a syzygy S_{ij} je definováno vztahem (4.3).

Důkaz: Je založen na lemmatu 4.8.4 a využívá definice 4.8.3. Podrobněji viz [3], str. 105. □

Z věty 4.8.5 vyplývá, že syzygy S_{ij} definované vztahem (4.3) tvoří bázi všech syzygy hlavních členů. Následující příklad ale ukazuje, že pro bázi $S(F)$ není zapotřebí vždy všech S_{ij} .

Příklad 4.12 Pro $F = (x^2y^2 + z, xy^2 - y, x^2y + yz)$ vzhledem k **lex** uspořádání s $x > y > z$ je

$$\begin{aligned} S_{12} &= (1, -x, 0), \\ S_{13} &= (1, 0, -y), \\ S_{23} &= (0, x, -y). \end{aligned} \tag{4.4}$$

Z (4.4) plyne, že $S_{23} = S_{13} - S_{12}$. Syzygy S_{23} je tedy nadbytečné, jelikož ho lze získat jako lineární kombinaci S_{12} a S_{13} . Bázi syzygy tedy tvoří $\{S_{12}, S_{13}\}$. Později bude ukázána metoda pro nalezení menší báze $S(F)$. ■

Věta 4.8.6 *Báze $G = \{g_1, \dots, g_t\}$ pro ideál I je Gröbnerovou bází právě tehdy, když pro každé syzygy $S = (h_1, \dots, h_t)$ v homogenní bázi $S(G)$ platí*

$$S \cdot G = \sum_{i=1}^t h_i g_i \longrightarrow_G 0.$$

Důkaz: Je analogický s důkazem věty 4.6.4. Podrobně viz [3], str. 106-107. □

Věta 4.6.4 je opět speciálním případem této věty. Vezme-li se $\{S_{ij}\}$ za bázi všech syzygy $S(G)$, potom polynomy $S_{ij} \cdot G$ jsou právě S-polynomy $S(g_i, g_j)$. K zužitkování síly věty 4.8.6 je nutné najít způsob, jak zmenšit bázi $S(G)$. Následující věta hovoří o tom, jak pro bázi $\{S_{ij} : i < j\}$ určit, které prvky mohou být vynechány.

Věta 4.8.7 *Nechť $G = \{g_1, \dots, g_t\}$ a nechť $\mathcal{S} \subset \{S_{ij} : 1 \leq i < j \leq t\}$ je báze $S(G)$. Navíc předpokládejme, že existují navzájem různé polynomy $g_i, g_j, g_k \in G$ takové, že platí*

$$\text{LT}(g_k) \text{ dělí } \text{LCM}(\text{LT}(g_i), \text{LT}(g_j)).$$

Potom jestliže $S_{ik}, S_{jk} \in \mathcal{S}$, pak $\mathcal{S} - \{S_{ij}\}$ je také báze $S(G)$.

Důkaz: Pro zjednodušení se bude předpokládat, že platí $i < j < k$. Necht' $x^{\gamma_{ij}} = \text{LCM}(\text{LM}(g_i), \text{LM}(g_j))$, podobně jsou definovány také $x^{\gamma_{ik}}$ a $x^{\gamma_{jk}}$. Z předpokladu potom plyne, že $x^{\gamma_{ik}}$ i $x^{\gamma_{jk}}$ dělí $x^{\gamma_{ij}}$. Snadno lze potom ověřit, že platí

$$S_{ij} = \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}} S_{ik} - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}} S_{jk}.$$

A tedy S_{ij} je v bázi zbytečný, protože ho lze vyjádřit jako lineární kombinaci S_{ik} a S_{jk} . $\square$

Nyní je možné formulovat vylepšený Buchbergerův algoritmus, který zahrnuje poznatky z vět 4.8.3 a 4.8.7. Pro úplnost je ale nutné zavést ještě jedno označení. V algoritmu bude používána uspořádaná dvojice (i, j) . Pro daná i, j , $i \neq j$ nebude ale vždy jasné, které z nich je větší. Proto bude používáno označení

$$[i, j] = \begin{cases} (i, j) & \text{pro } i < j, \\ (j, i) & \text{pro } i > j. \end{cases}$$

Věta 4.8.8 *Necht' $I = \langle f_1, \dots, f_n \rangle$ je polynomiální ideál. Potom Gröbnerovu bázi pro ideál I lze sestavit konečným počtem kroků následujícího algoritmu:*

```

INPUT:  $F = (f_1, \dots, f_s)$ 
OUTPUT: GRÖBNEROVA BÁZE  $G = (g_1, \dots, g_t)$  PRO IDEÁL  $I$ 
 $B := \{(i, j) | 1 \leq i < j \leq s\}$ 
 $G := F$ 
 $t := s$ 
WHILE  $B \neq \emptyset$  DO
  VYBER  $(i, j) \in B$ 
  IF  $\text{LCM}(\text{LT}(f_i), \text{LT}(f_j)) \neq \text{LT}(f_i)\text{LT}(f_j)$  AND NOT  $\text{Test}(f_i, f_j, B)$  THEN
     $S := \overline{S(f_i, f_j)}^G$ 
    IF  $S \neq 0$  THEN
       $t := t + 1$ ;  $f_t := S$ 
       $G := G \cup \{f_t\}$ 
       $B := B \cup \{(i, t) | 1 \leq i \leq t - 1\}$ 
     $B := B - \{(i, j)\},$ 

```

kde $\text{Test}(f_i, f_j, B)$ nabývá hodnoty true právě tehdy, když existuje $k \notin \{i, j\}$ takové, že dvojice $[i, k]$ a $[j, k]$ nejsou v B a současně $\text{LT}(f_k)$ dělí $\text{LCM}(\text{LT}(f_i), \text{LT}(f_j))$.

Důkaz: Je založen na větách uvedených v této části textu. To, že algoritmus skončí, vyplývá z podmínky ACC (věta 4.5.4). Podrobněji viz [3], str. 108-109. $\square$

Přestože je tento algoritmus podstatně lepší než základní verze Buchbergerova algoritmu, stále není optimální. Prováděné testy jsou mnohem méně pracné a umožní vynechat v některých případech velké množství výpočtů S-polynomů a následných dělení, která jsou nejpracnější částí algoritmu. Přesto je výpočetní doba v některých případech stále značná.

Jak bylo řečeno, nejpracnější částí algoritmu je provádění dělení S-polynomu prvky báze G . Jedním z možných způsobů urychlení dělení S-polynomu prvky báze G , které má implementační charakter, je uspořádání prvků báze f_i ve vzestupném pořadí vzhledem k hlavním členům s ohledem na používané uspořádání monomů.

Kapitola 5

Teorie eliminací

Tato kapitola bude věnována metodě eliminace proměnných ze soustavy polynomiálních rovnic a zejména její souvislosti s Gröbnerovouází. Základní principy teorie eliminací budou dány větou o eliminaci a větou o rozšíření. Zmíněna bude také geometrická interpretace uvedených vět.

5.1 Základní věty teorie eliminací

Nejdříve bude naznačeno, jak eliminace proměnných funguje. Řešme soustavu rovnic

$$\begin{aligned}x^2 + y + z &= 1, \\x + y^2 + z &= 1, \\x + y + z^2 &= 1.\end{aligned}\tag{5.1}$$

Pro ideál $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$ je redukovaná Gröbnerova báze vzhledem k lexikografickému uspořádání pro $x > y > z$

$$\begin{aligned}g_1 &= x + y + z^2 - 1, \\g_2 &= y^2 - y - z^2 + z, \\g_3 &= yz^2 + \frac{1}{2}z^4 - \frac{1}{2}z^2, \\g_4 &= z^6 - 4z^4 + 4z^3 - z^2.\end{aligned}\tag{5.2}$$

Z věty 3.4.2 je zřejmé, že soustavy (5.1) a (5.2) mají stejná řešení. Poslední rovnice je jen v proměnné z a lze ji přepsat do tvaru

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2 = z^2(z - 1)^2(z^2 + 2z - 1).$$

Kořeny g_4 tedy jsou 0, 1 a $-1 \pm \sqrt{2}$. Zpětným dosazením lze najít příslušná řešení y a x . Tímto postupem lze nalézt všechna řešení soustavy (5.1).

Řešení soustavy rovnic bylo možné provést popsáním způsobem ze dvou důvodů:

- Eliminace — Gröbnerova báze obsahuje rovnici g_4 , která je pouze v proměnné z , tzn. byly eliminovány proměnné x a y z poslední rovnice.
- Rozšíření — vyřešením rovnice $g_4 = 0$ lze z ostatních rovnic dopočítat odpovídající x a y a dostat tak řešení původní soustavy.

Základní myšlenkou teorie eliminací je, že eliminaci lze provádět zcela obecně, pro libovolnou soustavu polynomiálních rovnic a libovolný počet proměnných.

Definice 5.1.1 *Nechť $I \subset k[x_1, \dots, x_n]$. k -tým eliminačním ideálem I_k se nazývá ideál z $k[x_{k+1}, \dots, x_n]$ definovaný vztahem*

$$I_k = I \cap k[x_{k+1}, \dots, x_n].$$

Intuitivně se zdá, že I_k obsahuje všechny prvky Gröbnerovy báze, které obsahují jen proměnné $x_{k+1}, \dots, x_n$. Eliminace proměnných tedy znamená najít nenulové polynomy, které definují eliminační ideál I_k .

Věta 5.1.1 (O eliminaci) *Nechť $I \subset k[x_1, \dots, x_n]$ je ideál a nechť G je Gröbnerova báze pro ideál I vzhledem k **lex** uspořádání pro $x_1 > x_2 > \dots > x_n$. Potom pro každé $0 \leq k \leq n$ je*

$$G_k = G \cap k[x_{k+1}, \dots, x_n]$$

Gröbnerovou bází k -tého eliminačního ideálu I_k .

Důkaz: Zvolme k mezi 0 a n a předpokládejme, že $G = \{g_1, \dots, g_m\}$. Bez újmy na obecnosti je možné předpokládat, že $G_k = \{g_1, \dots, g_r\}$, tzn. prvních r prvků G leží v $k[x_{k+1}, \dots, x_n]$ (pokud by to nebyla pravda, provede se přeznačení).

Nejdříve se ukáže, že G_k je báze I_k . Jelikož určitě $G_k \subset I_k$, potom také $\langle g_1, \dots, g_r \rangle \subset I_k$, protože I_k je ideál. Zbývá tedy ukázat, že každý prvek I_k lze napsat ve tvaru $f = h_1 g_1 + \dots + h_r g_r$. To je možné ukázat pomocí algoritmu dělení. Provede se dělení polynomu f polynomy $g_1, \dots, g_m$ vzhledem k **lex** uspořádání. Je nutné si uvědomit následující dvě věci:

- jelikož $G = \{g_1, \dots, g_m\}$ je Gröbnerova báze I a $f \in I$, platí $\bar{f}^G = 0$,
- jelikož je použito lexikografické uspořádání, musí hlavní členy $g_{r+1}, \dots, g_m$ obsahovat některou z proměnných $x_1, \dots, x_k$. Proto pokud se použije algoritmus dělení, neobjeví se členy s $g_{r+1}, \dots, g_m$.

Odtud potom

$$f = h_1 g_1 + \dots + h_r g_r + 0 \cdot g_{r+1} + \dots + 0 \cdot g_m + 0,$$

z čehož plyne, že $f \in \langle g_1, \dots, g_r \rangle$. Tím je dokázáno, že G_k je báze I_k .

Zbývá ukázat, že G_k je Gröbnerovou bází. Podle věty 4.6.4 k tomu stačí, aby pro všechna $1 \leq i < j \leq r$ byl zbytek po dělení S-polynomu $S(g_i, g_j)$ prvky báze G_k roven nule. Ale všechny S-polynomy leží v I_k , jelikož tam leží i g_i a g_j . Odtud ale plyne, že zbytek

je roven nule. Tím je důkaz proveden. $\square$

Jako příklad lze použít opět soustavu (5.1) a jí příslušnou Gröbnerovu bázi (5.2). Z věty 5.1.1 plyne, že

$$\begin{aligned} I_1 &= I \cap \mathbb{C}[y, z] = \langle y^2 - y - z^2 + z, yz^2 + \frac{1}{2}z^4 - \frac{1}{2}z^2, z^6 - 4z^4 + 4z^3 - z^2 \rangle, \\ I_2 &= I \cap \mathbb{C}[z] = \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle. \end{aligned}$$

Je zřejmé, že Gröbnerova báze ve spojení s lexikografickým uspořádáním eliminuje nejen první proměnnou, ale také první dvě, první tři proměnné atd. Záleží jen na počtu proměnných v dané soustavě rovnic a také na počtu rovnic soustavy. Nevýhodou tohoto postupu je značná časová náročnost výpočtu Gröbnerovy báze vzhledem k **lex** uspořádání.

Druhým krokem potřebným pro řešení soustavy rovnic je rozšíření na úplné řešení. Jak bylo uvedeno v kapitole 4, ideálu $I \subset k[x_1, \dots, x_n]$ odpovídá afinní varieta

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \ \forall f \in I\}.$$

K popisu bodů afinní variety je nutné nejdříve najít řešení rovnice v jedné proměnné, získané eliminací ostatních proměnných. Poté se řešení postupně rozšiřuje přidáváním dalších proměnných.

Danému k mezi 0 a n odpovídá eliminační ideál I_k a řešení $(a_{k+1}, \dots, a_n) \in \mathbf{V}(I_k)$ se nazývají *parciální řešení* původní soustavy rovnic. K rozšíření $(a_{k+1}, \dots, a_n)$ na *úplné řešení* z $\mathbf{V}(I)$ je nutné nejprve přidat proměnnou x_k a dopočítat odpovídající $(a_k, a_{k+1}, \dots, a_n)$. Hledá se tedy a_k takové, že $(a_k, a_{k+1}, \dots, a_n)$ leží na varietě $\mathbf{V}(I_{k-1})$. Konkrétně je třeba najít $x_k = a_k$, které je řešením soustavy rovnic

$$g_1(x_k, a_{k+1}, \dots, a_n) = \dots = g_r(x_k, a_{k+1}, \dots, a_n) = 0.$$

Jelikož se pracuje s polynomy v jedné proměnné, všechna možná řešení a_k soustavy jsou rovna kořenům největšího společného dělitele polynomů $g_1, \dots, g_r$.

Problémy nastanou v případě, že polynomy $g_1, \dots, g_r$ nemají společný kořen, tzn. existují parciální řešení, která nelze rozšířit na úplná řešení. Jako příklad uvažujme soustavu rovnic

$$\begin{aligned} xy &= 1, \\ xz &= 1. \end{aligned} \tag{5.3}$$

Pro ideál $I = \langle xy - 1, xz - 1 \rangle$ je Gröbnerova báze $G = \langle y - z, xz - 1 \rangle$. Z prvního eliminačního ideálu $I_1 = \langle y - z \rangle$ plynou parciální řešení ve tvaru (a, a) , která lze rozšířit na úplná řešení $(1/a, a, a)$ s výjimkou bodu $(0, 0)$. Geometricky vyjadřuje rovnice $y = z$ rovinu ve E_3 . Varieta (5.3) potom vyjadřuje hyperbolu ležící v rovině $y = z$. Je tedy zřejmé, že bodu $(0, 0)$ opravdu neodpovídá žádné úplné řešení (viz obr. 5.1).

Následující věta říká, která parciální řešení $(a_2, \dots, a_n) \in \mathbf{V}(I_1)$ je možné rozšířit na úplná řešení $(a_1, \dots, a_n) \in \mathbf{V}(I)$. Pro zjednodušení bude věta omezena pouze pro případ, kdy byla eliminována jen proměnná x_1 .

Věta 5.1.2 (O rozšíření) *Nechť $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_n]$ a nechť I_1 je první eliminační ideál pro I . Pro každé $1 \leq i \leq s$ lze f_i napsat ve tvaru*

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{členy, ve kterých je } x_i \text{ stupně } < N_i,$$

kde $N_i \geq 0$ a $g_i \in \mathbb{C}[x_2, \dots, x_n]$ jsou nenulová. Předpokládejme, že existuje parciální řešení $(a_2, \dots, a_n) \in \mathbf{V}(I_1)$. Jestliže $(a_2, \dots, a_n) \notin \mathbf{V}(g_1, \dots, g_n)$, potom existuje $a_1 \in \mathbb{C}$ takové, že $(a_1, a_2, \dots, a_n) \in \mathbf{V}(I)$.

Důkaz: Je poměrně náročný, podrobně viz [3], str.163-164. □

Jak je vidět, věta je formulována pro $k = \mathbb{C}$. Proč je to důležité, lze ukázat na příkladě.

Příklad 5.1 Uvažujme $k = \mathbb{R}$ a soustavu rovnic

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

Eliminace x vede k rovnici $y = z$ a tedy parciální řešení jsou (a, a) pro všechny $a \in \mathbb{R}$. Pro $k = \mathbb{C}$ lze z rovnic $x^2 - y = 0$ a $x^2 - z = 0$ bez problémů dopočítat úplná řešení soustavy rovnic. Věta 5.1.2 zaručuje, že všechna řešení (a, a) lze rozšířit na úplná řešení. Nad $\mathbb{R}$ je ale situace jiná. Jelikož $x^2 = a$ nemá reálné řešení pro $a < 0$, lze na úplná řešení rozšířit pouze ta částečná řešení, pro která je $a \geq 0$. Odtud je vidět, že věta 5.1.2 neplatí pro $k = \mathbb{R}$. ■

Ačkoliv věta 5.1.2 o rozšíření je formulována jen pro případ, kdy byla ze soustavy rovnic eliminována pouze první proměnná x_1 , je možné ji použít pro eliminaci libovolného počtu proměnných.

Příklad 5.2 Mějme soustavu rovnic

$$\begin{aligned} x^2 + y^2 + z^2 &= 1, \\ xyz &= 1. \end{aligned} \tag{5.4}$$

Gröbnerova báze pro ideál $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$ vzhledem k **lex** uspořádání je

$$\begin{aligned} g_1 &= y^4 z^2 + y^2 z^4 - y^2 z^2 + 1, \\ g_2 &= x + y^3 z + y z^3 - y z. \end{aligned}$$

Z věty 5.1.1 o eliminaci potom vyplývá, že

$$\begin{aligned} I_1 &= I \cap \mathbb{C}[y, z] = \langle g_1 \rangle, \\ I_2 &= I \cap \mathbb{C}[z] = \{0\}. \end{aligned}$$

Jelikož $I_2 = \{0\}$, je $\mathbf{V}(I_2) = \mathbb{C}$ a tedy každé $c \in \mathbb{C}$ je parciálním řešením. K rozšíření na úplná řešení $(a, b, c) \in \mathbf{V}(I)$ se použije věta 5.1.2. Nejdříve se přejde od I_2 k $I_1 = \langle g_1 \rangle$. Koeficient u y^4 v polynomu g_1 je z^2 a tedy řešení lze rozšířit na (b, c) pro libovolné $c \neq 0$. To

je ale rozumné, protože g_1 nemá pro $c = 0$ řešení. Zbývá přejít od I_1 k I , což znamená najít takové a , aby $(a, b, c) \in \mathbf{V}(I)$. Dosazení $(y, z) = (b, c)$ do (5.4) vede ke dvěma rovnicím v proměnné x , ze kterých není na první pohled zřejmé, jestli mají nějaké společné řešení. Zde se ukáže síla věty 5.1.2 o rozšíření. Hlavní koeficienty u mocnin x jsou 1, resp. yz , a jelikož 1 je vždy různá od nuly, věta 5.1.2 o rozšíření zaručuje existenci $a \in \mathbb{C}$. Tím je dokázáno, že všechna parciální řešení $c \neq 0$ lze rozšířit na úplná řešení $(a, b, c) \in \mathbf{V}(I)$. ■

Užití věty 5.1.2 o rozšíření je zvláště jednoduché, pokud je koeficient u hlavního členu některé z rovnic soustavy roven nenulové konstantě. Tento případ je často užitečný, a proto bude formulován jako důsledek věty 5.1.2 o rozšíření.

Důsledek 5.1.3 *Nechť $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_n]$ a předpokládejme, že pro nějaké i má f_i tvar*

$$f_i = cx_1^N + \text{členy, ve kterých je } x_i \text{ stupně } < N,$$

kde $c \in \mathbb{C}$ je nenulové a $N > 0$. Je-li I_1 první eliminační ideál I a $(a_2, \dots, a_n) \in \mathbf{V}(I_1)$, potom existuje $a_1 \in \mathbb{C}$ takové, že $(a_1, a_2, \dots, a_n) \in \mathbf{V}(I)$.

Důkaz: Plyne okamžitě z věty 5.1.2 o rozšíření. Jelikož $g_i = c \neq 0$, je $\mathbf{V}(g_1, \dots, g_s) = \emptyset$ a tedy určitě $(a_2, \dots, a_n) \notin \mathbf{V}(g_1, \dots, g_s)$ pro všechna parciální řešení. □

Na závěr této části uvedeme několik příkladů.

Příklad 5.3 Chtějme najít všechna řešení soustavy rovnic

$$\begin{aligned} x^2 + 2y^2 &= 3, \\ x^2 + xy + y^2 &= 3. \end{aligned} \tag{5.5}$$

Redukovaná Gröbnerova báze pro ideál $I = \langle x^2 + 2y^2 - 3, x^2 + xy + y^2 - 3 \rangle$ vzhledem k lex uspořádání pro $x > y$ je

$$\begin{aligned} g_1 &= y^3 - y, \\ g_2 &= xy - y^2, \\ g_3 &= x^2 + 2y^2 - 3. \end{aligned} \tag{5.6}$$

První eliminační ideál je tedy $I_1 = I \cap k[y] = \langle g_1 \rangle = \langle y^3 - y \rangle$. Kořeny g_1 potom jsou

$$g_1 = y^3 - y = y(y-1)(y+1) = 0 \implies y_1 = 0, y_2 = -1, y_3 = 1.$$

Postupným dosazováním získaných kořenů do soustavy (5.5) se získají odpovídající hodnoty x_i a tedy řešení původní soustavy rovnic. Tedy

$$\begin{aligned} y_1 = 0 : \quad & \left. \begin{aligned} x^2 - 3 &= 0 \\ x^2 - 3 &= 0 \end{aligned} \right\} \implies \text{kořeny } x_{1,2} = \pm\sqrt{3} & \implies \text{řešení } [-\sqrt{3}, 0], \\ & & & [\sqrt{3}, 0] \\ y_2 = -1 : \quad & \left. \begin{aligned} x^2 - 1 &= 0 \\ x^2 - x - 2 &= 0 \end{aligned} \right\} \implies \text{společný kořen } x_1 = -1 & \implies \text{řešení } [-1, -1] \\ y_3 = 1 : \quad & \left. \begin{aligned} x^2 - 1 &= 0 \\ x^2 + x - 2 &= 0 \end{aligned} \right\} \implies \text{společný kořen } x_1 = 1 & \implies \text{řešení } [1, 1] \end{aligned}$$

Stejná řešení lze dostat i v případě, že se kořeny y_i dosadí do g_2, g_3 . Důležité je nevybrat si např. jen g_2 a hledat úplná řešení soustavy jen z jedné rovnice. Mezi řešení by tak byly zahrnuty i dvojice, které nejsou řešením původní soustavy rovnic.

Uvedeným postupem byla získána čtyři *přesná* řešení soustavy (5.5). Toto je ale ideální stav, který nemusí nastat vždy, jak se ukáže v následujícím příkladě. ■

Příklad 5.4 Chtějme najít všechna řešení soustavy rovnic

$$\begin{aligned} xy &= 4, \\ y^2 &= x^3 - 1. \end{aligned} \tag{5.7}$$

Redukovaná Gröbnerova báze pro ideál $I = \langle xy - 4, y^2 - x^3 + 1 \rangle$ vzhledem k **lex** uspořádání je

$$\begin{aligned} g_1 &= y^5 + y^3 - 64, \\ g_2 &= 16x - y^4 - y^2. \end{aligned} \tag{5.8}$$

Bohužel polynom g_1 nelze rozložit na součin jako v předchozím příkladě. Jeho kořeny jsou

$$y_1 = 2.2136, \quad y_{2,3} = 0.6804 \pm 2.2697i, \quad y_{4,5} = -1.7872 \pm 1.3984i$$

a musí se nalézt některou z numerických metod pro hledání kořenů polynomů v jedné proměnné. Nalezené kořeny se dosadí do $g_2 = 16x - y^4 - y^2$, odkud potom plynou řešení původní soustavy. Hledáním kořenů numerickou metodou se ale bohužel částečně ztrácí přesnost nalezených řešení a získaná řešení jsou pouze numerickými aproximacemi řešení soustavy (5.7). ■

5.2 Geometrická interpretace eliminace proměnných

V této části uvedeme geometrickou interpretaci vět uvedených v 5.1. Základní myšlenkou je, že eliminace odpovídá projekci variety na podprostor nižší dimenze. Bude také uvedena věta o uzávěru, která popisuje vztah mezi parciálními řešeními a eliminačními ideály. Pro jednoduchost bude uvažováno $k = \mathbb{C}$.

Nechť je dáno $V = \mathbf{V}(f_1, \dots, f_s) \subset \mathbb{C}^n$. Projekční zobrazení

$$\pi_k : \mathbb{C}^n \rightarrow \mathbb{C}^{n-k}$$

převede $(a_1, \dots, a_n)$ na $(a_{k+1}, \dots, a_n)$ a zajistí tak eliminaci prvních k proměnných $x_1, \dots, x_k$. Působí-li π_k na $V \subset \mathbb{C}^n$, je $\pi_k(V) \subset \mathbb{C}^{n-k}$. O vztahu mezi $\pi_k(V)$ a k -tým eliminačním ideálem vypovídá následující lemma.

Lemma 5.2.1 *Použijme výše uvedené označení. Nechť $I_k = \langle f_1, \dots, f_s \rangle \cap \mathbb{C}[x_{k+1}, \dots, x_n]$ je k -tý eliminační ideál. Potom v $\mathbb{C}^{n-k}$ platí*

$$\pi_k(V) \subset \mathbf{V}(I_k).$$

Důkaz: Zvolme polynom $f \in I_k$. Jestliže $(a_1, \dots, a_n) \in V$, potom $f(a_1, \dots, a_n) = 0$, protože $f \in \langle f_1, \dots, f_s \rangle$. Ale f obsahuje jen proměnné $x_{k+1}, \dots, x_n$ a tedy lze psát

$$f(a_{k+1}, \dots, a_n) = f(\pi_k(a_1, \dots, a_n)) = 0.$$

Odtud již plyne, že $f = 0$ pro všechny body $\pi_k(V)$. □

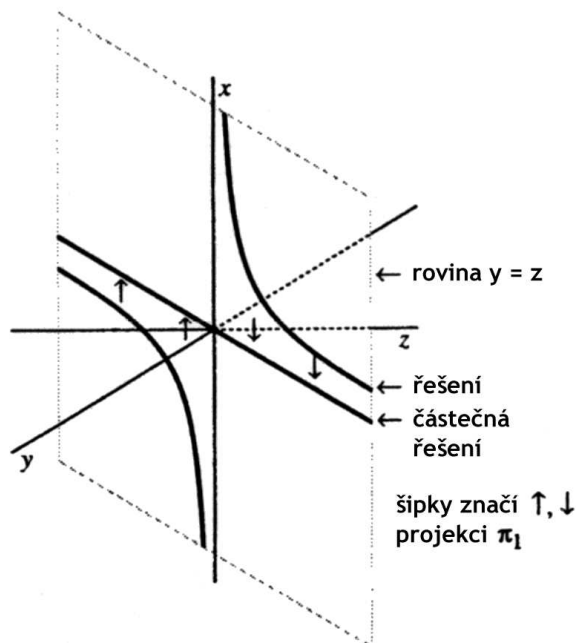
Stejně jako v 5.1, body variety $\mathbf{V}(I_k)$ se nazývají parciální řešení. S využitím lemmatu 5.2.1 lze $\pi_k(V)$ vyjádřit následujícím způsobem

$$\pi_k(V) = \{(a_{k+1}, \dots, a_n) \in \mathbf{V}(I_k) : \exists a_1, \dots, a_k \in \mathbb{C}, \text{ pro které } (a_1, \dots, a_k, a_{k+1}, \dots, a_n) \in V\}.$$

Tedy $\pi_k(V)$ obsahuje přesně ta parciální řešení, která lze rozšířit na úplná řešení. Například pro soustavu rovnic (5.3) z části 5.1

$$\begin{aligned} xy &= 1, \\ xz &= 1 \end{aligned} \tag{5.9}$$

zobrazuje obr. 5.1 vztah mezi úplnými řešeními soustavy rovnic (5.9) a jejími parciálními řešeními.



Obrázek 5.1: Parciální a úplná řešení soustavy rovnic (5.9)

V části 5.1 již bylo ukázáno, že $\mathbf{V}(I_1)$ je přímka $y = z$ v rovině yz a tedy

$$\pi_1(V) = \{(a, a) \in \mathbb{C}^2 : a \neq 0\}.$$

Jelikož $\pi_1(V)$ neobsahuje $(0,0)$, není to afinní varieta.

Základem pro porozumění existenci takových chybějících bodů je věta 5.1.2 o rozšíření z části 5.1. Ta je sice formulována jen pro π_1 , tzn. jen pro eliminaci první proměnné x_1 , ale přesto dává dobrý náhled na to, co se v takovém případě děje. Geometricky je možné větu o rozšíření formulovat následovně:

Věta 5.2.2 (Geometrická věta o rozšíření) *Nechť $V = \mathbf{V}(f_1, \dots, f_s) \subset \mathbb{C}^n$ a nechť g_i je definováno jako ve větě 5.1.2 o rozšíření v části 5.1. Jestliže I_1 je první eliminační ideál pro $\langle f_1, \dots, f_s \rangle$, potom v $\mathbb{C}^{n-1}$ platí*

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \dots, g_s) \cap \mathbf{V}(I_1)),$$

kde $\pi_1 : \mathbb{C}^n \rightarrow \mathbb{C}^{n-1}$ je projekce na posledních $n - 1$ souřadnic.

Důkaz: Věta plyne rovnou z lemmatu 5.2.1 a z věty 5.1.2. □

Věta 5.2.2 říká, že $\pi_1(V)$ zcela vyplňuje afinní varietu $\mathbf{V}(I_1)$, s výjimkou části ležící na $\mathbf{V}(g_1, \dots, g_s)$. Není ale zřejmé, jak velká část to je. Například soustava rovnic

$$\begin{aligned} (y - z)x^2 + xy &= 1, \\ (y - z)x^2 + xz &= 1 \end{aligned} \tag{5.10}$$

generuje stejný ideál jako soustava (5.9). Jelikož $g_1 = g_2 = y - z$ generuje první eliminační ideál, geometrická věta o rozšíření nám v tomto případě nic neříká o velikosti $\pi_1(V)$.

Nicméně i přesto je možné formulovat následující větu o vztahu mezi $\pi_k(V)$ a $\mathbf{V}(I_k)$.

Věta 5.2.3 (O uzávěru) *Nechť $V = \mathbf{V}(f_1, \dots, f_s) \subset \mathbb{C}^n$ a nechť I_k je k -tý eliminační ideál pro $\langle f_1, \dots, f_s \rangle$. Potom:*

1. $\mathbf{V}(I_k)$ je nejmenší afinní varieta obsahující $\pi_k(V) \subset \mathbb{C}^{n-k}$, tzn.
 - $\pi_k(V) \subset \mathbf{V}(I_k)$,
 - je-li Z jiná afinní varieta v $\mathbb{C}^{n-k}$ obsahující $\pi_k(V)$, potom $\mathbf{V}(I_k) \subset Z$.
2. Jestliže $V \neq \emptyset$, potom existuje afinní varieta $W \subsetneq \mathbf{V}(I_k)$ taková, že $\mathbf{V}(I_k) - W \subset \pi_k(V)$.

Důkaz: Je náročný, podrobně viz [3], str. 123-124. □

Je možné formulovat také geometrickou verzi důsledku 5.1.3, který říká, kdy je možné všechna parciální řešení rozšířit na úplná řešení.

Důsledek 5.2.4 *Nechť $V = \mathbf{V}(f_1, \dots, f_s) \subset \mathbb{C}^n$ a předpokládejme, že pro nějaké i lze f_i vyjádřit ve tvaru*

$$f_i = cx_1^N + \text{členy, ve kterých je } x_1 \text{ stupně } < N,$$

kde $c \in \mathbb{C}$ je nenulová konstanta a $N > 0$. Jestliže I_1 je první eliminační ideál, potom v $\mathbb{C}^{n-1}$ platí

$$\pi_1(V) = \mathbf{V}(I_1),$$

kde π_1 je projekce na posledních $n - 1$ souřadnic.

Na závěr je třeba zmínit, pro která tělesa uvedená tvrzení platí. Věta o rozšíření i věta o uzávěru (a jejich důsledky) jsou formulovány pro těleso komplexních čísel $\mathbb{C}$. Dá se ukázat (není to ale triviální), že jak věta o rozšíření, tak věta o uzávěru platí pro libovolné algebraicky uzavřené těleso k .

Kapitola 6

Aplikace metody Gröbnerovýchází

Tato kapitola bude věnována aplikacím teorie Gröbnerovýchází. Konkrétně půjde o příklady z oblasti geometrie, automatického dokazování, počítačové grafiky a robotiky. Nejprve je ale třeba se zabývat řešitelností soustav polynomiálních rovnic a její souvislostí s teorií Gröbnerovýchází. Z této části vyplynou některé důležité poznatky užitečné v celé kapitole.

6.1 Řešitelnost soustavy polynomiálních rovnic

Hledání redukované Gröbnerovy báze úzce souvisí s hledáním přesného řešení soustavy polynomiálních rovnic. Pokud soustava polynomiálních rovnic má řešení, potom dojde k eliminaci proměnných z rovnic soustavy a původní soustava je převedena na snáze řešitelnou soustavu rovnic, jak bylo předvedeno v části 5.1. Jak se projeví, že soustava polynomiálních rovnic nemá řešení, o tom hovoří následující věta.

Věta 6.1.1 (Řešitelnost soustavy rovnic) *Soustava rovnic*

$$f_1 = 0, \dots, f_s = 0,$$

kde $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ a k je algebraicky uzavřené těleso, nemá řešení právě tehdy, když redukovaná Gröbnerova báze ideálu $I = \langle f_1, \dots, f_s \rangle$ je $\{1\}$.

Důkaz: Viz [27], str. 38. □

Jelikož je věta formulována pouze pro algebraicky uzavřená tělesa, což je např. těleso komplexních čísel $\mathbb{C}$, je možné v praxi pouze rozhodnout, zda soustava polynomiálních rovnic nemá žádné obecně komplexní řešení. Často je ale třeba hledat reálná řešení soustavy rovnic. Bohužel těleso reálných čísel $\mathbb{R}$ není algebraicky uzavřené, a proto věta 6.1.1 pro $\mathbb{R}$ neplatí. Snadno lze najít soustavu polynomiálních rovnic, kde koeficienty budou reálná čísla a soustava má pouze komplexní řešení.

Je třeba si uvědomit, co znamená, že redukovaná Gröbnerova báze ideálu je $\{1\}$ a proč v takovém případě soustava polynomiálních rovnic nemá řešení. Jelikož koeficienty

polynomů jsou z číselného tělesa k , zřejmě se v Gröbnerově bázi objeví bázevý prvek a , kde $a \in k$, $a \neq 0$. To ale samozřejmě vede k rovnici $a = 0$, která nemá řešení. Proto soustava rovnic nemá řešení. Tento prvek potom způsobí, že při výpočtu minimální Gröbnerovy báze jsou vyloučeny všechny ostatní bázevé prvky.

Platnost věty 6.1.1 lze předvést na několika příkladech. Soustavy rovnic budou voleny tak, aby měly snadnou geometrickou interpretaci a bylo snadné určit, zda má soustava reálné řešení. Taková soustava rovnic může mít komplexní řešení, která nejsou z geometrické interpretace zpravidla na první pohled vidět.

Příklad 6.1 Soustava rovnic

$$\begin{aligned} x^2 + y^2 - z &= 0, \\ x^2 + y^2 + (z - 4)^2 - 1 &= 0, \\ x^2 + y^2 + (z - 6)^2 - \frac{9}{4} &= 0 \end{aligned} \tag{6.1}$$

představuje hledání průniku rotačního paraboloidu a dvou kulových ploch. Gröbnerova báze pro ideál $I = \langle x^2 + y^2 - z, x^2 + y^2 + (z - 4)^2 - 1, x^2 + y^2 + (z - 6)^2 - \frac{9}{4} \rangle$ vzhledem k **lex** uspořádání pro $x > y > z$ je

$$\begin{aligned} 1065/256 &= 0, \\ -4z + 75/4 &= 0, \\ x^2 + y^2 + z^2 - 12z + 135/4 &= 0, \\ x^2 + y^2 + z^2 - 8z + 15 &= 0, \\ x^2 + y^2 - z &= 0. \end{aligned}$$

Príslušná redukovaná Gröbnerova báze je vzhledem k prvnímu prvku Gröbnerovy báze samozřejmě $\{1\}$. Jelikož první rovnice nemůže být nikdy splněna, soustava nemá řešení nad $\mathbb{C}$. ■

Poznámka 6.1.2 Při výpočtu redukované Gröbnerovy báze může být výhodnější použít **grlex** uspořádání. Výpočet je často rychlejší než při použití **lex** uspořádání a věta 6.1.1 platí nezávisle na zvoleném uspořádání. Na druhou stranu při použití **grlex** uspořádání nemusí vždy dojít k úplné eliminaci proměnných, což může být nevýhodné z hlediska dalšího řešení soustavy polynomiálních rovnic.

Příklad 6.2 Soustava rovnic

$$\begin{aligned} x^2 + y^2 - z &= 0, \\ x^2 + y^2 + (z - 4)^2 - 1 &= 0, \\ x^2 + (y - 4)^2 + z^2 - 1 &= 0 \end{aligned} \tag{6.2}$$

představuje opět hledání průniku rotačního paraboloidu a dvou kulových ploch, pouze poloha jedné kulové plochy byla změněna. Pro ideál $I = \langle x^2 + y^2 - z, x^2 + y^2 + (z - 4)^2 - 1, x^2 + (y - 4)^2 + z^2 - 1 \rangle$ je redukovaná Gröbnerova báze vzhledem k **lex** uspořádání s $x > y > z$

$$\begin{aligned} z^2 - 7z + 15 &= 0, \\ y^2 + yz + 2y + 5z - 11/2 &= 0, \\ x + y - z - 2 &= 0. \end{aligned}$$

Kořeny polynomu $z^2 - 7z + 15 = 0$ jsou komplexní (konkrétně $z_{1,2} = 3.5 \pm 1.6583i$) a tedy neexistuje žádné reálné řešení. Nicméně soustava má řešení v oboru komplexních čísel. ■

Pokud koeficienty polynomů $f_1, \dots, f_s$, které definují soustavu rovnic, nejsou jen z číselného tělesa, ale obsahují parametry, je možné provést úpravu. Pokud $f_1, \dots, f_s$ jsou polynomy v proměnných $x_1, \dots, x_j$ s koeficienty, které závisí na parametrech $u_1, \dots, u_i$, potom lze psát, že $f_1, \dots, f_s \in k(u_1, \dots, u_i)[x_1, \dots, x_j]$. O této situaci již přímo věta 6.1.1 nehovoří. Redukovaná Gröbnerova báze $\{1\}$ v tomto případě znamená, že daná soustava rovnic nemá řešení pro některé hodnoty parametrů. Nemusí to ale znamenat, že nemá řešení pro *všechny* hodnoty parametrů $u_1, \dots, u_i$. Pro podrobnější analýzu je třeba zkoumat přímo Gröbnerovu bázi. Gröbnerova báze může obsahovat prvek $a \in k, a \neq 0$, ale také může obsahovat nějakou funkci g parametrů $u_1, \dots, u_i$. Pokud báze obsahuje prvek $a \in k, a \neq 0$, lze použít větu 6.1.1 a říci, že soustava rovnic nemá řešení pro libovolné hodnoty parametrů $u_1, \dots, u_i$. V případě, že Gröbnerova báze obsahuje funkci $g(u_1, \dots, u_i)$, je situace složitější. Pro hodnoty parametrů $u_1, \dots, u_i$, pro které platí $g(u_1, \dots, u_i) = 0$, totiž soustava rovnic *může* mít řešení. Pokud existují takové hodnoty parametrů, je třeba dořešit soustavu rovnic z nalezené Gröbnerovy báze (pokud je to možné), případně provést řešení původní soustavy rovnic s těmito parametry opět pomocí algoritmu hledání redukované Gröbnerovy báze. Jak to lze konkrétně provést, je uvedeno v následujícím příkladě.

Příklad 6.3 Uvažujme soustavu rovnic

$$\begin{aligned} x^2 + y^2 + z^2 - 1 &= 0, \\ x^2 + y^2 + (z - a)^2 - 1 &= 0, \\ x^2 + y^2 + (z - b)^2 - 1 &= 0, \end{aligned} \tag{6.3}$$

kde a, b jsou parametry. Tato soustava zřejmě pro jisté hodnoty parametrů nemá žádné reálné a dokonce ani komplexní řešení. Existují ale i hodnoty parametrů a, b , pro které soustava má dokonce nekonečně mnoho reálných řešení. Gröbnerova báze pro ideál generovaný rovnicemi soustavy (6.3) je

$$\begin{aligned} (ab^2 - a^2b)/(a - b) &= 0, \\ (2a - 2b)z + (b^2 - a^2) &= 0, \\ x^2 + y^2 + z^2 - 2bz + (b^2 - 1) &= 0, \\ x^2 + y^2 + z^2 - 2az + (a^2 - 1) &= 0, \\ x^2 + y^2 + z^2 - 1 &= 0 \end{aligned} \tag{6.4}$$

a redukovaná Gröbnerova báze je $\{1\}$. Odtud plyne, že je třeba podrobněji rozebrat případy $a = 0$, $b = 0$ a $a = b$. Pro $a = 0$ plyne z druhé rovnice (6.4) $z = b/2$ a po dosazení do libovolné zbývajících rovnic

$$x^2 + y^2 - \frac{4 - b^2}{4} = 0.$$

Pro $|b| < 2$ tedy existuje nekonečně mnoho reálných řešení, která leží na kružnici se středem v bodě $(0, 0, b/2)$ a poloměrem $\sqrt{4 - b^2}/2$. Pro $b = 2$ existuje jediné řešení $(0, 0, 1)$.

V ostatních případech existují pouze komplexní řešení soustavy rovnic (6.3). Zcela obdobný případ nastává pro $b = 0$.

Řešení lze s výhodou provést opakovaným použitím algoritmu hledání redukované Gröbnerovy báze. Po dosazení $a = 0$ do původní soustavy rovnic (6.3) je pro ideál $I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 1, x^2 + y^2 + (z - b)^2 - 1 \rangle$ redukovaná Gröbnerova báze vzhledem k **lex** uspořádání pro $x > y > z$

$$\begin{aligned} z - b/2 &= 0, \\ x^2 + y^2 - (4 - b^2)/4 &= 0. \end{aligned}$$

Řešení je tedy naprosto shodné jako v předchozím případě. Zcela obdobná situace opět nastává i pro $b = 0$.

Pokud je $a = b$, nelze soustavu dořešit přímo z Gröbnerovy báze. Problémy působí první a druhá rovnice soustavy (6.4), kde by docházelo k dělení nulou. Nicméně lze využít opakovaně metodu hledání redukované Gröbnerovy báze. Po dosazení $a = b$ do soustavy (6.3) je redukovaná Gröbnerova báze pro ideál $I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + (z - b)^2 - 1, x^2 + y^2 + (z - b)^2 - 1 \rangle$ vzhledem k **lex** uspořádání pro $x > y > z$

$$\begin{aligned} z - b/2 &= 0, \\ x^2 + y^2 - (4 - b^2)/4 &= 0 \end{aligned}$$

a je tedy naprosto stejná jako v případě $a = 0$. Soustava rovnic (6.3) tedy má řešení pouze pro $a = 0$, $b = 0$ a $a = b$. ■

6.2 Převod parametrického vyjádření afinní variety na implicitní

Tato část bude věnována podrobnému studiu převodu parametrického vyjádření afinních variet na implicitní vyjádření, což lze zkráceně nazývat *implicitizace*. Problém implicitizace lze s výhodou řešit užitím Gröbnerovy báze ideálu ve spojení s **lex** uspořádáním a je úzce spjat s teorií eliminací proměnných popsanou v kapitole 5. Problému implicitizace bude dále věnována kapitola 8, kde budou uvedeny další možné metody a přístupy k řešení tohoto problému.

Prvním případem je parametrizace zadaná pomocí polynomů. Polynomiální parametrizaci lze vyjádřit ve tvaru

$$\begin{aligned} x_1 &= f_1(t_1, \dots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \dots, t_m), \end{aligned} \tag{6.5}$$

kde $f_1, \dots, f_n$ jsou polynomy z $k[t_1, \dots, t_m]$. Geometricky představuje soustava (6.5) zobrazení $F : k^m \rightarrow k^n$ definované vztahem

$$F(t_1, \dots, t_m) = (f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)).$$

Potom $F(k^m) \subset k^n$ je podmnožina k^n parametrizovaná rovnicemi (6.5). Jelikož $F(k^m)$ nemusí být afinní varieta, řešením problému převodu parametrického vyjádření na implicitní je nalezení *nejmenší variety obsahující* $F(k^m)$.

Úkolem implicitizace tedy je vyloučení parametrů z parametrického vyjádření (6.5). Výsledné rovnice pak obsahují pouze proměnné $x_1, \dots, x_n$. Eliminaci proměnných lze provést pomocí výpočtu redukované Gröbnerovy báze pro ideál $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle$. K tomu stačí pouze vhodná volba uspořádání proměnných. Podrobně o tom hovoří následující věta.

Věta 6.2.1 (Polynomiální implicitizace) *Nechť k je nekonečné těleso a $F : k^m \rightarrow k^n$ je zobrazení definované polynomiální parametrizací (6.5). Nechť I je ideál $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subset k[t_1, \dots, t_m, x_1, \dots, x_n]$ a nechť $I_m = I \cap k[x_1, \dots, x_n]$ je m -tý eliminační ideál. Potom $\mathbf{V}(I_m)$ je nejmenší varieta v k^n obsahující $F(k^m)$.*

Důkaz: Viz [3], str. 128. □

Věta 6.2.1 dává algoritmus převodu polynomiální parametrizace na implicitní vyjádření. Polynomiální parametrizace (6.5) odpovídá ideálu $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle$, pro který se provede výpočet redukované Gröbnerovy báze vzhledem k **lex** uspořádání pro $t_1 > \dots > t_m > x_1 > \dots > x_n$. Členy báze, které neobsahují žádné t_i , představují implicitní vyjádření dané afinní variety.

Příklad 6.4 Uvažujme křivku zadanou parametrickými rovnicemi

$$x = t, \quad y = t^2, \quad z = t^3.$$

Plochu tečen této křivky potom lze vyjádřit ve tvaru

$$x = t + u, \quad y = t^2 + 2tu, \quad z = t^3 + 3t^2u.$$

Použitím algoritmu převodu polynomiální parametrizace na implicitní vyjádření dostaneme redukovanou

Gröbnerovu bázi o 7 prvcích, z nichž pouze jeden neobsahuje žádný z parametrů t, u a má tvar

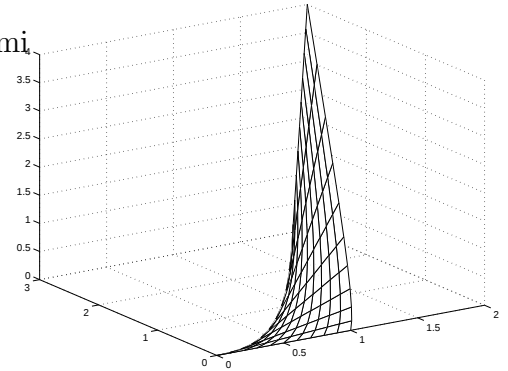
$$x^3z - \frac{3}{4}x^2y^2 - \frac{3}{2}xyz + y^3 + \frac{1}{4}z^2 = 0,$$

což je implicitní vyjádření dané plochy. ■

Dalším případem je tzv. *racionální implicitizace*. Zde mohou nastat jisté potíže, které lze dokumentovat na jednoduchém příkladě. Pro racionální parametrizaci plochy (u, v jsou parametry)

$$x = \frac{u^2}{v}, \quad y = \frac{v^2}{u}, \quad z = u \tag{6.6}$$

lze snadno ověřit, že libovolný bod (x, y, z) splňující (6.6) leží na ploše $x^2y = z^3$. Odstranění zlomků a provedení algoritmu převodu polynomiální parametrizace na implicitní vyjádření



pro ideál $I = \langle vx - u^2, uy - v^2, z - u \rangle \subset k[u, v, x, y, z]$ vede k druhému eliminačnímu ideálu ve tvaru $I_2 = I \cap k[x, y, z] = \langle z(x^2y - z^3) \rangle$ a tedy

$$\mathbf{V}(I_2) = \mathbf{V}(x^2y - z^3) \cup \mathbf{V}(z).$$

Odtud je zřejmé, že do výsledku byla přidána celá rovina $z = 0$ a tedy $\mathbf{V}(I_2)$ není nejmenší varieta obsahující danou parametrizaci. Problém je právě v odstranění zlomků, které se musí provést „lépe“, jelikož je třeba zajistit nenulovost jmenovatelů. Ideál I je možné upravit přidáním jedné proměnné a jedné rovnice, která zajistí nenulovost jmenovatelů u a v . Ideál I lze nahradit ideálem

$$J = \langle vx - u^2, uy - v^2, z - u, 1 - w(uv) \rangle \subset k[w, u, v, x, y, z],$$

kde rovnice $1 - wuv = 0$ zajistí nenulovost u a v ve všech bodech $\mathbf{V}(J)$. Třetí eliminační ideál potom je $J_3 = J \cap k[x, y, z] = \langle x^2y - z^3 \rangle$.

Racionální parametrizaci lze obecně vyjádřit ve tvaru

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)}, \end{aligned} \tag{6.7}$$

kde $f_1, g_1, \dots, f_n, g_n$ jsou polynomy z $k[t_1, \dots, t_m]$. Zobrazení F z k^m do k^n ale nelze definovat na celém k^m , jelikož je nutné vyjmout takové body $(t_1, \dots, t_m)$, pro které $g_i(t_1, \dots, t_m) = 0$ pro nějaké i . Označíme-li $W = \mathbf{V}(g_1, \dots, g_n) \subset k^m$, potom

$$F(t_1, \dots, t_m) = \left(\frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \dots, \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)} \right)$$

definuje zobrazení $F : k^m - W \rightarrow k^n$. Cílem je najít *nejmenší varietu v k^n obsahující $F(k^m - W)$* .

Věta 6.2.2 (Racionální implicitizace) *Nechť k je nekonečné těleso a nechť $F : k^m - W \rightarrow k^n$ je zobrazení definované racionální parametrizací (6.7). Nechť J je ideál $J = \langle g_1x_1 - f_1, \dots, g_nx_n - f_n, 1 - gy \rangle \subset k[y, t_1, \dots, t_m, x_1, \dots, x_m]$, kde $g = g_1 \cdot g_2 \cdots g_n$ a nechť $J_{m+1} = J \cap k[x_1, \dots, x_n]$ je $(m+1)$ -ní eliminační ideál. Potom $\mathbf{V}(J_{m+1})$ je nejmenší varieta v k^n obsahující $F(k^m - W)$.*

Důkaz: Obdobný jako důkaz věty 6.2.1. □

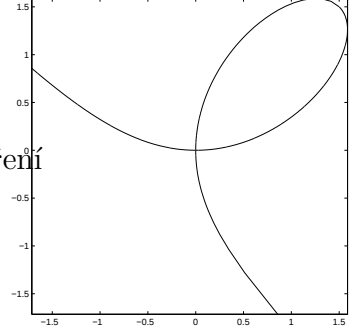
Věta 6.2.2 dává algoritmus převodu racionálně parametrizované afinní variety na implicitní vyjádření. V dané parametrizaci se odstraní zlomky vynásobením i -té rovnice funkcí g_i a přidáním rovnice $1 - g_1 \cdots g_n y = 0$ se zajistí nenulovost $g_1, \dots, g_n$ na dané varietě. Poté se pro ideál J provede výpočet redukované Gröbnerovy báze vzhledem k **lex** uspořádání pro $y > t_1 > \dots > t_m > x_1 > \dots > x_n$. Členy Gröbnerovy báze, které neobsahují žádnou z proměnných y, t_i , definují implicitní vyjádření dané afinní variety.

Příklad 6.5 Parametrické vyjádření Descartova listu lze zapsat ve tvaru

$$x = \frac{3at}{1+t^3}, \quad y = \frac{3at^2}{1+t^3}.$$

Algoritmus převodu racionální parametrizace na implicitní vyjádření vede k ideálu $I = \langle x(1+t^3)-3at, y(1+t^3)-3at^2, 1-w(1+t^3) \rangle \subset k[w, t, x, y]$. Redukovaná Gröbnerova báze ideálu I obsahuje 5 prvků, z nichž právě jeden neobsahuje proměnné w, t a má tvar

$$x^3 - 3axy + y^3 = 0,$$



což je známé implicitní vyjádření Descartova listu. ■

Příklad 6.6 Jednu z možných racionálních parametrizací koule lze vyjádřit ve tvaru

$$x = \frac{4ur^2}{u^2 + v^2 + 4r^2}, \quad y = \frac{4vr^2}{u^2 + v^2 + 4r^2}, \quad z = \frac{r(u^2 + v^2 - 4r^2)}{u^2 + v^2 + 4r^2}.$$

V tomto případě stačí použít algoritmus převodu polynomiální parametrizace na implicitní vyjádření, jelikož jmenovatele zlomků jsou vždy různé od nuly (vždy je $r \neq 0$). Redukovaná Gröbnerova báze ideálu generovaného rovnicemi parametrického vyjádření koule po odstranění zlomků obsahuje 5 prvků, z nichž pouze jeden neobsahuje parametry u, v a má tvar

$$x^2 + y^2 + z^2 - r^2 = 0.$$

To je známé implicitní vyjádření koule. ■

Z věty 6.2.2 dále plyne, že ke všem NURBS objektům lze najít jejich implicitní vyjádření. Podrobnější informace o problematice NURBS objektů lze najít např. v [21].

Mohlo by se zdát, že lze převést parametrické vyjádření afinní variety na implicitní jen pro variety zadané polynomiální nebo racionální parametrizací. To by ale znamenalo značné omezení, jelikož mnoho afinních variet (zejména křivek a ploch) lze snadno parametrizovat pomocí goniometrických funkcí. V některých případech sice lze najít racionální parametrizace, bývá to ale nesrovnatelně obtížnější.

Nicméně po jistých úpravách lze užít redukované Gröbnerovy báze i pro nalezení implicitního vyjádření některých afinních variet parametrizovaných pomocí goniometrických funkcí. Stačí zavést označení příslušných funkcí, např. $c_t = \cos t$, $s_t = \sin t$ (případně i pro další parametry), což vede k polynomům v proměnných c_t, s_t . Dále je nutné přidat identitu

$$c_t^2 + s_t^2 = 1,$$

jinak by počet rovnic byl příliš malý a nebylo by možné eliminovat všechny parametry. Dále už se postupuje podle algoritmů převodu polynomiální nebo racionální parametrizace na implicitní vyjádření.

Příklad 6.7 Parametrické vyjádření Bernoulliho lemniskáty lze zapsat ve tvaru

$$x = \frac{a \cos t}{1 + \sin^2 t}, \quad y = \frac{a \cos t \sin t}{1 + \sin^2 t}.$$

Zavede se označení $c_t = \cos t$, $s_t = \sin t$, což vede k polynomům v proměnných c_t , s_t , x , y , z ve tvaru

$$x(1 + s_t^2) - ac_t = 0, \quad y(1 + s_t^2) - ac_t s_t = 0. \quad (6.8)$$

Musí se ještě přidat identita

$$\cos^2 t + \sin^2 t = 1 \quad \longleftrightarrow \quad c_t^2 + s_t^2 - 1 = 0. \quad (6.9)$$

Nyní již stačí použít algoritmus převodu polynomiální parametrizace na implicitní vyjádření, jelikož jmenovatel zlomků nemůže být nikdy nulový. Pro ideál generovaný polynomy (6.8) a (6.9) má redukovaná Gröbnerova báze 5 prvků, z nichž pouze jeden neobsahuje žádnou z proměnných c_t , s_t a má tvar

$$x^4 + 2x^2y^2 - a^2x^2 + y^4 + a^2y^2 = 0.$$

To lze ještě přepsat do tvaru

$$(x^2 + y^2)^2 - a^2(x^2 - y^2) = 0,$$

což je hledané implicitní vyjádření Bernoulliho lemniskáty. ■

Příklad 6.8 Parametrické vyjádření anuloidu lze vyjádřit ve tvaru

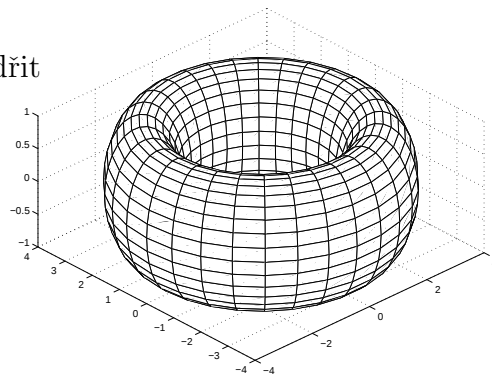
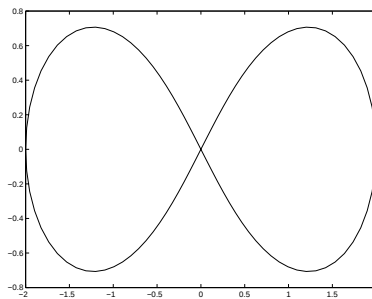
$$\begin{aligned} x &= r \cos u \cos t + R \cos t, \\ y &= r \cos u \sin t + R \sin t, \\ z &= r \sin u. \end{aligned}$$

Zavede se označení

$$c_u = \cos u, \quad c_t = \cos t, \quad s_u = \sin u, \quad s_t = \sin t,$$

což vede k polynomům v proměnných c_u , s_u , c_t , s_t , x , y , z ve tvaru

$$\begin{aligned} x - rc_u c_t - Rc_t &= 0, \\ y - rc_u s_t - Rs_t &= 0, \\ z - rs_u &= 0. \end{aligned} \quad (6.10)$$



Zbývá přidat identity

$$\begin{aligned}\cos^2 u + \sin^2 u = 1 &\longleftrightarrow c_u^2 + s_u^2 - 1 = 0, \\ \cos^2 t + \sin^2 t = 1 &\longleftrightarrow c_t^2 + s_t^2 - 1 = 0.\end{aligned}\tag{6.11}$$

Redukovaná Gröbnerova báze pro ideál generovaný polynomy (6.10) a (6.11) obsahuje 9 prvků, z nichž právě jeden neobsahuje žádnou z proměnných c_u, c_t, s_u, s_t a má tvar

$$x^4 + 2x^2y^2 + 2x^2z^2 - (2R^2 + 2r^2)x^2 + y^4 + 2y^2z^2 - (2R^2 + 2r^2)y^2 + z^4 - (2r^2 - 2R^2)z^2 + r^4 - 2r^2R^2 + R^4 = 0.$$

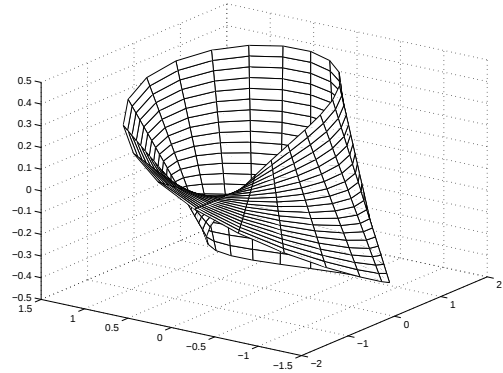
To lze ještě přepsat do tvaru

$$(x^2 + y^2 + z^2 - r^2 - R^2)^2 = 4R^2(z^2 - r^2),$$

což je hledané implicitní vyjádření anuloidu. ■

Příklad 6.9 Parametrické vyjádření Möbiova listu lze zapsat ve tvaru

$$\begin{aligned}x &= \cos u + v \sin \frac{1}{2}u \cos u, \\ y &= \sin u + v \sin \frac{1}{2}u \sin u, \\ z &= v \cos \frac{1}{2}u.\end{aligned}$$



Zavede se označení

$$c_1 = \cos u, \quad s_1 = \sin u, \quad c_2 = \cos \frac{1}{2}u, \quad s_2 = \sin \frac{1}{2}u.$$

To vede k polynomům

$$\begin{aligned}x &= c_1 + vs_2c_1, \\ y &= s_1 + vs_2s_1, \\ z &= vc_2,\end{aligned}\tag{6.12}$$

což jsou polynomy v proměnných $c_1, c_2, s_1, s_2, v, x, y, z$. Úkolem implicitizace je eliminovat proměnné c_1, c_2, s_1, s_2, v . Je nutné ještě přidat identity

$$\begin{aligned}\cos^2 u + \sin^2 u = 1 &\longleftrightarrow c_1^2 + s_1^2 - 1 = 0, \\ \cos^2 \frac{1}{2}u + \sin^2 \frac{1}{2}u = 1 &\longleftrightarrow c_2^2 + s_2^2 - 1 = 0.\end{aligned}\tag{6.13}$$

To ale ještě nestačí. Parametrické vyjádření (6.12) a identity (6.13) představují pouze 5 rovnic a je třeba eliminovat 5 parametrů. To je zřejmě málo, jelikož musí být alespoň o jednu rovnici více, než je počet proměnných, které chceme eliminovat. Musí se tedy přidat ještě další vztahy

$$\begin{aligned}\sin u = 2 \sin \frac{1}{2}u \cos \frac{1}{2}u &\longleftrightarrow s_1 - 2s_2c_2 = 0, \\ \cos u = \cos^2 \frac{1}{2}u - \sin^2 \frac{1}{2}u &\longleftrightarrow c_1 - c_2^2 + s_2^2 = 0.\end{aligned}\tag{6.14}$$

Redukovaná Gröbnerova báze pro ideál generovaný polynomy (6.12), (6.13) a (6.14) obsahuje 11 prvků, z nichž pouze jeden neobsahuje žádnou z proměnných c_1, c_2, s_1, s_2, v a má tvar

$$x^2y - 2x^2z + 2xz + y^3 - 2y^2z + yz^2 - y = 0. \quad (6.15)$$

Polynom (6.15) je implicitním vyjádřením Möbiova listu. ■

6.3 Automatické dokazování v geometrii

Základním principem automatického dokazování geometrických tvrzení je, že zavede-li se kartézský souřadnicový systém do euklidovské roviny, mnoho předpokladů a závěrů geometrických tvrzení lze vyjádřit ve tvaru polynomiálních rovnic souřadnic bodů v rovině.

Dá se ukázat, že ve tvaru polynomiálních rovnic lze zapsat např. tato geometrická vyjádření:

- $\overline{AB}$ je rovnoběžné se $\overline{CD}$.
- $\overline{AB}$ je kolmé na $\overline{CD}$.
- Body A, B, C leží na jedné přímce.
- Rovnost vzdáleností dvou bodů: $AB = CD$.
- C leží na kružnici se středem A a poloměrem AB .
- C je střed úsečky $\overline{AB}$.
- Ostrý úhel $\angle ABC$ je roven ostrému úhlu $\angle DEF$.
- $\overline{BD}$ půlí úhel $\angle ABC$.

Následující věta hovoří o tom, jak lze poznat, že dané tvrzení vyplývá z formulovaných předpokladů.

Věta 6.3.1 *Nechť jsou dány předpoklady $h_1 = 0, \dots, h_i = 0$ a $s_1 \neq 0, \dots, s_j \neq 0$ a chtějme ukázat, že tvrzení g vyplývá z platnosti uvedených předpokladů, přičemž $h_1, \dots, h_i, s_1, \dots, s_j, g \in \mathbb{Q}[u_1, \dots, u_k, x_1, \dots, x_l]$. Nechť dále*

$$f = \left((h_1 = 0 \wedge \dots \wedge h_i = 0 \wedge s_1 \neq 0 \wedge \dots \wedge s_j \neq 0) \Rightarrow g = 0 \right).$$

Potom výraz f je pravdivý nad algebraicky uzavřeným tělesem obsahujícím $\mathbb{Q}$ právě tehdy, když soustava rovnic

$$h_1 = 0, \dots, h_i = 0, s_1z_1 - 1 = 0, \dots, s_jz_j - 1 = 0, gz - 1 = 0, \quad (6.16)$$

kde $z_1, \dots, z_j$ jsou nově přidané proměnné, nemá řešení nad tímto algebraicky uzavřeným tělesem.

Důkaz: Viz [30]. □

Místo podrobného důkazu se provede pouze úvaha, odkud plyne tvrzení věty. Uvažujme soustavu (6.16). Pokud platí první část výroku f , tj.

$$h_1 = 0 \wedge \dots \wedge h_i = 0 \wedge s_1 \neq 0 \wedge \dots \wedge s_j \neq 0,$$

potom to znamená, že rovnice

$$h_1 = 0, \dots, h_i = 0, s_1 z_1 - 1 = 0, \dots, s_j z_j - 1 = 0$$

jsou určitě splněny, jelikož $s_j \neq 0$ pro každé j , a tedy určitě lze nalézt takové z_j , pro které platí rovnice $s_j z_j - 1 = 0$. Pokud soustava nemá řešení, potom to znamená, že poslední rovnice $1 - gz = 0$ nemůže být splněna. Pokud by g bylo různé od nuly, potom lze jistě nalézt takové z , aby rovnice splněna byla. Odtud tedy plyne, že musí být $g = 0$.

Poznámka 6.3.2 *Předpoklady $s_1 \neq 0, \dots, s_j \neq 0$ často vyjadřují omezení daného geometrického útvaru a vylučují různé degenerované případy daného objektu.*

Ověření, zda soustava rovnic (6.16) má řešení, lze provést pomocí Gröbnerovy báze ideálu a podrobněji byla tato problematika probrána v části 6.1. Stačí tedy ukázat, že redukovaná Gröbnerova báze vzhledem k **lex** uspořádání pro ideál generovaný polynomy určujícími soustavu rovnic (6.16) je $\{1\}$.

Počet rovnic soustavy a počet nových proměnných je možné ještě zredukovat. Místo soustavy rovnic (6.16) lze uvažovat soustavu

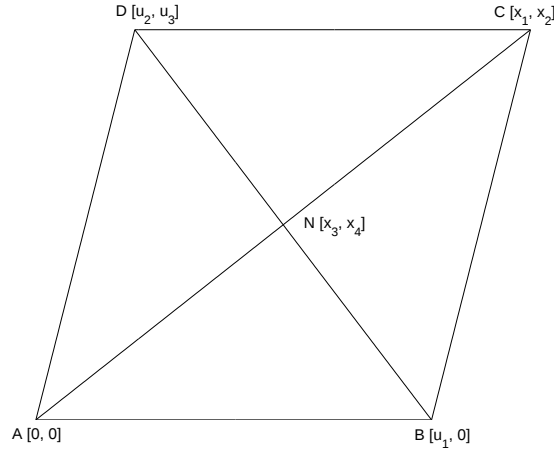
$$h_1 = 0, \dots, h_i = 0, s_1 \cdots s_j gz - 1 = 0. \tag{6.17}$$

Pokud soustava rovnic (6.17) nemá řešení, potom výraz f je pravdivý a tvrzení g vyplývá z předpokladů $h_1 = 0, \dots, h_j = 0$ s omezeními $s_1 \neq 0, \dots, s_j \neq 0$.

Existuje ale také další možnost ověření, zda tvrzení g vyplývá z předpokladů $h_1, \dots, h_i$, aniž je nutné uvažovat omezení $s_1, \dots, s_j$. Dá se ukázat, že g vyplývá z hypotéz $h_1, \dots, h_i$ právě tehdy, když $\{1\}$ je redukovanou Gröbnerovou bází ideálu $\langle h_1, \dots, h_i, 1 - yg \rangle$, kde $h_1, \dots, h_i, g \in \mathbb{R}(u_1, \dots, u_k)[x_1, \dots, x_l]$. Volné proměnné $u_1, \dots, u_k$ se berou pouze jako parametry a mohou se vyskytovat i ve jmenovatelích zlomků. V tomto případě je ale nutné zkoumat také přímo Gröbnerovu bázi, která může obsahovat polynom ve volných proměnných a ze kterého plynou degenerované případy, tzn. omezení $s_1, \dots, s_j$ za kterých dané tvrzení platí.

Jako vhodnější z uvedených metod se jeví metoda druhá, kdy se volné proměnné berou jako parametry. Vhodnější je zejména z časových důvodů, jelikož méně proměnných téměř vždy znamená také kratší výpočet, a to často velmi podstatně.

Použití obou možných způsobů bude předvedeno na několika příkladech.



Obrázek 6.1: Rovnoběžník

Příklad 6.10 Dokažme tvrzení, že úhlopříčky rovnoběžníka se navzájem půlí. Uvažujme rovnoběžník se souřadnicemi vrcholů podle obr. 6.1.

Vlastnosti rovnoběžníka se nemění vzhledem k posunutí a rotaci, proto jej lze posunout do počátku soustavy souřadnic. Proměnné u_1, u_2, u_3 jsou volné (ale nesmí být $u_1 = 0$ ani $u_3 = 0$, jinak by rovnoběžník degeneroval na úsečku) a určují rovnoběžník. Proměnné $x_1, \dots, x_4$ jsou na nich závislé (jsou jistě afinním invariantem). Nejdříve zformulujeme předpoklady rovnoběžnosti protilehlých stran, které zaručí, že se jedná o rovnoběžník. Platí:

$$\begin{aligned} \overline{AB} \parallel \overline{CD} &: h_1 = x_2 - u_3 = 0, \\ \overline{AD} \parallel \overline{BC} &: h_2 = (x_1 - u_1)u_3 - x_2u_2 = 0. \end{aligned}$$

Dále je nutné požadovat, aby trojice bodů A, N, C a B, N, D byly kolineární, tzn. ležely na jedné přímce. Odtud plynou další dva vztahy

$$\begin{aligned} A, N, C \text{ jsou kolineární} &: h_3 = x_4x_1 - x_3u_3 = 0, \\ B, N, D \text{ jsou kolineární} &: h_4 = x_4(u_2 - u_1) - (x_3 - u_1)u_3 = 0. \end{aligned}$$

Zbývá vyjádřit tvrzení, že bod N půlí obě úhlopříčky. To lze zapsat také pomocí polynomů, a to ve tvaru

$$\begin{aligned} AN = NC &: g_1 = x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2, \\ BN = ND &: g_2 = (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2, \end{aligned}$$

resp. ekvivalentně např. ve tvaru

$$\begin{aligned} AN = NC &: g_1 = x_1 - 2x_3 = 0, \\ BN = ND &: g_2 = u_1 - u_2 - 2(x_3 - u_2) = 0. \end{aligned}$$

Je dobré si všimnout, že uvedené vztahy obsahují čtyři závislé proměnné x_i a pro důkaz se vycházelo ze čtyř předpokladů. Všechna správně formulovaná tvrzení mají stejný počet předpokladů jako závislých proměnných.

K ověření, že tvrzení g_1 , resp. g_2 plyne z formulovaných předpokladů, je nutné zavést omezení

$$s_1 : u_1 \neq 0, \quad s_2 : u_3 \neq 0,$$

jelikož v obou případech by rovnoběžník degeneroval na úsečku. Podle věty 6.3.1 a následujících odstavců se pro daný případ uvažuje ideál $I_1 = \langle h_1, \dots, h_4, 1 - u_1 u_3 g_1 z \rangle$, resp. $I_2 = \langle h_1, \dots, h_4, 1 - u_1 u_3 g_2 z \rangle$. Redukovaná Gröbnerova báze pro ideál I_1 , resp. I_2 vzhledem k **lex** uspořádání je skutečně $\{1\}$.

Další možností je uvažovat ideál $J_1 = \langle h_1, \dots, h_4, 1 - g_1 z \rangle$, resp. $J_2 = \langle h_1, \dots, h_4, 1 - g_2 z \rangle$ a volné proměnné považovat za parametry. I v tomto případě je redukovaná Gröbnerova báze pro ideál J_1 , resp. J_2 vzhledem k **lex** uspořádání $\{1\}$. ■

Příklad 6.11 (Apolloniova úloha) Nechť $\triangle ABC$ je pravoúhlý trojúhelník s pravým úhlem u bodu A . Dokažme, že středy všech stran trojúhelníka a pata výšky z bodu A na stranu $\overline{BC}$ leží na jedné kružnici.

Souřadnice bodů označme podle obr. 6.2. Umístění lze zvolit tak, aby bod A měl souřadnice $(0, 0)$ a bod B měl souřadnice $(u_1, 0)$. Potom bod C má souřadnice $(0, u_2)$. Dále je nutné sestrojit středy jednotlivých stran trojúhelníka M_1, M_2 a M_3 . Pro závislé proměnné x_i platí

$$\begin{aligned} h_1 &= 2x_1 - u_1 = 0, \\ h_2 &= 2x_2 - u_2 = 0, \\ h_3 &= 2x_3 - u_1 = 0, \\ h_4 &= 2x_4 - u_2 = 0. \end{aligned}$$

Dále je třeba sestrojit patu výšky, tzn. bod $H = (x_5, x_6)$, pro který platí

$$\begin{aligned} AH \perp BC &: h_5 = x_5 u_1 - x_6 u_2 = 0, \\ B, H, C &\text{ jsou kolineární } : h_6 = x_5 u_2 + x_6 u_1 - u_1 u_2 = 0. \end{aligned}$$

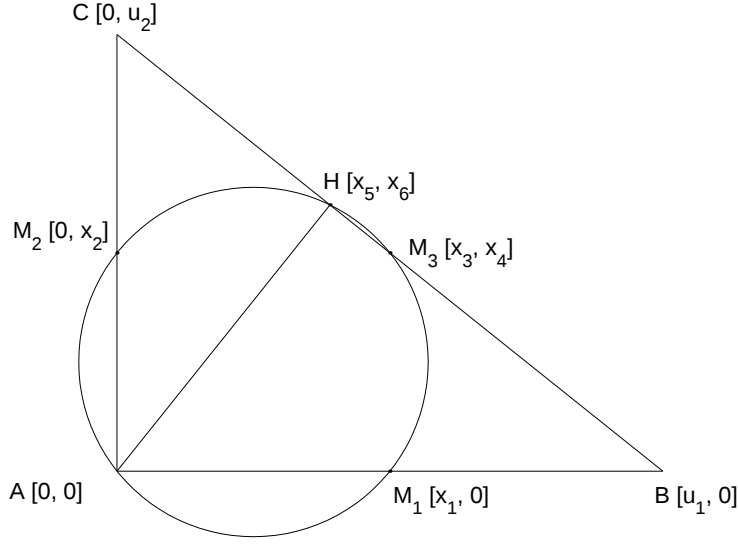
Zbývá ještě vyjádřit, že body M_1, M_2, M_3, H leží na jedné kružnici. Obecně samozřejmě čtyři body v rovině na jedné kružnici ležet nemusí. Ale tři body, které neleží na jedné přímce, vždy leží na jedné kružnici. Jestliže body M_1, M_2, M_3 neleží na jedné přímce, leží na jedné kružnici. Tedy dokážeme, že bod H leží na kružnici procházející těmito třemi body. Označme ještě souřadnice středu této kružnice $O = (x_7, x_8)$, což vede k předpokladům

$$\begin{aligned} M_1 O = M_2 O &: h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0, \\ M_1 O = M_3 O &: h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0. \end{aligned}$$

Chtějme dokázat, že $HO = M_1 O$, což znamená

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0.$$

Je vidět, že počet závislých proměnných x_i je opět stejný jako počet předpokladů. Nejdříve je možné uvažovat volné proměnné u_1, u_2 jako parametry, tzn. $h_1, \dots, h_8, g$ jsou polynomy z $\mathbb{R}(u_1, u_2)[x_1, \dots, x_8]$. Redukovaná Gröbnerova báze pro ideál $\langle h_1, \dots, h_8, 1 - yg \rangle$ je opravdu $\{1\}$ a tvrzení vyplývá z uvedených předpokladů.



Obrázek 6.2: Apolloniova úloha

Další možností je chápat $h_1, \dots, h_8, g$ jako polynomy z $\mathbb{R}[u_1, u_2, x_1, \dots, x_8]$. Potom je ale nutné vyloučit degenerované případy $u_1 = 0$ a $u_2 = 0$, kdy trojúhelník degeneruje na úsečku, příp. bod. Pro ideál $\langle h_1, \dots, h_8, 1 - u_1 u_2 y g \rangle$ je redukovaná Gröbnerova báze opět $\{1\}$. $\square$

Příklad 6.12 Necht' $\triangle ABC$ je libovolný trojúhelník v rovině. Dokažme, že všechny tři jeho výšky se protínají v jednom bodě (obr. 6.3).

Bez újmy na obecnosti lze trojúhelník zvolit tak, aby bod A byl v počátku a strana AB splývala s osou x . Bod B má potom souřadnice $(u_1, 0)$. Bod C je již libovolný a má souřadnice (u_2, u_3) . Dále zavedeme paty výšek H_1, H_2 a H_3 . Podle toho, kolik bod přidává závislých proměnných, tolik předpokladů se pro něj musí formulovat. Pro bod H_1 tedy stačí jedna podmínka, a to

$$CH_1 \perp AB : h_1 = u_1(x_1 - u_2) = 0.$$

Pro body H_2 a H_3 se musí formulovat po dvou podmínkách. První dva předpoklady jsou podmínky kolmosti

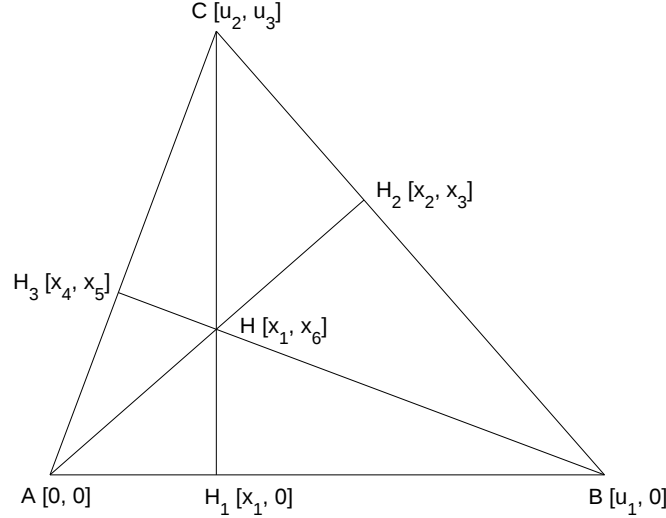
$$\begin{aligned} AH_2 \perp BC : h_2 &= x_2(u_2 - u_1) + x_3 u_3 = 0, \\ BH_3 \perp AC : h_3 &= u_2(x_4 - u_1) + u_3 x_5 = 0, \end{aligned}$$

zbylé dva jsou podmínky kolinearity

$$\begin{aligned} BH_2C \text{ jsou kolineární} : h_4 &= x_3(u_2 - u_1) - u_3(x_2 - u_1) = 0, \\ AH_3C \text{ jsou kolineární} : h_5 &= x_5 u_2 - u_3 x_4 = 0. \end{aligned}$$

Dále se zvolí bod $H = (x_1, x_6)$ na úsečce CH_1 tak, aby body BHH_3 byly kolineární. To lze vyjádřit podmínkou

$$BHH_3 \text{ jsou kolineární} : h_6 = x_6(x_4 - u_1) - x_5(x_1 - u_1) = 0.$$



Obrázek 6.3: Všechny tři výšky trojúhelníka se protínají v jednom bodě

Nyní již zbývá jen formulovat tvrzení. Chtějme dokázat, že za uvedených podmínek jsou také body AHH_2 kolineární, tzn.

$$AHH_2 \text{ jsou kolineární} : g = x_6x_2 - x_3x_1 = 0.$$

Nejdříve se uvažují volné proměnné u_1, u_2, u_3 jako parametry, tzn. $h_1, \dots, h_6, g$ jsou polynomy z $\mathbb{R}(u_1, u_2, u_3)[x_1, \dots, x_6]$. Pro ideál $\langle h_1, \dots, h_6, 1 - yg \rangle$ je potom redukovaná Gröbnerova báze $\{1\}$ a tvrzení vyplývá z uvedených předpokladů.

Je také možné chápat $h_1, \dots, h_6, g$ jako polynomy z $\mathbb{R}[u_1, u_2, u_3, x_1, \dots, x_6]$. Potom je ale nutné vyloučit degenerované případy $u_1 = 0$ a $u_3 = 0$, kdy se nevhodnou volbou volných proměnných u_1, u_2, u_3 nedostane trojúhelník. Potom pro ideál $\langle h_1, \dots, h_6, 1 - u_1u_3yg \rangle$ je redukovaná Gröbnerova báze $\{1\}$. ■

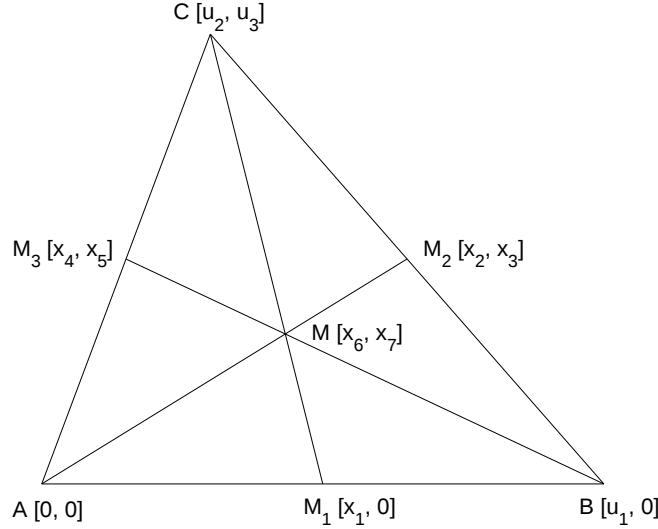
Příklad 6.13 Necht' $\triangle ABC$ je libovolný trojúhelník v rovině. Necht' M_1 je střed $\overline{BC}$, M_2 střed $\overline{AC}$ a M_3 střed $\overline{AB}$. Dokažme, že těžnice $\overline{AM_1}$, $\overline{BM_2}$ a $\overline{CM_3}$ se protínají v jediném bodě M (obr. 6.4).

Jako obvykle se umístění trojúhelníka zvolí tak, aby bod A byl v počátku souřadného systému a úsečka $\overline{AB}$ splývala s osou x . Dostáváme tedy souřadnice vrcholů trojúhelníka

$$A = (0, 0), \quad B = (u_1, 0), \quad C = (u_2, u_3).$$

Jelikož souřadnice středů stran jsou již určeny souřadnicemi vrcholů trojúhelníka, lze je vyjádřit pouze pomocí závislých proměnných. To vede k 5 závislým proměnným. Je tedy nutné formulovat 5 podmínek, popisujících závislé proměnné $x_1, \dots, x_5$. Každý z bodů M_i je středem příslušné strany, což dává tři podmínky ve tvaru

$$\begin{aligned} AM_1 = BM_1 : h_1 &= 2x_1 - u_1 = 0, \\ CM_2 = BM_2 : h_2 &= (u_2 - x_2)^2 + (u_3 - x_3)^2 - (u_1 - x_2)^2 - x_3^2 = 0, \\ AM_3 = CM_3 : h_3 &= (u_2 - x_4)^2 + (u_3 - x_5)^2 - x_4^2 - x_5^2 = 0. \end{aligned}$$



Obrázek 6.4: Všechny tři těžnice trojúhelníka se protínají v jediném bodě

Zbývá zapsat dvě podmínky. Body B, M_2, C , resp. A, M_3, C zřejmě musí ležet na jedné přímce, což vede ke zbývajícím dvěma podmínkám

$$\begin{aligned} B, M_2, C \text{ jsou kolineární} & : h_4 = x_3(u_2 - u_1) - u_3(x_2 - u_1) = 0, \\ A, M_3, C \text{ jsou kolineární} & : h_5 = x_5u_2 - u_3x_4 = 0. \end{aligned}$$

Bod M se zavede jako průsečík úseček $\overline{CM_1}$ a $\overline{AM_2}$. Takový bod jistě existuje (pro nede-generované případy trojúhelníka, tzn. pro $u_1 \neq 0$ a $u_3 \neq 0$) a musí pro něj platit

$$\begin{aligned} C, M, M_1 \text{ jsou kolineární} & : h_6 = x_7(u_2 - x_1) - u_3(x_6 - x_1) = 0, \\ A, M, M_2 \text{ jsou kolineární} & : h_7 = x_7x_2 - x_3x_6 = 0. \end{aligned}$$

Za uvedených předpokladů chtějme ukázat, že také body B, M, M_3 musí být kolineární, tzn.

$$B, M, M_3 \text{ jsou kolineární} : g = x_7(x_4 - u_1) - x_5(x_6 - u_1) = 0.$$

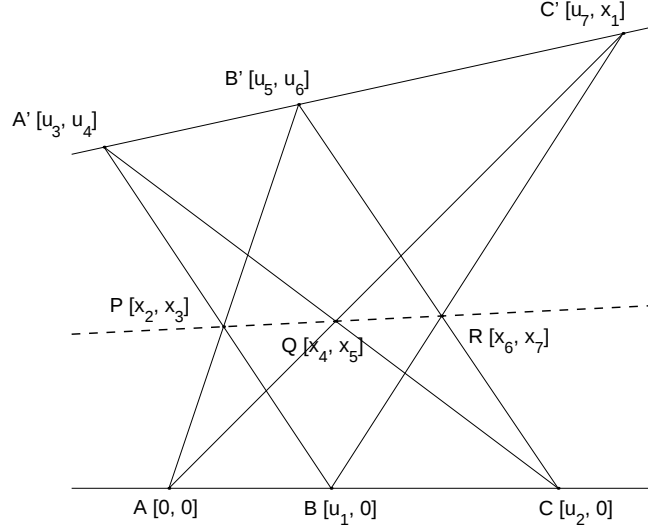
Redukovaná Gröbnerova báze v $\mathbb{R}(u_1, u_2, u_3)[x_1, \dots, x_7, y]$ vzhledem k **lex** uspořádání pro ideál $\langle h_1, \dots, h_7, 1 - yg \rangle$ je potom $\{1\}$. Tvrzení tedy vyplývá z uvedených předpokladů.

Provede-li se výpočet redukované Gröbnerovy báze v $\mathbb{R}[u_1, u_2, u_3, x_1, \dots, x_7, y]$, je nutné vyloučit degenerované případy trojúhelníka, tzn. vyloučit případy $u_1 = 0$ a $u_3 = 0$. Potom pro ideál $\langle h_1, \dots, h_7, 1 - u_1u_3yg \rangle$ je redukovaná Gröbnerova báze opět $\{1\}$. ■

Příklad 6.14 (Pappova věta) Mějme dvě kolineární trojice bodů A, B, C a A', B', C' . Nechť dále platí

$$P = \overline{AB'} \cap \overline{A'B}, \quad Q = \overline{AC'} \cap \overline{A'C}, \quad R = \overline{BC'} \cap \overline{B'C}.$$

Potom také P, Q, R jsou kolineární (obr. 6.5).



Obrázek 6.5: Pappova věta

Označení bodů a jim příslušných souřadnic provedeme podle obr. 6.5, odkud je vidět, že bod C' nemůže být volen zcela libovolně a jedna jeho souřadnice je závislá na volbě souřadnic bodů A' a B' . To je zřejmé z toho, že trojice bodů A' , B' , C' musí být kolineární. Je vidět, že dostaneme 7 volných proměnných a 7 závislých proměnných. Je nutné tedy formulovat 7 podmínek. Vzhledem k charakteru úlohy to budou výhradně podmínky kolinearity. Platí:

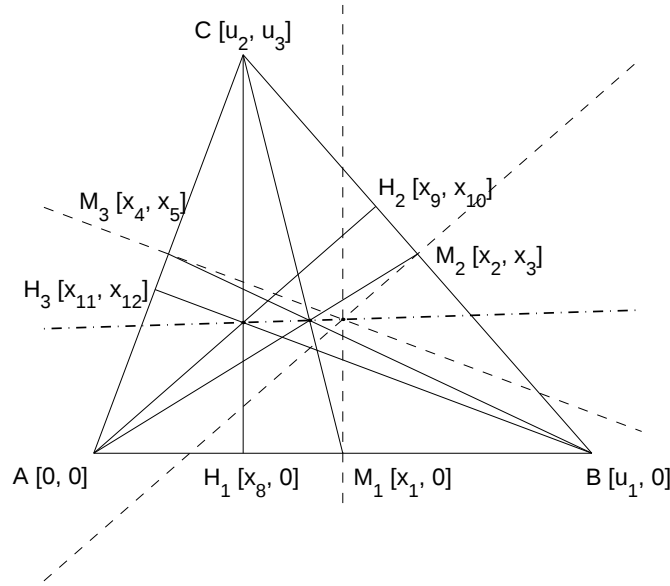
$$\begin{aligned}
A', B', C' \text{ jsou kolineární} & : h_1 = (u_6 - u_4)(u_7 - u_3) - (x_1 - u_4)(u_5 - u_3) = 0, \\
A', P, B \text{ jsou kolineární} & : h_2 = x_3(u_3 - u_1) - u_4(x_2 - u_1) = 0, \\
A', Q, C \text{ jsou kolineární} & : h_3 = x_5(u_3 - u_2) - u_4(x_4 - u_2) = 0, \\
B', P, A \text{ jsou kolineární} & : h_4 = u_5x_3 - u_6x_2 = 0, \\
B', R, C \text{ jsou kolineární} & : h_5 = x_7(u_5 - u_2) - u_6(x_6 - u_2) = 0, \\
C', Q, A \text{ jsou kolineární} & : h_6 = x_5u_7 - x_1x_4 = 0, \\
C', R, B \text{ jsou kolineární} & : h_7 = x_7(u_7 - u_1) - x_1(x_6 - u_1) = 0.
\end{aligned}$$

Zbývá ještě zformulovat tvrzení. Chtějme dokázat, že za uvedených předpokladů musí být také body P, Q, R kolineární, tzn.

$$P, Q, R \text{ jsou kolineární} : g = (x_5 - x_3)(x_6 - x_2) - (x_7 - x_3)(x_4 - x_2) = 0.$$

Redukovaná Gröbnerova báze v $\mathbb{R}(u_1, \dots, u_7)[x_1, \dots, x_7, y]$ vzhledem k **lex** uspořádání pro ideál $\langle h_1, \dots, h_7, 1 - yg \rangle$ je $\{1\}$. Tvrzení tedy vyplývá z uvedených předpokladů.

Provede-li se výpočet redukované Gröbnerovy báze v $\mathbb{R}[u_1, \dots, u_7, x_1, \dots, x_7, y]$, je nutné vyloučit degenerované případy, které pro tuto úlohu jsou $u_2 = 0$, $u_4 = 0$ a $u_7 = 0$. Potom pro ideál $\langle h_1, \dots, h_7, 1 - u_2u_4u_7yg \rangle$ je redukovaná Gröbnerova báze opět $\{1\}$. ■



Obrázek 6.6: Eulerova věta

Příklad 6.15 (Eulerova věta) Mějme libovolný $\triangle ABC$ v rovině. Dokažme, že střed kružnice opsané, průsečík výšek (ortocentrum) a průsečík těžnic (těžiště) trojúhelníka ABC leží na jedné přímce (obr. 6.6).

Souřadnice bodů se přiřadí podle obr. 6.6. Body H_1, H_2, H_3 představují paty výšek, body M_1, M_2, M_3 jsou středy stran. Je vidět, že opět jsou třeba jen 3 volné proměnné u_1, u_2, u_3 , určující body A, B, C a tím i umístění trojúhelníka. S využitím příkladu 6.12 lze formulovat podmínky pro bod H

$$\begin{aligned}
CH_1 \perp AB & : h_1 = u_1(x_8 - u_2) = 0, \\
AH_2 \perp BC & : h_2 = x_9(u_2 - u_1) + x_{10}u_3 = 0, \\
BH_3 \perp AC & : h_3 = u_2(x_{11} - u_1) + u_3x_{12} = 0, \\
BH_2C \text{ jsou kolineární} & : h_4 = x_{10}(u_2 - u_1) - u_3(x_9 - u_1) = 0, \\
AH_3C \text{ jsou kolineární} & : h_5 = x_{12}u_2 - u_3x_{11} = 0, \\
BHH_3 \text{ jsou kolineární} & : h_6 = x_{13}(x_{11} - u_1) - x_{12}(x_8 - u_1) = 0.
\end{aligned}$$

Podobně pro zavedení bodu M lze využít již formulovaných předpokladů z příkladu 6.13

$$\begin{aligned}
AM_1 = BM_1 & : h_7 = 2x_1 - u_1 = 0, \\
CM_2 = BM_2 & : h_8 = (u_2 - x_2)^2 + (u_3 - x_3)^2 - (u_1 - x_2)^2 - x_3^2 = 0, \\
AM_3 = CM_3 & : h_9 = (u_2 - x_4)^2 + (u_3 - x_5)^2 - x_4^2 - x_5^2 = 0, \\
B, M_2, C \text{ jsou kolineární} & : h_{10} = x_3(u_2 - u_1) - u_3(x_2 - u_1) = 0, \\
A, M_3, C \text{ jsou kolineární} & : h_{11} = x_5u_2 - u_3x_4 = 0, \\
C, M, M_1 \text{ jsou kolineární} & : h_{12} = x_7(u_2 - x_1) - u_3(x_6 - x_1) = 0, \\
A, M, M_2 \text{ jsou kolineární} & : h_{13} = x_7x_2 - x_3x_6 = 0.
\end{aligned}$$

Střed kružnice opsané O dostaneme jako průsečík os stran. To vede k podmínkám

$$\begin{aligned} OM_2 \perp BC & : h_{14} = (x_2 - x_{14})(u_2 - u_1) + u_3(x_3 - x_{15}) = 0, \\ OM_3 \perp AC & : h_{15} = u_2(x_4 - x_{14}) + u_3(x_3 - x_{15}) = 0. \end{aligned}$$

Ještě je třeba formulovat dokazované tvrzení. Chtějme dokázat, že za uvedených předpokladů musí být body H, M, O kolineární, tzn.

$$H, M, O \text{ jsou kolineární} : g = (x_7 - x_{15})(x_8 - x_{14}) - (x_{13} - x_{15})(x_6 - x_{14}) = 0.$$

Podmínky $h_1, \dots, h_{15}$ a dokazované tvrzení g je možné chápat jako polynomy z okruhu $\mathbb{R}(u_1, u_2, u_3)[x_1, \dots, x_{15}]$. Redukovaná Gröbnerova báze pro ideál $\langle h_1, \dots, h_{15}, 1 - yg \rangle$ je $\{1\}$. Tvrzení tedy vyplývá ze zadaných předpokladů.

I v tomto případě je ale také možné chápat podmínky $h_1, \dots, h_{15}$ a tvrzení g jako polynomy z $\mathbb{R}[u_1, u_2, u_3, x_1, \dots, x_{15}]$. Je ale nutné vyloučit degenerované případy trojúhelníka $u_1 = 0$ a $u_3 = 0$. Potom pro ideál $\langle h_1, \dots, h_{15}, 1 - u_1 u_3 yg \rangle$ je redukovaná Gröbnerova báze $\{1\}$. ■

6.4 Kótování a variační geometrie

Kótování objektu může velice dobře sloužit k variantnímu návrhu tohoto objektu. Popis objektu je v takovém případě dán okótováním a každá změna některé z kót vede ke změně metrické informace v popisu objektu a následně také k novému výkresu, zobrazujícímu daný objekt.

Nejdříve bude popsán potřebný aparát pro užití kót k variantnímu konstruování. Každá kóta bude generovat jednu (jednoduché podmínky) nebo dvě (složené podmínky) obecně nelineární algebraické rovnice, jejichž řešením lze dostat souřadnice opěrných bodů objektu. Mezi jednoduché podmínky patří:

Kóta rozdílu x -ových souřadnic: Pro dva body $b_m = (x_m, y_m)$ a $b_n = (x_n, y_n)$ lze pro kótu A_{mn} rozdílu x -ových souřadnic dostat podmínku

$$x_n - x_m = A_{mn}.$$

Kóta rozdílu y -ových souřadnic: Pro body $b_m = (x_m, y_m)$ a $b_n = (x_n, y_n)$ lze pro kótu B_{mn} rozdílu y -ových souřadnic dostat podmínku

$$y_n - y_m = B_{mn}.$$

Kóta vzdálenosti dvou bodů: Kóta vzdálenosti C_{mn} bodů b_m a b_n odpovídá podmínce

$$(x_m - x_n)^2 + (y_m - y_n)^2 = C_{mn}^2.$$

Kóta úhlu dvou přímek: Označme $\vec{p}_{mn} = (x_n - x_m, y_n - y_m)$ vektor určený body b_n a b_m . Kóta úhlu D_{ijkq} , který svírají vektory $\vec{p}_{ij}$ a $\vec{p}_{kq}$, odpovídá vztahu, vycházejícímu ze skalárního součinu těchto vektorů, tzn.

$$\cos D_{ijkq} = \frac{\vec{p}_{ij} \cdot \vec{p}_{kq}}{|\vec{p}_{ij}| |\vec{p}_{kq}|}.$$

Kóta průměru kružnice: Tato podmínka je totožná s jednou podmínkou typu vzdálenosti dvou bodů.

Mezi složené podmínky potom patří:

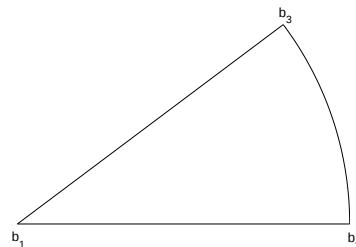
Kóta poloměru: Podmínka poloměru kružnice nebo kruhového oblouku je totožná se dvěma podmínkami typu vzdálenosti dvou bodů.

Kóta vzdálenosti dvou rovnoběžných přímek: Jestliže E_{ijkq} je vzdálenost dvou rovnoběžných přímek určených body $b_i b_j$, resp. $b_k b_q$, potom příslušné podmínky lze zapsat ve tvaru:

- podmínka rovnoběžnosti: $\vec{p}_{ij} \cdot \vec{n}_{kq} = 0$,
kde $\vec{n}_{kq}$ je vektor normály přímky $b_k b_q$.
- vztah pro vzdálenost E_{ijkq} : $\vec{p}_{ik} \cdot \vec{n}_{ij} = E_{ijkq} |\vec{p}_{ij}|$.
Jde tedy o průmět vektoru $\vec{p}_{ik}$ do směru vektoru normály k přímce $b_i b_j$.

Dále je potřeba vysvětlit pojmy zobecněné lomené čáry a množiny opěrných bodů. Nebudou zde uváděny přesné definice, pouze bude na příkladě pro představu ukázáno, jak vypadá konkrétní zápis zobecněné lomené čáry a odpovídající množiny opěrných bodů. Objektu na obrázku odpovídá zobecněná lomená čára

$$z = (b_1, b_2, (+, b_1), b_3, b_1).$$



Z obrázku je patrné, jakou část objektu představuje příslušná část zobecněné lomené čáry. Jen pro upřesnění, $(+, b_1)$ znamená oblouk v kladném směru (proti směru hodinových ručiček) se středem v bodě b_1 . Množina opěrných bodů potom tedy je

$$o(z) = \{b_1, b_2, b_3\}.$$

K určení zobecněné lomené čáry z obrázku je třeba určit souřadnice tří bodů, tzn. je nutné mít 6 rovnic. Umístění objektu v prostoru a jeho natočení představuje tři rovnice, zbývá tedy zadat tři rovnice (např. tři jednoduché podmínky). Ze zadání těchto podmínek ještě ale neplyne existence objektu.

Definice 6.4.1 *Nechť z je zobecněná lomená čára a $o(z) = \{o_1, \dots, o_n\}$ je množina opěrných bodů. Potom objekt je dimenzován, jestliže je dáno i jednoduchých podmínek a j složených podmínek a platí*

$$i + 2j + 3 = 2n.$$

Tato vlastnost se týká počtu podmínek potřebných k určení objektu. Neříká však nic o existenci geometrické interpretace tohoto objektu. Proto je nutné zavést pojem dobře dimenzovaného objektu. Nejdříve však ještě jedna definice.

Definice 6.4.2 *Nechť je dána množina bodů $\mathcal{B} = \{b_1, \dots, b_n\}$ a $m > 0$ podmínek rozdílu x -ových nebo y -ových souřadnic $f_i(b_{i_1}, \dots, b_{i_m}) = 0$ pro tyto body. Potom body b_k a b_q jsou relativně zadanými body, jestliže existuje posloupnost bodů $b_k = b_{j_0}, \dots, b_{j_{r-1}}, b_{j_r} = b_q$ v $\mathcal{B}$ taková, že*

$$f_{j_s}(b_{j_s}, b_{j_{s+1}}) = 0, \quad s = 0, \dots, r-1,$$

kde f_{j_s} je podmínka rozdílu x -ových souřadnic a existuje posloupnost bodů $b_k = b_{i_0}, \dots, b_{i_{u-1}}, b_{i_u} = b_q$ v $\mathcal{B}$ taková, že

$$f_{i_s}(b_{i_s}, b_{i_{s+1}}) = 0, \quad s = 0, \dots, u-1,$$

kde f_{i_s} je podmínka rozdílu y -ových souřadnic.

Definice 6.4.3 *Nechť zobecněná lomená čára z je dimenzována. Označme množinu opěrných bodů $o(z) = \{p_1, \dots, p_n\}$ a necht' $p_V = (x_V, y_V)$. Necht' je dáno i jednoduchých podmínek $f_k(z) = 0$, $k = 1, \dots, i$ a j složených podmínek $f_{rk}(z) = 0$, $r = 1, 2$, $k = 1, \dots, j$. Necht' alespoň tři z proměnných x_{i_0} , y_{i_0} , x_{i_1} , y_{i_1} jsou neznámými alespoň v jedné z rovnic $f_k(z) = 0$ nebo $f_{rk}(z) = 0$ a body p_{i_0} , p_{i_1} nejsou zadány relativně.*

Potom zobecněná lomená čára z je dobře dimenzována, jestliže alespoň jedna ze soustav

$$\begin{aligned} f_k(z) &= 0, & k &= 1, \dots, i, \\ f_{rk}(z) &= 0, & r &= 1, 2 \text{ a } k = 1, \dots, j, \\ x_{i_0} &= 0, \\ y_{i_0} &= 0, \\ x_{i_1} &= 0 \end{aligned} \tag{6.18}$$

nebo

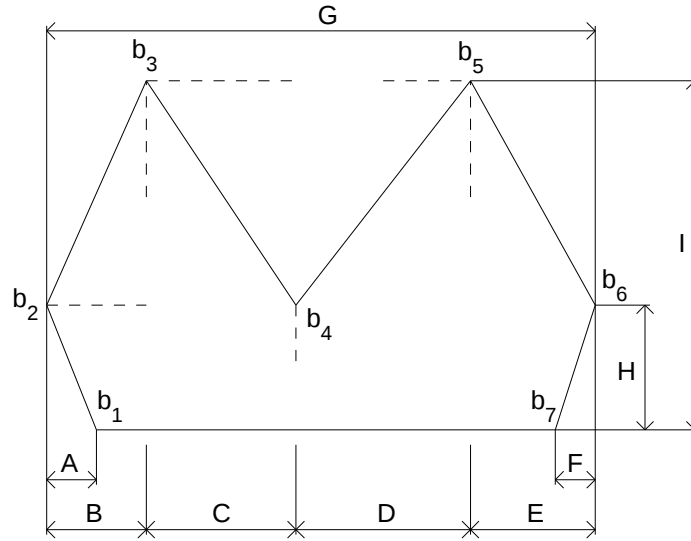
$$\begin{aligned} f_k(z) &= 0, & k &= 1, \dots, i, \\ f_{rk}(z) &= 0, & r &= 1, 2 \text{ a } k = 1, \dots, j, \\ x_{i_0} &= 0, \\ y_{i_0} &= 0, \\ y_{i_1} &= 0 \end{aligned} \tag{6.19}$$

má konečnou a neprázdnou množinu řešení.

Definice je skutečně korektní, jelikož se dá ukázat (viz [10]), že pro každou dimenzovanou zobecněnou lomenou čáru z a jí příslušnou množinu opěrných bodů $o(z)$ existují body p_{i_0} a p_{i_1} , které nejsou zadány relativně.

Je zřejmé, že soustavy (6.18) a (6.19) jsou soustavy $2n$ nelineárních algebraických rovnic. Řešení těchto soustav můžeme provést pomocí algoritmu hledání redukované Gröbnerovy báze ideálu. Stačí uvažovat ideál generovaný levými stranami rovnic soustav (6.18) nebo (6.19) a chápat je jako polynomy z $\mathbb{R}[x_1, y_1, \dots, x_n, y_n]$. Speciálním případem je objekt, který je popsán pouze kótami rozdílu x -ových nebo y -ových souřadnic. Objekt je pak popsán soustavou lineárních rovnic, která je snadno řešitelná i vylepšeným Buchbergerovým algoritmem. Takovou soustavu lze ale samozřejmě řešit mnohem jednodušeji např. Gaussovou eliminací. Uvedme si nyní příklad.

Příklad 6.16 Uvažujme zobecněnou lomenou čáru podle obr. 6.7. Snadno lze spočítat,



Obrázek 6.7: Objekt popsáný soustavou lineárních rovnic

že objekt je popsán 12 kótami, které odpovídají 12 jednoduchým podmínkám. Počet podmínek je tedy příliš vysoký, jelikož musí platit

$$i + 2j + 3 = 2n,$$

kde $n = 7$ je počet opěrných bodů a $j = 0$. Je nutné tedy odebrat některou z kót G , B , C , D , E . Vynechání kóty G vede k soustavě rovnic

$$\begin{array}{ll} x_2 - x_1 = -A & y_5 - y_1 = I \\ y_2 - y_1 = H & x_6 - x_5 = E \\ x_3 - x_2 = B & y_6 - y_1 = H \\ y_3 - y_1 = I & x_7 - x_6 = -F \\ x_4 - x_3 = C & x_1 = 0 \\ y_4 - y_1 = H & y_1 = 0 \\ x_5 - x_4 = D & y_7 = 0, \end{array} \quad (6.20)$$

které odpovídá redukovaná Gröbnerova báze

$$\begin{array}{rcl}
x_1 & = & 0 \\
x_2 + A & = & 0 \\
x_3 + A - B & = & 0 \\
x_4 - A - B - C & = & 0 \\
x_5 + A - B - C - D & = & 0 \\
x_6 + A - B - C - D - E & = & 0 \\
x_7 + A - B - C - D - E + F & = & 0
\end{array}
\qquad
\begin{array}{rcl}
y_1 & = & 0 \\
y_2 - H & = & 0 \\
y_3 - I & = & 0 \\
y_4 - H & = & 0 \\
y_5 - I & = & 0 \\
y_6 - H & = & 0 \\
y_7 & = & 0.
\end{array}
\tag{6.21}$$

Odtud jsou již vidět souřadnice opěrných bodů $b_1, \dots, b_7$. Soustavu 6.20 je samozřejmě možné řešit také pomocí Gaussovy eliminace.

Z obr. 6.7 je zřejmé, že nelze vynechat ani kótu I ani H , protože by tak byly odebrány dvě, resp. tři jednoduché podmínky místo jedné. Zbývá vyzkoušet, co se stane, odebere-li se některá z kót A, F místo výše uvedených. Soustava bude mít správný počet rovnic a objekt tedy bude dimenzován. Nicméně z obr. 6.7 je zřejmé, že nebude určen dostatečně a neměl by být dobře dimenzován. Záměna rovnice $x_7 - x_6 = -F$ za rovnici $x_6 - x_2 = G$ vede k soustavě rovnic, jejíž redukovaná Gröbnerova báze je $\{1\}$ a Gröbnerova báze obsahuje prvek $G - B - C - D - E = 0$, tzn. pro obecné parametry soustava nemá řešení. Pokud je ale rovnost splněna, soustava má nekonečně mnoho řešení, jelikož zcela chybí informace o x -ové souřadnici bodu b_7 a je možné ji tedy volit libovolně. Objekt tedy není dobře dimenzován. Obdobná situace nastává v případě vynechání kóty A . Pokud platí $G - B - C - D - E = 0$, pak má soustava nekonečně mnoho řešení, jinak řešení nemá. V každém případě objekt ani v tomto případě není dobře dimenzován. ■

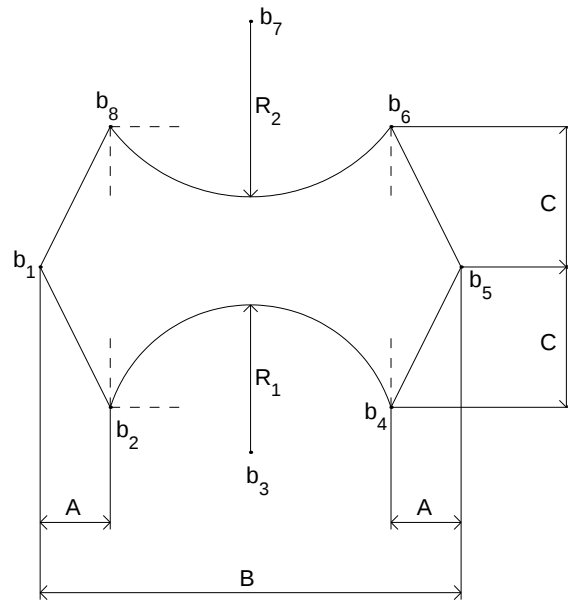
Toto je samozřejmě nejjednodušší případ okótování objektu a vzniklou soustavu rovnic je možné řešit jinými metodami (např. Gaussovou eliminací). Nyní se podíváme na příklad objektu, který už je popsán soustavou nelineárních algebraických rovnic.

Příklad 6.17 Uvažujme zobecněnou lomenou čáru podle obr. 6.8. Objekt je popsán 9 jednoduchými, 2 složenými podmínkami a obsahuje 8 opěrných bodů, tzn. platí

$$i + 2j + 3 = 2n.$$

Objekt je tedy dimenzován a zbývá zjistit, zda je dobře dimenzován. K tomu je třeba řešit soustavu rovnic

$$\begin{array}{rcl}
x_2 - x_1 & = & A \\
x_5 - x_4 & = & A \\
x_8 - x_1 & = & A \\
y_8 - y_1 & = & C \\
y_2 - y_1 & = & -C \\
x_1 & = & 0 \\
y_1 & = & 0 \\
y_5 & = & 0
\end{array}
\qquad
\begin{array}{rcl}
x_5 - x_1 & = & B \\
x_5 - x_6 & = & A \\
y_6 - y_1 & = & C \\
y_4 - y_1 & = & -C \\
(x_6 - x_7)^2 + (y_6 - y_7)^2 & = & R_2^2 \\
(x_8 - x_7)^2 + (y_8 - y_7)^2 & = & R_2^2 \\
(x_2 - x_3)^2 + (y_2 - y_3)^2 & = & R_1^2 \\
(x_4 - x_3)^2 + (y_4 - y_3)^2 & = & R_1^2.
\end{array}
\tag{6.22}$$



Obrázek 6.8: Objekt popsaný soustavou nelineárních algebraických rovnic

Redukovaná Gröbnerova báze pro ideál generovaný rovnicemi soustavy je

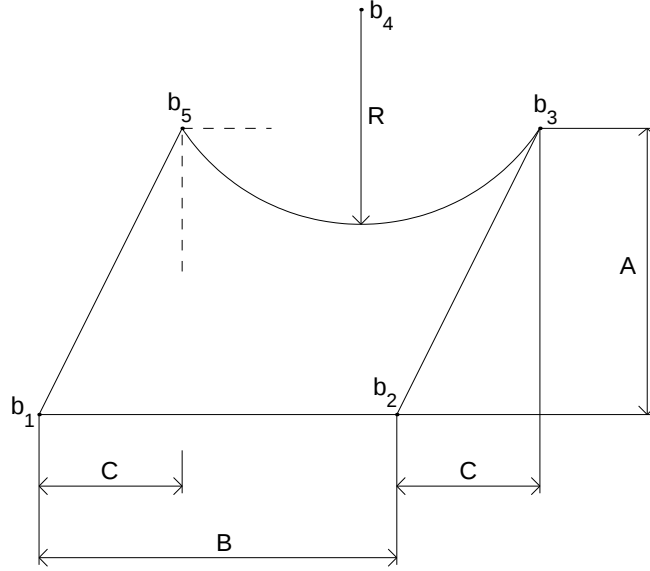
$$\begin{array}{ll}
 x_1 = 0 & y_1 = 0 \\
 x_2 - A = 0 & y_2 + C = 0 \\
 x_3 - B/2 = 0 & y_3^2 + 2Cy_3 - R_1^2 + 1/4B^2 - BA + C^2 + A^2 = 0 \\
 x_4 + A - B = 0 & y_4 + C = 0 \\
 x_5 - B = 0 & y_5 = 0 \\
 x_6 - B + A = 0 & y_6 - C = 0 \\
 x_7 - B/2 = 0 & y_7^2 - 2Cy_7 - R_2^2 + 1/4B^2 - BA + A^2 + C^2 = 0 \\
 x_8 - A = 0 & y_8 - C = 0.
 \end{array} \tag{6.23}$$

Je vidět, že nová soustava rovnic může mít až čtyři řešení v závislosti na tom, kolik reálných kořenů mají kvadratické rovnice pro souřadnice y_3 a y_7 . Lze tedy říci, že pro dostatečně velká R_1 a R_2 je objekt dobře dimenzován.

Pokud je $R_1 < (B - 2A)/2$, potom má rovnice pro y_3 pouze komplexní kořeny (dva komplexně sdružené) a objekt není možné sestavit, jelikož poloměr je příliš malý a není možné spojit opěrné body b_2 a b_4 kruhovým obloukem. Pro $R_1 = (B - 2A)/2$ existuje jeden dvojnásobný kořen a platí $y_3 = C$, pro $R_1 > (B - 2A)/2$ existují dva různé reálné kořeny.

Důvodem, proč pro dostatečně velké R_1 existují dva různé reálné kořeny, je volba orientace kruhového oblouku. Kruhový oblouk mezi opěrnými body b_2 a b_4 lze orientovat v kladném smyslu (proti směru hodinových ručiček) nebo v záporném smyslu (po směru hodinových ručiček). Podle orientace kruhového oblouku se vybere příslušný kořen kvadratické rovnice.

Zcela obdobnou úvahu lze provést pro hodnoty souřadnice y_7 a poloměr R_2 druhého kruhového oblouku. ■



Obrázek 6.9: Objekt, jehož popis obsahuje kótu vzdálenosti rovnoběžných přímek

Tato část bude uzavřena příkladem objektu, který obsahuje kótu vzdálenosti rovnoběžných přímek. Tato kóta je nepříjemná, jelikož generuje poměrně složité rovnice o velkém počtu členů, a proto značně komplikuje výpočet. To je také důvodem, proč je volen velmi jednoduchý objekt s malým počtem opěrných bodů.

Příklad 6.18 Uvažujme zobecněnou lomenou čáru podle obr. 6.9. Nejprve je nutné ověřit, zda je objekt dimenzován. Z obr. 6.9 lze snadno zjistit, že je $n = 5$, $i = 3$ a $j = 2$ a platí tedy rovnost

$$i + 2j + 3 = 2n.$$

Objekt tedy je dimenzován. To ale nestačí a je nutné ověřit, že je dobře dimenzován. To znamená řešit soustavu rovnic

$$\begin{aligned}
 x_1 &= 0 \\
 y_1 &= 0 \\
 y_2 &= 0 \\
 x_2 - x_1 &= B \\
 x_5 - x_1 &= C \\
 x_3 - x_2 &= C \\
 (x_3 - x_4)^2 + (y_3 - y_4)^2 &= R^2 \\
 (x_5 - x_4)^2 + (y_5 - y_4)^2 &= R^2 \\
 (x_2 - x_1)(y_3 - y_5) - (y_2 - y_1)(x_3 - x_5) &= 0 \\
 \left[(x_2 - x_1)(y_5 - y_1) - (y_2 - y_1)(x_5 - x_1) \right]^2 &= A^2 \left[(x_2 - x_1)^2 + (y_2 - y_1)^2 \right].
 \end{aligned} \tag{6.24}$$

Redukovaná Gröbnerova báze vzhledem k **lex** uspořádání pro ideál generovaný rovnicemi

soustavy (6.24) v $\mathbb{R}(A, B, C, R)[x_1, y_1, \dots, x_5, y_5]$ je

$$\begin{array}{rclcl}
x_1 & = & 0 & y_1 & = & 0 \\
x_2 - B & = & 0 & y_2 & = & 0 \\
x_3 - B - C & = & 0 & y_3 - y_5 & = & 0 \\
x_4 - B/2 - C & = & 0 & y_4^2 - 2y_5y_4 - R^2 - B^2/4 + A^2 & = & 0 \\
x_5 - C & = & 0 & y_5^2 - A^2 & = & 0.
\end{array} \tag{6.25}$$

Je vidět, že soustava může mít až 4 reálná řešení a objekt je tedy dobře dimenzován.

Ze soustavy (6.25) je vidět, že souřadnice y_5 může nabývat hodnot $\pm A$. Hodnota $y_5 = A$, resp. $y_5 = -A$ potom určuje, zda bude objekt umístěn nad osou x , resp. pod osou x , procházející opěrnými body b_1 a b_2 . Každé hodnotě souřadnice y_5 potom odpovídají až dva reálné kořeny kvadratické rovnice pro hodnoty souřadnice y_4 z důvodů probraných podrobněji v příkladě 6.17. ■

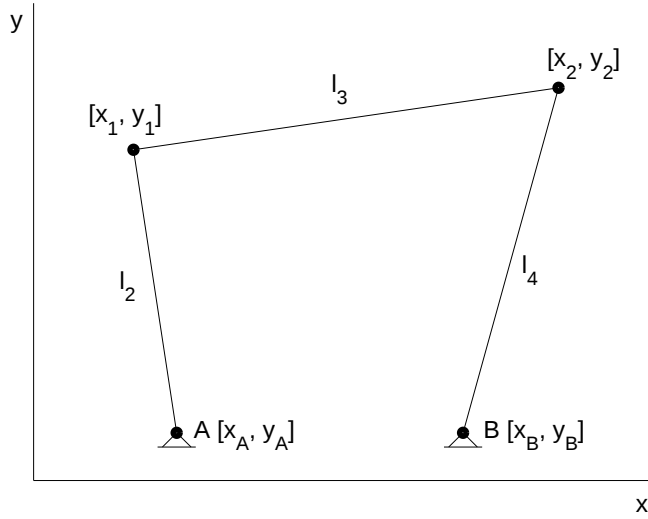
6.5 Robotika

Průmyslové roboty se v praxi užívají již od šedesátých let 20. století, a to většinou jako mechanické manipulátory. V poslední době nacházejí mnoho jiných uplatnění, např. jako letové simulátory, svařovací automaty, užívají se v lékařství, v kosmonautice, v televizní technice i jinde. Robotika jako vědní obor je velmi mladou disciplínou, která zasahuje do mnoha vědních oborů. Jedním z nich je i matematika, resp. geometrie, jejímž úkolem v robotice je popis pohybu robota a jeho interakce s vnějším prostředím (lokalizace překážek včetně vlastních částí robota). V současné době lze roboty rozdělit na:

1. *Roboty sériové*, u kterých se pohyb skládá z na sebe navazujících pohybů, přičemž jednotlivé části se mohou pohybovat nezávisle na sobě.
2. *Paralelní roboty (manipulátory)*, kde jednotlivé části robota jsou zařazeny vedle sebe a výsledný pohyb vzniká součinností všech částí, pohyb jedné části ovlivňuje polohu všech ostatních.
3. *Kombinované roboty*, které vznikají různými kombinacemi sériových a paralelních struktur, např. chodící stroje, mechanické ruky.

Z kinematického hlediska se robot skládá ze dvou mechanických soustav, pevné a hybné. Pevná soustava se nazývá báze a je pevně spojena s prostorem, ve kterém se pohyb odehrává. Hybná soustava je pevně spojena s nástrojem, případně s členem, pomocí kterého robot vykonává výsledný pohyb. Popis pohybu nástroje zprostředkovaného robotem je aplikací kinematiky a geometrie v robotice. Základní úlohy, které budou probrány podrobněji, jsou:

1. *Přímá úloha* - ze známé vzájemné polohy členů robota se hledá poloha nástroje robota nebo koncového členu (efektoru).



Obrázek 6.10: Klikový mechanismus

2. *Obrácená úloha (Inverzní kinematika)* - ze zadané polohy nástroje nebo koncového členu se hledá odpovídající „nastavení“ členů robota.

Závěr této části bude věnován příkladům užití Gröbnerovy báze ideálu pro řešení přímé i obrácené úlohy pro rovinné roboty.

Příklad 6.19 Řešení přímé úlohy bude provedeno pro případ klikového mechanismu, který je zobrazen na obr. 6.10. Klikový mechanismus lze popsat soustavou rovnic

$$\begin{aligned} (x_1 - x_A)^2 + (y_1 - y_A)^2 &= l_2^2, \\ (x_2 - x_1)^2 + (y_2 - y_1)^2 &= l_3^2, \\ (x_2 - x_B)^2 + (y_2 - y_B)^2 &= l_4^2. \end{aligned} \quad (6.26)$$

Bez újmy na obecnosti lze zvolit $x_A = 0$, $y_A = 0$ a $y_B = 0$, což dosazením do (6.26) vede k soustavě

$$\begin{aligned} x_1^2 + y_1^2 &= l_2^2, \\ (x_2 - x_1)^2 + (y_2 - y_1)^2 &= l_3^2, \\ (x_2 - x_B)^2 + y_2^2 &= l_4^2. \end{aligned} \quad (6.27)$$

Rovnice soustavy (6.27) lze chápat jako polynomy z $\mathbb{Q}(x_B, l_2, l_3, l_4)[x_1, y_1, x_2, y_2]$. V takovém případě ale hledání redukované Gröbnerovy báze pro ideál

$$I = \langle x_1^2 + y_1^2 - l_2^2, (x_2 - x_1)^2 + (y_2 - y_1)^2 - l_3^2, (x_2 - x_B)^2 + y_2^2 - l_4^2 \rangle$$

nedává dobré výsledky, jelikož soustava je tvořena 3 rovnicemi pro 4 neznámé x_1 , y_1 , x_2 , y_2 a nedojde k očekávané eliminaci proměnných x_1 , y_1 . Proto je výhodnější zvolit

jednu z proměnných jako parametr (např. x_2) a rovnice soustavy chápat jako polynomy z $\mathbb{Q}(x_B, l_2, l_3, l_4, x_2)[x_1, y_1, y_2]$. Redukovaná Gröbnerova báze pro ideál I vzhledem k **lex** uspořádání potom je

$$\begin{aligned} y_2^2 + (x_B - x_2)^2 - l_4^2 &= 0, \\ y_1^2 + f_1 y_1 y_2 + f_2 &= 0, \\ x_1 + \frac{1}{x_2} y_1 y_2 + f_3 &= 0, \end{aligned} \quad (6.28)$$

kde f_1, f_2, f_3 jsou složitější funkce parametrů x_B, l_2, l_3, l_4, x_2 . V závislosti na daných hodnotách parametrů x_B, l_2, l_3, l_4, x_2 lze ze soustavy (6.28) určit odpovídající hodnoty proměnných x_1, y_1, y_2 a najít tak jednu z možných poloh klikového mechanismu.

Ze soustavy (6.28) dále plyne, že musí být $x_2 \neq 0$, resp. $x_2 \neq \frac{x_B^2 - l_4^2}{2x_B}$. Tyto případy je třeba řešit samostatně.

Pro $x_2 = 0$ lze soustavu (6.27) přepsat do tvaru

$$\begin{aligned} x_1^2 + y_1^2 &= l_2^2, \\ x_1^2 + (y_2 - y_1)^2 &= l_3^2, \\ x_B^2 + y_2^2 &= l_4^2. \end{aligned} \quad (6.29)$$

Redukovaná Gröbnerova báze ideálu $J = \langle x_1^2 + y_1^2 - l_2^2, x_1^2 + (y_2 - y_1)^2 - l_3^2, x_B^2 + y_2^2 - l_4^2 \rangle$ potom je

$$\begin{aligned} y_2^2 - l_4^2 + x_B^2 &= 0, \\ 2y_1 - (l_2^2 - x_B^2 + l_4^2 - l_3^2)/(l_4^2 - x_B^2) &= 0, \\ 4x_1^2 + [(l_3 + l_2)^2 - l_4^2 + x_B^2][(l_3 - l_2)^2 - l_4^2 + x_B^2]/(l_4^2 - x_B^2) &= 0. \end{aligned} \quad (6.30)$$

Ze soustavy (6.30) je zřejmé, že musí být $l_4 \neq \pm x_B$. Příklad $l_4 = \pm x_B$ je třeba opět řešit samostatně. Soustavu (6.29) lze potom přepsat do tvaru

$$\begin{aligned} x_1^2 + y_1^2 &= l_2^2, \\ x_1^2 + (y_2 - y_1)^2 &= l_3^2, \\ y_2^2 &= 0, \end{aligned} \quad (6.31)$$

a tedy pro $l_2 = l_3$ má nekonečně mnoho řešení, pro $l_2 \neq l_3$ nemá řešení.

Pro $x_2 = \frac{x_B^2 - l_4^2}{2x_B}$ přejde soustava (6.27) do tvaru

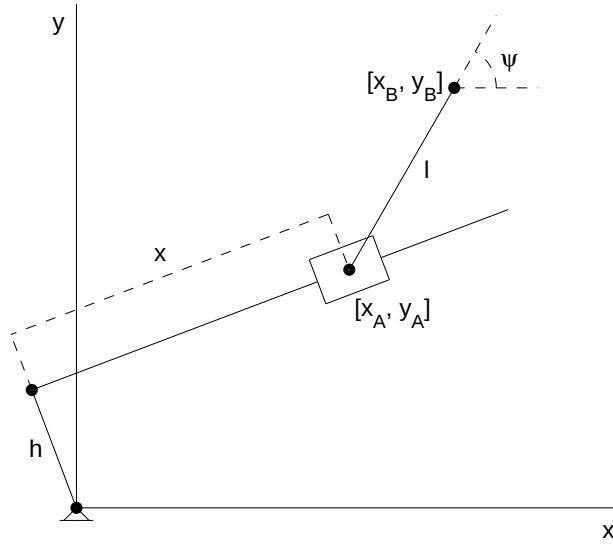
$$\begin{aligned} x_1^2 + y_1^2 &= l_2^2, \\ (x_B^2 - l_4^2 - 2x_B x_1)^2 + (y_2 - y_1)^2 &= l_3^2, \\ (x_B + l_4^2)^2 + y_2^2 &= l_4^2. \end{aligned} \quad (6.32)$$

Redukované Gröbnerova báze ideálu

$$J = \langle x_1^2 + y_1^2 - l_2^2, (x_B^2 - l_4^2 - 2x_B x_1)^2 + (y_2 - y_1)^2 - l_3^2, (x_B + l_4^2)^2 + y_2^2 - l_4^2 \rangle$$

potom je

$$\begin{aligned} y_2^2 + g_1 &= 0, \\ y_1 + g_2 y_2 &= 0, \\ x_1 + g_3 &= 0, \end{aligned} \quad (6.33)$$



Obrázek 6.11: Rovinný manipulátor

kde g_1 , g_2 a g_3 jsou složitější funkce parametrů x_B , l_2 , l_3 , l_4 . Z g_3 pak plyne, že nesmí být $l_2 = l_3$ a $x_B = l_4$. Pro $l_2 = l_3 \neq 0$ ale soustava (6.32) nemá řešení, pro $l_2 = l_3 = 0$ má jedno řešení. Pokud je $x_B = l_4$, potom má soustava (6.32) pro $l_2 = l_3$ nekonečně mnoho řešení, jinak řešení nemá.

Řešení soustavy (6.28) pro $x_2 \neq 0$ a $x_2 \neq (x_B^2 - l_4^2)/2x_B$, soustavy (6.30) pro $x_2 = 0$ a soustavy (6.33) pro $x_2 = (x_B^2 - l_4^2)/2x_B$ představují kompletní řešení přímé úlohy pro klikový mechanismus.

Například pro $l_2 = 6$, $l_3 = 9$, $l_4 = 7.5$, $x_B = 6$ a $x_2 = 11$ je určitě $x_2 \neq (x_B^2 - l_4^2)/2x_B$ i $x_2 \neq 0$. Řešení přímé úlohy

$$\begin{array}{ll} y_{21} &= 7.2284 & y_{22} &= -7.2284, \\ y_{11} &= 5.9312 & y_{12} &= -1.5009, \\ x_{11} &= -0.906 & x_{12} &= 5.8092 \end{array}$$

lze tedy najít řešením soustavy (6.28) a pro dané parametry představuje dvě možné polohy klikového mechanismu. ■

Příklad 6.20 Řešení problému inverzní kinematiky bude provedeno pro případ jednoduchého rovinného manipulátoru, zobrazeného na obr. 6.11. Tento rovinný manipulátor lze popsat soustavou rovnic

$$\begin{aligned} h^2 + x^2 &= x_A^2 + y_A^2, \\ (x_B - x_A)^2 + (y_B - y_A)^2 &= l^2, \\ \frac{y_B - y_A}{x_B - x_A} = \tan \psi &= k, \end{aligned} \tag{6.34}$$

kde jsou zadány souřadnice bodu B, tzn. x_B a y_B , a úhel ψ , resp. směrnice k . Rovnice soustavy (6.34) lze potom chápat jako polynomy z $\mathbb{Q}(x_B, y_B, k, h, l)[x, x_A, y_A]$. Redukovaná Gröbnerova báze pro ideál

$$I = \langle h^2 + x^2 - x_A^2 - y_A^2, (x_B - x_A)^2 + (y_B - y_A)^2 - l^2, y_B - y_A - k(x_B - x_A) \rangle,$$

generovaný rovnicemi soustavy (6.34), potom je

$$\begin{aligned} y_A^2 - 2y_B y_A + y_B^2 - \frac{l^2 k^2}{1+k^2} &= 0, \\ x_A - \frac{1}{k} y_A + \frac{y_B - k x_B}{k} &= 0, \\ x^2 - \frac{2(x_B + k y_B)}{k} y_A + \frac{h^2 k + 2x_B y_B - k x_B^2 + k y_B^2 - k l^2}{k} &= 0. \end{aligned} \quad (6.35)$$

Problémy při výpočtu x_A , y_A , x nastanou, jestliže $k = 0$. Tento případ je nutné řešit samostatně. Dosazení $k = 0$ do (6.34) vede k soustavě rovnic, jejíž redukovaná Gröbnerova báze je

$$\begin{aligned} y_A - y_B &= 0, \\ x_A^2 - 2x_B x_A + x_B^2 - l^2 &= 0, \\ x^2 - 2x_B x_A + x_B^2 - l^2 + h^2 - y_B^2 &= 0. \end{aligned} \quad (6.36)$$

Řešení soustavy (6.35) pro $k \neq 0$ a soustavy (6.36) pro $k = 0$ dávají kompletní řešení problému inverzní kinematiky pro daný rovinný manipulátor.

Například pro parametry $l = 5$, $h = 3$ a $x_B = 9$, $y_B = 10$, $\psi = \pi/3$ lze řešením soustavy (6.35) dostat hodnoty

$$\begin{array}{ll} y_{A_1} &= 14.3301 & y_{A_2} &= 5.6699, \\ x_{A_1} &= 11.5 & x_{A_2} &= 6.5, \\ x_1 &= 18.1274 & x_2 &= 8.0869. \end{array}$$

Existují tedy dvě možná nastavení parametrů daného rovinného manipulátoru pro zadanou polohu efektoru. ■

Kapitola 7

Rezultanty

Na rozdíl od teorie Gröbnerovýchází, existuje pouze velmi málo literatury, která je uceleně a přehledně věnována resultantům pro soustavy polynomiálních rovnic. Obvykle je věnována pouze jedna kapitola knihy resultantům pro polynomy v jedné proměnné, resp. eliminaci jedné proměnné ze soustavy nelineárních algebraických rovnic, jako je tomu např. v [3], [29], [32]. Tato kapitola tedy bude věnována zpracování přehledu základních typů resultantů, a to jak pro polynomy v jedné proměnné (Sylvesterův, Bézoutův resultant), tak ve více proměnných (resultanty Sylvesterova typu, Macaulayho, Dixonův, Dixonův dialytický resultant). Podrobnosti o dalších typech resultantů je možné najít např. v [24] nebo [9].

7.1 Resultanty pro polynomy v jedné proměnné

Začneme tedy s resultanty pro polynomy v jedné proměnné, později provedeme jejich zobecnění pro případ více proměnných. Pojem „resultantu“ se obvykle zavádí v souvislosti s hledáním podmínky pro existenci společného řešení výchozí soustavy polynomiálních rovnic.

Nechť $f, g \in k[x]$ jsou polynomy takové, že

$$\begin{aligned} f &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, & a_n &\neq 0, \\ g &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, & b_m &\neq 0. \end{aligned}$$

Pro tyto polynomy budeme chtít najít podmínku na koeficienty $a_i, b_j, i = 0, \dots, n, j = 0, \dots, m$, která zaručí existenci společného řešení polynomů f, g , nebo ekvivalentně řečeno podmínku existence společného faktoru polynomů f, g . Jinak řečeno, chceme vědět, kdy mají $f = 0, g = 0$ společný kořen.

Lemma 7.1.1 *Nechť $f, g \in k[x]$ jsou polynomy v jedné proměnné a $\deg(f) = n > 0, \deg(g) = m > 0$. Potom f a g mají společný faktor právě tehdy, když existují polynomy $A, B \in k[x]$ takové, že platí:*

1. A, B nejsou oba současně nulovými polynomy,

$$2. \deg(A) \leq m-1, \deg(B) \leq n-1,$$

$$3. Af + Bg = 0.$$

Důkaz: Viz [3]. □

Použijeme-li Lemma 7.1.1, můžeme odvodit metodu pro výpočet resultantu pro dva polynomy v jedné proměnné. Předpokládejme, že

$$\begin{aligned} A &= s_{m-1}x^{m-1} + s_{m-2}x^{m-2} + \cdots + s_1x + s_0, \\ B &= t_{n-1}x^{n-1} + t_{n-2}x^{n-2} + \cdots + t_1x + t_0. \end{aligned}$$

Dosazením do $Af + Bg = 0$ dostaneme polynom v proměnné x stupně $m+n$, který musí být nulový, aby polynomy f, g měly společný kořen (faktor). To znamená, že koeficienty u všech mocnin x musí být nulové, což vede na řešení soustavy lineárních algebraických rovnic pro neznámé $s_0, \dots, s_{m-1}, t_0, \dots, t_{n-1}$. Matice soustavy závisí na koeficientech vstupních polynomů $a_0, \dots, a_n, b_0, \dots, b_m$. Soustavu rovnic je možné zapsat ve tvaru:

$$\begin{aligned} s_0a_0 + t_0b_0 &= 0, \\ s_1a_0 + s_0a_1 + t_1b_0 + t_0b_1 &= 0, \\ &\vdots \\ s_{m-1}a_{n-1} + s_{m-2}a_n + t_{n-1}b_{m-1} + t_{n-2}b_m &= 0, \\ s_{m-1}a_n + t_{n-1}b_m &= 0, \end{aligned} \tag{7.1}$$

resp. v maticovém tvaru

$$\underbrace{\begin{bmatrix} a_0 & & & & & \\ a_1 & a_0 & & & & \\ a_2 & a_1 & \ddots & & & \\ \vdots & \vdots & & a_0 & \vdots & \vdots & b_0 \\ \vdots & \vdots & & a_1 & \vdots & \vdots & b_1 \\ a_n & \vdots & & \vdots & b_m & \vdots & \vdots \\ & a_n & & \vdots & b_m & \vdots & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_n & & & b_m \end{bmatrix}}_m \underbrace{\begin{bmatrix} b_0 & b_0 & & & & \\ b_1 & b_1 & & & & \\ b_2 & b_1 & \ddots & & & \\ \vdots & \vdots & & \vdots & \vdots & b_0 \\ \vdots & \vdots & & \vdots & \vdots & b_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ t_{n-2} & & & & & \vdots \\ t_{n-1} & & & & & \vdots \end{bmatrix}}_n \cdot \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{m-2} \\ s_{m-1} \\ t_0 \\ t_1 \\ \vdots \\ t_{n-2} \\ t_{n-1} \end{bmatrix} = \mathbf{O}.$$

Soustava rovnic (7.1) je homogenní soustavou, která má netriviální řešení tehdy a jen tehdy, když determinant matice soustavy je nulový. Odtud potom plyne, že determinant matice soustavy (7.1) představuje hledanou podmínku na koeficienty $a_i, b_j, i = 0, \dots, n, j = 0, \dots, m$, za které má soustava polynomiálních rovnic $f = 0, g = 0$ společné řešení. Obecně se tato podmínka nazývá *resultant pro soustavu polynomiálních rovnic*. Matice soustavy (7.1) je řádu $n+m$ a obvykle se nazývá *Sylvesterovou maticí* a determinant Sylvesterovy matice se nazývá *Sylvesterovým resultantem*.

Definice 7.1.1 *Nechť $f, g \in k[x]$ jsou polynomy v jedné proměnné. Rezultant $\text{Res}(f, g)$ je polynom v koeficientech polynomů f a g , který nabývá nulové hodnoty tehdy a jen tehdy, když f a g mají společný faktor.*

Poznamenejme, že stupeň rezultantu v koeficientech a_i polynomu f je roven m , tzn. $\deg_f(\text{Res}(f, g)) = m$, podobně potom $\deg_g(\text{Res}(f, g)) = n$. Celkový stupeň rezultantu tedy je $n + m$.

7.1.1 Sylvesterův rezultant, dialytická metoda

Sylvesterův rezultant pro polynomy v jedné proměnné patří mezi základní a velmi dobře známé rezultanty. Většina CAS (Computer Algebra System) softwarů obsahuje funkce pro výpočet právě Sylvesterova rezultantu. Jiným způsobem pro sestavení Sylvesterovy matice, než jsme ukázali v předchozí části, je tzv. *dialytická metoda*.

Uvažujme dvě množiny monomů

$$\mathbf{X} = \{x^{m-1}, x^{m-2}, \dots, x, 1\}, \quad \mathbf{Y} = \{x^{n-1}, x^{n-2}, \dots, x, 1\}.$$

Vynásobením polynomu f prvky množiny $\mathbf{X}$ a polynomu g prvky množiny $\mathbf{Y}$ dostaneme odpovídající polynomiální množiny $\mathbf{X}f$ a $\mathbf{Y}g$, které obsahují dohromady $n + m$ polynomů a je možné je vyjádřit maticově následujícím způsobem

$$\begin{bmatrix} x^{m-1}f \\ \vdots \\ xf \\ f \\ x^{n-1}g \\ \vdots \\ xg \\ g \end{bmatrix} = \underbrace{\begin{bmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_1 & a_0 & & \\ & & \ddots & & & & \ddots & \\ & & & a_n & \dots & & & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & b_m & \dots & & & b_0 \end{bmatrix}}_{\text{Syl}(f,g)} \begin{bmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{bmatrix}, \quad (7.2)$$

kde matice koeficientů je opět Sylvesterovou maticí. Monomiální množiny $\mathbf{X}$ a $\mathbf{Y}$ se obvykle nazývají *množinami násobitelů*, matice rezultantů zkonstruované pomocí množin násobitelů se nazývají *dialytické matice* a metoda sestavení matice rezultantu pomocí množin násobitelů se nazývá *dialytická metoda*.

Pro polynomy z $k[x_1, \dots, x_n]$, $n > 1$, existuje několik metod, které se liší právě volbou množin násobitelů (zobecnění Sylvesterova rezultantu pro tři polynomy ve dvou proměnných, Macaulayho rezultant, řídký rezultant, Dixonův dialytický rezultant). Každá z těchto metod potom dává kvalitativně odlišné výsledky – liší se velikost odpovídajících matic rezultantu, počet extra faktorů, které obsahuje determinant matice rezultantu apod. Některé z těchto rezultantů pro polynomy ve více proměnných budou podrobněji popsány v části 7.2.

Příklad 7.1 Mějme dva polynomy $f = x^2y - 1$ a $g = x^2 + y^2 + xy - 4$ a berme je jako polynomy v proměnné x s koeficienty, které závisí na proměnné y . Potom Sylvesterovu matici pro dané polynomy f a g je možné najít pomocí vztahu (7.2). Platí tedy

$$\begin{bmatrix} xf \\ f \\ xg \\ g \end{bmatrix} = \underbrace{\begin{bmatrix} y & 0 & -1 & 0 \\ 0 & y & 0 & -1 \\ 1 & y & y^2 - 4 & 0 \\ 0 & 1 & y & y^2 - 4 \end{bmatrix}}_{\text{Syl}(f,g)} \begin{bmatrix} x^3 \\ x^2 \\ x \\ 1 \end{bmatrix}$$

a Sylvesterův resultant je $\det(\text{Syl}(f, g)) = y^6 - 8y^4 + y^3 + 16y^2 - 8y + 1$. Na tomto příkladě je možné demonstrovat vztah mezi resultanty a Gröbnerovými bázemi. Jestliže najdeme Gröbnerovu bázi pro ideal $I = \langle f, g \rangle$ vzhledem k **lex** uspořádání pro $x > y$, dostaneme

$$I = \langle x - 4y^5 - y^4 + 32y^3 + 4y^2 - 64y + 16, y^6 - 8y^4 + y^3 + 16y^2 - 8y + 1 \rangle.$$

Generátorem prvního eliminačního ideálu $I_1 = I \cap \mathbb{C}[y]$ je tedy přesně polynom $y^6 - 8y^4 + y^3 + 16y^2 - 8y + 1$, který jsme získali jako resultant pro polynomiální soustavu $f = 0, g = 0$. ■

7.1.2 Bézoutův resultant

Naprosto odlišný způsob sestavení matice resultantu pro polynomy v jedné proměnné představil v roce 1779 Bézout. Později jeho metodu přepracoval Cayley a zavedl jiný způsob sestavení Bézoutovy matice, který bude uveden v následujících odstavcích.

Zatímco prvky Sylvesterovy matice jsou přímo koeficienty výchozích polynomů, prvky Bézoutovy matice jsou *polynomy* v koeficientech výchozích polynomů. Bez újmy na obecnosti, nechť $f, g \in k[x]$ jsou polynomy

$$\begin{aligned} f &= a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, & a_n &\neq 0, \\ g &= b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0, & b_m &\neq 0, \end{aligned}$$

a $m = \deg(g) \leq \deg(f) = n$.

Nechť s je nově přidaná proměnná. Uvažujme funkci polynomů f a g ve tvaru

$$\Delta(t, s) = \frac{\begin{vmatrix} f(t) & f(s) \\ g(t) & g(s) \end{vmatrix}}{s - t}. \quad (7.3)$$

Je zřejmé, že $\Delta(t, s)$ je polynom stupně $n - 1$ v proměnné s , kde koeficienty jsou polynomy stupně $n - 1$ v proměnné t .

Dělení v rovnici (7.3) je možné provést pomocí následujícího obecnějšího postupu. Potřebujeme vydělit polynom $f(x, y)$, který nabývá nulové hodnoty pro $x = y$, polynomem $x - y$. Na polynom $f(x, y)$ je možné nahlížet jako na polynom v jedné proměnné x , kde

koefficienty jsou polynomy v proměnné y . Dále se využije vyjádření podílu $1/(x - y)$ ve tvaru mocniné řady, tj.

$$\frac{1}{x - y} = \sum_{u=1}^{\infty} x^{-u} y^{u-1}.$$

Potom

$$\frac{\sum_{i=0}^n a_i(y) x^i}{x - y} = \sum_{i=0}^n a_i(y) x^i \sum_{u=1}^{\infty} x^{-u} y^{u-1} = \sum_{i=0}^n a_i(y) x^i \left(\sum_{u=1}^i x^{-u} y^{u-1} + \sum_{u=i+1}^{\infty} x^{-u} y^{u-1} \right).$$

Jelikož druhá suma na pravé straně obsahuje záporné mocniny x , výsledek dělení je polynomem pouze v případě, že je tato suma nulová. Tedy

$$\frac{\sum_{i=0}^n a_i(y) x^i}{x - y} = \sum_{i=1}^n a_i(y) x^i \sum_{k=0}^i x^k y^{i-1-k}. \quad (7.4)$$

Nyní je možné použít vztah (7.4) a přepsat (7.3) do tvaru

$$\begin{aligned} \Delta(t, s) &= f(t) \frac{g(t) - g(s)}{t - s} - g(t) \frac{f(t) - f(s)}{t - s} = \\ &= \sum_{k=0}^{m-1} \left(f(t) \sum_{i=k+1}^m b_i t^{i-k-1} - g(t) \sum_{i=k+1}^n a_i t^{i-k-1} \right) s^k - \sum_{k=m}^{n-1} \left(g(t) \sum_{i=k+1}^n a_i t^{i-k-1} \right) s^k. \end{aligned} \quad (7.5)$$

Samozřejmě je možné zapsat vztah (7.3) také v maticové formě

$$\Delta(t, s) = [1 \ s \ \dots \ s^{n-1}] \cdot \mathbf{D} \cdot \begin{bmatrix} 1 \\ t \\ \vdots \\ t^{n-1} \end{bmatrix}. \quad (7.6)$$

Potom srovnáním vztahů (7.5) a (7.6) je zřejmé, že koefficienty u mocnin $s^i, i = 0, \dots, n-1$, ve vztahu (7.5) je možné vyjádřit opět maticově

$$\begin{bmatrix} f \sum_{i=1}^m b_i t^{i-1} - g \sum_{i=1}^n a_i t^{i-1} \\ \vdots \\ f b_m - g \sum_{i=m}^n a_i t^{i-m} \\ -g \sum_{i=m+1}^n a_i t^{i-m-1} \\ \vdots \\ -g a_n \end{bmatrix} = \underbrace{\begin{bmatrix} c_{00} & \dots & c_{0,n-1} \\ \vdots & \ddots & \vdots \\ c_{n-1,0} & \dots & c_{n-1,n-1} \end{bmatrix}}_{\mathbf{D}} \begin{bmatrix} 1 \\ t \\ \vdots \\ t^{n-1} \end{bmatrix}, \quad (7.7)$$

kde

$$c_{ij} = \sum_{\substack{k \leq \min(i,j), \\ k+h=i+j+1}} (a_k b_h - a_h b_k) \quad (7.8)$$

a $b_{m+1} = \dots = b_n = 0$. Matice $\mathbf{D}$ je řádu n , nazývá se *Bézoutovou maticí* a obvykle se značí $\mathbf{Bez}(f, g)$. Determinant Bézoutovy matice vždy obsahuje rezultant jako jeden ze svých faktorů.

Je zřejmé, že konstrukce Bézoutovy matice je složitější a tedy časově náročnější než konstrukce Sylvesterovy matice, jelikož prvky Bézoutovy matice nejsou přímo koeficienty vstupních polynomů ale opět polynomy v koeficientech vstupních polynomů (v podstatě se jedná opět o determinanty určitých matic). Na druhou stranu, Bézoutova matice je výrazně menší než Sylvesterova matice – pro $n = m$ je Bézoutova matice rozměru $n \times n$ a Sylvesterova matice rozměru $2n \times 2n$. Výpočet determinantu Bézoutovy matice (a samotného rezultantu) může být tedy výrazně rychlejší.

Podívejme se nyní podrobněji na odvození vztahu (7.8) pro prvky Bézoutovy matice. Toto odvození je založeno na sestavení speciální transformační matice $\mathbf{R}$, která transformuje Sylvesterovu matici na Bézoutovu matici. Vyjděme opět ze vztahu (7.5), který je možné přepsat maticově do tvaru

$$\begin{aligned} \Delta(t, s) &= [f \ tf \ \dots \ t^{m-1}f \ g \ tg \ \dots \ t^{n-1}g] \underbrace{\begin{bmatrix} b_1 & b_2 & \dots & b_m \\ b_2 & \vdots & & \\ \vdots & b_m & & \\ b_m & & & \\ -a_1 & -a_2 & \dots & -a_n \\ -a_2 & \vdots & & \\ \vdots & -a_n & & \\ -a_n & & & \end{bmatrix}}_{\mathbf{R}} \begin{bmatrix} 1 \\ s \\ \vdots \\ s^{n-1} \end{bmatrix} = \\ &= [1 \ t \ \dots \ t^{n+m-1}] \cdot \underbrace{\begin{bmatrix} a_0 & & & b_0 \\ a_1 & \ddots & & b_1 & \ddots \\ \vdots & & a_0 & \vdots & b_0 \\ a_n & & a_1 & b_m & b_1 \\ & \ddots & \vdots & \ddots & \vdots \\ & & a_n & & b_m \end{bmatrix}}_{\mathbf{Syl}(f,g)} \cdot \mathbf{R} \cdot \begin{bmatrix} 1 \\ s \\ \vdots \\ s^{n-1} \end{bmatrix}. \end{aligned} \quad (7.9)$$

Dále je nutné upravit vztah (7.6) tak, abychom jej mohli jednoduše srovnat se vztahem (7.9) – rozšíříme tedy vektor $[1, t, \dots, t^n]$ až do mocniny $n + m - 1$ a současně upravíme

Bézoutovu matici přidáním nulových řádků. Tedy (7.6) přepíšeme do tvaru

$$\Delta(t, s) = [1 \ \dots \ t^{n-1} \ t^n \ \dots \ t^{n+m-1}] \begin{bmatrix} \mathbf{Bez}(f, g) \\ \mathbf{O}_{m \times n} \end{bmatrix} \begin{bmatrix} 1 \\ \vdots \\ s^{n-1} \end{bmatrix}. \quad (7.10)$$

Ze srovnání (7.9) a (7.10) už poté přímo plyne, že

$$\begin{bmatrix} \mathbf{Bez}(f, g) \\ \mathbf{O}_{m \times n} \end{bmatrix} = \mathbf{Syl}(f, g) \cdot \mathbf{R}. \quad (7.11)$$

Z (7.11) přímo plyne vztah (7.8) pro prvky Bézoutovy matice a také poskytuje jednu z možností jak zkonstruovat Bézoutovu matici pomocí maticového násobení.

Příklad 7.2 Uvažujme polynomy $f = x^2y - 1$ a $g = x^2 + y^2 + xy - 4$ jako polynomy v proměnné x s koeficienty, které závisí na proměnné y . Z rovnice (7.7), resp. z (7.11), potom plyne

$$\mathbf{Bez}(f, g) = \begin{bmatrix} -y & -y^3 + 4y - 1 \\ -y^3 + 4y - 1 & -y^2 \end{bmatrix},$$

resp.

$$\begin{aligned} \begin{bmatrix} \mathbf{Bez}(f, g) \\ \mathbf{O}_{2 \times 2} \end{bmatrix} &= \begin{bmatrix} -1 & 0 & y^2 - 4 & 0 \\ 0 & -1 & y & y^2 - 4 \\ y & 0 & 1 & y \\ 0 & y & 0 & 1 \end{bmatrix} \begin{bmatrix} y & 1 \\ 1 & 0 \\ 0 & -y \\ -y & 0 \end{bmatrix} = \\ &= \begin{bmatrix} -y & -y^3 + 4y - 1 \\ -y^3 + 4y - 1 & -y^2 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \end{aligned}$$

a tedy $\det(\mathbf{Bez}(f, g)) = -y^6 + 8y^4 - y^3 - 16y^2 + 8y - 1$. Dostáváme tedy stejný výsledek jako v případě Sylvesterova rezultantu (až na násobení číslem -1). ■

7.2 Rezultanty pro polynomy ve více proměnných

Stejně jako v případě rezultantů pro polynomy v jedné proměnné i rezultanty pro polynomy ve více proměnných poskytují podmínku pro existenci společného řešení soustavy polynomiálních rovnic $f_1 = 0, \dots, f_n = 0$ ve tvaru polynomu v koeficientech vstupních polynomů.

Velkou výhodou rezultantů pro polynomy ve více proměnných ve srovnání s metodou Gröbnerovýchází je, že eliminují n proměnných z $n + 1$ rovnic současně, a ne postupně jednu po druhé jako Gröbnerovy báze. Proto jsou rezultanty obvykle výpočetně rychlejší, alespoň pokud používáme klasické algoritmy pro obě metody. Avšak moderní algoritmy

pro výpočet Gröbnerovýchází se snaží poměrně úspěšně eliminovat tuto nevýhodu (viz např. [28],[5]).

Na druhé straně i rezultanty mají své nevýhody. Jednou z nich je, že obecně všechny formulace rezultantů pro polynomy ve více proměnných produkují tzv. *extra factory*. To znamená, že determinant matice rezultantu není obecně přímo rezultat, ale tzv. *projekční operátor*, který se skládá z rezultantu a dalších faktorů (extra faktorů), které do rezultantu nepatří a nesouvisí s ním. Je tedy ještě nutné eliminovat tyto extra faktory, což pochopitelně stojí další výpočetní čas.

Tato část je věnována několika formulacím rezultantů pro polynomy ve více proměnných. Nejprve provedeme zobecnění Sylvesterovy (dialytické) matice pro tři polynomy ve dvou proměnných – zobecnění pro více než dvě proměnné se obvykle neprovádí. Jako alternativa slouží tzv. Macaulayho matice, které je jednou z matic Sylvesterova typu (tzn. že prvky v matici jsou přímo koeficienty vstupních polynomů), konstruuje se pro obecný případ $n + 1$ polynomů v n proměnných také s využitím dialytické metody. Dále bude uvedeno zobecnění Bézoutovy matice pro polynomy v jedné proměnné, tzv. Dixonova matice pro polynomy ve více proměnných – nejprve pro speciální případ tří polynomů ve dvou proměnných z důvodu zajímavého vztahu k Sylvesterově matici, a poté pro obecný případ $n + 1$ polynomů v n proměnných. Na závěr bude uvedena jedna z nových formulací matice rezultantu, tzv. Dixonova dialytická matice. Jak název napovídá, jedná se o kombinaci obou zmíněných přístupů, jak dialytické, tak Bézoutovy (Dixonovy) metody. Nejprve se ale podíváme podrobněji na vztah „rezultantu“ a „projekčního operátoru“.

7.2.1 Rezultant a projekční operátor

Netriviální násobek rezultantu, který obvykle získáme jako determinant matice rezultantu, se nazývá *projekční operátor*.

Nechť $F = \{f_1, \dots, f_n\} \subset k[x_1, \dots, x_n]$, kde $f_i = \sum_{\alpha \in \mathcal{A}} c_{i,\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \sum_{\alpha \in \mathcal{A}} c_{i,\alpha} x^\alpha$ je n -tice polynomů představující soustavu polynomiálních rovnic. Při použití libovolné z metod konstrukce matice rezultantu na polynomiální soustavu F v podstatě sestrojíme jinou soustavu polynomiálních rovnic, kterou můžeme zapsat ve tvaru $F' = \mathbf{M}_{F'} \cdot \mathbf{X} = 0$, kde $\mathbf{X}$ obsahuje všechny monomy vyskytující se v polynomech F' . Dostáváme tak homogenní soustavu lineárních rovnic, která může mít netriviální řešení pouze v případě, že hodnost matice $\mathbf{M}_{F'}$ je menší než počet sloupců matice $\mathbf{M}_{F'}$. Jelikož předpokládáme, že koeficienty $c_{i,\alpha}$ jsou obecně symbolické, chceme najít podmínku na tyto symbolické koeficienty, jejíž splnění zaručuje existenci řešení soustavy F . V případě, že je hodnost $\mathbf{M}_{F'}$ rovna počtu sloupců $\mathbf{M}_{F'}$, determinant $\mathbf{M}_{F'}$ poskytuje právě tuto podmínku.

Avšak v obecném případě nemusí být matice (a velice často také není) čtvercovou maticí nebo je determinant matice rezultantu identicky roven nule, ačkoliv matice rezultantu závisí na parametrech. V takovém případě je výhodné použít tzv. *metodu RSC* pro extrakci projekčního operátoru z matice rezultantu. O této metodě hovoří následující věta.

Věta 7.2.1 (RSC, Rank Submatrix Construction) *Nechť F je soustava polynomiálních rovnic s parametry a nechť $\mathbf{M}_{F'}$ je matice rezultantu rozměru $m \times n$. Jestliže $\mathbf{C}_i$ je lineárně*

nezávislý sloupec matice $\mathbf{M}_{F'}$, odpovídající monomu x^α , a $\mathbf{Q}$ je libovolný maximální minor matice $\mathbf{M}_{F'}$, potom $\det(\mathbf{Q})$ je nějaký násobek rezultantu, který představuje podmínku pro existenci řešení ε soustavy F splňující podmínku $\varepsilon^\alpha \neq 0$.

Důkaz: See [9]. □

Jak vyplývá z Věty 7.2.1, projekční operátor je možné získat jako determinant libovolného maximálního minoru matice rezultantu. Je také dobré se uvědomit, že Věta 7.2.1 nepředpokládá žádnou speciální formulaci matice rezultantu a je tedy možné ji použít pro výpočet projekčního operátoru z libovolné matice rezultantu.

Pokud najdeme projekční operátor, dalším krokem je nalezení rezultantu, resp. identifikace extra faktorů, v tomto projekčním operátoru. Prvním krokem tedy obvykle bývá faktorizace projekčního operátoru. Poté je nutné pro každý faktor rozhodnout, zda patří do rezultantu nebo nikoliv na základě určité speciální podmínky, která vyplývá z dané řešení úlohy. Například, pokud hledáme implicitní vyjádření plochy zadané racionální parametrizací, je možné použít rezultanty pro eliminaci parametrů z dané parametrizace. Nicméně, často dostaneme více než jen implicitní vyjádření. Proto provedeme faktorizaci získaného projekčního operátoru a do každého faktoru dosadíme danou parametrizaci plochy. Faktory, které se po dosažení vynulují, tvoří implicitní vyjádření dané plochy.

7.2.2 Sylvesterův rezultant pro polynomy ve dvou proměnných

Sylvesterovu matici pro tři polynomy ve dvou proměnných je možné získat přímým zobecněním metody konstrukce Sylvesterovy matice pro dva polynomy v jedné proměnné. Necht

$$f(s, t) = \sum_{i=0}^m \sum_{j=0}^n a_{i,j} s^i t^j, \quad g(s, t) = \sum_{i=0}^m \sum_{j=0}^n b_{i,j} s^i t^j, \quad h(s, t) = \sum_{i=0}^m \sum_{j=0}^n c_{i,j} s^i t^j \quad (7.12)$$

jsou tři polynomy v proměnných s a t . Analogicky jako v případě jedné proměnné je možné zavést množinu polynomů

$$\{s^\sigma t^\tau f, s^\sigma t^\tau g, s^\sigma t^\tau h \mid \sigma = 0, \dots, 2m-1, \tau = 0, \dots, n-1\}. \quad (7.13)$$

Potom *Sylvesterova matice* opět obsahuje pouze koeficienty vstupních polynomů f , g a h a lze ji zapsat ve tvaru

$$\begin{aligned} & [f \ g \ h \ t(f \ g \ h) \ \dots \ t^{n-1}(f \ g \ h) \ s(f \ g \ h) \ st(f \ g \ h) \ \dots \ st^{n-1}(f \ g \ h) \ \dots \\ & \quad \dots \ s^{2m-1}(f \ g \ h) \ s^{2m-1}t(f \ g \ h) \ \dots \ s^{2m-1}t^{n-1}(f \ g \ h)] = \\ & = [1 \ t \ \dots \ t^{2n-1} \ s \ st \ \dots \ st^{2n-1} \ \dots \ s^{3m-1} \ s^{3m-1}t \ \dots \ s^{3m-1}t^{2n-1}] \cdot \mathbf{Syl}(f, g, h), \end{aligned} \quad (7.14)$$

kde je použito lexikografické uspořádání monomů pro $s > t$, tj. $1, t, \dots, t^{2n-1}, \dots, s^k, \dots, s^k t^{2n-1}, \dots, s^{3m-1}, \dots, s^{3m-1} t^{2n-1}$. Matice $\mathbf{Syl}(f, g, h)$ je řádu $6mn$ a determinant Sylvesterovy matice je *Sylvesterův rezultant*.

Na rozdíl od Sylvesterovy matice pro polynomy v jedné proměnné je zde použito jiné uspořádání polynomů f , g a h a jejich násobků na levé straně (7.14). Důvodem je, že

při použití tohoto uspořádání má Sylvesterova matice speciální, blokově diagonální strukturu, která může být výhodná při výpočtu determinantu matice. Pokud bychom zachovali uspořádání jako v případě jedné proměnné, byla by Sylvesterova matice pouze řídkou maticí bez další speciální vnitřní struktury. Samozřejmě je možné stejným způsobem modifikovat i definici Sylvesterovy matice pro polynomy v jedné proměnné a obě definice jsou ekvivalentní.

Sestavení Sylvesterovy matice pro polynomy ve dvou proměnných se tedy mírně liší od způsobu uvedeného pro Sylvesterovu matici pro polynomy v jedné proměnné. Každý sloupec opět obsahuje koeficienty polynomů f , g , h nebo jejich násobků z množiny (7.13). Pokud je polynom f (nebo g nebo h) vynásoben t , koeficienty f se posunou o jeden řádek dolů v příslušném sloupci (stejně jako v případě jedné proměnné). Pokud je polynom f (nebo g nebo h) vynásoben s , koeficienty f se posunou o $2n$ řádků dolů v příslušném sloupci. To nám dává zmíněnou blokovou strukturu Sylvesterovy matice. Nechť

$$f_i(t) = \sum_{j=0}^n a_{i,j} t^j, \quad g_i(t) = \sum_{j=0}^n b_{i,j} t^j, \quad h_i(t) = \sum_{j=0}^n c_{i,j} t^j \quad (7.15)$$

a nechť $\mathbf{S}_i$ je matice rozměru $2n \times 3n$ daná vztahem

$$[f_i \ g_i \ h_i \ t(f_i \ g_i \ h_i) \ \dots \ t^{n-1}(f_i \ g_i \ h_i)] = [1 \ \dots \ t^{2n-1}] \mathbf{S}_i, \quad (7.16)$$

kde

$$\mathbf{S}_i = \begin{bmatrix} a_{i,0} & b_{i,0} & c_{i,0} & & & & \\ \vdots & \vdots & \vdots & \ddots & & & \\ a_{i,n-1} & b_{i,n-1} & c_{i,n-1} & \ddots & a_{i,0} & b_{i,0} & c_{i,0} \\ a_{i,n} & b_{i,n} & c_{i,n} & \ddots & a_{i,1} & b_{i,1} & c_{i,1} \\ & & & \ddots & \vdots & \vdots & \vdots \\ & & & & a_{i,n} & b_{i,n} & c_{i,n} \end{bmatrix}.$$

Srovnáním (7.14) a (7.16) dostáváme blokovou strukturu Sylvesterovy matice ve tvaru

$$\mathbf{Syl}(f, g, h) = \begin{bmatrix} \mathbf{S}_0 & & & & & & \\ \vdots & \ddots & & & & & \\ \mathbf{S}_{m-1} & & \mathbf{S}_0 & & & & \\ \mathbf{S}_m & & \mathbf{S}_1 & \mathbf{S}_0 & & & \\ & \ddots & \vdots & \vdots & \ddots & & \\ & & \mathbf{S}_m & \mathbf{S}_{m-1} & & \mathbf{S}_0 & \\ & & & \mathbf{S}_m & & \mathbf{S}_1 & \\ & & & & \ddots & \vdots & \\ & & & & & \mathbf{S}_m \end{bmatrix}.$$

Na závěr této části si předvedeme sestavení Sylvesterovy matice na jednoduchém příkladě.

Příklad 7.3 Necht plocha S je dána parametrizací

$$x(s, t) = \frac{st + 1}{s + t + 1}, \quad y(s, t) = \frac{s}{s + t + 1}, \quad z(s, t) = \frac{t}{s + t + 1}. \quad (7.17)$$

Odstraněním jmenovatelů a při použití lexikografického uspořádání monomů pro $s > t > x > y > z$ dostáváme soustavu polynomiálních rovnic

$$\begin{aligned} -st + xs + xt + x - 1 &= 0, \\ (y - 1)s + yt + y &= 0, \\ zs + (z - 1)t + z &= 0. \end{aligned} \quad (7.18)$$

Polynomy (7.18) jsou stupně 1 v obou proměnných s a t . Množina monomů (7.13) je tedy v tomto případě $\{s^\sigma t^\tau f, s^\sigma t^\tau g, s^\sigma t^\tau h \mid \sigma = 0, 1, \tau = 0\}$. Z (7.14) potom plyne

$$[f \ g \ h \ sf \ sg \ sh] = [1 \ t \ s \ st \ s^2 \ s^2 t] \cdot \underbrace{\begin{bmatrix} x-1 & y & z & 0 & 0 & 0 \\ x & y & z-1 & 0 & 0 & 0 \\ x & y-1 & z & x-1 & y & z \\ -1 & 0 & 0 & x & y & z-1 \\ 0 & 0 & 0 & x & y-1 & z \\ 0 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}}_{\text{Syl}(f,g,h)}$$

a

$$\det(\text{Syl}(f, g, h)) = xy + xz - x + y^2 + 3yz - 2y + z^2 - 2z + 1$$

je implicitním vyjádřením plochy dané parametrizací (7.17).

Pro ověření, že získaný výsledek je skutečně rezultantem a tedy i implicitním vyjádřením dané plochy je možné využít Gröbnerovy báze. Redukovaná Gröbnerova báze pro ideál generovaný polynomy (7.18) vzhledem k lexikografickému uspořádání pro $s > t > x > y > z$ je

$$\begin{aligned} &\langle xy + xz - x + y^2 + 3yz - 2y + z^2 - 2z + 1, \\ &tz - t + x + y + 2z - 1, \\ &ty - x - y - z + 1, \\ &sz - x - y - z + 1, \\ &sy - s + x + 2y + z - 1, \\ &st - sx - tx - x + 1 \rangle. \end{aligned}$$

Je zřejmé, že generátor druhého eliminačního ideálu $I_2 = I \cap \mathbb{C}[x, y, z]$ je stejný jako vypočtený $\det(\text{Syl}(f, g, h))$. ■

7.2.3 Dixonův rezultant pro polynomy ve dvou proměnných

Konstrukce Bézoutovy matice pro dva polynomy v jedné proměnné je možné zobecnit pro tři polynomy ve dvou proměnných. Jako první toto zobecnění provedl Dixon v roce 1908.

Opět analogicky jako v případě polynomů v jedné proměnné, pro polynomy f, g a h (definované v (7.12)) je možné zavést funkci

$$\Delta(s, t, \bar{s}, \bar{t}) = \frac{\begin{vmatrix} f(s, t) & g(s, t) & h(s, t) \\ f(\bar{s}, t) & g(\bar{s}, t) & h(\bar{s}, t) \\ f(\bar{s}, \bar{t}) & g(\bar{s}, \bar{t}) & h(\bar{s}, \bar{t}) \end{vmatrix}}{(\bar{s} - s)(\bar{t} - t)}. \quad (7.19)$$

Je zřejmé, že čítec $\Delta(s, t, \bar{s}, \bar{t})$ nabývá nulové hodnoty pro $s = \bar{s}$ a $t = \bar{t}$. Odtud přímo plyne, že čítec $\Delta(s, t, \bar{s}, \bar{t})$ je beze zbytku dělitelný polynomem $(s - \bar{s})(t - \bar{t})$ a tedy že $\Delta(s, t, \bar{s}, \bar{t})$ je polynom v proměnných $s, \bar{s}, t, \bar{t}$. Polynom $\Delta(s, t, \bar{s}, \bar{t})$ se nazývá *Dixonův polynom* a je možné jej přepsat do tvaru

$$\Delta(s, t, \bar{s}, \bar{t}) = [1 \dots t^{2n-1} s \dots st^{2n-1} \dots s^{m-1} \dots s^{m-1}t^{2n-1}] \cdot \mathbf{Dix}(f, g, h) \cdot \begin{bmatrix} 1 \\ \vdots \\ \bar{t}^{n-1} \\ \vdots \\ \bar{s}^{2m-1} \\ \vdots \\ \bar{s}^{2m-1}\bar{t}^{n-1} \end{bmatrix}, \quad (7.20)$$

kde $\mathbf{Dix}(f, g, h)$ je čtvercová matice řádu $2mn$, která se nazývá *Dixonova matice* a její determinant se nazývá *Dixonův rezultant*.

Podobně jako v případě polynomů v jedné proměnné je možné odvodit transformační vztah, který převede Sylvesterovu matici pro polynomy ve dvou proměnných na Dixonovu matici pouze násobením speciální transformační maticí (více viz [8]). Vztah (7.19) je možné přepsat do tvaru

$$\begin{aligned} \Delta(s, t, \bar{s}, \bar{t}) = & \sum_{i=0}^m \sum_{j=0}^m \left(\sum_{u=0}^{i+j-1} s^{i+j-1-u} \cdot \bar{s}^u \cdot f(s, t) \cdot \frac{g_i(t)h_j(\bar{t}) - g_i(\bar{t})h_j(t)}{\bar{t} - t} + \right. \\ & + \sum_{u=0}^{i+j-1} s^{i+j-1-u} \cdot \bar{s}^u \cdot g(s, t) \cdot \frac{h_i(t)f_j(\bar{t}) - h_i(\bar{t})f_j(t)}{\bar{t} - t} + \\ & \left. + \sum_{u=0}^{i+j-1} s^{i+j-1-u} \cdot \bar{s}^u \cdot h(s, t) \cdot \frac{f_i(t)g_j(\bar{t}) - f_i(\bar{t})g_j(t)}{\bar{t} - t} \right). \end{aligned} \quad (7.21)$$

Polynom $\Delta(s, t, \bar{s}, \bar{t})$ je možné chápat jako polynom v proměnných $\bar{s}, \bar{t}$ s koeficienty, které závisí na s, t . Označíme-li tyto koeficienty $p_{u,0}, \dots, p_{u,n-1}$, $u = 0, \dots, 2m-1$, potom platí

$$\Delta(s, t, \bar{s}, \bar{t}) = \sum_{u=0}^{2m-1} \sum_{j=0}^{n-1} p_{u,j} \bar{s}^u \bar{t}^j. \quad (7.22)$$

Ze vztahu (7.21) potom plyne, že polynomy $p_{u,0}, \dots, p_{u,n-1}$, jsou dány lineární kombinací polynomů $s^i t^j f, s^i t^j g, s^i t^j h$, $0 \leq i \leq 2m-1, 0 \leq j \leq n-1$ a tedy existuje matice $\mathbf{F}$ rozměru $6mn \times 2mn$ taková, že

$$[(f \ g \ h) \dots s^{2m-1} t^{n-1} (f \ g \ h)] \cdot \mathbf{F} = [p_{0,0} \dots p_{0,n-1} \dots p_{2m-1,0} \dots p_{2m-1,n-1}]. \quad (7.23)$$

Jelikož první matice na levé straně (7.23) odpovídá levé straně (7.14) a pravá strana (7.23) odpovídá prvním dvěma členům pravé strany (7.20), je možné přepsat (7.23) do tvaru

$$\begin{aligned} [1 \dots t^{2n-1} \dots s^{3m-1} \dots s^{3m-1} t^{2n-1}] \cdot \mathbf{Syl}(f, g, h) \cdot \mathbf{F} = \\ = [1 \dots t^{2n-1} \dots s^{3m-1} \dots s^{3m-1} t^{2n-1}] \cdot \mathbf{Dix}(f, g, h). \end{aligned} \quad (7.24)$$

Přidáním $4mn$ nulových řádků k Dixonově matici a rozšířením vektoru na pravé straně dostáváme

$$\begin{aligned} [1 \dots t^{2n-1} \dots s^{3m-1} \dots s^{3m-1} t^{2n-1}] \cdot \mathbf{Syl}(f, g, h) \cdot \mathbf{F} = \\ = [1 \dots t^{2n-1} \dots s^{3m-1} \dots s^{3m-1} t^{2n-1}] \cdot \begin{bmatrix} \mathbf{Dix}(f, g, h) \\ \mathbf{O}_{4mn \times 2mn} \end{bmatrix}. \end{aligned} \quad (7.25)$$

Zmíněný transformační vztah mezi Sylvesterovou a Dixonovou maticí tedy je

$$\mathbf{Syl}(f, g, h) \cdot \mathbf{F} = \begin{bmatrix} \mathbf{Dix}(f, g, h) \\ \mathbf{O}_{4mn \times 2mn} \end{bmatrix}. \quad (7.26)$$

Nicméně stále nevíme nic bližšího o struktuře matice $\mathbf{F}$. Matice $\mathbf{F}$ je rozměru $6mn \times 2mn$ a lze ji zapsat blokově ve tvaru

$$\begin{bmatrix} \mathbf{F}_{0,0} & \dots & \mathbf{F}_{0,2m-1} \\ \vdots & & \vdots \\ \mathbf{F}_{2m-1,0} & \dots & \mathbf{F}_{2m-1,2m-1} \end{bmatrix},$$

kde každý blok má rozměr $3n \times n$. Vztah (7.23) můžeme přepsat následovně

$$[f \ g \ h \dots s^{2m-1} t^{n-1} (f \ g \ h)] \cdot \begin{bmatrix} \mathbf{F}_{0,u} \\ \vdots \\ \mathbf{F}_{2m-1,u} \end{bmatrix} = [p_{u,0} \dots p_{u,n-1}].$$

Z rovnic (7.21) a (7.22) vyplývá, že prvky matic $\mathbf{F}_{\sigma,u}$, $0 \leq \sigma \leq 2m-1$, jsou generovány koeficienty výrazů

$$\begin{aligned} \sum_{i+j=\sigma+u+1} \frac{g_i(t)h_j(\bar{t}) - g_i(\bar{t})h_j(t)}{\bar{t} - t}, \\ \sum_{i+j=\sigma+u+1} \frac{h_i(t)f_j(\bar{t}) - h_i(\bar{t})f_j(t)}{\bar{t} - t}, \end{aligned} \quad (7.27)$$

$$\sum_{i+j=\sigma+u+1} \frac{f_i(t)g_j(\bar{t}) - f_i(\bar{t})g_j(t)}{\bar{t} - t}.$$

Každý člen v těchto třech součtech je Bézoutovým polynomem pro dva polynomy v jedné proměnné a tedy každý tento člen generuje Bézoutovu matici. Proto každý blok $\mathbf{F}_{\sigma,u}$ obsahuje tři sumy Bézoutových matic, které se po řádcích prolínají (necht' B_i^j , $i = 1, 2, 3$, je j -tý řádek i -té matice; potom $\mathbf{F}_{\sigma,u} = [B_1^1; B_2^1; B_3^1; B_1^2; B_2^2; B_3^2; \dots]$). Tedy,

$$\mathbf{F}_{\sigma,u} = \text{prolínání po řádcích tří matic} \\ \sum_{i+j=\sigma+u+1} \mathbf{Bez}(g_i, h_j), \quad \sum_{i+j=\sigma+u+1} \mathbf{Bez}(h_i, f_j), \quad \sum_{i+j=\sigma+u+1} \mathbf{Bez}(f_i, g_j). \quad (7.28)$$

Navíc, bloky $\mathbf{F}_{\sigma,u}$ mají následující vlastnosti:

- $\mathbf{F}_{\sigma,u} = \mathbf{F}_{\sigma',u'}$, pokud $\sigma + u = \sigma' + u'$;
- $\mathbf{F}_{\sigma,u} = \mathbf{O}_{3n \times n}$, pokud $\sigma + u > 2m - 1$.

Z toho dále plyne, že

$$\mathbf{F}_{\sigma,u} = \begin{cases} \mathbf{F}_{0,\sigma+u}, & \sigma + u \leq 2m - 1, \\ \mathbf{O} & \text{jinak} \end{cases}$$

a platí

$$\mathbf{F} = \begin{bmatrix} \mathbf{F}_{0,0} & \dots & \mathbf{F}_{0,2m-1} \\ \vdots & & \vdots \\ \mathbf{F}_{2m-1,0} & \dots & \mathbf{F}_{2m-1,2m-1} \end{bmatrix} = \begin{bmatrix} \mathbf{F}_{0,0} & \mathbf{F}_{0,1} & \dots & \mathbf{F}_{0,2m-1} \\ \mathbf{F}_{0,1} & & & \\ \vdots & & & \\ \mathbf{F}_{0,2m-1} & & & \end{bmatrix}.$$

Pro zjednodušení můžeme vypustit první index u bloku a označit matice $\mathbf{F}_{0,j}$ symbolem $\mathbf{F}_j$. Potom

$$\mathbf{F} = \begin{bmatrix} \mathbf{F}_0 & \dots & \mathbf{F}_{2m-1} \\ \vdots & & \\ \mathbf{F}_{2m-1} & & \end{bmatrix}. \quad (7.29)$$

Na závěr si opět předvedeme sestavení Dixonovy matice a výpočet Dixonova resultantu na jednoduchém příkladě.

Příklad 7.4 Necht' plocha S je dána stejnou parametrizací jako v Příkladě 7.3. Dostáváme tedy stejnou výchozí soustavu polynomiálních rovnic

$$\begin{aligned} -st + xs + xt + x - 1 &= 0, \\ (y - 1)s + yt + y &= 0, \\ zs + (z - 1)t + z &= 0. \end{aligned}$$

Pro nalezení Dixonovy matice je možné využít vztah (7.26), jelikož již známe Sylvesterovu matici (viz Příklad 7.3). Stačí tedy najít transformační matici $\mathbf{F}$ a vynásobit ji Sylvesterovu matici. Dané polynomy jsou stupně 1 v obou proměnných s a t , tzn. $m = 1$, $n = 1$, a ze vztahu (7.29) plyne

$$\mathbf{F} = \begin{bmatrix} \mathbf{F}_0 & \mathbf{F}_1 \\ \mathbf{F}_1 & \mathbf{0} \end{bmatrix}.$$

Matice $\mathbf{F}$ má rozměr 6×2 a každý blok $\mathbf{F}_i$ má rozměr 3×1 . Z (7.28) vyplývá jak zkonstruovat bloky $\mathbf{F}_0$ a $\mathbf{F}_1$. Nejprve je nezbytné najít polynomy f_i , g_i a h_i , $i = 0, 1$, pomocí (7.15)

$$\begin{aligned} f_0 &= a_{00} + a_{01}t = x - 1 + xt & f_1 &= a_{10} + a_{11}t = x - t, \\ g_0 &= b_{00} + b_{01}t = y + yt & g_1 &= b_{10} + b_{11}t = y - 1, \\ h_0 &= c_{00} + c_{01}t = z + (z - 1)t & h_1 &= c_{10} + c_{11}t = z. \end{aligned}$$

Potom musíme vypočítat Bézoutovy rezultanty pro polynomy f_i , g_i , h_i , abychom mohli určit sumy uvedené v (7.28). Pro sestavení matice $\mathbf{F}_0$ bereme všechny sumy pro všechna i, j taková, že $i + j = 1$. Tedy

$$\begin{aligned} \sum_{i+j=1} \mathbf{Bez}(g_i, h_j) &= \mathbf{Bez}(g_0, h_1) + \mathbf{Bez}(g_1, h_0) = -yz + (y - 1)(z - 1) = -y - z + 1, \\ \sum_{i+j=1} \mathbf{Bez}(h_i, f_j) &= \mathbf{Bez}(h_0, f_1) + \mathbf{Bez}(h_1, f_0) = -z - x(z - 1) + xz = x - z, \\ \sum_{i+j=1} \mathbf{Bez}(f_i, g_j) &= \mathbf{Bez}(f_0, g_1) + \mathbf{Bez}(f_1, g_0) = -x(y - 1) + xy + y = x + y. \end{aligned}$$

Matice $\mathbf{F}_0$ dostáváme ve tvaru

$$\mathbf{F}_0 = \begin{bmatrix} -y - z + 1 \\ x - z \\ x + y \end{bmatrix}.$$

Podobně vypočteme prvky matice $\mathbf{F}_1$. Sumy bereme pro všechna i, j taková, že $i + j = 2$. Dostáváme

$$\begin{aligned} \sum_{i+j=2} \mathbf{Bez}(g_i, h_i) &= \mathbf{Bez}(g_1, h_1) = 0, \\ \sum_{i+j=2} \mathbf{Bez}(h_i, f_i) &= \mathbf{Bez}(h_1, f_1) = -z, \\ \sum_{i+j=2} \mathbf{Bez}(f_i, g_i) &= \mathbf{Bez}(f_1, g_1) = y - 1 \end{aligned}$$

a tedy

$$\mathbf{F}_1 = \begin{bmatrix} 0 \\ -z \\ y - 1 \end{bmatrix}.$$

Z bloků $\mathbf{F}_0$ a $\mathbf{F}_1$ již snadno sestavíme výslednou transformační matici $\mathbf{F}$ ve tvaru

$$\mathbf{F} = \begin{bmatrix} -y - z + 1 & 0 \\ x - z & -z \\ x + y & y - 1 \\ 0 & 0 \\ -z & 0 \\ y - 1 & 0 \end{bmatrix}.$$

Potom

$$\begin{bmatrix} \mathbf{Dix}(f, g, h) \\ \mathbf{O}_{4 \times 2} \end{bmatrix} = \underbrace{\begin{bmatrix} x - 1 & y & z & 0 & 0 & 0 \\ x & y & z - 1 & 0 & 0 & 0 \\ x & y - 1 & z & x - 1 & y & z \\ -1 & 0 & 0 & x & y & z - 1 \\ 0 & 0 & 0 & x & y - 1 & z \\ 0 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}}_{\mathbf{Syl}(f, g, h)} \underbrace{\begin{bmatrix} -y - z + 1 & 0 \\ x - z & -z \\ x + y & y - 1 \\ 0 & 0 \\ -z & 0 \\ y - 1 & 0 \end{bmatrix}}_{\mathbf{F}}$$

a po vynásobení dostaneme Dixonovu matici ve tvaru

$$\mathbf{Dix}(f, g, h) = \begin{bmatrix} x + y + z - 1 & -z \\ -y & -y - z + 1 \end{bmatrix}.$$

Determinant Dixonovy matice je

$$\det(\mathbf{Dix}(f, g, h)) = -xy - xz + x - y^2 - 3yz + 2y - z^2 + 2z - 1,$$

což je stejný výsledek jako jsme obdrželi ze Sylvesterovy matice (až na násobek číslem -1) v Příkladě 7.3. ■

Zbývající část této kapitoly bude věnována formulacím matic resultantů pro obecný případ $n + 1$ polynomů v n proměnných.

7.2.4 Matice Sylvesterova typu

Konstrukce matic resultantu Sylvesterova typu je založena na podobné myšlence jako dialytická metoda – pro danou soustavu polynomiálních rovnic $F = \{f_0, \dots, f_n\}$ chceme najít množinu monomů, tzv. *množinu násobitelů*, pomocí které můžeme získat novou soustavu polynomiálních rovnic F' .

Definice 7.2.1 *Nechť $f(x_1, \dots, x_n)$ je polynom a nechť $\mathbf{X}$ je množina násobitelů. Potom*

$$\mathbf{X}f = \{x^\alpha f \mid x^\alpha \in \mathbf{X}\}$$

je množina polynomů získaná násobením polynomu f prvky množiny $\mathbf{X}$.

Poznamenejme, že je-li ε řešením $f = 0$, potom je také řešením $\mathbf{X}f = \mathbf{0}$. Na druhou stranu, jestliže ε je řešením $\mathbf{X}f = \mathbf{0}$ a existuje monom $x^\alpha \in \mathbf{X}$ takový, že $\varepsilon^\alpha \neq 0$, potom ε je také řešením $f = 0$. Speciálně, pokud $\mathbf{X}$ obsahuje 1, potom množiny řešení $f = 0$ a $\mathbf{X}f = \mathbf{0}$ jsou shodné.

Nechť $\mathbf{X}_0, \mathbf{X}_1, \dots, \mathbf{X}_n$ jsou množiny násobitelů pro polynomy $f_0, \dots, f_n$. Potom je možné uvažovat novou soustavu rovnic

$$F' = \begin{cases} \mathbf{X}_0 f_0 \\ \mathbf{X}_1 f_1 \\ \vdots \\ \mathbf{X}_n f_n \end{cases} = \mathbf{M}_{F'} \cdot \mathbf{X},$$

kde $x^\alpha \in \mathbf{X}$, pokud $\alpha = \beta + \gamma$, $x^\beta \in \mathbf{X}_i$ a $x^\gamma \in f_i$ pro nějaké $0 \leq i \leq n$. Matice $\mathbf{M}_{F'}$ je potom *maticí rezultantu Sylvesterova typu*.

Definice 7.2.2 *Matice rezultantu je maticí Sylvesterova typu, jestliže prvky v této matici jsou buď nuly nebo koeficienty polynomů výchozí soustavy polynomiálních rovnic.*

Je zřejmé, že dialytická metoda vždy dává matici rezultantu Sylvesterova typu. Jiným příkladem matice rezultantu Sylvesterova typu je Macaulayho matice uvedená v následující části.

7.2.5 Macaulayho matice

Macaulayho matice je maticí rezultantu Sylvesterova typu se speciální volbou množin násobitelů pro dané polynomy výchozí soustavy rovnic. Nechť $F = \{f_0, \dots, f_n\}$ je soustava polynomiálních rovnic a necht'

$$N = \sum_{i=0}^n \deg(f_i) - n,$$

kde $\deg(f_i)$ je celkový stupeň polynomu f_i . Necht'

$$\mathbf{X} = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n \leq N\}$$

je množina monomů takových, že $|\mathbf{X}| = \binom{N+n}{n}$ a necht'

$$\begin{aligned} \mathbf{X}_0 &= \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n \leq N - \deg(f_0)\}, \\ \mathbf{X}_1 &= \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n \leq N - \deg(f_1) \wedge \alpha_1 < \deg(f_0)\}, \\ \mathbf{X}_2 &= \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n \leq N - \deg(f_2) \wedge \alpha_1 < \deg(f_0) \wedge \\ &\quad \wedge \alpha_2 < \deg(f_1)\}, \\ &\vdots \\ \mathbf{X}_n &= \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n \leq N - \deg(f_n) \wedge \\ &\quad \wedge \alpha_{i+1} < \deg(f_i), \forall i : i \leq n-1\}. \end{aligned}$$

Z konstrukce množin $\mathbf{X}_i$ vyplývá, že všechny monomy množiny polynomů $\mathbf{X}_i f_i$ leží v množině $\mathbf{X}$. Navíc,

$$\sum_{i=0}^n |\mathbf{X}_i| = |\mathbf{X}|.$$

Potom soustava polynomiálních rovnic

$$F' = \begin{cases} \mathbf{X}_0 f_0 \\ \mathbf{X}_1 f_1 \\ \vdots \\ \mathbf{X}_n f_n \end{cases} = \mathbf{M}_{F'} \cdot \mathbf{X}$$

má $|\mathbf{X}|$ rovnic a $|\mathbf{X}|$ monomů. Matice rezultantu získaná pomocí množin násobitelů X_i je tedy čtvercovou maticí a nazývá se *Macaulayho maticí*.

Macaulay také určil extra faktor, který je obsažen v projekčním operátoru získaném jako determinant Macaulayho matice. Tímto extra faktorem je determinant jisté submatice matice $\mathbf{M}_{F'}$.

Definice 7.2.3 Monom $x^\alpha \in \mathbf{X}$ se nazývá redukovaný, jestliže $x_i^{\deg(f_i)}$ dělí x^α pro právě jedno $i \in \{0, \dots, n\}$.

Jestliže vypustíme všechny řádky a sloupce příslušné redukovaným monomům x^α , dostaneme submatici $\mathbf{M}_{F'}$, jejíž determinant je přesně extra faktorem (až na znaménko) obsaženým v projekčním operátoru.

7.2.6 Dixonova matice

V části 7.2.3 již byla zmíněna konstrukce Dixonovy matice pro tři polynomy ve dvou proměnných. Tato část bude věnována zobecnění pro obecný případ $n + 1$ polynomů v n proměnných.

Nechť $F = \{f_0, \dots, f_n\} \subset \mathbb{Z}(a_1, \dots, a_m)[x_1, \dots, x_n]$ je množina $n + 1$ polynomů v n proměnných $x_1, \dots, x_n$ s koeficienty z tělesa $\mathbb{Z}(a_1, \dots, a_m)$. Analogicky jako v případě dvou proměnných nejprve zavedeme zobecněný Dixonův polynom.

Definice 7.2.4 Nechť $F = \{f_0, \dots, f_n\} \subset \mathbb{Z}(a_1, \dots, a_m)[x_1, \dots, x_n]$ je soustava polynomiálních rovnic a nechť

$$\delta(x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n) = \begin{vmatrix} f_1(x_1, x_2, \dots, x_n) & \dots & f_{n+1}(x_1, x_2, \dots, x_n) \\ f_1(\bar{x}_1, x_2, \dots, x_n) & \dots & f_{n+1}(\bar{x}_1, x_2, \dots, x_n) \\ f_1(x_1, \bar{x}_2, \dots, x_n) & \dots & f_{n+1}(x_1, \bar{x}_2, \dots, x_n) \\ \vdots & & \vdots \\ f_1(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) & \dots & f_{n+1}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) \end{vmatrix},$$

kde $\bar{x}_i$ jsou nově přidané proměnné a $f_j(\bar{x}_1, \dots, \bar{x}_k, x_{k+1}, \dots, x_n)$ získáme substitucí nových proměnných $\bar{x}_i$ za $x_i, i = 0, \dots, k$, v polynomu f_j . Potom Dixonův polynom je definován vztahem

$$\Delta(f_0, \dots, f_n; x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n) = \frac{\delta(x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n)}{(x_1 - \bar{x}_1) \cdots (x_n - \bar{x}_n)}. \quad (7.30)$$

Je zřejmé, že Dixonův polynom je skutečně polynomem, a ne racionální funkcí. Jelikož determinant δ v čitateli vztahu (7.30) nabývá nulové hodnoty pro libovolné $x_i = \bar{x}_i, 0 \leq i \leq n$, je dělitelný $(x_i - \bar{x}_i), \forall i$. Dixonův polynom je možné také přepsat do maticové podoby – viz následující definice.

Definice 7.2.5 *Dixonův polynom $\Delta(f_0, \dots, f_n; x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n)$ je možné zapsat ve tvaru*

$$\Delta(f_0, \dots, f_n; x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n) = \mathbf{X} \cdot \Theta \cdot \bar{\mathbf{X}},$$

kde $\mathbf{X} = (x^{\alpha_1}, \dots, x^{\alpha_l})$ je řádkový vektor obsahující uspořádanou množinu monomů v proměnných $x_1, \dots, x_n$ v Δ , a $\bar{\mathbf{X}} = (\bar{x}^{\beta_1}, \dots, \bar{x}^{\beta_k})$ je sloupcový vektor obsahující uspořádanou množinu monomů v proměnných $\bar{x}_1, \dots, \bar{x}_n$ v Δ . Prvek v i -tém řádku a j -tém sloupci matice Θ je koeficientem monomu $x^{\alpha_i} \bar{x}^{\beta_j}$ v Dixonově polynomu Δ . Matice Θ se nazývá Dixonova matice.

Podobně jako v případě Bézoutovy matice je Dixonova matice hustou maticí, jelikož její prvky nejsou přímo koeficienty polynomů výchozí soustavy polynomiálních rovnic ale determinanty matic těchto koeficientů. To představuje výhodu i nevýhodu oproti maticím Sylvesterova typu – Dixonova matice je výrazně menší než různé matice Sylvesterova typu, ale na druhou stranu je výpočetně náročnější její sestavení. Výhoda získaná menším rozměrem matice však obvykle převažuje nad zmíněnou nevýhodou – výpočet symbolického determinantu je velmi citlivý na velikost matice a menší matice rezultantu představují tedy velkou výhodu při extrakci projekčního operátoru z matice rezultantu.

Řešení soustavy polynomiálních rovnic $F = \{f_0, \dots, f_n\}$ je současně kořenem Dixonova polynomu. Proto lineární soustava

$$\mathbf{X} \cdot \Theta = 0$$

musí být řešitelná, pokud existuje řešení výchozí soustavy polynomiálních rovnic. A tedy, nulovost determinantu matice Θ je nutnou podmínkou pro existenci řešení soustavy polynomiálních rovnic F .

V některých případech nemusí být Dixonova matice Θ čtvercová nebo může být její hodnota menší než počet řádků a sloupců. V takovém případě je možné využít metodu RSC pro získání projekčního operátoru z takové matice.

7.2.7 Dixonova dialytická matice

Poslední formulací matice rezultantu zmíněnou v této kapitole bude tzv. *Dixonova dialytická matice*, která je maticí Sylvesterova typu a vychází z Dixonovy formulace matice rezultantu.

Pro se sestavení se používá jeden volitelný parametr – libovolný polynom g . Odlišné volby parametru g vedou k odlišným maticím rezultantu, s rozdílnými rozměry matic. Nicméně existují odhady a podmínky pro optimální volbu g , které zaručují minimalizaci rozměru matice a tím i minimalizaci stupně extra faktoru obsaženého v projekčním operátoru.

Nechť $g \in \mathbb{C}[x_1, \dots, x_n, a_1, \dots, a_m]$ je libovolný polynom a necht' $F = \{f_0, \dots, f_n\} \subset \mathbb{C}[x_1, \dots, x_n, a_1, \dots, a_m]$ je soustava polynomiálních rovnic. Označme

$$\Delta_i(g) = \Delta(f_0, \dots, f_{i-1}, g, f_{i+1}, \dots, f_n; x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n),$$

Dixonův polynom soustavy F , kde i -tý polynom byl nahrazen polynomem g .

Věta 7.2.2 *Polynomiální násobek Dixonova polynomu soustavy polynomiálních rovnic $F = \{f_0, \dots, f_n\}$ je možné vyjádřit jako součet součinů zadaných polynomů f_i a Dixonových polynomů zbývajících polynomů a daného polynomiálního násobku, tj.*

$$g\Delta(f_0, \dots, f_n; x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n) = \sum_{i=0}^n f_i \Delta_i(g), \quad (7.31)$$

kde g je libovolný polynom.

Důkaz: Viz [9]. □

Využijeme-li maticový zápis Dixonova polynomu, je možné přepsat polynom $\Delta_i(g)$ do tvaru

$$\Delta_i(g) = \overline{\mathbf{X}}_i \boldsymbol{\Theta}_i(g) \mathbf{X}_i,$$

kde $\boldsymbol{\Theta}_i(g)$ je Dixonova matice soustavy polynomiálních rovnic $\{f_0, \dots, f_{i-1}, g, f_{i+1}, \dots, f_n\}$. Vynásobíme-li $\Delta_i(g)$ polynomem f_i , dostáváme

$$\Delta_i(g)f_i = (\overline{\mathbf{X}}_i \boldsymbol{\Theta}_i(g) \mathbf{X}_i)f_i = (\overline{\mathbf{X}}_i \boldsymbol{\Theta}_i(g)) \cdot (\mathbf{X}_i f_i).$$

Potom vektory $\mathbf{X}_i$ je možné použít jako množiny násobitelů pro příslušné polynomy f_i a zkonstruovat dialytickou matici, tj.

$$F' = \begin{pmatrix} \mathbf{X}_0 f_0 \\ \mathbf{X}_1 f_1 \\ \vdots \\ \mathbf{X}_n f_n \end{pmatrix} = \mathbf{M}_{F'} \cdot \mathbf{Y}.$$

Následně, vyjdeme-li z (7.31), dostáváme

$$\begin{aligned}
g\Delta(f_0, \dots, f_n; x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n) &= \bar{\mathbf{X}}\boldsymbol{\Theta}g\mathbf{X} = \\
&= \sum_{i=0}^n \Delta_i(g)f_i = \sum_{i=0}^n \bar{\mathbf{X}}_i\boldsymbol{\Theta}_i(g)(\mathbf{X}_if_i) = \\
&= \bar{\mathbf{Y}}[\boldsymbol{\Theta}_0(g) : \boldsymbol{\Theta}_1(g) : \dots : \boldsymbol{\Theta}_n(g)] \begin{bmatrix} \mathbf{X}_0f_0 \\ \mathbf{X}_1f_1 \\ \vdots \\ \mathbf{X}_nf_n \end{bmatrix} = \\
&= \bar{\mathbf{Y}}(\mathbf{T} \cdot \mathbf{M}_{F'})\mathbf{Y} = \bar{\mathbf{Y}}\boldsymbol{\Theta}'\mathbf{Y},
\end{aligned}$$

kde

$$\bar{\mathbf{Y}} = \bigcup_{i=0}^n \bar{\mathbf{X}}_i \quad \text{a} \quad \mathbf{T} = \boldsymbol{\Theta}_0(g) : \boldsymbol{\Theta}_1(g) : \dots : \boldsymbol{\Theta}_n(g) \quad \text{a} \quad \boldsymbol{\Theta}' = \mathbf{T} \cdot \mathbf{M}_{F'}.$$

Odtud tedy plyne

$$\bar{\mathbf{X}}\boldsymbol{\Theta}g\mathbf{X} = \bar{\mathbf{Y}}\boldsymbol{\Theta}'\mathbf{Y}.$$

Důsledek 7.2.3 *Pro danou soustavu polynomiálních rovnic $F = \{f_0, \dots, f_n\}$ je možné odpovídající Dixonovu matici rozložit na součin dvou matic, z nichž jedna je dialytickou maticí, tj.*

$$\boldsymbol{\Theta} = \mathbf{T} \cdot \mathbf{M}_{F'},$$

kde $\mathbf{M}_{F'}$ je Dixonova dialytická matice pro danou soustavu F .

Tento důsledek je v podstatě zobecněním transformačního vztahu mezi Sylvesterovou a Bézoutovou maticí v případě polynomů v jedné proměnné a mezi Sylvesterovou a Dixonovou maticí pro tři polynomy ve dvou proměnných pro obecný případ polynomů v n proměnných.

Kapitola 8

Implicitizace křivek a ploch

Existují v zásadě dva standardní způsoby reprezentace algebraických variet – implicitní reprezentace a parametrická reprezentace. Podle toho, jaké operace potřebujeme provádět s danou algebraickou varietou, může být výhodnější implicitní nebo parametrická reprezentace. Parametrické vyjádření je výhodnější pro generování bodů na varietě, např. pro její vykreslení. Implicitní vyjádření je lepší v případě, že potřebujeme zjistit, zda daný bod leží na dané varietě, příp. uvnitř nebo vně dané variety. Dalším příkladem je hledání průnik dvou variet, kde je výhodné mít k dispozici implicitní vyjádření jedné variety a parametrické vyjádření druhé variety. Proto je důležitá existence metod pro přechod od jednoho vyjádření ke druhému.

Typickými objekty geometrického modelování jsou racionální Bézierovy křivky a plochy a NURBS (NeUniformní Racionální B-Spline) křivky a plochy, které jsou reprezentovány parametricky. Proto se v této kapitole zaměříme na problém *implicitizace*, tzn. na nalezení implicitního popisu parametricky zadané racionální algebraické variety.

V posledních letech jsou metody implicitizace algebraických variet intenzivně studovány. Základní přístup spočívá v použití metod eliminace proměnných, jako jsou rezultanty (viz kap. 7 nebo také [9],[13],[17],[24]) nebo Gröbnerovy báze (viz kap. 3 nebo také [3], [2]). Odstraněním jmenovatelů je parametrizace převedena na soustavu polynomiálních rovnic, z nichž jsou vylimínovány parametry. Obecně ale nemusí být získáno implicitní vyjádření nejmenší variety obsahující dané parametrické vyjádření. Při použití Gröbnerovýchází spočívá možné řešení v přidání jedné rovnice, která zaručí nenulovost jmenovatelů parametrizace (viz kap. 6). Odlišný způsob řešení toho problému je prezentován v [1].

V případě použití rezultantů přidání rovnice, která zajistí nenulovost jmenovatelů parametrizace, nepomůže. Determinant matice rezultantu (resp. maximálního minoru) může stále obsahovat extra faktory, které je nutné eliminovat ze získaného projekčního operátoru.

Obecně lze dále říci, že algoritmy implicitizace pomocí Gröbnerovýchází a rezultantů mají „problémy“ s parametrizacemi, které obsahují tzv. *base points*¹. V takovém případě je Dixonův rezultant (a libovolný jiný rezultant získaný jako determinant matice rezultantu)

¹Nechť $S(u, v) = (X(u, v), Y(u, v), Z(u, v), W(u, v))$ je parametrizace plochy v projektivním prostoru. *Base point* je taková dvojice $(u_0, v_0) \in \mathbb{C}^2$, že platí $X(u_0, v_0) = 0 \wedge Y(u_0, v_0) = 0 \wedge Z(u_0, v_0) = 0 \wedge W(u_0, v_0) = 0$.

identicky roven nule. K extrakci nenulového projekčního operátoru z matice rezultantu je možné použít metodu RSC (viz kap. 7 nebo také [9], [11], [12] a [24]). V případě použití Gröbnerovýchází nedochází k úplné eliminaci proměnných (implicitní vyjádření není obsaženo v ideálu generovaném parametrickými rovnicemi), což je možné řešit přidáním rovnice zajišťující nenulovost jmenovatelů parametrizace, jak bylo zmíněno výše. Dalším možným řešením je perturbace vstupních polynomů pomocí vhodně zvolených polynomů, které nenabývají nulové hodnoty pro base points dané parametrizace (viz [16], [15]). Poté eliminujeme parametry ze získané soustavy rovnic a implicitní vyjádření je obsaženo v koeficientu u nejnižší mocniny zvolené perturbační proměnné.

Další metodou implicitizace algebraických variet je *metoda moving curves a moving surfaces* (viz [25], [26]). Implicitní vyjádření je získáno opět jako determinant speciálně vytvořené matice, která může být dokonce menší než odpovídající matice rezultantu. Například, pokud použijeme metody moving conics (quadrics) pro implicitizaci racionálních křivek (ploch) bez base points, velikosti získané matice je čtvrtinou odpovídající Dixonovy matice. Jestliže existují base points pro danou křivku (plochu), metoda se v podstatě zjednoduší – sníží se stupeň některých prvků v matici nebo se dokonce zmenší získaná matice.

S využitím znalostí metod moving lines a moving planes, články [6] a [7] prezentují metodu pro implicitizaci racionálních křivek a ploch, kde implicitní vyjádření je získáno jako determinant speciální matice Sylvesterova typu (řádká matice, jednoduché prvky) s rozměrem Bézoutovy matice.

V posledních letech se objevil zajímavý přístup implicitizace křivek a ploch využívající numerických metod – klasické polynomiální interpolace (viz [18], [19]). Po sestavení matice rezultantu (články jsou založeny na použití Macaulayho rezultantu, ale je možné využít libovolné formulace matice rezultantu), je determinant interpolován pomocí klasické Lagrangeovy interpolační metody (pro implicitizaci křivek), příp. se využije rozšíření pro případ více proměnných (pro plochy).

Článek[31] uvádí velmi jednoduchou metodu implicitizace, která je založena na odhadu stupně implicitního vyjádření a hledá koeficienty obecného polynomu odhadnutého stupně pomocí řešení soustavy lineárních rovnic.

8.1 Implicitizace pomocí Gröbnerovýchází a rezultantů

Základní metodou implicitizace algebraických variet je použití metod eliminace proměnných pro eliminace parametrů z parametrického vyjádření algebraické variety. Necht

$$\mathbf{C}(t) = \left(\frac{X(t)}{W(t)}, \frac{Y(t)}{W(t)} \right) \quad (8.1)$$

je racionální parametrizace rovinné křivky C . Potom odstraněním jmenovatelů dostáváme soustavu rovnic

$$\begin{aligned} x \cdot W(t) - X(t) &= 0, \\ y \cdot W(t) - Y(t) &= 0. \end{aligned} \quad (8.2)$$

Eliminací parametru t ze soustavy (8.2) pomocí Gröbnerovýchází nebo resultantů získáme polynom $F(x, y)$ pouze v proměnných x, y , který obsahuje implicitní vyjádření pro danou křivku C . Výjimkou jsou parametrizace obsahující base points, kdy není možné eliminovat parametr pomocí těchto metod přímo – touto situací se budeme podrobněji zabývat později. Nicméně, i když parametrizace neobsahuje base points, $F(x, y)$ může obsahovat také extra faktory². Není tedy garantováno, že $F(x, y)$ představuje *nejmenší* varietu, která obsahuje křivku C danou parametrizací (8.1). To lze zajistit (při použití Gröbnerovýchází) přidáním jedné proměnné a jedné rovnice

$$1 - s \cdot W(t) = 0. \quad (8.3)$$

Rovnice (8.3) zaručí nenulovost jmenovatele parametrizace (8.1). Eliminací proměnných s, t ze soustavy rovnic (8.2)+(8.3) dostáváme polynom $R(x, y)$, který představuje nejmenší varietu obsahující křivku C (viz kap. 6). Polynom $R(x, y)$ je tedy implicitním vyjádřením křivky C dané parametrizací (8.1). Při použití resultantů toto bohužel garantovat nelze, ani po přidání rovnice (8.3) k soustavě (8.2).

Analogicky je možné najít implicitní vyjádření racionálně parametrizované plochy. Necht

$$\mathbf{S}(u, v) = \left(\frac{X(u, v)}{W(u, v)}, \frac{Y(u, v)}{W(u, v)}, \frac{Z(u, v)}{W(u, v)} \right) \quad (8.4)$$

je racionální parametrizace plochy S . Odstraněním jmenovatelů dostáváme soustavu rovnic

$$\begin{aligned} x \cdot W(u, v) - X(u, v) &= 0, \\ y \cdot W(u, v) - Y(u, v) &= 0, \\ z \cdot W(u, v) - Z(u, v) &= 0. \end{aligned} \quad (8.5)$$

Eliminací parametrů u, v (opět za předpokladu, že parametrizace (8.4) nemá base points) získáme polynom $F(x, y, z)$ pouze v proměnných x, y, z , který obsahuje implicitní vyjádření dané plochy a obecně také extra faktory. Obdobně je tedy možné přidat rovnici

$$1 - s \cdot W(u, v) = 0 \quad (8.6)$$

pro zaručení nenulovosti jmenovatelů parametrizace (8.5). Potom eliminací proměnných s, u, v pomocí Gröbnerovýchází dostaneme polynom $R(x, y, z)$, který reprezentuje nejmenší varietu obsahující danou plochu S a je tedy implicitním vyjádřením plochy S .

Jak již bylo zmíněno výše, *base point* je každé společné řešení $(u_0, v_0) \in \mathbb{C}^2$ soustavy rovnic

$$X(u, v) = 0, \quad Y(u, v) = 0, \quad Z(u, v) = 0, \quad W(u, v) = 0.$$

Jestliže parametrizace plochy obsahuje base point, obě metody selhávají při nalezení implicitního vyjádření plochy S . Nyní si vysvětlíme, co to způsobuje.

²Extra faktory jsou faktory $F(x, y)$, které nepatří do implicitního vyjádření křivky C . Přesněji, faktory $F(x, y)$, pro které $F\left(\frac{X(t)}{W(t)}, \frac{Y(t)}{W(t)}\right) = 0$ tvoří implicitní vyjádření dané křivky C . Ostatní faktory jsou extra faktory.

Použijeme-li rezultanty, projekční operátor získaný z matice rezultantu pro soustavu (8.5) vzhledem k parametrizaci s base point(s) je identicky nulový. Jestliže $(u_0, v_0) \in \mathbb{C}^2$ je base point parametrizace $\mathbf{S}(u, v)$, potom substitucí do (8.5) dostáváme

$$\begin{aligned}x \cdot 0 - 0 &= 0, \\y \cdot 0 - 0 &= 0, \\z \cdot 0 - 0 &= 0.\end{aligned}$$

Soustava rovnic (8.5) má tedy netriviální řešení (u_0, v_0) nezávislé na x, y, z . Jelikož resultant představuje nutnou a postačující podmínku existenci společného řešení výchozí soustavy rovnic, je resultant v tomto případě identicky nulový.

Použití Gröbnerovýchází pro implicitizaci křivek a ploch je založena na faktu, že implicitní vyjádření je obsaženo v ideálu I generovaném polynomy soustavy (8.5). Při vhodné volbě uspořádání jsme toto implicitní vyjádření schopni získat z vypočtené Gröbnerovy báze. Problémem parametrizací s base points je, že odpovídající ideál I neobsahuje žádný polynom nezávislý na u, v (kromě 0) a tedy ideál I v tomto případě neobsahuje implicitní vyjádření plochy S . Nechť

$$I = \langle x \cdot W(u, v) - X(u, v), y \cdot W(u, v) - Y(u, v), z \cdot W(u, v) - Z(u, v) \rangle \quad (8.7)$$

je ideál generovaný rovnicemi (8.5) a nechť (u_0, v_0) je base point parametrizace (8.4). Předpokládejme, že I obsahuje polynom $F(x, y, z)$ nezávislý na u, v . Potom je možné zapsat polynom $F(x, y, z)$ ve tvaru

$$\begin{aligned}F(x, y, z) &= A_1(x, y, z, u, v)(x \cdot W(u, v) - X(u, v)) + \\&+ A_2(x, y, z, u, v)(y \cdot W(u, v) - Y(u, v)) + \\&+ A_3(x, y, z, u, v)(z \cdot W(u, v) - Z(u, v)).\end{aligned}$$

Jelikož toto musí platit nezávisle na volbě (u, v) , musí tento vztah platit také pro (u_0, v_0) . Tedy,

$$\begin{aligned}F(x, y, z) &= A_1(x, y, z, u_0, v_0)(x \cdot W(u_0, v_0) - X(u_0, v_0)) + \\&+ A_2(x, y, z, u_0, v_0)(y \cdot W(u_0, v_0) - Y(u_0, v_0)) + \\&+ A_3(x, y, z, u_0, v_0)(z \cdot W(u_0, v_0) - Z(u_0, v_0)) = \\&= 0.\end{aligned}$$

Odtud vyplývá, že jediným polynomelem nezávislým na u, v v ideálu I je nulový polynom a všechny ostatní polynomy obsahují u nebo v .

Existuje několik možností jak problém s base points řešit:

- je možné přidat rovnici (8.6) pro zajištění nenulovosti jmenovatele $W(u, v)$, což eliminuje base points,
- je možné použít metodu perturbací, tzn. modifikovat výchozí soustavu rovnic (8.5) pomocí vhodně zvolených polynomů (viz [15], [16]),
- pokud použijeme rezultanty pro eliminaci parametrů, je možné využít metodu RSC pro extrakci projekčního operátoru z matice rezultantu i v případě, že determinant matice rezultantu je nulový (viz [9], [24]).

8.2 Implicitizace pomocí moving curves a moving surfaces

Metody moving curves (pro křivky) a moving surfaces (pro plochy) spočívají v sestavení speciální matice, jejíž determinant je implicitním vyjádřením dané algebraické variety. Podrobnější popis metod je možné najít v [25], [26].

Nechť $\mathbf{Q}(t) = (X(t), Y(t), W(t))$ je racionální rovinná křivka stupně n v projektivním rozšíření $\mathbb{E}_2$. *Moving curve stupně m* je definována vztahem

$$C(\mathbf{X}; t) = \sum_{j=0}^m f_j(\mathbf{X})t^j = 0,$$

kde $\mathbf{X} = (x, y, w)$ a $f_j(\mathbf{X})$ je polynom stupně d , a představuje množinu algebraických křivek lišících se v závislosti na t . Řekneme, že moving curve *sleduje* racionální křivku $\mathbf{Q}(t)$, jestliže pro všechna t leží bod $\mathbf{Q}(t)$ na moving curve, tj. platí

$$C(\mathbf{Q}(t); t) = \sum_{j=0}^m f_j(X(t), Y(t), W(t))t^j \equiv 0.$$

Nejčastěji se používají dva typy moving curves – moving lines a moving conics. *Moving line stupně $m - 1$* je možné definovat ekvivalentně dvěma způsoby:

$$L_{m-1}(x, y)t^{m-1} + \dots + L_1(x, y)t + L_0(x, y) = 0$$

nebo

$$A(t)x + B(t)y + C(t) = 0,$$

kde $L_i(x, y)$ jsou lineární polynomy v proměnných x, y a $A(t), B(t), C(t)$ jsou polynomy stupně $m - 1$ v proměnné t (alespoň jeden z nich). Pro libovolné t_0 moving line představuje implicitní rovnici přímky v rovině xy .

Moving line sleduje racionální křivku $\mathbf{Q}(t)$, jestliže platí

$$A(t)\frac{X(t)}{W(t)} + B(t)\frac{Y(t)}{W(t)} + C(t) \equiv 0$$

nebo ekvivalentně

$$A(t)X(t) + B(t)Y(t) + C(t)W(t) \equiv 0.$$

Geometricky to znamená, že implicitně zadaná přímka odpovídající parametru t prochází bodem dané racionální křivky, který odpovídá stejnému parametru t .

Pro danou racionální křivku $\mathbf{Q}(t)$ stupně m obvykle hledáme moving lines stupně $m - 1$

$$L_{m-1}(x, y)t^{m-1} + \dots + L_1(x, y)t + L_0(x, y) = 0, \quad (8.8)$$

kteřé sledují křivku $\mathbf{Q}(t)$. Jelikož každý polynom $L_i(x, y)$ je lineární v x, y , můžeme (8.8) přepsat do tvaru

$$(A_{m-1}x + B_{m-1}y + C_{m-1})t^{m-1} + \dots + (A_1x + B_1y + C_1)t + (A_0x + B_0y + C_0) = 0. \quad (8.9)$$

Dosadíme-li za x a y souřadnice racionální parametrizace křivky $\mathbf{Q}(t)$, tj. racionální funkce $X(t)/W(t)$ a $Y(t)/W(t)$ a vynásobíme-li získaný vztah polynomem $W(t)$, dostaneme polynom stupně $2m - 1$ v proměnné t

$$(A_{m-1}X(t) + B_{m-1}Y(t) + C_{m-1}W(t))t^{m-1} + \dots + (A_0X(t) + B_0Y(t) + C_0W(t)) = 0. \quad (8.10)$$

Pokud má moving line (8.9) sledovat křivku $\mathbf{Q}(t)$, potom musí být polynom (8.10) identicky nulový. To vede na řešení homogenní soustavy $2m$ lineárních rovnic pro $3m$ neznámých A_k, B_k, C_k . Maticově lze tuto soustavu zapsat ve tvaru

$$[X \ Y \ W \ \dots \ t^{m-1}X \ t^{m-1}Y \ t^{m-1}W] \cdot \begin{bmatrix} A_0 \\ B_0 \\ C_0 \\ \vdots \\ A_{m-1} \\ B_{m-1} \\ C_{m-1} \end{bmatrix} = 0, \quad (8.11)$$

kde řádky matice koeficientů odpovídají mocninám t a sloupce koeficientům polynomů $t^k X, t^k Y, t^k W, k = 0, \dots, m - 1$.

Homogenní soustava $2m$ lineárních rovnic pro $3m$ neznámých má alespoň m lineárně nezávislých řešení. Pokud

$$\begin{aligned} p_1(t) &= L_{1,m-1}(x, y)t^{m-1} + \dots + L_{1,1}(x, y)t + L_{1,0}(x, y) = 0, \\ &\vdots \\ p_m(t) &= L_{m,m-1}(x, y)t^{m-1} + \dots + L_{m,1}(x, y)t + L_{m,0}(x, y) = 0 \end{aligned} \quad (8.12)$$

jsou tato lineárně nezávislá řešení soustavy (8.11), potom

$$R(x, y) = \begin{vmatrix} L_{1,0} & \dots & L_{1,m-1} \\ \vdots & & \vdots \\ L_{m,0} & \dots & L_{m,m-1} \end{vmatrix} = 0$$

je implicitním vyjádřením racionální křivky $\mathbf{Q}(t)$, za předpokladu, že křivka nemá base points.

Věta 8.2.1 *Metoda moving lines vždy generuje správné implicitní vyjádření racionální křivky, pokud daná racionální křivka neobsahuje base points.*

Důkaz: Viz [26]. □

Pokud křivka obsahuje base points, potom musí být metoda modifikována – racionální křivka stupně m s r base points je reprezentována implicitně polynomem stupně $m - r$. Detaily modifikace zmíněné metody pro racionální křivky s base points je možné najít v [26].

Metoda moving lines je velmi blízká metodě implicitizace založené na použití Bézoutova rezultantu. Obě metody produkují matice řádu m pro danou racionální křivku stupně m . Navíc, řádky Bézoutovy matice představují moving lines dané racionální křivky a je možné dokázat, že řádky matice generovaná metodou moving lines jsou lineárními kombinacemi řádek Bézoutovy matice.

Hlavní výhoda metody moving curves pro implicitizaci křivek spočívá v použití moving curves s báзовými funkcemi vyššího stupně. Jak již bylo zmíněno výše, používají se zejména moving conics. *Moving conic* stupně $m - 1$ je definována ekvivalentně dvěma způsoby:

$$C_{m-1}(x, y)t^{m-1} + \dots + C_1(x, y)t + C_0(x, y) = 0 \quad (8.13)$$

nebo

$$A(t)x^2 + B(t)xy + C(t)y^2 + D(t)x + E(t)y + F(t) = 0, \quad (8.14)$$

kde $C_j(x, y)$ jsou polynomy stupně dva v proměnných x, y a $A(t), B(t), C(t), D(t), E(t), F(t)$ jsou polynomy stupně $m - 1$ v t .

Podobně jako v případě moving lines, moving conic (8.14) sleduje racionální křivku $\mathbf{Q}(t)$, jestliže nabývá nulové hodnoty na této křivce, tj.

$$\begin{aligned} &A(t)X^2(t) + B(t)X(t)Y(t) + C(t)Y^2(t) + \\ &+ D(t)X(t)W(t) + E(t)Y(t)W(t) + F(t)W^2(t) \equiv 0. \end{aligned}$$

Geometricky to znamená, že implicitně zadaná kuželosečka odpovídající parametru t prochází bodem racionální křivky, který odpovídá stejnému parametru t .

Každý koeficient $C_j(x, y)$ ve vztahu (8.13) je kvadratickým polynomem v proměnných x, y . Vztah (8.13) je tedy možné přepsat do tvaru

$$\begin{aligned} &(A_{m-1}x^2 + B_{m-1}xy + C_{m-1}y^2 + D_{m-1}x + E_{m-1}y + F_{m-1})t^{m-1} + \\ &\quad \vdots \\ &+ (A_0x^2 + B_0xy + C_0y^2 + D_0x + E_0y + F_0) = 0. \end{aligned} \quad (8.15)$$

Pro nalezení implicitního vyjádření racionální křivky $\mathbf{Q}(t)$ stupně $2m$ hledáme moving conics stupně $m - 1$, které sledují $\mathbf{Q}(t)$. Opět dosadíme parametrizaci křivky $\mathbf{Q}(t)$ reprezentovanou polynomy $X(t)/W(t)$ a $Y(t)/W(t)$ za x a y a vynásobíme celou rovnicí $W^2(t)$, čímž dostaneme

$$\begin{aligned} &(A_{m-1}X(t)^2 + B_{m-1}X(t)Y(t) + \dots + E_{m-1}Y(t)W(t) + F_{m-1}W^2(t))t^{m-1} + \\ &\quad \vdots \\ &+ (A_0X(t)^2 + B_0X(t)Y(t) + C_0Y(t)^2 + D_0X(t)W(t) + E_0Y(t)W(t) + F_0W^2(t)) = 0. \end{aligned} \quad (8.16)$$

Jelikož polynomy $X(t)$, $Y(t)$, $W(t)$ jsou stupně $2m$ v proměnné t , levá strana (8.16) je polynomem stupně $5m - 1$ v proměnné t . Polynom (8.16) musí být opět identicky nulový, aby (8.16) sledovala racionální křivku $\mathbf{Q}(t)$. Koeficienty polynomu (8.16) tedy musí být identicky nulové, což vede na řešení homogenní soustavy $5m$ lineární rovnic pro $6m$ neznámých $A_k, B_k, C_k, D_k, E_k, F_k, k = 0, \dots, m - 1$

$$[X^2 \ XY \ Y^2 \ XW \ YW \ W^2 \ \dots \ t^{m-1}X^2 \ t^{m-1}XY \ t^{m-1}Y^2 \ t^{m-1}XW \ t^{m-1}YW \ t^{m-1}W^2] \cdot \begin{bmatrix} A_0 \\ B_0 \\ C_0 \\ \vdots \\ D_{m-1} \\ E_{m-1} \\ F_{m-1} \end{bmatrix} = 0, \quad (8.17)$$

kde řádky matice koeficientů odpovídají mocninám t , sloupce odpovídají koeficientům polynomů $t^k X^2, t^k XY, t^k Y^2, t^k XW, t^k YW, t^k W^2, k = 0, \dots, m - 1$. Homogenní soustava (8.17) má alespoň m lineárně nezávislých řešení

$$\begin{aligned} q_1(t) &= C_{1,m-1}(x, y)t^{m-1} + \dots + C_{1,1}(x, y)t + C_{1,0}(x, y) = 0, \\ &\vdots \\ q_m(t) &= C_{m,m-1}(x, y)t^{m-1} + \dots + C_{m,1}(x, y)t + C_{m,0}(x, y) = 0. \end{aligned} \quad (8.18)$$

Koeficienty moving conics (8.18) tvoří matici $C(x, y) = (C_{ij}(x, y))$ rozměru $m \times m$. Determinant této matice je dobrým kandidátem na implicitní vyjádření dané racionální křivky. V některých případech se ale může stát, že $\det(C(x, y))$ je identicky roven nule, a to i v případě, že křivka neobsahuje base points. Následující věta uvádí nutnou a postačující podmínku, za které metoda moving conics poskytuje implicitní vyjádření racionální křivky sudého stupně.

Věta 8.2.2 *Metoda moving conics poskytuje implicitní vyjádření racionální křivky stupně $2m$ bez base points právě tehdy, když neexistuje žádná moving line stupně $m - 1$, která sleduje křivku. Navíc, pokud existuje moving line stupně $m - 1$, která sleduje křivku, libovolný determinant získaný metodou moving conics je identicky nulový.*

Důkaz: Viz [26]. □

Nechť $\mathbf{S}(u, v) = (X(u, v), Y(u, v), Z(u, v), W(u, v))$ je racionální parametrizace plochy v projektivním rozšíření $\mathbb{E}_3$ a

$$X(u, v) = \sum_{i=0}^m \sum_{j=0}^n a_{ij} u^i v^j, \quad Y(u, v) = \sum_{i=0}^m \sum_{j=0}^n b_{ij} u^i v^j,$$

$$Z(u, v) = \sum_{i=0}^m \sum_{j=0}^n c_{ij} u^i v^j, \quad W(u, v) = \sum_{i=0}^m \sum_{j=0}^n d_{ij} u^i v^j.$$

Moving surface je definován vztahem

$$g(\mathbf{X}; u, v) = \sum_{i=1}^{\sigma} h_i(\mathbf{X}) \gamma_i(u, v) = 0,$$

kde $\mathbf{X} = (x, y, z, w)$, $h_i(\mathbf{X}) = 0, i = 1, \dots, \sigma$ jsou implicitně zadané plochy a $\gamma_i(u, v), i = 1, \dots, \sigma$ jsou polynomy v proměnných u, v . Moving surface sleduje racionální plochu $\mathbf{S}(u, v)$, jestliže pro všechna (u, v) leží odpovídající bod $\mathbf{S}(u, v)$ na daném moving surface, tj. platí

$$g(\mathbf{S}(u, v); u, v) = \sum_{i=1}^{\sigma} h_i(X(u, v), Y(u, v), Z(u, v), W(u, v)) \gamma_i(u, v) \equiv 0.$$

Obvykle se používají pouze moving planes a moving quadrics. *Moving plane* stupně (σ_1, σ_2) je dána vztahem

$$\sum_{i=0}^{\sigma_1} \sum_{j=0}^{\sigma_2} (A_{i,j}x + B_{i,j}y + C_{i,j}z + D_{i,j}w) \cdot u^i v^j = 0. \quad (8.19)$$

Pro pevně dané hodnoty u and v představuje vztah (8.19) implicitní rovnici roviny. Moving plane sleduje racionální plochu $\mathbf{S}(u, v)$, jestliže

$$\sum_{i=0}^{\sigma_1} \sum_{j=0}^{\sigma_2} (A_{i,j}X(u, v) + B_{i,j}Y(u, v) + C_{i,j}Z(u, v) + D_{i,j}W(u, v)) \cdot u^i v^j \equiv 0. \quad (8.20)$$

Levá strana rovnice (8.20) je polynomem stupně $m + \sigma_1$ v proměnné u a stupně $n + \sigma_2$ v proměnné v . Položíme-li koeficienty u monomů $u^i v^j, i = 0, \dots, m + \sigma_1, j = 0, \dots, n + \sigma_2$ rovny nule, dostaneme homogenní soustavu $(m + \sigma_1 + 1)(n + \sigma_2 + 1)$ lineárních rovnic pro $4(\sigma_1 + 1)(\sigma_2 + 1)$ neznámých $\{A_{i,j}, B_{i,j}, C_{i,j}, D_{i,j}\}, i = 0, \dots, \sigma_1, j = 0, \dots, \sigma_2$. Řešení této soustavy dává systém moving planes, které sledují danou plochu $\mathbf{S}(u, v)$.

Pro moving planes se obvykle volí $\sigma_1 = 2m - 1, \sigma_2 = n - 1$. Dostáváme tedy homogenní soustavu $6mn$ lineárních rovnic pro $8mn$ neznámých, která má alespoň $2mn$ lineárně nezávislých řešení. Moving planes, které sledující zadanou plochu $\mathbf{S}(u, v)$, získáme z řešení této soustavy ve tvaru

$$\begin{aligned} L_1 &\equiv \sum_{i=0}^{2m-1} \sum_{j=0}^{n-1} (A_{i,j}^1 x + B_{i,j}^1 y + C_{i,j}^1 z + D_{i,j}^1 w) \cdot u^i v^j = 0, \\ &\vdots \\ L_{2mn} &\equiv \sum_{i=0}^{2m-1} \sum_{j=0}^{n-1} (A_{i,j}^{2mn} x + B_{i,j}^{2mn} y + C_{i,j}^{2mn} z + D_{i,j}^{2mn} w) \cdot u^i v^j = 0. \end{aligned} \quad (8.21)$$

Determinant matice koeficientů u monomů $u^i v^j$ v (8.21), tj.

$$\begin{vmatrix} A_{0,0}^1 x + B_{0,0}^1 y + C_{0,0}^1 z + D_{0,0}^1 w & \cdots & A_{2m-1,n-1}^1 x + \cdots + D_{2m-1,n-1}^1 w \\ \vdots & & \vdots \\ A_{0,0}^{2mn} x + B_{0,0}^{2mn} y + C_{0,0}^{2mn} z + D_{0,0}^{2mn} w & \cdots & A_{2m-1,n-1}^{2mn} x + \cdots + D_{2m-1,n-1}^{2mn} w \end{vmatrix}$$

nabývá nulové hodnoty, jestliže (x, y, z, w) leží na ploše $\mathbf{S}(u, v)$. Odtud tedy vyplývá, že pokud tento determinant není identicky roven nule, potom je násobkem implicitního vyjádření plochy $\mathbf{S}(u, v)$. Metoda moving planes generuje matici stejného rozměru jako implicitizace ploch za použití Dixonova rezultantu a obě tyto metody jsou ekvivalentní – každý řádek Dixonovy matice představuje jednu moving plane sledující plochu $\mathbf{S}(u, v)$.

Zajímavým způsobem, jak zmenšit rozměr matice generované metodou, je použití moving quadrics. *Moving quadric stupně* (σ_1, σ_2) je dána vztahem

$$\sum_{i=0}^{\sigma_1} \sum_{j=0}^{\sigma_2} (A_{i,j} x^2 + B_{i,j} y^2 + C_{i,j} z^2 + D_{i,j} xy + E_{i,j} xz + F_{i,j} yz + G_{i,j} xw + H_{i,j} yw + I_{i,j} zw + J_{i,j} w^2) \cdot u^i v^j = 0. \quad (8.22)$$

Pro pevně dané hodnoty u and v představuje vztah (8.22) implicitní rovnici kvadriky. Moving quadric sleduje racionální plochu $\mathbf{S}(u, v)$, jestliže

$$\sum_{i=0}^{\sigma_1} \sum_{j=0}^{\sigma_2} (A_{i,j} X(u, v)^2 + B_{i,j} Y(u, v)^2 + \cdots + I_{i,j} Z(u, v) W(u, v) + J_{i,j} W(u, v)^2) \cdot u^i v^j = 0. \quad (8.23)$$

Levá strana rovnice (8.23) je polynomem stupně $2m + \sigma_1$ v proměnné u a stupně $2n + \sigma_2$ v proměnné v . Položíme-li koeficienty u monomů $u^i v^j$, $i = 0, \dots, 2m + \sigma_1$, $j = 0, \dots, 2n + \sigma_2$ rovny nule, dostaneme homogenní soustavu $(2m + \sigma_1 + 1)(2n + \sigma_2 + 1)$ lineárních rovnic pro $10(\sigma_1 + 1)(\sigma_2 + 1)$ neznámých $\{A_{i,j}, B_{i,j}, \dots, I_{i,j}, J_{i,j}\}$, $i = 0, \dots, \sigma_1$, $j = 0, \dots, \sigma_2$. Řešení této soustavy dává systém moving quadrics, které sledují danou plochu $\mathbf{S}(u, v)$.

Pro moving quadrics se obvykle volí $\sigma_1 = m - 1$, $\sigma_2 = n - 1$. Z (8.23) tedy dostáváme homogenní soustavu $9mn$ lineárních rovnic pro $10mn$ neznámých, která má alespoň mn lineárně nezávislých řešení. Moving quadrics, které sledující zadanou plochu $\mathbf{S}(u, v)$, získáme z řešení této soustavy ve tvaru

$$\begin{aligned} Q_1 &\equiv \sum_{i=0}^{\sigma_1} \sum_{j=0}^{\sigma_2} (A_{i,j}^1 x^2 + B_{i,j}^1 y^2 + \cdots + I_{i,j}^1 zw + J_{i,j}^1 w^2) \cdot u^i v^j = 0, \\ &\vdots \\ Q_{mn} &\equiv \sum_{i=0}^{\sigma_1} \sum_{j=0}^{\sigma_2} (A_{i,j}^{mn} x^2 + B_{i,j}^{mn} y^2 + \cdots + I_{i,j}^{mn} zw + J_{i,j}^{mn} w^2) \cdot u^i v^j = 0. \end{aligned} \quad (8.24)$$

Determinant matice koeficientů u monomů $u^i v^j$ v (8.24), tj.

$$\begin{vmatrix} A_{0,0}^1 x^2 + B_{0,0}^1 y^2 + \cdots + J_{0,0}^1 w^2 & \cdots & A_{m-1,n-1}^1 x^2 + B_{m-1,n-1}^1 y^2 + \cdots + J_{m-1,n-1}^1 w^2 \\ \vdots & & \vdots \\ A_{0,0}^{mn} x^2 + B_{0,0}^{mn} y^2 + \cdots + J_{0,0}^{mn} w^2 & \cdots & A_{m-1,n-1}^{mn} x^2 + B_{m-1,n-1}^{mn} y^2 + \cdots + J_{m-1,n-1}^{mn} w^2 \end{vmatrix}$$

nabývá nulové hodnoty, jestliže (x, y, z, w) leží na ploše $\mathbf{S}(u, v)$. Odtud tedy vyplývá, že pokud tento determinant není identicky roven nule, potom je násobkem implicitního vyjádření plochy $\mathbf{S}(u, v)$. Je zřejmé, že při použití moving quadrics je získaná matice výrazně menší – pouze rozměru $mn \times mn$, oproti matici rozměru $2mn \times 2mn$ v případě moving planes, resp. Dixonova rezultantu.

8.3 Implicitizace pomocí polynomiální interpolace

Tato metoda je založena na použití Lagrangeovy interpolace ve dvou a více proměnných pro nalezení rezultantu, a tedy i implicitního vyjádření křivky nebo plochy dané racionální parametrizací.

Nechť

$$\mathbf{C}(t) = \left(\frac{X(t)}{W(t)}, \frac{Y(t)}{W(t)} \right), \quad \text{GCD}(X, Y, W) = 1$$

je racionální parametrizace rovinné algebraické křivky C . Jelikož GCD je zde největším společným dělitelem daných polynomů, podmínka $\text{GCD}(X, Y, W) = 1$ znamená, že polynomy X, Y, W nemají žádný společný faktor. Pro takovou parametrizaci je implicitní vyjádření $F(x, y)$ dané křivky C obsaženo v rezultantu $\text{Res}(xW(t) - X(t), yW(t) - Y(t))$ (viz kap. 8.1). Podmínku $\text{GCD}(X, Y, W) = 1$ je možné odebrat, ale pak zahrneme také parametrizace s base points – matice rezultantu může být singulární a je nutné použít metodu RSC, tzn. najít maximální minor.

Stěžejním bodem metody je volba interpolačního prostoru, tzn. odhad maximálních stupňů v proměnných x a y hledaného implicitního vyjádření. Pro účely odhadu těchto stupňů zkrátíme společné faktory (pokud existují) ve složkách parametrizace $\mathbf{C}(t)$, tzn. obecně dostáváme parametrizace $\mathbf{C}(t) = (X_1(t)/W_1(t), Y_2(t)/W_2(t))$, kde $\text{GCD}(X_1, W_1) = \text{GCD}(Y_2, W_2) = 1$.

Věta 8.3.1 *Nechť $\mathbf{C}(t) = (X_1(t)/W_1(t), Y_2(t)/W_2(t))$ je proper racionální parametrizace ireducibilní křivky C , pro kterou platí $\text{GCD}(X_1, W_1) = \text{GCD}(Y_2, W_2) = 1$ a nechť $F(x, y)$ je implicitní vyjádření křivky C . Potom*

$$\begin{aligned} m &= \max\{\deg_t(X_1), \deg_t(W_1)\} = \deg_y(F) \\ n &= \max\{\deg_t(Y_2), \deg_t(W_2)\} = \deg_x(F). \end{aligned}$$

Důkaz: Viz [18]. □

Věta nám tedy říká, že polynom $F(x, y)$ představující implicitní vyjádření křivky C patří do prostoru polynomů $\Pi_{n,m}(x, y)$.

Polynom $F(x, y)$ je možné najít pomocí klasické Lagrangeovy interpolace. Pro interpolační uzly $(x_i, y_j), i = 0, \dots, n, j = 0, \dots, m$ a interpolovaná data $f_{ij} \in K, i = 0, \dots, n, j = 0, \dots, m$ chceme najít polynom

$$F(x, y) = \sum_{(i,j) \in I} c_{ij} x^i y^j \in \Pi_{n,m}(x, y), \quad I = \{(i, j) | i = 0, \dots, n, j = 0, \dots, m\}$$

takový, že

$$F(x_i, y_j) = f_{ij}, \forall (i, j) \in I. \quad (8.25)$$

Interpolační podmínky (8.25) je možné zapsat jako soustavu lineárních rovnic

$$\mathbf{A}\mathbf{c} = \mathbf{f}, \quad (8.26)$$

kde matice koeficientů $\mathbf{A}$ je dána Kroneckerovým součinem³ $\mathbf{A} = \mathbf{V}_x \otimes \mathbf{V}_y$, kde $\mathbf{V}_x, \mathbf{V}_y$ jsou Vandermondeovy matice

$$\mathbf{V}_x = \begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix}, \mathbf{V}_y = \begin{pmatrix} 1 & y_0 & y_0^2 & \dots & y_0^m \\ 1 & y_1 & y_1^2 & \dots & y_1^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & y_m & y_m^2 & \dots & y_m^m \end{pmatrix},$$

$\mathbf{c}$ je sloupcový vektor neznámých koeficientů implicitního vyjádření $F(x, y)$ a $\mathbf{f}$ je sloupcový vektor obsahující interpolovaná data.

Interpolační uzly (x_i, y_j) se obvykle volí $x_i = i, i = 0, \dots, n$ a $y_j = j, j = 0, \dots, m$, což také zaručuje regularitu matice $\mathbf{A}$. Interpolovaná data f_{ij} odpovídají hodnotám rezultantu $F(i, j)$ v daném interpolačním uzlu (i, j) . Pokud tedy je $\mathbf{M}(x, y)$ symbolická Bézoutova matice rezultantu a $\mathbf{M}_{ij} = \mathbf{M}(i, j)$, potom $f_{ij} = \det \mathbf{M}_{ij}$.

Speciální strukturu matice $\mathbf{A}$ je možné využít k rychlejšímu řešení soustavy (8.26). Využijeme-li jednu z vlastností Kroneckerova součinu, uvedenou ve Větě 8.3.2, řešení soustavy lineárních rovnic (8.26) s maticí koeficientů $\mathbf{A} = \mathbf{V}_x \otimes \mathbf{V}_y$ může být převedeno na řešení $n + 1$ soustav se stejnou maticí soustavy $\mathbf{V}_y$ s následným řešením $m + 1$ soustav se stejnou maticí soustavy $\mathbf{V}_x$.

Definice 8.3.1 Operátor **vec** vytváří sloupcový vektor z dané matice $\mathbf{A}$ skládáním sloupců matice $\mathbf{A} = [\mathbf{a}_1 \ \mathbf{a}_2 \ \dots \ \mathbf{a}_n]$ pod sebe, tj.

$$\mathbf{vec}(\mathbf{A}) = \begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_n \end{bmatrix}$$

³Kroneckerův součin $\mathbf{B} \otimes \mathbf{D}$ je definován pomocí bloků, tzn. výsledná matice je složena z bloků $(b_{kl}\mathbf{D})$, kde $\mathbf{B} = (b_{kl})$.

Věta 8.3.2

$$\text{vec}(\mathbf{AXB}) = (\mathbf{B}^T \otimes \mathbf{A})\text{vec}(\mathbf{X}). \quad (8.27)$$

Důkaz: Necht' $\mathbf{B} = [\mathbf{b}_1 \ \mathbf{b}_2 \ \dots \ \mathbf{b}_n]$ je matice rozměru $m \times n$ a $\mathbf{X} = [\mathbf{x}_1 \ \mathbf{x}_2 \ \dots \ \mathbf{x}_m]$. Potom, k -tý sloupec matice $\mathbf{AXB}$ je

$$\begin{aligned} (\mathbf{AXB})_{:,k} &= \mathbf{AXb}_k = \mathbf{A} \sum_{i=1}^m x_i b_{i,k} = [b_{1,k}\mathbf{A} \ b_{2,k}\mathbf{A} \ \dots \ b_{m,k}\mathbf{A}] \underbrace{\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_m \end{bmatrix}}_{\text{vec}(\mathbf{X})} = \\ &= \underbrace{[b_{1,k}, b_{2,k}, \dots, b_{m,k}]_{\mathbf{b}_k^T}}_{\mathbf{b}_k^T} \otimes \mathbf{A} \text{vec}(\mathbf{X}). \end{aligned}$$

Skládáním sloupců pod sebe dostáváme

$$\text{vec}(\mathbf{AXB}) = \begin{bmatrix} (\mathbf{AXB})_{:,1} \\ (\mathbf{AXB})_{:,2} \\ \vdots \\ (\mathbf{AXB})_{:,n} \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1^T \otimes \mathbf{A} \\ \mathbf{b}_2^T \otimes \mathbf{A} \\ \vdots \\ \mathbf{b}_n^T \otimes \mathbf{A} \end{bmatrix} \text{vec}(\mathbf{X}) = (\mathbf{B}^T \otimes \mathbf{A})\text{vec}(\mathbf{X}).$$

□

Položíme-li tedy $\mathbf{A} = \mathbf{V}_y$, $\mathbf{B} = \mathbf{V}_x^T$, $\mathbf{X} = \mathbf{C}$, kde

$$\mathbf{C} = \begin{bmatrix} c_{00} & \dots & c_{0n} \\ \dots & & \dots \\ c_{m0} & \dots & c_{mn} \end{bmatrix}, \quad \mathbf{c} = \text{vec}(\mathbf{C})$$

a podobně

$$\mathbf{F} = \begin{bmatrix} f_{00} & \dots & f_{0n} \\ \dots & & \dots \\ f_{m0} & \dots & f_{mn} \end{bmatrix}, \quad \mathbf{f} = \text{vec}(\mathbf{F}),$$

potom dosazením do (8.27) dostáváme

$$\text{vec}(\mathbf{V}_y \mathbf{C} \mathbf{V}_x^T) = \underbrace{(\mathbf{V}_x \otimes \mathbf{V}_y)}_{\mathbf{A}} \mathbf{c} = \mathbf{f} = \text{vec}(\mathbf{F}).$$

Odtud vyplývá, že

$$\text{vec}(\mathbf{V}_y \mathbf{C} \mathbf{V}_x^T) = \text{vec}(\mathbf{F}) \implies \mathbf{V}_y \mathbf{C} \mathbf{V}_x^T = \mathbf{F}.$$

Označíme-li $\mathbf{C} \mathbf{V}_x^T = \mathbf{W}$, potom $\mathbf{V}_y \mathbf{W} = \mathbf{F}$. Shrnutí – místo řešení soustavy rovnic (8.26) s maticí soustavy rozměru $(m+1)(n+1)$ je možné řešit $n+1$ soustav rovnic

$$\mathbf{V}_y \mathbf{W} = \mathbf{F}$$

a následně $m + 1$ soustav rovnic

$$\mathbf{V}_x \mathbf{C}^T = \mathbf{W}^T.$$

Jelikož $\mathbf{V}_x$ a $\mathbf{V}_y$ jsou Vandermondeovy matice, je možné využít speciálních metod pro řešení soustav lineárních rovnic s maticí soustavy tohoto typu. Podrobněji viz [18].

Metodu je možné poměrně přímo zobecnit pro racionální plochy. Necht

$$\mathbf{S}(u, v) = \left(\frac{X(u, v)}{W(u, v)}, \frac{Y(u, v)}{W(u, v)}, \frac{Z(u, v)}{W(u, v)} \right)$$

je racionální parametrizace plochy S . Odstraněním jmenovatelů ve složkách parametrizace dostáváme polynomy

$$X(u, v) - xW(u, v), \quad Y(u, v) - yW(u, v), \quad Z(u, v) - zW(u, v) \quad (8.28)$$

s celkovými stupni d_0, d_1, d_2 .

První krokem je opět určení interpolačního prostoru $\Pi_{l,m,n}(x, y, z)$ tak, že Macaulayho rezultant $R(x, y, z)$ pro polynomy (8.28) vzhledem k u, v je z $\Pi_{l,m,n}(x, y, z)$. Platí (viz [19]), že

$$\begin{aligned} l = \deg_x(R(x, y, z)) &\leq d_1 d_2, \\ m = \deg_y(R(x, y, z)) &\leq d_0 d_2, \\ n = \deg_z(R(x, y, z)) &\leq d_0 d_1. \end{aligned}$$

Dále následuje opět standardní interpolace pro interpolační uzly $(x_i, y_j, z_k), i = 0, \dots, l, j = 0, \dots, m, k = 0, \dots, n$ a interpolovaná data $r_{ijk}, i = 0, \dots, l, j = 0, \dots, m, k = 0, \dots, n$ v interpolačním prostoru $\Pi_{l,m,n}(x, y, z)$ pro nalezení rezultantu $R(x, y, z)$. To vede na řešení soustavy lineárních rovnic

$$\mathbf{A} \mathbf{c} = \mathbf{r}, \quad (8.29)$$

kde matice soustavy je dána Kroneckerovým součinem $(\mathbf{V}_x \otimes \mathbf{V}_y) \otimes \mathbf{V}_z$ a $\mathbf{V}_x, \mathbf{V}_y, \mathbf{V}_z$ jsou Vandermondeovy matice, $\mathbf{c}$ je sloupcový vektor neznámých koeficientů implicitního vyjádření $R(x, y, z)$ a $\mathbf{r}$ je sloupcový vektor obsahující interpolovaná data.

Interpolační uzly se obvykle volí jako mřížkové body, tj. $(x_i, y_j, z_k) = (i, j, k), i = 0, \dots, l, j = 0, \dots, m, k = 0, \dots, n$. Interpolovaná data r_{ijk} odpovídají hodnotám implicitního vyjádření (rezultant) $R(i, j, k)$ v mřížkových bodech (i, j, k) . Jestliže je tedy $\mathbf{M}(x, y, z)$ symbolická Macaulayho matice (nebo libovolná jiná symbolická matice rezultantu) získaná eliminací parametrů u, v z rovnic (8.28) a $\mathbf{M}_{ijk} = \mathbf{M}(i, j, k)$, potom $r_{ijk} = \det \mathbf{M}_{ijk}$.

I v tomto případě je možné využít speciální strukturu matice $\mathbf{A}$ pro rychlejší řešení soustavy (8.29). Jelikož matice $\mathbf{A}$ je Kroneckerovým součinem matic $\mathbf{V}_x, \mathbf{V}_y$ a $\mathbf{V}_z$, řešení soustavy lineárních rovnic s maticí soustavy $\mathbf{A}$ rozměru $(l + 1)(m + 1)(n + 1)$ může být převedeno na postupné řešení $(n + 1)$ soustav rovnic s maticí soustavy $\mathbf{V}_z$, následované řešením $(m + 1)$ soustav rovnic s maticí soustavy $\mathbf{V}_y$ a na závěr řešením $(l + 1)$ soustav rovnic s maticí soustavy $\mathbf{V}_x$. Více o této metodě je možné najít v [19].

8.4 Přímá metoda implicitizace

Jednoduchá a přímočará metoda implicitizace křivek a ploch daných racionální parametrizací byla prezentována nedávno v [31]. Metoda je založena na odhadu stupně hledaného implicitního vyjádření s následným řešením soustavy lineární rovnic pro neznámé koeficienty tohoto implicitního vyjádření.

Metoda je zavedena pro racionální plochy, ale podobně funguje i pro racionální křivky. Nechť

$$\mathbf{S}(u, v) = \left(\frac{X(u, v)}{W(u, v)}, \frac{Y(u, v)}{W(u, v)}, \frac{Z(u, v)}{W(u, v)} \right) \quad (8.30)$$

je racionální parametrizace plochy S . Hlavním úkolem je nalezení polynomu $F(x, y, z)$ tak, že

$$F(x, y, z) = F\left(\frac{X(u, v)}{W(u, v)}, \frac{Y(u, v)}{W(u, v)}, \frac{Z(u, v)}{W(u, v)}\right) \equiv 0.$$

Nejprve je tedy potřeba odhadnout stupeň hledaného polynomu F , a to pomocí:

1. určení celkového stupně polynomu F , nebo
2. určení stupňů polynomu F v jednotlivých proměnných x, y, z .

V případě, že je dán celkový stupeň polynomu F , můžeme F zapsat ve tvaru

$$F = \sum_{\substack{i \geq 0, j \geq 0, k \geq 0 \\ i+j+k \leq n}} a_{ijk} x^i y^j z^k, \quad \sum_{\substack{i \geq 0, j \geq 0, k \geq 0 \\ i+j+k=n}} a_{ijk}^2 > 0, \quad (8.31)$$

kde koeficienty a_{ijk} jsou neznámé. Dosazením (8.30) do (8.31) dostáváme

$$\sum_{\substack{i \geq 0, j \geq 0, k \geq 0 \\ i+j+k \leq n}} a_{ijk} \frac{X^i Y^j Z^k}{W^i W^j W^k} = \frac{g}{h} = 0. \quad (8.32)$$

Jelikož g musí být identicky rovno nule, koeficienty u všech monomů $u^\alpha v^\beta$ v g se musí rovnat nule. Každý z těchto koeficientů je polynomem v proměnných a_{ijk} a představuje jednu z rovnic soustavy lineárních rovnic, jejímž řešením najdeme neznámé koeficienty implicitního vyjádření F . Plocha (8.30) má implicitní vyjádření stupně $\leq n$ právě tehdy, když tato lineární soustava má netriviální řešení $\bar{a}_{ijk}$. Implicitní vyjádření racionální plochy (8.30) potom dostaneme jako nekonstantní faktor $F|_{a_{ijk}=\bar{a}_{ijk}}$ v proměnných x, y, z .

Pokud jsou dány stupně polynomu F v jednotlivých proměnných x, y, z (např. pomocí vztahů (8.29), můžeme F zapsat ve tvaru

$$F = \sum_{i=0}^{n_x} \sum_{j=0}^{n_y} \sum_{k=0}^{n_z} a_{ijk} x^i y^j z^k. \quad (8.33)$$

Dále metoda pokračuje analogicky jako v případě použití celkového stupně. Podrobněji viz také [31].

Literatura

- [1] Alonso, C., Gutierrez, J., Recio, T.: *An Implicitization Algorithm with Fewer Variables*. Computer Aided Geometric Design, Vol. 12, Issue 3, pp. 251-258, Elsevier, 1995.
- [2] Becker, T., Weispfenning, V.: *Gröbner bases - A Computational Approach to Commutative Algebra*. Graduate Text in Mathematics. Springer-Verlag, New York, 1993.
- [3] Cox, D., Little, J., O'Shea, D.: *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
- [4] de Berg, M., van Kreveld, M., Overmars, M., Schwarzkopf, O.: *Computational geometry. Algorithms and Applications*, Springer-Verlag, Berlin, 2000.
- [5] Faugère, J.-C.: *A New Efficient Algorithm for Computing Gröbner Bases (F_4)*. Journal of Pure and Applied Algebra, Vol. 139, Issue 1-3, pp. 61-88, Elsevier, 1999.
- [6] Chionh, E., Zhang M., Goldman R.: *Implicitization Matrices in the Style of Sylvester with the Order of Bezout*. In Proceedings of Curve & Surface Design: International Conference Saint-Malo, pp. 17-26, 2000.
- [7] Chionh, E., Zhang, M., Goldman R.: *Efficient Implicitization of Rational Surfaces by Moving Planes*. In Proceedings of ASCM 2000, pp. 142-151, 2000.
- [8] Chionh E., Zhang M., Goldman, R.: *Fast Computation of the Bezout and Dixon Resultant Matrices*. Journal of Symbolic Computation, Vol. 33, Issue 1, pp. 13-29, 2002.
- [9] Chtcherba, A.-D.: *A new Sylvester-type Resultant Method based on the Dixon-Bézout Formulation*. Dissertation. Department of Computer Science, University of New Mexico, 2003.
- [10] Ježek, F.: *Datové struktury a algoritmy počítačové grafiky pro konstruování pomocí počítače*. Kandidátská disertační práce. Plzeň, 1985.
- [11] Kapur, D., Saxena, T., Yang, L.: *Algebraic and Geometric Reasoning Using Dixon Resultants*. In Proceedings of International Symposium on Symbolic and Algebraic Computation 1994 (ISSAC '94), Oxford, United Kingdom, pp. 99-107, 1994.

- [12] Kapur, D., Saxena, T.: *Comparison of Various Multivariate Resultant Formulations*. In Proceedings of International Symposium on Symbolic and Algebraic Computation 1995 (ISSAC '95), Montreal, Canada, pp. 187-194, 1995.
- [13] Kapur, D., Saxena, T.: *Sparsity Considerations in Dixon Resultants*. In Proceedings of 28th Annual ACM Symposium on Theory of Computing (STOC '96), Philadelphia, USA, pp. 184-191, 1996.
- [14] Kuroš, A. G.: *Kapitoly z obecné algebry*. Academia, 1977.
- [15] Manocha D., Canny, F.: *Implicit Representation of Rational Parametric Surfaces*. Journal of Symbolic Computation, Vol. 13, Issue 5, pp. 485-510, Academic Press, 1992.
- [16] Manocha, D., Canny, F.: *Algorithm for Implicitizing Rational Parametric Surfaces*. Computer Aided Geometric Design, Vol. 9, Issue 1, pp. 25-51, Elsevier, 1992.
- [17] Manocha, D.: *Efficient Algorithms for Multipolynomial Resultant*. The Computer Journal (Special Issue on Quantifier Elimination), Vol. 36, Issue 5, pp. 485-496, Oxford University Press, 1993.
- [18] Marco, A., Martínez, J.J.: *Using Polynomial Interpolation for Implicitizing Algebraic Curves*. Computer Aided Geometric Design, Vol. 18, Issue 4, pp. 309-319, Elsevier, 2001.
- [19] Marco, M., Martínez, J.J.: *Implicitization of Rational Surfaces by Means of Polynomial Interpolation*. Computer Aided Geometric Design, Vol. 19, Issue 5, pp. 327-344, Elsevier, 2002.
- [20] Míka, S.: *Numerické metody*. Lineární algebra. Vydavatelství ZČU, Plzeň, 1996.
- [21] Piegl, L., Tiller, W.: *The NURBS Book*. Springer, Berlin, 1997.
- [22] Ralston, A.: *Základy numerické matematiky*. Academia, Praha, 1973.
- [23] Rosický, J.: *Algebra. Grupy a okruhy*. Vydavatelství MU, Brno, 2000.
- [24] Saxena T.: *Efficient Variable Elimination using Resultants*. Doctoral Thesis, Department of Computer Science, State University of New York at Albany, 1996.
- [25] Sederberg, T., Chen, F.: *Implicitization using Moving Curves and Surfaces*. In Computer Graphics Proceedings, Annual Conference Series, pp. 301-308, ACM SIGGRAPH, 1995.
- [26] Sederberg, T., Goldman, R., Du, H.: *Implicitizing Rational Curves by the Method of Moving Algebraic Curves*. Journal of Symbolic Computation, Vol. 23, Issue 2-3, pp. 153-175, Academic Press, 1997.

- [27] Slovák, J.: *Geometrické algoritmy II. - Polynomiální objekty*. Pomocný studijní text. Brno, 1995.
- [28] Tran, Q.-N.: *A Fast Algorithm for Gröbner Basis Conversion and its Applications*. Journal of Symbolic Computation, Vol. 30, Issue 4, pp. 451-467, Academic Press, 2000.
- [29] Von zur Gathen, J., Gerhard, J.: *Modern Computer Algebra*. Cambridge University Press, 1999.
- [30] Wang, D.: *Automated Deduction in Geometry*. International Workshop on Automated Deduction in Geometry, Toulouse, France, September 1996, Selected Papers. Springer-Verlag, Berlin, 1997.
- [31] Wang, D.: *A simple method for implicitizing rational curves and surfaces*. Journal of Symbolic Computation, Vol. 38, Issue 1, pp. 899-914, Elsevier, 2004.
- [32] Winkler, F.: *Polynomial Algorithms in Computer Algebra*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Wien, 1996.