SMT 18.10.2018

Algebry jsou dány nosnou množinou a operacemi nad touto množinou

Tyto operace můžou být různých arit:

- nulární, unární, binární, obecně n-ární

Příklady typů algebry:

- $(A, \circ)$, kde $\circ$ je binární operace na A je algebra typu (2)
- $(A, \circ, {}^{-1}, 1)$ je typu $(2, 1, 0)$

Základní algebry s jednou bin. operací

$(A, \circ)$ grupoid — Např. $(\mathbb{N}, +)$, $(\mathbb{N}, -)$ není grupoid

$5 - 10 \notin \mathbb{N}$

$\downarrow$

$(A, \circ)$ pologrupa - $\circ$ je asociativní operace — $\forall x, y, z \in A$:

$(x \circ y) \circ z = x \circ (y \circ z)$

$\downarrow$

$(A, \circ, 1)$ monoid - 1 je neutrální prvek operace $\circ$

$e \in A$ je neutrální prvek, pokud platí $\forall a \in A$:

$$\left.\begin{array}{ll} e \circ a = a & \text{.. levý neutrální prvek} \\ a \circ e = a & \text{.. pravý N.P} \end{array}\right\} \text{neutrální prvek}$$

Př. $(\Sigma^*, \circ, \varepsilon)$

$(A, \circ, 1, ^{-1})$ grupa $\quad \forall x \in A: x \circ x^{-1} = 1 \wedge x^{-1} \circ x = 1$

tj. ke každému prvku existuje jeden inverzní prvek

y je inverzní prvek k x pokud platí:

$$\left.\begin{array}{ll} x \cdot y = e & \text{... pravý inverzní prvek} \\ y \cdot x = e & \text{.. levý inverzní prvek} \end{array}\right\} \text{inverzní prvek}$$

Př. $(\mathbb{R}, +, 0, -)$ $\quad (\mathbb{Z}_m, +, 0, -)$

$\downarrow$

$(A, \circ, 1, ^{-1})$ komutativní (abelovská) grupa - $\circ$ je komutativní

$\forall x, y \in A: x \circ y = y \circ x$

Př.1/ Algebra $(A, \circ)$, $A = \{a, b, c\}$ a $\circ$ je dána pomocí Cayleyovy tabulky:

$\circ$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

Co je $(A, \circ)$ za algebru?

- asociativita? musí platit $\forall x,y,z \in A: (x \circ y) \circ z = x \circ (y \circ z)$

$$\underbrace{(a \circ \_) \circ \_}_{\text{cokoliv}} = a = a \circ \underbrace{(\_ \circ \_)}_{\text{cokoliv}}$$

$$(b \circ \_) \circ \_ = b = b \circ (\_ \circ \_)$$

$$(c \circ \_) \circ \_ = c = c \circ (\_ \circ \_)$$

Operace je asociativní

- neutrální prvek: aby existoval neutrální prvek, musel by existovat sloupec a odpovídající řádek obsahující stejné prvky jako v hlavičce tabulky.

⟶ existují pouze pravé neutrální prvky $\forall x \in A: x \circ a = x$

⟶ neexistuje neutrální prvek

Je to pologrupa

Př. 2/ Algebra $(A, \circ)$, $A = \{a, b, c\}$, bin. operace $\circ$, která je definována:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Co je $(A, \circ)$ za algebru?

- komutativita – tabulka je symetrická podle diagonály
- neutrální prvek – 1. řádek a 1. sloupec obsahuje stejné prvky jako v hlavičce ⇒ neutrální prvek = a
- asociativita:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

tabulka je stejná (až na přeznačení prvků) s $(\mathbb{Z}_3, +)$

⇒ operace $\circ$ je asociativní

- inverzní prvky
  $a \mapsto a$
  $b \mapsto c$
  $c \mapsto b$ ✓

$(A, \circ)$ je abelovská grupa.

Pozn. Další vlastnosti operací:

- ∘ je operace s dělením, pokud platí: $\forall a,b \in A \; \exists x,y \in A$:

$$\left.\begin{array}{ll} a \circ x = b & \text{levý zákon o dělení} \\ y \circ a = b & \text{pravý zákon o dělení} \end{array}\right\} \text{operace s dělením}$$

Je operace z Př 1 operace s dělením?

→ všechny sloupce a řádky by musely obsahovat všechny prvky alespoň jednou – první řádek neobsahuje všechny prvky = není to operace s dělením

- ∘ je operace s krácením, pokud platí $\forall a, x_1, x_2, y_1, y_2 \in A$:

$$\left.\begin{array}{ll} a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2 & \text{.. levý ZK} \\ y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2 & \text{.. pravý ZK} \end{array}\right\} \text{operace s krácením}$$

Je operace z Př 1 operace s krácením?

→ všechny sloupce a řádky by musely obsahovat každý prvek max. jednou ⇒ není to op. s krácením

Pozn.) Pro konečné algebry jsou zákony o dělení ~~z~~ ekvivalentní zákonům o krácení.

Př 3) Algebra $(\mathbb{N}, \cdot)$ platí zákon o krácení, ale neplatí zákon o dělení
(např. pro 2,3 neexistuje $x \in \mathbb{N}: 2 \cdot x = 3$)

Př 4) Máme strukturu $(A, \circ)$, kde $A = \{(x,y) \mid x, y \in \mathbb{Z}\}$ a operace $\circ$ je definována následovně $(x,y) \circ (s,t) = (x+s, y+t)$

Co je to za algebru?

- grupoid: $\forall x, y, s, t \in \mathbb{Z}$ platí $(x,y) \circ (s,t) = (x+s, y+t)$ a
  $x+s \in \mathbb{Z}$ a $y+t \in \mathbb{Z}$, $\circ$ je uzavřena na A
  $\rightarrow$ je to grupoid

- pologrupa: platí asoc. zákon?
  $[(x,y) \circ (s,t)] \circ (u,v) = (x+s, y+t) \circ (u,v) = (x+s+u, y+t+v)$
  $(x,y) \circ [(s,t) \circ (u,v)] = (x,y) \circ (s+u, t+v) = (x+s+u, y+t+v)$
  $\rightarrow$ je to pologrupa

- monoid : neutrálny prvek ?

$$(x,y) \circ (0,0) = (x,y) \qquad (0,0) \in \mathbb{Z} \times \mathbb{Z}$$

$$(0,0) \circ (x,y) = (x,y)$$

$\rightarrow$ je to monoid

- grupa : inverzní prvky ?

$$(x,y) \circ (u,v) = (0,0)$$

$$(x+u, y+v) = (0,0) \implies \begin{matrix} u = -x \in \mathbb{Z} \\ v = -y \in \mathbb{Z} \end{matrix}$$

inverzní prvek k (x,y) je $(-x,-y)$

$\rightarrow$ je to grupa

- komutativita

$$(x,y) \circ (s,t) = (x+s, y+t) = (s+x, t+y) = (s,t) \circ (x,y)$$

sčítání je komutativní

$\rightarrow$ je to abelovská grupa

Př. 5)

Máme množinu $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \begin{array}{l} a \neq 0 \\ b \neq 0, \ a,b \in \mathbb{R} \end{array} \right\}$ s operací násobení matic.

$(A, \cdot)$ grupa?

- grupoid

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in A$$

- asociativita:

$$\left[\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right] \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} ace & 0 \\ 0 & bdf \end{pmatrix}$$

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \left[\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix}\right] = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} ce & 0 \\ 0 & df \end{pmatrix} = \begin{pmatrix} ace & 0 \\ 0 & bdf \end{pmatrix}$$

$\rightarrow$ je to asociativní $\Rightarrow$ pologrupa

- neutrální prvek: jednotková matice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$

- inverzní prvky: $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} ax & 0 \\ 0 & by \end{pmatrix} \Rightarrow \begin{matrix} x = \frac{1}{a} \\ y = \frac{1}{b} \end{matrix}$$

, vzhledem k tomu že $a, b \neq 0$, tak

$$\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix} \in A \longrightarrow \text{je to grupa}$$

<u>Př 6</u> Mějme grupu $A = (\mathbb{R}, \cdot, 1, {}^{-1})$. Jak vypadá podalgebra B generovaná množinou $\{\sqrt[3]{2}\}$?

Nejmenší množina, která obsahuje $\sqrt[3]{2}$ a je uzavřena na operace $\cdot, {}^{-1}, 1$:

Množina $\{\sqrt[3]{2}^k \mid k \in \mathbb{N}\}$ je uzavřena na $\cdot, 1$. Musíme rozšířit, aby byla uzavřena i na $^{-1}$ $\longrightarrow \{\sqrt[3]{2}^k \mid k \in \mathbb{Z}\}$ (inv. prvek k $\sqrt[3]{2}^k$ je $\sqrt[3]{2}^{-k}$)

$$B = (\{\sqrt[3]{2}^k \mid k \in \mathbb{Z}\}, \cdot, 1, {}^{-1})$$

Základní algebry se 2 bin. operacemi

$(A, +, 0, -, \cdot)$ je okruh, pokud platí

$(A, +, 0, -)$ je abelovská grupa

$(A, \cdot)$ je pologrupa

$\cdot$ je distributivní nad $+$ t.j. $\forall a,b,c \in A$:

$a \cdot (b+c) = a \cdot b + a c$

$(b+c) \cdot a = b a + c a$

$(A, +, 0, -, \cdot)$ je komutativní okruh, pokud

$\cdot$ je komutativní operace

$(A, +, 0, -, \cdot, 1)$ je okruh s jednotkovým prvkem, pokud

1 je neutrální prvek vzhledem k $\cdot$

$(A, +, 0, -, \cdot, 1)$ kom. okruh s jedn. prvkem

$(A, +, 0, -, \cdot, 1)$ je obor integrity, pokud

$0 \neq 1$ (je netriviální)

$\forall x, y \in A$: $x \neq 0 \wedge y \neq 0 \Rightarrow x \cdot y \neq 0$

$(A, +, 0, -, \cdot, 1)$ je těleso, pokud

$0 \neq 1$ $(A \setminus \{0\}, \cdot)$ je grupa

$(A, +, 0, -, \cdot, 1)$ je pole, pokud $\cdot$ je kom.

Příklad dělitelů nuly: $(\mathbb{Z}_6, +, \cdot)$

$$[2]\cdot[3] = [6] = [0] \text{ přitom } [2] \neq [0] \wedge [3] \neq [0]$$

$(\mathbb{Z}_p, +, \cdot)$ je obor integrity, p je prvočíslo

Př. 7) Algebra $(A, \oplus, \odot)$, kde $A = \mathbb{Q} \times \mathbb{Q}$ a operace jsou dány následovně:

$$(x,y) \oplus (s,t) = (x+s, y+t)$$
$$(x,y) \odot (s,t) = (xs + 2yt, xt + ys)$$

Je $(A, \oplus, \odot)$ obor integrity? $(A, \oplus)$ je komutativní grupa, což bylo dokázáno dříve (zde je to rozšířeno jen na vac. číslo)

• je $(A, \odot)$ pologrupa?

- grupoid $(x,y) \odot (s,t) = (\underbrace{xs + 2yt}_{\in \mathbb{Q}}, \underbrace{xt + ys}_{\in \mathbb{Q}})$ ✓
- asociativita $[(x,y) \odot (s,t)] \odot (u,v) = (xs + 2yt, xt + ys) \odot (u,v)$

$$= (xsu + 2ytu + 2xtv + 2ysv, xsv + 2ytv + xtu + ysu)$$

$$(x,y) \odot [(s,t) \odot (u,v)] = (x,y) \odot (su + 2tv,\ sv + tu) =$$

$$= (xsu + 2xtv + 2ysv + 2ytu,\ xsv + xtu + ysu + 2ytv)$$

$\rightarrow$ $(A, \odot)$ je pologrupa

- je $\odot$ distributivní nad $\oplus$?

$$(x,y) \odot [(s,t) \oplus (u,v)] = (x,y) \odot (s+u, t+v) = (xs + xu + 2yt + 2yv,$$
$$xt + xv + ys + yu)$$

$$[(x,y) \odot (s,t)] \oplus [(x,y) \odot (u,v)] = (xs + 2yt,\ xt + ys) \oplus (xu + 2yv,\ xv + yu)$$
$$= (xs + 2yt + xu + 2yv,\ xt + ys + xv + yu) \checkmark$$

$\rightarrow$ levý distr. zákon platí, pravý se ukáže analogicky

$\Rightarrow$ je to okruh

- komutativní operace $\odot$?

$$(x,y)\odot(s,t) = (xs+2yt,\ xt+ys) = (sx+2ty,\ tx+sy) = (s,t)\odot(x,y)\ \checkmark$$

$\longrightarrow$ komutativní okruh

- má $(A,\odot)$ neutrální prvek?

$$(x,y)\odot(1,0) = (x\cdot 1+2y\cdot 0,\ x\cdot 0+y\cdot 1) = (x,y)$$

- Je $(A,\oplus,\odot)$ obor integrity?
  - netriviální okruh, tj. $(0,0)\neq(1,0)$
  - má dělitele nuly? $\longrightarrow$ muselo by platit $(x,y)\odot(s,t)=(0,0)$ $\wedge\ (x,y)\neq(0,0)\ \wedge\ (s,t)\neq(0,0)$

$$(x,y)\odot(s,t) = (0,0)$$
$$(xs+2yt,\ xt+ys) = (0,0) \qquad xs+2yt=0 \quad \wedge \quad xt+ys=0$$

- pokud $x=0$, potom $y=0$ nebo $t=0 \wedge s=0$ $\Rightarrow$ není splněna podmínka

- podobně pro y, s, t

Máme rovnice $xs+2yt=0 \wedge xt+ys=0$

$$\Downarrow$$

$$x = -\frac{2yt}{s}$$

Dosadíme

$$-\frac{2yt}{s}\cdot t + ys = 0$$

$$ys = \frac{2yt^2}{s}$$

$$ys^2 = 2yt^2$$

$$s^2 = 2t^2$$

$$\frac{s}{t} = \pm\sqrt{2}$$

$\frac{s}{t} \in \mathbb{Q}$

$\sqrt{2}$ není racionální číslo

$\Rightarrow$ nejsou zde dělitelé nuly

$\Rightarrow$ je to obor integrity

Aplikace: exponentiation by squaring

→ chceme spočítat 3^4 $\quad ((3\cdot 3)\cdot 3)\cdot 3$ $\quad$ 3 násobení

s využitím asociativity $(3\cdot 3)\cdot(3\cdot 3)$ $\quad$ 2 násobení

→ pro výpočet a^n je potřeba $O(\log_2 n)$ násobení

Tento způsob lze zobecnit na univerzální algebry

- násobení matic nad libovolným polookruhem s jed. prvkem $\mathcal{R} = (R, \oplus, 0, \otimes, 1)$

$(R, \oplus, 0, \otimes, 1)$ je <u>polookruh</u> s jednotkovým prvkem, pokud platí

$(R, \oplus, 0)$ je komutativní monoid

$(R, \otimes, 1)$ je monoid

$\otimes$ je distributivní nad $\oplus$

$A \otimes B$

matice nad $\mathcal{R}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} (a\otimes e)\oplus(b\otimes g) & (a\otimes f)\oplus(b\otimes h) \\ (c\otimes e)\oplus(d\otimes g) & (c\otimes f)\oplus(d\otimes h) \end{pmatrix}$$

$\cdot \rightsquigarrow \otimes$

$+ \rightsquigarrow \oplus$

Je násobení nad $\mathcal{R}$ asociativní?

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \otimes \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} ae \oplus bg & af \oplus bh \\ ce \oplus dg & cf \oplus dh \end{pmatrix} \otimes \begin{pmatrix} i & j \\ k & l \end{pmatrix}$$

$$= \begin{pmatrix} (ae \oplus bg)i \oplus (af \oplus bh)k & (ae \oplus bg)j \oplus (af \oplus bh)l \\ (ce \oplus dg)i \oplus (cf \oplus dh)\cdot k & (ce \oplus dg)j \oplus (cf \oplus dh)l \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} \otimes \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} ei \oplus fk & ej \oplus fl \\ gi \oplus hk & gj \oplus hl \end{pmatrix}$$

$$= \begin{pmatrix} a(ei \oplus fk) \oplus b(gi \oplus hk) & \dots \\ \dots & \dots \end{pmatrix}$$

Porovnáme prvky $[1,1]$:

$$(ae \oplus bg)i \oplus (af \oplus bh)k = aei \oplus bgi \oplus afk \oplus bhk$$

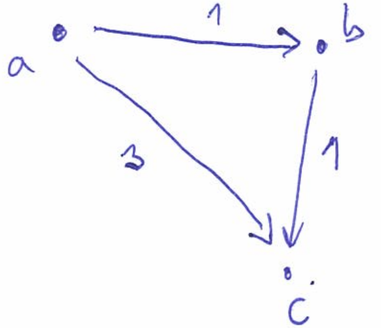
$$a(ei \oplus fk) \oplus b\cdot(gi \oplus hk) = aei \oplus afk \oplus bgi \oplus bhk$$

$\otimes$ distribuuje nad $\oplus$ + komutativita $\oplus$

Pro výpočet A^k nad $\mathbb{R}$ můžeme využít exponation by squaring

$$O(kn^3) \rightsquigarrow O(n^3 \log_2 k)$$

Aplikace: Nejkratší cesty v grafu ze všech do všech (ohodnocený, orientovaný graf)



Tento graf je dán maticí

$$M = \begin{array}{c|ccc} & a & b & c \\ \hline a & 0 & 1 & 3 \\ b & \infty & 0 & 1 \\ c & \infty & \infty & 0 \end{array}$$

→ můžeme ji rozumět jako matici nejkratších cest délky max. 1

Cesty délky max. 2

$$N = \begin{pmatrix} 0 & 1 & 2 \\ \infty & 0 & 1 \\ \infty & \infty & 0 \end{pmatrix}$$

$$N[a,c] = \underset{\Sigma}{\underset{\Downarrow}{\min}} \left(M[a,a] \underset{\cdot}{\underset{\Downarrow}{+}} M[a,c],\ M[a,b] \underset{\cdot}{\underset{\Downarrow}{+}} M[b,c],\ M[\cancel{b}\,a,c] \underset{\cdot}{\underset{\Downarrow}{+}} M[c,c] \right)$$

Násobení matic nad polookruhem $\mathcal{R} = (\mathbb{R} \cup \{\infty\}, \min, \infty, +, 0)$

$$N = M \otimes M$$

Matici nejkratších cest délky max. i dostaneme jako M^i. Matici nejkratších cest dostame jako M^{n-1}, kde n je počet vrcholů v grafu.

Můžeme využít exp. by squaring s čas. složitostí $O(n^3 \log n)$

- Podobně pokud uvažujeme orientovaný graf bez ohodnocení hran, můžeme tranzitivní uzávěr grafu spočítat předchozím algoritmem, jen násobení matic je nad $(\{0,1\}, \max, 0, \min, 1)$.