motivační příklad   exponentiation by squaring

jak rychle spočítat 3^4? $((3.3).3).3$ – 3 násobení

$-\ 3.3$ ($x.x$)   2 násobení

obecně a^n – zhruba $\log_2 n$ násobení. Funguje díky asociativitě násobení.

Jednoduchý princip zobecnitelný metodami univ. algebry pro mnoho různých aplikací.

Např. násobení matic je také asociativní. Ukážeme pro čtvercové matice 2×2, pro jednoduchost:

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} ae+bg, & af+bh \\ ce+dg, & cf+dh \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} (ae+bg)i+(af+bh)k, & (ae+bg)j+(af+bh)l \\ (ce+dg)i+(cf+dh)k, & (ce+dg)j+(cf+dh)l \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} ei+fk, & ej+fl \\ gi+hk, & gj+hl \end{pmatrix} = \begin{pmatrix} a(ei+fk)+b(gi+hk), & \dots \\ \dots, & \dots \end{pmatrix}$$

Porovnáme pozice $[1,1]$:

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

$\parallel$ ← $+$ je komutativní ②   ✓

$$a(ei+fk) + b(gi+hk) = aei + afk + bgi + bhk$$

① $\cdot$ distribuuje nad $+$

V důkazu asociativity násobení matic jsme použili ① a ②, tj. že $(\mathbb{R},+,\cdot)$ je polookruh.

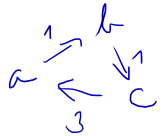
Identifikace kritických vlastností $+, \cdot$ nám umožňuje věci výše zobecnit:

Stejný důkaz by fungoval pro násobení matic vytvořené nad libovolným polookruhem $(A,\oplus,\otimes)$.

Pro každé takové násobení matic proto můžeme použít exponentiation by squaring.

Aplikace: * Nejkratší cesty ze všech do všech

Mějme graf daný maticí M:



	a	b	c
a	0	1	∞
b	∞	0	1
c	3	∞	0

Mějme ji rozumět jako maticí nejkratších cest délky max. 1.

Cesty délky max 2 dostaneme z M, kde ta matice N např. $N[a,c]$ je $\min(0+3, 1+1, 3+1)$.

Podobně jako násobení matic: $\sum(0\cdot 1, 1\cdot 1, 3\cdot 1)$

jen $\sum \to \min$, $\cdot \to +$.

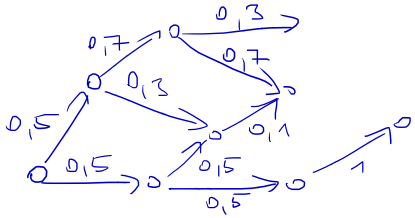
	a	b	c
a	0	1	2
b	∞	0	1
c	3	∞	0

Matice cest délek max i cesty dostaneme jako mocniny M^n matice M, při násobení matic nad polookruhem $(\mathbb{R}, \min, +)$. Nejkratší cesty $= M^n$, kde n je počet vrcholů.

↳ Můžeme použít exp. by squaring, dostáváme algoritmus složitosti $O(n^3 \log n)$.

* Podobně, pokud váhy hran udávají šířku cesty, a chci vědět max. šířku cesty co cestou dostane z a do b. Řešením je stejný algoritmus, jen násobení matic je nad $(\mathbb{R}, \max, \min)$.

* Podobně, pokud váhy udávají pravděpodobnost výběru hrany ve zdrojovém vrcholu, a chci znát pravděpodobnost, s jakými náhodná procházka skončí ve kterém vrcholu. Pracuje se polookruhu $(\mathbb{R}, +, \cdot)$. Zase jde o násobení matic.



Šablony v C++ jako implementace
univ. algebry

kód parametrizovaný algebrou, funguje správně, pokud
má algebra určité vlastnosti

např. tento kód spočítá $base^n$ pokud · je asoc

```
template < class A > // A = (A, ·) kde · je asoc - A je pologrupa
A power (int n, A base)
    if (n ≥ 2) {                    ← celoč. děl.
        A P' = power (n/2, base)
        A P = P'.P'
    }
    if (even(n)) P = P. base
    return P
```

Předchozí algoritmus pro cesty ve všech do všech ve skutečnosti není optimální, má složitost $O(n^3 \log n)$. Floyd-Warshall má složitost $O(n^3)$. Floyd-Warshall vlastně může být chápán jako aplikace jiné obecné metody - Kleeneho algoritmu pro výpočet řešení rovnic nad Kleeneho algebrou - výpočet regulárního výrazu pro konečný automat.

Kleeneho algoritmus původně nad Kleeneho algebrou regulárních množin — $+$ je sjednocení, $\circ$ konkatenace, * iterace.

Floyd-Warshall je Kleeneho algoritmus nad Kleeneho algebrou kde $+$ je minimum, $\circ$ je sčítání a $n^* = -\infty$ pro $n < 0$, jinak $n^* = 0$.

Mnoho dalších aplikací Kleeneho algoritmu.

Dokažte, že prvky dané podgrupy grupy afinních transformací (ve 2D)
- grupa afinních transformací $A = (A, \circ)$ kde
  A jsou matice formy $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ d_x & d_y & 1 \end{bmatrix}$ a ab není násobek cd
  $\circ$ je násobení matic
- posunutí jsou množina transformací P formy $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ d_x & d_y & 1 \end{bmatrix}$
- některé dle

1) $P \subseteq A$
2) $e \in P$
3) $\forall a, b \in P: a \circ b \in P$
4) $\forall a \in P: a^{-1} \in P$

víme že
platí $\forall a, b: \bar{a}^{-1} \circ b \in P$ a 1) a 2),
potom 3) a 4), protože

$\bar{a}^{-1} \circ e = \bar{a}^{-1} \in P$ (4)

$(\bar{a}^{-1})^{-1} \circ b = a \circ b \in P$ (3)

1) - různé ✓

2) $e = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ je neutrální prvek ∘ a je v P ✓

3) a 4) - pomocí $\forall a, b \in P : a^{-1} \circ b \in P$

nechť $a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ dx & dy & 1 \end{bmatrix}$, potom a^{-1} je $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -dx & -dy & 1 \end{bmatrix}$.

nechť $b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ dx' & dy' & 1 \end{bmatrix}$. Potom $a^{-1} \circ b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -dx+dx' & -dy+dy' & 1 \end{bmatrix} \in P$ ✓

$(P, \circ)$ je tedy podgrupou A.

Mějme grupu $A = (\mathbb{R}, *)$. Je podalgebra generovaná $\sqrt[3]{2}$ podgrupou A?

Tzn. je $B = (\{\sqrt[3]{2}^k \mid k \in \mathbb{Z}\}, *)$ podalgebra A?

1) má B neutrální prvek? $\sqrt[3]{2}^0 = 2^{\frac{0}{3}} = 2^0 = 1$ ✓

2) má B inverzní prvky? pro každé k je $2^{\frac{-k}{3}}$ v B a $2^{\frac{k}{3}} * 2^{\frac{-k}{3}} = 1$ ✓

3) je B uzavřená na $*$? $2^{\frac{k}{3}} * 2^{\frac{l}{3}} = 2^{\frac{k+l}{3}} \left(= \sqrt[3]{2}^{k+l}\right)$ ✓

B je tedy podgrupou A.

Permutace je bijekce na množině M do M.

S_n je bijekce na $\langle 1, n \rangle$ do $\langle 1, n \rangle$.

Mějme s a δ z S_9 takové, že

$$s = \{(1,2), (2,4), (3,7), (4,2), (5,1), (6,9), (7,8), (8,6), (9,5)\}$$

a

$$\delta = \{(1,5), (2,2), (3,1), (4,4), (5,3), (6,8), (7,7), (8,6), (9,9)\}$$

a) Rozložte s a δ na součiny nezávislých cyklů.

$s = (1\ 3\ 7\ 8\ 6\ 9\ 5) \circ (2\ 4)$

$\delta = (1\ 5\ 3) \circ (6\ 8)$

$s = (1\,3\,7\,8\,6\,9\,5) \circ (2\,4)$ $\quad t = (1\,5\,3) \circ (6\,8)$

b) spočtěte $s \circ t$ a $t \circ s$

$s \circ t = (1\,3\,7\,8\,6\,9\,5) \circ (2\,4) \circ (1\,5\,3) \circ (6\,8) = (8\,9\,5\,7) \circ (2\,4)$

$t \circ s = (1\,5\,3) \circ (6\,8) \circ (1\,3\,7\,8\,6\,9\,5) \circ (2\,4) = (2\,4) \circ (9\,3\,7\,6)$

Vidíme si, že $s \circ t \neq t \circ s$. Skládání permutací není komutativní.

c) spočtěte $s^{120} \circ t^{-3}$

$s'^{7} = id$, $s''^{2} = id$, tedy $s^{2\cdot 7} \circ s^{14} = id$.

$s^{120} = s^{120 \bmod 14} = s^{8} = s'^{8} \circ s''^{8} = s^{8 \bmod 7} \circ s''^{8 \bmod 2} = s'^{1} \circ s''^{0} = s' = (1\,3\,7\,8\,6\,9\,5)$

$t^{-3} = (t^{-1})^3$, $t^{-1} = (3\,5\,1) \circ (8\,6)$, a $(t^{-1})^3 = (8\,6)$

Tedy $s^{120} \circ t^{-3} = (1\,3\,7\,8\,6\,9\,5) \circ (8\,6) = (8\,9\,5\,1\,3\,7)$

Určete podgrupu S_8 generovanou množinou

$X = \{ \underbrace{(4521)\circ(46315 2)}_{a}, \underbrace{(4521)\circ(456)\circ(13)}_{b} \}$

Jedy, máme najít nejmenší mn. X' : $X \subseteq X'$ a X' je uzavřená na $\circ$

Rozložíme a, b na součin nezáv. cyklů

$a = (463)\circ(125)$, $b = (24)\circ(13)\circ(56)$

Generujeme prvky X' následovně a a b dokud dostáváme nové prvky.

$a \circ a = (436)\circ(152)$

$a \circ b = (145326)$

$(a \circ a)\circ a = id$

$(a \circ b)\circ a = (162354)$

$(a \circ a)\circ b = (162354)$

⋮

Jiný prvek se už při dalších násobeních a a b nedá dostat.

Jedy $X' = \{ a, b, a\circ a, a\circ b, a\circ b\circ a, a\circ a\circ a \}$.

Rešitev je ne sorčin transpozic

$$\sigma = (13) \circ (37) \circ (78) \circ (69) \circ (95) \circ (51) \circ (24)$$

parita permutacije je produkt parit transpozic