CO JE TO DISKRÉTNÍ MATEMATIKA

DEN OTEVŘENÝCH DVEŘÍ (NA MFF UK (PRAHA))

28. 11. 2024

Martin Klazar

Zdroje:

- `https://en.wikipedia.org/wiki/Discrete_mathematics` (i další Wikipedie)
- Vlastní zkušenosti a znalosti

Ale co znamená slovo *diskrétní*? Pochází z francouzského *discret*, a to zase z latinského *discernere*, rozlišovat. V češtině má dva různé významy:

- důvěrný (materiál, informace); ale i člověk schopný uchovat informaci v tajnosti
- nespojitý, přetržitý (ve vědě a technice)

Pozor ale na to, že v angličtině *discrete(ly)* má jen druhý z uvedených významů. První má slovo *discreet(ly)*. Nás bude zajímat jen druhý význam. Etymologii slova *matematika* probírat nebudeme.

- *Disciplíny diskrétní matematiky.* Podle Wikipedie jsou tyto:

1. Teoretická informatika
2. Teorie informace
3. Matematická logika
4. Teorie množin

5. Kombinatorika
6. Teorie grafů
7. Teorie čísel
8. Algebraické struktury
9. Diskrétní analogie spojité matematiky
   (a) Diskrétní (matematická) analýza
   (b) Diskrétní geometrie
   (c) Diskrétní modelování

V praxi je ovšem veškerá matematika diskrétní, že . . .

• *Teoretická informatika.* Teoretické, to jest matematické, pohledy na praktické používání počítačů. Zakladatel? Jistě *Alan M. Turing (1912–1954)*, který jasně řekl, co to je algoritmus. Ještě se k ní vrátíme.

• *Teorie informace.* Kolik informace se dá daným kanálem přenést a co s tím udělá šum? Na to se prvně ptal a dal odpověď *Claude Shannon (1916–2001)*.

• *Matematická logika.* Jak dokázat, že něco nejde dokázat, i když to je pravda? Na to se musí studovat matematická logika. Když ji nechcete studovat, ale jste z Brna, běžte alespoň do Pekařské ulice podívat se na desku *Kurta Gödela (1906–1978)*, který to za nás vyřešil.

• *Teorie množin.* Velitel jednotky vydal rozkaz: vojenský holič XY povinně oholí ty vojáky, co se sami neholí, ale jenom je. XY se ptá: „Můžu se teda sám vůbec voholit?“ Matematická verze: nechť

$$x := \{y \mid y \notin y\}, \text{ je pak } x \in x \text{ nebo ne?}$$

Tento paradox, s nímž přišel v r. 1901 *Bertrand Russel (1872–1970)*, ve své době ukázal, že formalizace teorie množin nebude zase tak jednoduchá věc.

• *Kombinatorika.* Kolem r. 1779 švýcarský matematik *Leonhard Euler (1707–1783)*, působící v Berlíně a Petrohradu, řešil úlohu: Lze rozmístit 36 důstojníků ze 6 jednotek a s 6 hodnostmi, kteří tvoří právě 36 kombinací (jednotka, hodnost), do čtvercové formace 6×6 tak, aby se v žádném sloupci a v žádné řadě neopakovala ani jednotka ani hodnost? V r. 1901 *Gaston Tarry (1843–1913)* dokázal, že nelze.

Kombinatorika je ale mnohem starší. *Blaise Pascal (1623–1662)* vydal spis *Traité du triangle arithmétique* v r. 1665 a tento Δ již dříve popsal v bohužel ztracené knize perský matematik *Al-Karaji (asi 953–asi 1029)*.

• *Teorie grafů.* Týž L. Euler zato v r. 1736 (snadno) vyřešil úlohu, kterou mu poslali radní (?) města Königsbergu: Můžeme přejít všech 7 mostů přes (řeku) Pregolu tak, abychom šli přes každý most jen jednou a procházku ukončili zase na začátku? Na což jim L. Euler odpověděl: „No, asi těžko můžete, purkmistři, když vám tam z každého ze čtyř kusů souše, na něž Pregola a její ramena Königsberg dělí, vychází lichý počet mostů. V procházce, kterou byste chtěli, ale každému vstupu na kus souše odpovídá výstup z něho, takže by naopak každý z těch počtů mostů měl být sudý. To jste mohli vyřešit sami i beze mě.“ (To si dělám trochu legraci.)

• *Teorie čísel.* Tzv. *Skolemův problém*, kterým ilustrujeme Teorii čísel, patří rovněž do Teoretické informatiky, kterou jsme na začátku poněkud odbyli. Je nazvaný podle norského matematika

a logika *Thoralfa Skolema (1887–1963)*. Musíme být teď trochu formálnější.

Lineárně rekurentní posloupnost, krátce LRP, je každá posloupnost $(a_n) = (a_1, a_2, \dots)$ celých čísel, která pro nějaká celá čísla $k > 0$ a $c_1, \dots, c_k$ splňuje pro každý index $n > k$ rekurentní vztah

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} \ .$$

LRP je tedy jednoznačně určena prvními k hodnotami $a_1, \dots, a_k$ a koeficienty $c_1, \dots, c_k$. Asi znáte *Fibonacciova čísla* (F_n) daná hodnotami $F_1 = F_2 = 1$ a rekurencí $F_n = F_{n-1} + F_{n-2}$:

$$(F_n) = (1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ \dots) \ .$$

Skolemův problém je tato otázka: Existuje Turingův stroj $\mathcal{T}$, tj. algoritmus, počítačový program, který pro každý vstup $2k$ celých čísel $a_1, \dots, a_k, c_1, \dots, c_k$ na výstupu spočítá odpověď ANO nebo NE podle toho, zda LRP (a_n) odpovídající vstupu obsahuje nulu, tj. $a_n = 0$ pro nějaké n.

Takový rozhodovací algoritmus je známý pouze pro $k \leq 4$.

• *Algebraické struktury.* Některé kombinatorické či grafové výsledky se dokazují pomocí algebry. Např. Věta o přátelství. Je-li $G = (V, E)$ takový konečný graf, že každé dva různé vrcholy mají právě jednoho společného souseda, pak existuje vrchol sousedící se všemi.

Vysvětlíme to formálně i neformálně. V je konečná množina a $E \subset \binom{V}{2}$. Tvrdí se, že když $\forall\, u,\, v \in V$ s $u \neq v$ $\exists!\, w \in V$, že $\{u, w\} \in E$ i $\{v, w\} \in E$, pak $\exists\, u \in V$, že $\forall\, v \in V$ $(\{u,\, v\} \in E)$. Neformálně: mají-li každí dva lidé právě jednoho společného přítele, pak existuje osoba (politik-čka), která se přátelí se všemi.

Nejjednodušší známý důkaz je založený na *lineární algebře* a dokazuje více, že všechny grafy přátelství (grafy splňující předpoklad věty) jsou právě kolekce trojúhelníků visících za společný vrchol. Pro nekonečné grafy věta neplatí.

• *Diskrétní analogie spojité matematiky.* Zde se omezíme jen na pár hesel, na více není čas.

• *Diskrétní (matematická) analýza.* Např. numerické řešení diferenciálních rovnic diskretizační metodou.

• *Diskrétní geometrie. Thomas Hales (1958)* v letech 1998–2017 dokázal domněnku *Johanesse Keplera (1571–1630)*, že nejhustší pakování koulí v prostoru jsou pyramidy pomerančů.

• *Diskrétní modelování.* Třeba *Metoda konečných prvků.* Na závěr zpátky do Brna! K její matematické teorii podstatně přispěl *Miloš Zlámal (1924–1997)*, profesor Vysokého učení Technického v Brně.

DĚKUJI ZA POZORNOST!