Matematika pro informatiku

Ústní zkouška

leden 2014

Obsah

Rejstřík

Část I

Algebra, teorie čísel, teorie grafů

1 Grupoidy, pologrupy, monoid a grupy, základní vlastnosti a definice

- Všechny mají společnou strukturu – neprázdnou množinu objektu a binární operaci
- Značíme $G = (M, \circ)$, kde M je množina a $\circ$nějaká binární operace
- Důvod, proč se tímto zabýváme: pokud dokážeme nějaké tvrzení pro obecnou strukturu, bude toto tvrzení platit i pro všechny konkrétní struktury, které od ní „dědí“
  - Jedná se tedy o triviální důkaz asociativity

Hierarchie struktur:

- Grupoid – uzavřenost nad operací
- Pologrupa – asociativita ($(x \circ y) \circ z = x \circ (y \circ z)$)
- Monoid – neutrální prvek
  - $(\exists e \in M)(\forall a \in M)(a \circ e = a \circ e = a)$
- Grupa – inverzní prvek
  - $(\forall a \in M)(\exists a^{-1} \in M)(a \circ a^{-1} = e)$
- Abelovská grupa – komutativita ($x \circ y = y \circ x$)

Tyto struktury od sebe skutečně „dědí“, tj. každá pologrupa je grupoid, každý monoid je pologrupa atp.

Pokud máme zadanou dvojici „množina a operace“ zjistíme, o co se jedná, jen postupným testováním.

Klíčová slova: Binární operace, neutrální prvek, inverzní prvek, Abelovská grupa, Cayleho tabulka, jednoznačné dělení, podgrupa.

2 Podgrupy, generátory a podgrupy generované množinami

3 Cyklické grupy, generátory

4 Homomorfizmus, izomorfizmus – vlastnosti a příklady izomorfních grupy

- **Homomorfismus** – zobrazení z jedné struktury do jiné stejného typu, které zachovává veškerou důležitou strukturu.

- **Izomorfismus** – bijektivní (prostý a na) homomorfismus.

Kleinova grupa – nejmenší necyklická grupa. Jedná se o direktní součin dvou kopií cyklické grupy řádu 2.

$$V = (\mathbb{Z}_2 \times \mathbb{Z}_2,\ \circ)$$

Klíčová slova: Izomorfní grupa, bijekce, Kleinova grupa, symetrická grupa, grupa permutací

.

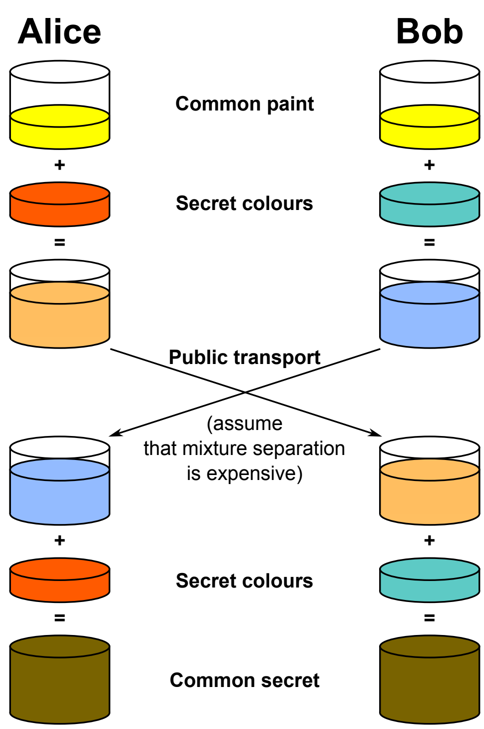
5 Problém diskrétního logaritmu v různých grupách, Diffie-Hellman Key Exchange

- **Diskrétní** – celá čísla a konečné objekty. Diskrétní objekty jsou prezentovány pomocí konečných grafů a množin. „Diskrétní“ je opak „spojitého“.
- **Logaritmus** – matematická funkce, která je inverzní k exponenciální funkci.

Neexistuje žádný rychlý algoritmus řešící problém diskrétního logaritmu, používá se proto v asymetrické kryptografii.

Def: Máme grupu $\mathbb{Z}_p^\times$ řádu $p-1$, α je nějaký její generátor a β je její prvek. Řešit problém diskrétního logaritmu znamená najít celé číslo $1 \leq x \leq p-1$ takové, že

$$\alpha^x \equiv \beta \pmod{p}$$



Obrázek 1: Diffie-Hellman Key Exchange Schema

- Díky této vlastnosti máme jednosměrnou (one-way) funkci pro asymetrickou kryptografii. Protože najít
$$\beta \equiv \alpha^x \pmod p$$
je jednoduché, pokud známe x, α a p. Najít však x pokud známe β a α je velmi obtížné. (Jinak řečeno: násobení a mocnění prvočísel je velmi rychlé a snadné).
  - **Inverzní operace k mocnění** je diskrétní logaritmus.
  - Na tomto principu je založena **RSA** (Rivest, Shamir, Adleman).

6 Tělesa, okruhy, obory integrity

7 Konečná tělesa obecně, konečná tělesa s prvočíselným řádem

8 Konečná tělesa neprvočíselného řádu, ireducibilní polynom, okruh polynomů

9 Základní vlastnosti kongruence, Eulerova a Fermatova věta, čínská věta o zbytcích, efektivní mosnění

10 Prvočísla a testování prvočíselnosti

11 Bipartitní grafy, párování v bipartitním grafu

12 Stabilní párování

13 Bioinformatika: problémy spojené se sekvencováním DNA

Část II

Numerika, optimalizace, fuzzy matematika

14 Limity a derivace funkcí více proměnných, gradient, Jacobiho matice, Hessián

14.1 Limita funkce více proměnných

- Limitou jedné proměnné můžeme odhalovat spojitost či nespojitost funkcí v určitém bodě
- U funkcí jedné proměnné jsme se k vyšetřovanému bodu přibližovali v jednom směru. U funkcí více proměnných je možné přiblížit se k bodu nekonečně mnoha způsoby (po přímkách, spirálách, výsečích...).

- Funkce má limitu v hromadném bodě a limitu b, jestliže pro každé okolí bodu b existuje prstencové okolí bodu a.

14.2 Gradient

Vektorové pole určující směr a velikost největšího růstu skalárního pole.

14.3 Jacobiho matice

Matice parciálních derivací, jejíž determinant se nazývá *jakobián*.

$$J_f = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

14.4 Hessián

Nebo-li Hessova matice je matice parciálních derivací druhých řádů.

$$\nabla^2 f(x_1, \ldots, x_n) = \begin{pmatrix} \frac{\partial^2 f}{\partial {x_1}^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial {x_2}^2} & \cdots & \frac{\partial^2 f}{\partial x_2 \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \frac{\partial^2 f}{\partial x_n \partial x_2} & \cdots & \frac{\partial^2 f}{\partial {x_n}^2} \end{pmatrix}$$

15 Lokální a globální extrémy funkcí více proměnných

Každé x splňující $\nabla f(x) = 0$ nazýváme **kritický bod** f. Dle definitnosti Hessovy matici zjistíme (Sylvestrovým kritériem nebo kvadratickou formou matice), jaké typu tento kritický bod je.

16 Konstrukce Riemannova integrálu funkce jedné a více proměnných

- Riemannův integrál vychází z faktu, že snadno vypočteme obsah obdélníka. Budeme tedy **aproximovat oblast pod grafem** funkce pomocí vhodných obdélníků.[1]
- Mějme $a,\ b \in \mathbb{R},\ a < b$, pak množina $\sigma = \{x_0,\ x_1, \ldots, x_n\}$ $(a = x_0 < x_1 < \ldots < x_n = b)$ se nazývá rozdělení intervalu, který je ekvidistantní (zachovává konstantní vzdálenost mezi prvky).
- $\int_a^{\overline{b}}$ je horní integrální součet, $\int_{\underline{b}}^a$ je dolní integrální součet. Navíc platí, že $\int_{\underline{b}}^a \leq \int_a^{\overline{b}}$.
- Pokud je funkce na intervalu integrovatelná, je možné integraci vyjádřit pomocí primitivní funkce (Newtonova formule)

$$\int\limits_a^b f(x)\,\mathrm{d}x = [F(x)]_a^b = F(b) - F(a)\,.$$

[1] http://math.feld.cvut.cz/mt/txtd/1/txc3da1a.htm

- Počítání s určitými integrály:
  - per partes,
  - substituce.
- Místo intervalu můžeme mít např. pravoúhelník

$$D = [a,\ b] \times [c,\ d]$$

- Vlastnosti dvojného integrálu:
  - Linearita – pokud jsou $f,\ g$ integrovatelné na D, pak jsou na D integrovatelné $f + g$.
  - Nerovnosti – pokud jsou $f,\ g$ integrovatelné na D a $f \leq g$, pak $\iint_D f(x) \leq \iint_D g(x)$.
  - Věta: $\iint_D f(x,\ y)$ je možné rozepsat jako $\int_a^b \left(\int_c^d f(x,\ y) \right)$.
- Můžeme integrovat i nad obecnější oblastí:
  - typ 1 – shora a zdola,
  - typ 2 – zleva a zprava.
  - Lagrangeova funkce

17 Strojová čísla a reprezentace s pohyblivou řádovou čárkou

18 Chyby vznikající při výpočtech s pohyblivou řádovou čárkou

19 Numerické metody řešení soustav lineárních rovnic

20 Vlastní čísla a mocninná metoda

21 Typy optimalizačních úloh a optimalizačních metod

22 Optimalizační metody pro spojité funkce

23 Optimalizace s omezeními

24 Vzdálenost a další míry podobnosti

Vzdálenosti číselných vektorů:

24.1 Minkovského

$$\|x\| = \left\| \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \right\| = \sqrt[p]{\sum_{i=1}^{n} |x_i|^p},\ p \in [1,\ \infty]$$

24.2 Eukleidovská

$$\|x\| = \sqrt{\langle x,\ x\rangle} = \sqrt{x^T x} = \sqrt{\sum_{i=1}^{n} x_i^2}$$

24.3 Manhattanská

$$\|x\| = \sum_{i=1}^{n} |x_i|\,,\ p = \infty:\ \|x\| = \max_{i=1,\ldots,n} |x_i|$$

24.4 Další míry podobnosti

Podobnost náhodných veličin dle **korelačních koeficientů**:

- Pearsonův (=lineární)
- Spearmanův
- Kendallův

Podobnost **binárních** vektorů

- Hammingova vzdálenost

25 Fuzzy množiny

Fuzzy matematika – matematika neurčitost nějakého prvku u z universa U k množině A.

- U klasických množin buď nějaký prvek do množiny patří nebo do ní nepatří. Toto je možné definovat jednoznačným výčtem prvků nebo definicí vlastností.
- V teorii fuzzy množin existuje *funkce příslušnosti*, která přiřazuje nějakému prvku u jeho stupeň příslušnosti k A.
- Využití v informatice: shlukování dat, hledání podobných obrázků.

25.1 Operace s fuzzy množinami

- Průnik
- Sjednocení
- Doplněk

Klíčová slova: T-normy, T-konormy.

26 Přístupy k neurčitosti založené na pravděpodobnostních rozděleních: kopule, entropie

27 Kombinování neurčitosti pomocí fuzzy pravidlových systémů a fuzzy integrálů