

Matematika pro informatiku

Ústní zkouška

leden 2014

Obsah

I	Algebra, teorie čísel, teorie grafů	3
1	Grupoidy, pologrupy, monoid a grupy, základní vlastnosti a definice	3
2	Podgrupy, generátory a podgrupy generované množinami	3
3	Cyklické grupy, generátory	3
4	Homomorfismus, izomorfismus – vlastnosti a příklady izomorfních grupy	3
5	Problém diskrétního logaritmu v různých grupách, Diffie-Hellman Key Exchange	4
6	Tělesa, okruhy, obory integrity	6
7	Konečná tělesa obecně, konečná tělesa s prvočíselným řádem	6
8	Konečná tělesa neprvočíselného řádu, ireducibilní polynom, okruh polynomů	6
9	Základní vlastnosti kongruence, Eulerova a Fermatova věta, čínská věta o zbytcích, efektivní mosnění	6
10	Prvočísla a testování prvočíselnosti	6
11	Bipartitní grafy, párování v bipartitním grafu	6
12	Stabilní párování	6
13	Bioinformatika: problémy spojené se sekvencováním DNA	6

II Numerika, optimalizace, fuzzy matematika	6
14 Limity a derivace funkcí více proměnných, gradient, Jacobiho matice, Hessián	6
15 Lokální a globální extrémy funkcí více proměnných	6
16 Konstrukce Riemannova integrálu funkce jedné a více proměnných	6
17 Výpočet Riemannova integrálu funkce jedné a více proměnných	6
18 Výpočet Riemannova integrálu funkce více proměnných	6
19 Strojová čísla a reprezentace s pohyblivou řádovou čárkou	6
20 Chyby vznikající při výpočtech s pohyblivou řádovou čárkou	6
21 Numerické metody řešení soustav lineárních rovnic	6
22 Vlastní čísla a mocninná metoda	6
23 Typy optimalizačních úloh a optimalizačních metod	6
24 Optimalizační metody pro spojité funkce	6
25 Optimalizace s omezeními	6
26 Vzdálenost a další míry podobnosti	6
27 Fuzzy množiny a operace s nimi	6
28 Přístupy k neurčitosti založené na pravděpodobnostních rozděleních: kopule, entropie	6
29 Kombinování neurčitosti pomocí fuzzy pravidlových systémů a fuzzy integrálů	6

Část I

Algebra, teorie čísel, teorie grafů

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

- Všechny mají společnou strukturu – neprázdnou množinu objektů a binární operaci
- 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
- Grupa – inverzní prvek
- 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 Homomorfismus, izomorfismus – 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.

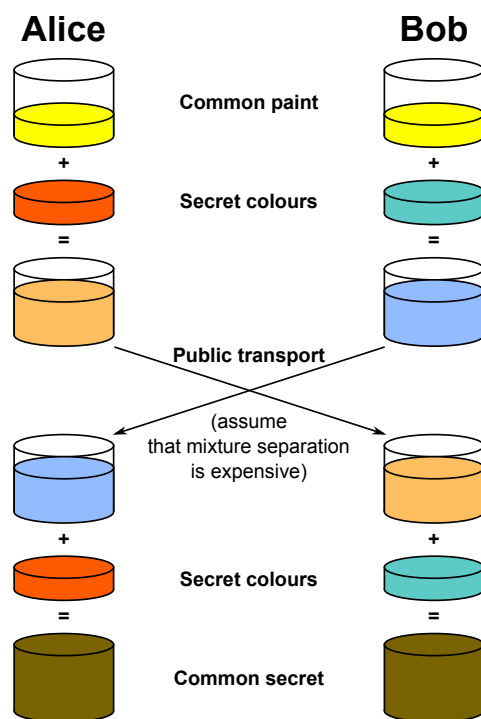
5 Problém diskrétního logaritmu v různých grupách, Diffie-Hellman Key Exchange

- **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 mocnění
- 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
- 15 Lokální a globální extrémy funkcí více proměnných
- 16 Konstrukce Riemannova integrálu funkce jedné a více proměnných
- 17 Výpočet Riemannova integrálu funkce jedné a více proměnných
- 18 Výpočet Riemannova integrálu funkce více proměnných
- 19 Strojová čísla a reprezentace s pohyblivou řádovou čárkou
- 20 Chyby vznikající při výpočtech s pohyblivou řádovou čárkou
- 21 Numerické metody řešení soustav lineárních rovnic
- 22 Vlastní čísla a mocninná metoda
- 23 Typy optimalizačních úloh a optimalizačních metod
- 24 Optimalizační metody pro spojitě funkce