

Matematika pro informatiku

Souhrn látky

leden 2014

Obsah

1	Množiny s jednou binární operací	4
1.1	Hierarchie množin	4
1.2	Základní pojmy	5
2	Podgrupy	5
3	Cyklické grupy a generátory	6
3.1	Aditivní grupy \mathbb{Z}^+	7
3.2	Multiplikativní grupy \mathbb{Z}^\times	7
3.3	Eulerova funkce	8
3.4	Řešený příklad z midtermu	9
4	Homomorfismus a izomorfismus	9
4.1	Důležité vlastnosti	10
4.2	Věty	10
4.3	Skládání permutací	10
5	Okruhy a tělesa	11
5.1	Okruh	11
5.2	Obor integrity	11
5.3	Konečné (Galoisovo) těleso	11
5.3.1	Zápis konečných těles	12
5.4	Výpočet nad tělesem s ireducibilním polynomem	12
5.4.1	A – Dělení polynomu	12
5.4.2	B – Rozšířeným Euklidovým algoritmem	13
5.4.3	„Klasická“ metoda nalezení inverzního prvku	13
5.5	Ireducibilní polynom	14
5.5.1	Ireducibilní polynomy v \mathbb{Z}_2	15
5.6	Rozšířený Euklidův algoritmus	15
6	Teorie čísel	16
6.1	Bézoutovy koeficienty	16

7	Modulární aritmetika	17
7.1	Inverzní modulo	17
7.2	Lineární kongruentní rovnice	18
7.3	Malá Fermatova věta	18
7.4	Eulerova věta	19
7.5	Čínská věta o zbytcích	20
8	Numerická matematika a strojová čísla	22
8.1	IEEE-754	24
8.2	Hladový algoritmus	24
9	Párování v grafu	25
9.1	Bipartitní graf	25
9.2	Párování v grafu	25
9.3	Stabilní párování	26
10	Vyšetření průběhu funkce	26
11	Derivace a parciální derivace	27
11.1	Definice	27
11.2	Přehled základních derivací	28
11.3	Gradient	28
11.4	Jacobiho matice	29
11.5	Parciální derivace vyšších řádů	29
11.6	Gradient ve směru a v bodě	29
12	Funkce více proměnných	30
12.1	Hessova matice	30
12.2	Definitnost	30
12.2.1	Sylvestrovo kritérium	31
12.2.2	Kvadratická forma matice	31
12.3	Tečná rovina	32
13	Integrály	32
13.1	Tabulkové integrály	32
13.2	Newtonova formule	32
13.3	Integrály přes obdélníkovou oblast	33
13.4	Integrály přes obecnou oblast	33
14	Numerické metody řešení soustav lineárních rovnic	34
15	Fuzzy matematika	35
15.1	Vzdálenost a podobnost	35
15.2	Fuzzy množiny	36
15.2.1	Průnik (součin) fuzzy množin (T -normy)	36
15.2.2	De Morganovy zákony a T -konormy (součet – sjednocení)	36
15.3	Kopule	37
15.4	Defuzzifikace	37
16	Optimalizace	37
16.1	Typy optimalizačních úloh	37
16.2	typy optimalizačních metod	37

Rejstřík

úplný graf, 25

Absolutní chyba, 22, 24
aditivní kód, 22

charakteristika, 11

Hessián, 30

izomorfní grupa, 10

jakobián, 29

Kleinova grupa, 5

magický čtverec, 4
multiplikativní grupa tělesa, 11

per partes, 32

regulární graf, 25
relativní chyba, 22, 24

stupeň vrcholu, 25

universum, 35

vlastní podgrupa, 6

1 Množiny s jednou binární operací

1.1 Hierarchie množin

Obecně se jedná o dvojici **množina a binární operace** \circ na ní, která vezme nějaké dva objekty z M a jednoznačně jim přiřadí jiný objekt.

$$(M, \circ) \\ M \circ M \rightarrow M$$

Grupoid M je *uzavřená* vůči operaci \circ .

$$\forall a, b \in M \ a \circ b \in M$$

Pologrupa Operace je nad M *asociativní*.

$$\forall a, b, c \in M \ (a \circ b) \circ c = a \circ (b \circ c)$$

Monoid Existuje právě jeden (v každém monoidu)¹ *neutrální prvek*.

$$\exists e \in M \ \forall a \in M \ e \circ a = a \circ e = a$$

Grupa Všechny prvky (každý prvek) mají právě² jeden *inverzní prvek*.

$$\forall a \in M \ \exists a^{-1} \in M \ a \circ a^{-1} = a^{-1} \circ a = e$$

Abelovská grupa Operace \circ je *komutativní*.

$$\forall a, b \in M \ a \circ b = b \circ a$$

- Z definice plyne, že každá grupa je monoid, každý monoid je pologrupa a každá pologrupa je grupoid.

$$\text{grupoid} \supset \text{pologrupa} \supset \text{monoid} \supset \text{grupa}$$

Cayleyho tabulka

Pokud má množina M z dvojice (M, \circ) konečný počet prvků, lze její strukturu (danou operací \circ) kompletně zachytit v tzv. *Cayleyho tabulce*.

- **Neutrální prvek** e se v Cayleyho tabulce pozná tak, že „jeho“ řádek i sloupec je stejný, jako první řádek a sloupec tabulky.
- **Inverzní prvek** k prvku najdeme, tak že v jeho sloupci a řádku nalezneme neutrální prvek e .
- **Uzavřenost** poznáme tak, že všechny buňky tabulky obsahují jen prvky z M .
- **Asociativitu** operace z tabulky poznáme těžko.

Cayleyho tabulka každé grupy tvoří *magický čtverec*. Magický čtverec pro n prvkovou množinu M je matice $n \times n$ taková, že v každém řádku i sloupci jsou vždy všechny prvky množiny M .

¹Přednáška 3 – handout, věta 11.

²Přednáška 3 – handout, věta 12.

Příklad Cayleho tabulky

$$\mathbb{Z}_4^+ = \{0, 1, 2, 3\}$$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

0 je neutrální prvek, její řádek i sloupec se rovnají záhlaví.

$$1^{-1} = 3$$

$$2^{-1} = 2$$

$$3^{-1} = 1$$

Inverze

1.2 Základní pojmy

Řád (pod)grupy $G = (M, \circ)$ nazýváme počet prvků množiny M . Je-li M nekonečná množina, je i řád nekonečný. Podle řádu rozlišujeme konečné a nekonečné grupy. Řád (pod)grupy můžeme značit pomocí „#“.

Jednoznačné dělení V každé grupě (G, \circ) mají pro libovolné $a, b \in G$ rovnice

$$a \circ x = b \text{ a } y \circ a = b \text{ jediné řešení.}$$

\mathbb{Z} Celá čísla $\{-2, -1, 0, 1, 2\}$.

\mathbb{N} Přirozená čísla $\{1, 2, 3\}$.

\mathbb{N}^0 Přirozená čísla **včetně** nuly.

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

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

2 Podgrupy

Buď $G = (M, \circ)$ grupa. Podgrupou grupy G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že

- $N \subset M$,
- $H = (N, \circ)$ je grupa.
- **Každý prvek grupy generuje podgrupu** (ty se však mohou překrývat).
- V každé grupě $G = (M, \circ)$ (s alespoň dvěma prvky) existují vždy alespoň dvě *triviální podgrupy*:
 - grupa obsahující pouze neutrální prvek: $(\{e\}, \circ)$
 - a grupa samotná: $G = (M, \circ)$.

- Ostatním podgrupám, které nejsou triviální, se říká netriviální nebo *vlastní podgrupa*.
- Analogie s lineárním prostorem a lineárním podprostorem.

Langrangeova věta

Buď H podgrupa konečné grupy G . Potom řád H dělí řád G . Grupa s prvočíselným řádem má pouze triviální podgrupy.

- Věta neříká, že existuje podgrupa takového řádu. Pokud však nějakou podgrupu nalezneme, musí mít právě řád dělitele.

Příklad

$$\begin{aligned}\mathbb{Z}_{15}^\times &= \{1, 2, 4, 7, 8, 11, 13, 14\} \quad (G) \\ \#\mathbb{Z}_{15}^\times &= 8\end{aligned}$$

Podgrupy G budou:

- Dvě triviální řádu $\#1 = e = \{1\}$ a $\#(\#\mathbb{Z}_{15}^\times) = \{\mathbb{Z}_{15}^\times\}$
- A další (*vlastní*) podgrupy řádů $\#4$ a $\#2$, protože $(\#4 \text{ a } \#2) \mid 8$:

$$\begin{aligned}\langle 7 \rangle = \langle 13 \rangle &= \{1, 4, 7, 13\}, \{1, 2, 4, 8\} \\ \langle 2 \rangle = \langle 3 \rangle &= \{1, 14\}, \{1, 11\}\end{aligned}$$

Generátory podgrupy $\langle 7 \rangle = \langle 13 \rangle$ generují stejnou podgrupu a $\langle 2 \rangle = \langle 3 \rangle$ generují stejnou podgrupu.

3 Cyklické grupy a generátory

- V cyklické grupě $G = (M, \circ)$ řádu n platí pro všechny prvky $a \in M$, že $a^n = e$, kde e je neutrální prvek.
- Neutrální prvek \neq generátor.
- Grupa prvočíselného řádu (počet prvků je prvočíslo) je cyklická.
- Libovolná podgrupa cyklické grupy je opět cyklická grupa.
- Je-li G **cyklická multiplikativní** grupa řádu n a a nějaký její generátor, potom a^k je také generátor tehdy, a jen tehdy, když k a n jsou nesoudělná (tj. $\gcd(k, n) = 1$).
- V cyklické grupě řádu n je počet generátorů roven $\varphi(n)$.

Příklad – základní ukázka grupy

$$\begin{aligned}\mathbb{Z}_4^+ &= \{0, 1, 2, 3\} \\ \#\mathbb{Z}_4^+ &= 4 \\ e &= 0 \\ 2^4 &= (16)_{MOD 4} = 0\end{aligned}$$

3.1 Aditivní grupy \mathbb{Z}^+

- Všechny aditivní grupy jsou cyklické.
- Aditivní grupa modulo n je rovna $\langle k \rangle$ (generátoru) tehdy, a jen tehdy, když k a n jsou nesoudělná čísla.
- Počet prvků grupy $\mathbb{Z}_{\text{MOD}}^+$ je MOD.

Příklad

$$\begin{aligned}\mathbb{Z}_{15}^+ &= \{0, 1, 2, 3, \dots, 14\} \\ \mathbb{Z}_{15}^+ &= \{\langle 1 \rangle, \langle 2 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 7 \rangle, \langle 8 \rangle, \langle 9 \rangle, \langle 11 \rangle, \langle 12 \rangle, \langle 13 \rangle, \langle 14 \rangle\}\end{aligned}$$

Generátorem jsou všechna čísla nesoudělná s 15.

3.2 Multiplikativní grupy \mathbb{Z}^\times

Multiplikativní cyklická grupa

\mathbb{Z}_n^\times je cyklická tehdy a jen tehdy, když $n = 2, 4, p^k, 2p^k$, kde p je liché prvočíslo a $k \in \mathbb{N}^+$.

- Multiplikativní grupa modulo p , kde p je prvočíslo, je množina $\{1, 2, \dots, p-1\}$ s operací násobení modulo p . Tuto grupu značíme \mathbb{Z}_p^\times .
 - Grupa \mathbb{Z}_p^\times je vždy cyklická.
 - Řád této grupy \mathbb{Z}_p^\times je $p-1$ a má tedy $\varphi(p-1)$ generátorů.
- Prvky multiplikativní grupy jsou nesoudělné s jejím modulem, řád multiplikativní grupy tedy získáme jako:

$$\#\mathbb{Z}_{\text{MOD}}^\times = \varphi(\text{MOD}).$$

Příklad

$$\begin{aligned}\mathbb{Z}_3^\times &= \{1, 2\} \\ \mathbb{Z}_7^\times &= \{1, 2, 3, 4, 5, 6\} \\ (6 * 6)_{\text{MOD } 7} &= 1 \\ (6 * 5)_{\text{MOD } 7} &= 2 \\ &\dots\end{aligned}$$

Příklad II.

Najděte podgrupy následující multiplikativní grupy

$$\begin{aligned}\mathbb{Z}_{22}^\times &= \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\} (G) \\ \#\mathbb{Z}_{22}^\times &= 10\end{aligned}$$

Tato grupa je cyklická, protože

$$\begin{aligned}22 &= 11 * 2 (= 2 * \mathbb{P}^1) \\ \varphi(10) &= 4\end{aligned}$$

Její podgrupy budou (triviální grupy vynecháme) řádů

$$10 = 2 * 5 \rightarrow \#2 \text{ a } \#5$$

Podgrupy nalezneme pomocí generátorů podgrupy (každý prvek grupy G) postupným uzavíráním:

$$\begin{aligned}\langle 3 \rangle &= \{3\} \\ &= \{3, 3 * 3\} = \{3, 9\} \\ &= \{3, 9, (9 * 3)_{22}\} = \{3, 9, 5\} \\ &= \{3, 9, 5, 5 * 3\} = \{3, 9, 5, 15\} \\ &= \{3, 9, 5, 15, (15 * 3)_{22}\} = \{3, 9, 5, 15, \boxed{1}\}\end{aligned}$$

Vygenerovaná podgrupa je řádu 5, což je v pořádku.

Stejným způsobem pokračujeme pro všechny prvky $z G$. Zjistíme, že generátory podgrupy

$$\langle 7 \rangle, \langle 13 \rangle, \langle 17 \rangle \text{ a } \langle 19 \rangle$$

vygenerují celou grupu G , jsou tedy jejími generátory (jejich počet sedí s $\varphi(10)$).

3.3 Eulerova funkce

Eulerova funkce $\varphi(n)$, kde $n \geq 2$, je definována jako počet kladných celých čísel, která jsou nižší než n a jsou s n nesoudělná.

$$\begin{aligned}\varphi(1) &= 1; \varphi(2) = 1 \\ \varphi(p) &= p - 1, p \in \mathbb{P} \\ \varphi(p^k) &= (p - 1) * p^{k-1}, p \in \mathbb{P} \\ \varphi(n * m) &= \varphi(n) * \varphi(m), n, m \in \mathbb{N} \text{ a } n, m \text{ jsou nesoudělná}\end{aligned}$$

3.4 Řešený příklad z midtermu

Grupa \mathbb{Z}_{26}^\times je cyklická. Pro jakou množinu A je následující výrok pravdivý: Prvek a je generátor grupy \mathbb{Z}_{26}^\times jestliže $a^n \neq 1$ pro všechna $n \in A$.

- (A) $A = \{2, 4, 7, 13\}$
- (B) $A = \{4, 7\}$
- (C) $A = \{4, 6\}$
- (D) Ani pro jednu z nabízených možností.
- (E) $A = \{1, 2, 3, 4, 6\}$

Poznámka k zadání: Hledáme taková čísla, na která když umocníme generátor, výsledek se nebude rovnat 1.

Při řešení vycházíme z následujících dvou vět:

- Řád podgrupy dělí řád grupy.
- V cyklické grupě platí $a^n = e$, kde n je řád grupy a e její neutrální prvek.

Pokud je a generátor grupy (řeceno v zadání), musí dle předchozího platit, že a^1, a^2, \dots, a^{n-1} se **nerovnájí** e . Dále budeme vycházet z vlastnosti, že pokud prvek není generátorem grupy, je generátorem některé její podgrupy (viz sekce Podgrupy). Z čehož plyne, že a^h , kde h je řád podgrupy, by bylo 1. Řády podgrup grupy \mathbb{Z}_{26}^\times mohou být $\{2, 3, 4, 6\}$ ($\varphi(26) = 12$).

Správná odpověď je tedy **C)** $A = \{4, 6\}$ – jinými slovy jestliže $a^4 \neq 1 \wedge a^6 \neq 1$, pak a je generátorem (o obdobně pokud by $a^4 = 1$ ($1 = e$, a 4 není řádem grupy) a by bylo generátorem nějaké podgrupy).

4 Homomorfismus a izomorfismus

Homomorfismus Zobrazení, které zachovává operace. Budte $G = (M, \circ_G)$ a $H = (N, \circ_H)$ dva grupoidy. Zobrazení $\varphi : M \rightarrow N$ nazveme homomorfismem G do H , jestliže

$$\forall x, y \in M \text{ platí } \varphi(x \circ_G y) = \varphi(x) \circ_H \varphi(y).$$

Slovy: Jestliže na libovolné dva prvky v grupě G aplikujeme operaci grupy G a pak je zobrazíme do grupy H , **dostaneme vždy stejný výsledek**, jako kdybychom je (prvky grupy G) nejdříve zobrazili do grupy H a **potom** aplikovali operaci grupy H .

Izomorfismus pokud je homomorfismus navíc *bijekcí*, tj.

$$a : G \rightarrow H \text{ a } b : H \rightarrow G, \quad a \circ b = id_H \text{ a } b \circ a = id_G.$$

- Oba **zachovávají strukturu danou binární operací** – je jedno, jestli nejdříve aplikujeme operaci a pak zobrazíme. nebo nejdříve zobrazíme a pak aplikujeme operaci.
- Pro definici homomorfismu vyžadujeme **pouze uzavřenost množiny** vůči binární operaci. Homomorfismus je proto definován na nejobecnějších grupoidech. V kapitole Hierarchie množin jsme ukázali, že jednotlivé struktury od sebe dědí – definice homomorfismu se tedy přenáší i na grupy.

- Inverzní zobrazení k izomorfnímu zobrazení je izomorfní zobrazení.
- Grupy, mezi kterými existuje izomorfismus, se nazývají **izomorfní**.
- **Počet různých izomorfismů** se rovná³ faktoriálu z počtu generátorů (odpovídá počtu bijektivních zobrazení).

4.1 Důležité vlastnosti

- Izomorfní grupy musí mít stejný řád.
- Neutrální prvek jedné grupy se homomorfismem zobrazí vždy na neutrální prvek té druhé.
- Také inverze se zachovávají ve smyslu toho, že $\varphi(x^{-1}) = \varphi(x)^{-1}$.
- Je-li φ homomorfismus grupy G do H , pak $\varphi(G)$ je podgrupa v H .
- Všechny izomorfní grupy jsou totožné, mají jen jinak pojmenované prvky.

4.2 Věty

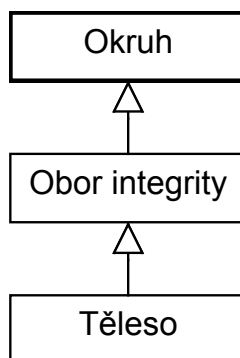
- Neutrální prvek jedné grupy se homomorfismem zobrazí vždy na neutrální prvek té druhé.
- Je-li φ homomorfismus grupy G do H , pak $\varphi(G)$ je podgrupa v H .
- Libovolné dvě nekonečné cyklické grupy jsou izomorfní. Pro každé $n \in \mathbb{N}$ jsou libovolné dvě cyklické grupy řádu n izomorfní.
- **Cayleyova věta:** Libovolná konečná grupa je izomorfní s nějakou grupou permutací.
- Obecně platí pro kartézský součin dvou grup H a G řádů n a m toto: kartézský součin je cyklická grupa právě když G a H jsou cyklické a n a m nesoudělné

4.3 Skládání permutací

$$\left(\begin{array}{ccc} & \downarrow [3] & \\ 1 & 2 & \textcolor{red}{3} \\ & & \boxed{2} \end{array} \right) \circ \left(\begin{array}{ccc} \downarrow [1] & & \\ & 1 & \\ \textcolor{red}{3} \leftarrow [2] & 2 & 3 \\ & & 1 \end{array} \right) = \left(\begin{array}{ccc} & & \\ & & \\ \boxed{2} & 3 & 1 \end{array} \right)$$

³Tato vlastnost byla odvozena z pozorování.

5 Okruhy a tělesa



Obrázek 1: Hierarchie okruhů, oborů integrity a těles

5.1 Okruh

Buďte M neprázdná množina a „+“ a „*“ binární operace. Řekněme, že $R = (M, +, *)$ je okruh, pokud platí:

- $(M, +)$ je Abelovská grupa (komutativita)
- $(M, *)$ je grupoid (uzavřené)
- Platí levý a pravý distributivní zákon:

$$(\forall a, b, c \in M) (a(b + c) = ab + ac \wedge (b + c)a = ba + ca)$$

5.2 Obor integrity

- Každý obor integrity je zároveň okruh.

5.3 Konečné (Galoisovo) těleso

Okruh $T = (M, +, *)$ se **nazývá těleso**, jestliže $(M \setminus \{0\}, *)$ je grupa. Tuto grupu nazýváme multiplikativní grupou tělesa T . Nulu musíme vyjmout, protože nemá inverzi:

$$0^{-1} = ??$$

- Existují pouze tělesa řádu p^n , kde p je prvočíslo a n je přirozené číslo. Prvočíslo p se nazývá **charakteristika**.
- V tělesech je neutrálním prvkem číslo 1. V tělese $GF(2^3)$ je např. neutrální číslo binární řetězec 001.
- Tělesa mají konečný počet prvků.

5.3.1 Zápis konečných těles

$$\begin{aligned} 101 &= x^2 + 0x + 1 \\ 202 &= 2x^2 + 0x + 2 \end{aligned}$$

$$(-1)_3 = 2$$

(O kolik čísel se musíme posunout doleva, abychom získali 3.)

$$GF(M^\#) = (2^4)$$

je řád:

$$\begin{aligned} \# &= 4 \rightarrow a, b, c, d \\ y &= ax^{\#-1} + bx^{\#-2} + \dots = ax^3 + bx^2 + cx + d \end{aligned}$$

M je modulo, ve kterém počítáme:

$$M = 2 \rightarrow a, b, c, d = \{0, 1\}$$

5.4 Výpočet nad tělesem s ireducibilním polynomem

5.4.1 A – Dělením polynomu

V tělese

$$GF(2^4)$$

vyřešte rovnici

$$1111y = 0110 + 0101y,$$

kde se počítá modulo ireducibilní polynom

$$P(x) = x^4 + x^3 + 1.$$

$$\begin{aligned} 1111y - 0101y &= 0101 \\ y(1111 - 0101) &= 0101 \end{aligned}$$

Počítáme v modulo 2, proto:

$$\begin{aligned} 1 + 1 &=_{MOD 2} 0 \\ - &=_{MOD 2} + \end{aligned}$$

$$\begin{aligned} y1010 &= 0101 \\ y &= ax^3 + bx^2 + cx + d \\ (ax^3 + bx^2 + cx + d) * (x^3 + 0x^2 + x + 0 * 1) &= 0x^3 + x^2 + 0x + 1 \\ \dots &= \dots \end{aligned}$$

Rovnici roznásobíme a vydělíme (běžné dělení polynomu polynomem) ireducibilním polynomem:

$$(ax^6 + bx^5 + ax^4 + \dots) \div (P(x) = x^4 + x^3 + 1) = 0$$

Ve zbytku po dělení odhadneme koeficienty a, b, c, d , aby rovnice vycházela. V našem případě:

$$\begin{aligned} a &= 1 \\ b &= 0 \\ c &= 0 \\ d &= 0 \end{aligned}$$

Koeficienty dosadíme do předpisu y , čímž získáme finální výsledek:

$$y = ax^3 + bx^2 + cx + d = x^3 = \mathbf{1000}$$

5.4.2 B – Rozšířeným Euklidovým algoritmem

Nejprve osamostatníme v původní rovnici y , zde nám nutně vyjde dělení (resp. násobení inverzí):

$$\begin{aligned} y(1010) &= 0110 \\ y &= 0110 * (1010)^{-1} \end{aligned}$$

Nyní vypočítáme inverzi $1010 (= x^3 + x)$:

	$\mathbf{x^4 + x^3 + 1}$ $\mathbf{x^3 + x}$	$\mathbf{x^3 + x}$ 0 1	$\mathbf{x^4 + x^3 + 1}$ 1 0
$\frac{x^4+x^3+1}{x^3+x} = x + 1$	$x^2 + x + 1$	$0 - [1 * (x + 1)] = \mathbf{x + 1}$	$1 - [0 * (x + 1)] = \mathbf{1}$
$\frac{x^3+x}{x^2+x+1} = x + 1$	$x + 1$	$1 - (x + 1)^2 = \mathbf{x^2}$	$0 - 1 * (x + 1) = \mathbf{x + 1}$
$\frac{x^2+x+1}{x+1} = x$	$\mathbf{1}$	$(x + 1) - (x * x^2) = \mathbf{x^3 + x + 1}$	

S inverzí dopočítáme x :

$$y = (x^2 + x) * (x^3 + x + 1) = x^5 + x^4 + x^3 + \mathbf{x^2} + \mathbf{x^2} + x$$

Výsledek vydělíme ireducibilním polynomem:

$$(x^5 + x^4 + x^3 + x) \div (x^4 + x^3 + 1) = x, \text{ zb. } \mathbf{x^3 = 1000}$$

5.4.3 „Klasická“ metoda nalezení inverzního prvku

Zadání: „V tělese $GF(3^2)$, kde se násobí modulo polynom $x^2 + 1$, najděte inverzní prvek k prvku 12.“

- Budeme počítat v modulo 3.
- Polynom bude maximálně prvního stupně, tzn. $ax + b$.

$$12 = \mathbf{x + 2}$$

Musíme nalézt takové koeficienty polynomu, aby platil výraz

$$(\mathbf{x + 2}) * (ax + b) = \mathbf{1} \text{ (pozn.: 1 je neutrální prvek).}$$

Výraz roznásobíme a vydělíme ireducibilním polynomem

$$(ax^2 + bx + 2ax + 2b) \div (x^2 + 1) = a, \text{ zbytek: } x(2a + b) + 2b - a.$$

Nyní budeme ve zbytku hledat taková a a b , aby se výraz rovnal původní 1 , resp. $0x + 1$. Řešením je tedy soustava dvou rovnic o dvou neznámých

$$x \left(\underbrace{2a + b}_{=0} \right) + \underbrace{2b - a}_1 = 0x + 1 \Rightarrow$$

$$2a + b = 0 \quad (1)$$

$$2b - a = 1 \quad (2)$$

Z první rovnice vyjádříme a , nezapomínejme, že počítáme v $GF(3)$

$$\begin{aligned} 2a &= -b \\ |-b|_3 &= 2b \Rightarrow \\ 2a &= 2b \\ a &= b, \end{aligned}$$

dosadíme a do druhé rovnice

$$\begin{aligned} 2a - a &= 1 \\ \mathbf{a} &= \mathbf{1} \Rightarrow \mathbf{b} = \mathbf{1}. \end{aligned}$$

Tyto koeficienty dosadíme do polynomu $ax + b$

$$ax + b; a = b = 1.$$

Výsledná inverze k prvku 12 je

$$\underline{\underline{x + 1 \text{ } (= 11)}}.$$

5.5 Ireducibilní polynom

- K je okruh, $K[x]$ je komutativní okruh polynomů nad okruhem K .

Ireducibilní polynom

Buď $P(x) \in K[x]$ stupně alespoň 1. Řekněme, že $P(x)$ je ireducibilní nad K , jestliže pro každé dva polynomy $A(x)$ a $B(x)$ z $K[x]$ platí

$$A(x) * B(x) = P(x) \Rightarrow (\text{stupeň } A(x) = 0 \vee \text{stupeň } B(x) = 0).$$

- Slovy: Ireducibilní polynom je polynom, který nelze rozložit na součin jiných polynomů s nižším stupněm (vyjma polynomů stupně nula). Ireducibilní polynomy jsou **prvočísla mezi polynomy**.

5.5.1 Ireducibilní polynomy v \mathbb{Z}_2 **Tip**

V \mathbb{Z}_2 testujeme ireducibilitu pro polynomy, které končí $\boxed{\dots + 1}$, v \mathbb{Z}_3 testujeme polynomy, které končí $\boxed{\dots + 1}$ nebo $\boxed{\dots + 2}$ atd. Toto pravidlo neplatí pro polynomy stupně 1.

Stupeň 0

0	NE	} Nevyhovují definici
1	NE	

Stupeň 1

x	ANO	} Všechny jejich násobky již nebudeme brát v úvahu
$x + 1$	ANO	

Stupeň 2

x^2	NE (násobek x)
$x^2 + 1$	NE
$x^2 + x$	NE (násobek x)
$x^2 + x + 1$	ANO

Stupeň 3

x^3	NE
$x^3 + 1$	NE
$x^3 + x + 1$	ANO
$x^3 + x^2$	NE
$x^3 + x^2 + 1$	ANO
$x^3 + x^2 + x$	NE
$x^3 + x^2 + x + 1$	NE
$x^3 + x$	NE

Stupeň 4

$x^4 + x + 1$	ANO
$x^4 + x^3 + 1$	ANO
$x^4 + x^3 + x^2 + x + 1$	ANO

5.6 Rozšířený Euklidův algoritmus

		X	ireduc.
	ireduc.	<input type="checkbox"/>	<input type="checkbox"/>
	X	<input type="checkbox"/>	<input type="checkbox"/>
÷	zbytek	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	GCD	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Příklad

Hledáme $5 * x \equiv 1 \text{ MOD } 17$ tj. inverzi 5.

		5	17
	17	0_A	1_C
	5	1_B	0_D
$\frac{17}{5} = 3$	zb. 2	-3_X	1_Y
$\frac{5}{2} = 2$	zb. 1	7	-2

$$-3_X = 0_A - (3 * 1_B)$$

$$1_Y = 1_C - (3 * 0_D)$$

$$-2 = 0_D - (2 * 1_Y)$$

$$7 = 1_B - [2 * (-3_X)] \text{ (výsledná inverze)}$$

Příklad „Petrův postup“

Hledáme $5 * x \equiv 1 \text{ MOD } 17$ tj. inverzi 5.

$? \times$	17	0	1
$3 \times$	5	1	0
$2 \times$	2	-3	1
	1	<u>7</u>	-2
	0		

6 Teorie čísel

6.1 Bézoutovy koeficienty

Bézoutovy koeficienty α a β

$$\alpha * N_1^+ + \beta * N_2^+ = GCD(N_1^+, N_2^+)$$

- Koeficienty je možné vypočítat pomocí Rozšířený Euklidův algoritmus
- GCD je možné vypočítat pomocí Euklidova algoritmu

Příklad „Petrův postup“

Hledáme $\alpha * 12 + \beta * 42 = 6$

		α	β
$? \times$	42	0	1
$3 \times$	12	1	0
$2 \times$	6	<u>-3</u>	<u>1</u>
	0		

$$-3 * 12 + 1 * 42 = 6.$$

Příklad výpočtu GCD

$$GCD(27, 45) = ?$$

$$45 = 1 * 27 + 18$$

$$27 = 1 * 18 + 9$$

$$18 = 2 * \boxed{9} + 0 \quad (\rightarrow \perp)$$

$$GCD(27, 45) = \underline{9}$$

Pokud $\gcd(m, n) = 1$, pak říkáme, že m a n jsou nesoudělná.

7 Modulární aritmetika

Algoritmus 1 Výpočet modula ze záporného čísla

```

1 int mod(int x, int m)
2 {
3     return (x%m + m)%m;
4 }

```

Ukázka použití:

```

1 >>> mod(-6, 5)
2 4
3 >>> mod(-2, 3)
4 1
5 >>> mod(-1, 3)
6 2

```

7.1 Inverzní modulo

- Inverzi lze nalézt, jen když jsou základ a modulo nesoudělné.

Příklad

Nalezněte

$$|5^{-1}|_{11} = ?.$$

Musí tedy platit

$$(5 * x) \bmod 11 = 1.$$

Řešení

$$x = 9, \text{ protože } 5 * 9 = 45 \text{ a } (45)_{11} = 1.$$

Příklad II.

V Z_{223}^\times najděte inverzi k číslu 63.

- Inverzi nalezneme pomocí Rozšířeného Euklidova algoritmu.

$$\begin{array}{c|ccc}
 & & \mathbf{223} & \mathbf{63} \\
 & \mathbf{223} & 1 & 0 \\
 & \mathbf{63} & 0 & 1 \\
 \hline
 \vdots & \vdots & \vdots & \vdots \\
 1 & 1 & \boxed{-46} & -9
 \end{array}$$

$$inv. = -46$$

Výsledek převedeme do kladného modula

$$inv. = -46 + 223 = \underline{\underline{177}}.$$

7.2 Lineární kongruentní rovnice

Rovnice

$$\boxed{a * x \equiv b \pmod{M}}$$

má řešení, jestliže („⁴ – dělí)

$$GCD(a, M) | b.$$

Řešení:

Najdi $\alpha \in \mathbb{Z}$ tak, že $\alpha * a + \beta * M = GCD(a, M)$, pak

$$x \equiv \frac{\alpha * b}{GCD(a, M)} \left(\text{mod} \frac{M}{GCD(a, M)} \right)$$

7.3 Malá Fermatova věta

$$a^{p-1} \equiv 1 \pmod{p}$$

$$p \in \mathbb{P}, GCD(a, p) = 1$$

⁴ $a|b$ znamená „a dělí b“ tzn. $a < b$. Např. $2|16$.

Příklad

Spočítejte

$$381^{152} \bmod 13$$

$$GCD(381, 13) = 1, \mathbf{p} \in \mathbb{P}.$$

Modulo je prvočíslo, MFV tedy můžeme použít

$$\begin{aligned} 381^{12} &\equiv 1 \pmod{13} \\ 152 &= 12 * 12 + 8 \\ |381^{12*12+8}|_{13} &= \cancel{|381^{12*12}|_{13}} * |381^8|_{13} \\ |381|_{13} &= 4 \\ 4^8 &= \left((4^2)^2\right)^2 \\ |4^2|_{13} &= 3 \\ |(3^2)^2|_{13} &= |81|_{13} = \underline{\underline{3}}. \end{aligned}$$

7.4 Eulerova věta

- Zobecnění Malé Fermatovy věty

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$n \in \mathbb{N}, GCD(a, n) = 1$$

Příklad

Spočítejte

$$3^{15} \bmod 28.$$

Modulo není prvočíslo, můžeme tedy použít Eulerovu větu

$$GCD(3, 28) = 1, p \notin \mathbb{P}$$

$$\begin{aligned} \varphi(28) &= \varphi(2^2 * 7) = (2-1) * 2 * \varphi(7) = 2 * 6 = \mathbf{12} \\ 3^{15} &= 3^{\mathbf{12}} * 3^3 \end{aligned}$$

$$\begin{aligned} |3^{\varphi(28)}|_{28} &\equiv 1 \pmod{28} \\ |3^{12} * 3^3|_{28} &\equiv 1 \pmod{28} \\ |\cancel{3^{12}} * 3^3|_{28} &\equiv 1 \pmod{28} \\ &\equiv 3^3 \equiv \underline{\underline{27}}. \end{aligned}$$

7.5 Čínská věta o zbytcích

Jsou dána přirozená čísla m_1, m_2, \dots, m_k po dvou nesoudělná. Pak pro libovolná celá čísla a_1, a_2, \dots, a_k existuje celé číslo x takové, že

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\&\vdots \\x &\equiv a_k \pmod{m_k}.\end{aligned}$$

Tato soustava rovnic má řešení x a toto řešení je určeno jednoznačně v modulo

$$M = m_1 * m_2 * \dots * m_k.$$

Příklad^a

Řešte následující soustavu:

$$\begin{aligned}x &= 2 \pmod{3} \\x &= 1 \pmod{8} \\x &= 7 \pmod{13}\end{aligned}$$

Řešení bude ve tvaru:

$$x = 2 * q_1 + 1 * q_2 + 7 * q_3 \pmod{(3 * 8 * 13)}; 3 * 8 * 13 = 312$$

První koeficient:

$$\begin{aligned}s_1 &= \prod_{j \neq 1} m_j = 8 * 13 = 104 \\t_1 &= (s_1)^{-1} = (104)^{-1} = (2)^{-1} = 2 \pmod{3} \\q_1 &= s_1 * t_1 = 104 * 2 = 208 \pmod{312}\end{aligned}$$

Druhý koeficient:

$$\begin{aligned}s_2 &= \prod_{j \neq 2} m_j = 3 * 13 = 39 \\t_2 &= (s_2)^{-1} = (39)^{-1} = (7)^{-1} = 7 \pmod{8} \\q_2 &= s_2 * t_2 = 39 * 7 = 273 \pmod{312}\end{aligned}$$

Třetí koeficient:

$$\begin{aligned}s_3 &= \prod_{j \neq 3} m_j = 3 * 8 = 24 \\t_3 &= (s_3)^{-1} = (24)^{-1} = (11)^{-1} = 6 \pmod{13} \\q_3 &= s_3 * t_3 = 24 * 6 = 144 \pmod{312}\end{aligned}$$

Celkový výsledek:

$$x = 2 * 208 + 1 * 273 + 7 * 144 = 1697 = 137 \pmod{312}$$

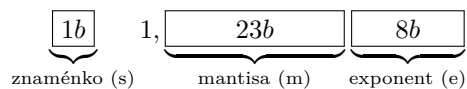
Soustavu rovnic tedy řeší tato celá čísla:

$$x = 137 + k * 312, k \in \mathbb{Z}$$

^a<http://voho.cz/wiki/matematika/cinska-veta-o-zbytcich/>

8 Numerická matematika a strojová čísla

Struktura strojově zapsaného čísla



$$\text{resp.: } (-1)^z * (1, m)_2 * 2^{e-b}$$

- Obsahuje skrytou 1,
- V jednoduché přesnosti má exponent **rozsah** $-128, +127$ a je zapsán v aditivním kódu.
 - Př.: „Číslo jsme normalizovali posunem o 9 míst doleva.“

$$\begin{aligned}
 e - 127 &= 9 \\
 e &= (136)_{10} = (10001000)_2
 \end{aligned}$$

- Do strojového formátu je možné zapsat pouze zlomky ve tvaru $\frac{x}{2^y}$, kde x a y jsou celá čísla
 - Všechna ostatní čísla, mají binární reprezentaci nekonečnou a periodickou

Při převodu dochází k chybám (vlivem zaokrouhlování nebo krácení). Necht α je přibližnou reprezentací čísla a a je skutečná hodnota čísla. **Absolutní chybu** spočítáme jako

$$|\alpha - a|$$

a **relativní chybu** pro $a \neq 0$ jako

$$\frac{|\alpha - a|}{|a|}.$$

„Pravítko“ na převod z a do binární soustavy

□	□	□	□	□	□	□	□	□	□	□
1024	512	256	128	64	32	16	8	4	2	1

Zápis čísel ve tvaru 2^n

Číslo ve tvaru

$$2^{-n}$$

má binární reprezentaci

$$0, \underbrace{000 \dots 000}_{(n-1) \times 0} 1.$$

Číslo ve tvaru

$$2^n$$

má binární reprezentaci

$$1 \underbrace{000 \dots 000}_{n \times 0}.$$

Odčítání binárních čísel

$$1 - 1 = 0$$

$$1 - 0 = 1$$

$$0 - 1 = 1 \text{ (+ přenos)}$$

Příklad

$$\begin{array}{r} 1 \ 0 \ 0 \\ - \ 1 \ 1 \\ \hline 0 \ 0 \ 1 \end{array}$$

Pokud převádíme zlomek, který je strojovým číslem, nemusíme používat hladový algoritmus, ale pomůžeme si rozkladem na mocniny 2. Např. chceme-li rozložit číslo

$$\frac{49}{512} = \frac{32 + 16 + 1}{2^9} = \underbrace{\frac{2^5}{2^9}}_{9-5=\boxed{4}} + \underbrace{\frac{2^4}{2^9}}_{9-4=\boxed{5}} + \underbrace{\frac{2^0}{2^9}}_{9-0=\boxed{9}}$$

Číslo bude ve tvaru 0, a následovat bude $9 \times$ nula:

$$0, \underbrace{000 \ 1}_{[4][5]} \underbrace{1 \ 0001}_{[9]}.$$

8.1 IEEE-754

Přesnost	Délka mantisy („m“)	Délka exponentu („d“)	„b“
binary32 (single)	23	8	127
binary64 (double)	52	11	1023
binary128 (quadruple)	112	15	16383

Tabulka 1: Počty cifer standardu IEEE-754

- Ve standardu jsou popsány i situace NaN, +Inf, -Inf.
- Pokud reprezentujeme čísla mimo rozsah, dochází k přetečení (overflow) resp. podtečení (underflow).
- **Absolutní chyba** je $|\alpha - a|$, kde α je reprezentace čísla a .
- Pro $a \neq 0$ se **relativní chyba** rovná $\frac{|\alpha - a|}{|a|}$.

8.2 Hladový algoritmus

- Slouží pro získání binární reprezentace čísel

Příklad

$$\left(\frac{1}{13}\right)_{10} = (?)_2$$

Zvolíme l , tak aby platilo

$$\begin{aligned} 2^l &\leq \frac{1}{13} < 2^{l+1} \\ l &= -4 \\ \frac{1}{16} &\leq \frac{1}{13} < \frac{1}{8} \end{aligned}$$

Protože $l = -4$, bude výsledné číslo ve tvaru

$$0, \underbrace{000}_{\#4} \underbrace{?}_{\#5} \underbrace{?}_{\#6} \underbrace{?}_{\#7} \dots$$

Algoritmus:

$$l' = |l| = 4$$

*	(> 1 or < 1)	Výsledek	Do dalšího kroku	Výsledné číslo
$\frac{1}{13} * 2^4$	$\frac{16}{13}$	$> 1 \rightarrow \#4 = 1$	$\frac{16}{13} - 1 = \frac{3}{13}$	0,000 1
$\frac{3}{13} * 2$	$\frac{6}{13}$	$< 1 \rightarrow \#5 = 0$	\times	0,0001 0
$\frac{6}{13} * 2$	$\frac{12}{13}$	$< 1 \rightarrow \#6 = 0$	\times	0,00010 0
$\frac{12}{13} * 2$	$\frac{24}{13}$	$> 1 \rightarrow \#7 = 1$	$\frac{24}{13} - 1 = \frac{11}{13}$	0,000100 1
\vdots	\vdots	\vdots	\vdots	\vdots
$\frac{8}{13} * 2$	$res = \frac{16}{13} \rightarrow \perp$	\times	\times	0,00010011101100 0
				\times

9 Párování v grafu

9.1 Bipartitní graf

Bipartitní graf je takový graf, jehož množinu vrcholů je možné rozdělit na dvě disjunktní množiny tak, že žádné dva vrcholy ze stejné množiny nejsou spojeny hranou.

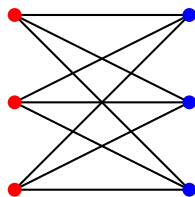
$$\begin{aligned} G &= (W, E) \\ W &= V \cup U \end{aligned}$$

V a U jsou neprázdné disjunktní množiny a pro každou hranu platí, že jeden její vrchol je z V a druhý z W .

- **Úplný bipartitní graf** je, jestliže z každého vrcholu jedné množiny vedou hrany do všech vrcholů druhé množiny. Tedy platí

$$E = U \times W$$

nebo-li v grafu existují všechny hrany s touto vlastností.



Obrázek 2: Úplný bipartitní graf

- (Bipartitní) graf je **regulární**, jestliže všechny jeho vrcholy mají stejný stupeň. **Stupeň vrcholu** je počet hran, které z daného vrcholu vedou.

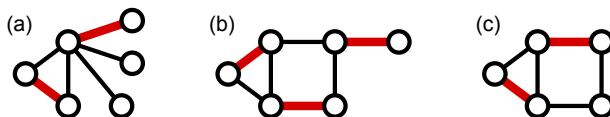
9.2 Párování v grafu

Párování v grafu – definice

Buď $G = (W, E)$ graf. $M \subset E$ (podmnožina hran grafu G) se nazývá párování v grafu G , jestliže žádné dvě hrany z M nemají společný vrchol.

Jinými slovy: Vrcholy grafů dáváme do párů. Pár může vzniknout jen tam, kde byla hrana. Přitom každý vrchol může být jen v jednom páru.

- **Maximální párování** – žádné jiné párování nemá více hran (nebo-li párování obsahuje nejvyšší možný počet hran). Graf může mít více maximálních párování.
 - Párování je rovněž maximální, jestliže v grafu neexistuje M -zlepšující cesta.



Obrázek 3: Možná maximální párování v grafu, více hran už žádné jiné párování nemá

- **M -saturovanost** vrcholu (též nasycenost vrcholu) – vrchol je již obsažen v nějakém párování.
- **Perfektní párování** (někdy též úplné) znamená, že jsou všechny vrcholy M -saturované (tj. všechny vrcholy grafu jsou součástí nějakého párování / páru). Perfektní párování je vždy maximální.
- **M -střídající cesta** je taková cesta, jejíž vrcholy střídavě leží a neleží v párování.
- **M -zlepšující cesta** je taková M -střídající cesta, jejíž koncové body nejsou saturované (přidáním hrany, která je spojuje, získáme opět párování, které bude mít však o jednu cestu více).

9.3 Stabilní párování

- Pár (z, p) , $z \in P$, $p \in P$ je **nestabilní** v M , jestliže
 - z a p nejsou spárování v M ,
 - spárováním z a p by si polepšil jak zaměstnanec z , tak zaměstnavatel nabízející pozici p ,
- M je stabilní, jestliže v M neexistuje nestabilní pár.
- V úplném bipartitním grafu **stabilní** párování vždy alespoň jedno existuje.

Dvořící algoritmus

Dokud není splněna ukončovací podmínka, probíhá každý den takto:

- **Ráno:** každá žena stojí na svém balkóně. Každý muž stojí pod balkónem ženy, která je nejvýše v jeho seznamu, a dvoří se jí. Muži s prázdným seznamem jsou doma.
- **Odpoledne:** každá žena, pod jejíž balkónem jsou alespoň dva muži, řekne tomu v seznamu nejvýše položenému, aby přišel zítra a ostatním, ať už nechodí.
- **Večer:** každý odehnáný muž si škrtne ze svého seznamu ženu, která ho dnes odehnala.

Ukončovací podmínka: každé ženě se dvoří nejvýše jeden muž.

- Párování, nalezená pomocí dvořícího algoritmu, jsou extrémní. neb pro ty na balkóně dopadnou nejhůře (mohou si vybírat jen z těch, kteří za nimi přijdou) a pro ty pod balkónem nejlépe (jdou za tím nejlepším partnerem).

10 Vyšetření průběhu funkce

- Určíme **definiční obor** funkce.
- **Průsečíky** s :
 - **osou x** získáme dosazením $y = 0$ do f
 - **osou y** získáme dosazením $x = 0$ do f .
- **Body podezřelé z extrémů** získáme pomocí rovnice

$$f'(x) = 0 \rightarrow x_1 = A, x_2 = B, \dots$$

- jejich y souřadnice získáme dosazením kořenů z předchozí rovnice do původní funkce f .

- Pro ověření, zda body podezřelé z extrémů jsou maximum nebo minimum, dosadíme do vztahu

$$f''(x \leftarrow A, x \leftarrow B, \dots).$$

- Pokud je tento výsledek **menší než nula** (< 0), jedná se o **lokální maximum**,
- pokud je tento výsledek **větší než nula** (> 0), jedná se o **lokální minimum**.

11 Derivace a parciální derivace

11.1 Definice

Definice parciální derivace v bodě a

$$a = (a_1, \dots, a_k) \in D_f$$

$$\frac{\partial f}{\partial x_1} = \lim_{x_1 \rightarrow a_1} \frac{f(x_1, a_2, \dots, a_k) - f(a)}{x_1 - a_1}$$

a podobně pro x_2, \dots, x_k .

Pozn.:

- „ ∂ “ je „*partial*“ nebo také „*old-style Greek delta*“, značí parciální derivaci

11.2 Přehled základních derivací

Přehled základních derivací

$$C \frac{d}{dx} = 0$$

$$x^n \frac{d}{dx} = n * x^{n-1}$$

$$\sin x \frac{d}{dx} = \cos x$$

$$\cos x \frac{d}{dx} = -\sin x$$

$$\tan x \frac{d}{dx} = \frac{1}{\cos^2 x}$$

$$\cot x \frac{d}{dx} = -\frac{1}{\sin^2 x}$$

$$e^x \frac{d}{dx} = e^x$$

$$\ln a \frac{d}{dx} = \frac{1}{x}$$

$$\log_a x \frac{d}{dx} = \frac{1}{x \ln a}$$

$$a^x \frac{d}{dx} = a^x \ln a$$

$$\arcsin x \frac{d}{dx} = \frac{1}{\sqrt{1-x^2}}$$

$$\arccos x \frac{d}{dx} = -\frac{1}{\sqrt{1-x^2}}$$

$$(u * v)' = u' * v + u * v'$$

$$\left(\frac{u}{v}\right)' = \frac{u' * v - u * v'}{v^2}$$

11.3 Gradient

- Vektor značící směr nejrychlejšího růstu funkce f .
- Gradient v bodě je vektor nejrychlejšího růstu funkce f z tohoto bodu.
- Gradient skalárně vynásobený vektorem je derivace funkce f v tomto bodě ve směru tohoto vektoru.

Definice gradientu

$$\nabla f(b) = \left(\frac{\partial}{\partial x_1} f(b); \frac{\partial}{\partial x_2} f(b); \dots; \frac{\partial}{\partial x_n} f(b) \right)$$

Pozn.:

- „ ∇ “ je „nabla“, značí gradient

11.4 Jacobiho matice

- Matice parciálních derivací.
- Determinant Jacobiho matice se nazývá *jakobián*.

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

11.5 Parciální derivace vyšších řádů

- 2. parciální derivace = parciální derivace parciálních derivací
- Značení:

$$\begin{aligned} \frac{\partial^2 f}{\partial x_i^2} &= \frac{\partial}{\partial x_i} \frac{\partial f}{\partial x_i} \quad [= \text{derivuj parciální derivaci podle } x \text{ podle } x] \\ \frac{\partial^2 f}{\partial x_i \partial x_j} &= \frac{\partial}{\partial x_j} \frac{\partial f}{\partial x_i} \quad [= \text{derivuj parciální derivaci podle } x \text{ podle } y] \end{aligned}$$

11.6 Gradient ve směru a v bodě**Norma (velikost) vektoru**

$$\|\vec{a}\| = \sqrt{a_1^2 + a_2^2 + \dots + a_n^2}$$

Normalizace vektoru

$$\vec{n} = \frac{\vec{a}}{\|\vec{a}\|} = \left(\frac{a_1}{\|\vec{a}\|}; \frac{a_2}{\|\vec{a}\|}; \dots; \frac{a_n}{\|\vec{a}\|} \right)$$

- Mějme funkci $f(x, y)$, směr \vec{s} a bod $B[a, b]$
- **Gradient v bodě:** Spočteme ∇f v bodě B , tedy $\nabla f(x \leftarrow a, y \leftarrow b)$
 - Další možný zápis gradientu v bodě: $\frac{\partial f}{\partial x}(a, b) = \dots, \frac{\partial f}{\partial y}(a, b) = \dots,$
- Výsledný gradient v bodě a ve směru je („ $*$ “ je skalární součin):

$$\nabla f(B) * \vec{n}.$$

Dále nás může zajímat v **jakém směru či směrech funkce v daném bodě klesá či roste**. Gradient v bodě skalárně vynásobíme obecným vektorem (x, y) , a ptáme se, kdy je výsledek menší než nula (směrnice klesá) či větší než nula (směrnice roste).

12 Funkce více proměnných

- **Kritický bod** – Bod, ve kterém je gradient (všechny derivace) roven nulovému vektoru $\nabla f = (0, 0, 0)$.

– Nalezneme vyřešením soustavy lineárních rovnic.

- Body grafu funkce $f(x, y) = z$ mají souřadnice

$$(x, y, f(x, y)).$$

- Eukleidovská vzdálenost bodů je

$$|AB| = \sqrt{(A - B)^2} = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}$$

12.1 Hessova matice

- Hesseovu maticí zjistíme, zda je kritický bod extrém a případně jaký (minimum, maximum nebo sedlový bod).
- Pokud máme **více bodů podezřelých z extrémů**, dosadíme je do Hesseovy matice, kterou následně vyšetříme.

Definice Hessovy matice

$$\nabla^2 f(x_1, \dots, x_n) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial x_2^2} & \cdots & \frac{\partial^2 f}{\partial x_2 \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \frac{\partial^2 f}{\partial x_n \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_n^2} \end{pmatrix} \left[= \begin{pmatrix} \text{x podle x} & \text{x podle y} & \text{x podle z} \\ \text{y podle x} & \text{y podle y} & \text{y podle z} \\ \text{z podle x} & \text{z podle y} & \text{z podle z} \end{pmatrix} \right]$$

- *Hessián* je zkrácené pojmenování pro Hessovu matici.

12.2 Definitnost

- Vlastnost regulárních⁵ matic, která je definována jako

$$(v) * (A) * (v)^T \text{ např.: } \begin{pmatrix} x & y \end{pmatrix} * (A) * \begin{pmatrix} x \\ y \end{pmatrix}$$

- Pokud je výsledek po vynásobení libovolným vektorem
 - vždy > 0 je matice pozitivně definitní,
 - vždy < 0 je matice negativně definitní.
- Pokud má výsledek po vynásobení různými vektory různá znaménka, je matice indefinitní.

⁵Čtvercová matice, jejíž determinant je různý od nuly, tzn. $\det(A) \neq 0$

12.2.1 Sylvestrovo kritérium

- Můžeme použít pouze pro *symetrické matice*.
- Spočítáme *rohové subdeterminanty*:

$$\nabla^2 f = \left(\underbrace{\begin{array}{ccc|ccc} \boxed{M1} & \cdots & \cdots & & & \\ \cdots & \boxed{M2} & \cdots & & & \\ \cdots & \cdots & \boxed{M3} & & & \end{array}}_{\text{Hasseova matice}} \right)$$

Vyhodnocení výsledků

- Pokud $\forall i : \det(M_i) > 0 \Leftrightarrow$ matice M je **pozitivně definitní**.
- Pokud $\forall j : \det(M_{2j+1}) < 0$ a $\det(M_{2j}) > 0 \Leftrightarrow$ matice M je **negativně definitní**
 - tj.: „–“ (levý horní roh) \rightarrow „+“ \rightarrow „–“ $\rightarrow \dots$ (pravý dolní roh).
- Pokud má matice na diagonále **alespoň dva prvky**, kde je jeden kladný a druhý záporný, je matice **indefinitní**
- Pokud neplatí ani jedno, není možné touto metodou definitnost určit (přesněji řečeno: Hesseova matice není pozitivně ani negativně definitní) a musíme použít jinou metodu.

Determinant matice pomocí Sarussova pravidla

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = (a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{12}a_{23}a_{31}) - (a_{13}a_{22}a_{31} + a_{12}a_{21}a_{33} + a_{23}a_{32}a_{11})$$

12.2.2 Kvadratická forma matice

$$\vec{v} = (x, y, z) :$$

$$(x \ y \ z) \underbrace{\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}}_{\text{Hesseova matice}} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = (x(a+d+g) \ y(b+e+h) \ z(c+f+i)) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \dots$$

- Do výsledku dosazujeme libovolné vektory a zjišťujeme, zda je celý výraz kladný nebo záporný:
 - Je výraz vždy kladný \rightarrow Hesseova matice je **pozitivně definitní** \rightarrow bod je lokální minimum
 - Je výraz vždy záporný \rightarrow Hesseova matice je **negativně definitní** \rightarrow bod je lokální maximum
 - Je výraz kladný i záporný \rightarrow Hesseova matice je **indefinitní** \rightarrow bod je *sedlový bod*
 - Matice může být i „semidefinitní“ a to tehdy, když pro nenulový vektor je výsledek nulový

12.3 Tečná rovina

- Obecná rovnice roviny:

$$ax + by + cz + d = 0$$

Rovnice tečné roviny ke grafu funkce $f(x, y)$ v bodě $[a, b]$

$$\frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(a, b)(y - b) - z + f(a, b) = 0$$

Jedná se tedy o rovinu s normálovým vektorem

$$\vec{n} = \left(\frac{\partial f}{\partial x}(a, b), \frac{\partial f}{\partial y}(a, b), -1 \right).$$

13 Integrály

13.1 Tabulkové integrály

Přehled tabulkových integrálů

$$\begin{aligned} \int 0 \, dx &= c \\ \int a \, dx &= ax + c \\ \int x^n \, dx &= \frac{1}{n+1} x^{n+1} + c \text{ pro } x > 0, n \in \mathbb{R} \text{ a } n \neq -1 \\ \int \frac{1}{x} \, dx &= \ln |x| + c \text{ pro } x \neq 0 \\ \int e^x \, dx &= e^x + c \\ \int a^x \, dx &= \frac{a^x}{\ln(a)} + c \text{ pro } a > 0, \text{ a } a \neq 1 \\ \int \sin x \, dx &= -\cos x + c \\ \int \cos x \, dx &= \sin x + c \end{aligned}$$

Integrace *per partes* (integrace po částech):

$$\int u * v' = uv - \int u' * v$$

13.2 Newtonova formule

Vyjádření integrálu na intervalu $\langle a, b \rangle$ pomocí primitivní funkce $F(x)$ se nazývá Newtonova formule. Platí, pokud je funkce $f(x)$ spojitá na intervalu $\langle a, b \rangle$ a funkce $F(x)$ je k ní na intervalu $\langle a, b \rangle$ primitivní.

$$\int_a^b f(x) dx = [F(x)]_a^b = F(b) - F(a)$$

13.3 Integrály přes obdélníkovou oblast

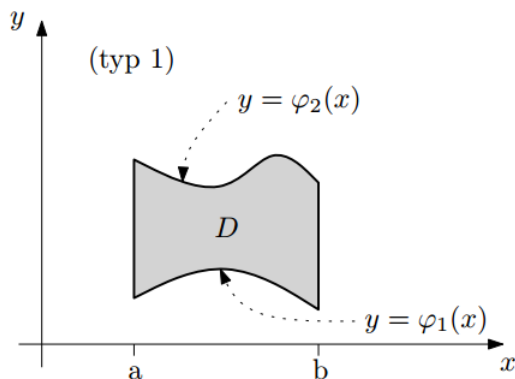
$$\iint_D f(x, y) dx dy = \int_a^b \left(\int_c^d f(x, y) dy \right) dx$$

13.4 Integrály přes obecnou oblast

Uvažujeme dva typy oblastí

- **Typ 1:** x je z intervalu $\langle a, b \rangle$ a y je omezené spojitými funkcemi $\varphi_1(x)$ a $\varphi_2(x)$.

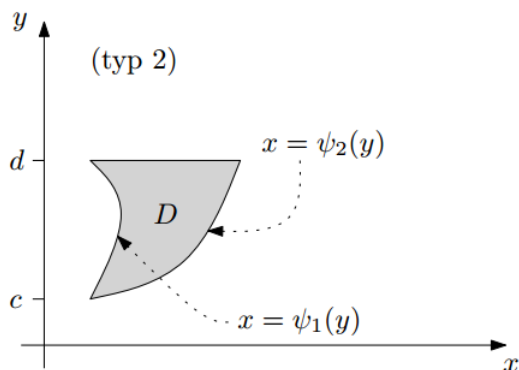
$$\iint_D f(x, y) dx dy = \int_a^b \left(\int_{\varphi_1(x)}^{\varphi_2(x)} f(x, y) dy \right) dx$$



Obrázek 4: Dva typy integrálů přes obecnou oblast

- **Typ 2:** y je z intervalu $\langle c, d \rangle$ a x je omezené spojitými funkcemi $\psi_1(y)$ a $\psi_2(y)$.

$$\iint_D f(x, y) dx dy = \int_c^d \left(\int_{\psi_1(y)}^{\psi_2(y)} f(x, y) dx \right) dy$$



Obrázek 5: Dva typy integrálů přes obecnou oblast

Poznámka k příkladu 2.2 ve cvičení 12: Vypočítejte $\iint_D f(x+y)^2 dx dy$. Zde budeme vyjadřovat y pomocí x (tj. $f(y) = x \dots$ – funkce ohraničující „shora“ a „zdola“ trojúhelník), poté se budeme automaticky omezovat na ose x .

$$\int_{x_1}^{x_2} \left(\int_{y_1}^{y_2} (\dots) dy \right) dx$$

14 Numerické metody řešení soustav lineárních rovnic

- Přímá metoda – počítá řešení v konečném počtu kroků tak, že v teoretické absolutní přesnosti dává přesné řešení.
 - Např. Gaussova eliminace (se složitostí $\mathcal{O}(n^3)$).
- Iterační metoda – hledají přibližná řešení problému tak, že konstruují posloupnost přibližných řešení (vektorů) x_0, x_1, \dots tak, že každé další řešení je odvození z předchozího. Další členy vypočítáme z předpisu

$$Qx_k = (Q - A)x_{k-1} + b$$

pro všechna $k > 0$. Na začátku (kdy ještě nemáme předchozí výsledek) se volí x_k náhodně. Předpis pro řešený problém je

$$Ax = b.$$

V iterační metodě počítáme chybu (odchylku) jako $\|Ax_k - b\|$.

Konkrétní zvolené Q závisí na zvolené metodě:

- Richardsonova metoda

$$Q = I = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

- Jacobiho metoda

$$Q = D = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & a_{2,2} & \ddots & \cdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & a_{n,n} \end{pmatrix}$$

- superrelaxační metoda (SOR metoda)

$$Q = \frac{1}{\omega} D + L, \text{ kde } \omega \in \mathbb{R} \setminus \{0\}$$

Značení matic:

- L je dolní trojúhelníková matice s prvky matice A ,
- D je diagonální matice s prvky matice A na diagonále,
- I je jednotková matice.

15 Fuzzy matematika

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.

15.1 Vzdálenost a podobnost

Vzdálenost $\downarrow \sim$ podobnost \uparrow

Vzdálenosti založené na normě vektoru:

- Minkovského

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

- Eukleidovská

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

- Manhatanská

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

- Mahalanobisova vzdálenost – vzdálenost realizací x, y náhodných vektorů X, Y splňujících $\text{var}X = \text{var}Y$.
– Jde o obecné měřítko vzdálenosti beroucí v úvahu korelaci mezi parametry

Další míry podobnosti náhodných veličin dle korelačních koeficientů:

- Pearsonův
- Spearmanův
- Kendallův

Podobnost binárních vektorů:

- Hammingova vzdálenost

15.2 Fuzzy množiny

- Fuzzy logika může operovat se všemi hodnotami z intervalu $\langle 0; 1 \rangle$, kterých je nekonečně mnoho.

15.2.1 Průnik (součin) fuzzy množin (T -normy)

Průnik je definován jako binární operace

$$T : \langle 0, 1 \rangle^2 \rightarrow \langle 0, 1 \rangle$$

, která splňuje následující operace

- komutativita ,
- asociativita
- monotonie
- okrajová podmínka

Příklady norem

- Gödelova (drastická) norma

$$\mu_{A \cup B}(x) = \max(\mu_A(x); \mu_B(x))$$

- Łukasiewiczzova norma

$$\mu_{A \cup B}(x) = \min(\mu_A(x) + \mu_B(x); 1)$$

- Součinnová norma

$$\mu_{A \cup B}(x) = (\mu_A(x) + \mu_B(x); 1) - (\mu_A(x) * \mu_B(x); 1)$$

15.2.2 De Morganovy zákony a T -konormy (součet – sjednocení)

- Komutativita

$$\perp(a, b) = \perp(b, a)$$

- Monotonie

$$\perp(a, b) \leq \perp(c, d) \text{ když } a \leq c \text{ a } b \leq d$$

- Asociativita

$$\perp(a, \perp(b, c)) = \perp(\perp(a, b), c)$$

- Identický element

$$\perp(a, 0) = a$$

15.3 Kopule

- Kopule je pojítka mezi fuzzy matikou a pravděpodobností.
- Kopule se hodí v pravděpodobnosti, kde ukazují závislost mezi dvěma náhodnými veličinami.

15.4 Defuzzifikace

- Defuzzifikace - zobrazení fuzzy množiny do jejího univerza.
- K čemu to je - mám přístroj řízený fuzzy množinou, ale abych ho nastavil, potřebuju znát jednu konkrétní hodnotu.

16 Optimalizace

16.1 Typy optimalizačních úloh

- **Diskrétní (==kombinatorické)** – proměnné z konečné, často velmi velké, množiny. Např. požadavek, proměnné x_i celá čísla či $x_i \in \{0, 1\} \rightarrow$ integer programming problems.
- **Spojité** – proměnné reálná čísla či prvky z nespočetných množin. Jednodušší řešení - lze použít spojitost a hladkost funkce, napoví hodně o chování funkce v okolí daného bodu.

Algoritmy mohou být:

- Deterministické
- Stochastické – každý běh jiný

16.2 typy optimalizačních metod

- Hladká optimalizace - Využívá parciální derivace cílové funkce - Gradient f – směr nejprudšího růstu do lokálního maxima - -Gradient f – směr nejprudšího poklesu - Někdy se používá i 2. Parciální derivace – Hessova matice
- Stochastická – evoluční a genetické algoritmy