# 3 - Komprimace dat

## (ztrátová a neztrátová komprimace, algoritmy pro kompresi textu, obrazu, audia a videa)

**Ztrátová a neztrátová komprimace** - u bezztrátové se zpětnou dekomprimací data rekonstruují tak, že jsou totožná s daty původními. Ztrátová během komprese vypustí data, která nejsou příliš důležitá (například frekvence mimo rozsah lidských smyslů).

**Algoritmy pro kompresi textu, obrazu, audia a videa** - mohou být statické (stále stejné) nebo dynamické (mění se dle vstupních dat, dva průchody vstupem) a proudové (po bytech) nebo blokové (po blocích dat).

- Text - Bzip2 - RLE + BWT (poslední sloupec seřazených rotací vstupu) + MTF + Huffman (aritmetické kódování u Bzip, lepší).
- Obraz
    - Bezztrátové - RLE (např. u GIFu) / LZW (slovník) + Huffman
    - Ztrátové - JPEG - redukujeme barvy zprůměrováním barevných složek sousedních pixelů, provedeme diskrétní kosinovou transformaci a vynecháme vysokofrekvenční změny (lidské oko na ně není citlivé) - kvantizace, poté RLE + Huffman metodou cikcak, protože většina koeficientů v pravém dolním rohu má nulovou hodnotu.
- Audio - MP3 - omezíme frekvenční rozsah dle lidského ucha (20 Hz - 20 kHz), nakvantujeme hodnoty tak, aby vzniklý šum byl pod rozlišovací schopností ucha. Využijeme maskování, hlasitý tón zastíní slabší signál v době, kdy zní, ale i chvíli po něm (asi 100 ms) a chviličku před ním (2 - 5 ms). Zbytek zakódujeme huffmanovým kódováním.
- Video - MPEG - rozdělí jednotlivé snímky na 3 kategorie, I, B a P. Rámec I je nezávisle zobrazitelný, zkomprimován pouze jako JPEG, rámec P je určen pouze rozdílem oproti předchozímu I nebo P a rámec B je zkomprimován pouze rozdílem oproti předchozímu a následujícímu I nebo P (popřípadě zcela vynechán). Obvyklá sekvence je I B B P B B P B B P B B I

# 4 - Kryptologie

## (vývoj kryptografie a kryptoanalýzy, symetrická kryptografie (DES, AES), asymetrická kryptografie (RSA, certifikáty, digitální podpis), kvantová kryptografie)

**Vývoj kryptografie a kryptoanalýzy** - kryptografie je skrývání zpráv, kryptoanalýza prolomením kryptografie, kryptografie dnes vyhrává. (od nejstarší po nejmladší)

- Substituční šifry - nahrazování jednotlivých písmen jinými (např. Césarova)
- Transpozice - proházení pořadí písmen.
- Frekvenční analýza - základní nástroj kryptoanalýzy.
- Vigenérova šifra - dá se rozluštit, ale pokud je klíč stejně dlouhý jako zpráva, náhodný a jedinkrát použitý, tak je matematicky dokázána nerozluštitelnost.
- Enigma - rozluštěno Turingem.
- Kód Navajů

**Symetrická kryptografie (DES, AES)** - šifrování a dešifrování pomocí stejného klíče.

- DES - rozdělí vstupní text do bloků, nad každým provede různé nahrazování symbolů a permutace pomocí klíče. V dnešní době však prolomitelný hrubou silou, dá se řešit trojnásobnou aplikací (3DES).
- AES - lepší a novější alternativa k 3DES. Také se jedná o blokovou šifru, nad každým blokem provádí nahrazování symbolů a bitové operace.

**Asymetrická kryptografie (RSA, certifikáty, digitální podpis)** - šifrování pomocí veřejného klíče, dešifrování pomocí soukromého klíče (řeší problém distribuce klíče).

- RSA - postavena na předpokladu že rozklad čísla na součin prvočísel (faktorizace) je velmi obtížný.
- Certifikáty - digitálně podepsaný veřejný šifrovací klíč, který je podepsaný důvěryhodnou třetí stranou (je důvěra tranzitivní? Web of Trust (síť důvěry) si myslí, že ano, veřejná správa jim však nedůvěřuje). HTTPS důvěryhodné kořenové certifikáty jsou přímo součástí WWW prohlížeče. Zněmožňuje padělat veřejné klíče.
- Digitální podpis - opačný přístup než běžné šifrování, zpráva je zašifrována pomocí soukromého klíče a může ji rozšifrovat každý pomocí veřejného klíče, čímž si ověří, že zprávu skutečně poslal majitel soukromého klíče. Dá se kombinovat, čímž dosáhneme toho, že zprávu přečte pouze adresát a ví, že ji poslal pravý odesilatel.

**Kvantová kryptografie** - vychází z kvantové fyziky a využívá hlavně toho, že některé jevy jsou náhodné a hlavně měření mění stav, což lze detekovat a odhalit tím případný odposlech. Jednou z možností kvantové kryptografie je využití polarizace fotonů, kde odposlech fotonů s jinou polarizační bází než je u odesilatele vede k náhodnému stavu fotonu, a tak s 50% šancí dorazí k příjemci chybně a odposlech je odhalen.

# 10 - Teoretická informatika

## (konečné a nekonečné množiny, Cantorova metoda diagonalizace, množinové operace, relace, zobrazení, algebraické struktury)

**Konečné a nekonečné množiny**

- Konečné - mají počet prvků
- Nekonečné - určujeme mohutnost (kardinalitu), množiny mají stejnou mohutnost, pokud mezi nimi existuje bijekce.
    - Spočetné - mají stejnou mohutnost jako množina přirozených čísel (množina sudých čísel), tedy mohutnost (kardinální číslo) alef0.
    - Nespočetné - ostatní (množina reálných čísel), tedy mohutnost množiny všech podmnožin spočetné množiny, což označujeme za mohutnost kontinua c. Nejvyšší kardinální číslo neexistuje, potenční množina má vždy vyšší mohutnost.

**Cantorova metoda diagonalizace** - důkaz sporem, že existují nespočetné množiny. Napíšeme do matice všechna reálná čísla a vezmeme číslo z diagonály, kterému změníme všechny číslice. Nové číslo je reálné, ale evidentně není v matici, protože v místě původní diagonály bude mít vždy jinou číslici -> nelze vytvořit nekonečnou posloupnost nespočetné množiny. Podobným způsobem se dokazuje, že existují problémy neřešitelné Turingovým strojem.

**Množinové operace, relace, zobrazení**

- Množinové operace - sjednocení, průnik, rozdíl a doplněk
    - Potenční množina - množina všech podmnožin.
- Relace - podmnožina kartézského součinu.
    - Kartézský součin - množina všech uspořádaných dvojic, kde první prvek patří do první množiny a druhý prvek do druhé množiny.
- Zobrazení - speciální případ binární relace, kde je zajištěna jednoznačnost obrazu ke každému vzoru.
    - Injektivní (prosté) - jeden obraz má právě jeden vzor.
    - Surjektivní (na) - každý obraz má alespoň jeden vzor.
    - Bijektivní - injektivní i surjektivní zobrazení.

**Algebraické struktury** - je v matematice každá množina, na které jsou definované nějaké operace a daná množina je vzhledem k těmto operacím uzavřená, tzn. že výsledkem operace nad prvky této množiny je vždy také prvek této množiny.

- Jedna operace - grupoid (jedna operace), pologrupa (asociativní grupoid), monoid (pologrupa s neutrálním prvkem), grupa (monoid s inverzními prvky).
- Dvě operace - polookruh (N s nulou), okruh (Z, existují inverzní prvky pro sčítání), těleso (R, existují inverzní prvky pro sčítání i násobení).

# 11 - Umělá inteligence

## (inteligentní agenti - definice, význam, vlastnosti a autonomie. Základní typy IA, jejich struktura, komunikace. Multiagentní systémy. Samoučící se agenti a teorie her)

**Inteligentní agenti - definice, význam, vlastnosti a autonomie.**

- Definice - objekt, který vnímá své prostředí pomocí senzorů a působí na něj pomocí efektorů, jsou schopni inteligentně a výkonně působit na své okolí.
    - Ideální racionální agent - Pro jakoukoliv sekvenci vnímání, ideální racionální agent učiní vše, co se od něj očekává pro maximalizaci míry jeho výkonnosti, a to na základě evidence poskytnuté sekvencí vnímání a znalosti, kterou agent disponuje.
- Význam - schopnost ulehčit lidské práci na určité úrovni autonomie.
- Vlastnosti
    - Autonomie - je schopen dosáhnout svých záměrů bez vnějších zásahů, tj. pouze interakcí s prostředím.
    - Reaktivita - schopnost průběžně reagovat na změny prostředí.
    - Intencionalita - schopnost uvažovat o svých dlouhodobých cílech.
    - Sociální inteligence - schopnost komunikovat s ostatními agenty.
- Autonomie - IA by měl mít schopnost se učit na základě vnímání a využít toho k úspěšné činnosti v širokém rozsahu prostředí.

**Základní typy IA, jejich struktura, komunikace** - mapování ze sekvencí vnímání do akcí pomocí explicitní vyhledávací tabulky není často možné, protože se jedná o obrovské množství možných vjemů (nehledě na možnost neočekávané změny prostředí). Jiné přístupy (inkrementy):

- Jednoduší reflexní agenti - sloučíme části tabulky na IF-THEN pravidla, (brzdí-li automobil před námi, zabrzdíme také).
- Agenti sledující svět - správné rozhodnutí nemusí být možno udělat pouze na základě okamžitého vjemu, proto si udržujeme informace o vývoji světa nezávisle na agentovi a o účincích agentovi akce na svět.
- Agenti zaměřeni na cíl - uvažuje o budoucnosti, vybírá správnou akci k dosažení cíle, (kam máme jet na křižovatce?)
- Užitkově zaměření agenti - řeší jak dosáhnout cíle s nejvyšším užitkem (reálná hodnota), díky tomu můžeme řešit kompromisní řešení nebo volit nejpravděpodobnější možnosti.

**Multiagentní systémy** - simulované prostředí se síťovým charakterem, v němž dochází k interakci agentů mezi sebou a / nebo s prostředím, ve kterém se nacházejí. Tito agenti řeší

společně problémy, které přesahuji možnosti a znalosti každého z nich. (Např. simulace mraveniště)

**Samoučící se agenti a teorie her**

- Samoučící agenti - agenti, jejichž akce jsou ovlivněny předchozími zkušenostmi. Uchovávají si historii činností, kterou berou v potaz při další akci.
- Teorie her - disciplína aplikované matematiky řešící konfliktní rozhodovací situace. Hry zapisujeme buď pomocí matic (normální forma, většinou současné hry jako kámen-nůžky-papír) nebo pomocí stromů (extenzivní forma, většinou sekvenční hry jako piškvorky). Hry v extenzivní formě můžeme řešit pomocí algoritmu Minimax, nebo jeho optimaluzace alfa-beta prořezávání, kde vynecháváme procházení některých stavů, protože nemůžou ovlivnit výsledek.

# 12 - Umělá inteligence

## (prohledávání stavového prostoru - základní algoritmy, princip, použití. Heuristické postupy. Plánování (plány a jejich reprezentace) a rozhodování)

**Prohledávání stavového prostoru - základní algoritmy, princip, použití**

- Neinformované
    - BFS - prohledávání do šířky, vyber uzel, expanduj jeho sousedy a vlož je do fronty OPEN, opakuj dokud není fronta prázdná. Možné vylepšení pomocí seznamu CLOSED pro již projité uzly.
    - DFS - prohledávání do hloubky, vyber uzel, expanduj jeho sousedy a vlož je do zásobníku OPEN, opakuj dokud není zásobník prázdný. Možné vylepšení pomocí seznamu CLOSED pro již projité uzly.
- Informované (best-first-search) - uzly s nejlepším ohodnocením jsou expandovány jako první, snaha zabránit v zabloudění
    - UCS - uniformně cenové hledání - dijkstrův algoritmus, prioritní fronta na základě délky trasy do daného okamžiku.
    - Greedy search - lačné hledání - prioritní fronta na základě heuristiky odhadu délky do cíle. Připomíná během DFS (není optimální).
    - A* - prioritní fronta na základě délky trasy do daného okmažiku + heuristiky odhadu délky do cíle. Stejně jako UCS je optimální, pokud heuristika nikdy nepřeceňuje (přijatelná heuristika), ale může být efektivnější.

**Heuristické postupy** - různé způsoby, často experimentální: problém 8 čtverečků v 9 polích. Prvním způsobem je heuristika na základě počtu špatných čtverečků (0-8), druhým způsobem je součet manhattanských vzdáleností čtverečků od jejich správné pozice. Zjišťujeme, že druhá heuristika je vždy lepší, tedy dominuje první.

**Plánování (plány a jejich reprezentace) a rozhodování** - podobné jako agent řešící problémy, ale v tomto případě agent konstruuje plány k dosaženích svých cílů, které následně provede. Reprezentace plánů je většinou ve formálních jazycích (např. logika). Výhodou je, že takový agent může přidávat akce k plánu, kdykoliv jsou ty akce zapotřebí, také můžeme cíle snadněji dekomponovat na jednotlivé subcíle.