Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Bakalářské státnice

Peter Černo, 2010
petercerno@gmail.com

Anotace: Studium je zakončeno státní závěrečnou zkouškou. Ta má dvě části, jimiž jsou obhajoba bakalářské práce a ústní část. K oběma částem státní závěrečné zkoušky se posluchač poprvé přihlašuje najednou. Studium je úspěšně zakončeno po úspěšném absolvování obou těchto částí.

Podmínky pro přihlášení ke státní závěrečné zkoušce:

1. získání alespoň 180 kreditů
2. splnění všech povinných předmětů zvoleného oboru
3. splnění povinně volitelných předmětů zvoleného oboru ve stanoveném rozsahu
4. odevzdání vypracované bakalářské práce ve stanoveném termínu.

Předmět lze splnit jeho úspěšným absolvováním nebo uznáním z předchozího studia.

Ústní část státní závěrečné zkoušky se skládá ze dvou předmětů, jimiž jsou Základy matematiky a Základy informatiky. Požadavky ke zkoušce se pro jednotlivé obory mírně odlišují, značná část požadavků je však stejná a vychází z obsahu výuky společných povinných předmětů. Odlišnosti mezi jednotlivými obory spočívají převážně v tom, na které znalosti je u zkoušky kladen důraz a požadují se podrobněji. Případné specifické požadavky pro jednotlivé obory jsou převážně pokryty výukou povinně volitelných předmětů.

Požadavky znalostí ke státní závěrečné zkoušce:

Základy matematiky:

1. Čísla

   Vlastnosti přirozených, celých, racionálních, reálných a komplexních čísel. Posloupnosti a limity. Cauchyovské posloupnosti.

2. Základy diferenciálního počtu

   Reálné funkce jedné reálné proměnné. Spojitost, limita funkce v bodě (vlastní i nevlastní). Některé konkrétní funkce (polynomy, racionální lomené funkce, goniometrické a cyklometrické funkce, logaritmy a exponenciální funkce). Derivace: definice a základní pravidla, věty o střední hodnotě, derivace vyšších řádů. Některé aplikace (průběhy funkcí, Newtonova metoda hledání nulového bodu, Taylorův polynom se zbytkem).

3. Integrál

   Primitivní funkce, metody výpočtu. Určitý (Riemannův) integrál, užití určitého integrálu. Vícerozměrný integrál a Fubiniho věta.

4. Základy teorie funkcí více proměnných

   Parciální derivace a totální diferenciál, věty o střední hodnotě, extrémy funkcí více proměnných, věta o implicitních funkcích.

5. Metrické prostory

   Definice metrického prostoru, příklady. Definice topologického prostoru. Spojitost, otevřené a uzavřené množiny.

6. Základní algebraické struktury

   Grupa, okruh, těleso - definice a příklady. Malá Fermatova věta. Dělitelnost a ireducibilní rozklady polynomů. Rozklady polynomů na kořenové činitele pro polynom s reálnými, racionálními, komplexními koeficienty. Násobnost kořenů a jejich souvislost s derivacemi mnohočlenu.

7. Vektorové prostory

   Základní vlastnosti vektorových prostorů, podprostory, generování, lineární závislost a nezávislost. Věta o výměně. Konečně generované vektorové prostory, base. Lineární zobrazení.

8. Skalární součin

   Vlastnosti v reálném i komplexním případě. Norma. Cauchy-Schwarzova nerovnost. Kolmost. Ortogonální doplněk a jeho vlastnosti.

9. Řešení soustav lineárních rovnic

   Lineární množiny ve vektorovém prostoru, jejich geometrická interpretace. Řešení soustavy rovnic je lineární množina. Frobeniova věta. Řešení soustavy úpravou matice. Souvislost soustavy řešení s ortogonálním doplňkem.

10. Matice

    Matice a jejich hodnost. Operace s maticemi a jejich vlastnosti. Inversní matice. Regulární matice, různé charakteristiky. Matice a lineární zobrazení, resp. změny souřadných soustav.

11. Determinanty

    Definice a základní vlastnosti determinantu. Úpravy determinantů, výpočet. Geometrický smysl determinantu. Minory a inversní matice. Cramerovo pravidlo.

12. Vlastní čísla a vlastní hodnoty

    Vlastní čísla a vlastní hodnoty lineárního operátoru resp. čtvercové matice. Jejich výpočet, základní vlastnosti. Uvedení matice na diagonální tvar v případě různých vlastních čísel. Informace o Jordanově tvaru v obecném případě.

13. Algebra

    Grupa, okruh, těleso - definice a příklady. Podgrupa, normální podgrupa, faktorgrupa, ideál. Homomorfismy grup a dalších struktur. Podílová tělesa.

14. Diskrétní matematika

    Uspořádané množiny. Množinové systémy, párování, párování v bipartitních grafech (systémy různých reprezentantů). Kombinatorické počítání. Princip inkluze a exkluze. Latinské čtverce a projektivní roviny.

15. Teorie grafů

    Základní pojmy teorie grafů, reprezentace grafu. Stromy a jejich základní vlastnosti, kostra grafu. Eulerovské a hamiltonovské grafy. Rovinné grafy, barvení grafů.

16. Pravděpodobnost a statistika

    Náhodné jevy, podmíněná pravděpodobnost, nezávislost náhodných jevů. Náhodné veličiny, střední hodnota, rozdělení náhodných veličin, normální a binomické rozdělení. Lineární kombinace náhodných veličin. Bodové odhady, intervaly spolehlivosti, testování hypotéz, t-test, chíkvadrát test, lineární regrese.

17. Kompaktnost, úplnost, posloupnosti a řady funkcí

    Kompaktní metrické prostory, kompaktní topologické prostory. Úplné metrické prostory. Aplikace metrických a topologických prostorů. Stejnoměrná konvergence. Mocninné a Taylorovy řady. Fourierovy řady. Aplikace.

18. Optimalizační metody

    Minimaxové věty. Geometrická interpretace - mnohostěny. Základy lineárního programování, věty o dualitě, algoritmy - simplexová a elipsoidová metoda.

Základy informatiky:

1. Logika

   Jazyk, formule, sémantika, tautologie. Rozhodnutelnost, splnitelnost, pravdivost, dokazatelnost. Věty o kompaktnosti a úplnosti výrokové a predikátové logiky. Normální tvary výrokových formulí, prenexní tvary formulí predikátové logiky.

2. Automaty a jazyky

   Chomského hierarchie, třídy automatů a gramatik, determinismus a nedeterminismus. Uzávěrové vlastnosti tříd jazyků.

3. Algoritmy a datové struktury

   Časová složitost algoritmů, složitost v nejhorším a průměrném případě. Třídy složitosti P a NP, převoditelnost, NP-úplnost. Metoda ,,rozděl a panuj" - aplikace a analýza složitosti. Binární vyhledávací stromy, vyvažování, haldy. Hašování. Sekvenční třídění, porovnávací algoritmy, přihrádkové třídění, třídící sítě. Grafové algoritmy - prohledávání do hloubky a do šířky, souvislost, topologické třídění, nejkratší cesta, kostra grafu, toky v sítích. Tranzitivní uzávěr. Algoritmy vyhledávání v textu. Algebraické algoritmy - DFT, Euklidův algoritmus. Základy kryptografie, RSA. Pravděpodobnostní algoritmy - testování prvočíselnosti. Aproximační algoritmy.

4. Databáze

   Architektury databázových systémů. Konceptuální, logická a fyzická úroveň pohledů na data, B-stromy a jejich varianty. Relační datový model, relační algebra, normální formy, referenční integrita. SQL. Transakční zpracování, vlastnosti transakcí. Technologie XML, XML Schema.

5. Architektury počítačů a sítí

   Architektury počítače. Procesory, multiprocesory. Vstupní a výstupní zařízení, ukládání a přenos dat. Architektury OS. Procesy, vlákna, plánování. Synchronizační primitiva, vzájemné vyloučení. Zablokování a zotavení z něj. Organizace paměti, alokační algoritmy. Principy virtuální paměti, stránkování. Systémy souborů, adresářové struktury. Bezpečnost, autentizace, autorizace, přístupová práva. ISO/OSI vrstevnatá architektura sítí. TCP/IP. Spojované a nespojované služby, spolehlivost, zabezpečení protokolů.

6. Programovací jazyky

   Principy implementace procedurálních a objektově orientovaných jazyků, oddělený překlad, sestavení. Objektově orientované programování. Neprocedurální programování, logické programování. Generické programování – šablony a generika.

18.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

1 ČÍSLA

1.1 $\mathbb{R}(+,\cdot,-,0,1)$ KOMUTATÍVNE TELESO
TJ. KOMUTATÍVNY OKRUH T.Ž. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

+ VLASTNOSTI USPORIADANIA $\leq$
ČIASTOČNÉ USPORIADANIE, $\forall x,y \in \mathbb{R}: x \leq y \vee y \leq x$
⊕ $\forall x,y,z \in \mathbb{R}: x \leq y \Rightarrow x+z \leq y+z$
⊕ $\forall x,y,z \in \mathbb{R}: x \leq y \wedge 0 \leq z \Rightarrow x \cdot z \leq y \cdot z$!
+ NETRIVIALITA : $0 \neq 1$
+ ÚPLNOSŤ : $(\mathbb{R}, \leq)$ JE ÚPLNÝ ZVÄZ

1.2 $S \subseteq \mathbb{R}$ INDUKTÍVNA. $\mathbb{N} = \bigcap \{S,\ S \subseteq \mathbb{R}$ INDUKTÍVNA$\}$
VLASTNOSTI $\mathbb{N}$, $\mathbb{N}$ JE DOBRE USP.
ARCHIMEDOVA VLASTNOSŤ
PEANOVE AXIÓMY, $0, \sigma, 0 \notin \operatorname{rng} \sigma$, σ JE PROSTÁ, AX. INDUKCIE
KONŠTRUKCIA : $0 := \emptyset$, $\sigma(x) = x \cup \{x\}$

1.3 ZAVEDENIE $\mathbb{Z}$, $\mathbb{Q}$ (PODIELOVÉ TELESO)
EXISTENCIA $\lfloor \cdot \rfloor$, HUSTOTA $\mathbb{Q}$, N-TÁ ODMOCNINA

1.4 ZAVEDENIE $\mathbb{C}$, KOMPLEXNE ZDRUŽENÉ ČÍSLO, ABS. HODN.
GONIOMETRICKÝ TVAR, MOIVREOVA VETA

1.5 $\{a_n\}_{n=1}^{\infty}$, $\lim_{n\to\infty} a_n$, ZÁKLADNÉ VLASTNOSTI
VLASTNÝCH, NEVLASTNÝCH LIMÍT,
LIMES SUPERIOR, LIMES INFERIÓR

POZRI
$\lim \sqrt[n]{n} = 1$

PLATÍ : $\lim a_n = A \in \mathbb{R}^* \iff \limsup a_n = \liminf a_n = A \in \mathbb{R}^*$
HROMADNÁ HODNOTA POSTUPNOSTI

1.6 CAUCHYOVSKÉ POSTUPNOSTI :
BOLZANO - CAUCHYOVA PODMIENKA

BOLZANO - WEIERSTRASS : Z KAŽDEJ OHRANIČENEJ POSTUPNOSTI MÔŽEME VYBRAŤ KONVERGENTNÚ PODPOSTUPNOSŤ

LEMMA: KEĎ MÁ CAUCHYOVSKÁ POSTUPNOSŤ KONVERGENTNÚ PODPOSTUPNOSŤ, POTOM JE KONVERGENTNÁ

BOLZANO - CAUCHY : $\{a_n\}_{n=1}^{\infty}$ JE KONVERGENTNÁ $\Leftrightarrow$ JE CAUCHYOVSKÁ.

$\Rightarrow$) ZREJMÉ, $\Leftarrow$) CAUCHYOVSKÁ POSTUPNOSŤ JE OHRANIČENÁ

2 ZÁKLADY DIFERENCIÁLNEHO POČTU

PRSTENCOVÉ OKOLIE, OKOLIE, LIMITA, SPOJITOSŤ 2.1, 2.2

HEINEHO VETA : NECH $f: M \to \mathbb{R}$, $M \subseteq \mathbb{R}$ JE DEFINOVANÁ NA NEJAKOM PRSTENCOVOM OKOLÍ BODU $a \in \mathbb{R}^*$. POTOM $\lim_{x \to a} f(x) = A \in \mathbb{R}^* \Leftrightarrow \forall \{x_n\}_{n=1}^{\infty}$: $x_k \in \operatorname{dom} f$ $\forall k \in \mathbb{N}$, $x_k \neq a$ $\forall k \in \mathbb{N}$ PLATÍ $(\lim x_n = a \Rightarrow \lim f(x_n) = A)$.

VETA O LIMITE ZLOŽENEJ FUNKCII :

$\lim_{x \to a} g(x) = A$, $\lim_{x \to A} f(x) = B$, $a, A, B \in \mathbb{R}^*$ A PLATÍ BUĎ

(P1) : f JE SPOJITÁ V A $(f(A) = B)$, ALEBO (VONKAJŠIA JE SPOJITÁ)

(P2) : $\exists \delta > 0 : \forall x \in P(a, \delta) : g(x) \neq A$ (VNÚT. JE „LOKÁLNE PROSTÁ")

POTOM : $\lim_{x \to a} f \circ g(x) = B$

VETA O LIMITE MONOTÓNNEJ FCII.

VETA O SPOJITOM OBRAZE INTERVALU : AK $f: I \to \mathbb{R}$ JE SPOJITÁ NA INTERVALE I $\Rightarrow$ $f(I)$ JE INTERVAL

DARBOUXOVA VETA : f JE SPOJITÁ NA $\langle a, b \rangle$, $f(a) < f(b)$. POTOM $\forall y \in (f(a), f(b))$ $\exists x \in (a, b)$: $f(x) = y$.

VETA: f SPOJITÁ NA $\langle a, b \rangle$ NADOBÚDA MAXIMA A MINIMA ($\Rightarrow$ JE OHRANIČENÁ) NA $\langle a, b \rangle$.

18.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

2.3 EXPONENCIÁLNA FCIA. exp :

(i) $\exp(x+y) = \exp x \cdot \exp y$, (ii) $\exp(x) \geq 1 + x$

$\lim_{x\to 0} \frac{e^x - 1}{x} = 1$

LOGARITMUS $\ln = \exp^{-1}$, $\lim_{x\to 0} \frac{\ln(x+1)}{x} = 1$

OBECNÁ MOCNINA $a^b = \exp(b \cdot \log a)$

GONIOMETRICKÉ FCIE.

(i) $s(x+y) = s(x) \cdot c(y) + c(x) \cdot s(y)$
(ii) $c(x+y) = c(x) \cdot c(y) - s(x) \cdot s(y)$
(iii) s NEPÁRNA, c PÁRNA
(iv) $s > 0$ NA $(0, \pi)$, $s(0) = s(\pi)$

$\sin = s$, $\cos = c$
$tg = \frac{\sin}{\cos}$, $cotg = \frac{\cos}{\sin}$

$\lim_{x\to 0} \frac{\arcsin x}{x} = 1$, $\lim_{x\to 0} \frac{\arccos x}{\sqrt{1-x}} = 1$, $\lim_{x\to 0} \frac{\mathrm{arctg}\, x}{x} = 1$

2.4 DERIVÁCIA $f'(a) = \lim_{h\to 0} \frac{f(a+h) - f(a)}{h}$, $f'_+(a)$, $f'_-(a)$

VETA: AK f MÁ V a VLASTNÚ DERIVÁCIU $\Rightarrow$ f JE SPOJITÁ V a

ARITMETIKA DERIVÁCIÍ

VETA O DERIVÁCII ZLOŽENEJ FUNKCIE: NECH f MÁ DERIVÁCIU V y_0, g MÁ DERIVÁCIU V x_0, g JE SPOJITÁ V x_0 A $g(x_0) = y_0$. POTOM $(f \circ g)'(x_0) = f'(y_0) \cdot g'(x_0) = f'(g(x_0)) \cdot g'(x_0)$.

VETA O DERIVÁCII INVERZNEJ FUNKCIE: NECH f JE SPOJITÁ, RÝDZO MONOTÓNNA NA (a,b) A MÁ V $x_0 \in (a,b)$ VLASTNÚ DERIVÁCIU $f'(x_0)$ RÔZNU OD NULY. POTOM MÁ f^{-1} VLASTNÚ DERIVÁCIU V BODE $y_0 = f(x_0)$, $(f^{-1})'(y_0) = 1 / f'(x_0)$.

NUTNÁ PODMIENKA LOKÁLNEHO EXTRÉMU: f MÁ V a LOKÁLNY EXTRÉM $\Rightarrow$ $f'(a)$ NEEXISTUJE v $f'(a) = 0$.

ROLLEOVA VETA: f SPOJITÁ NA $\langle a,b \rangle$, $f'(x)$ EXISTUJE PRE $\forall x \in (a,b)$, $f(a) = f(b)$ $\Rightarrow \exists \xi \in (a,b) : f'(\xi) = 0$.

LAGRANGEOVA VETA O STREDNEJ HODNOTE:

f SPOJITÁ NA $\langle a,b\rangle$, f' EXISTUJE NA (a,b)
$\Rightarrow \exists \xi \in (a,b): f'(\xi) = (f(b) - f(a))/(b-a)$.

CAUCHYOVA VETA O STREDNEJ HODNOTE:

f, g SPOJITÉ NA $\langle a,b\rangle$, f', g' EX. NA (a,b), $g' \neq 0$ NA (a,b)
$\Rightarrow \exists \xi \in (a,b): (f(b) - f(a))/(g(b) - g(a)) = f'(\xi)/g'(\xi)$.

L'HOSPITALOVO PRAVIDLO: $a \in \mathbb{R}^*$, f, g SÚ DEFINOVANÉ NA NEJAKOM $P(a,\delta)$, f, g MAJÚ VL. DERIVÁCIE NA $P(a,\delta)$, $g' \neq 0$ NA $P(a,\delta)$ A EXISTUJE $\lim\limits_{x\to a} f'(x)/g'(x)$.
AK PLATÍ: (i) $\lim\limits_{x\to a} f(x) = \lim\limits_{x\to a} g(x) = 0$, ALEBO
(ii) $\lim\limits_{x\to a+} |g(x)| = +\infty$
POTOM $\lim\limits_{x\to a} f(x)/g(x) = \lim\limits_{x\to a} f'(x)/g'(x)$.

VETA O LIMITE DERIVÁCIE: f SPOJITÁ SPRAVA V a, EXISTUJE $\lim\limits_{x\to a+} f'(x) = A \in \mathbb{R}^*$. POTOM $f'_+(a) = A$.

VZŤAH DERIVÁCIE A MONOTÓNIE

NUTNÁ PODMIENKA INFLEXIE: $f''(a) \neq 0 \Rightarrow f$ NEMÁ V a INFLEXIU

POSTAČUJÚCA PODMIENKA INFLEXIE: f MÁ SPOJITÚ DERIVÁCIU NA (a,b), $z \in (a,b)$, $\forall x \in (a,z): f''(x) > 0$, $\forall x \in (z,b): f''(x) < 0$ (RESP. NAOPAK)
$\Rightarrow z$ JE BOD INFLEXIE f.

[RÝDZA] KONVEXNOSŤ / KONKÁVNOSŤ (DEFINÍCIA)

AK f JE KONVEXNÁ NA I, a JE VNÚTORNÝ BOD ($a \in \operatorname{Int} I$), POTOM $\exists f'_+(a)$, $\exists f'_-(a)$. (VLASTNÉ)
AK f JE KONVEXNÁ NA $(a,b) \Rightarrow f$ JE SPOJITÁ NA (a,b)
VZŤAH f'' A KONVEXITY / KONKÁVITY
ASYMPTOTA: $\lim\limits_{\substack{x\to+\infty \\ (-\infty)}} [f(x) - (ax+b)] = 0$

$\Leftrightarrow \lim\limits_{\substack{x\to+\infty \\ (-\infty)}} f(x)/x = a$, $\lim\limits_{\substack{x\to+\infty \\ (-\infty)}} f(x) - ax = b$

3/4

18.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

2.5 TALOROV POLYNÓM FUNKCIE f RÁDU n V BODE a

$T_n^{f,a}(x) = f(a) + f'(a)(x-a) + \dots + f^{(n)}(a)/n! \cdot (x-a)^n .$

VETA: NECH EXISTUJE VLASTNÁ $f^{(n)}(a)$, st $P \subseteq n$.
POTOM $\lim_{x \to a} \frac{f(x) - P(x)}{(x-a)^n} = 0 \Leftrightarrow P = T_n^{f,a}$

OBECNÝ TVAR ZVYŠKU: NECH $x > a$,
f MÁ VLASTNÚ $(n+1)$-VÚ DERIVÁCIU NA $\langle a, x \rangle$,
φ JE SPOJITÁ NA $\langle a, x \rangle$, MÁ VLASTNÉ DERIV. NA $(a, x) \neq 0$
POTOM: $\exists \xi \in (a,x) : R_n^{f,a}(x) = f(x) - T_n^{f,a}(x) =$

$$\boxed{\frac{1}{n!} \cdot \frac{\varphi(x) - \varphi(a)}{\varphi'(\xi)} \cdot f^{(n+1)}(\xi) \cdot (x-\xi)^n .}$$

$\varphi(t) = (x-t)^{n+1}$
LAGRANGEOV TVAR: $R_n^{f,a}(x) = \frac{1}{(n+1)!} \cdot f^{(n+1)}(\xi) \cdot (x-a)^{n+1}$

$\varphi(t) = t$
CAUCHYHO TVAR: $R_n^{f,a}(x) = \frac{1}{n!} \cdot f^{(n+1)}(\xi) \cdot (x-\xi)^n \cdot (x-a)$

POZNÁMKY:

- $\lim a_n \cdot b_n = \lim a_n \cdot \lim b_n$

$$\boxed{|A \cdot B - a_n \cdot b_n| = |A \cdot B - A \cdot b_n + A \cdot b_n - a_n \cdot b_n| \leq}$$
$$\leq |A| \cdot \underbrace{|B - b_n|}_{\leq \frac{\varepsilon}{2|A|+1}} + \underbrace{|b_n|}_{\leq K} \cdot \underbrace{|A - a_n|}_{\leq \frac{\varepsilon}{2K}}$$

- $(\forall n)(a_n \leq b_n) \rightarrow A \leq B$. AK $A > B$, $\varepsilon < (B-A)/2$

- $\{a_n\}_{n=1}^{\infty}$ ZHORA OHRANIČENÁ, NEKLESAJÚCA

$\boxed{s = \sup a_n}$. $\forall \varepsilon > 0 \ \exists n_0 : a_{n_0} \geq s - \varepsilon/2 \Rightarrow \forall n \geq n_0 : a_n > s - \varepsilon$

$\Rightarrow \lim_{n \to \infty} a_n = s .$

- KAŽDÁ KONVERGENTNÁ POSTUPNOSŤ JE CAUCHYOVSKÁ:
  $|a_n - a_m| \le |a_n - A| + |A - a_m|$

- KEĎ MÁ CAUCH. POST. KONV. PODPOSTUPNOSŤ, JE KONVERG. 2.
  $|a_n - x| \le |a_n - a_{k_n}| + |a_{k_n} - x|$

  Z OHRANIČ. POST. MOŽNO VYBRAŤ KONVERG. PODPOSTUPNOSŤ 1.
  $\boxed{M := \{x \mid x < a_n \text{ PRE NEKONEČNE VEĽA INDEXOV } n\}}$
  $\boxed{s := \sup M \Rightarrow \forall \varepsilon > 0 : s - \varepsilon < a_n < s + \varepsilon \text{ PRE } \infty \text{ VEĽA } n}$

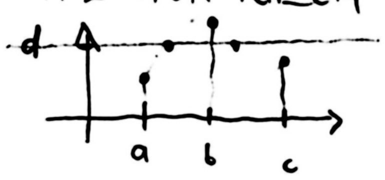
- BOLZANO-CAUCHY: CAUCHYOVSKÁ POST. KONVERGUJE
  $\varepsilon := 1 \Rightarrow \exists n_0 : \forall m, n \ge n_0 \ |a_m - a_n| < 1$, TJ.
  $\forall n \ge n_0 : \boxed{a_{n_0} - 1 < a_n < a_{n_0} + 1} \Rightarrow$ OHRANIČENOSŤ $\Rightarrow$

- $\lim_{x \to a} f(x) = b \Leftrightarrow \forall \varepsilon > 0 \, \exists \delta > 0 \, \forall x \in D \ \boxed{0 < |x - a|} < \delta \Rightarrow |f(x) - b| < \varepsilon$

- NECH f JE SPOJITÁ NA $\langle a, b \rangle$, $f(a) < 0 < f(b)$ $\Rightarrow \exists c \in (a,b) : f(c) = 0$. **DARBOUXOVA VETA**
  $\boxed{M := \{x \mid a \le x \le b, \ f(x) \le 0\}, \ c := \sup M}$ MUSÍ BYŤ $f(c) = 0$

- J JE INTERVAL $\Leftrightarrow \forall a, b \in J \ \ a \le c \le b \Rightarrow c \in J$
- f JE SPOJITÁ NA INTERVALE $J \Rightarrow f[J]$ JE INTERVAL

- SPOJITÁ PROSTÁ FUNKCIA NA INTERVALE JE RÝDZO MONOTÓNNA
  PRE SPOR NECH $a < b < c$, $f(a), f(c) < f(b)$



  NECH $\max\{f(a), f(c)\} < d < f(b)$
  $\Rightarrow$ NA INTERVALOCH $\langle a, b \rangle$, $\langle b, c \rangle$
  f NADOBÚDA HODNOTU d ↯

- RÝDZO MONOTÓNNA f NA INT. J JE SPOJITÁ $\Leftrightarrow f[J]$ JE INTERVAL

18.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

- $f: D \to \mathbb{R}$ JE SPOJITÁ $\Leftrightarrow$ $\forall \{x_n\}_{n=1}^{\infty}$ KONVERG. V D
  $\lim f(x_n) = f(\lim x_n)$
  $\Rightarrow$) ZREJMÉ $\Leftarrow$) AK f NIE JE SPOJITÁ ... ZREJMÉ
- SPOJITÁ f NA KOMPAKTNOM $\langle a,b \rangle$ NADOBÚDA MAXIMA (MINIMA)

  $\boxed{\begin{array}{l} s := \sup \{ f(x) \mid x \in \langle a,b \rangle \}, \\ \text{VOLME } x_n \in \langle a,b \rangle \text{ TAK, ŽE } f(x_n) > s - \frac{1}{n} \quad (\text{RESP. } f(x_n) > n) \end{array}}$ PRE $s = +\infty$

  Z $\{x_n\}_{n=1}^{\infty}$ MÔŽME VYBRAŤ KONVERGENTNÚ $\{x_{k_n}\}_{n=1}^{\infty}$, $y_n := x_{k_n}$ $\boxed{\lim y_n = y_0 \in \langle a,b \rangle}$

  ZREJME $k_n \geq n \Rightarrow f(y_n) > s - \frac{1}{n}$ (RESP. $f(y_n) > n$)

  $y_0 := \lim y_n$, $f(y_0) = \lim f(y_n) \Rightarrow s < \infty$ A ZREJME $\lim f(y_n) = s$.
- SPOJITÝ OBRAZ KOMPAKT. INTERVALU JE KOMPAKTNÝ INTERVAL
- $(f \circ g)'(x_0) = f'(g(x_0)) \cdot g'(x_0)$

$$\boxed{\begin{array}{l} f(g(x_0)+k) - f(g(x_0)) = A \cdot k + k \cdot \mu(k) \\ g(x_0+h) - g(x_0) = B \cdot h + h \cdot \nu(h) \end{array}} \qquad \begin{array}{l} \lim_{k \to 0} \mu(k) = 0 \\ \lim_{h \to 0} \nu(h) = 0 \end{array}$$

$$\boxed{f(g(x_0+h)) - f(g(x_0)) = f(g(x_0) + \underline{g(x_0+h) - g(x_0)}) - f(g(x_0)) =}$$
$$= \underline{f(g(x_0) + \underline{B \cdot h + h \cdot \nu(h)}) - f(g(x_0))} =$$
$$= A \cdot (B \cdot h + h \cdot \nu(h)) + (B \cdot h + h \cdot \nu(h)) \cdot \mu(B \cdot h + h \cdot \nu(h)) =$$
$$= A \cdot B \cdot h + h \cdot \Big[\underbrace{A \cdot \nu(h) + (B + \nu(h)) \cdot \mu(B \cdot h + h \cdot \nu(h))}_{\to 0} \Big]$$

- ROLLEOVA VETA: f SPOJITÁ NA $\langle a,b \rangle$, f' EX. VLASTNÁ NA (a,b), $f(a) = f(b)$, $\Rightarrow \exists c \in (a,b): f'(c) = 0$

  f NA $\langle a,b \rangle$ NADOBÚDA MAXIMA A MINIMA.
  2 PRÍPADY: max = min, max > min

LAGRANGEOVA VETA O STR. H. $f'(c) = (f(b) - f(a)) / (b-a)$
$F(x) = (f(x) - f(a)) \cdot (b-a) - (f(b) - f(a)) \cdot (x-a)$

CAUCHYHO VETA: $g(a) \neq g(b)$, $g' \neq 0$, $f'(c)/g'(c) = (f(b) - f(a)) / (g(b) - g(a))$
$F(x) = (f(x) - f(a)) \cdot (g(b) - g(a)) - (f(b) - f(a)) \cdot (g(x) - g(a))$

- L'HOSPITALOVO PRAVIDLO: NECH f, g MAJÚ DERIVÁCIE NA PRSTENCOVOM OKOLÍ BODU a, $\lim_{x \to a} f(x) = \lim_{x \to a} g(x) = 0$, AK $\lim_{x \to a} \frac{f'(x)}{g'(x)} = L$, POTOM AJ $\lim_{x \to a} f(x)/g(x) = L$.

$$\left| \frac{f(x)}{g(x)} - L \right| = \left| \frac{f(x) - f(a)}{g(x) - g(a)} - L \right| = \left| \frac{f'(\xi)}{g'(\xi)} - L \right|$$ (CAUCHYHO VETA O STR. HODNOTE)

- TAYLOR: NECH f MÁ NA $J = (a - \Delta, a + \Delta)$ DERIVÁCIE AŽ DO RÁDU $(n+1)$, $x \in J$ (BUNO $x > a$), φ JE SPOJITÁ NA $\langle a, b \rangle$, φ MÁ NA (a, b) VLASTNÉ NENULOVÉ DERIVÁCIE

$\Rightarrow \exists \xi$ MEDZI a A x TAKÉ, ŽE

$$R_n^{f,a}(x) = f(x) - T_n^{f,a}(x) = f(x) - \left[f(a) + \frac{f'(a)}{1!}(x-a) + \dots + \frac{f^{(n)}(a)}{n!}(x-a)^n \right] =$$

$$= \boxed{\frac{\varphi(x) - \varphi(a)}{\varphi'(\xi)} \cdot \frac{f^{(n+1)}(\xi)}{n!} (x - \xi)^n}$$

$$\boxed{F(\underline{\underline{t}}) := f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(t)}{k!} (x - \underline{\underline{t}})^k}$$

$$F(x) = 0, \quad F(a) = R_n^{f,a}(x)$$

$$\frac{d}{dt} F(t) = \dots = - \frac{f^{(n+1)}(t)}{n!} (x-t)^n$$

$$\boxed{\frac{F(a)}{g(a) - g(x)} = \frac{F(a) - F(x)}{g(a) - g(x)} = - \frac{f^{(n+1)}(\xi)}{n! \, g'(\xi)} \cdot (x - \xi)^n}$$

PRE LAGRANGEOV TVAR $\boxed{g(t) = (x-t)^{n+1}}$

19.08.2008 Tu
PETER ČERNO

ŠTÁTNICE

3 POSTUPNOSTI A RADY FUNKCIÍ

3.1 SPOJITOSŤ ZA PREDPOKLADU ROVNOMERNEJ KONVERGENCIE

BODOVÁ KONVERGENCIA $f_n \to f$ NA M
$\Leftrightarrow \forall x \in M: \lim_{n\to\infty} f_n(x) = f(x)$

ROVNOMERNÁ KONVERGENCIA $f_n \rightrightarrows f$ NA M
$\Leftrightarrow \forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0\ \forall x \in M\ |f_n(x) - f(x)| < \varepsilon.$

PLATÍ $f_n \rightrightarrows f \Leftrightarrow \forall \varepsilon > 0\ \exists n_0\ \forall n \geq n_0\ \sup_M |f_n - f| < \varepsilon. \Leftrightarrow \lim_{n\to\infty} \sup |f_n - f| = 0$

LOKÁLNE ROVNOMERNÁ KONVERGENCIA $\overset{loc}{\rightrightarrows}$
$\forall x \in M\ \exists \varepsilon > 0\ \ f_n \rightrightarrows$ NA $M \cap (x-\varepsilon, x+\varepsilon)$

BOLZANO - CAUCHY NUTNÁ A POSTAČUJÚCA PODMIENKA ROVNOMERNEJ KONVERGENCIE
$f_n \rightrightarrows \Leftrightarrow \forall \varepsilon > 0\ \exists n_0\ \forall m, n \geq n_0\ \forall x \in M\ |f_n(x) - f_m(x)| < \varepsilon.$

MOORE - OSGOOD: AK $f_n \rightrightarrows f$ NA (a, b) A PRE
$\forall n \in \mathbb{N}\ \exists \lim_{x\to a+} f_n(x) = c_n$, POTOM $\exists \lim_{x\to a+} f(x) = \lim_{n\to\infty} c_n$
INÝ ZÁPIS: $\lim_{x\to a+} \lim_{n\to\infty} f(x) = \lim_{n\to\infty} \lim_{x\to a+} f_n(x)$.

$f_n \overset{loc}{\rightrightarrows} f$, f_n SÚ OHRANIČENÉ $\Rightarrow$ f JE OHRANIČENÁ NA I
$f_n \overset{loc}{\rightrightarrows} f$, f_n SÚ SPOJITÉ $\Rightarrow$ f JE SPOJITÁ NA I

NECH $\{f_n\}_{n=1}^{\infty}$ JE POSTUPNOSŤ FUNKCIÍ, KAŽDÁ MÁ VLASTNÚ DERIVÁCIU f_n' NA (a, b) A
(i) $\exists c \in (a, b)$: POSTUPNOSŤ $f_n(c)$ KONVERGUJE !!
(ii) $f_n' \rightrightarrows f$ NA (a, b)
POTOM $f_n \rightrightarrows F$ NA (a, b) A $F' = f$.

RAD FUNKCIÍ $\sum_{n=1}^{\infty} u_n$ KONVERGUJE NA M BODOVO, ROVNOMERNE, LOKÁLNE ROVNOMERNE $\Leftrightarrow$ NA M KONVERGUJE BODOVO, ROVN., LOK. ROVN. POSTUPNOSŤ ČASTOČNÝCH SÚČTOV

NUTNÁ PODMIENKA ROVNOMERNEJ KONVERGENCIE
$\sum_{n=1}^{\infty} u_n \rightrightarrows \;\Rightarrow\; u_n \rightrightarrows 0$.

BOLZANO-CAUCHY NUTNÁ A POSTAČUJÚCA PODM. ROVN. KONV.
$\sum_{n=1}^{\infty} u_n \rightrightarrows \;\Leftrightarrow\; \forall \varepsilon > 0\ \exists n_0\ \forall n \geq n_0\ \forall k\ \forall x \in M\ \left|\sum_{i=1}^{k} u_{n+i}(x)\right| < \varepsilon$

POROVNÁVACIE KRITÉRIUM: $\forall n\ |u_n| \leq v_n$ A $\sum v_n \rightrightarrows \;\Rightarrow\; \sum u_n \rightrightarrows$

WEIERSTRASSOVO KRITÉRIUM: $\forall n\ |u_n| \leq c_n$ A $\sum c_n$ KONV. $\Rightarrow \sum u_n \rightrightarrows$

$\sum u_n$ KONVERGUJE ABSOLÚTNE ROVN. $\Leftrightarrow \sum |u_n| \rightrightarrows$

LEIBNIZOVO KRITÉRIUM: AK $\forall x \in M\ \forall n\ u_n(x) \geq u_{n+1}(x) \geq 0$
A $u_n \rightrightarrows 0$, POTOM $\sum (-1)^n u_n \rightrightarrows$

DIRICHLETOVO KRITÉRIUM: MAJME $\{u_n\}_{n=1}^{\infty}$, $\{v_n\}_{n=1}^{\infty}$.

(i) $\exists K > 0\ \forall n\ \forall x \in M\ \left|\sum_{i=1}^{n} u_i(x)\right| < K$

(ii) $\forall x \in M$ $\{v_n(x)\}_{n=1}^{\infty}$ MONOTÓNNA, $v_n \rightrightarrows 0$

POTOM $\sum u_n \cdot v_n \rightrightarrows$

ABELOVO KRITÉRIUM: MAJME $\{u_n\}_{n=1}^{\infty}$, $\{v_n\}_{n=1}^{\infty}$

(i) $\exists K > 0\ \forall n\ \forall x \in M\ |v_n(x)| < K$ TJ v_n SÚ ROVNOMERNE OHRANIČ.
A PRE $\forall x \in M$ JE POSTUPNOSŤ $\{v_n(x)\}_{n=1}^{\infty}$ MONOTÓNNA

(ii) $\sum u_n \rightrightarrows$

POTOM $\sum u_n \cdot v_n \rightrightarrows$

19.08.2008 TU
PETER ČERNO

ŠTÁTNICE

3.2 MOCNINNÉ RADY

NECH $z_0 \in \mathbb{C}$, $a_0, a_1, \ldots \in \mathbb{C}$ SÚ KOMPLEXNÉ KOEFICIENTY POTOM RAD $\sum_{n=0}^{\infty} a_n (z-z_0)^n$ NAZÝVAME MOCNINNÝM RADOM SO STREDOM z_0. ĎALEJ PREDPOKLADÁME $z_0 = 0$.

EXISTUJE $R \in \langle 0; +\infty)$ POLOMER KONVERGENCIE, ŽE NA MNOŽINE $B(0,R) = \{z \in \mathbb{C} \mid |z| < R\}$ KRUH KONVERGENCIE KONVERGUJE RAD $\sum_{n=0}^{\infty} a_n z^n$ ABSOLÚTNE LOKÁLNE ROVNOMERNE A PRE $|z| > R$ $\sum a_n z^n$ DIVERGUJE.

Z CAUCHYOVHO KRITÉRIA AK $\exists\, L = \limsup_{n\to\infty} \sqrt[n]{|a_n|} > 0$, POTOM $R = 1/L$

Z D'ALEMBERTOVHO KRITÉRIA AK $\exists\, L = \limsup_{n\to\infty} \frac{|a_{n+1}|}{|a_n|} > 0$, POTOM TAKTIEŽ $R = 1/L$.

V REÁLNOM OBORE NAZÝVAME KRUH KONV. INTERVALOM KONV.

MAJME MOCNINNÝ RAD $\sum_{n=0}^{\infty} a_n x^n$ (v $\mathbb{R}$) S POLOMEROM $R > 0$, KTORÝ KONVERGUJE NA INTERVALE KONV. I LOKÁLNE ROVNOMERNE K f.

POTOM: (i) MOCNINNÝ RAD $\sum_{n=0}^{\infty} (n+1) \cdot a_{n+1} x^n$ MÁ POLOMER R A NA I KONVERGUJE LOK. ROVNOMERNE K f'

(ii) RAD $F(0) + \sum_{n=1}^{\infty} \frac{a_{n-1}}{n} \cdot x^n$ MÁ POLOMER R A NA I KONVERGUJE LOK. ROVNOMERNE K F, KDE $F' = f$ NA I.

(ZREJME f JE SPOJITÁ NA I)

3.3 TAYLOROVE RADY

NECH f MÁ V BODE a DERIVÁCIE VŠETKÝCH RÁDOV. POTOM $\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n$ NAZÝVAME TAYLOROVÝ RAD FUNKCIE f SO STREDOM a.

1. FUNKCIA f JE V BODE x SÚČTOM SVOJHO TAYLOROVHO RADU SO STREDOM a $\Leftrightarrow$ $\lim_{n\to\infty} f(x) - T_n^{f,a}(x) = \lim_{n\to\infty} R_n^{f,a}(x) = 0$.

2. NECH $a < x$, f MÁ NA INTERVALE $\langle a, x \rangle$ DERIVÁCIE VŠETKÝCH RÁDOV.
   AK EXISTUJE $C > 0$ TAKÉ, ŽE PRE $\forall n \in \mathbb{N}$ A $\forall t \in (a, x)$ JE $|f^{(n)}(t)| < C$,
   POTOM f JE V BODE x SÚČTOM SVOJHO TAYLOROVHO RADU SO STREDOM V BODE a.

3. NECH $\sum_{n=0}^{\infty} a_n (x-a)^n$ JE MOCNINNÝ RAD SO STREDOM V BODE a A S POLOMEROM KONVERGENCIE $R > 0$.
   TENTO RAD NA SVOJOM INTERVALE KONVERGENCIE I KONVERGUJE LOKÁLNE ROVNOMERNE K NEJAKEJ FUNKCII f.
   PLATÍ, ŽE $\sum_{n=0}^{\infty} a_n (x-a)^n$ JE TAYLOROVÝM RADOM FUNKCIE f NA I SO STREDOM V BODE a,
   TJ. $a_n = \frac{f^{(n)}(a)}{n!}$ $\forall n \geq 0$.

ŠTÁTNICE

3.4 FOURIEROVE RADY

NECH $f: \mathbb{R} \to \mathbb{R}$ JE $2l$ - PERIODICKÁ, LEBESGUEOVSKY INTEGROVATEĽNÁ NA OHRANIČENÝCH INTERVALOCH

OZNAČME

$$a_n = \frac{1}{l} \int_{-l}^{l} f(x) \cdot \cos\left(n \cdot x \cdot \frac{l}{\pi}\right) \qquad n = 0, 1, 2, \ldots$$

$$b_n = \frac{1}{l} \int_{-l}^{l} f(x) \cdot \sin\left(n \cdot x \cdot \frac{l}{\pi}\right) \qquad n = 1, 2, 3, \ldots$$

POTOM RAD $\frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cdot \cos\left(nx\frac{l}{\pi}\right) + b_n \sin\left(nx\frac{l}{\pi}\right)\right)$

NAZÝVAME TRIGONOMETRICKÝ FOURIEROV RAD PRISLÚCHAJÚCI f A a_n, b_n SÚ FOURIEROVE KOEFICIENTY.

AK f JE PO ČASTIACH HLADKÁ, TJ. $\exists$ KONEČNE VEĽA BODOV $x_1, \ldots, x_k \in \langle -l, l \rangle$, f AJ f' SÚ SPOJITÉ NA INTERVALOCH MEDZI TÝMITO BODMI A V TÝCHTO BODOCH MAJÚ LIMITY ZĽAVA AJ SPRAVA.

POTOM PRÍSL. TRIG. FOURIEROV RAD BODOVO KONVERGUJE NA $\mathbb{R}$ K $(f(x+) + f(x-))/2$

AK JE NAVYŠE f SPOJITÁ NA $\mathbb{R}$, POTOM F.R. KONV. ROVNOM.

PARSEVALOVA ROVNOSŤ: NECH f JE SPOJITÁ (S VÝNIMKOU KON. POČTU BODOV) A $\int_a^{a+2l} f^2(x)\,dx < \infty$ PRE NEJAKÉ $a \in \mathbb{R}$, $l > 0$. POTOM

$$\frac{1}{l} \int_a^{a+2l} f^2(x)\,dx = \frac{a_0^2}{2} + \sum_{n=1}^{\infty} (a_n^2 + b_n^2)$$

KDE a_n, b_n SÚ FOURIEROVÉ KOEFICIENTY $2l$-PERIODICKEJ FUNKCIE $\hat{f}$ ZHODNEJ S f NA $(a, a+2l)$.

4 INTEGRÁL

4.1 PRIMITÍVNA FUNKCIA

FUNKCIU F NAZÝVAME PRIMITÍVNOU FUNKCIOU K FUNKCII f NA INTERVALE (a,b) AK PRE $\forall x \in (a,b)$ EXISTUJE VLASTNÁ $F'(x) = f(x)$.

AK F, G SÚ PRIMITÍVNE FUNKCIE K FUNKCII f NA (a,b), POTOM $F - G = konšt.$ NA (a,b)

FORMÁLNY ZÁPIS : $\int f(x)\,dx = F(x) + C$

PER PARTES : NECH F JE PRIM. FCIA K f NA (a,b) A G JE PRIM. FCIA KU g NA (a,b)

POTOM $\int Fg\,dx = F \cdot G - \int f \cdot G$, KEĎ MÁ PRAVÁ STRANA ZMYSEL

SUBSTITÚCIA : FORMÁLNE IDE VŽDY O ZÁPIS :

$$\boxed{\int f(y)\,dy = \int f(g(x)) \cdot g'(x)\,dx, \qquad y = g(x)}$$

1. VETA O SUBSTITÚCII : NECH F JE PRIMITÍVNA FUNKCIA K FCII. f NA (A,B), g JE SPOJITÁ A MÁ VLASTNÉ DERIVÁCIE NA (a,b), PRIČOM $g[(a,b)] \subseteq (A,B)$, POTOM

$$\int f(g(x))\, g'(x)\,dx = F(g(x)) + C \quad \text{NA } (a,b)$$

2. VETA O SUBSTITÚCII : f JE SPOJITÁ NA (A,B) A g JE BIJEKCIA $(a,b) \to (A,B)$, KTORÁ MÁ V KAŽDOM BODE (a,b) VLASTNÚ DERIVÁCIU.
NECH H JE PRIMITÍVNA FUNKCIA K FUNKCII $f(g(x)) \cdot g'(x)$ NA (a,b). POTOM

$$\int f(y) \cdot dy = H(g^{-1}(y)) + C \quad \text{NA } (A,B)$$

19.08.2008 Tu
PETER ČERNO

ŠTÁTNICE

4.2 URČITÝ RIEMANNOV INTEGRÁL

$D \equiv a = x_0 < x_1 < \dots < x_n = b$ DELENIE INTERVALU $\langle a, b \rangle$
D' JE ZJEMNENIE D AK KAŽDÝ BOD D JE TIEŽ BODOM D'
$\mathcal{D}$ MNOŽINA VŠETKÝCH DELENÍ $\langle a, b \rangle$

NECH f JE OHRANIČENÁ FUNKCIA NA $\langle a, b \rangle$

$s(f, D) = \sum_{i=1}^{n} m_i \cdot (x_i - x_{i-1})$, $S(f, D) = \sum_{i=1}^{n} M_i \cdot (x_i - x_{i-1})$

KDE $m_i = \inf\limits_{\langle x_{i-1}, x_i \rangle} f$, $M_i = \sup\limits_{\langle x_{i-1}, x_i \rangle} f$

AK D' JE ZJEMNENIE D, POTOM
$s(f, D) \leq s(f, D')$, $S(f, D) \geq S(f, D')$

PRE DVE DELENIA D_1, D_2 VŽDY $s(f, D_1) \leq S(f, D_2)$

OZNAČME $\overline{\int_a^b} f(x)\, dx = \inf\limits_{D} S(f, D)$,
$\underline{\int_a^b} f(x)\, dx = \sup\limits_{D} s(f, D)$

AK $\overline{\int_a^b} f(x) dx = \underline{\int_a^b} f(x) dx$, HOVORÍME, ŽE f MÁ NA $\langle a, b \rangle$ RIEMANNOV (URČITÝ INTEGRÁL) $(\mathcal{R}) \int_a^b f(x) dx := \overline{\int_a^b} f(x) dx$.

<u>KRITÉRIUM EXISTENCIE</u> : RIEM. INT. f NA $\langle a, b \rangle$ EXISTUJE
$\Leftrightarrow \forall \varepsilon > 0\ \exists D : |S(f, D) - s(f, D)| < \varepsilon$.

MONOTÓNIA A LINEARITA R.I.

AK JE f OHRANIČENÁ NA $\langle a, b \rangle$ A SPOJITÁ AŽ NA KONEČNE VEĽA BODOV, POTOM JE RIEMANNOVSKY INTEGROVATEĽNÁ

NECH f JE OHRANIČENÁ NA $\langle a,b\rangle$

(i) AK $\exists\ (R)\int_a^b f \Rightarrow \forall \langle c,d\rangle \subseteq \langle a,b\rangle\ \exists\ (R)\int_c^d f$

(ii) $c \in (a,b) \Rightarrow (R)\int_a^b f = (R)\int_a^c f + (R)\int_c^b f \Leftrightarrow$ JE ASPOŇ JEDNA STRANA DEF. (ADITIVITA RIEM. INT.)

RIEMANNOV INTEGRÁL AKO PRIMITÍVNA FUNKCIA

NECH f JE OHRANIČENÁ NA $\langle a,b\rangle$

DEFINUJME NA $\langle a,b\rangle$ $F(x) := \int_a^x f(t)\,dt$

(i) F JE SPOJITÁ NA $\langle a,b\rangle$

(ii) AK PRE $x_0 \in (a,b)$ JE f SPOJITÁ V x_0, POTOM V x_0 EXISTUJE VLASTNÁ $F'(x_0)$ A $F'(x_0) = f(x_0)$.

ZÁKLADNÁ VETA ANALÝZY: NECH f JE SPOJITÁ NA $\langle a,b\rangle$ A F JE PRIMITÍVNA FUNKCIA K f NA (a,b). POTOM $\exists\ F(a+) = \lim_{x\to a+} F(x)$, $F(b-) = \lim_{x\to b-} F(x)$ A PLATÍ $(R)\int_a^b f(x)\,dx = F(b-) - F(a+)$.

NEWTONOV INTEGRÁL

NECH F JE PRIMITÍVNA FCIA. K f NA (a,b)

NEWTONOVÝM INTEGRÁLOM f CEZ (a,b) ROZUMIEME $(N)\int_a^b f(x)\,dx = F(b-) - F(a+)$, KEĎ OBE LIMITY NA PRAVEJ STRANE EXISTUJÚ A SÚ VLASTNÉ.

VZŤAH RIEMANNOVHO A NEWTONOVHO INTEGRÁLU: AK f JE SPOJITÁ NA $\langle a,b\rangle$, POTOM

$$(R)\int_a^b f(x)\,dx = (N)\int_a^b f(x)\,dx.$$

19.08.2008 Tu
PETER ČERNO

ŠTÁTNICE

APLIKÁCIA URČITÉHO INTEGRÁLU

1. DĹŽKA KRIVKY $L(f) = \int_a^b \sqrt{1+(f'(x))^2}\, dx$
2. OBJEM ROTAČNÉHO TELESA, $f > 0$ NA $\langle a, b \rangle$
   $\pi \int_a^b f^2(x)\, dx$
3. INTEGRÁLNE KRITÉRIUM KONVERGENCIE RADU
   $\sum_{n=1}^{\infty} f(n)$ KONVERGUJE $\Leftrightarrow$ $(N)\int_{n_0}^{\infty} f(x)\, dx < \infty$ $\quad n_0 \in \mathbb{N}$

!!! f JE SPOJITÁ, NEZÁPORNÁ, NERASTÚCA NA $\langle n_0 - 1, +\infty)$

4.3 VIACROZMERNÝ RIEMANNOV INTEGRÁL

KOMPAKTNÝ INTERVAL V E_n: $J = \langle a_1, b_1 \rangle \times \dots \times \langle a_n, b_n \rangle$
DELENIE $D = (D_1, \dots, D_n)$ $\quad D_i$ JE DELENIE $\langle a_i, b_i \rangle$
ZJEMNENIE D': $\forall i$ D'_i ZJEMŇUJE D_i
ČLEN ROZDELENIA $K = \langle t_{1,i_1}, t_{1,i_1+1} \rangle \times \dots \times \langle t_{n,i_n}, t_{n,i_n+1} \rangle$
$|D|$ = MNOŽINA VŠETKÝCH ČLENOV
OBJEM $\mathrm{vol}\, J = (b_1 - a_1) \dots (b_n - a_n)$

$s(f, D) = \sum_{K \in |D|} m_K \cdot \mathrm{vol}\, K, \quad S(f, D) = \sum_{K \in |D|} M_K \cdot \mathrm{vol}\, K$

$\overline{\int_J} f = \overline{\int_J} f(\vec{x})\, d\vec{x} = \inf_D S(f, D), \quad \underline{\int_J} f = \sup_D s(f, D)$

(PODOBNE AKO U JEDNOROZM. RIEM INT.)

TAKÉ ISTÉ KRITÉRIUM EXISTENCIE

FUBINIOVA VETA: AK $J = J' \times J''$ JE KOMP. INT. V E_n, POTOM $\int_J f(\vec{x},\vec{y})\, d\vec{x}\, d\vec{y} = \int_{J'} \left(\int_{J''} f(\vec{x},\vec{y})\, d\vec{y} \right) d\vec{x} =$

$= \int_{J''} \left(\int_{J'} f(\vec{x},\vec{y})\, d\vec{x} \right) d\vec{y}$

NECH $U \subseteq \mathbb{R}^n$ JE OTVORENÁ $\vec{f} = (f_1, \dots, f_n)^T : \mathbb{R}^n \to \mathbb{R}^n$,

JAKOBIÁN $\dfrac{D(f_1, \dots, f_n)}{D(x_1, \dots, x_n)} = \dfrac{D(\vec{f})}{D(\vec{x})} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_n}{\partial x_1} & \dots & \frac{\partial f_n}{\partial x_n} \end{pmatrix}$

$\vec{f}$ JE REGULÁRNE AK MÁ SPOJITÉ PARC. DERIVÁCIE NA U A $\forall \vec{x} \in U : \dfrac{D(f_1, \dots, f_n)}{D(x_1, \dots, x_n)}(\vec{x}) \neq 0$.

VETA O SUBSTITÚCII: NECH $U \subseteq \mathbb{R}^n$ JE OTVORENÁ, $\varphi : U \to \mathbb{R}^n$ JE REGULÁRNE ZOBRAZENIE A $A \subseteq U$ JE UZAVRENÁ V $\mathbb{R}^n$.

AK EXISTUJE $\int_{\varphi(A)} f(\vec{x})\, d\vec{x}$, POTOM

$$\int_A f(\varphi(\vec{t})) \cdot \frac{D(\varphi)}{D(\vec{t})}(\vec{t})\, d\vec{t} = \int_{\varphi(A)} f(\vec{x})\, d\vec{x}$$

20.08.2008
PETER ČERNO

ŠTÁTNICE

5 ZÁKLADY TEORIE FUNKCIÍ VIAC PREMENNÝCH

5.1 PARCIÁLNE DERIVÁCIE A TOTÁLNY DIFERENCIÁL

PARCIÁLNA DERIVÁCIA : $f : \mathbb{R}^n \to \mathbb{R}$

$$\frac{\partial f}{\partial x_i}(x) = \lim_{t \to 0} \frac{f(x_1, \dots, x_i + t, \dots, x_n) - f(x_1, \dots, x_n)}{t}$$

GRADIENT $\nabla f(x) = \left(\frac{\partial f}{\partial x_1}(x), \dots, \frac{\partial f}{\partial x_n}(x) \right)$

DERIVÁCIA V SMERE $v \in \mathbb{R}^n \setminus \{0\}$

$$D_v f(x) = \lim_{t \to 0} \left(f(x + t \cdot v) - f(x) \right) / t .$$

ZREJME $\frac{\partial f}{\partial x_i} f(x) = D_{e_i} f(x)$

TOTÁLNY DIFERENCIÁL

f MÁ V BODE a TOTÁLNY DIFERENCIÁL, KEĎ $\exists$ LIN. ZOBRAZENIE $D f(a)(h)$ TAKÉ, ŽE

$$\lim_{\|h\| \to 0} \frac{f(x+h) - f(x) - D f(a)(h)}{\|h\|} = 0$$

AK EXISTUJE, POTOM EXISTUJÚ AJ VŠETKY PARC. DER. V BODE a,

$D_h f(a) = D f(a)(h) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) \cdot h_i$,

f JE V BODE a SPOJITÁ.

ARITMETIKA TOT. DIF. : NECH f, g MAJÚ V a TOT. DIFER.

POTOM $D(f+g)(a) = D f(a) + D g(a)$

$D(\alpha f)(a) = \alpha \cdot D f(a)$

$D(f \cdot g)(a) = f(a) \cdot D g(a) + g(a) \cdot D f(a)$

$D(f/g)(a) = \frac{g(a) \cdot D f(a) - f(a) \cdot D g(a)}{g^2(a)}$ AK $g(a) \neq 0$

DIFERENCIÁL ZLOŽENÉHO ZOBRAZENIA

NECH $f: \mathbb{R}^n \to \mathbb{R}$ MÁ TOTÁLNY DIFERENCIÁL V BODE $a \in \mathbb{R}^n$ A $g_1, \dots, g_n : \mathbb{R}^m \to \mathbb{R}$ MAJÚ TOTÁLNY DIF. V BODE $b \in \mathbb{R}^m$, PRIČOM $a_i = g_i(b)$ $\forall i \in \{1, \dots, n\}$.

POTOM ZLOŽENÁ FUNKCIA $F: \mathbb{R}^m \to \mathbb{R}$

$F(x) = f(g_1(x), \dots, g_n(x))$ MÁ V BODE b TOTÁLNY DIF.

A PLATÍ:

$$DF(b)(h) = \sum_{i=1}^{m} \frac{\partial F}{\partial x_i}(b) \cdot h_i =$$

$$= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \frac{\partial f}{\partial x_j} \underbrace{(g_1(b), \dots, g_n(b))}_{a} \cdot \frac{\partial g_j}{x_i}(b) \right) \cdot h_i$$

POSTAČUJÚCA PODMIENKA EXISTENCIE TOT. DIF.

AK f MÁ V a SPOJITÉ PARC. DERIVÁCIE $\Rightarrow$ MÁ V a TOT. DIFERENCIÁL

NECH f MÁ NA OTVORENEJ $M \subseteq \mathbb{R}^n$ PARC. DERIVÁCIU $\frac{\partial f}{\partial x_i}$

POTOM DEFINUJEME V $a \in M$ $\frac{\partial^2 f(a)}{\partial x_i \partial x_j} = \frac{\partial}{\partial x_j}\left(\frac{\partial}{\partial x_i} f\right)(a)$.

KEĎ MÁ KAŽDÁ PARC. DERIVÁCIA f V BODE a TOT. DIF., POTOM DEFINUJEME TOT. DIF. 2. RÁDU AKO BILIN. FORMU

$$D^2 f(a) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R},$$

$$D^2 f(a)(h, k) = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\partial^2 f(a)}{\partial x_i \partial x_j} h_i \cdot k_j$$

KEĎ f MÁ SPOJITÚ PARC. DERIVÁCIU $\frac{\partial^2 f(a)}{\partial x_r \partial x_j}$, POTOM MÁ AJ $\frac{\partial^2 f(a)}{\partial x_j \partial x_r}$ A OBE SA ROVNAJÚ.

20.08.2008
PETER ČERNO

ŠTÁTNICE

5.2 VETA O STREDNEJ HODNOTE

$f : \mathbb{R}^n \to \mathbb{R}$, $a, b \in \mathbb{R}^n$, f MÁ SPOJITÉ PARCIÁLNE DERIVÁCIE NA ÚSEČKE MEDZI BODMI a A b.
POTOM $\exists \xi \in (0,1)$ TAKÉ, ŽE

$$f(b) - f(a) = \nabla f(a + \xi(b-a)) \cdot (b-a) =$$
$$= \sum_{i=1}^n \frac{\partial f}{\partial x_i}(a + \xi(b-a)) \cdot (b_i - a_i)$$

5.3 VETA O IMPLICITNÝCH FUNKCIÁCH

NECH $F : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ MÁ SPOJITÉ PARCIÁLNE DERIVÁCIE
$x_0, y_0 \in \mathbb{R}$, $F(x_0, y_0) = 0$, $\frac{\partial F}{\partial y}(x_0, y_0) \neq 0$.
POTOM EXISTUJE U OKOLIE x_0 A V OKOLIE y_0 TAKÉ, ŽE
$\forall x \in U \ \exists! y \in V : F(x, y) = 0$, OZNAČME TAKÉ $y = \varphi(x)$.
POTOM φ JE DIFERENCOVATEĽNÁ NA OKOLÍ U A PLATÍ

$$\frac{\partial \varphi}{\partial x}(x) = - \frac{\frac{\partial F}{\partial x}(x, \varphi(x))}{\frac{\partial F}{\partial y}(x, \varphi(x))}$$

NECH $F : G \to \mathbb{R}$, $G \subseteq \mathbb{R}^{n+1}$ OTVORENÁ MÁ SPOJ. PARC. DER.,
$x_0 \in \mathbb{R}^n$, $y_0 \in \mathbb{R}$, $F(x_0, y_0) = 0$, $\frac{\partial F}{\partial y}(x_0, y_0) \neq 0$,
POTOM ...

$$\frac{\partial \varphi}{\partial x_i}(x) = - \frac{\frac{\partial F}{\partial x_i}(x, \varphi(x))}{\frac{\partial F}{\partial y}(x, \varphi(x))}$$

VETA O INVERZNEJ FUNKCII:

NECH $F=(f_1,\dots,f_n)^T : G\to\mathbb{R}^n$, $G\subseteq\mathbb{R}^n$ OTVORENÁ

f_i MAJÚ SPOJITÉ PARCIÁLNE DERIVÁCIE

$x_0\in G : |JF(x_0)| = \det\begin{pmatrix} \partial f_1/\partial x_1 & \cdots & \partial f_1/\partial x_n \\ \cdots & & \cdots \\ \partial f_n/\partial x_1 & \cdots & \partial f_n/\partial x_n \end{pmatrix}(x_0) \neq 0$, $y_0=F(x_0)$

$\Rightarrow$ EXISTUJÚ OKOLIA U BODU x_0 A V BODU y_0 TAKÉ, ŽE $F: U\to V$ JE BIJEKCIA A PLATÍ

$$J F^{-1}(y_0) = (JF(x_0))^{-1}$$

5.4 EXTRÉMY FUNKCIÍ VIAC PREMENNÝCH

LAGRANGEOVE MULTIPLIKÁTORY

$G\subseteq\mathbb{R}^n$ OTVORENÁ $F, g_1,\dots,g_m : G\to\mathbb{R}$ $m<n$

MAJÚ SPOJITÉ PARC. DERIVÁCIE.

NECH $M=\{x\in G \mid g_1(x)=\dots=g_m(x)=0\}$

F MÁ NA M V BODE $a\in M$ LOK. EXTRÉM

A $\nabla g_1(a),\dots,\nabla g_m(a)$ SÚ LIN. NEZÁVISLÉ

$\Rightarrow \exists \lambda_1,\dots,\lambda_m\in\mathbb{R}$:

$$DF(a)+\lambda_1 Dg_1(a)+\dots+\lambda_m Dg_m(a)=0$$

TJ. $\frac{\partial F}{\partial x_i}(a)+\lambda_1\frac{\partial g_1}{\partial x_i}(a)+\dots+\lambda_m\frac{\partial g_m}{\partial x_i}(a)=0 \quad \forall i$

20.08.2008 We
PETER ČERNO

ŠTÁTNICE

6 METRICKÉ PRIESTORY

6.1 DEFINÍCIA A PRÍKLADY

METRICKÝ PRIESTOR (M, d) $d: M \times M \to \mathbb{R}$ ...

EKVIVALENTNÁ DEF. UZAVRENEJ MNOŽINY

$A \subseteq (M, d)$ JE UZAVRENÁ $\Leftrightarrow$ $\forall \{x_n\}_{n=1}^{\infty} \subseteq A$

AK x_n KONVERGUJE $\Rightarrow$ LIMITA $\lim_{n\to\infty} x_n \in A$.

6.2 SPOJITOSŤ A ROVNOMERNÁ SPOJITOSŤ

$f: (X, \rho) \to (Y, \sigma)$ JE SPOJITÉ V BODE $x \in X$

$\Leftrightarrow$ $\forall \varepsilon > 0 \ \exists \delta > 0 \ \forall y \in X \ \rho(x, y) < \delta \Rightarrow \sigma(f(x), f(y)) < \varepsilon$

EKVIVALENTNÉ TVRDENIA:

1. f JE SPOJITÉ
2. $\forall V \subseteq Y$ OKOLIE $f(x) \in Y$ $\exists U \subseteq X$ OKOLIE x: $f[U] \subseteq V$
3. $\forall V \subseteq Y$ OTVORENÚ JE $f^{-1}[V]$ OTVORENÁ
4. $\forall A \subseteq Y$ UZAVRENÚ JE $f^{-1}[A]$ UZAVRENÁ
5. $\forall M \subseteq X$ $f[\bar{M}] \subseteq \overline{f[M]}$
6. $\forall M \subseteq Y$ $\overline{f^{-1}[M]} \subseteq f^{-1}[\bar{M}]$
7. $\forall \{x_n\}_{n=1}^{\infty} \subseteq X$ x_n KONVERGUJE $\Rightarrow$ $f(\lim x_n) = \lim f(x_n)$.

$f: (X, \rho) \to (Y, \sigma)$ JE ROVNOMERNE SPOJITÉ

$\Leftrightarrow$ $\forall \varepsilon > 0 \ \exists \delta > 0 \ \forall x, y \in X \ \rho(x, y) < \delta \Rightarrow \sigma(x, y) < \varepsilon$.

HOMEOMORFIZMUS

PODPRIESTORY METR. PRIESTORU

ZACHOVÁVAJÚ (ROVNOMERNÚ) SPOJITOSŤ

6.3 KOMPAKTNÉ A ÚPLNÉ PRIESTORY

PRIESTOR (X, ρ) JE $\boxed{\text{KOMPAKTNÝ}} \Leftrightarrow$
Z KAŽDEJ POSTUPNOSTI MOŽNO VYBRAŤ KONVERGENTNÚ PODPOSTUPNOSŤ.

KAŽDÝ KONEČNÝ PRIESTOR JE KOMPAKTNÝ
KAŽDÝ $\langle a, b \rangle \subseteq \mathbb{R}$ JE KOMPAKTNÝ

KAŽDÝ KOMPAKTNÝ PODPRIESTOR METR. PRIESTORU JE UZAVRETÝ
KEĎ JE (X, ρ) KOMPAKTNÝ, POTOM KAŽDÝ UZAVRETÝ PODPRIESTOR JE TAKTIEŽ KOMPAKTNÝ

NECH (X, ρ) JE KOMPAKTNÝ, $f: (X, \rho) \to (Y, \sigma)$ SPOJITÉ. POTOM
(i) f JE ROVNOMERNE SPOJITÉ
(ii) $f[X]$ JE KOMPAKTNÝ PODPRIESTOR PR. Y
(iii) f JE PROSTÉ $\Rightarrow$ f JE HOMEOMORFIZMUS (ROVNOMERNÝ)

PRIESTOR (X, ρ) JE OHRANIČENÝ $\Leftrightarrow \exists K > 0$
$\forall x, y \in X: \rho(x, y) < K$.

PODPRIESTOR EUKLIDOVSKÉHO PRIESTORU JE KOMPAKTNÝ $\Leftrightarrow$ JE OHRANIČENÝ A UZAVRETÝ

KAŽDÝ KOMPAKTNÝ $I \subseteq \mathbb{R}$ NADOBÚDA MINIMA A MAXIMA

DÔSLEDOK : (X, ρ) JE KOMPAKTNÝ, $f: (X, \rho) \to \mathbb{R}$ SPOJITÁ, POTOM f NADOBÚDA NA X SVOJHO MINIMA AJ MAXIMA

20.08.2008 We
PETER ČERNO

STÁTNICE

NECH (X, ρ) JE METRICKÝ PRIESTOR. POSTUPNOSŤ $\{x_n\}_{n=1}^{\infty}$ SA NAZÝVA $\boxed{\text{CAUCHYOVSKÁ}}$ $\Leftrightarrow$
$\forall \varepsilon > 0 \ \exists n_0 \ \forall m, n \geq n_0 : \rho(x_m, x_n) < \varepsilon$.

KAŽDÁ KONVERGENTNÁ POSTUPNOSŤ JE CAUCHYOVSKÁ
AK MÁ CAUCHYOVSKÁ POSTUPNOSŤ $\{x_n\}_{n=1}^{\infty}$ KONVERGENTNÚ PODPOSTUPNOSŤ, POTOM x_n KONVERGUJE

METRICKÝ PRIESTOR (X, ρ) NAZÝVAME $\boxed{\text{ÚPLNÝ}}$.
$\Leftrightarrow$ KAŽDÁ CAUCHYOVSKÁ POSTUPNOSŤ JE KONVERGENTNÁ

! KAŽDÝ KOMPAKTNÝ PRIESTOR JE ÚPLNÝ
PODPRIESTOR Y ÚPLNÉHO PRIESTORU X JE KOMPAKTNÝ $\Leftrightarrow$?
Y JE UZAVRETÝ A OHRANIČENÝ V X

! PODPRIESTOR Y ÚPLNÉHO PRIESTORU X JE ÚPLNÝ $\Leftrightarrow$ Y JE UZAVRETÝ V X.

ROVNOMERNÝ HOMEOMORFIZMUS ZACHOVÁVA ÚPLNOSŤ

VETA O PEVNOM BODE

$f : (X, \rho) \to (Y, \sigma)$ JE KONTRAHUJÚCE
$\Leftrightarrow \exists q \in (0,1) : \forall x, y \in X : \sigma(f(x), f(y)) \leq q \cdot \rho(x, y)$

$\boxed{\text{PICKARDOVA - BANACHOVA VETA}}$:

KAŽDÉ KONTRAHUJÚCE ZOBRAZENIE $f : (X, \rho) \to (X, \rho)$ MÁ PRÁVE JEDEN PEVNÝ BOD A KAŽDÁ POSTUPNOSŤ ITERÁCIÍ TOHTO ZOBRAZENIA KONVERGUJE K TOMUTO BODU.

21. 08. 2008 1h
PETER ČERNO

ŠTÁTNICE

7 DIFERENCIÁLNE ROVNICE

ROVNICE, V KTORÝCH AKO NEZNÁMA VYSTUPUJE FUNKCIA

OBYČAJNÉ DIF. ROVNICE: NEZNÁMA Y JE FUNKCIA 1 PREMENNEJ, VYSTUPUJÚ DERIVÁCIE IBA PODĽA TEJTO PREM.

PARCIÁLNE DIF. ROVNICE: Y FUNKCIA VIACERÝCH PREM., VYSTUPUJÚ PARCIÁLNE DERIVÁCIE

OBYČAJNÉ DIF. ROVNICE 1. RÁDU

(1) $y' = f(x, y)$, KDE $f: \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$,

NEZNÁMA $y: \mathbb{R} \to \mathbb{R}^n$.

RIEŠENÍM ROZUMIEME (y, I), KDE I JE INTERVAL NA KTOROM PLATÍ (1)

OBYČAJNÉ DIF. ROVNICE n-TÉHO RÁDU

(2) $F(x, y, y', y'', \ldots, y^{(n)}) = 0$,

KDE $F: \mathbb{R}^{n+2} \to \mathbb{R}$, NEZNÁMA $y: \mathbb{R} \to \mathbb{R}$

(UŽ NEUVAŽUJEME VEKT. FCIE)

OPÄŤ RIEŠENÍM ROZUMIEME DVOJICU (y, I) ...

ŠPECIÁLNE TYPY:

1. ROVNICA SO <u>SEPAROVANÝMI PREMENNÝMI</u>

$$y' \cdot h(y) = g(x)$$

2. <u>LINEÁRNE</u> DIF. ROVNICE <u>1. RÁDU</u>

$$y' + p(x) \cdot y = q(x)$$

3. LINEÁRNE DIF. ROVNICE (n-TÉHO RÁDU)

$y^{(n)} + a_{n-1}(x)\, y^{(n-1)} + \dots + a_0(x)\, y = f(x)$

V PRÍPADE $f=0$ HOVORÍME O HOMOGÉNNEJ ROVNICI

SPECIÁLNY PRÍPAD: KONŠTANTNÉ KOEFICIENTY

JE MOŽNO NÁJSŤ FUNDAMENTÁLNY SYSTÉM S VYUŽITÍM CHARAKTERISTICKÉHO POLYNÓMU

$\lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0$

POKIAĽ JE PRAVÁ STRANA LIN. ROVNICE S KONŠT. KOEF. V ŠPECIÁLNOM TVARE (KVAZIPOLYNÓM), POTOM EXISTUJE ANALYTICKÉ VYJADRENIE AJ PRE 1 RIEŠENIE TAKEJTO NEHOMOGÉNNEJ DIF. ROVNICE

4. SÚSTAVA LIN. DIF. ROVNÍC 1. RÁDU S KONŠT. KOEF.

$y' = A \cdot y + f \quad , \quad A \in \mathbb{R}^{n\times n} \,, \quad f: \mathbb{R} \to \mathbb{R}^n$

NEZNÁMA $y: \mathbb{R} \to \mathbb{R}^n$

V PRÍPADE $f=0$ HOVORÍME O HOMOGÉNNEJ SÚSTAVE

ŠPECIÁLNE POJMY:

EXAKTNÉ ROVNICE

INTEGRAČNÝ FAKTOR

VARIÁCIA KONŠTÁNT

21.08.2008Th
PETER ČERNO

ŠTÁTNICE

(1.) ROVNICA SO SEP. PREMENNÝMI

$$y' \cdot h(y) = g(x)$$

NECH g, h SÚ DEFINOVANÉ A SPOJITÉ NA INT. I, J

NECH G, H SÚ PRÍSLUŠNÉ PRIMITÍVNE FCIE NA INT. I, J

POTOM RIEŠENIA y S HODNOTAMI V INTERVALE J SÚ PRÁVE R. SPĹŇAJÚCE $H(y(x)) = G(x) + c$, KDE $c \in \mathbb{R}$

(2.) LIN. DIF. ROVNICE 1. RÁDU

$$y' + p(x) \cdot y = q(x)$$

NECH P JE PRIMITÍVNA FUNKCIA K p.

VYNÁSOBENÍM ROVNICE INTEGRAČNÝM FAKTOROM $e^{P(x)}$

DOSTÁVAME $\left(y \cdot e^{P(x)}\right)' = q(x) \cdot e^{P(x)}$

EXAKTNÉ ROVNICE

$y' f(x,y) + g(x,y) = 0$ MOŽNO PREPÍSAŤ NA

$$\frac{\partial}{\partial x} F(x, y(x)) = 0$$

$$\Leftrightarrow \frac{\partial f}{\partial x} = \frac{\partial g}{\partial y}$$

PREDPOKLADÁME, ŽE f, g MAJÚ SPOJITÉ PARC. DERIVÁCIE

(3.) LIN. DIF. ROVNICE

NECH $a_0(x), \ldots, a_{n-1}(x), f(x)$ SÚ SPOJITÉ NA (α, β).
PRE FCIU y, KTORÁ MÁ SPOJITÚ n-TÚ DERIVÁCIU POLOŽME
$L(y) = y^{(n)} + a_{n-1}(x)\, y^{(n-1)} + \ldots + a_0(x) \cdot y$.

(i) MNOŽINA VŠETKÝCH MAX. RIEŠENÍ $L(y) = 0$ TVORÍ VEKTOROVÝ PRIESTOR DIMENZIE n

(ii) KEĎ JE y_0 JEDNO RIEŠENIE $L(y) = f$, POTOM VŠETKY RIEŠENIA MAJÚ TVAR $y_0 + y_h$, KDE $L(y_h) = 0$.

METÓDA VARIÁCIE KONŠTÁNT

MAJME $y' + a_0(x) \cdot y = f(x)$

NECH y_h JE RIEŠENIE HOM. DIF. ROVNICE

PARTIKULÁRNE RIEŠENIE NEHOM. DIF. ROVNICE HĽADAJME V TVARE $\underline{y_0(x) = k(x) \cdot y_h(x)}$.

HĽADANIE FUNDAMENTÁLNEHO SYSTÉMU PRE LIN. DIF. ROVNICE n-TÉHO RÁDU S KONŠTANTNÝMI KOEF.

(*) $y^{(n)} + a_{n-1} y^{(n-1)} + \dots + a_0 y = 0$

$a_0, \dots, a_{n-1} \in \mathbb{R}$.

CHARAKTERISTICKÝ POLYNÓM $\chi(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0$.

(i) AK JE $\lambda \in \mathbb{R}$ KOREŇ NÁSOBNOSTI p, POTOM $e^{\lambda x}, \; x e^{\lambda x}, \dots, x^{p-1} e^{\lambda x}$ SÚ RIEŠENIA (*)

(ii) AK JE $\alpha \pm i\beta \in \mathbb{C} \setminus \mathbb{R}$ KOREŇ NÁSOBNOSTI p, POTOM

$e^{\alpha x}\cos \beta x, \quad x e^{\alpha x} \cos \beta x, \quad \dots, \quad x^{p-1} e^{\alpha x} \cos \beta x,$

$e^{\alpha x}\sin \beta x, \quad x e^{\alpha x} \sin \beta x, \quad \dots, \quad x^{p-1} e^{\alpha x} \sin \beta x$

SÚ RIEŠENIA (*)

VŠETKY TIETO RIEŠENIA TVORIA FUNDAMENTÁLNY SYSTÉM.

ŠPECIÁLNA PRAVÁ STRANA (KVAZIPOLYNÓM):

$$f(x) = e^{\alpha x}\left(P_1(x) \cos \beta x + P_2(x) \sin \beta x\right)$$

21.08.2008 Th
PETER ČERNO

ŠTÁTNICE

(4.) SÚSTAVA LIN. DIF. ROVNÍC 1. RÁDU (S KONŠT. KOEF.)

(*) $y' = A(x) \cdot y + b(x)$ $\quad A \in \mathbb{R} \to \mathbb{R}^{n \times n}, \; b : \mathbb{R} \to \mathbb{R}^n$

NEZNÁMA $y : \mathbb{R} \to \mathbb{R}^n$ $\quad y = (y_1, \ldots, y_n)^T$

PREDPOKLADÁME, ŽE a_{ij}, b_i SÚ SPOJITÉ.

OPÄŤ MNOŽINA $\forall$ RIEŠENÍ HOMOG. SÚSTAVY TVORÍ VEKTOROVÝ PRIESTOR DIMENZIE n.

WRONSKIÁN

MAJME $f_1, \ldots, f_n : I \to \mathbb{R}^n$

$$W(x) = W_{f_1, \ldots, f_n}(x) := \det \left(f_1(x), \ldots, f_n(x) \right)$$

AK SÚ $f_1, \ldots, f_n$ RIEŠENÍM $y' = A \cdot y$ $\quad A \in \mathbb{R}^{n \times n}$

POTOM PLATÍ:

$f_1, \ldots, f_n$ SÚ LIN. ZÁVISLÉ $\iff W(x) = 0 \;\; \forall x \in I$

$W(x) = 0 \;\; \forall x \in I \iff \exists x_0 \in I : W(x_0) = 0$

8 ALGEBRA

POZRI SYLABUS J. ŽEMLIČKY

LINEÁRNA ALGEBRA A LIN. PROG.

VIĎ J. MATOUŠEK: LIN. PROGR. A LIN. ALG.
PRO INFORMATIKY

KOMBINATORIKA A TEÓRIA GRAFOV

VIĎ J. MATOUŠEK, J. NEŠETŘIL:
KAPITOLY Z DISKRÉTNÍ MATEMATIKY
T. VALLA, J. MATOUŠEK:
KOMBINATORIKA A GRAFY I

25.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

1 LOGIKA

VÝROKOVÁ LOGIKA

PRVOTNÉ FORMULE, JAZYK L_P, VÝROKOVÁ FORMULA

(1.) SÉMANTIKA VÝR. LOGIKY : PRAVD. OHODN., SPLNITEĽNOSŤ, TAUT., $\models$

VETA O KOMPAKTNOSTI : T JE SPLNITEĽNÁ $\Leftrightarrow$ $\forall$ KONEČNÁ $T_0 \subseteq T$: T_0 JE SPLNITEĽNÁ

DÔSLEDOK : $T \models A \Leftrightarrow \exists$ KONEČNÁ $T_0 \subseteq T$: $T_0 \models A$

(2.) FORMÁLNY SYSTÉM VÝR. LOGIKY

AXIÓMY (SCHÉMY) :
- A1 $A \to (B \to A)$
- A2 $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- A3 $(\neg B \to \neg A) \to (A \to B)$

ODV. PRAVIDLO : MODUS PONENS (MP), $A, A \to B \ / \ B$

DÔKAZ, DOKÁZATEĽNÁ FORMULA, DÔKAZ Z PREDPOKLADOV, $\vdash$

METAVETA O DEDUKCII : $T \vdash A \to B \Leftrightarrow T, A \vdash B$

ZÁKL. VETY :
- v1: $A \to A$
- v2: $\neg A \to (A \to B)$
- v3: $\neg\neg A \to A$
- v4: $A \to \neg\neg A$
- v5: $(A \to B) \to (\neg B \to \neg A)$
- v6: $A \to (\neg B \to \neg(A \to B))$
- v7: $(\neg A \to A) \to A$

LEMMA O NEUT. FORMULI : $T, A \vdash B, \ T, \neg A \vdash B \ \Rightarrow \ T \vdash B$

NECH v JE OHODN. PRVOTNÝCH FORMULÍ

DEFINUJME $A^v := \begin{cases} A \Leftrightarrow \bar{v}(A) = 1 \\ \neg A \Leftrightarrow \bar{v}(A) = 0 \end{cases}$

NECH A OBSAHUJE PRVOTNÉ FORMULE $p_1, \dots, p_n$.

POTOM : $p_1^v, \dots, p_n^v \vdash A^v$

$\Rightarrow$ VETA O ÚPLNOSTI : $\vdash A \Leftrightarrow \models A$ ($\Rightarrow$ JE V. O KOREKTNOSTI)

SPORNÁ / BEZSPORNÁ MNOŽINA FORMULÍ

MNOŽINA FORMULÍ T JE BEZSPORNÁ $\Leftrightarrow$ JE SPLNITEĽNÁ

(VYPLÝVA Z VETY O ÚPLNOSTI A KOMPAKTNOSTI)

DÔSLEDOK: SILNÁ VETA O ÚPLNOSTI: $T \vdash A \Leftrightarrow T \models A$.

VETA O EKVIVALENCII: NECH FORMULA A' VZNIKNE Z FORMULE A NAHRADENÍM NIEKTORÝCH VÝSKYTOV PODFORMULÍ $A_1, \dots, A_n$ FORMULAMI $A_1', \dots, A_n'$. KEĎ JE $\vdash A_1 \Leftrightarrow A_1', \dots, \vdash A_n \Leftrightarrow A_n'$, POTOM $\vdash A \Leftrightarrow A'$

VETA O DÔKAZE ROZBOROM PRÍPADOV:

$T, A \vee B \vdash C \Leftrightarrow T, A \vdash C \wedge T, B \vdash C$.

25.08.2008 Po
PETER ČERNO

ŠTÁTNICE

PREDIKÁTOVÁ LOGIKA

JAZYK, TERM, [ATOMICKÁ] FORMULA,
VOĽNÝ / VIAZANÝ VÝSKYT, OTV. / UZAV. FORMULA

1. SÉMANTIKA PREDIKÁTOVEJ LOGIKY

RELAČNÁ ŠTRUKTÚRA $\mathcal{M}$ (REALIZÁCIA JAZYKA L)
UNIVERZUM M, REALIZÁCIE FUNKCIÍ, RELÁCIÍ

OHODNOTENIE PREMENNÝCH e

TARSKÉHO DEFINÍCIA PRAVDY $\mathcal{M} \models A[e]$

A JE SPLNENÁ V $\mathcal{M} \Leftrightarrow \forall e : \mathcal{M} \models A[e]$

UZAVRETÁ A JE SPLNENÁ V $\mathcal{M} \Leftrightarrow \exists e : \mathcal{M} \models A[e]$

SUBSTITÚCIA TERMOV ZA PREMENNÉ
$t_{x_1,\dots,x_n}[t_1,\dots,t_n]$

$A_x[t]$ VZNIKNE Z A NAHRADENÍM KAŽDÉHO VOĽNÉHO VÝSKYTU x TERMOM t.
PODOBNE $A_{x_1,\dots,x_n}[t_1,\dots,t_n]$

TERM t JE SUBSTITUOVATEĽNÝ ZA x DO FLE. $A \Leftrightarrow$
PRE KAŽDÚ PREMENNÚ y TERMU t
NEEXISTUJE PODFORMULA $(\forall y) B$ ALEBO $(\exists y) B$,
V KTOREJ BY BOL VOĽNÝ VÝSKYT x

LEMMA: KEĎ $\mathcal{M}$ JE REALIZÁCIA L, A JE FORMULA, $t, t_1, \dots, t_n$ SÚ TERMY, e OHODNOTENIE T., Ž. $t_i[e] = m_i$ $\forall i = 1, \dots, n$, POTOM

(i) $t_{x_1, \dots, x_n}[t_1, \dots, t_n][e] = t[e(x_1/m_1, \dots, x_n/m_n)]$

(ii) $\mathcal{M} \models A_{x_1, \dots, x_n}[t_1, \dots, t_n][e] \Leftrightarrow \mathcal{M} \models A[e(x_1/m_1, \dots, x_n/m_n)]$

OZNAČME P MNOŽINU VŠETKÝCH ATOMICKÝCH FORMULÍ JAZYKA L A VŠETKÝCH FORMULÍ $(\forall x)B$, $(\exists x)B$, KDE x JE PREM. A B JE FORMULA. POTOM PLATÍ:

KEĎ A JE TAUTOLÓGIA VÝR. LOGIKY NAD P, POTOM A JE VETOU PREDIKÁTOVEJ LOGIKY

2. FORMÁLNY SYSTÉM PREDIKÁTOVEJ LOGIKY 1. RÁDU BEZ ROVNOSTI

AXIÓMY : A1, A2, A3

AXIÓM ŠPECIFIKÁCIE : A FORMULA, x PREMENNÁ, t TERM SUBSTITUOVATEĽNÝ ZA x DO A, POTOM:
$(\forall x)A \to A_x[t]$

SCHÉMA PRESKOKU: A, B FORMULE, PREMENNÁ x NEMÁ VOĽNÝ VÝSKYT V A, POTOM
$(\forall x)(A \to B) \to (A \to (\forall x)B)$

ODVODZOVACIE PRAVIDLÁ:

MODUS PONENS : $A, A \to B \;/\; B$

PRAVIDLO GENERALIZÁCIE : $A \;/\; (\forall x)A$

25.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

PRAVIDLO ZAVEDENIA $\forall$: x NEMÁ VOĽNÝ VÝSKYT V A

$A \to B$ / $A \to (\forall x) B$

PRAVIDLO ZAVEDENIA $\exists$: x NEMÁ VOĽNÝ VÝSKYT V B

$A \to B$ / $(\exists x) A \to B$

VETA O INŠTANCIÁCH : A' JE INŠTANCIA A

A / A'

VETA O UZÁVERE : A' JE UZÁVER A

$\vdash A \Leftrightarrow \vdash A'$

VETA O DISTRIBÚCII KVANTIFIKÁTOROV :

$A \to B$ / $(\forall x) A \to (\forall x) B$, $(\exists x) A \to (\exists x) B$

FORMULA A' JE <u>VARIANTOU</u> FORMULE A $\Leftrightarrow$ A' VZNIKNE Z A NAHRADENÍM PODFORMULÍ TVARU $(\square x) B$ FORMULAMI $(\square y) B_x[y]$, KDE y NIE JE VOĽNÁ V B, $\square \in \{\forall, \exists\}$.

VETA O VARIANTÁCH : A' JE VARIANTA A

$\vdash A \Leftrightarrow A'$

VETA O DEDUKCII : T MNOŽINA FORMULÍ, A UZAVRETÁ FORMULA, B FORMULA

$T \vdash A \to B \Leftrightarrow T, A \vdash B$

VETA O KONŠTANTÁCH: NECH T JE MNOŽINA FORMULÍ JAZYKA L, A JE FORMULA JAZYKA L, L' VZNIKNE Z L PRIDANÍM NOVÝCH SYMBOLOV $c_1, \dots, c_n$ PRE KONŠTANTY
POTOM: $T \vdash A \iff T \vdash A_{x_1, \dots, x_n}[c_1, \dots, c_n]$

(UŽITOČNÁ, AK CHCEME DOKÁZAŤ $\vdash A \to B$, KDE A MÁ VOĽNÉ PREMENNÉ)

VETA O REDUKCII:
$T \vdash A \iff \exists B_1, \dots, B_n$ UZÁVERY NEJAKÝCH FORMULÍ Z T : $\vdash B_1 \to (B_2 \to \dots (B_n \to A) \dots)$

VETA: A' UZÁVER A. POTOM
$T \vdash A \iff T, \neg A'$ JE SPORNÁ

A JE V PRENEXNOM TVARE $\iff$
$A = (\square_1 x_1) \dots (\square_n x_n) B$
$\square_i \in \{\forall, \exists\}$, x_i SÚ RÔZNE PREMENNÉ, B OTVORENÉ JADRO

VETA: KU KAŽDEJ A $\exists A'$ V PREN. TVARE: $\vdash A \leftrightarrow A'$.

PRENEXNÉ OPERÁCIE:

a) PODFORMULU B NAHRAĎ VARIANTOU B'
b) $\neg (\square x) B$ NAHRAĎ $(\bar{\square} x) \neg B$
c) $B \to (\square x) C$, x NEMÁ VOĽNÝ VÝS. V B, NAHRAĎ $(\square x)(B \to C)$
d) $(\square x) B \to C$, x —II— V C, NAHRAĎ $(\bar{\square} x)(B \to C)$
e) $(\square x) B \wedge C$, x —II— V C, NAHRAĎ $(\square x)(B \wedge C)$

4/5

25.08.2008 Mo.
PETER ČERNO

STÁTNICE

3. FORMÁLNY SYSTÉM PREDIKÁTOVEJ LOGIKY 1. RÁDU S ROVNOSŤOU

NAVIAC AXIÓMY:

R1 AK x JE PREMENNÁ, POTOM $x = x$

R2 AK $x_1, \dots, x_n, y_1, \dots, y_n$ SÚ PREM., f n-ÁRN. F. SYMBOL, POTOM $(x_1 = y_1 \to \dots (x_n = y_n \to f(x_1, \dots, x_n) = f(y_1, \dots, y_n)) \dots)$

R3 p n-ÁRNY PREDIKÁT. SYMBOL, POTOM $(x_1 = y_1 \to \dots (x_n = y_n \to (p(x_1, \dots, x_n) \to p(y_1, \dots, y_n))) \dots)$

VETA: $\vdash x = y \to y = x$

$\vdash x = y \to (y = z \to x = z)$

VETA: NECH $t_1, \dots, t_n, s_1, \dots, s_n$ SÚ TERMY, $\vdash t_i = s_i \; \forall i$

(i) KEĎ TERM s VZNIKNE Z t ZÁMENOU NIEKTORÝCH VÝSKYTOV t_i TERMAMI s_i, POTOM $\vdash t = s$

(ii) KEĎ FORMULA B VZNIKNE Z FORMULE A ZÁMENOU NIEKTORÝCH VÝSKYTOV t_i TERMAMI s_i (OKREM PRÍPADOV, KEĎ t_i JE PREMENNÁ x VIAZANÁ KVANTIFIKÁTOROM), POTOM $\vdash A \Leftrightarrow B$

A JE SÉMANTICKÝ DÔSLEDOK T,
A JE T-PLATNÁ FORMULA, $T \models A$
$\Leftrightarrow$ $\forall \mathcal{M}; \mathcal{M} \models T : \mathcal{M} \models A$, T.J.
A JE SPLNENÁ V KAŽDOM MODELI TEÓRIE T

<u>VETA O KOREKTNOSTI</u>: $T \vdash A \Rightarrow T \models A$

DÔSLEDOK: KEĎ MÁ TEÓRIA T MODEL $\mathcal{M}$,
POTOM JE BEZSPORNÁ

DÔSLEDOK: PREDIKÁTOVÁ LOGIKA JE BEZSPORNÁ

<u>VETA O ÚPLNOSTI</u>: T JE TEÓRIA JAZYKA L
(i) $T \vdash A \Leftrightarrow T \models A$
(ii) T JE BEZSPORNÁ $\Rightarrow$ T MÁ MODEL

(i) JE DÔSLEDOK (ii), STAČÍ DOKÁZAŤ (ii))

<u>ÚPLNÁ TEÓRIA T</u>: T JE <u>BEZSPORNÁ</u>
A PRE KAŽDÚ <u>UZAVRETÚ</u> A : BUĎ $T \vdash A$, ALEBO $T \vdash \neg A$

<u>HENKINOVA TEÓRIA T</u>: PRE KAŽDÚ <u>UZAVRETÚ</u>
$(\exists x) B$ EXISTUJE KONŠTANTA c :
$T \vdash (\exists x) B \to B_x[c]$

5/5

25.08.2008 Mo
PETER ČERNO

ŠTÁTNICE

JAZYK L' JE ROZŠÍRENÍM JAZYKA L $\Leftrightarrow$ L' OBSAHUJE KAŽDÝ ŠPECIÁLNY SYMBOL (A PRÍPADNE AJ =) JAZYKA L

TEÓRIA T' S JAZYKOM L' JE ROZŠÍRENÍM TEÓRIE T S JAZYKOM L $\Leftrightarrow$ JAZ. L' JE ROZŠÍRENÍM JAZ. L, ĽUBOVOĽNÁ FORMULA JAZYKA L, KTORÁ JE VETOU TEÓRIE T, JE TIEŽ VETOU TEÓRIE T'.

TEÓRIA T' S JAZYKOM L' JE KONZERVATÍVNE ROZŠÍRENIE TEÓRIE T S JAZYKOM L, KEĎ T' JE ROZŠÍRENÍM T A KAŽDÁ FORMULA JAZYKA L, KTORÁ JE VETOU T', JE TIEŽ VETOU T.

VETA O KONŠTANTÁCH: ROZŠÍRENIE TEÓRIE O NOVÉ KONŠTANTY JE KONZERVATÍVNE

LEMMA: (i) KEĎ JE BEZSPORNÁ T' ROZŠÍRENÍM T, POTOM AJ T JE BEZSPORNÁ.
(ii) KEĎ JE T' KONZERVATÍVNE ROZŠÍRENIE T, POTOM T JE BEZSPORNÁ $\Leftrightarrow$ T' JE BEZSPORNÁ

VETA (HENKIN): KU KAŽDEJ TEÓRII T MOŽNO ZOSTROJIŤ HENKINOVU T_H, KTORÁ JE KONZ. ROZŠÍRENÍM T

VETA (LINDENBAUM): KAŽDÁ BEZSPORNÁ TEÓRIA T MÁ ÚPLNÉ ROZŠÍRENIE S ROVNAKÝM JAZYKOM

REDUKCIA A EXPANZIA ŠTRUKTÚR: NECH T' JE ROZŠÍRENIE T S JAZYKOM L. KEĎ JE $\mathcal{M}'$ MODEL T', POTOM $\mathcal{M} = \mathcal{M}'|L$ JE MODEL T.

DÔKAZ VETY O ÚPLNOSTI:

NECH T JE BEZSPORNÁ TEÓRIA

HENKIN: EXISTUJE K NEJ KONZ. ROZŠÍRENIE T_H (HENK.T.) ZREJME T_H JE TIEŽ BEZSPORNÁ

LINDENBAUM: T_H MÁ ÚPLNÉ ROZŠÍRENIE T_H' S TÝM ISTÝM JAZYKOM

PLATÍ, ŽE KAŽDÁ ÚPLNÁ HENKINOVA TEÓRIA MÁ MODEL. NECH $\mathcal{M}'$ JE MODEL T_H'. POTOM $\mathcal{M} := \mathcal{M}'|L$ JE MODEL T. $\square$

DÔSLEDOK:

<u>VETA O KOMPAKTNOSTI</u>: MNOŽINA FORMULÍ T MÁ MODEL $\Leftrightarrow$ KAŽDÁ JEJ KON. PODMN. MÁ MODEL.

26.08.2008 Tu
PETER ČERNO

ŠTÁTNICE

REKURZÍVNA FUNKCIA $f : \mathbb{N}^k \to \mathbb{N}$: EFEKTÍVNE VYČÍSLITEĽNÁ (MÁ PRESNÚ DEFINÍCIU)

REKURZÍVNA (ROZHODNUTEĽNÁ) MNOŽINA PRIR. ČÍSIEL : MÁ REKURZÍVNU CHARAKTERISTICKÚ FUNKCIU

PRE LOGIKU 1. RÁDU SO SPOČETNÝM JAZYKOM L, KTORÉHO SYMBOLY DOKÁŽEME EFEKTÍVNE OČÍSLOVAŤ, VIEME PRIRADIŤ KÓDY #A VŠETKÝM FORMULÁM

CHURCH (VETA O NEROZHODNUTEĽNOSTI PRED. LOGIKY)
PRE LOGIKU 1. RÁDU SO SPOČETNÝM JAZYKOM L, KT. OBSAHUJE ASPOŇ 1 KONŠTANTU, ASPOŇ 1 FUNKČNÝ SYMBOL ARITY $k > 0$ A PRE KAŽDÉ $n \geq 0$ SPOČETNE VEĽA PREDIKÁTOVÝCH SYMBOLOV ARITY n PLATÍ, ŽE $\{\#A \mid A \text{ UZAVRETÁ}, L \models A\}$ JE NEROZHODNUTEĽNÁ

VETA O NEROZHODNUTEĽNOSTI PRED. LOGIKY
PRE LOGIKU 1. RÁDU BEZ ROVNOSTI S JAZYKOM L, KTORÝ OBSAHUJE ASPOŇ 2 BINÁRNE PREDIKÁTY PLATÍ, ŽE $\{\#A \mid A \text{ UZAVRETÁ}, L \models A\}$ JE NEROZHODNUTEĽNÁ

ROBINSNOVA ARITMETIKA $\underline{Q}$

R1	$S(x) \neq 0$
R2	$S(x) = S(y) \to x = y$
R3	$x \neq 0 \to (\exists y)(S(y) = x)$
R4	$x + 0 = x$
R5	$x + S(y) = S(x+y)$
R6	$x \cdot 0 = 0$
R7	$x \cdot S(y) = x \cdot y + x$
R8	$x \leq y \leftrightarrow (\exists z)(x + z = y)$

PEANOVA ARITMETIKA P MÁ TIE ISTÉ AXIOMY, AŽ NATO ŽE NAMIESTO 3. AXIÓMU MÁ SCHÉMU

$$A_x[0] \to ((\forall x)(A \to A_x[S(x)]) \to (\forall x)A)$$

ÚPLNÁ ARITMETIKA $Th(\mathbb{N}) = \{A \mid A$ JE UZAVRETÁ, $\mathbb{N} \models A\}$ (TIEŽ PRAVDIVÁ ARITMETIKA)

$\mathbb{N}$ JE ŠTANDARDNÝ MODEL ARITMETIKY

PLATÍ $Q \subset P \subset Th(\mathbb{N})$

Q JE REKURZÍVNE AXIOMATIZOVATEĽNÁ (KONEČNE VEĽA AXIÓMOV), DÁ SA DOKÁZAŤ, ŽE TIEŽ P JE REK. AXIOM., AVŠAK $Th(\mathbb{N})$ UŽ NIE JE

PRE TEÓRIU T S JAZYKOM ARITMETIKY MÔŽME DEFINOVAŤ KÓDY $\#A$ FORMULÍ A, A POLOŽME:

$Thm(T) = \{\#A \mid A$ JE UZAVRETÁ, $T \vdash A\}$

TEÓRIA T JE ROZHODNUTEĽNÁ $\overset{def.}{\iff}$ $Thm(T)$ JE REKURZÍVNA

CHURCH (VETA O NEROZHODNUTEĽNOSTI ARITMETIKY)

KAŽDÉ BEZSPORNÉ ROZŠÍRENIE ROBINSNOVEJ ARITMETIKY JE NEROZHODNUTEĽNÉ

GÖDEL - ROSSER (VETA O NEÚPLNOSTI ARITMETIKY)

ŽIADNE BEZSPORNÉ REKURZÍVNE AXIOMATIZOVATEĽNÉ ROZŠÍRENIE ROBINSOVEJ ARITMETIKY NIE JE ÚPLNÁ TEÓRIA.

26.08.2008 Tu
PETER ČERNO

ŠTÁTNICE

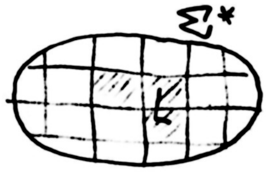
2 AUTOMATY A JAZYKY

KONGRUENCIA $\sim$: EKVIVALENCIA NA Σ^*

PRAVÁ KONGRUENCIA : $\forall u,v,w \in \Sigma^* : u \sim v \Rightarrow uw \sim vw$ (STAČÍ $w \in \Sigma$)

KONEČNÉHO INDEXU : $|\Sigma^*/\sim| < \infty$

NERODOVA VETA :



L JE REGULÁRNY JAZYK $\Leftrightarrow$
$\exists$ PRAVÁ KONGR. $\sim$ KONEČNÉHO INDEXU
TAKÁ, ŽE L JE ZJEDNOTENÍM NEJAKÝCH TR. ROZ. $\Sigma^*/\sim$

ITERAČNÁ PUMPING LEMMA

n VEZMEME POČET STAVOV PRÍSL. AUTOMATU

L REGULÁRNY JAZYK $\Rightarrow$
$\boxed{\exists n \in \mathbb{N}}$ $\forall z \in L\ |z| \geq n\ \exists u,v,w \in \Sigma^*$:
$z = uvw$, $|uv| \leq n$, $|v| \geq 1$, $\forall i \geq 0 : uv^iw \in L$.

DÔSLEDOK : REG. JAZYK L JE NEKONEČNÝ
$\Leftrightarrow \exists u \in L : n \leq |u| < 2n$

A, B SÚ EKVIVALENTNÉ $\Leftrightarrow L(A) = L(B)$

$h: Q_1 \to Q_2$ JE (AUTOMATOVÝ) HOMOMORFIZMUS $\Leftrightarrow$

(i) $h(q_1) = q_2$

(ii) $h(\delta_1(q,x)) = \delta_2(h(q),x)$

(iii) $q \in F_1 \Leftrightarrow h(q) \in F_2$

AK h JE HOMOM. $A \to B$, POTOM A A B SÚ EKVIV.

q JE DOSIAHNUTEĽNÝ STAV $\Leftrightarrow \exists w \in \Sigma^*: \delta^*(q_0, w) = q$

p, q SÚ EKVIVALENTNÉ $\Leftrightarrow$ PÍŠEME $p \sim q$

$\forall w \in \Sigma^*: \delta^*(p, w) \in F \Leftrightarrow \delta^*(q, w) \in F$

$p \sim^i q$ ZVAŽUJEME IBA SLOVÁ $|w| \leq i$

$p \sim^0 q \equiv p \in F \Leftrightarrow q \in F$

$p \sim^{i+1} q \equiv p \sim^i q \;\&\; \forall x \in \Sigma\; \delta(p, x) \sim^i \delta(q, x)$

AUTOMATOVÁ KONGRUENCIA $\equiv$

JE EKVIVALENCIA NA Q

$\forall p, q \in Q: \quad p \equiv q \Rightarrow (p \in F \Leftrightarrow q \in F) \;\&$

$\forall x \in \Sigma: \delta(p, x) \equiv \delta(q, x)$

EKVIVALENCIA STAVOV $\sim$ JE AUTOMATOVÁ KONGRUENCIA

PODIELOVÝ AUTOMAT $A/\equiv$ EKVIVALENTNÝ S A

ŽIADNE DVA STAVY $A/\sim$ NIE SÚ EKVIVALENTNÉ

REDUKOVANÝ AUTOMAT, REDUKT A

VETA: KU KAŽDÉMU A EXISTUJE REDUKT

VETA O IZOMORFIZME REDUKTOV:

DVA REDUKOVANÉ AUTOMATY SÚ EKVIVALENTNÉ $\Leftrightarrow$ SÚ IZOMORFNÉ

$\Rightarrow$) PRE $q \in Q_1 \quad \exists u \in \Sigma^*: \delta_1^*(q_1, u) = q$

POLOŽÍME $h(q) := \delta_2^*(q_2, u)$

26.08.2008 Tu
PETER ČERNO

STÁTNICE

NEDETERMINISTICKÝ KONEČNÝ AUTOMAT

MÁME $\delta : Q \times \Sigma \to \boxed{\mathcal{P}(Q)}$
A POČIATOČNÝ STAV JE $\boxed{S \subseteq Q}$

$w = x_1 \dots x_n$ JE PRIJÍMANÉ $\Leftrightarrow$
$\exists q_1, \dots, q_{n+1} \in Q : \; q_1 \in S, \; q_{i+1} \in \delta(q_i, x_i), \; q_{n+1} \in F$

VETA: $\forall$ NFA A $\exists$ DFA B : $L(A) = L(B)$

$Q_B = \mathcal{P}(Q_A), \quad q_0 = S_A, \quad F_B = \{K \mid K \cap F_A \neq \emptyset\}$
$\delta_B(K, x) = \bigcup_{q \in K} \delta_A(q, x)$

λ-PRECHOD : PRECHOD BEZ ČÍTANIA SYMBOLU

λ-UZÁVER(q) = q A ∀ STAV p : $\exists\, q \xrightarrow{\lambda} \cdot \xrightarrow{\lambda} \cdot \dots \xrightarrow{\lambda} \cdot\, p$

DVOJSMERNÝ AUTOMAT

$\delta : Q \times \Sigma \to Q \boxed{\times \{-1, 0, +1\}}$

W JE PRIJÍMANÉ $\Leftrightarrow$ ČÍTACIA HLAVA PO PRVÝKRÁT OPUSTILA SLOVO W VPRAVO V NIEKTOROM KONCOVOM STAVE

MNOŽINOVÉ OPERÁCIE NA JAZYKOCH $\cup, \cap, -, \overline{}$,

UZAVRETOSŤ TRIEDY REG. JAZYKOV $\mathcal{F}$: STAČÍ UVÁŽIŤ KARTÉZSKY SÚČIN AUTOMATOV.

REŤAZCOVÉ OPERÁCIE NA JAZYKOCH

ZREŤAZENIE $\cdot$, MOCNINY, ITERÁCIE $+$, $*$, OTOČENIE,

ĽAVÝ KVOCIENT L_1 PODĽA L_2:

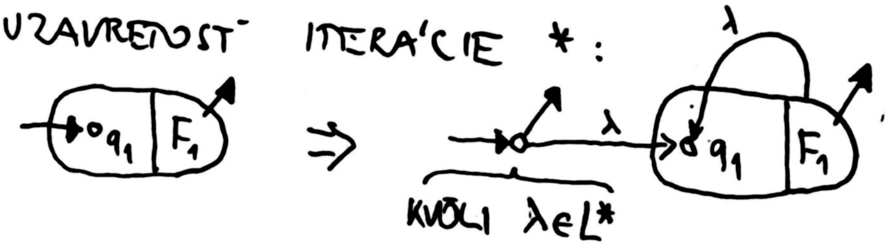
$$L_2 \backslash L_1 = \{ v \mid \exists u \in L_2 : uv \in L_1 \}$$

PRAVÝ KVOCIENT L_1 PODĽA L_2:

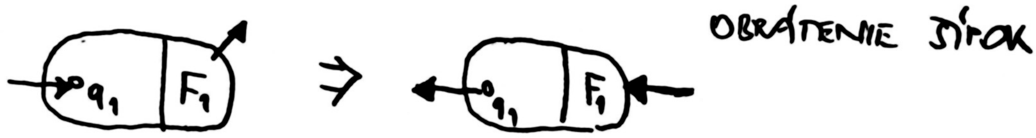
$$L_1 / L_2 = \{ v \mid \exists u \in L_2 : vu \in L_1 \}$$

UZAVRETOSŤ ZREŤAZENIA:

UZAVRETOSŤ ITERÁCIE *:



UZAVRETOSŤ REVERZIE:



SUBSTITÚCIA JAZYKOV

$\forall x \in \Sigma$ NECH $\sigma(x)$ JE JAZYK V ABECEDE Y_x

DEFINUJME $\sigma : \Sigma^* \to P(Y^*)$, KDE $Y = \bigcup_{x \in \Sigma} Y_x$

$\sigma(\lambda) = \{\lambda\}$, $\sigma(u \cdot v) = \sigma(u) \cdot \sigma(v)$

$\sigma(L) := \bigcup_{w \in L} \sigma(w)$

σ JE SUBSTITÚCIA, NEVYPÚŠŤAJÚCA AK $\sigma(x) \not\ni \lambda$ $\forall x$

VETA: $L \in \mathcal{F}$, $\forall x \in \Sigma$ $\sigma(x) \in \mathcal{F} \Rightarrow \sigma(L) \in \mathcal{F}$.

27.08.2008 We
PETER ČERNO

ŠTÁTNICE

REGULÁRNE JAZYKY

TRIEDA $RJ(\Sigma)$ JE NAJMENŠIA TRIEDA JAZYKOV, KT:
1. OBSAHUJE JAZYK $\emptyset$
2. $\forall x \in \Sigma$ OBSAHUJE JAZYK $\{x\}$
3. $A, B \in RJ(\Sigma) \Rightarrow A \cup B,\ A \cdot B,\ A^* \in RJ(\Sigma)$

KLEENOVA : $L \in RJ(\Sigma) \Leftrightarrow \exists$ DFA $A : L = L(A)$

$\Leftarrow$) MÁME $A = (Q, \Sigma, \delta, q_1, F)$
DEFINUJME $R_{ij} = \{w \in \Sigma^* \mid \delta^*(q_i, w) = q_j\}$
POTOM $L(A) = \bigcup_{q_i \in F} R_{1i}$
DEFINUJME R^k_{ij} = SLOVÁ $q_i \xrightarrow{w} q_j$ BEZ POUŽITIA STAVOV q_m $m > k$
ZREJME $R^0_{ij} \in RJ(\Sigma)$, $R^{k+1}_{ij} = R^k_{ij} \cup R^k_{i,k+1} \cdot (R^k_{k+1,k+1})^* \cdot R^k_{k+1,j}$, $R_{ij} = R^n_{ij}$

REGULÁRNE VÝRAZY

$RV(\Sigma)$ JE NAJMENŠIA MN. SLOV NAD AB. $\Sigma \cup \{\emptyset, \lambda, +, \cdot, *, (,)\}$
TAKÁ, ŽE : $\emptyset, \lambda \in RV(\Sigma)$, $\Sigma \subseteq RV(\Sigma)$
$\alpha, \beta \in RV(\Sigma) \Rightarrow (\alpha+\beta), (\alpha \cdot \beta), \alpha^* \in RV(\Sigma)$

HODNOTA $[\alpha]$ JE DEF. AKO:
$[\emptyset] = \emptyset$, $[\lambda] = \{\lambda\}$, $[x] = \{x\}$ $\forall x \in \Sigma$
$[(\alpha+\beta)] = [\alpha] \cup [\beta]$, $[(\alpha \cdot \beta)] = [\alpha] \cdot [\beta]$, $[\alpha^*] = [\alpha]^*$

MOOREOV STROJ : $A = (Q, X, Y, \delta, \mu, q_0)$
Y = VÝSTUPNÁ ABECEDA, $\mu : Q \to Y$ ZNAČKOVACIA FCIA.

MEALYHO STROJ : $A = (Q, X, Y, \delta, \lambda, q_0)$
Y = VÝST. AB., $\lambda : Q \times X \to Y$ VÝSTUPNÁ FCIA.

PREPISOVACÍ (PRODUKČNÝ) SYSTÉM $R=(V,P)$

V JE ABECEDA, P MN. PREPIS. PRAVIDIEL $u \to v$

$w \Rightarrow z \iff \exists u,v,x,y \in V^*: w = xuy,\ z = xvy,\ (u \to v) \in P$

$w \Rightarrow^* z \iff w = u_1 \Rightarrow u_2 \Rightarrow \dots \Rightarrow u_n = z$ (DERIVÁCIA)

GENERATÍVNA GRAMATIKA $G=(V_N, V_T, S, P)$

V_N NETERMINÁLY, V_T TERMINÁLY, $S \in V_N$ POČIATOČNÝ NET. SYM.

P SYSTÉM PRODUKCIÍ $u \to v$, $u,v \in (V_N \cup V_T)^*$

$L(G) = \{ w \mid w \in V_T^* \ \&\ S \Rightarrow^* w \}$

CHOMSKÉHO HIERARCHIA

$\mathcal{L}_0$ (REKURZÍVNE SPOČETNÉ JAZYKY)

OBECNÉ PRAVIDLÁ

$\mathcal{L}_1$ (KONTEXTOVÉ JAZYKY)

$\alpha X \beta \to \alpha w \beta$ $\quad X \in V_N;\ \alpha,\beta \in (V_N \cup V_T)^*,\ w \in (V_N \cup V_T)^+$

VÝNIMKA: $S \to \lambda$. POTOM SA ALE S NEVYSKYTUJE NA PRAVEJ STRANE ŽIADNEHO PRAVIDLA

$\mathcal{L}_2$ (BEZKONTEXTOVÉ JAZYKY)

$X \to w$ $\quad X \in V_N,\ w \in (V_N \cup V_T)^*$

$\mathcal{L}_3$ (REGULÁRNE / PRAVÉ LINEÁRNE JAZYKY) $\quad \mathcal{L}_3 = \mathcal{F}$

$X \to wY,\ X \to w$ $\quad X,Y \in V_N,\ w \in V_T^*$

PLATÍ $\mathcal{L}_0 \supset \mathcal{L}_1 \supset \mathcal{L}_2 \supset \mathcal{L}_3$

EXISTUJÚ EŠTE ĽAVÉ LIN. G. A LINEÁRNE GRAMATIKY

BEZKONTEXTOVÁ GRAMATIKA JE NEVYPÚŠŤAJÚCA $\iff$ NEOBSAHUJE PRAVIDLÁ $X \to \lambda$

KU KAŽDEJ BEZKON. G EXISTUJE NEVYPÚŠŤAJÚCA G_0: $L(G_0) = L(G) \setminus \{\lambda\}$.

27.08.2008 We
PETER ČERNO

ŠTÁTNICE

BEZKONTEXTOVÉ GRAMATIKY

BEZK. GR. G SA NAZÝVA **REDUKOVANÁ** $\Leftrightarrow$

1) $\forall X \in V_N \; \exists w \in V_T^*: X \Rightarrow^* w$
2) $\forall X \in V_N - \{S\} \; \exists u, v \in (V_N \cup V_T)^*: S \Rightarrow^* uXv$ (DOSIAHNUTEĽ.)

KU KAŽDEJ BEZKONTEXTOVEJ GR. G, $L(G) \neq \emptyset$ MOŽNO ZOSTROJIŤ EKVIVALENTNÚ REDUKOVANÚ GR.

1. NAJSKÔR VYHODÍME NETERMINÁLY, KT. NEGEN. TERMIN. SLOVO
2. VYHODÍME NEDOSIAHNUTEĽNÉ NETERMINÁLY

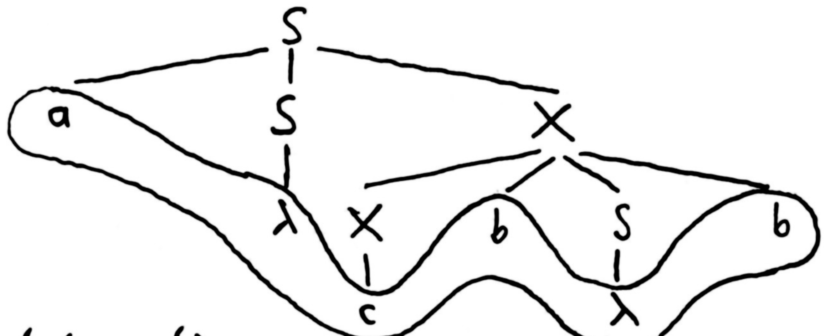
ĽAVÉ PREPÍSANIE $w \Rightarrow z$, KEĎ SA PREPISUJE NAJĽAVEJŠÍ NETERMINÁL

ĽAVÁ DERIVÁCIA VZNIKÁ POUŽITÍM IBA ĽAVÝCH PREPÍSANÍ

$X \Rightarrow^* w \Leftrightarrow$ EXISTUJE ĽAVÁ (PRAVÁ) DERIVÁCIA w Z X

DERIVAČNÝ STROM

G: $S \to aSX \mid \lambda$
$X \to XbSb \mid c$



KAŽDÝ DERIVAČNÝ STROM JEDNOZNAČNE URČUJE ĽAVÚ (PRAVÚ) DERIVÁCIU.

BEZKONTEXTOVÁ GRAMATIKA G JE **VIACZNAČNÁ** (NEJEDNOZNAČNÁ) KEĎ $\exists w \in L(G)$, KTORÉ MÁ DVE RÔZNE ĽAVÉ DERIVÁCIE
INAK JE G JEDNOZNAČNÁ

BEZKONTEXTOVÝ JAZYK L JE JEDNOZNAČNÝ AK $\exists$ JEDNOZNAČNÁ BEZK. GR. GENERUJÚCA TENTO JAZYK

INAK JE L (PODSTATNE) NEJEDNOZNAČNÝ

ZÁSOBNÍKOVÝ AUTOMAT

$M = (Q, X, Y, \delta, q_0, Z_0, F)$

Y .. NEPRÁZDNA KONEČNÁ ZÁSOBNÍKOVÁ ABECEDA

!! $\delta : Q \times (X \cup \{\lambda\}) \times Y \to \mathcal{P}_{FIN}(Q \times Y^*)$!!

Z_0 .. POČIATOČNÝ ZÁSOBNÍKOVÝ SYMBOL

VYKONANIE INŠTRUKCIE $(p, a, Z) \to (q, w)$:
- ZMENA STAVU Z p NA q
- AK JE $a \neq \lambda$, PREČÍTANIE SYMBOLU a
- ZMAZANIE VRCHNÉHO SYMBOLU ZÁSOBNÍKA Z
- PRIDANIE w NA ZÁSOBNÍK (NAJVYŠŠIE BUDE PRVÉ PÍSMENO)

SITUÁCIA ZÁS. AUTOMATU (p, u, v)

$p \in Q$, $u \in X^*$ (ZVYŠOK SLOVA), $v \in Y^*$ (OBSAH ZÁSOBNÍKU)

$E_1 = (p, au, Zv)$ VEDIE NA $E_2 = (q, u, wv) \Leftrightarrow (q, w) \in \delta(p, a, Z)$

PÍŠEME $E_1 \vdash E_2$, $\vdash^*$ JE TRANZITÍVNY UZÁVER

VÝPOČET KONČÍ AK :
- ZÁSOBNÍK JE PRÁZDNY
- NIE JE DEF. ŽIADNA INŠTRUKCIA

(POZOR! PO PREČÍTANÍ SLOVA EŠTE MÔŽE $\exists$ POUŽITEĽNÁ INŠTRUKCIA)

a) PRIJÍMANIE KONCOVÝM STAVOM : SLOVO JE CELÉ PREČÍTANÉ A SME V KONCOVOM STAVE

b) PRIJÍMANIE PRÁZDNYM ZÁSOBNÍKOM : SLOVO JE CELÉ PREČÍTANÉ A ZÁSOBNÍK JE PRÁZDNY

SÚ EKVIVALENTNÉ

a) $L(M) = \{ w \in X^* \mid \exists v \in Y^*, q \in F : (q_0, w, Z_0) \vdash^* (q, \lambda, v) \}$

b) $N(M) = \{ w \in X^* \mid \exists q \in Q : (q_0, w, Z_0) \vdash^* (q, \lambda, \lambda) \}$

27.08.2008 We
PETER ČERNO

ŠTÁTNICE

KAŽDÝ BEZKONTEXTOVÝ JAZYK JE ROZPOZNÁVANÝ ZÁSOBNÍKOVÝM AUTOMATOM PRÁZDNYM ZÁSOBNÍKOM

$$\boxed{\begin{array}{l} G=(V_N, V_T, S, P) \to M=(\{p\}, V_T, V_N \cup V_T, \delta, p, S, \emptyset) \\ \delta(p, \lambda, X) = \{(p, w) \mid (X \to w) \in P\} \quad \forall X \in V_N \\ \delta(p, a, a) = \{(p, \lambda)\} \quad \forall a \in V_T \end{array}}$$

– PLATÍ AJ OPAČNÉ TVRDENIE

NEDETERMINIZMUS ZÁS. AUTOMATU:
1. MNOŽINA MOŽNÝCH PRECHODOV
2. OPRACOVANIE ZÁS. BEZ ČÍTANIA VSTUPU (λ-PRECHOD)

ZÁSOBNÍKOVÝ AUTOMAT $M=(Q, X, Y, \delta, q_0, Z_0, F)$ JE DETERMINISTICKÝ $\Leftrightarrow$

(1) $\forall p \in Q \ \forall a \in X \cup \{\lambda\} \ \forall Z \in Y \quad |\delta(p, a, Z)| \leq 1$

(2) $\forall p \in Q \ \forall Z \in Y \quad \delta(p, \lambda, Z) \neq \emptyset \Rightarrow \forall a \in X: \delta(p, a, Z) = \emptyset$

– DETERMINISTICKÉ BEZKONTEXTOVÉ JAZYKY
SÚ ROZPOZNÁVANÉ DZA KONCOVÝM STAVOM
(OBSAHUJÚ REG. JAZYKY)

$\cup$I

BEZPREFIXOVÉ BEZKONTEXTOVÉ JAZYKY
SÚ ROZPOZNÁVANÉ DZA PRÁZDNYM ZÁSOBNÍKOM
AK M JE DZA, $u \in N(M) \Rightarrow \forall w \in X^+ : uw \notin N(M)$

VETA: BEZPREFIXOVÝ BKJ JE DETERMINISTICKÝ BKJ

VETA: AK L JE DETERMINISTICKÝ BKJ,
POTOM $L\#$ JE BEZPREFIXOVÝ BKJ

GRAMATIKA JE V <u>GREIBACHOVEJ NORMÁLNEJ FORME</u>
$\Leftrightarrow$ $\forall$ PRAVIDLÁ MAJÚ TVAR $A \to au$, $a \in V_T$, $u \in V_N^*$

KU KAŽDÉMU BKJ L $\exists$ GRAMATIKA G V GREIB. NORMÁLNEJ FORME T. Ž. $L(G) = L - \{\lambda\}$

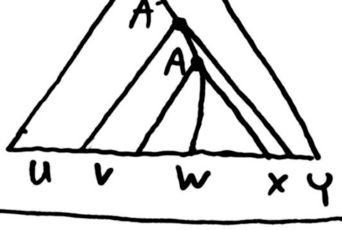
GRAMATIKA JE V <u>CHOMSKÉHO NORMÁLNEJ FORME</u>
$\Leftrightarrow$ $\forall$ PRAVIDLÁ SÚ TVARU: $X \to YZ$, $X \to a$, $a \in V_T$, $X, Y, Z \in V_N$

KU KAŽDÉMU BKJ L $\exists$ GR. G V CHOM. NORMÁLNEJ FORME T. Ž. $L(G) = L - \{\lambda\}$

<u>PUMPING LEMMA</u> PRE BEZKONTEXTOVÉ JAZYKY

AK L JE BKJ $\Rightarrow$ $\exists\, p, q \in \mathbb{N}$:
$\forall z \in L$ $|z| > p$: $z = uvwxy$
(1) $|vwx| \leq q$
(2) $v \neq \lambda \vee x \neq \lambda$
(3) $\forall i \geq 0$ $uv^iwx^iy \in L$

IDEA: V DERIVAČNOM STROME PRE z VEZMIME NAJDLHŠIU CESTU



27.08.2008 We
PETER ČERNO

ŠTÁTNICE

ALGORITMUS CYK

PRÍSLUŠNOSŤ $a_1 \dots a_n$ DO BKJ L

VEZMIME PRÍSLUŠNÚ GRAMATIKU V ChNF

MYŠLIENKA: $X_{i,j} = \{A \mid A \Rightarrow^* a_i \dots a_j\}$

(1) $X_{i,i} = \{A \mid (A \to a_i) \in P\}$

(2) $X_{i,j} = \{A \mid \exists k: i \le k < j \ \exists (A \to BC) \in P \ B \in X_{i,k} \ \& \ C \in X_{k+1,j}\}$

(3) $a_1 \dots a_n \in L \Leftrightarrow S \in X_{1,n}$

DYCKOV JAZYK

D_n NAD ABECEDOU $\{a_1, a_1', \dots, a_n, a_n'\}$

MÁ GRAMATIKU: $S \to \lambda \mid SS \mid a_1 S a_1' \mid \dots \mid a_n S a_n'$

JE NÍM MOŽNÉ POPÍSAŤ VÝPOČTY ĽUBOVOĽNÉHO ZÁSOBNÍKOVÉHO AUTOMATU

VETA: PRE KAŽDÝ BKJ L $\exists$ REGULÁRNY R TAK, ŽE $L = h(D \cap R)$ PRE VHODNÝ DYCKOV JAZYK D A HOMOMORFIZMUS h.*

R .. POPISUJE VŠETKY MOŽNÉ KROKY VÝPOČTU

D .. VYBERIE IBA KOREKTNÉ VÝPOČTY

h .. VYMAŽE POMOCNÉ SYMBOLY

---

* HOMOMORFIZMUS h: $h(x) = w_x$ (ŠPECIÁLNY PRÍP. SUBSTIT.)

PLATÍ: $L \in \mathcal{F} \Rightarrow h(L), h^{-1}(L) \in \mathcal{F}$

BEZKONTEXTOVÉ JAZYKY NIE SÚ UZAVRENÉ NA $\cap$

$\{a^i b^i c^j \mid i,j \geq 0\} \cap \{a^i b^j c^j \mid i,j \geq 0\}$

(DETERM.) BKJ SÚ UZAVRENÉ NA PRIENIK S REG. JAZYKOM

NIEČO AKO KARTÉZSKY SÚČIN DFA A ZA (PRÍJ. STAVOM)

BKJ SÚ UZAVRENÉ NA $\cup$

ZJEDNOTENIE GRAMATÍK

$\Rightarrow$ BKJ NIE SÚ UZAVRENÉ NA DOPLNOK

BKJ SÚ UZAVRENÉ NA

(1) ZRKADLOVÝ OBRAZ : $G: X \to w^R$

(2) ZREŤAZENIE : $G: S \to S_1 S_2$

(3) ITERÁCIU : $G: S' \to S S' \mid \lambda$ (POPR. POZ. ITERÁCIU)

BKJ SÚ UZAVRENÉ NA SUBSTITÚCIU ($\Rightarrow$ HOMOMORFIZMUS)

LISTY V DERIVAČNOM STROME GENERUJÚ ĎALŠIE STROMY

BKJ SÚ UZAVRENÉ NA INVERZNÝ HOMOMORFIZMUS

$h^{-1}(L) = \{w \mid h(w) \in L\}$

MÁME ZÁSOBNÍKOVÝ AUTOMAT M PRE L A ČÍTAME w

BKJ SÚ UZAVRENÉ NA ĽAVÝ (PRAVÝ) KVOCIENT S REG. J.

$R\backslash L = \{w \mid \exists u \in R : uw \in L\}$ $L/R = \{w \mid \exists u \in R \ wu \in L\}$

	RJ	BKJ	DBKJ
ZJEDNOTENIE	✓	✓	✗
PRIENIK	✓	✗	✗
PRIENIK S RJ	✓	✓	✓
DOPLNOK	✓	✗	✓
SUBST / HOMOMORF.	✓	✓	✗
INV. HOMOMORF	✓	✓	✓

!

28.08.2008 Th
PETER ČERNO

STÁTNICE

GRAMATIKA JE <u>SEPAROVANÁ</u> $\Longleftrightarrow$ $\forall$ PRAVIDLÁ SÚ TVARU:

(1) $\alpha \to \beta$, KDE $\alpha, \beta \in V_N^+$

(2) $X \to u$, KDE $X \in V_N$, $u \in V_T \cup \{\lambda\}$

KU KAŽDEJ GRAMATIKE MOŽNO ZOSTROJIŤ EKVIVAL. SEPAROVANÚ GRAMATIKU

GRAMATIKA JE <u>MONOTÓNNA</u> (NEMPÚŠŤAJÚCA)
$\Longleftrightarrow$ $\forall (u \to v) \in P : |u| \leq |v|$

KU KAŽDEJ MONOTÓNNEJ GRAMATIKE MOŽNO NÁJSŤ EKVIVALENTNÚ KONTEXTOVÚ GRAMATIKU.

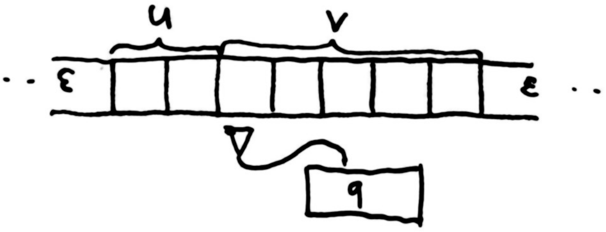
<u>TURINGOV STROJ</u> $T = (Q, \Sigma, \delta, q_0, F)$

Σ NEPRÁZDNA KON. MN. SYMBOLOV, OBSAHUJE ε

!! $\delta : (Q - F) \times \Sigma \longrightarrow Q \times \Sigma \times \{-1, 0, 1\}$!!

VÝPOČET KONČÍ, KEĎ NIE JE DEF. ŽIADNA INŠTR.

<u>KONFIGURÁCIA TS</u>



ZAPISUJEME
uqv

SLOVO w JE PRIJÍMANÉ TS $T \Leftrightarrow q_0 w \vdash^* upv,\ p \in F$

$L(T) = \{ w \in (\Sigma - \{\varepsilon\})^* \mid q_0 w \vdash^* upv,\ p \in F \}$

JAZYK L NAZÝVAME <u>REKURZÍVNE SPOČETNÝ</u>
$\Leftrightarrow$ JE PRIJÍMANÝ NEJAKÝM TURINGOVÝM STROJOM

TRIEDA REKURZÍVNE SPOČ. JAZYKOV JE TRIEDA $\mathcal{L}_0$

<u>NEDETERMINISTICKÝ TURINGOV STROJ</u>

$$\delta : (Q - F) \times \Sigma \to \mathcal{P}(Q \times \Sigma \times \{-1, 0, 1\})$$

w JE PRIJÍMANÉ $\Leftrightarrow$ EXISTUJE VÝPOČET $q_0 w \vdash^* upv,\ p \in F$

NTS PRIJÍMAJÚ PRÁVE REK. SPOČETNÉ JAZYKY $\mathcal{L}_0$

<u>LINEÁRNE OHRANIČENÝ AUTOMAT</u> (LOA)

JE NTS, KDE NA PÁSKE JE OZNAČENÝ ĽAVÝ $\underline{\ell}$
A PRAVÝ $\underline{r}$ KONIEC, TIETO SYMBOLY NEMOŽNO
PREPÍSAŤ A NESMÚ SA PREKROČIŤ

w JE PRIJÍMANÉ LOA $\Leftrightarrow q_0 \underline{\ell} w \underline{r} \vdash^* upv,\ p \in F$

LOA ROZP. PRÁVE TRIEDU $\mathcal{L}_1$ (KONTEXTOVÉ JAZYKY)

TS T <u>ROZHODUJE JAZYK L</u> $\Leftrightarrow L = L(T)$
A PRE KAŽDÉ SLOVO w JE VÝPOČET <u>KONEČNÝ</u>

JAZYKY ROZHODNUTEĽNÉ TS = <u>REKURZÍVNE JAZYKY</u>

VETA (POST) : L JE REK. $\Leftrightarrow L$ AJ $-L$ SÚ REK. SPOČETNÉ.

<u>ALGORITMICKY NEROZHODN. PROBLÉMY</u> :

(1) PROBLÉM ZASTAVENIA TS (HALTING PROBLEM)
(2) POSTOV KORESP. PROBLÉM $[u_1, v_1], \dots, [u_n, v_n]$
(3) PRE BKJ $G_1, G_2 : L(G_1) \cap L(G_2) = \emptyset$, PRE BKJ $G : L(G) = V_T^*$

28.08.2008 Th
PETER ČERNO

ŠTÁTNICE

3 ALGORITMY A DÁTOVÉ ŠTRUKTÚRY

3.1 ČASOVÁ ZLOŽITOSŤ

DOBA SPRACOVANIA ÚLOHY $T(n)$, n = VEĽKOSŤ VSTUPU
V NAJHORŠOM, NAJLEPŠOM, PRIEMERNOM PRÍPADE

$f(n) = O(g(n)) \Leftrightarrow \exists c>0\ \exists n_0\ \forall n \geq n_0 : 0 \leq f(n) \leq c \cdot g(n)$

$f(n) = \Omega(g(n)) \Leftrightarrow \exists c>0\ \exists n_0\ \forall n \geq n_0 : 0 \leq c \cdot g(n) \leq f(n)$

$f(n) = \Theta(g(n)) \Leftrightarrow \exists c_1, c_2 > 0\ \exists n_0\ \forall n \geq n_0 : 0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n)$

$f(n) = o(g(n)) \Leftrightarrow \forall c>0\ \exists n_0\ \forall n \geq n_0 : 0 \leq f(n) < c \cdot g(n)$

PRE $f, g \geq 0$ $\lim_{n \to \infty} \frac{f(n)}{g(n)} = 0 \Rightarrow f(n) = o(g(n))$

AMORTIZOVANÁ ANALÝZA

PRIEMERNÝ ČAS NA JEDNU OPERÁCIU PRI VYKONANÍ SEKVENCIE OPERÁCIÍ NAD DÁTOVÝMI ŠTRUKTÚRAMI

1. AGREGAČNÁ ANALÝZA (AGGREGATE ANALYSIS)

SPOČÍTAME CELKOVÝ ČAS $T(n)$ VYKONANIA n OPERÁCIÍ V NAJHORŠOM PRÍPADE, AMORTIZOVANÁ CENA NA OPERÁCIU JE POTOM $T(n)/n$. NEVÝHODA:
JE ROVNAKÁ PRE $\forall$ TYPY OPERÁCIÍ !!!

2. ÚČTOVNÁ METÓDA (ACCOUNTING METHOD)

PRE KAŽDÝ TYP OPERÁCIE DEFINUJEME POPLATOK (CHARGE) TÁTO CENA URČUJE AMORTIZOVANÚ CENU OPERÁCIE
KEĎ AMORT. CENA OPERÁCIE JE VYŠŠIA AKO SKUTOČNÁ CENA, POTOM ROZDIEL PRIPOČÍTAME NA ÚČET
TENTO ÚČET MÔŽE BYŤ POUŽITÝ NESKÔR NA ZAPLATENIE OPERÁCIÍ, KTORÝCH SKUTOČNÁ CENA JE VYŠŠIA AKO ICH AMORTIZOVANÁ CENA

3. POTENCIÁLNA METÓDA

DEFINUJEME POTENČNÚ FUNKCIU ϕ, KTORÁ MAPUJE STAV DATOVEJ ŠTRUKTÚRY NA REÁLNE ČÍSLO $\phi(D)$ NAZÝVANÉ POTENCIÁL

ZAČNEME S DATOVOU ŠTRUKTÚROU D_0

NECH c_i JE SKUTOČNÁ CENA i-TEJ OPERÁCIE NA D_{i-1}

AMORTIZOVANÚ CENU $\hat{c}_i$ POTOM DEFINUJEME AKO:

$$\hat{c}_i = c_i + \phi(D_i) - \phi(D_{i-1})$$

KEĎ VIEME DEFINOVAŤ POTENČNÚ FCIU. ϕ TAK, ŽE $\phi(D_n) \geq \phi(D_0)$, POTOM

$\sum_{i=1}^{n} \hat{c}_i$ JE HORNÝ ODHAD $\sum_{i=1}^{n} c_i$

STAČÍ POŽADOVAŤ $\phi(D_0) = 0$ A $\phi(D_i) \geq 0 \ \forall i$

3.2 TRIEDY ZLOŽITOSTI P A NP, PREVODITEĽNOSŤ, NP-ÚPLNOSŤ

P = PROBLÉMY RIEŠITEĽNÉ V POLYNOMIÁLNOM ČASE

NP = PROBLÉMY VERIFIKOVATEĽNÉ V POLYN. ČASE

TJ. AK MÁME CERTIFIKÁT RIEŠENIA, SME SCHOPNÍ V POLYNOMIÁLNOM ČASE OVERIŤ PLATNOSŤ TOHTO CERTIFIKÁTU.

NAPR. PRE HAMILT. KRUŽNICU V $G=(V,E)$ BY BOL CERTIFIKÁT POSTUPNOSŤ VRCHOLOV $(v_1, \dots, v_{|V|})$

ZREJME $P \subseteq NP$

NPC = PROBLÉM JE NP-COMPLETE AK JE V NP A JE TAKÝ „ŤAŽKÝ" AKO KAŽDÝ INÝ PROBLÉM V NP

AK EXISTUJE POL. ALG. PRE JEDEN NPC PROBLÉM, POTOM EXISTUJE PRE VŠETKY NPC PROBLÉMY

28.08.2008Th
PETER ČERNO

ŠTÁTNICE

REDUKCIA

MAJME ROZHODOVACÍ PROBLÉM (DECISION PROBLEM) A, NECH α JE JEHO INŠTANCIA

PREDPOKLADAJME, ŽE POZNÁME ROZHODOVACÍ PROBLÉM B Z TRIEDY P A ŽE VIEME KAŽDÚ INŠTANCIU α PROBL. A REDUKOVAŤ NA INŠTANCIU β PROBL. B V POLYNOMIÁLNOM ČASE TAK, ŽE OBE INŠTANCIE MAJÚ ROVNAKÉ RIEŠENIA (ODPOVEDE).

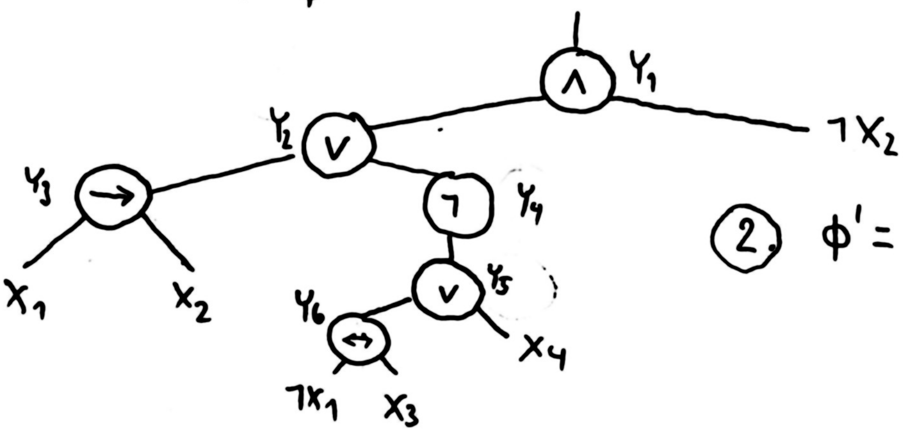
POTOM A PATRÍ DO TRIEDY P.

VETA: EXISTUJE NPC PROBLÉM: (COOK-LEVIN 1971)
SAT = SPLNITEĽNOSŤ LOG. FORMULÍ JE NPC

VETA: 3-SAT JE NPC

MAJME $\phi = ((x_1 \to x_2) \vee \neg((\neg x_1 \Leftrightarrow x_3) \vee x_4)) \wedge \neg x_2$

1. $\to$ STROM K ϕ:



2. $\phi' = y_1 \wedge (y_1 \Leftrightarrow (y_2 \wedge \neg x_2))$
$\wedge\ (y_2 \Leftrightarrow (y_3 \vee y_4))$
$\dots$
$\wedge\ (y_6 \Leftrightarrow (\neg x_1 \Leftrightarrow x_3))$

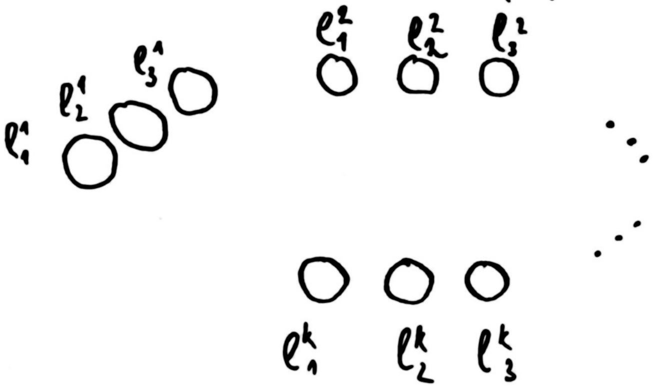
3. NÁJDEME CNF TVARY JEDN. RIADKOV ϕ'

4. $C_i = (l_1 \vee l_2) \rightsquigarrow (l_1 \vee l_2 \vee p) \wedge (l_1 \vee l_2 \vee \neg p)$
$C_i = (l) \rightsquigarrow (l \vee p \vee q) \wedge \dots \wedge (l \vee \neg p \vee \neg q)$

VETA: <u>CLIQUE</u> = {(G, k) : G MÁ KLIKU VEĽKOSTI k} JE NPC

REDUKCIA Z 3-CNF-SAT:

MAJME 3-CNF $C_1 \wedge \dots \wedge C_k = \varphi$



G: l_i^r JE SPOJENÝ S l_j^s :

$\Leftrightarrow$ (1) $r \neq s$

(2) l_i^r NIE JE NEGÁCIA l_j^s

φ JE SPLNITEĽNÁ $\Leftrightarrow$ G MÁ KLIKU VEĽKOSTI k.

VETA: <u>VERTEX-COVER</u> = {(G, k) :
G MÁ VRCHOLOVÉ POKRYTIE VEĽKOSTI k} JE NPC

REDUKCIA Z CLIQUE:

G MÁ KLIKU VEĽKOSTI k $\Leftrightarrow$
$\bar{G} = (V, \bar{E})$ MÁ VRCHOLOVÉ POKRYTIE VEĽKOSTI $|V| - k$

ĎALŠIE NPC PROBLÉMY:

HAM-CYCLE
TSP (TRAVELING-SALESMAN PROBLEM
SUBSET-SUM = $\{(S, t) : \exists S' \subseteq S : t = \sum_{s \in S'} s\}$
INDEPENDENT-SET
3-COLOR

28.08.2008 Th
PETER ČERNO

ŠTÁTNICE

3.2 METÓDA ROZDEĽUJ A PANUJ (DIVIDE & CONQUER)

DIVIDE : ROZDEĽ PROBLÉM NA PODPROBLÉMY
CONQUER: VYRIEŠ PODPROBLÉMY REKURZÍVNE
COMBINE: SKOMBINUJ RIEŠENIA PODPROBLÉMOV NA VRIEŠENIE PROBLÉMU

PRÍKLAD : MERGE SORT

ANALÝZA ZLOŽITOSTI

REKURENCIA JE ROVNICA, KTORÁ POPISUJE FUNKCIU POMOCOU JEJ HODNÔT NA MENŠÍCH VSTUPOCH

PREDPOKLADÁME, ŽE $T(n) = \Theta(1)$ PRE MALÉ n

PRÍKLAD REKURENCIE: $T(n) = 2 \cdot T(n/2) + \Theta(n)$

1. SUBSTITUČNÁ METÓDA

NAJSKÔR UHÁDNEME TVAR RIEŠENIA A POTOM POUŽIJEME MAT. INDUKCIU NA NÁJDENIE KONŠTÁNT A DÔKAZ ODHADU

2. MASTER THEOREM

NECH $a \geq 1$, $b > 1$, $f(n)$ JE FCIA. $F: \mathbb{N}_0 \to \mathbb{N}$

$$T(n) = a \cdot T(n/b) + f(n) \quad \left(\text{KDE } \tfrac{n}{b} = \left\lfloor \tfrac{n}{b} \right\rfloor \text{ ALEBO } \left\lceil \tfrac{n}{b} \right\rceil \right)$$

a) $f(n) = O(n^{\log_b a - \varepsilon})$, $\varepsilon > 0 \Rightarrow T(n) = \Theta(n^{\log_b a})$

b) $f(n) = \Theta(n^{\log_b a}) \Rightarrow T(n) = \Theta(n^{\log_b a} \lg n)$

c) $f(n) = \Omega(n^{\log_b a + \varepsilon})$, $\varepsilon > 0$, $a \cdot f(n/b) \leq c f(n)$ PRE $c < 1$ $\forall n \geq n_0 \Rightarrow T(n) = \Theta(f(n))$.

29.08.2008 Fr
PETER ČERNO

ŠTÁTNICE

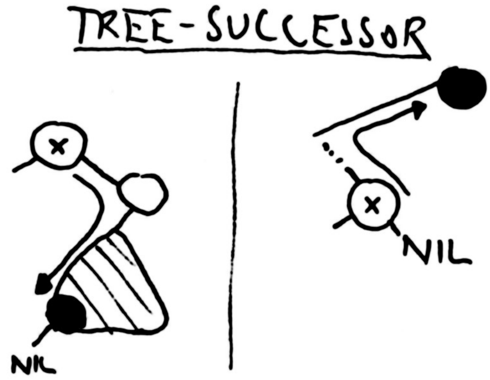
3.4 BINÁRNE VYHĽADÁVACIE STROMY (BINARY SEARCH TREES)

KAŽDÝ UZOL (NODE) OBSAHUJE :
KĽÚČ key, [+SATELITNÉ DATA],
left, right, p: UKAZATELE NA ĽAVÝ, PRAVÝ PODUZOL, NA PREDKA

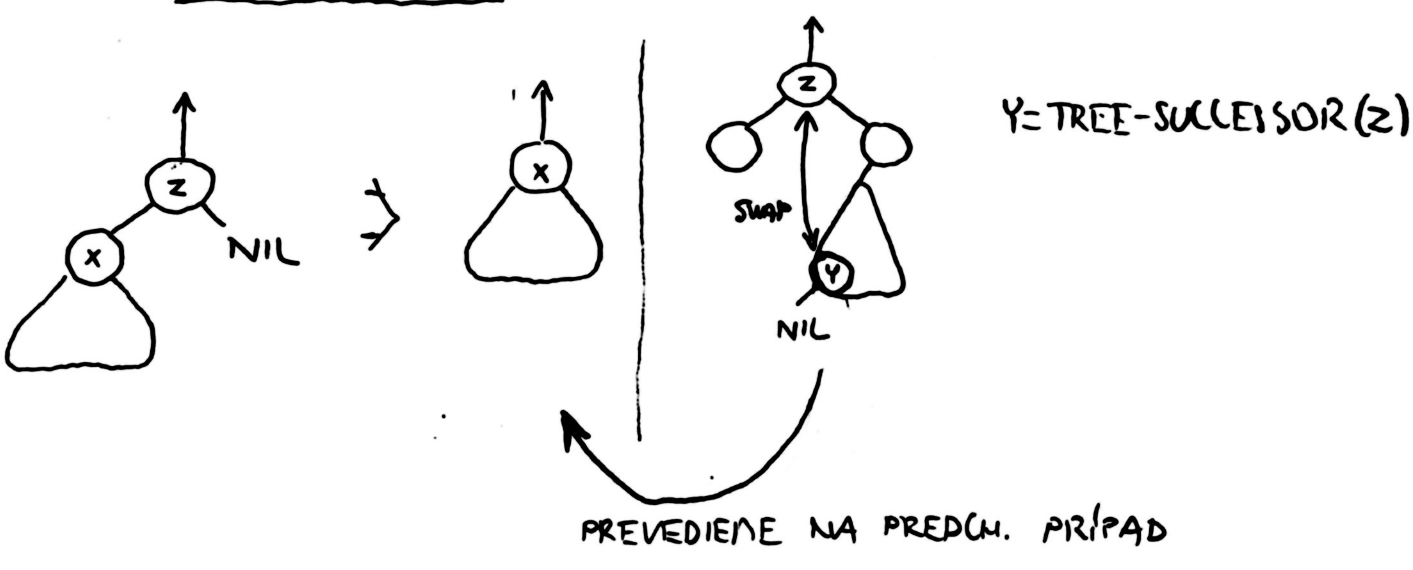
BINARY-SEARCH-TREE PROPERTY :
NECH x JE UZOL. AK y JE UZOL V ĽAVOM PODSTROME x, POTOM $key[y] \leq key[x]$
AK V PRAVOM, POTOM $key[y] \geq key[x]$

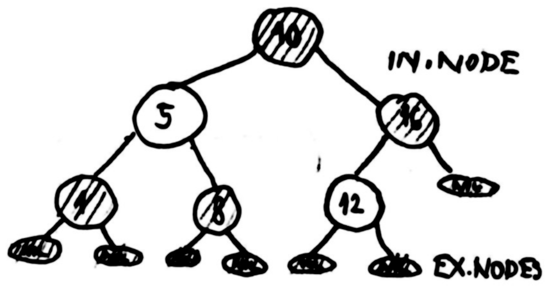
OPERÁCIE :
- TREE-SEARCH (x, k)
- TREE-MINIMUM (x)
- TREE-MAXIMUM (x)
- TREE-SUCCESSOR (x)
- TREE-PREDECESSOR (x)
- TREE-INSERT (T, z)
- TREE-DELETE (T, z)

TREE-SUCCESSOR



TREE-DELETE





RED-BLACK TREES
ČERVENO-ČIERNE STROMY

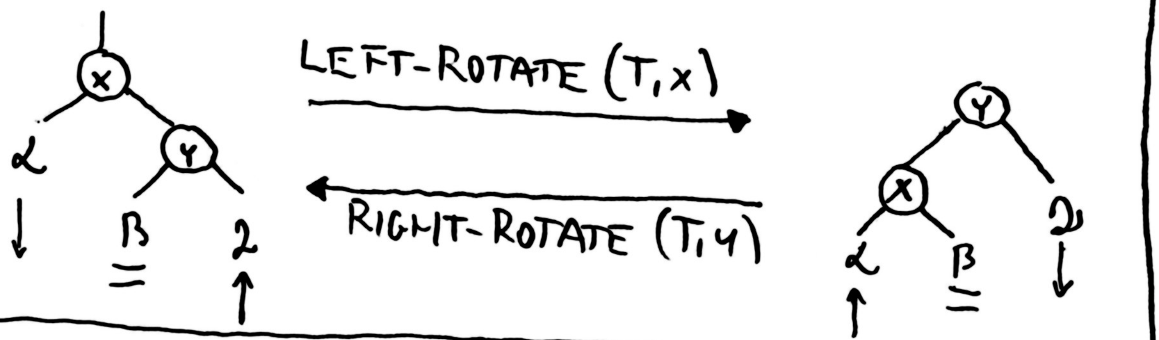
RB TREE JE BST TAKÝ, ŽE:

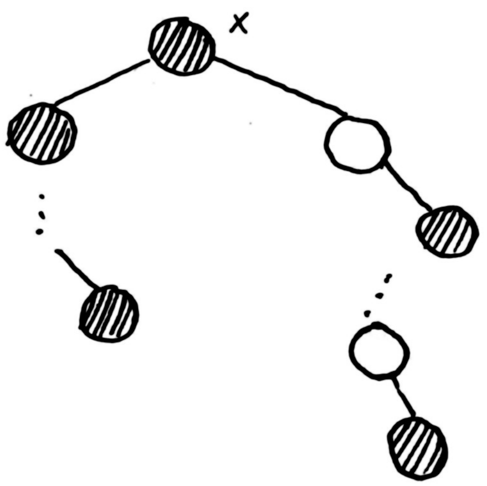
1. KAŽDÝ UZOL JE BUĎ ČERVENÝ ALEBO ČIERNY
2. KOREŇ JE ČIERNY

! OSTATNÉ UZLY SÚ INTERNAL N. !

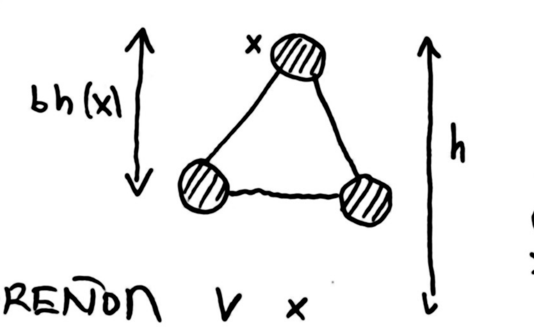
3. KAŽDÝ LIST (NIL) JE ČIERNY (EXTERNAL NODE)
4. KEĎ JE UZOL ČERVENÝ, POTOM OBA JEHO POTOMKOVIA SÚ ČIERNI
5. PRE KAŽDÝ UZOL x: ∀ CESTY Z UZLU x DO LISTOV OBSAHUJÚ TEN ISTÝ POČET ČIERNYCH UZLOV

POMOCNÉ OPERÁCIE:





$$\frac{\#\ \text{NAJDLHŠIA CESTA}}{\#\ \text{NAJKRATŠIA CESTA}} \leq 2$$



bh(x) = POČET ČIERNYCH UZLOV NA CESTE Z x DO LISTOV **OKREM UZLU x!**

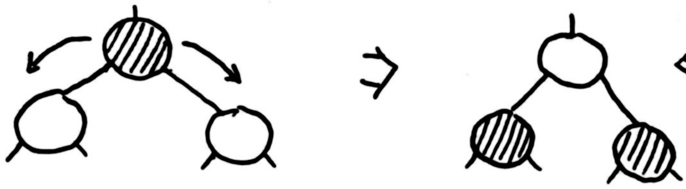
KAŽDÝ RB PODSTROM S KOREŇOM V x OBSAHUJE ASPOŇ $2^{bh(x)}-1$ INTERNAL UZLOV (INDUKCIA PODĽA h(x) = VÝŠKA PODSTROMU S KOR. V x)

$$bh(x) \geq \tfrac{1}{2} h(x) \Rightarrow n \geq 2^{h/2}-1 \Rightarrow h \leq 2 \log_2(n+1)$$

29.08.2008 Fr
PETER ČERNO

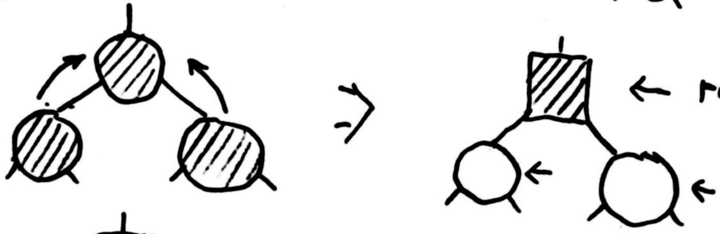
ŠTÁTNICE

POVOLENÉ FAREBNÉ ZÁMENY:



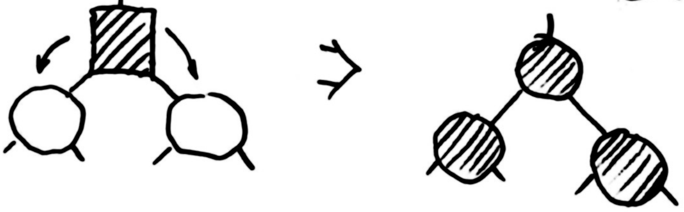
← MÔŽE DÔJSŤ K PORUŠENIU PODMIENKY 2 ALEBO 4

← MÔŽE DÔJSŤ K PORUŠENIU PODMIENKY 4



← PORUŠENIE PODMIENKY 1

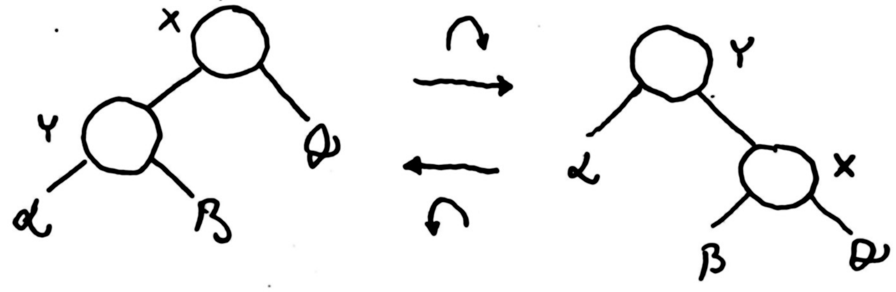
← MÔŽE DÔJSŤ K PORUŠENIU PODMIENKY 4



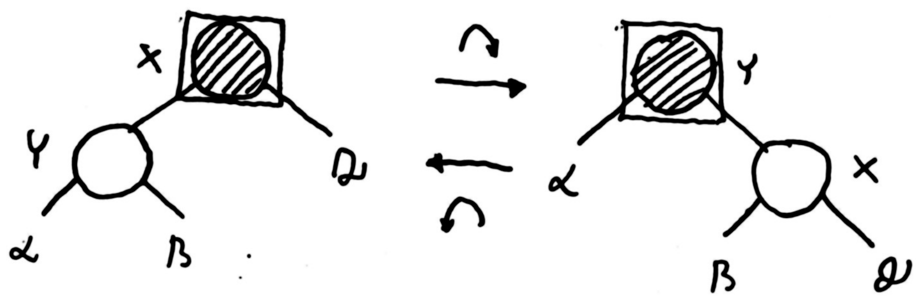
> ZA KAŽDÚ CENU SA SNAŽÍME ZACHOVAŤ PODMIENKU 5

POVOLENÉ ROTÁCIE:

TYP 1:



TYP 2:



ROTÁCIE PRI INÝCH FARBÁCH NIE SÚ POVOLENÉ

$\boxed{\text{RB-INSERT}(T, z)}$

```
BST-INSERT(T, z)
color[z] ← RED
RB-INSERT-FIXUP(T, z)
```

MÔŽE DÔJSŤ K PORUŠENIU PODMIENKY 2 ALEBO 4

RB-INSERT-FIXUP(T, z)

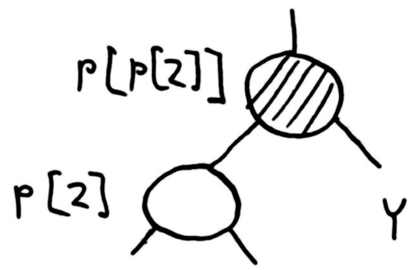
```
while color[p[z]] = RED do
  ...
color[root[T]] ← BLACK
```

INVARIANT: NA ZAČIATKU CYKLU JE color[z] = RED

BÚNO NECH p[z] = left[p[p[z]]]

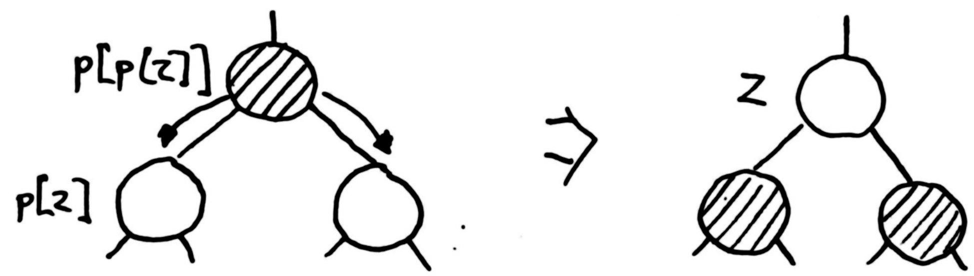
POLOŽME y ← right[p[p[z]]]

p[p[z]] URČITE EXISTUJE A JE ČIERNY



2 PRÍPADY:

1. color[y] = RED. POTOM:

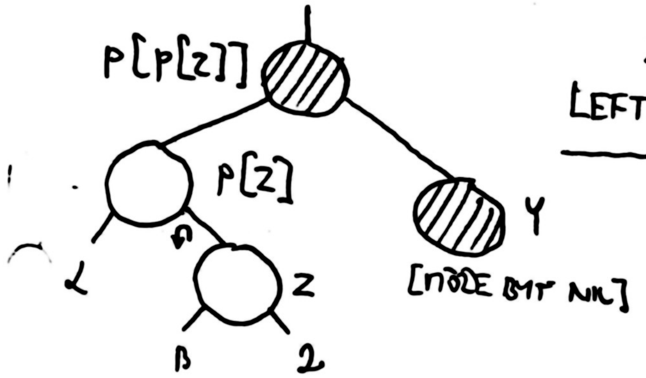


29.08.2008 Fr
PETER ČERNO

ŠTÁTNICE

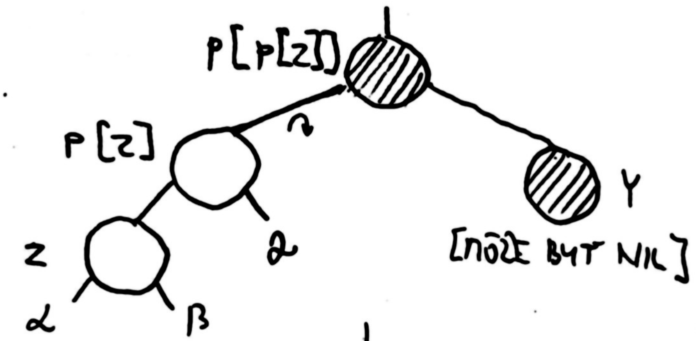
2. color [y] = BLACK

a) z = right [p[z]]

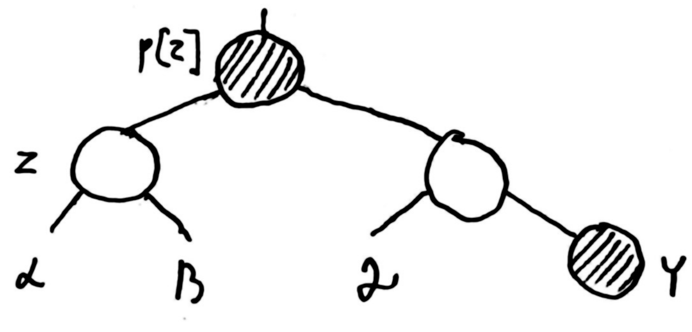


z ← p[z]
LEFT-ROTATE(T, z)
→ PREVEDIEME NA PRÍPAD b)

b) z = left [p[z]]



↓ RIGHT-ROTÁCIA TYPU 2



VÝSLEDNÝ STROM UŽ JE KOREKTNÝ RB-TREE

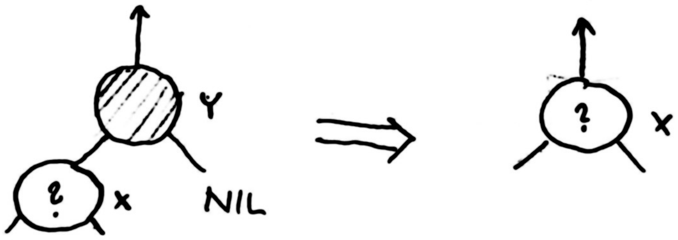
POZNÁMKA: PRI RB-INSERT-FIXUP SÚ MAX. 2 ROTÁCIE.

RB-DELETE(T, z)

POSTUPUJEME AKO PRI BST-DELETE(T, z)

POKIAĽ MAL VRCHOL, KTORÝ SME SKUTOČNE VYNECHALI ČIERNU FARBU, ZAVOLÁME

RB-DELETE-FIXUP(T, x), KDE x JE AKO NA OBR.:



RB-DELETE-FIXUP(T, x)

while $x \neq root[T]$ & $color[x] = BLACK$ do

[...

$color[x] \leftarrow BLACK$

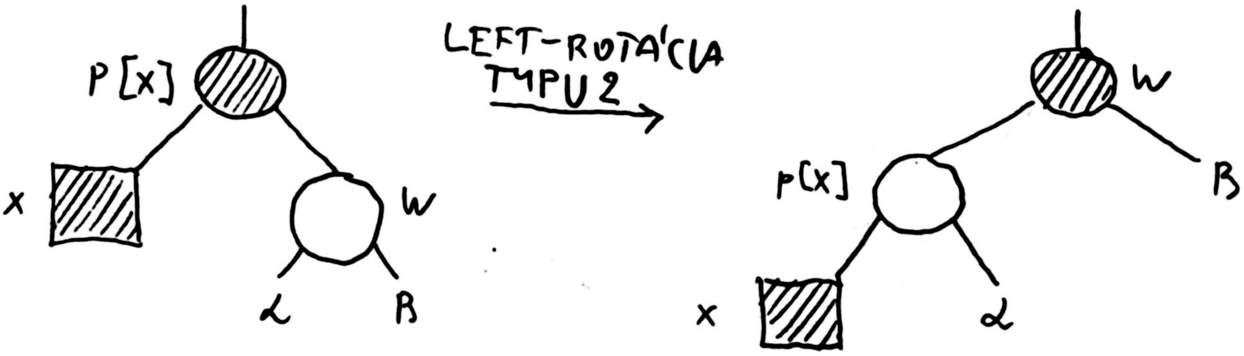
BÚNO $x = left[p[x]]$

POLOŽME $w \leftarrow right[p[x]]$

p[x] URČITE EXISTUJE A JE $\neq$ NIL

2 PRÍPADY

1. $color[w] = RED$

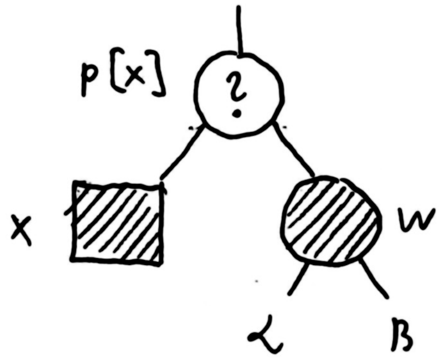


PO $w \leftarrow right[p[x]]$ MÁME PRÍPAD 2 !!

29.08.2008 Fr
PETER ČERNO

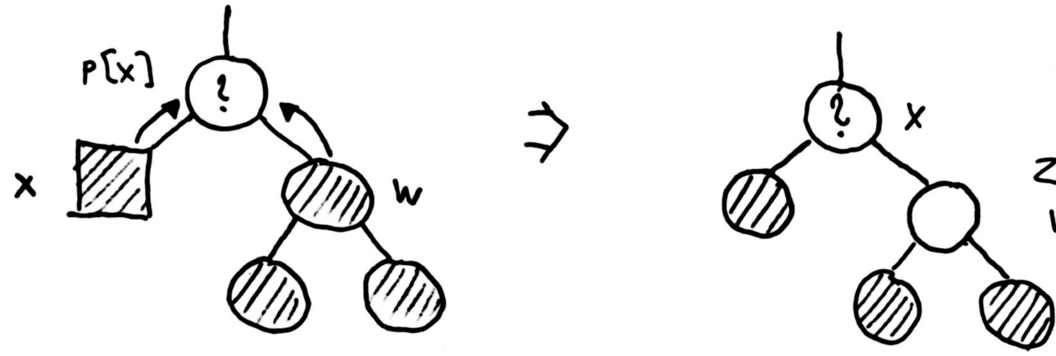
ŠTÁTNICE

2. color [w] = BLACK



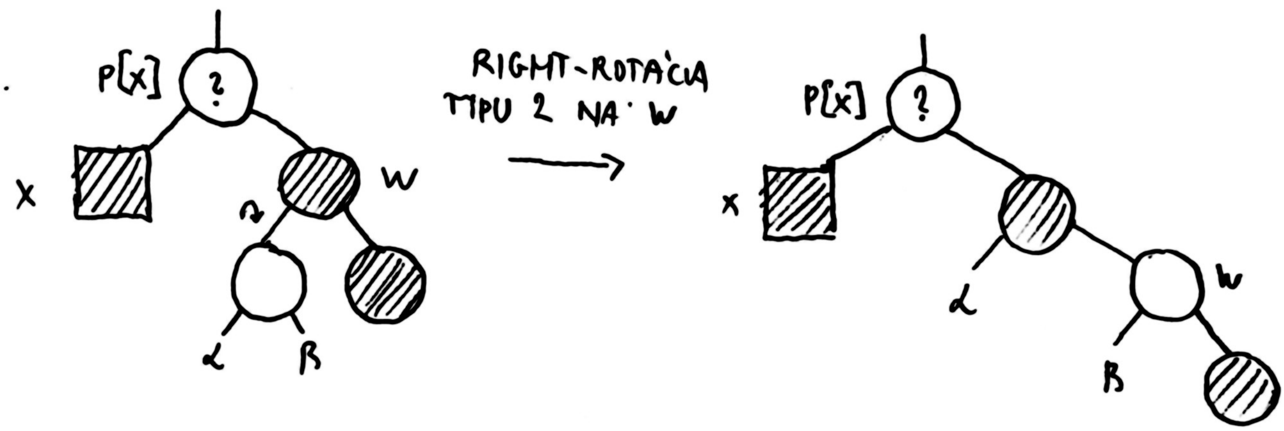
w ≠ NIL, TO MUSÍ MAŤ NÁSLEDNÍKOV, PRETOŽE x JE DOUBLE BLACK !!

a) color [left [w]] = color [right [w]] = BLACK



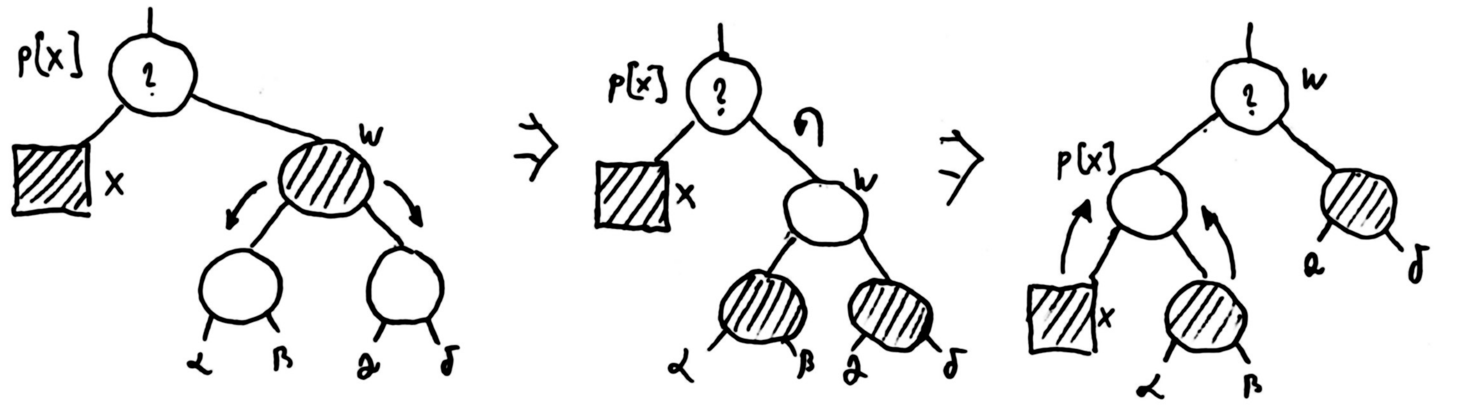
SKOK NA ZAČIATOK while-CYKLU !

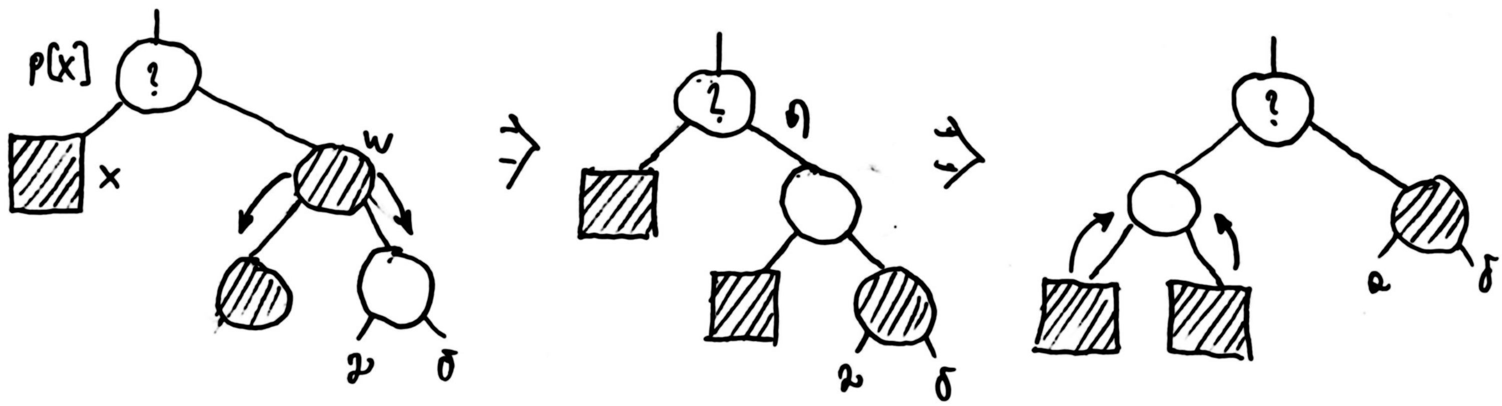
b) color [right [w]] = BLACK



POLOŽÍME w ← right [p [x]]
A DOSTÁVAME PRÍPAD c)

c) color[right[w]] = RED





POLOŽÍME $x \leftarrow root[T]$ A SME HOTOVÍ !!!

ANALÝZA:

PRÍPAD 1 SA PREVEDIE NA PRÍPAD 2 A TAM TO SKONČÍ V BODE 2a)

POSÚVAME SA VYŠŠIE VŽDY LEN V 2a) (POKIAĽ NEBOLA ROTÁCIA)

PRÍPAD 2b) SA PREVEDIE NA 2c) A TAM TO SKONČÍ !

NAJVIAC 2 ROTÁCIE !!

29.08.2008 Fr
PETER ČERNO

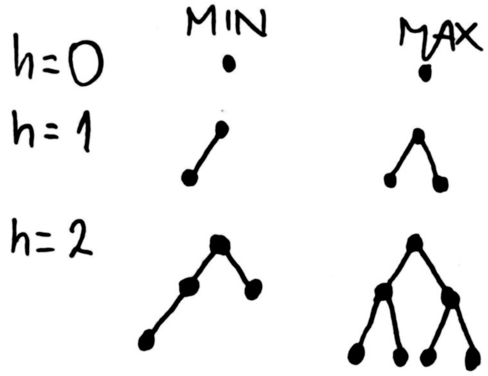
ŠTÁTNICE

AVL STROMY (ADELSON-VELSKY & LANDIS)

HORNÝ ODHAD PRE HĹBKU AVL STROMU

$bf(x) \stackrel{def}{:=} h(left[x]) - h(right[x])$, $h(nil) = -1$

$\forall x : |bf(x)| \le 1$



PLATÍ

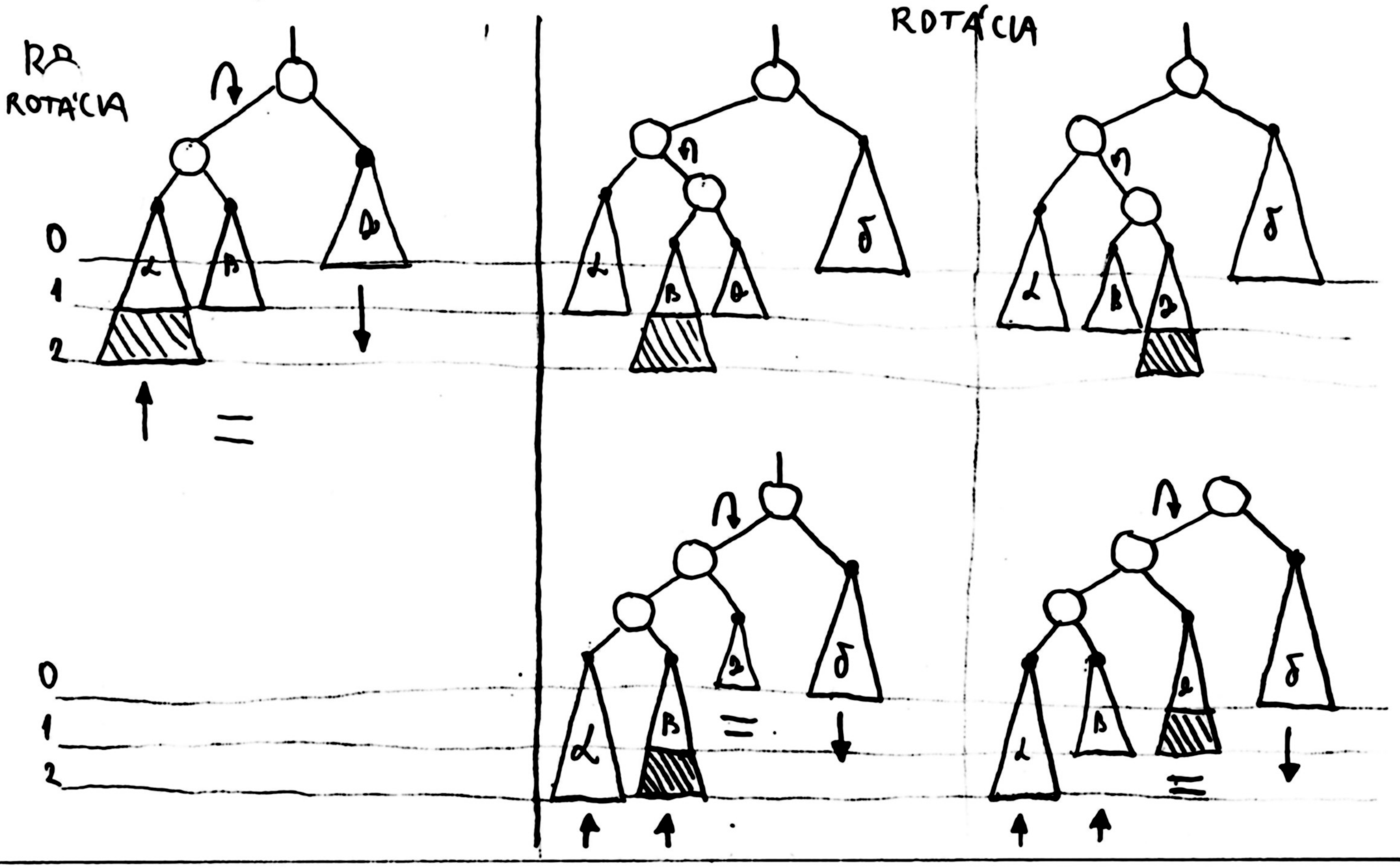
$N_h(T) = 1 + N_{h-1}(T_L) + N_{h-1}(T_R) \ge$

$\ge 1 + min_{h-1} + min_{h-2}$

n	0	1	2	3	4	5	6
F_n	0	1	1	2	3	5	8

VYJDE $min_h = F_{h+3} - 1$

$F_n \le \frac{2}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$



HALDA (HEAP)

DYNAMICKÁ MNOŽINA SO STROMOVOU ŠTRUKTÚROU

MAX-HEAP: AK Y JE POTOMOK X, POTOM $key[x] \geq key[y]$
MIN-HEAP: -||- $key[x] \leq key[y]$

BINARY HEAP .. HALDA REPR. TAKMER KOMPLETNÝM BIN. STROMOM
ULOŽENÁ V POLI $A[1 .. length[A]]$, MÁ heap-size [A] PRVKOV
KOREŇ JE NA POZÍCII 1
$PARENT(i) = \lfloor i/2 \rfloor$, $LEFT(i) = 2i$, $RIGHT(i) = 2i+1$

MAX-HEAPIFY (A, i)
PREDPOKLADÁ, ŽE PODSTROMY S KOREŇMI LEFT(i), RIGHT(i)
SÚ MAX-HEAPS, NECHÁ PREBUBLAŤ A[i] SMEROM DOLU
TAK, ŽE PODSTROM S KOREŇOM V i SA STANE MAX-HEAP

```
BUILD-MAX-HEAP(A)
  heap-size [A] ← length[A]
  for i ← ⌊length[A]/2⌋ downto 1 do
    MAX-HEAPIFY (A,i)
```

ČASOVÁ ZLOŽITOSŤ
$O(n)$
WORST-CASE

```
HEAPSORT(A)
  BUILD-MAX-HEAP (A)
  for i ← length[A] downto 2 do
    SWAP A[1] ↔ A[i]
    heap-size [A] ← heap-size [A] - 1
    MAX-HEAPIFY (A,1)
```

ČASOVÁ ZLOŽITOSŤ
$O(n \log n)$
WORST-CASE

FIBBONACIHO HALDA:
AMORTIZOVANÁ O(1) PRE VLOŽENIE, HĽADANIE MINIMA
TVORÍ JU SKUPINA STROMOV MHOWSÚCA MIN-HEAP VLASTN.
POUŽÍVAJÚ SA PRE EFEKTÍVNU IMPL. NAPR. DIJKSTR. ALG.

29.08.2008 Fr
PETER ČERNO

ŠTÁTNICE

HAŠOVANIE

DANÉ UNIVERZUM U, CHCEME REPREZENTOVAŤ PODMNOŽINU $S \subseteq U$, $|S| << |U|$

OPERÁCIE :

- MEMBER(x)
- INSERT(x)
- DELETE(x)

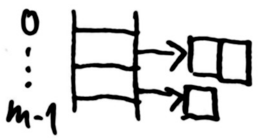
$h: U \to \{0, 1, \dots, m-1\}$ HAŠOVACIA FUNKCIA

PRVOK $x \in S$ JE ULOŽENÝ NA RIADKU $h(x)$

KOLÍZIA $h(s) = h(t)$ PRE $s \neq t$

FAKTOR NAPLNENIA $\alpha = \frac{n}{m}$, KDE $n = |S|$

HASHOVANIE SO SEPAROVANÝMI REŤAZCAMI



OČAKÁVANÝ POČET TESTOV $e^{-\alpha} + \alpha$ V NEÚSP. PRÍPADE
$1 + \alpha/2$ V ÚSPEŠNOM PRÍPADE

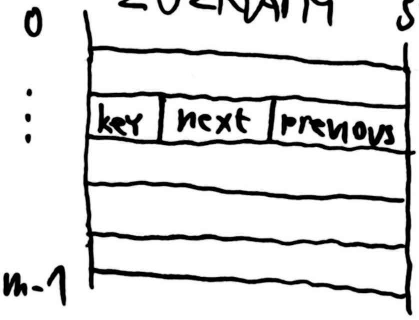
HASHOVANIE S USPORIADANÝMI REŤAZCAMI

V NEÚSPEŠ. PRÍPADE $e^{-\alpha} + 1 + \alpha/2 + \dots$

HAŠOVANIE S PREMIESTŇOVANÍM

HASH. S 2 UKAZATEĽMI OBSAHUJE next A begin

ZOZNAMY SÚ UKLADANÉ DO TABUĽKY



INSERT
- VOĽNÉ MIESTO
- OBSADENÉ PRVKOM, KTORÝ TAM PATRÍ (VLOŽÍME NA KONIEC Z.) TJ. previous = ∅
- OBSADENÉ PRVKOM, KTORÝ TAM NEPATRÍ (PRESUNIEME) TJ. KEĎ previous ≠ ∅

P. TESTOV $\approx e^{-\alpha} + \alpha$
$\approx 1 + 1/\alpha$

POZRETˇ ZRASTAJÚCE HASHOVANIE NA WIKI !! LISCH EISCH LICH VICH EICH

HASHOVANIE S LINEÁRNYM PRIDÁVANÍM

PRI KOLÍZII HĽADÁME PRVÝ NASLEDUJÚCI VOĽNÝ RIADOK

AK $m \geq 2n$ POTOM S VYSOKOU PRAVDEPODOBNOSŤOU JE NAJDLHŠÍ OSTROVČEK DLHÝ $O(\log m)$

UNIVERZÁLNE HASHOVANIE

MÁME MNOŽINU $\mathcal{H}$ HASH FCIÍ. $h: U \to \{0, \dots, m-1\}$

$\mathcal{H}$ SA NAZÝVA UNIVERZÁLNA $\Leftrightarrow$

$\forall k, l \in U$ $k \neq l$ JE POČET HASH. FCIÍ. $h \in \mathcal{H}$ TAKÝCH, ŽE $h(k) = h(l)$ NAJVAC $|\mathcal{H}| / m$

TJ. PRAVDEPODOBNOSŤ KOLÍZIE PRE $k \neq l$ JE $\leq 1/m$

NECH $U = \{0, \dots, p-1\}$ p JE VEĽKÉ PRVOČÍSLO

PRE $0 < a < p$, $0 \leq b < p$ POLOŽME

$h_{a,b}: U \to \{0, \dots, m-1\}$ $x \mapsto [(ax+b) \bmod p] \bmod m$

MNOŽINA $\mathcal{H}$ TAKÝCHTO FCIÍ. JE UNIVERZÁLNA.

NECH $M \subseteq U$, $|M| = n$, $h \in \mathcal{H}$

$C(M, h)$ = # KONFLIKTOV PRI POUŽITÍ h NA M

PLATÍ $\frac{1}{|\mathcal{H}|} \sum_{h \in \mathcal{H}} C(M, h) \leq \frac{n(n-1)}{m}$.

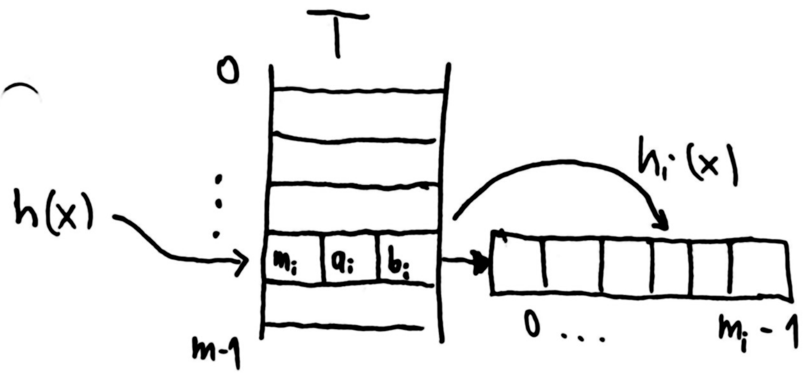
29.08.2008 Fr
PETER ČERNO

ŠTÁTNICE

PERFEKTNÉ HASHOVANIE

MNOŽINA KĽÚČOV $M \subseteq U$ JE VOPRED ZNÁMA
WORST-CASE # PRÍSTUPOV DO PAMÄTI MÁ BYŤ $O(1)$

SCHÉMA: DVOJÚROVŇOVÉ UNIVERZÁLNE HAŠHOVANIE



ŽIADNE KOLÍZIE !

KLADIEME $m = n$, $m_i = n_i^2$
h VYBERÁME Z $\mathcal{H}_{m,p}$, h_i Z $\mathcal{H}_{m_i,p}$

OČAKÁVANÉ MNOŽSTVO POUŽITEJ PAMÄTE: $O(n)$

EXTERNÉ HAŠHOVANIE

DÁTA UKLADÁME NA EXTERNÉ MÉDIUM (HDD)
EXTERNÁ PAMÄŤ ROZDELENÁ NA STRÁNKY

SNAŽÍME SA MINIMALIZOVAŤ POČET
NAČÍTANÍ A ZÁPISOV STRÁNOK NA EXTERNÉ MÉDIUM !

SOS (SCHÉMA ORG. SÚBOROV) = PAMÄŤOVÁ ŠTRUKTÚRA + ALGORITMY OPERÁCIÍ
VYVÁŽENOSŤ SOS: a) OHRANIČENIE DĹŽKY CESTY V ŠTRUKT.
b) ROVNOMERNÁ NAPLNENOSŤ LOG. STRÁNOK

ROZDELENIE SOS:

STATICKÉ (NESPĹŇAJÚ a) ANI b)) - KLASICKÉ SOS

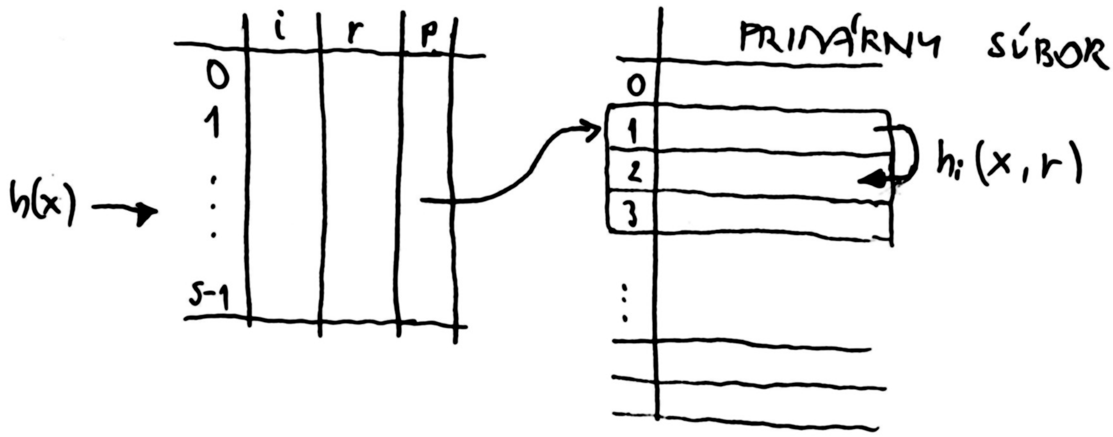
SEMIDYNAMICKÉ (SPĹŇAJÚ IBA a)) -

PERF. HASH. CORMACKA; LARSON & KALJI

DYNAMICKÉ (SPĹŇAJÚ a) AJ b)) -

ROZŠíRITEĽNÉ HASH. (FAGIN), LINEÁRNE HASH. (LITWIN)

CORMACK DANÉ s, $h(x)$, $h_i(x,r)$, FCIA. FREE(r)



LARSON & KALJI

M .. POČET STRÁNOK

M.d BITOV .. SEPARÁTORY STRÁNOK

$h_1(x), \dots, h_M(x)$ PREHĽADÁV. POSTUPNOSŤ

$s_1(x), \dots, s_M(x)$ POSTUPNOSŤ SIGNATÚR

M=5, d=3

FAGIN

$h(x) \to \{0, \dots, 2^{r+1}-1\}$

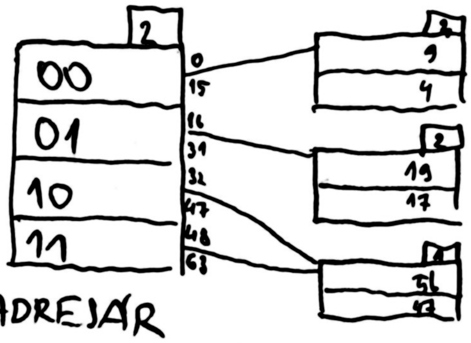
d .. HĹBKA ADRESÁRA

d' .. LOKÁLNE HĹBKY STRÁNOK

(BERÚ SA PRVÉ BITY!!)

$r+1=6$, $b=2$ BLOK. FAKTOR

$h(k) = k \bmod 64$



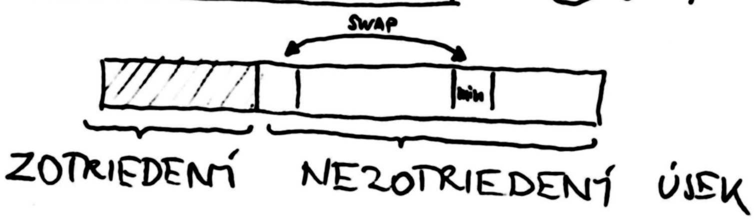
ADRESÁR

30.08.2008 Sa
PETER ČERNO

ŠTÁTNICE

3.6 SEKVENČNÉ TRIEDENIE, .., TRIEDIACE SIETE

SELECTION SORT $\Theta(n^2)$



1. NÁJDI NAJMENŠÍ PRVOK Z NEZOTRIEDENÉHO ÚSEKU
2. PRIDAJ NA KONIEC ZOTRIEDENÉHO ÚSEKU

INSERTION SORT $O(n^2)$ $\Theta(n + |I(\pi)|)$

EFEKTÍVNY NA ČIASTOČNE PREDTRIEDENÉ ÚDAJE
STABILNÝ : ZACHOVÁVA PORADIE PRVKOV S ROVNAKÝM KĽÚČOM
INPLACE : NEPOTREBUJE POMOCNÉ DAT. ŠTRUKTÚRY

```
for j ← 2 to length[A] do
   key ← A[j]
   i ← j-1
   while i > 0 & A[i] > key do
      A[i+1] ← A[i]; i ← i-1
   A[i+1] ← key
```

VARIANTA INSERTION SORTU : SHELL SORT

BUBBLE SORT $O(n^2)$

PRECHÁDZA POLE A PREHADZUJE $A[i] > A[i+1]$
SKONČÍ, AK NEDOŠLO K PREHODENIU
VARIANTA : SHAKE (COCKTAIL) SORT

HEAPSORT $\Theta(n \cdot \log n)$

INPLACE, NIE JE STABILNÝ
POUŽÍVA SA MAX-HEAP

MERGESORT $\Theta(n \log n)$

JE MOŽNÉ POUŽIŤ NA VONKAJŠIE TRIEDENIE

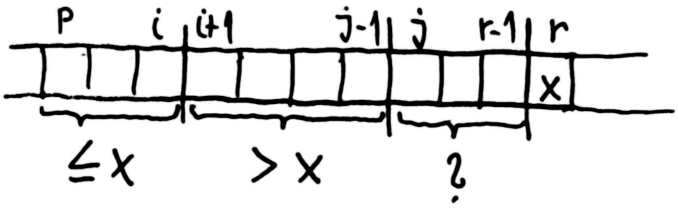
```
MERGE-SORT (A, p, r)
  if p < r then
      q ← ⌊(p+r)/2⌋
      MERGE-SORT(A, p, q)
      MERGE-SORT (A, q+1, r)
      MERGE (A, p, q, r)
```

QUICKSORT $O(n^2)$, V PRIEMERNOM PRÍPADE $\Theta(n \log n)$

```
QUICKSORT (A, p, r)
  if p < r then
      q ← PARTITION (A, p, r)
      QUICKSORT(A, p, q-1)
      QUICKSORT(A, q+1, r)
```

```
PARTITION (A, p, r)
  x ← A[r]
  i ← p-1
  for j ← p to r-1 do
    if A[j] ≤ x then
       i ← i+1
       swap A[i] ↔ A[j]
  swap A[i+1] ↔ A[r]
  return i+1
```

INVARIANT




```
RANDOMIZED-PARTITION (A, p, r)
  swap A[RANDOM (p, r)] ↔ A[r]
  return PARTITION (A, p, r)
```

30.08.2008 Sa
PETER ČERNO

ŠTÁTNICE

PRIEHRADKOVÉ TRIEDENIE

COUNTING SORT $\Theta(n+k)$

PREDPOKLADAJME, ŽE HODNOTY POĽA A SA NACHÁDZAJÚ V ROZSAHU $0, 1, \dots, k$

```
Counting-Sort (A, B, k)
  for i ← 0 to k do  C[i] ← 0
  for j ← 1 to length[A] do  C[A[j]] ++
  for i ← 1 to k do  C[i] ← C[i] + C[i-1]
  for j ← length[A] downto 1 do
      B[C[A[j]]] ← A[j]
      C[A[j]] --
```

JE STABLE !!

VARIANTA: BUCKET SORT: DO 1 PRIEHRADKY SA DÁVAJÚ KĽÚČE Z NEJAKÉHO ROZSAHU, INTERVALU

1. LEAST SIGNIFICANT DIGIT RADIX SORT

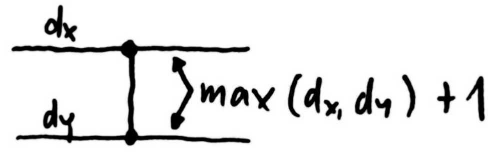
```
Radix-Sort (A, d)
  for i ← 1 to do
     STABLE SORT NA A PODĽA DIGIT i
```

VŠETKY PRVKY MAJÚ d DIGITS

2. MOST SIGNIFICANT DIGIT (ZALOŽENÁ NA BUCKET SORTE)
   1. ROZDEĽ DO PRIEHRADOK PODĽA NAJVÝZNAMN. DIGIT
   2. (REKURZÍVNE) ZOTRIEĎ PRIEHRADKY
   3. ZLEP PRIEHRADKY DOHROMADY

MOŽNO TRIEDIŤ PODĽA KĽÚČOV RÔZNEJ DĹŽKY
HODÍ SA NA LEXIKOGRAFICKÉ TRIEDENIE

TRIEDIACE SIETE (SORTING NETWORKS)



HĹBKA SPOJU

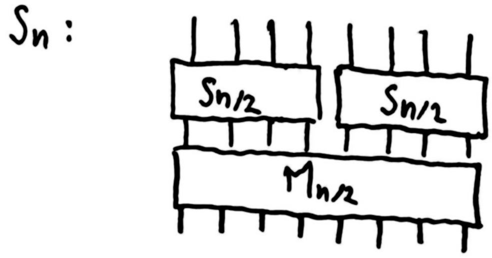
SORTING NETWORK JE COMPARISION NETWORK, KTORÁ UTRIEDI KAŽDÚ VSTUPNÚ SEKVENCIU
KAŽDÁ MÁ HĹBKU ASPOŇ $\log_2 n$

LEMMA: f NEKLESAJÚCA

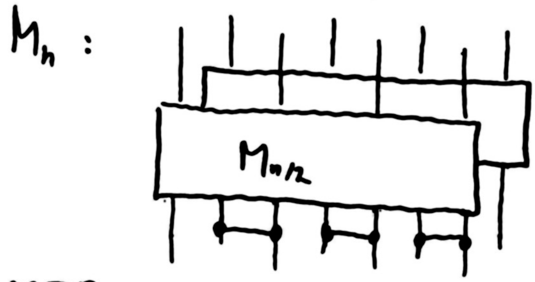
$\vec{a} \to$ COMPARISION NETWORK $\to \vec{b}$, POTOM $f(\vec{a}) \to$ COMPARISION NETWORK $\to f(\vec{b})$

ZERO-ONE PRINCIPLE: KEĎ COMPARISION NETWORK UTRIEDI $\forall \vec{a} \in \{0,1\}^n$, POTOM JE TO SORTING NETWORK.

$\underline{n = 2^k}$



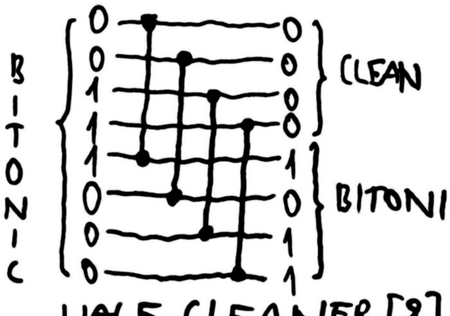
SORT. NETW.



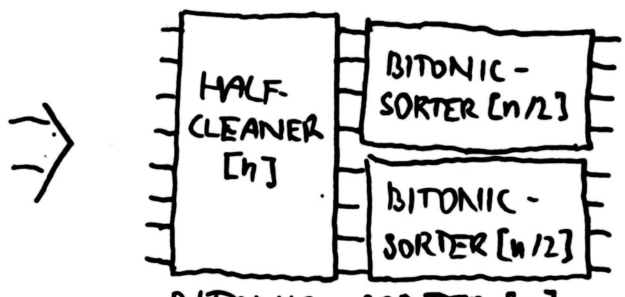
MERGE. NETW.

BITONICKÉ TRIEDENIE (BITONIC SORTING NETWORKS)

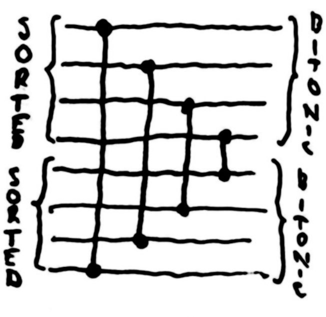
BITONICKÁ POST. - POSTUPNOSŤ, KTORÚ MOŽNO CYKLICKY SHIFTNÚŤ NA POST., KTORÁ ↗ A POTOM ↘
ZERO-ONE: $0^i 1^j 0^k$, $1^i 0^j 1^k$ $i,j,k \geq 0$



HALF-CLEANER [8]



BITONIC-SORTER [n]



30.08.2008 So
PETER ČERNO

ŠTÁTNICE

3.7 GRAFOVÉ ALGORITMY

BREADTH-FIRST SEARCH (PREHĽ. DO ŠÍRKY)

ORIENT. AJ NEORIENT. GRAFY

BFS (G, s) $O(m+n)$

foreach $u \in V_G \setminus \{s\}$ do
  color[u] ← WHITE, d[u] ← +∞, π[u] ← NIL
color[s] ← GRAY, d[s] ← 0, π[s] ← NIL
ENQUEUE(Q, s)
while Q ≠ ∅ do
  u ← DEQUEUE(Q)
  foreach $(u,v) \in E_G$ if color[v] = WHITE then
    color[v] ← GRAY, d[v] ← d[u]+1, π[v] ← u
    ENQUEUE(Q, v)
  color[u] ← BLACK

INVARIANT:
FRONTA POZOSTÁVA ZO ŠEDÝCH VR.

BFS OBJAVÍ KAŽDÝ VRCHOL DOSIAHNUTEĽNÝ Z s
$\forall v \quad d[v] = \delta(s,v)$, $s \rightsquigarrow \pi[v] \rightarrow v$ JE NAJKRATŠIA CESTA

$G_\pi = (V_\pi, E_\pi)$ JE BREADTH-FIRST TREE
$V_\pi = \{v \in V_G \mid \pi[v] \neq NIL\} \cup \{s\}$
$E_\pi = \{(\pi[v], v) \mid \pi[v] \neq NIL\}$

DEPTH-FIRST SEARCH (PREHĽ. DO HĹBKY)

ORIENT. AJ NEORIENT. GRAFY

UDRŽIAVANÉ 2 TIMESTAMPS :

$d[v]$ .. ČAS OBJAVENIA VRCHOLU v

$f[v]$ .. ČAS OPUSTENIA VRCHOLU v

DFS (G) $\Theta(m+n)$

foreach $u \in V_G$ do color[u] ← WHITE, π[u] ← NIL
time ← 0
foreach $u \in V_G$ do if color[u] = WHITE then
  DFS-VISIT (u)

DFS-VISIT (u)
 color[u] ← GRAY
 time++, d[u] ← time
(*) foreach $(u,v) \in E_G$ if color[v] = WHITE then
   π[v] ← u, DFS-VISIT (v)
 color[u] ← BLACK
 time++, f[u] ← time

$G_\pi = (V, E_\pi)$, $E_\pi = \{(\pi[v], v) \mid \pi[v] \neq NIL\}$

JE DEPTH-FIRST FOREST

KLASIFIKÁCIA HRÁN :

TREE EDGE (u,v) : $(u,v) \in E_\pi$, KEĎ V (*) JE color[v]=WHITE

BACK EDGE (u,v) : SPÁJA u S PREDKOM v V D-F TREE

KEĎ V (*) JE color[v] = GRAY

FORWARD EDGE (u,v) : u S POTOMKOM v

CROSS EDGE : VŠETKY OSTATNÉ

→ KEĎ V (*) JE color[v] = BLACK

30.08.2008 Sa
PETER ČERNO

ŠTÁTNICE

ARTIKULÁCIE A MOSTY

NECH $G=(V,E)$ JE SÚVISLÝ, NEORIENTOVANÝ GRAF
NECH $G_\pi=(V,E_\pi)$ JE DEPTH-FIRST TREE GRAFU G

KOREŇ G_π JE ARTIKULÁCIA V G $\Leftrightarrow$ MÁ ASPOŇ DVOCH NÁSLEDNÍKOV V G_π

NECH u NIE JE KOREŇ G_π. POTOM u JE ARTIKULÁCIA V G $\Leftrightarrow$ u MÁ NÁSLEDNÍKA v, ŽE NEEXISTUJE ŽIADNA BACK EDGE Z v ANI Z POTOMKA v DO PREDKA u

DEFINUJME $low[u] = \min \begin{cases} d[u] \\ d[w] : (v,w) \text{ JE BACK EDGE, } v \text{ JE POTOMOK } u \end{cases}$ $O(|E|)$

- u JE ARTIKULÁCIA V G $\Leftrightarrow$
  $\exists (u,v) \in E_G : d[u] < d[v]$ & $low[v] \geq d[u]$

(u,v) JE MOST $\Leftrightarrow$ $d[u] < d[v]$ & $low[v] > d[u]$

TOPOLOGICKÉ TRIEDENIE

TOPOLOGICAL-SORT(G) $\Theta(m+n)$
  DFS(G) NA SPOČÍTANIE $f[v]$ $\forall v \in V_G$
    PRI OPUSTENÍ VRCHOLU v VLOŽ v DO FRONTY L
  return L

G JE ACYKLICKÝ $\Leftrightarrow$ DFS NEDETEKUJE BACK EDGE

STRONGLY - CONNECTED - COMPONENTS (G) $\Theta(m+n)$

1. DFS (G) NA SPOČÍTANIE $f[u]$ $\forall u \in V_G$
2. DFS (G^T) AVŠAK V HLAVNOM CYKLE DFS
   BERIEME VRCHOLY PODĽA KLESAJÚCEHO $f[u]$ Z 1. KROKU
3. NA VÝSTUP IDÚ VRCHOLY KAŽDÉHO
   DEPTH - FIRST TREE SPOČÍTANÉHO V 2. KROKU

HĽADANIE NAJKRATŠEJ CESTY < SINGLE SOURCE s / ALL PAIRS

DANÝ ORIENTOVANÝ GRAF $G=(V,E)$ A OHODN. HRÁN $w: E \to \mathbb{R}$

```
INITIALIZE-SINGLE-SOURCE (G, s)
  foreach v ∈ V_G do  d[v] ← ∞,  π[v] ← NIL
  d[s] ← 0

RELAX (u, v, w)
  if d[v] > d[u] + w(u,v) then
     d[v] ← d[u] + w(u,v),  π[v] ← u
```

BELLMAN - FORD $\Theta(n \cdot m)$

```
BELLMAN-FORD (G, w, s)
  INITIALIZE-SINGLE-SOURCE (G, s)
  for i ← 1 to |V_G|-1 do
     foreach (u,v) ∈ E_G do RELAX(u, v, w)
  foreach (u,v) ∈ E_G do
     if d[v] > d[u] + w(u,v) then return FALSE
  return TRUE
```

ZÁPORNÝ CYKLUS

30.08.2008 Sa
PETER ČERNO

ŠTÁTNICE

NAJKRATŠIA CESTA V DAG

DAG-SHORTEST-PATH (G, w, s) $\Theta(m+n)$
  $L \leftarrow$ TOPOLOGICAL-SORT (G)
  INITIALIZE-SINGLE-SOURCE (G, s)
  foreach $u \in L$ foreach $(u,v) \in E_G$ do
    RELAX (u, v, w)

POUŽITIE: PERT CHART ANALYSIS
CRITICAL PATH = NAJDLHŠIA CESTA V DAG

DIJKSTRA

PREDPOKLAD: $\forall (u,v) \in E_G : w(u,v) \geq 0$!!

DIJKSTRA (G, w, s) $\Theta((m+n)\log n)$
  INITIALIZE-SINGLE-SOURCE (G, s)
  $S \leftarrow \emptyset$ MN. VRCHOLOV S DEFINITÍVNE URČENOU $d[u]$
  $Q \leftarrow V_G$ KĽÚČ JE $d[u]$, MIN-HEAP
  while $Q \neq \emptyset$ do → INVARIANT: $Q = V_G \setminus S$
    $u \leftarrow$ EXTRACT-MIN (Q)
    $S \leftarrow S \cup \{u\}$
    foreach $(u,v) \in E_G$ do RELAX(u, v, w)

POZOR! TREBA UPRAVIŤ HALDU Q $\Theta(\log n)$

FLOYD - WARSHALL

FLOYD-WARSHALL (W)
$D^{(0)} \leftarrow W$, $\Pi^{(0)} \leftarrow \begin{cases} \pi_{ij}^{(0)} = NIL \iff i=j \vee w_{ij} = +\infty \\ \pi_{ij}^{(0)} = i \iff i \neq j \;\&\; w_{ij} < +\infty \end{cases}$
for $k \leftarrow 1$ to n do
  for $i \leftarrow 1$ to n do
    for $j \leftarrow 1$ to n do
      $d_{ij}^{(k)} \leftarrow \min\left(\underset{\Downarrow\; \pi_{ij}^{(k-1)}}{d_{ij}^{(k-1)}},\; \underset{\Downarrow\; \pi_{kj}^{(k-1)}}{d_{ik}^{(k-1)} + d_{kj}^{(k-1)}} \right)$
      $\pi_{ij}^{(k)} \leftarrow$
return $D^{(n)}$, $\Pi^{(n)}$

TRANZITÍVNY UZÁVER

TRANSITIVE-CLOSURE (G)
$T^{(0)} \leftarrow A + I$ A JE MATICA SUSEDNOSTI GRAFU G
for $k \leftarrow 1$ to n do
  for $i \leftarrow 1$ to n do
    for $j \leftarrow 1$ to n do
      $t_{ij}^{(k)} \leftarrow t_{ij}^{(k-1)} \vee \left(t_{ik}^{(k-1)} \;\&\; t_{kj}^{(k-1)} \right)$
return $T^{(n)}$

30.08.2008 So
PETER ČERNO

ŠTÁTNICE

DISJOINT-SET FORESTS

POUŽÍVANÉ 2 HEURISTIKY: UNION-BY-RANK, PATH-COMPRESSION

MAKE-SET(x)
  $\pi[x] \leftarrow x$, $d[x] \leftarrow 1$

FIND-SET(x)
  if $x \neq \pi[x]$ then $\pi[x] \leftarrow$ FIND-SET($\pi[x]$)
  return $\pi[x]$

UNION(x, y)
  LINK(FIND-SET(x), FIND-SET(y))

LINK(x, y)
  if $d[x] \leq d[y]$ then $\pi[x] \leftarrow y$, $d[y] \leftarrow d[y] + d[x]$
  else $\pi[y] \leftarrow x$, $d[x] \leftarrow d[x] + d[y]$

MINIMÁLNA KOSTRA (MINIMUM SPANNING TREE)

$G = (V, E)$ JE SÚVISLÝ NEORIENT. GRAF, $w: E \to \mathbb{R}$ OHODN. HRÁN

GENERIC-MST(G, w)
  $A \leftarrow \emptyset$
  while A NETVORÍ KOSTRU do
    NECH (u,v) JE BEZPEČNÁ PRE A.
    $A \leftarrow A \cup \{(u,v)\}$
  return A

VETA: NECH $A \subseteq E_G$, A JE ČASŤOU NEJAKEJ MINIMÁLNEJ KOSTRY. NECH $(S, V_G \setminus S)$ JE AKÝKOĽVEK REZ REŠPEKTUJÚCI A. KEĎ (u,v) JE ĽAHKÁ HRANA KRÍŽIACA S, POTOM (u,v) JE BEZPEČNÁ PRE A.

KRUSKALOV (BORŮVKŮV) ALGORITMUS

MST-KRUSKAL (G, w) $\qquad \Theta(m.\log n)$

$A \leftarrow \emptyset$

foreach $v \in V_G$ do MAKE-SET(v)

SORT(E_G) PODĽA w

foreach $(u,v) \in E_G$ do

  if FIND-SET$(u) \neq$ FIND-SET(v) then

    $A \leftarrow A \cup \{(u,v)\}$

    UNION(u,v)

return A

PRIMOV (JARNÍKŮV) ALGORITMUS

MST-PRIM (G, w, r) $\qquad \Theta(m \log n)$

foreach $u \in V_G$ do key$[u] \leftarrow \infty$, $\pi[u] \leftarrow$ NIL

key$[r] \leftarrow 0$

$Q \leftarrow V_G$ KĽÚČ JE key$[u]$, MIN-HEAP

while $Q \neq \emptyset$ do

  $u \leftarrow$ EXTRACT-MIN(Q)

  foreach $(u,v) \in E_G$ do

    if $v \in Q$ & $w(u,v) <$ key$[v]$ then

      $\pi[v] \leftarrow u$, key$[v] \leftarrow w(u,v)$

INVARIANT: 1. $A = \{(v, \pi[v]) \mid v \in V_G \setminus \{r\} \setminus Q\}$

2. VRCHOLY UMIESTNENÉ DO MIN. KOSTRY SÚ VO $V_G \setminus Q$

3. $\forall v \in Q : \pi[v] \neq$ NIL $\Rightarrow$ key$[v] < \infty$

A key$[v]$ JE VÁHA NEJAKEJ ĽAHKEJ HRANY $(v, \pi[v])$ SPÁJAJÚCEJ v S NEJAKÝM VRCHOLOM UŽ UMIESTNENÝM V MINIMÁLNEJ KOSTRE

30.08.2008 So
PETER ČERNO

ŠTÁTNICE

TOKY V SIEŤACH

SIEŤ (FLOW NETWORK) $G=(V,E)$ JE ORIENTOVANÝ GRAF, KU KAŽDEJ $(u,v)\in E_G$ JE PRIRADENÁ KAPACITA $c(u,v)\geq 0$, PRE $(u,v)\notin E_G$ KLADIEME $c(u,v)=0$

ROZLIŠUJEME 2 VRCHOLY: ZDROJ (SOURCE) s, STOK (SINK) t

PREDPOKLADÁME, ŽE PRE $\forall v\in V_G$ v LEŽÍ NA NEJAKEJ $s \rightsquigarrow v \rightsquigarrow t$.

TOK (FLOW) V G JE $f: V_G\times V_G \to \mathbb{R}$ TAKÁ, ŽE:

CAPACITY CONSTRAINT: $\forall u,v\in V_G: f(u,v)\leq c(u,v)$

SKEW SYMETRY: $\forall u,v\in V_G: f(u,v)=-f(v,u)$

FLOW CONSERVATION: $\forall u\in V_G\setminus\{s,t\}: \sum_{v\in V_G} f(u,v)=0$

VEĽKOSŤ TOKU $|f| := f(s,V_G)$

PLATÍ $|f| = f(s,V) = f(V,V) - f(V-s,V) = -f(V-s,V) =$
$= f(V,V-s) = f(V,t) + f(V,V-s-t) = f(V,t)$

REZERVNÁ KAPACITA (RESIDUAL CAPACITY)
$c_f(u,v) = c(u,v) - f(u,v)$

SIEŤ REZERV $G_f=(V_G,E_f)$, KDE
$E_f = \{(u,v)\in V_G\times V_G \mid c_f(u,v)>0\}$

$(u,v)\in E_f$ SA NAZÝVA REZERVNÁ HRANA

CESTA $p: s\rightsquigarrow t$ V G_f SA NAZÝVA ZLEPŠUJÚCA (AUGUMENTING PATH)

$c_f(p) := \min\{c_f(u,v) \mid (u,v)\in p\}$ REZERVNÁ KAPACITA p

VETA: KEĎ f JE TOK V G, f' TOK V G_f, POTOM $f+f'$ JE TOK V G, $|f+f'| = |f| + |f'|$.

REZ (CUT) (S,T) JE PARTÍCIA V_G NA S A $T = V_G - S$, PRIČOM $s \in S$ A $t \in T$.

KAPACITA REZU $= c(S,T)$

ZREJME PRE KAŽDÝ TOK f PLATÍ $|f| = f(S,T) \leq c(S,T)$

MAX-FLOW MIN-CUT THEOREM

NASLEDUJÚCE TVRDENIA SÚ EKVIVALENTNÉ:

(1) f JE MAXIMÁLNY TOK V G

(2) G_f NEOBSAHUJE ŽIADNU ZLEPŠUJÚCU CESTU

(3) $|f| = c(S,T)$ PRE NEJAKÝ REZ (S,T)

FORD-FULKERSON (G, s, t)

foreach $(u,v) \in E_G$ do $f[u,v] \leftarrow f[v,u] \leftarrow 0$

(*) while $\exists p : s \rightsquigarrow t$ v G_f do

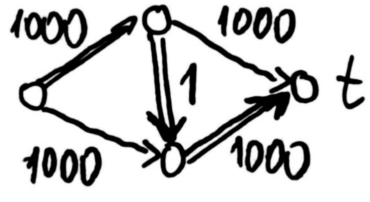
  $c_f(p) \leftarrow \min \{ c_f(u,v), (u,v) \in p \}$

  foreach $(u,v) \in p$ do

    $f[u,v] \leftarrow f[u,v] + c_f(p)$

    $f[v,u] \leftarrow -f[u,v]$

ZLÁ ČASOVÁ ZLOŽITOSŤ :



EDMONDS-KARP

CESTU p V (*) HĽADÁME POMOCOU BFS

$\Rightarrow$ ČASOVÁ ZLOŽITOSŤ $\underline{\underline{O(n \cdot m^2)}}$

30.08.2008 Su
PETER ČERNO

ŠTÁTNICE

DINIC

ALGORITMUS POSTUPUJE PO FÁZACH:

(1) V SIETI REZERV G_f UVAŽUJEME IBA HRANY, KTORÉ LEŽIA NA NEJAKEJ NAJKRATŠEJ CESTE $s \rightsquigarrow t$. (2x BFS)

(2) VEZMEME JEDNU Z NAJKRATŠÍCH ZLEPŠUJÚCICH CIEST A ZLEPŠÍME PODĽA NEJ TOK: $O(n)$
(VYUŽÍVAME TU TZV. current arc DATOVÚ ŠTRUKTÚRU)

(3) VYHODÍM SLEPÉ CESTY V SIETI REZERV
AMORTIZOVANÁ ZLOŽITOSŤ ZA CELÚ FÁZU: $O(m)$

(4) BODY (2),(3) OPAKUJEM, KÝM JE TO MOŽNÉ, NAJVIAC $O(m)$ KRÁT

ĎALŠIA FÁZA, VZRASTIE DISTANCE LABEL $d(s)$

KEĎŽE FÁZ JE NAJVIAC n A KAŽDÁ MÁ ZLOŽITOSŤ $O(n \cdot m)$
JE CELKOVÁ ZLOŽITOSŤ DINICOVHO ALGORITMU
$\underline{\underline{O(n^2 m)}}$

PUSH-RELABEL ALGORITMY

(PREFLOW)
VLNA $f: V_G \times V_G \to \mathbb{R}$ ZACHOVÁVA
CAPACITY CONSTRAINTS A SKEW SYMMETRY, AVŠAK
$f(V_G, u) \geq 0 \quad \forall u \in V_G - \{s\}$

$e(u) := f(V_G, u)$ SA NAZÝVA PREBYTOK (EXCESS)

HOVORÍME, ŽE $u \in V_G - \{s, t\}$ PRETEKÁ (OVERFLOWING)
$\iff e(u) > 0$

s, t NIE SÚ NIKDY PRETEKAJÚCE VRCHOLY

(HEIGHT FC.)
FUNKCIA $h: V_G \to \mathbb{N}_0$ SA NAZÝVA VÝŠKOVÁ FUNKCIA
$\iff h(s) = |V_G|,\ h(t) = 0,\ \underline{h(u) \leq h(v) + 1}\ \forall (u,v) \in E_f$

TJ. $h(u) > h(v) + 1 \Rightarrow (u,v) \notin E_f$.

PUSH (u,v)

IBA AK u PRETEKÁ, $c_f(u,v) > 0$, $h[u] = h[v] + 1$
$d_f(u,v) \leftarrow \min(e[u], c_f(u,v))$
$f[u,v] \leftarrow f[u,v] + d_f(u,v)$, $f[v,u] \leftarrow -f[u,v]$
$e[u] \leftarrow e[u] - d_f(u,v)$, $e[v] \leftarrow e[v] + d_f(u,v)$

RELABEL (u)

IBA AK u PRETEKÁ A PRE $\forall (u,v) \in E_f : h[u] \leq h[v]$
$h[u] \leftarrow 1 + \min\{h[v] \mid (u,v) \in E_f\}$

GENERIC-PUSH-RELABEL (G) $\quad O(n^2 \cdot m)$
INITIALIZE-PREFLOW (G, s)
while $\exists$ APLIKOVATEĽNÝ PUSH ALEBO RELABEL
VYKONAJ TÚTO OPERÁCIU

31.08.2008 Su
PETER ČERNO

ŠTÁTNICE

3.9 VYHĽADÁVANIE VZORKOV V TEXTE

AHO - CORASICK

Σ ABECEDA, TEXT $x = \sigma_1 \dots \sigma_n \in \Sigma^*$, $K = \{y_1, \dots, y_k\} \subseteq \Sigma^*$
$y_i = \tau_{i,1} \dots \tau_{i,\ell(i)}$, $\ell = \sum_{i=1}^{k} \ell(i)$
CHCEME NÁJSŤ $\forall$ (i, j) : $y_j \sqsupset \sigma_1 \dots \sigma_i$

```
AHO-CORASICK-MATCHER (f, g, out)        O(n)
  state ← 0                   f → DOPREDNÁ FUNKCIA
  for i ← 1 to n do           g → SPÄTNÁ FUNKCIA
!!   while g(state, σi) = ⊥ do state ← f(state)   !!
     state ← g(state, σi)
     foreach j ∈ out(state) do
        REPORT (i, j)
```

(1) KAŽDÝ STAV JEDNOZNAČNE KOREŠPONDUJE S PREDPONOU NEJAKÉHO SLOVA V K
(2) NECH state KOREŠPONDUJE S PREDPONOU w.
a) POTOM f(state) KOREŠP. S NAJVÄČŠOU VLASTNOU PRÍPONOU w, KTORÁ ZODPOVEDÁ NEJAKÉMU STAVU (VIĎ (1))
b) $j \in out(state) \Leftrightarrow y_j \sqsupset w$

INVARIANT: PO PREČÍTANÍ ZNAKU σ_i SA ALG. NACHÁDZA V STAVE state S KOREŠP. PREDPONOU w, ŽE w JE NAJVÄČŠIA PRÍPONA $\sigma_1 \dots \sigma_i$, KTORÁ EŠTE KOREŠPONDUJE S NEJAKÝM STAVOM

NA ZAČIATKU PREDP. ŽE PRE $\forall i . \forall \sigma : g(i,\sigma) = \perp$

AHO - CORASICK - FORWARD

for $i \leftarrow 1$ to k do INSERT(y_i)

$\boxed{\begin{array}{l}\text{foreach } \sigma \in \Sigma \text{ do} \\ \quad \text{if } g(0,\sigma) = \perp \text{ then } g(0,\sigma) \leftarrow 0\end{array}}$!

INSERT ($\tau_1 \ldots \tau_j$)

state $\leftarrow 0$

for $i \leftarrow 1$ to j do

if $g(state, \tau_i) = \perp$ then

count ++

$g(state, \tau_i) \leftarrow$ count

state $\leftarrow g(state, \tau_i)$

AHO - CORASICK - BACKWARD $O(\ell)$

$f(0) \leftarrow 0$

$Q \leftarrow \emptyset$

foreach $\sigma \in \Sigma$ do

if $r \leftarrow g(0,\sigma) \neq 0$ then

$f(r) \leftarrow 0$, Q.ENQUEUE(r)

while $Q \neq \emptyset$ do → INVARIANT : V Q SA NACHÁDZAJÚ IBA STAVY S DEF. f A out

s $\leftarrow$ Q.DEQUEUE

foreach $\sigma \in \Sigma$ do if $r \leftarrow g(s,\sigma) \neq \perp$ then

$s' \leftarrow f(s)$

!! $\boxed{\text{while } g(s',\sigma) = \perp \text{ do } s' \leftarrow f(s')}$!!

$f(r) \leftarrow g(s',\sigma)$

out(r) $\leftarrow$ o(r) $\cup$ out($f(r)$)

Q.ENQUEUE(r)

31.08.2008 Su
PETER ČERNO

ŠTÁTNICE

KNUTH - MORISS - PRATT

HĽADÁME VZOR $P[1..m]$ V TEXTE $T[1..n]$

PREFIXOVÁ FUNKCIA $\boxed{\pi[i] = \max\{k < i \mid P_k \sqsupset P_i\}}$

KMP - MATCHER $O(n)$

$\xrightarrow{\lambda} (0) \xrightarrow{P[1]} (1) \xrightarrow{P[2]} (2) \xrightarrow{P[3]} \cdots \xrightarrow{P[m]} (m) \nearrow$

```
    state ← 0
    for i ← 1 to n do
!!     while state > 0 & P[state+1] ≠ T[i] do        !!
          state ← π[state]
       if P[state+1] = T[i] then state ← state+1
       if state = m then
          REPORT i
          state ← π[state]
```

KMP - PREFIX $O(m)$

INVARIANT : $k = \pi[i-1]$

```
    π[1] ← 0
    k ← 0
    for i ← 2 to m do
!!     while k>0 & P[k+1] ≠ P[i] do k ← π[k]        !!
       if P[k+1] = P[i] then k ← k+1
       π[i] ← k
```

RABIN - KARP

$O((n-m+1) \cdot m)$

```
base ← |Σ|
patt ← text ← 0
for i ← 1 to m do
    patt ← base * patt + P[i]
    text ← base * text + T[i]
tmp ← base^(m-1)
i ← 0
while i < n-m do
   if text = patt then
      if T[i+1 ... i+m] = P[1..m] then
         REPORT i+m
   i ← i+1
   if i < n-m then
      text ← base * (text - tmp * T[i]) + T[i+m]
```

31.08.2008 Su
PETER ČERNO

ŠTÁTNICE

3.10 ALGEBRAICKÉ ALGORITMY

PRINCIPIÁLNY n-TÝ KOREŇ JEDNOTKY $\omega_n = e^{2\pi i/n}$

$\{\omega_n^0, \dots, \omega_n^{n-1}\}\ (\cdot, ^{-1}, 1) \cong \mathbb{Z}_n(+, -, 0)$

CANCELLATION LEMMA: $\omega_{dn}^{dk} = \omega_n^k$

$2 \mid n \Rightarrow \omega_n^{n/2} = \omega_2 = -1, \quad \omega_n^k = -\omega_n^{k+n/2},$

$\{(\omega_n^0)^2, \dots, (\omega_n^{n-1})^2\} = \{\omega_{n/2}^0, \dots, \omega_{n/2}^{n/2-1}\}$

$n \nmid k \Rightarrow \sum_{j=0}^{n-1} (\omega_n^k)^j = \dfrac{(\omega_n^k)^n - 1}{\omega_n^k - 1} = 0$

$n \mid k \Rightarrow \sum_{j=0}^{n-1} (\omega_n^k)^j = n$

PREDPOKLADAJME, ŽE $\underline{n = 2^k,\ k \in \mathbb{N}_0}$

DISKRÉTNA FOURIEROVÁ TRANSFORMÁCIA

$\vec{a} = (a_0, \dots, a_{n-1})^T \overset{DFT_n}{\rightsquigarrow} \vec{y} = (y_0, \dots, y_{n-1})^T$

$y_k = \sum_{j=0}^{n-1} a_j (\omega_n^k)^j = A(\omega_n^k)$, KDE $A = \sum_{j=0}^{n-1} a_j x^j$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & (\omega_n^1)^1 & \dots & (\omega_n^1)^{n-1} \\ \dots \\ 1 & (\omega_n^{n-1})^1 & \dots & (\omega_n^{n-1})^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \qquad W_{ij} = \omega_n^{ij}, \quad i,j \in \{0, \dots, n-1\}$$

INVERZNÁ DFT

$(W^{-1})_{ij} = \frac{1}{n} \cdot \omega^{-ij}$

$$(W \cdot W^{-1})_{ij} = \frac{1}{n} \sum_{k=0}^{n-1} \omega_n^{ik} \cdot \omega_n^{-kj} = \frac{1}{n} \sum_{k=0}^{n-1} \omega^{(i-j)k} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

FAST FOURIER TRANSFORM (FFT)

NECH $n = 2^k$, $k \in \mathbb{N}_0$, $a_0, \dots, a_{n-1} \in \mathbb{R}$

$A(x) = \sum_{j=0}^{n-1} a_j x^j$

OZNAČME $A^{[0]}(x) = a_0 + a_2 x + \dots + a_{n-2} x^{n/2 - 1}$

$A^{[1]}(x) = a_1 + a_3 x + \dots + a_{n-1} x^{n/2 - 1}$

POTOM PLATÍ $A(x) = A^{[0]}(x^2) + x \cdot A^{[1]}(x^2)$

$\Rightarrow \quad A(\omega_n^k) = A^{[0]}(\omega_{n/2}^k) + \omega_n^k \cdot A^{[1]}(\omega_{n/2}^k)$

AK UVAŽUJEME $k \in \{0, \dots, \frac{n}{2} - 1\}$

POTOM $A(\omega_n^{k+\frac{n}{2}}) = A^{[0]}(\omega_{n/2}^k) - \omega_n^k \cdot A^{[1]}(\omega_{n/2}^k)$

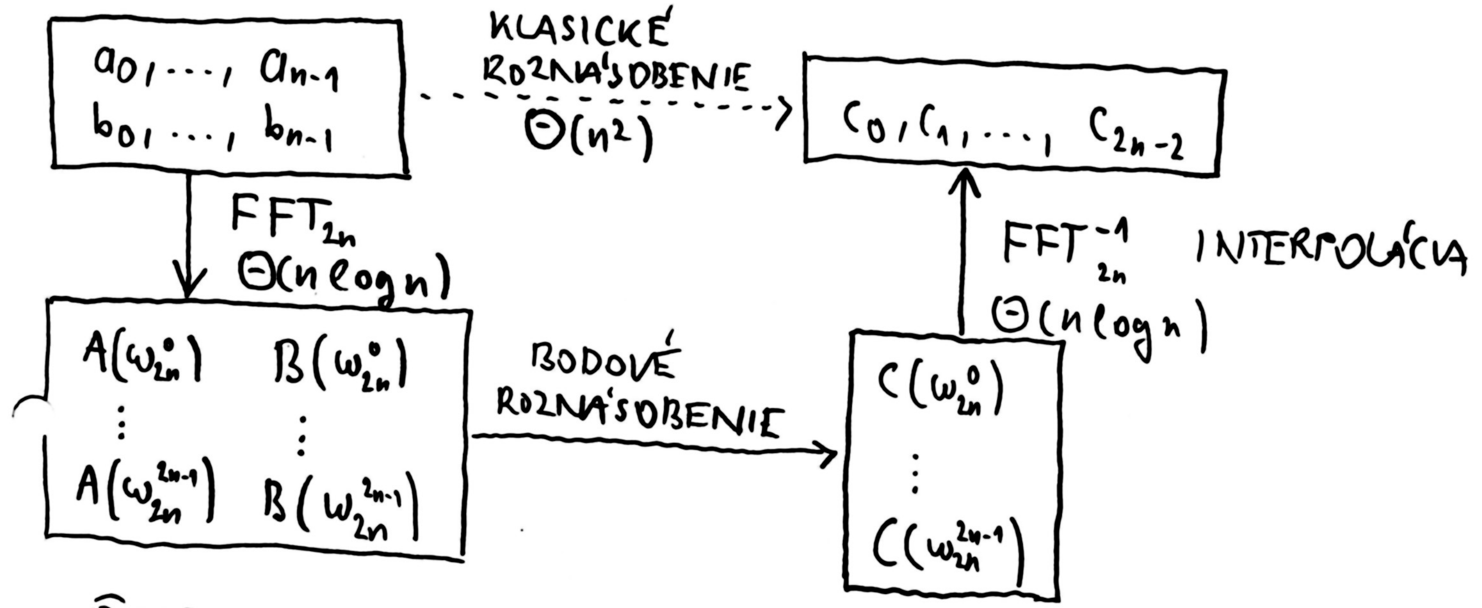
RECURSIVE - FFT(a) $\quad \Theta(n \cdot \log n)$

```
n ← length[a]
if n = 1 then RETURN a
ω_n ← e^{2πi/n} , ω ← 1
a^[0] ← (a_0, a_2, ..., a_{n-2})
a^[1] ← (a_1, a_3, ..., a_{n-1})
y^[0] ← RECURSIVE-FFT(a^[0])
y^[1] ← RECURSIVE-FFT(a^[1])
for k ← 0 to n/2 - 1 do
    y_k ← y_k^[0] + ω · y_k^[1]
    y_{k+n/2} ← y_k^[0] - ω · y_k^[1]
    ω ← ω · ω_n
RETURN y
```

31.08.2008 Su
PETER ČERNÝ

ŠTÁTNICE

APLIKÁCIA: EFEKTÍVNE NÁSOBENIE POLYNÓMOV



ĎALŠIE POUŽITIE:
- SPEKTRÁLNA ANALÝZA (NYQUIST-SHANNON SAMPLING THM.)
- DATOVÁ KOMPRESIA (DISKR. KOSÍNOVÁ TRANSFORMÁCIA)
- NÁSOBENIE VEĽKÝCH INTEGEROV
- JPEG, MPEG

EUKLIDOV ALGORITMUS $O(\log(\min\{a,b\}))$

```
EUCLID (a, b)
   if b = 0 then RETURN a
   else RETURN EUCLID(b, a mod b)

EXTENDED-EUCLID (a, b)
   if b = 0 then RETURN (a, 1, 0)
   (d, x, y) ← EXTENDED-EUCLID (b, a mod b)
   RETURN (d, y, x - ⌊a/b⌋y)
```

$\gcd(a,b) = xa + yb$

3.11 ZÁKLADY KRYPTOGRAFIE, RSA, DES

PRENÁŠAME REŤAZEC BITOV, T.J. ČÍSLO $\in \{0, \dots, M\}$
ŠIFRA = $e: \{0, \dots, M\} \to \{0, \dots, N\}$
KĽÚČ = $d: \{0, \dots, N\} \to \{0, \dots, M\}$
PRIČOM $d \circ e = id$, T.J. e JE PROSTÁ

KOMUTUJÚCE ŠIFRY $e_A \circ e_B = e_B \circ e_A$ $(e_A, e_B \in S_M)$

<u>KRYPTOGRAFIA S VEREJNÝM KĽÚČOM</u> (ASYMETRICKÁ ŠIFRA)
KAŽDÝ ÚČASTNÍK MÁ PUBLIC P_X A SECRET S_X KĽÚČ
$P_X, S_X \in S_D$, $P_X \circ S_X = S_X \circ P_X = id_D$
(1) S_X VLASTNÍ IBA X, (P_X VLASTNÍ KAŽDÝ)
(2) S_X NEMOŽNO EFEKTÍVNE VYČÍSLIŤ NA ZÁKLADE P_X

PLAINTEXT = SPRÁVA
CIPHERTEXT = ZAŠIFROVANÁ SPRÁVA

<u>DIGITÁLNY PODPIS</u>:
A POŠLE DVOJICU $(M, S_A(M)) \to B$ (ŠIFROVANIE)
B DOSTANE (M, M') A OVERÍ, ČI $M = P_A(M')$

<u>HYBRIDNÉ ŠIFROVANIE</u>

ASYMETRICKÉ ŠIFROVANIE JE POMALÉ
SYMETRICKÁ ŠIFRA POUŽÍVA TEN ISTÝ KĽÚČ K

A POŠLE DVOJICU $(K(M), P_B(K)) \to B$

<u>HYBRIDNÁ AUTENTIZÁCIA (DIG. PODPIS)</u>
PRE DLHÚ SPRÁVU JE NÁROČNÉ SPOČÍTAŤ $S_A(M)$
POUŽÍVA SA HASHOVACIA FCIA. (MD5, SHA1, ...)
JE ŤAŽKÉ NÁJSŤ $M_1 \neq M_2$ TAK, ABY $h(M_1) = h(M_2)$

31.08.2008 Su
PETER ČERNO

ŠTÁTNICE

CERTIFIKAČNÁ AUTORITA

(1) EXISTUJE CERTIFIKAČNÁ AUTORITA Z
(2) ALICA (A) ZÍSKA OD Z BEZPEČNOU CESTOU PODPÍSANÝ CERTIFIKÁT $(C, S_Z(C))$
$C =$ "ALICIN KĽÚČ JE P_A"
(3) TÚTO DVOJICU PRIPOJÍ ALICA KU KAŽDEJ SPRÁVE

RSA (RIVEST, SHAMIR, ADELMAN)

(1) ZVOĽME DVE VEĽKÉ PRVOČÍSLA p, q
(2) POLOŽME $n = p \cdot q$, $r = \varphi(n) = (p-1) \cdot (q-1)$
(3) ZVOĽME NEPÁRNE e NESÚDELITEĽNÉ S r A NÁJDIME d TAKÉ, ŽE $e \cdot d \equiv 1 \pmod r$
(4) $\underline{\underline{(e, n)}}$ JE PUBLIC KEY, $\underline{\underline{(d, n)}}$ JE SECRET KEY

PRE $M \in \{0, \dots, n-1\}$

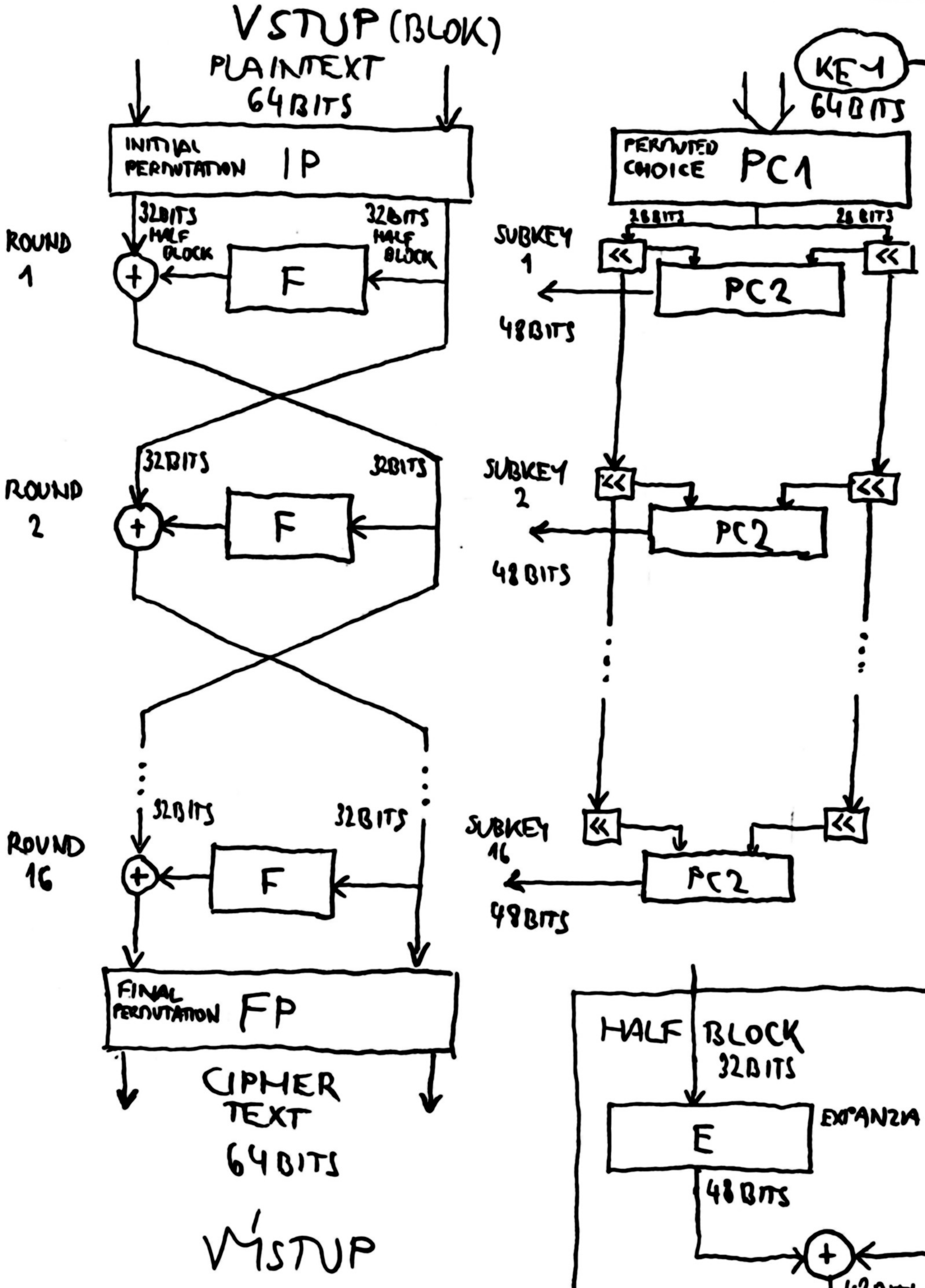
$$P(M) := M^e \pmod n,$$
$$S(M) := M^d \pmod n$$

PRE $\forall M \in \{0, \dots, n-1\}$

$$P(S(M)) = S(P(M)) = M^{ed} \pmod n$$
$$\equiv M^{ed \bmod \varphi(n)} \pmod n$$
$$= M.$$

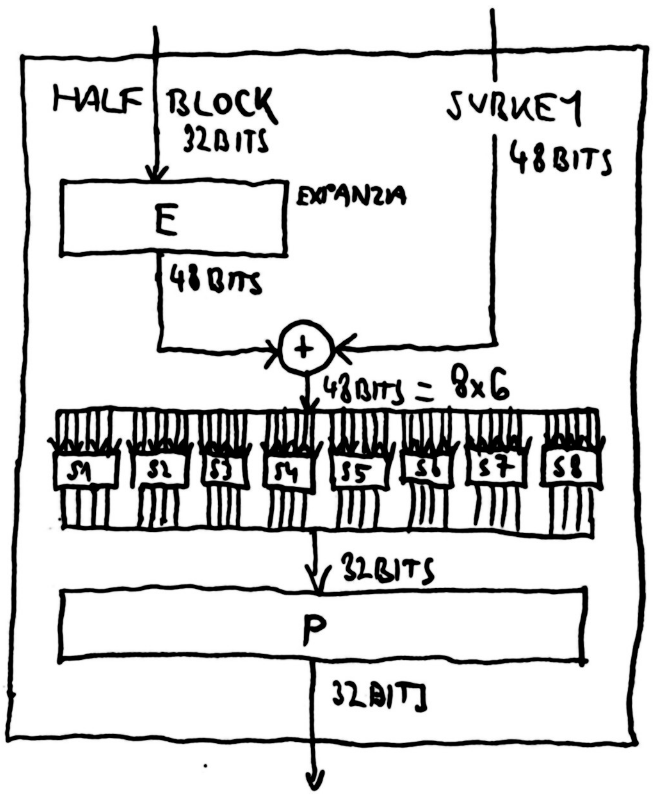
DES (DATA ENCRYPTION STANDARD)

BLOKOVÁ ŠIFRA, SYMETRICKÝ KĽÚČ



STRANY SI HO MUSIA VYMENIŤ PO BEZPEČNOM KANÁLE

PRE DEŠIFROVANIE SA SUBKĽÚČE MUSIA GENEROVAŤ V OPAČNOM PORADÍ (NAMIESTO DOĽAVA SA POSÚVA DOPRAVA)



F

MIEŠANIE S KĽÚČOM

31.08.2008 Su
PETER ČERNO

ŠTÁTNICE

3.12 PRAVDEPODOBNOSTNÉ ALGORITMY

RANDOMIZOVANÉ ALGORITMY SÚ ODOLNEJŠIE PROTI MOŽNOSTI ZÁMERNE ZLÝCH VSTUPOV

PRAVDEPODOBNOSTNÉ ALGORITMY - OBČAS DAJÚ NESPRÁVNY VÝSLEDOK ⇒ SÚ VHODNEJŠIE, AK VÝSLEDOK JE ÁNO / NIE

(*) VETA (FERMAT): AK p JE PRVOČÍSLO, POTOM $a^{p-1} \equiv 1 \pmod p$ PRE $\forall a \in \mathbb{Z}_p^*$

VETA (NIVEN & ZUCKERMAN): $n>1$ $\mathbb{Z}_n^*(\cdot, ^{-1}, 1)$ JE CYKLICKÁ PRÁVE PRE $n=2, 4, p^e, 2p^e$ KDE $p>2$ JE PRVOČÍSLO A $e \in \mathbb{N}$

AK g JE PRIMITÍVNY KOREŇ $\mathbb{Z}_n^*$, $a \in \mathbb{Z}_n^*$, POTOM $\exists!\, z \in \{0, \dots, \phi(n)-1\} : g^z \equiv a \pmod n$

z JE DISKRÉTNY LOGARITMUS a MODULO n, $z = ind_{n,g}(a)$

PLATÍ $g^x \equiv g^y \pmod n \Leftrightarrow x \equiv y \pmod{\varphi(n)}$

(**) VETA: AK $p>2$ JE PRVOČÍSLO, $e \geq 1$, POTOM $x^2 \equiv 1 \pmod{p^e}$ MÁ PRÁVE DVE RIEŠENIA : $x=1$, $x=-1$

DÔKAZ. $(g^{ind_{n,g}(x)})^2 \equiv g^{ind_{n,g}(1)} \pmod n$

$\Leftrightarrow 2 \cdot ind_{n,g}(x) \equiv ind_{n,g}(1) \equiv 0 \pmod{\phi(n)}$

$\phi(n) = (p-1)p^{e-1}$

HNEĎ VIDÍME, ŽE EXISTUJÚ PRÁVE 2 RIEŠENIA : $x=1$, $x=-1$

DÔSLEDOK: AK $x^2 \equiv 1 \pmod n$ PRE $1 < x < n-1$ ⇒ n JE ZLOŽENÉ.

MILLER-RABIN RANDOMIZOVANÝ PRIMALITY TEST

```
WITNESS (a, n)
   NECH n-1 = 2^t u, t≥1, 2∤u
   x_0 ← a^u (mod n)
   for i ← 1 to t do
       x_i ← x_{i-1}^2
(**)       if x_i = 1 & x_{i-1} ≠ 1 & x_{i-1} ≠ n-1 then RETURN TRUE
(*)  if x_t ≠ 1 then RETURN TRUE
   RETURN FALSE
```

AK WITNESS (a, n) VRÁTI TRUE,
KDE $n > 2$ JE NEPÁRNE ČÍSLO A $1 \leq a \leq n-1$
POTOM n JE ZLOŽENÉ ČÍSLO

```
MILLER-RABIN (n, s)
   for j ← 1 to s do
      a ← RANDOM (1, n-1)
      if WITNESS (a, n) then RETURN COMPOSITE
   RETURN PRIME
```

VETA: AK $n > 2$ JE NEPÁRNE ZLOŽENÉ ČÍSLO, POTOM EXISTUJE ASPOŇ $\frac{n-1}{2}$ ČÍSIEL $a \in \{1, \dots, n-1\}$ TAKÝCH, ŽE WITNESS(a, n) VRÁTI TRUE.

$\Rightarrow$ PRAVDEPODOBNOSŤ CHYBY JE 2^{-s}.

11.08.2008 Su
PETER ČERNO

ŠTÁTNICE

3.13 APROXIMAČNÉ ALGORITMY

PREDPOKLADAJME, ŽE MÁME OPTIMALIZAČNÝ PROBLÉM, KDE KAŽDÉ POTENCIÁLNE RIEŠENIE MÁ KLADNÚ CENU (MINIMALIZAČNÝ / MAXIMALIZAČNÝ PROBLÉM)

POMEROVÁ CHYBA (APPROXIMATION RATIO)

$$\rho(n) \geq \max\left(\frac{c}{c^*}, \frac{c^*}{c}\right)$$

c .. CENA RIEŠENIA VYPRODUK. APROXIMAČNÝM ALGORITMOM
c^*.. CENA OPTIMÁLNEHO RIEŠENIA

1-APROXIMAČNÝ ALG. PRODUKUJE VŽDY OPTIMÁLNE RIEŠ.

APROXIMAČNÁ SCHÉMA PRE OPTIMAL. PROBLÉM A
VSTUP: (λ, ε), KDE λ JE INŠTANCIA A A $\varepsilon > 0$
→ $(1+\varepsilon)$-APROXIMAČNÝ ALGORITMUS APLIK. NA λ

POLYNOMIAL TIME: PRE $\forall \varepsilon > 0$ BEŽÍ V POLYNOMIÁLNOM ČASE VZHĽADOM NA $n = \langle \lambda \rangle$ VEĽKOSŤ VSTUPU

FULLY POLYNOMIAL TIME: ČASOVÁ ZLOŽITOSŤ JE POLYNOMIÁLNA VZHĽADOM NA $1/\varepsilon$ A n.

PRÍKLADY:

APPROX-VERTEX-COVER (G) $\rho(n) = 2$
APPROX-TSP-TOUR (G, c) $\rho(n) = 2$, MUSÍ PLATIŤ Δ-NEROVN.
SET-COVERING (X, F) $\rho(n) = H(\max_{S \in F} |S|)$
APPROX-SUBSET-SUM (S, t, ε) $\rho(n) = 1+\varepsilon$

APPROX-VERTEX-COVER (G)

$C \leftarrow \emptyset$, $E' \leftarrow E_G$
while $E' \neq \emptyset$ do LET $(u,v) \in E'$
  $C \leftarrow C \cup \{u,v\}$
  ODSTRÁŇ Z E' VŠETKY HRANY INCIDENTNÉ S u, v
return C

MÁME DANÝ ÚPLNÝ NEORIENTOVANÝ $G = K_n$ A $c: \binom{V}{2} \to \mathbb{R}_0^+$
c SPĹŇA Δ-INQ : $c(u,v) \leq c(u,w) + c(w,v)$

APPROX-TSP-TOUR (G, c)

$T \leftarrow$ MINIMUM-SPANNING-TREE (G)
VYPÍŠ VRCHOLY T V PORADÍ PREORDER

MÁME $(X, \mathcal{F})$, $\mathcal{F} \subseteq \mathcal{P}(X)$, $\bigcup \mathcal{F} = X$
HĽADÁME $\mathcal{C} \subseteq \mathcal{F}$: $\bigcup \mathcal{C} = X$, MINIMALIZUJEME $|\mathcal{C}|$

SET-COVERING $(X, \mathcal{F})$

V KAŽDOM KROKU VYBERIEME $S \in \mathcal{F}$, KT. POKRÝVA
ČO NAJVIAC NEPOKRYTÝCH VRCHOLOV

APPROX-SUBSET-SUM (S, t, ε)

$n \leftarrow |S|$
$L_0 \leftarrow \langle 0 \rangle$
for $i \leftarrow 1$ to n do
  $L_i \leftarrow$ MERGE-LISTS $(L_{i-1}, L_{i-1} + x_i)$
  ODSTRÁŇ Z L_i PRVKY VÄČŠIE AKO t
  $L_i \leftarrow$ TRIM $(L_i, \varepsilon/2n)$
return max L_n

TRIM (L, δ) ODSTRÁNI Z L ČO NAJVIAC PRVKOV TAK, ABY PRE KAŽDÝ ODSTRÁNENÝ $y \in L$ $\exists z \in L'$: $\frac{y}{1+\delta} \leq z \leq y$

01.09.2008 Mo
PETER ČERNO

ŠTÁTNICE

4 DATABÁZY

4.1 PODSTATA A ARCHITEKTÚRY DB SYSTÉMOV

DATABÁZA = LOGICKY USPORIADANÁ KOLEKCIA NAVZÁJOM SÚVISIACICH DÁT, JE SEBAVYSVETĽUJÚCA

SYSTÉM RIADENIA BÁZY DÁT (SRBD, DBMS) = SOFTWÉROVÝ SYSTÉM, KTORÝ POSKYTUJE ZDIEĽANÝ PRÍSTUP K DATABÁZE, ZABEZPEČUJE BEZPEČNOSŤ A INTEGRITU DÁT

DATABÁZOVÝ SYSTÉM = DATABÁZA + SRBD (+ADMIN)

1. DATABÁZOVÉ MODELY

SCHÉMA = POPISUJE OBJEKTY V DB A VZŤAHY MEDZI NIMI

MODEL = ŠTRUKTÚRA DÁT (SCHÉMA) + OPERÁCIE

PLOCHÝ MODEL

JEDNA 2D TABUĽKA, STĹPEC - DÁTA POPISUJÚCE 1 VLASTNOSŤ
RIADOK - POPIS 1 OBJEKTU

RELAČNÝ MODEL

MODEL UCHOVÁVANIA ENTÍT / VZŤAHOV V TABUĽKÁCH
DÁTOVÁ ENTITA / VZŤAH JE REPR. RIADKOM V TABUĽKE
ATRIBÚT A JE REPR. STĹPCOM V TABUĽKE
SCHÉMA TABUĽKY $S(A_1 : T_1, A_2 : T_2, \ldots)$
S = NÁZOV TAB., A_i ATRIBÚTY A T_i SÚ ICH TYPY
SCHÉMA RELAČNEJ DATABÁZY = MNOŽINA SCHÉM TABULIEK + ĎALŠIE VECI AKO INTEGR. OBMEDZENIA, ...

NIE SÚ POVOLENÉ IDENTICKÉ RIADKY
KAŽDÝ RIADOK JE IDENTIFIKOVATEĽNÝ JEDNÝM
ALEBO VIACERÝMI ATRIBÚTMI V RÁMCI TABUĽKY
= NADKĽÚČ, KĽÚČ = MINIM. NADKĽÚČ

RELÁCIA $R \subseteq D_1 \times \ldots \times D_n$
D_i SÚ DOMÉNY ATRIBÚTOV A_i
SCHÉMA RELÁCIE $R(A_1 : D_1, \ldots, A_n : D_n)$

DOTAZOVANIE REL. DÁT < RELAČNÝ KALKUL / RELAČNÁ ALGEBRA

NORMALIZÁCIA REL. SCHÉM: DEKOMPOZÍCIA & SYNTÉZA

HIERARCHICKÝ MODEL

DATA ORGANIZOVANÉ DO STROMOVEJ ŠTRUKTÚRY
DOVOĽUJÚ VZŤAHY 1:N MEDZI DVOMI DRUHMI DÁT
NEVÝHODY: NUTNOSŤ POZNAŤ CELÚ CESTU
K ZÁZNAMU V ŠTRUKTÚRE
NESCHOPNOSŤ SYSTÉMU REPREZENTOVAŤ REDUNDANCIE

SIEŤOVÝ MODEL

DATA ORGANIZOVANÉ POMOCOU ZÁZNAMOV A MNOŽÍN
ZÁZNAMY OBSAHUJÚ POLE DÁT
MNOŽINY DEFINUJÚ VZŤAHY 1:N (1 VLASTNÍK, N PRVKOV)
UMOŽŇUJE REPREZENTOVAŤ AJ REDUNDANTNÉ DÁTA
FYZICKY SÚ MNOŽINY (TJ. VZŤAHY) REPREZENTOVANÉ
UKAZATEĽMI NA UMIESTNENIE DÁT NA DISKU
→ VYSOKÝ VÝKON PRI VYHĽADÁVANÍ,
VYSOKÉ NÁKLADY NA REORGANIZÁCIU

OBJEKTOVÝ MODEL

POUŽITIE DÁTOVÝCH TYPOV (OBJEKTOV), NEEXISTUJÚ ŠTANDARDY

01.09.2008 Mo
PETER ČERNO

ŠTÁTNICE

2. ARCHITEKTÚRY DB SYSTÉMOV

{ CENTRALIZOVANÉ
DISTRIBUOVANÉ

{ JEDNOUŽÍVATEĽSKÉ
VIACUŽÍVATEĽSKÉ

DISTRIBUOVANÝ DB SYSTÉM

- IMPLEMENTÁCIA ZAHŔŇA ROZLOŽENIE DAT NA VIAC PC - UZLY
- POPIS DAT JE INTEGROVANÝ V GLOBÁLNEJ DATABÁZOVEJ SCHÉME
- DATA V UZLOCH SÚ SPRACOVÁVANÉ LOKÁLNYMI SRBD
- KOMUNIKÁCIA JE ORGANIZOVANÁ V SIEŤOVEJ PREVÁDZKE

+ VÝHODY: VYŠŠIA EFEKTIVITA, DOSTUPNOSŤ, ROZŠÍRITEĽNOSŤ
− NEVÝHODY: ZLOŽITOSŤ IMPLEMENTÁCIE, BEZPEČNOSŤ

VIACUŽÍVATEĽSKÝ DB SYSTÉM

UMOŽŇUJE SÚČASNÝ PRÍSTUP VIAC UŽÍVATEĽOV
JE NUTNÉ ZABEZPEČIŤ INTEGRITU A KONZISTENCIU DAT:

(1) UZAMYKANIE

(2) MULTIVERSION CONCURENCY CONTROL
PRI POŽIADAVKU O AKTUALIZÁCIU ZÁZNAMU V TAB. JE VYTVORENÁ KÓPIA, KTORÁ NIE JE PRE OSTATNÍCH UŽÍVATEĽOV AŽ DO COMMITU VIDITEĽNÁ

4.2 KONCEPTUÁLNA, LOGICKÁ A FYZICKÁ ÚROVEŇ POHĽADU NA DATA

DATOVÉ MODELOVANIE - PROCES VYTVORENIA KONKRÉTNEHO DATOVÉHO MODELU (SCHÉMY)

(1) KONCEPTUÁLNA SCHÉMA - TRIEDY ENTÍT A ICH VZŤAHY
(2) LOGICKÁ SCHÉMA - VÝZNAM KONCEPT. SCHÉMY Z HĽADISKA DATAB. MODELU
V RELAČNOM MODELI - POPIS TABULIEK (REL. SCHÉM)
V HIERARCH. MODELI - XML TAGY
(3) FYZICKÁ SCHÉMA - FYZICKÉ ULOŽENIE DAT
SOS - SEKV. SÚBORY, B-STROMY, ...

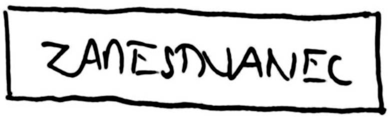
1. KONCEPTUÁLNA SCHÉMA (DATOVÝ MODEL)

POPISUJE TRIEDY ENTÍT, ICH ATRIBÚTY A VZŤAHY MEDZI NIMI

PRÍKLAD: - EACH PERSON MAY BE THE VENDOR IN ONE OR MORE ORDERS
- EACH ORDER MUST BE FROM ONE AND ONLY ONE PERSON
...

STANDARD PRE KONCEPTUÁLNE MODELOVANIE: ER DIAGRAM (ENTITY - RELATIONSHIP DIAGRAM)

HODIA SA PRE [RELAČNÝ] ALEBO [OBJEKTOVÝ] DB MODEL ALE NIE NAPR. PRE XML APOD.



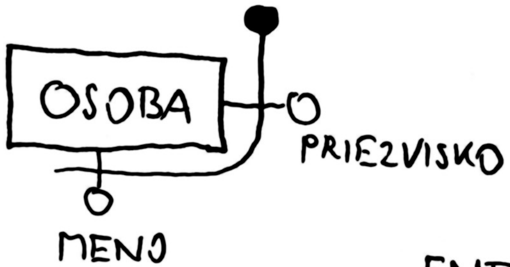
ENTITNÝ TYP

ENTITNÝ TYP S ATRIBÚTOM

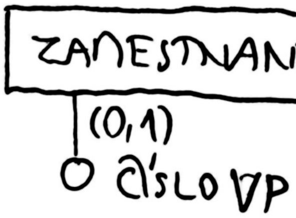
ENTITNÝ TYP S IDENTIFIKÁTOROM

01.09.2008 Mo
PETER ČERNO

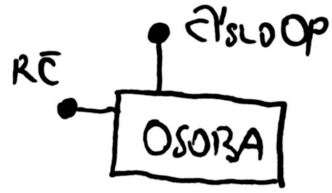
ŠTÁTNICE



ENTITNÝ TYP S VIACATRIBÚTOVÝM IDENTIFIKÁTOROM

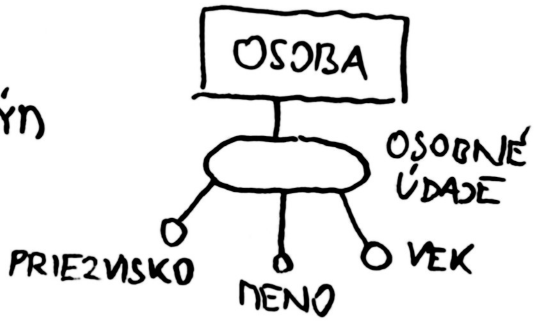


ENTITNÝ TYP S NEPOVINNÝM ATRIBÚTOM



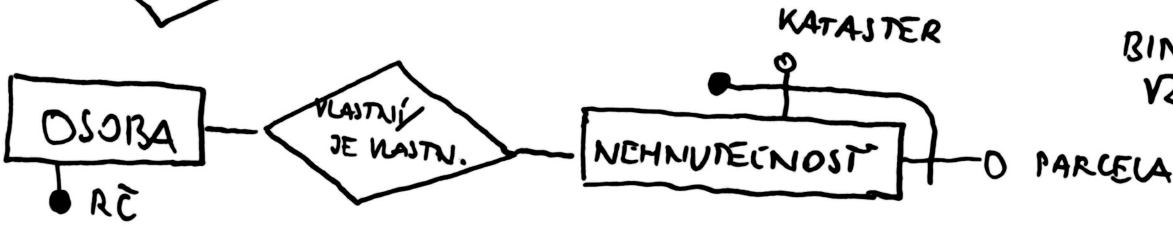
ENTITNÝ TYP S VIAC JEDNOATR. IDENTIFIKÁTORMI

ENTITNÝ TYP S VIACHODNOTOVÝM ATRIBÚTOM



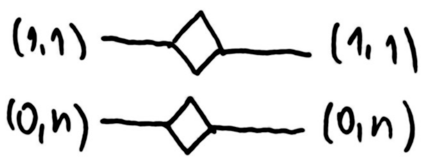
ENTITNÝ TYP SO ZLOŽENÝM ATRIBÚTOM

VZŤAHOVÝ TYP



BINÁRNY VZŤAH

1:N (ONE-TO-MANY)



ONE-TO-ONE

MANY-TO-MANY

SLABÝ ENTITNÝ TYP

4.3 RELAČNÝ DATOVÝ MODEL, RELAČNÝ KALKUL, RELAČNÁ ALGEBRA

RELAČNÝ DATOVÝ MODEL

RELÁCIA $R \subseteq D_1 \times \dots \times D_n$ ($\equiv$ DATA V TABUĽKE)

D_i SÚ ATRIBÚTOVÉ DOMÉNY, D. TYPY

SCHÉMA RELÁCIE JE URČENÁ VÝČTOM ATRIB. A ICH TYPOV

$R(A) \equiv R(A_1 : D_1, \dots, A_n : D_n)$ ($\equiv$ SCHÉMA TABUĽKY)

PRVOK RELÁCIE R $\equiv$ RIADOK TABUĽKY

PROBLÉMY NÁVRHU RELAČNEJ SCHÉMY:

(1) REDUNDANCIA

(2) AKTUALIZAČNÉ ANOMÁLIE (INSERT / DELETE / UPDATE)

RIEŠENIE: NORMALIZÁCIA DB SCHÉMY, NORMÁLNE FORMY, ALGORITMY: DEKOMPOZÍCIA, SYNTÉZA

RELAČNÁ ALGEBRA

DOTAZ, MOŽIVA MNOŽINY OPERÁCIÍ NA DB RELÁCIACH

1. PREMENOVANIE ATRIBÚTOV: $R^* \langle a_i \to b_i, a_j \to b_j, \dots \rangle$
2. MNOŽINOVÉ OPERÁCIE: $\cup, \cap, -, \times$
   $\langle R_1^*, R_1(A) \rangle \cup \langle R_2^*, R_2(A) \rangle = \langle R_1^* \cup R_2^*, R_x(A) \rangle$ $R_1(A) = R_2(A)$
3. PROJEKCIA
   $\langle R^*[C], R(A) \rangle = \langle \{u[C] \mid u \in R^*\}, R(C) \rangle$, KDE $C \subseteq A$
4. SELEKCIA
   $\langle R^*(\varphi), R(A) \rangle = \langle \{u \in R^* \mid \varphi(u)\}, R(A) \rangle$
5. PRIRODZENÉ SPOJENIE
   $\langle R^*, R(A) \rangle * \langle S^*, S(B) \rangle = \langle \{u \mid u[A] \in R^* \,\&\, u[B] \in S^*\}, R_x(A \cup B) \rangle$
6. Θ - SPOJENIE, DELENIE, ...

01.09.2008 Mo
PETER ČERNO

ŠTÁTNICE

RELAČNÝ KALKUL

VYUŽITIE APARÁTU PREDIKÁTOVEJ LOGIKY 1. RÁDU PRE DOTAZY
DOMÉNOVÝ KALKUL (DRK) – DATA NA ÚROVNI ATRIBÚTOV
n-TICOVÝ KALKUL (NRK) – DATA NA ÚROVNI n-TIC PRVKOV

1. DOMÉNOVÝ KALKUL

DATABÁZOVÝ PREDIKÁT $R(x, y, \dots)$
- R JE ZÁROVEŇ NÁZOV TABUĽKY
- PREDIKÁT PRE KONKRÉTNE HODNOTY ATRIBÚTOV NADOBÚDA true $\Leftrightarrow$ V RELÁCII R EXISTUJE PRVOK S TÝMITO HODNOTAMI

PRÍKLAD DOTAZU: $\{(x,y) \mid KINO(x,y)\}$
V KT. FILMOCH HRALI $\forall$ HERCI ?
$\{(f) \mid FILM(f) \,\&\, \forall h\, (HEREC(h) \Rightarrow FILM(f,h))\}$

2. n-TICOVÝ KALKUL

TAKMER TAKÉ ISTÉ AKO DRK, ALE PREMENNÉ SÚ CELÉ PRVKY RELÁCIE (RIADKY)
PRÍKLAD DOTAZU: $\{t \mid KINO(t) \,\&\, t.FILM = \text{"TITANIC"}\}$
VÝSLEDOK MOŽNO PROJEKTOVAŤ NA URČITÉ ATRIBÚTY
$\{t[NÁZOV\_KINA] \mid KINO(t)\}$

DRK AJ NRK SÚ <u>RELAČNE ÚPLNÉ</u>
RELAČNÁ ALGEBRA PRACUJE S RELÁCIAMI (CELÉ TABUĽKY)
NRK PRACUJE S PRVKAMI RELÁCIÍ (CELÉ RIADKY)
DRK PRACUJE S PRVKAMI ATRIBÚTOV (PRVKY RIADKOV)

4.4 ALGORITMY NÁVRHU SCHÉM RELÁCIÍ

PROBLÉMY NÁVRHU RELAČNEJ SCHÉMY:

(1) REDUNDANCIA

(2) AKTUALIZAČNÉ ANOMÁLIE (INSERT / DELETE / UPDATE)

RIEŠENIE: NORMALIZÁCIA DB SCHÉMY, NORMÁLNE FORMY, ALG. DEKOMPOZÍCIA & SYNTÉZA

__FUNKČNÁ ZÁVISLOSŤ__ (FZ) $f: X \to Y$ NAD SCHÉMOU $R(A)$ KDE $X, Y \subseteq A$, n-TICA z X FUNKČNE URČUJE m-TICU z Y.

$X \to a$, KDE $a \in A$ JE __ELEMENTÁRNA FZ__

__ROZŠÍRENÁ SCHÉMA__: $R(A, F)$, F SÚ FZ NAD ATR. A

__KĽÚČ__ $K \subseteq A$: $K \to A$, K JE MINIMÁLNA S TOUTO VLASTNOSŤOU

__KĽÚČOVÝ ATRIBÚT__: JE OBSIAHNUTÝ V NEJAKOM KĽÚČI

__ARMSTRONGOVÉ PRAVIDLÁ__: MAJME $R(A, F)$, $X, Y, Z \subseteq A$

(1) $Y \subseteq X \Rightarrow X \to Y$ (TRIVIÁLNA FZ)

(2) $X \to Y \;\&\; Y \to Z \Rightarrow X \to Z$ (ASOCIATIVITA)

(3) $X \to Y \;\&\; X \to Z \Rightarrow X \to YZ$ (KOMPOZÍCIA)

(4) $X \to YZ \Rightarrow X \to Y \;\&\; X \to Z$ (DEKOMPOZÍCIA)

- SÚ KOREKTNÉ
- SÚ ÚPLNÉ
- (1), (2), (3) SÚ NEZÁVISLÉ

__UZÁVER F^+__ JE MNOŽINA $\forall$ FZ, KT. MOŽNO ODVODIŤ Z F ARMSTRONGOVÝMI PRAVIDLAMI

$f \in F$ JE __REDUNDANTNÁ__ $\Leftrightarrow$ $(F - \{f\})^+ = F^+$

__POKRYTIE__ MNOŽINY FZ F JE MN. FZ G: $F^+ = G^+$

__KANONICKÉ POKRYTIE__ - IBA ELEMENTÁRNE FZ

__NEREDUNDANTNÉ POKR. F__ - F PO ODSTR. $\forall$ REDUND. FZ

5/6

01.09.2008 Mo
PETER ČERNO

ŠTÁTNICE

UZÁVER MNOŽINY ATRIBÚTOV X^+ VZHĽADOM K FZ F JE MN. ∀ ATRIBÚTOV FUNKČNE ZÁVISLÝCH NA X

$X^+ = A \Rightarrow X$ JE NADKĽÚČ

MAJME FZ $X \to Y \in F$ A $a \in X$ T.Ž. $Y \subseteq (X-a)^+$
$\Rightarrow a$ JE **REDUNDANTNÝ ATRIBÚT** V $X \to Y$

REDUKOVANÁ FZ NA ĽAVEJ STRANE NEOBSAHUJE REDUNDANTNÉ ATRIBÚTY

MINIMÁLNE POKRYTIE = NEREDUNDANTNÉ KANONICKÉ POKRYTIE, KT. SA SKLADÁ IBA Z REDUKOVANÝCH FZ

KONŠTRUUJEME: NAJSKÔR ODSTRÁNENÍM REDUNDANTNÝCH ATRIBÚTOV VO FZ
AŽ POTOM ODSTRÁNENÍM RED. ZÁVISLOSTÍ

NORMÁLNE FORMY

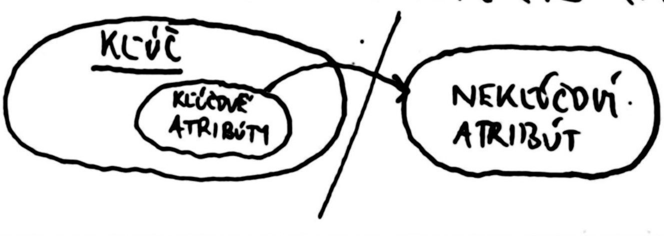
PRVÁ NORMÁLNA FORMA (1NF)

KAŽDÝ ATRIBÚT SCHÉMY RELÁCIE JE ELEMENTÁRNEHO TYPU A JE NEŠTRUKTUROVANÝ (ZÁKLADNÁ PODMIENKA PLOCHOSTI DATABÁZE)

DRUHÁ NORMÁLNA FORMA (2NF)

1NF +

NEEXISTUJÚ ČIASTOČNÉ ZÁVISLOSTI NEKĽÚČOVÝCH ATTR. NA KĽÚČI, T.J. $\forall x \in NK \neg\exists KK : KK \to x$, $KK \subset$ KĽÚČ



TRANZITÍVNA ZÁVISLOSŤ NA KĽÚČI

FZ $A \to B$ TAKÁ, ŽE $A \not\to$ KĽÚČ, TJ. A NIE JE NADKĽÚČ

OBDRŽÍME TRANZITIVITU: KĽÚČ $\to A \to B$

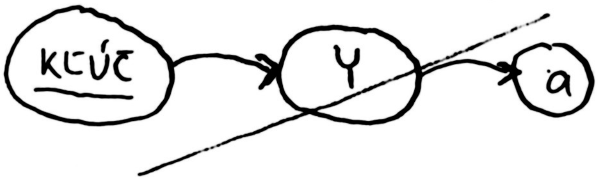
PRÍKLAD V 2NF: <u>PSČ</u> → MESTO → ŠTÁT

V TOMTO STĹPCI VYSOKÁ REDUNDANCIA !!

TRETIA NORMÁLNA FORMA (3NF)

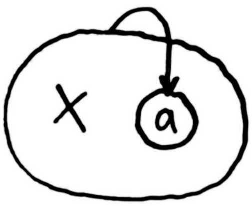
2NF +

ŽIADNY NEKĽÚČOVÝ ATRIBÚT NIE JE TRANZITÍVNE ZÁVISLÝ NA ŽIADNOM KĽÚČI



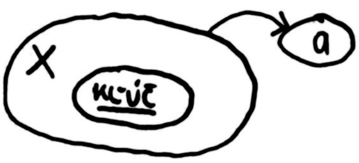
⇔ PRE KAŽDÚ ZÁVISLOSŤ $X \to a$, $X \subseteq A$, $a \in A$ PLATÍ:

a)



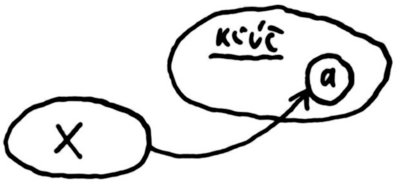
TRIVIÁLNA ZÁVISLOSŤ

b)



X JE NADKĽÚČ

c)



a JE KĽÚČOVÝ ATRIBÚT

BOYCE-CODDOVA NORMÁLNA FORMA (BCNF)

2NF +

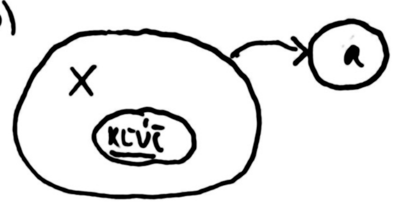
KAŽDÝ ATRIBÚT JE NETRANZITÍVNE ZÁVISLÝ NA KĽÚČI

⇔ PRE KAŽDÚ ZÁVISLOSŤ $X \to a$ $X \subseteq A$, $a \in A$ PLATÍ

a)

TRIVIÁLNA ZÁVISLOSŤ

b)



X JE NADKĽÚČ

01.09.2008 Po
PETER ČERNO

ŠTÁTNICE

ALGORITMY NÁVRHU SCHÉM RELÁCIÍ

SCHÉMY RELÁCIÍ BY MALI BYŤ NAVRHNUTÉ TAK, ABY ZODPOVEDALI DOPREDU PRIPRAVENÉMU KONCEPTUÁLNEMU MODELU (ER DIAGRAMY) + ABY SPĹŇALI ČO NAJPRÍSNEJŠIE POŽIADAVKY NA NORMÁLNE FORMY

- 2 PRÍSTUPY:

(1) ZÍSKANIE MN. REL. SCHÉM (NAPR. PREVOD Z ER DIAGRAMOV) → NORMALIZÁCIA KAŽDEJ TAB. (RIZIKO PRÍLIŠNÉHO ROZDROBENIA DATABÁZE)
(2) UNIVERZÁLNA SCHÉMA DATABÁZE VRÁTANE FZ → NORMALIZÁCIA VYKONANÁ GLOBÁLNE

NORMALIZÁCIA RELAČNEJ SCHÉMY

JEDINÝ SPÔSOB: DEKOMPOZÍCIA NA VIAC SCHÉM
- KRITÉRIA: (1) BEZSTRATOVOSŤ
 (2) POKRYTIE ZÁVISLOSTÍ
 (3) POŽIADAVOK NA NF (3NF ALEBO BCNF)

DEKOMPOZÍCIA $R(A, F)$ DO $R_1(A_1, F_1)$, $R_2(A_2, F_2)$ JE BEZSTRATOVÁ $\Leftrightarrow$ $A_1 \cap A_2 \to A_1 \vee A_1 \cap A_2 \to A_2$
ZACHOVÁVA POKRYTIE ZÁVISLOSTÍ $\Leftrightarrow$ $F^+ = F_1^+ \cup F_2^+$

ALGORITMUS DEKOMPOZÍCIA:
DO BCNF, ZACHOVÁVA BEZSTRATOVOSŤ, ALE NIE POKR. ZÁV.

ALGORITMUS SYNTÉZA:
DO 3NF, ZACHOVÁVA POKR. ZÁVISLOSTÍ, BEZSTRATOVOSŤ MOŽNO ZAISTIŤ PRIDANÍM SCH. S UNIV. KĽ.

ALG. DEKOMPOZÍCIA

DECOMPOSITION (A_i, F_i)

1. SPOČÍTAŤ F^+
2. while $\exists R_i(A_i, F_i) \notin BCNF$, T.J.
   $\exists X \to Y \in F_i : X \to A_i \notin F^+$ do
   $R_i(A_i, F_i)$ ROZLOŽ NA:
   $R_1(A_i - Y, F^+[A_i - Y])$
   $R_2(X \cup Y, F^+[X \cup Y])$

ALG. SYNTÉZA

SYNTHESIS (A, F)

1. VYTVOR MINIMÁLNE POKRYTIE G (Z FZ F)
2. ZLÚČ FZ Z G S ROVNAKOU ĽAVOU STRANOU
3. VYPUSTI SCHÉMY, KTORÉ SÚ PODMNOŽINY INÝCH SCH.

REFERENČNÁ INTEGRITA

POMÁHA UDRŽOVAŤ VZŤAHY
KONTROLA PRÍPUSTNÝCH HODNÔT
KONTROLA EXISTENCIE POLOŽKY (PODĽA CUDZ. KĽÚČA)

02.09.2008 Tu
PETER ČERNO

ŠTÁTNICE

4.5 ZÁKLADY SQL

SQL (STRUCTURED QUERY LANGUAGE)
  ŠTANDARDNÝ JAZYK PRE PRÍSTUP K REL. DATABÁZAM (DOTAZY)
    DDL (DEFINITION DATA LANGUAGE)
    DML (DATA MANIPULATION LANGUAGE)

SQL JE ŠTANDARD PODĽA NORIEM ANSI/ISO
- SQL 86 – PRVÝ NÁSTREL, IBM
- SQL 89 – MALÁ REVÍZIA MOTIVOVANÁ KOMERČNOU SFÉROU
- *SQL 92 – TABUĽKY S METADATAMI, VONKAJŠIE SPOJ., MN. OPERÁCIE, KASKÁDOVÉ MAZANIE, TRANSAKCIE, KURZORY, VÝNIMKY
- SQL 1999 – OBJEKTOVO-REL. ROZŠÍRENIE, NOVÉ DAT. TYPY, PODPORA PRE EXTERNÉ DAT. SÚBORY, MULTIMÉDIA
- SQL 2003 – XML MANAGEMENT

KOMERČNÉ PRODUKTY: VÄČŠINOU SQL92, SQL99,
  NIE STRIKTNE: T-SQL (MICROSOFT SQL SERVER),
  PL-SQL (ORACLE)

DOTAZY V SQL

```
SELECT [DISTINCT] VÝRAZ1 [[AS] C_ALIAS1] [, ...]
FROM ZDROJ1 [[AS] T_ALIAS1] [, ...]
[WHERE PODMIENKA_R]
[GROUP BY VÝRAZ_G1 [, ...]]
[HAVING PODMIENKA_S]
[ORDER BY VÝRAZ_O1 [, ...] ASC/DESC]
```

SELECT ZDIEĽA PRVKY REL. KALKULU AJ REL. ALGEBRY

POVOĽUJE DUPLICITNÉ RIADKY AJ NULL HODNOTY

* SQL 92: ∃ ENTRY, TRANSITIONAL, INTERMEDIATE, FULL

<výraz> = <názov stĺpca>, <konštanta>, +, -, *, /
[DISTINCT] COUNT (<názov stĺpca>)
[DISTINCT] SUM / AVG (<výraz>)
MIN / MAX (<výraz>)

zdroje sú TABUĽKY ALEBO VNORENÉ SELECTY

<podmienka> = <výraz> BETWEEN <x> AND <y>
<výraz> LIKE "% _ ..."
<výraz> IS [NOT] NULL
<výraz> > = <> < <= >= <výraz>
ALL/ANY <dotaz>
<výraz> [NOT] IN <zoznam hodnôt> / <dotaz>
EXIST (<dotaz>)

GROUP BY = AGREGÁCIA PODĽA UNIKÁTNYCH HODNÔT MENOVANÝCH STĹPCOV
HAVING = PODMIENKA NA AGREGÁCIU
ORDER BY = PODĽA ČOHO SA MÁ VÝSTUP UTRIEDIŤ

VYHODNOCOVANIE PRÍKAZU SELECT

1. NAJSKÔR SA SKOMBINUJÚ DATA ZO ∀ ZDROJOV (FROM)
AK SÚ ODDELENÉ ČIARKAMI → KARTÉZSKY SÚČIN
OD SQL 92 - JOIN ON, NATURAL JOIN, OUTER JOIN
2. VYRADIA SA RIADKY, KT. NEVYHOVUJÚ PODMIENKE WHERE
3. RIADKY SA ZOSKUPIA DO SKUPÍN PODĽA *GROUP BY
4. VYRADIA SA TIE, KT. NEVYHOVUJÚ PODMIENKE HAVING
5. VÝSLEDOK SA ZOTRIEDI PODĽA ORDER BY
6. V PRÍPADE DISTINCT SA VYRADIA DUPLICITNÉ RIADKY

---

* GROUP BY PRED VYTVORENÍM SKUPÍN ZOTRIEDI RIADKY PODĽA VÝRAZOV V KLAUZULI

02. 09. 2008 Tu
PETER ČERNO

ŠTÁTNICE

PRÍKAZ CREATE TABLE

```
CREATE TABLE názovt (
    názov_stĺpca <dat_typ> [DEFAULT NULL / hodnota]
      [CONSTRAINT meno] [NOT NULL / UNIQUE /
       PRIMARY KEY] + [REFERENCES tabuľka (stĺpec)
    ... [CHECK (podmienka)]                  <akcia>]
    [UNIQUE / PRIMARY KEY (stĺpec, ...)
     FOREIGN KEY (stĺpec, ...)
     REFERENCES tabulka (stĺpec, ...)
     CHECK (podmienka)                  ]
);
```

1.O. STĹPCA – the [CONSTRAINT meno] … [CHECK (podmienka)] part

1.O. TABUĽKY – the UNIQUE / PRIMARY KEY … CHECK (podmienka) part

```
<akcia> = [ON UPDATE / ON DELETE] [CASCADE / SET NULL / SET DEFAULT / NO ACTION]
```

NAPRÍKLAD:

```
CREATE TABLE users (
    username VARCHAR(20) DEFAULT '' NOT NULL,
    password VARCHAR(50) DEFAULT '' NOT NULL,
    ...
    PRIMARY KEY (username)
);
```

<dat_typ> = VARCHAR(n), BIT(n), INTEGER, FLOAT, DECIMAL, ...

PRÍKAZY PRE MANIPULÁCIU SO SCHÉMOU

ÚPRAVA TABUĽKY :

ALTER TABLE názov_t
ADD COLUMN <def stĺpca> ,
ADD <I.O. TABUĽKY>
ALTER COLUMN stĺpec [SET / DROP]
DROP COLUMN stĺpec
DROP CONSTRAINT meno i.o.

ZMAZANIE TABUĽKY:

DROP TABLE tabuľka

VYTVORENIE POHĽADU :

CREATE VIEW meno (stĺpec , ...)
AS <dotaz>

PRÍKAZY PRE MANIPULÁCIU S DÁTAMI

INSERT INTO tabuľka (stĺpec, ...)
VALUES (výraz , ...) / <dotaz>

UPDATE tabuľka SET (stĺpec = NULL/výraz/dotaz , ...)
WHERE podmienka

DELETE FROM tabuľka
WHERE podmienka

MNOŽINOVÉ OPERÁCIE

UNION, INTERSECTION, EXCEPT

02.09.2008 Tu
PETER ČERNO

STÁTNICE

4.6 TRANSAKČNÉ SPRACOVANIE, UZAMYKACIE PROTOKOLY, ZABLOKOVANIE

TRANSAKCIA = POSTUPNOSŤ AKCIÍ (DB OPERÁCIÍ A INÝCH) S KTORÔU SA ZAOBCHÁDZA AKO S 1 CELKOM

POŽADOVANÉ VLASTNOSTI TRANSAKČNÉHO SPRACOVANIA TZV. ACID VLASTNOSTI:

- ATOMICITY = TRANSAKCIA JE VYKONANÁ BUĎ CELÁ ALEBO VÔBEC (ZAISTUJE SRBD)
- CONSISTENCY = TR. ZACHOVÁVA DB V KONZISTENTNOM STAVE
- ISOLATION = VIAC SÚBEŽNE BEŽIACICH TR. O SEBE NEVIE
- DURABILITY = OP. VYKONANÉ ÚSPEŠNE UKONČENOU TRANS. SÚ TRVALO ULOŽENÉ V DB

SPÔSOB UKONČENIA TRANS. { COMMIT - ÚSPEŠNÉ UKONČENIE TR.
ROLLBACK - [UŽÍVATEĽ / SYSTÉM / HW] }

TRANSAKČNÝ ROZVRH - JE ZOTRIEDENÝ ZOZNAM AKCIÍ NIEKOĽKO TRANSAKCIÍ (AKCIE RÔZNYCH TR. SÚ RÔZNE PREložené) JE TO "RUNTIME" HISTÓRIE UŽ VYKONANÝCH AKCIÍ

- ROZVRHOVAČ (SCHEDULER) - VYTVÁRA ROZVRH PRE DANÚ MN. TRANS. ROZVRH JE VYTVÁRANÝ DYNAMICKY

SÉRIOVÝ ROZVRH - NEJAKÁ PERMUTÁCIA CELÝCH TRANSAKCIÍ

DÔVOD PREKLADANÝCH ROZVRHOV:

(1) PARALELIZÁCIA NEDATABÁZOVÝCH AKCIÍ
(2) RÝCHLE VYKONANIE MALÝCH TRANSAKCIÍ

ROZVRH JE USPORIADATEĽNÝ ⇔ VEDIE KU KONZISTENTNÉMU STAVU DB, TJ. KU STAVU, KU KT. DOJDEME NEJAKÝM SÉRIOVÝM ROZ.

TÁTO VLASTNOSŤ ZARUČUJE: IZOLÁCIU TR. A KONZISTENCIU DB

KONFLIKTY (PRAMENIA Z PORADIA DVOJÍC AKCIÍ V ROZRHU VYKONANÉ NA 1 OBJEKTE RÔZNYMI TRANSAKCIAMI)

WR - ČÍTANIE NEPOTVRDENÝCH DÁT (DIRTY READ)
RW - NEOPAKOVATEĽNÉ ČÍTANIE
WW - PREPÍSANIE NEPOTVRDENÝCH DÁT (BLIND WRITE)

DVA ROZVRHY SÚ <u>KONFLIKTOVO EKVIVALENTNÉ</u> ⟺ MAJÚ ROVNAKÉ KONFLIKTNÉ PÁRY

ROZVRH JE <u>KONFLIKTOVO USPORIADATEĽNÝ</u> ⟺ JE KONFLIKTOVO EKVIVAL. NEJAKÉMU SÉRIOVÉMU ROZVRHU
⟺ <u>PRECEDENČNÝ GRAF</u> JE ACYKLICKÝ

KONFLIKTOVÁ USPORIADATEĽNOSŤ NEZOHĽADŇUJE:
(1) ROLLBACK - ROZVRH MÔŽE BYŤ <u>NEZOTAVITEĽNÝ</u>
(2) DYNAMICKÚ POVAHU DB - MÔŽE VZNIKNÚŤ <u>FANTÓM</u>

POSTAČUJÚCA PODMIENKA JE <u>POHĽADOVÁ USPORIADATEĽNOSŤ</u>

<u>ZOTAVITEĽNÝ ROZVRH</u> - TRANSAKCIA T JE POTVRDENÁ AŽ POTOM, ČO SA POTVRDIA VŠETKY TRANSAKCIE, KTORÉ ZMENILI DÁTA, ČÍTANÉ A ZAPISOVANÉ V T

AK V ZOTAVITEĽNOM ROZVRHU NAVIAC DOCHÁDZA K ČÍTANIU ZMIEN IBA POTVRDENÝCH TRANSAKCIÍ, NEMÔŽE DÔJSŤ ANI KU <u>KASKÁDOVÉMU RUŠENIU TRANS.</u>

ROZVRHOVAČ TRANSAKCIÍ VOLÍ NEJAKÝ <u>PROTOKOL</u> TAK, ABY BOLI ZACHOVANÉ POŽADOVANÉ VLASTNOSTI

UZAMYKACIE PROTOKOLY (2PL, S2PL, C2PL, ...)
VYUŽÍVAJÚ SA ZÁMKY
ALTERNATÍVNE PROTOKOLY
OPTIMISTICKÉ RIADENIE
ČASOVÉ RAZÍTKA

02.09.2008 Tu
PETER ČERNO

ŠTÁTNICE

UZAMYKACIE PROTOKOLY

EXKLUZÍVNY ZÁMOK X(A) - ČÍTAŤ A ZAPISOVAŤ DO A
MÔŽE IBA VLASTNÍK ZÁMKU

ZDIEĽANÝ (SHARED) ZÁMOK S(A) - MÔŽE BYŤ ZDIEĽANÝ VIAC TR.
ODOMYKÁ SA POŽIADAVKOM U(A)

DVOJFÁZOVÝ UZAMYKACÍ PROTOKOL (2PL)

(1) KEĎ CHCE TRANSAKCIA ČÍTAŤ (MODIFIKOVAŤ) ENTITU A, MUSÍ ZÍSKAŤ ZDIEĽANÝ (EXKLUZÍVNY) ZÁMOK NA A
(2) TRANS. NEMÔŽE ZAMYKAŤ, AK UŽ NEJAKÝ ZÁMOK UVOLNILA

⇒ 2 FÁZY: ZAMYKANIE, ODOMYKANIE

2PL ZARUČUJE, ŽE PRECEDENČNÝ GRAF JE ACYKLICKÝ, TJ. ROZVRH JE KONFLIKTOVO USPORIADATEĽNÝ
2PL NEGARANTUJE ZOTAVITEĽNOSŤ ROZVRHU, NEVYLUČUJE VZNIK DEADLOCKU

STRIKTNÝ DVOJFÁZOVÝ UZAMYKACÍ PROTOKOL (S2PL)

TO ISTÉ AKO 2PL, AŽ NA:
(2) VŠETKY ZÁMKY SÚ UVOLNENÉ PRI UKONČENÍ TRANSAKCIE

S2PL OPROTI 2PL NAVIAC GARANTUJE:
ZOTAVITEĽNOSŤ + ZABEZP. PROTI KASKÁDOVÉMU RUŠENIU

DETEKCIA DEADLOCKU:
(1) WAITS-FOR-GRAF - DETEKCIA CYKLU
(2) POKIAĽ TRANSAKCIA ČAKÁ MOC DLHO, ASI UVIAZLA, ROLLBACK

PREVENCIA UVIAZNUTIA :

(1) PRIORITNÉ UPREDNOSTŇOVANIE :

WAIT - DIE

WOUND - WAIT

(2) KONZERVATÍVNY 2PL PROTOKOL (C2PL)

POŽADUJE, ABY ∀ ZÁMKY, KT. TRANS. BUDE POTREBOVAŤ, BOLI ŽIADANÉ NA ZAČIATKU TRANSAKCIE

V PRAXI SA NEPOUŽÍVA

FANTÓM - MÔŽE VZNIKNÚŤ AK UVAŽUJEME AJ OPERÁCIE VKLADANIA A MAZANIA

PREVENCIA :

(1) AK NEEXISTUJÚ INDEXY, JE NUTNÉ UZAMKNÚŤ VŠETKO, ČO BY MOHLO BYŤ FANTÓMOM NEG. OVPLYVNENÉ (CELÚ TABUĽKU ALEBO AJ VIAC TABULIEK)

(2) AK EXISTUJÚ INDEXY, JE MOŽNÉ VYHNÚŤ SA FANTÓMOVI NA ÚROVNI INDEXU (INDEX LOCKING)

(3) PREDIKÁTOVÉ UZAMYKANIE, ŤAŽKO IMPL., ZRIEDKA POUŽ.

ALTERNATÍVNE PROTOKOLY

OPTIMISTICKÉ RIADENIE (3 FÁZY) :

1. READ : DB → LOKÁLNY DÁTOVÝ PRIESTOR
2. VALIDATION : TRANS. PREDLOŽÍ SRBD SVOJ DÁTOVÝ PRIESTOR
3. WRITE : AK JE VŠETKO OK ⇒ LOK. DATA → DB

ČASOVÉ RAZÍTKA : ČASOVÉ RAZÍTKO TRANS. TS(T)

ČÍTACIE RAZÍTKO RTS(O) (READ TIMESTAMP)

ZAPISOVACIE RAZÍTKO WTS(O) (WRITE TIMESTAMP)

(1) T CHCE ČÍTAŤ O :

a) TS(T) < WTS(O) → ROLLBACK T

b) TS(T) > WTS(O) → OK, ZMENA RTS(O)

(2) T CHCE ZAPÍSAŤ DO O :

a) TS(T) < RTS(O) → ROLLBACK T

b) TS(T) < WTS(O) → NIČ NEZAPÍŠ.

c) T ZMENÍ O AJ WTS(O)

02.09.2008 Tu
PETER ČERNO

ŠTÁTNICE

4.7 ORGANIZÁCIA DÁT NA VONKAJŠEJ PAMÄTI, B-STROMY A ICH VARIANTY

LOGICKÝ ZÁZNAM, TYP ZÁZNAMU $\{A_1 : D_1, \ldots, A_n : D_n\}$ — MENO ATR.: $D_i = dom(A_i)$ DOMÉNA (ATRIBÚT)

HOMOGÉNNY SÚBOR: $S(A_1 : D_1, \ldots, A_n : D_n)$

[**NEHOMOGÉNNY SÚBOR** (HROMADA, HEAP)]

AK MÁ HOM. SÚBOR RÔZNE ZÁZNAMY $\Rightarrow$ **KĽÚČ** $K = \{A_{j_1}, \ldots A_{j_k}\}$

+ **VYHĽADÁVACÍ KĽÚČ** – JE MOŽNÉ PODĽA NEHO HĽADAŤ ZÁZNAMY
(1) HODNOTOVÝ, (2) HAŠOVANÝ, (3) RELATÍVNY

FYZICKÝ ZÁZNAM .. R BYTE (PREDPOKLADÁME R = konšt.)

FYZICKÁ STRÁNKA = **BLOK** (JEDNOTKA PRENOSU RAM $\Leftrightarrow$ DISK)
[VÄČŠINOU NÁSOBOK SEKTORU] .. B BYTE

$b = \frac{B}{R}$ **BLOKOVACÍ FAKTOR**

ZÁZNAMY $\begin{cases} \text{BLOKOVANÉ} & b > 1 \\ \text{NEBLOKOVANÉ} & b = 1 \\ \text{PRERASTENÉ} & b < 1 \end{cases}$

SCHÉMA ORGANIZÁCIE SÚBORU (SOS) = $\frac{\text{PAMÄŤ.}}{\text{ŠTRUKT.}}$ + $\frac{\text{ALGORITMY}}{\text{OPERÁCIÍ}}$

PRIMÁRNY SÚBOR = NESIE UŽIV. DATA, N ZÁZNAMOV

CIEĽ NÁVRHU SOS: MINIMALIZOVAŤ # OP. S LOG. STRÁNKAMI

VYVÁŽENOSŤ ŠTRUKTÚRY:
(a) OHRANIČENIE DĹŽKY CESTY V ŠTRUKTÚRE
(b) ROVNOMERNÁ NAPLNENOSŤ LOG. STRÁNOK

SOS $\begin{cases} \text{STATICKÉ} \\ \text{DYNAMICKÉ (SPĹŇAJÚ (a) AJ (b))} \end{cases}$

SÉRIOVÉ ČÍTANIE – USPORIAD. PODĽA VYHĽ. KĽÚČA

SEKVENČNÉ ČÍTANIE – DANÉ IMPLEMENTÁCIOU

VONKAJŠIA PAMÄŤ

MAGNETICKÁ PÁSKA - SEKVENČNOSŤ,

KAPACITA(C=1600BYTE/PALEC), DĹŽKA BLOKU=𝔹, DĹŽKA MEDZIBLOK. MEDZERY=IBG, MUSÍME U= 𝔹/(𝔹+IBG)

𝔹 = B/C, TJ. AK B=2400BYTE, POTOM 𝔹=1,5 PALCA

MAGNETICKÝ DISK - PRIAMY PRÍSTUP

STOPA = KRUŽNICA NA 1 POVRCHU

CYLINDER = ∀ STOPY O ROVNAKOM PRIEMERE

s (SEEK) - PRIEM. ČAS PRESUNU RAMIENKA (VYSTAVOVACIA DOBA)

r (ROTATIONAL DELAY / LATENCY) - ½ ČASU OTÁČKY DISKU

btt (BLOCK TRANSFER TIME) - ČAS PRENOSU BLOKU PO ZBERNICI

DÁ SA ODVODIŤ Z PRENOS. RÝCHLOSTI t A Z B

ZÓNOVÉ UKLADANIE - CYLINDRY SÚ ROZDELENÉ DO ZÓN S RÔZNYM POČTOM SEKTOROV

rpm (ROTATION PER MINUTE) - 7200 rpm, 10 000 rpm

ROZHRANIA: PATA, SATA, SCSI

RAID: REDUNDANT ARRAY OF INEXPENSIVE DISKS

OPTICKÉ DISKY, JUKEBOXY, FLASH

STATICKÉ METÓDY ORGANIZÁCIE SÚBOROV

NESPĹŇAJÚ PODMIENKY MYVÁŽENOSTI ŠTRUKTÚRY SOS

OPERÁCIE: INSERT, DELETE, UPDATE, FETCH + REORGANIZATION

HROMADA
USPORIADANÝ SEKVENČNÝ SÚBOR
INDEX SEKVENČNÝ SÚBOR
INDEXOVANÝ SÚBOR
INVERTOVANÝ (INDEXOVANÝ V DBS)
SÚBOR S PRIAMYM PRÍSTUPOM

02.09.2008 Tu
PETER ČERNO

ŠTÁTNICE

USPORIADANÝ SEKVENČNÝ SÚBOR

ZÁZNAMY USPORIADANÉ PODĽA KĽÚČA, AKTUALIZOVANÉ ZÁZNAMY SA VLOŽIA DO ZVLÁŠTNEHO SÚBORU (SÚBOR AKTUALIZÁCIÍ (TRANSAKCIÍ)) A AŽ PRI REORGANIZATIONI SÚ PRIDANÉ DO PRIMÁRNEHO

PRE MÉDIA S PRIAMYM PRÍSTUPOM: $T_{FETCH} = \lceil \log_2(N/\lfloor b \rfloor) \rceil \cdot (s+r+btt)$

INDEXSEKVENČNÝ SÚBOR

PRIMÁRNY SEKVENČNÝ SÚBOR + OBLASŤ PRETEČENIA

ÚROVNE INDEXU 1..x, ÚROVEŇ 0 = BLOKY PRIM. SÚBORU

INDEX ÚROVNE j OBSAHUJE BLOKY SO ZOTRIEDENÝMI ZÁZNAMAMI (K, s_K), KDE s_K JE UKAZATEĽ NA BLOK (j-1)-TEJ ÚROVNE, KT. PRVÝ ZÁZNAM MÁ KĽÚČ K.

X-TÁ ÚROVEŇ - 1 BLOK = HLAVNÝ INDEX (MASTER)

$x = \lceil \log_p(N/\lfloor b \rfloor) \rceil$, KDE $p = \lfloor B/(V+P) \rfloor$

VEĽKOSŤ KĽÚČA ↑ ↑ VEĽKOSŤ s_K

OBLASŤ PRETEČENIA: NOVÉ ZÁZNAMY SA REŤAZIA ZA SEBA V OBLASTI PRETEČENIA (KAŽDÝ Z NICH MÁ POINTER NA ĎALŠÍ ZÁZNAM)

INDEXOVANÝ SÚBOR

PRIMÁRNY SÚBOR + INDEXY (NEINDEXUJÚ SA BLOKY, ALE ZÁZNAMY)

1. ÚROVEŇ INDEXU: ZOTRIEDENÉ ZÁZNAMY (IBA KĽÚČ, MHL.) + ODKAZY DO PRIMÁRNEHO SÚBORU (N ZÁZNAMOV)

OSTATNÉ ÚROVNE INDEXU: (K, s_K), s_K = BLOK NIŽŠEJ ÚROVNE INDEXU, K JE PRVÝ ZÁZNAM TOHTO BLOKU

CLUSTEROVANÝ INDEX - ZÁZNAMY S PODOBNOU HODNOTOU INDEX. ATRIBÚTU SÚ BLÍZKO SEBA V PRIM. SÚBORE (MAX 1)

BITOVÉ MAPY - PRE ATRIBÚTY S MALOU DOMÉNOU

SÚBOR S PRIAMYM PRÍSTUPOM

UVAŽUJME $B=R$, t.j. $b=1$

PRIMÁRNE ZÁZNAMY SÚ ROZPTÝLENÉ V PAMÄŤOVOM PRIESTORE $M*R$, $M \geq N$

HASH. FUNKCIA $h: K^* \to \{0,\dots,M-1\}$

FAKTOR NAPLNENIA: $\lambda = N/M$

PRI HASHOVANÍ S LINEÁRNYM PREHĽADÁVANÍM JE OČAKÁVANÁ VEĽKOSŤ REŤAZCA KOLÍZIÍ $EL = 1/(1-\lambda)$

TRIEDENIA NA VONKAJŠEJ PAMÄTI

TRIEDENIE ZLIEVANÍM (MERGESORT)

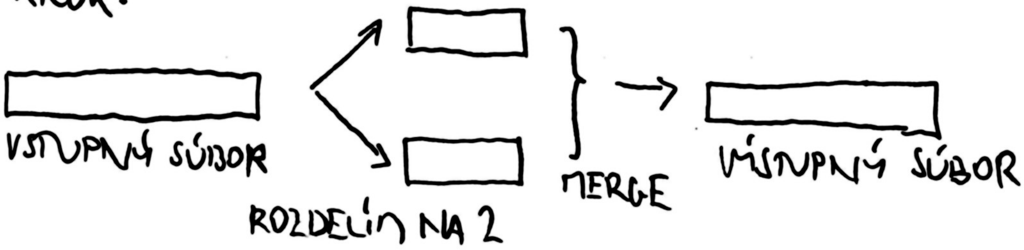
n-CESTNÉ TRIEDENIE

TRIEDENIE MAX d-HALDOU $(i \mapsto d(i-1)+2,\dots,d\cdot i+1)$

VYTVÁRANIE DLHÝCH BEHOV POMOCOU DVOJITEJ HALDY

TRIEDENIE ZLIEVANÍM

1 KROK:



V 1. KROKU ZÍSKAM USP. POSTUPNOSTI DĹŽKY 2

V KAŽDOM ĎALŠOM SA DĹŽKA USP. POST. ZDVOJNÁSOBÍ

$\Rightarrow \lceil \log n \rceil$ KROKOV

VYLEPŠENIE: STRIEDAVÉ ZAPISOVANIE VÝSTUPU DO 2 SÚBOROV

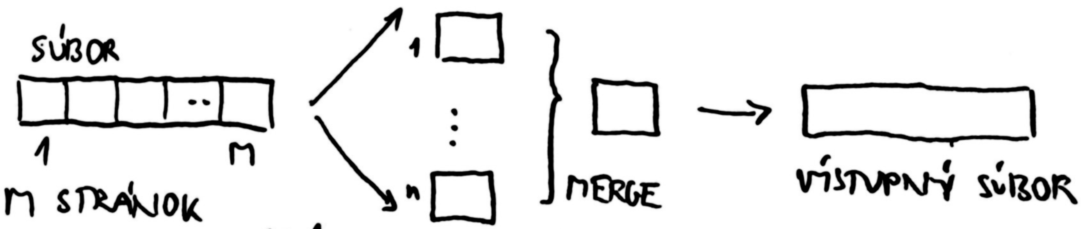
$\Rightarrow$ NEMUSÍM DELIŤ

02.09.2008 Tu
PETER ČERNO

ŠTÁTNICE

n-CESTNÉ TRIEDENIE

K DISPOZÍCII MÁM n+1 STRÁNOK VO VNÚTORNEJ PAMÄTI



V 1. KROKU NAČÍTAM n STRÁNOK

- V ĎALŠÍCH KROKOCH ZLIEVAŤ VŽDY <u>n NAJKRATŠÍCH BEHOV</u>

$O(2M \lceil \log_n M/n \rceil)$

DVOJITÁ HALDA

V PAMÄTI UDRŽUJEM 2 HALDY (n PRVKOV) V POLI $A[1..n]$

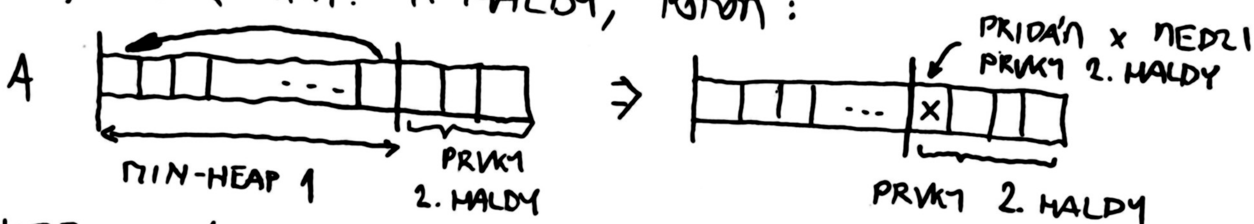
NAJSKÔR NAČÍTAM n PRVKOV A VYTVORÍM MIN-HEAP $\Theta(n)$

V KAŽDOM ĎALŠOM KROKU:

1. ZAPÍŠEM MIN. PRVOK 1. HALDY NA VÝSTUP
2. NAČÍTAM ĎALŠÍ PRVOK x VSTUPNÉHO SÚBORU

a) $x \geq$ min. 1. HALDY, POTOM
PREPÍŠEM TÝMTO PRVKOM KOREŇ 1. HALDY
A NECHÁM HO PREBUBLAŤ SMEROM DOLU

b) $x <$ min. 1. HALDY, POTOM:



!! KEĎ SA 1. HALDA VYČERPÁ, ZOSTANÚ MI V POLI A UŽ IBA PRVKY 2. HALDY ⇒ VYTVORÍM MIN-HEAP $\Theta(n)$ A ZAČNEM NOVÝ BEH.

V NAJHORŠOM PRÍPADE ALG. DÁVA ROVNAKÚ VEĽKOSŤ BEHOV AKO OBYČAJNÁ HALDA, V PRIEM. JE 2x LEPŠÍ.

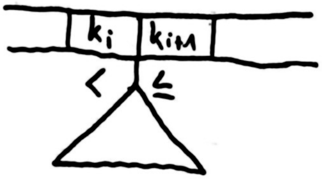
B-STROMY

B-STROM RÁDU m JE VÝŠKOVO VYVÁŽENÝ STROM:

(1) KOREŇ MÁ ASPOŇ 1 ZÁZNAM (2 POTOMKOV)

(2) VNÚTORNÝ UZOL MÁ $\lceil m/2 \rceil$ AŽ m POTOMKOV

(3)



(4) VŠETKY VETVY (OD KOREŇA K LISTOM) SÚ ROVNAKO DLHÉ

REDUNDANTNÝ B-STROM - VŠETKY DATA SÚ ULOŽENÉ V LISTOCH, VNÚT. UZLY (A KOREŇ) OBSAHUJÚ IBA VYHĽADÁVACIE KĽÚČE

OPERÁCIE:

SEARCH - JEDNODUCHÝ PRIECHOD DO HĹBKY

INSERT - NÁJDEM MIESTO PRE VLOŽENIE
AK UZOL OBSAHUJE m SYNOV → ŠTIEPIM NA DVA
(TOTO SA MÔŽE PROPAGOVAŤ SMEROM K VYŠŠÍM VRSTVÁM)

DELETE - AK MENEJ AKO $\lceil m/2 \rceil$ SYNOV → MUSÍM PREBERAŤ DATA OD SUSEDNÝCH UZLOV V ZLIEVAŤ

VYLEPŠENIA: VYVAŽOVANIE STRÁNOK, ODLOŽENÉ ŠTIEPENIE (KAŽDÝ LIST MÁ STRÁNKU PRETEČENIA)

B+ STROMY - VŠETKY UZLY NA ROVNAKEJ ÚROVNI SÚ SPOJENÉ DO SPOJOVÉHO ZOZNAMU

B* STROMY -

(2) VNÚTORNÝ UZOL MÁ $\lceil (2m-1)/3 \rceil$ AŽ m POTOMKOV

ŠTIEPIA SA 2 LISTY DO 3 ALEBO 3 DO 4 (PRI VKLADANÍ)

PODOBNE ZLIEVAJÚ SA 3 UZLY DO 2 ALEBO 4 DO 3 (DELETE)

02.09.2008 Tu
PETER ČERNO

ŠTÁTNICE

PREFIXOVÉ STROMY (TRIE)

REDUNDANTNÝ STROM, DATA SÚ KĽÚČOVANÉ REŤAZCAMI A SÚ ULOŽENÉ V LISTOCH

VYHĽADÁVACIE KĽÚČE SÚ VŽDY ČO NAJKRATŠIE MOŽNÉ PREFIXY REŤAZCOV NUTNÉ K ODLÍŠENIU UZLOV

STROMY S PREMENNOU DĹŽKOU ZÁZNAMU

- LISTY SA NEŠTIEPIA PODĽA POČTU ZÁZNAMOV, ALE ZHRUBA NA POLOVICU

(2) CELKOVÁ DĹŽKA ZÁZNAMOV V UZLE JE $\lceil B/2 \rceil$ AŽ B

PROBLÉMY: TENDENCIA DLHŠÍCH ZÁZNAMOV STÚPAŤ AŽ KU KORENI

PRI VKLADANÍ MÔŽE DÔJSŤ K ŠTIEPENIU NA 3 STRÁNKY

MÔŽE DÔJSŤ K ZMENŠENIU STROMU AJ PRI VKLADANÍ

VIACROZMERNÉ B-STROMY

- POUŽÍVAJÚ SA, KEĎ JE NUTNÉ HĽADAŤ ZÁZNAMY PODĽA VIAC ATRIBÚTOV

PRE 1. ATRIBÚT JE POTREBNÝ 1 STROM

V ŇOM JE PRE KAŽDÝ KĽÚČ ODKAZ NA CELÝ STROM 2. ATRIBÚTU, ... ATĎ.

STROMY ROVNAKÉHO ATRIBÚTU SÚ V SPOJOVOM ZOZNAME

5 ARCHITEKTÚRY POČÍTAČOV A SIETÍ

5.1 ARCHITEKTÚRY POČÍTAČOV
5.2 PROCESORY, MULTIPROCESORY
5.3 I/O ZARIADENIA, UKLADANIE A PRENOS DÁT
5.4 ARCHITEKTÚRY OS
5.5 PROCESY, VLÁKNA, PLÁNOVANIE
5.6 SYNCHRONIZAČNÉ PRIMITÍVA, VZÁJOMNÉ VYLÚČENIE
5.7 ZABLOKOVANIE A ZOTAVENIE SA Z NEHO
5.8 ORGANIZÁCIA PAMÄTI, ALOKAČNÉ ALGORITMY
5.9 PRINCÍPY VIRTUÁLNEJ PAMÄTI, STRÁNKOVANIE
5.10 SYSTÉMY SÚBOROV, STRÁNKOVANIE
5.11 BEZPEČNOSŤ, AUTENTIFIKÁCIA, AUTORIZÁCIA, PRÍST. PRÁVA
5.12 ISO/OSI VRSTEVNATÁ ARCHITEKTÚRA
5.13 TCP/IP
5.14 SPOJOVANÉ / NESPOJOVANÉ SLUŽBY, SPOĽAHLIVOSŤ, ZABEZPEČENIE PROTOKOLOV

03.08.2008
PETER ČERNO

ŠTÁTNICE

5.1 ARCHITEKTÚRY POČÍTAČOV

COMPUTER ARCHITECTURE = ATRIBÚTY SYSTÉMU VIDITEĽNÉ PROGRAMÁTOROM, MAJÚ VPLYV NA LOGICKÉ VYKONÁVANIE PROGRAMU

COMPUTER ORGANIZATION = HW DETAILY NEVIDITEĽNÉ PRE PROGRAMÁTORA

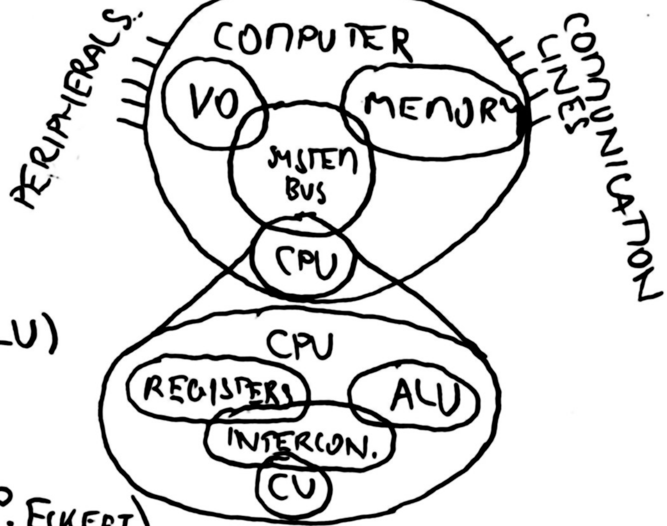
HIERARCHICKÝ SYSTÉM - NA KAŽDEJ ÚROVNI POZOSTÁVA Z KOMPONENT A ICH VZÁJOMNÝCH VZŤAHOV

- ŠTRUKTÚRA - SPÔSOB PREPOJENIA KOMPONENT
- FUNKCIA - OPERÁCIE KAŽDEJ KOMPONENTY

FUNKCIE POČÍTAČA: DATA PROCESSING, STORAGE, MOVEMENT, CONTROL

ŠTRUKTÚRA POČÍTAČA:

- CENTRAL PROCESSING UNIT (CPU)
- MAIN MEMORY
- I/O (INPUT / OUTPUT)
- SYSTEM INTERCONNECTIONS



CPU: CONTROL UNIT (CU)

- ARITHMETIC AND LOGIC UNIT (ALU)
- REGISTERS
- CPU INTERCONNECTION

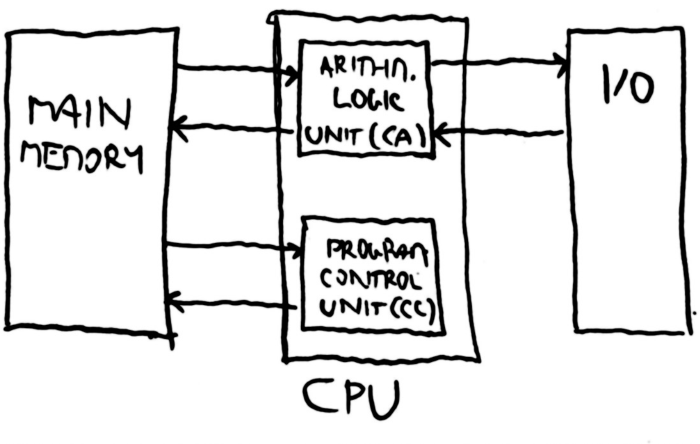
PRVÝ POČÍTAČ: ENIAC 1946 (J. MAUCHLY, J.P. ECKERT)

VON NEUMANN MACHINE

[INSTITUTE FOR ADVANCED STUDIES, PRINCETON]

STORED-PROGRAM CONCEPT, IAS COMPUTER

PROTOTYP VŠETKÝCH SÚČASNÝCH GENERAL-PURPOSE COMPUTERS



MAIN MEMORY UKLADÁ DATA AJ INŠTRUKCIE

ALU OPERUJE NA BIN. DÁTACH

CU INTERPRETUJE A VYKONÁVA INŠTRUKCIE

NIEKTORÉ DÔLEŽITÉ REGISTRE

PROGRAM COUNTER (PC) - OBSAHUJE ADRESU ĎALŠEJ INŠTRUKCIE

INSTRUCTION REGISTER (IR) - KÓD VYKONÁVANEJ INŠTR.

STACK POINTER (SP) - UKAZATEĽ NA VRCHOL ZÁSOBNÍKU

MEMORY ADDRESS REGISTER (MAR) - ADRESA DO OP. PAMÄTI

MEMORY BUFFER REGISTER (MBR) - SLOVO ČÍT./ZAP. DO PAMÄTI

HARVARDSKÁ ARCHITEKTÚRA

2 DRUHY PAMÄTÍ - INŠTRUKCIE A DATA

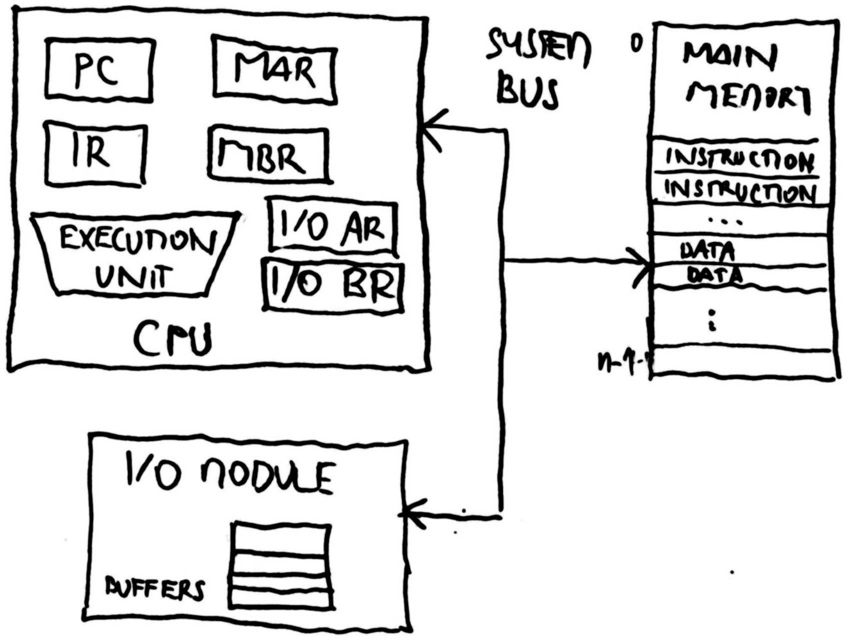
PRÍKLAD: DSP PROCESORY, MIKROKONTROLÉRY

HISTÓRIA

1. GENERÁCIA (VACUUM TUBES - ELEKTRÓNKY): ENIAC
2. GEN. (TRANSISTORS): IBM 7094
3. GEN. (INTEGRATED CIRCUITS): IBM SYSTEM /360, DEC PDP-8

MOOROV ZÁKON (GORDON MOORE, SPOLUZAKLADATEĽ INTELU)
POČET TRANZISTOROV NA 1 ČIPE SA KAŽDÝM ROKOM ZDVOJNÁSOBÍ (NESKÔR KAŽDÝCH 18 MESIACOV)

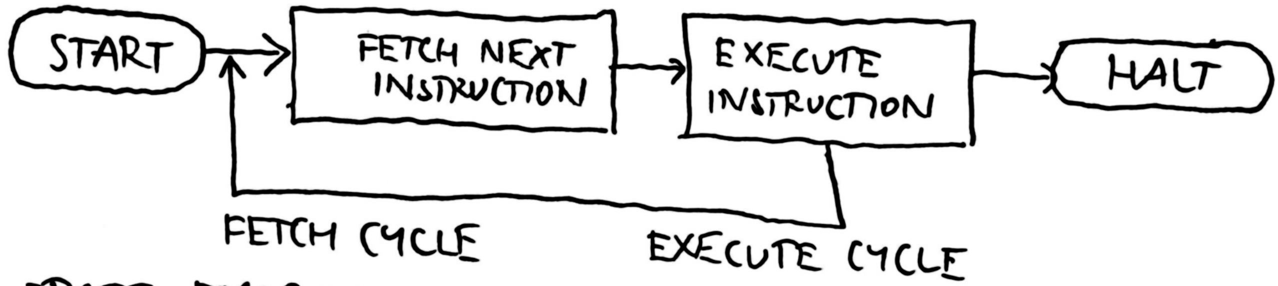
COMPUTER COMPONENTS (TOP-LEVEL VIEW)



03.09.2008 We
PETER ČERNO

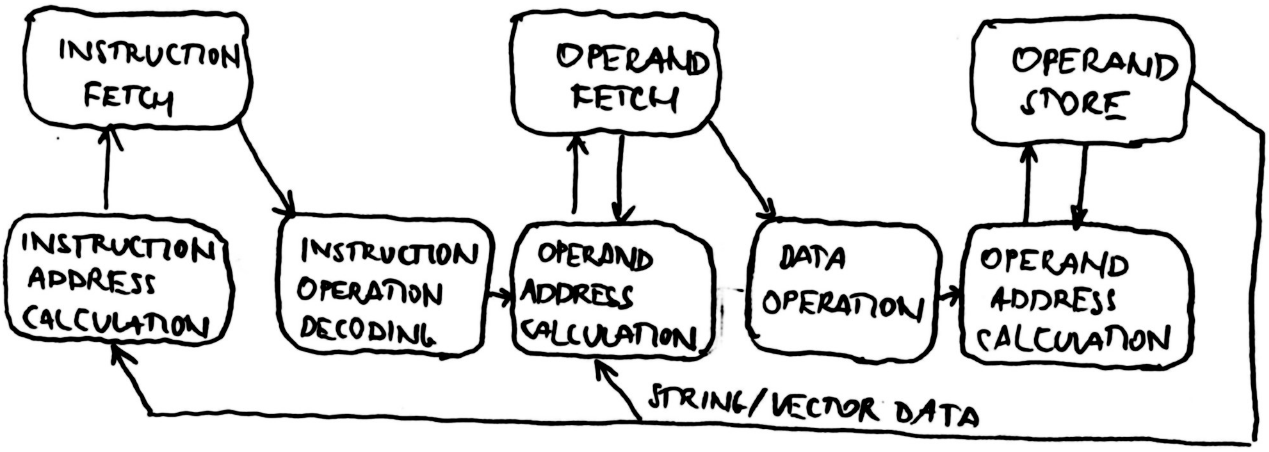
STÁTNICE

ZÁKLADNÝ INSTRUCTION CYCLE



STATE DIAGRAM

- FETCH → DECODE → LOAD → EXECUTE → STORE



PRERUŠENIA (INTERRUPTS)

- PROGRAM / TIMER / IO / HARDWARE FAILURE

  JE NUTNÉ PRIDAŤ INTERRUPT CYCLE DO INSTRUCTION CYCLE

PRERUŠENIE: (1) SUSPENDUJE VYKONÁVANIE AKTUÁLNEHO PROGRAMU, ULOŽÍ JEHO KONTEXT
(2) NASTAVÍ ADRESU PC NA OBSLUHU PRERUŠENIA (INTERRUPT HANDLER)

BUS (ZBERNICA)

SPÁJA 2 ALEBO VIAC ZARIADENÍ, JE ZDIEĽANÁ

BUS { DATA BUS
ADDRESS LINES
CONTROL LINES (MEMORY WRITE, MEMORY READ, I/O WRITE, I/O READ, TRANSFER ACK, BUS REQUEST, BUS GRANT, INTERRUPT REQUEST, INTERRUPT ACK, CLOCK, RESET)

PCI (PERIPHERAL COMPONENT INTERCONNECT)
POPULÁRNA HIGH-BANDWIDTH ZBERNICA

ORGANIZÁCIA POČÍTAČA

VIAC-ÚROVŇOVÁ

L_0 (MIKROPROGRAMOVÁ) - TECHNICKÉ VYBAVENIE PC (NAD 0,1)
L_1 (STROJOVÝ JAZYK PC) - VIRTUÁLNY STROJ NAD HW RIEŠENÍM
L_2 (ÚROVEŇ OPERAČNÉHO SYSTÉMU) -
DOPLNENIE L_1 O SÚBOR MAKROINŠTR., NOVÁ ORGAN. PAMÄTI
L_3 (ÚROVEŇ ASSEMBLERU) - NAJNIŽŠÍ ĽUDSKY ORIENT. JAZYK
L_4 (ÚROVEŇ VYŠŠÍCH PROG. JAZYKOV)
L_5 (ÚROVEŇ APLIKAČNÝCH PROGRAMOV)

ARCHITEKTÚRA - POHĽAD PROGRAMÁTORA

1. ZÁKL. DATOVÉ ŠTRUKTÚRY, REPREZENTÁCIA DÁT
2. ADRESOVÉ KONVENCIE
3. INŠTRUKČNÝ SÚBOR, REGISTROVÝ MODEL
4. RIADENIE CHODU, STAV PC
5. VSTUPY / VÝSTUPY

03.09.2008
PETER ČERNO

ŠTÁTNICE

ARCHITEKTÚRA - POHĽAD NÁVRHÁRA

1. ŠÍRKA DATOVÝCH CIEST
2. STUPEŇ ZDIEĽANIA
3. DEF. ŠPEC. JEDNOTIEK
4. PARALELIZMY
5. ORGANIZÁCIA PAMÄTI A I/O
6. STUPEŇ PREDIKCIE

BIG ENDIAN : MOST SIGNIFICANT BYTE AT LOWEST ADDR.
LITTLE ENDIAN : LEAST SIGN. BYTE AT LOWEST ADDR.

5.2 PROCESORY, MULTIPROCESORY

CPU : REGISTERS, CONTROL UNIT, ALU, [FPU]
+ CACHE, VIAC JADIER, SoC (SYSTEM ON CHIP)

DELENIE PODĽA INŠTRUKČNEJ SADY

CISC (COMPLEX INSTRUCTION SET COMPUTER)
ROZSIAHLA INŠTR. SADA, RÔZNE VARIANTY INŠTR.
x86 - ROZKLADÁ ZLOŽITÉ INŠTR. NA MICRO-OPERATIONS

RISC (REDUCED INSTRUCTION SET COMPUTER)
NAPR. SPARC, ARM

POST-RISC : SPOJENIE RISCOVÝCH VLASTNOSTÍ S TECH. ZVÝŠENIA VÝKONU (OUT-OF-ORDER EXEC., PARALELIZMUS)

VLIW (VERY LONG INSTRUCTION WORD) -
VYKONÁVA OPERÁCIE PARALELNE NA ZÁKLADE FIXNÉHO ROZVRHU, KT. JE URČENÝ PRI KOMPILÁCII

EPIC (EXPLICITLY PARALLEL INSTRUCTION COMPUTING) -
= INDEPENDENCE ARCHITECTURE,
INTEL'S IA-64 ARCH., ITANIUM, ITANIUM 2
CIEĽ : ZVÝŠIŤ SCHOPNOSŤ MIKROPROCESOROV VYKONÁVAŤ INŠTR. PARALELNE, POUŽITÍM KOMPILÁTORA

ORTOGONÁLNA INŠTRUKČNÁ SADA : ŽIADNA INŠTRUKCIA NEPREDPOKLADÁ IMPLICITNÉ POUŽITIE NIEKTORÝCH REGISTROV

TECHNIKY PRE ZVÝŠENIE VÝKONU

NAJJEDNODUCHŠÍ CPU - NON-PIPELINED SCALAR ARCHITECTURE

PARALELIZMUS V PROCESOROCH:

(1) INSTRUCTION LEVEL PARALLELISM

(2) THREAD LEVEL PARALLELISM

INSTRUCTION PIPELINING

ROZDELENIE SPRACOVANIA INŠTR. NA VIAC MENŠÍCH KROKOV

SUPERSCALARITA

SUPERSCALAR DESIGN - DLHÁ INŠTRUKČNÁ PIPELINE
VIAC IDENTICKÝCH EXECUTION JEDNOTIEK

OUT-OF-ORDER EXECUTION

ZARADENIE INŠTRUKCIE DO INŠTR. POOL → VYBERIE SA INŠTR. A VYKONÁ SA VO SVOJEJ EXECUTION JEDN. → VÝSLEDKY SA UCHOVÁVAJÚ VO FRONTE REORDER BUFFER

PREDIKCIA SKOKOV

DYNAMICKÁ PREDIKCIA SKOKOV, HEURISTIKY, PREKLADAČ ODHADNE PRAVDEPODOBNOSŤ SKOKU

ŠPEKULATÍVNE VYKONÁVANIE KÓDU

DATA PARALELISM

SIMD INŠTRUKCIE, VEKTOROVÉ PROCESORY

03.09.2008 We
PETER ČERNO

ŠTÁTNICE

MULTIPROCESORY

JE POUŽITÝCH VIAC CPU V RÁMCI 1 SYSTÉMU

SIMD (SINGLE-INSTRUCTION, MULTIPLE-DATA) : VECTOR PROCESSING

MISD - REDUNDANCIA VO FAIL-SAFE SYSTÉMOCH

MIMD -

SYMETRIA { SMP (SYMMETRIC MULTIPROCESSING SYSTEMS)
ASMP (ASYMMETRIC —||—)
NUMA (NON UNIFORM MEMORY ACCESS)
CLUSTERED MULTIPROCESSING

TESNOSŤ SPOJENIA MULTIPROCESOROV :

TIGHTLY COUPLED - MULTIPLE CPUs CONN. AT THE BUS LEVEL

CHIP MULTIPROCESSORS - MULTI-CORE COMPUTING

LOOSELY-COUPLED - CLUSTERS, VIAC STANDALONE PROCESOROV, SPOJENÝCH CEZ VYSOKORÝCHLOSTNÝ KOMUNIKAČNÝ SYSTÉM (GIGABIT ETHERNET)

5.3 VSTUPNO/VÝSTUPNÉ ZARIADENIA

MOŽNO K NIM PRISTUPOVAŤ POMOCOU < PORTOV / PAMÄŤOVÝM MAPOVANÍM

CHARAKTERISTIKY

DRUH (BLOKOVÉ / ZNAKOVÉ)
PRÍSTUP (SEKVENČNÝ / NÁHODNÝ)
KOMUNIKÁCIA (SYNCHRÓNNA / ASYNCHRÓNNA)
ZDIEĽANIE (PREEMPTÍVNE / VYHRADENÉ - SPOOLING)
RÝCHLOSŤ
SMER DÁT - R/W, R/O, W/O

PRENOS DÁT MEDZI ZARIADENÍM A CPU

POLLING - AKTÍVNE ČAKANIE NA ZMENU.
PRERUŠENIE - ASYNCHRÓNNE PRERUŠENIE OD ZARIADENIA
DMA (DIRECT MEMORY ACCESS)

CIELE I/O SOFTWARE

NEZÁVISLOSŤ ZARIADENIA,
JEDNOTNÉ POMENOVANIE,
OBSLUHA CHÝB

5.4 ARCHITEKTÚRY OS

MONOLITICKÝ SYSTÉM

NAJSTARŠÍ (IBM360, UNIX, WIN)
∀ SLUŽBY VO VNÚTRI VYKONÁVANÉ V CHRÁNENOM MÓDE
NEVÝHODY: HORŠIA ÚDRŽBA, ROZŠIROVANIE ZA BEHU KOMPLIKOV.

VIRTUÁLNE STROJE   NAPR. VM PRE IBM360

NAD HW VRSTVA VM - VYTVÁRA PRE PROCESY ILÚZIU HOLÉHO HW
DNES: DEFINUJÚ ABSTRAKTNÝ STROJ (.NET CLR, JAVA VM)

MIKROJADRO

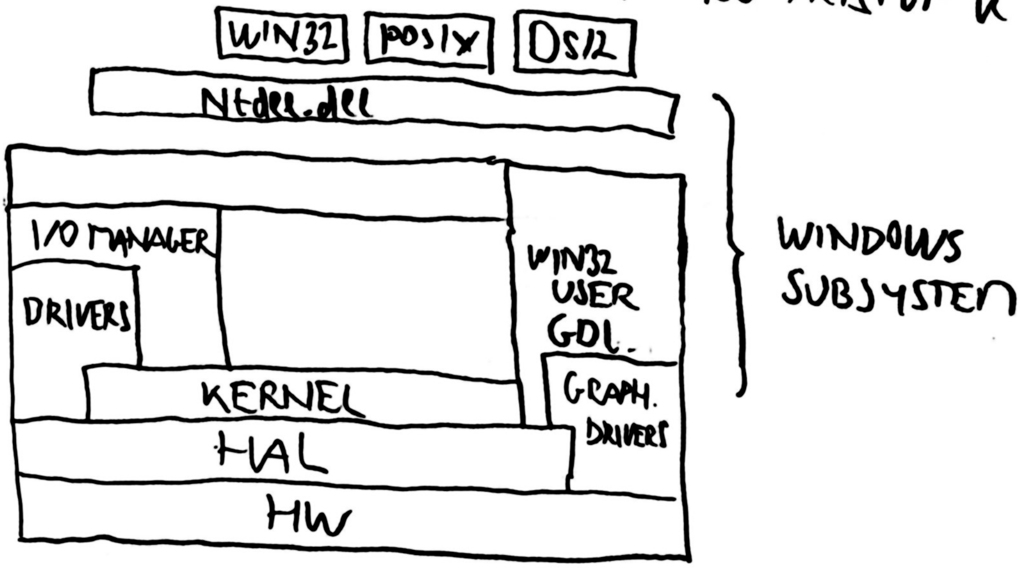
CIEĽ: ČO NAJMENŠIE JADRO, EXPERIMENTÁLNE,
VEĽA PROCESOV (NAPR. AJ FILESYSTEM), MODULOV..
KOMUNIKÁCIA KLIENT / SERVER
JEDINÝ KOMERČNÝ OS: CHORUS (ÚSPEŠNE)

03.09.2008 We
PETER ČERNO

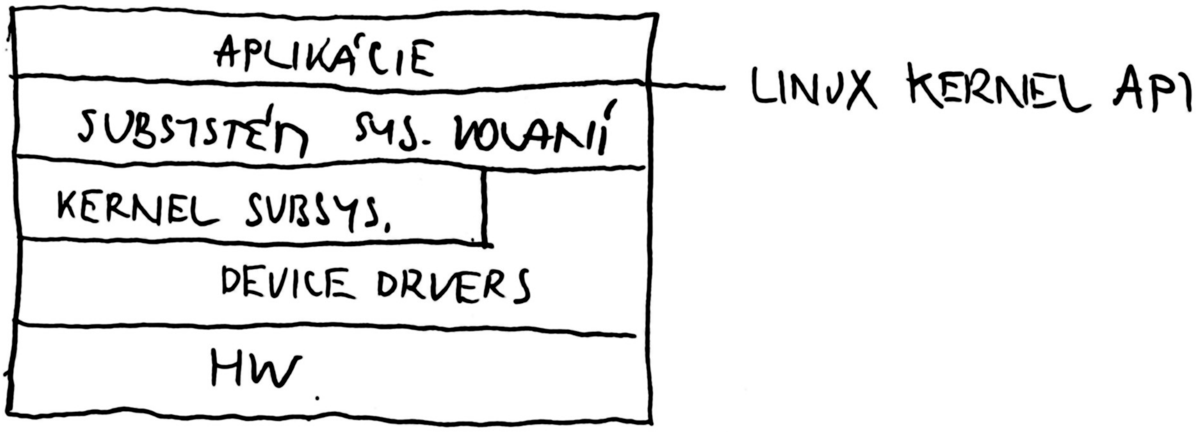
ŠTÁTNICE

ARCHITEKTÚRA WIN NT

- JADRO MALÉ (CCA 1MB), NEUTRÁLNE VZHĽADOM K VYŠŠÍM VRSTVÁM
  MOŽNO NAD NIM VYBUDOVAŤ RÔZNE SYSTÉMY (WIN, POSIX, OS/2)
- ROZHRANIE OS A UŽÍV. PROGRAMOV – WINAPI,
  NAD NIM SA NACHÁDZAJÚ RÔZNE DLL
- MEDZI KERNELOM A HW JE HAL (HARDWARE ABSTRACTION LAYER) → KERNEL MOŽNO UPRAVIŤ ĽAHKO NA INÉ ARCHITEKTÚRY
- JEDINE GRAFICKÉ DRIVERY MAJÚ PRÍSTUP K HW



ARCHITEKTÚRA LINUXU



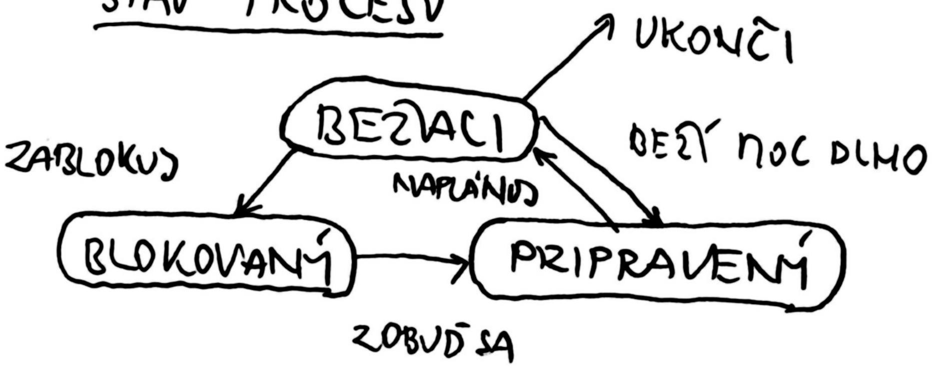
5.5 PROCESY, VLÁKNA, PLÁNOVANIE

PROCES - SPUSTENÝ PROGRAM,
MÁ PAMÄŤ, PROSTRIEDKY, PRÁVA, ID (PID), SIGNÁLY

VLÁKNO (THREAD) - MIESTO VYKONÁVANIA
INŠTRUKCIÍ V PAMÄTI
HODNOTA PROG. ČÍTAČA (PC), STAV REGISTROV, ZÁSOBNÍK

OPROTI WINDOWS / SOLARIS LINUX NEMÁ PODPORU
PRE VLÁKNA, ALE PROCESY MÔŽU ZDIEĽAŤ PAMÄŤ

STAV PROCESU



PLÁNOVANIE

PLÁNOVAČ (SCHEDULER), PLÁNOVANIE < PREEMPTÍVNE / NEPREEMPTÍVNE

CIELE PLÁNOVANIA:

(1) SPRAVODLIVOSŤ (KAŽDÝ PROCES DOSTANE CPU)
(2) EFEKTÍVNOSŤ (PLNÉ VYŤAŽENIE CPU)
(3) MINIMÁLNA DOBA ODPOVEDE
(4) PRIECHODNOSŤ (MAX. POČET SPRACOVANÝCH PROCESOV)
(5) MINIMÁLNA RÉŽIA SYSTÉMU

03.09.2008 W
PETER ČERNO

ŠTÁTNICE

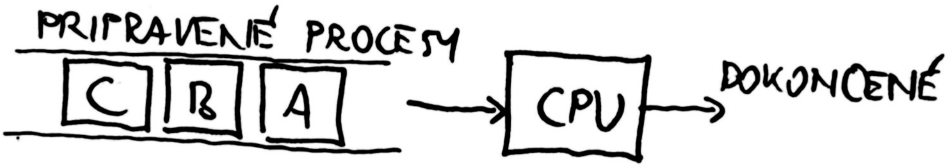
KRITÉRIA PLÁNOVANIA

(1) VIAZANOSŤ PROCESU / VO NA DEDEN CPU
(2) PROCES JE DÁVKOVÝ / INTERAKTÍVNY
(3) PRIORITA PROCESU
(4) VÝPADKY STRÁNOK
(5) KOLKO SKUTOČNÉHO ČASU PROCES OBDRŽAL

PLÁNOVACIE ALGORITMY

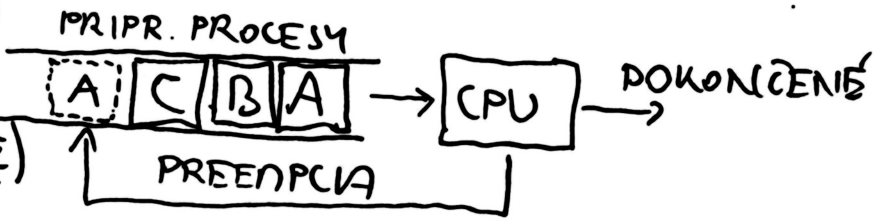
FIFO

NEPREEMPTÍVNE



ROUND ROBIN (RR)

PREEMPTÍVNE,
ČASOVÉ KVANTUM (TIMESLICE)



VIAC FRONT SO SPÄTNOU VÄZBOU

PROCESU Z i-TEJ FRONTY JE PRIDELENÝ PROCESOR, AŽ KEĎ VO FRONTÁCH 1,..., i-1 NIE JE PRIPRAVENÝ ŽIADEN PROCES.

a) AK PROCES SKONČIL I/O OPERÁCIOU, JE BLOKOVANÝ A PRESUNUTÝ DO FRONTY i-1
b) AK PROCES SKONČIL PREEMPCIOU, JE PRIPRAVENÝ A PRESUNUTÝ DO FRONTY i+1

PLÁNOVANIE V SMP (SYMMETRIC MULTIPROC. SYSTEMS)

FRONTA CPU ČAKAJÚCICH NA PRIPRAVENÉ PROCESY
- AKTÍVNE ČAKANIE - SPOTREBOVÁVA ENERGIU
- PASÍVNE ČAKANIE - ŠPECIÁLNE INŠTRUKCIE

AFINITA PROCESOV K CPU

REAL-TIME

OBVYKLE APLIKÁCIA RIADENÁ UDALOSŤAMI
KAŽDÝ TASK MÁ REÁLNY ČAS NA DOKONČENIE
HW PROSTRIEDKY OBVYKLE PREDIMENZOVANÉ

→ HARD REAL-TIME : PREPÁSNUTIE DEADLINU → KRITICKÝ PROBL.
→ SOFT REAL-TIME

PLÁNOVANIE VO WINDOWS:

PLÁNUJE SA NA ÚROVNI VLÁKIEN
PLÁNOVAČ ROZPRESTRENÝ PO CELOM JADRE
PRIORITY: 16 REAL-TIME ÚROVNÍ, 15 PREMENLIVÝCH, 1 SYSTÉMOVÁ
ČASOVÉ KVANTÁ

PLÁNOVANIE V LINUXE:

RUNQUEUE PRE KAŽDÝ CPU
DVE PRIORITNÉ FRONTY (AKTÍVNE, VYČERPANÉ PROCESY)
BITOVÁ MASKA OBSADENOSTI

04. 09. 2008 Th
PETER ČERNO

ŠTÁTNICE

S.6 SYNCHRONIZAČNÉ PRIMITÍVA, VZÁJOMNÉ VYLÚČENIE

INTER PROCESS COMMUNICATION (IPC)

RACE CONDITION - SITUÁCIA KEĎ DVA ALEBO VIAC PROCESOV ČÍTA/ZAPISUJE ZDIELANÉ DATA, A VÝSLEDOK ZÁVISÍ NA TOM AKO SÚ JEDNOTLIVÉ PROCESY NAPLÁNOVANÉ

CRITICAL REGION (SECTION) - ČASŤ PROGRAMU, KDE SA PRISTUPUJE K ZDIELANEJ PAMÄTI

MUTUAL EXCLUSION (VZÁJOMNÉ VYLÚČENIE) - NEJAKÝ SPÔSOB ZABEZPEČENIA PROTI RACE CONDITIONS

PODMIENKY VZÁJOMNÉHO VYLÚČENIA:

(1) ŽIADNE DVA PROCESY NEMÔŽU BYŤ SÚČASNE VO VNÚTRI ICH KRITICKÝCH REGIÓNOV (VYHNUTIE SA RACE CONDITIONS)
(2) NEMÔŽME NIČ PREDPOKLADAŤ O RÝCHLOSTI ALEBO POČTE CPU
(3) ŽIADNY PROCES, KTORÝ JE MIMO KRITICKÝ REGIÓN, NEMÔŽE BLOKOVAŤ OSTATNÉ PROCESY
(4) ŽIADNY PROCES BY NEMAL ČAKAŤ DONEKONEČNA NA VSTÚPENIE DO KRITICKEJ SEKCIE

VZÁJOMNÉ VYLÚČENIE POMOCOU AKTÍVNEHO ČAKANIA [BUSY WAITING]

1. ZAKÁZANIE PRERUŠENÍ (DISABLING INTERRUPTS)

KAŽDÝ PROCES ZAKÁŽE PRERUŠENIA HNEĎ AKO VSTÚPI DO KRITICKEJ SEKCIE, A PO OPUSTENÍ ICH ZNOVU POVOLÍ

POUŽÍVA SA V KERNELI OS

2. LOCK VARIABLES

```
while (TRUE) {
  noncritical_section();
  while (lock != 0);
  lock = 1; (*)
  critical_section();
  lock = 0;
}
```

NEFUNKČNÉ RIEŠENIE

MÔŽE NASTAŤ RACE CONDITION: STAČÍ AK JE PROCES V TOMTO BODE PREPLÁNOVANÝ

3. STRICT ALTERNATION (DÔSLEDNÉ STRIEDANIE)

```
while (TRUE) {
   while (turn != 0);
   critical_region();
   turn = 1
   noncritical_region();
}
```

(a)

```
while (TRUE) {
   while (turn != 1);
   critical_region(),
   turn = 0;
   noncritical_region(),
}
```

(b)

LOCK, KTORÝ POUŽÍVA AKTÍVNE ČAKANIE SA NAZÝVA SPIN LOCK

PROBLÉM: PORUŠENIE BODU (3) - MÔŽE SA STAŤ, ŽE PROCES (a) JE BLOKOVANÝ, ZATIAĽ ČO (b) SA NACHÁDZA V NEKRITICKEJ OBLASTI

V TOMTO RIEŠENÍ UŽ ALE NEDÔJDE K RACE CONDITION

4. PETERSNOVE RIEŠENIE

```
int turn;                 NA ZAČIATKU = 0
int interested[N];        N=2, NA ZAČIATKU NULOVÉ POLE
```

```
void enter_region (int proc) {
   int other;
   other = 1 - proc;
   interested [proc] = TRUE;
   turn = proc;
   while (turn == proc &&
     interested [other] == TRUE);
}
```

```
void leave_region (int proc) {
   interested [proc] = FALSE;
}
```

04.09.2008 Th
PETER ČERNO

ŠTÁTNICE

PRED VSTUPOM DO KRITICKÉHO REGIÓNU PROCES ZAVOLÁ enter_region SO SVOJÍM VLASTNÝM ČÍSLOM TOTO VOLANIE DONÚTI PROCES ČAKAŤ, AK JE TO NUTNÉ NA KONCI KR. REG. PROCES ZAVOLÁ leave_region

AK OBA PROCESY ZAVOLAJÚ SIMULTÁNNE enter_region, POTOM BUDE ČAKAŤ TEN PROCES, KTORÝ AKO POSLEDNÝ VYKONÁ OP. turn = proc.

5. TSL INŠTRUKCIA (TEST AND SET LOCK)

VÄČŠINA POČÍTAČOV, NAJMÄ TIE S VIAC PROCESORMI, MAJÚ NASLEDUJÚCU INŠTRUKCIU:

TSL RX, LOCK

PREČÍTA OBSAH PAMÄŤOVÉHO SLOVA LOCK DO REGISTRU RX A ULOŽÍ NENULOVÚ HODNOTU NA PAMÄŤOVÉ MIESTO LOCK. TÁTO INŠTRUKCIA JE NEDELITEĽNÁ, CPU VYKONÁVAJÚCI TSL INŠTRUKCIU ZABLOKUJE MEMORY BUS.

POUŽIJEME ZDIEĽANÚ PREMENNÚ LOCK NA KOORDINÁCIU PRÍSTUPU DO ZDIEĽANEJ PAMÄTI

AK LOCK == 0, AKÝKOĽVEK PROCES MÔŽE NASTAVIŤ LOCK NA 1 A VSTÚPIŤ DO KRITICKEJ SEKCIE. PO OPUSTENÍ KR. SEK. MUSÍ NASTAVIŤ LOCK NA 0.

```
enter_region:
    TSL  RX, LOCK
    CMP  RX, #0
    JNE  enter_region
    RET

leave_region:
    MOV  LOCK, #0
    RET
```

PRIORITY INVERSION PROBLEM - VZNIKÁ PRI BUSY WAITING, KEĎ PROCES S VYSOKOU PRIORITOU AKTÍVNE ČAKÁ, KDEŽTO PROCES S NIŽŠOU PRIORITOU JE V KRITICKEJ SEKCII A NIE JE NIKDY NAPLÁNOVANÝ

SLEEP & WAKE UP

PRODUCER-CONSUMER PROBLEM (BOUND BUFFER PROBLEM)

```
int count = 0;
void producer(void) {
    int item;
    while (TRUE) {
        item = produce_item();
        if (count == N) sleep();
        insert_item(item)
        count = count + 1;
        if (count == 1)
            wakeup(consumer);
    }
}
```

```
void consumer(void) {
    int item;
    while (TRUE) {
        if (count == 0) (*) sleep();
        item = remove_item();
        count = count - 1;
        if (count == N-1)
            wakeup(producer)
        consume_item(item);
    }
}
```

MÔŽE NASTAŤ RACE CONDITION (NECHRÁNENÝ count)

PREDPOKLADAJME, ŽE V BODE (*) JE consumer PREPLÁNOVANÝ A SPUSTÍ SA producer.

TEN VLOŽÍ PRVÝ item A ZOBUDÍ consumer-A.

AVŠAK KEĎŽE consumer NIE JE USPANÝ, NIČ SA NESTANE

KEĎ SA TERAZ producer PREPLÁNUJE A SPUSTÍ SA consumer, HNEĎ ZA (*) SA USPÍ

SKÔR ČI NESKÔR producer NAPLNÍ buffer A USPÍ SA.

⇒ OBA PROCESY SPIA.

04.09.2008 Th
PETER ČERNO

STÁTNICE

SEMAPHORES (SEMAFÓR)

MÔŽE NADOBÚDAŤ HODNOTU 0 = ŽIADEN wakeup NIE JE SAVED
KLADNÚ HODNOTU = JEDEN / VIAC wakeup JE PENDING

DVE OPERÁCIE: UP, DOWN

DOWN (SEMAPHORE s)
WAIT UNTIL s > 0
s := s − 1

UP (SEMAPHORE s)
s := s + 1

MUSIA TO BYŤ ATOMICKÉ OPERÁCIE !!
AK OPERÁCIA NA SEMAFÓRE ZAČALA, ŽIADEN INÝ PROCES NEMÔŽE K SEMAFÓRU PRISTUPOVAŤ, KÝM SA OPERÁCIA NESKONČÍ ALEBO NEZABLOKUJE

OPERÁCIA UP ZVÝŠI HODNOTU SEMAFÓRU. AK JEDEN ALEBO VIAC PROCESOV SPALI NA TOM SEMAFÓRE, SYSTÉM VYBERIE NÁHODNE JEDEN, KT. MÔŽE VYKONAŤ down

PRODUCER – CONSUMER PROBLEM WITH SEMAPHORES

```
semaphore mutex = 1;
semaphore empty = N;
semaphore full = 0

void producer(void) {
    int item;
    while (TRUE) {
        item = produce_item();
        down(&empty);
        down(&mutex);
        insert_item(item);
        up(&mutex);
        up(&full);
    }
}

void consumer(void) {
    int item;
    while (TRUE) {
        down(&full);
        down(&mutex);
        item = remove_item();
        up(&mutex);
        up(&empty);
        consume_item(item);
    }
}
```

MUTEX

VHODNÉ NA ZABEZPEČENIE MUTUAL EXCLUSION
= BINÁRNY (0/1) SEMAFÓR = LOCKED / UNLOCKED

JE MOŽNÉ IMPLEMENTOVAŤ V USER-SPACE POMOCOU
TSL INŠTRUKCIE

MONITOR

IMPLEMENTOVANÝ PREKLADAČOM, JE MOŽNÉ SI
PREDSTAVIŤ AKO TRIEDU

NAJVIAC 1 PROCES MÔŽE BYŤ AKTÍVNYM V MONITORE !!

CONDITION VARIABLES
DVE OPERÁCIE : wait (cond-var) .. ZABLOKUJE PROC.
signal (cond-var) : MUSÍ TO BYŤ POSLEDNÁ AKCIA
DANÉHO PROCESU V MONITORE, AKTIVUJE NEJAKÝ
ČAKAJÚCI PROCES NA cond-var.

MESSAGE PASSING (SPRÁVY)

JE MOŽNÉ POUŽIŤ AJ V DISTRIBUOVANÝCH SYST.

DVE PRIMITÍVA : send, receive
PREDSTAVUJÚ SYSTÉMOVÉ VOLANIA
send (destination, &message) .. POŠLE SPRÁVU
receive (source, &message) .. OBDRŽÍ SPRÁVU
AK ŽIADNA NIE JE ← ZABLOKUJE SA
VRÁTI CHYBOVÝ KÓD

BARRIERS

POUŽÍVAJÚ SA PRE SKUPINU PROCESOV V APLIKÁCIÁCH,
KT. MOŽNO ROZDELIŤ NA FÁZY

KEĎ PROCES DOSIAHNE BARIÉRU, ZABLOKUJE SA,
KÝM VŠETKY PROCESY NEDOSIAHNU BARIÉRU.

04.09.2008 Th
PETER ČERNO

ŠTÁTNICE

THE DINING PHILOSOPHERS PROBLEM

5 FILOZOFOV SEDÍ OKOLO OKRÚHLEHO STOLU, KAŽDÝ Z NICH MÁ TANIER SO ŠPAGETAMI, NA JEDENIE SÚ POTREBNÉ DVE VIDLIČKY MEDZI SUSED. TANIERMI SÚ VIDLIČKY (SPOLU 5) ŽIVOT FILOZOFA POZOSTÁVA Z STRIEDAJÚCICH SA OBDOBÍ JEDENIA A MYSLENIA

PROBLÉM: NAPÍSAŤ PROGRAM TAK, ABY KAŽDÝ FILOZOF VYKONÁVAL TO NA ČO JE URČENÝ A VYHNÚŤ SA TZV. STARVATION

5.7 ZABLOKOVANIE [DEADLOCK] A ZOTAVENIE SA

PROSTRIEDOK (RESOURCE)

PREEMPTÍVNY - CPU, PAMÄŤ
NEPREEMPTÍVNY - CD-ROM, TLAČIAREŇ (PROBLEMATICKÉ)

PRÁCA S PROSTRIEDKAMI:

(1) ŽIADOSŤ (REQUEST) O PROSTRIEDOK (BLOKUJÚCA OP.)
(2) POUŽÍVANIE PROSTRIEDKU
(3) UVOLNENIE (RELEASE) PROSTRIEDKU

MNOŽINA PROCESOV JE ZABLOKOVANÁ (DEADLOCKED), AK KAŽDÝ PROCES V MNOŽINE ČAKÁ NA UDALOSŤ, KTORÚ MÔŽE SPÔSOBIŤ IBA INÝ PROCES V MNOŽINE

COFFMANOVÉ PODMIENKY :

(1) MUTUAL EXCLUSION CONDITION: KAŽDÝ ZDROJ JE BUĎ PRIRADENÝ PRÁVE 1 PROCESU, ALEBO VOĽNÝ
(2) HOLD AND WAIT CONDITION: PROCESY AKTUÁLNE VLASTNIACE NEJAKÉ PROSTRIEDKY MÔŽU POŽADOVAŤ NOVÉ PR.
(3) NO PREEMPTION CONDITION: PRIDELENÉ PROSTRIEDKY NEMÔŽU BYŤ PROCESOM ODOBRANÉ
(4) CIRCULAR WAIT CONDITION: EXISTUJE KRUHOVÝ REŤAZEC PROCESOV, KDE KAŽDÝ Z NICH ČAKÁ NA PROSTRIEDOK VLASTNENÝ ĎALŠÍM ČLÁNKOM

RIEŠENIE ZABLOKOVANIA

OSTRICH ALGORITHM (PŠTROSÍ ALGORITMUS)

ZABLOKOVANIE SA NEDETEKUJE, ANI SA MU NEZABRAŇUJE

DETEKCIA A ZOTAVENIE

DETEKCIA CYKLU V RESOURCE GRAFU

RIEŠENIE DEADLOKU: ODOBRANIE PR. / ZABITIE PROCESU / ROLLBACK

VYHÝBANIE SA

BANKÉROV ALGORITMUS - BANKÉR MÁ KLIENTOV A TÝM SĽÚBI URČITÚ VÝŠKU ÚVERU

BANKÉR POŽIČIA PENIAZE IBA VTEDY, KEĎ ZOSTANE BANKA V BEZPEČNOM STAVE

PREVENCIA NAPADNUTIE 1 Z COFFMANOVÝCH PODM.

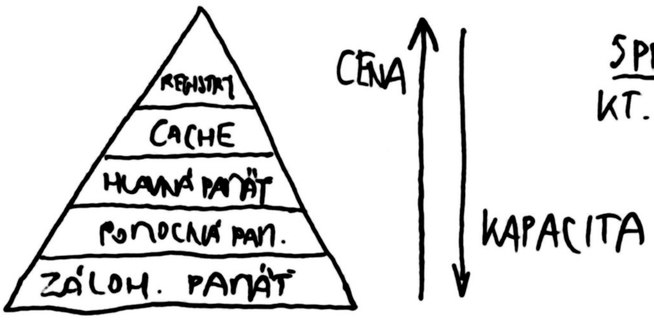
→ (1) : SPOOLING (PROSTRIEDOK SPRAVUJE 1 SYSTÉMOVÝ PROC.)
→ (2) : ŽIADAŤ O ∀ PROSTRIEDKY NA ZAČIATKU
→ (4) : ∀ PROSTRIEDKY JEDNOZNAČNE OČÍSLOVANÉ, ŽIADAŤ MOŽNO IBA VO VZOSTUPNOM PORADÍ

04.09.2008 Th
PETER ČERNO

ŠTÁTNICE

5.8 ORGANIZÁCIA PAMÄTI, ALOKAČNÉ ALG.

HIERARCHIA PAMÄTI



SPRÁVCA PAMÄTI - ČASŤ OS, KT. SPRAVUJE PAMÄŤOVÚ HIERARCHIU
(1) INFO O VOĽNEJ PAMÄTI
(2) PRIDEĽOVANIE PAMÄTI
(3) VÝMENA PAMÄŤ ⟷ DISK

OVERLAY - PROGRAM JE ROZDELENÝ NA NEZÁVISLÉ ČASTI, KTORÉ SA ZNESTIA DO PAMÄTI

MULTIPROGRAMOVANIE S FIXNÝMI PARTÍCIAMI

PAMÄŤ ROZDELENÁ NA FIXNÉ PARTÍCIE
(a) KU KAŽDEJ PARTÍCII JE FRONTA ČAKAJÚCICH PROCESOV
(b) JEDNA FRONTA PRE ∀ PARTÍCIE

PROBLÉMY : RELOKÁCIA, OCHRANA (BASE A LIMIT REGISTERS)

SWAPING

AK PAMÄŤ NESTAČÍ NA UDRŽANIE ∀ PROCESOV
SWAPING - NAHRATIE PROGRAMU DO PAMÄTI (CELÉHO PROGRAMU) CHVÍĽU MU DAŤ CPU, VRÁTENIE PROGRAMU SPÄŤ NA DISK
NA ROZDIEL OD FIXNÝCH PARTÍCIÍ SA POČET, UMIESTNENIE A VEĽKOSŤ PARTÍCIÍ DYNAMICKY MENÍ

INFORMÁCIE O OBSADENOSTI PAMÄTI

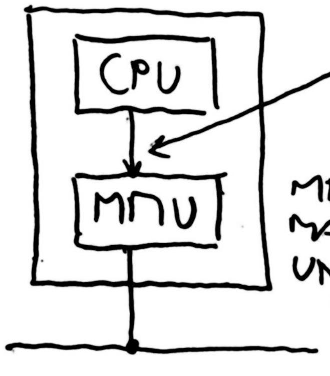
BITMAPA - BLOKY PEVNEJ VEĽKOSTI
SPOJOVÝ ZOZNAM → ALGORITMY NA PRIDEĽOVANIE:
FIRST-FIT, NEXT-FIT, BEST-FIT, WORST-FIT
BUDDY SYSTEM - PAMÄŤ ROZDELENÁ NA BLOKY O VEĽK. 2^n

FRAGMENTÁCIA

(1) EXTERNÁ - VOĽNÝ PAM. PRIESTOR ROZDELENÝ NA MALÉ KÚSKY
(2) INTERNÁ - NEVYUŽITIE CELÉHO PRID. PRIESTORU

ZOSYPANIE (MEMORY COMPACTION)

VIRTUÁLNA PAMÄŤ



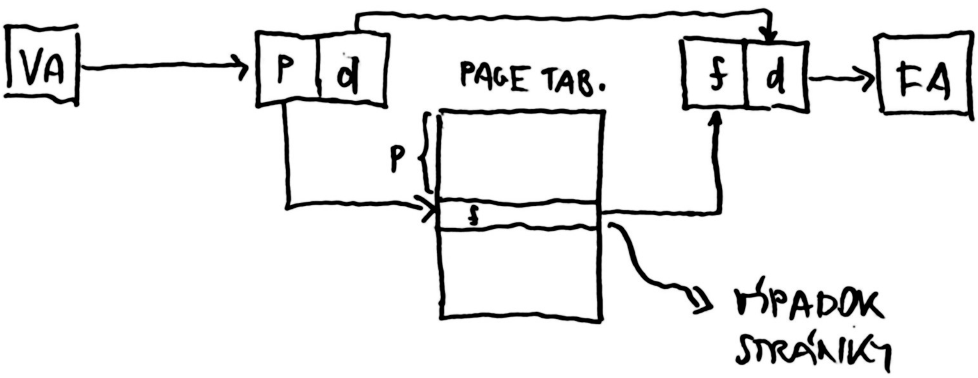
CPU POSIELA VIRTUÁLNE ADR → MMU

MEMORY MANAGEMENT UNIT - PREVÁDZA VIRT. ADR. NA FYZICKÉ

PROCESY PRACUJÚ S VIRT. ADRESAMI

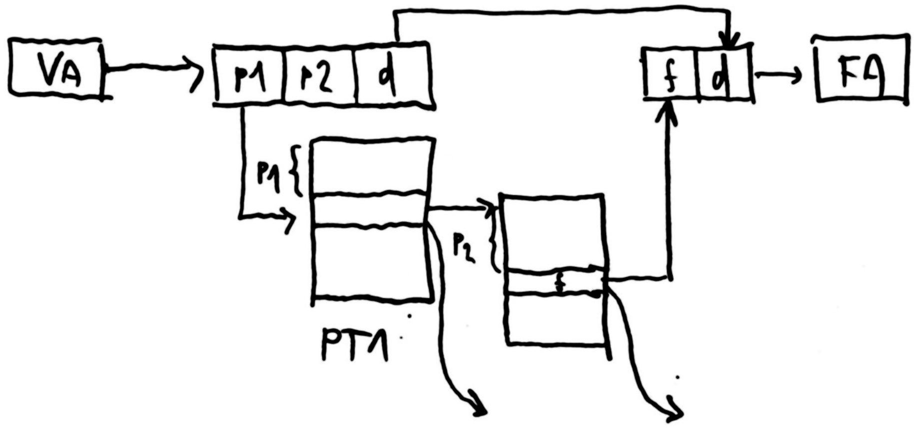
+ ILÚZIA VÄČŠEJ PAMÄTI
+ OCHRANA

VAP ROZDELENÝ NA STRÁNKY (PAGES)
FAP ROZDEL. NA RÁMCE ROVNAKEJ VEĽKOSTI (PAGE FRAMES)



STRÁNK. TAB. (PAGE TABLES) LEŽIA V PAMÄTI

VIACÚROVŇOVÉ STRÁNKOVANIE



04.09.2008Th
PETER ČERNO

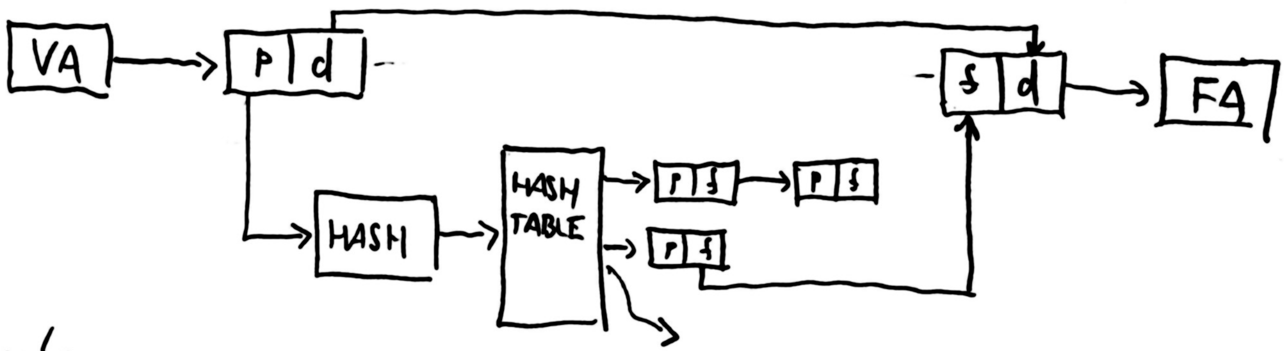
STÁTNICE

TLB (TRANSLATION LOOKASIDE BUFFER)

RÝCHLA ASOCIAČNÁ PAMÄŤ S STRÁNK. TABUĽKY
VYUŽÍVA SA LOKALITA CHOVANIA PROGRAMOV

INVERZNÉ STRÁNKOVACIE TABUĽKY

VYUŽÍVA TLB, HASH. TABUĽKA
POUŽÍVA SA KEĎ FAP << VAP (64-BIT CPU)



VÝPADOK STRÁNKY (PAGE FAULT)

(1) VÝNIMKA CPU → TRAP DO O.S., T.J. ULOŽÍ SA KONTEXT CPU
(2) ZISTIŤ VA
(3) KONTROLA PLATNOSTI VA A PRÁV
(4) NÁJDENIE VOĽNÉHO RÁMCA, POPR. ODSTRÁNENIE NEJAKÉHO POUŽÍVANÉHO RÁMCA
(5) NAČÍTANIE Z DISKU POŽADOVANÚ STRÁNKU A ZAVEDENIE MAPOVANIA
(6) OBNOVENIE KONTEXTU CPU

ALGORITMY PRE VÝMENU STRÁNOK:
OPTIMÁLNA STRÁNKA, NRU, FIFO,
DRUHÁ ŠANCA, HODINY, LRU, NÁHODNÁ

1. OPTIMÁLNA STRÁNKA

VYHADZUJEM STRÁNKU, NA KT. SA BUDE PRISTUPOVAŤ ZA NAJVÄČŠÍ POČET INŠTRUKCIÍ

NEDÁ SA IMPLEMENTOVAŤ

2. NRU (NOT RECENTLY USED)

KAŽDÁ STRÁNKA MÁ PRÍZNAKY A (ACCESED), D (DIRTY)

RAZ ZA ČAS SA VYNULUJÚ VŠETKY A

PRI VÝPADKU ROZDELÍM STRÁNKY PODĽA (A,D) DO TRIED A VYHADZUJEM NEJAKÚ STR. Z NAJNIŽŠEJ TRIEDY

3. FIFO

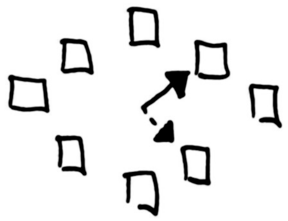
VYKAZUJE BELADIOVU ANOMÁLIU

3* DRUHÁ ŠANCA: AK A=1, ZARADÍM NA KONIEC FIFO

4. HODINY (CLOCK)

MODIFIKÁCIA DRUHEJ ŠANCE

1. AŽ 2 RUČIČKY



5. LRU (LEAST RECENTLY USED)

VYHADZUJE SA NAJDÁVNEJŠIE POUŽITÁ STRÁNKA

HW RIEŠENIA:

(1) 64-BITOVÝ COUNTER

(2) n-RÁMCOV → MATICA n×n BITOV

PRI POUŽITÍ RÁMCA k NASTAVÍM V MATICI RIADOK k NA SAMÉ 1 A NÁSLEDNE VYNULUJEM STĹPEC k

SEGMENTÁCIA (. . .

PROGRAM ROZDELENÝ NA SEGMENTY

VAP DVOJROZMERNÝ (s, d), FAP JEDNOROZMERNÝ

PREVOD ADRESY SEGMENTOVOU TABUĽKOU

- PRI VÝPADKU: CELÝ SEGMENT

05.09.2008 Fr
PETER ČERNO

ŠTÁTNICE

5.10 SYSTÉMY SÚBOROV, ADRESÁROVÉ ŠTRUKTÚRY

SÚBOR - POMENOVANÁ MNOŽINA SÚVISEJÚCICH INFO
(1) POMENOVANIE
(2) ATRIBÚTY - MENO, TYP, UMIESTNENIE, VEĽKOSŤ, OCHR., ČASY, ...
(3) ŠTRUKTÚRA - POST. BYTOV, SEKV. ZÁZNAMOV, STROM
(4) TYPY: BEŽNÉ (DÁTOVÉ), ADRESÁRE, ŠPECIÁLNE
(5) PRÍSTUP: SEKV., PRIAMY, PAMÄŤOVÉ MAPOVANIE

ALOKÁCIA (ULOŽENIE) SÚBORU
(1) SÚVISLÁ
(2) SPOJOVÁ (FAT)
(3) INDEXOVÁ (UNIX A i-NODE)

ADRESÁRE - ZVLÁŠTNY TYP SÚBORU   HARD/SOFT LINK
HIERARCHICKÁ ŠTRUKTÚRA - STROM / DAG / OBECNÝ GRAF

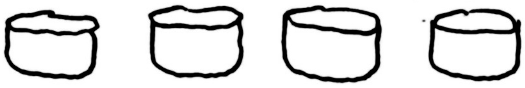
FILESYSTEM: (1) SPRÁVA SÚBOROV & ADRESÁROV
(2) SPRÁVA VOĽNÉHO MIESTA
NAPR.: FAT, NTFS, EXT2/EXT3
NTFS - RIADIACE ŠTRUKTÚRY V MFT (MASTER FILE TABLE)
RUN LIST

PLÁNOVANIE POHYBU HLÁV NA DISKU

FCFS (FIRST-COME FIRST-SERVED)
SSTF (SHORTEST SEEK TIME FIRST)
LOOK (VÝŤAH)
C-LOOK (CIRCULAR LOOK)

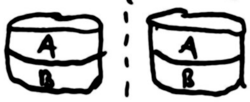
RAID (REDUNDANT ARRAY OF INEXPENSIVE DISKS)

JBOD (JUST BUNCH OF DISKS)



RAID 0 (STRIPPING)

RAID 1 (MIRRORING)



RAID 0+1 (STRIP + MIRROR)

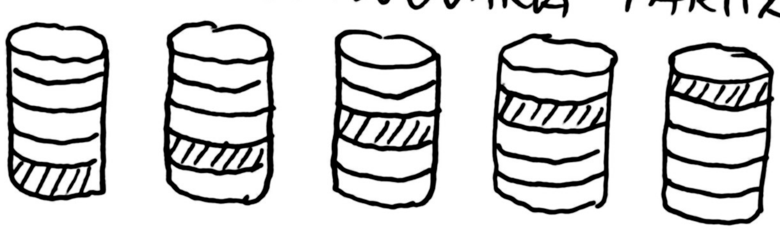
RAID 2 7 BITOVÝ HAMMINGOV PARITNÝ KÓD
PO BITOCH NA JEDNOTLIVÉ DISKY

RAID 3 1 PARITNÝ DISK 4+1

RAID 4 STRIPPING + PARITNÝ DISK

← ÚZKE HRDLO

RAID 5 DISTRIBUOVANÁ PARITA + STRIPPING



RAID 6 DISTRIBUOVANÁ PARITA P+Q A STRIPPING

5.11 BEZPEČNOSŤ, AUTENT., AUTOR., PRÍSTUPOVÉ PRÁVA
DEF.: OCHRANA, AUTORIZÁCIA, BEZPEČNOSŤ, PRÁVO, DOMÉNA OCHRANY
ACL (ACCESS CONTROL LIST) / C-LIST (CAPABALITY LIST)
CIELE ÚTOKU - DÔVERNOSŤ / CELISTVOSŤ DÁT, DOSTUPNOSŤ SYS.
AUTENTIFIKÁCIA - HESLO / FYZ. OBJEKT (USB) / BIOMETRIKA

05.09.2008 Fr
PETER ČERNO

ŠTÁTNICE

5.12 ARCHITEKTÚRA ISO/OSI

SIEŤOVÝ MODEL JE UCELENÁ PREDSTAVA O TOM, AKO MAJÚ BYŤ SIETE RIEŠENÉ. (NAPR. RM ISO/OSI)
ZAHŔŇA: + POČET VRSTIEV
+ PREDSTAVU O TOM, ČO MÁ KTORÁ VRSTVA NA STAROSTI
NEZAHŔŇA: - KONKR. PREDSTAVU O TOM, AKO MÁ KTORÁ VRSTVA PLNIŤ ÚLOHY (TJ. PROTOKOLY)

SIEŤOVÁ ARCHITEKTÚRA OBSAHUJE NAVIAC KONKRÉTNE PROTOKOLY (NAPR. RODINA PROTOKOLOV TCP/IP)

REFERENČNÝ MODEL ISO/OSI

BOL POKUSOM VYTVORIŤ UNIV. SIEŤ. ARCHITEKTÚRU → SKONČIL AKO MODEL
POCHÁDZA ZO SVETA SPOJOV
BOL „OFICIÁLNYM RIEŠENÍM", KT. PRESADZOVALI ORGÁNY ŠTÁTU
OSI - POSLEDNÁ ITERÁCIA NÁZVU: OPEN SYSTEM INTERCONNECTION
VZNIKAL OD ZELENÉHO STOLU, MAXIMALISTICKÝM SPÔSOBOM
VÝSLEDOK BOL ODSŤ MIMO REÁLNU PRAX
VEĽA PREDPOKLADOV SA UKÁZALO AKO CHYBNÉ
VZNIKALI IMPLEMENTOVATEĽNÉ PODMNOŽINY, GOSIP

KRITÉRIA PRE VOĽBU VRSTIEV:
ČINNOSTI NA ROVNAKEJ ÚROVNI ABSTRAKCIE V 1 VRSTVE
ABY BOLO MOŽNÉ PREVZIAŤ UŽ EXISTUJÚCE ŠTANDARDY
MINIMALIZOVAŤ DÁTOVÉ TOKY MEDZI VRSTVAMI
ROVNOMERNÁ VYŤAŽENOSŤ VRSTIEV

7 VRSTIEV, LINKOVÁ SA ROZPADLA NA LLC A MAC

APLIKAČNÁ VRSTVA	↑ VRSTVY ORIENTOVANÉ NA PODPORU APLIKÁCIÍ
PREZENTAČNÁ VRSTVA	
RELAČNÁ VRSTVA	
TRANSPORTNÁ VRSTVA	PRISPÔSOBOVACIA VRSTVA
SIEŤOVÁ VRSTVA	↓ VRSTVY ORIENTOVANÉ NA PRENOS DÁT
LINKOVÁ VRSTVA	
FYZICKÁ VRSTVA	

(1) <u>FYZICKÁ VRSTVA</u> - PRENOS BITOV

RIEŠI: KÓDOVANIE, MODULÁCIU, ČASOVANIE, SYNCHRONIZÁCIU, ...
SLUŽBY: PRIJMI BIT, ODOŠLI BIT
PRENOSOVÉ MÉDIA: DRÔTOVÉ / BEZDRÔTOVÉ
PARAMETRE: ŠÍRKA PÁSMA, MODULAČNÁ RÝCHL., PRENOSOVÁ RÝCHL.

(2) <u>LINKOVÁ VRSTVA</u> - PRENOS RÁMCOV (FRAMES)

ZAISŤUJE PRENOS IBA K BEZPROSTREDNÝM SUSEDOM
MÔŽE FUNGOVAŤ: SPOĽAHLIVO / NESPOĽAHLIVO,
SPOJOVANE / NESPOJOVANE, BEST EFFORT / QoS
RIADENIE TOKU - NEZAHLTENIE PRÍJEMCU
< PODVRSTVA LLC
PODVRSTVA MAC - PRÍSTUP KU ZDIEĽANÉMU MÉDIU

(3) <u>SIEŤOVÁ VRSTVA</u> - PRENOS PAKETOV (PACKETS)

ZAISŤUJE DORUČENIE PAKETU AŽ KU KONKR. ADRESÁTOVI
MÔŽE POUŽÍVAŤ RÔZNE ALGORITMY SMEROVANIA (ROUTING):
ADAPTÍVNY / NEADAPTÍVNY, IZOLOVANÝ / DISTRIBUOVANÝ,
CENTRALIZOVANÝ, ...

(4) <u>TRANSPORTNÁ VRSTVA</u> - ZAISŤUJE PRISPÔSOBENIE,
END-TO-END KOMUNIKÁCIU
MÔŽE ZMENIŤ: NESPOĽAHLIVÝ CH. → SPOĽAHLIVÝ,
NESPOJOVANÝ PRENOS → SPOJOVANÝ
PRÍKLAD: TCP - SPOJOVANÝ, SPOĽAHLIVÝ PRENOS
UDP - NESPOJOVANÝ, NESPOĽAHLIVÝ PRENOS

05.09.2008 Fr
PETER ČERNO

ŠTÁTNICE

(5) RELAČNÁ VRSTVA – ZAISŤUJE VEDENIE RELÁCIÍ, SYNCHRONIZÁCIU, ŠIFROVANIE, PODPORU TRANSAKCIÍ
JE NAJVIAC KRITIZOVANÁ V RM ISO/OSI

(6) PREZENTAČNÁ VRSTVA – KONVERZIA DÁT, LINEARIZÁCIA VIACROZM. POLÍ, SPÔSOB UKLADANIA VIAC-BYTOVÝCH POLOŽIEK DO PAMÄTI, ...

(7) APLIKAČNÁ VRSTVA – JADRO APLIKÁCIÍ (JE MOŽNÉ ŠTANDARDIZOVAŤ) (NAPR. EMAIL)

RM ISO/OSI PORAZENÝ RODINOU PROTOKOLOV TCP/IP
NIEKTORÉ PROTOKOLY BOLI PREVZATÉ
X 400 (EL. POŠTA), X500 (ADRESÁROVÉ SLUŽBY, ZJEDNODUŠENÍM VZNIKOL ÚSPEŠNÝ PROTOKOL LDAP)

5.13 RODINA PROTOKOLOV TCP/IP

<table>
<tr><td rowspan="3">APLIKAČNÁ</td><td>APLIKAČNÁ</td></tr>
<tr><td>PREZENTAČNÁ</td></tr>
<tr><td>RELAČNÁ</td></tr>
<tr><td>TRANSPORTNÁ</td><td>TRANSPORTNÁ</td></tr>
<tr><td>SIEŤOVÁ</td><td>SIEŤOVÁ</td></tr>
<tr><td rowspan="2">VRSTVA SIEŤOVÉHO ROZHRANIA</td><td>LINKOVÁ</td></tr>
<tr><td>FYZICKÁ</td></tr>
</table>

JE TO SIEŤOVÁ ARCHIT.: TCP/IP PROTOCOL SUITE
POSTUP VZNIKU: NAJSKÔR PROTOKOLY, POTOM VRSTVY,
V AKADEMICKOM PROSTREDÍ, ZMENY SÚ „ADITÍVNE"

IP OVER EVERYTHING, EVERYTHING OVER IP

VZNIK TCP/IP SÚVISÍ S INTERNETOM (ARPANETOM)
PRE RUTINNÚ PREVÁDZKU ARPANETU BOLO TREBA VYVINÚŤ RUTINNÉ PROTOKOLY

PROTOKOLY TCP/IP BOLI VYVÍJANÉ AKO DEFINITÍVNE RIEŠENIE PRE VZNIKAJÚCI INTERNET

POŽIADAVKY NA ARPANET:
NESMIE TO MAŤ CENTRÁLNU ČASŤ
MUSÍ TO BYŤ ROBUSTNÉ

POŽIADAVKY NA PROTOKOLY TCP/IP:
INTERNETWORKING - VZÁJOMNÉ PREPOJENIE SIETÍ

ČO SA NEPOŽADOVALO - ZABEZPEČENIE, QoS
TCP/IP PREDPOKLADÁ, ŽE SIETE SÚ NESPOJOVANÉ, NESPOĽAHLIVÉ A BEST EFFORT
TCP/IP DEFINUJE:
(1) APLIKAČNÁ VRSTVA - JEDNOTNÉ ZÁKLADY APLIKÁCIÍ (EMAIL, PRENOS SÚBOROV, REMOTE LOGIN, ...)
(2) TRANSPORTNÁ VRSTVA - JEDNOTNÉ TRANSPORTNÉ PROTOKOLY (TCP A UDP)
(3) SIEŤOVÁ VRSTVA - JEDNOTNÝ PRENOSOVÝ PROTOKOL IP
TCP/IP NEDEFINUJE VRSTVU SIEŤOVÉHO ROZHRANIA
VÝNIMKA: PROTOKOLY SLIP A PPP (2-BOD. SPOJENIA)

PROTOKOL IP - JEDNOTNÁ PRIKRÝVKA NA SIEŤ. ROZHRANIA, MÁ VŠADE ROVNAKÉ VLASTNOSTI A POSKYTUJE ROVNAKÉ SLUŽBY
NESPOJOVANÝ, NESPOĽAHLIVÝ, BEST-EFFORT
JEDNOTNÉ ADRESOVANIE
32 BITOVÉ ADRESY IP ADRESY
+ PREVODNÉ MECHANIZMY: IP ADRESA ⟷ FYZICKÁ LINKOVÁ ADRESA
VÝNIMKA: IP PROTOKOL AJ VYŠŠIE VRSTVY VIDIA MTU !!!
(MAXIMUM TRANSFER UNIT) - MAX. VEĽKOSŤ LINKOVÉHO RÁMCA

05.09.2008 Fr
PETER ČERNO

ŠTÁTNICE

IPv4

32 BITOVÉ, LOGICKY DVOJZLOŽKOVÉ: SIEŤOVÁ, RELATÍVNA ČASŤ
VYCHÁDZA Z PREDSTAVY KATENETOVÉHO MODELU
TCP/IP PREDPOKLADÁ DVA TYPY UZLOV:
HOSTITEĽSKÝ POČÍTAČ, SMEROVAČ (IP ROUTER)
TÉZA: KAŽDÝ UZOL BY MAL MAŤ PRIRADENÚ
CELOSVETOVO UNIKÁTNU IP ADRESU
(PRESNEJŠIE KAŽDÉ ROZHRANIE)
AUTORI TCP/IP VYCHÁDZALI Z PREDPOKLADU, ŽE BUDE:
MALÝ POČET VEĽKÝCH SIETÍ - TRIEDA A 8:24

0	ADR. SIETE	ADRESA UZLU

7 BITOV

STREDNÝ POČET STREDNE VEĽKÝCH SIETÍ - TRIEDA B 16:16

1	0	ADR. SIETE	ADR. UZLU

14 BITOV

VEĽKÝ POČET MALÝCH SIETÍ - TRIEDA C 24:8

1	1	0	ADR. SIETE	ADR. UZLU

21 BITOV

PROBLÉM VYČERPANIA ∀ IP ADRIES, DOČASNÉ RIEŠENIA
→ SUBNETTING, CIDR (IP ADRESY PO ĽUBOVOĽNÝCH KVANTÁCH 2^n)
MEDZI ADRESAMI EXISTUJÚ AJ VYHRADENÉ ADRESY

DEFINITÍVNE RIEŠENIE:
NOVÁ VERZIA PROTOKOLU IPv6, ADRESY VEĽKOSTI 128 BITOV

IPv6

TRVALÉ RIEŠENIE NEDOSTATKU ADRIES,
PRESADZUJE SA POMALY

ZAPISUJE SA AKO 8 SKUPÍN PO 4 HEXADECIMÁLNYCH ČÍSLACH

3 TYPY ADRIES:

INDIVIDUÁLNE (UNICAST) - IDENTIFIKUJÚ 1 ROZHRANIE
SKUPINOVÉ (MULTICAST) - SKUPINA ZARIADENÍ
VÝBEROVÉ (ANYCAST) - URČUJE SKUPINU, DATA IDÚ IBA 1 ČLEN.

NEOBSAHUJE BROADCAST ADRESY

IPv6 ZAVÁDZA KONCEPCIU DOSAHU - ADRESA JE JEDNOZNAČNÁ IBA V RÁMCI SVOJHO DOSAHU (GLOBÁLNY/LINKOVÝ ...)

INDIVIDUÁLNE GLOBÁLNE IP ADRESY

16 BITOV	16 BITOV	16 BITOV	16 BITOV	64 BITOV
2 0 0 1	PRIDEĽUJE RIR	PRIDEĽUJE LIR	ADR. PODSIETE	ADR. ROZHRANIA
	REGIONÁLNY REGISTRÁTOR	LOKÁLNY REGISTRÁTOR		

ADRESA ROZHRANIA BY MALA MAŤ V SEBE ZAKÓDOVANÚ MAC ADR.
IPv6 PODPORUJE QoS A BEZPEČNOSŤ (IPSEC).

ROUTING (SMEROVANIE)

HLAVNÁ ÚLOHA SIEŤOVEJ VRSTVY: DORUČOVAŤ DATA OD ZDROJA AŽ K PRÍJEMCOVI

SMEROVANIE - ROZHODNUTIE O ĎALŠOM ODCHODZOM SMERE
FORWARDING - FAKTICKÉ PRENESENIE PACKETU V ODCH. SMERE

ĎALŠIE ÚLOHY: CONGESTION CONTROL
ZAISTENIE QoS

05.09.2008 F
PETER ČERNO

ŠTÁTNICE

OPAKOVAČ (REPEATER) - PREPOJUJE SIETE NA FYZICKEJ VRSTVE
PREPÍNAČ (SWITCH) - PREPÁJA SIETE NA LINKOVEJ VRSTVE
SMEROVAČ (ROUTER) - ZABEZPEČUJE ROUTING & FORWARDING

SMEROVACIE TABUĽKY (ROUTING TABLES)

OBSAHUJE (PRE KAŽDÝ RIADOK):
CIEĽOVÚ ADRESU - PREFIX
AKCIU, ČO SPRAVIŤ S DATAGRAMOM - T.J. ČI DORUČIŤ PRIAMO ADRESÁTOVI, ALEBO PREDAŤ SUSEDOVI
ĎALŠIE ÚDAJE (AKO NAPR. VZDIALENOSŤ CIEĽU ATĎ.)

SMEROVANIE SA VYKONÁ PRE KAŽDÝ DATAGRAM, VYBERÁ SA NAJDLHŠÍ MATCHUJÚCI PREFIX

SMEROVACIE ALGORITMY

(1) NEADAPTÍVNE (STATICKÉ)
(2) ADAPTÍVNE (DYNAMICKÉ) - REAGUJE NA PRIEBEŽNÉ ZMENY V SIETI, PRIEBEŽNE POČÍTA OPTIMÁLNE TRASY, VYŽADUJE PRAVIDELNÝ PRÍSUN AKTUÁL. INFORMÁCIÍ

RÔZNE DRUHY SMEROVANIA:
CENTRALIZOVANÉ - ROUTE SERVER
IZOLOVANÉ - ZÁPLAVOVÉ, HORÚCI ZEMIAK, SPÄTNÉ UČENIE, SOURCE ROUTING; (UZLY NESPOLUPRACUJÚ)
DISTRIBUOVANÉ - UZLY SPOLUPRACUJÚ
(a) VECTOR DISTANCE ROUTING
(b) LINK STATE ROUTING
HIERARCHICKÉ SMEROVANIE

DISTRIBUOVANÉ SMEROVANIE

NAJČASTEJŠIA VARIANTA SMEROVANIA
SMEROVAČE VZÁJOMNE SPOLUPRACUJÚ
VÝPOČET OPT. CESTY MÔŽE BYŤ
DISTRIBUOVANÝ – KAŽDÝ POČÍTA KUS, UZLY SI VZÁJOMNE PREDÁVAJÚ ČASTI VÝPOČTU
NEZÁVISLÝ – UZLY SI PREDÁVAJÚ IBA PODKLADY (INFORMÁCIE O DOSTUPNOSTI A ZMENÁCH)

(a) VECTOR-DISTANCE ROUTING

KAŽDÝ SMEROVAČ SI UDRŽUJE TABUĽKU SVOJICH NAJMENŠÍCH VEKTOROV VZDIALENOSTÍ OD VŠETKÝCH OSTATNÝCH UZLOV
SMEROVAČE SI TIETO INFORMÁCIE NAVZÁJOM VYMIEŇAJÚ, ALE VÝMENA PREBIEHA IBA MEDZI PRIAMYMI SUSEDMI !!
VÝPOČET OPT. CIEST JE TÝM PÁDOM DISTRIBUOVANÝ
PROBLÉM: COUNT-TO-INFINITY
RIEŠENIE: SPLIT-HORIZON: SMEROVAČ NEBUDE INZEROVAŤ SPÄŤ
POISONED REVERSE: INZERUJE SPÄŤ HODNOTU ∞
(EXISTUJÚ TOPOLÓGIE, KDE TOTO RIEŠENIE ZLYHÁVA)

PROTOKOL RIP (ROUTING INFORMATION PROTOCOL)
POČET PRESKOKOV MAX. 15, 16 = NEKONEČNO
OBSAH SM. TAB. (DISTANCE VECTOR) JE ROZOSIELANÝ KAŽ. 30 sek
RIP JE ZLE ŠKÁLOVATEĽNÝ, MÁLO STABILNÝ, POUŽITEĽNÝ IBA PRE MALÉ SIETE

(b) LINK-STATE

KAŽDÝ UZOL PRAVIDELNE MONITORUJE PRIECHODNOSŤ SPOJENÍ K SVOJIM SUSEDOM. KAŽDÚ ZMENU DISTRIBUUJE PO CELEJ SIETI
KAŽDÝ UZOL MÁ ÚPLNÚ INFORMÁCIU O TOPOLÓGII SIETE, SÁM SI POČÍTA NAJKRATŠIE CESTY POMOCOU DIJKSTROVHO ALG.

05.09.2008 Fr
PETER ČERNO

ŠTÁTNICE

PROTOKOL OSPF (OPEN SHORTEST PATH FIRST)

PO ZAPNUTÍ SI KAŽDÝ UZOL ZISTÍ AKÝCH MÁ PRIAMYCH SUSEDOV - PROTOKOL HELLO

UZOL PRIEBEŽNE ZISŤUJE DOBU ODOZVY SVOJICH SUSEDOV - POSIELA IM ECHO PAKETY

KAŽDÝ UZOL PRAVIDELNE ZOSTAVUJE PAKET, DO KT. DÁ NAMERANÉ HODNOTY OD SVOJICH SUSEDOV,

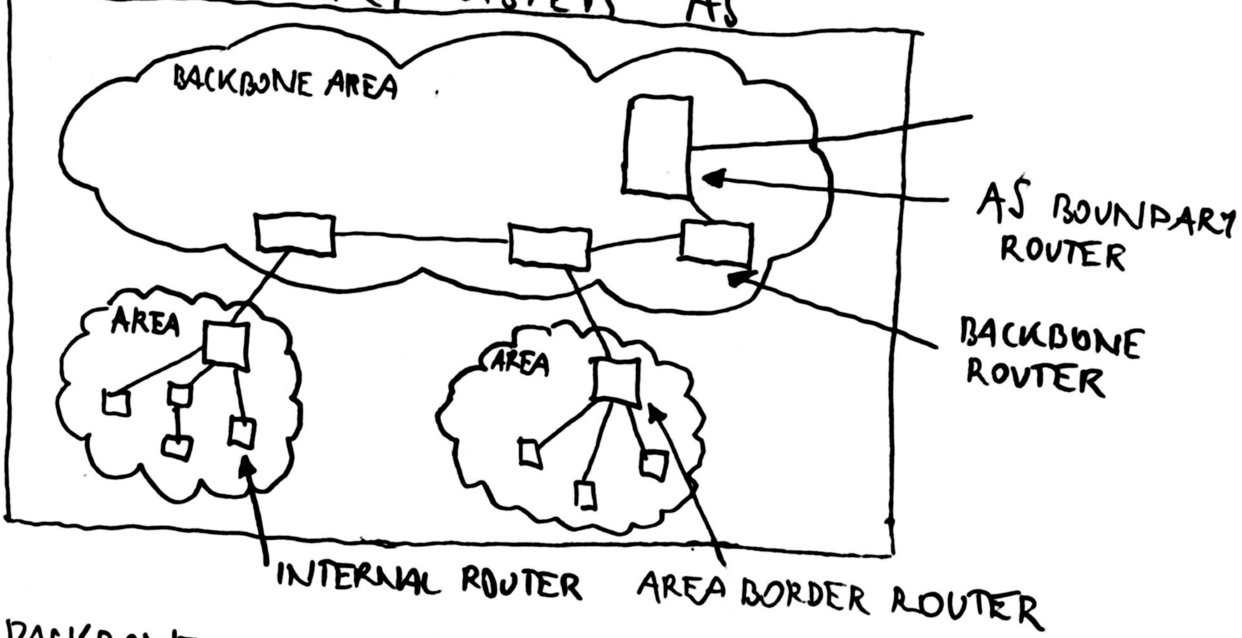
- TENTO PAKET ROZOŠLE OSTATNÝM UZLOM POMOCOU ZÁPLAVOVÉHO SMEROVANIA

PAKETY STAČÍ ROZOSIELAŤ IBA PRI ZMENE

HODÍ SA PRE VÄČŠIE SIETE

HIERARCHICKÉ SMEROVANIE, AUTONÓMNE SYS.

AUTONÓMNY SYSTÉM AS



BACKBONE AREA - KOSTRA V RÁMCI AS

AREA - OBLASŤ V RÁMCI AS PRIPOJENÁ K BACKBONE AREA

DETAILNÉ SMEROVACIE INFORMÁCIE NEOPÚŠŤAJÚ OBLASŤ (AREA)

IGP (INTERIOR GATEWAY PROTOCOLS) - V RÁMCI AS, OSPF, RIP, IGRP, EIGRP

EGP (EXTERIOR -||-) - MEDZI AS,

BGP (BORDER GATEWAY PROTOCOL)

FRAGMENTÁCIA

MTU (MAXIMUM TRANSMISSION UNIT) - MAXIMÁLNA VEĽKOSŤ PAKETU, KT. JE SCHOPNÉ PRENIEST JEDNO SIEŤOVÉ ZARIADENIE NA DRUHÉ

PRI PRENOSOVOM PROTOKOLE TCP JE PRI SMEROVANÍ PAKETU DO PRENOSOVÉHO KANÁLU S NIŽŠÍM MTU VYKONANÁ FRAGMENTÁCIA PAKETU

PRI PROTOKOLE UDP NIE JE FRAGMENTÁCIA PODPOROVANÁ, PAKET JE V TAKOM PRÍPADE ZAHODENÝ

V IPv4 JE MOŽNÉ DELIŤ AJ FRAGMENTOVANÉ PAKETY, V IPv6 MUSÍ FRAGMENTÁCIU ZABEZPEČIŤ ODOSIELATEĽ

POUŽÍVA SA PROTOKOL ICMP (INTERNET CONTROL MESSAGE PROT.)

SPOĽAHLIVOSŤ, FLOW CONTROL, CONGESTION CONT.

FLOW CONTROL - IDE O POINT-TO-POINT ZÁLEŽITOSŤ MEDZI 1 ODOSIELATEĽOM A 1 PRÍJEMCOM

CONGESTION CONTROL - TÝKA SA CELEJ SIETE, DÁTOVÝ TOK OD ∀ UŽÍVATEĽOV SA SČÍTA A NESMIE PREKROČIŤ HRANICU, KT. JE SIEŤ SCHOPNÁ ZVLÁDNUŤ

ZAHLTENIE - STAV, KEDY MUSÍ PRENOSOVÁ SIEŤ ZAHADZOVAŤ PAKETY, PRETOŽE ICH NEDOKÁŽE PRENIESŤ

RIEŠENIE <
- DOPREDNÉ TECHNIKY (OPEN LOOP) - TRAFFIC CONDITION.
- SPÄTNOVÄZBOVÉ TECHNIKY (CLOSED LOOP)

V SIEŤOVEJ VRSTVE TCP/IP - PROTOKOL ICMP

TRANSPORTNÁ VRSTVA: ZAISŤUJE END-TO-END KOMUN., VYKONÁVA MULTIPLEX/DEMULTIPLEX, VYROVNÁVA ROZDIELY: SPOJ/NESPOJ CHAR., SPOĽAHLIVOSŤ, QoS PREDCHÁDZA/RIADI ZAHLTENIE A RIADI TOK

TCP (TRANSMISSION CONTROL PROTOCOL) - SPOJOVANÝ, SPOĽAHLIVÝ

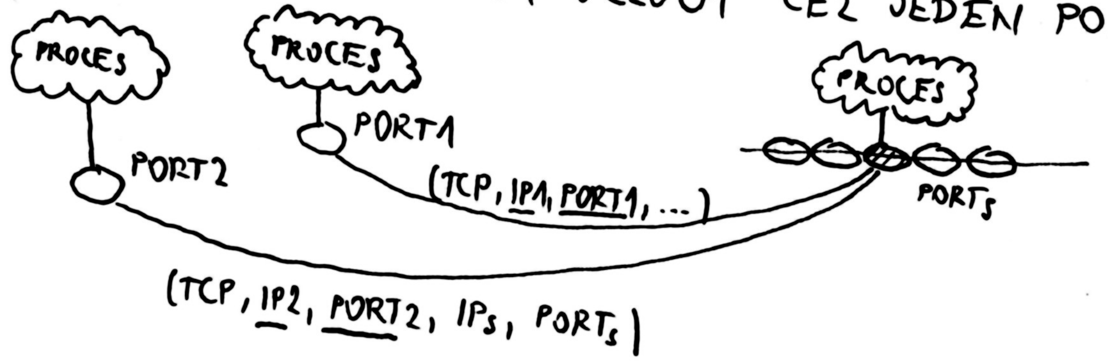
UDP (USER DATAGRAM PROTOCOL) - NESPOJOVANÝ, NESPOĽAHLIVÝ

05.09.2008 Fr
PETER ČERNO

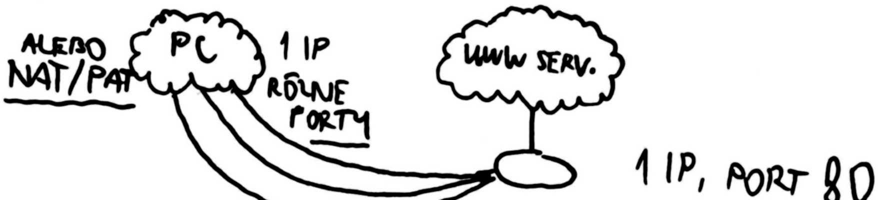
STÁTNICE

TRANSPORTNÁ VRSTVA (NA ROZDIEL OD SIEŤOVEJ) MUSÍ ROZLIŠOVAŤ RÔZNE ENTITY NA ÚROVNI VYŠŠÍCH VRS.
IDEA: IDENTIFIKOVAŤ PRECHODNÉ BODY MEDZI TRANSP. A VYŠŠOU VRSTVOU
ISO/OSI - SAP (SERVICE ACCESS POINT)
TCP/IP - PORT

JEDNA ENTITA (PROCES) MÔŽE KOMUNIKOVAŤ S VIAC ENTITAMI NA INÝCH UZLOCH CEZ JEDEN PORT



JEDNA ENTITA MÔŽE KOMUNIKOVAŤ S VIAC ENTITAMI NA ROVNAKOM UZLE, ALEBO NA RÔZNYCH UZLOCH ZA JEDNÝM NAT/PAT UZLOM



TCP

TCP POUŽÍVA KONTINUÁLNE POTVRDZOVANIE SO SELEKT. OPAK.
MONITORUJE SPRÁVANIE SIETE (DOBU OBRÁTKY RTT ROUND TRIP TIME)
A VYHODNOCUJE VÁŽENÝ PRIEMER A ROZPTYL RTT
(ČAKACIA DOBA VYCHÁDZA TESNE NAD STRED. HODNOTOU RTT)

POTVRDZOVANIE JE NESAMOSTATNÉ, POUŽÍVA SA PIGGYBACKING, T.J. VKLADÁ SA DO PACKETOV CESTUJÚCICH OPAČNÝM SMEROM

TCP PRIJÍMA / UDÁVA DATA PO BYTOCH – PRACUJE S DÁTOVÝM PRÚDOM (BYTE STREAM)
DATA BUFFERUJE → VKLADÁ DO TCP SEGMENT A ODOSIELA AŽ PO NAPLNENÍ (JE MOŽNÉ VYŽADAŤ – OP. PUSH)

RIADENIE TOKU – METÓDA OKIENKA
OKIENKO UDÁVA VEĽKOSŤ VOĽNÝCH BUFFEROV NA STRANE PRÍJEMCA

NADVIAZANIE / RUŠENIE SPOJENIA – 3-FÁZOVÝ HANDSHAKE
SYN → SYN-ACK → ACK
x x+1, y y+1

OHRANA PRED ZAHLTENÍM
KAŽDÁ STRATA DÁT CHÁPANÁ AKO DÔSLEDOK ZAHLTENIA
PO STRATE PAKETU POŠLE ZNOVU, ALE NEPOSIELA ĎALŠÍ, ČAKÁ NA POTVRDENIE!
KEĎ PRÍDE POTVRDENIE VČAS, ZDVOJNÁSOBÍ DATA (DVA PAKETY)
...

QoS – TRAFFIC CONDITIONING, INTEGRATED SERVICES, DIFFERENTIATED SERVICES

NAT (NETWOR ADDRESS TRANSLATION)

STATIC NAT / DYNAMIC NAT / PAT

FUNKCIA SIEŤOVÉHO ROUTERU PRE ZMENU IP ADRIES
MASKARÁDA (MASKOVANIE) – ROUTER MENÍ IP ADRESY Z NEJAKÉHO ROZSAHU (LAN) NA SVOJU IP ADRESU
NAT JE VLASTNE PROXY SERVER (NA SIEŤOVEJ VRSTVE)
VÝHODY: UMOŽŇUJE PRIPOJENIE VIAC POČÍTAČOV DO INTERNETU CEZ 1 ZDIEĽANÚ VEREJNÚ IP ADRESU
NEVÝHODY: NEFUNGUJÚ NIEKTORÉ PROTOKOLY (AKTÍVNE FTP)

NAT TRAVERSAL – ALGORITMUS NA PROBLÉM SPOJENIA DVOCH UZLOV V PRIVÁTNYCH TCP/IP SIEŤACH, KT. POUŽÍVAJÚ NAT ZARIADENIA. (P2P, VoIP)

05.09.2008 Fr
PETER ČERNO

ŠTÁTNICE

ARP (ADDRESS RESOLUTION PROTOCOL)

POUŽÍVA SA K ZÍSKANIU ETHERNETOVEJ (MAC) ADRESY SUSEDNÉHO STROJA Z JEHO IP ADRESY.

NA ODOSLANIE IP DATAGRAMU PROSTREDNÍCTVOM ETHERNETU JE NUTNÉ POZNAŤ CELÚ ETH. ADRESU

ODOSIELATEĽ ODOŠLE ARP REQUEST OBSAHUJÚCI HĽADANÚ IP ADRESU + ÚDAJE O SEBE (IP ADR. + MAC ADR.)

VLASTNÍK IP ADRESY ODOŠLE ARP REPLY

INFO O MAC ADRESÁCH SA UKLADAJÚ DO ARP CACHE

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

NA ODOSIELANIE CHYBOVÝCH SPRÁV,
OBVYKLE SA NEPOUŽÍVA SIEŤOVÝMI APLIKÁCIAMI PRIAMO
(VÝNIMKA JE NÁSTROJ ping → POSIELA ECHO REQUEST)

NAJPOUŽÍVANEJŠIE ICMP DATAGRAMY:

- ECHO - POŽIADAVOK NA ODPOVEĎ
- ECHO REPLY - ODPOVEĎ NA POŽIADAVOK
- DESTINATION UNREACHABLE - NEDOSTUPNOSŤ CIEĽA
- REDIRECT - PRESMEROVANIE
- TIME EXCEEDED - VYPRŠAL ČASOVÝ LIMIT

BEZPEČNOSŤ - IPSEC, AH, ESP, TRANSPORT MODE, TUNNEL MODE, FIREWALLS !!

IPSEC - SÚSTAVA VZÁJOMNE PREVIAZANÝCH OPATRENÍ A PROTOKOLOV PRE ZABEZPEČENIE KOMUNIKÁCIE POMOCOU IP PROTOKOLU,
FUNGUJE NA ÚROVNI SIEŤOVEJ VRSTVY (JJ POD TCP, UDP)
PODPOROVANÉ V IPv4 AJ IPv6 (POVINNÉ)
ZAISTUJE DÔVERNOSŤ (ŠIFR. DATA), INTEGRITU, AUTENTIFIKÁCIU (OVERENIE PÔVODU ODOSIELATEĽA), KRYPTOVANIE
SA (SECURITY ASSOCIATION) - POINT-TO-POINT BEZP. SPOJ

o IPSEC MÓDY: TRANSPORT MODE -
IP HLAVIČKA NECHRÁNENÁ (KVÔLI NAT), TELO ŠIFROVANÉ
TUNNEL MODE - PAKETY SÚ CELÉ ŠIFROVANÉ A VLOŽENÉ DO ĎALŠIEHO PAKETU
POVINNÉ PRE SECURITY GATEWAYS

o IPSEC PROTOKOLY:

AH (AUTHENTICATION HEADER)
KOMUNIKUJÚCE STRANY SA DOHODNÚ NA KĽÚČI, K DATAM SA PRIPOJUJE HASH, DATA SA NEŠIFRUJÚ

ESP (ENCAPSULATING SECURITY PAYLOAD)
VYKONÁVA AUTENTIZÁCIU AJ ŠIFRUJE OBSAH

FIREWALL

SLEDOVANIE A FILTROVANIE KOMUNIKÁCIE NA SIETI
NA RÔZNYCH VRSTVÁCH ←
- SIEŤOVÁ (IP ADRESY)
- TRANSPORTNÁ (PORTY)
- APLIKAČNÁ (OBSAH)

06.09.2008 Sa
PETER ČERNO

ŠTÁTNICE

6 PROGRAMOVACIE JAZYKY

6.1 PRINCÍPY A ZÁKLADY IMPLEMENTÁCIE OBJEKTOVO-ORIENTOVANÝCH JAZYKOV ...

STRUKTÚROVANÉ PROGRAMOVANIE -
ROZDELENIE PROGRAMU NA PROCEDÚRY (RUTINY, FUNKCIE, ...)
PRÍKLADY JAZYKOV: PASCAL, C, ADA

RIADENIE TOKU (CONTROL FLOW STATEMENTS):
JUMP, IF-THEN-ELSE, LOOP, SUBROUTINES, HALT

VÝNIMKY - ŠPECIÁLNY PRÍKAZ RIADENIA TOKU
(STACK UNWINDING = ODVÍJANIE ZÁSOBNÍKU)

VOLACIE KONVENCIE

PASCAL: UPRATUJE VOLANÁ FCIA., ARGUMENTY SA UKLADAJÚ NA ZÁSOBNÍK ZĽAVA DOPRAVA
C: UPRATUJE VOLAJÚCA FCIA., ARGUMENTY SA UKLADAJÚ ZPRAVA DOĽAVA (KVÔLI FCIÁM. S PREMENNÝM POČTOM PARAMETROV)

ORGANIZÁCIA PAMÄTI (PAMÄŤ PROCESU)

(1) KÓD PROGRAMU (KÓDOVÝ SEGMENT) -
VYTVORENÝ PRI PREKLADE, SÚČASŤ SPUSTITEĽNÉHO SÚBORU, NEMENNÝ, CHRÁNENÝ PROTI ZÁPISU

(2) STATICKÉ DATA (DATOVÝ SEGMENT)
DATA PROGRAMU, KT. VEĽKOSŤ JE ZNÁMA UŽ PRI PREKLADE A KT. POZÍCIA SA POČAS PROGRAMU NEMENÍ
GLOBÁLNE PREMENNÉ, LOKÁLNE DATA AKO static, KONŠTANTY

(3) HALDA (HEAP SEGMENT)
VYTVÁRANÁ ŠTARTOVACÍM MODULOM (C RUNTIME LIBRARY),
UKLADAJÚ SA SEM DYNAMICKY VZNIKAJÚCE OBJEKTY (malloc, new)

(4) VOĽNÁ PAMÄŤ
POSTUPNE SA ZAPĹŇA Z JEDNEJ STRANY ZÁSOBNÍK, Z DRUHEJ HALDA

(5) ZÁSOBNÍK (STACK)
INFORMÁCIE O VOLANÍ PROCEDÚR (AKTIVAČNÉ ZÁZNAMY),
ÚSCHOVA LOKÁLNYCH DÁT,
TYPICKY RASTIE OD KONCA PAMÄTI K NIŽŠÍM ADRESÁM

OBJEKTOVO - ORIENTOVANÉ PROGRAMOVANIE

OBJEKTY - PRVKY MODELOVANEJ REALITY
ABSTRAKCIA - KAŽDÝ OBJEKT PRACUJE AKO BLACK-BOX
ZAPUZDRENIE - NEMOŽNO PRIAMO PRISTUPOVAŤ K VNÚTORNOSTIAM OBJ.
KOMPOZÍCIA - OBJEKT OBSAHUJÚCI INÉ OBJEKTY
DEDIČNOSŤ - KAŽDÝ OBJEKT JE INŠTANCIOU TRIEDY,
TRIEDY MÔŽU DEDIŤ OD INÝCH TRIED
POLYMORFIZMUS - MÔŽME DOSADIŤ POTOMKA ZA PREDKA

TRIEDA - DEFINUJE KONCEPT OBJEKTU, ATRIBÚTY + OPERÁCIE

C++ : KEĎ JE TRIEDA B POTOMKOM TRIEDY A, POTOM
PAMÄŤOVÁ REPR. TR. B OBSAHUJE ČASŤ = PAM. REPR. TR. A
IMPLICITNÁ KONVERZIA B → A

VIRTUÁLNE FUNKCIE

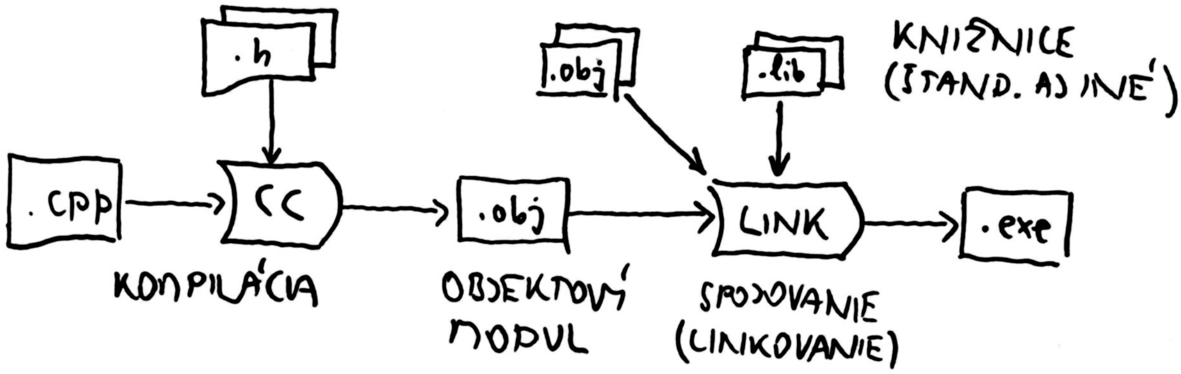
JEJ SPRÁVANIE JE URČENÉ ZA BEHU PROGRAMU
ZÁVISÍ OD SKUTOČNÉHO TYPU OBJEKTU (URČENÉHO ODKAZOM)
DÔLEŽITÉ KVÔLI POLYMORFIZMU

SKRYTÝ POINTER NA TABUĽKU VIRTUÁLNYCH FUNKCIÍ
VO VNÚTRI KAŽDÉHO OBJEKTU
PRE KAŽDÚ TRIEDU EXISTUJE JEDNA TAKÁ TABUĽKA

06.09.2008 So
PETER ČERNO

ŠTÁTNICE

6.2 ODDELENÝ PREKLAD, ZOSTAVENIE, RIADENIE PREKLADU



ZMYSEL ODDELENÉHO PREKLADU MODULOV - URÝCHLENIE CELKOVÉHO PREKLADU

STATICKÉ LINKOVANIE - PRI ODDELENOM PREKLADE JEDNOTLIVÉ OBJECT MODULY EŠTE NEOBSAHUJÚ PRIAMO ADRESY ∀ FCIÍ A EXTERNÝCH IDENTIFIKÁTOROV LINKER SA POSTARÁ O DOSADENIE SPRÁVNYCH ADRIES

DYNAMICKÉ LINKOVANIE - NASTÁVA PO VOLANÍ OPERAČNÉHO SYSTÉMU - ZAVEDENIE DYNAMICKEJ KNIŽNICE DO PAMÄTI

MAKEFILE - ZMYSLOM PROGRAMU MAKE JE RIADENIE PREKLADU A LINKOVANIE

6.3 NEPROCEDURÁLNE PROGRAMOVANIE, LOGICKÉ PROGRAMOVANIE

DEKLARATÍVNE PROGRAMOVANIE - PROGRAM JE ZALOŽENÝ NA TOM, ČO SA POČÍTA, NIE AKO SA POČÍTA

LOGICKÉ A FUNKCIONÁLNE PROG. SÚ ŠPECIÁLNYM PRÍPADOM DEKL. PROG.

LOGICKÉ PROG. JE ZALOŽENÉ NA VYHODNOCOVANÍ VZOROV - TVRDENÍ A CIEĽOV (PROLOG)

FUNKCIONÁLNE PROG. VYCHÁDZA Z λ-KALKULU (CHURCH)
{ TYPOVANÉ - HASKELL
{ NETYPOVANÉ - LISP, SCHEME
PROGRAM JE CHÁPANÝ AKO 1 FCIA OBSAHUJÚCA VSTUPNÉ PARAMETRY A 1 VÝSTUP

PROLOG

ZALOŽENÝ NA PREDIKÁTOVEJ LOGIKE 1. RÁDU (HORNOVE KLAUZULE), VYUŽITIE V AI
UNIFIKÁCIA, REKURZIA, BACKTRACKING
DÁTOVÉ TYPY = TERMY, ATÓMY, ŠTRUKTÚRY, ZOZNAMY

HASKELL

POUŽÍVA SKRÁTENÉ VYHODNOCOVANIE, DODRŽUJE REFERENČNÚ TRANSPARENTNOSŤ
PRÍSNE TYPOVANIE PREMENNÝCH

LISP (LIST PROCESSING)

VYUŽITIE HLAVNE V AI

06.01.2008 Sa
PETER ČERNO

ŠTÁTNICE

6.4 ŠTRUKTÚRA PREKLADAČA, LEXIKÁLNA, SYNTAKTICKÁ ANALÝZA

PREKLADAČ JE ZOBRAZENIE $L_{in} \to L_{out}$
PRE NEJAKÉ DVA JAZYKY L_{in} GENEROVANÝ GR. G_{in}
A L_{out} GEN. GR G_{out} ALEBO PRIJÍMANÝ AUT. A_{out}

BEŽNÉ PROG. JAZYKY SÚ ± BEZKONTEXTOVÉ,
POPR. SA NA BEZKONTEXTOVÉ PREVÁDZAJÚ

POUŽITIE: KOMPILÁTORY, SYNTAX HIGHLIGHTING,
PRETTY PRINTER, STATICKÉ KONTROLY PROGRAMU,
INTERPRETRY, DATABÁZOVÉ STROJE, DOTAZOVACIE JAZYKY

PREKLAD PROGRAMU

(1) ZDROJOVÝ KÓD $\xrightarrow{\text{PREPROCESOR}}$ TEXTOVÝ SÚBOR
(2) TEXT. SÚBOR $\xrightarrow{\text{PREKLADAČ}}$ ASSEMBLER
(3) ASEMBLEROM SA PREVEDIE NA OBJECT-FILE
(4) LINKER VYTVORÍ SPUSTITEĽNÝ SÚBOR

FÁZA PREKLADU PREKLADAČOM

FRONT-END (ANALÝZA ZDROJ. KÓDU PO LEXIKÁLNEJ
A) SYNTAKTICKEJ STRÁNKE, PREVOD DO MEDZIKÓDU)
(1) LEXIKÁLNA ANALÝZA - PREVÁDZA VSTUPNÝ TEXT
DO BINÁRNEJ FORMY - SLED IDENTIFIKÁTOROV A KONŠTÁNT
(2) SYNTAKTICKÁ ANALÝZA - ROZPOZNÁVA, ČI VSTUP
PATRÍ DO JAZYKA, BUDUJE „SYNTAKTICKÝ STROM" KÓDU
(3) SÉMANTICKÁ ANALÝZA - SKÚMA SÉMANTIKU
(KONTROLA TYPOV, POUŽÍVANIE DEF. PREMENNÝCH)
(4) GENEROVANIE MEDZIKÓDU - BINÁRNA FORMA KÓDU
(5) OPTIMALIZÁCIA MEDZIKÓDU

BACK-END:

(1) GENEROVANIE KÓDU - PRE KONKRÉTNU CPU ARCHITEKTÚRU
(2) OPTIMALIZÁCIA NÍZKOÚROVŇOVÉHO KÓDU

SYNTAX DRIVEN COMPILATION

NAJDÔLEŽITEJŠIA ČASŤ DNEŠNÝCH PREKLADAČOV
SYNTAKTICKÁ ANAL. SA VYKONÁVA ČASTO SPOLU
SO SÉMANTICKOU ANAL. A GENEROVANÍM MEDZIKÓDU
(VŠETKO 1 ZÁS. AUTOMAT)

AUTOMATICKÉ GENEROVANIE ČASTÍ PREKLADAČA

EXISTUJÚ NÁSTROJE, KT. GENERUJÚ NIEKTORÉ ČASTI
PREKLADAČA - GEN. LEXIKÁLNYCH ANALYZÁTOROV (FLEX),
SYNTAKTICKÝCH ANAL. = PARSEROV (BISON, COCO/R)
GENERÁTORY GENERÁTOROV KÓDU - MONO JIT COMPILER

MEDZIKÓD

VYSOKOÚROVŇOVÝ MEDZIKÓD - ROZHRANIE PRE PRECHOD
MEDZI FRONT-ENDOM A BACK-ENDOM

LEXIKÁLNA ANALÝZA - ZODPOVEDNÁ ZA ROZPOZNÁVANIE
ELEMENTOV ZDROJOVÉHO JAZYKA (IDENTIF., KĽÚČOVÉ SL., ...)

TOKEN - VÝSTUP LEX. ANALÝZY, 1 NEDELITEĽNÝ ELEMENT
LEXÉM - SEKVENCIA ZNAKOV V ZDROJ. SÚBORE, KT.
ZODPOVEDÁ NEJAKÉMU PATTERNU NEJAKÉHO TOKENU
LITERÁL - KONŠTANTA V ZDROJ. JAZYKU

ATRIBUT TOKENU - NAPR. RELAČNÝ OPERÁTOR
MÁ SPRESNENIE NAPR. „MENŠÍ ALEBO ROVNO"

PROBLÉMY LEX. ANALÝZY: ZAROVNANIE TEXTU,
IDENTIFIKÁTORY S MEDZERAMI, KĽÚČ. SLOVÁ AKO IDENTIF.,
KONTEXTOVO ZÁVISLÉ TOKENY

06.01.2008 Sa
PETER ČERNO

ŠTÁTNICE

SYNTAKTICKÁ ANALÝZA

(1) ROZHODNUTIE, ČI VSTUP PATRÍ DO SPRACOV. JAZYKA
(2) SYNTAXOU RIADENÝ PREKLAD
(3) STAVBA DERIVAČNÉHO STROMU

VYKONÁVANÁ ZÁSOBNÍKOVÝM AUTOMATOM

DERIVAČNÝ STROM

NEJEDNOZNAČNOSŤ (NAPR. DANGLING ELSE)
NUTNÉ ODSTRÁNIŤ → VYROBIŤ JEDNOZNAČNÚ GRAMATIKU
TAKISTO ĽAVÚ REKURZIU: $A \Rightarrow^* A\alpha$ TREBA ODSTRÁNIŤ
PROBLÉM MÔŽE BYŤ AJ ĽAVÁ FAKTORIZÁCIA: $A \to \alpha B$, $A \to \alpha\alpha$

INTERPRETOVANÝ JAZYK

ZDROJOVÝ JAZYK SA PREKLADÁ DO KÓDU NEJAKÉHO ABSTRAKTNÉHO STROJA
JIT (JUST IN TIME COMPILATION)
PODPORA GARBAGE COLLECTION

6.6 POJMY A PRINCIPY OBJEKTOVÉHO NÁVRHU

ANALÝZA

(1) KONCEPČNÝ MODEL – NEZÁVISLÝ NA IMPLEM.
ZACHYTÁVA KONCEPTY V PROBLÉMOVEJ DOMÉNE
(2) USE CASE – SCENÁR AKO UŽÍVATEĽ INTERAGUJE SO SYSTÉMOM

345676893

ICQ ROMAN

(3) SYSTEM SEQUENCE DIAGRAM - SCENÁRIO USE-CASEu
(4) UI DOKUMENTÁCIA
(5) RELAČNÝ DATOVÝ MODEL

DIZAJN

(1) DEFINOVANIE OBJEKTOV, CLASS DIAGRAMS
(2) IDENTIFIKOVANIE ATRIBÚTOV
(3) POUŽITIE NÁVRHOVÝCH VZOROV
(4) DEFINOVANIE APLIKAČNÉHO FRAMEWORKU
...

6.7 GENERICKÉ PROGRAMOVANIE

ZÁPIS ALGORITMU TAK, ABY PRACOVAL NAD OBECNÝM TYPOM,
KONKRÉTNY KOD DOSTANEME AŽ PO SUBSTITÚCII KONKR. TYPU
NAPR. TEPLATES (ŠABLONY) V C++
PRÍKLADY: TRIEDA PARAMETRIZOVANÁ TYPOM

```
template <typename T>
class List {...};
```

TYPOVO NEZÁVISLÁ FUNKCIA

```
template <typename T>
void Swap (T &a, T& b)
```

KNIŽNICA

ZBIERKA PROCEDÚR, FUNKCIÍ, ~~DAT.~~ TYPOV, POSKYTUJE API
PRÍKLAD: STL (v C++), DIRECT X, OPEN GL

NÁVRHOVÉ VZORY (DESIGN PATTERNS)

TVORIVÉ - FACTORY METHOD, ABSTR. FACTORY, BUILDER, SINGLETON, PROTOTYPE
ŠTRUKTÚR. - ADAPTER, BRIDGE, COMPOSITE, DECORATOR, FACADE, PROXY
BEHAV. - INTERPR., TEMPL. METHOD, COMMAND, STRATEGY, ...

07.08.2008 Su
PETER ČERNO

ŠTÁTNICE

ZHRNUTIE

1 ČÍSLA

$\lim a_n = A \Leftrightarrow \limsup a_n = \liminf a_n = A$, $A \in \mathbb{R}^*$
BOLZANO-WEIERSTRASS : Z KAŽDEJ OHRANIČ. POST. MÔŽEME VYBRAŤ KONVERGENTNÚ PODPOSTUPNOSŤ
BOLZANO-CAUCHY

2 ZÁKLADY DIFERENCIÁLNEHO POČTU

HEINEHO VETA, VETA O LIMITE ZLOŽENEJ FCIE.,
DARBOUXOVA VETA, f SPOJ. NA $\langle a,b\rangle$ NADOBÚDA MAX., MIN.
VETA O DER. ZLOŽENEJ FCIE., INV. FCIE.
ROLLEOVA VETA, LAGRANGEOVA VETA, CAUCHYOVA VETA
L'HOSPITALOVO PRAVIDLO, VETA O LIMITE DERIVÁCIE
INFLEXIA, KONVEXNOSŤ, KONKÁVNOSŤ
TAYL. POL. $T_n^{f,a}(x) = f(a) + f'(a)\frac{x-a}{1!} + \dots + f^{(n)}(a)\frac{(x-a)^n}{n!}$

OBECNÝ TVAR ZVYŠKU: NECH $x > a$, f MÁ VLASTNÚ $(n+1)$-VÚ DERIVÁCIU NA $\langle a,x\rangle$, φ JE SPOJITÁ NA $\langle a,x\rangle$ A MÁ VLASTNÚ $\varphi' \neq 0$ NA (a,x) $\Rightarrow$
$\exists \xi \in (a,x)$: $R_n^{f,a}(x) = f(x) - T_n^{f,a}(x) =$

$$\boxed{\frac{1}{n!}\,\frac{\varphi(x)-\varphi(a)}{\varphi'(\xi)}\cdot f^{(n+1)}(\xi)\cdot(x-\xi)^n}$$

LAGR. TVAR $\varphi(t) = (x-t)^{n+1}$
CAUCH. TVAR $\varphi(t) = t$

3 POSTUPNOSTI A RADY FUNKCIÍ

BOLZANO-CAUCHYHO NUTNÁ A POSTAČ. PODM. K $f \rightrightarrows$
MOORE-OSGOOD,
PRE $\{f_n\}_{n=1}^{\infty}$ NECH $\forall n$ f_n' VLASTNÁ NA (a,b),
$\exists c \in (a,b)$: $f_n(c)$ KONVERGUJE, $f_n' \rightrightarrows f$ NA (a,b)
$\Rightarrow f_n \rightrightarrows F$ NA (a,b), $F' = f$.
RAD FUNKCIÍ, NUTNÁ PODM. $\sum f_n \rightrightarrows \;\Rightarrow f_n \rightrightarrows 0$

POROVNÁVACIE KRIT., WEIERSTRASSOVÉ KRIT., LEIBNIZOVO KR.,
DIRICHLETOVO KR. : (i) $\exists K > 0 \ \forall n \ |\sum_{i=1}^{n} u_i| < K$
(ii) $\forall x \ \{v_n(x)\}_{n=1}^{\infty}$ MONOTÓNNA, $v_n \rightrightarrows 0$
POTOM $\sum u_n \cdot v_n \rightrightarrows$
ABELOVO KR. : (i) $\exists K > 0 \ \forall n \ |v_n| < K$, $\forall x \ \{v_n(x)\}$ MON.
(ii) $\sum u_n \rightrightarrows$
$\Rightarrow \sum u_n \cdot v_n \rightrightarrows$

MOCNINNÉ RADY $\sum_{n=0}^{\infty} a_n (z - z_0)^n$, POLOMER KONVERGENCIE
TAYLOROVE RADY $\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} (x-a)^n$
FOURIEROVE RADY : f $2l$-PERIODICKÁ, LEB. INT. NA OHRANIČ. INT.

$$a_n = \frac{1}{l} \int_{-l}^{+l} f(x) \cdot \cos\left(n x \cdot \frac{l}{\pi}\right) \quad n = 0, 1, 2, \ldots$$
$$b_n = \frac{1}{l} \int_{-l}^{+l} f(x) \cdot \sin\left(n x \cdot \frac{l}{\pi}\right) \quad n = 1, 2, 3, \ldots$$
FOURIEROVE KOEFICIENTY !!

$\frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cos\left(n x \cdot \frac{l}{\pi}\right) + b_n \sin\left(n x \cdot \frac{l}{\pi}\right)\right)$ TRIGONOM. FOUR. RAD
AK f PO ČASTIACH HLADKÁ, POTOM BODOVO $\to \frac{f(x+) + f(x-)}{2}$
PARSEVALOVA ROVNOSŤ : $\frac{1}{l} \int_a^{a+2l} f^2(x)\, dx = \frac{a_0^2}{2} + \sum_{n=1}^{\infty} (a_n^2 + b_n^2)$

4 INTEGRÁL

$\int F \cdot g = F \cdot G - \int f \cdot G$

PRIMITÍVNA FUNKCIA, PER PARTES, SUBSTITÚCIA
FORMÁLNE IDE O: $\int f(y) \cdot dy = \int f(g(x)) \cdot g'(x)\, dx$
1. VETA O SUBST. : F PRIM. FCIA K f NA (A, B),
g SPOJITÁ, VL. DERIVÁCIE NA (a, b), $g[(a,b)] \subseteq (A, B)$
$\Rightarrow \int f(g(x))\, g'(x)\, dx = F(g(x)) + C$ NA (a, b)
2. VETA O SUBST. : f SPOJITÁ NA (A, B),
g BIJEKCIA $(a, b) \to (A, B)$, VL. DERIVÁCIE NA (a, b)
AK H JE PRIMIT. FCIA K $f(g(x))\, g'(x)$ NA (a, b),
$\Rightarrow \int f(y) \cdot dy = H(g^{-1}(y)) + C$ NA (A, B)

URČITÝ RIEMANNOV INT., DELENIE $\langle a, b \rangle$, $s(f, D)$, $S(f, D)$,
KRITÉRIUM EXISTENCIE, POST. PODM. EXISTENCIE
ADITIVITA RIEM. INTEGRÁLU

07.09.2008 Su
PETER ČERNO

ŠTÁTNICE

RIEMANNOV INT. AKO PRIMIT. FCIA: NECH f JE OHRAN. NA $\langle a,b\rangle$ DEFINUJME $F(x) = \int_a^x f(t)\,dt$ NA $\langle a,b\rangle$. POTOM
(i) F JE SPOJITÁ NA $\langle a,b\rangle$ (ii) AK f JE SPOJITÁ V $x_0 \in (a,b)$, POTOM $F'(x_0) = f(x_0)$

ZÁKLADNÁ VETA ANALÝZY: NECH f JE SPOJITÁ NA $\langle a,b\rangle$, F PRIMITÍVNA K f NA (a,b). POTOM $\exists\, F(a+), F(b-)$ A PLATÍ $(R)\int_a^b f(x)\,dx = F(b-) - F(a+)$.

NEWTONOV INTEGRÁL: $(N)\int_a^b f(x)\,dx = F(b-) - F(a+)$.
DĹŽKA KRIVKY, OBJEM ROTAČNÉHO TELESA
INTEGRÁLNE KRIT. KONV. !!! f SPOJITÁ, NEZÁPORNÁ, NERASTÚCA !!!
$\sum_{n=1}^{\infty} f(n)$ KONV. $\Leftrightarrow$ $(N)\int_{n_0}^{\infty} f(x)\,dx < \infty$, $n_0 \in \mathbb{N}$

VIACROZMERNÝ INT.: KOMPAKTNÝ INTERVAL V E_n, DELENIE, ČLEN ROZDELENIA D, $|D|$ MAX. $\forall$ ČLENOV, vol J

FUBINIOVA VETA: $J = J' \times J''$ KOMPAKT. V E_n, POTOM
$\int_J f(\vec{x},\vec{y})\,d\vec{x}\,d\vec{y} = \int_{J'}\left(\int_{J''} f(\vec{x},\vec{y})\,d\vec{y}\right)d\vec{x} = \int_{J''}\left(\int_{J'} f(\vec{x},\vec{y})\,d\vec{x}\right)d\vec{y}$.

$\vec{f}$ JE REGULÁRNE $\Leftrightarrow$ MÁ SPOJ. PARC. DER. NA U A $\frac{D(f_1,\dots,f_n)}{D(x_1,\dots,x_n)}(\vec{x}) \neq 0$ NA $\vec{U}$

SUBSTITÚCIA: $U \subseteq \mathbb{R}^n$ OTVORENÁ, JAKOBIÁN $\longrightarrow$
$\varphi: U \to \mathbb{R}^n$ REGULÁRNE ZOBR., $A \subseteq U$ UZAVRETÁ V $\mathbb{R}^n$
$\Rightarrow \int_A f(\varphi(\vec{t}))\cdot \frac{D(\varphi)}{D(\vec{t})}(\vec{t})\cdot d\vec{t} = \int_{\varphi(A)} f(\vec{x})\,d\vec{x}$ (AK $\exists$ PRAVÁ STRANA)

5. ZÁKLADY TEÓRIE FUNKCIÍ VIAC PREMENNÝCH

PARCIÁLNA DERIVÁCIA $\frac{\partial f}{\partial x_i}$, GRADIENT ∇f, DERIVÁCIA V SMERE $D_v f$
TOTÁLNY DIFERENCIÁL $Df(a)(h)$ LIN. ZOBR.:
$$\lim_{\|h\|\to 0} \frac{f(x+h) - f(x) - Df(a)(h)}{\|h\|} = 0$$
AK EXISTUJE, POTOM $D_h f(a) = Df(a)(h) = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(a)\cdot h_i$
ARITMETIKA TOT. DIF.

DIF. ZLOŽENÉHO ZOBRAZENIA: $\exists Df(a)$, $\exists Dg_i(b)\ \forall i$, $a_i = g_i(b)$
$\Rightarrow F(x) = f(g_1(x), \dots, g_n(x))$ $\exists DF(b)$ A PLATÍ
$$DF(b)(h) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \frac{\partial f}{\partial y_j}(a) \cdot \frac{\partial g_j}{\partial x_i}(b) \right) \cdot h_i$$
$$\Rightarrow \frac{\partial F}{\partial x_i}(b) = \sum_{j=1}^{n} \frac{\partial f}{\partial y_j}(a) \cdot \frac{\partial g_j}{\partial x_i}(b)$$

POSTAČ. PODMIENKA $\exists$ TOT. DIF.: SPOJITÉ PARC. DERIVÁCIE

KEĎ MÁ KAŽDÁ PARC. DERIVÁCIA V BODE a TOT. DIFERENCIÁL, POTOM TOT. DIF. 2. RÁDU $D^2 f(a): \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$,
$$D^2 f(a)(h, k) = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\partial^2 f(a)}{\partial x_i \partial x_j} h_i \cdot h_k.$$

VETA O STR. HODNOTE: f MÁ SPOJ. PARC. DERIVÁCIE NA ÚSEČKE a, b.
$$\Rightarrow \exists \xi \in (0,1): f(b) - f(a) = \nabla f(a + \xi(b-a)) \cdot (b-a).$$

VETA O IMPLICITNÝCH FUNKCIÁCH:

(1) $F: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ SPOJITÉ PARC. DERIVÁCIE, $x_0, y_0 \in \mathbb{R}$, $F(x_0, y_0) = 0$,
$\frac{\partial F}{\partial y}(x_0, y_0) \neq 0$ $\Rightarrow$ $\exists U$ OKOLIE x_0, V OKOLIE y_0
$\forall x \in U\ \exists! y \in V: F(x,y) = 0$, OZNAČME $y = \varphi(x)$.
POTOM φ JE DIFERENCOVATEĽNÁ NA U A PLATÍ
$$\frac{\partial \varphi}{\partial x}(x) = - \frac{\frac{\partial F}{\partial x}(x, \varphi(x))}{\frac{\partial F}{\partial y}(x, \varphi(x))}$$

(2) $F: G \to \mathbb{R}$, $G \subseteq \mathbb{R}^{n+1}$ OTVORENÁ, SPOJ. PARC. DERIVÁCIE,
$x_0 \in \mathbb{R}^n$, $y_0 \in \mathbb{R}$, $F(x_0, y_0) = 0$, $\frac{\partial F}{\partial y}(x_0, y) \neq 0$, POTOM ...
$$\frac{\partial \varphi}{\partial x_i}(x) = - \frac{\frac{\partial F}{\partial x_i}(x, \varphi(x))}{\frac{\partial F}{\partial y}(x, \varphi(x))}$$

VETA O INVERZNEJ FCII. $F: G \to \mathbb{R}^n$, $G \subseteq \mathbb{R}^n$ OTVORENÁ,
f_i MAJÚ SPOJ. PARC. DERIVÁCIE, $x_0 \in G$, $|JF(x_0)| \neq 0$, $y_0 = F(x_0)$
$\Rightarrow$ EXISTUJÚ OKOLIA U, V BODOV x_0, y_0 T.Ž.
F JE BIJEKCIA $U \to V$ A $JF^{-1}(y_0) = (JF(x_0))^{-1}$

07.09.2008 Su
PETER ČERNO

ŠTÁTNICE

LAGRANGEOVE MULTIPLIKÁTORY : $G \subseteq \mathbb{R}^n$ OTV., $F, g_1, \dots, g_m : G \to \mathbb{R}$ ($m<n$) SPOJ. PARC. DERIVÁCIE, $M = \{x \in G \mid g_1(x) = \dots = g_m(x) = 0\}$.
AK F MÁ NA M LOK. EXTRÉM V BODE $a \in M$ A $\nabla g_1(a), \dots, \nabla g_m(a)$ SÚ LIN. NEZÁVISLÉ
$\Rightarrow \exists \lambda_1, \dots, \lambda_m \in \mathbb{R} : DF(a) + \lambda_1 Dg_1(a) + \dots + \lambda_m Dg_m(a) = 0.$

6. METRICKÉ PRIESTORY

METRICKÝ PRIESTOR (M, d), OTVORENÉ MN., OKOLIA, TOPOLÓGIA ...
$A \subseteq M$ JE UZ. $\Leftrightarrow$ (AK $\{x_n\} \subseteq A$ KONV. $\Rightarrow \lim x_n \in A$.)
$f : (X, \rho) \to (Y, \sigma)$ JE SPOJITÉ (7 EKV.), ROVNOMERNE SPOJITÉ, HOMEOMORFIZMUS
(X, ρ) JE KOMPAKTNÝ $\Leftrightarrow$ Z KAŽDEJ POSTUPNOSTI MOŽNO VYBRAŤ KONVERGENTNÚ PODPOSTUPNOSŤ
!!! KAŽDÝ KOMPAKTNÝ PODPRIESTOR (METR. PR.) JE UZAVRETÝ
!!! KEĎ JE (X, ρ) KOMPAKTNÝ $\Rightarrow$ KAŽDÝ UZAV. PODPR. JE KOMPAKTNÝ !!
NECH f JE SPOJITÉ ZOBR. KOMPAKT. (X, ρ) DO (Y, σ)
(i) f JE ROVNOMERNE SPOJITÉ
(ii) $f[X]$ JE KOMPAKTNÝ PODPR. Y
(iii) f JE PROSTÉ $\Rightarrow$ f JE ROVN. HOMEOM. $X \to f[X]$

PODPRIESTOR EUKL. PR. JE KOMP. $\Leftrightarrow$ JE OHRANIČ. A UZAVR.
KAŽDÝ KOMP. $I \subseteq \mathbb{R}$ NADOBÚDA MAXIMA, MINIMA.

(X, ρ) JE ÚPLNÝ $\Leftrightarrow$ KAŽDÁ CAUCH. POST. KONVERGUJE.
!!! KAŽDÝ KOMPAKTNÝ PRIESTOR JE ÚPLNÝ !!!
!!! PODPR. Y ÚPLNÉHO PR. X JE ÚPLNÝ $\Leftrightarrow$ Y JE UZAVRENÝ V X !!!

PICKARDOVA - BANACHOVA VETA : KAŽDÉ KONTRAHUJÚCE ZOBRAZENIE ÚPLNÉHO PRIESTORU DO SEBA MÁ PRÁVE JEDEN PEVNÝ BOD A KAŽDÁ POSTUPNOSŤ ITERÁCIÍ TOHTO ZOBR. KONVERGUJE K TOMUTO BODU

7 DIFERENCIÁLNE ROVNICE

OBYČAJNÉ DIF. R. 1. RÁDU : $y' = f(x,y)$, $f: \mathbb{R}\times\mathbb{R}^n \to \mathbb{R}^n$, $y: \mathbb{R}\to\mathbb{R}^n$

OBYČ. DIF. R. n-TÉHO RÁDU : $F(x, y, y', \dots, y^{(n)}) = 0$, $F: \mathbb{R}^{n+2} \to \mathbb{R}$, $y: \mathbb{R}\to\mathbb{R}$

1. ROV. SO SEPAR. PREM. : $y' \cdot h(y) = g(x)$ $\qquad H(y(x)) = G(x) + C$
2. LIN. DIF. ROV. 1. RÁDU : $y' + p(x)\cdot y = q(x)$, INTEGR. FAKTOR $e^{P(x)}$

   $(y\cdot e^{P(x)})' = q(x)\cdot e^{P(x)}$

   EXAKTNÉ ROV. : $y' f(x,y) + g(x,y) = 0 \rightsquigarrow \frac{\partial}{\partial x} F(x, y(x)) = 0 \Leftrightarrow \frac{\partial f}{\partial x} = \frac{\partial g}{\partial y}$

3. LIN. DIF. ROV. n-TÉHO RÁDU: $L(y) \equiv y^{(n)} + a_{n-1}(x)\, y^{(n-1)} + \dots + a_0(x)\cdot y = f(x)$

   AK SÚ $\forall$ FCIE SPOJITÉ NA (α, β), POTOM

(i) MNOŽINA $\forall$ RIEŠENÍ $L(y) = 0$ JE VEKT. PRIESTOR DIM. n

(ii) $\forall$ RIEŠENIA $L(y) = f$ MAJÚ TVAR $y_0 + y_h$, KDE $L(y_0) = f$, y_h HOM. RIEŠ.

METÓDA VARIÁCIE KONŠTÁNT

NECH $y' + a_0(x)\, y = f(x)$ MÁ HOM. RIEŠENIE y_h.

y_0 HĽADÁME V TVARE $k(x)\cdot y_h(x)$.

FUNDAMENTÁLNY SYS. PRE LIN. DIF. ROV. n-TÉHO RÁDU S KONŠT. KOEF.

CHARAKT. POLYNÓM $\chi(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0$

!! $\lambda \in \mathbb{R}$ KOREŇ NÁS. p : $e^{\lambda x}, \dots, x^{p-1} e^{\lambda x}$

$\alpha \pm i\beta$ NÁS. p : $e^{\alpha x}\cos\beta x, \dots, x^{p-1} e^{\alpha x}\cos\beta x$ (AJ PRE $\sin$)

ŠPECIÁLNA PRAVÁ STRANA: $e^{\alpha x}(P_1(x)\cos\beta x + P_2(x)\sin\beta x)$

4. SÚSTAVA LIN. DIF. ROV. 1. RÁDU

   $y' = A(x)\cdot y + b(x)$, $A: \mathbb{R}\to\mathbb{R}^{n\times n}$, $b: \mathbb{R}\to\mathbb{R}^n$

   MN. RIEŠ. HOM. SÚSTAVY - VEKT. PRIESTOR DIM. n

   WRONSKIÁN $f_1, \dots, f_n : I \to \mathbb{R}^n$

   $W_{f_1,\dots,f_n}(x) = \det\left(f_1(x), \dots, f_n(x)\right)$

!! AK $f_1, \dots, f_n$ SÚ RIEŠENIA $y' = A\cdot y$, $A \in \mathbb{R}^{n\times n}$

POTOM : $f_1, \dots, f_n$ SÚ LIN. ZÁVISLÉ $\Leftrightarrow W(x) = 0\ \forall x \in I$

$\Leftrightarrow \exists x_0 \in I\ W(x_0) = 0$.

07.09.2008 Sa
PETER ČERNO

ŠTÁTNICE

8 ALGEBRA

POZRI SYLABUS J. ŽEMLIČKY

LINEÁRNA ALGEBRA

MATICA V ODSTUPŇOVANOM TVARE $\exists r, 0 \le r \le m, \dots,$ PIVOTY
GAUSSOVA ELIMINÁCIA
A JE REGULÁRNA $\Leftrightarrow$ $Ax = 0$ MÁ JEDINÉ RIEŠENIE $x = 0$
VEKTOROVÝ PRIESTOR V NAD TELESOM T, PODPRIESTOR
PODPRIESTOR GENEROVANÝ X: $\mathcal{L}(X)$, LIN. KOMBINÁCIA
RIADKOVÝ / STĹPCOVÝ PRIESTOR A, JADRO Ker A
$(v_1, \dots, v_n)$ JE LIN. NEZ. $\Leftrightarrow$ $(a_1 v_1 + \dots + a_n v_n = 0 \Rightarrow a_1 = \dots = a_n = 0)$
B JE SYSTÉM GEN. $\Leftrightarrow$ span(B) = V, KONEČNE GEN. PR.
BÁZA = LIN. NEZÁVISLÝ SYS. GENERÁTOROV
LEMMA O VÝMENE: AK $G = (v_1, \dots, v_n)$ JE SYS. GEN,
$w = a_1 v_1 + \dots + a_n v_n$, POTOM AK $a_i \neq 0$, POTOM A)
$(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n)$ JE SYS. GEN.
<u>STEINITZOVA VETA O VÝMENE</u>: KEĎ JE $N = (w_1, \dots, w_m)$
LIN. NEZ. SYS. A $G = (v_1, \dots, v_n)$ SYS. GEN, POTOM:
$m \le n$ A NIEKTORÉ Z m VEKT. G MOŽNO NAHRADIŤ VEKT. N → SYS. GEN.
VEKTOR SÚRADNÍC $[v]_B$
HODNOSŤ MATICE $\text{rank}(A) := \dim R(A)$
NÁSOBENIE REG. MATICOU ZĽAVA (≡ ELEM. RIADKOVÉ ÚPRAVY)
NEMENIA RIADKOVÝ PRIESTOR, ANI <u>DIMENZIU</u> STĹPC. PR.
$\Rightarrow \text{rank}(A) = \dim \mathcal{S}(A)$, $\text{Ker}\, A + \text{rank}(A) = n$
<u>LINEÁRNE ZOBRAZENIE</u> $f: U \to V$ <u>NAD ROVNAKÝM T</u>
NECH B JE BÁZA U, POTOM ZOBR. $f: B \to V$ SA DÁ
ROZŠÍRIŤ NA LIN. ZOBR. $U \to V$ PRÁVE JEDNÝM SPÔSOBOM

MATICA f VZHĽADOM K BÁZAM B, C : $[f]_B^C = \left([f(b_j)]_C \right)$

$\forall u \in U$: $[f(u)]_C = [f]_B^C \cdot [u]_B$

MATICA PRECHODU OD B K C : $[id]_B^C$

AFINNÝ PODPRIESTOR : $F \subseteq V$, KT. JE BUĎ PRÁZDNA, ALEBO TVARU $x + U$, KDE U JE PODPRIESTOR V

$f^{-1}(b)$ JE AF. PODPR. U A MÁ TVAR $x_0 + \mathrm{Ker} f$, KDE $f(x_0) = b$

PRIESTORY SO SKALÁRNYM SÚČINOM NAD $\mathbb{C}$ (ALEBO $\mathbb{R}$) !!!

$\langle u | v \rangle : V \times V \to \mathbb{R}$ $\quad \langle v|v\rangle \geq 0 \quad = 0 \Leftrightarrow v = 0$

$\langle au|v\rangle = a\langle u|v\rangle$, $\langle u+v|w\rangle = \langle u|w\rangle + \langle v|w\rangle$, $\langle v|u\rangle = \overline{\langle u|v\rangle}$

STANDARDNÝ SK. SÚČIN $x^T y$, NORMA $\|\cdot\|$, $\sqrt{\langle v|v\rangle}$

l_1 NORMA (MANHATTANSKÁ), l_∞ (MAXIMOVÁ)

CAUCHY-SCHWARZ : $\langle u|v\rangle \leq \|u\| \cdot \|v\|$ $\quad (p(t) = \langle u+tv | u+tv\rangle)$

ORTOGONÁLNY SYSTÉM, ORTONORMÁLNY $z_1, \dots, z_n$

$\langle v | z_i \rangle$ FOURIEROV KOEF.

GRAM-SCHMIDTOVA ORTOGONAL. : VSTUP: BÁZA $v_1, \dots, v_n$

$y_k = v_k - \sum_{i=1}^{k-1} \langle v_k | z_i \rangle \cdot z_i$, $\quad z_k = y_k / \|y_k\|$

ORTOGONÁLNY DOPLNOK $M^\perp = \{ v \in V \mid \langle v|x\rangle = 0 \ \forall x \in M \}$

ORTOGONÁLNA MATICA A : $AA^T = I$

ORTOGONÁLNA PROJEKCIA NA W

DETERMINANT $\det(A) = \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^n a_{i,\pi(i)}$

$\det(A^T) = \det(A)$, det JE LIN. FCIA. KAŽDÉHO RIADKU / STĹPCA

A JE REG. $\Leftrightarrow \det(A) \neq 0$, $\quad \det(A \cdot B) = \det(A)\det(B)$

$(A^{-1})_{ij} = (-1)^{i+j} \det(A_{ji}) / \det(A)$

CRAMEROVO PRAVIDLO : A REGULÁRNA, $Ax = b$, $x_i = \dfrac{\det(A_{i \to b})}{\det(A)}$

VLASTNÉ ČÍSLA $f: V \to V$,

AK A JE MATICA f VZHĽADOM K B, POTOM TAT^{-1} JE MATICA f VZHĽADOM K B', KDE $T = [id]_B^{B'}$

A, A' SÚ PODOBNÉ $\Leftrightarrow A' = TAT^{-1}$ PRE T REGULÁRNU

07. 09. 2008 SU
PETER ČERNO

ŠTÁTNICE

(PODOBNE PRE MATICU A)

$\lambda \in T$ JE VL. ČÍSLO $f \iff \exists v \neq 0 : f(v) = \lambda v$, v JE VL. VEKTOR K λ

VETA: AK $\lambda_1, \dots, \lambda_k$ SÚ RÔZNE VL. ČÍSLA A $v_1, \dots, v_k$ SÚ PRÍSLUŠNÉ VL. VEKTORY $\Rightarrow$ SÚ LIN. NEZÁVISLÉ

VLASTNÉ ČÍSLA SÚ PRÁVE KORENE CHAR. POL. $p_A(t) = \det(A - tI)$.

PRE PODOBNÉ MATICE A, B JE $p_A = p_B$.

PRE $p_A(t) = (-1)^n t^n + c_{n-1} t^{n-1} + \dots + c_0$ JE $c_0 = \det A$, $c_{n-1} = (-1)^{n-1} \operatorname{trace} A$

MATICA A NIE JE DIAGONIZ. $\iff$ MÁ VLASTNÉ ČÍSLO $\lambda \in \mathbb{C}$: $\operatorname{Ker}(A - \lambda I) <$ NÁSOBNOSŤ λ V $p_A(t)$

JORDANOV NORMÁLNY TVAR, JORDANOVE BUNKY

ORTOGONÁLNE $f : V \to V$: $\langle f(u) | f(v) \rangle = \langle u | v \rangle$

VETA: KAŽDÁ SYMETRICKÁ $A \in \mathbb{R}^{n \times n}$ MÁ $\forall$ VL. ČÍSLA REÁLNE A EXISTUJE ORTOGONÁLNA T TAKÁ, ŽE TAT^{-1} JE DIAGONÁLNA.

NECH A JE SYMETRICKÁ

$\Rightarrow$ POZITÍVNE [SEMI] DEFINITNÁ A : $\forall x \neq 0 \; x^T A x > 0 \quad (\geq)$

(i) A JE POZ. [SEMI] DEF.
(ii) $\forall$ VL. ČÍSLA SÚ KLADNÉ (NEZÁPORNÉ)
(iii) $\exists U : U^T U = A$ (PRI POZ. DEF. $\operatorname{rank}(U) = n$)

U MÔŽE BYŤ HORNÁ Δ $\to$ CHOLESKÉHO ROZKLAD

$x^T A y$ DEF. SKALÁRNY SÚČIN NA $\mathbb{R}^n$

KVADRATICKÁ FORMA $f(x_1, \dots, x_n) = \sum_{i=1}^{n} \sum_{\underline{\underline{j=i}}}^{n} a_{ij} x_i x_j$

$f(x) = x^T B x$, B JE MATICA KV. FORMY (JE SYMETRICKÁ)

BILINEÁRNA FORMA $b : V \times V \to T$ (LINEÁRNA V OBOCH ZLOŽ.)

$\Rightarrow$ KVADR. FORMA $f(v) = b(v, v)$

PRE BÁZU $v_1, \dots, v_n$ JE $B_{ij} = \frac{1}{2}\left(f(v_i + v_j) - f(v_i) - f(v_j)\right)$

SYLVESTROV ZÁKON ZOTRVAČNOSTI KV. FORIEM

PRE KAŽDÚ SYMETRICKÚ A $\exists$ REGULÁRNA S (S ORTOGON. STĹPCAMI), ŽE $S^T B S$ JE DIAGONÁLNA S $+1, -1, 0$, $\#{+1}$, $\#{-1}$ SA NEMENÍ

KOMBINATORIKA A TEÓRIA GRAFOV

J. MATOUŠEK, J. NEŠETŘIL -
KAPITOLY Z DISKRÉTNÍ MATEMATIKY

T. VALLA, J. MATOUŠEK -
KOMBINATORIKA A GRAFY II

07. 09. 2008 Su
PETER ČERNO

ŠTÁTNICE

1 LOGIKA

VETA O KOMPAKTNOSTI VÝR. LOGIKY : T JE SPLNITEĽNÁ $\Leftrightarrow$ KAŽDÁ KONEČNÁ $T_0 \subseteq T$ JE SPLNITEĽNÁ
FORMÁLNY SYSTÉM VÝR. LOGIKY, DÔKAZ, DOKÁZ. FORMULA, $\vdash$
VETA O DEDUKCII, LEMMA O NEUT. FORMULI
$p_1^v, \dots, p_n^v \vdash A^v \Rightarrow$ VETA O ÚPLNOSTI : $\vdash A \Leftrightarrow \models A$
MNOŽINA FORMULÍ JE BEZSPORNÁ $\Leftrightarrow$ JE SPLNITEĽNÁ
SILNÁ VETA O ÚPLNOSTI : $T \vdash A \Leftrightarrow T \models A$
VETA O EKVIVALENCII, VETA O DÔKAZE ROZBOROM PRÍPADOV
JAZYK 1. RÁDU, TERM, ATOMICKÁ FORMULA, FORMULA,
VOĽNÝ / VIAZANÝ VÝSKYT, OTVORENÁ / UZAVRETÁ FORMULA
RELAČNÁ ŠTRUKTÚRA $\mathcal{M}$, UNIVERZUM M, OHODNOTENIE e
TARSKÉHO DEFINÍCIA PRAVDY : $\mathcal{M} \models A[e]$, $\mathcal{M} \models A$
SUBSTITÚCIA TERMOV $t_{x_1, \dots x_n}[t_1, \dots, t_n]$, $A_{x_1, \dots, x_n}[t_1, \dots, t_n]$
SUBSTITUOVATEĽNÝ TERM
FORMÁLNY SYSTÉM BEZ ROVNOSTI : A1, A2, A3
AX. ŠPECIFIKÁCIE : $(\forall x)A \to A_x[t]$
SCHÉMA PRESKOKU : $(\forall x)(A \to B) \to (A \to (\forall x)B)$ x NEMÁ VOĽNÝ VÝSKYT V A
ODV. PRAVIDLÁ : MP, PRAVIDLO GENERALIZÁCIE $A \,/\, (\forall x)A$
PRAVIDLO ZAVEDENIA $\forall$: $A \to B \,/\, A \to (\forall x)B$, x NEMÁ V.V. V A
PR. ZAVEDENIA $\exists$: $A \to B \,/\, (\exists x)A \to B$ x NEMÁ VOĽNÝ VÝS. V B
VETA O INŠTANCIÁCH : $A \,/\, A'$ A' JE INŠT. A
VETA O UZÁVERE : $\vdash A \Leftrightarrow \vdash A'$ A' JE UZÁVER A
VETA O DISTRIBÚCII KVANT. : $A \to B \,/\, (\Box x)A \to (\Box x)B$
A' JE VARIANTA A $(\Box x)B \rightsquigarrow (\Box y)B_x[y]$ y NIE JE V. V B
VETA O VARIANTÁCH : $\vdash A \Leftrightarrow A'$ A' JE VARIANTA A
VETA O DEDUKCII : $T \vdash A \to B \Leftrightarrow T, A \vdash B$, A UZAVRETÁ
VETA O KONŠT. : $T \vdash A \Leftrightarrow T \vdash A_{x_1, \dots, x_n}[c_1, \dots, c_n]$

VETA O REDUKCII: $T \vdash A \Leftrightarrow \exists$ UZÁVERY $B_1, \dots, B_n$ NEJAKÝCH FÚĽ Z T: $\vdash B_1 \to (B_2 \to \dots (B_n \to A) \dots)$

$T \vdash A \Leftrightarrow T, \neg A'$ JE SPORNÁ, A' JE UZÁVER A

PRENEXNÝ TVAR: $(\square_1 x_1) \dots (\square_n x_n) B$, B = OTVORENÉ JADRO

PRENEXNÉ OPERÁCIE:

(a) B NAHRAĎ VARIANTOU B'

(b) $\neg(\square x) B$ NAHRAĎ $(\bar{\square} x) \neg B$

(c) $B \to (\square x) C$ NAHRAĎ $(\square x)(B \to C)$, x NEMÁ V.V. V B

(d) $(\square x) B \to C$ NAHRAĎ $(\bar{\square} x)(B \to C)$, —″— V C

(e) $(\square x) B \triangle C$ NAHRAĎ $(\square x)(B \triangle C)$ —″— V C

FORMÁLNY SYSTÉM S ROVNOSŤOU: NAVYŠE R1, R2, R3

R1 $x = x$, R2 $x_1 = y_1 \to (\dots (x_n = y_n \to f(\vec{x}) = f(\vec{y})) \dots)$

R3 $x_1 = y_1 \to (\dots (x_n = y_n \to (p(\vec{x}) \to p(\vec{y}))) \dots)$

$\Rightarrow$ SYMETRIA, TRANZITIVITA $=$, VETA O ZÁMENE t_i, s_i

T-PLATNÁ FORMULA: $T \models A$, A SPLNENÁ V KAŽDOM MODELI T

VETA O KOREKTNOSTI: $T \vdash A \Rightarrow T \models A$

VETA O ÚPLNOSTI: (i) $T \vdash A \Leftrightarrow T \models A$

(ii) T JE BEZSPORNÁ $\Leftrightarrow$ T MÁ MODEL

ÚPLNÁ TEÓRIA: BEZSPORNÁ & $\forall$ UZÁV. A: $T \vdash A \vee T \vdash \neg A$

HENKINOVA TEÓRIA $\forall (\exists x) B \; \exists c$: $T \vdash (\exists x) B \to B_x[c]$

T' [KONZERVATÍVNE] ROZŠÍRENIE T

HENKIN: KU KAŽDEJ T MOŽNO ZOSTR. KONZ. HENK. ROZŠÍRENIE T_H

LINDENBAUM: BEZSP. T MÁ ÚPLNÉ ROZŠÍR. S TÝM ISTÝM JAZYKOM

REDUKCIA A EXPANZIA ŠTRUKTÚR $\mathcal{M}' \rightsquigarrow \mathcal{M} = \mathcal{M}'|_L$

KAŽDÁ ÚPLNÁ HENKINOVA TEÓRIA MÁ MODEL

VETA O KOMPAKTNOSTI: T MÁ MODEL $\Leftrightarrow$ $\forall T_0$ KONEČNÁ $\subseteq T$ MÁ MODEL.

07.09.2008 Su
PETER ČERNO

ŠTÁTNICE

REKURZÍVNA FUNKCIA $f: \mathbb{N}^k \to \mathbb{N}$, REK. (ROZH.) MNOŽINA
UVAŽOVANÉ SPOČETNÝ JAZYK, EFEKTÍVNE OČ. $\#A$ FLÍ.

CHURCH (VETA O NEROZHODNUTEĽNOSTI PRED. LOGIKY)
ZA URČITÝCH PREDP. JE $\{\#A \mid A$ UZAVRETÁ, $\models A\}$ NEROZ.

ROBINSNOVA ARITMETIKA Q
$R1, R2, R3 \to S$, $R4, R5 \to +$, $R6, R7 \to \cdot$ $R8 \to \leq$

PEANOVA ARITMETIKA P, NAMIESTO $R3$ MÁ
$A_x[0] \to ((\forall x)(A \to A_x[S(x)]) \to (\forall x)(A))$

ÚPLNÁ ARITMETIKA : $Th(\mathbb{N}) = \{A \mid A$ UZAVR. $\mathbb{N} \models A\}$
Q, P SÚ REKURZÍVNE AXIOMAT., $Th(\mathbb{N})$ NIE JE

POLOŽME $Thm(T) := \{\#A \mid A$ UZAVRETÁ, $T \vdash A\}$
T JE ROZHODNUTEĽNÁ $\Leftrightarrow$ $Thm(T)$ JE REKURZÍVNA

CHURCH (VETA O NEROZHODNUTEĽNOSTI ARITMETIKY):
KAŽDÉ BEZSPORNÉ ROZŠÍRENIE ROBINSNOVEJ AR.
JE NEROZHODNUTEĽNÉ. !!

GÖDEL-ROSSER (VETA O NEÚPLNOSTI ARITMETIKY):
ŽIADNE BEZSPORNÉ, REKURZÍVNE AXIOMATIZOVATEĽNÉ
ROZŠÍRENIE ROBINSN. ARITM. NIE JE ÚPLNÁ TEÓRIA. !!

2 AUTOMATY A JAZYKY

KONGRUENCIA $\sim$ (EKV. NA Σ^*), PRAVÁ, KON. INDEXU

NERODOVA VETA  Σ^*

POČET STAVOV DFA

PUMPING LEMMA : L REG. $\boxed{\Rightarrow}$ $\exists n : \forall |z| \geq n \;\; z = uvw \ldots$

$h : Q_1 \to Q_2$ AUT. HOMOMORFIZMUS $\Rightarrow$ EKVIVALENCIU

DOSIAHNUTEĽNÝ STAV, STAVOVÁ EKV. $\sim$ (PO KROKOCH)

AUTOMATOVÁ KONGR. $\equiv$ NA Q $\quad p \equiv q \Rightarrow (p \in F \Leftrightarrow q \in F)$ & δ

PODIELOVÝ AUTOMAT $A/\equiv$

VETA O IZOMORFIZME REDUKTOV

NFA : $\delta : Q \times \Sigma \to P(Q)$, PRIJÍMANIE SLOV,

λ-PRECHOD, λ-UZÁVER (q)

DVOJSMERNÝ AUTOMAT : $\delta : Q \times \Sigma \to Q \times \{-1, 0, +1\}$

MNOŽINOVÉ OP. NA JAZYKOCH : $\cup, \cap, -, \overline{}$, (KARTÉZSKY SÚČIN DFA)

REŤAZCOVÉ OP. NA JAZYKOCH, $\cdot$, MOCNINY, ITER. $+, *$, R

$L_2 \backslash L_1$, L_1 / L_2

SUBSTITÚCIA JAZYKOV $\sigma(x)$ JAZYK V Y_x, $\sigma : \Sigma^* \to P(Y^*)$

TRIEDA $RJ(\Sigma)$: (1) $\emptyset$, (2) $\{x\}$ $\forall x \in \Sigma$, (3) UZ. NA: $\cup, \cdot, *$

KLEENOVA VETA : $L \in RJ(\Sigma) \Leftrightarrow \exists$ DFA $A : L = L(A)$

$\Leftarrow)$ R^k_{ij} = SLOVÁ $q_i \overset{w}{\rightsquigarrow} q_j$ BEZ POUŽITIA q_m $m > k$

$R^{k+1}_{ij} = R^k_{ij} \cup R^k_{i,k+1} \cdot \left(R^k_{k+1,k+1}\right)^* \cdot R^k_{k+1,j}$

REGULÁRNE VÝRAZY $(\alpha + \beta)$, $(\alpha \cdot \beta)$, α^*, $\emptyset$, λ, x, $[\alpha]$

MOOREOV STROJ : NAVYŠE $\boxed{\mu} : Q \to \boxed{Y}$ ZNAČKOVACIA F.

MEALYHO STROJ : NAVYŠE $\boxed{\lambda} : Q \times \Sigma \to \boxed{Y}$ VÝSTUPNÁ F.

07. 09. 2008 Su
PETER ČERNO

ŠTÁTNICE

PREPISOVACÍ (PRODUKČNÝ) SYSTÉM $R = (V, P)$
$w \Rightarrow z$ $\quad w = xuy$, $z = xvy$, $(u \to v) \in P$, $w \Rightarrow^* z$

GENERATÍVNA GRAMATIKA $G = (V_N, V_T, S, P)$, $L(G)$

CHOMSKÉHO HIERARCHIA :

$\mathcal{L}_0$ (REK. SPOČETNÉ) - OBECNÉ PRAVIDLÁ
$\mathcal{L}_1$ (KONTEXTOVÉ) - $\alpha X \beta \to \alpha w \beta$ $\quad w \in (V_N \cup V_T)^+$ (VÝNIMKA $S \to \lambda$)
$\mathcal{L}_2$ (BEZKONTEXTOVÉ) - $X \to w$
$\mathcal{L}_3$ (REGULÁRNE) - $X \to wY$, $X \to w$

NEVYPÚŠŤAJÚCA BEZK. GRAMATIKA: $\cancel{X \to \lambda}$

BKG REDUKOVANÁ : (1) $\forall X$ (1) $X \Rightarrow^* w$, (2) $S \Rightarrow^* uXv$

ĽAVÉ PREPÍSANIE, DERIVÁCIA, DERIVAČNÝ STROM
JEDNOZNAČNOSŤ BKG.

ZÁSOBNÍKOVÝ AUTOMAT $M = (Q, X, Y, \delta, q_0, Z_0, F)$

!! $\delta : Q \times (X \cup \{\lambda\}) \times Y \to P_{FIN}(Q \times Y^*)$

PRIJÍMANIE KONCOVÝM STAVOM(a) / PRÁZDNYM ZÁSOB.(b)
(a) $(q_0, w, Z_0) \vdash^* (q, \lambda, v)$ $\quad q \in F$
(b) $(q_0, w, Z_0) \vdash^* (q, \lambda, \lambda)$

DETERMINISTICKÝ ZA :
(1) DET. BEZKONTEXTOVÉ JAZYKY (KONC. STAVOM)
$\cup|$
(2) DET. BEZPREFIXOVÉ JAZYKY (PRÁZ. ZÁSOBNÍKOM)

L JE DBKJ $\Rightarrow$ L# JE BEZPREF. BKJ

GREIBACHOVA NF : $\quad A \to aU$, $a \in V_T$, $U \in V_N^*$

CHOMSKEHO NF : $\quad X \to YZ$, $X \to a$

PUMPING LEMMA $L \in BKJ \Rightarrow \boxed{\exists\, p, q \in \mathbb{N}}$

$\forall z \in L\ |z| > p : z = uvwxy$

(1) $|vwx| \leq q$, (2) $vx \neq \lambda$, (3) $uv^iwx^iy \in L\ \forall i$

ALGORITMUS CYK : $a_1 \dots a_n \in BKJ\ L$?

$\boxed{X_{i,j} = \{A \mid A \Rightarrow^* a_i \dots a_j\}}$

DYCKOV JAZYK D_n : $S \to \lambda \mid SS \mid a_1 S a_1' \mid \dots \mid a_n S a_n'$

PRE KAŽDÝ BKJ L $\exists$ REGULÁRNY R, DYCKOV D T.Ž. $L = h(D \cap R)$ PRE VHODNÝ HOMOMORFIZMUS

	RJ	BKJ	DBKJ
ZJEDNOTENIE	✓	✓	✗
PRIENIK	✓	✗ (*)	✗
PRIENIK S RJ	✓	✓	✓
DOPLNOK	✓	✗	✓
SUBST. / HOMOM.	✓	✓	✗
INV. HOM.	✓	✓	✓

(*) $\{a^ib^ic^j\} \cap \{a^ib^jc^j\}$

SEPAROVANÁ GR. : (1) $\alpha \to \beta$, $\alpha, \beta \in V_N^+$ (2) $X \to u$, $u \in V_T \cup \{\lambda\}$

KU KAŽDEJ GR. MOŽNO ZOSTROJIŤ EKV. SEPAROVANÚ

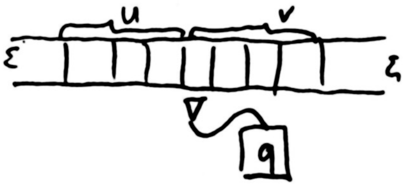
MONOTÓNNA $u \to v \Rightarrow |u| \leq |v|$

KU KAŽDEJ MON. GR MOŽNO ZOSTR. EKV. KONTEXTOVÚ

TURINGOV ST. $T = (Q, \Sigma, \delta, q_0, F)$

!! $\delta : (Q - F) \times \Sigma \to Q \times \Sigma \times \{-1, 0, +1\}$

KONFIGURÁCIA : uqv



PRID. REK. SPOČETNÉ JAZYKY

NTS ~ TS ~ $\mathcal{L}_0$

LOA ~ $\mathcal{L}_1$

REKURZÍVNE JAZYKY = ROZHODN. TS.

07.09.2008 Su
PETER ČERNO

STÁTNICE

3 ALGORITMY A DÁTOVÉ ŠTRUKTÚRY

AMORTIZOVANÁ ANALÝZA - AGREGAČNÁ ANALÝZA, ÚČTOVNÁ METÓDA, POTENCIÁLNA METÓDA

TRIEDY ZLOŽITOSTI: P = RIEŠITEĽNÉ V POL. ČASE, NP = VERIFIKOVATEĽNÉ V POL. ČASE, NPC

REDUKCIA (PRE DECESION PROBLEMS)

COOK-LEVIN: SAT JE NPC,

ĎALŠIE NPC: 3-SAT, CLIQUE, VERTEX-COVER, HAM-CYCLE, TSP, SUBSET-SUM, INDEP.-SET, 3-COLOR

DIVIDE & CONQUER: MERGE-SORT

ANALÝZA ZLOŽITOSTI: 1. SUBST. METÓDA

2. MASTER THEOREM: $T(n) = aT(n/b) + f(n)$, $n^{\log_b a}$

BINARY SEARCH TREES (BST)

RED-BLACK TREE: KOREŇ, LISTY (NIL), bh

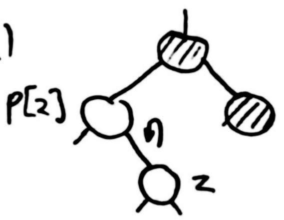
POVOLENÉ FAREBNÉ ZÁMENY A ROTÁCIE

RB-INSERT-FIXUP (T, z)
while color[p[z]] = RED do
[...
color[root[T]] ← BLACK

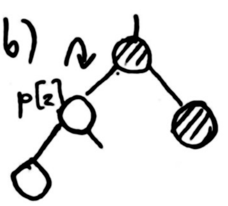
2 PRÍPADY

color[y] = RED
color[y] = BLACK

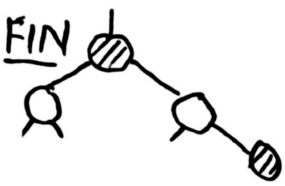
2a)



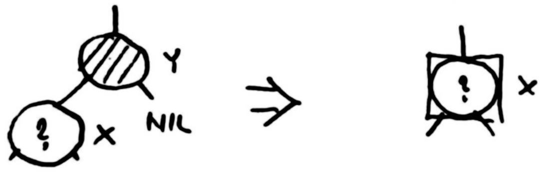
2b)



FIN



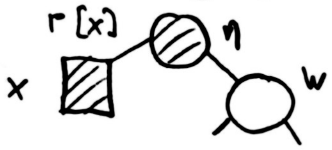
RB-DELETE-FIXUP (T, x)



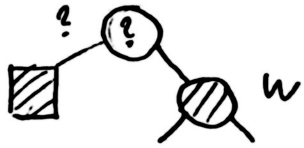
w ← right(p[x])

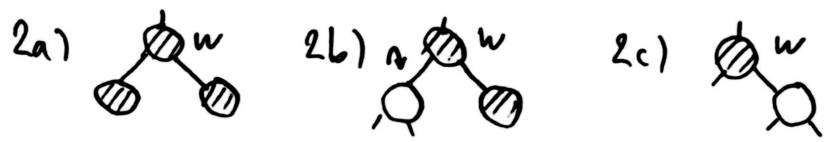
while x ≠ root[T] & color[x] = BLACK do
[...
color[x] ← BLACK

1. color[w] = RED

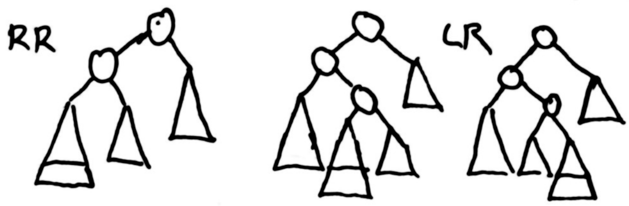


2. color[w] = BLACK





AVL STROMY $bf = h(left) - h(right)$ $h(nil) = -1$



$|bf| \leq 1$

HALDA (HEAP), FIBONNACI HEAP

HAŠOVANIE - UNIVERZUM U, $S \subseteq U$, $|S| << |U|$

MEMBER, INSERT, DELETE

HASH FCIA. h, FAKTOR NAPLNENIA, KOLÍZIA

(1) SO SEPAROVANÝMI REŤAZCAMI

(2) S USPORIAD. REŤAZCAMI

(3) S PREMIESTŇOVANÍM - key, next, previous

(4) ZRASTAJÚCE HASHOVANIE

(5) HASH. S LINEÁRNYM PRIDÁVANÍM

$m \geq 2n \Rightarrow$ NAJDLHŠÍ OSTROVČEK $O(\log m)$

07.09.2008 Su
PETER CERNO

ŠTÁTNICE

UNIVERZÁLNE HASHOVANIE – MN. $\mathcal{H}$ JE UNIV.
$\Leftrightarrow \forall k \neq l \in U$ JE # $h \in \mathcal{H} : h(k) = h(l)$ NAJVIAC $\frac{|\mathcal{H}|}{m}$

$0 < a < p,\ 0 \le b < p$ $\quad h_{a,b}(x) = [(ax+b) \bmod p] \bmod m$

$\frac{1}{|\mathcal{H}|} \cdot \sum_{h \in \mathcal{H}} c(M,h) \le \frac{n(n-1)}{m}, \quad |M| = n$

PERFEKTNÉ HASHOVANIE – $M \subseteq U$ VOPRED ZNÁMA
PRÍSTUPOV : $O(1)$ SCHÉMA: DVOJÚROVŇ. UNIV. HASH

EXTERNÉ HASHOVANIE – DATA NA EXT. MÉDIUM (HDD)
MINIMALIZUJEME # ZÁPISOV / ČÍTANÍ STRÁNOK DISKU
PERF. HASH CORMACKA, LARSON & KALJI
ROZŠÍRITEĽNÉ HASH. FAGIN, LINEÁRNE HASH. LITWIN

SEKVENČNÉ TRIEDENIE

SELECTION SORT 

$\Theta(n^2)$

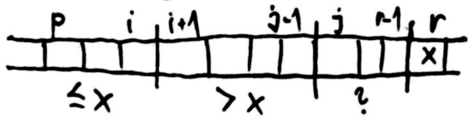
INSERTION SORT $\Theta(n + |I(\pi)|)$ $O(n^2)$, STABLE

BUBBLE SORT, SHAKE SORT $O(n^2)$

HEAPSORT $\Theta(n \log n)$ INPLACE, NIE JE STABLE !

MERGESORT $\Theta(n \log n)$ AJ NA VONK. TRIEDENIE

QUICKSORT $O(n^2)$, PRIEM. $\Theta(n \log n)$

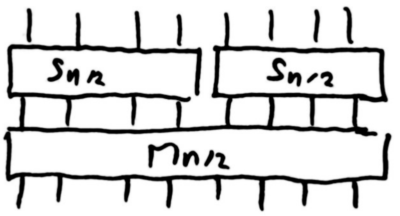
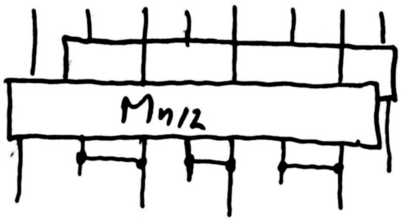
PARTITION(A, p, r) 

COUNTING SORT $\Theta(n+k)$ STABLE

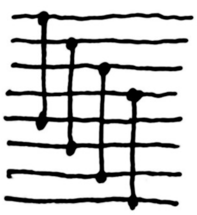
LEAST SIGNIFICANT DIGIT – RADIX SORT
MOST –||– (ZALOŽ. NA BUCKET-SORT) – LEXIKOGR. TR. RÔZNE DLHÉ KĽÚČE

TRIEDIACE SIETE - ZERO-ONE PRINCIPLE

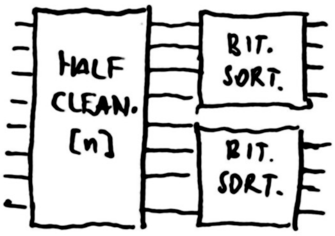
S_1 : M_1 : 

S_n :  M_n : 

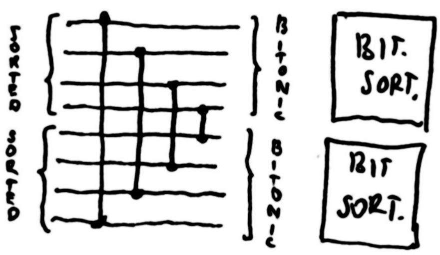
HALF-CLEANER



BITONIC SORTER



MERGE



<u>GRAFOVÉ ALG.</u> BFS, DFS, TOPOLOGICAL-SORT, STRONGLY-CONNECTED-COMPONENTS,

<u>HĽADANIE NAJKRATŠEJ CESTY</u> : SINGLE-SOURCE :

RELAX (u, v, w) if $d[v] > d[u] + w(u,v)$ then ... $\pi[v] \leftarrow u$

BELLMAN-FORD $\Theta(n \cdot m)$

DAG-SHORTEST-PATH $\Theta(n+m)$ - CRITICAL PATH

DIJKSTRA $\Theta((m+n) \log n)$ $w \geq 0$!!

ALL-PAIRS : FLOYD-WARSHALL $\Theta(n^3)$

TRANSITIVE-CLOSURE

DISJOINT-SET FORESTS (UNION-BY-RANK, PATH-COMPR.)

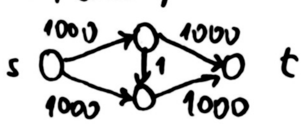
<u>MINIMÁLNA KOSTRA</u> : KRUSKAL, BORŮVKA, PRIM

<u>TOKY V SIETACH</u>

SIEŤ, TOK, SIEŤ REZERV, ZLEPŠUJÚCA CESTA, REZ (S,T), $|f| \leq c(S,T)$

MAX-FLOW MIN-CUT THEOREM

FORD-FULKERSON



EDMONDS-KARP $O(n \cdot m^2)$

DINIC $O(n^2 m)$ FÁZY, DISTANCE LABELS, BLOK. TOK

07.09.2008 Su
PETER ČERNO

ŠTÁTNICE

PUSH – RELABEL – VLNA (PREFLOW), PREBYTOK (EXCESS), PRETEKAŤ (OVERFLOW), VÝŠKOVÁ FUNKCIA
PUSH (u,v), RELABEL (u)
GENERICKÝ GOLDBERGOV PUSH-RELABEL $O(n^2 m)$

VYHĽADÁVANIE VZORKOV V TEXTE:

AHO-CORASICK – DOPREDNÁ, SPÄTNÁ FUNKCIA
KMP – PREFIXOVÁ FCIA. $\pi[i] = \max\{k < i \mid P_k \sqsupset P_i\}$
RABIN-KARP $O((n-m+1) \cdot m$

ALGEBRAICKÉ ALGORITMY

DFT $\vec{a} \rightsquigarrow \vec{y} = W \cdot \vec{a} = (A(\omega_n^0), \dots, A(\omega_n^{n-1}))$, DFT^{-1}
FFT $A^{[0]}(x), A^{[1]}(x)$, $A(x) = A^{[0]}(x^2) + x A^{[1]}(x^2)$

$$A(\omega_n^k) = A^{[0]}(\omega_{n/2}^k) + \omega_n^k A^{[1]}(\omega_{n/2}^k)$$

$$\omega_n^{k+\frac{n}{2}} = -\omega_n^k \quad !!! \quad \text{Π. } k = 0, \dots, \tfrac{n}{2}-1$$

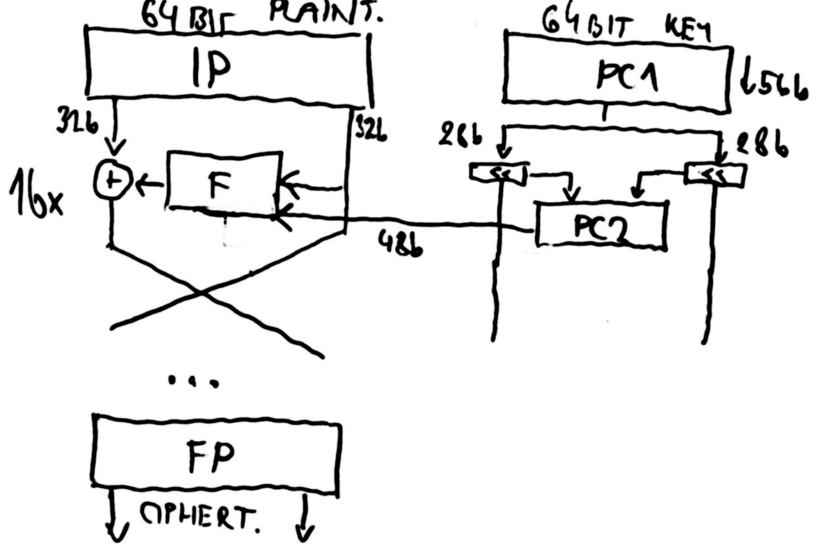
EUKLIDOV ROZŠÍRENÝ ALG.

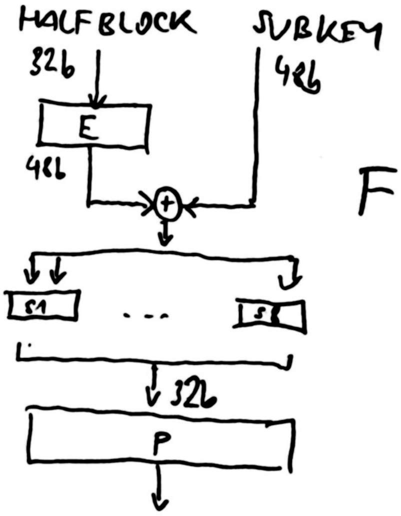
ZÁKLADY KRYPTOGRAFIE

ŠIFRA, KĽÚČ, KOMUTUJÚCE ŠIFRY, KRYPT. S VEREJNÝM KĽ.
DIGITÁLNY PODPIS $(M, S_A(M)) \to B$
HYBRIDNÉ ŠIFROVANIE $(K(M), P_B(K)) \to B$
HYBRIDNÁ AUTENTIZÁCIA
CERTIFIKAČNÁ AUTORITA

RSA (RIVEST, SHAMIR, ADELMAN)
(1) p, q (2) $n = p \cdot q$, $r = \varphi(n) = (p-1)(q-1)$
(3) e NESÚDELITEĽNÉ S r, $d \cdot e \equiv 1 \pmod r$
(4) (e,n) PUBLIC, (d,n) SECRET
$P(M) = M^e \pmod n$, $S(M) = M^d \pmod n$

DES (DATA ENCRYPTION STANDARD)





RANDOMIZOVANÉ, PRAVDEPODOBNOSTNÉ (MILLER - RABIN)

(1) FERMAT: $a^{p-1} \equiv 1 \pmod p$ $\quad a \in \mathbb{Z}_p^*$

(2) NIVEN & ZUCKERMAN: $\mathbb{Z}_n^*(\cdot, ^{-1}, 1)$ JE CYKL. $n = 2, 4, p^e, 2p^e, p > 2$

$g^{ind_{n,g}(a)} \equiv a \pmod n$

(3) $x^2 \equiv 1 \pmod{p^e}$, $p > 2$ MÁ RIEŠ.: $x = \pm 1$

→ WITNESS(a, n) $\quad n-1 = 2^t u$, $\quad x_i = a^{2^i u}$ ...

APROXIMAČNÉ ALG.

OPTIMALIZAČNÝ PROBLÉM, CENA c, POMEROVÁ CHYBA $\rho(n) \geq \max\left(\frac{c}{c^*}, \frac{c^*}{c}\right)$

APROXIMAČNÁ SCHÉMA: POLYN. TIME, FULLY POL. TIME $P(n, 1/\varepsilon)$

APPROX-VERTEX-COVER(G) $\rho(n) = 2$

APPROX-TSP-TOUR(G,c) $\rho(n) = 2$ Δ-NEROVNOSŤ

SET-COVERING$(X, \mathcal{F})$ $\quad H(\max_{S \in \mathcal{F}} |S|)$

APPROX-SUBSET-SUM(S, t, ε) $\quad \rho(n) = 1 + \varepsilon$

07. 09. 2008 Su
PETER ČERNO

ŠTÁTNICE

4 DATABÁZY

DATABÁZA, SRBD, DB SYSTÉM, DB MODEL - SCHÉMA + OP.
DB MODELY: PLOCHÝ, RELAČNÝ, HIERARCHICKÝ, SIEŤOVÝ (ZAZN. MNOŽINY),
OBJEKTOVÝ MODEL

DB ARCHITEKTÚRY: CENTRAL. / DISTRIB., JEDNOUŽ. / VIACUŽ.

DÁTOVÉ MODELOVANIE: PROCES VYTV. DAT. MODELU
(1) KONCEPTUÁLNA SCH. (2) LOGICKÁ SCH. (3) FYZICKÁ SCH.
ER DIAGRAMY

RELAČNÝ DÁTOVÝ MODEL $R \subseteq D_1 \times \ldots \times D_n$, $R(A_1 : D_1, \ldots, A_n : D_n)$
RELAČNÁ ALG. - MNOŽ. OPERÁCIE $\cup, \cap, -, \times$, PROJ., SELEK., ...
RELAČNÝ KALKUL - DOMÉNOVÝ / n-TICOVÝ
FZ, $R(A, F)$, ARMSTRONG. PRAV., F^+,
REDUND. ZÁV., POKRYTIE (KANONICKÉ) (NEREDUND.),
REDUKOVANÁ FZ, MINIMÁLNE POKRYTIE
NORMÁLNE FORMY: 1NF, 2NF, 3NF (TRANZ. ZÁV. NA KL.)
BOYCE - CODDOVA NF (BCNF)
NORMALIZÁCIA REL. SCHÉMY: BEZSTRAT., POKRYTIE ZÁV., NF
BEZSTRAT. $R(A, F) \to R_1(A_1, F_1), R_2(A_2, F_2) \Leftrightarrow A_1 \cap A_2 \to A_1 \vee A_1 \cap A_2 \to A_2$
POKR. ZÁV. $F^+ = F_1^+ \cup F_2^+$

ALG. DEKOMPOZÍCIA - DO BCNF, BEZSTR., ~~POKR. ZÁV.~~
$X \to Y \in F_i$, $X \to A_i \notin F^+ \Rightarrow R_1(A_i - Y, \ldots), R_2(X \cup Y, \ldots)$

ALG. SYNTÉZA - 3NF, ~~BEZSTR.~~, POKR. ZÁV.
(1) $F \to$ MINIM. POKRYTIE G, (2) ZLÚČ SCHÉMY S ROVNAKOU ĽAV. STRAN.

SQL, DDL, DML

SELECT .. FROM .. WHERE .. GROUP BY .. HAVING .. ORDER BY ASC DESC
CREATE TABLE ... (...)

TRANSAKCIA, ACID, COMMIT / ROLLBACK,
TRANSAKČNÝ ROZVRH, SCHEDULER
KONFLIKTY WR, RW, WW, KONFL. EKV., USPORIAD.
PRECEDENČNÝ GRAF, ZOTAVITEĽNÝ ROZVRH
PROTOKOL < UZAMYKACÍ (2PL, S2PL, C2PL, ...)
ALTERNATÍVNY (OPTIMIST. RIADENIE, ČAS. RAZÍTKA)
2PL - 2 FÁZY (ZAM., ODOMYK.)
S2PL - ODOMYK. NA KONCI TR., GARANTUJE ZOTAVIT., PROTI KASK. RUŠ. TR.
DETEKCIA DEADLOCKU - WAITS-FOR GRAF
PREVENCIA: WAIT-DIE, WOUND-WAIT
FANTOM, INDEX LOCKING
OPTIMIST. RIAD. (3 FÁZY): READ, VALIDATION, WRITE
ČASOVÉ RAZÍTKA TS(T), RTS(O), WTS(O)

ORGANIZÁCIA DÁT NA VONK. PAMÄTI:

LOGICKÝ / FYZICKÝ ZÁZNAM R, FYZ. STRÁNKA B,
BLOKOVACÍ FAKTOR, SOS = PAMÄŤ. ŠTR. + ALG. OP.,
VYVÁŽENOSŤ SOS a) b)
VONKAJŠIA PAMÄŤ: MAG. PÁSKA, MAGN. DISK (STOPA,
CYLINDER, s, r, btt, ZÓNOVÉ UKLADANIE, RAID)
STATICKÉ METÓDY: HROMADA (HEAP)
USP. SEKV. SÚBOR - +(SÚBOR TRANSAKCIÍ / AKTUALIZÁCIÍ)
INDEX SEKV. SÚBOR - INDEX + OBL. PRETEČENIA
INDEXOVANÝ SÚBOR - INDEXUJÚ SA ZÁZNAMY, CLUSTER. INDEX
BITOVÉ MAPY
SÚBOR S PRIAMYM PRÍSTUPOM (B=R)
TRIEDENIA NA VONK. PAMÄTI: MERGESORT,
n-CESTNÉ, MAX. d-HALDOU, DVOJITÁ HALDA (DLHÉ BEHY)
B-STROM, REDUNDANTNÝ B-STROM,
B+-STROM, B*-STROM $\lceil \frac{2m-1}{3} \rceil$ ... m POTOMKOV
PREFIX. STROMY (TRIE), S PRED. DĹŽKOU ZÁZNAMU $\lceil \frac{B}{2} \rceil$ .. B
VIACROZMERNÉ B-STROMY

07.09.2008 Su
PETER ČERNO

ŠTÁTNICE

5 ARCHITEKTÚRY POČÍTAČOV A SIETÍ

ARCHITEKTÚRA / ORGANIZÁCIA,
VON NEUMANN MACHINE (IAS COMP., STORED-PROGRAM CONC.)
PC, IR, SP, MAR, MBR,
HARVARDSKÁ ARCHITEKTÚRA - MIKROKONTROLÉRY
MOOROV ZÁKON, INSTRUCTION CYCLE
FETCH → DECODE → LOAD → EXECUTE → STORE
PRERUŠENIA (INTERRUPTS), BUS (ZBERNICA) PCI
ORGANIZÁCIA PC: L_0 (MIKROPROGR.), L_1 (STROJ. JAZYK),
L_2 (OPER. SYS.), L_3 (ASSEMBLER), L_4 (VYŠŠIE JAZ.) L_5 (APP.)
ARCHITEKTÚRA PC: ZÁKL. DAT. ŠTRUKT., REPR. DÁT,
ADR. KONV., REGISTRE, INŠTRUKCIE, IO
PROCESORY / MULTIPROCESORY
CISC, RISC, POST-RISC, VLIW, EPIC (IA-64)
INSTR. PIPELINING, SUPERSCALAR, OUT-OF-ORDER EX.,
PREDIKCIA SKOKOV, ŠPEKULATÍVNE VYK. KÓDU, VEKT. PROCESORY
SIMD, MISD, MIMD
SMP, ASMP, NUMA
IO ZARIADENIA: BLOK./ZNAK., SEKV./NÁH.,
SYNCH./ASYNCH., PREEM./SPOOLING, RÝCHLOSŤ, R, RW, W
POLLING, INTERRUPT, DMA

OPERAČNÉ SYS.

MONOLITICKÝ, VIRT. STROJE, MIKROJADRO
ARCHITEKTÚRA WINNT, LINUX
PROCES, VLÁKNO, STAV PROCESU

PLÁNOVANIE (PREEMPT. / NEPR.), SCHEDULER
FIFO, ROUND ROBIN, VIAC FRONT, PLÁN. V SMP
REAL-TIME (SOFT / HARD)

INTERPROCESS COMMUNICATION, RACE CONDITION,
CRITICAL REGION, MUTUAL EXCLUSION, PODMIENKY (4)
ZAKÁZANIE PRERUŠENÍ - KERNEL
LOCK VARIABLES - NEFUNKČNÉ!
STRICT ALTERNATION - BLOK. PROCESU V NEKR. SEKCII!
PETERSN. RIEŠENIE - interested, turn
TSL RX, LOCK (TEST AND LOCK)
PRODUCER-CONSUMER PROBLEM
SEMAFÓRY - UP / DOWN
MUTEX, MONITOR, MESSAGE PASSING, BARRIERS
DINING PHILOSOPHERS PROBLEM
DEADLOCK - COFFMANOVE PODMIENKY (4)
OSTRICH, DETEKCIA A ZOTAVENIE, BANKÉR. ALG., PREVENCIA

ORGANIZÁCIA PAMÄTI

OVERLAY, FIXNÉ PARTÍCIE, SWAPING, VIRT. PAMÄŤ
TLB (TRANSLATION LOOKASIDE BUFFER)
VÝPADOK STRÁNKY, ALGORITMY:
OPT. STRÁNKA, NRU, FIFO, 2. ŠANCA, HODINY, LRU,

FILESYSTEM

PLÁNOVANIE POHYBU HLAV HDD - FCFS, SSTF, LOOK, C-LOOK
RAID, JBOD, ...

BEZPEČNOSŤ, AUTENTIZÁCIA, AUTORIZÁCIA, ...

ACL, C-LIST