A6M33SSL: Statistika a spolehlivost v lékařství
Teorie spolehlivosti

Vojta Vonásek
vonasek@labe.felk.cvut.cz

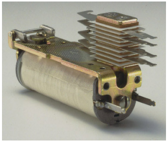
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra kybernetiky

Vícestavové prvky

- Prvky/soustavy mohou mít obecně více typů poruch
- Např. zářivka:
  - svítí (bezporuchový stav)
  - svítí ale se změněnou barevnou teplotou
  - svítí a občas blikne
  - svítí a "bzučí", . . .

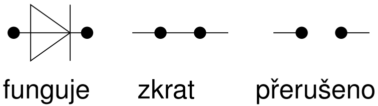
Tří-stavové prvky:

- Dva typy poruch:
  - porucha "přerušením"("open mode failure")
  - porucha "zkratem"("close mode failure")
- Vhodné pro diody, tranzistory, ventily, relé obvody
- Three Miles Island: porucha ventilu v "otevřeném"stavu
- **Přidání redundantních prvků může snížit nebo i zvýšit spolehlivost soustavy**



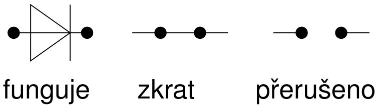
Tří-stavové prvky

- Tři stavy: x (funguje), x_z (zkrat), x_p (přerušení)
- $q_z = P(x_z)$ je pravděpodobnost, že je prvek ve stavu "zkrat"
- $q_p = P(x_p)$ je pravděpodobnost, že je prvek ve stavu "přerušení"
- Q_z = pravděpodobnost, že je celá soustava "ve zkratu"
- Q_p = pravděpodobnost, že je celá soustava "přerušená"



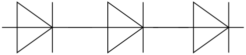
Tří-stavové prvky

- Tři stavy: x (funguje), x_z (zkrat), x_p (přerušení)
- $q_z = P(x_z)$ je pravděpodobnost, že je prvek ve stavu "zkrat"
- $q_p = P(x_p)$ je pravděpodobnost, že je prvek ve stavu "přerušení"
- Q_z = pravděpodobnost, že je celá soustava "ve zkratu"
- Q_p = pravděpodobnost, že je celá soustava "přerušená"



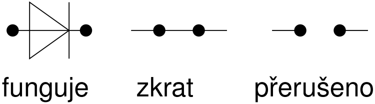
Sériové zapojení

$$
\begin{aligned}
Q_z &= q_{1z} \cdot q_{2z} \cdots q_{nz} \\
Q_p &= 1 - (1 - q_{1p})(1 - q_{2p}) \cdots (1 - q_{np}) \\
R &= 1 - Q_z - Q_p \\
R &= \sum_{i=1}^{n} \binom{n}{i} r^i q_z^{n-i}
\end{aligned}
$$



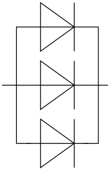
Tří-stavové prvky

- Tři stavy: x (funguje), x_z (zkrat), x_p (přerušení)
- $q_z = P(x_z)$ je pravděpodobnost, že je prvek ve stavu "zkrat"
- $q_p = P(x_p)$ je pravděpodobnost, že je prvek ve stavu "přerušení"
- Q_z = pravděpodobnost, že je celá soustava "ve zkratu"
- Q_p = pravděpodobnost, že je celá soustava "přerušená"



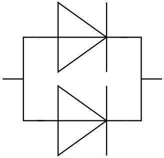
Paralelní zapojení

$$
\begin{aligned}
Q_z &= 1 - (1 - q_{1z})(1 - q_{2z}) \cdots (1 - q_{nz}) \\
Q_p &= q_{1p} \cdot q_{2p} \cdots q_{np} \\
R &= 1 - Q_z - Q_p \\
R &= \sum_{i=1}^{n} \binom{n}{i} r^i q_p^{n-i}
\end{aligned}
$$



Tří-stavové prvky: příklad

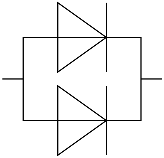
- Pravděpodobnost zkratu: $q_z = 0.6$
- Pravděpodobnost přerušení: $q_p = 0.2$
- Určete R, Q_z a Q_p soustavy.



Pravděpodobnost bezporuchového stavu samotné diody je $R_d = 1 - q_z - q_p = 1 - 0.6 - 0.2 = 0.2$.

$$\begin{aligned} Q_z &= 1 - (1 - q_z)^2 = 1 - (1 - 0.6)^2 = 0.84 \\ Q_p &= q_p^2 = 0.2^2 = 0.04 \\ R &= 1 - Q_z - Q_p = 1 - 0.84 - 0.04 = 0.12 \end{aligned}$$

Tří-stavové prvky: příklad



- Pravděpodobnost zkratu: $q_z = 0.6$
- Pravděpodobnost přerušení: $q_p = 0.2$
- Určete R, Q_z a Q_p soustavy.

Pravděpodobnost bezporuchového stavu samotné diody je $R_d = 1 - q_z - q_p = 1 - 0.6 - 0.2 = 0.2$.

$$\begin{aligned} Q_z &= 1 - (1 - q_z)^2 = 1 - (1 - 0.6)^2 = 0.84 \\ Q_p &= q_p^2 = 0.2^2 = 0.04 \\ R &= 1 - Q_z - Q_p = 1 - 0.84 - 0.04 = 0.12 \end{aligned}$$

Přidáním dalšího prvku paralelně došlo ke zhoršení spolehlivosti!

Tří-stavové prvky

- Přidáním prvků v sérii zvyšujeme pravděpodobnost přerušení
- Přidáním prvků paralelně zvyšujeme pravděpodobnost zkratu
- Jak zvolit počet prvků, aby byla pravděpodobnost bezporuchového provozu maximální?

Sériové zapojení

$$n_0 = \frac{\log\left(\frac{q_p}{1-q_z}\right)}{\log\left(\frac{q_z}{1-q_p}\right)}$$

Paralelní zapojení

$$n_0 = \frac{\log\left(\frac{q_z}{1-q_p}\right)}{\log\left(\frac{q_p}{1-q_z}\right)}$$

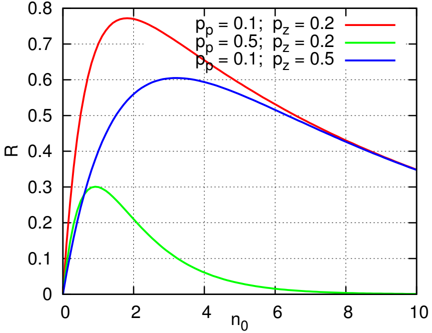
$$n = \begin{cases} \lfloor n_0 \rfloor + 1 & \text{když } n_0 \text{ není celé číslo} \\ n_0 \text{ nebo } n_0 + 1 & \text{pokud } n_0 \text{ je celé číslo} \end{cases}$$

Tří-stavové prvky

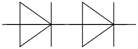
Příklad: Relé má pravděpodobnost přerušení $q_p = 0.1$ a zkratu $q_z = 0.2$. Kolik těchto prvků je třeba zapojit sériově, aby byla maximalizována R?

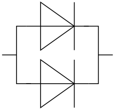
$$n_0 = \frac{\log\left(\frac{q_p}{1-q_z}\right)}{\log\left(\frac{q_z}{1-q_p}\right)} = \frac{\log\left(\frac{0.1}{1-0.2}\right)}{\log\left(\frac{0.2}{1-0.1}\right)} = 1.38$$

Optimální počet prvků je $n = \lfloor n_0 \rfloor + 1 = 2$.



Tří-stavové obvody: příklad

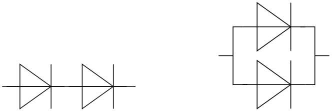




		Sériové			Paralelní		
q_z	q_p	Q_z	Q_p	R	Q_z	Q_p	R
0.6	0.2	0.36	0.36	0.28	0.84	0.04	0.12
0.2	0.2	0.04	0.36	0.6	0.36	0.04	0.6
0.1	0.2	0.01	0.36	0.63	0.19	0.04	0.77

- Porucha zkratem nevadí v sériovém zapojení
- Porucha přerušením nevadí v paralelním zapojení

Tří-stavové obvody: příklad



		Sériové			Paralelní		
q_z	q_p	Q_z	Q_p	R	Q_z	Q_p	R
0.6	0.2	0.36	0.36	0.28	0.84	0.04	0.12
0.2	0.2	0.04	0.36	0.6	0.36	0.04	0.6
0.1	0.2	0.01	0.36	0.63	0.19	0.04	0.77

- Porucha zkratem nevadí v sériovém zapojení
- Porucha přerušením nevadí v paralelním zapojení

- Pokud převažují poruchy typu "zkrat", je lepší sériové zapojení
- Pokud převažuje porucha "přerušením", je lepší paralelní zapojení

Zvýšení spolehlivosti systémů

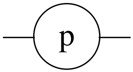
- Vstupem je požadovaná míra spolehlivosti po určenou dobu
- Volba lepších materiálů, technologie výroby, konstrukce ...
- Použití prvků s vyšší spolehlivostí
- Volba zapojení komponent
- Zálohování (zvýšení redundance)
  - Stálé
  - Majoritní
  - S přepínáním

Nelze dosáhnout absolutní spolehlivosti systému.

Stálé zálohování prvků

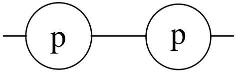
- Prvky v záloze jsou trvale zapnuty
- Náklady na běžící zálohu

Výchozí prvek



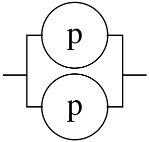
Záloha v sérii

- Vhodná při častých poruchách typu "zkrat"
- Např. spínací obvody



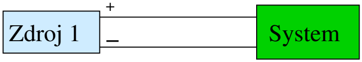
Paralelní záloha

- Vhodná při častých poruchách typu "přerušení"
- Vhodné pro systémy, kdy lze připustit současný běh záloh (např. datové zálohy, poč. sítě)
- Nevhodné např. pro regulační obvody



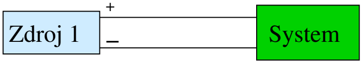
Stálé zálohování soustav

- Výchozí systém

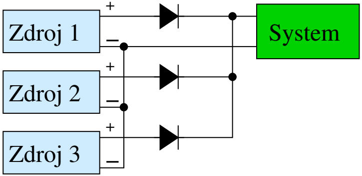


Stálé zálohování soustav

- Výchozí systém

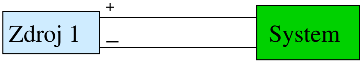


- Paralelní záloha napájení

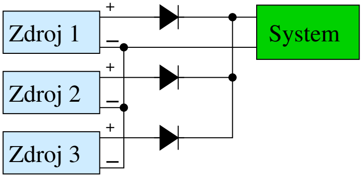


Stálé zálohování soustav

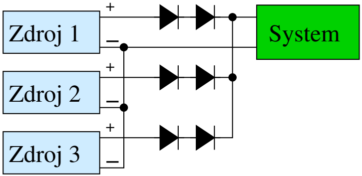
- Výchozí systém



- Paralelní záloha napájení

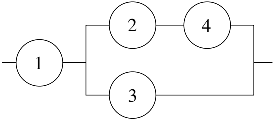


- Zvýšení odolnosti vůči poruchám diod



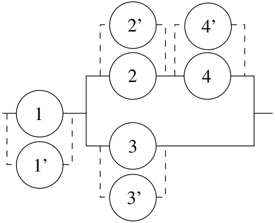
Stálé zálohování soustav

Výchozí systém



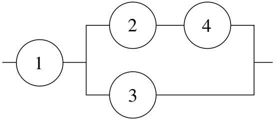
Zálohování jednotlivých prvků

- Každý prvek je zálohován samostatně



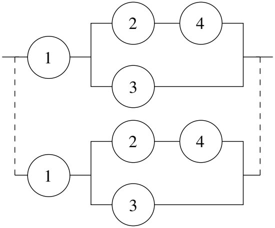
Stálé zálohování soustav

Výchozí systém



Zálohování soustavy

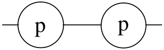
- Soustava se zálohuje jako celek



Zálohování prvků nebo soustavy

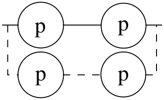
Je lepší zálohování "po prvcích"nebo "celé soustavy"(uvažujme stejné dvoustavové prvky)?

Původní systém: $R = p^2$



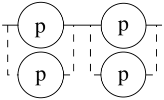
Záloha celé soustavy:

$$R_s = 1 - (1 - p^2)^2 = 2p^2 - p^4$$



Záloha po prvcích:

$$R_p = (2p - p^2)^2 = 4p^2 - 4p^3 + p^4$$



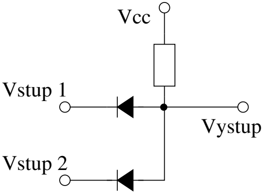
Porovnáním R_p a R_s, např:

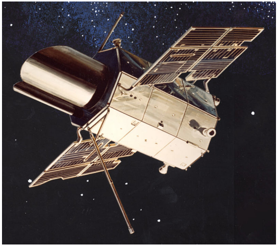
$$R_p - R_s = 2(p - 2p)^2$$

zjistíme, že záloha po prvcích je v tomto případě lepší. Toto lze zobecnit na n dvoustavových stejných prvků, obecně to ale neplatí!

Příklad paralelního zálohování

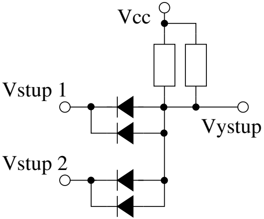
- Obvod realizuje operaci AND
- Možné poruchy: diody, rezistory
- Záloha použita např. v NASA Orbiting Astronomical Observatory

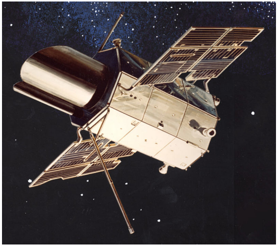




Příklad paralelního zálohování

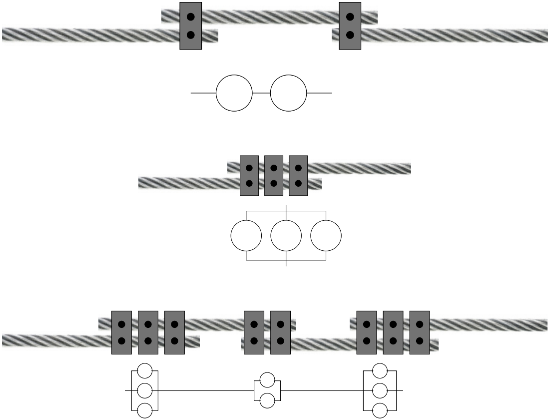
- Obvod realizuje operaci AND
- Možné poruchy: diody, rezistory
- Záloha použita např. v NASA Orbiting Astronomical Observatory





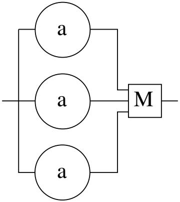
Příklad paralelního zálohování

- Spojky lan
- Porucha spojky: spojení se přeruší
- Podobně u mostních konstrukcí



Zálohování majoritou

- n systémů běží současně
- Bere se ten výstup, který má majorita systémů
- n liché
- Vhodné pro digitální systémy
- Předpoklad: fungující majorizační člen
- Jen pro systémy, kde lze určit majoritu
- Typicky pro "digitální"systémy
- Zálohy běží $\rightarrow$ spotřeba, náklady, údržba



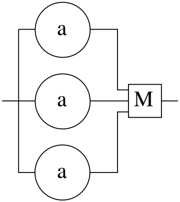
Použití:

- integrované obvody
- ECC pamětí
- Výpočty ve vesmíru (např. na satelitech)
- Komunikace, např. protokol FlexRay (automobilový průmysl)
- První použití Maj. systémů v čs. počítači SAPO (1957–1960)

Zálohování majoritou

- Prvky fungují s pravděpodobností p
- Uvažujme soustavu s $n = 3$ prvky.
- Pro správnou funkčnost jsou třeba alespoň 2 prvky

Pravděpodobnost, že funguje právě m prvků:



$$P_m = \binom{n}{m} p^m (1-p)^{n-m}$$

Spolehlivost majoritního zálohování:

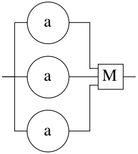
$$R = \sum_{m=2}^{n} \binom{n}{m} p^m (1-p)^{n-m} = P_2 + P_3$$

$$R = 3p^2(1-p) + p^3$$

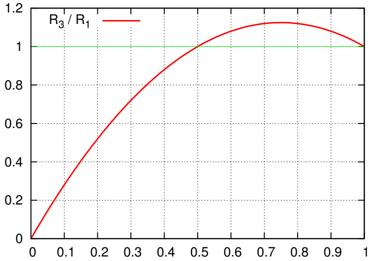
Spolehlivost majoritního zálohování

- Systém se třemi prvky
- Spolehlivost 1 prvku je p
- Alespoň 2 musí fungovat

$$R_3 = 3p^2(1-p) + p^3$$



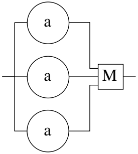
Porovnání spolehlivost oproti nezálohovanému prvku: R_3/p :



Poměr $R_3/p > 1$ pokud $p > 0.5$.

Spolehlivost majoritního zálohování

- Systém se třemi prvky
- Spolehlivost 1 prvku je p
- Alespoň 2 musí fungovat



$$R_3 = 3p^2(1-p) + p^3$$

Majoritní zálohování zlepšuje spolehlivost pokud p každého prvku je $p > 0.5$.

Obecně volíme lichý počet členů, tj. $2n+1$. Spolehlivost pak je:

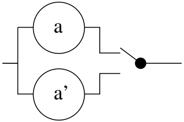
$$R = \sum_{m=n+1}^{2n+1} \binom{2n+1}{m} p^m (1-p)^{2n+1-m}$$

Pokud uvažujeme poruchu majorizačního členu (jeho spolehlivost je R'):

$$R = R \cdot R'$$

Zálohování přepínáním

- Též záloha s okamžitou obnovou
- Při poruše prvke se přepne na prvek v záloze
- Předpokládáme, že prvek v záloze nestárne



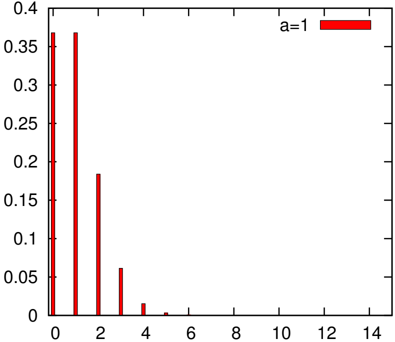
- Vyžaduje (včas) rozpoznat chybu
- Vyžaduje spolehlivý přepínač
- Prvek v záloze nemusí běžet (ale musí se rychle zapnout)
- Pravděpodobnost poruchy lze modelovat Poissonovým rozdělením

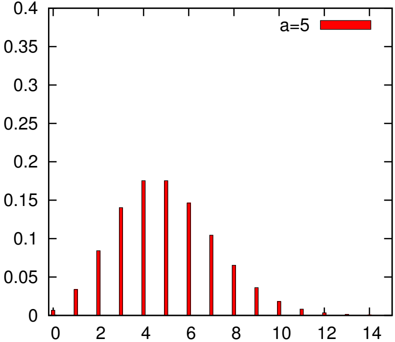
Poissonovo rozdělení

- Pro vyhodnocení pravděpodobnosti počtu jevů v určitém intervalu (intervaly času, délky, km, apod)
- Předpokládejme, že v jednom itervalu se průměrně děje a událostí

Pravděpodobnost výskytu x událostí je:

$$P(X = x) = \frac{a^x}{x!}\mathrm{e}^{-a}$$





Poissonovo rozdělení

- Pro vyhodnocení pravděpodobnosti počtu jevů v určitém intervalu (intervaly času, délky, km, apod)
- Předpokládejme, že v jednom itervalu se průměrně děje a událostí

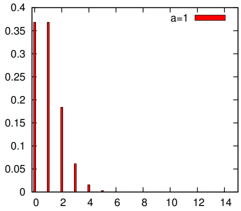
Pravděpodobnost výskytu x událostí je:

$$P(X = x) = \frac{a^x}{x!}\mathrm{e}^{-a}$$

Příklad: Ve serverovně se každý měsíc porouchá v průměru 1 HDD. Jaká je pravděpodobnost, že se porouchají tři disky?

$$a = 1$$

$$P(X = 3) = \frac{a^3}{3!}\mathrm{e}^{-a} = 0.061$$



Poissonovo rozdělení

- Pro vyhodnocení pravděpodobnosti počtu jevů v určitém intervalu (intervaly času, délky, km, apod)
- Předpokládejme, že v jednom itervalu se průměrně děje a událostí

Pravděpodobnost výskytu x událostí je:

$$P(X = x) = \frac{a^x}{x!} \mathrm{e}^{-a}$$

Ve spolehlivosti $a = \lambda t$, kde λ je intenzita poruch

$$P_x(t) = \frac{(\lambda t)^x}{x!} \mathrm{e}^{-\lambda t}$$

- intenzita poruch je konstantní $\lambda \rightarrow$ pouze pro normální období života prvku

Poissonovo rozdělení — příklad

- Průměrný počet poruch na tažném lanu je 0.05 za rok
- Vypočetěte pravděpodobnost $0, 1, 2, \ldots$ poruch během 20 let

$$P_x(t) = \frac{(\lambda t)^x}{x!} \mathrm{e}^{-\lambda t}$$

Intenzita poruch je $\lambda = 0.05/$rok.

$$P_0(20) = \frac{(0.05 \cdot 20)^0}{0!} \mathrm{e}^{-0.05 \cdot 20} = \mathrm{e}^{-1} = 0.367$$

$$P_1(20) = \frac{(0.05 \cdot 20)^1}{1!} \mathrm{e}^{-0.05 \cdot 20} = 0.367$$

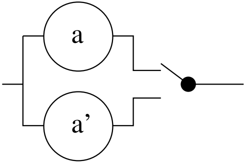
$$P_2(20) = \frac{(0.05 \cdot 20)^2}{2!} \mathrm{e}^{-0.05 \cdot 20} = 0.183$$

$$P_3(20) = \frac{(0.05 \cdot 20)^3}{3!} \mathrm{e}^{-0.05 \cdot 20} = 0.061$$

Zálohování přepínáním

Předpoklady

- Poruchy prvků v záloze nejsou závislé na běžícím prvku
- Prvky jsou stejné a mají konstantní intenzitu poruch λ
- Přepínací (a měřící) prvek je 100% spolehlivý



Systém s dvěma prvky (tj. jeden je v záloze) je funkční, pokud nastane max 1 porucha:

$$P_0(t) = \frac{(\lambda t)^0}{0!} \mathrm{e}^{-\lambda t} = \mathrm{e}^{-\lambda t} \qquad P_1(t) = \frac{(\lambda t)^1}{1!} \mathrm{e}^{-\lambda t} = \lambda t \mathrm{e}^{-\lambda t}$$

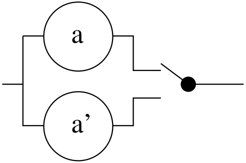
Pravděpodobnost, že tento systém běží je:

$$R(t) = P_0(t) + P_1(t) = \mathrm{e}^{-\lambda t}(1 + \lambda t)$$

Zálohování přepínáním

Předpoklady

- Poruchy prvků v záloze nejsou závislé na běžícím prvku
- Prvky jsou stejné a mají konstantní intenzitu poruch λ
- Přepínací (a měřící) prvek je 100% spolehlivý

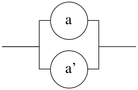


Obecně Systém s n **prvky v záloze** může vykázat max n poruch

$$R(t) = \sum_{x=0}^{n} P_x(t) = \sum_{x=0}^{n} \frac{(\lambda t)^x}{x!} \mathrm{e}^{-\lambda t}$$

Porovnání paralelní zálohy a zálohy s přepínáním

Paralelní záloha

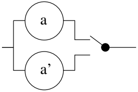


- Záložní prvky trvale v provozu (stárnou)
- Výstupy záloh se nesmí rušit
- Záloha je okamžitá
- Není třeba detekovat poruchu

$$R(t) = 2\mathrm{e}^{-\lambda t} - \mathrm{e}^{-2\lambda t}$$

$$T_s = \frac{3}{2}\lambda$$

Záloha s přepínáním



- Prvek v záloze je vypnut (nestárne)
- Přepínání není nekonečně krátké
- Přepínání může selhat

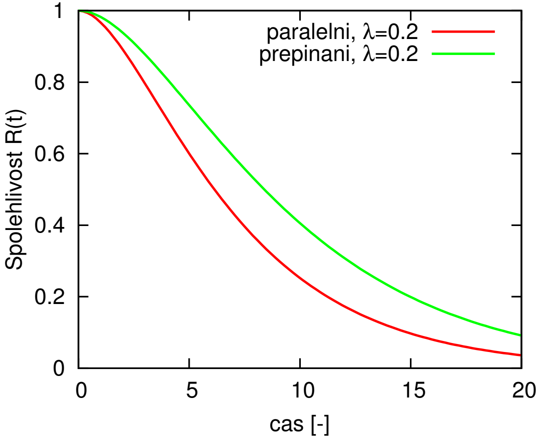
$$R(t) = \mathrm{e}^{\lambda t}(1 + \lambda t)$$

$$T_s = \frac{2}{\lambda}$$

Paralelní zálohování je horší než záloha s přepínáním

Porovnání paralelní zálohy a zálohy s přepínáním

Pro $n = 2$ prvky, $\lambda = 0.2$



Porovnání paralelní zálohy a zálohy s přepínáním

Pro n prvků, $\lambda = 0.2$