Náhodné čísla a ich použitie na riešenie matematických úloh

Radoslav Harman

Katedra aplikovanej matematiky a štatistiky
FMFI UK

Akadémia trojstenu
14.12.2007

Ako získame náhodné čísla?

- Fyzikálne generátory „pravých“ náhodných čísiel
  Výhody: skutočne nepredvídateľné
  Nevýhody: náročné zariadenia, pomalé generovanie
- Algoritmické generátory „pseudonáhodných“ čísiel
  Výhody: rýchle, lacné, s overenými vlastnosťami
  Nevýhody: založené na deterministických predpisoch

Použitie náhodných čísiel

- Stochastické modelovanie (napr. šírenie epidémií)
- Monte-Carlo metódy (napr. výpočet objemov a integrálov)
- Stochastické optimalizačné metódy (napr. simulované žíhanie)
- Pravdepodobnostné algoritmy (napr. testy prvočíselnosti)
- Kryptografia, počítačová grafika a iné oblasti

Lineárny kongruenčný generátor

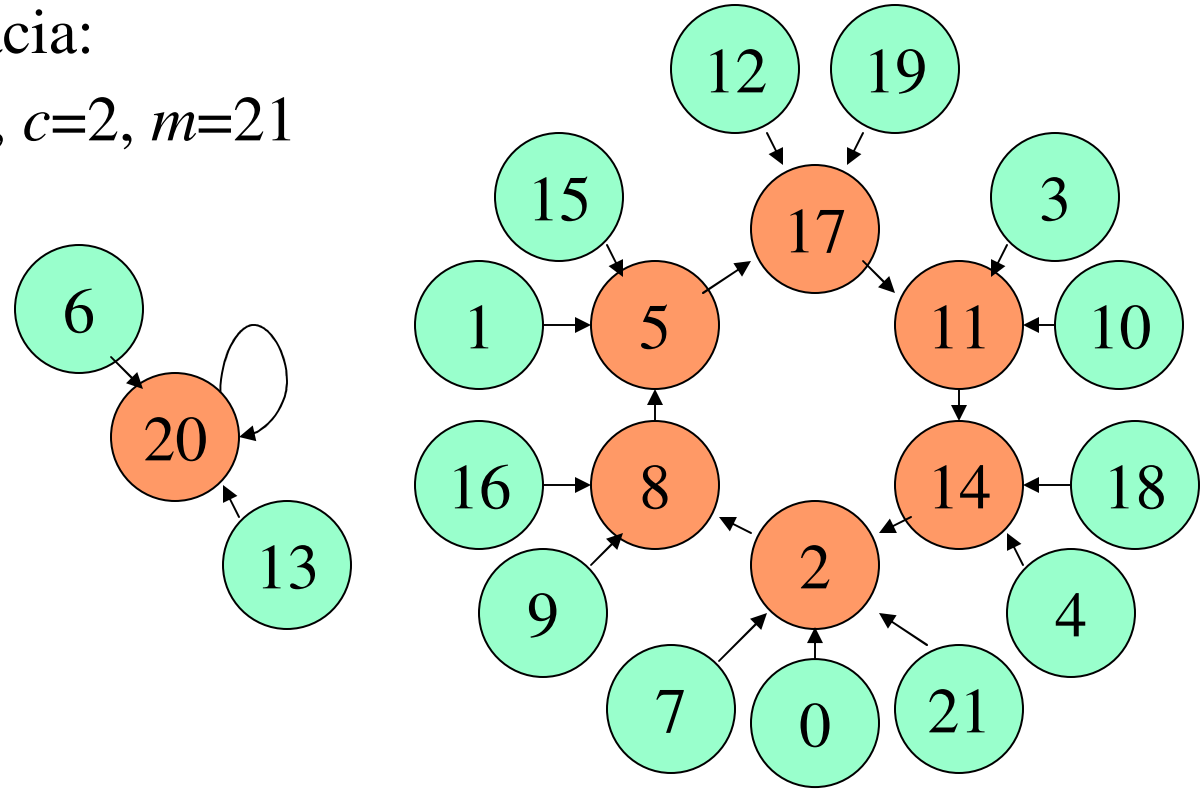
Parametre: m (modulus), a (multiplikátor), c (inkrement)

x_1 ... štartovacie číslo („seed“) od 0 do m-1

$$x_{i+1} := (ax_i + c) \bmod m \quad \text{... pre } i=1,2,3,...$$

Ilustrácia:

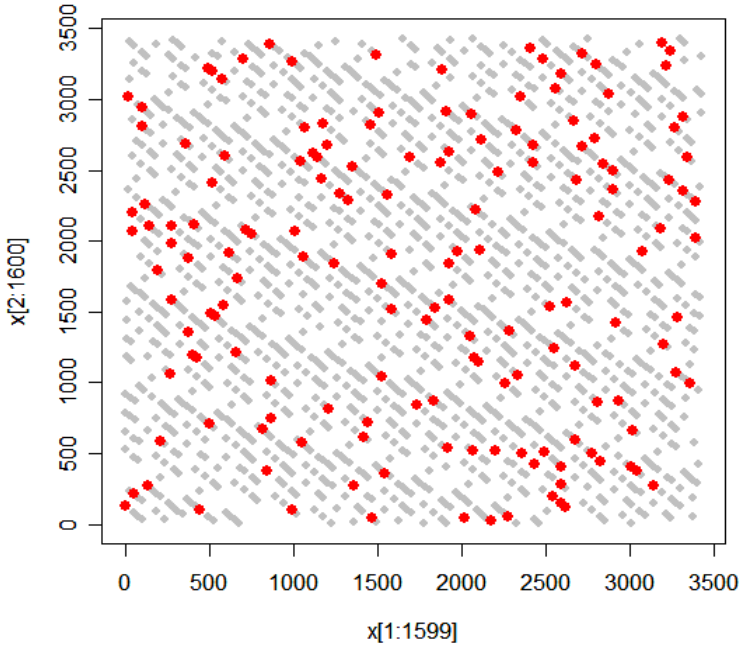
a=3, c=2, m=21



Dôležitá charakteristika: perióda. Príklad tvrdenia o perióde:

Nech a=1 mod 4, c je nepárne a nech m je mocnina dvojky. Potom generátor LCG(a,c,m) má periódu m pre každé x_1.

Problémy: realizácie majú vždy „lineárnu štruktúru“.

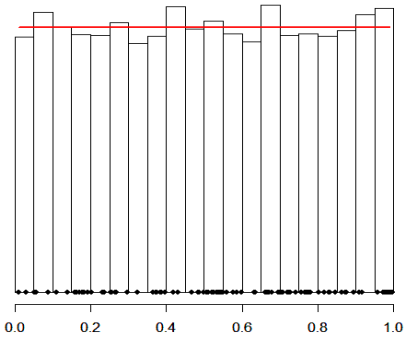


Je potrebné vykonať štatistické testy *rovnomernosti* a *nezávislosti*

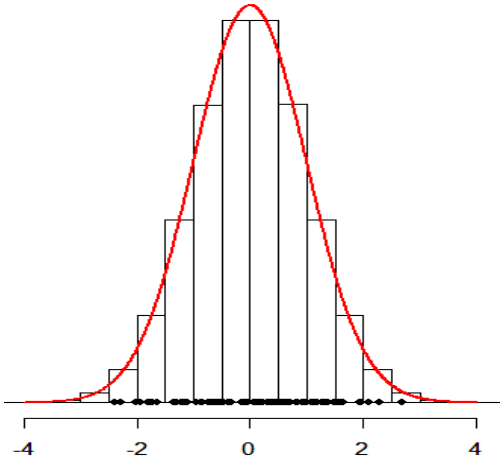
„Minimal standard“ $a = 16807$, $c = 0$, $m = 2^{31}-1 = 2\ 147\ 483\ 647$

Prečo si vystačíme s generátorom rovnomerného rozdelenia náhodných čísiel?

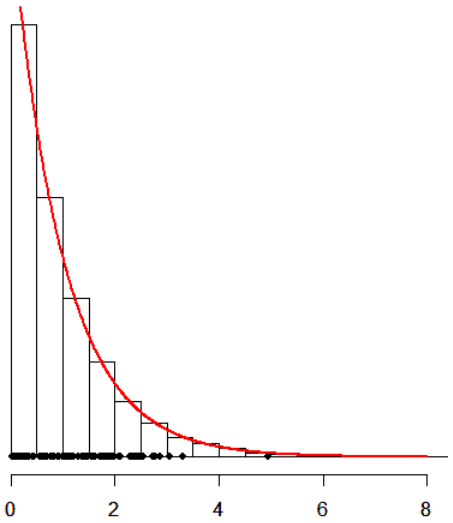
Ak máme rovnomerné rozdelenie, potom



špeciálna transformácia
dá Gaussove rozdelenie



iná transformácia
dá exponenciálne rozdelenie



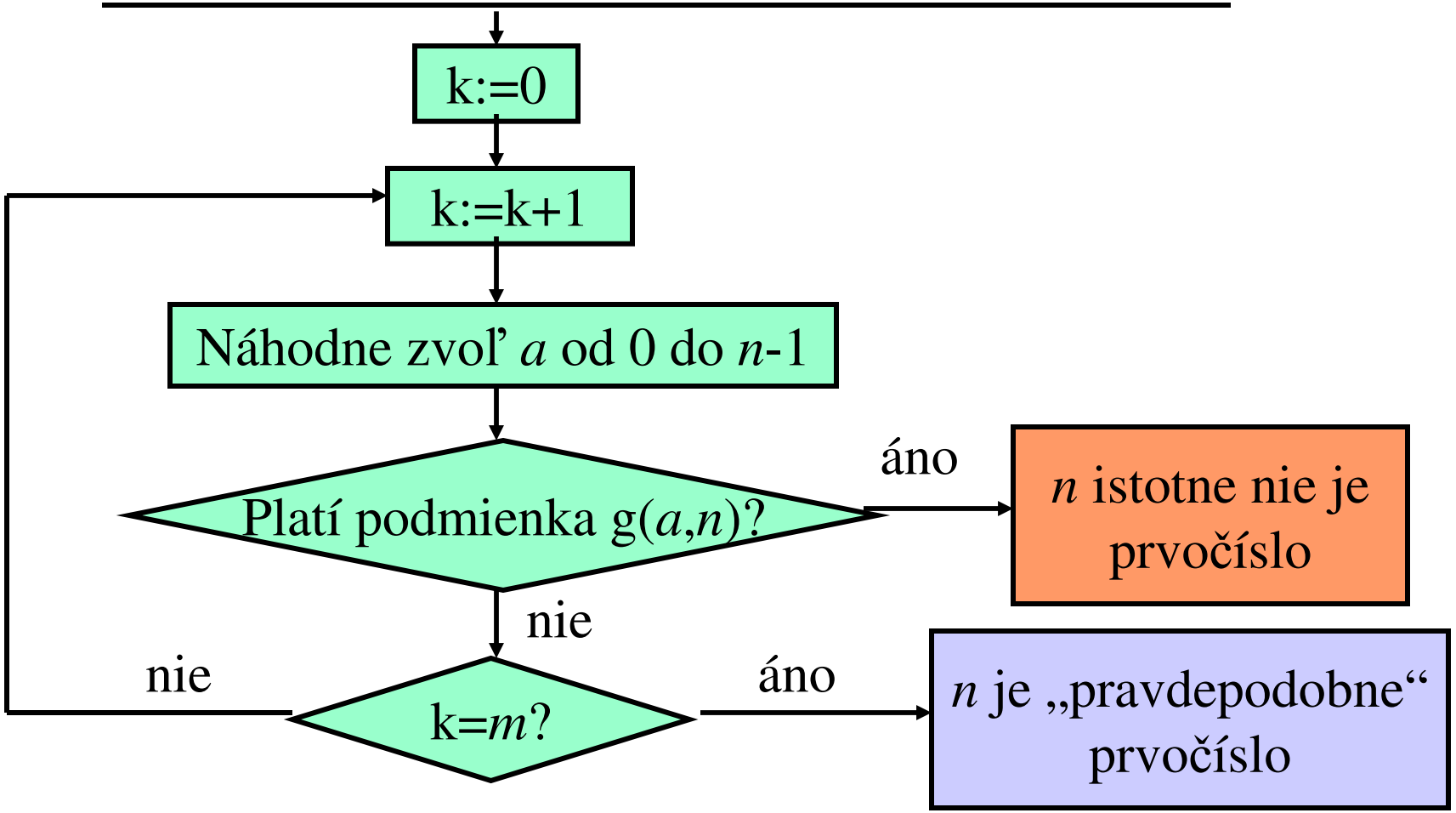
atď.

• • •

Pravdepodobnostné testy prvočíselnosti

Otázka: Je zadané číslo *n* prvočíslo?

Vstup: testované číslo *n*, počet opakovaní testu *m*



Millerov-Rabinov test

Podmienka g(a,n) znie:

$$a^d \neq 1 \bmod n \quad \textit{a súčasne} \quad a^{d\,2^r} \neq (n-1) \bmod n$$

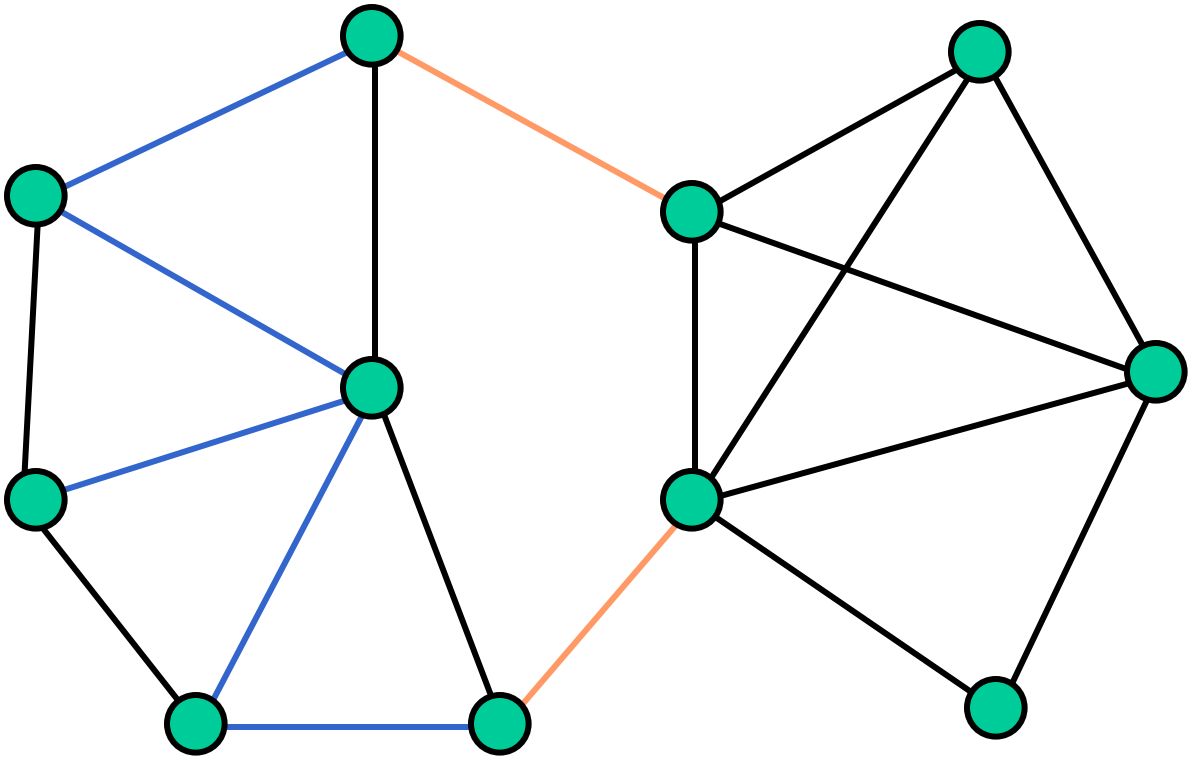
pre všetky $r=0,\ldots,s\text{-}1$, *kde* $n\text{-}1=d.2^s$, *d je nepárne.*

Pre akékoľvek prvočíslo MR-test určite vráti výsledok
„*n* je pravdepodobne prvočíslo“.

Pre akékoľvek zložené číslo *n* je pravdepodobnosť omylu
(t.j. výsledku „*n* je pravdepodobne prvočíslo“) menšia ako $1/4^m$

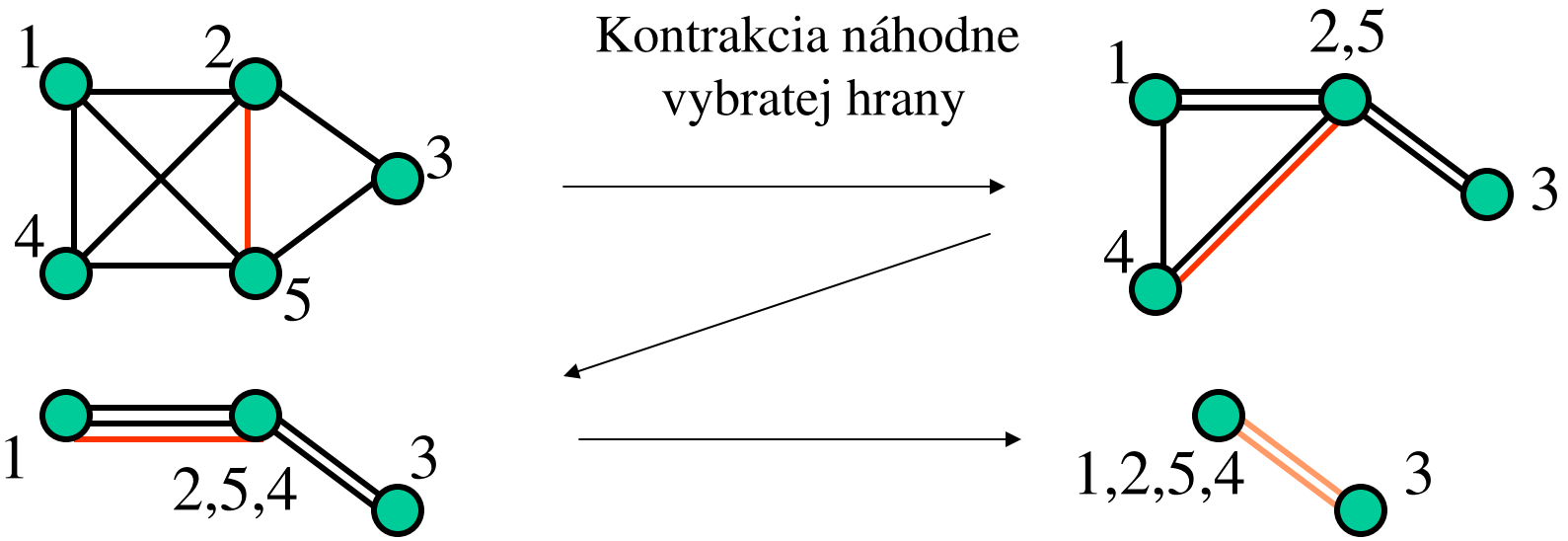
(Pre $m=20$ je $1/4^m < 0{,}000001$)

Hľadanie minimálneho rezu grafu



Rez grafu je taká množina hrán, ktorú keď odstánime, tak medzi niektorými vrcholmi už nebude existovať cesta (t.j. graf prestane byť súvislý). Minimálny rez je rez s minimálnym možným počtom hrán.

Znáhodnený algoritmus na hľadanie minimálneho hranového rezu grafu



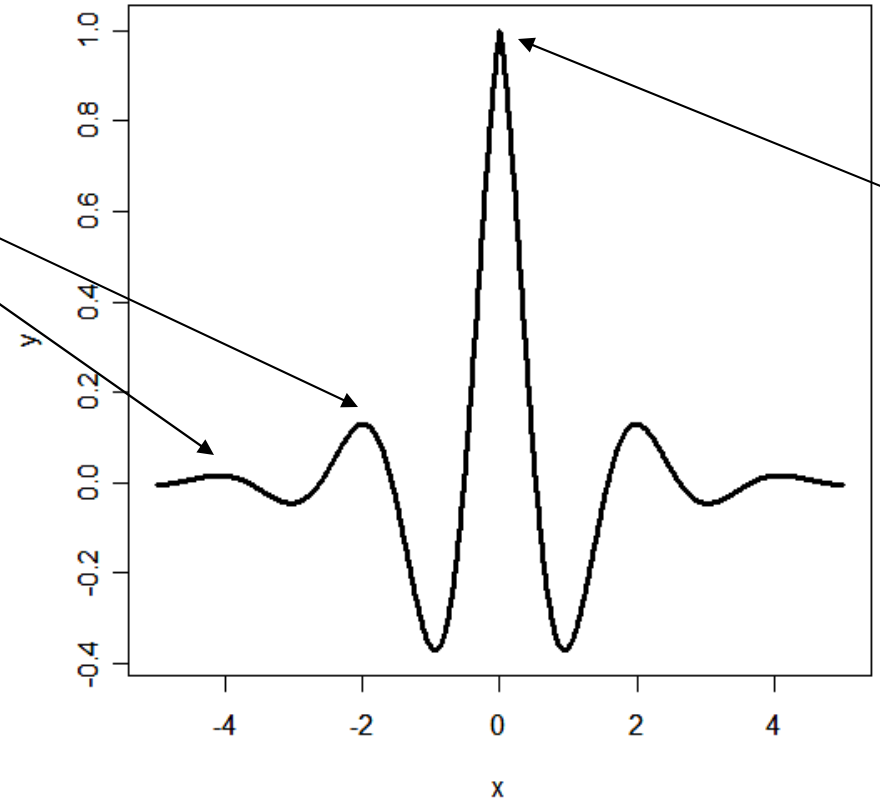
Pravdepodobnosť, že algoritmus nájde min. rez je aspoň $\frac{2}{n^2 - n}$

Ak algoritmus zopakujeme $n^2 \ln n$ krát, tak pravdepodobnosť nájdenia minimálneho rezu je viac ako $1 - 1/n^2$

Napríklad ak n=10 a opakujeme 231 krát, tak nájdeme min. rez na 99%.

Hľadanie globálneho maxima funkcie

lokálne maximá

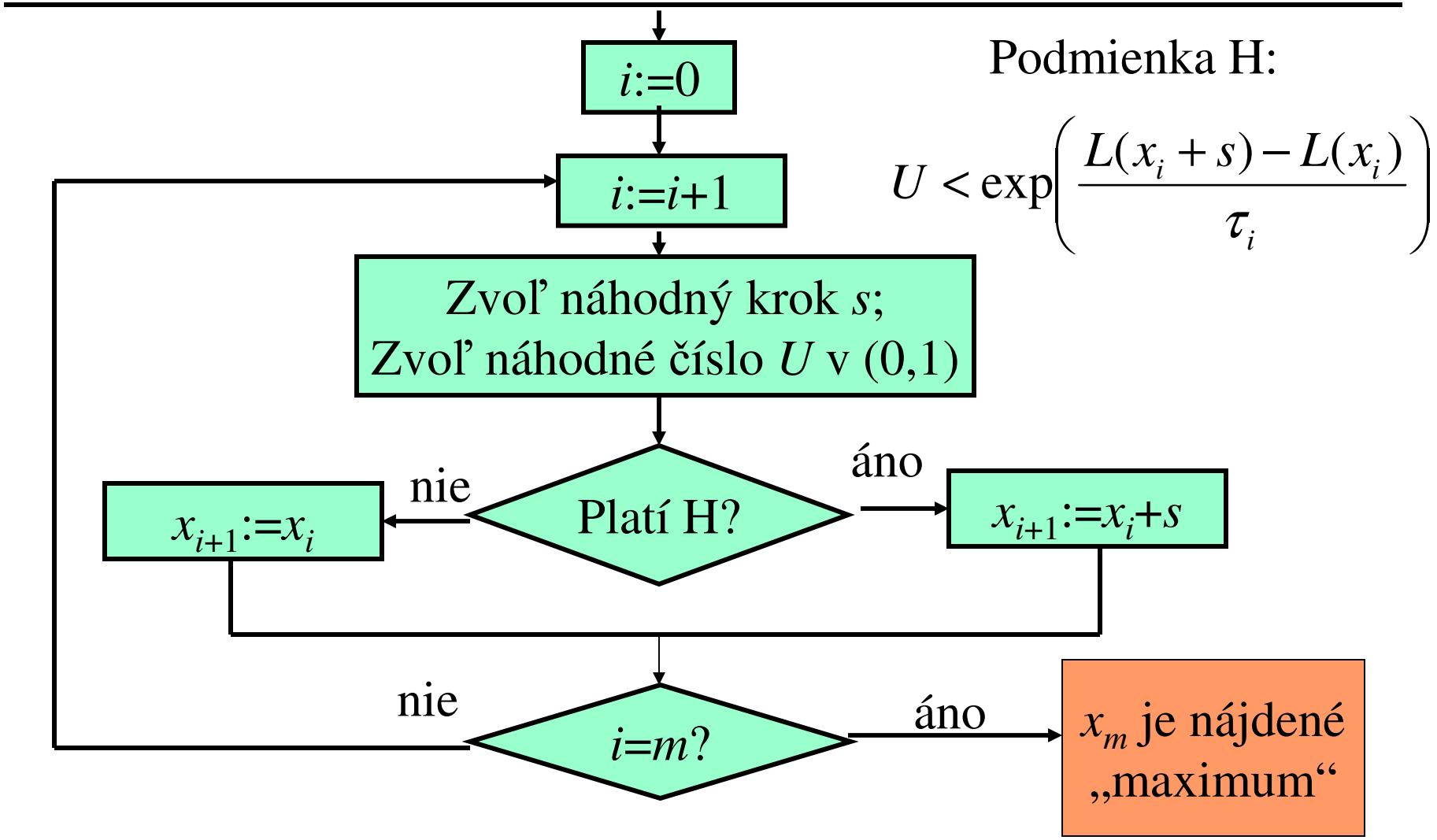


globálne maximum

Deterministické metódy (typu „choď v smere najväčšieho stúpania“) zostanú stáť v lokálnom maxime. **Simulované žíhanie** je jedna zo stochastických maximalizačných metód, ktoré vedia „vyskočiť“ z lokálnych miním.

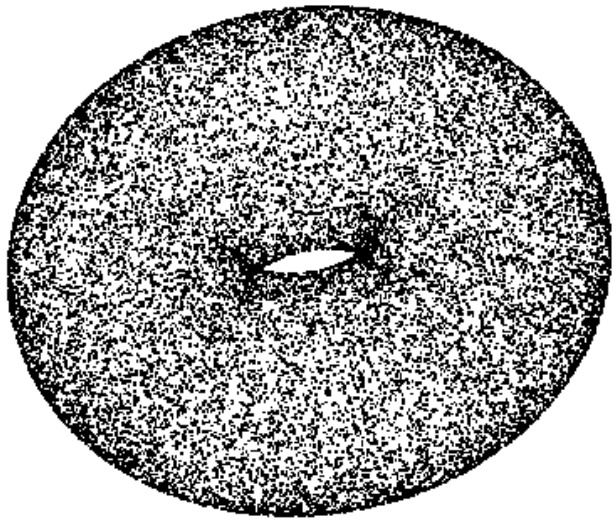
Simulované žíhanie (zjednodušene)

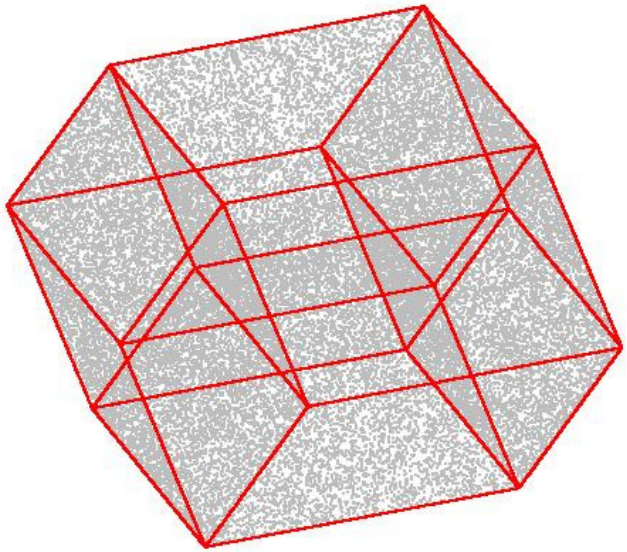
Vstup: funkcia L, počet krokov m, štartovací bod x_1, „teploty“ $\tau_1, \tau_2, \ldots$



Podmienka H:

$$U < \exp\left(\frac{L(x_i + s) - L(x_i)}{\tau_i}\right)$$





Ďakujem za pozornosť!