

Existuje náhoda? A načo nám je?

Mišo Forišek

<misof@mfnotes.ksp.sk>
Department of Computer Science
Faculty of Mathematics, Physics, and Informatics
Comenius University, Bratislava, Slovakia

Marec 2007

1 Filozofický úvod

Existuje náhoda? Čo myslíte vy?

Jeden možný pohľad prináša filozof Demokritos (áno, ten, čo vymyslel atóm): „Čo nám pripadá náhodné, je v skutočnosti len nepoznané, a príroda je zo svojej podstaty deterministická.“ (voľný preklad)

Príklad: dvaja páni sa dohodnú, že na druhý deň ráno pošlú sluhov presne o ôsmej po vodu. Keď sa sluhovia stretnú pri studni, považujú to za náhodu.

Opačný názor má Epikuros.

Hry ako kocky a ruleta na prvý pohľad podporujú Epikurovu teóriu, na druhý ale skôr Demokritovu. Ak vieme v nejakom okamihu povedať polohu a smer pohybu kocky, vieme predpovedať, čo s ňou bude ďalej.

Do 19teho storočia sa skôr verilo Demokritovi. (Einstein: „Boh nehrá v kocky.“) Svoju úlohu zohralo aj to, že ľudia sa náhody báli, podobne ako napr. sa báli pripustiť, že Galileo má pravdu a Zem nie je centrom vesmíru.

Potom prišla teória chaosu (nevýznamne malé zmeny môžu v niektorých systémoch viesť k diametrálne odlišným výsledkom) a dorazila to kvantová mechanika.

Súvisiaca otázka s „existuje náhoda?“ je otázka „existuje slobodná vôľa?“.

Existuje teda náhoda? Nevieme. Tu sa už dostávame do sveta fyzikálnych teórií, a tie nikdy nebudeme vedieť naisto dokázať. Momentálne to vyzerá tak, že možnosť „áno“ je pravdepodobnejšia.

2 Pomôže nám existencia náhody?

Pravdepodobnostné vs. deterministické porovnávanie dvoch súborov.

Predstavme si, že máme dve krabičky, ktoré fungujú nasledovne: Vopcháme k , vypadne nám náhodné prvočíslo z intervalu 1 až k . (Dve ich máme preto, že nejaký humorista určite skôr alebo neskôr jednu pokazí tým, že jej zadá $k = 1$.)

3 Keď bolo tých svedkov tak veľa...

... prečo potom neexistuje efektívne deterministické riešenie?

Problém je v tom, že svedkovia sú pre rôzne vstupy rozmiestnení veľmi divoko, a nech by sme si povedali ľubovoľnú „stratégiu hľadania svedka“, vždy môže prísť zlý bubák a podstrčiť nám taký vstup, kde budeme mať po chlebe.

4 Ak je to nepresné, je to nanič.

Nech napríklad má naše porovnávanie v konkrétnej situácii šancu 1/1000, že dá zlú odpoveď. Príde biznismen a povie, že také riziko si nemôže dovoliť. Čo s ním?

Riešenie ľahké, nech to pustí 10-krát a má kľud. Hardvérové chyby sú častejšie.

5 Rôzne druhy využitia náhody

Randomizovaný QuickSort a Select ako príklady Las Vegas algoritmov.

Porovnávanie núl a jednotiek v konečnej pamäti.

Zostrojenie našej čiernej krabičky – generovanie náhodných prvočísel.

6 Miller-Rabinov test prvočíselnosti

Rovnica $x^2 \equiv 1 \pmod{p}$ má práve dve riešenia: ± 1 . Totiž rovnicu môžeme prepísať nasledovne: p delí $(x-1)(x+1)$, a z toho to už vidieť.

Teraz nech p je nepárne prvočíslo. Začneme s tým, že z Malej Fermatovej vety vieme, že pre každé a nedeliteľné p platí: $a^{p-1} \equiv 1 \pmod{p}$.

Teraz, keďže p bolo nepárne, $p-1$ je párne. A máme teda $(a^{(p-1)/2})^2 \equiv 1 \pmod{p}$. A vidíme, že sú dve možnosti: $a^{(p-1)/2} = \pm 1$. A nič nám nebráni pokračovať v úvahe ďalej.

Nech teda $p-1 = 2^s d$, kde d je už nepárne. Zoberme si postupnosť: $a^{p-1} = a^{2^s d}, a^{2^{s-1} d}, \dots, a^d$. Sú dve možnosti, ako táto postupnosť vyzerá: Buď sú to samé jednotky, alebo je to niekoľko jednotiek, potom mínus jednotka, a potom garbage čo nás už nebude zaujímať.

Načo je nám toto dobré?

Majme nejaké n , ktoré sa tvári, že je prvočíslo. Zapišme $n-1$ ako $2^s d$. Teraz zvolíme náhodné a a spočítame vyššie uvedenú postupnosť. Ak vyzerá nejakou ináč (teda a^d nie je 1, a žiadne $a^{2^r d}$ nie je -1), práve sme odhalili, že n nie je prvočíslo.

Aby to malo praktický význam, čo potrebujeme? Dost' veľa svedkov. Našťastie je tomu tak. Dá sa dokázať, že ak n je zložené, aspoň $3/4$ možných hodnôt a budú svedkovia.

Iný pohľad na to isté: Vieme, že $a^{12} \equiv 1 \pmod{13}$. Potom vieme, že 13 delí

$$(a^{12} - 1) = (a^6 + 1)(a^6 - 1) = (a^6 + 1)(a^3 + 1)(a^3 - 1)$$

A to, čo náš test kontroluje, je, že či je niektorá zo zátvoriek súdeliteľná s 13.

7 Modulárna aritmetika

V \mathbb{Z}_p vieme „deliť“. Inými slovami, tvrdíme, že platí: Nech $u, x, y \in \mathbb{Z}$, $p \nmid u$. Potom ak $ux \equiv uy \pmod{p}$, tak $x \equiv y \pmod{p}$.

Dôkaz: Nech $ux \equiv uy \pmod{p}$. Toto je ekvivalentné s tvrdením, že p delí $ux - uy = u(x - y)$. Keďže p a u sú nesúdeliteľné, vyplýva z toho, že p delí $x - y$ a vyhrali sme.

Všimnime si hodnoty $a, 2a, \dots, (p-1)a$. Tvrdíme, že všetky tieto hodnoty dávajú po delení p navzájom rôzne nenulové zvyšky.

Že sú nenulové je zjavné. Nech pre nejaké dve i, j platí $ai \equiv aj \pmod{p}$. Už vieme, že potom nutne $i \equiv j \pmod{p}$ a sme hotoví.

Ako dôsledok môžeme uviesť, že ku každému a nedeliteľnému p existuje práve jedno $b \in \{1, \dots, p-1\}$ také, že $ab = 1$. Toto b značíme a^{-1} a voláme inverzný prvok k a . Dobré je to na to, že v \mathbb{Z}_p namiesto delenia a môžeme násobiť a^{-1} .

8 Dôkaz Malej Fermatovej vety

Keďže hodnoty kp sú prehádzaním hodnôt k , platí:

$$a \times 2a \times \dots \times (p-1)a \equiv 1 \times 2 \times \dots \times (p-1) \pmod{p}$$

Ľavú stranu vieme upraviť:

$$a^{p-1} \left(1 \times 2 \times \dots \times (p-1) \right) \equiv 1 \times 2 \times \dots \times (p-1) \pmod{p}$$

A teraz obe strany vydělíme $1 \times 2 \times \dots \times (p-1)$ a máme to.

9 Dôsledok Malej Fermatovej vety

Nech a je nedeliteľné p , a nech $p > 2$. Potom inverzný prvok k a vieme nájsť ako $a^{p-2} \pmod p$. A toto vieme vypočítať v čase $O(\log p)$.

Disclaimer. Tieto poznámky môžete voľne používať na ľubovoľné nekomerčné účely. Na akékoľvek komerčné využitie je potrebný súhlas autora. Ak v mojich poznámkach objavíte nejakú chybu, prípadne ich nejakým spôsobom viete doplniť, budem rád, ak mi dáte vedieť.

Pre potreby prípadného citovania má tento kus poznámok evidenčné číslo MF-0009.