Studentský matematicko-fyzikální časopis
ročník XII číslo 2

Termín odeslání: 9. 12. 2005

Zadání témat a úloh

Téma 4 – Generátory náhodných čísel

Víra v nepredikovatelnost vesmíru, víra v jeho nedeterminističnost výhodou.

Život je možná jen náhoda, ale vzhledem k jeho těžké poznatelnosti nikdo neví, jak dobrý generátor náhodných čísel vlastně je. Co je to dobrý náhodný generátor? Pro nás to bude jakýkoli náhodný děj s vhodným rozdělením pravděpodobnosti jeho jevů. Bylo by taky velmi užitečné, aby byl tento děj opakovatelný a to s co nejnezávislejšími výsledky.

Kromě různých generátorů se spojitým rozdělením pravděpodobnosti se zaměříme spíše na ty s konečnou množinou výstupních jevů M, kde u každého z jevů $x \in M$ známe jeho pravděpodobnost $P(x)$. Jako výstup by bylo vhodné mít vždy celé číslo v rozsahu 0 až $(n-1)$ s rovnoměrným rozdělením, konkrétně např. jednotlivé bity.

Co byste použili jako náhodný generátor vy? Co byste použili pro stroj (počítač), který neumí házet kostkou a potřebuje náhodných dat velké množství? Dokázali byste vytvořit generátor reálných čísel z intervalu $\langle 0, 1\rangle$ s rovnoměrným rozdělením z běžně dostupných pomůcek či dějů? Originalitě vašich nápadů se meze nekladou ...

Další problém je kvalita generátoru – pseudonáhodnost lze dosáhnout snadno např. iterováním $x_{i+1} = (x_i C_1 + C_2) \bmod C_3$ a používáním $x_i \bmod C_4$ jako i-tého náhodného čísla. (zde $C_4 \ll C_1 < C_3$) Jak dobrý (špatný) takový generátor je? (Jak těžké je uhádnout jeho vnitřní stav – pro známé parametry – a nějak omezit množinu možných výsledků? Uvědomte si, jak je tohle důležité například pro šifrování.)

Co je entropie generátoru? Nepřesně řečeno je to přibližný počet náhodných a nezávislých bitů získatelných z výsledku. (Například si nemůžu na zákadě jednoho hodu šestistěnnou kostkou k_6 vybrat z 2^3 možností, $2 < H(k_6) < 3$.) Entropie děje je přibližně $H(P) \approx \min\{-\log_2 P(x)\}$. Jak ale z nějakého rozdělení získat jednotlivé bity? Zkuste to například pro rozdělení $P(0) = 1/3$, $P(1) = 2/3$. Nezapomeňte, že můžete data z více výsledků kombinovat.

Své návrhy fyzických zdrojů pravděpodobnosti zkuste i podložit zdůvodněním jejich předpokládaných vlastností.

Úloha 2.1 – Ruská ruleta (4b)

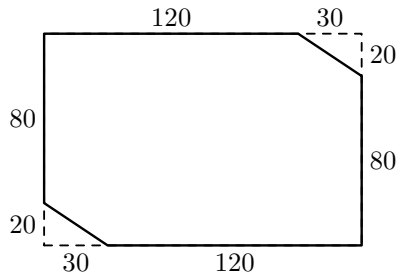
Jako profesionální mafiáni máte jistě praxi ve hře „Ruská ruleta“. Pravidla jsou následující: Do zásobníku šestiranného revolveru se vloží jeden náboj a na

začátku hry se zásobník protočí (jinými slovy, náboj se přesune na náhodné místo). Začíná hrát soupeř. Podrží si revolver u hlavy a stiskne spoušť. Poté (pokud stále ještě žije) podá pistoli vám. Je na vás, zda zásobník protočíte nebo ne, a poté stisknete spoušť vy. Hra pokračuje, dokud není jeden z hráčů po smrti.

a) Pokud jste chytří a protočíte zásobník vždy, když jste na tahu, a soupeř je hloupý a neprotočí zásobník nikdy, kolikrát za hru se průměrně stiskne spoušť?
b) Pokud soupeř vždy zopakuje se zásobníkem to co vy (tj. protočí pokud jste protočili a neprotočí pokud jste neprotočili) a soupeř začíná (s protočeným zásobníkem samozřejmě), jak hrát, aby byla pravděpodobnost vaší smrti co nejmenší?

Úloha 2.2 – Rohož (4b)

Při neopatrné manipulaci s ohněm shořely krbové rohoži dva rohy (viz obrázek). Vaším úkolem je rohož opravit rozstříháním na co nejméně kousků libovolného tvaru tak, aby se z nich dala beze zbytku sestavit čtvercová rohož. Nastříhané kousky nelze převracet. Pokuste se dokázat, že vaše řešení je optimální a řešení s menším počtem kousků nemůže existovat.



Úloha 2.3 – Cyklista na kolotoči (4b)

Představte si cyklistu, který jede na kolotoči po obvodu tak, že v inerciální soustavě se nepohybuje (jede obvodovou rychlostí opačným směrem, než se pohybuje kolotoč). Z pohledu inerciální soustavy na něj nepůsobí žádná síla (takže se nemusí nijak naklánět, aby ji vyrovnával). Podívejme se však na stejný děj z pohledu soustavy spojené s kolotočem: Na cyklistu působí síla odstředivá, takže se musí naklonit, aby ji kompenzoval.

Jak je možné, že popis tohoto děje ve dvou různých vztažných soustavách dává různé výsledky?

Adresa redakce:

M&M, OVVP, UK MFF
Ke Karlovu 3
121 16 Praha 2

Telefon: +420 221 911 235
E-mail: MaM@atrey.karlin.mff.cuni.cz
WWW: http://mam.mff.cuni.cz

Časopis M&M je zastřešen Oddělením pro vnější vztahy a propagaci Univerzity Karlovy, Matematicko-fyzikální fakulty a vydáván za podpory středočeské pobočky Jednoty českých matematiků a fyziků.