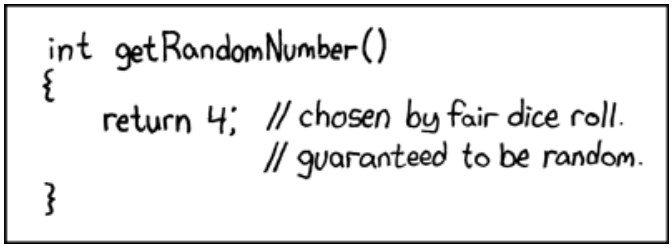
Generatorji slu"cajnih "stevil

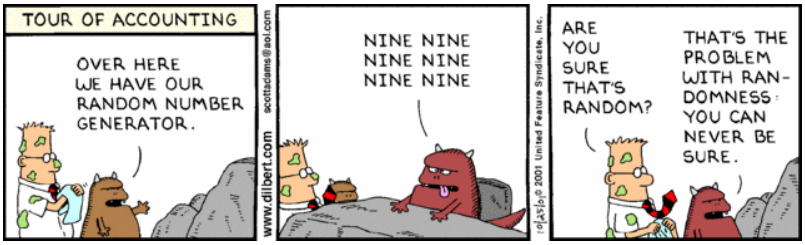
Miha Čančula

26. november 2011

Povzetek

The generation of random numbers is too important to be left to chance. – Robert R. Coveyou, *Oak Ridge National Laboratory* ˙





1 Enakomerne porazdelitve

Najenostavnejša je bila primerjava med generatorji, ki vrnejo naključna števila, ki so enakomerno razporejena po nekem intervalu. Takšnih generatorjev je tudi največ, zato sem jih lahko primerjal. Za vsakega sem izračunal porazdelitev verjetnosti z razdelitvijo v 100 predalčkov, nato pa na ti porazdelitvi izvajal statistične teste. Uporabil sem naslednje generatorje:

1. Funkcija `rand()` iz standardne knjižnice jezika `C`
2. Linuxova datoteka `/dev/urandom`
3. Kalkulatorski generator, opisan v navodilih
4. "Mersennov vrtinec", implementiran v `GSL`

Poleg teh generatorjev sem za primerjavo vključil še dva izvora naključnih števil, ki števil ne generirata s številskim algoritmom, ampak jih izračunata težko predvidljivih dogodkov. V nasprotju z generatorji na ta način ne moremo dobiti poljubnega števila naključnih števil, zato sem velikost vzorca omejih na 4096 števil, kjer ima vsako število 32 bitov.

1. Linuxova datoteka `/dev/random`, ki naključnost dobi iz dogodkov v računalniku, na primer s premikanjem miške
2. Spletna stran `random.org`, ki naključnost dobi iz meritev atmosferskega šuma

Test	Enodimenzionalni χ^2			Dvodimenzionalni χ^2			Kolmogorov-Smirnov		
Velikost vzorca	2^{12}	2^{18}	2^{24}	2^{12}	2^{18}	2^{24}	2^{12}	2^{18}	2^{24}
`rand()`									
`/dev/urandom`									
Kalkulatorski									
Mersenne									
`/dev/random`									
`random.org`									

Tabela 1: Statistični testi enakomernosti naključnih števil

2 Smeri v prostoru

Za generacijo naključnih meri v prostoru najprej potrebujemo generator enakomernih naključnih števil. V ta namen sem uporabil kar najboljši generator iz prve naloge, to je bil Mersennov vrtinec. Knjižnica `GSL` ima vgrajeno rutino, ki s pomočjo enakomernega generatorja vrne naključen enotski vektor v treh dimenzijah. Kljub temu pa sem za primerjavo še sam napisal takšen generator. Za primer brez sevanja je algoritem enostaven, saj vemo da mora biti porazdelitev verjetnosti enakomerna po spremenljivkah φ in $\cos\vartheta$. Če sta r_1 in r_2 dve naključni števili z intervala $[0, 1)$, lahko prostorski kot zapišemo kot

$$\varphi = 2\pi r_1 \tag{1}$$
$$\vartheta = \arccos(2r_2 - 1) \tag{2}$$

Pri dipolnem sevanju je porazdelitev verjetnosti po kotu ϑ bolj zapletena.

$$\frac{\partial p}{\partial \vartheta} \propto \sin^3\vartheta \tag{3}$$
$$\mathrm{d}p = A\sin^3\vartheta\,\mathrm{d}\vartheta = A(1-\cos^2\vartheta)\,\mathrm{d}(\cos\vartheta) \tag{4}$$
$$= A\,\mathrm{d}\left(\cos\vartheta - \frac{\cos\vartheta^3}{3}\right) \tag{5}$$

Če upostevamo, da je r_2 enakomerno razporejen, dobimo enačbo za ϑ.

$$\frac{\cos^3\vartheta}{3} - \cos\vartheta + A(r_2 - x_0) = 0 \tag{6}$$

Da izrazimo $\cos\vartheta$ s pomočjo r_2 bomo morali rešitiv polinom tretje stopnje. Iz pogoja $\int \mathrm{d}p = 1$ in upoštevanja omejitve $\cos\vartheta \in [-1, 1]$ določimo konstanti A in x_0.

3 Gaussova porazdelitev

Tu je postopek podoben kot pri generiranju naključnih smeri. Uporabimo generator enakomerno porazdeljenih števil, ki jih transformiramo na tak način, da bo porazdelitev transformirank Gaussova. V ta namen se največ uporabljata Box-Mullerjeva transformacija in metoda "zigurat".