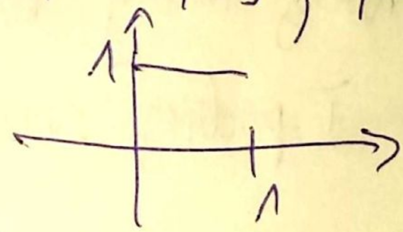
PSK - zajęcia zaplanowane na 2.04

<u>Wstęp</u>. <u>Stochastyczne</u> ujęcie ZJAWISKA SYMULACJI (a także jest najefektywniejsze) <u>wymaga</u> umiejętności stosowania procedury GENEROWANIA LICZB LOSOWYCH (RANDOM NUMBERS), czyli liczb z przedziału $[0,1)$, które są reprezentowane przez zmienną $X \in \mathcal{U}([0,1))$, czyli

$$\Omega \ni \omega \longrightarrow X(\omega) \in [0,1),$$ gdzie

funkcja gęstości ma postać:



<u>Powstaje pytanie</u>: jak zrealizować ten proces/procedurę?

W dobie „przedkomputerowej" stosowano do tego celu tzw. GENERATORY FIZYCZNE. Sprowadzało się do tzw. „generowania ręcznego" albo „mechanicznego" w postaci: obracania kołem, rzucania monetą/kością, losowaniem karty.

W dobie IT robi się to przy użyciu tzw. GENERATORÓW PROGRAMOWYCH.

Ponieważ wykonywane (przez komputer) takiego programu ma <u>charakter deterministyczny</u> (bo zostało zaplanowane!)

nie można wyniku tych realizowanych procesu / procedury nazywać LOSOWYM.
Z drugiej strony algorytmy realizujące te procesy dbają o to, aby:

(i) ich wynikiem były liczby z $[0,1]$

(ii) przyjmowały się w warunkach statystycznej niezależności.

Z tego powodu nazywamy je LICZBAMI (PSEUDO)LOSOWYMI.
Metodologia określająca (PSEUDO)LOSOWY SPOSÓB GENEROWANIA polega na:

a) zainicjowaniu wartości początkowej $x_0 \in [0,1)$, zwanej też „ziarnem" (ang. SEED)

b) stosowaniu rekurencji, celem generowania kolejnych liczb, gdzie postać tej rekurencji jest następująca:

$$x_n = a x_{n-1} \pmod{m}, \text{ gdzie}$$

a oraz $m \in \mathbb{Z}_+$ (dane liczby dodatnie
całkowite = naturalne)

Mamy wz:

$$\boxed{\begin{array}{ll} X_n = X_0 & \text{dla } n=0 \\ X_n = a X_{n-1} \ (\mathrm{mod}\ m) & \text{dla } n \geq 1 \\ \text{gdzie } a, m \in \mathbb{Z}_+ \text{ dane} & \end{array}}$$

Uwagi:

1°. Przypomnienie relacji modulo (czyli kongruencji).

Niech dana będzie liczba $p \in \mathbb{Z}_+$.

Mówimy, że $n, m \in \mathbb{Z}$ przystają modulo p,

$$n = m \ (\mathrm{mod}\ p) \equiv r_p(n) = r_p(m),$$

gdzie $r_p(n)$ oznacza resztę z dzielenia n przez p.

Potrzebna jest więc ZASADA PODZIELNOŚCI:

Niech dana będzie liczba całkowita $k \in \mathbb{Z}$ oraz ustalona liczba $d \in \mathbb{Z}_+$.

Wtedy istnieją dokładnie dwie liczby N, r:

$$k = N \cdot k + r, \text{ gdzie } r \in [0, k-1].$$

Wtedy $r = r_k(w)$ - nazywamy resztą z dzielenia k przez k.

Np. $7 = 1 \cdot 4 + 3$ ($k=7$, $d=4$)

$-9 = (-3) \cdot 4 + 3$

$r_4(7) = r_4(-9) = 3$

2°. Podstawowa własność kongruencji mówi, że

$n \equiv m \pmod p \equiv p \mid n-m$,

czyli n i m są w relacji mod p $\equiv$ p dzieli ich różnicę.

W przykładzie powyżej $7-(-9)=16$ i podzielne przez 4.

3°. Relacja mod ma 3 podstawowe własności znane z kursu MAT. DYSKRETNEJ:

- zwrotna : $n \equiv n \pmod p$
- symetryczna $n \equiv m \pmod p \Longrightarrow m \equiv n \pmod p$
- przechodnia $n \equiv m \pmod p$ i $m \equiv s \pmod p \Longrightarrow n \equiv s \pmod p$

co wynika wprost z uwagi 2.

WIEMY, że każda relacja o trzech własnościach jest RELACJĄ RÓWNOWAŻNOŚCI.

TO z kolei oznacza, że generuje ona partycję zbioru na którym jest określona.

Każdy atom takiej partycji jest właśnie klasą abstrakcji danej liczby:

$$[n]_{mod\,p} = \{ m : n \equiv m \ (mod\, p) \}.$$

4°. Wracamy do naszego algorytmu

$$x_n = x_0 \quad n = 0$$

$$x_n = a x_{n-1} \ (mod\, m) \text{ dla } n \geq 1$$

$$a, m \in \mathbb{Z}_+$$

Mamy kolejno:

$$x_1 = a x_0 \ (mod\, m)$$

$$x_2 = a x_1 \ (mod\, m)$$

itd.

Zatem $r_m(X_1) = r_m(aX_0) \in \{0,1,2,\dots,m-1\}$

oraz $X_1 = r_m(X_1) \pmod m$

Dlatego $\frac{X_1}{m} \in [0,1)$. Podobnie dla $\frac{X_n}{m}$.

Liczby $\frac{X_n}{m}$, $n \geq 1$ są tymi pseudolosowymi liczbami, które przybliżają wartości zmiennej losowej $X \in \mathcal{J}[0,1]$.

Weźmy przykład rachunkowy:

Przyjmijmy, że $X_0 = 7/4$, $a = 4$, $m = 9$

Wtedy kolejno:

$$X_1 = aX_0 \pmod 9 \equiv X_1 = 1 \pmod 9$$

i $\frac{X_1}{9} = 1/9$

$$X_2 = aX_1 \pmod 9 \equiv X_2 = 4 \pmod 9$$

i $\frac{X_2}{9} = 4/9$

$$X_3 = aX_2 \pmod 9 \equiv X_3 = 16 \pmod 9 \equiv$$

$$X_3 = 7 \pmod 9$$

$$\frac{X_3}{9} = 7/9$$

$x_4 = a x_3 \pmod 9 \equiv x_4 = 28 \pmod 9 \equiv$

$x_4 = 1 \pmod 9$

$\frac{x_4}{9} = 1/9$. itd.

<u>Uwagi</u>:

Ponadto pełne, i wartości $\frac{x_n}{m}$ wygenerowane algorytmem przyszły <u>mogą się powtarzać</u> —
TAK JEST ZAWSZE.

DLATEGO stałe a i m muszą spełniać następujące kryteria

1) dla ustalonej wartości seed x_0, $\overbrace{\frac{x_n}{m}}^{\text{pojawianie się}}$ powinno przebiegać w warunkach statyst. niezależności

2) Okres powtórzenia się wartości

$$\frac{x_n}{m} = \frac{x_k}{m} \qquad k > n,$$

czyli $k-n$ powinien być odpowiednio <u>duży</u>!

3) X_n powinny dać się obliczyć na maszynie.

Wykazano, że na 32-bitowej maszynie

$m = 2^{31} - 1$, $a = 7^5$ daje

$k - n = 16.807$

ZADANIE 1 (o algorytmie kwadratowym von Neumanna).

Cel: generowanie liczb (pseudo)losowych o jednakowej liczbie cyfr m, gdzie m jest parzyste. Liczby te są całkowite.

Algorytm. 1°. Zainicjuj algorytm liczbą całkowitą X_0

2°. Weź ostatnią wygenerowaną liczbę X_{n-1}

3°. Oblicz $Y_n \stackrel{df}{=} X_{n-1}^2$

4°. Jeśli to potrzebne dopisz odpowiednią liczbę zer na początku Y_n, tak aby otrzymać liczbę $2m$ cyfrową

5°. Za X_n przyjmij m środkowych cyfr z modyfikacji Y_n.

Oczekiwania. Napisać program realizujący ten algorytm dla (np. $n=100$ liub).

Podam przykład liczby, aby algorytm był bardziej zrozumiały.

Weźmy $m=2$ i $X_0=12$ (seed).

Wtedy mamy kolejno:

I przebieg: $Y_1 = X_0^2 = 144$

$$Y_1 \xrightarrow{\text{modyf.}} \tilde{Y}_1 = 0144$$

$$X_1 = 14$$

II przebieg: $Y_2 = X_1^2 = 196$

$$Y_2 \to \tilde{Y}_2 = 0196$$

$$X_2 = 19$$

itd.

Mamy ciąg $(14, 19, \ldots)$, których X_0 odrzucamy!

Podamy teraz klasyczny przykład użycia liczb (pseudo)losowych, bowiem po raz pierwszy były do tego celu wykorzystane.

Przykład. Obliczymy całkę

$$\Theta = \int_0^1 g(x)\,dx$$

Idea postępowania: dla rozkładu jednostajnego $X \in U([0,1])$, jeśli weźmy zmienną losową $Y = g(X)$, to

$$EY = \int_{-\infty}^{+\infty} u f_Y(u)\,du = \int_{-\infty}^{+\infty} g(u) f_X(u)\,du,$$

~~Ale $F_Y(t) = P(\{\omega\in\Omega : Y(\omega) < t\}) = P(\{\omega\in\Omega : g(X(\omega)) < t\})$ i trzeba założyć, że g jest ciągła na $[0,1]$~~

czyli $EY = \int_0^1 g(u)\,du = \Theta$, z def. f_X.

Wydaje nie wspomnieć wartości oczekiwanej zm. losowej Y.

Z mocnego prawa wielkich liczb Bernoulliego wiemy, że:

a) biorąc ciąg $X_1, X_2, \ldots, X_n, \ldots$ niezależnych zm. losowych o rozkł. $U([0,1])$,

b) zamieniając go na
$$Y_1 = g(X_1),\ Y_2 = g(X_2), \ldots$$

c) uśredniając go
$$\sum_{i=1}^{n} \frac{g(X_i)}{n}$$ otrzymujemy ciąg

zbieżny do $Eg(X) = \Theta$

Efekt (teoretyczny) zaprezentowany wyżej możemy praktycznie zrealizować za pomocą liczb (pseudo)losowych.

Takie podejście do rozwiązania problemu leży u podstaw METOD MONTE CARLO, o czym mowa będzie później

ZADANIE 2

Obliczyć aproksymując MMC wartość całki $\int_0^1 e^{-x^2}\,dx$.

Wskazówka. Korzystając z ZAD 1 mamy $(x_k)_{k=1}^{1000}$ ciąg liczb (pseudo)losowych i obliczamy $\sum_{i=1}^{1000} \frac{e^{-x_i^2}}{1000}$.

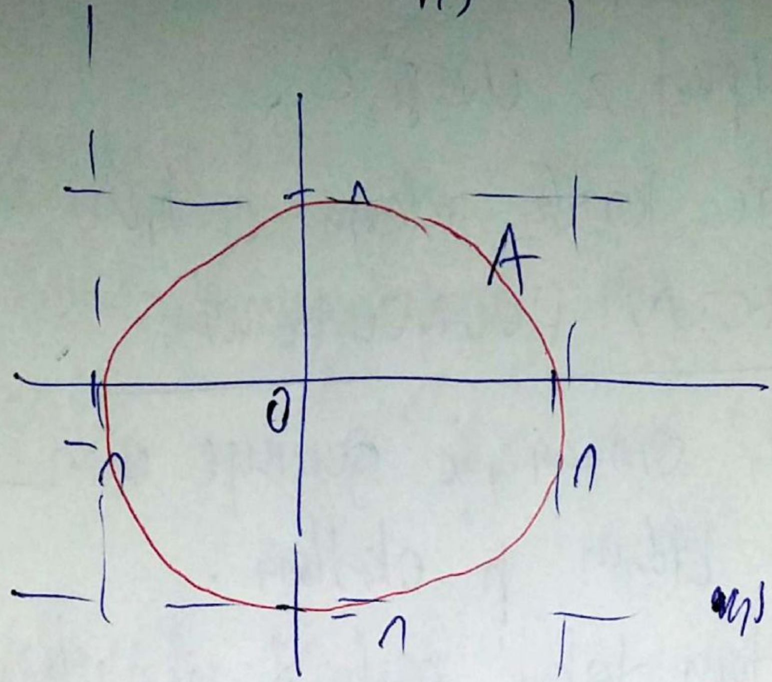
Innym dobrze znanym przykładem z zastosowania liczb (pseudo)losowych na wczesnym etapie jest problem aproksymacji liczby π.

Aproksymacja liczby π (I podejście)

Weźmy zbiór

$$A = [-1,1] \times [-1,1]$$ jak na rys. 1

poniżej.



rys 1

Niech X, Y niezależne zm losowe o rozkł. jednostajnym na $[-1,1]$ każda i weźmy wektor losowy

$$\Omega \ni \omega \longrightarrow (X(\omega), Y(\omega)) \in A$$

Wpisujemy w kwadrat okrąg jak wyżej, który ogranicza koło O o środku $(0,0)$ i promieniu 1

Interesuje nas zdarzenie

$$C = \{\omega \in \Omega : (X,Y)(\omega) \in O\}$$

Z założenia mamy model geometryczny, a ten

$$P(C) = \frac{\text{pole koła}}{\text{pole kwadratu}} = \frac{\pi 1^2}{4} = \frac{\pi}{4}$$

Ale
$$(X,Y)(\omega) \in O \equiv X^2(\omega) + Y^2(\omega) \leq 1$$

Zatem
$$P\left(\{\omega \in \Omega : X^2(\omega) + Y^2(\omega) \leq 1\}\right) = \frac{\pi}{4}$$

Mamy „klucz" do π !

Musimy go „nieco" poprawić, aby zastosować MPWLB, gdzie mowa jest o wartości oczekiwanej.

W tym celu definiujemy zm. losową
$$\Omega \ni \omega \longrightarrow Z(\omega) = \begin{cases} 1 & X^2(\omega) + Y^2(\omega) \leq 1 \\ 0, & \text{dla pozostałych } \omega \end{cases}$$

Wtedy
$$EZ = P\left(\{\omega \in \Omega : Z(\omega) = 1\}\right)$$
$$= P\left(\{\omega \in \Omega : X^2(\omega) + Y^2(\omega) \leq 1\}\right).$$

Mamy do pokonania jeszcze jeden problem: potrzebujemy dwie zmienne losowe X, Y.
Pokażemy jak zrobić je z jednej:

Niech $U \in \mathcal{U}([0,1])$.

Wtedy $2U \in \mathcal{U}([0,2])$, oraz

$$2U - 1 \in [-1,1]$$

Mając więc $U_1 = U$, oraz biorąc kopię U_1, w postaci U_2, dostajemy dla

$$X = 2U_1 - 1, \quad Y = 2U_2 - 1$$

wektor (X,Y), o którym mowa wyżej.

ZADANIE 3

Stosując powyższą metodologię (opartą na kolejności HMC) oszacuj π.

WSK. 1) Wykorzystaj ZADANIE 1

2) Po wygenerowaniu $(x_1, x_2 .. x_n)$

Więc $u_k^1 = 2x_k - 1$ $\quad k = 1, 2 \ldots n$

$u_k^2 = 2x_k + 1$ $\quad (n = 100)$

takie, że $(2u_k - 1)^2 + (2u_k + 1)^2 \in 1$,

i wskazać liczbę tych k, które spełniają powyższy warunek.