4. Generatory liczb losowych:

- generator liniowy kongruencyjny LCG (postać ciągu Lehmera, parametry, okres generatora, obliczanie kolejnych wyrazów ciągu):

  - ciąg Lehmera: $x_i = (a * x_{i-1} + 1) \bmod m$
  - uogólniony: $\boldsymbol{x_i = (a * x_{i-1} + c) \bmod m}$
  - służy do obliczania kolejnych wyrazów ciągu
  - parametry:
    - a – mnożnik, 0 < a < m;
    - m – moduł, 0 < m;
    - c – przyrost, 0 <= c < m;
    - x_0 – ziarno, początkowa wartość, którą inicjuje się generator;
    - x_i – i-ta liczba pseudolosowa;
    - x_{i-1} – poprzednia liczba pseudolosowa;
  - maksymalna długość cyklu wynosi m, pod warunkiem wystąpienia:
    - c i m są względnie pierwsze;
    - a - 1 jest podzielne przez wszystkie czynniki pierwsze m;
    - a - 1 jest wielokrotnością 4, jeśli m jest wielokrotnością 4;

- test struktury przestrzennej:

  - wykonuje się go dla (n-1) par wyrazów ciągu n liczb pseudolosowych: (x_1,x_2), (x_2,x_3), (x_3,x_4), ..., (x_{n-1},x_n)
  - dla których robimy wykres rozrzutu i obserwujemy, czy ułożenie punktów nie jest zbyt równomierne;
  - mają być +- równomierne, ale NIGDY w pełni równomierne, by mogły reprezentowć liczby losowe;

- cechy ciągu liczb generowanego przez LCG:

  - jest deterministyczny - zainicjowany tą samą wartością daje zawsze taki sam ciąg pseudolosowych liczb;
  - pod pewnymi względami jest nieodróżnialny od ciągu uzyskanego z prawdziwie losowego źródła;
  - liczby ciągu posiadają równomierny rozkład prawdopodobieństwa;
  - liczby ciągu mogą przyjmować wartości od 0 do m – 1;
  - w danym cyklu (okresie odługości maksymalnie m) liczby nie mogą siępowtarzać;

- fizyczne i programowe generatory liczb losowych (przykłady, różnice)

  FIZYCZNE:
  - mechaniczne: np. rzut monetą, losowanie z urny, ruletka;
  - oparte o procesy fizyczne: np. szum biały w urządzeniach elektrycznych, rozpad radioaktywny, promieniowanie kosmiczne;

PROGRAMOWE:
- liniowe: np. generator LCG, generator multiplikatywny;
- mieszane: np. generatory na rejestrach przesuwnych, generator Fibonacciego;
- nieliniowe: generator nielinowy Eichenauera-Lehna, generator Eichenauera-Hermanna;

RÓŻNICE:

FIZYCZNE GENERATORY	PROGRAMOWE GENERATORY
ciągi liczb losowych (niezależne, nieskorelowane)	ciągi liczb pseudolosowych (zależne, w pewnym stopniu skorelowane)
wymagana ciągła kalibracja (testowanie parametrów)	wymagany odpowiedni dobór parametrów, by maksymalizować długość okresu ciągu
czasochłonne	szybkie
kłopoty techniczne z obsługą	łatwość obsługi
brak powtarzalności serii	powtarzalność ciągów generowanych liczb
brak wpływu na liczbę wymiarów	dowolna liczba wymiarów
brak wpływu na rozkład generowanych liczb	możliwość generowania dowolnego rozkładu

- zastosowania ciągów liczb losowych:

  - w kryptografii (generowanie kluczy);
  - w grach losowych;
  - w wyznaczaniu próby z generalnej populacji;
  - w symulacjach różnych procesów losowych (generowanie pseudolosowych warunków początkowych);
  - w testowaniu algorytmów dla losowych zestawów danych;
  - w algorytmice:

    - algorytmy genetyczne - selekcja oraz mutacja
    - algorytmy heurystyczne - symulowane wyżarzanie
    - sztuczna inteligencja - początkowe wartości połączeń pomiędzy neuronami
    - algorytmy probabilistyczne - metody Monte-Carlo

- generowanie liczb losowych z rozkładu $N(\mu;\delta)$ na podstawie próby z rozkładu $N(0;1)$

  - dla uzyskania rozkładu normalnego korzystamy z metody eliminacji Boxa-Müllera jeżeli na wejściu mamy rozkład jednostajny;
  - tu jednak mamy rozkład normalny, co ułatwia sprawę;
  - y – to nasze $N(\mu;\delta)$, x – to nasze $N(0;1)$
  - $y = \delta x + \mu$;

- generowanie liczb losowych z rozkładu $U(a;b)$ na podstawie próby z rozkładu $U(0;1)$

  y – to nasze $U(a;b)$, x – to nasze $U(0;1)$

  y = x(b-a)+a; // rozkład ciągły
  y = round(x(b-a+1)+a-0.5); // rozkład dyskretny

- generowanie liczb losowych z rozkładu wykładniczego na podstawie próby z rozkładu U(0;1) (metoda odwracania dystrybuanty)

  - metodę odwracania dystrybuanty da się stosować jedynie dla odwracalnych funkcji (NIE dla rozkładu normalnego);
  - dystrybuanta $F(X) = P(X \le x) = \int_{-\infty}^{x} f(t)dt$
  - dla rozkładu wykładniczego $f(t) = \lambda e^{-\lambda x}$
  - zatem $F(X) = \begin{cases} 1 - e^{-\lambda x}, & x \ge 0 \\ 0, & x < 0 \end{cases}$
  - a teraz szukamy funkcji odwrotnej (odbicie względem prostej y = x):

$$
\begin{aligned}
y &= \lambda e^{-\lambda x} \\
1 - y &= e^{-\lambda x} \\
\ln(1 - y) &= -\lambda x \\
x &= -\frac{1}{\lambda}\ln(1 - y)
\end{aligned}
$$

Zatem jeżeli otrzymaliśmy próbę z rozkładu U(0;1) i zapisaliśmy ją w wektorze x, to wygenerowanie liczb losowych zapiszemy do wektora y, po następującej transformacji:

$$y = -\frac{1}{\lambda}\ln(1 - x)$$

Opracowała: Maria Łysik, 13.01.13