Przedstawienie sposobów generowania liczb losowych i pseudolosowych.

Liczby losowe wykorzystywane są w wielu aspektach świata cyfrowego, takich jak gry, bankowość, grafika czy kryptografia, ale czym tak właściwie one są? Dana liczba może powtórzyć się raz, cztery razy lub wcale, szansa na wystąpienie każdej z liczb jest jednakowa.  
Obraz zawierający pianino/fortepian, klawiatura

Opis wygenerowany automatycznie  
Aby wygenerować naprawdę przypadkową liczbę, komputer musiałby monitorować naturalnie występujący proces niedeterministyczny[[1]](#footnote-1). Jest to zarówno kosztowne, jak i powolne, więc większość komputerów osobistych nie posiada prawdziwych generatorów liczb losowych.

Liczbami pseudolosowymi nazywamy nieprzewidywalną sekwencje liczb (należy jednak pamiętać, nieprzewidywalna, ale nie niepowtarzalna). Generatory liczb losowych[[2]](#footnote-2) przeprowadzają proste, losowe działanie matematyczne pomnożone przez (najczęściej) losowe, stosunkowo krótkie ziarno[[3]](#footnote-3) i w wyniku oddają nam pseudolosową liczbę. Jednak początkowe ziarno w końcu się powtórzy, a ciąg zapętli, co spowoduje ponowne wyświetlenie tych samych liczb. Im początkowe ziarno będzie dłuższe, tym więcej czasu zanim liczby zaczną się powtarzać.

Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Opis wygenerowany automatycznie

Generowanie liczb losowych jest praktyką stosowaną od starożytności do współczesności, zaczynając od archaicznych metod jak zwykły rzut kośćmi lub monetą, rozwijaliśmy losowania dalej. Metody mechaniczne takie jak ruletki generujące liczby od 1 do 36 (plus zero). Wyżej już omówione metody matematyczne (pseudolosowe). Metody fizyczne jak np. Szum termiczny (wykorzystywane są fluktuacje[[4]](#footnote-4) termiczne w przewodnikach elektrycznych do generowania liczb losowych). Kończąc na mechanizmach kwantowych.

Kwantowy sprzętowy generator liczb losowych to rozwiązanie wykorzystujące zjawiska kwantowe do wytwarzania liczb losowych, o wyniku czy stanach i liczbach losowych decyduje proces fizyczny.  
W największym uproszczeniu – w urządzeniu takim wygenerowany impuls laserowy niosący paczkę fotonów zostaje stłumiony do poziomu energii poniżej pojedynczego fotonu za pomocą regulowanego tłumika. Następnie taki „pojedynczy foton” w sposób losowy obiera drogę w sprzęgaczu światłowodowym. Bity 0 lub 1 generowane są na podstawie odpowiedzi od poszczególnych detektorów sprzęgacza.  
Ciężko jednoznacznie stwierdzić, czy kwantowe generowanie liczb jest lepsze od klasycznego. Niepodważalnie jest bezpieczniejsze, ze względu na prawdziwą losowość i odporność na przewidywanie. Jednak koszt, szeroka dostępność oraz prostota implementacji to zdecydowanie zalety generowania klasycznego.

Aby wskazać różnicę między losowością, a pseudolosowością musimy wyobrazić sobie wykres zmieniający się zależnie od każdej liczby. Nazywamy to błądzeniem losowym.

Obraz zawierający tekst, diagram, linia, Wykres

Opis wygenerowany automatycznie

Poniżej widzimy generowanie ścieżek losowych (kolor biały) i pseudolosowych (kolor niebieski). Obraz zawierający zrzut ekranu, Wielobarwność, sztuka, płatek śniegu

Opis wygenerowany automatycznie  
Możemy zauważyć, że ścieżka losowa jest w pełni chaotyczna, a pseudolosowa w pewnym momencie się powtarza (co spowodowane jest powtórzeniem się ziarna) i zapętla.

W przeciwieństwie do liczb pseudolosowych, losowe nie są tworem algorytmu. Dla maszyny bardzo trudne byłoby wypisać w pełni losową liczbę, dla której szansa na powtórzenie się będzie zawsze taka sama (jak np. w przypadku rzucania przez człowieka kostką). Pseudolosowość jednak mimo swojej nieprzewidywalności, w końcu będą powtarzać ten sam ciąg.

1. Proces, którego wynik nie jest jednoznacznie określony przez jego początkowy stan. Oznacza to, że mając ten sam stan początkowy, proces może zakończyć się różnymi rezultatami. [↑](#footnote-ref-1)
2. Random number generator (RNG) [↑](#footnote-ref-2)
3. Ziarno losowe (random seed) to liczba używana do zainicjowania generatora liczb pseudolosowych. [↑](#footnote-ref-3)
4. Przypadkowe, niedające się przewidzieć, odchylenia od wartości średniej zmiennej losowej. [↑](#footnote-ref-4)