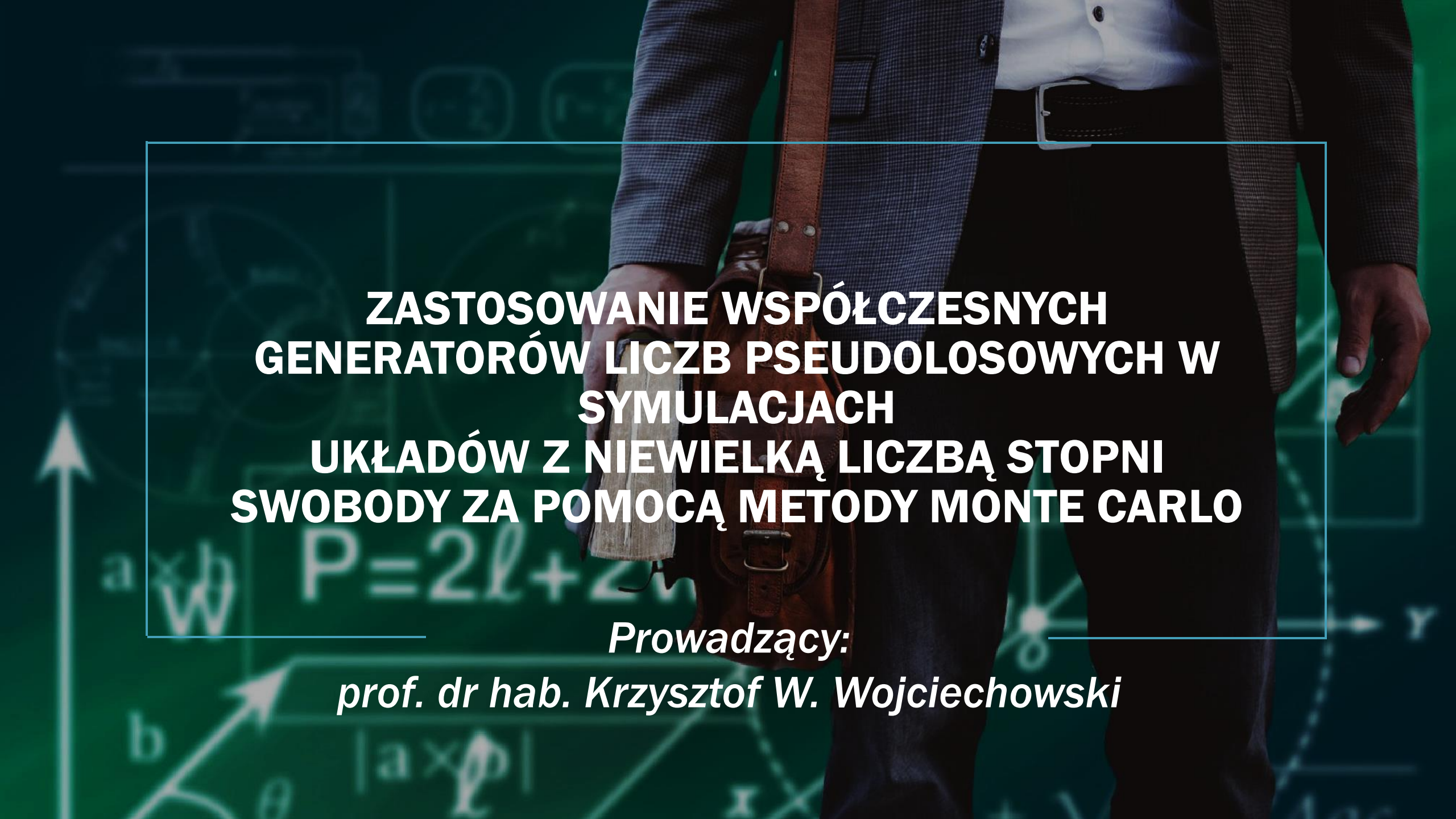
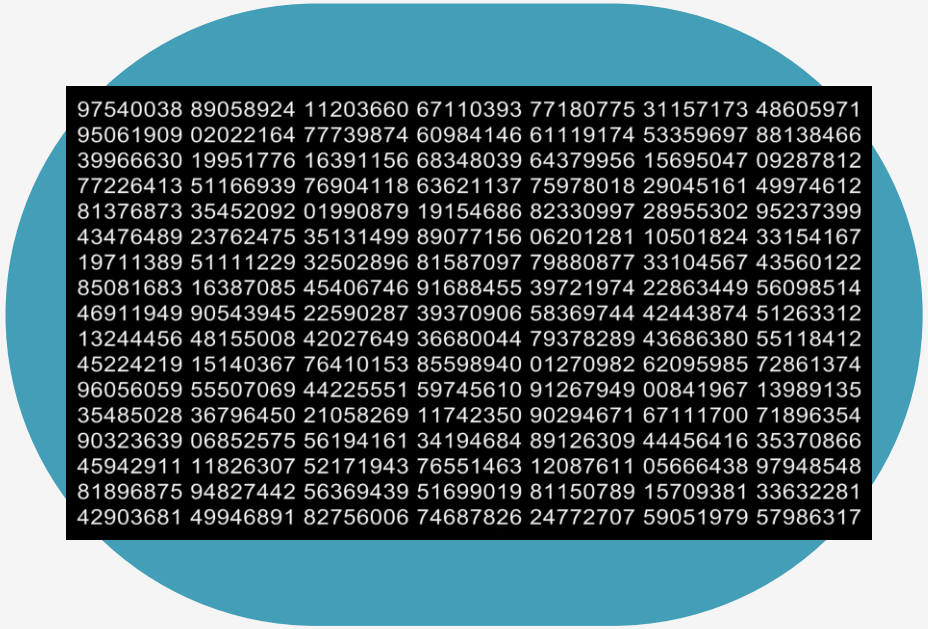


ZASTOSOWANIE WSPÓŁCZESNYCH GENERATORÓW LICZB PSEUDOLOSOWYCH W SYMULACJACH UKŁADÓW Z NIEWIELKĄ LICZBĄ STOPNI SWOBODY ZA POMOCĄ METODY MONTE CARLO

Prowadzący:

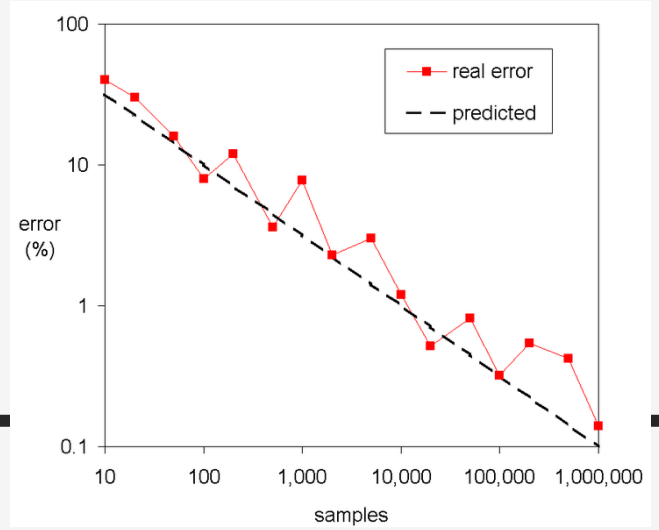
prof. dr hab. Krzysztof W. Wojciechowski

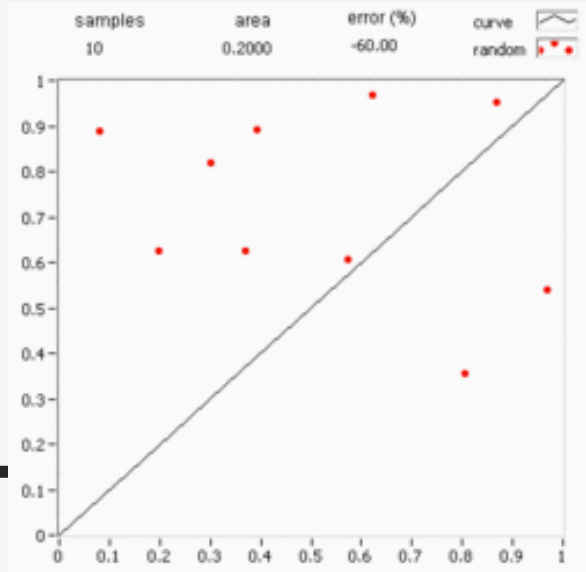
Spis treści

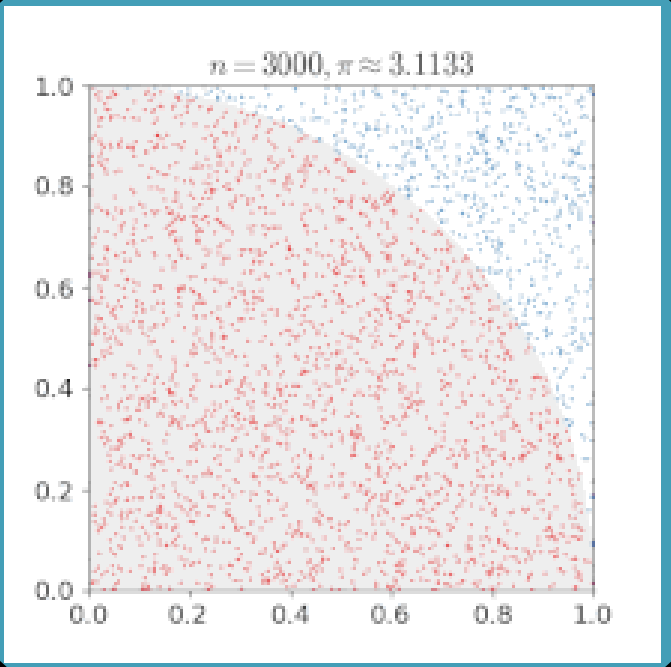


Metody Monte Carlo

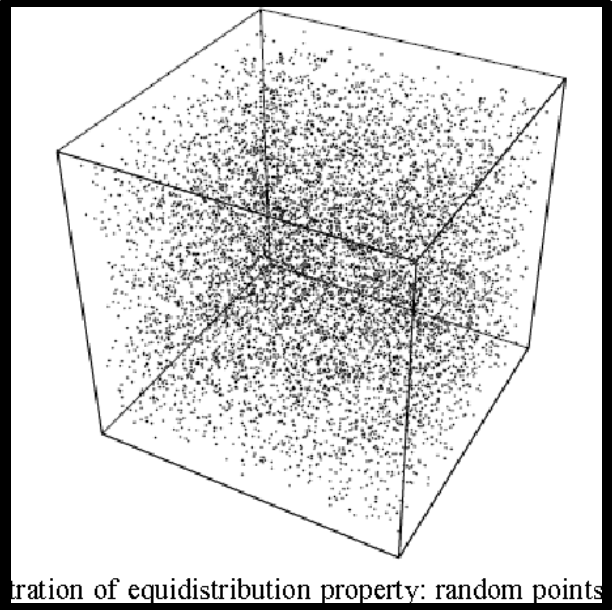
- Metody stosowane do modelowania matematycznego procesów zbyt złożonych aby można było przewidzieć ich wyniki za pomocą podejścia analitycznego.
- Istotną rolę odgrywa w nich losowanie wielkości charakteryzujących proces, przy czym losowanie to musi być dokonywane zgodnie ze znanym rozkładem.
- Głównie używane w trzech klasach problemów: optymalizacji, całkowaniu numerycznym oraz generowaniu obrazów z rozkładu prawdopodobieństwa.
- W fizyce używana głównie do symulowania układów z małą liczbą punktów swobody takich jak: ciecze, nieuporządkowane materiały, silnie sprzężone ciała stałe czy struktury komórkowe
- Dokładność tych metod zależna jest od liczby sprawdzeń oraz jakości użytego generatora liczb pseudolosowych.







Generatory liczb pseudolosowych



- Program, który na podstawie niewielkiej ilości informacji (ziarno) generuje deterministycznie ciąg bitów, który pod pewnymi względami jest nieodróżnialny od ciągu uzyskanego z prawdziwie losowego źródła
- Generatory nie generują ciągów prawdziwie losowych – generator inicjowany ziarnem, które może przyjąć *k* różnych wartości, jest w stanie wyprodukować co najwyżej *k* różnych ciągów liczb.
- *W algorytmach probabilistycznych (całkowanie Monte Carlo) potrzebne jest jedynie źródło wartości o cechach przybliżonych do liczb prawdziwie losowych, chociaż jakość losowości może być decydująca dla dokładności obliczeń.*
- *Dlatego przy zastosowaniu każdego nowego generatora do obliczeń numerycznych należy sprawdzić jego właściwości statystyczne (np. długość cyklu, równomierność rozkładu). Można też skorzystać z jednego ze standardowych testów jak test pokerowy czy test serii.*
- *Przykładowe generatory liczb losowych:*
  - *Mersenne Twister*
  - *SNWS*
  - *RDRAND*
  - *RAN2*
  - *Hoover*
  - *LCG*
  - *Xorshift*

Mersenne Twister

Szybki, wysokiej jakości liczby pseudolosowe, rok 1997.

Nazwa od liczby pierwszej Mersenne'a

Zaprojektowany z myślą o metodach Monte Carlo i innych symulacjach statystycznych

Nie nadaje się do kryptografii, obserwacja 624 iteracji (dla MT19937) pozwala przewidzieć kolejne.

32 bitowa długość słowa

Domyślny generator wielu języków programowania czy programów oraz bibliotek

Okres $2^{19937} - 1$

Wysoki stopień równomiernego rozmieszczenia

Spełnia liczne testy statystycznej losowości (np. diehard), spełnia większość testów bardziej rygorystycznych jak TestU01 Crush

SNWS generator

(Shuffled Nested Weyl Sequence)

Polega na Teorii Weyla (Weyl Sequence) i jej wersji zagnieżdżonej oraz przetasowanej

Stworzony przez Holiana i współpracowników z myślą o symulacjach dynamiki molekularnej na dużą skalę w 1994 roku

Przechodzi testy min. jednorodności, korelacji, wyżarzania oraz „Monkey Test”

Bardzo łatwy w implementacji, bardzo szybki, potrzebuje mało pamięci

Zmodyfikowana wersja dla symulacji Monte Carlo

RDRAND

Instrukcja zwracania losowej liczby z sprzętowego RNG znajdującego się na procesorze Intela wykorzystującego ziarno z źródła entropii procesora

AMD dało wsparcie instrukcji w 2015r

Bezpieczny dla kryptografii

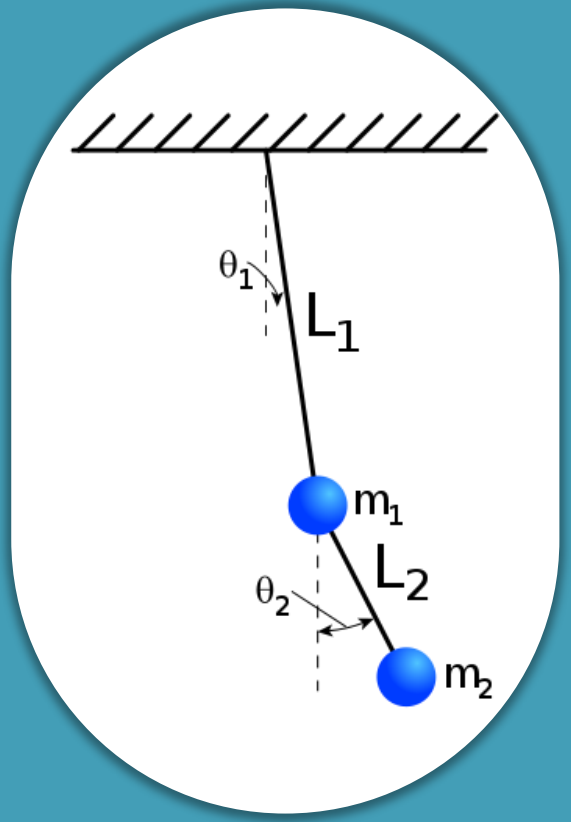
Wykorzystywany w min certyfikatach OpenSSL

Wykorzystywany przy metodach Monte Carlo min. przy modelowaniu fizycznych właściwości brązowych karłów.

Zdecydowanie wolniejszy dla metod Monte Carlo w porównaniu do Mersenne Twister (20x) czy standardowego generatora języka C czy Pythona.

Nie powinno jednak porównywać się pod tym kątem generatorów, które są kryptograficznie bezpieczne do normalnych

Układy z małą liczbą stopni swobody



Stopień swobody to zmienna pozwalająca opisać stan układu fizycznego.

Liczba stopni swobody to najmniejsza liczba niezależnych zmiennych potrzebnych do jednoznacznego opisania stanu układu.

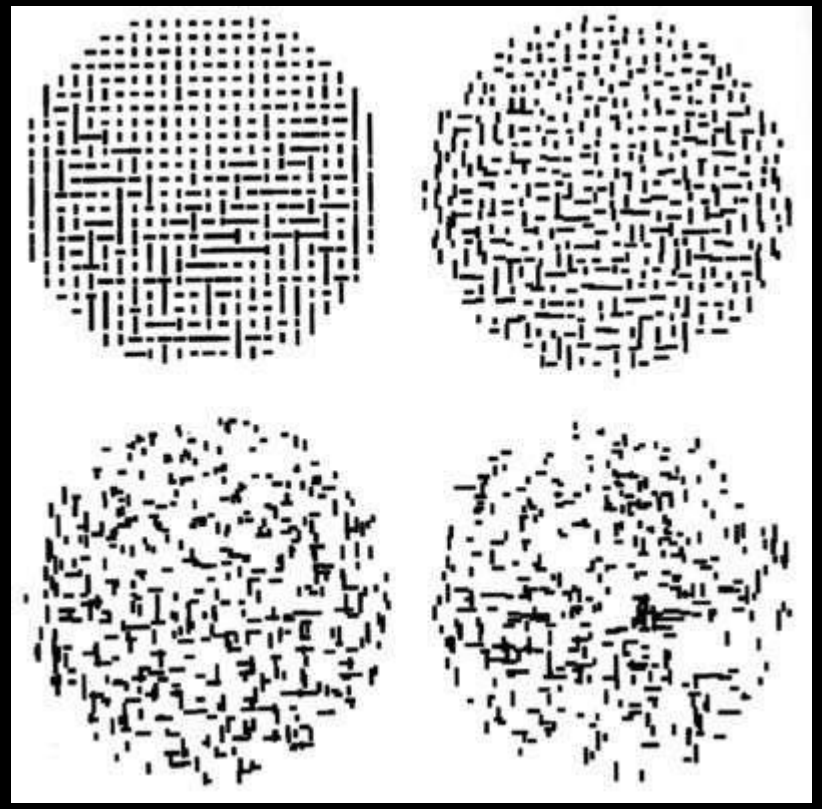
np. ciało punktowe w przestrzeni ma trzy stopnie swobody, ciało ślizgające – dwa, wahadło drgające w płaszczyźnie – jeden, a ciało sztywne – sześć (3 współrzędne środka masy, 3 rotacyjne)

Testy generatorów

Generatory można badać na wiele różnych sposobów, żaden generator nie będzie idealny do każdego eksperymentu czy danych, dlatego bardzo ważne jest wybranie odpowiedniego do naszych potrzeb. Pomocne przy tym są testy generatorów, min.

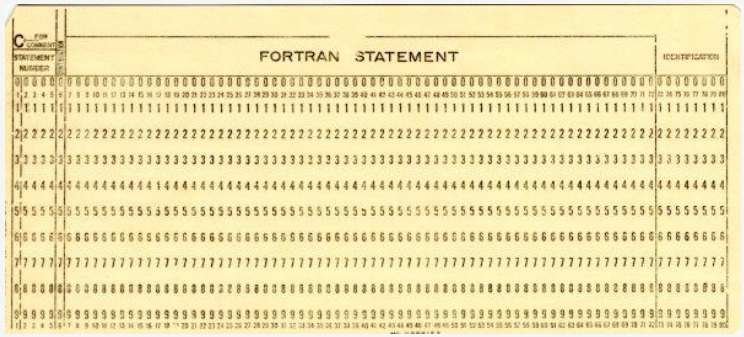
- TestU01
- Diehard tests

Przy badaniu generatorów należy pamiętać o tym jakich wyników oczekujemy i na czym nam bardziej zależy, np. bezpieczeństwo czy szybkość?



Fortran

- Jeden z pierwszych języków programowania,
- Powstał w 1957r w IBM dla zastosowań naukowych i inżynierskich,



- Cały czas powszechnie stosowany ze względu na prostą składnię oraz wysoką wydajność,
- Testowane są nim obecnie najszybsze i najpotężniejsze superkomputery.

- Obecne wersje umożliwiają programowanie strukturalne, obiektowe, modularne oraz równoległe.
- Dodatkowo w nowszych kompilatorach są obecne możliwości graficzne, które pozwalają na wizualizację wyników obliczeń (wykresy, tablice wielowymiarowe)

Bibliografia

Kroese, D. P.; Brereton, T.; Taimre, T.; Botev, Z. I. (2014). "Why the Monte Carlo method is so important today". WIREs Comput Stat. 6 (6): 386–392. doi:10.1002/wics.1314. S2CID 18521840.

Efficient Monte Carlo simulations using a shuffled nested Weyl sequence random number generator
By: Tretiakov, KV; Wojciechowski, KW
PHYSICAL REVIEW E Volume: 60 Issue: 6 Pages: 7626-7628 Part: B Published: DEC 1999

Barker, Elaine; Barker, William; Burr, William; Polk, William; Smid, Miles (July 2012). "Recommendation for Key Management" (PDF). NIST Special Publication 800-57. NIST. Retrieved 19 August 2013.

"Pseudorandom number generators". Khan Academy. Retrieved 2016-01-11.

M. Matsumoto & T. Nishimura, „Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator”, ACM Trans. Model. Comput. Simul. 8, 3 (1998).

Weyl, H. (September 1916). "Über die Gleichverteilung von Zahlen mod. Eins" [On the uniform distribution of numbers modulo one]. Mathematische Annalen (in German). 77 (3): 313–352. doi:10.1007/BF01475864. S2CID 123470919.

W. Królikowski, W. Rubinowicz: Mechanika teoretyczna. Warszawa: PWN, 2012

The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness". Florida State University. 1995. Archived from the original on 2016-01-25.

Wojciech Sobieski, GNU Fortran z elementami wizualizacji danych, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie, Olsztyn 2008

Pierre L’Ecuyer & Richard Simard (2007), "TestU01: A Software Library in ANSI C for Empirical Testing of Random Number Generators", ACM Transactions on Mathematical Software, 33: 22.

DZIĘKUJĘ ZA UWAGĘ

Kacper Kalinowski