Home Work 3

Błądzenie losowe i testy NIST

Maksymilian Neumann

Testy NIST

Test dla kolejno dla lcg, pcg64 oraz SHA1(Neumann):

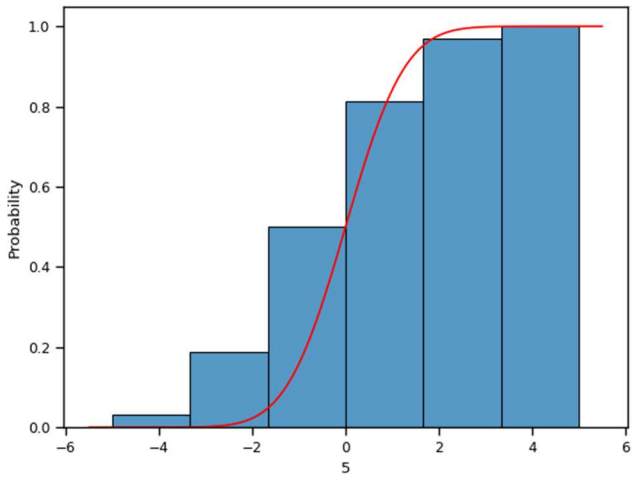
1. Frequency (Monobit) Test	0.821201420327966 1	Passed
2. Frequency Test within a Block	0.38232523884681685	Passed
3. Runs Test	1.7712336155758526	Failed
4. Test for the Longest Run of Ones in a Block	0.48152178448416894	Passed
5. Binary Matrix Rank Test	0.40399103016220805	Passed
6. Non-overlapping Template Matching Test	0.4264255379584908	Passed
7. Overlapping Template Matching Test	0.2531156403851712	Passed
8. Maurer's "Universal Statistical" Test	0.4038269121400919	Passed
9. Linear Complexity Test	0.21796974086852366	Passed
10. Serial Test	P-value 1: 0.48132623285233855 P-value 2: 0.234833447710184	Passed
11. Approximate Entropy Test	0.09287263700511576	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.5272163770886866 P-value Reverse: 1	Passed
13. Random Excursions Test	0.021566348721240504	Passed
14. Random Excursions Variant Test	0.0633941673048164	Passed

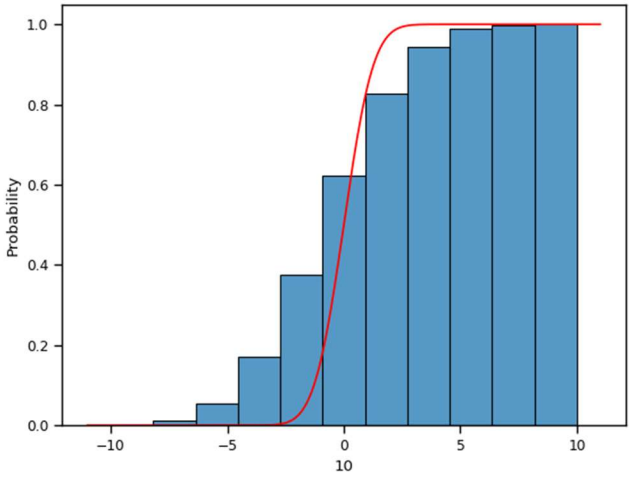
1. Frequency (Monobit) Test	0.11828798885902247	Passed
2. Frequency Test within a Block	0.4809278703318018	Passed
3. Runs Test	0.9741212251612348	Passed
4. Test for the Longest Run of Ones in a Block	0.421874210359249	Passed
5. Binary Matrix Rank Test	0.7351688115943131	Passed
6. Non-overlapping Template Matching Test	0.25267775574109	Passed
7. Overlapping Template Matching Test	0.19628566559055352	Passed
8. Maurer's "Universal Statistical" Test	0.1845070863919529	Passed
9. Linear Complexity Test	0.12689499015061098	Passed
10. Serial Test	P-value 1: 0.2951374792112702 P-value 2: 0.9776621534517412	Passed
11. Approximate Entropy Test	0.37527701069041697	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.11832062120208509 P-value Reverse: 1	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

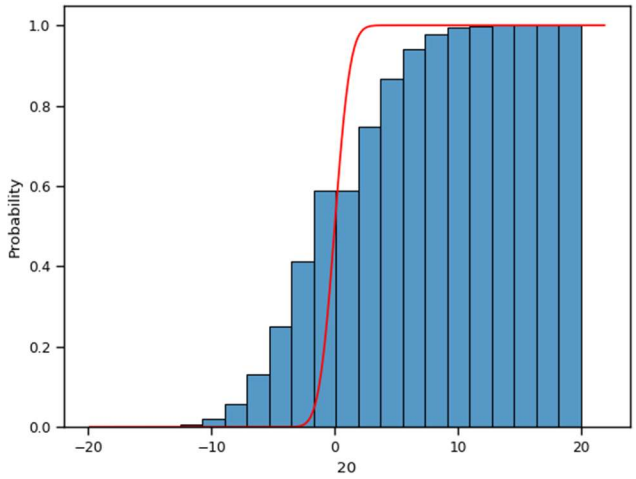
1. Frequency (Monobit) Test	0.0036504344044422377	Failed
2. Frequency Test within a Block	0.0425851362887876	Passed
3. Runs Test	1.2500234824164698	Failed
4. Test for the Longest Run of Ones in a Block	8.092123239563899e-11	Failed
5. Binary Matrix Rank Test		Error
6. Non-overlapping Template Matching Test		Error
7. Overlapping Template Matching Test		Error
8. Maurer's "Universal Statistical" Test		Error
9. Linear Complexity Test		Error
10. Serial Test		Error
11. Approximate Entropy Test	4.1015095449815045e-18	Failed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.007300868808884253 P-value Reverse: 0.5030486441117152	Failed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

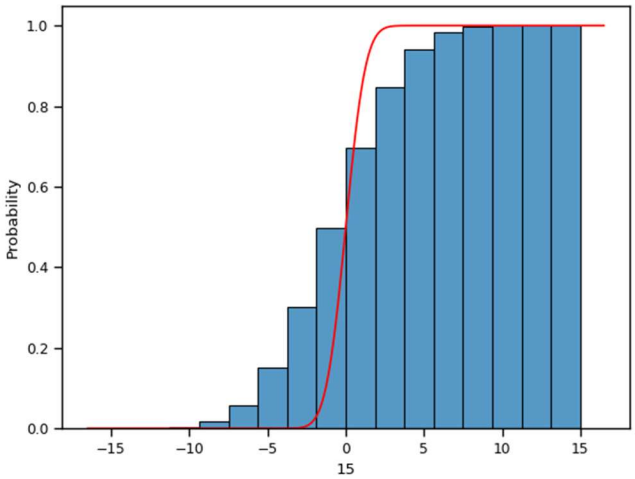
Możemy zobaczyć, że lcg poległo na 3 teście natomiast pcg64 przeszło go, ale wystąpił błąd na dwóch ostatnich, widzimy również, że SHA1(Neumann) przeszło tylko 1 test a na reszcie albo wystąpił błąd albo ich nie przeszedł za pewne większość tego spowodowana jest zbyt małą ilością bitów do testów. Z ukazanych wybrał bym pcg64 jako

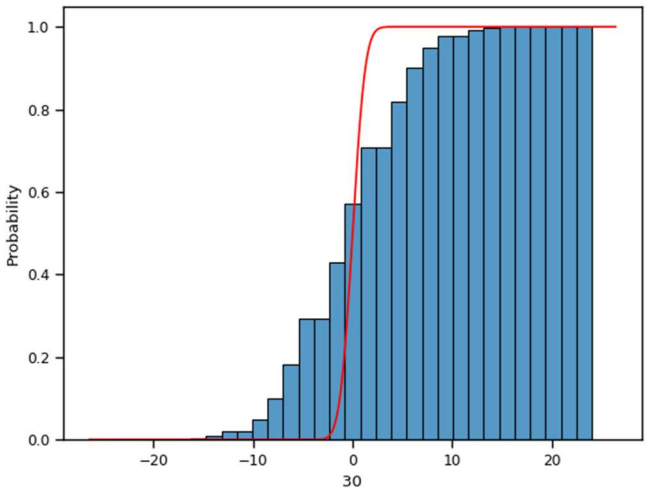
Błądzenie losowe

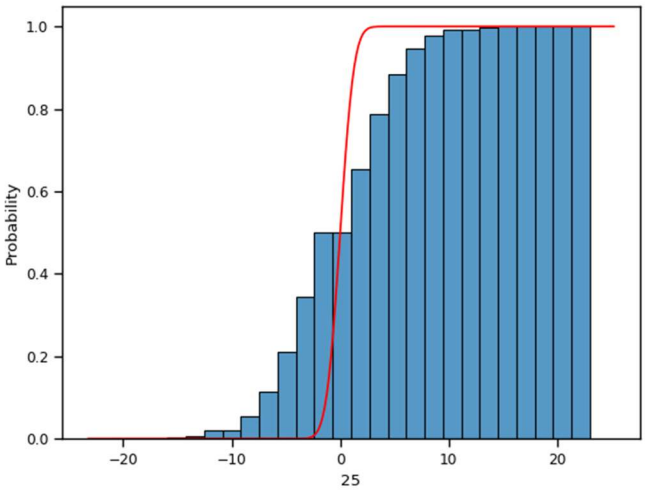




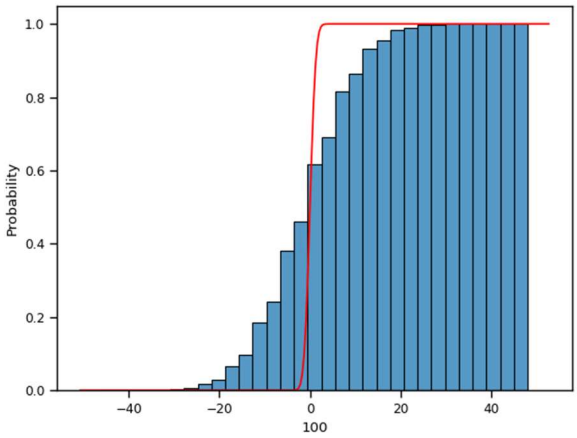








Możemy zobaczyć, że aproksymacja rozkładem normalnym jest gorsza im zwiększa się N.



Błądzenie losowe (czas nad osią x)

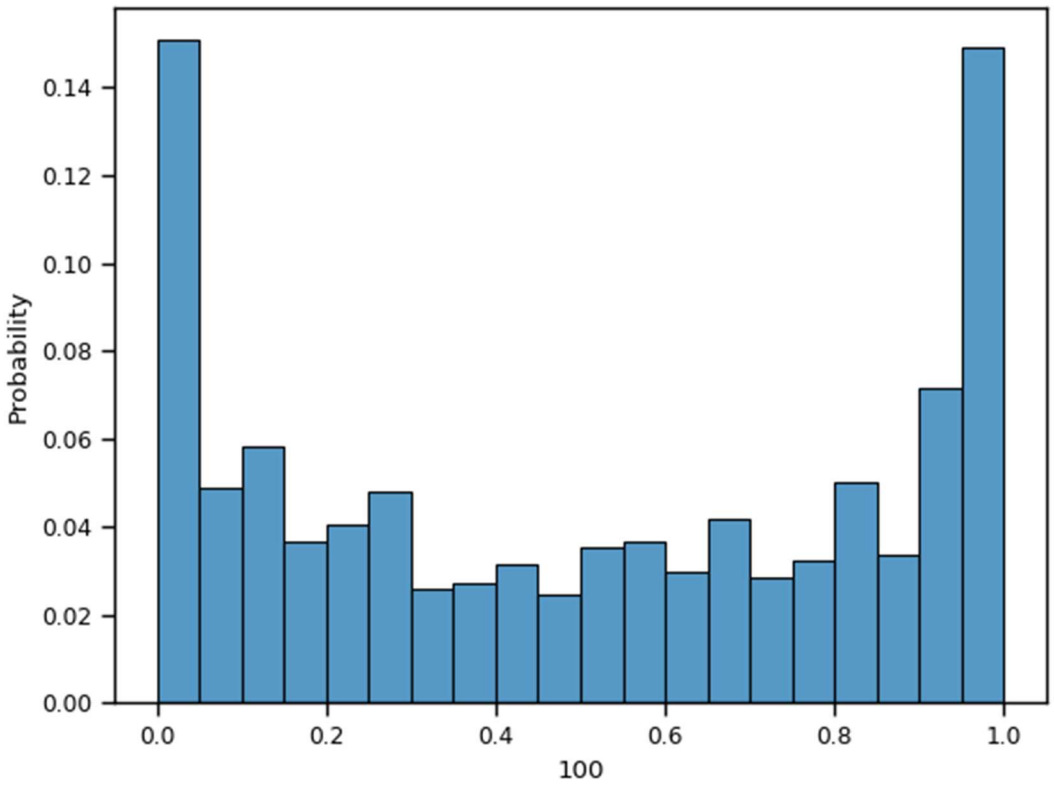


Chart 1 Rozkład Czasu Spędzonego nad Ox /Czas Całkowity dla N=100

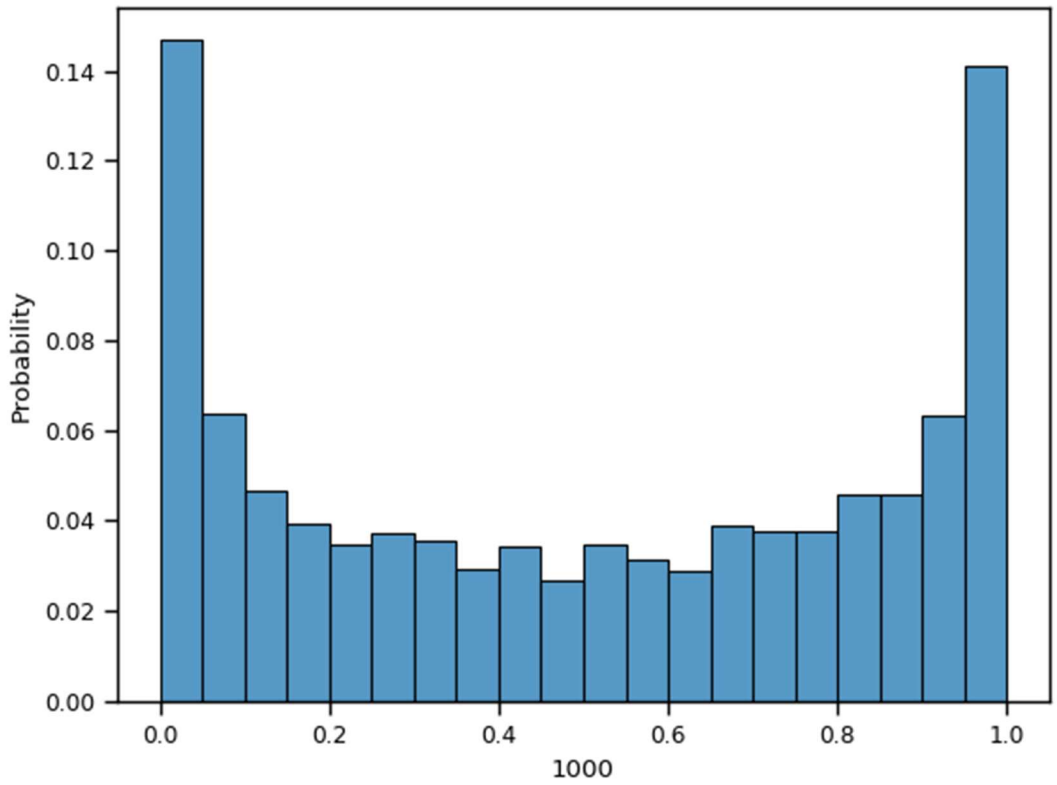


Chart 2 Rozkład Czasu Spędzonego nad Ox /Czas Całkowity dla N=1000

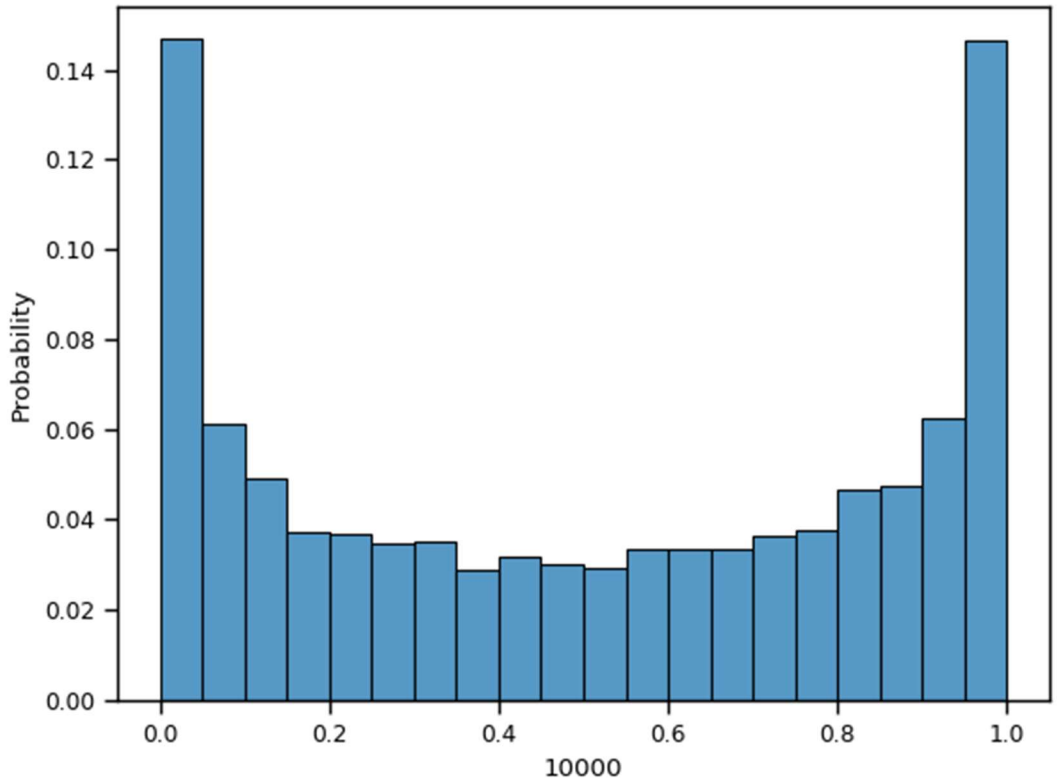
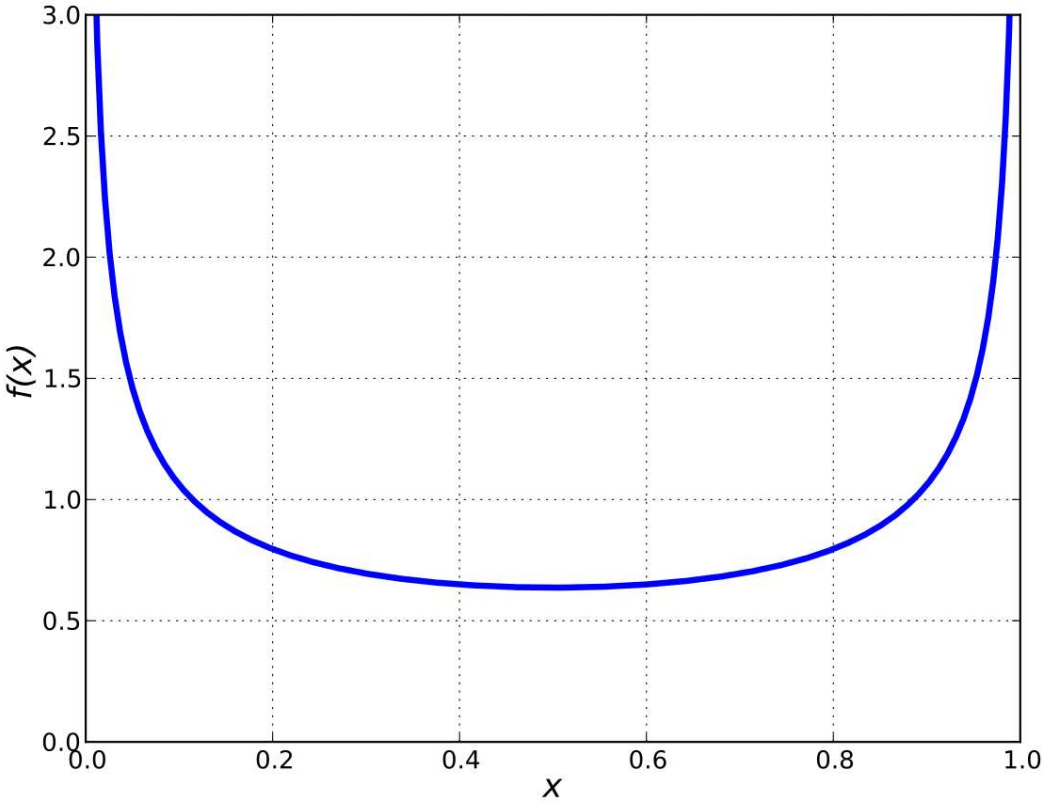


Chart 3 Rozkład Czasu Spędzonego nad Ox /Czas Całkowity dla N=10000



Po porównaniu rozkładów czasu naszych błądzeń losowych nad osią x podzielonych przez całkowity ich czas z rozkładem arcsin możemy wysunąć hipotezę, iż rozkład naszego eksperymentu ma właśnie rozkład arcsin.