Raport
Laboratorium Bezpieczeństwa Systemów Teleinformatycznych (c. 1)

Wykonali:	**Data Oddania:**
Marcin Cichowski, Jacek Kwieciński	31.05.2021r.
Link do repozytorium:	

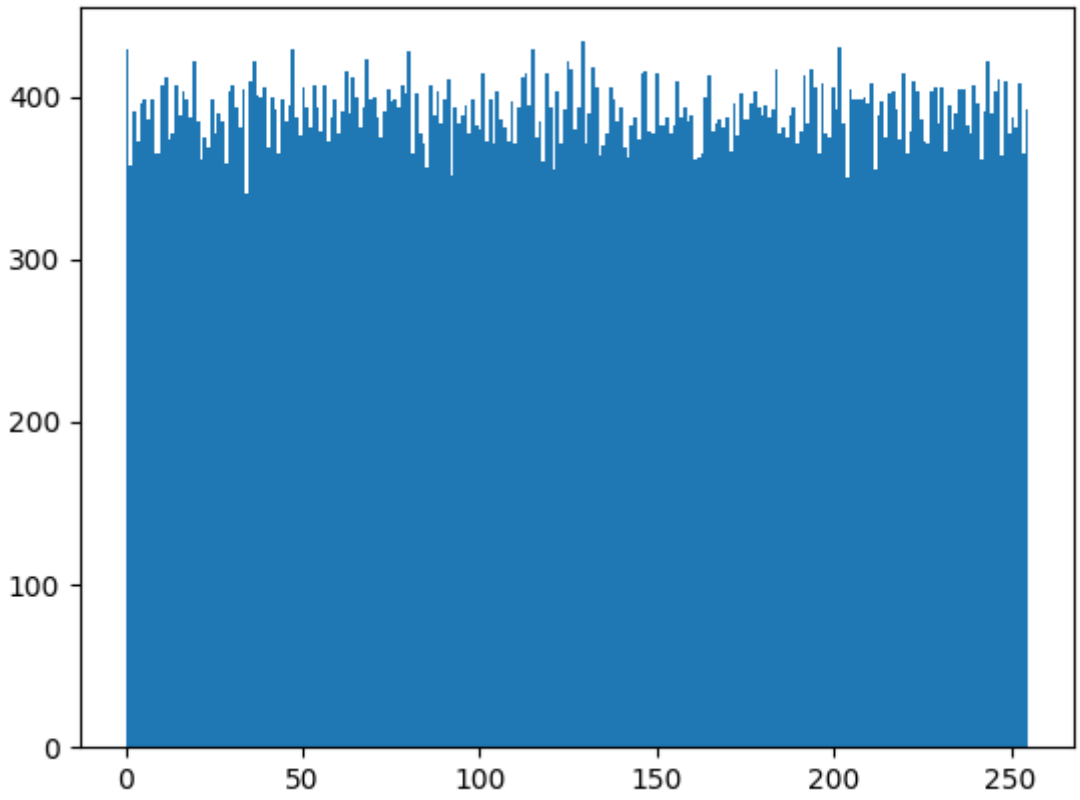
Podstawa opracowania:

Wang Xing-yuan, “Random Numbers Generated from Audio and Video Sources”, Mathematical Problems in Engineering Volume 2013, Article ID 285373, 7 pages

---

Zakres danych testowych:

Na potrzeby realizowania pakietu testów wygenerowano 4 000 000 liczb 8-bitowych o empirycznym rozkładzie bliskiemu równomiernemu przedstawionemu poniżej:



Entropia wylosowanych liczb wynosi: 7.99862 bita

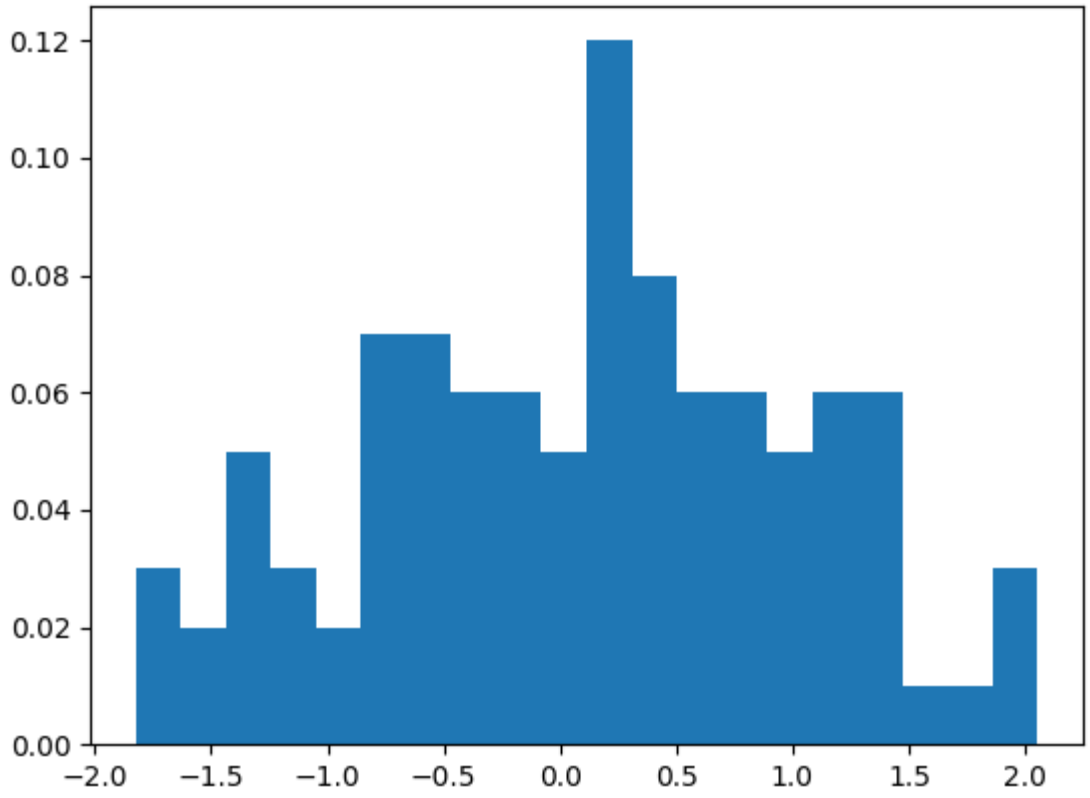
Entropia wyliczona zgodnie ze wzorem: $e = -\sum i\ pi\ log2\ (pi\ )$

Test nr 1 – Parking lot Test:

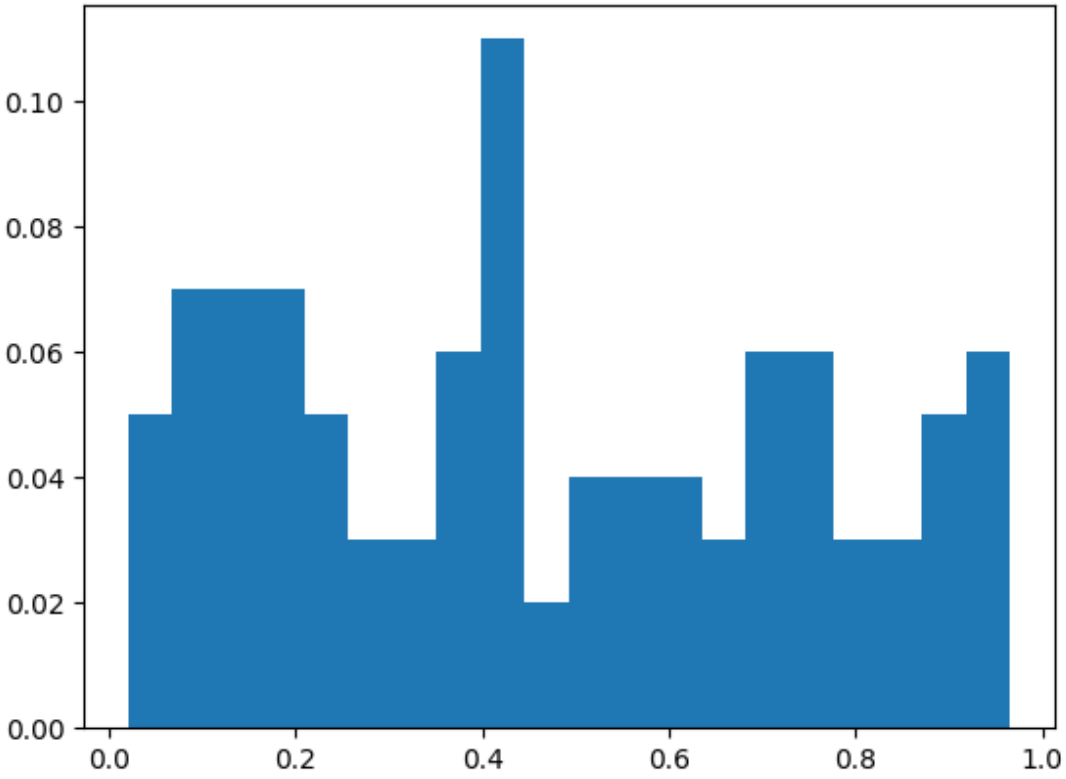
Na potrzeby przeprowadzenia testu ciąg danych został podzielony na 24000 32-bitowych liczb. Każda liczba została rzutowana na zmiennoprzecinkową liczbę z zakresu <1-100> wskazując na współrzędne dyskretnej przestrzeni 100x100

Wykonano 10 testów w każdym teście wykonano 12000 prób parkowania zliczając próby zakończone sukcesem *k*. Wynik testów został znormalizowany zgodnie ze wzorem: *(k - 3523)/21.9.*

Poniższy wykres przedstawia empiryczny rozkład sukcesów:



Dla wygenerowanych 100 rozkładów empirycznych wykonano test Kołmogorowa-Smirnowa w odniesienu do rozkładu normalnego, z każdego porównania uzyskując wartość *p.* Dla 100 wartości *p* uzyskano rozkład empiryczny przedstawiony poniżej:



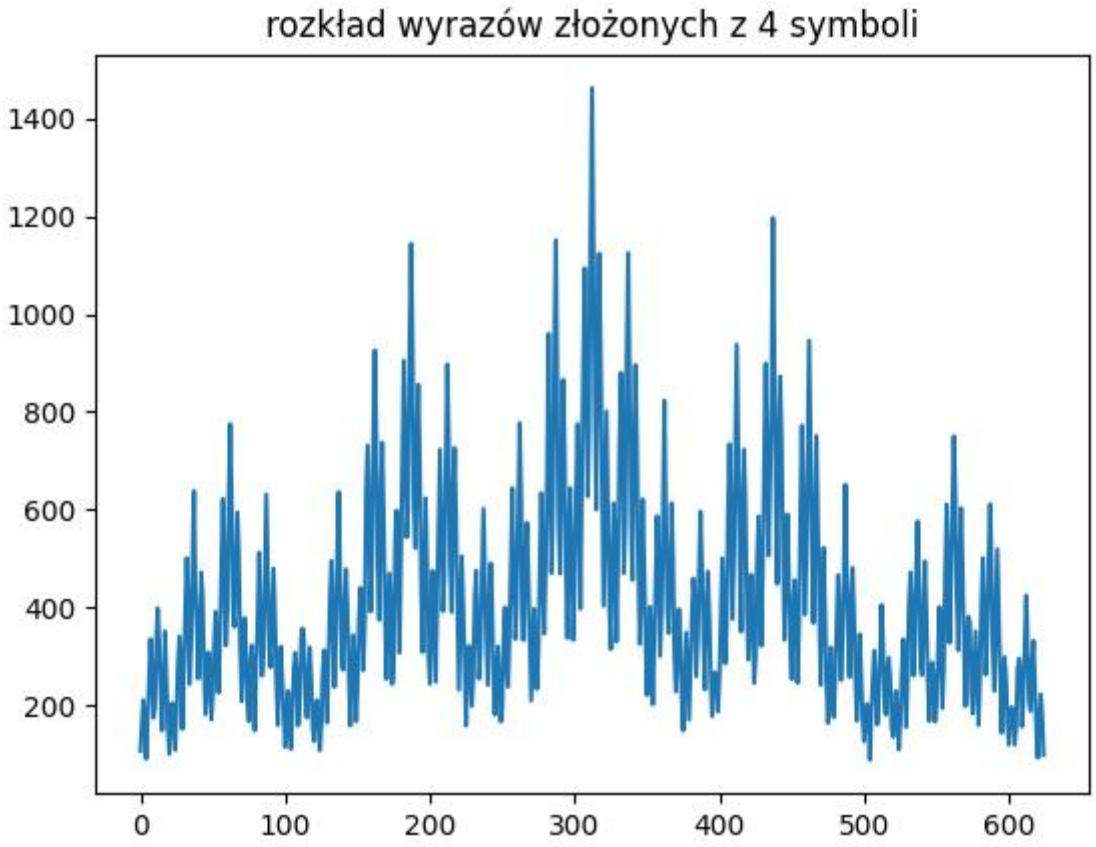
Rzutowanie rozkładu wartości *p* (oczekiwanego rozkładu równomiernego) na rozkład normalny i weryfikacja zgodności dopasowania za pomocą testu Kołmogorowa-Smirnowa wykazała, że *p= 0.31394323972408533* , więc wartość prawdopodobną mieszczącą się w zakresie *p < 0.025 lub p>0.975.*

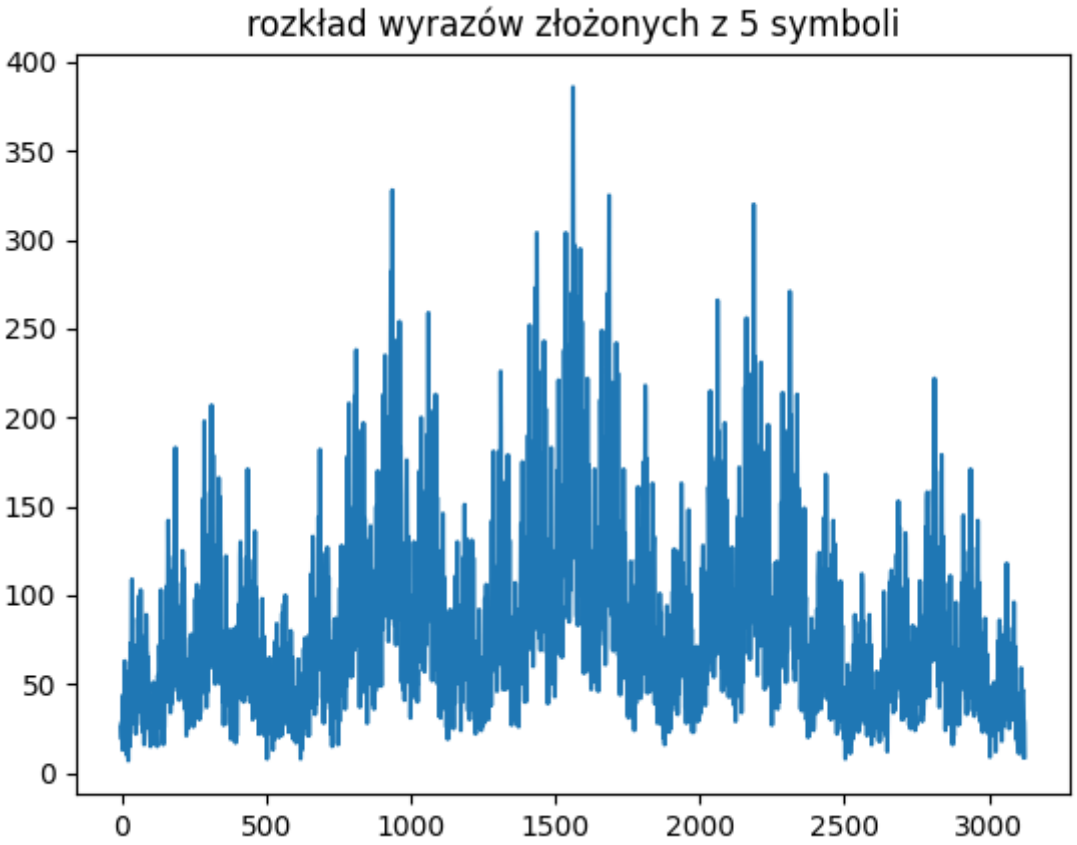
Uzyskany w wyniku przeprowadzonych testów rozkład wartości p jest wystarczająco bliski oczekiwanemu rozkładowi normalnemu. Zauważamy jeden wyróżniającą się wartość.

Test nr 2 – Count the ones:

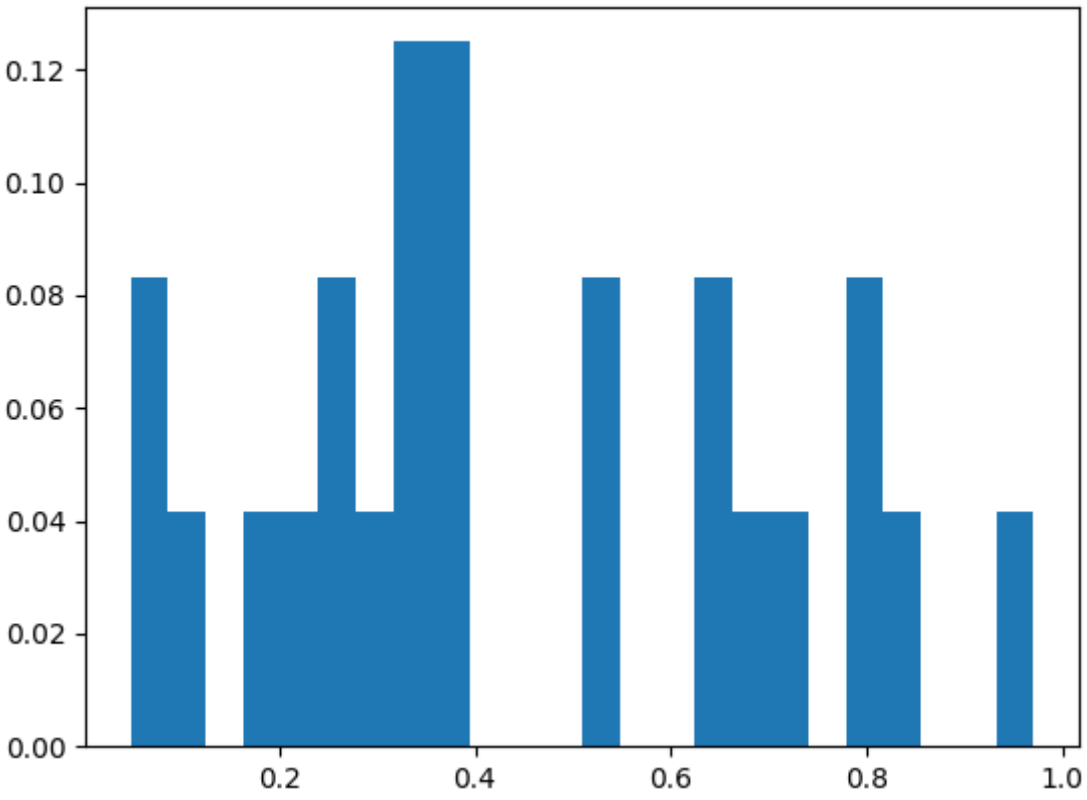
Na potrzeby przeprowadzenia testu ciąg danych został podzielony na 256000 8-bitowych liczb. Każda liczba zostaję zmieniona na literę odpowiadającą liczbie jedynek w reprezentacji bitowej liczby. A={0-2}, B={3}, C={4}, D={5}, E={6-8}

Wykonano 24 testy , w każdym pobrano 256000 8-bitowych liczb, z których po skonwertowaniu na litery utworzono nakładające się wyrazy 4 oraz 5 literowe. Następnie policzono ilość występowań każdej kombinacji dla odpowiedniej długości literałów. Poniżej przedstawiono rozkład częstotliwości występowania literałów 4 oraz 5 literowych:

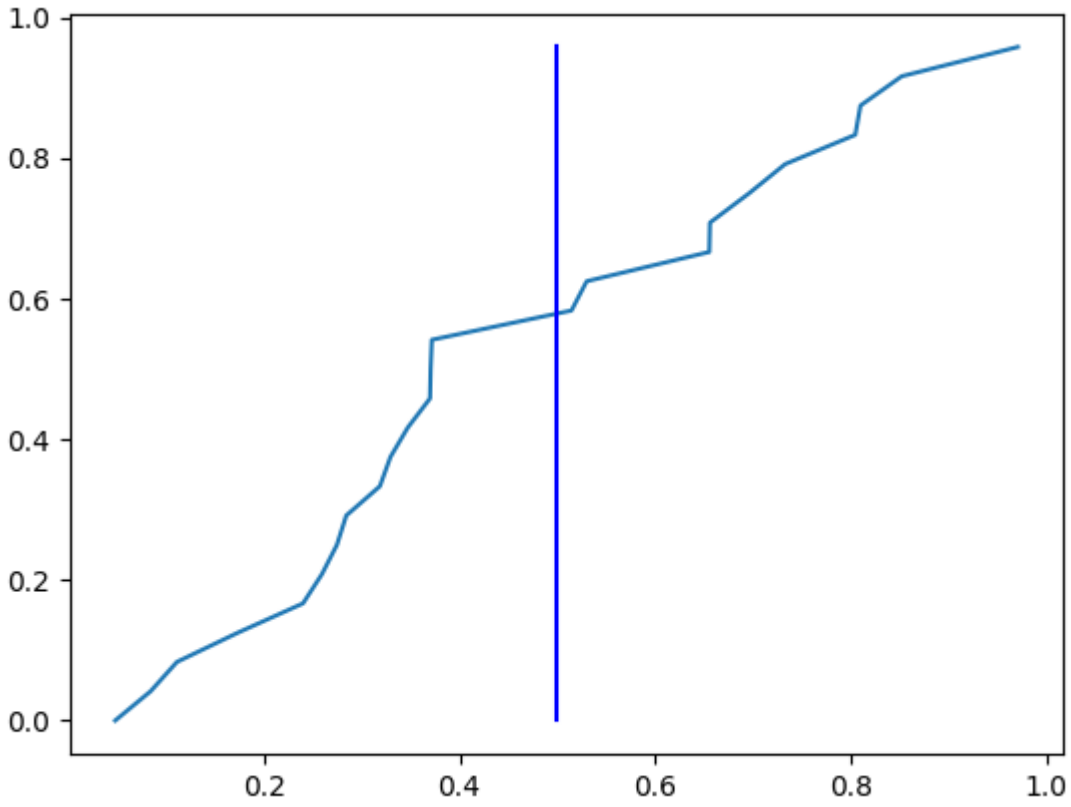




Wynik testu został znormalizowany zgodnie ze wzorem $\frac{(Q5 - Q4 - 2500)}{(\sqrt{5000})}$. Poniższy rozkład empiryczny przedstawia wyniki testów.

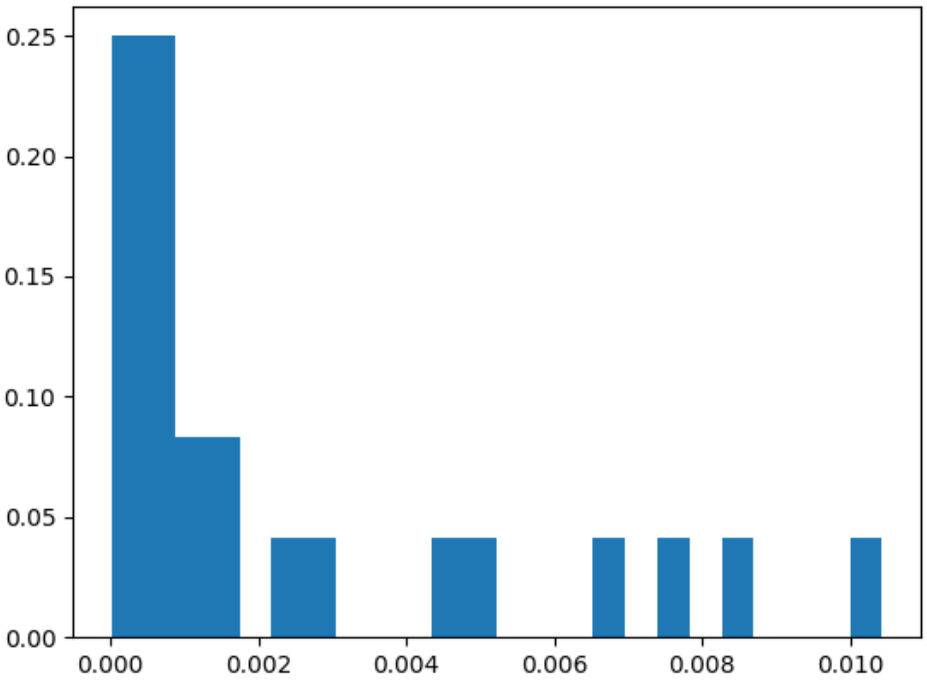


Wykonano test zgodności Kołmogorowa-Smirnowa dla poszczególnych testów z wynikiem *p = 0.20161556869818043* więc wartość prawdopodobną mieszczącą się w zakresie *p < 0.025 lub p>0.975.* Poniżej przedstawiono wykres CDF:



Test nr 3 – Binary Rank test:

Na potrzeby przeprowadzenia testu ciąg danych został podzielony na 40000 macierzy 32x32 złożonych z 32-bitowych liczb. Każdy wiersz odpowiada jednej liczbie binarnej. Każda komórka odpowiada jednemu bitowi 32-bitowej liczby. Następnie wyliczono rząd każdej macierzy przy pomocy metody eliminacji Gaussa. W zależności od rzędu zliczamy ilość występowań dla macierzy rzędu 32, 31, 30 oraz dla rzędów mniejszych od 30. Test sprawdza liniową niezależność liczb losowych od siebie na podstawie testu chi-square. Wykonano test zgodności Kołmogorowa-Smirnowa dla poszczególnych testów z wynikiem *p = 5.492592954455168e-48* więc wartość prawdopodobną nie mieszczącą się w zakresie *p < 0.025 lub p>0.975.* Wykonano 24 testy z których wyznaczono empiryczny rozkład przedstawiony poniżej:



Uwagi:

Testy wykonano na własnym generatorze liczb losowych oraz na generatorze wbudowanym w bibliotece random. Wartości generowane dla testu Binary Rank test mogą nie być wiarygodne z powodu zbyt małej ilości danych wejściowych do generowania mimo zastosowania buforowania. Powodem takiego podejścia jest długość generowania pliku z liczbami losowymi, który potrafi generować 100000 liczb 8-bitowych w około 30 minut.