Fundusze Europejskie Inteligentny Rozwój

Projekt realizowany w ramach Programu Operacyjnego Inteligentny Rozwój, poddziałanie 1.1.1 "Badania przemysłowe i prace rozwojowe realizowane przez przedsiębiorstwa", współfinansowany ze środków Budżetu Państwa oraz Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego

JURAND - Narodowy Kwantowy Generator Liczb Losowych (POIR.01.01.01-00-0173/15-00)

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Wizualizacja wyników statystycznych kwalifikujących model weryfikacji losowości kwantowej w jego części obliczeniowej wraz z wnioskami

W. A. Jacak, J. E. Jacak, W. A. Donderowicz, L. Jacak

Wyniki w zakresie kwalifikacji modelu obliczeniowego parametryzowanego dla weryfikacji losowości kwantowej na podstawie przykładowych próbek losowych ciągów binarnych wygenerowanych laboratoryjnie w ramach procesów kwantowych

Przykładowe 5 części ciągów losowych generowanych kwantowo, każdy o długości 800 mln bitów (sumarycznie 4000 mln bitów) [zapisane w formacie binarnym].

- cs_100mb_1.dat – część pierwsza; generacja ciągła, proces generacji: fluktuacje prądowe oparte o szumy białe na klastrze tranzystorów półprzewodnikowych (efekt empirycznie weryfikowany jako kwantowy w związku z tunelowaniem elektronów w złączu diody półprzewodnikowej
- cs_100mb_2.dat – część druga; generacja ciągła, proces generacji: układ optyki kwantowej bezsplątaniowy (atenuowane źródło wielofotonowe niskiej intensywności; rozdzielacz wiązki; detektory fotonowe niskiej czułości dla rejestracji silnie tłumionych impulsów z rozkładem statystycznym wartości średniej pojedynczych fotonów w impulsie - w reżimie polaryzacyjnym, a także w efektach kwantowych własności fazowych światła, tj. w reżimie przesunięć fazowych w zakresie rejestrowanych fotonów przy zastosowaniu układów interferometrów Macha-Zehndera)
- cs_100mb_3.dat – częśc trzecia; generacja ciągła, proces generacji: układ optyczny splątaniowy (źródło splątania – dwójłomny kryształ BBO rozdzielający wiązkę w efekcie procesu SPDC, w punktach przecięcia stożków rozdzielenia wiązki występuje pary fotonów splątanych polaryzacyjnie; rozdzielacze wiązek 50/50; detektory wysokiej czułości, jednofotonowe diody lawinowe, chłodzone piezoelektrycznie - odrębne wykazanie złamania nierówności Bella [tj. wykazanie czysto kwantowej natury korelacji wyników pomiarów łamiącej limity statystyki klasycznej w rozdziale 6])
- cs_100mb_4.dat – część czwarta; próbka mozaikowa w skali czasowej z periodem godzinnym (akwizycja 10 części); proces jak próbka _1
- cs_100mb_5.dat – część piąta; próbka mozaikowa w skali czasowej oraz mozaika źródłowa źródeł _1 _2 i _3
- cs_100mb_1-5.dat – konkatenacja części _1 do _5 w jeden ciąg 4000 mln bitów

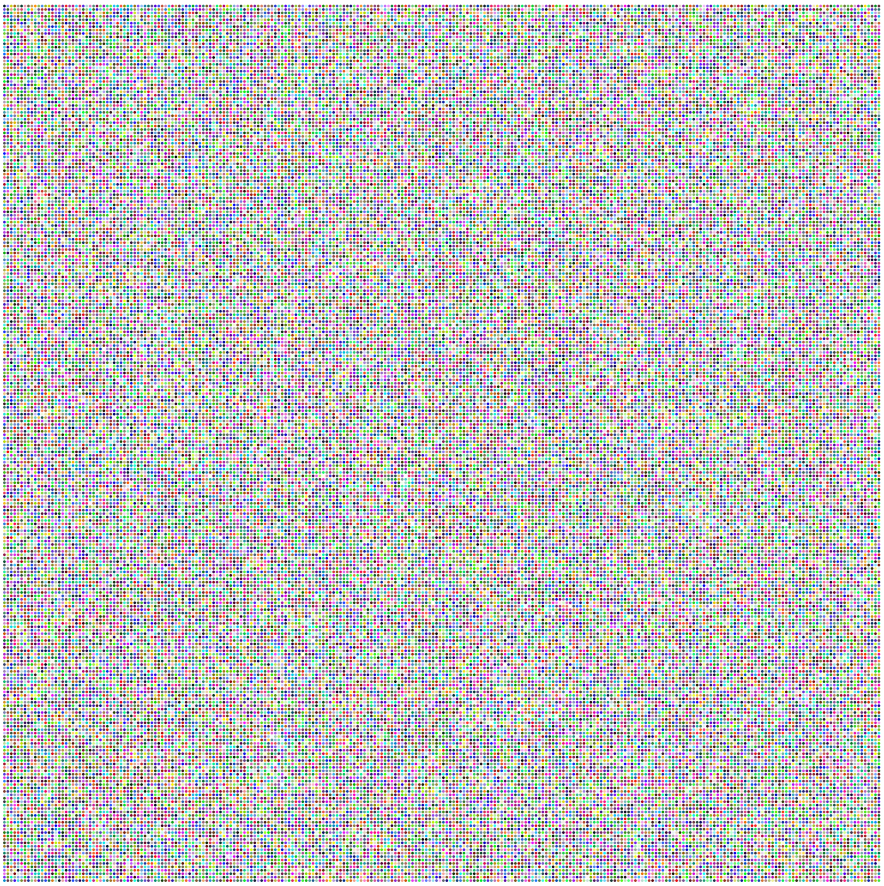
Graficzna reprezentacja losowości jednorodnie wybranej próbki o rozmiarze 196 608 bajtów z każdej z 5 części ciągów generowanych kwantowo (obraz o rozmiarze 256 na 256 punktów w kolorze RGB (0-255,0-255,0-255)).

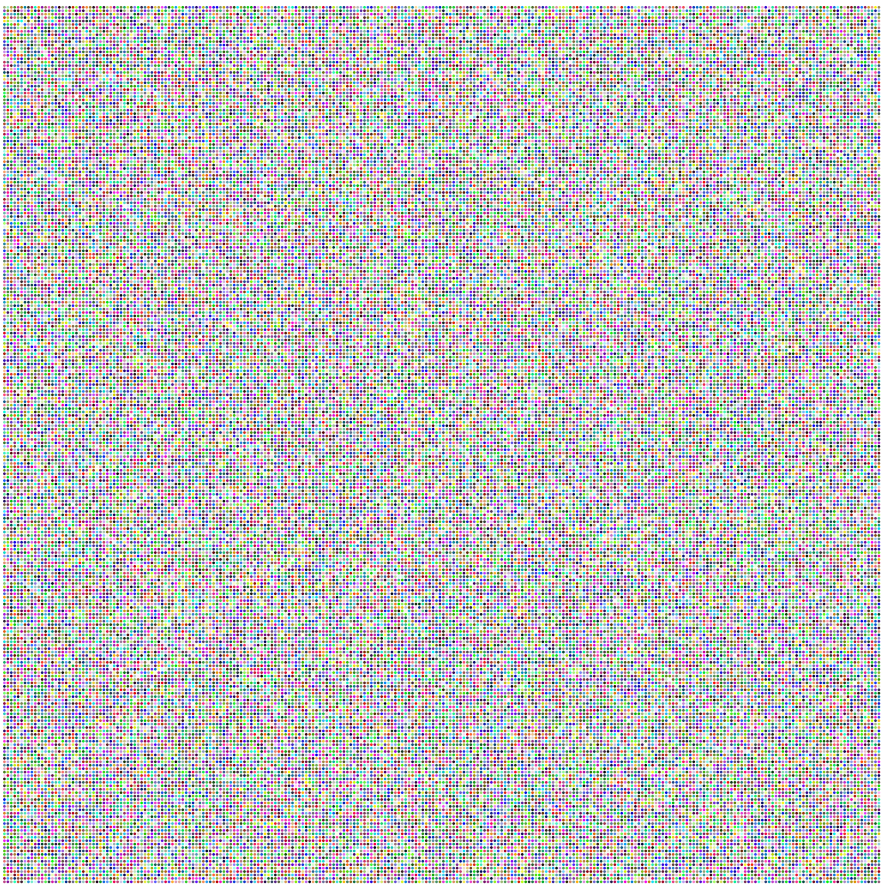
Fundusze Europejskie Inteligentny Rozwój

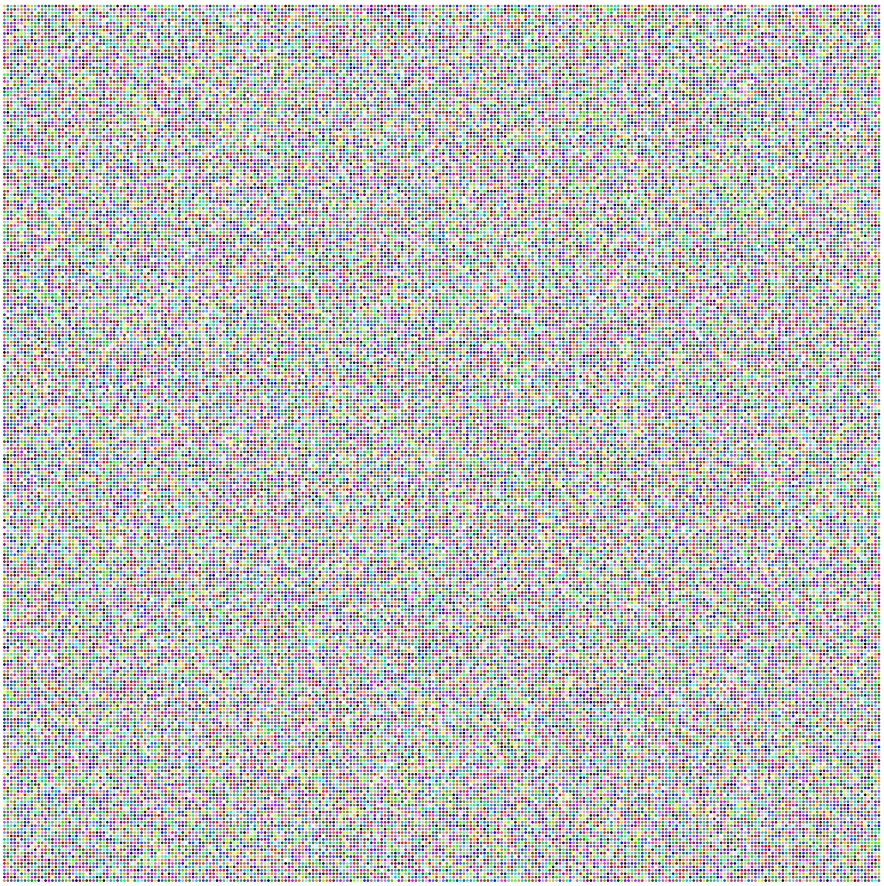
Projekt realizowany w ramach Programu Operacyjnego Inteligentny Rozwój, poddziałanie 1.1.1 "Badania przemysłowe i prace rozwojowe realizowane przez przedsiębiorstwa", współfinansowany ze środków Budżetu Państwa oraz Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego

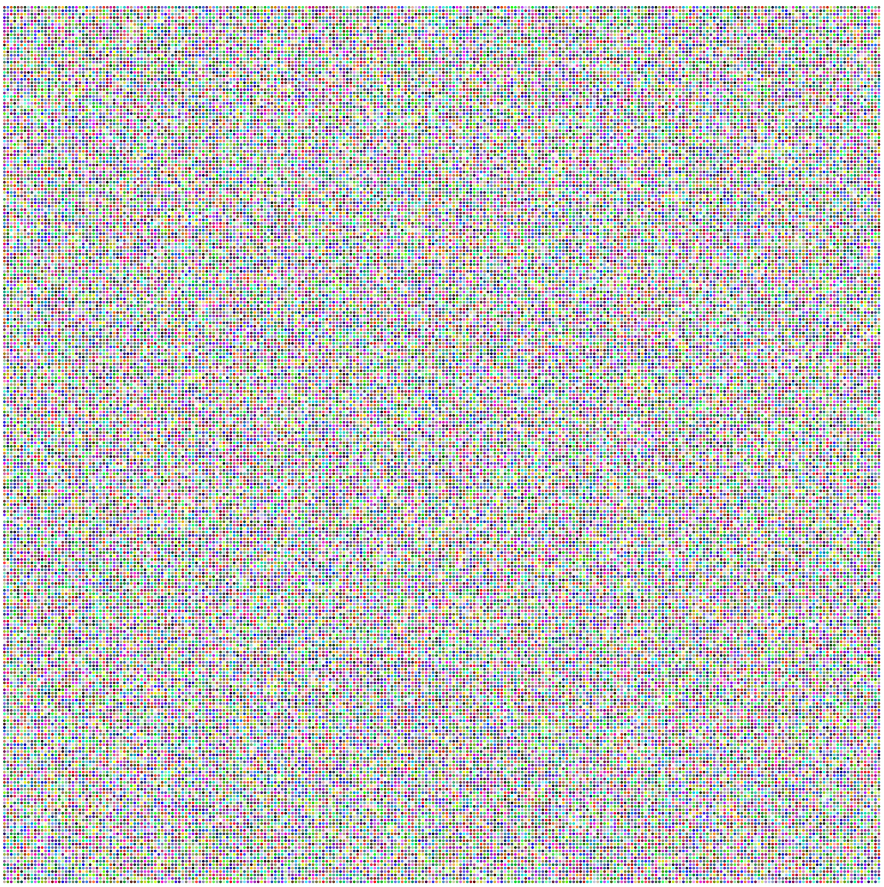
JURAND - Narodowy Kwantowy Generator Liczb Losowvch (POIR.01.01.01-00-0173/15-00)

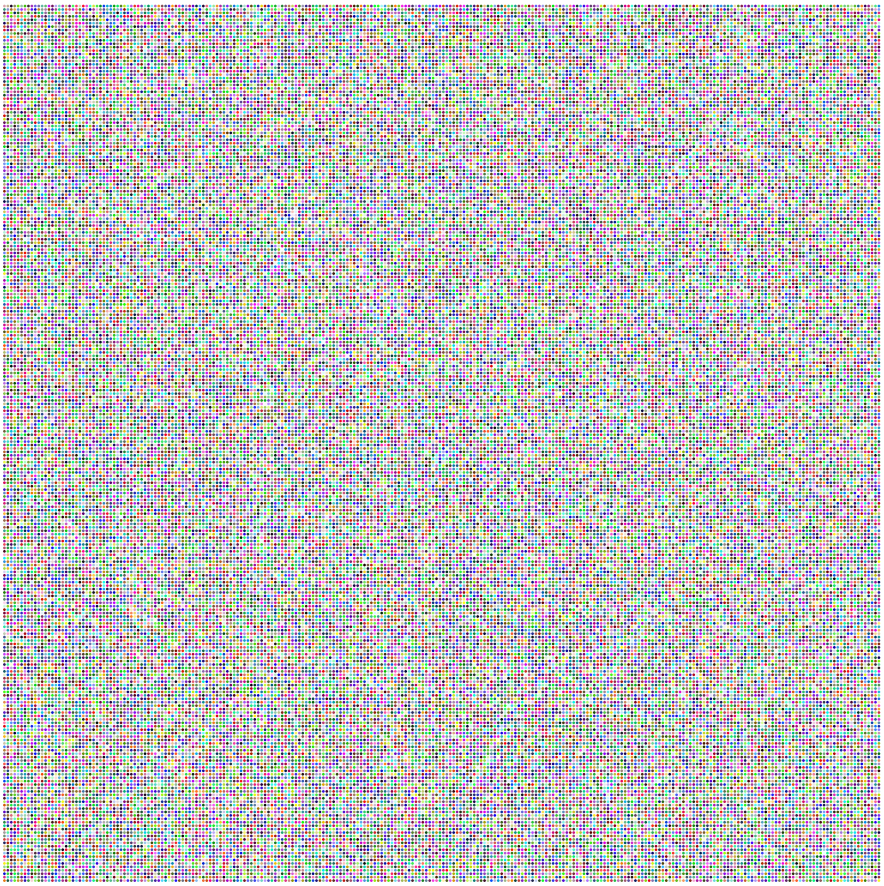
Unia Europejska Europejski Fundusz Rozwoju Regionalnego



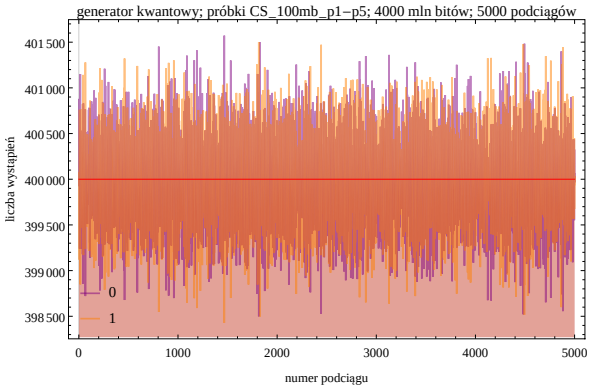


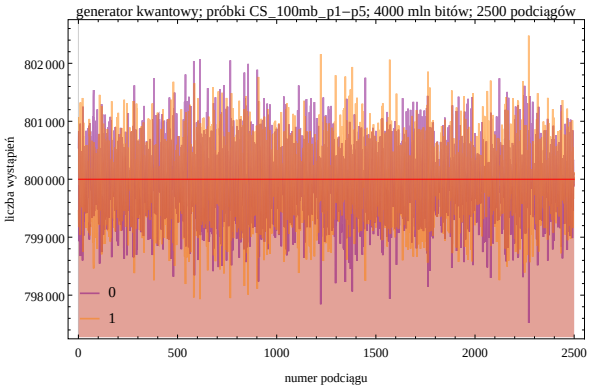


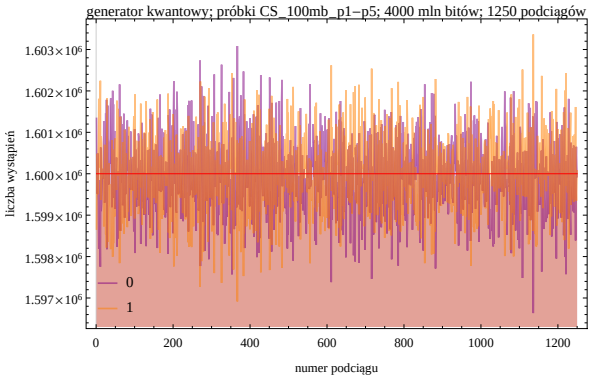


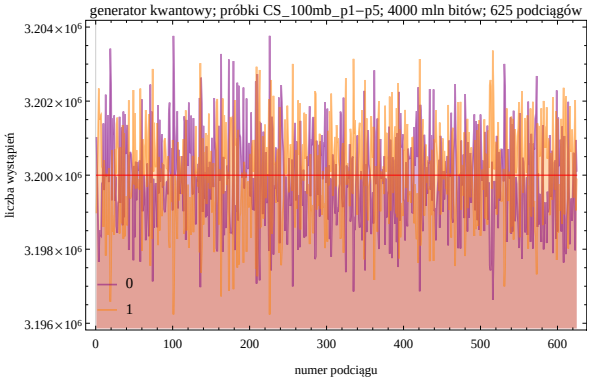


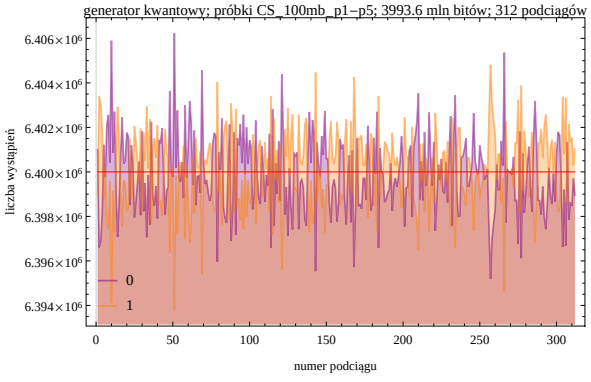
Próbki ciągów losowych generowanych kwantowo w układach laboratoryjnych inżynierii kwantowej zostały poddane analizom losowości w ramach modelu testowania w części statystycznych procedur ze zmiennymi parametrami, na którą składa się kilkanaście podstawowych wariantów testów (z możliwymi rozszerzeniami wariantów, w znacznym stopniu, wraz ze złożonością poszukiwanych korelacji; np. testy wyszukiwania wzorców aperiodycznych). Przeprowadzone testy nie wykazały odchyleń od prawdziwej losowości analizowanych próbek, zarówno przy parametrach zbliżonych do poziomów przyjętych jako standard dla testowania pseudolosowych generatorów liczb dla zastosowań kryptograficznych, jak i dla parametrów znacznie zwiększających czułość testów w kierunku konfiguracji modelu weryfikacji losowości kwantowej, m.in. w zakresie o rząd wyższego poziomu istotności (alfa=0,1, tj. 10%) czy bardziej złożonych wzorców (zgodnie z dyskusją przedstawioną w szczegółowych wyjaśnieniach). Oczywisty problem bariery klasycznego zalgorytmizowanego testowania statystycznego ciągów losowych związanej z ograniczonymi zasobami obliczeniowymi przetwarzania środowiska testującego pojawia się szybko np. ze względu na eksponencjalny wzrost liczby wariantów poszukiwanych wzorców aperiodycznych, np. dla długości 9 bitów jest 148 możliwych aperiodycznych wzorców, a dla dwa razy większej długości, czyli 18 bitów jest już możliwych 70340 aperiodycznych wzorców (w ramach kwalifikacji modelu testy realizowano dla wzorców 15 bitowych przy 8848 możliwych aperiodycznych wzorcach) – w przypadku poszukiwania korelacji dalekozasięgowych liczba wzorców staje się tak duża, że testowanie ich występowania staje się w rzeczywistości niemożliwe wobec ograniczonych zasobów obliczeniowych. Poniższe wyniki podkreślają właśnie ten fakt poprzez zestawienie rezultatów testów przy parametrach ogólnie przyjętych jako standardowe oraz parametryzacji weryfikacji ciągów losowych wygenerowanych kwantowo (która teoretycznie może być parametryzowana w sposób arbitralnie czuły na odchylenia klasyczne, ale w praktyce na drodze stają przedmiotowe ograniczenia w zakresie zasobów obliczeniowych i parametryzacja weryfikacji losowości kwantowej polega na optymalizowaniu zakresów czułości wykrywania odchyleń statystycznych i potencjalnych dalekozasięgowych korelacji w racjonalnym czasie obliczeniowym). Testy zostały pomyślnie zakończone na próbkach o charakterze empirycznie weryfikowanym jako źródła kwantowe (w zakresie eksperymentu kwantowo-mechanicznego), nie wskazując na brak losowości w którymkolwiek z ciągów, co kwalifikuje sparametryzowany dla weryfikacji losowości kwantowej statystyczny model obliczeniowy.

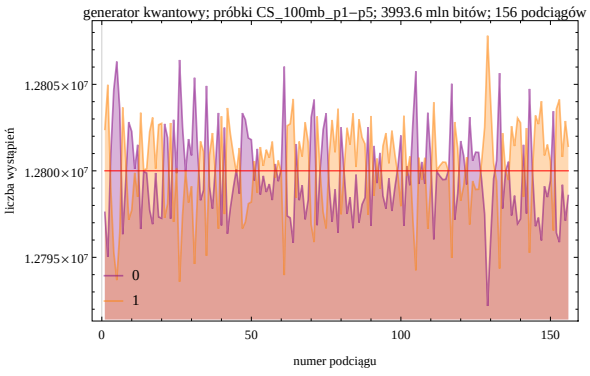

generator kwantowy; próbki CS_100mb_p1−p5; 4000 mln bitów; 5000 podciągów
liczba wystąpień
numer podciągu
0
1

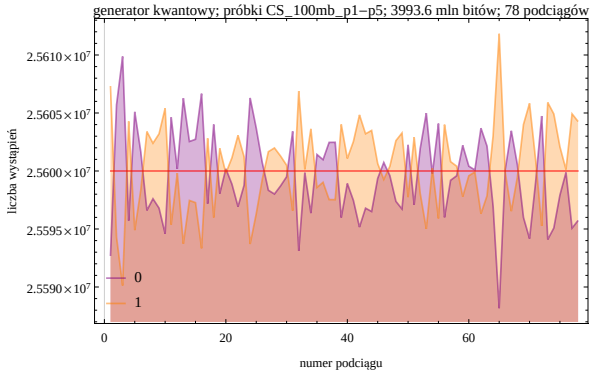

generator kwantowy; próbki CS_100mb_p1−p5; 4000 mln bitów; 2500 podciągów
liczba wystąpień
numer podciągu
0
1

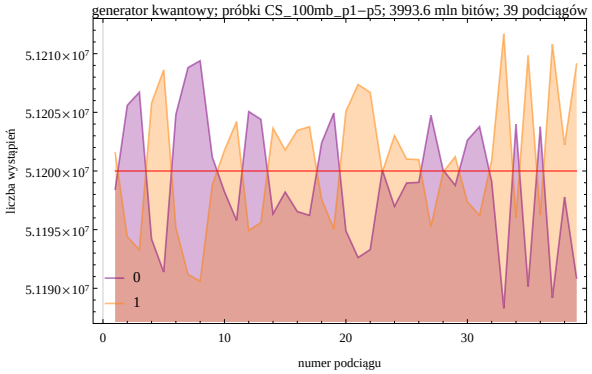

generator kwantowy; próbki CS_100mb_p1−p5; 4000 mln bitów; 1250 podciągów
liczba wystąpień
numer podciągu
0
1

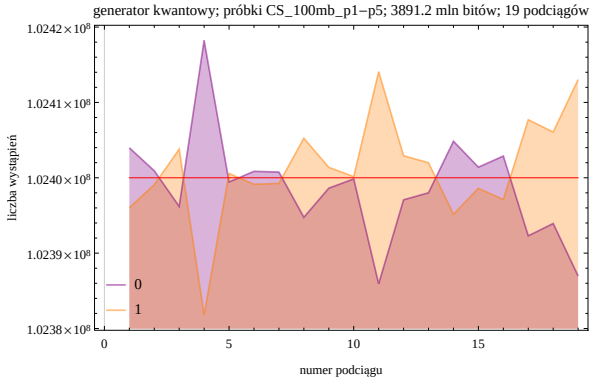

generator kwantowy; próbki CS_100mb_p1−p5; 4000 mln bitów; 625 podciągów
liczba wystąpień
numer podciągu
0
1

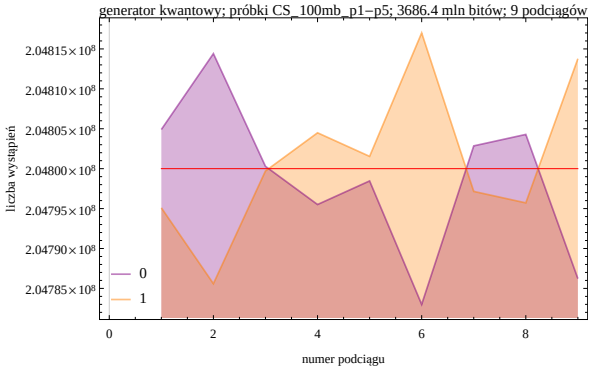

generator kwantowy; próbki CS_100mb_p1−p5; 3993.6 mln bitów; 312 podciągów
liczba wystąpień
numer podciągu
0
1


generator kwantowy; próbki CS_100mb_p1−p5; 3993.6 mln bitów; 156 podciągów
liczba wystąpień
numer podciągu
0
1



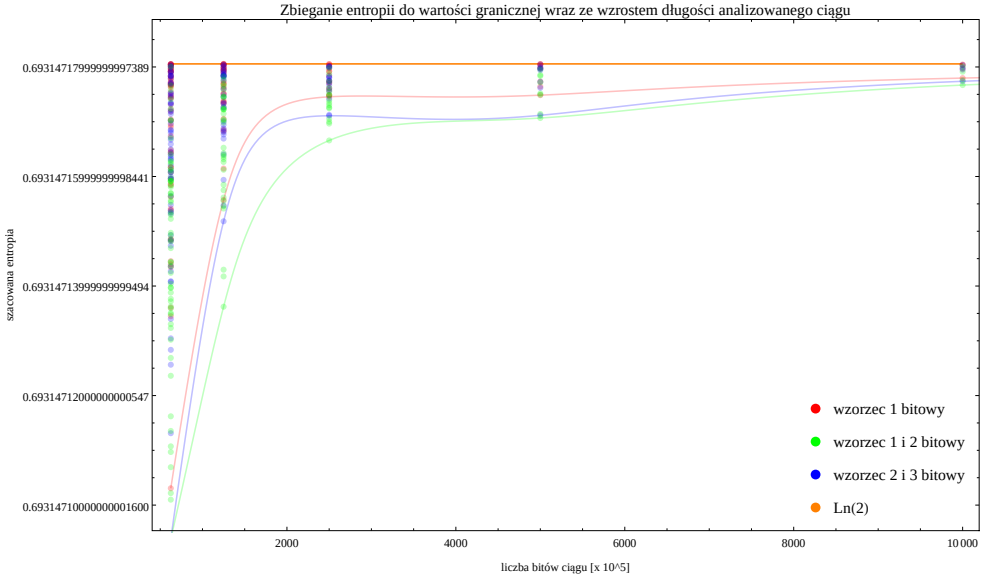


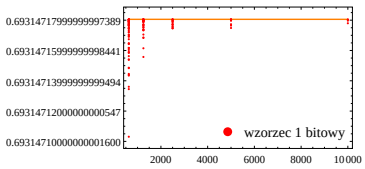


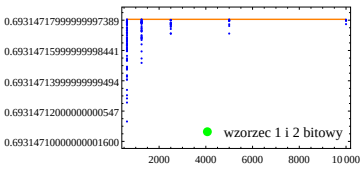


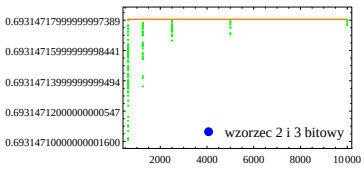
0.1 Przybliżenie entropii generowanych ciągów kwantowych z wykazania osiągania granicznej wartości odchylenia 2^{-64}

Zbieganie wartości 0,1,2-entropii do wartości granicznej $\log 2$ dla próbkowanego ciągu 4000 mln bitów (próbki o rozmiarach 2000, 1000, 500, 250, 125, 65,2 mln bitów).



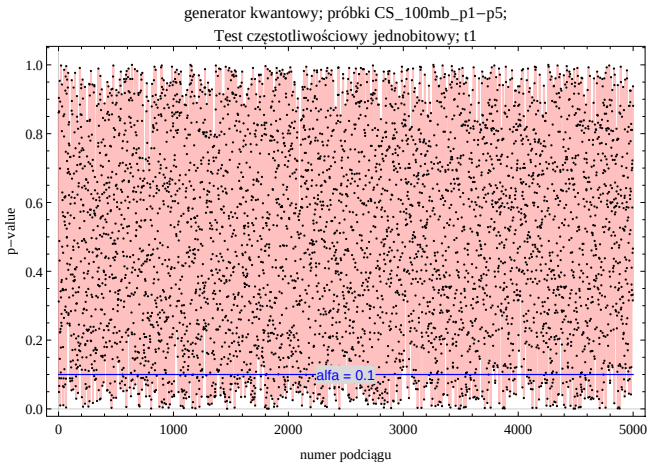




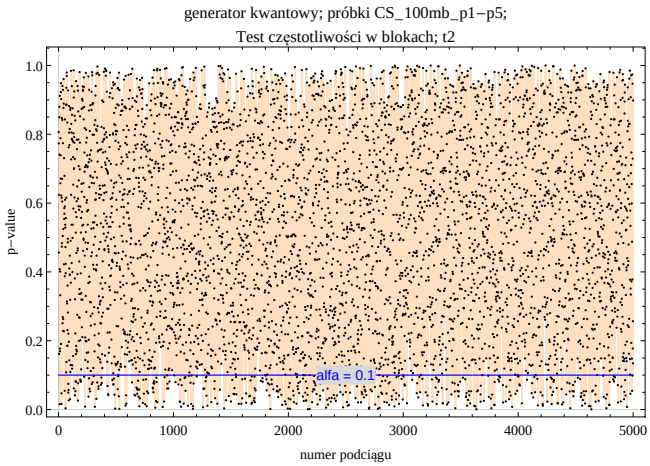


0.2 Zestawienie wyników testów statystycznych weryfikacji losowości kwantowej (wszystkie testy zakończone sukcesem)

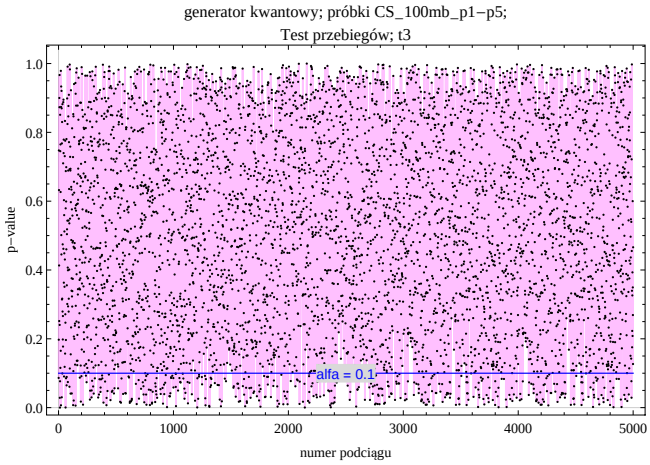
0.2.1 Test częstotliwościowy jednobitowy

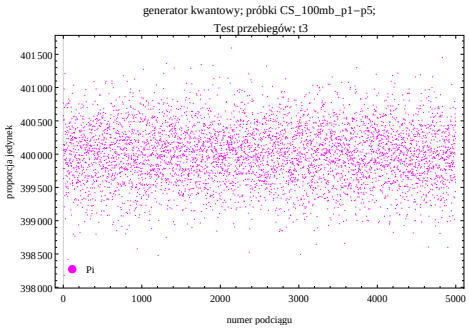


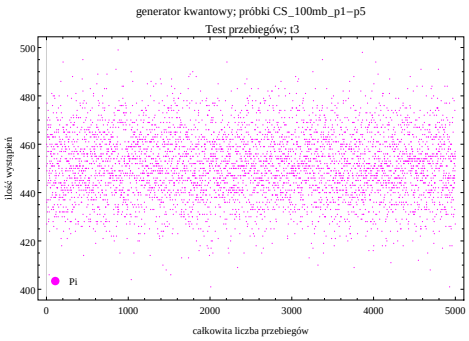
0.2.2 Test częstotliwościowy w blokach



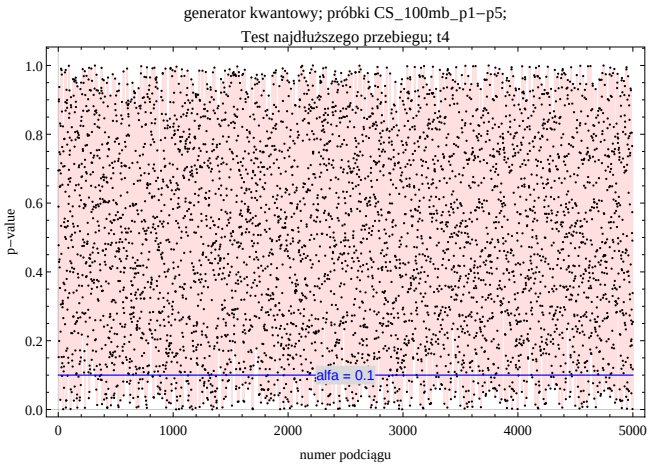
0.2.3 Test przebiegów

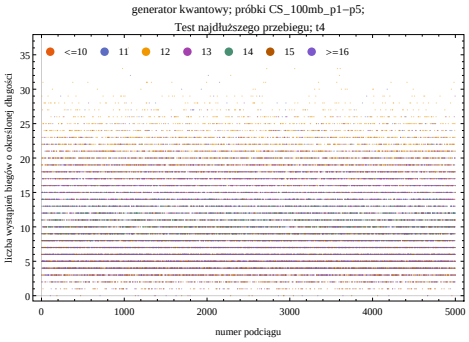




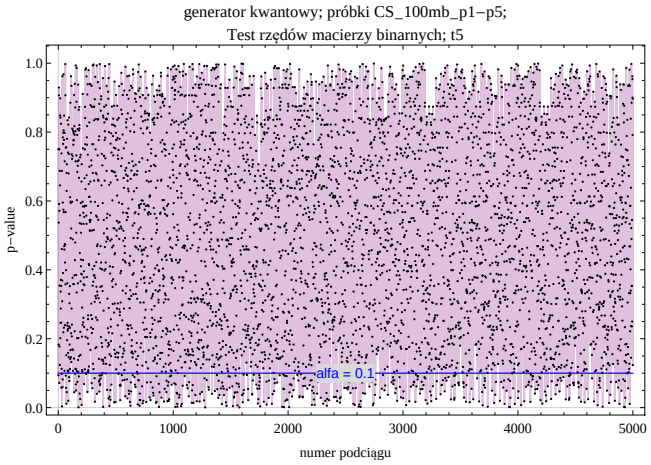


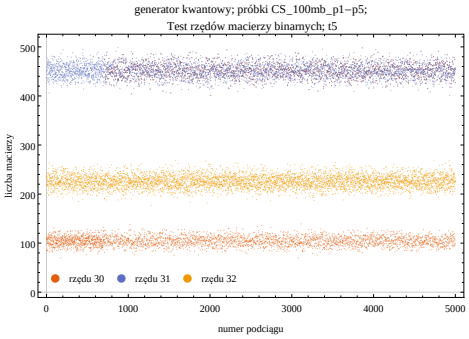
0.2.4 Test najdłuższego przebiegu



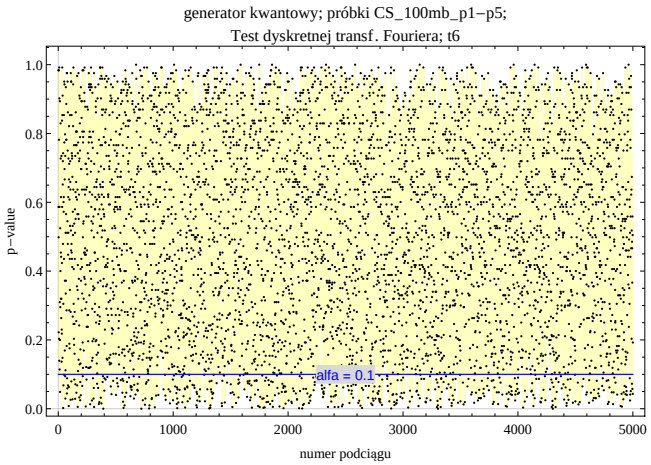


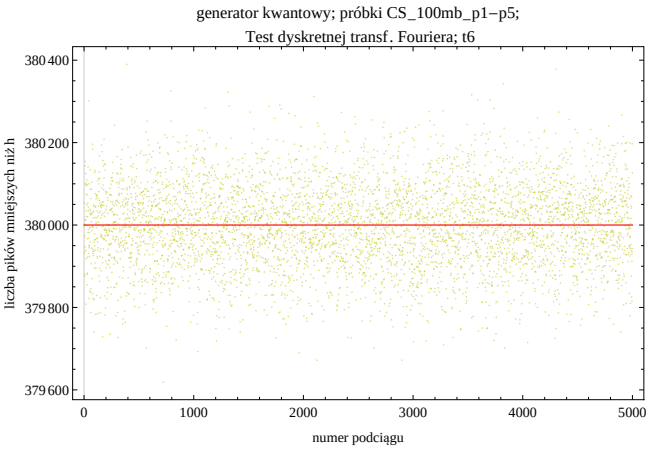
0.2.5 Test rzędów macierzy binarnych



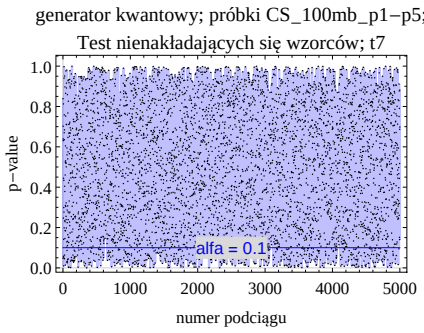


0.2.6 Test dyskretnej transformaty Fouriera

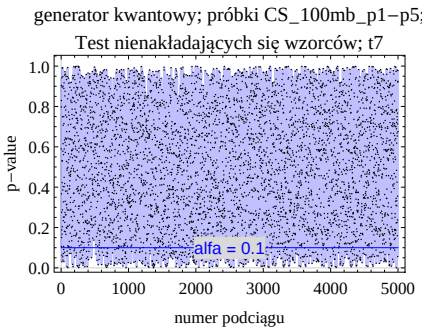




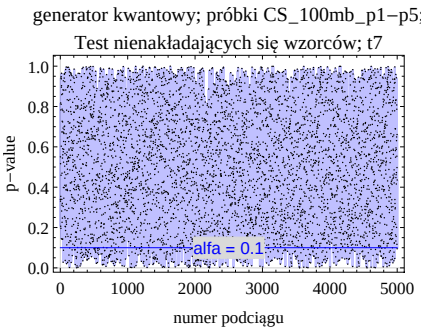
0.2.7 Test występowania nienakładających się wzorców



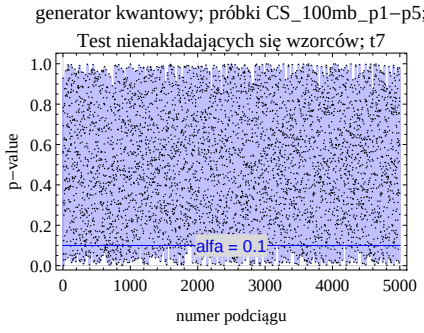
(a) wzorzec aperiodyczny: 000000001110111



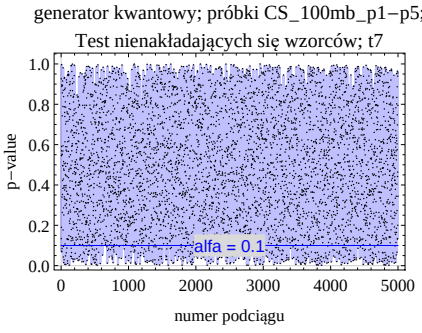
(b) wzorzec aperiodyczny: 000001111111111



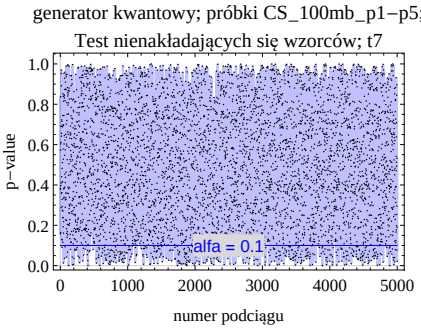
(c) wzorzec aperiodyczny: 000011111000101



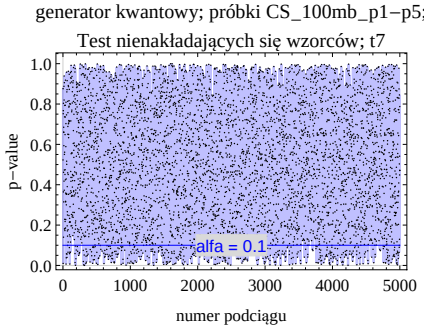
(a) wzorzec aperiodyczny: 000101111001001



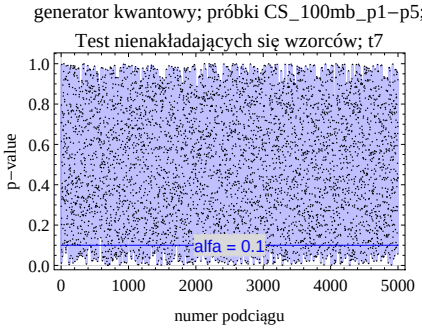
(b) wzorzec aperiodyczny: 001000000011111



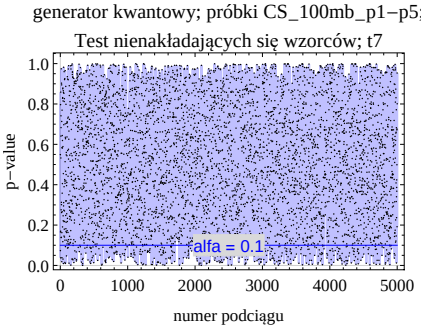
(c) wzorzec aperiodyczny: 001010000011101



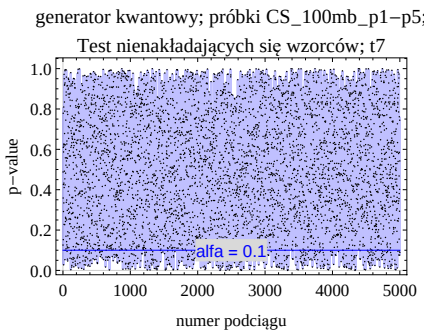
(a) wzorzec aperiodyczny: 001101000100101



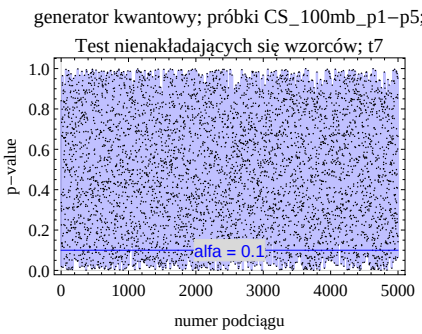
(b) wzorzec aperiodyczny: 010000001010111



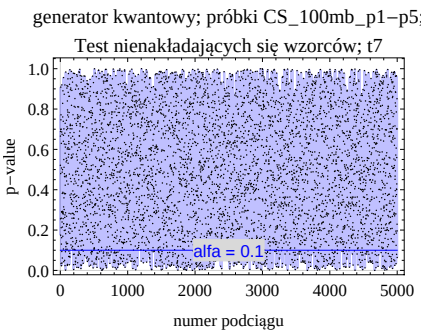
(c) wzorzec aperiodyczny: 010011110000011



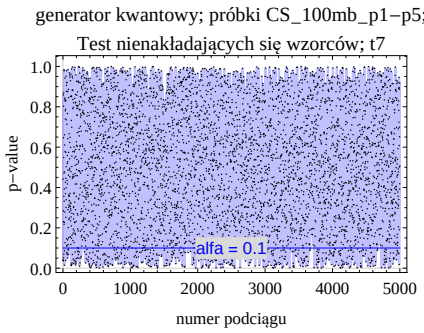
(a) wzorzec aperiodyczny: 010100101010111



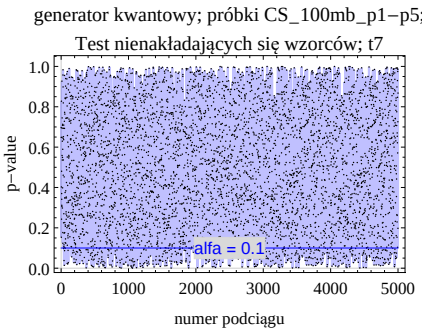
(b) wzorzec aperiodyczny: 100100010110000



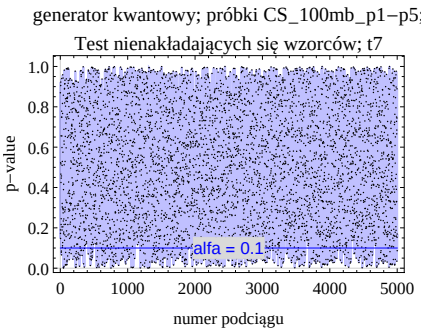
(c) wzorzec aperiodyczny: 100110000101000



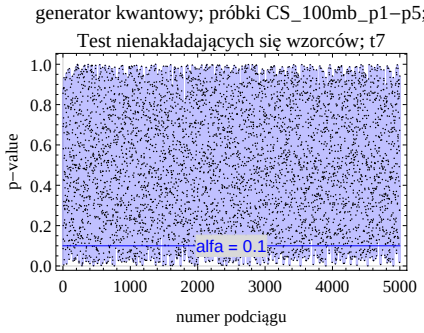
(a) wzorzec aperiodyczny: 100111010110000



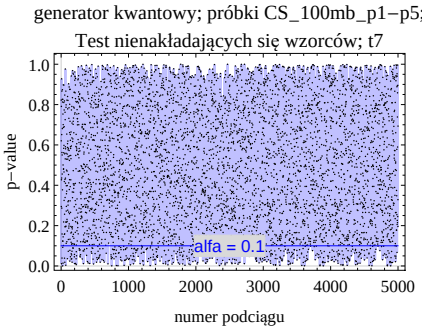
(b) wzorzec aperiodyczny: 101000000001000



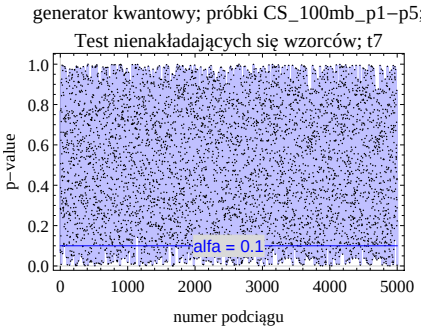
(c) wzorzec aperiodyczny: 110000111111010



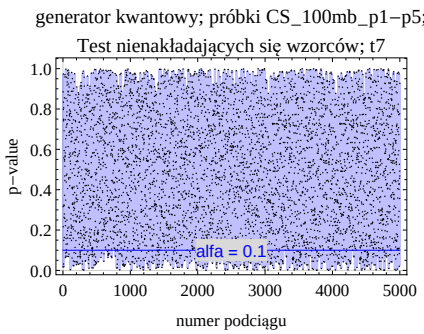
(a) wzorzec aperiodyczny: 111000111101010



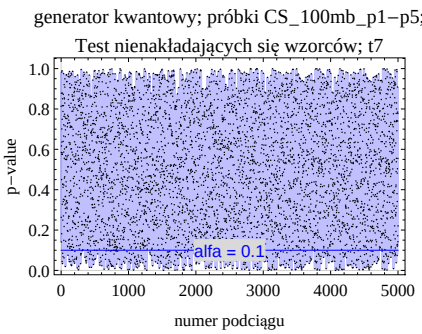
(b) wzorzec aperiodyczny: 111100110111010



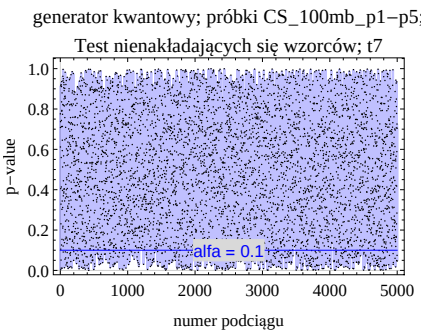
(c) wzorzec aperiodyczny: 111110000100000



(a) wzorzec aperiodyczny: 111111000111010

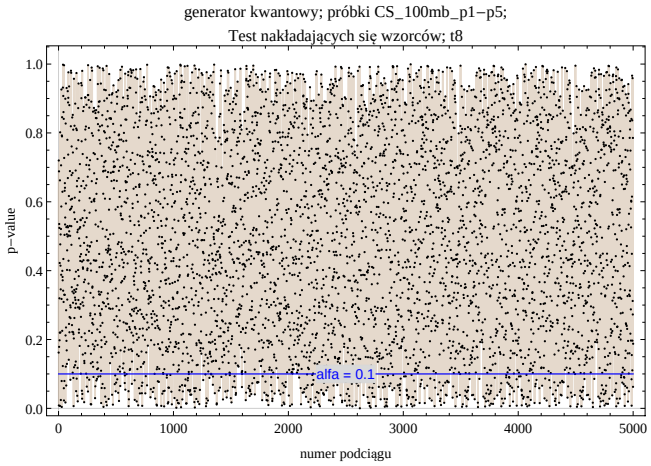


(b) wzorzec aperiodyczny: 111111100011000

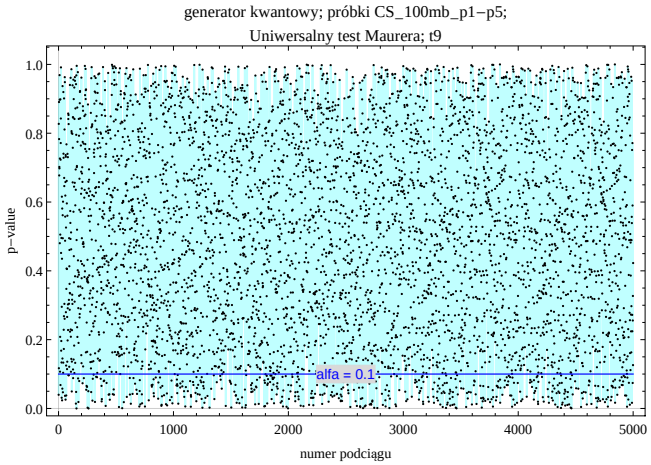


(c) wzorzec aperiodyczny: 111111110010100

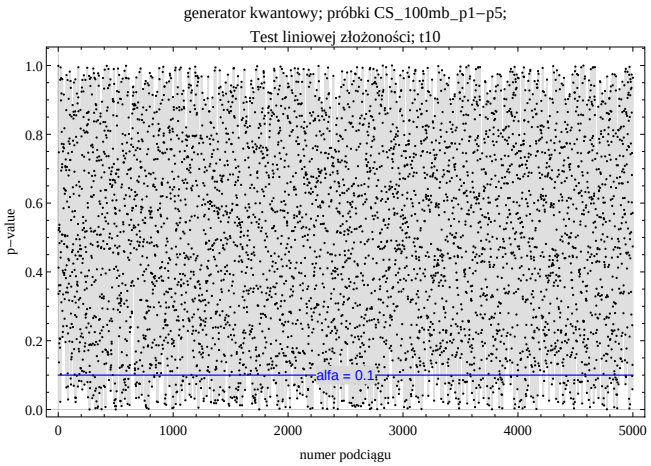
0.2.8 Test występowania nakładających się wzorców

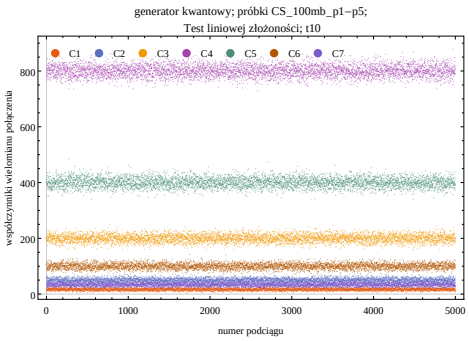


0.2.9 Uniwersalny statystyczny test Maurera

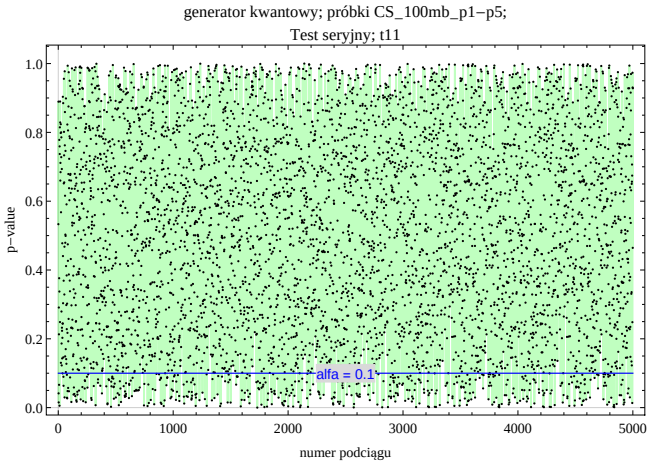


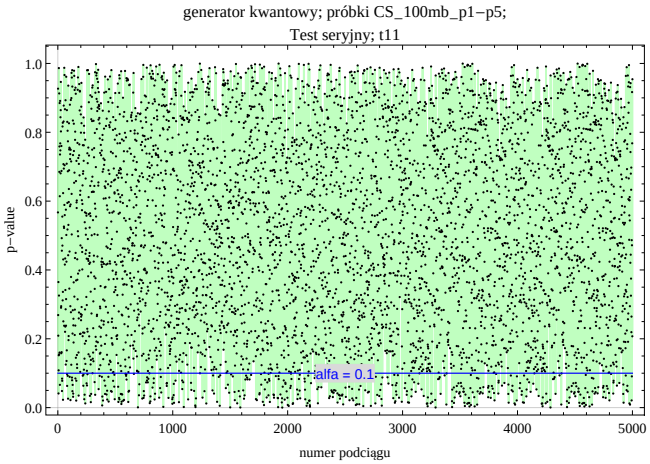
0.2.10 Test liniowej złożoności



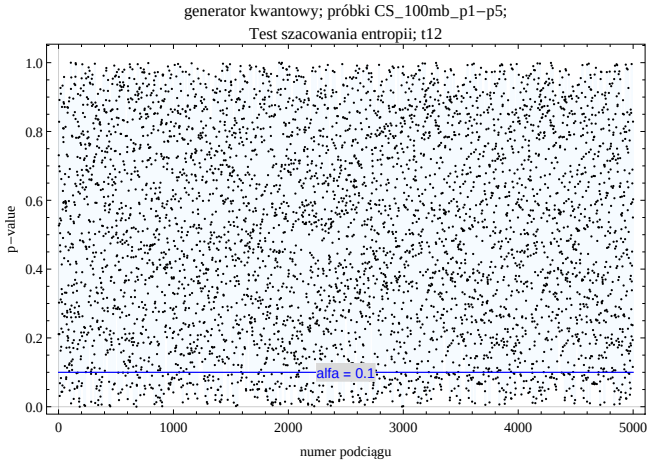


0.2.11 Test seryjny

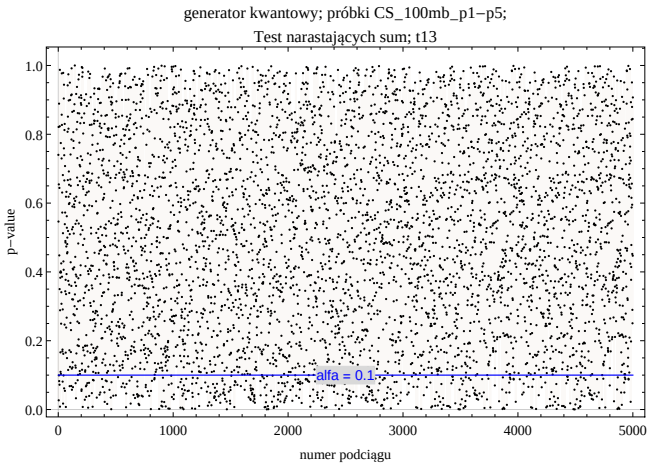


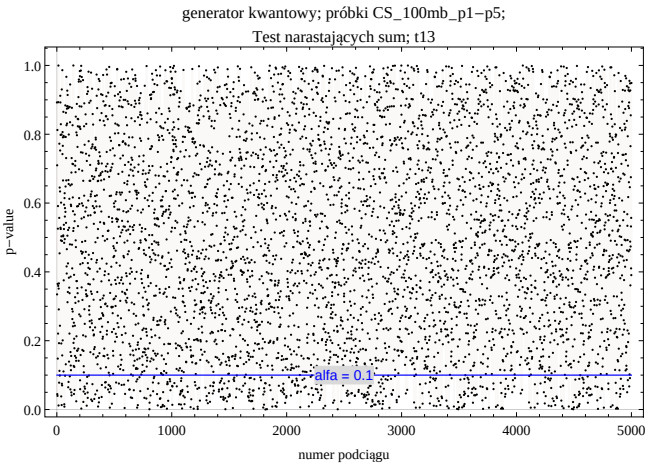


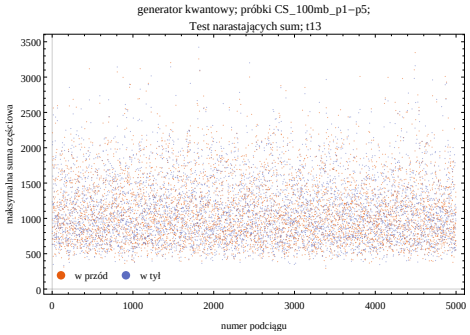
0.2.12 Test szacowania entropii



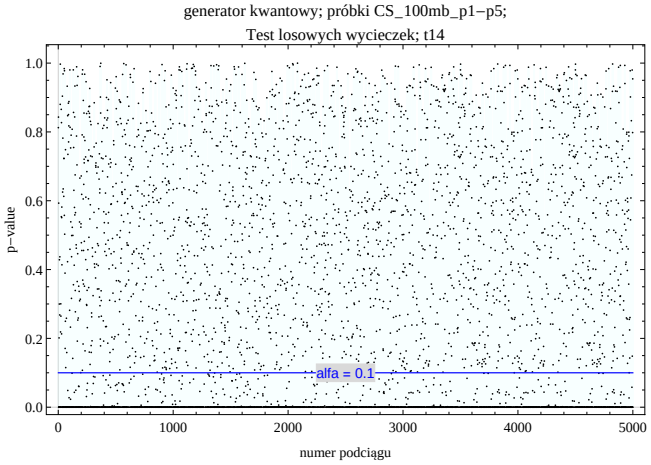
0.2.13 Test narastających sum

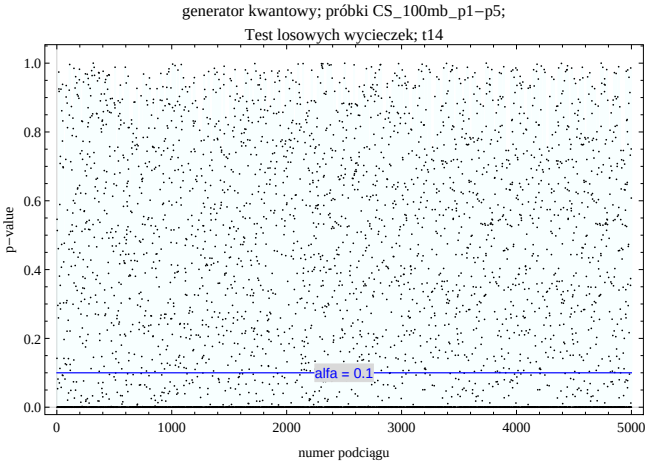


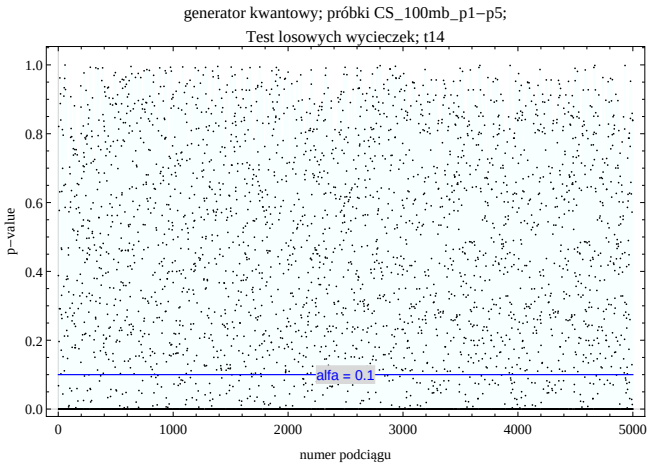


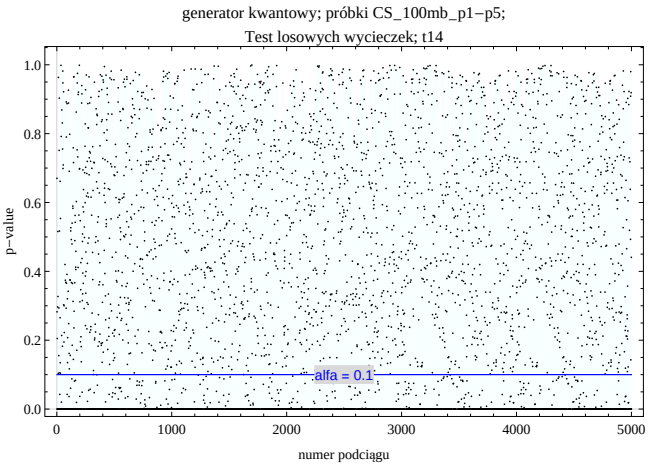


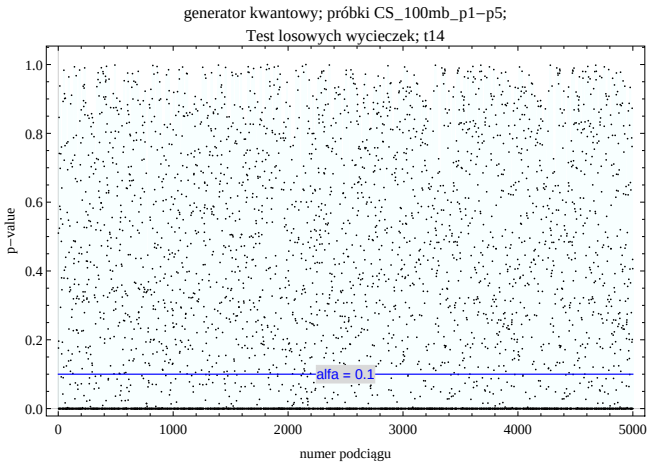
0.2.14 Test losowych wycieczek

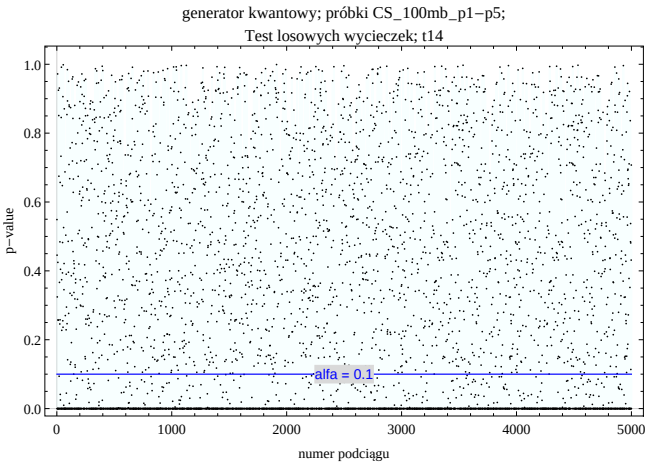


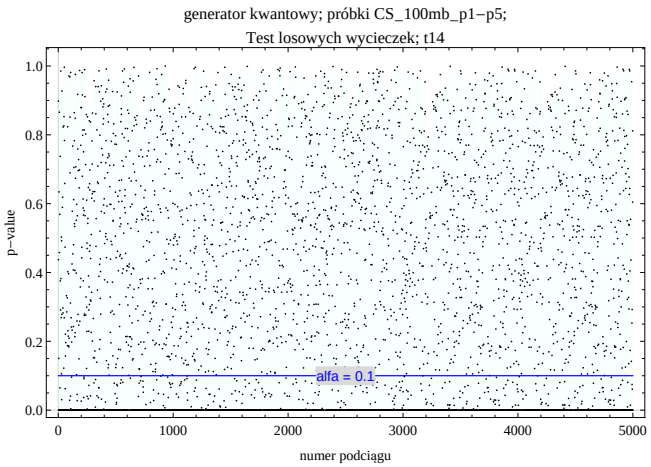


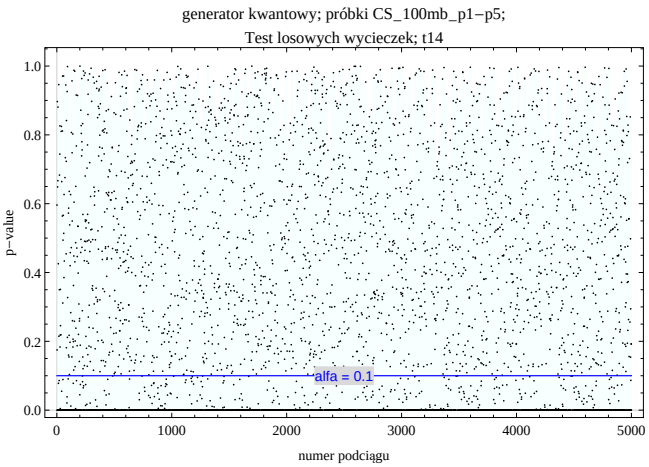




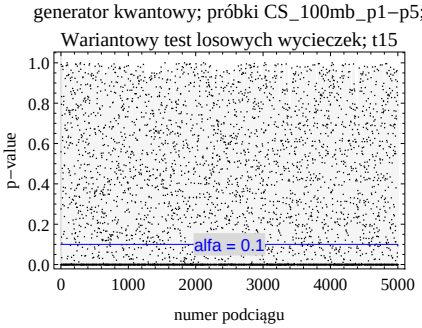


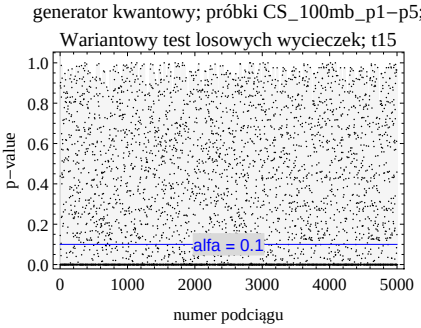


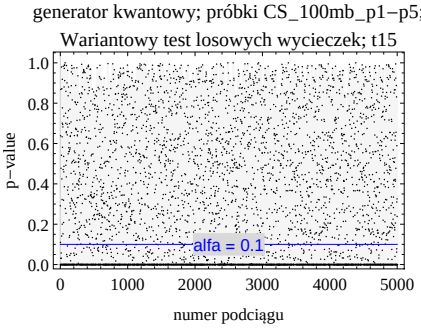


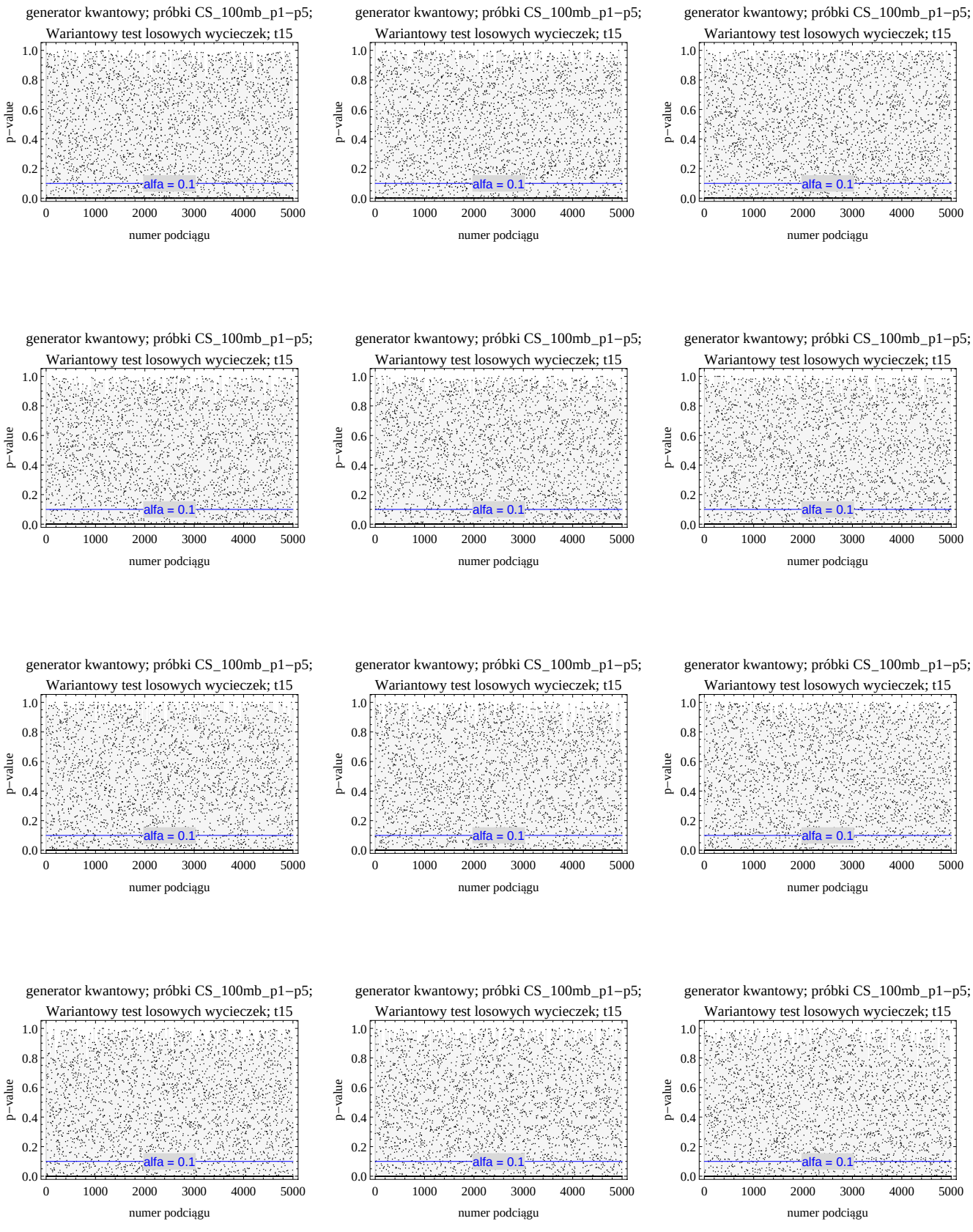


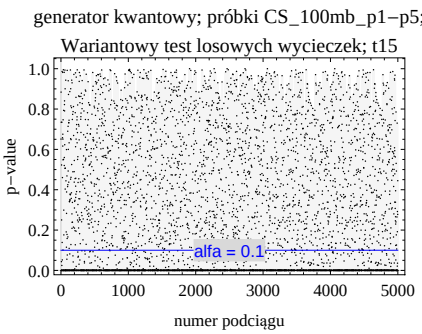
0.2.15 Wariantowy test losowych wycieczek

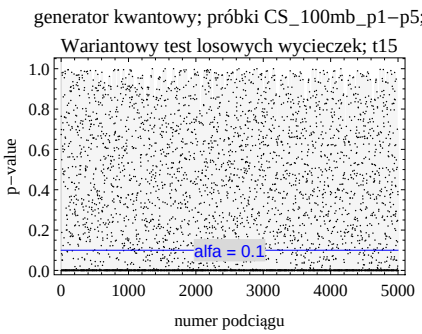


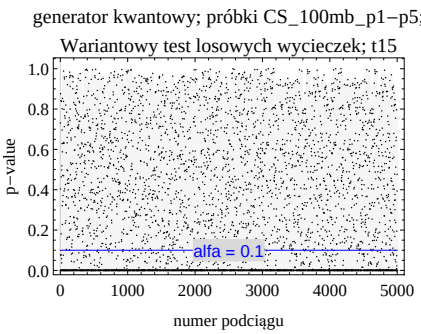





generator kwantowy; próbki CS_100mb_p1−p5;
Wariantowy test losowych wycieczek; t15
p−value
numer podciągu
alfa = 0.1


generator kwantowy; próbki CS_100mb_p1−p5;
Wariantowy test losowych wycieczek; t15
p−value
1.0
0.8
0.6
0.4
0.2
0.0
alfa = 0.1
0
1000
2000
3000
4000
5000
numer podciągu


generator kwantowy; próbki CS_100mb_p1−p5;
Wariantowy test losowych wycieczek; t15
p−value
1.0
0.8
0.6
0.4
0.2
0.0
alfa = 0.1
0
1000
2000
3000
4000
5000
numer podciągu


generator kwantowy; próbki CS_100mb_p1−p5;
Wariantowy test losowych wycieczek; t15
p−value
1.0
0.8
0.6
0.4
0.2
0.0
alfa = 0.1
0
1000
2000
3000
4000
5000
numer podciągu