Wiktor Bachta

ZADANIE DOMOWE 4

1. Nierówności ogonowe dla rozkładu dwumianowego Bin(n, 1/2)

$P(X \geq \frac{6}{5}E(X))$

Markow:

$P(X \geq \frac{6}{5}E(X)) \leq \frac{E(X)}{\frac{6}{5}E(X)} = \frac{5}{6}$

Czebyszew (z wykorzystaniem symetrii rozkładu):

$P(X \geq \frac{6}{5}E(X)) = \frac{1}{2}P(|X - E(X)| \geq \frac{1}{5}E(X)) \leq \frac{1}{2}\frac{var(X)}{(\frac{1}{5}E(X))^2} = \frac{25 \cdot \frac{1}{4}n}{2 \cdot \frac{1}{4}n^2} = \frac{25}{2n}$

	Markow	Czebyszew	dokładna wartość
100	>0.5	0.125	0.028444
1000	>0.5	0.0125	1.3642e-10
10 000	>0.5	0.00125	8.7022e-90

$P(|X - E(X)| \geq \frac{1}{10}E(X))$

Markow (z wykorzystaniem symetrii rozkładu):

$P(|X - E(X)| \geq \frac{1}{10}E(X)) = 2 \cdot P(X \geq \frac{11}{10}E(X)) \leq 2\frac{E(X)}{\frac{11}{10}E(X)} = \frac{20}{11} > 1$

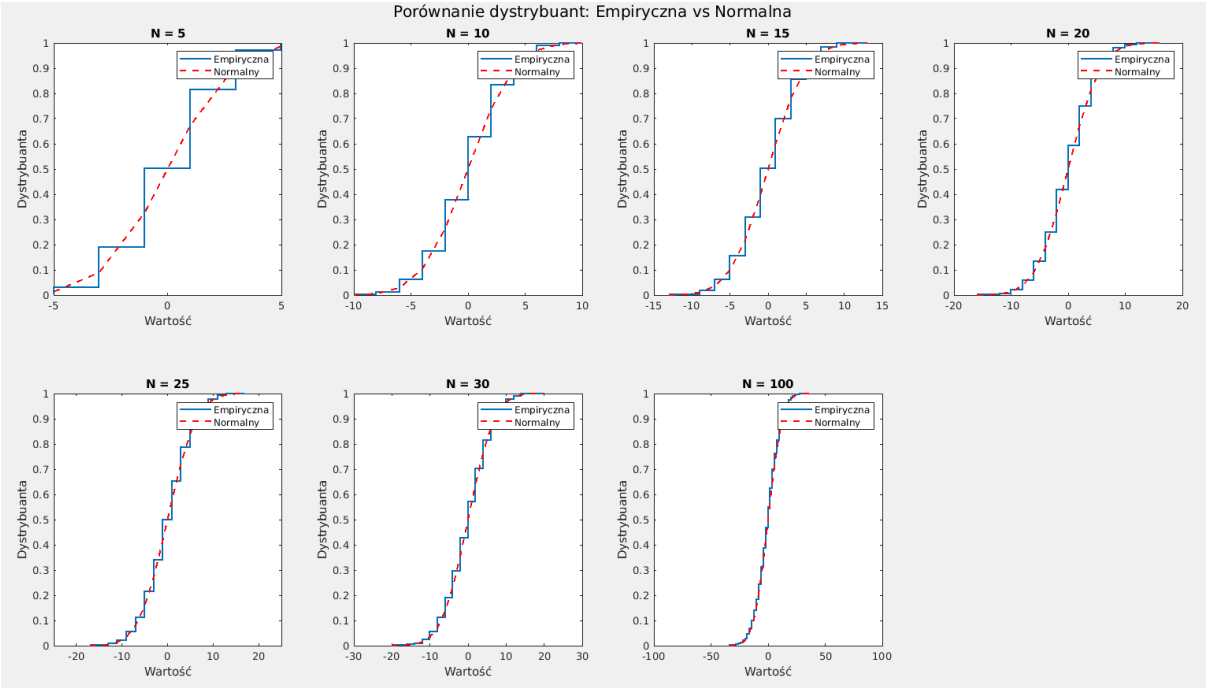
Czebyszew:

$P(|X - E(X)| \geq \frac{1}{10}E(X)) \leq \frac{var(X)}{(\frac{1}{10}E(X))^2} = \frac{100 \cdot \frac{1}{4}n}{\frac{1}{4}n^2} = \frac{100}{n}$

	Markow	Czebyszew	dokładna wartość
100	>1	1	0.0066371
1000	>1	0.1	0.0017305
10 000	>1	0.01	1.5511e-23

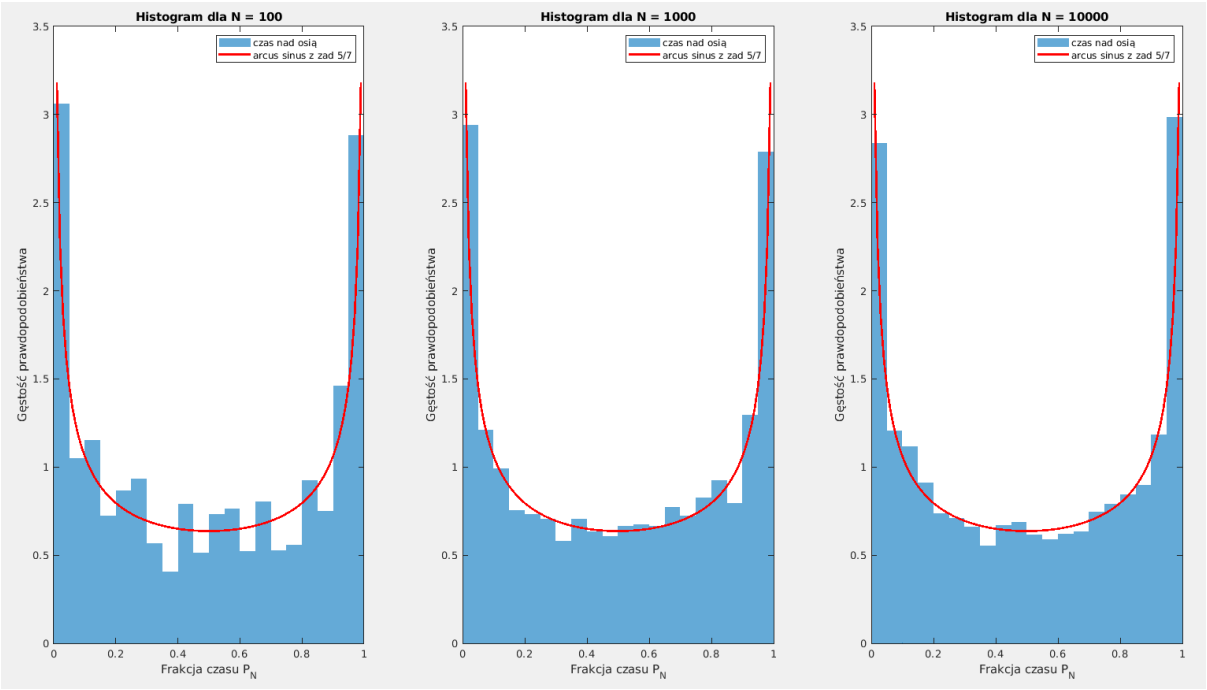
W oszacowaniach nierówność Markowa okazała się bezużyteczna. Nierówność Czebyszewa dała sensowne wyniki, ale i tak bardzo dalekie dokładnej wartości prawdopodobieństwa. W dodatku, wraz z rosnącym n, rezultaty nierówności szybko tracą na dokładności przybliżenia.

2. Błądzenie losowe na liczbach całkowitych



Do wyznaczenia dystrybuanty empirycznej wygenerowałem po 10 000 wartości zmiennej Sn dla każdego n. Jak widać na wykresach, przybliżenie sumy n i.i.d. zmiennych losowych rozkładem normalnym daje bardzo dobre rezultaty już dla $n \geqslant 30$.

3. Błądzenie losowe na liczbach całkowitych - czas nad osią OX



Wynik eksperymentu może wydawać się nieintuicyjny, spodziewając się, że ścieżka losowa średnio spędzi 50% czasu nad osią OX i 50% czasu pod nią. Jednak po zastanowieniu, otrzymany rezultat ma sens. Jeżeli ścieżka znajduje się nad osią OX, to z większym prawdopodobieństwem pozostanie nad tą osią w kolejnych krokach. Analogicznie, jeśli jest ona pod osią OX. Dlatego rozkład częściej osiąga skrajne wartości, gdzie ścieżka jest prawie cały czas pod lub nad osią OX.

4. Testowanie generatorów liczb pseudolosowych (PRNG)

c)

1. Linear Congruential Generator in Python

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.9760670531717747	Passed
2. Frequency Test within a Block	0.09331348291565053	Passed
3. Runs Test	0.6128560175384068	Passed
4. Test for the Longest Run of Ones in a Block	0.970458821593197	Passed
5. Binary Matrix Rank Test	0.4249769541412142	Passed
6. Non-overlapping Template Matching Test	0.6326800603275016	Passed
7. Overlapping Template Matching Test	0.419817198662813	Passed
8. Maurer's "Universal Statistical" Test	0.04729842316621202	Passed
9. Linear Complexity Test	0.48217276339498405	Passed
10. Serial Test	P-value 1: 0.8803303889061517 P-value 2: 0.6142613960933927	Passed
11. Approximate Entropy Test	0.8966999443870396	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.8039800130489358 P-value Reverse: 1	Passed
13. Random Excursions Test	0.14718765373922604	Passed
14. Random Excursions Variant Test	0.24277228162825115	Passed

2. Mersenne Twister in Python

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.08988588006267961	Passed
2. Frequency Test within a Block	0.8248844884936912	Passed
3. Runs Test	0.4997530519482475	Passed
4. Test for the Longest Run of Ones in a Block	0.754142780709024	Passed
5. Binary Matrix Rank Test	0.17760927297325746	Passed
6. Non-overlapping Template Matching Test	0.8372269947637401	Passed
7. Overlapping Template Matching Test	0.45182149620967194	Passed
8. Maurer's "Universal Statistical" Test	0.2568108098148545	Passed
9. Linear Complexity Test	0.8548677313347895	Passed
10. Serial Test	P-value 1: 0.1893799432577494 P-value 2: 0.5015837210170484	Passed
11. Approximate Entropy Test	0.4526655260209037	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.1786376770723841 P-value Reverse: 0.5509381998709804	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

3. JavaScript pseudo RNG

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.8760330212212882	Passed
2. Frequency Test within a Block	0.23871352234478388	Passed
3. Runs Test	1.21128218786392	Failed
4. Test for the Longest Run of Ones in a Block	0.052612635670535896	Passed
5. Binary Matrix Rank Test	0.6564611437140461	Passed
6. Non-overlapping Template Matching Test	0.5474651189847952	Passed
7. Overlapping Template Matching Test	0.20985188279476735	Passed
8. Maurer's "Universal Statistical" Test	0.8222084718622612	Passed
9. Linear Complexity Test	0.25468926186388746	Passed
10. Serial Test	P-value 1: 0.953057539389354 P-value 2: 0.7886993290873143	Passed
11. Approximate Entropy Test	0.9679665397862017	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.331429597783816 P-value Reverse: 0.43694570314849646	Passed
13. Random Excursions Test	0.08392372799278329	Passed
14. Random Excursions Variant Test	0.3840304185555483	Passed

Zaskakująco, wybrane generatory liczb losowych przeszły większość testów. Nawet generator LCG spełnił je wszystkie (a “dobry” generator JavaScript pseudo RNG nie - o czym w punkcie d). Nie ma także wyraźnej hierarchii wśród generatorów ze względu na P-value. Na tej podstawie można wnioskować, że na potrzeby symulacji statystycznych można wykorzystać pierwszy i drugi z wybranych generatorów. Trzeci z nich może okazać się wadliwy, aby to zweryfikować należy przeprowadzić więcej testów. Warto też zaznaczyć, że niespełniony test świadczy o prawdopodobnie złym generatorze, ale spełniony test nie gwarantuje, że generator jest dobry.

d)

Nawet jeśli Kubuś Puchatek posiada idealny generator losowych bitów, to nie ma gwarancji, że przejdzie wszystkie testy NIST. Dlaczego? Ponieważ wciąż istnieje bardzo małe, ale niezerowe prawdopodobieństwo, że wygenerowany ciąg bitów będzie miał niesatysfakcjonujące dla testów właściwości. Bardzo skrajnym zobrazowaniem tego zjawiska może być np. wygenerowanie 10000-bitowego ciągu samych jedynek. Wtedy generator Kubusia Puchatka zostanie poddany w wątpliwość, mimo to, że jako idealny generator stworzył ten ciąg z prawdopodobieństwem $\frac{1}{2^{10000}}$.