Testy

fragment wykładu

Ciągi statystycznie losowe - testy

- Testy statystyczne FIPS 140-2
- **Test pojedynczych bitów** dla ciągów o długości 20 000 bitów:
- $$9725 < n(1) < 10275$$
- **Test serii:** seria w danym ciągu to maksymalny podciąg następujących po sobie zer lub jedynek
-

Długość serii	Przedział
1	2315-2685
2	1114-1386
3	527-723
4	240-384
5	103-209
6 i więcej	103-209

Testy cd.

- **Test długiej serii** - serię zer albo jedynek nazywamy długą, jeśli ma długość 26 lub więcej. Test zakończy się sukcesem jeśli w próbce o długości 20 000 bitów nie ma takiej serii.
- **Test pokerowy:**
  - ciąg o długości 20 000 bitów należy podzielić na 5000 segmentów.
  - należy policzyć i zapamiętać liczbę wystąpień każdej z możliwych 16 - 4 bitowych wartości

Test pokerowy cd.

- Niech s(i), gdzie 0 <= i <= 15 oznacza liczbę wystąpień segmentów o wartości dziesiętnej i.
- Test zakończy się sukcesem, jeśli 2,16 < X < 46,17,
- gdzie X:

$$x = \frac{16}{5000} \cdot \sum_{i=0}^{15} s(i)^2 - 5000$$