

## Test losowości $\chi^2$

Testowanie losowości generatora ciągu binarnego.

Hipoteza zerowa  $H_0$  (Ciąg ma charakter losowy).

Hipoteza alternatywna  $H_1$  (Ciąg nie ma charakteru losowego).

poziom istotności  $\alpha$ .

Weryfikacja powyższych hipotez za pomocą testu  $\chi^2$  przebiega następująco:

1. Generujemy długi binarny ciąg losowy.

Dzielimy go na bloki np. 4-bitowe.

$n$  – liczba bloków,  $n > 80$ ,

$k$  – liczba możliwych wartości w bloku, (dla bloków 2-bitowych  $k = 4$  liczb dwubitowych, dla bloków 4-bitowych  $k = 16$  liczb czterobitowych)

2. Przyjmujemy, że  $p_i = \frac{1}{k}$ .

3. Wyznaczamy liczbę  $n_i$  wystąpień  $i$  – tej wartości we wszystkich blokach,  $i = 1, 2, \dots, k$ .

$$\sum_{i=1}^k n_i = n$$

4. Obliczamy

$$u_n = \sum_{i=1}^k \frac{(n_i - np_i)^2}{np_i} = \frac{1}{n} \sum_{i=1}^k \frac{(n_i)^2}{p_i} - n$$

5. Wyznaczamy zbiór krytyczny obustronny

$$K = \langle 0 ; k_1 \rangle \cup \langle k_2 ; \infty \rangle ,$$

gdzie  $k_1, k_2$  wyznaczamy z tablicy rozkładu  $\chi^2$  z  $k - 1$  stopniami swobody .

$$P(Y_{k-1} \geq k_1) = 1 - \frac{\alpha}{2} , \quad P(Y_{k-1} \geq k_2) = \frac{\alpha}{2}$$

Podejmujemy decyzję:

odrzucaamy hipotezę  $H_0$ , gdy  $u_n \in K$   
przyjmujemy hipotezę  $H_0$ , gdy  $u_n \notin K$

### **Test pokerowy 4 bitowy.**

Hipoteza zerowa  $H_0$  (Ciąg ma charakter losowy).  
poziom istotności  $\alpha$ .

Generujemy długi binarny ciąg losowy. Dzielimy go na bloki 4-bitowe.

$n$  – liczba bloków,  $n > 80$ ,

$k$  – liczba możliwych wartości w bloku, dla bloków 4-bitowych  $k = 16$  liczb czterobitowych)

Przyjmujemy, że  $p_i = \frac{1}{16}$ .

Wyznaczamy liczbę  $n_i$  wystąpień  $i$  – tej wartości we wszystkich blokach,  $i = 1, 2, \dots, 16$ .

$$\sum_{i=1}^{16} n_i = n$$

Obliczamy

$$u_n = \frac{16}{n} \sum_{i=1}^{15} (n_i)^2 - n$$

6. Wyznaczamy zbiór krytyczny obustronny

$$K = \{ < 0 ; k_1 \} \cup \{ < k_2 ; \infty \} ,$$

gdzie  $k_1, k_2$  wyznaczamy z tablicy rozkładu  $\chi^2$  z  $k - 1$  stopniami swobody .

$$P(Y_{k-1} \geq k_1) = 1 - \frac{\alpha}{2} ,$$

$$P(Y_{k-1} \geq k_2) = \frac{\alpha}{2}$$

Podajemy decyzję:

Nie ma podstaw do odrzucenia ciągu gdy

$$k_1 < u_n < k_2$$

## Wyznaczanie liczby jedynek w ciągu binarnym

Przykład. (*test monobitowy*)

Wyznaczanie liczby jedynek w równomiernym ciągu binarnym.

Niech  $n = 10000$ , poziom istotności  $\alpha = 0,01$ .

$$H_0(p = 0,5), \quad H_1(p \neq 0,5)$$

$$K = (-\infty ; -k > \cup < k ; \infty),$$

$$\Phi(k) = 1 - \frac{\alpha}{2}$$

$$U_n = \frac{W - 0,5}{\sqrt{0,5(1-0,5)}} \sqrt{n}$$

gdzie  $W$  – średnia liczba jedynek w ciągu.

Wtedy  $k = 2,58$ ,

$$\begin{aligned} K &= (-\infty ; -k > \cup < k ; \infty) = \\ &= (-\infty ; -2,58 > \cup < 2,58 ; \infty) \end{aligned}$$

Aby test był pozytywny dla generatora liczba jedynek  $k$  powinna być w granicach

$$-2,58 < \frac{\frac{k}{10000} - 0,5}{\sqrt{0,5(1-0,5)}} \sqrt{10000} < 2,58$$

Czyli

od 4872 do 5128

**Zadanie:** wykonać powyższy przykład dla poziomu istotności  $\alpha = 0,001$ .

### **Test entropii (Maurera)**

Generujemy długi binarny ciąg losowy. Dzielimy go na bloki  $L$ -bitowe (zwykle  $L = 8, \dots, 16$ ).

$Q$  – sekwencja inicjująca,

$K$  – sekwencja testowa,

Długość próbki  $N = (Q + K)L$ .

Uwaga,

$$Q > 5 \cdot 2^L, \quad K \gg Q$$

zatem dla np.  $L = 8$        $Q > 5 \cdot 2^8 = 1280$

## Statystyka testowa

$$U = \frac{1}{K} \sum_{n=Q}^{Q+K-1} \log_2 A_n$$

$A_n$  – odległość  $n$ -tego bloku od jego ostatniego wystąpienia (lub  $n$  gdy blok występuje pierwszy raz),

Stawiamy hipotezę:  $H_0$ (entropia istotna),  
Pożądana jest istotna entropia.

Zbiór krytyczny

$$K_r = \langle 0 ; k_1 \rangle \cup \langle k_2 ; \infty \rangle =$$

Wyznaczanie  $k_1 < k_2$ :

$$k_1 = E - k\sigma,$$

$$k_2 = E + k\sigma$$

gdzie  $\Phi(k) = 1 - \frac{\alpha}{2}$ , dla poziomu istotności  $\alpha$ .

$$\sigma = \sqrt{\frac{V}{K}} \quad K - \text{długość sekwencji testowej}$$

Zestawienie wartości  $E$ ,  $V$  dla przykładowych  $L$ .

| <b>L</b> | <b>E</b>    | <b>V</b> |
|----------|-------------|----------|
| 8        | 7,1836655   | 3,238    |
| 9        | 8,17642476  | 3,311    |
| 10       | 9,17232431  | 3,356    |
| 11       | 10,17003223 | 3,384    |
| 12       | 11,1687649  | 3,401    |
| 13       | 12,1680703  | 3,410    |
| 14       | 13,1676926  | 3,416    |
| 15       | 14,1674884  | 3,419    |
| 16       | 15,1673788  | 3,421    |

Nie ma podstaw do odrzucenia ciągu gdy

$$k_1 < u < k_2$$