

Test dei Generatori di Numeri Casuali

Michela Meo

Maurizio M. Munafò

Michela.Meo@polito.it - Maurizio.Munafò@polito.it

Test dei Generatori

- L'obiettivo dei test dei generatori di numeri casuali è verificare che la sequenza di numeri generati abbia delle caratteristiche stocastiche "simili" a quelle di una sequenza casuale teorica

Test dei Generatori

- Ogni numero Z_i nella sequenza casuale generata dovrebbe essere un'istanza *indipendente* di una v.c. con distribuzione *uniforme* in $(0,1)$
- La sequenza dovrebbe avere due proprietà:
 - **Uniformità**
 - **Indipendenza**
- I test servono a verificare le proprietà di uniformità e indipendenza dei numeri prodotti da un generatore

Test dei Generatori

- Molti test sono *empirici*
- Sono basati sul confronto tra
 - il *risultato* di un'operazione eseguita sulle sequenze generate
 - la *distribuzione* teorica del risultato di quella operazione quando l'operazione è eseguita su sequenze generate da un generatore ideale

Test dei Generatori

- Solitamente i test si riconducono a 3 tipologie:
 - **Test del chi-quadro**: confronto con la distribuzione chi-quadro, che deriva dalla somma di quadrati di variabili normali
 - **Test della normale**: confronto con la normale, che si ha in presenza della somma di tante variabili indipendenti
 - **Test di Kolmogorov-Smirnov**: basato sullo scarto massimo tra la stima di una distribuzione cumulativa ottenuta da un numero finito di campioni e la distribuzione stessa

Chi-quadro o χ^2

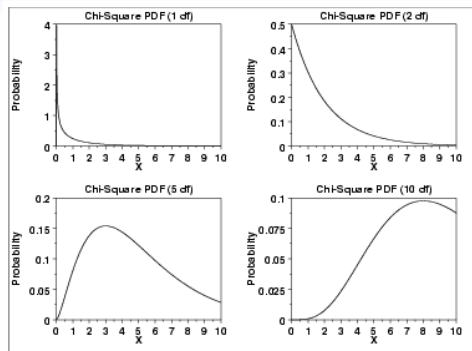
- La distribuzione χ^2 (chi-quadro) con k gradi di libertà risulta quando k variabili indipendenti con distribuzione normale $N(0,1)$ sono elevate al quadrato e sommate.

- La pdf è
$$f(x) = \frac{e^{-\frac{x}{2}} x^{\frac{k}{2}-1}}{2^{\frac{k}{2}} \Gamma(\frac{k}{2})} \quad x \geq 0$$

dove $\Gamma()$ è la funzione Gamma definita

$$\Gamma(a) = \int_0^{\infty} t^{a-1} e^{-t} dt$$

Chi-quadro o χ^2

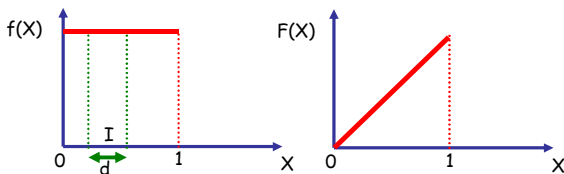


Test dei Generatori

- Data un'ipotesi H_0 (es. uniformità), si definisce un livello α di significatività del test come

$$\alpha = P(\text{rifiuto ipotesi } H_0 | H_0 \text{ vera})$$
 di solito si sceglie $\alpha = 0.01, 0.05, 0.10$
- Un generatore ideale fallisce il test con probabilità α
- Un test positivo significa che *non ci sono prove che H_0 non valga*
- Un test statistico andrebbe ripetuto un certo numero di volte, N (un generatore ideale fallirebbe il test per αN volte)

Test dei Generatori



- Dato un intervallo I lungo d compreso in $(0,1)$
 - Di N osservazioni mi aspetto di osservarne un numero pari a Nd nell'intervallo I (uniformità)
 - La probabilità che un'osservazione cada in I è la stessa delle osservazioni precedenti (indipendenza)

Test di uniformità del chi-quadro

- Definisco n intervalli equispaziati in $(0,1)$, gli intervalli sono lunghi $1/n$
- Si generano N istanze e si calcola il numero O_i di istanze che cadono nell'intervallo i -esimo e lo si confronta con il valore atteso, $E_i = N/n$
- Si calcola

$$X = \sum_{i=1}^n \frac{(O_i - E_i)^2}{E_i}$$
- Se il generatore è uniforme e N è grande, X è distribuita come il chi-quadro con $n-1$ gradi di libertà

Test di uniformità del chi-quadro

- Dal confronto tra X e la distribuzione chi-quadro con $n-1$ gradi di libertà, si decide se accettare o rifiutare l'ipotesi H_0 di uniformità
- Se $X > \chi^2_{n-1, \alpha}$ rifiuto l'ipotesi H_0 con livello di significatività pari ad α
- I valori $\chi^2_{n-1, \alpha}$ sono noti e tabulati

Test di uniformità del chi-quadro

- Esempio:** uso $n=10, N=100$, quindi $E_i=10$ e osservo i seguenti valori

O_i	8	8	10	9	12	8	10	14	10	11
$O_i - E_i$	-2	-2	0	-1	2	-2	0	4	0	1
$(O_i - E_i)^2 / E_i$	0.4	0.4	0	0.1	0.4	0.4	0	1.6	0	0.1

- Si ottiene $X=3.4$
- Il chi-quadro con livello $\alpha=0.05$ e $n-1=9$ gradi di libertà vale 16.9 (maggiore di X), quindi l'ipotesi non è rifiutata

Test di Kolmogorov-Smirnov

- Confronta la cumulativa $F(x)$ teorica con la distribuzione $S(x)$ empirica
- Avendo generato N istanze $Z_i, i=1\dots N$, si definisce $S_N(x)$ come il rapporto tra il numero di istanze minori di x e N
- Se il generatore è uniforme, $S_N(x)$ tende a $F(x)$ per N che tende a infinito

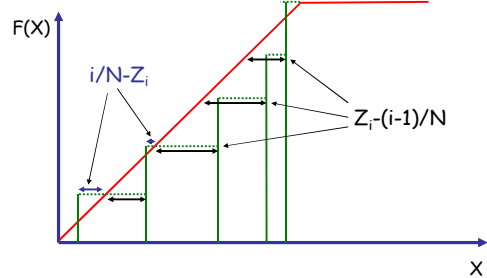
Test di Kolmogorov-Smirnov

- Si calcola la massima deviazione $D = \max |F(x) - S_N(x)|$
- Si confronta D con la massima deviazione teorica che si otterrebbe nel caso di N istanze generate da un generatore ideale
- Le deviazioni teoriche sono riportate nelle tabelle dei valori critici del test di K-S

Test di Kolmogorov-Smirnov

- Ordina le istanze Z_j per valori crescenti ottenendo la sequenza ordinata Z_i
- Calcola
$$D^+ = \max_{1 \leq i \leq N} \left\{ \frac{i}{N} - Z_i \right\} \quad D^- = \max_{1 \leq i \leq N} \left\{ Z_i - \frac{i-1}{N} \right\}$$
- Calcola $D = \max(D^+, D^-)$
- Confronta con le tabelle del comportamento teorico

Test di Kolmogorov-Smirnov



Test di Kolmogorov-Smirnov

- Valori critici di Kolmogorov-Smirnov

Gradi di libertà N	D_α con $\alpha=0.10$	D_α con $\alpha=0.05$	D_α con $\alpha=0.01$
1	0.950	0.975	0.995
...
5	0.510	0.565	0.669
...
10	0.368	0.410	0.490
...
20	0.264	0.294	0.356

Test di Kolmogorov-Smirnov

- Dato il grado di libertà N , se $D > D_\alpha$ l'ipotesi di uniformità è respinta con livello di significatività α
- Esempio: estraggo 0.44, 0.81, 0.14, 0.05, 0.93, eseguire il test di uniformità di Kolmogorov-Smirnov con livello di significatività $\alpha=0.05$ ($D_\alpha=0.565$)

Test di Kolmogorov-Smirnov

- Esempio: estraggo 0.44, 0.81, 0.14, 0.05, 0.93 e voglio $\alpha=0.05$
 - $D=0.26$
 - $D_{\alpha}=0.565$, con $N=5$, $\alpha=0.05$
 - $D < D_{\alpha}$, quindi l'ipotesi di uniformità non è respinta

Z_i	0.05	0.14	0.44	0.81	0.93
$i/5$	0.2	0.4	0.6	0.8	1
$i/5 - Z_i$	0.15	0.26	0.16	-0.01	0.07
$Z_i - (i-1)/5$	0.05	-0.06	0.04	0.21	0.13

Test di Uniformità

- Il test del chi-quadro richiede N maggiore di 100 e E_i almeno 5
- Il test di Kolmogorov-Smirnov può essere fatto anche per valori di N più piccoli, ma valori grandi di N sono preferibili
- Kolmogorov-Smirnov è più efficace
- Entrambi non dicono nulla sulla correlazione tra i campioni successivi o sull'ordine con cui vengono generati

Serial test (correlazione)

- E' una generalizzazione del test del chi-quadro applicato a serie di numeri
- Può fallire se c'è correlazione tra istanze successive
- Divido l'intervallo $(0,1)$ in n intervalli I_i e considero degli spazi t -dimensionali T_j ottenuti da combinazioni di intervalli I_i

$$T_j = (I_{k_1}, I_{k_2}, \dots, I_{k_t})$$
per ogni combinazione di k_1, k_2, \dots, k_t con $k_i=1, 2, \dots, n$

Serial Test

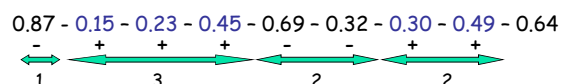
- Genero N tuple consecutive non sovrapposte di numeri del tipo
$$U_1 = (Z_1, Z_2, \dots, Z_t), U_2 = (Z_{t+1}, \dots, Z_{2t}), \dots$$
 - Conto il numero di volte O_j che una tupla cade nell'intervallo t -dimensionale T_j
 - Confronto O_j con il valore atteso $E_j = N/n^t$ tramite la formula
$$X = \sum_{i=1}^{n^t} \frac{(O_i - E_i)^2}{E_i}$$
- Se il generatore è uniforme e N grande, X è distribuita come il chi-quadro con $n^t - 1$ gradi di libertà

Run Test (correlazione)

- Data una sequenza, associo un + a quei numeri il cui successore nella sequenza è maggiore e un - a quei numeri il cui successivo è minore
- Otengo una sequenza di simboli + e -
- Si definisce *run* una sequenza di simboli uguali
- Si verifica che il numero totale di run e la loro lunghezza siano vicini al valore teorico atteso

Run Test Up and Down

- Data una sequenza, associo un simbolo '+' a quei numeri il cui successore nella sequenza è maggiore e un simbolo '-' a quei numeri il cui successivo è minore



Run Test Up and Down

- Se a è il numero totale di run, la media e la varianza di a sono dati da

$$\mu = \frac{2N-1}{3} \quad \sigma^2 = \frac{16N-29}{90}$$

- Per $N > 20$, la distribuzione di a è approssimata da una normale con media μ e varianza σ^2 , $N(\mu, \sigma^2)$

Run Test Up and Down

- Definendo

$$Z = \frac{a - \mu}{\sigma} = \frac{a - [(2N-1)/3]}{\sqrt{(16N-29)/90}}$$

Z è distribuita secondo una normale con media 0 e varianza 1, $N(0,1)$

- L'ipotesi di indipendenza non può essere respinta con livello di significatività α se

$$-z_{\alpha/2} \leq Z \leq z_{\alpha/2}$$

Run Test Intorno alla Media

- Si esegue un run test definendo con il simbolo '+' i numeri che sono maggiori della media (0,5 per un'uniforme) e con '-' quelli minori della media
- Se n_1 è il numero di osservazioni con il simbolo + e n_2 quelle con -, N il totale, il numero di run b ha media e varianza pari a

$$\mu = \frac{2n_1n_2}{N} + \frac{1}{2} \quad \sigma^2 = \frac{2n_1n_2(2n_1n_2 - N)}{N^2(N-1)}$$

Run Test Intorno alla Media

- Per n_1 e n_2 maggiori di 20, b tende a essere distribuito come una normale
- La variabile Z definita come

$$Z = \frac{b - \mu}{\sigma}$$

è una normale $N(0,1)$ a cui si può applicare il test statistico della normale

Test della Lunghezza dei Run

- Si creano sequenze per il run test, o del tipo up and down o per quello intorno alla media
- Si conta il numero O_i di sequenze osservate di lunghezza i in una sequenza di N numeri
- Si confronta O_i con il valore teorico Y_i

Test della Lunghezza dei Run

- Il valore atteso di Y_i , per il run test up and down vale

- Per $i \leq N-2$:

$$E(Y_i) = \frac{2}{(i+3)!} [N(i^2 + 3i + 1) - (i^3 + 3i^2 - i - 4)]$$

- Per $i=N-1$:

$$E(Y_i) = \frac{2}{N!}$$

Test della Lunghezza dei Run

- Il valore atteso di Y_i , per il run test intorno alla media vale

$$E(Y_i) = \frac{Nw_i}{E(I)}$$

dove, per $N > 20$

$$E(I) = \frac{n_1}{n_2} + \frac{n_2}{n_1}$$

$$w_i = \binom{n_1}{N}^i \binom{n_2}{N} + \binom{n_1}{N} \binom{n_2}{N}^i$$

Test della Lunghezza dei Run

- Se il valore osservato del numero di run test di lunghezza i è pari a O_i , si esegue il test del chi-quadro, con

$$\chi^2 = \sum_{i=1}^L \frac{[O_i - E(Y_i)]^2}{E(Y_i)}$$

e con $L-1$ gradi di libertà, $L=N-1$ per i run up and down e $L=N$ per i run intorno alla media

Test di Autocorrelazione

- Verifica se c'è correlazione tra i numeri che compaiono in determinate posizioni all'interno di una sequenza
- Si sceglie la distanza m di numeri che intercorrono tra i numeri da analizzare e si crea così la sequenza

$$R_i, R_{i+m}, R_{i+2m}, \dots, R_{i+(M+1)m}$$

- Se sono indipendenti, l'autocorrelazione è nulla

Test di Autocorrelazione

- Uno stimatore dell'autocorrelazione è ρ_{im}

$$\rho_{im} = \frac{1}{M+1} \left[\sum_{k=0}^M R_{i+km} R_{i+(k+1)m} \right] - \frac{1}{4}$$

- Lo stimatore ha deviazione standard pari a

$$\sigma_{im} = \frac{\sqrt{13M+7}}{12(M+1)}$$

Test di Autocorrelazione

- Quindi la variabile

$$Z = \frac{\rho_{im}}{\sigma_{im}}$$

ha una distribuzione normale $N(0,1)$

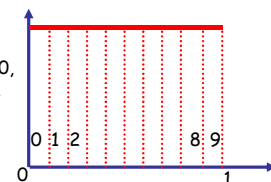
- Con livello di significatività α , non si rifiuta l'ipotesi di indipendenza se

$$-z_{\alpha/2} \leq Z \leq z_{\alpha/2}$$

Test dei Gap

- Si divide il supporto $(0,1)$ in un numero (es. 10) di sotto-intervalli di uguale lunghezza
- Si associa a ogni numero generato una cifra che rappresenta l'intervallo che lo comprende

Es. a 0.023 associo 0,
a 0.876 associo 8, ...



Test dei Gap

- Si considera la sequenza di cifre e se ne studia la correlazione
- Data una cifra n , si ha un *gap* di lunghezza i quando, tra 2 occorrenze della cifra n , intercorrono i cifre diverse da n
- Si confronta, tramite il test di Kolmogorov-Smirnov, la distribuzione della lunghezza dei gap con la distribuzione teorica che si otterrebbe se le cifre fossero scorrelate

Test dei Gap

- Per es., la probabilità di un gap di lunghezza 5 osservando la cifra 3, è dato da

$$P(\text{gap } 5) = P(z_{k+1} \neq 3) P(z_{k+2} \neq 3) \dots P(z_{k+5} \neq 3) P(z_{k+6} = 3) = 0.9^5 \cdot 0.1$$

- La distribuzione teorica è quindi data da

$$P(\text{gap} \leq x) = F(x) = 0.1 \sum_{n=0}^x (0.9)^n = 1 - 0.9^{x+1}$$

Poker Test

- Deriva dal gioco del poker e consiste nell'osservare le cifre a gruppi e studiarne le caratteristiche
- Nel caso di gruppi di 3 cifre, i pattern che si possono osservare sono
 1. Le cifre sono tutte diverse
 2. Le cifre sono tutte uguali
 3. C'è una coppia di numeri uguali
- Si confronta l'occorrenza di questi 3 possibili pattern con quella teorica

Poker Test

- Se i, j, k sono le 3 cifre di un gruppo, la probabilità di 3 cifre diverse tra loro è

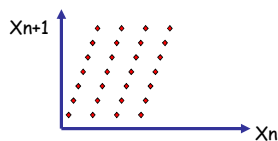
$$P_1 = P(j \neq i) P(k \neq i, k \neq j) = 0.9 \cdot 0.8$$
- La probabilità di 3 cifre uguali tra loro è

$$P_2 = P(j=i) P(k=j) = 0.1 \cdot 0.1$$
- La probabilità di una coppia è

$$P_3 = 1 - P_1 - P_2 = \binom{3}{2} 0.1 \cdot 0.9$$

Spectral Test

- Valuta quanto densamente le tuple (Z_1, Z_2, \dots, Z_t) riempiono uno spazio t -dimensionale
- Per es. i generatori congruenti lineari generano punti che a coppie riempiono il piano lungo un numero finito di linee



Spectral Test

- In uno spazio t -dimensionale, i generatori congruenti lineari generano punti su piani $(t-1)$ -dimensionali paralleli
- Maggiore è la distanza tra questi piani, peggiori sono le prestazioni del generatore