Testing a Random Number Generator: formal properties and automotive application

Federico Mattioli

Alma Mater Studiorum Università di Bologna

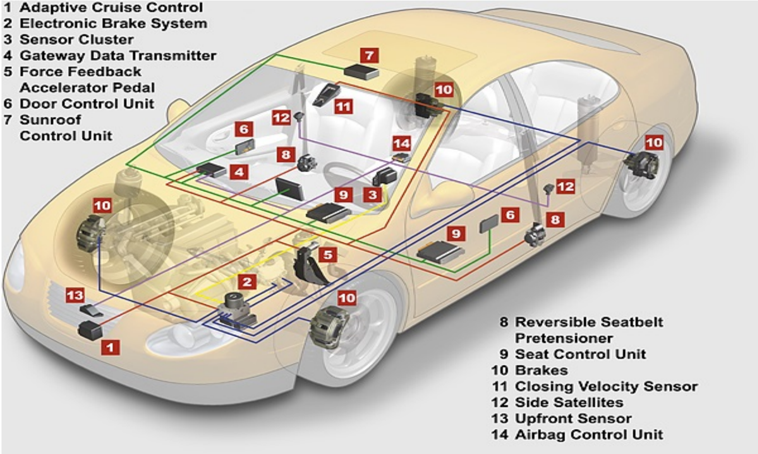
29 marzo 2019

Relatore: Chiar.ma Prof.ssa Giovanna Citti
Correlatore: Chiar.ma Dott.ssa Elisa Bragaglia

Indice

Il sistema di ECU

Il funzionamento di un autoveicolo moderno è garantito da sistemi elettronici: le centraline (Electronic Control Unit: ECU).



Random Number Generators

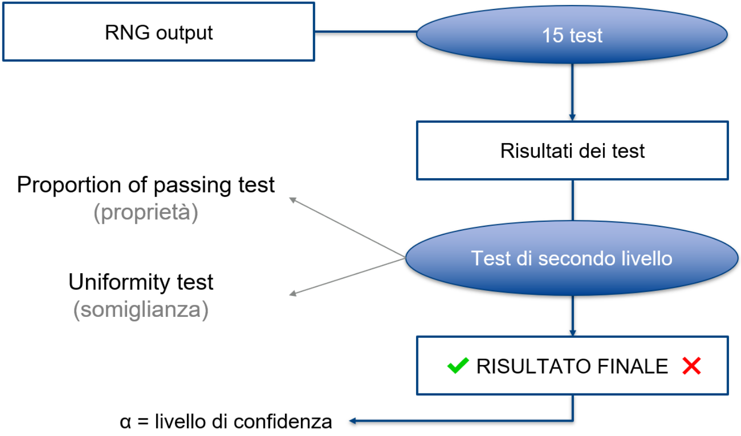
Principio di Kerckhoff

Un sistema crittografico deve rimanere sicuro anche se è completamente noto, ad accezione della chiave.

Le sequenze di numeri casuali vengono generate da sistemi detti Random Number Generator (RNG):

- Pseudo Random Number Generator (PRNG);
- True Random Number Generator (TRNG);
- Hybrid Random Number Generator (HRNG).

Metodo generale



15 test statistici

- National Institute of Standards and Technology (NIST);
- H_0, ipotesi nulla: la sequenza è casuale;
- T: statistica teorica alla base del test;
- $P\text{-}value = P(T > T(obs)|H_0)$: probabilità che una sequenza sia meno casuale di quella osservata;
- complessità crescente:
  - numero di 0 e 1;
  - ricorrenze di pattern;
  - complessità algoritmica;
  - entropia;
  - passeggiata aleatoria.

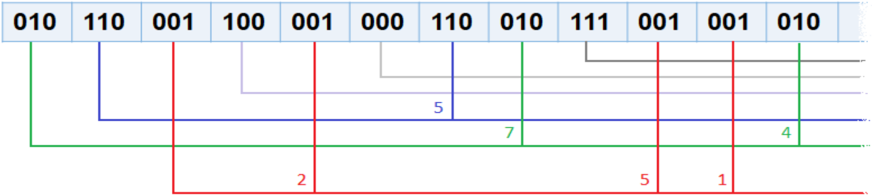
Maurer's universal statistical test

Teorema (Primo teorema di Shannon)

Sia $X = \{X_n\}_{n \in I}$ un processo stocastico con entropia $H(X)$. La lunghezza media $L(C)$ di ogni codice istantaneo è t.c.

$$\frac{1}{n} L(C) \xrightarrow{n \to \infty} H(X).$$

$$T_n = \sum log_2(\text{dist. pattern uguali})$$



Teorema (Teorema del limite centrale)

Sia $\{X_n\}_{n\in I}$ *un processo stocastico di v.a. i.i.d. con media* μ *e varianza* σ^2. *Allora la v.a.*

$$T_n = \frac{X_1 + \cdots + X_n - n\mu}{\sqrt{n}\sigma}$$

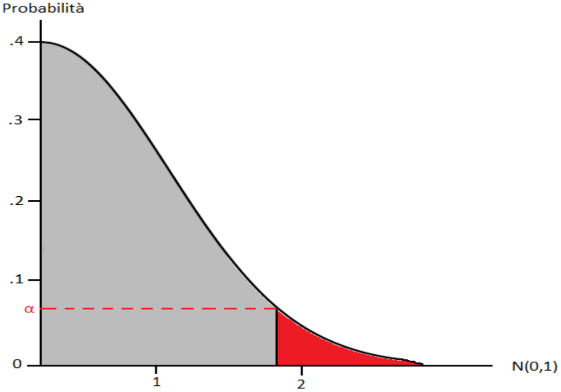
converge in legge alla distribuzione normale standard, per n che tende ad infinito.

Per effettuare il test è necessario conoscere:

$$\mu = 2^{-L}\sum_{i=1}^{\infty}(1-2^{-L})^{i-1} log_2 i,$$

$$\sigma = c(L,K)\sqrt{\frac{2^{-L}\sum_{i=1}^{\infty}(1-2^{-L})^{i-1}(log_2 i)^2 - \mu^2}{K}}.$$

$$P\text{-}value = P(T > T(obs)|H_0) = erfc\left(\left|\frac{T_n - \mu}{\sqrt{2}\sigma}\right|\right)$$



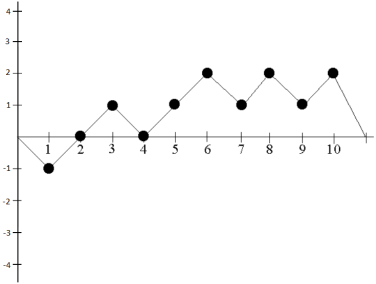
Random excursions test

Definizione (Passeggiata aleatoria)

Sia $X = \{X_n\}_{n \in I}$ *un processo stocastico di v.a. i.i.d.. Una passeggiata aleatoria è una sequenza stocastica* $\{S_n\}_{n \in I}$ *definita da*

$$S_n = \sum_{k=1}^{n} X_k \qquad con \;\; S_0 = 0.$$

Il test analizza il numero di visite degli stati $x = -4, \ldots, 4$ per ogni ciclo della passeggiata.



Per ogni stato x della passeggiata aleatoria si calcolano le probabilità teoriche π_i attraverso

Teorema (Probabilità di visita dello stato x)

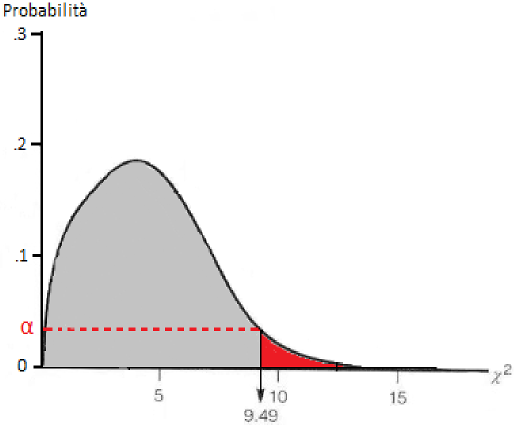
Le probabilità di vistare lo stato $x \neq 0$ un numero i di volte sono date da:

$$\pi_i(x) = \begin{cases} 1 - \frac{1}{2|x|} & \text{per } i = 0, \\ \frac{1}{4x^2}\left(1 - \frac{1}{2|x|}\right)^{i-1} & \text{per } i > 0. \end{cases}$$

Probabilità teoriche π_i e frequenze osservate v_i vengono confrontate attraverso:

$$\chi^2(x) = \sum_{i=0}^{5} \frac{(v_i(x) - J\pi_i(x))^2}{J\pi_i(x)}.$$

$$P\text{-}value(x) = P(T > T(obs)|H_0)(x) = igamc\left(\frac{5}{2}, \frac{\chi^2(x)}{2}\right)$$



Proprietà di un RNG: test di secondo livello

- Una sequenza passa un singolo test se *P-value* $> \alpha$.
- Ogni test fornisce:
  - risultato;
  - *P-value*.

Obiettivo

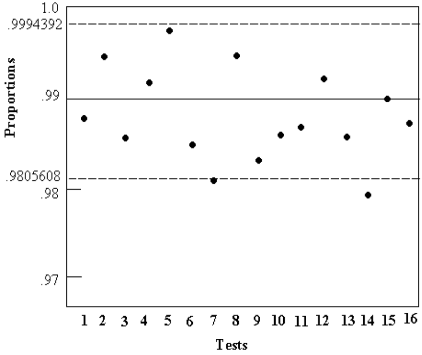
Valutare il buon funzionamento del Random Number Generator.

- Numero di sequenze da testare: $k \geq 100$;
- Test di secondo livello:
  - proportion of passing test;
  - uniformity test.

Test di secondo livello: proportion of passing test

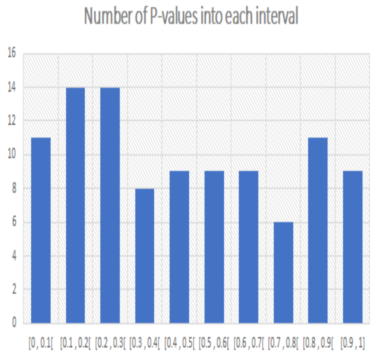
La proporzione di sequenze che passa il singolo test, deve essere contenuta nell'intervallo:

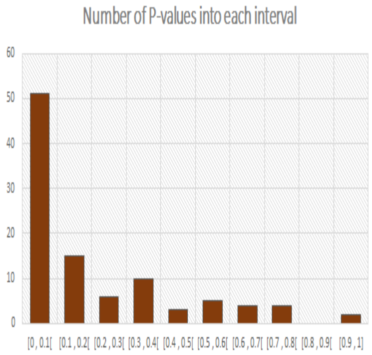
$$(1-\alpha) \pm c\sqrt{\frac{\alpha(1-\alpha)}{k}}.$$



Test di secondo livello: uniformity test

Distribuendo i *P-value* ottenuti da ogni test in classi, si verifica che questi siano vicini alla distribuzione uniforme:





Grazie per l'attenzione!