Probabilità e Numeri Casuali

Gregorio D'Agostino

10 Maggio 2021

Spazio di probabilità

Numeri Casuali

Proprietà dei generatori congruenziali

Concetto di Probabilità

- Gli appellativi della probabilità sono molteplici: percepita, soggettiva etc. In generale si intende farmalizzare un concetto per la valutazione di eventi (non necessariamente la loro frequenza). Qui useremo un trattamento puramente matematico prescindendo dalle interpretazioni.

Esistono in letteratura diverse definizioni. Qui si seguirà il metodo assiomatico secondo la scuola di Kolmogorov.

Andrey Kolmogorov nato il 25 aprile1903 a Tambov, Russia e morto il 20 ottobre October 20, 1987 a Mosca, Russia.

Concetto di Probabilità

- Gli appellativi della probabilità sono molteplici: percepita, soggettiva etc. In generale si intende farmalizzare un concetto per la valutazione di eventi (non necessariamente la loro frequenza). Qui useremo un trattamento puramente matematico prescindendo dalle interpretazioni.

Esistono in letteratura diverse definizioni. Qui si seguirà il metodo assiomatico secondo la scuola di Kolmogorov.

Andrey Kolmogorov nato il 25 aprile1903 a Tambov, Russia e morto il 20 ottobre October 20, 1987 a Mosca, Russia.

- Altre definizioni sono basate su ipotesi di convergenza delle frequenze (in parte tautologiche) o su principi generali (De Finetti).

Concetto di Probabilità

- Gli appellativi della probabilità sono molteplici: percepita, soggettiva etc. In generale si intende farmalizzare un concetto per la valutazione di eventi (non necessariamente la loro frequenza). Qui useremo un trattamento puramente matematico prescindendo dalle interpretazioni.

Esistono in letteratura diverse definizioni. Qui si seguirà il metodo assiomatico secondo la scuola di Kolmogorov.

Andrey Kolmogorov nato il 25 aprile1903 a Tambov, Russia e morto il 20 ottobre October 20, 1987 a Mosca, Russia.

- Altre definizioni sono basate su ipotesi di convergenza delle frequenze (in parte tautologiche) o su principi generali (De Finetti).
- Tutte le definizioni portano a teorie equivalenti.

Spazio di Probabilità

- Si definisce una terna composta da uno "Spazio degli eventi elementari" Ω, l'algebra degli eventi composti misurabili $\mathcal{F}$ e la misura di "Probabilità" $\mathcal{P}$:

$$S \stackrel{def}{=} (\Omega, \mathcal{F}, \mathcal{P}) .$$

Spazio di Probabilità

- Si definisce una terna composta da uno "Spazio degli eventi elementari" Ω, l'algebra degli eventi composti misurabili $\mathcal{F}$ e la misura di "Probabilità" $\mathcal{P}$:

$$S \stackrel{def}{=} (\Omega, \mathcal{F}, \mathcal{P}) .$$

- Lo spazio degli eventi elementari è uno spazio che rappresenta l'astrazione delle possibili situazioni, dette eventi, che si possono presentare. In genere questi spazi sono definiti da numeri o più frequentemente ogni evento è definito da una collezione di numeri.

Spazio di Probabilità

- Si definisce una terna composta da uno "Spazio degli eventi elementari" Ω, l'algebra degli eventi composti misurabili $\mathcal{F}$ e la misura di "Probabilità" $\mathcal{P}$:

$$S \stackrel{def}{=} (\Omega, \mathcal{F}, \mathcal{P}) .$$

- Lo spazio degli eventi elementari è uno spazio che rappresenta l'astrazione delle possibili situazioni, dette eventi, che si possono presentare. In genere questi spazi sono definiti da numeri o più frequentemente ogni evento è definito da una collezione di numeri.
- Lo spazio degli eventi può essere discreto (corrispondenza biunivoca con i naturali), finito o numerabile; o più complesso (continuo se in corrispondenza con i numeri reali o ancora più complesso.)
  Esempio di spazio di eventi discreto: la sequenza del numero di pazienti in un ospedale con 30 posti letto. Praticamente sono tutte le possibili sequenze di numeri compresi tra 0 e 30.

Spazio degli eventi elementari

- Esempi di spazio di eventi continuo: la traiettoria di una cometa $\vec{r}(t)$. Oppure il livello del suono in una stanza nel tempo $x(t)$. In questo caso ogni evento elementare è una funzione del tempo.

Spazio degli eventi elementari

- Esempi di spazio di eventi continuo: la traiettoria di una cometa $\vec{r}(t)$. Oppure il livello del suono in una stanza nel tempo $x(t)$. In questo caso ogni evento elementare è una funzione del tempo.
- Esempi ancora più complessi: l'evoluzione nel tempo di una membrana. In questo caso bisogna dare una funzione $z = f(x, y, t)$ per ogni istante.

Spazio degli eventi elementari

- Esempi di spazio di eventi continuo: la traiettoria di una cometa $\vec{r}(t)$. Oppure il livello del suono in una stanza nel tempo $x(t)$. In questo caso ogni evento elementare è una funzione del tempo.
- Esempi ancora più complessi: l'evoluzione nel tempo di una membrana. In questo caso bisogna dare una funzione $z = f(x, y, t)$ per ogni istante.
- Altri esempi: Le configurazioni di un sistema complesso (come una infrastruttra ospedaliera o informatica nel tempo). In questo caso bisogna conosce molte funzioni.

Spazio degli eventi elementari

- Esempi di spazio di eventi continuo: la traiettoria di una cometa $\vec{r}(t)$. Oppure il livello del suono in una stanza nel tempo $x(t)$. In questo caso ogni evento elementare è una funzione del tempo.
- Esempi ancora più complessi: l'evoluzione nel tempo di una membrana. In questo caso bisogna dare una funzione $z = f(x, y, t)$ per ogni istante.
- Altri esempi: Le configurazioni di un sistema complesso (come una infrastruttra ospedaliera o informatica nel tempo). In questo caso bisogna conosce molte funzioni.
- Per esigenze di tempo ci focalizzeremo sugli spazi discreti.

Spazio degli eventi compositi misurabili

- In molti casi non ci interessa il dettagli del sistema, ma solo se verifica certe proprietà o condizioni. Ad esempio nel caso dei degenti di una corsia possiamo essere interessati solo al fatto se sono minori di 20 e maggiori di 5. Oppure se sono in numero pari o dispari. Questi condizioni vengono verificate per collezioni di eventi elementari, ovvero per insiemi di eventi elementari. Gli insiemi di eventi elementari vengono detti eventi compositi.

Spazio degli eventi compositi misurabili

- In molti casi non ci interessa il dettagli del sistema, ma solo se verifica certe proprietà o condizioni. Ad esempio nel caso dei degenti di una corsia possiamo essere interessati solo al fatto se sono minori di 20 e maggiori di 5. Oppure se sono in numero pari o dispari. Questi condizioni vengono verificate per collezioni di eventi elementari, ovvero per insiemi di eventi elementari. Gli insiemi di eventi elementari vengono detti eventi compositi.
- I sottoinsiemi dello spazio Ω formano l'insieme degli eventi compositi. Questo insieme forma un'algebra di insiemi (abbiamo già visto).

Spazio degli eventi compositi misurabili

- In molti casi non ci interessa il dettagli del sistema, ma solo se verifica certe proprietà o condizioni. Ad esempio nel caso dei degenti di una corsia possiamo essere interessati solo al fatto se sono minori di 20 e maggiori di 5. Oppure se sono in numero pari o dispari. Questi condizioni vengono verificate per collezioni di eventi elementari, ovvero per insiemi di eventi elementari. Gli insiemi di eventi elementari vengono detti eventi compositi.
- I sottoinsiemi dello spazio Ω formano l'insieme degli eventi compositi. Questo insieme forma un'algebra di insiemi (abbiamo già visto).
- Ma non tutti gli eventi compositi sono interessanti o rilevanti. L'algebra generata (per intersezione ed unione) dagli eventi interessanti o rilevanti si chiama "algebra degli eventi compositi misurabili". Questa ($\mathcal{F}$) è l'unica algebra che ci interessa. Vedremo cosa significa il termine misurabile.

Spazio degli eventi compositi misurabili - cont

- Per essere un'algebra deve essere chiusa rispetto all'unione e l'intersezione di insiemi e devono valere le due proprietà distribuitive.

Spazio degli eventi compositi misurabili - cont

- Per essere un'algebra deve essere chiusa rispetto all'unione e l'intersezione di insiemi e devono valere le due proprietà distribuitive.
- L'insieme vuoto $\emptyset$ e l'insieme Ω devono appartenere sempre a $\mathcal{F}$. Rappresentano gli elementi neutri rispetto all'unione ed all'intersezione.

Probabilità o misura di probabilità

- La probabilità è una funzione definita sullo spazio $\mathcal{F}$ (NON su Ω!):

$$\mathcal{P} : \mathcal{F} \to \mathbb{R};$$

che gode delle seguenti proprietà:

Probabilità o misura di probabilità

- La probabilità è una funzione definita sullo spazio $\mathcal{F}$ (NON su Ω!):

$$\mathcal{P} : \mathcal{F} \to \mathbb{R};$$

che gode delle seguenti proprietà:

- Definizione in segno:

$$\forall A \in \mathcal{F} : p(A) \geq 0;$$

Probabilità o misura di probabilità

- La probabilità è una funzione definita sullo spazio $\mathcal{F}$ (NON su Ω!):

$$\mathcal{P} : \mathcal{F} \to \mathbb{R};$$

che gode delle seguenti proprietà:

- Definizione in segno:

$$\forall A \in \mathcal{F} : p(A) \geq 0;$$

- Normalizzazione:

$$\forall A \in \mathcal{F} : p(A) \leq 1;\ p(\Omega) = 1;$$

Probabilità o misura di probabilità

- La probabilità è una funzione definita sullo spazio $\mathcal{F}$ (NON su Ω!):

$$\mathcal{P} : \mathcal{F} \to \mathbb{R};$$

che gode delle seguenti proprietà:

  - Definizione in segno:

$$\forall A \in \mathcal{F} : p(A) \geq 0;$$

  - Normalizzazione:

$$\forall A \in \mathcal{F} : p(A) \leq 1;\ p(\Omega) = 1;$$

  - Additività per eventi incompatibili (disgiunti)

$$\forall A, B \in \mathcal{F} : A \cap B = \emptyset \Rightarrow p(A \cup B) = p(A) + p(B).$$

Significato di probabilità e additività

- Il significato della probabilità è assimilabile ad una stima, una valutazione (una misura dal punto di vista matematico). Per ogni evento siamo in grado di darne una estensione , una gradualità. Tale estensione può essere intesa come ad esempio il gradimento o l'importanza di un evento. Nel caso più comune la frequenza ipotizzata.

Significato di probabilità e additività

- Il significato della probabilità è assimilabile ad una stima, una valutazione (una misura dal punto di vista matematico). Per ogni evento siamo in grado di darne una estensione , una gradualità. Tale estensione può essere intesa come ad esempio il gradimento o l'importanza di un evento. Nel caso più comune la frequenza ipotizzata.
- L'additività significa che se due eventi (compositi) non possono verificarsi simultaneamente allora la loro probabilità è la somma delle probabilità. Quando definiamo stima della bellezza ad esempio, affinché sia una probabilità deve essere decomponibile: un punteggio per il colore degli occhi, un punteggio per il naso, un punteggio per l'altezza, il peso etc. Nella vita reale la nostra definizione di bellezza non è additiva perché alcuni elementi non si sommano. I capelli rossi ricci possono non piacere, ma possono piacere lisci. Una donna alta ma esile può risultare più piacevo di una alta, ma giunonica. Un uomo calvo, ma palestrato può suscitare del fascino etc

Additività e sigma-additività

- La sigma-additività è l'additività per un insieme numerabile di eventi disgiunti:

$$\forall e_1, \ldots, e_n \in \mathcal{F} : e_i \cap e_j = \emptyset \Rightarrow \lim_{n \to \infty} p\left(\bigcup_{i=1,n} e_i\right) = \sum_{i=1}^{\infty} p(e_i).$$

Si tratta di una ipotesi tecnica necessaria per evitare paradossi di insiemi la cui probabilità tende a zero e la cui unione invece non ha probabilità nulla.

Eventi complementari

- Due eventi si dicono complementari se la loro unione coincide con Ω.

Eventi complementari

- Due eventi si dicono complementari se la loro unione coincide con Ω.
- Il complementare di un evento (composito) A si indica con il simbolo $\bar{A}$

$$\bar{A} \stackrel{def}{=} \{e : \ e \notin A\}.$$

Eventi complementari

- Due eventi si dicono complementari se la loro unione coincide con Ω.
- Il complementare di un evento (composito) A si indica con il simbolo $\bar{A}$

$$\bar{A} \stackrel{def}{=} \{e : \ e \notin A\}.$$

- Le relazioni con l'unione e l'intersezione sono ovvie:

$$\overline{A \cap B} = \bar{A} \cup \bar{B};$$

$$\overline{A \cup B} = \bar{A} \cap \bar{B}.$$

Probabilità condizionata

- Un insieme si dice a misura nulla se la sua probabilità è zero.

Probabilità condizionata

- Un insieme si dice a misura nulla se la sua probabilità è zero.
- Un insieme B a misura non nulla ($p(B) \neq 0$) definisce una nuova probabilità detta condizionata:

$$p(A|B) \stackrel{def}{=} \frac{p(A \cap B)}{p(B)}.$$

Probabilità condizionata

- Un insieme si dice a misura nulla se la sua probabilità è zero.
- Un insieme B a misura non nulla ($p(B) \neq 0$) definisce una nuova probabilità detta condizionata:

$$p(A|B) \stackrel{def}{=} \frac{p(A \cap B)}{p(B)}.$$

- Gli insiemi $A \cap B$ formano un'algebra di insiemi misurabili (sottoinsieme di $\mathcal{F}$).

Probabilità condizionata

- Un insieme si dice a misura nulla se la sua probabilità è zero.
- Un insieme B a misura non nulla ($p(B) \neq 0$) definisce una nuova probabilità detta condizionata:

$$p(A|B) \stackrel{def}{=} \frac{p(A \cap B)}{p(B)}.$$

- Gli insiemi $A \cap B$ formano un'algebra di insiemi misurabili (sottoinsieme di $\mathcal{F}$).
- La nuova definizione soddisfa le condizioni di definitezza in segno, normalizzazione e sigma-additività.

Esempio classico di probabilità condizionata

- Negli anni sessanta in USA esisteva un gioco alla tv in cui dentro una scatosa su tre c'era un premio.

Esempio classico di probabilità condizionata

- Negli anni sessanta in USA esisteva un gioco alla tv in cui dentro una scatosa su tre c'era un premio.
- Un giocatore doveva scegliere alla cieca una scatola.

Esempio classico di probabilità condizionata

- Negli anni sessanta in USA esisteva un gioco alla tv in cui dentro una scatosa su tre c'era un premio.
- Un giocatore doveva scegliere alla cieca una scatola.
- Il presentatore mostra che una delle altre due scatole è vuota. Poi chiede al giocatore se vuole scambiare le scatole. Cosa fareste?

Esempio classico di probabilità condizionata

- Negli anni sessanta in USA esisteva un gioco alla tv in cui dentro una scatosa su tre c'era un premio.
- Un giocatore doveva scegliere alla cieca una scatola.
- Il presentatore mostra che una delle altre due scatole è vuota. Poi chiede al giocatore se vuole scambiare le scatole. Cosa fareste?
- Conviene cambiare. Il calcolo della probabilità condizionata lo dimostra. A="Vince la scatola iniziale"; B="Vince una delle due scatole del presentatore"; C="Una delle due scatole del presentatore è vuota". Per la scatola del giocatore:

$$p(A|C) = \frac{p(A \cap C)}{p(C)} = \frac{1/3}{1};$$

Esempio classico di probabilità condizionata

- Negli anni sessanta in USA esisteva un gioco alla tv in cui dentro una scatosa su tre c'era un premio.
- Un giocatore doveva scegliere alla cieca una scatola.
- Il presentatore mostra che una delle altre due scatole è vuota. Poi chiede al giocatore se vuole scambiare le scatole. Cosa fareste?
- Conviene cambiare. Il calcolo della probabilità condizionata lo dimostra. A="Vince la scatola iniziale"; B="Vince una delle due scatole del presentatore"; C="Una delle due scatole del presentatore è vuota". Per la scatola del giocatore:

$$p(A|C) = \frac{p(A \cap C)}{p(C)} = \frac{1/3}{1};$$

- Per la scatola del presentatore

$$p(B|C) = \frac{p(B \cap C)}{p(C)} = \frac{2/3}{1};$$

Definizioni

- Una variabile stocastica ξ è una funzione dello spazio degli eventi elementari (non in $\mathcal{F}$!):

$$\forall e \in \Omega : \xi = f(e);$$

per la quale la diseguaglianza $\xi < x$ ha senso e definisce insiemi misurabili U_x.

$$U_x \stackrel{def}{=} \{e : \xi = f(e) < x\} \in \mathcal{F}.$$

Definizioni

- Una variabile stocastica ξ è una funzione dello spazio degli eventi elementari (non in $\mathcal{F}$!):

$$\forall e \in \Omega : \xi = f(e);$$

per la quale la diseguaglianza $\xi < x$ ha senso e definisce insiemi misurabili U_x.

$$U_x \stackrel{def}{=} \{e : \xi = f(e) < x\} \in \mathcal{F}.$$

- Quando il co-dominio della funzione è un sottoinsieme dei reali la variabile si dice reale. Quando il co-dominio è uno spazio discreto la variabile si dice discreta.

Definizioni

- Una variabile stocastica ξ è una funzione dello spazio degli eventi elementari (non in $\mathcal{F}$!):

$$\forall e \in \Omega : \xi = f(e);$$

per la quale la diseguaglianza $\xi < x$ ha senso e definisce insiemi misurabili U_x.

$$U_x \stackrel{def}{=} \{e : \xi = f(e) < x\} \in \mathcal{F}.$$

- Quando il co-dominio della funzione è un sottoinsieme dei reali la variabile si dice reale. Quando il co-dominio è uno spazio discreto la variabile si dice discreta.
- La funzione di probablità è definita come la probabilità dei boreliani della variabile stocastica.

$$F(x) \stackrel{def}{=} \mathcal{P}(U_x).$$

Definizioni

- Una variabile stocastica ξ è una funzione dello spazio degli eventi elementari (non in $\mathcal{F}$!):

$$\forall e \in \Omega : \xi = f(e);$$

per la quale la diseguaglianza $\xi < x$ ha senso e definisce insiemi misurabili U_x.

$$U_x \stackrel{def}{=} \{e : \xi = f(e) < x\} \in \mathcal{F}.$$

- Quando il co-dominio della funzione è un sottoinsieme dei reali la variabile si dice reale. Quando il co-dominio è uno spazio discreto la variabile si dice discreta.
- La funzione di probablità è definita come la probabilità dei boreliani della variabile stocastica.

$$F(x) \stackrel{def}{=} \mathcal{P}(U_x).$$

- Definizione in segno e normalizzazione: $0 \leq F(x) \leq 1$.

Variabili Indipendenti

- Due eventi si dicono indipendenti se la probabilità della loro intersezione è uguale al prodotto delle loro probabilità:

$$p(A \cap B) = p(A) \cdot p(B).$$

Variabili Indipendenti

- Due eventi si dicono indipendenti se la probabilità della loro intersezione è uguale al prodotto delle loro probabilità:

$$p(A \cap B) = p(A) \cdot p(B).$$

- Alternativamente si può dire che la probabilità non cambia se viene condizionata dall'altro evento:

$$p(A|B) = \frac{p(A \cap B)}{p(B)} = \frac{p(A) \cdot p(B)}{p(B)} = p(A).$$

Variabili Indipendenti

- Due eventi si dicono indipendenti se la probabilità della loro intersezione è uguale al prodotto delle loro probabilità:

$$p(A \cap B) = p(A) \cdot p(B).$$

- Alternativamente si può dire che la probabilità non cambia se viene condizionata dall'altro evento:

$$p(A|B) = \frac{p(A \cap B)}{p(B)} = \frac{p(A) \cdot p(B)}{p(B)} = p(A).$$

- Due variabili aleatorie (ξ ed η) si dicono indipendenti se tutti lo sono tutti i loro eventi misurabili (boreliani).
$U_X = \{\xi < x\}$, $V_y = \{\eta < y\}$.

$$p(U_x \cap V_y) = p(U_x) \cdot p(V_y) = F_\xi(x) \cdot F_\eta(y).$$

quando esistono anche le probabilità di assumere dei valori specifici sono indipendenti:

$$\rho_{\xi\eta}(x, y) \stackrel{def}{=} p(\xi = x, \eta = y) = p(\xi = x) \cdot p(\eta = y) = \rho_\xi(x)\rho_\eta(y).$$

Variabili discrete uniformi

- Per le variabili discrete gli eventi $A_x = \{\xi = x\}$ sono misurabili. I valori ammissibili di x (co-dominio) sono discreti e dunque indicizzabili ($x \in \{x^1, x^2, \ldots, x^M\}$. Per ogni valore x^i si può costruire l'evento (composito) in cui la variabile assume tale valore:

$$A_{x^i} = U_{x^{i+1}} \cap \overline{U_{x^i}} = (\{\xi < x^{i+1}\}) \cap (\{\xi \geq x^i\}).$$

Variabili discrete uniformi

- Per le variabili discrete gli eventi $A_x = \{\xi = x\}$ sono misurabili. I valori ammissibili di x (co-dominio) sono discreti e dunque indicizzabili ($x \in \{x^1, x^2, \ldots, x^M\}$. Per ogni valore x^i si può costruire l'evento (composito) in cui la variabile assume tale valore:

$$A_{x^i} = U_{x^{i+1}} \cap \overline{U_{x^i}} = (\{\xi < x^{i+1}\}) \cap (\{\xi \geq x^i\}).$$

- La probabilità ρ_i che la variabile assuma un valore si calcola facilmente a partire dalla funzione di probabilità:

$$\rho_i \stackrel{def}{=} p(\xi = x^i) = p(A_{x^i}) = p(U_{x^{i+1}} \cap \overline{U_{x^i}}) = F(x^{i+1}) - F(x^i);$$

in cui si è supposto che le x^i siano ordinate: $x^{i+1} > x^i$.

Variabili discrete uniformi

- Per le variabili discrete gli eventi $A_x = \{\xi = x\}$ sono misurabili. I valori ammissibili di x (co-dominio) sono discreti e dunque indicizzabili ($x \in \{x^1, x^2, \ldots, x^M\}$. Per ogni valore x^i si può costruire l'evento (composito) in cui la variabile assume tale valore:

$$A_{x^i} = U_{x^{i+1}} \cap \overline{U_{x^i}} = (\{\xi < x^{i+1}\}) \cap (\{\xi \geq x^i\}).$$

- La probabilità ρ_i che la variabile assuma un valore si calcola facilmente a partire dalla funzione di probabilità:

$$\rho_i \stackrel{def}{=} p(\xi = x^i) = p(A_{x^i}) = p(U_{x^{i+1}} \cap \overline{U_{x^i}}) = F(x^{i+1}) - F(x^i);$$

  in cui si è supposto che le x^i siano ordinate: $x^{i+1} > x^i$.
- Una variabile possiede una distribuzione uniforme se $p(A_x)$ non dipende da x. Se vi sono N valori possibili:

$$\forall i : \rho_i = p(A_{x^i}) = \frac{1}{N}.$$

Probabilità degli eventi delle variabili discrete uniformi

- Una variabile aleatoria discreta uniforme non può assumere infiniti valori, perchè sarebbero tutti a misura nulla e la loro somma dovrebbe dare l'unità:

$$\forall i : \rho_i = p(\xi = x^i) = p(A_{x^i}) = \frac{1}{N} \to 0.$$

Probabilità degli eventi delle variabili discrete uniformi

- Una variabile aleatoria discreta uniforme non può assumere infiniti valori, perchè sarebbero tutti a misura nulla e la loro somma dovrebbe dare l'unità:

$$\forall i : \rho_i = p(\xi = x^i) = p(A_{x^i}) = \frac{1}{N} \to 0.$$

- Invece una variabile aleatoria continua uniforme assume sempre infiniti valori, ma in generale l'assunzione di un valore specifico non è un evento misurabile o è un evento a misura nulla.

Definizioni - cont

- Una catena stocastica è una successione di variabili stocastiche ξ_i ordinate da un indice. L'indice definisce la cronologia. Malgrado la denominazione, l'indice non corrisponde necessariamente ad un ordine temporale.

Definizioni - cont

- Una catena stocastica è una successione di variabili stocastiche ξ_i ordinate da un indice. L'indice definisce la cronologia. Malgrado la denominazione, l'indice non corrisponde necessariamente ad un ordine temporale.
- La funzione di probabilità della catena stocastica è definita analogamente al caso della singola variabile. Per gli intervalli di tempo finiti ($0 \leq i \leq n$), si definiscono le funzioni ad n punti:

$$\Phi_{\xi_1 \xi_2 \ldots \xi_n}(x_1, x_2, \ldots, x_n) \stackrel{def}{=} \mathcal{P}(\xi_1 \in U_{x_1}, \xi_2 \in U_{x_2}, \cdots, \xi_n \in U_{x_n}).$$

Definizioni - cont

- Una catena stocastica è una successione di variabili stocastiche ξ_i ordinate da un indice. L'indice definisce la cronologia. Malgrado la denominazione, l'indice non corrisponde necessariamente ad un ordine temporale.
- La funzione di probabilità della catena stocastica è definita analogamente al caso della singola variabile. Per gli intervalli di tempo finiti ($0 \leq i \leq n$), si definiscono le funzioni ad n punti:

$$\Phi_{\xi_1 \xi_2 \ldots \xi_n}(x_1, x_2, \ldots, x_n) \stackrel{def}{=} \mathcal{P}(\xi_1 \in U_{x_1}, \xi_2 \in U_{x_2}, \cdots, \xi_n \in U_{x_n}).$$

- Ad esempio la funzione a due punti (detto propagatore):

$$\Phi_{\xi_{i_1} \xi_{i_2}}(x, y) \stackrel{def}{=} \mathcal{P}(\xi_{i_1} \in U_x, \xi_{i_2} \in U_y).$$

Definizioni - cont

- Una catena stocastica si dice stazionaria se traslando gli indici le sue funzioni ad n punti non cambiano:

$$\Phi_{\xi_1\xi_2\ldots\xi_n}(x_1, x_2, \ldots, x_n) = \Phi_{\xi_{1+\tau}\xi_{2+\tau}\ldots\xi_{n+\tau}}(x_1, x_2, \ldots, x_n);$$

quindi si può scrivere:

$$\Phi_{\xi_1\xi_2\ldots\xi_n}(x_1, x_2, \ldots, x_n) \stackrel{def}{=} \Phi(x_1, x_2, \ldots, x_n).$$

Generatori di Variabili casuali o numeri aleatori

- Un generatore di numeri aleatori è un sistema che genera dei numeri in un intervallo in modo non deterministico. I numeri generati costituiscono una catena stocastica $(\xi_1 \xi_2 \ldots \xi_n \ldots)$.

Generatori di Variabili casuali o numeri aleatori

- Un generatore di numeri aleatori è un sistema che genera dei numeri in un intervallo in modo non deterministico. I numeri generati costituiscono una catena stocastica $(\xi_1 \xi_2 \ldots \xi_n \ldots)$.
- Un generatore di numeri casuali è un sistema che genera una sequenza di variabili stocastiche numeriche che devono Soddisfare le seguenti proprietà:

Generatori di Variabili casuali o numeri aleatori

- Un generatore di numeri aleatori è un sistema che genera dei numeri in un intervallo in modo non deterministico. I numeri generati costituiscono una catena stocastica $(\xi_1 \xi_2 \ldots \xi_n \ldots)$.
- Un generatore di numeri casuali è un sistema che genera una sequenza di variabili stocastiche numeriche che devono Soddisfare le seguenti proprietà:
  - Stazionarietà della catena

Generatori di Variabili casuali o numeri aleatori

- Un generatore di numeri aleatori è un sistema che genera dei numeri in un intervallo in modo non deterministico. I numeri generati costituiscono una catena stocastica $(\xi_1 \xi_2 \ldots \xi_n \ldots)$.
- Un generatore di numeri casuali è un sistema che genera una sequenza di variabili stocastiche numeriche che devono Soddisfare le seguenti proprietà:
  - Stazionarietà della catena
  - Indipendenza della variabili ξ_i

Generatori di Variabili casuali o numeri aleatori

- Un generatore di numeri aleatori è un sistema che genera dei numeri in un intervallo in modo non deterministico. I numeri generati costituiscono una catena stocastica $(\xi_1 \xi_2 \ldots \xi_n \ldots)$.
- Un generatore di numeri casuali è un sistema che genera una sequenza di variabili stocastiche numeriche che devono Soddisfare le seguenti proprietà:
  - Stazionarietà della catena
  - Indipendenza della variabili ξ_i
  - Tutte le variabili aleatorie ξ_i sono uguali, cioè possono assumere gli stessi valori con le stesse probabilità.

Generatori di Variabili casuali o numeri aleatori

- Un generatore di numeri aleatori è un sistema che genera dei numeri in un intervallo in modo non deterministico. I numeri generati costituiscono una catena stocastica $(\xi_1 \xi_2 \ldots \xi_n \ldots)$.
- Un generatore di numeri casuali è un sistema che genera una sequenza di variabili stocastiche numeriche che devono Soddisfare le seguenti proprietà:
  - Stazionarietà della catena
  - Indipendenza della variabili ξ_i
  - Tutte le variabili aleatorie ξ_i sono uguali, cioè possono assumere gli stessi valori con le stesse probabilità.
  - Distribuzione uniforme di tutte le variabili ξ_i.

Generatori di Variabili Casuali uniformi "True Random Variable Generators"

- Esistono fenomeni realmente casuali. Tipicamente quando si utilizzano degli strumenti al di là dei limiti imposti dalla precisione dello strumento le ultime cifre sono casuali.

Generatori di Variabili Casuali uniformi "True Random Variable Generators"

- Esistono fenomeni realmente casuali. Tipicamente quando si utilizzano degli strumenti al di là dei limiti imposti dalla precisione dello strumento le ultime cifre sono casuali.
- Esistono siti (ad esempio www.random.org) che misurando le fluttuazioni dell'atmosfera forniscono dei numeri veramente casuali.

Generatori di Variabili Casuali uniformi "True Random Variable Generators"

- Esistono fenomeni realmente casuali. Tipicamente quando si utilizzano degli strumenti al di là dei limiti imposti dalla precisione dello strumento le ultime cifre sono casuali.
- Esistono siti (ad esempio www.random.org) che misurando le fluttuazioni dell'atmosfera forniscono dei numeri veramente casuali.
- Intel commercializza un chip che "campiona" (misura a tempi costanti) il rumore termico amplificando la tensione in certi conduttori (termo-resistori).

Generatori di Variabili Casuali uniformi "True Random Variable Generators"

- Esistono fenomeni realmente casuali. Tipicamente quando si utilizzano degli strumenti al di là dei limiti imposti dalla precisione dello strumento le ultime cifre sono casuali.
- Esistono siti (ad esempio www.random.org) che misurando le fluttuazioni dell'atmosfera forniscono dei numeri veramente casuali.
- Intel commercializza un chip che "campiona" (misura a tempi costanti) il rumore termico amplificando la tensione in certi conduttori (termo-resistori).
- La bell ha un generatore basato sul tempo di accesso ad un settore di un disco rigido.

Generatori di Variabili Casuali uniformi "True Random Variable Generators"

- Esistono fenomeni realmente casuali. Tipicamente quando si utilizzano degli strumenti al di là dei limiti imposti dalla precisione dello strumento le ultime cifre sono casuali.
- Esistono siti (ad esempio www.random.org) che misurando le fluttuazioni dell'atmosfera forniscono dei numeri veramente casuali.
- Intel commercializza un chip che "campiona" (misura a tempi costanti) il rumore termico amplificando la tensione in certi conduttori (termo-resistori).
- La bell ha un generatore basato sul tempo di accesso ad un settore di un disco rigido.
- Un altro progetto open-source è www.lavarnd.org.

Generatori di Variabili Casuali uniformi "True Random Variable Generators"

- Esistono fenomeni realmente casuali. Tipicamente quando si utilizzano degli strumenti al di là dei limiti imposti dalla precisione dello strumento le ultime cifre sono casuali.
- Esistono siti (ad esempio www.random.org) che misurando le fluttuazioni dell'atmosfera forniscono dei numeri veramente casuali.
- Intel commercializza un chip che "campiona" (misura a tempi costanti) il rumore termico amplificando la tensione in certi conduttori (termo-resistori).
- La bell ha un generatore basato sul tempo di accesso ad un settore di un disco rigido.
- Un altro progetto open-source è www.lavarnd.org.
- Si può usare (una volta per ogni sessione) i centesimi di secondo dall'inizio dell'esecuzione del sistema operativo. I numeri random che si usano una sola volta si chiamano nonce.

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.
- Per verificare la bontà dei generatori di numeri pseudo-ramdom si usano Test statistici (analisi sequenze prodotte):
  - Next-bit test. Conoscendo i primi n bit generati (senza conoscere il seme) non si può conoscere il bit successivo. Yao test.

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.
- Per verificare la bontà dei generatori di numeri pseudo-ramdom si usano Test statistici (analisi sequenze prodotte):
  - Next-bit test. Conoscendo i primi n bit generati (senza conoscere il seme) non si può conoscere il bit successivo. Yao test.
  - Frequenza degli zeri (o degli uno) "Frequency monobits".

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.
- Per verificare la bontà dei generatori di numeri pseudo-ramdom si usano Test statistici (analisi sequenze prodotte):
  - Next-bit test. Conoscendo i primi n bit generati (senza conoscere il seme) non si può conoscere il bit successivo. Yao test.
  - Frequenza degli zeri (o degli uno) "Frequency monobits".
  - Discrete Fourier trasform. Test di periodicità.

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.
- Per verificare la bontà dei generatori di numeri pseudo-ramdom si usano Test statistici (analisi sequenze prodotte):
  - Next-bit test. Conoscendo i primi n bit generati (senza conoscere il seme) non si può conoscere il bit successivo. Yao test.
  - Frequenza degli zeri (o degli uno) "Frequency monobits".
  - Discrete Fourier trasform. Test di periodicità.
  - Test di compressibilità (Maurer)

Generatori di Variabili Casuali pseudo-random "Pseudo-Random Variable Generators"

- Una sequenza pseudo-randon è un sequenza deterministica che possiede le proprietà di uniformità ed indipendenza (apparente).
- Un generatore di numeri pseudo-randon genera tali sequenze.
- Per verificare la bontà dei generatori di numeri pseudo-ramdom si usano Test statistici (analisi sequenze prodotte):
  - Next-bit test. Conoscendo i primi n bit generati (senza conoscere il seme) non si può conoscere il bit successivo. Yao test.
  - Frequenza degli zeri (o degli uno) "Frequency monobits".
  - Discrete Fourier trasform. Test di periodicità.
  - Test di compressibilità (Maurer)
  - "Run test". Si verifica la frequenza delle sotto-sequenze da L bit nella sequenza totale. Ad esempio sequenza di k zeri consecutivi.

Generatori di numeri pseudo-random

- Tutti i generatori di numeri pseudo-random ricevono in ingresso un numero x_0, detto seme, corrispondente ad una sequenza di bit di lunghezza assegnata e forniscono in uscita una sequenza molto più lunga.

Generatori di numeri pseudo-random

- Tutti i generatori di numeri pseudo-random ricevono in ingresso un numero x_0, detto seme, corrispondente ad una sequenza di bit di lunghezza assegnata e forniscono in uscita una sequenza molto più lunga.
- Tutti i generatori di numeri random sono facilmente computabili.

Generatori di numeri pseudo-random

- Tutti i generatori di numeri pseudo-random ricevono in ingresso un numero x_0, detto seme, corrispondente ad una sequenza di bit di lunghezza assegnata e forniscono in uscita una sequenza molto più lunga.
- Tutti i generatori di numeri random sono facilmente computabili.
- Molti generatori agiscono in forma iterativa ed utilizzano una parte delle sequenza in uscita come sequenza di ingresso per l'iterazione successiva.

$$x_{i+1} = f(x_i, xi - 1, \ldots).$$

I blocchi di bit x_i di solito sono di dimensione (lunghezza) pari al seme.

Generatori lineari modulari o congruenziali

- L'algoritmo per la generazione consta di questi passi:

Generatori lineari modulari o congruenziali

- L'algoritmo per la generazione consta di questi passi:
- Viene assegnato un numero iniziale detto seme x_0.

Generatori lineari modulari o congruenziali

- L'algoritmo per la generazione consta di questi passi:
- Viene assegnato un numero iniziale detto seme x_0.
- I valori successivi sono determinati con un procedimento iterativo tramite una legge di trasformazione affine (polinomio di primo grado):

$$x_{i+1} \stackrel{def}{=} a \cdot x_i + b \, (mod \ n)$$

Generatori lineari modulari o congruenziali

- L'algoritmo per la generazione consta di questi passi:
- Viene assegnato un numero iniziale detto seme x_0.
- I valori successivi sono determinati con un procedimento iterativo tramite una legge di trasformazione affine (polinomio di primo grado):

$$x_{i+1} \stackrel{def}{=} a \cdot x_i + b \, (mod \ n)$$

- La presenza della congruenza rende l'algoritmo meno prevedibile

Generatori lineari modulari o congruenziali

- I generatori congruenziali sono i più semplici PRNS (Pseudo Random Number Generator). L'algoritmo per la generazione consta di questi passi:

Generatori lineari modulari o congruenziali

- I generatori congruenziali sono i più semplici PRNS (Pseudo Random Number Generator). L'algoritmo per la generazione consta di questi passi:
- Viene assegnato un numero iniziale detto seme x_0.

Generatori lineari modulari o congruenziali

- I generatori congruenziali sono i più semplici PRNS (Pseudo Random Number Generator). L'algoritmo per la generazione consta di questi passi:
- Viene assegnato un numero iniziale detto seme x_0.
- I valori successivi sono determinati con un procedimento iterativo tramite una legge di trasformazione affine (polinomio di primo grado):

$$x_{i+1} \stackrel{def}{=} a \cdot x_i + b \ (mod \ n)$$

Generatori lineari modulari o congruenziali

- I generatori congruenziali sono i più semplici PRNS (Pseudo Random Number Generator). L'algoritmo per la generazione consta di questi passi:
- Viene assegnato un numero iniziale detto seme x_0.
- I valori successivi sono determinati con un procedimento iterativo tramite una legge di trasformazione affine (polinomio di primo grado):

$$x_{i+1} \stackrel{def}{=} a \cdot x_i + b \ (mod \ n)$$

- La presenza della congruenza rende l'algoritmo meno prevedibile

Periodo dei generatori lineari modulari

- I problemi fondamentali sono essenzialmente la capacità di generare tutti i valori possibili e la frequenza con cui vengono assunti.

Periodo dei generatori lineari modulari

- I problemi fondamentali sono essenzialmente la capacità di generare tutti i valori possibili e la frequenza con cui vengono assunti.
- Il primo problema equivale a trovare la periodicità dell'algoritmo. Se deve generare una ed una sola volta tutti i numeri tra 0 ed il modulo n (meno 1), il periodo deve essere pari al modulo.

Periodo dei generatori lineari modulari

- I problemi fondamentali sono essenzialmente la capacità di generare tutti i valori possibili e la frequenza con cui vengono assunti.
- Il primo problema equivale a trovare la periodicità dell'algoritmo. Se deve generare una ed una sola volta tutti i numeri tra 0 ed il modulo n (meno 1), il periodo deve essere pari al modulo.
- Siccome il risultato delle operazioni algebriche non dipende dal rappresentante possiamo iterare il procedimento prima e poi applicare al congruenza. Vediamo il termine k-esimo:

$$
\begin{aligned}
&x_1 = a \cdot x_0 + b, \\
&x_2 = a \cdot x_1 + b = a(a \cdot x_0 + b) + b = a^2 \cdot x_0 + b \cdot (a + 1) \\
&\dots \\
&x_k = a^k \cdot x_0 + b \cdot \left(\sum_{i=0}^{k-1} a^i \right) = a^k \cdot x_0 + b \cdot \left(\frac{a^k - 1}{a - 1} \right).
\end{aligned}
$$

Periodo dei generatori lineari modulari - cont

- Il periodo m corrisponde al valore minimo per cui si riottiene un valore precedente:

$$x_{i+m} = x_i;$$

Periodo dei generatori lineari modulari - cont

- Il periodo m corrisponde al valore minimo per cui si riottiene un valore precedente:

$$x_{i+m} = x_i;$$

- Eseguire k+m iterazioni equivale a partire da x_k ed eseguire m iterazioni:

$$x_{k+m} = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right);$$

Periodo dei generatori lineari modulari - cont

- Il periodo m corrisponde al valore minimo per cui si riottiene un valore precedente:

$$x_{i+m} = x_i;$$

- Eseguire k+m iterazioni equivale a partire da x_k ed eseguire m iterazioni:

$$x_{k+m} = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right);$$

- La condizione di periodicità equivale a

$$\forall x_k : x_k = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right) \ (mod\ n).$$

Periodo dei generatori lineari modulari - cont

- Il periodo m corrisponde al valore minimo per cui si riottiene un valore precedente:

$$x_{i+m} = x_i;$$

- Eseguire k+m iterazioni equivale a partire da x_k ed eseguire m iterazioni:

$$x_{k+m} = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right);$$

- La condizione di periodicità equivale a

$$\forall x_k : x_k = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right) \ (mod\ n).$$

- $$\forall x_k : \left(\frac{a^m - 1}{a - 1} \right) \cdot (x_k \cdot (a - 1) + b) = 0 \ (mod\ n).$$

Periodo dei generatori lineari modulari - cont

- Il periodo m corrisponde al valore minimo per cui si riottiene un valore precedente:

$$x_{i+m} = x_i;$$

- Eseguire k+m iterazioni equivale a partire da x_k ed eseguire m iterazioni:

$$x_{k+m} = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right);$$

- La condizione di periodicità equivale a

$$\forall x_k : x_k = a^m \cdot x_k + b \cdot \left(\frac{a^m - 1}{a - 1} \right) \ (mod\ n).$$

-

$$\forall x_k : \left(\frac{a^m - 1}{a - 1} \right) \cdot (x_k \cdot (a - 1) + b) = 0 \ (mod\ n).$$

- Se $a - 1$ è primo con n il primo fattore si annullerà per qualche $m \leq \lambda(n) < n$ (λ di Carlmichael): $a^m = 1$.

Periodo dei generatori lineari modulari - cont

- Se vogliamo la periodicità completa l'ipotesi $a-1$ primo con n si deve scartare. Se $a-1$ non è primo con n, l'equazione diofantea:

$$x_k \cdot (a-1) + b = 0 \ (mod \ n).$$

non ammette soluzioni se b è primo con n. Inoltre $x_k \cdot (a-1) + b$ è sempre primo con n.

Periodo dei generatori lineari modulari - cont

- Se vogliamo la periodicità completa l'ipotesi $a-1$ primo con n si deve scartare. Se $a-1$ non è primo con n, l'equazione diofantea:

$$x_k \cdot (a-1) + b = 0 \ (mod \ n).$$

non ammette soluzioni se b è primo con n. Inoltre $x_k \cdot (a-1) + b$ è sempre primo con n.

- Quindi una condizione necessaria è che b sia primo con n ed $a-1$ non lo sia. Sotto queste condizioni il problema si semplifica perché $x_k \cdot (a-1) + b$ non possiede divisori in comune con n e quindi l'altro fattore deve annullarsi:

$$\frac{a^m - 1}{a-1} \equiv 0 \ (mod \ n).$$

che in $\mathbb{Z}$ diviene:

$$\frac{a^m - 1}{a-1} = \alpha n.$$

Periodo dei generatori lineari modulari - cont

- Come abbiamo fatto molte volte, utilizziamo al decomposizione di n in fattori primi e proiettiamo l'equazione diofantea:

$$n = \left((p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_i)^{h_i} \cdots (p_M)^{h_M} \right) = n_1 \cdot n_2 \cdots n_i \cdots n_M;$$

in cui $n_i \stackrel{def}{=} (p_i)^{h_i}$.

Periodo dei generatori lineari modulari - cont

- Come abbiamo fatto molte volte, utilizziamo al decomposizione di n in fattori primi e proiettiamo l'equazione diofantea:

$$n = \left((p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_i)^{h_i} \cdots (p_M)^{h_M} \right) = n_1 \cdot n_2 \cdots n_i \cdots n_M;$$

  in cui $n_i \stackrel{def}{=} (p_i)^{h_i}$.

- Proiettando:

$$\begin{cases} \frac{a^m-1}{a-1} & \equiv & 0 & (mod & n_1), \\ \frac{a^m-1}{a-1} & \equiv & 0 & (mod & n_2), \\ \cdots & & & & \\ \frac{a^m-1}{a-1} & \equiv & 0 & (mod & n_M). \end{cases}$$

Periodo dei generatori lineari modulari - cont

- Come abbiamo fatto molte volte, utilizziamo al decomposizione di n in fattori primi e proiettiamo l'equazione diofantea:

$$n = \left((p_1)^{h_1} \cdot (p_2)^{h_2} \cdots (p_i)^{h_i} \cdots (p_M)^{h_M} \right) = n_1 \cdot n_2 \cdots n_i \cdots n_M;$$

  in cui $n_i \stackrel{def}{=} (p_i)^{h_i}$.
- Proiettando:

$$\begin{cases} \frac{a^m-1}{a-1} & \equiv & 0 & (mod & n_1), \\ \frac{a^m-1}{a-1} & \equiv & 0 & (mod & n_2), \\ \cdots & & & & \\ \frac{a^m-1}{a-1} & \equiv & 0 & (mod & n_M). \end{cases}$$

- Se $a-1$ è primo con qualcuno degli n_i il suo periodo in n_i è al più $p_i^{h_i-1}(p_i-1)$. Se tutti gli altri periodi fossero massimi (cioè n_i) il periodo totale sarebbe comunque $n \cdot /(p_i-1)/p_i$ che è minore di n. Quindi $a-1$ è multiplo di $p_1 p_2 \cdots p_M$.

Periodo dei generatori lineari modulari - cont

- Scriviamo a esplicitamente:

$$a = \alpha \cdot p_1 p_2 \cdots p_M + 1;$$

cioè per ogni p_i, a è della forma $a = \alpha_i \cdot p_i + 1$.

Periodo dei generatori lineari modulari - cont

- Scriviamo a esplicitamente:

$$a = \alpha \cdot p_1 p_2 \cdots p_M + 1;$$

  cioè per ogni p_i, a è della forma $a = \alpha_i \cdot p_i + 1$.
- In $\mathbb{Z}$ la condizione di massima periodicità diviene:

$$\frac{a^m - 1}{a - 1} = \beta n.$$

Periodo dei generatori lineari modulari - cont

- Scriviamo a esplicitamente:

$$a = \alpha \cdot p_1 p_2 \cdots p_M + 1;$$

cioè per ogni p_i, a è della forma $a = \alpha_i \cdot p_i + 1$.

- In $\mathbb{Z}$ la condizione di massima periodicità diviene:

$$\frac{a^m - 1}{a - 1} = \beta n.$$

- esplicitando la forma di a:

$$a^m - 1 = \beta n \cdot (a - 1) = \beta n';$$

in cui $n' = n * p_1 p_2 \cdots p_M = (p_1)^{h_1+1}(p_2)^{h_2+1} \cdots (p_M)^{h_M+1}$.

Periodo dei generatori lineari modulari - cont

- Scriviamo a esplicitamente:

$$a = \alpha \cdot p_1 p_2 \cdots p_M + 1;$$

cioè per ogni p_i, a è della forma $a = \alpha_i \cdot p_i + 1$.

- In $\mathbb{Z}$ la condizione di massima periodicità diviene:

$$\frac{a^m - 1}{a - 1} = \beta n.$$

- esplicitando la forma di a:

$$a^m - 1 = \beta n \cdot (a - 1) = \beta n';$$

in cui $n' = n * p_1 p_2 \cdots p_M = (p_1)^{h_1+1}(p_2)^{h_2+1} \cdots (p_M)^{h_M+1}$.

- Il problema equivale alle periodicità di potenza n in $\mathbb{Z}_{n'}$.

Periodo dei generatori lineari modulari - cont

- Abbiamo già visto che tutti i termini del tipo $1 + \gamma p$ (con p dispari) hanno periodicità p^{h-1} in $\mathbb{Z}_{p^h}$.

Periodo dei generatori lineari modulari - cont

- Abbiamo già visto che tutti i termini del tipo $1 + \gamma p$ (con p dispari) hanno periodicità p^{h-1} in $\mathbb{Z}_{p^h}$.
- Proiettando su tutti gli $\mathbb{Z}_{p_i^{h_i+1}}$ si ottiene che il periodo di $1 + \gamma p_1 p_2 \cdots p_M$ è $(p_1)^{h_1+1-1}(p_2)^{h_2+1-1} \cdots (p_M)^{h_M+1-1} = p_1^{h_1} p_2^{h_2} \cdots p_M^{h_M} = n$.
- Infatti, come abbiamo visto:

$$(1 + \gamma p)^{p^k} = 1 + \gamma p \cdot p^k + ...$$

e solo per $k = h - 1$ sparisce ogni termine in p di grado minore di h.

Vediamo il caso n pari

- La regola dei periodi vale per tutti i fattori primi dispari, ma non per i pari. Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

Vediamo il caso n pari

- La regola dei periodi vale per tutti i fattori primi dispari, ma non per i pari. Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi se tra i fattori c'è il numero due dobbiamo scegliere $a = 1+\alpha 2^2 p_2 p_3 \cdots p_M$. In questo caso $n' = n*4*p_2 p_3 \cdots p_M$.

Vediamo il caso n pari

- La regola dei periodi vale per tutti i fattori primi dispari, ma non per i pari. Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi se tra i fattori c'è il numero due dobbiamo scegliere $a = 1+\alpha 2^2 p_2 p_3 \cdots p_M$. In questo caso $n' = n*4*p_2 p_3 \cdots p_M$.
- $1+4\gamma$ ha effettivamente periodo 2^{h-2} in $\mathbb{Z}_{2^h}$ e periodo 2^h in $\mathbb{Z}_{2^{h+2}}$. Quindi in $\mathbb{Z}_{n'}$ il periodo è sempre n.

Vediamo il caso n pari

- La regola dei periodi vale per tutti i fattori primi dispari, ma non per i pari. Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi se tra i fattori c'è il numero due dobbiamo scegliere $a = 1+\alpha 2^2 p_2 p_3 \cdots p_M$. In questo caso $n' = n*4*p_2 p_3 \cdots p_M$.
- $1+4\gamma$ ha effettivamente periodo 2^{h-2} in $\mathbb{Z}_{2^h}$ e periodo 2^h in $\mathbb{Z}_{2^{h+2}}$. Quindi in $\mathbb{Z}_{n'}$ il periodo è sempre n.
- In conclusione i numeri a e b devono essere scelti in modo che b sia primo con n ed $a-1$ sia divisibile per $p_1 p_2 \cdots p_M$ se è dispari e per il doppio se è pari.

Vediamo il caso n pari

- La regola dei periodi vale per tutti i fattori primi dispari, ma non per i pari. Il problema è che $(2+1)^2 = 3^2 = 9 = 1+8 = 1+2^3$:

$$(2+1)^2 = 4+4+1 = 8+1 \neq 4+1+8*k;$$

- Quindi se tra i fattori c'è il numero due dobbiamo scegliere $a = 1+\alpha 2^2 p_2 p_3 \cdots p_M$. In questo caso $n' = n*4*p_2 p_3 \cdots p_M$.
- $1+4\gamma$ ha effettivamente periodo 2^{h-2} in $\mathbb{Z}_{2^h}$ e periodo 2^h in $\mathbb{Z}_{2^{h+2}}$. Quindi in $\mathbb{Z}_{n'}$ il periodo è sempre n.
- In conclusione i numeri a e b devono essere scelti in modo che b sia primo con n ed $a-1$ sia divisibile per $p_1 p_2 \cdots p_M$ se è dispari e per il doppio se è pari.
- Esempio $n = 2^4 = 16$ possiamo scegliere un qualsiasi dispari per b mentre a deve essere $4\alpha+1$ cioè $5, 9, 13$.

Risposta ai test dei generatori congruenziali.

- Gli algoritmi congruenziali superano il test di uniformità perché forniscono tutti i numeri con la stessa frequenza.

Risposta ai test dei generatori congruenziali.

- Gli algoritmi congruenziali superano il test di uniformità perché forniscono tutti i numeri con la stessa frequenza.
- Gli algoritmi congruenziali non superano i test di aperiodicità perché hanno esattamente un periodo N.

Risposta ai test dei generatori congruenziali.

- Gli algoritmi congruenziali superano il test di uniformità perché forniscono tutti i numeri con la stessa frequenza.
- Gli algoritmi congruenziali non superano i test di aperiodicità perché hanno esattamente un periodo N.
- Gli algoritmi congruenziali non superano i test di ripetitività (non capita mai che un numero riappaia prima di N iterazioni) e quindi vengono modificati dividendo per cento o per mille il numero pseudo-random fornito (ma mantenendo tutte le cifre nella generazione).

Risposta ai test dei generatori congruenziali.

- Gli algoritmi congruenziali superano il test di uniformità perché forniscono tutti i numeri con la stessa frequenza.
- Gli algoritmi congruenziali non superano i test di aperiodicità perché hanno esattamente un periodo N.
- Gli algoritmi congruenziali non superano i test di ripetitività (non capita mai che un numero riappaia prima di N iterazioni) e quindi vengono modificati dividendo per cento o per mille il numero pseudo-random fornito (ma mantenendo tutte le cifre nella generazione).
- George Marsaglia ha definito una collezione di test denominati "die hard", sono disponibili in Python, c, fortran e mathlab.

Risposta ai test dei generatori congruenziali.

- Gli algoritmi congruenziali superano il test di uniformità perché forniscono tutti i numeri con la stessa frequenza.
- Gli algoritmi congruenziali non superano i test di aperiodicità perché hanno esattamente un periodo N.
- Gli algoritmi congruenziali non superano i test di ripetitività (non capita mai che un numero riappaia prima di N iterazioni) e quindi vengono modificati dividendo per cento o per mille il numero pseudo-random fornito (ma mantenendo tutte le cifre nella generazione).
- George Marsaglia ha definito una collezione di test denominati "die hard", sono disponibili in Python, c, fortran e mathlab.
- Introducendo dei nuovi semi genuinamente casuali si può ovviare a molti problemi di regolarità.

Tabella dei software che usano i generatori affini modulari: Linear congruential generators

- Attenzione preso da wikipedia (aprile 2016) quindi non garantito:

Source	*m*	(multiplier) *a*	(increment) *c*	output bits of seed in *rand()* / *Random(L)*
Numerical Recipes	2^{32}	1664525	1013904223	
Borland C/C++	2^{32}	22695477	1	bits 30..16 in *rand()*, 30..0 in *lrand()*
glibc (used by GCC)[5]	2^{31}	1103515245	12345	bits 30..0
ANSI C: Watcom, Digital Mars, CodeWarrior, IBM VisualAge C/C++ [6]	2^{31}	1103515245	12345	bits 30..16
C99, C11: Suggestion in the ISO/IEC 9899 [7]	2^{31}	1103515245	12345	bits 30..16
Borland Delphi, Virtual Pascal	2^{32}	134775813	1	bits 63..32 of *(seed * L)*
Microsoft Visual/Quick C/C++	2^{32}	214013 ($343FD_{16}$)	2531011 ($269EC3_{16}$)	bits 30..16
Microsoft Visual Basic (6 and earlier)[8]	2^{24}	1140671485 ($43FD43FD_{16}$)	12820163 ($C39EC3_{16}$)	
RtlUniform from Native API[9]	$2^{31} - 1$	2147483629 ($7FFFFFED_{16}$)	2147483587 ($7FFFFFC3_{16}$)	
Apple CarbonLib, C++11's `minstd_rand0` [10]	$2^{31} - 1$	16807	0	see MINSTD
C++11's `minstd_rand` [10]	$2^{31} - 1$	48271	0	see MINSTD
MMIX by Donald Knuth	2^{64}	6364136223846793005	1442695040888963407	
Newlib, Musl	2^{64}	6364136223846793005	1	bits 63...32
VMS's **MTH$RANDOM**,[11] old versions of glibc	2^{32}	69069	1	
Java's java.util.Random, POSIX [ln]rand48, glibc [ln]rand48[_r]	2^{48}	25214903917 ($5DEECE66D_{16}$)	11	bits 47...16
POSIX[12] [jm]rand48, glibc [mj]rand48[_r]	2^{48}	25214903917 ($5DEECE66D_{16}$)	11	bits 47...15
POSIX [de]rand48, glibc [de]rand48[_r]	2^{48}	25214903917 ($5DEECE66D_{16}$)	11	bits 47...0
Formerly common: RANDU [4]	2^{31}	65539	0	

Esercizi

- Svolgere a mano il caso $n = 16$.

Esercizi

- Svolgere a mano il caso $n = 16$.
- Scrivere una programma con Octave che simuli un generatore con $n = 2^{16}$ ed $n = 27 = 3^3$.

Esercizi

- Svolgere a mano il caso $n = 32e9$.

Esercizi

- Svolgere a mano il caso $n = 32e9$.
- Opzionale Scrivere una programma con Octave che simuli un generatore con $n = 2^{16}$ ed $n = 27 = 3^3$.

Messaggio

- Abbiamo introdotto i concetti basilari della probabilitá ed in particolare il concetto di distribuzione uniforme o random.

Messaggio

- Abbiamo introdotto i concetti basilari della probabilitá ed in particolare il concetto di distribuzione uniforme o random.
- La generazione di numeri random è un processo delicato che richiede dispositivi specifici e tempi di acquisizione lunghi. Pertanto si utilizzano generatori di numeri pseudorandom che presentano proprietà simili.

Messaggio

- Abbiamo introdotto i concetti basilari della probabilitá ed in particolare il concetto di distribuzione uniforme o random.
- La generazione di numeri random è un processo delicato che richiede dispositivi specifici e tempi di acquisizione lunghi. Pertanto si utilizzano generatori di numeri pseudorandom che presentano proprietà simili.
- Abbiamo analizzato le proprietà del generatori pseudorandom congruenziali e dimostratone l'uniformità.

Messaggio

- Abbiamo introdotto i concetti basilari della probabilitá ed in particolare il concetto di distribuzione uniforme o random.
- La generazione di numeri random è un processo delicato che richiede dispositivi specifici e tempi di acquisizione lunghi. Pertanto si utilizzano generatori di numeri pseudorandom che presentano proprietà simili.
- Abbiamo analizzato le proprietà del generatori pseudorandom congruenziali e dimostratone l'uniformità.
- In seguito vedremo il metodo moderno Mersenne Twister per generare i numeri pseudo-random.