Titolo unità didattica: Numeri pseudocasuali e simulazioni stocastiche [16]

Titolo modulo : Proprietà dei numeri pseudocasuali [01-T]

Generalità sui numeri casuali e pseudocasuali e sul loro uso

Argomenti trattati:

- ✓ numeri casuali e numeri pseudocasuali
- ✓ algoritmi per la generazione di numeri pseudocasuali
- ✓ simulazione di fenomeni casuali
- ✓ cammino casuale

Prerequisiti richiesti: AP-07-06-T, AP-12-01-T

un fenomeno è **casuale** (**random**)
se **non è prevedibile**

- ✓ il risultato del lancio di un dado
- ✓ dati i risultati di una sequenza di (n-1) lanci di un dado, il risultato dell'n-simo lancio
- ✓ l'estrazione di un numero dalla *ruota del lotto*
- ✓ l'esatto punto di arrivo di una goccia su un ombrello
- ✓ facendo cadere una penna su una scrivania, l'angolo che si determina tra la direzione della penna e un bordo della scrivania
- ✓ l'esatto istante del decadimento di un atomo radioattivo

una **successione di numeri** è **casuale** se l'n-simo numero della successione non dipende dai precedenti (non è prevedibile dai precedenti (n-1) numeri)

un fenomeno è **pseudocasuale**

o **statisticamente casuale** (**pseudorandom**)

se **sembra** essere **casuale**

ma non lo è

una **successione di numeri** è **pseudocasuale** se essa **non** contiene **forme di regolarità riconoscibili**

la successione delle cifre di π è **pseudocasuale**,

poiché non contiene contiene forme di regolarità riconoscibili, ma vi è un meccanismo deterministico (algoritmo) che descrive la successione

una successione di numeri è considerata pseudocasuale se non esiste un algoritmo a complessità polinomiale che è in grado di stabilire se essa è diversa da una successione casuale

un **generatore di numeri pseudocasuali**

è un **algoritmo**

che genera una successione

di numeri pseudocasuali

sono basati su opportune formule ricorrenti

- ✓ generatore lineare a congruenza
- ✓ generatore di Fibonacci ritardato
- ✓ …

generatore lineare a congruenza

$$n_{k+1} = \mathrm{mod}\left(\left(a \cdot n_k + b\right), m\right)$$

n_0 è fissato arbitrariamente ed è detto **seed**

la successione di numeri pseudocasuali creata da un generatore **dipende dal seed**

una successione di numeri pseudocasuali può essere sempre **riprodotta**

riproducibilità delle simulazioni basate su numeri psudocasuali

generatore lineare a congruenza

esempio

$$n_{k+1} = \mathrm{mod}\left(\frac{n_k \cdot 110351245 + 12345}{65436}, 32768 \right)$$

una successione di numeri pseudocasuali è sempre **periodica**

un **buon generatore** genera successioni di numeri pseudocasuali di **periodo molto grande**

generatore di Fibonacci ritardato

$$n_{k+1} = \mathrm{mod}\left(\left(n_{k-p} + n_{k-q}\right), m\right)$$

$$n_{k+1} = \mathrm{mod}\left(\left(n_{k-p} \cdot n_{k-q}\right), m\right)$$

$$n_{k+1} = \mathrm{mod}\left(\left(n_{k-p} \ \mathrm{XOR} \ n_{k-q}\right), m\right)$$

$$m = 2^{32}, 2^{64}$$

$$p < q < k$$

i numeri di una successione pseudocasuale appartengono a un **intervallo** prefissato

esempio $[0, M]$

i numeri di una successione pseudocasuale sono estratti da una **distribuzione** prefissata

esempio

- distribuzione uniforme
- distribuzione normale
- .....

cambio di intervallo

distribuzione uniforme

si vuole trasformare una successione di numeri interi

$$n_k \in [0, M]$$

M e B interi

$B < M$

in una successione di numeri interi

$$t_k \in [0, B]$$

$$t_k = \mathrm{mod}(n_k, B+1)$$

cambio di intervallo

distribuzione uniforme

si vuole trasformare una successione di numeri interi

$$n_k \in [0, M]$$

M e B interi

$(B\text{-}A) < M$

in una successione di numeri interi

$$t_k \in [A, B]$$

$$t_k = A + \mathrm{mod}(n_k, B + 1 - A)$$

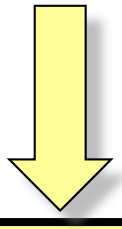
cambio di intervallo

si vuole trasformare una successione di numeri

$$n_k \in [0, M]$$

in una successione di numeri

$$t_k \in [A, B]$$



$$t_k = A + \frac{(B - A)}{M} \cdot n_k$$

simulazione di fenomeni casuali

un metodo (algoritmo) che utilizza **successioni di numeri pseudocasuali** per **simulare fenomeni casuali** è detto **metodo Monte Carlo**

esempio — simulazione di un lancio di un dado (**6** facce)

si genera un elemento di una successione di numeri pseudocasuali interi nell'intervallo **[1,6]**

esempio — simulazione di 10 lanci di una coppia di dadi

si generano 20 elementi di una successione di numeri pseudocasuali interi nell'intervallo **[1,6]**

simulazione di fenomeni casuali

Monte Carlo

esempio

simulazione della scelta casuale di un carattere dell'alfabeto italiano (21 lettere)

si genera un elemento di una successione di numeri pseudocasuali interi nell'intervallo **[1,21]**

esempio

simulazione della generazione casuale di una parola di 5 lettere

si generano 5 elementi di una successione di numeri pseudocasuali interi nell'intervallo **[1,21]**

esempio

simulazione della generazione casuale della posizione di una casella in una scacchiera 5x5

si generano 2 elementi di una successione di numeri pseudocasuali interi nell'intervallo **[1,5]**

simulazione di fenomeni casuali

Monte Carlo

esempio

simulazione della generazione casuale di un punto del quadrato [0,1]x[0,1] del piano

si generano 2 elementi di una successione di numeri pseudocasuali reali nell'intervallo **[0,1]**

esempio

simulazione della generazione casuale di un punto del rettangolo [2,5]x[3,8] del piano

si generano 2 elementi di una successione di numeri pseudocasuali reali nell'intervallo **[0,1]** , si trasforma il **primo** numero dall'intervallo **[0,1]** all'intervallo **[2,5]**, e poi si trasforma il **secondo** numero dall'intervallo **[0,1]** all'intervallo **[3,8]**

simulazione di fenomeni casuali

Monte Carlo

esempio

simulazione dell'estrazione casuale di una carta da un mazzo di carte francesi (52 carte)

si genera un elemento di una successione di numeri pseudocasuali interi nell'intervallo **[1,52]**

esempio

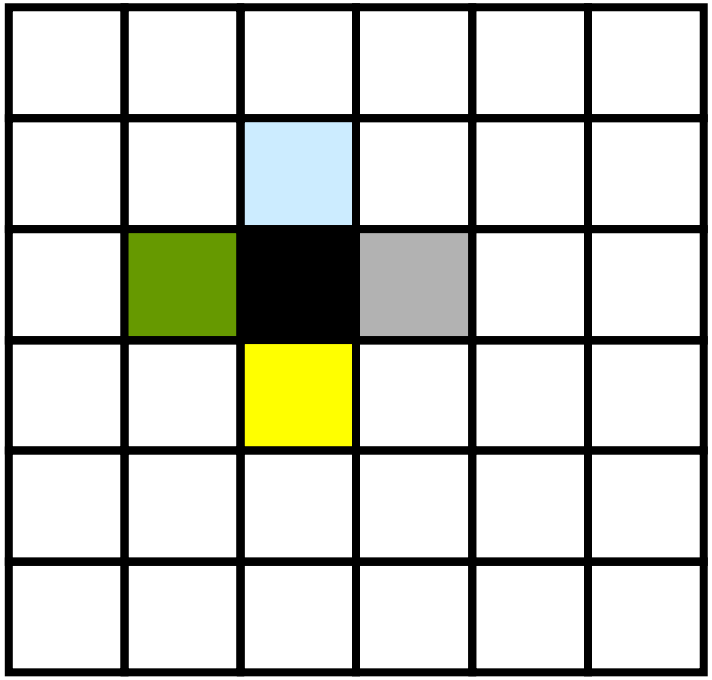
simulazione della *mischiatura* casuale di un mazzo di 40 carte

si generano N elementi di una successione di numeri pseudocasuali interi nell'intervallo **[1,40]**; i primi due numeri determinano gli indici delle due carte che devono scambiare la loro posizione nel mazzo; la successiva coppia di numeri determina gli indici di altre due carte che devono scambiare la loro posizione nel mazzo; e così via, effettuando N/2 scambi di coppie di carte del mazzo

esempio

simulazione del movimento casuale di una pedina su una scacchiera di 10x10 caselle (**cammino casuale**)

ipotesi: una pedina si può muovere con la **stessa probabilità** solo in una delle **4 caselle vicine** alla casella dove si trova



si genera una successione di numeri pseudocasuali interi nell'intervallo **[0,3]**

0 → nord

1 → est

2 → sud

3 → ovest

fare attenzione quando la pedina si trova sul bordo della scacchiera

esempio

simulazione del movimento casuale di una pedina su una scacchiera di 10x10 caselle (**cammino casuale**)

ipotesi: una pedina si può muovere in una delle **4 caselle vicine** alla casella dove si trova, ma con diversa probabilità secondo la legge:

- ✓ probabilità 50% a nord
- ✓ probabilità 30% a est
- ✓ probabilità 10% a sud
- ✓ probabilità 10% a ovest

si genera una successione di numeri pseudocasuali interi nell'intervallo **[1,100]**

1,2,..,50 → nord
51,..,80 → est
81,..,90 → sud
91,..,100 → ovest