Domande Orale Secondo Modulo: Analisi e Progettazione di Algoritmi (APA)

1 Ordinamento

1. Costruisci l'input peggiore per una versione deterministica di QuickSort che sceglie come pivot (a) il primo elemento di una sequenza e (b) l'elemento mediano

2. Supponi di avere una probabilità congiunta di 100 variabili casuali di Bernoulli non indipendenti. Se devi calcolare il valore atteso della somma partendo da questa distribuzione quanti sono i termini da sommare? Quanti invece se utilizzi il fatto che il valore atteso di una somma è uguale alla somma dei valori attesi? Che cosa cambia se fossero indipendenti?

3. Nell'assunzione che la sequenza S consista dei primi n numeri naturali, spiega per quale motivo la probabilità che i sia confrontato con j può essere espressa come

$$\frac{2}{|i-j|+1}$$

2 Teoria dei giochi

4. Determina il migliore degli scenari possibili per Roberta e Carlo data una matrice M dei pagamenti in un gioco a somma zero

5. Che cosa sono le strategie miste e, in particolari, le strategie miste ottimali?

6. Che cosa puoi fare per ottenere un limite inferiore al costo computazionale atteso di un algoritmo randomizzato?

3 Valutazione dell'albero di un gioco

7. Produci un esempio di un albero di un gioco per il quale un algoritmo deterministico deve valutare tutte le foglie

8. Dimostra che nel caso base di un albero binario di un gioco un algoritmo randomizzato controlla, in media, 3 delle 4 foglie

4 Taglio minimo

9. Spiega il motivo per il quale se k è la cardinalità di un taglio minimo per un grafo G con n vertici, il numero di archi non può essere minore di nk/2.

10. Sia G un grafo connesso di n vertici e taglio minimo uguale a k. Se E_i è l'evento di non selezionare un arco di S all'i-esima iterazione di $MCMinCut$, spiega il motivo per cui

$$Pr(E_i|E_1, E_2, \ldots, E_{i-1}) \geq \frac{2}{n-i+1}$$

11. Se un algoritmo Monte Carlo ottiene il risultato corretto con probabilità p, quante volte deve essere ripetuto per restituire il risultato corretto almeno una volta con probabilità del 99.9%?

5 Accordo bizantino

12. Per quali motivi raggiungere il consenso distribuito è un problema complicato?

13. Quali sono le specifiche per il raggiungimento del consenso bizantino e quali le motivazioni per i vincoli di consenso e validità?

14. Spiega il motivo per cui se $n = 3f$ e $T = 2f$ il protocollo $MGByzantineGeneral$ potrebbe non raggiungere mai un accordo

15. Siano dati $n = 3f + 1$ processi, f dei quali inaffidabili. Per quale motivo, se n è abbastanza grande e il bit di ogni processo affidabile è inizializzato uniformemente a caso, i $2f + 1$ processi affidabili raggiungono l'accordo dopo il primo round con grande probabilità?

6 Test di primalità

16. Verifica che gli elementi di Z_{10}^+ che non sono coprimi di 10 non ammettono inverso e quindi non possono appartenere a Z_{10}^*

17. Determina gli elementi di Z_{12}^* e verifica che ogni elemento è l'inverso di se stesso.

18. Eseguendo a mano i passi di MCPrimalityTest verifica che per ogni $a \in \{2, \ldots, 5\}$, 7 è probabilmente primo.

7 Verifiche di uguaglianza

19. Per quale motivo verificare il prodotto di due matrici $n \times n$ richiede solo $O(n^2)$ moltiplicazioni?

20. Come costruiresti un insieme di numeri primi minori di l^2?

21. Poni $l = 8$ e costruisci due file a e b di 8 bit con $a \neq b$. Campiona un numero primo a caso tra 2 e 64 e confronta le due fingerprint ottenute. Spiega quale strategia consentirebbe di determinare tutti i numeri primi per i quali le fingerprint sono uguali.