Universidad de Chile
Departamento de Ciencias de la Computación
CC4102 - Diseño y Análisis de Algoritmos

Auxiliar 12 - "Algoritmos Probabilísticos"

Profesor: Pablo Barceló
Auxiliar: ~~Manuel~~ Ariel Cáceres Reyes

23 de Junio del 2017

P1. Polinomios

Dados 3 polinomios en una variable p, q de grado n y r de grado $2n$. Muestre un algoritmo probabilístico que tome tiempo $\mathcal{O}(n)$ en determinar si $pq = r$.

P2. Matrices

Dadas 3 matrices cuadradas A, B y C de tamaño $n \times n$. Muestre un algoritmo probabilístico que tome tiempo $\mathcal{O}(n^2)$ en determinar si $AB = C$.

P3. Las Vegas vs Monte Carlo

a) Muestre que si se tiene un algoritmo de tipo Las Vegas de tiempo esperado T y una constante $c > 0$. Se puede construir, para el problema, un algoritmo Monte Carlo de tiempo cT y probabilidad de error a lo más $1/c$.

b) ¿Siempre se puede transformar un algoritmo Monte Carlo en un algoritmo de tipo Las Vegas? ¿Que restricción adicional sobre el problema podemos colocar para que sea cierto?

P4. Conjunto Independiente

Un conjunto independiente de un grafo $G = (V, E)$, con $|V| = n$ y $|E| = m$, es un subconjunto V' de V sin aristas de E entre elementos de V'. El problema de encontrar un conjunto independiente de cierto tamaño es NP-completo. Considere que V' , de tamaño r, se escoge al azar de V . Sea X la cantidad de aristas de E que conectan nodos de V' (X es una variable aleatoria).

(a) Considere una arista de E en particular. Calcule la probabilidad de que esta arista conecte dos nodos de V'. Acote la esperanza de X, $E(X)$.

(b) Diseñe un algoritmo Monte Carlo que encuentre un conjunto independiente de tamaño $\epsilon n/\sqrt{m}$ con probabilidad $1 - \epsilon^2$, para cualquier $0 < \epsilon < 1$.

P1. Elegimos uniformemente $x \in \{0, \ldots, 4n+1\}$ y luego respondemos `true` si $p(x) \cdot q(x) = r(x)$ y `false` en otro caso.

- En el caso de que la igualdad sea correcta, el algoritmo responde `true` de manera correcta.
- Sin embargo, cuando la igualdad es falsa ($pq \neq r$) el algoritmo podría responder erróneamente `true` en caso que $p(x) \cdot q(x) = r(x)$ o equivalentemente cuando el polinomio $g = pq - r$ se hace cero, i.e. cuando x es cero de g.
  Veamos que g es de grado a lo más $2n+1$ por lo que tiene a lo más $2n+1$ raíces, y luego la probabilidad que el algoritmo se equivoque es:

$$\mathbb{P}(x \; es \; raiz \; de \; g) \leq \frac{2n+1}{4n+2} = \frac{1}{2}$$

P2. Elegimos un vector aleatorio r uniformemente en $\{0,1\}^n$. Respondemos `true` si $A(Br) = Cr$ y `false` en otro caso. Al igual que en la P1 se cumple que cuando es cierto que $AB = C$ el algoritmo responde correctamente `true`, sin embargo, en caso que $AB \neq C$ puede que el algoritmo de todas formas responda `true` erróneamente lo que sucede en caso que $A(Br) = Cr$ o equivalentemente $(AB - C)r := Dr = P = 0$.

Como $D \neq 0$, existe un $d_{i,j} \neq 0$, la probabilidad de que la coordenada i de P sea 0 es:

$$\begin{aligned}
\mathbb{P}(p_i = 0) &= \mathbb{P}\left(\sum_{k=1}^{n} d_{i,k} r_k = 0\right) \\
&= \mathbb{P}(d_{i,j} r_j + y = 0) \\
&= \mathbb{P}(d_{i,j} r_j + y = 0 | y = 0)\,\mathbb{P}(y = 0) + \mathbb{P}(d_{i,j} r_j + y = 0 | y \neq 0)\,\mathbb{P}(y \neq 0) \\
&= \mathbb{P}(r_j = 0)\,\mathbb{P}(y = 0) + \mathbb{P}(r_j = 1 \wedge y = -d_{i,j})\,(1 - \mathbb{P}(y = 0)) \\
&\leq \mathbb{P}(r_j = 0)\,\mathbb{P}(y = 0) + \mathbb{P}(r_j = 1)\,(1 - \mathbb{P}(y = 0)) \\
&= \frac{1}{2}\mathbb{P}(y = 0) + \frac{1}{2}(1 - \mathbb{P}(y = 0)) \\
&= \frac{1}{2}
\end{aligned}$$

, luego la probabilidad de error del algoritmo en este caso es:

$$\mathbb{P}(P = 0) \leq \mathbb{P}(p_i = 0) \leq \frac{1}{2}$$

P3. Preliminares :

- Desigualdad de Markov: Si X es una variable aleatoria no negativa con valor esperado positivo entonces

$$\forall c > 0, \; \mathbb{P}(X \geq c\mathbb{E}(X)) \leq \frac{1}{c}$$

- Algoritmo Montecarlo: Algoritmo probabilístico que termina en un tiempo determinado, pero tiene una probabilidad de error distinta de 0.
- Algoritmo Las Vegas: Algoritmo probabilístico con probabilidad de error 0, pero que no asegura el término de su ejecución, solo asegura un valor esperado finito del tiempo que demora.

a) Si tenemos un algoritmo A "Las Vegas" que resuelve el problema en tiempo esperado $T > 0$, creamos el siguiente algoritmo "Montecarlo":

- Correr A por cT tiempo, si ha terminado, respondemos lo mismo que A, si no respondemos "`null`".

Definamos la variable aleatoria X como el tiempo que demora el algoritmo A. Por Desigualdad de Markov sabemos que $\mathbb{P}(X \geq cT) \leq \frac{1}{c}$, pero $\mathbb{P}(X \geq cT)$ es la probabilidad de que A se demore más de cT y por lo tanto una cota superior a la probabilidad de que nuestro algoritmo "Montecarlo" se equivoque.

b) La condición para hacer la transformación es contar con un procedimiento eficiente que verifique el `output` dado por el algoritmo "Montecarlo" sea correcto, pues si lo tenemos podemos hacer un algoritmo "Las Vegas" que corra el "Montecarlo" hasta que este último entregue una respuesta correcta.

P4. a)

$$\begin{aligned}\mathbb{E}(X) &= \mathbb{E}\left(\sum_{e\in E} \mathbb{1}(e \textit{ conecta nodos de } V')\right) \\ &= \sum_{e\in E} \mathbb{P}(e \textit{ conecta nodos de } V')\end{aligned}$$

Ahora, para calcular esta probabilidad, tomemos una arista $e = (u, v) \in E$ y miremos la probabilidad de que el V' escogido contenga a u y v (que es la misma que $u, v \in V'$. Este calculo lo haremos pensando que hay $\binom{n}{r}$ formas de escoger V' y $\binom{n-2}{r-2}$ de estas contienen

tanto a u como a v. Es decir :

$$\begin{aligned}
\mathbb{E}(X) &= \sum_{e \in E} \mathbb{P}(e \textit{ conecta nodos de } V') \\
&= \sum_{e \in E} \frac{\binom{n-2}{r-2}}{\binom{n}{r}} \\
&= m \frac{\frac{(n-2)!}{(n-r)!(r-2)!}}{\frac{n!}{(n-r)!r!}} \\
&= m \frac{r(r-1)}{n(n-1)} \\
&\leq m \frac{r^2}{n^2}
\end{aligned}$$

b) Si tomamos $r = \frac{\epsilon n}{\sqrt{m}}$, por Markov tenemos que:

$$\begin{aligned}
\mathbb{P}(error) = \mathbb{P}(X \geq 1) &\leq \mathbb{E}(X) \\
&\leq m \left(\frac{\frac{\epsilon n}{\sqrt{m}}}{n} \right)^2 \\
&= \epsilon^2
\end{aligned}$$

,y entonces, $\mathbb{P}(no\ error) \geq 1 - \epsilon^2$