



Ayudantía 7

12 de octubre, 2018

Problema 1

Se tiene un conjunto S de n elementos. Además se tienen conjuntos $S_1, \dots, S_k$, donde $S_i \subseteq S$ y $|S_i| \geq r \forall i$. Dado conjuntos de esta forma, donde $k < 2^{r-2}$, se necesita asignar uno de dos colores a cada elemento, de forma que cada S_i tenga al menos un elemento de cada color.

- Describa un algoritmo de monte carlo que permita encontrar una coloración como la descrita en tiempo lineal, y acote su probabilidad de error.
- Describa un algoritmo de las vegas que permita encontrar una coloración como la descrita en tiempo lineal, y acote la probabilidad de que entregue **sin resultado**.

Solución:

- El algoritmo es simplemente asignar colores de manera aleatoria a los elementos de S . Para acotar la probabilidad de error, definamos las siguientes variables auxiliares:

$$C_i = \begin{cases} 1 & \text{todos los elementos de } S_i \text{ tienen color 0} \\ 0 & \text{en otro caso} \end{cases}$$

$$U_i = \begin{cases} 1 & \text{todos los elementos de } S_i \text{ tienen color 1} \\ 0 & \text{en otro caso} \end{cases}$$

Con esto podemos acotar la probabilidad de error:

$$\begin{aligned} Pr[error] &= Pr \left[\bigcup_{i=1}^k (C_i \cup U_i) \right] \\ &\leq \sum_{i=1}^k \left(\left(\frac{1}{2} \right)^r + \left(\frac{1}{2} \right)^r \right) \\ &= k \cdot \left(\frac{1}{2} \right)^{r-1} \\ &\leq 2^{r-2} \cdot \left(\frac{1}{2} \right)^{r-1} \\ &= \frac{1}{2} \end{aligned}$$

- Dada una coloración, es posible chequear si la coloración es válida en tiempo lineal (basta recorrer los conjuntos y verificar que cada uno tiene por lo menos un elemento de cada color. Esto asume que puedo recuperar la coloración de un elemento en $O(1)$). Dado que podemos chequear si una coloración es válida, podemos transformar el algoritmo de Monte Carlo anterior en un algoritmo de Las Vegas simplemente revisando que el resultado entregado

sea correcto. Por lo tanto, el algoritmo es: asignar colores de manera aleatoria, y si la coloración es válida entregarla como output. Si no es válida, entregar **sin resultado**.

La probabilidad de entregar **sin resultado** es igual a la probabilidad de error del algoritmo de monte carlo: $\frac{1}{2}$.

Problema 2

A necesita enviar un mensaje de m bits a B , quien conoce el largo del mensaje. Para esto, A representa el mensaje como un número M , define $p = \frac{M}{2^m}$ y luego envía a B un 1 con probabilidad p y 0 con probabilidad $(1 - p)$ todas las veces que sean necesarias. Luego B calcula el promedio de los primeros t mensajes y determina el entero M' que minimiza la distancia entre $M'/2^m$ y el promedio obtenido. B asume que el mensaje enviado es M' . ¿Cuanto debe ser t para que la probabilidad de error sea menor a ε ?

Solución:

Sean $X_1, \dots, X_t$ los mensajes enviados y $\overline{X_t} = \frac{X_1 + \dots + X_t}{t}$. Tenemos que

$$E[\overline{X_t}] = \frac{E[X_1] + \dots + E[X_t]}{t} = \frac{tp}{t} = p$$

Para estimar el mensaje M' , lo que hace B es simplemente calcular $\overline{X_t} \cdot 2^m$ y aproximar al entero más cercano. Eso minimiza la distancia entre $M'/2^m$ y $\overline{X_t}$. B se equivoca cuando la distancia entre $\overline{X_t} \cdot 2^m$ y M es mayor o igual a $\frac{1}{2}$, puesto que en ese caso al aproximar $\overline{X_t} \cdot 2^m$ se va a llegar al entero equivocado. Por lo tanto, tenemos que

$$\begin{aligned} Pr[error] &= Pr \left[|\overline{X_t} \cdot 2^m - M| \geq \frac{1}{2} \right] \\ &= Pr \left[|\overline{X_t} \cdot 2^m - p \cdot 2^m| \geq \frac{1}{2} \right] \\ &= Pr \left[|\overline{X_t} - p| \cdot 2^m \geq \frac{1}{2} \right] \\ &= Pr \left[|\overline{X_t} - p| \geq \frac{1}{2 \cdot 2^m} \right] \\ &= Pr \left[|\overline{X_t} - E[\overline{X_t}]| \geq \frac{1}{2 \cdot 2^m} \right] \end{aligned}$$

Esta ultima probabilidad puede ser acotada con la desigualdad de Chebyshev:

$$Pr[error] \leq Pr \left[|\overline{X_t} - E[\overline{X_t}]| \geq \frac{1}{2 \cdot 2^m} \right] \leq Var(\overline{X_t}) \cdot (2 \cdot 2^m)^2$$

Tenemos que

$$\begin{aligned} Var(\overline{X_t}) &= \left(\frac{1}{t} \right)^2 (Var(X_1) + \dots + Var(X_t)) \\ &= \left(\frac{1}{t} \right)^2 t \cdot (p(1 - p)) \\ &= \frac{p(1 - p)}{t} \end{aligned}$$

Así, necesitamos que

$$\frac{p(1 - p)}{t} \cdot (2 \cdot 2^m)^2 \leq \varepsilon$$

Notemos que $p(1-p)$ es siempre menor o igual a $\frac{1}{4}$. Por lo tanto, nos basta acotar que

$$\frac{(2 \cdot 2^m)^2}{4t} \leq \varepsilon$$

Esto se cumple cuando $t > \frac{2^m}{\varepsilon}$.

Problema 3

Sea φ una fórmula proposicional en DNF, vale decir, una fórmula de la forma $D_1 \vee \dots \vee D_m$, donde cada D_i es una conjunción de literales, es decir, una conjunción de variables proposicionales y negaciones de variables proposicionales. Por ejemplo, $(x_1 \wedge x_2) \vee (\neg x_2 \wedge x_3 \wedge \neg x_5) \vee (\neg x_2 \wedge \neg x_3)$ es una fórmula DNF. Suponemos que $m \geq 2$, cada conjunción D_i contiene $l_i \geq 1$ literales ($1 \leq i \leq m$), y que D_i no contiene literales repetidos ni complementarios (no contiene al mismo tiempo a una variable proposicional y a su negación).

En esta pregunta vamos a desarrollar un algoritmo aleatorizado para aproximar el número de valuaciones que satisfacen a φ , lo cual es denotado como $\#DNF(\varphi)$.

1. Defina $S_i = |\{\sigma \mid \sigma(D_i) = 1\}|$, para cada $i \in \{1, \dots, m\}$. ¿Cuál es el valor de S_i ? ¿Puede ser calculado de forma eficiente? Justifique su respuesta.

Solución:

Asumo que existen n variables $x_1, \dots, x_n$.

Luego, para satisfacer a D_i el valor de l_i variables está fijo (determinado por los literales de D_i), pero las otras $n - l_i$ variables son variables libres y pueden tomar cualquier valor. Cada una de las $n - l_i$ variables libres puede tomar uno de dos valores. Por lo tanto, $S_i = 2^{n-l_i}$.

Esto puede ser calculado fácilmente: basta determinar n , l_i y luego calcular 2^{n-l_i} , lo que se puede hacer todo en tiempo polinomial.

2. Defina $M = \sum_{i=1}^m S_i$ y $d(\sigma) = |\{i \in \{1, \dots, m\} \mid \sigma(D_i) = 1\}|$ para cada valuación σ . Utilizando estos valores, defina una variable aleatoria Y tal que para cada valuación σ se tiene que

$$Y(\sigma) = \begin{cases} \frac{M}{d(\sigma)} & \sigma(\varphi) = 1 \\ 0 & \sigma(\varphi) = 0 \end{cases}$$

Para obtener un valor de Y se realizan los siguientes pasos: escoger $i \in \{1, \dots, m\}$ con probabilidad $\frac{S_i}{M}$, luego escoger una valuación σ tal que $\sigma(D_i) = 1$ con distribución uniforme, y finalmente retornar $Y(\sigma)$. Demuestre las siguientes propiedades:

- Para cada valuación σ se tiene que $Pr(\text{escoger } \sigma) = \frac{d(\sigma)}{M}$
- $E(Y) = \#DNF(\varphi)$

Solución:

- Por probabilidades totales tenemos que

$$Pr[\text{escoger } \sigma] = \sum_{i=1}^m Pr[\text{escoger } \sigma \mid \text{se escogió } i] \cdot Pr[\text{escoger } i]$$

Tenemos que $Pr[\text{escoger } i] = \frac{S_i}{M}$ por enunciado. Además,

$$\begin{aligned} Pr[\text{escoger } \sigma \mid \text{se escogió } i] &= \begin{cases} \frac{1}{S_i} & \sigma(D_i) = 1 \\ 0 & \sigma(D_i) = 0 \end{cases} \\ &= \frac{\sigma(D_i)}{S_i} \end{aligned}$$

Por lo tanto,

$$\begin{aligned}
 Pr[\text{escoger } \sigma] &= \sum_{i=1}^m Pr[\text{escoger } \sigma \mid \text{se escogió } i] \cdot Pr[\text{escoger } i] \\
 &= \sum_{i=1}^m \frac{\sigma(D_i)}{S_i} \cdot \frac{S_i}{M} \\
 &= \sum_{i=1}^m \frac{\sigma(D_i)}{M} \\
 &= \frac{\sum_{i=1}^m \sigma(D_i)}{M} \\
 &= \frac{d(\sigma)}{M}
 \end{aligned}$$

■ Se tiene que

$$\begin{aligned}
 E(Y) &= \sum_{\sigma} Y(\sigma) \cdot Pr[\text{escoger } \sigma] \\
 &= \sum_{\sigma \mid \sigma(\varphi)=1} Y(\sigma) \cdot Pr[\text{escoger } \sigma] + \sum_{\sigma \mid \sigma(\varphi)=0} Y(\sigma) \cdot Pr[\text{escoger } \sigma] \\
 &= \sum_{\sigma \mid \sigma(\varphi)=1} Y(\sigma) \cdot Pr[\text{escoger } \sigma] \\
 &= \sum_{\sigma \mid \sigma(\varphi)=1} \frac{M}{d(\sigma)} \cdot \frac{d(\sigma)}{M} \\
 &= \sum_{\sigma \mid \sigma(\varphi)=1} 1 \\
 &= \#DNF(\varphi)
 \end{aligned}$$

3. Suponga que $Y_1, \dots, Y_k$ son k variables aleatorias independientes, y suponga que cada una de ellas es idéntica a Y . Demuestre que

$$E\left(\frac{1}{k} \sum_{i=1}^k Y_i\right) = E(Y)$$

Además, dado $\varepsilon \in (0, 1)$, demuestre que

$$Pr\left(\left|\frac{1}{k} \sum_{i=1}^k Y_i - E(Y)\right| \geq \varepsilon \cdot E(Y)\right) \leq \frac{Var(Y)}{k \cdot \varepsilon^2 \cdot E(Y)^2}$$

Solución:

■ Esto se desprende directamente de la linealidad de la esperanza:

$$E\left(\frac{1}{k} \sum_{i=1}^k Y_i\right) = \frac{1}{k} \sum_{i=1}^k E(Y_i) = \frac{1}{k} \sum_{i=1}^k E(Y) = \frac{k}{k} E(Y) = E(Y)$$

■ Se utiliza la desigualdad de Chebyshev:

$$\begin{aligned}
Pr\left(\left|\frac{1}{k}\sum_{i=1}^k Y_i - E(Y)\right| \geq \varepsilon \cdot E(Y)\right) &= Pr\left(\left|\frac{1}{k}\sum_{i=1}^k Y_i - E\left(\frac{1}{k}\sum_{i=1}^k Y_i\right)\right| \geq \varepsilon \cdot E(Y)\right) \\
&\leq \frac{Var\left(\frac{1}{k}\sum_{i=1}^k Y_i\right)}{\varepsilon^2 E(Y)^2} \\
&= \frac{\frac{1}{k^2} k Var(Y)}{\varepsilon^2 E(Y)^2} \\
&= \frac{Var(Y)}{k \cdot \varepsilon^2 \cdot E(Y)^2}
\end{aligned}$$

4. Demuestre que para cada valuación σ tal que $\sigma(\varphi) = 1$ se tiene que $\frac{M}{m} \leq Y(\sigma) \leq M$. A partir de esto demuestre que $\frac{M}{m} \leq E(Y) \leq M$.

Solución:

Se tiene que $Y(\sigma) = \frac{M}{d(\sigma)}$, donde $1 \leq d(\sigma) \leq m$ puesto que $\sigma(\varphi) = 1$. Por lo tanto, reemplazando $d(\sigma)$ se obtiene que $\frac{M}{m} \leq Y(\sigma) \leq M$.

Además, se tiene que $\min_{\sigma} (Y(\sigma)) \leq E(Y) \leq \max_{\sigma} (Y(\sigma))$. En otras palabras, el valor esperado de Y está entre el mínimo y el máximo de Y . Como Y está acotado entre $\frac{M}{m}$ y M , esto implica que la esperanza también está acotada en este rango, es decir, $\frac{M}{m} \leq E(Y) \leq M$.

5. Demuestre que

$$Var(Y) \leq \left(\frac{M}{m}\right)^2 \cdot (m-1)^2$$

A partir de esto demuestre que:

$$\frac{Var(Y)}{E(Y)^2} \leq (m-1)^2$$

Solución:

Por el ítem anterior se sabe que $Y - E(Y) \leq M - \frac{M}{m}$. Por lo tanto, tenemos que

$$\begin{aligned}
Var(Y) &= E([Y - E(Y)]^2) \\
&\leq E\left(\left[M - \frac{M}{m}\right]^2\right) \\
&= \left[M - \frac{M}{m}\right]^2 \\
&= \left(\frac{Mm - M}{m}\right)^2 \\
&= \left(\frac{M(m-1)}{m}\right)^2 \\
&= \left(\frac{M}{m}\right)^2 \cdot (m-1)^2
\end{aligned}$$

Además, por el ítem anterior también sabemos que $\frac{M}{m} \leq E(Y)$. Reemplazando en la inecuación anterior se obtiene

$$\begin{aligned}
\text{Var}(Y) &\leq \left(\frac{M}{m}\right)^2 \cdot (m-1)^2 \\
&\leq E(Y)^2 \cdot (m-1)^2 \\
\Rightarrow \frac{\text{Var}(Y)}{E(Y)^2} &\leq (m-1)^2
\end{aligned}$$

6. Utilizando los resultados anteriores demuestre que para cada $\varepsilon \in (0, 1)$

$$Pr\left(\frac{|\frac{1}{k}\sum_{i=1}^k Y_i - \#DNF(\varphi)|}{\#DNF(\varphi)} < \varepsilon\right) \geq 1 - \frac{(m-1)^2}{k \cdot \varepsilon^2}$$

En particular, indique qué valor del número de muestras k nos asegura que vamos a tener un error menor al 1 % con probabilidad $\frac{99}{100}$, vale decir, qué valor de k nos asegura que:

$$Pr\left(\frac{|\frac{1}{k}\sum_{i=1}^k Y_i - \#DNF(\varphi)|}{\#DNF(\varphi)} < \frac{1}{100}\right) \geq \frac{99}{100}$$

Solución:

Tenemos que

$$\begin{aligned}
Pr\left(\frac{|\frac{1}{k}\sum_{i=1}^k Y_i - \#DNF(\varphi)|}{\#DNF(\varphi)} < \varepsilon\right) &= Pr\left(\frac{|\frac{1}{k}\sum_{i=1}^k Y_i - E(Y)|}{E(Y)} < \varepsilon\right) \\
&= Pr\left(\left|\frac{1}{k}\sum_{i=1}^k Y_i - E(Y)\right| < \varepsilon \cdot E(Y)\right) \\
&= 1 - Pr\left(\left|\frac{1}{k}\sum_{i=1}^k Y_i - E(Y)\right| \geq \varepsilon \cdot E(Y)\right) \\
&= 1 - \frac{\text{Var}(Y)}{k \cdot \varepsilon^2 \cdot E(Y)^2} && \text{(Por la parte 3)} \\
&\geq 1 - \frac{(m-1)^2}{k \cdot \varepsilon^2} && \text{(Por la parte 5)}
\end{aligned}$$

Para acotar el valor de k basta satisfacer

$$1 - \frac{(m-1)^2}{k \cdot \varepsilon^2} \geq \frac{99}{100}$$

con $\varepsilon = \frac{1}{100}$. Despejando k se obtiene

$$\begin{aligned}
1 - \frac{(m-1)^2}{k \cdot \frac{1}{100^2}} &\geq \frac{99}{100} \\
\frac{1}{100} &\geq \frac{100^2(m-1)^2}{k} \\
k &\geq 100^3(m-1)^2
\end{aligned}$$

Problema 4

- Demuestre que un número es divisible por 11 si y solo si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

Solución:

Sea $x = \sum_{i=0}^{n-1} 10^i x_i$ un número cualquiera de n dígitos, donde los x_i son los dígitos de x . Sin pérdida de generalidad se asume que el número de dígitos es par (si no lo fuera, basta agregar un dígito 0 a la izquierda). Tenemos que

$$\begin{aligned}
11 \mid x &\iff x \equiv 0 \pmod{11} \\
&\iff \sum_{i=0}^{n-1} 10^i x_i \equiv 0 \pmod{11} \\
&\iff \sum_{i=0}^{n-1} (-1)^i x_i \equiv 0 \pmod{11} \\
&\iff \sum_{i=0}^{\frac{n}{2}-1} (-1)^{2i} x_{2i} + \sum_{i=0}^{\frac{n}{2}-1} (-1)^{2i+1} x_{2i+1} \equiv 0 \pmod{11} \\
&\iff \sum_{i=0}^{\frac{n}{2}-1} x_{2i} + \sum_{i=0}^{\frac{n}{2}-1} -x_{2i+1} \equiv 0 \pmod{11} \\
&\iff \sum_{i=0}^{\frac{n}{2}-1} x_{2i} - \sum_{i=0}^{\frac{n}{2}-1} x_{2i+1} \equiv 0 \pmod{11} \\
&\iff 11 \mid \sum_{i=0}^{\frac{n}{2}-1} x_{2i} - \sum_{i=0}^{\frac{n}{2}-1} x_{2i+1}
\end{aligned}$$

- Demuestre que un número n es divisible por 7 si y solo si al extraer el último dígito de n , multiplicarlo por 2 y restárselo al resto de los dígitos, entonces se obtiene otro número divisible por 7. Por ejemplo, 133 es divisible por 7 pues $13-3 \cdot 2=7$ es divisible por 7.

Solución:

Sea x igual al ejercicio anterior. Tenemos que

$$\begin{aligned}
7 \mid x &\iff x \equiv 0 \pmod{7} \\
&\iff \sum_{i=0}^{n-1} 10^i x_i \equiv 0 \pmod{7} \\
&\iff \sum_{i=1}^{n-1} 10^i x_i + 10^0 x_0 \equiv 0 \pmod{7} \\
&\iff \sum_{i=1}^{n-1} 10^i x_i + x_0 \equiv 0 \pmod{7} \\
&\iff \sum_{i=1}^{n-1} 10^i x_i - 20x_0 \equiv 0 \pmod{7} \\
&\iff 10 \left(\sum_{i=1}^{n-1} 10^{i-1} x_i - 2x_0 \right) \equiv 0 \pmod{7} \\
&\iff \sum_{i=1}^{n-1} 10^{i-1} x_i - 2x_0 \equiv 0 \pmod{7} \\
&\iff 7 \mid \sum_{i=1}^{n-1} 10^{i-1} x_i - 2x_0
\end{aligned}$$

donde el penúltimo paso es válido pues 7 es primo y $10 \not\equiv 0 \pmod{7}$.