



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC2283 Diseño y análisis de algoritmos
2° semestre 2019

Ayudantía 7

Dudas a Antonio López (alopez7@uc.cl)

Problema 1

Dados dos polinomios $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ en $\mathbb{Q}$, decimos que $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ son equivalentes si para toda secuencia $a_1, \dots, a_n$ de números en $\mathbb{Q}$ se tiene que $p(a_1, \dots, a_n) = q(a_1, \dots, a_n)$.

Dados dos polinomios $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ en $\mathbb{Q}$, decimos que $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ son linealmente-equivalentes si existe un polinomio $r(x_1, \dots, x_n)$ tal que: (i) $r(x_1, \dots, x_n)$ es nulo o es un polinomio de grado menor o igual a 1, y (ii) $p(x_1, \dots, x_n)$ es equivalente a $q(x_1, \dots, x_n) + r(x_1, \dots, x_n)$. Por ejemplo los polinomios $p(x, y) = x(x-1) + 2y$ y $q(x, y) = (x-1)(x-2) + y + 1$ son linealmente-equivalentes puesto que

$$p(x, y) = q(x, y) + r(x, y)$$

donde $r(x, y) = 2x + y - 3$.

De un algoritmo aleatorizado que resuelva el problema de determinar si dos polinomios $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ son linealmente-equivalentes. Su algoritmo debe funcionar en tiempo polinomial en el peor caso y su probabilidad de error debe ser menor o igual a $\frac{1}{2^{100}}$. Además, usted debe justificar claramente por qué su algoritmo es correcto, funciona en tiempo polinomial y tiene probabilidad de error acotada por $\frac{1}{2^{100}}$.

Solución: Nuestro objetivo es crear un polinomio lineal a partir de la diferencia de p con q y luego comprobar si es equivalente a $p - q$ usando el algoritmo aleatorizado visto en clases. En concreto construiremos un polinomio $r = a_0 + a_1 \cdot x_1 + \dots + a_n \cdot x_n$, donde cada a_i se obtiene a partir de $p - q$. Algoritmo es como sigue:

function LINEALMENTE-EQUIVALENTES(p, q)

```
 $r = p - q$   
 $coefs[0..n] = [0, \dots, 0]$   
 $coefs[0] = r(0, \dots, 0)$   
for  $i = 1..n$  do  
   $v = (0, \dots, 0)$   
   $v[i] = 1$   
   $coefs[i] = r(v) - coefs[0]$   
 $rp(x_1, \dots, x_n) = coefs[0] + coefs[1] \cdot x_1 + \dots + coefs[n] \cdot x_n$   
return EquivPolAleatorizado( $r, rp$ )
```

El algoritmo es correcto ya que si p es linealmente-equivalente a q , r es equivalente a rp , y si p no es linealmente-equivalente a q , el algoritmo retorna **false** con probabilidad $\frac{1}{100}$. Por lo tanto la probabilidad de error del algoritmo es $\frac{1}{100}$. Para que la probabilidad de error sea menor a $\frac{1}{2^{100}}$ es necesario que se ejecute 16 veces.

Problema 2

Dados dos polinomios $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ en $\mathbb{Q}$, decimos que $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ son equivalentes si para toda secuencia $a_1, \dots, a_n$ de números en $\mathbb{Q}$ se tiene que $p(a_1, \dots, a_n) = q(a_1, \dots, a_n)$.

Decimos que un polinomio $r(x_1, \dots, x_n)$ es una forma cuadrática si

$$r(x_1, \dots, x_n) = \sum_{i=1}^n \sum_{j=i}^n a_{i,j} x_i x_j$$

donde cada $a_{i,j} \in \mathbb{Q} \forall (1 \leq i, j \leq n)$

De un algoritmo aleatorizado que resuelva el problema de determinar si un polinomio $p(x_1, \dots, x_n)$ es equivalente a una forma cuadrática. Su algoritmo debe funcionar en tiempo polinomial en el peor caso y su probabilidad de error debe ser menor a $\frac{1}{2^{100}}$. Además, usted debe justificar claramente por qué su algoritmo es correcto, funciona en tiempo polinomial y tiene probabilidad de error acotada por $\frac{1}{2^{100}}$.

Solución: Este problema es similar al anterior solo que hay que construir la forma cuadrática y luego comparar los polinomios construidos con el algoritmo visto en clases. El algoritmo es el siguiente:

```
function FORMA_CUADRÁTICA( $r$ )
   $coefs[1..n, 1..n] = [0, \dots, 0]$ 
  for  $i = 1..n$  do
     $v = (0, \dots, 0)$ 
     $v[i] = 1$ 
     $coefs[i, i] = r(v)$ 
  for  $i = 1..n$  do
    for  $j = i + 1..n$  do
       $v = (0, \dots, 0)$ 
       $v[i] = 1$ 
       $v[j] = 1$ 
       $coefs[i, j] = r(v) - coefs[i, i] - coefs[j, j]$ 
   $rp =$  Construir polinomio cuadrático con coeficientes  $coefs$ 
  return EquivPolAleatorizado( $r, rp$ )
```

Al igual que antes si los polinomios resultantes son equivalentes entonces retorna **true** y si no, se equivoca con probabilidad $\frac{1}{100}$.

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 posicionales 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 en 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 tiene literales repetidos ni complementarios (no contiene al mismo tiempo 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 $S_i = |\{\sigma | \sigma(D_i) = 1\}|$, 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 $d(\sigma) = |\{i \in \{1, \dots, m\} | \sigma(D_i) = 1\}|$ 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 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

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

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

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

Por lo tanto,

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

$$\begin{aligned}
&= \frac{\sum_{i=1}^m \sigma(D_i)}{M} \\
&= \frac{d(\sigma)}{M}
\end{aligned}$$

- Se tiene que

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

3. Suponga que $Y_1, \dots, Y_k$ son k variables aleatorias independientes, y 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:

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

- Se utiliza la desigualdad de Chebyshev:

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

$$\begin{aligned}
&= \frac{\frac{1}{k^2}k \cdot \text{Var}(Y)}{\varepsilon^2 \cdot E(Y)^2} \\
&= \frac{\text{Var}(Y)}{k \cdot \varepsilon^2 \cdot E(Y)^2}
\end{aligned}$$

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 ese rango, es decir, $\frac{M}{m} \leq E(Y) \leq M$.

5. Demuestre que

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

A partir de esto demuestre que:

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

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

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

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

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

$$\leq E(Y)^2 \cdot (m-1)^2$$

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

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

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

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:

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

Solución: Tenemos que

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

Por la parte 3,

$$= 1 - \frac{\text{Var}(Y)}{k \cdot \varepsilon^2 \cdot E(Y)^2}$$

Por la parte 5,

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

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

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

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

$$k \geq 100^3(m-1)^2$$