



PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Diseño y Análisis de Algoritmos - IIC2283

Interrogación 3

Tiempo: 2.5 horas

1. En esta pregunta usted debe demostrar la Identidad de Bézout, para luego generalizarla.

- (a) [1 punto] Demuestre que para cada par $a, b \in \mathbb{N}$ tal que $a, b > 0$, existen $s, t \in \mathbb{Z}$ tales que:

$$\text{MCD}(a, b) = s \cdot a + t \cdot b$$

- (b) [0.5 puntos] Demuestre que para cada secuencia $a_1, \dots, a_k \in \mathbb{N}$ tal que $k \geq 2$ y $a_1, \dots, a_k > 0$, existen $s_1, \dots, s_k \in \mathbb{Z}$ tales que:

$$\text{MCD}(a_1, \dots, a_k) = s_1 \cdot a_1 + \dots + s_k \cdot a_k$$

2. 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 en DNF. Suponemos que $m \geq 2$, cada conjunción D_i contiene $\ell_i \geq 1$ literales ($1 \leq i \leq m$), y que D_i no contiene literales repetidos ni complementarios (no contiene al mismo tiempo a una variables 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 $\#\text{DNF}(\varphi)$.

- (a) [0.3 puntos] 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 manera eficiente? Justifique su respuesta
- (b) 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 realiza 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.

- (b.1) [0.4 puntos] Para cada valuación σ se tiene que $\Pr(\sigma) = \frac{d(\sigma)}{M}$
- (b.2) [0.4 puntos] $E(Y) = \#\text{DNF}(\varphi)$
- (c) [0.5 puntos] 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:

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

- (d) [0.3 puntos] 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 $\frac{M}{m} \leq E(Y) \leq M$.
- (e) [0.6 puntos] Demuestre que:

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

A partir de esto demuestre que:

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

- (f) [0.5 puntos] 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 asegura que:

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

3. [1.5 puntos] Dados dos polinomios $p(x_1, \dots, x_n)$ y $q(x_1, \dots, x_n)$ en $\mathbb{Q}$, recuerde que 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 $p(a_1, \dots, a_n) = q(a_1, \dots, a_n)$. Además, decimos que un polinomio $r(x_1, \dots, x_n)$ es una forma cuadrática si

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

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

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 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 $\frac{1}{2^{100}}$.