Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC2283 - Diseño y Análisis de Algoritmos - 2do semestre 2022

INTERROGACIÓN 2

Puntaje: Cada pregunta posee el mismo puntaje. Cada ítem dentro de una misma pregunta posee el mismo puntaje. Ítems de preguntas entregadas en blanco se evaluarán con un puntaje correspondiente a obtener 0.5 puntos de 6 en ese ítem.

Pregunta 1

Sea $a \in \mathbb{Z} - \{0\}$ y $n \in \mathbb{N} - \{0\}$. Demuestre que a tiene inverso en módulo n si, y solo si, $\gcd(a, n) = 1$

Pregunta 2

Sea **Moneda**() un procedimiento que retorna 1 con probabilidad p y 0 con probabilidad $1 - p$, donde $p \in [0, 1]$. Se define el procedimiento **EstimarMoneda**() como el siguiente algoritmo:

EstimarMoneda(n)
    $s := 0$
    for $i := 1$ **to** n **do**
        $s := s +$ **Moneda**()
    return $\frac{s}{n}$

1. Dado $\epsilon \in (0, 1)$, demuestre que:

$$\Pr(|\textbf{EstimarMoneda}(n) - p| < \epsilon) \geq 1 - \frac{p(1-p)}{n\epsilon^2}$$

2. Calcule un valor de n tal que para todo $p \in [0, 1]$, el valor retornado por **EstimarMoneda**(n) tiene un error de estimación de p de a lo más 1% con una probabilidad mayor o igual a $\frac{999}{1000}$. Es decir, el valor de n encontrado debe satisfacer:

$$\forall p \in [0, 1].\ \Pr\left(|\textbf{EstimarMoneda}(n) - p| < \frac{1}{100}\right) \geq \frac{999}{1000}$$

   Hint: Puede utilizar el resultado del ítem anterior aunque no lo haya demostrado.

Pregunta 3

Considere el siguiente algoritmo de Las Vegas que realiza una búsqueda de un elemento x en una lista desordenada $L[1 \ldots n]$ que NO tiene elementos repetidos.

BúsquedaAleatoria($L[1 \ldots n], x$)
    escoja al azar y con distribución uniforme un número i
        del conjunto de números naturales $\{1, ..., n\}$
    if $L[i] = x$
        return i
    else
        return *sin_resultado*

1. Encuentre el número esperado de veces que se debería ejecutar **BúsquedaAleatoria** en promedio hasta obtener una respuesta correcta en función de n. Puede asumir que el elemento x siempre estará presente en $L[1 \dots n]$.

2. Construya un algoritmo de Monte Carlo a partir del algoritmo **BúsquedaAleatoria** que resuelva el mismo problema y cuya probabilidad de error sea a lo más $\frac{1}{2}$. Explique por qué su algoritmo cumple con lo pedido.

   Hint: La desigualdad
   $$\left(1 - \frac{1}{n}\right)^{an} < e^{-a}$$
   que se cumple para $a > 0$ y $n \geq 1$ puede resultar útil.

3. Demuestre un caso general del punto anterior. Sea $\mathcal{A}$ un algoritmo de Las Vegas tal que el tiempo esperado total de un algoritmo que ejecuta $\mathcal{A}$ hasta obtener una respuesta correcta es $T(n)$. Demuestre que para cada $c \geq 0$ siempre existe un algoritmo $\mathcal{B}$ de Monte Carlo que computa el mismo problema que $\mathcal{A}$ en tiempo $c \cdot T(n)$ y cuya probabilidad de error es a lo más $1/c$.

Formulario

Algoritmos aleatorizados

Un algoritmo de **Monte Carlo** es tal que siempre entrega una respuesta, pero esa respuesta puede tener una probabilidad de estar errada.

Un algoritmo de **Las Vegas** es tal que, si entrega respuesta, esta es correcta, pero puede existir una probabilidad de que el algoritmo no entregue respuesta.

Medidas sobre variables aleatorias

Para una variable aleatoria X de recorrido $\Omega \subseteq \mathbb{R}$ la **esperanza** de X (denotada como $\mathrm{E}(X)$) se define como:

$$\mathrm{E}(X) = \sum_{r \in \Omega} r \cdot \Pr(X = r)$$

Por otro lado, la **varianza** de X (denotada como $\mathrm{Var}(X)$) se define como:

$$\mathrm{Var}(X) = \mathrm{E}((X - \mathrm{E}(X))^2) = \mathrm{E}(X^2) - \mathrm{E}(X)^2$$

Distribuciones útiles

Una variable aleatoria X sigue una distribución de Bernoulli de parámetro $0 < p < 1$ (denotada como $X \sim \mathrm{Bernoulli}(p)$) si:

$$\Pr(X = x) = \begin{cases} 1 - p & \text{si } x = 0 \\ p & \text{si } x = 1 \end{cases}$$

En particular se tiene que si $X \sim \mathrm{Bernoulli}(p)$ entonces:

$$\mathrm{E}(X) = p \qquad \mathrm{Var}(X) = p(1 - p)$$

Por otro lado, una variable aleatoria X sigue una distribución geométrica con parámetro $0 < p < 1$ (denotada como $X \sim \mathrm{Geométrica}(p)$) si:

$$\Pr(X = x) = p(1 - p)^x$$

En particular se tiene que si $X \sim \mathrm{Geométrica}(p)$ entonces:

$$\mathrm{E}(X) = \frac{1}{p} \qquad \mathrm{Var}(X) = \frac{1 - p}{p^2}$$

Desigualdades importantes

Sea X una variable aleatoria no negativa. Luego para todo $a \in \mathbb{R}^+$ se cumple la **desigualdad de Markov**:

$$\Pr(X \geq a) \ \leq \ \frac{\mathrm{E}(X)}{a}$$

Un caso particular de la desigualdad anterior es la **desigualdad de Chebyshev**:

$$\Pr(|X \geq \mathrm{E}(X)| \geq a) \ \leq \ \frac{\mathrm{Var}(X)}{a^2}$$

Máximo común divisor

Sean $a, b \in \mathbb{Z} - \{0\}$. Se define el **máximo común divisor** $\gcd(a, b)$ de a y b como el mayor número d tal que d divide a a y a b al mismo tiempo (es decir $d \mid a$ y $d \mid b$).

Inverso modular

Para $a, b, n \in \mathbb{Z} - \{0\}$, decimos que b es **inverso de** a **en módulo** n si

$$a \cdot b \equiv 1 \pmod{n}$$

Identidad de Bézout

Para cada $a, b \in \mathbb{N}$ tales que $a \neq 0$ o $b \neq 0$, existen $s, t \in \mathbb{Z}$ tales que

$$\gcd(a, b) = s \cdot a + t \cdot b$$