



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

Diseño y Análisis de Algoritmos - IIC2283
Rúbrica Interrogación 2

1. En esta pregunta usted va a analizar un algoritmo para transformar una moneda cargada en una moneda no cargada. De manera más precisa, sea **Moneda()** un procedimiento que retorna 0 con probabilidad p y 1 con probabilidad $1 - p$, donde $0 < p < 1$, y defina **Lanzar()** como el siguiente algoritmo:

```
Lanzar()  
   $a_1 := \text{Moneda}()$   
   $a_2 := \text{Moneda}()$   
  if  $a_1 \neq a_2$  then return  $a_1$   
  else return sin_resultado
```

- (a) [0.7 puntos] Calcule $\Pr(\text{Lanzar}() \text{ retorne sin_resultado})$.

Corrección: Se asigna 0.7 puntos por calcular correctamente la probabilidad pedida

- (b) [0.7 puntos] Demuestre que $\Pr(\text{Lanzar}() \text{ retorne } 0) = \Pr(\text{Lanzar}() \text{ retorne } 1)$, vale decir, **Lanzar()** se puede considerar como una moneda no cargada.

Corrección: Se asigna 0.7 puntos por demostrar que ambas probabilidades son iguales. Esta demostración puede hacerse calculando ambas probabilidades, o razonando directamente sobre ellas.

- (c) [0.6 puntos] Considere la siguiente versión modificada del algoritmo **Lanzar()**:

```
RepLanzar()  
   $a_1 := \text{Moneda}()$   
   $a_2 := \text{Moneda}()$   
  while  $a_1 = a_2$   
     $a_1 := \text{Moneda}()$   
     $a_2 := \text{Moneda}()$   
  return  $a_1$ 
```

Indique cuál es el número esperado de veces que se debe llamar al procedimiento **Moneda()** hasta que **RepLanzar()** entregue un resultado. Nótese que este número esperado es una función de p , y recuerde que p es la probabilidad de que **Moneda()** retorne 0.

Corrección: El puntaje de esta pregunta se asigna de la siguiente forma.

- [0.3 puntos] Se explica a qué corresponde el valor a calcular (por ejemplo, se indica que corresponde a la esperanza de una variable aleatoria con distribución geométrica de parámetro p).
 - [0.6 puntos] Se explica a qué corresponde el valor a calcular y se realiza correctamente el cálculo.
2. [1.6 puntos] Dada una función $f : A \rightarrow B$, recuerde que: (i) f es 1-1 si para cada $a, b \in A$ tal que $a \neq b$, se tiene que $f(a) \neq f(b)$; (ii) f es sobre si para cada $b \in B$, existe $a \in A$ tal que $f(a) = b$; (iii) f es biyectiva si f es 1-1 y sobre. Además, dada una función $g : B \rightarrow C$, recuerde que la composición $(g \circ f) : A \rightarrow C$ es una función definida como $(g \circ f)(x) = g(f(x))$. Sea $n \geq 1$ un número natural, y sea \mathcal{B}_n el conjunto de todas las biyecciones $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. Demuestre que (\mathcal{B}_n, \circ) es un grupo, donde \circ es la composición de funciones.

Corrección: El puntaje de esta pregunta se asigna de la siguiente forma.

- [0.4 puntos] Se demuestra que la operación \circ es cerrada en \mathcal{B}_n (vale decir, \circ es una función de $\mathcal{B}_n \times \mathcal{B}_n$ en \mathcal{B}_n).
 - [0.8 puntos] Se demuestra que la operación \circ es cerrada en \mathcal{B}_n y que la operación \circ es asociativa.
 - [1.2 puntos] Se demuestra que la operación \circ es cerrada en \mathcal{B}_n , que la operación \circ es asociativa y que la función identidad $f(x) = x$ es el elemento neutro.
 - [1.6 puntos] Se demuestra que la operación \circ es cerrada en \mathcal{B}_n , que la operación \circ es asociativa, que la función identidad $f(x) = x$ es el elemento neutro, y que cada función $f \in \mathcal{B}_n$ tiene un inverso en \mathcal{B}_n bajo la operación \circ .
3. Sea p un número primo.
- (a) [1.2 puntos] Demuestre que un polinomio $r(x)$ de grado k tiene a lo más k raíces en módulo p , vale decir, existen a lo más k elementos $a \in \{0, \dots, p-1\}$ tales que $r(a) \equiv 0 \pmod{p}$.

Corrección: El puntaje de esta pregunta se asigna de la siguiente forma.

- [0.6 puntos] La idea de la demostración es correcta, aunque puede estar incompleta.
- [1.2 puntos] La idea de la demostración y su formalización son correctas.

- (b) [1.2 puntos] Suponiendo que p es impar, sean

$$\begin{aligned} S_p^+ &= \{a \in \mathbb{Z}_p^* \mid a^{\frac{p-1}{2}} \equiv 1 \pmod{p}\}, \\ S_p^- &= \{a \in \mathbb{Z}_p^* \mid a^{\frac{p-1}{2}} \equiv -1 \pmod{p}\}. \end{aligned}$$

Demuestre que $|S_p^+| = |S_p^-| = \frac{p-1}{2}$.

Corrección: El puntaje de esta pregunta se asigna de la siguiente forma.

- [0.6 puntos] La idea de la demostración es correcta, aunque puede estar incompleta.
- [1.2 puntos] La idea de la demostración y su formalización son correctas.