IIC2283 — Diseño y Análisis de Algoritmos
Ayudantía 10

Problema 1

Un grupo G es conmutativo cuando para todos $x, y \in G$, se cumple que $xy = yx$. Como notación, se definirá que $[a, b] = a^{-1}b^{-1}ab$.

Parte 1 Demuestre que $ab = ba$ si y solo si $[a, b] = 1$.

Solución Si $ab = ba$, entonces

$$\begin{aligned} aba^{-1}b^{-1} &= baa^{-1}b^{-1} \\ &= bb^{-1} \\ &= 1 \end{aligned}$$

y en sentido contrario, $aba^{-1}b^{-1} = 1$ implica

$$\begin{aligned} aba^{-1}b^{-1}ba &= ba \\ aba^{-1}a &= ba \\ ab &= ba \end{aligned}$$

Parte 2 Decimos que un grupo G es *generado por* $S \subseteq G$ si todo elemento $g \in G$ se puede obtener como el producto de elementos de S, o inversos de elementos de S. Es decir, si $g \in G$, y G es generado por S, entonces $g = x_1 \cdots x_n$, donde x_i o x_i^{-1} pertenece a S.

Desarrolle y analice un algoritmo que dados un conjunto finito $S = (g_1, \ldots, g_n)$, y una operación binaria como caja negra, determine si el grupo generado por S es conmutativo.

Al decir que la operación binaria funciona como caja negra, nos referimos a que es posible obtener el resultado de $a \circ b$ en tiempo $O(1)$, pero no se conoce el funcionamiento interno de la función. Para esto, se asume que la función define un grupo.

Idea de solución El algoritmo es verificar si los generadores conmutan entre si:

```
function VERIFICAR({g_1, ..., g_n})
    for i = 1, ..., n do
        for j = 1, ..., n do
            if g_i g_j ≠ g_j g_i then
                return NO
            end if
        end for
    end for
    return SI
end function
```

Este algoritmo funciona en tiempo $O(n^2)$ en el peor caso. Para demostrar que el resultado es correcto, falta verificar que $g_i g_j^{-1} = g_j^{-1} g_i$, y que $g_i^{-1} g_j^{-1} = g_j^{-1} g_i^{-1}$. Con esas dos propiedades, como todos los elementos del grupo generado corresponden a productos de generadores, o inversos de generadores, y estos conmutan entre si, entonces si $a = x_1 \cdots x_m$ y $b = y_1 \cdots y_k$:

$$ab = x_1 \cdots x_m \cdot y_1 \cdots y_k = y_1 \cdots y_k \cdot x_1 \cdots x_m = ba$$

Parte 3 Dado un grupo G, se define el centro de G como:

$$Z(G) = \{x \in G | \text{ para todo } y \in G \text{ se cumple que } [x, y] = 1\}$$

y además, para cada elemento $g \in G$, el centralizador de g como:

$$C(g) = \{x \in G | [x, g] = 1\}$$

Demuestre que $Z(G)$ es un subgrupo de G, y que para todo $g \in G$, $C(g)$ también es un subgrupo.

Idea de solución Se demuestra que $Z(G)$ es subgrupo. La otra parte es similar. Para esto, se verifican las propiedades:

- Por construcción $Z(G)$ es un subconjunto de G,
- Por definición, $1 \in Z(G)$,
- Si $a, b \in Z(G)$, entonces se verifica ab: para todo $t \in G$

  $$abt = a(bt) = a(tb) = (at)b = tab$$

  y por lo tanto $ab \in Z(G)$
- Si $a \in Z(G)$, entonces para todo $t \in G$:

  $$\begin{aligned} at &= ta \\ t &= a^{-1}ta \\ ta^{-1} &= a^{-1}t \end{aligned}$$

  y por lo tanto $a^{-1} \in Z(G)$.

Parte 4 Dado un grupo $G = \langle g_1, \ldots, g_n \rangle$, definimos un subproducto aleatorio como

$$g_1^{\epsilon_1} \cdots g_n^{\epsilon_n} \in G$$

donde los valores de $\{\epsilon_i\}_i$ son elegidos de forma uniforme e independiente desde $\{0, 1\}$.

Demuestre que si H es un subgrupo propio de G, entonces:

$$Pr[g_1^{\epsilon_1} \cdots g_n^{\epsilon_n} \notin H] \geq \frac{1}{2}$$

Para esto puede ser útil definir $\ell = \text{mín}\{i | g_i \notin H\}$, y luego expresar el subproducto aleatorio como $u g_\ell^{\epsilon_\ell} v$.

Idea de solución Se necesita calcular $\mathbf{Pr}[u g_\ell^{\epsilon_\ell} v \notin H]$. Para eso, se utilizan probabilidades totales, dependiendo de si v pertenece o no a H:

$$\mathbf{Pr}[u g_\ell^{\epsilon_\ell} v \notin H] = \mathbf{Pr}[u g_\ell^{\epsilon_\ell} v \notin H | v \in H] p + \mathbf{Pr}[u g_\ell^{\epsilon_\ell} v \notin H | v \notin H](1 - p)$$

donde $p = \mathbf{Pr}[v \in H]$. En el primer término, si $v \in H$, entonces $u g_\ell^{\epsilon_\ell} v \notin H$ si y solo si $\epsilon_\ell = 1$, lo que ocurre con probabilidad $1/2$. Por otra parte, si $v \notin H$, y $\epsilon_\ell = 0$, entonces $u g_\ell^{\epsilon_\ell} v \notin H$, por lo tanto la segunda probabilidad condicional es mayor o igual a $1/2$. Luego:

$$\mathbf{Pr}[u g_\ell^{\epsilon_\ell} v \notin H] \geq 1/2p + 1/2(1 - p) = 1/2.$$

Parte 5 Proponga y analice un algoritmo aleatorizado que dados generadores $(g_1, \ldots, g_n) = S$, y una operación binaria como caja negra, determine si el grupo generado por S es conmutativo.

Idea de solución Generar dos subproductos aleatorios independientes h_1, h_2, y verificar si $h_1 h_2 = h_2 h_1$. Si son iguales, retornar que es conmutativo, y si son distintos, retornar que no es conmutativo. Esto requiere una cantidad lineal de operaciones del grupo, por lo que es más eficiente que el algoritmo de la parte 2.

Para acotar la probabilidad de error, se tiene que si el grupo es conmutativo, entonces retorna SI con probabilidad 1. Por otra parte, si no es conmutativo, entonces se necesita acotar la probabilidad de que los subproductos aleatorios conmuten entre sí. Para esto, se considera $\Pr[h_1 \notin C(h_2) | G \text{ no es conmutativo}]$:

$$\Pr[h_1 \notin C(h_2)] = \Pr[h_1 \notin C(h_2) | h_2 \in Z(G)] \Pr[h_2 \in Z(G)] + \Pr[h_1 \notin C(h_2) | h_2 \notin Z(G)] \Pr[h_2 \notin Z(G)]$$

Luego, se utilizan los siguientes resultados:

$$\begin{aligned} \Pr[h_1 \notin C(h_2) | h_2 \in Z(G)] &= 0 \\ \Pr[h_1 \notin C(h_2) | h_2 \notin Z(G)] &\geq 1/2 \\ \Pr[h_2 \notin Z(G)] &\geq 1/2 \end{aligned}$$

para obtener que $\Pr[h_1 \notin C(h_2)] \geq 1/4$. Luego, se concluye que

$$\Pr[h_1 h_2 = h_2 h_1 | G \text{ no es conmutativo}] \leq 3/4$$

Problema 2

Proponga y analice un algoritmo que permita evaluar

$$1 + x + x^2 + \cdots + x^n \mod m$$

de forma eficiente. Para esto considere primero el caso con m primo, y luego el caso general. Para el análisis se considera que las operaciones básicas son la multiplicación módulo m, y el cálculo de $x \mod y$.

Idea de solución Si $x \equiv 1 \mod m$, entonces el polinomio evalúa a $n \mod m$. En otro caso, se considera que:

$$(1 + x + x^2 + \cdots + x^n)(x - 1) = x^{n+1} - 1$$

Si m es primo, entonces basta evaluar $(x^{n+1} - 1)(x - 1)^{-1}$ usando algoritmos estándar como exponenciación rápida. En el caso general, $(x-1)^{-1}$ no existe para todo x, por lo que se calcula $(x^{n+1} - 1) \mod m(x-1)$, y luego se divide el resultado por $(x - 1)$. Para justificar esto, se usa que si $a \cdot n \equiv t \mod n \cdot m$, entonces t es divisible por n, y además $a \equiv t/n \mod m$. Si definimos t como $(x^{n+1} - 1) \mod m(x-1)$, entonces $(1 + x + \cdots + x^n)(x - 1) \equiv t \mod m(x-1)$, y por el resultado anterior, t es divisible por $(x - 1)$, y $(1 + x + x^2 + \cdots + x^n) \equiv t/(x-1) \mod m$.

Problema 3

En este problema puede ser útil el siguiente resultado: Si p es primo, entonces existen a, b, tales que el orden de a en $\mathbb{Z}_p^*$ es $p - 1$, y el orden de b en $\mathbb{Z}_{p^2}^*$ es $p(p-1)$.

Parte 1 Demuestre que si $n = p_1 \cdots p_k$, con $\{p_i\}_i$ primos impares distintos, tales que $p_j - 1 | n - 1$ para todo j entre 1 y k, entonces n es un número de Carmichael.

Idea de solución Se considera a coprimo con n arbitrario, y se busca demostrar que $a^{n-1} \equiv 1 \mod n$. Para cada p_j, por el teorema de Fermat, se tiene que

$$a^{p_j-1} \equiv 1 \mod p_j$$

Luego, como $p_j - 1 | n - 1$, entonces también se cumple que

$$a^{n-1} \equiv 1 \mod p_j$$

y por lo tanto que cada p_j divide a $a^{n-1} - 1$. Como todos dividen a ese número, entonces $n | a^{n-1} - 1$, y por lo tanto $a^{n-1} \equiv 1 \mod n$.

Parte 2 Demuestre que si $n = p^k u$ es un número de Carmichael, donde p es primo, y u no es divisible por p, y además a es un elemento de orden $p - 1$ en $\mathbb{Z}_p$, entonces existe a_1 tal que $a_1 \equiv a \mod p$, y $a_1 \equiv 1 \mod u$. Concluya que $p - 1$ divide a $n - 1$.

Idea de solución La existencia de a_1 es directa del teorema chino del resto. Luego, por construcción a_1 es coprimo con p y con u, y por lo tanto también es coprimo con n. Por otra parte, como $a_1 \equiv a \mod p$, entonces a_1 tiene orden $p - 1$ en $\mathbb{Z}_p$, pero también, como n es un número de Carmichael, $a_1^{n-1} \equiv 1 \mod n$. De esta última equivalencia se concluye que $a_1^{n-1} \equiv 1 \mod p$, y por lo tanto que $p - 1 | n - 1$.

Parte 3 Demuestre que si n es un número de Carmichael, entonces para todo primo p, p^2 no divide a n.

Idea de solución Se puede usar la misma construcción del caso anterior, pero eligiendo a como un término de orden $p(p-1)$ en $\mathbb{Z}_{p^2}$. En ese caso se obtiene que $a_1^{n-1} \equiv 1 \mod p^2$, y que como a_1 tiene orden $p(p-1)$, entonces $p(p-1) | n - 1$, lo que es una contradicción, por que implica que $p | n - 1$, cuando se asumió que $p | n$.

Parte 4 Proponga una caracterización de los números de Carmichael, y demuestre que 1729 cumple las condiciones.

Idea de solución Juntando los resultados anteriores, se tiene que n es un número de Carmichael si y solo si $n = p_1 \cdots p_m$, donde cada p_j es un primo impar distinto, tal que $p_j - 1 | n - 1$. En el caso de 1729, se tiene que $1729 = 7 \cdot 13 \cdot 19$, y además que $6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96 = 1728$.