Pontificia Universidad Católica de Chile
Facultad de Ingenieria
Departamento de Ciencias de la Computación
IIC2283 - Diseño y Análisis de Algoritmos

Ayudantía 9

26 de octubre, 2018

Problema 1

En esta pregunta consideramos listas de números naturales mayores a cero, con al menos un elemento y sin repeticiones. Dadas dos listas L_1 y L_2, con n elementos, definimos $\texttt{EXP}(L_1, L_2)$ de la siguiente forma:

$$\prod_{i=1}^{n} L_1[i]^{L_2[i]}$$

Dadas dos listas L_1 y L_2 con n elementos y dos biyecciones $\pi_1, \pi_2 : \{1, ..., n\} \to \{1, ..., n\}$, definimos $\texttt{PERM-EXP}(L_1, \pi_1, L_2, \pi_2)$ como

$$\prod_{i=1}^{n} L_1[\pi_1(i)]^{L_2[\pi_2(i)]}$$

Construya un algoritmo codicioso que, dadas dos listas L_1 y L_2 con n elementos, retorne dos biyecciones $\pi_1, \pi_2 : \{1, ..., n\} \to \{1, ..., n\}$ que maximizan el valor de $\texttt{PERM-EXP}(L_1, \pi_1, L_2, \pi_2)$. Su algoritmo debe funcionar en tiempo polinomial, y además debe demostrar que funciona correctamente.

Solución:

Un posible algoritmo es:

function SORTING_PERM(L[1...n])
  $L_2 = [(L[i], i)$ `for i in 1...n`$]$
  L_2.sort()
  $\pi = \{i : L_2[i][2]$ `for i in 1...n`$\}$
  return π

function MAX_PERM(L_1, L_2)
  return (Sorting_Perm(L_1), Sorting_Perm(L_2))

La idea es que `Sorting_Perm` entrega una permutacion que *ordena la lista*, es decir, la lista L ordenada es igual a $[L[\pi(1)], L[\pi(2)], ..., L[\pi(n)]]$, donde π es la permutación retornada por `Sorting_Perm`. Esto funciona en tiempo polinomial: lo único que se hace es ordenar las listas y hacer un par de pasadas lineales.

Falta demostrar que las permutaciones retornadas son óptimas.

Sea π_1^g, π_2^g la solución entregada por `Max_Perm` para L_1, L_2 y sea π_1^*, π_2^* una solución óptima.

Notar que dado una permutacion π_3 cualquiera, tenemos que

$$\prod_{i=1}^{n} L_1[\pi_1(i)]^{L_2[\pi_2(i)]} = \prod_{i=1}^{n} L_1[\pi_1(\pi_3(i))]^{L_2[\pi_2(\pi_3(i))]} = \prod_{i=1}^{n} L_1[\pi_1 \circ \pi_3(i)]^{L_2[\pi_2 \circ \pi_3(i)]}$$

ya que π_3 simplemente cambia el orden de los factores, pero mantiene el resultado.

Sea π_3^* tal que $\pi_1^* \circ \pi_3^*$ ordena L_1, es decir, $\pi_1^* \circ \pi_3^* = \pi_1^g$.

Tenemos dos casos:

1. $\pi_2^* \circ \pi_3^* = \pi_2^g$

   En esto caso tenemos que

   $$\prod_{i=1}^{n} L_1[\pi_1^*(i)]^{L_2[\pi_2^*(i)]} = \prod_{i=1}^{n} L_1[\pi_1^* \circ \pi_3^*(i)]^{L_2[\pi_2^* \circ \pi_3^*(i)]} = \prod_{i=1}^{n} L_1[\pi_1^g(i)]^{L_2[\pi_2^g(i)]}$$

   Lo que indica que nuestra solución también es óptima.

2. $\pi_2^* \circ \pi_3^* \neq \pi_2^g$

   En este caso tenemos que $\pi_2^* \circ \pi_3^*$ no ordena la lista L_2 (si lo hiciera, sería igual a π_2^g).

   Sean i', j', donde $i' < j'$ tales que

   $$L_2[\pi_2^* \circ \pi_3^*(i')] > L_2[\pi_2^* \circ \pi_3^*(j')]$$

   Sabemos que tales i', j' existen puesto que $\pi_2^* \circ \pi_3^*$ no ordena la lista L_2.

   Sea $\pi_4(k) = \begin{cases} \pi_2^* \circ \pi_3^*(j') & k = i' \\ \pi_2^* \circ \pi_3^*(i') & k = j' \\ \pi_2^* \circ \pi_3^*(k') & e.o.c. \end{cases}$

   Tenemos que

   $$\begin{aligned}
   \texttt{Perm-Exp}(L_1, \pi_1^*, L_2, \pi_2^*) &= \prod_{i=1}^{n} L_1[\pi_1^*(i)]^{L_2[\pi_2^*(i)]} \\
   &= \prod_{i=1}^{n} L_1[\pi_1^* \circ \pi_3^*(i)]^{L_2[\pi_2^* \circ \pi_3^*(i)]} \\
   &= \prod_{i \neq i', j'} \left(L_1[\pi_1^* \circ \pi_3^*(i)]^{L_2[\pi_2^* \circ \pi_3^*(i)]} \right) \\
   &\quad \cdot L_1[\pi_1^* \circ \pi_3^*(i')]^{L_2[\pi_2^* \circ \pi_3^*(i')]} \cdot L_1[\pi_1^* \circ \pi_3^*(j')]^{L_2[\pi_2^* \circ \pi_3^*(j')]} \\
   &< \prod_{i \neq i', j'} \left(L_1[\pi_1^* \circ \pi_3^*(i)]^{L_2[\pi_2^* \circ \pi_3^*(i)]} \right) \\
   &\quad \cdot L_1[\pi_1^* \circ \pi_3^*(i')]^{L_2[\pi_2^* \circ \pi_3^*(j')]} \cdot L_1[\pi_1^* \circ \pi_3^*(j')]^{L_2[\pi_2^* \circ \pi_3^*(i')]} \quad (*) \\
   &= \prod_{i \neq i', j'} \left(L_1[\pi_1^* \circ \pi_3^*(i)]^{L_2[\pi_2^* \circ \pi_3^*(i)]} \right) \\
   &\quad \cdot L_1[\pi_1^* \circ \pi_3^*(i')]^{L_2[\pi_4(i')]} \cdot L_1[\pi_1^* \circ \pi_3^*(j')]^{L_2[\pi_4(j')]} \\
   &= \prod_{i=1}^{n} L_1[\pi_1^* \circ \pi_3^*(i)]^{L_2[\pi_4(i)]} \\
   &= \texttt{Perm_Exp}(L_1, \pi_1^* \circ \pi_3^*, L_2, \pi_4)
   \end{aligned}$$

   Esto es una contradicción pues habiamos supuesto que π_1^*, π_2^* eran soluciones óptimas. Por lo tanto, no puede darse el caso en que $\pi_2^* \circ \pi_3^* \neq \pi_2^g$.

   Notar que $(*)$ es verdadero pues dado $a < b$, $x < y$ se tiene que

   $$a^y \cdot b^x = a^x \cdot a^{y-x} \cdot b^x < a^x \cdot b^{y-x} \cdot b^x = a^x \cdot b^y$$

Así, en todos los casos se tiene que nuestra solución (π_1^g, π_2^g) también es óptima. ∎

Problema 2

Fije un número natural $n \geq 2$. La función ϕ de Euler es definida como $\phi(n) = |\mathbb{Z}_n^*|$.

Dado $a \in \mathbb{Z}_N^*$, el orden de a en $\mathbb{Z}_N^*$ se define como el menor número natural $k \geq 1$ tal que $a^k \equiv 1 \mod n$. Por ejemplo, el orden de 1 en $\mathbb{Z}_8^*$ es 1 puesto que $1^1 \equiv 1 \mod 8$, el orden de 3 en $\mathbb{Z}_8^*$ es 2 puesto que $3 \not\equiv 1 \mod 8$ y $3^2 \equiv 1 \mod 8$, y el orden de 3 en $\mathbb{Z}_{11}^*$ es 5.

Sea $a \in \mathbb{Z}_n^*$. Demuestre lo siguiente:

1. Existe un número $k \geq 1$ tal que $a^k \equiv 1 \mod n$, por lo que a tiene orden en $\mathbb{Z}_n^*$.

   Solución:

   De la identidad de Bezout es fácil demostrar que dado $MCD(a, n) = 1$, también se cumple que $MCD(a^h, n) = 1$.

   Sea $J = \{a^i \mod N \mid i \geq 1\}$. Por lo que acabamos de decir, tenemos que $J \subseteq \mathbb{Z}_N^*$, lo que implica que J es finito. Sea $k = |J|$.

   Consideremos los valores $a^1, a^2, ..., a^n$ donde $n > k$. Dado que $n > k$, pero $a^i \mod N \in J \; \forall i$, tenemos que existen i', j' con $i' < j'$ tales que

   $$\begin{aligned} a^{i'} &\equiv a^{j'} \mod N \\ a^{i'} &\equiv a^{i'+(j'-i')} \mod N \\ a^{i'} &\equiv a^{i'+k'} \mod N \\ 1 &\equiv a^{k'} \mod N \end{aligned}$$

2. Si k es el orden de a en $\mathbb{Z}_N^*$, entonces se tiene que k divide a $\phi(n)$.

   Solución:

   Sea $J = \{a^1 \mod N, a^2 \mod N, ..., a^k \mod N = 1\}$. Tenemos que $(J, \cdot)$ es un grupo, puesto que

   - $\cdot$ es asociativo
   - $1 = a^k \in J$
   - $a^x \cdot a^{k-x} \equiv 1 \mod N \implies$ todo elemento tiene inverso

   Además, $J \subseteq \mathbb{Z}_n^*$. Por lo tanto, J es un subgrupo de $\mathbb{Z}_N^*$. Por el teorema de Lagrange, esto implica que

   $$\begin{aligned} &|J| \mid |\mathbb{Z}_n^*| \\ \implies &k \mid \phi(N) \end{aligned}$$

3. $a^{\phi(n)} \equiv 1 \mod n$.

   Solución:

   Se tiene que

   $$\begin{aligned} a^{\phi(n)} &= a^{k_1 \cdot k} \\ &= (a^k)^{k_1} \\ &\equiv 1^{k_1} \mod N \\ &\equiv 1 \mod N \end{aligned}$$

4. El teorema de Fermat.

   Solución:

   Basta tomar la proposición anterior y el hecho que dado un primo p, $\phi(p) = p - 1$.

Problema 3

Definición: Un número a es *raíz primitiva módulo* n si y solo si el menor valor de h tal que

$$a^h \equiv 1 \mod n$$

es $h = \phi(n)$.

Definición: Un grupo S se dice *cíclico* si existe $a \in S$ tal que $S = \{a^k \mid k \in \mathbb{N}\}$. En ese caso se dice que a es un *generador* de S.

Sea $n \in \mathbb{Z}$ tal que existe por lo menos una raíz primitiva módulo n. Demuestre lo siguiente:

1. $\mathbb{Z}_n^*$ es isomorfo a $\mathbb{Z}_{\phi(n)}$

   Solución:

   Sea a una raiz primitiva módulo n. Dados $i, j < \phi(n)$, se cumple que $a^i \not\equiv a^j \mod n$ (si fueran equivalentes, a no sería una raíz primitiva).

   Sea $J = \{a^i \mod n \mid i \in \{0, ..., \phi(n)-1\}\}$. Tenemos que $J \subseteq \mathbb{Z}_n^*$. Además, $|J| = \phi(n) = |\mathbb{Z}_n^*|$. Por lo tanto, $J = \mathbb{Z}_n^*$.

   Tenemos que $\mathbb{Z}_\phi(n) = \{0, 1, 2, ..., \phi(n) - 1\}$.

   Se define $f : \mathbb{Z}_\phi(n) \to \mathbb{Z}_n^*$ como $f(i) = a^i \mod N$.

   La función f cumple que

   - f tiene inverso: $f^{-1}(b) = j$, donde $j = \min_i\{i \mid a^i \equiv b \mod N\}$.
   - f conserva la estructura: $f(i + j) = a^{i+j} \mod n = a^i \cdot a^j \mod n = f(i) \cdot f(j) \mod n$.

   Por lo tanto, f es un isomorfismo entre $\mathbb{Z}_{\phi(n)}$ y $\mathbb{Z}_n^*$.

2. $(\mathbb{Z}_m, +)$ es un grupo cíclico

   Solución:

   Tomemos $g = 1$. Para todo $b \in \mathbb{Z}_m$, se cumple que $b = g^b$ (en notación aditiva: $g^b = g + ... + g$ (b veces), es decir, corresponde a aplicar b veces la operación del grupo sobre g).

   Por lo tanto, g es un generador de $\mathbb{Z}_m$, lo que implica que $\mathbb{Z}_m$ es cíclico.

3. a es generador de $\mathbb{Z}_m$ si y solo si $MCD(a, m) = 1$

   Solución:

$$\begin{aligned}
MCD(a,m) = 1 &\implies \exists d: \ a \cdot d \equiv 1 \mod m && \text{(notacion multiplicativa)} \\
&\implies a + a + ... + a \equiv 1 \mod m \\
&\implies a^d \equiv 1 \mod m && \text{(notacion aditiva)} \\
&\implies \forall b \in \mathbb{Z}_m, b \equiv 1^b \equiv (a^d)^b \equiv a^{db} \mod m \\
&\implies a \text{ es generador de } \mathbb{Z}_m
\end{aligned}$$

$$\begin{aligned}
a \text{ es generador de } \mathbb{Z}_m &\implies 1 \equiv a^d \mod m && \text{(notacion aditiva)} \\
&\implies 1 \equiv a + a + ... + a \mod m \\
&\implies 1 \equiv a \cdot d \mod m && \text{(notacion multiplicativa)} \\
&\implies a \text{ tiene inverso modulo } m \\
&\implies MCD(a, m) = 1
\end{aligned}$$

4. Z_n^* tiene $\phi(\phi(n))$ raíces primitivas.

   Solución:

   Directo de 1 y 3. Por la parte 3, $\mathbb{Z}_{\phi(n)}$ tiene $\phi(\phi(n))$ generadores. Por la parte 1, como $\mathbb{Z}_{\phi(n)}$ y $\mathbb{Z}_n^*$ son isomorfos, entonces $\mathbb{Z}_n^*$ tambien tiene $\phi(\phi(n))$ generadores, y cada generador en $\mathbb{Z}_n^*$ es también una raíz primitiva. Esto último es fácil de demostrar por contradicción: si un elemento no es raíz primitiva, entonces no puede ser generador.

Problema 4

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

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

   Solución:

   $$\begin{aligned} ab = ba &\iff b^{-1}ab = a \\ &\iff a^{-1}b^{-1}ab = 1 \\ &\iff [a, b] = 1 \end{aligned}$$

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

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

   Solución:

   Tenemos que

   $$\begin{aligned} g_i g_j = g_j g_i &\iff g_j = g_i^{-1} g_j g_i \\ &\iff g_j g_i^{-1} = g_i^{-1} g_j \qquad (1) \\ &\iff g_i^{-1} = g_j^{-1} g_i^{-1} g_j \\ &\iff g_i^{-1} g_j^{-1} = g_j^{-1} g_i^{-1} \quad (2) \end{aligned}$$

   Es decir, si dos generadores conmutan, entonces sus inversos conmutan y cada uno conmuta con el inverso del otro. Por lo tanto, si todos los generadores en S conmutan, entonces todos los elementos del grupo generado por S también conmutan.

   Con esto, el algoritmo es simplemente chequear si todos los pares en S conmutan. Esto toma tiempo cuadrático.

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

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

   Además, para cada elemento $g \in G$, se define el centralizador de g como

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

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

   Solución:

   p.d. $Z(G)$ es subgrupo de G

   - $Z(G) \subseteq G$

- neutro: $1 \in Z(G)$
- cerrado: Si $a, b \in Z(G)$ entonces $abt = atb = tab \; \forall t \implies ab \in Z(G)$
- inverso: $a \in Z(G) \implies at = ta \implies t = a^{-1}ta \implies ta^{-1} = a^{-1}t \implies a^{-1} \in Z(G)$ ■

p.d. $C(g)$ es subgrupo de G

- $C(g) \subseteq G$
- neutro: $1 \in C(g)$
- cerrado: Si $a, b \in C(g)$ entonces $abg = agb = gab \implies ab \in Z(G)$
- inverso: $a \in C(g) \implies ag = ga \implies g = a^{-1}ga \implies ga^{-1} = a^{-1}g \implies a^{-1} \in C(g)$ ■

4. Dado un grupo $G = \langle g_1, ..., g_n \rangle$ (generado por $S = (g_1, ..., g_n)$), definimos un subproducto aleatorio como

$$r = g_1^{\epsilon_1} \cdot ... \cdot g_n^{\epsilon_n} \in G$$

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

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

$$Pr[r \notin H] \geq \frac{1}{2}$$

Solución:

H no contiene todos los generadores g_i, pues si lo hiciera entonces no sería un subgrupo propio.

Sea $l = \min_i \{i \mid g_i \notin H\}$. Tenemos que $r = g_1^{\epsilon_1} \cdot ... \cdot g_n^{\epsilon_n} \in G = ug_l^{e_l}v$, donde $u \in H$ por definición de l.

Para calcular la probabilidad pedida condicionamos sobre el evento $v \in H$:

$$\begin{aligned} Pr[r \notin H] &= Pr[r \notin H \mid v \in H] \cdot Pr[v \in H] + Pr[r \notin H | v \notin H] \cdot Pr[v \notin H] \\ &= \frac{1}{2} Pr[v \in H] + Pr[r \notin H | v \notin H] \cdot Pr[v \notin H] \\ &\geq \frac{1}{2} Pr[v \in H] + \frac{1}{2} Pr[v \notin H] \\ &= \frac{1}{2} \end{aligned}$$

Donde el penúltimo paso es válido pues $Pr[r \notin H | v \notin H] \geq Pr[e_l = 0] = \frac{1}{2}$.

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

El algoritmo es simplemente generar dos r, r' subproductos aleatorios independientes y verificar si $[r, r'] = 1$. Esto toma tiempo $O(n)$.

Cuando G es conmutativo, la probabilidad de error es 0.

Cuando G no es conmutativo, tenemos que

$$\begin{aligned} Pr\left[[r, r'] \neq 1\right] &= Pr[r' \notin C(r)] \\ &= Pr[r' \notin C(r) \mid r \in Z(G)] \cdot Pr[r \in Z(G)] + Pr[r' \notin C(r) \mid r \notin Z(G)] \cdot Pr[r \notin Z(G)] \end{aligned}$$

Pero $Pr[r' \notin C(r) \mid r \in Z(G)] = 0$ pues si $r \in Z(G)$, entonces $C(r) = G$. Además, $Pr[r' \notin C(r) \mid r \notin Z(G)] \geq \frac{1}{2}$ y $Pr[r \notin Z(G)] \geq \frac{1}{2}$ por lo demostrado en la parte 3 y el teorema de Lagrange.

$$
\begin{aligned}
\therefore Pr\left[[r, r'] \neq 1\right] &= Pr[r' \notin C(r) \mid r \in Z(G)] \cdot Pr[r \in Z(G)] + Pr[r' \notin C(r) \mid r \notin Z(G)] \cdot Pr[r \notin Z(G)] \\
&= Pr[r' \notin C(r) \mid r \notin Z(G)] \cdot Pr[r \notin Z(G)] \\
&\geq \frac{1}{2} \cdot \frac{1}{2} \\
&= \frac{1}{4}
\end{aligned}
$$

Esto implica que $Pr[error] = Pr[[r, r'] = 1] \leq \frac{3}{4}$.