Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Ayudantía Repaso Examen

6 de julio de 2024

Martín Atria, Caetano Borges, José Caraball

---

1 Cardinalidad

Determine si el subconjunto de los números reales que tienen un número infinito de 1s en su representación decimal es numerable o no. Demuestre su respuesta.

Solución

Llamemos C al conjunto en cuestión. Sea $C' \subseteq C$, tal que todo elemento $x \in C'$ cumple que $0 < c < 1$. Demostraremos que C' no es numerable, lo que implica que C no es numerable. Lo haremos por diagonalización.

Por contradicción, supongamos que C' es numerable. Esto implica que todos sus elementos $x \in C'$ se pueden listar en una secuencia $S = x_1, x_2, x_3, \ldots$. Expandiendo esta representación:

x_i	Representación decimal
x_1	$x_{11}x_{12}x_{13}\ldots$
x_1	$x_{21}x_{22}x_{23}\ldots$
x_3	$x_{31}x_{32}x_{33}\ldots$
$\vdots$	$\vdots$

Consideremos un elemento x_j definido inductivamente de la siguiente manera

- Base: los primeros $n-1$ dígitos de x_j son iguales a los de x_1, donde n es la posición del primer dígito 1 en x_1. Como $x_1 \in C'$, tiene infinitos 1s, por lo que existe un 1 que es el primero, y cuya posición es un número finito. Esta posición es n_1. En este punto, diremos que el n-ésimo dígito de x_j es 2, y que el (n_1+1)-ésimo es 1, es decir, justo antes de agregar el primer 1 de x_1, le agregamos un 2. Con ello, x_j ya es necesariamente distinto a x_1, ya que si x_1 tenía k dígitos 2 justo antes de su primer 1, entonces x_j tiene $k+1$ dígitos 2 ahí, por lo que son distintos.

- Inductivamente, dado que a x_j ya le hemos agregado los dígitos correspondientes a x_i (por eso el caso base de $i = 1$), tomaremos todos los dígitos después del $(n_{i-1} + 1)$-ésimo hasta el primer dígito 1 de x_i que aparezca en este tramo, le agregaremos el 2 justo antes del 1 al igual que en la base, y los agregamos a x_j en la posición n_i. Con esto, como x_i tenía k dígitos 2 justo antes de la posición n_i, y x_j tiene $k + 1$ dígitos 2 justo antes de su i-ésimo 1, tenemos que $x_j \neq x_i$.

Como entre cada n_i para cada x_i hay un número finito de dígitos, x_j efectivamente es un número que tiene infinitos dígitos 1 en su representación decimal y es tal que $0 < x_j < 1$, por lo que $x_j \in C'$. Sin embargo, $x_j \neq x_i$ para todo i, por lo que x_j no está en la secuencia anterior. Esto es una contradicción, ya que habíamos supuesto que todos los elementos estaban en la secuencia. Luego, concluímos que C' no es numerable. Como $C' \subseteq C$, esto implica que C no es numerable. □

2 Algoritmos

1. Demuestre que $n! \in \mathcal{O}(n^n)$ pero que $n^n \notin \mathcal{O}(n!)$

Solución
Recordemos que $f \in \mathcal{O}(g) \Leftrightarrow (\exists c \in \mathbb{R}^+)(\exists n_0 \in \mathbb{N})(\forall n \geq n_0)(f(n) \leq c \cdot g(n))$.
a) $n! \in \mathcal{O}(n^n)$: con $c = 1$, se tiene que $\forall n$:

$$\begin{aligned} n! = \quad & n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 \\ \leq \quad & n \cdot n \cdot n \cdots n \cdot n \cdot n = n^n \end{aligned}$$

b) $n^n \notin \mathcal{O}(n!)$: Debemos demostrar la negación de la definición de $\mathcal{O}$. Recordemos de lógica de predicados que

$$\neg\exists x\varphi(x) \equiv \forall x\neg\varphi(x)$$
$$\neg\forall x\varphi(x) \equiv \exists x\neg\varphi(x)$$

Se tiene que:

$$\begin{aligned} n^n \notin \mathcal{O}(n!) &\Leftrightarrow \neg(\exists c \in \mathbb{R}^+)(\exists n_0 \in \mathbb{N})(\forall n \geq n_0)(f(n) \leq c \cdot g(n)) \\ &\equiv (\forall c \in \mathbb{R}^+)\neg(\exists n_0 \in \mathbb{N})(\forall n \geq n_0)(f(n) \leq c \cdot g(n)) \\ &\equiv (\forall c \in \mathbb{R}^+)(\forall n_0 \in \mathbb{N})\neg(\forall n \geq n_0)(f(n) \leq c \cdot g(n)) \\ &\equiv (\forall c \in \mathbb{R}^+)(\forall n_0 \in \mathbb{N})(\exists n \geq n_0)\neg(f(n) \leq c \cdot g(n)) \\ &\equiv (\forall c \in \mathbb{R}^+)(\forall n_0 \in \mathbb{N})(\exists n \geq n_0)(f(n) > c \cdot g(n)) \end{aligned}$$

Demostraremos que para un $c \in \mathbb{R}^+$ arbitrario, existe un punto desde el que n^n siempre es mayor a $cn!$. Consideremos un c cualquiera. Por inducción:

BI: Sea $n = c!$. Debemos demostrar que $(c!)^{c!} > c(c!)!$. Se tiene que

$$\begin{aligned}(c!)^{c!} = \quad & c! \cdot c! \cdot c! \cdots c! \cdot c! \\ > \quad & c! \cdot (c!-1) \cdot (c!-2) \cdots 2 \cdot 1 \cdot c = c(c!)!\end{aligned}$$

con lo que la propiedad se cumple.
HI: Supondremos que la propiedad se cumple para n, es decir, que $n^n > cn!$.
TI: Demostraremos que la propiedad se cumple para $n+1$, es decir, que $(n+1)^{n+1} > c(n+1)!$. Por HI se tiene que

$$\begin{aligned} n^n &> cn! && / \cdot (n+1) \\ (n+1)n^n &> c(n+1)n! = c(n+1)! \end{aligned}$$

Como $(n+1)^{n+1} = (n+1)(n+1)^n > (n+1)n^n$, por transitividad concluímos que

$$(n+1)^{n+1} > c(n+1)!$$

que es lo que queríamos demostrar.
Con ello, demostramos por inducción que para cualquier c, existe un punto (un n) desde el cual n^n siempre es mayor que $cn!$, correctamente satisfaciendo que

$$(\forall n_0 \in \mathbb{N})(\exists n \geq n_0)(n^n > cn!)$$

□

2. Analice las complejidades de tiempo en el peor y mejor caso para el siguiente algoritmo:

Algorithm 1 Insertion Sort

```
for i = 1 to n do
    for j = i to 1 do
        if L[j] < L[j − 1] then
            L[j − 1], L[j] ← L[j], L[j − 1]
        else
            break
        end if
    end for
end for
    return L
```

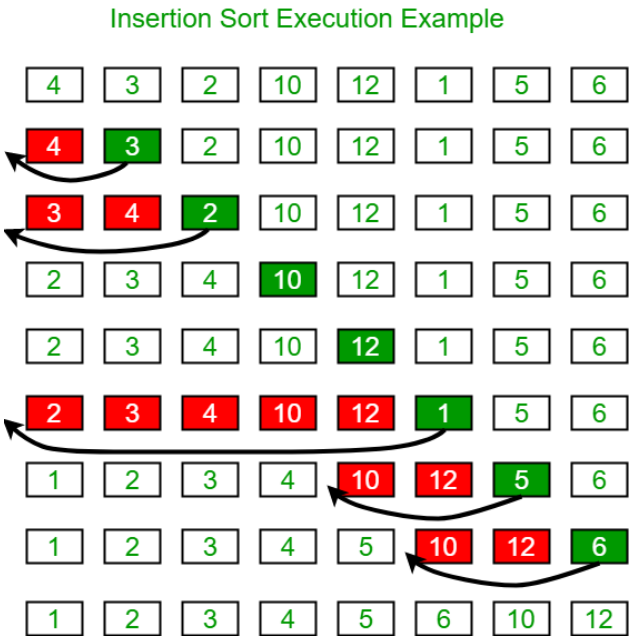

Figure 1: Fuente: https://media.geeksforgeeks.org/wp-content/uploads/insertionsort.png

Solución
Vale la pena simular una ejecución del algoritmo para ganar intuición (Ver Figura 1).

De la simulación podemos notar que lo que hace el algoritmo es recorrer la lista una vez y cada elemento lo mueve hacia atrás hasta la posición donde debería quedar.

Notamos que este proceso de 'mover el elemento hasta su posición correcta' se lleva a cabo con el *for* de la línea 2. Es claro que el mejor caso es que en este for no se mueva el elemento y se pase al break de la línea 6 inmediatamente. Esto ocurre justamente cuando nos encontramos con un elemento que ya está en su posición correcta. Luego, el mejor caso es cuando la lista L venía ordenada, ya que en este caso recorremos los elementos de L una vez con el for de la línea 1, pero nunca hacemos nada en el for de la línea 2. Este caso toma tiempo $\Omega(n)$, ya que sólo recorre la lista una vez, sin hacer nada cada vez que se mira cada elemento.

Por otro lado, es claro que el peor caso que se presenta al mirar un elemento de L se tiene cuando en el for de la línea 2, en vez de pasar al break de la línea 6 inmediatamente, se debe mover el elemento hasta el principio de la lista (es decir, el elemento se hacen la mayor cantidad posible de iteraciones sobre el for de la línea 2). Luego, el peor caso es cuando la lista viene ordenada al revés (de mayor a menor), ya que en este caso cada vez que miramos un elemento lo tenemos que llevar hasta el principio. En este caso el algoritmo toma $1 + 2 + 3 + \ldots + n \in O\left(n^2\right)$ pasos.

3 Grafos

1. Demuestre que al menos uno de G y $\bar{G}$ es conexo.

Solución
Si G es conexo, entonces no hay nada más que probar. Supongamos que G no es conexo. Esto implica que podemos dividir a G en k componentes conexas distintas $V_1, \ldots, V_k$. Como V_1 es una componente conexa distinta a V_2, no existe ninguna arista que una a un nodo de V_1 con uno de V_2. Luego, en $\bar{G}$ todo $v \in V_1$ tendrá aristas a todo $v \in V_2$, por lo que las componentes pasan a estar conectadas. Esto se cumple para todo k, con lo que concluímos que $\bar{G}$ es conexo.

2. Sea $G = (V, E)$ un grafo tal que para toda terna $a, b, c \in V$ se tiene que

$$\delta(a) + \delta(b) + \delta(c) \geq |V| - 2$$

Demuestre que G tiene a lo más 2 componentes conexas.

Solución
Si G es conexo, no hay nada que probar. Supongamos que existen dos vértices $x, y \in V$ sin un camino que los conecte. Claramente x e y no pueden ser adyacentes. Además, si $N(x) \cap N(y) \neq \varnothing$, entonces existe un vértice z adyacente a x e y, lo que implicaría que existe un camino entre los dos. Entonces sabemos que $N(x) \cap N(y) = \varnothing$.
Ahora, para todo otro vértice $z \in V$, o z es adyacente a x, adyacente a y, o adyacente a ninguno. Supongamos que z no es adyacente a x o y. Sabemos por enunciado que $\delta(x)+\delta(y)+\delta(z) \geq n-2$. Como x, y, z no son adyacentes entre sí, $N(x) \cup N(y) \cup N(z) \subseteq V \backslash \{x, y, z\}$. Por el principio del palomar, tiene que haber al menos un vértice que pertenece a al menos dos de las vecindades. Como sabemos que $N(x)$ y $N(y)$ son disjuntos, esto implica que z comparte un vecino con al menos uno de x e y. Entonces, todos los vértices de G pertenecen a una componente conexa de x o y.

4 Teoría de Números

1. Suponga que $a, b, m \in \mathbb{Z}$ con $m > 0$ son tales que $\gcd(a, m) = \gcd(b, m) = 1$. Sean $x, y \in \mathbb{Z}$ tal que $a^x \equiv b^x \pmod{m}$ y $a^y \equiv b^y \pmod{m}$. Si $d = \gcd(x, y)$ demuestre que

$$a^d \equiv b^d \pmod{m}$$

Solución
El enunciado nos da mucha información. Una buena estrategia puede ser listar las implicancias de esta información:

- $\gcd(a, m) = \gcd(b, m) = 1 \longrightarrow a$ y b tienen inverso mod m.
- $d = \gcd(x, y) \longrightarrow$ Identidad de Bézout: $\exists s, t \in \mathbb{Z} : sx + ty = d$.

Como a y b tienen inverso mod m, incluso si s es negativo se tiene que $(a^x)^s$ y $(b^x)^s$ existen en $\mathbb{Z}_m$. Lo mismo para y y t. Luego, podemos escribir

$$\begin{aligned}(a^x)^s &\equiv (b^x)^s \pmod m\\ (a^y)^t &\equiv (b^y)^t \pmod m\end{aligned}$$

Y luego, por propiedad de congruencias mod m, podemos multiplicar las congruencias y obtenemos que

$$\begin{aligned}a^{sx} \cdot a^{ty} &\equiv b^{sx} \cdot b^{ty} \pmod m\\ a^{sx+ty} &\equiv b^{sx+ty} \pmod m\\ a^d &\equiv b^d \pmod m\end{aligned}$$

□

2. Sean p, q dos números primos distintos. Demuestre que, si

$$\begin{aligned}a^q &\equiv a \pmod p\\ a^p &\equiv a \pmod q\end{aligned}$$

entonces $a^{pq} \equiv a \pmod{pq}$.

Solución

Por el Pequeño Teorema de Fermat se tiene que para todo a

$$\begin{aligned}a^p &\equiv a \pmod p\\ a^q &\equiv a \pmod q\end{aligned}$$

Si combinamos esto con la información del enunciado obtenemos que

$$\begin{aligned}(a^q)^p &\equiv a^q \pmod p\\ &\equiv a \pmod p\end{aligned}$$

y por otra parte,

$$\begin{aligned}(a^p)^q &\equiv a^p \pmod q\\ &\equiv a \pmod q\end{aligned}$$

Esto implica la existencia de $x, y \in \mathbb{Z}$ tal que

$$\begin{aligned}a^{pq} - a &= xp\\ a^{pq} - a &= yq\end{aligned}$$

Con lo que $xp = yq$. Como p y q son primos, necesariamente $y \mid p$, por lo que, con $k = \frac{y}{p}$ se tiene que

$$x = kq$$

Lo que finalmente implica que

$$\begin{aligned} & a^{pq} - a = kqp \\ \iff \quad & a^{pq} \equiv a \pmod{pq} \end{aligned}$$

□