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

Examen

02 de Julio de 2025

Duración: 3:50 hrs.

Pregunta 1

Demuestre que si n es un entero positivo, entonces

$$(x_1 + x_2 + \ldots + x_m)^n = \sum_{n_1+n_2+\ldots+n_m=n} \frac{n!}{n_1!n_2!\cdots n_m!} \cdot x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m}.$$

Solución

- Al expandir sucesivamente el producto de n factores de la forma $(x_1+x_2+\ldots+x_m)\cdot(x_1+x_2+\ldots+x_m)^{n-1}$, obtenemos monomios repetidos de la forma $x_1^{n_1}x_2^{n_2}\cdots x_m^{n_m}$, para $n_1+n_2+\ldots+n_m = n$.
- El número de formas en que se puede producir tal monomio es las maneras de elegir el término x_1 en n_1 de estos n factores, x_2 en n_2 de los restantes factores, y así sucesivamente. Esto puede lograrse de la siguiente cantidad de formas:

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-n_2-\cdots-n_{m-1}}{n_m}.$$

- Al resolver este producto obtenemos que el resultado es precisamente

$$\frac{n!}{n_1!n_2!\cdots n_m!}.$$

Pauta (6 ptos)

- 2.0 puntos por expandir la multiplicación e indentificar que hay términos que se repiten.
- 2.0 puntos por contar la repetición de términos.
- 2.0 puntos por concluir el resultado.

Pregunta 2

Sea R un predicado de aridad $n+1$ en Lógica de Predicados, utilizaremos el vocabulario μ definido como $\{R, =\}$. Dada un interpretación $\mathcal{I}$, $R^{\mathcal{I}}$ es la interpretación de R bajo $\mathcal{I}$.

1. Decimos que una relación $(n+1)$-aria R sobre A codifica una función n-aria si, para todo $(a_1, ..., a_n) \in A^n$, existe un único $c \in A$ tal que $(a_1, ..., a_n, c) \in R$. Escriba (utilizando sólo cuantificadores $\forall$ y $\exists$) una fórmula φ tal que para toda interpretación $\mathcal{I}$ sobre μ se cumple lo siguiente:

$$\mathcal{I} \models \varphi \quad \Longleftrightarrow \quad R^{\mathcal{I}} \text{ codifica una función } n\text{-aria.}$$

2. Sea $n = 2$. Considere toda $\mathcal{I}$ sobre μ en la que $R^{\mathcal{I}}$ codifica una función binaria (2-aria), denotada por $f_{\mathcal{I}} : A \times A \to A$. Recuerde que una función binaria f sobre A es *asociativa*, si para todo $a, b, c \in A$ se cumple que $f(f(a, b), c) = f(a, f(b, c))$. Construya una fórmula ψ tal que:

$$\mathcal{I} \models \psi \quad \Longleftrightarrow \quad f_{\mathcal{I}} \text{ es asociativa.}$$

Solución

1. La fórmula es

$$\forall x_1 \forall x_2 ... \forall x_n \big(\exists y R(x_1, x_2, ..., x_n, y) \;\wedge\; \neg\exists y \exists z (R(x_1, x_2, ..., x_n, y) \wedge R(x_1, x_2, ..., x_n, z) \wedge \neg(y = z))\big).$$

2. La fórmula es

$$\forall x \forall y \forall z \forall u \forall v \forall w \,\big(R(x, y, u) \wedge R(u, z, v) \wedge R(y, z, w) \;\to\; R(x, w, v)\big).$$

Pauta (6 ptos)

- 3.0 puntos por la primera fórmula.
- 3.0 puntos por la segunda fórmula.

Pregunta 3

Sea $G = (V, E)$ un grafo (no dirigido, sin loops, ni aristas múltiples) con $n \geq 3$ vértices. Denotamos por $\delta(G)$ el mínimo grado de un vértice en G. Demuestre que si $\delta(G) \geq 2$, entonces G contiene al menos un ciclo.

Solución

- Considere el camino $(v_1, \ldots, v_{k-1}, v_k)$ más largo en G (si el grafo no es conexo, tome como G alguna componente). Dado que este es el camino más largo en G, entonces todos los vecinos de v_k deben ya estar en el camino.

- Dado que v_k tiene al menos dos vecinos, entonces al menos uno de esos vecinos, digamos v_i, debe estar ya en el camino y ser diferente a v_{k-1}. Concluimos que $(v_i, v_{i+1}, \ldots, v_k, v_i)$ es un ciclo en G.

Pauta (6 ptos)

- 3.0 puntos por tomar un camino que cumple alguna propiedad especial (que sea el más largo, pase por n nodos, usa $n-1$ aristas, etc.).

- 3.0 puntos por concluir bien que el camino es o contiene un ciclo.

Pregunta 4

En esta pregunta ocupamos $\text{mcd}(a, b)$ para denotar el máximo común divisor entre $a, b > 0$.

1. Demuestre que si $a > b$, entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$, donde $r = a \bmod b$.
2. Usando 1., demuestre que existen enteros s, t tal que $\text{mcd}(a, b) = sa + tb$.
3. Demuestre que si $sa + tb = \text{mcd}(a, b) = 1$, entonces $sa \equiv_b 1$ (s es inverso de a en módulo b).
4. Demuestre que si $\text{mcd}(a, b) = 1$, entonces la ecuación $ax \equiv_b c$ tiene solución x.

Solución

1. Dado que existe k tal que $a = kb + a \bmod b$. Si c divide a b y r, entonces también divide a a. Y como $a - kb = a \bmod b$, si c divide a a y b, también divide a r (y a b).
2. Algoritmo de Euclides genera una secuencia de restos $r_0 = a$, $r_1 = b$, $r_2 = a \bmod b$, ..., $r_j = r_{j-2} \bmod r_{j-1}$. Notamos que el último resto no nulo es $\text{mcd}(a, b)$ y que existe k_j tal que (i) $r_{j-2} = k_j \cdot r_{j-1} + r_j$. Suponemos que $r_i = \text{mcd}(a, b)$, por inducción encontraremos s_i y t_i tal que $r_i = s_i \cdot a + t_i \cdot b$.

   CB: $r_0 = 1 \cdot a + 0 \cdot b$ y $r_1 = 0 \cdot a + 1 \cdot b$.

   HI: Asumimos que existen enteros $s_{i-2}, t_{i-2}, s_{i-1}, t_{i-1}$ tal que $r_{i-2} = s_{i-2} \cdot a + t_{i-2} \cdot b$ y $r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$.

   TI: De (i) sabemos que $r_i = r_{i-2} - k_i \cdot r_{i-1}$, entonces:

$$\begin{aligned}
r_i &= (s_{i-2} \cdot a + t_{i-2} \cdot b) - k_i \cdot (s_{i-1} \cdot a + t_{i-1} \cdot b) \\
r_i &= (s_{i-2} - k_i \cdot s_{i-1}) \cdot a + (t_{i-2} - k_i \cdot t_{i-1}) \cdot b \\
s_i &= s_{i-2} - k_i \cdot s_{i-1} \\
t_i &= t_{i-2} - k_i \cdot t_{i-1}
\end{aligned}$$

3. Dado que $sa + tb = 1$, tenemos que $sa - 1 = -tb$. Por lo tanto, $sa - 1$ es divisible por b.

   Alternativa: Dado que $sa + tb = 1$, tenemos que $sa \bmod b = 1 \bmod b$. Por lo tanto, $sa \equiv_b 1$.
4. Dado que $\text{mcd}(a, b) = 1$, existe s tal que $sa \equiv_b 1$. Multiplique la ecuación por s en ambos lados obteniendo $sax \equiv_b sc$. Concluímos que $x = sc$ es una solución.

Pauta (6 ptos)

- 1.5 puntos por el ítem 1.
- 1.5 puntos por el ítem 2.
- 1.5 puntos por el ítem 3.
- 1.5 puntos por el ítem 4.