PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN
IIC1253 - MATEMÁTICAS DISCRETAS

Pauta Examen

13 de diciembre de 2025

Duración: 3 hrs.

Pregunta 1

Construya una fórmula proposicional en CNF equivalente a la fórmula $(x \wedge \neg y) \vee (y \wedge \neg z) \vee (z \wedge \neg x)$.

Solución:

Alternativa 1:

Construimos la tabla de verdad para la formula $\varphi = (x \wedge \neg y) \vee (y \wedge \neg z) \vee (z \wedge \neg x)$:

x	y	z	φ
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Luego la tabla de verdad de $\neg\varphi$ es:

x	y	z	$\neg\varphi$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Alternativa 1.1:

Podemos aplicar el método visto en clases para obtener una DNF a partir de la tabla de verdad de $\neg\varphi$. De esta forma obtenemos la DNF:

$$(\neg x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z)$$

Luego para φ, aplicando la ley de De Morgan, obtenemos la siguiente CNF equivalente:

$$\neg\big((\neg x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z)\big) = (x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z)$$

Alternativa 1.2:

Otra alternativa es notar, mirando la tabla de verdad de φ, que la fórmula toma valor 1 si y sólo si entre x, y, z por lo menos una variable toma valor 1 y por lo menos una toma valor 0. Es decir, la fórmula es equivalente a la siguiente CNF:

$$(x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z).$$

Alternativa 2:

Se puede encontrar una CNF aplicando la regla de distributividad:

$$\begin{aligned}(x \wedge \neg y) \vee (y \wedge \neg z) \vee (z \wedge \neg x) =& (x \vee y \vee z) \wedge (x \vee y \vee \neg x) \wedge (x \vee \neg z \vee z) \wedge (x \vee \neg z \vee \neg x) \\ & \wedge (\neg y \vee y \vee z) \wedge (\neg y \vee y \vee \neg x) \wedge (\neg y \vee \neg z \vee z) \wedge (\neg y \vee \neg z \vee \neg x)\end{aligned}$$

Distribución de puntajes:
6.0 pts por entregar una CNF equivalente correcta y explicar el desarrollo. Descuentos a criterio del corrector.

Pregunta 2

Demuestre por inducción que $2^n \geq (1{,}7)^n + n$ para todo número natural $n \geq 3$.

Solución

Mostramos primero el caso base. Para $n = 3$, tenemos

$$1{,}7^3 + 3 = 4{,}913 + 3 < 8 = 2^3$$

Ahora mostramos el paso inductivo. Nuestra hipótesis inductiva es que $2^n \geq (1,7)^n + n$ para $n \geq 3$. Mostremos la propiedad para $n + 1$. Efectivamente,

$$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot ((1{,}7)^n + n) = 2 \cdot 1{,}7^n + 2n$$

Notar que $2 \cdot 1{,}7^n \geq 1{,}7 \cdot 1{,}7^n = 1{,}7^{n+1}$ (ya que $2 \geq 1,7$) y $2n \geq n + 1$ ya que $n \geq 3$. Concluimos que $2^{n+1} \geq 1{,}7^{n+1} + (n + 1)$.

Distribución de puntajes:
1.0 pts por caso base, 1.0 pts por plantear correctamente la hipótesis inductiva, 4.0 pts por demostrar correctamente el paso inductivo (o tesis inductiva). Descuentos a criterio del corrector.

Pregunta 3

Sea $f\colon A \to A$ un función de A en A. Definimos $PF(f) = \{a \in A \mid f(a) = a\}$.

(a) Demuestre que $PF(f) \subseteq PF(f \circ f)$ para todo conjunto A y función $f\colon A \to A$.

(b) De un ejemplo de un conjunto A y una función $f\colon A \to A$ tal que $PF(f \circ f) \not\subseteq PF(f)$.

Solución

(a) Sea $a \in PF(f)$. Entonces, $f(a) = a$. De eso sale que $f \circ f(a) = f(f(a)) = f(a) = a$. Por lo tanto $a \in PF(f \circ f)$.

(b) Sea $A = \{1, 2\}$ y $f\colon A \to A$ tal que $f(1) = 2, f(2) = 1$. Por definición, $PF(f) = \varnothing$. Por el otro lado, $f \circ f(1) = f(f(1)) = f(2) = 1$, así que $1 \in PF(f \circ f)$. Obtenemos que en ese caso $PF(f \circ f) \not\subseteq PF(f)$.

Distribución de puntajes:
3.0 pts parte (a) y 3.0 pts parte (b). Descuentos a criterio del corrector.

Pregunta 4

En esta pregunta trabajaremos con secuencias infinitas de 0's y 1's, es decir, secuencias $(a_n)_{n\geq 0}$ tal que $a_n \in \{0, 1\}$, para todo $n \geq 0$. Denotamos por $\mathcal{S}$ al conjunto de todas las secuencias infinitas de 0's y 1's. Decimos que una secuencia $(a_n)_{n\geq 0} \in \mathcal{S}$ es *especial* si no tiene tres 0's consecutivos ni tres 1's consecutivos, vale decir, no existe $k \geq 0$ tal que $a_k = a_{k+1} = a_{k+2} = 0$ y no existe $\ell \geq 0$ tal que $a_\ell = a_{\ell+1} = a_{\ell+2} = 1$. Denotamos por $\mathcal{E}$ al conjunto de todas las secuencias especiales. Demuestre que $\mathcal{S} \approx \mathcal{E}$.

Solución

Ya que $\mathcal{E} \subseteq \mathcal{S}$, tenemos $\mathcal{E} \preceq \mathcal{S}$. Por el teorema de Schröder–Bernstein, basta mostrar que $\mathcal{S} \preceq \mathcal{E}$. Es decir, hay que construir una función $f\colon \mathcal{S} \to \mathcal{E}$ inyectiva. Dado una secuencia infinita $a = (a_n)_{n\geq 0}$ de 0's y 1's, definimos:

$$f(a) = 0^{a_0+1}10^{a_1+1}10^{a_2+1}1\ldots$$

Es decir, cambiamos cada 0 en la secuencia a por 01, y cada 1 por 001. La secuencia resultante es especial porque tiene no más que dos 0's consecutivos y no más que un 1 consecutivo. Dado $f(a)$, se puede definir a únicamente: por ejemplo, $a_0 = 0$ si hay un 0 hasta el primer 1 en $f(a)$ y $a_0 = 1$ si hay dos 0's hasta el primer 1; así mismo, a_1 se puede definir a través del número de 0's entre el primer y el segundo 1 en $f(a)$. En general, para $n \geq 1$, $a_n = 0$ si hay un 0 entre el n-ésimo 1 y el $(n+1)$-ésimo 1, y $a_n = 1$ si hay dos 0's entre el n-ésimo 1 y el $(n+1)$-ésimo 1. Por lo tanto, $f(a)$ siempre tiene una única preimagen, es decir, f es inyectiva.

Distribución de puntajes:
2.0 pts por la parte $\mathcal{E} \preceq \mathcal{S}$ y 4.0 pts por la parte $\mathcal{S} \preceq \mathcal{E}$. Descuentos a criterio del corrector.

Pregunta 5

Responda las siguientes preguntas.

(a) Sea $p \geq 2$ un número primo y $a \in \{1, \ldots, p-1\}$. Demuestre que para cada $b, c \in \mathbb{N}$ tal que $b \equiv_{p-1} c$, se tiene que $a^b \bmod p = a^c \bmod p$.

(b) Sea $n \geq 2$ un número compuesto (n no es un número primo). Demuestre que existe un número $a \in \{1, \ldots, n-1\}$ tal que $a^{n-1} \bmod n \neq 1$.

Solución

(a) Sin pérdidada de generalidad, podemos asumir que $b \geq c$. Entonces, ya que $b \equiv_{p-1} c$, tenemos $b - c = k(p-1)$ para algún $k \in \mathbb{N}$. Ahora, ya que $a \in \{1, \ldots, p-1\}$, tenemos que p no divide a, así que por el pequeño teorema de Fermat tenemos $a^{p-1} \equiv_p 1$. Por lo tanto,

$$a^b = a^{c+k(p-1)} = a^c \cdot (a^{p-1})^k \equiv_p a^c \cdot (1)^k = a^c,$$

y eso nos da $a^b \bmod p = a^c \bmod p$.

(b) Ya que $n \geq 2$ no es número primo, posee un divisor d tal que $1 < d < n$. Vale decir, $d \in \{1, 2, \ldots, n-1\}$. Demostremos que $d^{n-1} \bmod n \neq 1$.

Alternativa 1: Por contradicción, supongamos que $d^{n-1} \bmod n = 1$. Entonces, existe $q \in \mathbb{Z}$ tal que $d^{n-1} = qn + 1$. Luego, $1 = d^{n-1} - qn$. Tenemos que $d | d^{n-1}$ porque $n \geq 2$ y sabemos que $d | n$. Entonces, d divide a 1, lo cual es una contradicción porque $d > 1$.

Alternativa 2: Por contradicción, supongamos que $d^{n-1} \bmod n = 1$. En particular, esto nos dice que $d \cdot d^{n-2} \bmod n = 1$, y entonces d^{n-2} es inverso de d modulo n (notar que d^{n-2} es un entero bien definido, ya que $n \geq 2$). Esto es una contradicción ya que $mcd(d, n) > 1$. (Recordar el teorema visto en clases: x tiene inverso modulo n si y solo si $mcd(x, n) = 1$.)

Distribución de puntajes:
3.0 pts por la parte (a) y 3.0 pts por la parte (b). Descuentos a criterio del corrector.