PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

IIC1253 - Matemáticas Discretas
1° semestre 2014 - Prof. Gabriel Diéguez

Examen

Nombre: ________________________________ **N° alumno:** _______________ **N° lista:** ________

Parte A (20 %)

Instrucciones

- Marque sólo una alternativa.
- En las líneas siguientes a cada pregunta debe **justificar brevemente** su respuesta.
- Si no justifica o la justificación es incorrecta, no se considerará la alternativa que haya marcado.
- Cada pregunta vale 0,375 ptos.
- Tiempo: 50 mins.

1. Sean A y B dos conjuntos no enumerables. ¿Cuál de las siguientes afirmaciones es siempre verdadera?

    a) $A \cup B$ no es enumerable.
    b) $A \cap B$ no es enumerable.
    c) A es equinumeroso con $\mathbb{R}$.
    d) B es equinumeroso con $2^{\mathbb{N}}$.

2. Respecto al protocolo RSA, ¿cuál de las siguientes afirmaciones es falsa?

    a) Los números e y d deben ser coprimos.
    b) $E(D(M)) = M$.
    c) N debe ser difícil de factorizar.
    d) $D(E(M)) = M$.

---

3. De las siguientes relaciones, ¿cuál es un orden total?

    a) Consecuencia lógica $\models$
    b) Divide a $|$
    c) Subconjunto $\subseteq$
    d) Menor o igual $\leq$

---

4. En un curso del DCC el profesor necesita dividir a los alumnos en k grupos, con la condición de que ninguno de los miembros del grupo se conozca. Para resolver esto, construye un grafo $G = (V, E)$, donde cada vértice en V es una persona, y dos vértices (i.e. personas) estarán conectadas en E si se conocen. ¿Cuál de las siguientes afirmaciones es suficiente para satisfacer la restricción?

    a) G tiene k componentes conexas.
    b) G es k-coloreable.
    c) G es un árbol.
    d) G es bipartito.

---

5. Sea un vocabulario $\mathcal{L} = \{R, f, c\}$, donde R es una relación, f es una función y c es una constante. Suponga que x es una variable.

   De las siguientes, ¿cuál no es una $\mathcal{L}$-fórmula?

   a) $\exists x(f(c) = f(x) \wedge R(x))$
   b) $f(x) = c$
   c) $\forall x(f(x) \vee f(c))$
   d) $f(x) = f(x)$

---

6. Sea la fórmula en lógica proposicional $\varphi = p \rightarrow (q \rightarrow r)$. Determine de cuál de los siguientes conjuntos de fórmulas es consecuencia lógica la fórmula φ:

   a) $\{p \wedge q\}$
   b) $\{q \wedge r\}$
   c) $\{p \vee q\}$
   d) $\{q \vee r\}$

---

7. Considere el siguiente algoritmo iterativo:

   Precondiciones: A es un arreglo de números naturales, y n es el largo del arreglo.
   Postcondiciones: m es el mayor número del arreglo A.

```
i ← 1
m ← A[0]
while i ≠ n do
    if A[i] > m then
        m ← A[i]
        i ← i + 1
    end if
end while
return m
```

   Suponiendo que el input entregado al programa cumple las precondiciones, ¿qué se puede decir sobre la corrección de este algoritmo?

   a) Depende del input entregado.
   b) No es correcto, ya que no se detiene.
   c) Es correcto, pues tiene un invariante para el loop que calcula el máximo.
   d) No es correcto, pues no se satisfacen las postcondiciones cuando se detiene.

---

8. Se tiene la siguiente definición inductiva de los números naturales:

   El conjunto de los números naturales $\mathbb{N}$ es el menor conjunto que satisface las siguientes reglas:

   - $\varnothing \in \mathbb{N}$
   - Si $x \in \mathbb{N}$, entonces $\delta(x) \in \mathbb{N}$

   ¿Cuál de las siguientes es una definición válida para el operador δ?

   a) $\delta(x) = x$
   b) $\delta(x) = x + 1$
   c) $\delta(x) = x \cup \{x\}$
   d) $\delta(x) = x \cap \{x\}$

---

9. Dada la función $f(n) = \log_{10}(n)$, ¿cuál de las siguientes afirmaciones es falsa?

   a) $f(n) \in \Omega(\log_{1000}(n))$
   b) $f(n) \in O(n)$
   c) $f(n) \in \Omega(n)$
   d) $f(n) \in O(2^n)$

---

10. ¿Cuántas aristas tiene $K_{m,n}$?

    a) $m \cdot n$
    b) $\max\{m, n\}$
    c) $m + n$
    d) $\frac{(m+n)^2}{2}$

---

11. La siguiente es una ecuación de recurrencia para el tiempo de ejecución T de un algoritmo en función de su input $n \geq 0$:

$$T(n) = \begin{cases} 3 & n > 2 \\ 5 \cdot T(\lceil \frac{n}{2} \rceil) + 3 \cdot T(\lfloor \frac{n}{2} \rfloor) + 150 \cdot n^3 & n \leq 2 \end{cases}$$

¿Cuál es el orden de complejidad del tiempo de ejecución del algoritmo?

a) $\Theta(1)$
b) $\Theta(n)$
c) $\Theta(n^3)$
d) $\Theta(n^3 \log n)$

---

12. Sean $a, b, c, d, n \in \mathbb{Z}$ con $n > 1$, tales que $a \equiv b \bmod n$ y $c \equiv d \bmod n$. ¿Cuál de las siguientes afirmaciones NO es necesariamente cierta?

a) $a \bmod n = b \bmod n$
b) $(a + c) \equiv (b + d) \bmod n$
c) $\exists k \in \mathbb{Z}((a = b + kn) \wedge (c = d + kn))$
d) $(a \cdot c) \equiv (b \cdot d) \bmod n$

---

13. ¿Cuándo decimos que un problema de decisión es tratable?

a) Cuando está en la clase de complejidad P.
b) Cuando está en la clase de complejidad NP.
c) Cuando existe un algoritmo que lo resuelve.
d) Cuando existe un algoritmo que lo resuelve y siempre se detiene.

---

14. Dado un conjunto de personas P, se tiene una relación de vecindad $R \subseteq P \times P$, en que dos personas estarán relacionadas si viven en el mismo barrio. Es deseable que esta relación siga las reglas usuales de la vecindad: si una persona es vecina de otra, entonces se cumpla lo inverso, y que si una persona tiene un vecino, y ese vecino tiene otro vecino, entonces los tres son vecinos. Por simplicidad, se asume que una persona es vecina de sí misma. ¿Qué debe cumplir R para seguir las reglas de la vecindad?

   a) R debe ser antisimétrica.
   b) R debe ser una relación de orden total.
   c) R debe ser una función.
   d) R debe ser una relación de equivalencia.

---

15. Sean p, q, r las siguientes proposiciones:

   p: Ganamos los penales q: Pinilla le pega al palo r: Chile es campeón del mundo

   ¿Cuál de las siguientes fórmulas en lógica proposicional representa a la oración "Si hubiéramos ganado los penales o Pinilla no le hubiera pegado al palo, Chile habría sido campeón del mundo"?

   a) $(p \vee r) \wedge (\neg q \vee r)$
   b) $(\neg p \vee r) \wedge (q \vee r)$
   c) $(p \wedge \neg q) \rightarrow r$
   d) $(p \vee \neg q) \leftrightarrow r$

---

16. Considere la siguiente definición inductiva de una propiedad $Prop(\cdot)$ sobre fórmulas en lógica de primer orden:

   Sea $\mathcal{L}$ un vocabulario y φ una $\mathcal{L}$-fórmula:

   - Si φ es atómica, entonces $Prop(\varphi) = 0$.
   - Si $\varphi = (\neg\psi)$, entonces $Prop(\varphi) = 1 + Prop(\psi)$.
   - Si $\varphi = (\psi_1 \star \psi_2)$, donde $\star \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, entonces $Prop(\varphi) = 1 + \text{máx}\{Prop(\psi_1), Prop(\psi_2)\}$.
   - Si $\varphi = (\exists x\psi)$ o $\varphi = (\forall x\psi)$, entonces $Prop(\varphi) = Prop(\psi)$.

   Dada una fórmula en lógica de primer orden φ, ¿qué representa la propiedad $Prop(\varphi)$?

   a) El número total de cuantificadores de φ.
   b) La cantidad de paréntesis de φ.
   c) El número máximo de conectivos anidados de φ.
   d) El número de $\mathcal{L}$-términos de φ.

PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

IIC1253 - Matemáticas Discretas
1° semestre 2014 - Prof. Gabriel Diéguez

Examen

Parte B (80 %)

1. Conteste 4 de las siguientes 5 preguntas (si las contesta todas se corregirán las primeras 4):
   a) Demuestre que el Principio del Buen Orden, el Principio de Inducción Simple y el Principio de Inducción Fuerte son equivalentes.
   b) Demuestre que el intervalo real $[0,1]$ no es enumerable.
   c) Dé un ejemplo de una relación de equivalencia y otra de orden parcial y demuestre que lo son.
   d) Demuestre que $\{\neg, \wedge\}$ es funcionalmente completo.
   e) Enuncie el (pequeño) teorema de Fermat y su corolario, y demuestre este último.
2. Considere el siguiente problema de decisión:

$$HALF-CLIQUE = \{G \mid G \text{ es un grafo de } n \text{ vértices que tiene un clique de tamaño } \tfrac{n}{2}\}$$

   En esta pregunta usted mostrará que este problema es NP-completo.
   a) Demuestre que $HALF-CLIQUE$ está en NP. Para esto:
      I) [0,5 ptos.] Dado un grafo G, encuentre un certificado $c(G)$ de tamaño polinomial con respecto a G que permita chequear en tiempo polinomial si $G \in HALF-CLIQUE$.
      II) [0,5 ptos.] Escriba un algoritmo en pseudo-código que reciba como input un grafo G y su certificado $c(G)$, que usando el certificado determine si $G \in HALF-CLIQUE$. Su algoritmo debe tener complejidad polinomial.
      III) [1,5 ptos.] Demuestre que su algoritmo es correcto.
      IV) [1,5 ptos.] Determine la complejidad exacta de su algoritmo.
   b) Sea el problema de decisión

$$CLIQUE = \{(G,k) \mid G \text{ es un grafo de } n \text{ vértices que tiene un clique de tamaño } k\}$$

   En ayudantía se demostró que $CLIQUE$ es NP-completo. Entonces, para terminar de mostrar que $HALF-CLIQUE$ es NP-completo, debe realizar lo siguiente:
      I) [1 pto.] Dado un grafo G de n vértices y $0 < k \leq n$, explique cómo construir en tiempo polinomial un nuevo grafo G' a partir de G, de manera que $(G,k) \in CLIQUE$ si y sólo si $G' \in HALF-CLIQUE$. No es necesario que escriba un algoritmo en pseudo-código ni que muestre formalmente la complejidad, pero debe explicar **claramente** cómo construir el grafo y por qué se puede hacer en tiempo polinomial.
      II) [0,5 ptos.] Demuestre que si $(G,k) \in CLIQUE$, entonces $G' \in HALF-CLIQUE$.
      III) [0,5 ptos.] Demuestre que si $G' \in HALF-CLIQUE$, entonces $(G,k) \in CLIQUE$.