



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

Lógica para Ciencia de la Computación - IIC2212
Interrogación 1

Problema 1 [1.5 puntos]

Sea $n \geq 2$ un número natural fijo. La estructura $\mathbb{Z}_n = (\{0, \dots, n-1\}, +, \cdot)$ se define de la siguiente forma. Sean a y b dos números en el conjunto $\{0, \dots, n-1\}$. Entonces se tiene que $a + b$ es el resto módulo n de la suma usual entre a y b , y $a \cdot b$ es el resto módulo n de la multiplicación usual entre a y b . Por ejemplo, las siguientes son las tablas de las operaciones $+$ y $\cdot$ para $n = 5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Sea V un conjunto infinito de variables. El conjunto de expresiones aritméticas $E(V)$ es definido como el menor conjunto que satisface las siguiente reglas:

- $V \subseteq E(V)$.
- Si $e_1 \in E(V)$ y $e_2 \in E(V)$, entonces $(e_1 + e_2) \in E(V)$ y $(e_1 \cdot e_2) \in E(V)$.

Por ejemplo, $(u \cdot (v + w))$ y $(u + (u \cdot v))$ son expresiones en $E(V)$, suponiendo que u , v y w son variables en V .

Sea e una expresión aritmética que menciona a las variables $x_1, \dots, x_k$. Dados $i_1, \dots, i_k \in \{0, \dots, n-1\}$, decimos que $x_1 \rightarrow i_1, \dots, x_k \rightarrow i_k$ es una raíz para e en $\mathbb{Z}_n$ si la evaluación de e en $\mathbb{Z}_n$ con cada x_j reemplazado por i_j ($j \in \{1, \dots, k\}$) da como resultado 0. Por ejemplo, $u \rightarrow 2, v \rightarrow 4$ es una raíz para la expresión aritmética $(u + (u \cdot v))$ en $\mathbb{Z}_5$, como también lo es $u \rightarrow 0, v \rightarrow 0$. Finalmente, decimos que una raíz $x_1 \rightarrow i_1, \dots, x_k \rightarrow i_k$ para e en $\mathbb{Z}_n$ es *no trivial* si al menos uno de los números i_j ($j \in \{1, \dots, k\}$) es distinto de 0. Así, por ejemplo, $u \rightarrow 2, v \rightarrow 4$ es una raíz no trivial de $(u + (u \cdot v))$ en $\mathbb{Z}_5$, mientras que $u \rightarrow 0, v \rightarrow 0$ no lo es.

- [1 punto] Encuentre un algoritmo eficiente que dada una expresión aritmética e , genere una fórmula φ tal que e tiene una raíz no trivial en $\mathbb{Z}_n$ si y sólo si φ es satisfacible.
- [0.5 puntos] Aplique la metodología desarrollada en (a) para el caso de $n = 3$ y la expresión aritmética $(x + (y \cdot (x + y)))$.

Importante: Decimos que un algoritmo es eficiente si el número de pasos ejecutado por el algoritmo es m^c cuando la entrada tiene largo m , donde c es una constante.

Problema 2 [1.5 puntos]

Una *cláusula de Horn* es una cláusula que tiene a lo más un literal positivo. Por ejemplo $\neg p$, $(\neg p \vee \neg q)$ y $(p \vee \neg q \vee \neg r \vee \neg s)$ son todas cláusulas de Horn, mientras que $(p \vee q \vee \neg r)$ no es una cláusula de Horn porque tiene dos literales positivos. Demuestre que existe una fórmula que no es equivalente a ningún conjunto de cláusulas de Horn.

Problema 3 [1.5 puntos]

Un grafo G es una tupla (N, A) , donde N es un conjunto de nodos y $A \subseteq N \times N$ es un conjunto de arcos. Un grafo es no dirigido si cada vez que $(a, b) \in A$ se tiene que $(b, a) \in A$. Un grafo $G' = (N', A')$ es un subgrafo de $G = (N, A)$ si $N' \subseteq N$ y $A' \subseteq A$.

Un grafo no dirigido $G = (N, A)$ es 3-coloreable si existe una asignación de 3 colores para los nodos de G tal que nodos adyacentes reciben colores distintos. Formalmente, G es 3-coloreable si existe una función $f : N \rightarrow \{\text{blanco}, \text{azul}, \text{rojo}\}$ tal que para cada $(a, b) \in A$ se tiene que $f(a) \neq f(b)$.

Sea $G = (N, A)$ un grafo tal que $N = \mathbb{N}$ y para todo subgrafo finito G' de G , se tiene que G' es 3-coloreable. Utilice herramientas del cálculo proposicional para demostrar que G es 3-coloreable.

Problema 4 [1.5 puntos]

En clases se demostró que es necesario agregar la regla de factorización a la regla de resolución para obtener un sistema de demostración que satisface la noción de completitud débil. Suponga que se reemplaza estas dos reglas por la *regla de resolución extendida*:

$$\frac{C_1 \vee \ell \vee C_2 \vee \ell \vee \cdots \vee C_{n-1} \vee \ell \vee C_n \quad D_1 \vee \bar{\ell} \vee D_2 \vee \bar{\ell} \vee \cdots \vee D_{m-1} \vee \bar{\ell} \vee D_m}{C_1 \vee C_2 \vee \cdots \vee C_{n-1} \vee C_n \vee D_1 \vee D_2 \vee \cdots \vee D_{m-1} \vee D_m}$$

donde $n \geq 2$, $m \geq 2$, cada C_i ($i \in \{1, \dots, n\}$) es una cláusula y cada D_j ($j \in \{1, \dots, m\}$) también es una cláusula. Por ejemplo, las siguientes son dos aplicaciones de la regla de resolución extendida:

$$\frac{p \vee p \quad \neg p \vee \neg p \vee \neg p}{\square} \qquad \frac{q \vee p \vee \neg r \vee p \vee p \quad \neg p \vee \neg r \vee s \vee t \vee \neg p}{q \vee \neg r \vee \neg r \vee s \vee t}$$

Dada una cláusula C y un conjunto de cláusulas Σ , una demostración por resolución extendida de C a partir de Σ es una secuencia de cláusulas $C_1, C_2, \dots, C_n$ tal que:

- Para cada $i \leq n$:
 - $C_i \in \Sigma$ o
 - existen $j, k < i$ tales que C_i es obtenido desde C_j y C_k usando la regla de resolución extendida.
- $C_n = C$.

Si C es demostrable desde Σ por resolución extendida, entonces usamos la notación $\Sigma \vdash_E C$. Nótese que la regla de resolución extendida es correcta, por lo que se tiene que el sistema es correcto: Si $\Sigma \vdash_E C$, entonces $\Sigma \models C$. En esta pregunta usted debe verificar si la regla de resolución extendida satisface la noción de completitud débil. Vale decir, demuestre o de un contraejemplo para la siguiente afirmación: Si $\Sigma \models \square$, entonces $\Sigma \vdash_E \square$.