Práctico 2 Parte 2 Complejidad Computacional

Julián Viera

jviera@fing.edu.uy
julviera44@gmail.com

16 de septiembre de 2021

Agenda

El lenguaje $\neq SAT$

Sea ϕ una fórmula booleana $3CNF$. Una *asignacion* $\neq$ para las variables de ϕ es una asignación de valores de verdad en dónde cada cláusula contiene dos literales con valor de verdad distintos. En otras palabras, una *asignacion* $\neq$ satisface ϕ sin asignarle $TRUE$ a los tres literales de cualquier cláusula de ϕ.

Resulta claro que si una fórmula $3CNF$ tiene una *asignacion* $\neq$, dicha fórmula es satisfactible con esa asignación, ya que en cada cláusula va a haber al menos un literal con valor de verdad 1.

Se define el lenguaje $\neq SAT$ como el conjunto de fórmulas $3CNF$ que tienen una *asignacion* $\neq$.

Se lo conoce también con el nombre NAE 3SAT (Not All Equal 3SAT)

Ejemplo de fórmula del lenguaje $\neq SAT$

Ejemplo de fórmula $3CNF$ que pertenece a $\neq SAT$:
$\Phi_1 = (x_3 \vee \overline{x_1} \vee x_2) \wedge (x_1 \vee \overline{x_3} \vee \overline{x_2}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$
La asignación $(x_1, x_2, x_3) = (1, 1, 1)$ es una *asignacion* $\neq$ para Φ_1 ya que en cada cláusula hay literales con distinto valor de verdad.

Ejemplo de fórmula $3CNF$ que no pertenece a $\neq SAT$:
$\Phi_2 = (x_1 \vee \overline{x_2} \vee \overline{x_2}) \wedge (x_1 \vee x_2 \vee x_2) \wedge (\overline{x_1} \vee x_2 \vee x_2)$
Φ_2 pertenece a $3SAT$ pues se satisface con la asignación $(x_1, x_2) = (1, 1)$, pero no tiene una *asignacion* $\neq$, por lo que no pertenece a $\neq SAT$ (en particular para $(x_1, x_2) = (1, 1)$, en la segunda cláusula todos los literales toman el valor 1).

Se tiene entonces el resultado general $\neq SAT \subset 3SAT$.

Ejercicio 12 - Planteo del problema

El problema planteado consiste en probar que $\neq SAT$ es NP-completo.

Se sugiere:

1. Probar que la negación de una *asignacion* $\neq$ es también una *asignacion* $\neq$.
2. Considerar una reducción del problema $3SAT$ a $\neq SAT$, consistente en reemplazar cada cláusula $c_i = (y_1 \vee y_2 \vee y_3)$ de la fórmula $3CNF$ por las dos cláusulas $(y_1 \vee y_2 \vee z_i)$ y $(\overline{z_i} \vee y_3 \vee b)$, dónde z_i es una nueva variable para cada cláusula c_i y b es una nueva variable única global.

Prueba de que $\neq SAT \in NP$

Sea Φ una fórmula $3CNF$ instancia del problema $\neq SAT$.
Un potencial cerificado para $\neq SAT$ consiste en una asignación particular de valores de verdad a las variables de Φ.
El certificado puede verificarse en tiempo polinomial en el número de cláusulas de la fórmula, recorriendo secuencialmente las cláusulas de la misma y corroborando que en toda cláusula hayan dos literales con valor de verdad distintos (lo que asegura también que toda cláusula evalúa en 1, y por lo tanto la fórmula se satisface).

Si n es el número de cláusulas de Φ, la verificación insume tiempo $\mathcal{O}(n)$.
$\Longrightarrow \neq SAT \in NP$

Prueba de que la negación de una *asignacion* $\neq$ es una *asignacion* $\neq$

Sea Z una *asignacion* $\neq$ para la fórmula 3CNF Φ.
Sea c_i una cláusula cualquiera de Φ, $c_i = (x_i \vee y_i \vee z_i)$.
Consideramos sin perder generalidad que en c_i y bajo la asignación Z los literales x_i y z_i tienen valores de verdad opuestos.
En la negación $\overline{Z}$ de Z, como se invierten todos los valores de verdad, en c_i y bajo $\overline{Z}$ los literales x_i y z_i también van a tener valores de verdad opuestos.
$\Longrightarrow \overline{Z}$ es una *asignacion* $\neq$ para las variables de Φ.

Prueba de que la reducción propuesta $3SAT \leq_P \neq SAT$ es polinomial

Sea Φ una fórmula $3CNF$ instancia del problema $3SAT$.
Su instancia correspondiente $f(\Phi)$ en $\neq SAT$ se construye recorriendo secuencialmente las cláusulas de Φ y por cada una de ellas generando dos cláusulas de $f(\Phi)$.
$c_i = (y_1 \vee y_2 \vee y_3) \Longrightarrow f(c_i) = (y_1 \vee y_2 \vee z_i) \wedge (\overline{z_i} \vee y_3 \vee b)$

Si n es el número de cláusulas de Φ, este construcción demanda tiempo $\mathcal{O}(n)$.
$\Longrightarrow$ la reducción propuesta es polinomial.

Correctitud de la reducción propuesta

Probaremos que Φ es una instancia SI de $3SAT \Leftrightarrow f(\Phi)$ es una instancia SI de $\neq SAT$.

$\Longrightarrow$

Ⓗ Φ es una instancia SI de $3SAT$

Ⓣ $f(\Phi)$ es una instancia SI de $\neq SAT$

Sea $\Phi \in 3SAT$. Consideramos una cláusula genérica de Φ, $c_i = (y_1 \vee y_2 \vee y_3)$.

Por la forma de la reducción, $f(c_i) = (y_1 \vee y_2 \vee z_i) \wedge (\overline{z_i} \vee y_3 \vee b)$.

Elegimos $b = 0$. Como Φ es satisfactible por hipótesis, al menos uno de los $y_i = 1, i = 1, 2, 3$.

Si $y_1 = 1$ o $y_2 = 1$, se toma $z_i = 0$ y se verifica entonces que:

1. Ambas cláusulas de $f(c_i)$ evalúan en 1
2. Ambas cláusulas de $f(c_i)$ tienen literales con valor de verdad distinto: el y_i que vale 1 y zi en la primera cláusula, y b y $\overline{z_i}$ en la segunda.

Correctitud de la reducción propuesta

Si $y_1 = y_2 = 0$, entonces necesariamente debe ser $y_3 = 1$ ya que c_i se satisface en Φ. En este caso elegimos $z_i = 1$, y se verifica:

1. Ambas cláusulas de $f(c_i)$ evalúan en 1
2. Ambas cláusulas de $f(c_i)$ tienen literales con valor de verdad opuesto: los dos y_i y z_i en la primer cláusula y b e y_3 en la segunda

$\Longrightarrow$ se encontró una asignación de valores de verdad que satisface $f(\Phi)$,cumpliendo la condición de que en toda cláusula de $f(\Phi)$ hay dos literales con valor de verdad distinto

$\Longrightarrow$ $f(\Phi)$ es una instancia SI de $\neq SAT$

Correctitud de la reducción propuesta

$\Longleftarrow$

(H) $f(\Phi)$ es una instancia SI de $\neq SAT$

(T) Φ es una instancia SI de $3SAT$

Sea $f(\Phi) \in \neq SAT$. Consideramos una cláusula genérica de $f(\Phi)$:
$f(c_i) = (y_1 \vee y_2 \vee z_i) \wedge (\overline{z_i} \vee y_3 \vee b)$, con $c_i = (y_1 \vee y_2 \vee y_3) \in \Phi$.
Sea Z una *asignacion* $\neq$ para $f(\Phi)$, existente por hipótesis.
Se consideran dos casos:
Caso (1); En Z se tiene $b = 0$.
En este caso al menos uno de los $y_i = 1, i = 1, 2, 3$. Si esto no fuera así, debería ser $z_i = 1$ para que en la primera cláusula hayan dos literales opuestos, pero en ese caso los tres literales de la segunda cláusula valen 0 y se contradice la hipótesis de que Z sea una *asignacion* $\neq$ para $f(\Phi)$.
$\Longrightarrow c_i = (y_1 \vee y_2 \vee y_3)$ evalúa en 1 en Z, $\forall c_i \in \Phi$.

Correctitud de la reducción propuesta

Caso ②; En Z se tiene $b = 1$.
En este caso consideramos $\overline{Z}$, la negación de la asignación Z.
Por la propiedad demostrada anteriormente, se cumple también que $\overline{Z}$ es una *asignacion* $\neq$ para $f(\Phi)$.
En $\overline{Z}$ se verifica que $b = 0$, por lo que observamos que este caso se reduce al caso ①.
$\Longrightarrow c_i = (y_1 \vee y_2 \vee y_3)$ evalúa en 1 en $\overline{Z}$, $\forall c_i \in \Phi$.
$\Longrightarrow$ se encontró una asignación de valores de verdad que satisface Φ.
$\Longrightarrow$ Φ es una instancia SI de $3SAT$.

La clase de problemas coNP

Complemento $\overline{L}$ de un lenguaje L : $\overline{L} = \{0,1\}^* \setminus L$

$coNP = \{L \;/\; \overline{L} \in NP\}$

Un lenguaje L es coNP-completo si:

1. $L \in coNP$
2. $L^* \in coNP \implies L^* \leq_P L$.

Ejercicio 13 - Planteo del problema

Probar que un lenguaje L es NP-completo si y solo si $\overline{L}$ es coNP-completo

Prueba del Directo

$\Longrightarrow$

(H) L es NP-completo

(T) $\overline{L}$ es coNP-completo

(1) $\overline{L} \in coNP$ pues $\overline{\overline{L}} = L \in NP$

(2) Sea $\overline{L^*} \in coNP \Longrightarrow L^* \in NP \overset{(H)}{\Longrightarrow} L^* \leq_P L$

$\Longrightarrow x \in L^* \Leftrightarrow f(x) \in L \Longrightarrow x \notin L^* \Leftrightarrow f(x) \notin L$

$\Longrightarrow x \in \overline{L^*} \Leftrightarrow f(x) \in \overline{L} \Longrightarrow \overline{L^*} \leq_P \overline{L}$

De (1) y (2) $\Longrightarrow \overline{L}$ es coNP-completo.

Prueba del Recíproco

$\Longrightarrow$

Ⓗ $\overline{L}$ es coNP-completo

Ⓣ L es NP-completo

① $\overline{L} \in coNP \Longrightarrow$ por definición de coNP $\overline{\overline{L}} = L \in NP$

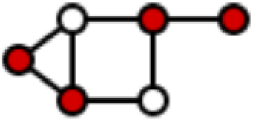
② Sea $L^* \in NP \Longrightarrow \overline{L^*} \in coNP \overset{H}{\Longrightarrow} \overline{L^*} \leq_P \overline{L}$
$\Longrightarrow \exists f /\ x \in \overline{L^*} \Leftrightarrow f(x) \in \overline{L} \Longrightarrow x \notin \overline{L^*} \Leftrightarrow f(x) \notin \overline{L}$
$\Longrightarrow x \in L^* \Leftrightarrow f(x) \in L \Longrightarrow L^* \leq_P L$

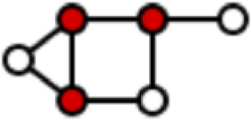
De ① y ② $\Longrightarrow$ L es NP-completo.

Vertex Cover de un grafo

Dado G grafo simple no dirigido, un *vertex cover* (cubrimiento de vértices) de G es un subconjunto S de nodos de G tal que para toda arista (u, v) de G, al menos uno de los nodos u o v pertenecen a S (toda arista del grafo tiene al menos un extremo en un nodo de S).

En los ejemplos siguientes, los nodos en rojo constituyen dos *vertex cover* distintos de un mismo grafo. En el caso de la derecha, se tiene un *vertex cover* minimal, en el sentido de que es el cubrimiento de vértices con menor número de nodos posibles para ese grafo.

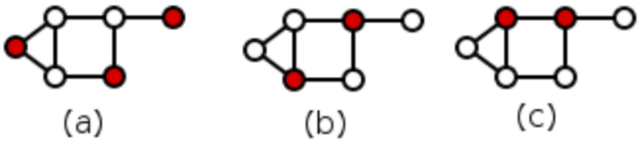




Dominating Set de un grafo

Dado G grafo simple no dirigido, un *dominating set* (conjunto dominante) de G es un subconjunto S de nodos de G tal que todo nodo de G o bien pertenece a a S o es adyacente a algún nodo de S.

En los ejemplos siguientes, los nodos en rojo constituyen conjuntos dominantes para un mismo grafo. En los casos b) y c), se trata de *dominating sets* minimales en el sentido de que son los conjuntos dominantes con el menor número de nodos posibles para ese grafo.



Dominating Set vs *Independent Set*

Los dominating sets está estrechamente vinculados a los independent sets.

Todo independent set <u>*maximal*</u> de un grafo G es un dominating set para G. Esto lo ejemplifica el conjunto de nodos en rojo de (a), que es un independent set maximal de G y a la vez es un dominating set de G.

No se verifica en cambio que un dominating set <u>*minimal*</u> de G sea necesariamente un independent set de G, como lo muestra el ejemplo (c) en donde tenemos un dominating set minimal que no es un independent set.

(a) (b) (c)

Planteo del problema 10

$VERTEX\ COVER = \{< G, k > / G$ tiene un vertex cover de a lo sumo k nodos $\}$

$DOMINATING\ SET = \{< G, k > / G$ tiene un dominating set de a lo sumo k nodos $\}$

El problema planteado consiste en probar que *DOMINATING SET* es NP-completo, dando una reducción a él del problema *VERTEX COVER*, el cual se asume como NP-completo.

Prueba de que *DOMINATING SET* $\in$ *NP*

Sea $< G, k >$ la instancia del problema *DOMINATING SET*.
Sea A la matriz de adyacencia nxn del grafo G de n nodos.
Un cerificado para *DOMINATING SET* consiste en un conjunto C de nodos de G que constituyen un dominating set. Lo podemos representar como un vector de booleanos de largo n, en donde un 1 indica pertenencia al dominating set.
El algoritmo verificador:

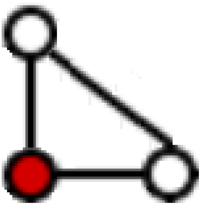
1. Chequea que $|C| \leq k$. Esto se hace recorriendo el vector booleano de C en tiempo $\mathcal{O}(n)$.
2. Recorre todos los nodos del grafo que no pertenecen al certificado C y comprueba que cada uno tenga al menos un adyacente en C. Esta verificación se puede hacer en tiempo $\mathcal{O}(n^2)$ en el peor caso, ya que implica recorrer por filas la matriz de adyacencia A.

$\Longrightarrow$ *DOMINATING SET* $\in$ *NP*

Reducción de *VERTEX COVER* a *DOMINATING SET*

Hay que encontrar una reducción de tiempo polinomial del problema *VERTEX COVER* a *DOMINATING SET*, lo que prueba que *DOMINATING SET* es NP-hard.

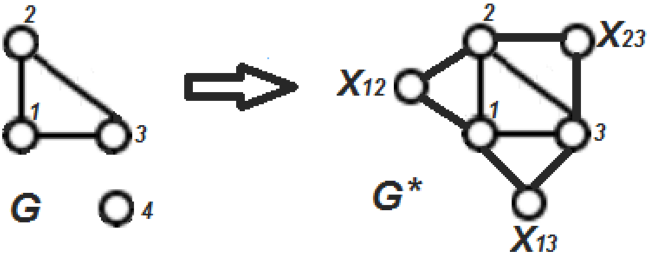
La transformación identidad de una instancia $< G, k >$ de *VERTEX COVER* a una instancia $< G, k >$ de *DOMINATING SET* no funciona, como puede verse en el ejemplo simple de la figura. En este caso si se elige $k = 1$, se tiene que $< G, 1 >$ es una instancia SI de *DOMINATING SET* pero es una instancia NO de *VERTEX COVER*.



Reducción de *VERTEX COVER* a *DOMINATING SET*

Sea $< G, k >$ una instancia de *VERTEX COVER*. La reducción propuesta mapea $< G, k >$ en $< G^*, k^* >$ en donde:

1. G^* contiene todos los nodos <u>no aislados</u> y todas las aristas de G. Por cada arista (u, v)en G, se crea un nuevo nodo X_{uv} en G^* y se añaden las aristas (u, X_{uv}) y (v, X_{uv}).
2. Se toma $k^* = k$.



Prueba de que *VERTEX COVER* $\leq_P$ *DOMINATING SET* es polinomial

Sea $< G, k >$ una instancia de *VERTEX COVER*. G se supone con n nodos y e aristas.
La instancia correspondiente $f(< G, k >) =< G^*, k >$ en *DOMINATING SET* se construye recorriendo todas las aristas de G y para cada una de ellas generando la misma arista en G^*, así como el nuevo nodo asociado a la arista y y las dos nuevas aristas correspondientes.
Si G y G^* se representan por sus respectivas matrices de adyacencia A_{nxn} y $A^*_{(n+e)x(n+e)}$, el tiempo de construcción de $A^*_{(n+e)x(n+e)}$ es $\mathcal{O}(n^2)$.

$\Longrightarrow$ la reducción propuesta es polinomial.

Correctitud de la reducción propuesta

Probaremos que $< G, k > \in VERTEX\ COVER \Leftrightarrow f(< G, k >) = < G^*, k > \in DOMINATING\ SET$.

Abreviaremos vertex cover como VC y dominating set como DS.

$(\Longrightarrow)$

(H) $< G, k >$ es una instancia SI de $VERTEX\ COVER$

(T) $< G^*, k >$ es una instancia SI de $DOMINATING\ SET$

Sea $< G, k > \in VERTEX\ COVER$. Por (H), G tiene un VC H con $|H| \leq k$.

Sea un nodo cualquiera $v \in G^*$ / $v \notin H$. Hay dos casos:

1. $v \in G \xRightarrow{\text{definición de VC}}$ existe arista entre v y un cierto nodo w de H en $G \xRightarrow{\text{definición de f}}$ existe arista entre v y $w \in H$ en G^*.
2. $v \notin G \xRightarrow{\text{definición de f}} v$ es adyacente a dos nodos u y w de G / (u, v) es arista de $G \xRightarrow{\text{definición de VC}} u$ o w o ambos pertenecen a $H \Longrightarrow$ existe arista entre v y un nodo de H en G^* .

De (1) y (2) $\xRightarrow{\text{definición de DS}}$ H es un DS de G^*, con $|H| \leq k$

Correctitud de la reducción propuesta ($\Longleftarrow$)

H $< G^*, k >$ es una instancia SI de *DOMINATING SET*

T $< G, k >$ es una instancia SI de *VERTEX COVER*

Sea $< G^*, k > \in$ *DOMINATING SET*. Por H, G^* tiene un DS D con $|D| \leq k$.

Probaremos primero que G^* tiene un DS D' con $|D'| \leq k$ y todos los nodos de D' pertenecientes a G.

Sea $x \in D$ y $x \notin G \xRightarrow{\text{definición de f}} x$ es del tipo X_{uv} con (u, v) arista de G. Distinguimos dos casos:

1. Si $u \in D$ o $v \in D$, considero $D' = D - \{X_{uv}\} \Longrightarrow D'$ sigue siendo un DS para G^*, con $|D'| = |D| - 1 \leq k$.
2. Si $u \notin D$ y $v \notin D$, considero $D' = D - \{X_{uv}\} + \{u\}$ que sigue siendo un DS para G^*, con $|D'| = |D| \leq k$.

Dada una arista $(u, v) \in G \Longrightarrow$ se cumple que u o v o ambos pertenecen al DS D' de G^*, pues de lo contrario el nodo X_{uv} de G^* no sería adyacente a ningún nodo del DS D' de G^*.

$\xRightarrow{\text{definición de VC}} D'$ es un VC para G, con $|D'| \leq k$.

Definiciones de la clase coNP y planteo del problema 14

DEFINICION ① $coNP = \{L \ / \ \overline{L} \in NP\}$

DEFINICION ② $\forall L \subseteq \{0,1\}^*$, $L \in coNP$ si existe un polinomio $p : \mathbb{N} \longrightarrow \mathbb{N}$ y una MT de tiempo polinomial M de modo que: $\forall x \in \{0,1\}^*$: $x \in L \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}$, $M(x,u) = 1$.

El problema consiste en probar que las definiciones ① y ② de la clase coNP son equivalentes.

Prueba del Directo

① $\Longrightarrow$ ②

Sea L / $\overline{L} \in NP \Longrightarrow$ por definición de la clase NP, $\exists\ p : \mathbb{N} \longrightarrow \mathbb{N}$ y una MT de tiempo polinomial M de modo que:
$\forall x \in \{0,1\}^*$: $x \in \overline{L} \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}$ / $M(x,u) = 1$.
$\Longrightarrow x \notin \overline{L} \Leftrightarrow \nexists u \in \{0,1\}^{p(|x|)}$ / $M(x,u) = 1$
$\Longrightarrow x \notin \overline{L} \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}$, $M(x,u) = 0$
Sea la MT $M^*/M^*(x,u) = 0$ si $M(x,u) = 1$ y$M^*(x,u) = 1$ si $M(x,u) = 0$
$\Longrightarrow x \notin \overline{L} \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}$, $M^*(x,u) = 1$
$\Longrightarrow x \in L \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}$, $M^*(x,u) = 1$
$\Longrightarrow L \in coNP$ de acuerdo a la defínción ② $\blacksquare$

Prueba del Recíproco

② $\Longrightarrow$ ①

Sea $L \in coNP$ de acuerdo a la defínción ②
$\Longrightarrow \exists\ p, M / \forall x \in \{0,1\}^*$: $x \in L \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)},\ M(x,u) = 1.$
$\Longrightarrow x \notin L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}\ /\ M(x,u) = 0$
$\Longrightarrow x \in \overline{L} \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}\ /\ M^*(x,u) = 1$
$\Longrightarrow \overline{L} \in NP$ ■