UNIVERSIDAD DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

Matemáticas Discretas para la Computación - CC3101
Control 1 - Semestre Otoño 2017

1. *a*) Una relación binaria R sobre A se dice *euclideana* si satisface lo siguiente:

   Para todo $a, b, c \in A$, si $(a, b) \in R$ y $(a, c) \in R$ entonces $(b, c) \in R$.

   ¿Es cierto que R es de equivalencia si y solo si es refleja y euclideana?

   b) Sean $(S_1, \preceq_1)$ y $(S_2, \preceq_2)$ órdenes (parciales). Definimos su *producto cartesiano* $(S_{1,2}, \preceq_{1,2})$ de tal forma que: (i) $S_{1,2} = S_1 \times S_2$, y (ii) $(a, b) \preceq_{1,2} (c, d)$ si y solo si $a \preceq_1 c$ y $b \preceq_2 d$. Demuestre que si $|S_1|, |S_2| \geq 2$, entonces $(S_{1,2}, \preceq_{1,2})$ no es un orden total.

   Solución:

   a) Sí, es cierto. Asuma primero que R es de equivalencia. Por definición es refleja, por lo que solo debemos demostrar que es euclideana. Suponga entonces que $(a, b) \in R$ y $(a, c) \in R$. Luego, $(c, a) \in R$ por que R es simétrica. Por tanto, $(c, b) \in R$ por transitividad, y $(b, c) \in R$ por simetría.

   Asuma que R es refleja y euclideana. Primero demostramos que es simétrica. Asuma que $(a, b) \in R$. Además, $(a, a) \in R$ por reflexividad. Luego, $(b, a) \in R$ por que R es euclideana. Ahora demostramos que R es transitiva. Asuma que $(a, b) \in R$ y $(b, c) \in R$. Sabemos que R es simétrica, por lo que $(b, a) \in R$. Pero entonces $(a, c) \in R$ por propiedad euclideana.

   b) Asuma por contradicción que es un orden total. Tome dos elementos distintos $a, b \in S_1$ y dos elementos distintos $c, d \in S_2$. Por hipótesis, (a, c) y (b, d) son comparables con respecto a $\preceq_{1,2}$. Supongamos sin pérdida de generalidad que $(a, c) \preceq_{1,2} (b, d)$. Luego, por definición, $a \preceq_1 b$ y $c \preceq_2 d$. De la misma forma, (a, d) y (b, c) son comparables. Pero dado que $a \preceq_1 b$ esto implica que $d \preceq_2 c$. Como $\preceq_2$ es una relación antisimétrica, esto solo puede ocurrir si $c = d$, lo que es una contradicción.

2. El largo $l(\phi)$ de una fórmula ϕ en la lógica proposicional $\mathcal{L}(p)$ es el número de símbolos que aparecen en la fórmula al leerla de izquierda a derecha. (Asumimos que todos los paréntesis están presentes, incluidos los externos). Por ejemplo, $l(p) = 1$, si $p \in P$, y $l((p \wedge (\neg q))) = 8$, si $p, q \in P$. Del mismo modo, definimos $v(\phi)$ como el número de proposiciones en P que observamos al leer ϕ de izquierda a derecha. Por ejemplo, $v(p) = 1$ y $v((p \vee p)) = 2$, si $p \in P$.

   a) Demuestre que para toda fórmula ϕ en $\mathcal{L}(P)$ que no utiliza el conectivo $\neg$ se cumple que:

   $$l(\phi) \ \leq \ 3 \cdot v(\phi)^2.$$

   b) Lo anterior dice que el largo de una fórmula sin negación está acotado polinomialmente por el número de ocurrencias de proposiciones en ella. Demuestre que esto no se sigue cumpliendo si ahora permitimos utilizar la negación $\neg$.

c) Encuentre una restricción sintáctica del lenguaje $\mathcal{L}(P)$ que sea funcionalmente completa (es decir, para cada fórmula ϕ en $\mathcal{L}(P)$ existe una fórmula ϕ' en el lenguaje restringido tal que $\phi \equiv \phi'$), y para la cual se cumpla la propiedad de que el largo de una fórmula está acotado polinomialmente por el número de ocurrencias de proposiciones en ella. Es decir, existe $k \geq 1$ tal que para toda fórmula ϕ en el lenguaje restringido se cumple que $l(\phi)$ es $O(v(\phi)^k)$.

Solución:

a) Por inducción en el número n de conectivos usados en las fórmulas del lenguaje sin negación $\neg$. Si $n = 0$ entonces $\phi = p$, para $p \in P$. Claramente $l(p) = 1 \leq 3v(p)^2$. Considere ahora una fórmula ϕ con $n+1$ conectivos. Por tanto, $\phi = (\alpha \star \beta)$, donde $\star \in \{\vee, \wedge, \rightarrow\}$. Entonces $l(\phi) = 3 + l(\alpha) + l(\beta)$. Pero lo anterior por hipótesis inductiva es menor o igual a $3 + 3 \cdot v(\alpha)^2 + 3 \cdot v(\beta)^2$. Por tanto, $l(\phi) \leq 3(v(\alpha)^2 + v(\beta)^2 + 1) \leq 3(v(\alpha) + v(\beta))^2$. Lo último es cierto ya que $v(\alpha), v(\beta) \geq 1$. Concluimos que $l(\phi) \leq 3 \cdot v(\phi)^2$, pues $v(\phi) = v(\alpha) + v(\beta)$.

b) Las fórmulas $(\neg(\neg(\dots(\neg p)\dots))$ pueden ser arbitrariamente largas, pero tienen solo una ocurrencia de variable proposicional.

c) Podemos prohibir las fórmulas de la forma $(\neg(\neg\phi))$. Sabemos que esto no cambia el poder expresivo, ya que $(\neg(\neg\phi)) \equiv \phi$. Demostraremos por inducción en el número n de conectivos usados en las fórmulas del lenguaje restringido que para toda fórmula ϕ se cumple que $l(\phi) \leq 4 \cdot v(\phi)^2$. El caso base es tal como en item (a). Consideremos ahora el caso inductivo. Hay dos posibilidades para ϕ, que sea de la forma $(\neg\alpha)$, o que sea de la forma $(\alpha \star \beta)$. Consideremos el primer caso. Por definición, entonces, α debe ser de la forma p o $(\theta \star \psi)$. En el primer caso tenemos que $l(\phi) = 4 \leq 4 \cdot v(\phi)^2$. En el segundo caso tenemos $l(\phi) = 6 + l(\theta) + l(\psi)$. Pero lo anterior por hipótesis inductiva es menor o igual a $6 + 4 \cdot v(\theta)^2 + 4 \cdot v(\psi)^2$. Por tanto, $l(\phi) \leq 4(v(\alpha)^2 + v(\beta)^2 + 3/2) \leq 4(v(\alpha) + v(\beta))^2$. Lo último es cierto ya que $v(\alpha), v(\beta) \geq 1$. Concluimos que $l(\phi) \leq 4 \cdot v(\phi)^2$, pues $v(\phi) = v(\theta) + v(\psi)$. Para el caso en que ϕ es de la forma $(\alpha \star \beta)$ la demostración es similar.

3. Una fórmula de la lógica proposicional $\mathcal{L}(P)$ está en *3CNF* si es de la forma:

$$\bigwedge_{1 \leq i \leq n} (l_i^1 \vee l_i^2 \vee l_i^3), \tag{1}$$

donde para cada $1 \leq i \leq n$ y $1 \leq j \leq 3$ se tiene que existe $p \in P$ tal que $l_i^j = p$ ó $l_i^j = \neg p$. Por ejemplo, $(p \vee q \vee \neg r) \wedge (\neg p \vee s \vee r)$ es una fórmula en 3CNF, pero $p \vee (r \wedge q)$ no lo es.

Sea R una relación binaria sobre A. Un *cubrimiento* de R es un $S \subseteq A$ tal que para cada par $(a, b) \in R$ se tiene que $a \in S$ o $b \in S$.

Dada una fórmula ϕ en 3CNF como en la Ecuación (1), se le pide construir un conjunto A y una relación binaria R sobre A tal que:

$$\phi \text{ es satisfacible} \quad \Longleftrightarrow \quad R \text{ tiene un cubrimiento de tamaño } 2n.$$

El costo de todos los pasos efectuados en su construcción debe ser a lo más $O(n^k)$, para un $k \geq 1$ fijo (es decir, que no depende de ϕ).

Hint: El conjunto A consiste de los elementos $\{v_{i,j} \mid 1 \leq i \leq n,\ 1 \leq j \leq 3\}$ que representan los diferentes literales que ocurren en ϕ. La relación R se define sobre A de tal forma que el complemento de cualquiera de sus cubrimientos de tamaño $2n$ codifica una valuación $\sigma : P \to \{0, 1\}$ que satisface ϕ, y correspondientemente, toda valuación $\sigma : P \to \{0, 1\}$ que satisface ϕ naturalmente define el complemento de un cubrimiento de A de tamaño $2n$.

Solución: El conjunto A consiste de los elementos $\{v_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq 3\}$. La relación R contiene todos los pares de la forma $(v_{i,j}, v_{i,j'})$ tal que $1 \leq i \leq n$ y $j \neq j'$, además de los pares $(v_{i,j}, v_{k,p})$ tal que $1 \leq i, k \leq n$, $i \neq k$, y $l_i^j \equiv \neg l_k^p$.

Asuma entonces que ϕ es satisfacible. Por tanto, existe valuación $\sigma : P \to \{0, 1\}$ tal que $\sigma(\phi) = 1$. Es decir, para cada $1 \leq i \leq n$ existe $j_i \in \{1, 2, 3\}$ tal que $\sigma(j_i) = 1$. Tome entonces el conjunto de todos los elementos en $A' := A \setminus \bigcup_{1 \leq i \leq n} \{v_{i,j_i}\}$. El conjunto A' tiene tamaño $2n$. Podemos demostrar, además, que es un cubrimiento de R. De hecho, todo par de la forma $(v_{i,j}, v_{i,j'})$ está claramente cubierto por los dos elementos de la forma $v_{i,l}$ y $v_{i,l'}$ que están en A'. Considere ahora un arco de la forma $(v_{i,j}, v_{k,p})$ en R, tal que $1 \leq i, k \leq n$, $i \neq k$, y $l_i^j \equiv \neg l_k^p$. Luego, $j \neq j_i$ o $p \neq j_k$. De otra forma $\sigma(l_i^j) = \sigma(l_k^p) = 1$, lo que es imposible puesto que l_i^j es equivalente a la negación de l_k^p. Por tanto, $v_{i,j}$ o $v_{k,p}$ está en A'.

Asuma en la otra dirección que existe cubrimiento A' de tamaño $2n$. El cubrimiento debe contener a lo menos dos elementos de la forma $v_{i,j}$ para cada $1 \leq i \leq n$. Por tanto, dado que A' tiene $2n$ elementos por cada $1 \leq i \leq n$ existe un subconjunto A_i de $\{v_{i,1}, v_{i,2}, v_{i,3}\}$ que contiene exactamente dos elementos tal que $A_i \subseteq A'$. Defina $\sigma(l_i^j) = 1$ ssi $v_{i,j} \notin A'$. Claramente esta asignación satisface la fórmula ϕ. Sin embargo, falta demostrar que está bien definida; es decir, que no hay una proposición en P tal que $\sigma(p) = 1$ y $\sigma(p) = 0$. Para que esto ocurriera necesitaríamos que exista $v_{i,j}, v_{k,p} \notin A'$ tal que $l_i^j = q$ y $l_k^p = \neg q$, para algún $q \in P$. Sin embargo, en tal caso por definición tendríamos que el par $(v_{i,j}, v_{k,p}) \in R$, y este arco no está cubierto por A', lo que es una contradicción.

Claramente, la construcción puede realizarse en tiempo polinomial.