Ma50b Complejidad Computacional **1 de Julio de 2010**

Control 3

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: R. Briceño*

TIEMPO: 5.0 HRS.

PROBLEMA 1:

(i).- Se define el lenguaje DAPATH (por *directed acyclic path*) como la colección de $\langle G,s,t\rangle$ tales que $G=(V,E)$ es un grafo acíclico, $s,t\in V$ y existes un s-t camino en G.

(i.1).- (1.5 pts) Pruebe que DAPATH es NL-duro.

Indicación: Use un argumento similar al utilizado para demostrar que PATH es NL-completo.

(i.2).- (1.5 pts) Pruebe que DAPATH está en NL.

(ii).- (3.0 pts) Se define el lenguaje LP (por *programación lineal*) como la colección de $\langle A,b,c,k\rangle$ donde $A\in\mathbb{Z}^{m\times n}$, $b\in\mathbb{Z}^m$, $c\in\mathbb{Z}^n$ y $k\in\mathbb{Z}$ son tales que existe un $x\in\mathbb{Q}^n$ que satisface $Ax\leq b$ y $c^Tx\geq k$. Pruebe que LP es P-duro.

PROBLEMA 2:

(i).- (3.0 pts) A $C(\cdot,\cdot)$ circuito Booleano en $\ell+m$ entradas le asociamos la familia de conjuntos $\mathcal{S}_C=\{S_\alpha:\alpha\in\{0,1\}^\ell\}$ donde $S_\alpha=\{x\in\{0,1\}^m:C(\alpha,x)=1\}$. Definimos la dimensión de Vapnik-Chervonenkis de $\mathcal{S}_C$, denotada $\mathrm{VC}(\mathcal{S}_C)$, como el cardinal más grande del conjunto $X\subseteq\{0,1\}^m$ tal que para cualquier $X'\subseteq X$ hay algún $\alpha\in\{0,1\}^\ell$ para el cual $S_\alpha\cap X=X'$.

Se define el lenguaje VC$-$DIM como la colección de $\langle C(\cdot,\cdot),k\rangle$ donde $C(\cdot,\cdot)$ es un circuito Booleano tal que $\mathrm{VC}(\mathcal{S}_C)\geq k$. Pruebe que VC$-$DIM está en Σ_3^{P}.[1]

Indicación: Encuentre primero una buena cota en $\mathrm{VC}(\mathcal{S}_C)$ en función de $|\mathcal{S}_C|$.

(ii).- (3.0 pts) Sea $\varphi=\varphi(x_1,\ldots,x_n)$ una fórmula Booleana en forma conjuntiva normal. Pruebe que si φ tiene menos de n^t claúsulas cada una con al menos $t\log_2 n$ literales distintos, entonces φ se puede satisfacer.

Indicación: Use el método probabilista.

PROBLEMA 3: Decimos que existe un generador de bits pseudo-aleatorio a tiempo polinomial criptográficamente seguro si:

- Existe una máquina de Turing que en la entrada $\langle p(\cdot),\rho\rangle$, $p(\cdot)$ polinomio y $\rho\in\{0,1\}^n$, calcúla en tiempo polinomial $G_{n,p(\cdot)}(\rho)$ donde $G_{n,p(\cdot)}:\{0,1\}^n\to\{0,1\}^{p(n)}$.

[1] La dimensión de Vapnik-Chervonenkis de una familia de conjuntos es un concepto importante en *Machine Learning Theory*. El lenguaje VC$-$DIM es en efecto Σ_3^{P}-completo, siendo un poco frecuente ejemplo de un lenguaje natural completo para tal nivel de la jerarquía polinomial.

- Existe $S(n) > n^{\omega(1)}$ tal que para cualquier circuito Booleano C en $p(n)$ entradas y de tamaño a lo más $S(n)$ se tiene que para todo $n \in \mathbb{N}$,

$$\left| \mathbb{P}_{x \in_R \{0,1\}^n} \left(C(G_{n,p(\cdot)}(x)) = 1 \right) - \mathbb{P}_{y \in_R \{0,1\}^{p(n)}} \left(C(y) = 1 \right) \right| \leq \frac{1}{S(n)} .$$

(i).- (3.0 pts) Pruebe que si existe un generador de bits pseudo-aleatorio a tiempo polinomial criptográficamente seguro, entonces BPP $\subseteq \bigcap_{\varepsilon > 0}$ DTIEMPO(2^{n^ε}).

(ii).- (3.0 pts) Pruebe que si existe un generador de bits pseudo-aleatorio a tiempo polinomial criptográficamente seguro, entonces P $\neq$ NP.