Ma50b Complejidad Computacional **14 de Julio de 2012**

Examen

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: D. Salas, P. Muñoz*

TIEMPO: 3.5 HRS.

PROBLEMA 1:

(i).- (1.5 pts) Un puerta lógica del tipo NOR es una puerta lógica con dos entradas que implementa la negación del OR (es decir, que evalua a 1 si y sólo si sus dos entradas evaluan a 0). Sea NorCVAL el lenguaje conformado por las instancias $\langle C, \omega \rangle$ donde C es un circuito Booleano en n entradas cuyas puertas lógicas son solamente del tipo NOR, $\omega \in \{0,1\}^n$, y $C(\omega) = 1$. Pruebe que NorCVAL es P-completo.

(ii).- (2.5 pts) En ocasiones, se requiere decidir si cierto material que viene en "planchas" rectangulares (madera, tela, etc.) puede ser recortado, por un máquina con ciertas restricciones en los cortes que puede realizar, de manera de obtener pedazos rectangulares dados más pequeños. La dificultad de resolver el problema de factibilidad asociado está capturada por el problema de decisión asociado al lenguaje RectTiling conformado por las instancias $\langle (A,B); (a_1,b_1), \ldots, (a_k,b_k) \rangle$ donde $a_1, \ldots, a_k, b_1, \ldots, b_k, A, B$ son enteros no-negativos tales que en un rectángulo principal de lados A y B se pueden dibujar k rectángulos internos de lados a_i por b_i, $i \in \{1, \ldots, k\}$, de forma que sus lados sean paralelos a los lados del rectángulo principal y de forma que dos cualesquiera de los k rectángulos internos, o no se intersectan, o se intersectan sólo en sus fronteras. Pruebe que RectTiling es NP-completo.

(iii).- (2.0 pts) Se define Sudoku como el conjunto de instancias $\langle A \rangle$ donde $A = (A_{i,j})_{i,j}$ es una matríz de $n^2 \times n^2$ donde cada $A_{i,j}$ es $\square$ o un número en $[n^2] = \{1, \ldots, n^2\}$. La instancia $\langle A \rangle$ está en Sudoku si los $A_{i,j}$ iguales a $\square$ pueden ser reemplazados por números en $[n^2]$ de forma que cada valor $1, \ldots, n^2$ aparezca exactamente una vez en: (1) cada fila, (2) cada columna, y (3) cada bloque $B_{s,t}$ de $n \times n$, donde $A = (B_{s,t})_{s,t=1,\ldots,n}$. Pruebe que Sudoku $\leq_{\mathrm{P}}$ SAT.

PROBLEMA 2:

(i).- Sea $\mathbb{F}$ cuerpo finito de característica (prima) p. Se define la permanente de $A = (a_{i,j})_{i,j} \in \mathbb{F}^{n \times n}$ por

$$\mathrm{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)} .$$

Es fácil ver que si se pueden realizar eficientemente las operaciones aritméticas sobre $\mathbb{F}$, entonces $\mathrm{Perm}(A)$ puede calcularse en espacio polinomial y hay fuerte evidencia de que no se puede calcular en tiempo polinomial. El proposito del siguiente problema es mostrar un sistema interactivo (explícito) de demostración para verificar que $\mathrm{Perm}(A)$ es igual a un $k \in \mathbb{F}$ dado.

(i.1).- (1.0 pts) Pruebe que $\mathrm{Perm}(A) = \sum_{i=1}^{n} a_{1,i} \mathrm{Perm}(A_{1,i})$ donde $A_{1,i} \in \mathbb{F}^{(n-1)\times(n-1)}$ es la submatríz de A que se obtiene al remover la fila 1 y la columna i de la matríz A.

(i.2).- (1.0 pts) Asumiendo que $p > n$, pruebe que existe una matríz $D_A(x)$ de tamaño $(n-1) \times (n-1)$ cuyos coeficientes son polinomios en $\mathbb{F}[x]$ de grado a lo más n y tal que $D_A(\mathbf{i}) = A_{1,i}$ para

todo $i \in \{1,\ldots,n\}$ (donde, para $i \in \mathbb{N}$, denotamos por $\mathbf{i}$ al elemento de $\mathbb{F}$ correspondiente a $\mathbf{1}$, la unidad de $\mathbb{F}$, sumado consigo mismo i veces). Concluya que $\mathrm{Perm}\,(D_A(x))$ es un polinomio en $\mathbb{F}[x]$ de grado a lo más $n(n-1) < n^2$.

(i.3).- (2.0 pts) Sea L_{perm} la colección de instancias $\langle A, p, q, k\rangle$ donde A es una matríz de $n \times n$ a coeficientes en $\mathbb{F}_q$ (cuerpo de cardinalidad q y característica prima p) y $k \in \mathbb{F}_q$ son tales que $\mathrm{Perm}\,(A) = k$ en $\mathbb{F}_q$. Determine el menor valor de p que pueda (en función de n) para que el siguiente protocolo coloque a L_{perm} en IP (inicialmente $k_1 = k$ y $A_1 = A$). Justifique e indique cuáles son los polinomios Q_m, $m = 1,\ldots,n-1$, que el probador honesto envía.

Repetir para $m = 1,\ldots,n-1$

$P \to V : Q_m \in \mathbb{F}_q[x]$ polinomio de grado $(n-m+1)^2$.

V : Rechazar si $\displaystyle\sum_{i=1}^{n-m+1} (A_m)_{1,i} Q_m(\mathbf{i}) \neq k_m$. En caso contrario, elegir $b_m \in_R \{1,\ldots,p\}$

y definir $k_{m+1} = Q_m(\mathbf{b_m})$ y $A_{m+1} = D_{A_m}(\mathbf{b_m}) \in \mathbb{F}_q^{(n-m)\times(n-m)}$.

$V \to P : \mathbf{b_m}$.

Aceptar si $k_n = \mathrm{Perm}\,(A_n)$.

(ii).- (2.0 pts) Se define P/poli como la clase de lenguajes $L \subseteq \{0,1\}^*$ para los que existe una familia de circuitos Booleanos $(C_n)_{n\in\mathbb{N}}$ y un polinomio $p(\cdot)$ tales que $|C_n| \leq p(n)$, C_n tiene n entradas, y para todo $\omega \in \{0,1\}^*$ se tiene que:

$$\omega \in L \iff C_n(\omega) = 1\,, \text{ donde } n = |\omega|\,.$$

Pruebe que BPP $\subseteq$ P/poli.

Indicación: Utilice el método probabilista para probar que si $L \in$ BPP, entonces existe una máquina de Turing probabilista M y un polinomio $p(\cdot)$ para los cuales hay un $\rho_o \in \{0,1\}^{p(n)}$ tal que para todo $\omega \in \{0,1\}^n$ se tiene que $M(\omega,\rho_0) = 1$ si y sólo si $\omega \in L$.