MA4701. Optimización Combinatorial. 2013.
Profesor: José Soto
Escriba(s): José Coronado, Juan Granier y Pedro Vergara I.
Fecha: 25 de Noviembre de 2013.

Cátedra 24

Teorema 1. *Teorema de Khachiyan*

Considere el problema

$$\begin{array}{lll} (P) & \text{máx} & \{c^T x : Ax \leq b\} \\ & s.a & A \in \mathbb{Z}^{mxd} \\ & & b \in \mathbb{Z}^m \\ & & c \in \mathbb{Z}^d \end{array}$$

El problema (P) se puede resolver usando un número polinomial en m, d y log(U) de llamadas a un oráculo de separación para $\{Ax \leq b\}$ (toma O(md) revisar fila por fila), donde U es el máximo valor absoluto de un coeficiente de A,b y c; es decir, $U = \text{máx}\{||A||_\infty, ||b||_\infty, ||c||_\infty\}$

Demostración. Esquema (es muy larga desarrollarla completamente)

- Basta poder revisar factibilidad x^* es óptimo de P. que es equivalente a revisar la factibilidad en el nuevo poliedro $\{\binom{x}{y} : Ax \leq b, A^T y = c, y \geq 0, c^T x = b^T y\}$ que sea no vacío.

  Luego podemos dedicarnos a probar factibilidad de un poliedro $Q = \{x : Ax \leq b\}$, con A y b distintos a los anteriores. Ya que si somos capaces de crear un algortimo polinomial para este problema, lo tenemos para el anterior.

- Podemos suponer que si el poliedro Q no es vacío, entonces tiene vértices. Para esto, basta diagonalizar A de la forma, $A \to [A' : 0]$, donde A' tiene sus columnas l.i. Se puede probar que el sistema diagonalizado $A'x \leq b'$ tiene vértices.

  Veamos ahora un lema que nos permitirá probar que los vértices de Q son racionales de descripción pequeña.

  Lema 1. *Si C es invertible (buscamos $x = p$), C y p tienen coordenadas enteras. Entonces el vector $x = C^{-1}p$ tiene todas sus coordenadas racionales y su numerador y denominador tienen valor absoluto $\leq (dU)^d$,*
  $U = \text{máx}\{||C||_\infty, ||p||_\infty\}$

  Demostración. La fórmula de Cramer dice que:

  $$|(C^{-1}p)_j| = \frac{|det(C; p; j)|}{|det(C)|},$$

  donde $(C; p; j)$ es la matriz obtenida al reemplazar la j-ésima columna de C por p.
  $det(X) = \sum_{\sigma \in S^d} (sgn(\sigma) \prod_{i=1}^{d} X_{i,\sigma(i)}) \Rightarrow |det(X)| \leq d!(||X||_\infty)^d \leq d^d U^d$.
  El lema se concluye notando que para $X \in \{C, (C; p; j)\}$. □

  Gracias al lema anterior, podemos reemplazar Q por $Q \cap B_\infty(0, d^d U^d) \subseteq B_2(0, d^d U^d \sqrt{d})$. En efecto, como Q es un poliedro con vértices, $Q \neq \emptyset \Leftrightarrow Q \cap B_\infty(0, d^d U^d) \neq \emptyset$.

- Finalmente, para trabajar en un poliedro con volumen, cambiamos $Q = \{x\colon Ax \leq b\}$ por $Q_{\text{expandido}} = Ax \leq b + \epsilon \mathbb{1}$ donde $\epsilon = \frac{1}{2(dU)^d d}$

Lema 2. $Q = \{x\colon Ax \leq b\} = \emptyset \Leftrightarrow Q_{expandido} = \{x\colon Ax \leq b + \epsilon\mathbb{1}\} = \emptyset$

Demostración. $\Leftarrow$) directo
$\Rightarrow$) por Lema de Farkas, $\exists y$ t.q. $A^T y = 0, b^T y = -1$. Usando el Lema 1 podemos además suponer que $|y|$ tiene todas sus coordenadas $\leq (dU)^d$.

¿Qué pasa si $x^* \in \{Ax \leq b + \epsilon\mathbb{1}\}$?

En este caso, $0 = y^T(Ax^*) \leq y^T(b + \epsilon\mathbb{1}) = -1 + (y^T\mathbb{1})\epsilon \leq -1 + d(dU)^d\epsilon \leq -\frac{1}{2}$, lo cual es una contradicción.

□

Del Lema 2 , tenemos que si Q es no vacío, entonces contiene un punto x^*. Esto implica que el poliedro expandido contiene $\prod_{i=1}^{d}[x_i^*, x_i^* + \delta]$, para un δ positivo suficientemente pequeño.

En efecto, si $x' \in \prod_{i=1}^{d}[x_i^*, x_i^* + \delta], entonces Ax' = Ax^* + A(x' - x^*) \leq b + \underbrace{dU\delta}_{\leq \epsilon}$.

Tomando $\delta \leq \frac{\epsilon}{dU} = \frac{1}{2(dU)^{d+1}d}$ tenemos que $\prod_{i=1}^{d}[x_i^*, x_i^* + \delta] \in Q_{\text{expandido}}$.

De aquí se concluye que $Vol(Q_{\text{expandido}}) \geq \delta^d = \frac{1}{(2(dU)^{d+1}d)^d} \geq (2dU)^{-d^3}$. Por otro lado, del Lema 1, sabemos que $Vol\binom{Elipsoide}{inicial} \leq (2dU)^{d^3}$. En conclusión, podemos usar Método Elipsoide en $Q_{\text{expandido}}$.
Esto toma $O(d\, log\frac{vol.\, inicial}{vol.\, final}) = O(dd^6 log(2dU)) = O(d^7 log(2dU))$ llamadas al oráculo para $Q_{\text{expandido}}$.

De lo anterior, se concluye que existe un algortimo polinomial para resolver (P), aunque es muy lento.

□

Gracias a los teoremas vistos en esta clase y la clase pasada, tenemos que PL se puede resolver en tiempo polinomial en la medida que tengamos acceso a un oráculo de separación para el poliedro. En particular, el siguiente corolario es interesante.

Corolario 1. *Podemos encontrar un matching de peso máximo en un grafo no bipartito en tiempo polinomial, resolviendo un PL.*

Complejidad de Problemas (P vs NP)

Sea Σ un alfabeto finito (por ejemplo, $\{0, 1\}$), y sea Σ^* el conjunto de todas las palabras en Σ. Dado $x \in \Sigma^*$, $|x|$ representa su largo. Un lenguaje L es un subconjunto Ł $\subseteq \Sigma^*$.

Todo problema de decisión (ej: ¿Posee G un árbol generador?) se puede expresar como una pregunta, ¿$x \in$ Ł?
Ejemplo, $L_{Conexo} = \{\langle G\rangle : G \text{ es conexo}\}$, donde $\langle G\rangle$ corresponde a una codificación de G en Σ.

Un algoritmo A es una función (que demora cierto tiempo en evualuarse) que devuelve SI o NO.

Decimos que:

- A termina si $\forall x \in \Sigma^*$, $A(x)$ se completa en tiempo finito.
- A decide un lenguaje L si
  - $A(x) = SI, \forall x \in L$.
  - $A(x) =$ NO, $\forall x \notin L$.

- A es polinomial si existe un polinomio p tal que $A(x)$ termina después de $\leq p(|x|)$ operaciones básicas, $\forall x \in \Sigma^*$.

Una clase es un conjunto de lenguajes (problemas).

Definimos 2 clases especiales:

- $\mathcal{P}$ es la clase de los lenguajes L que son decidibles en tiempo polinomial.
  ↑
  Polinomial time decidable Por ejemplo: Ł$_{Conexo} \in P$.

- $\mathcal{NP}$ es una clase más compleja.
  ↑
  Non deterministic polynomial time decidable

La definición de $\mathcal{NP}$ es la siguiente.
$L \in \mathcal{NP} \Leftrightarrow$ existe un algoritmo polinomial V que llamamos verificador tal que

- $\forall x \in L, \exists y \in \Sigma^*$, con $|y|$ polinomial en $|x|$, tal que $V(x, y) = SI$
- Si $x \notin L \Rightarrow \forall y \in \Sigma^*$, con $|y|$ polinomial en $|x|$, tal que $V(x, y) = NO$

Para todo $x \in L$, la palabra y se conoce como certificado corto de pertenencia.

Ejemplo (Camino Hamiltoniano):

Ham-Path = $\{\langle G\rangle : \exists P \subseteq V(G)$ camino que pasa por todos los vertices de V(G) exactamente una vez$\}$
No se sabe si Ham-Path está en $\mathcal{P}$, pero se sospecha fuertemente de que esto no es asi.

- ¿Ham-Path $\in \mathcal{P}$?
- Ham-Path $\in \mathcal{NP}$

En efecto, si G tiene camino Hamiltoniano $\mathcal{P} \Rightarrow \langle \mathcal{P}\rangle$ es un certificado para verificar que $\langle G\rangle \in$ Ham-Path pues podemos decidir en tiempo polinomial si P es un camino Hamiltoniano de G.

Intuitivamente, P corresponde a los problemas fáciles y $\mathcal{NP}$ corresponde a problemas que se pueden verificar de manera fácil.

Una pregunta abierta desde los 70 es si la clase $\mathcal{P} = \mathcal{NP}$. Lo que si se sabe es que $\mathcal{P} \subseteq \mathcal{NP}$.
$\mathcal{P} = \mathcal{NP}$ tiene consecuencias increíbles.

Dentro de las consecuencias negativas, en cuanto al hacking, encontrar claves de acceso de un correo electrónico y de cuentas bancarias. Dentro de las consecuencias positivas, usos en la biología, agilizando los algortimos de búsqueda para encontrar curas al sida, cáncer u otras enfermedades terminales, la cual su cura no ha sido encontrada.