Lecture 20

CSE 522: Advanced Algorithms

December 10, 2004
Lecturer: Kamal Jain
Notes: Ning Chen

Theorem 1 *(Jain'04) Given a convex set S, via a strong separation oracle with a guarantee that the set contains a point with binary encoding length ϕ, a point in S can be found in polynomial time of (n, ϕ), where n is the dimension.*

Theorem 2 *(Simultaneous diophantine approximation problem) Given α_1, $\alpha_2, \ldots, \alpha_n \in \mathbb{Q}$, and $0 < \epsilon < 1$, we can find integers $p_1, p_2, \ldots, p_n$ and q in polynomial time of $(n, \log \frac{1}{\epsilon})$ such that*

$$|p_i - q\alpha_i| \leq \epsilon, \text{ for } \forall i, \text{ and } \ 0 < q \leq \epsilon^{-n} \cdot 2^{\frac{n(n+1)}{4}} \triangleq Q.$$

Proof. Consider lattice

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} & \\ 0 & 0 & \cdots & 1 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n & \frac{\epsilon}{Q} \end{pmatrix}$$

where there are $n+1$ rows and $n+1$ columns. Due to the last lecture, we can find a vector v such that

$$||v||_2 \leq 2^{\frac{(n+1)-1}{4}} \cdot \sqrt[n+1]{det(L)},$$

which implies that

$$||v||_2 \leq 2^{\frac{n}{4}} \left(\frac{\epsilon}{\epsilon^{-n} \cdot 2^{\frac{n(n+1)}{4}}} \right)^{\frac{1}{n+1}} = \epsilon.$$

Thus, $||v||_\infty \leq ||v||_2 \leq \epsilon$. Let $v = \sum_{i=1}^{n} p_i v_i + q v_{i+1}$, where v_i is the i-th row vector of the lattice, p_i and q are integers, for each i.

Consider the last coordinate of v, we have $\frac{q\epsilon}{Q} \leq ||v||_\infty \leq \epsilon$, which implies that $q \leq Q$. Similarly consider other coordinates, we have $|p_i - q\alpha_i| \leq \epsilon$. $\square$

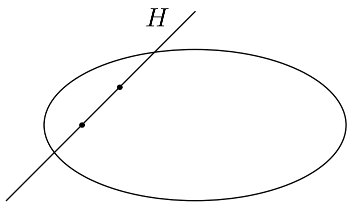
Remark. Dirichlet's Theorem says that $0 < q \leq \epsilon^{-n}$. But it's not constructive.

Proof of Theorem 1. Consider $B = [-2^\phi, 2^\phi]^n$, which contains points of encoding length at most ϕ. Let $C = S \cap B$. Note that $C \neq \emptyset$. We start by ellipsoid algorithm with initial value $(2\sqrt{n}2^\phi)^n \leq (2n2^\phi)^n$. If we find a point in C, we are done. Otherwise, run ellipsoid algorithm until we have value smaller or equal to $\frac{1}{2^{2n\phi}n^n}$. Note that we need time

$$n^2 \cdot \log \left(2^{2n\phi} n^n \cdot (2n2^\phi)^n\right) = \phi \cdot poly(n)$$

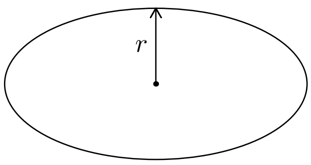
to do this.

Note that all points with encoding length at most ϕ lie on a hyperplane of dimension $n-1$.

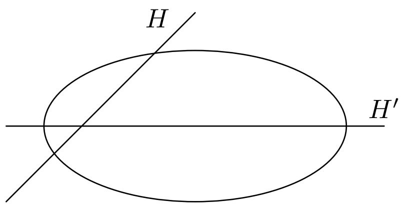


Computer recursively to find such a point. Let $C_n = S \cap B$, $C_{n-1} = C_n \cap H$. Shrink the ellipsoid until the value is smaller than v, whose value will be determined later.

Let smallest radius of ellipse be r.



Thus half of the smallest (small enough that H' is a good approximation of H) axis is smaller or equal to $nv^{1/n}$.



Claim. The coefficients of H are polynomially small.

Proof. Let $H' : \vec{w} \cdot \vec{x} = \vec{w} \cdot \vec{v}$. For any $\vec{x} \in E$, $|\vec{w} \cdot \vec{x} - \vec{w} \cdot \vec{v}| < r \leq n \cdot v^{1/n}$. Assume $w_1, \dots, w_n$ are coefficients. Then due to Theorem 2, we can compute $p_1, \dots, p_n, \pi, q \leq 2^{n^2} \epsilon^{-n}$, such that

$$|w_i q - p_i| < \epsilon, \text{ and } |\vec{w}\vec{v}q - \pi| < \epsilon.$$

Claim. There is ϵ, v such that $H \equiv \vec{b} \cdot x = \pi$.

Proof. Consider $z \in E$, $z \in \mathbb{Q}$, and z has denominator smaller or equal to 2^{ϕ}. Also, $z \in H$.

$$\begin{aligned}
|\vec{p} \cdot \vec{z} - \pi| &= |p_1 z_1 + \cdots + p_n z_n - \pi| \\
&\leq |(w_1 q + \epsilon_1) z_1 + \cdots + (w_n q + \epsilon_n) z_n - (\vec{w}\vec{v}q - \epsilon_{n+1})| \\
&\leq q(\vec{w}\vec{z} - \vec{w}\vec{v}) + \epsilon ||z_1|| + \epsilon \\
&\leq 2^{n^2} \epsilon^{-n} n v^{1/n} + \epsilon n 2^{\phi} \\
&< \frac{1}{2^{n\phi}}
\end{aligned}$$

Choose ϵ such that

$$\epsilon n 2^{\phi} \leq \frac{1}{2 \cdot 2^{n\phi}},$$

which implies

$$\epsilon \leq \frac{1}{4n \cdot 2^{(n+1)\phi}}.$$

Choose v such that

$$2^{n^2} \epsilon^{-n} n v^{1/n} \leq \frac{1}{2 \cdot 2^{n\phi}}.$$

Therefore,

$$v \leq \frac{1}{2^{n^2} n^n 4 n^{n^2} 2^{n^2 \phi(n+1)}},$$

Thus,

$$\log(\frac{1}{v}) \leq \phi \cdot poly(n),$$

which completes the proof of the theorem. □

References

[1] Kamal Jain, *A Polynomial Time Algorithm for Computing the Arrow-Debreu Market Equilibrium for Linear Utilities*, FOCS 2004, 286-294.

[2] László Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, SIAM Society for Industrial and Applied Mathematics, 1986.