ILP in NP

Gorav Jindal

February 12, 2020

Abstract

The proof (from [KM78]) of the fact that ILP $\in$ NP is presented.

1 Introduction

By the Integer Linear Programming Problem we mean the question: "Given positive integers m and n, an $m \times n$ integral matrix A and an $m \times n$ integral vector b, does there exist an integral vector x satisfying $Ax \geq b$?" Let $\mathbb{Z}^n$ denote the integer-valued vectors of $\mathbb{R}^n$ and define:

$$S \overset{\text{def}}{=\!=} \{x \mid Ax \geq b \text{ and } x \in \mathbb{Z}^n\}. \tag{1}$$

Let a be the largest absolute value of any entry in A. We prove the following Theorem 1.1.

Theorem 1.1. *There exists a polynomial $q(.,.)$ such that for any positive integers m and n and any $m \times n$ integral matrix A and any $m \times 1$ integral vector b, the set $S \overset{def}{=\!=} \{x \mid Ax \geq b \text{ and } x \in \mathbb{Z}^n\}$ is nonempty if and only if there is an x in S such that $\|x\|_1 \leq 2^{q(n,m)}$.*

Lemma 1.1. *If D is an integral $k \times n$ matrix with $\operatorname{rank}(D) < n$, there is an non-zero integer vector $f = (f_1, f_2, \ldots, f_n)$ with $f \in \ker(D)$ and $\|f\|_1 \leq n(dk)^k$. Here d is the largest absolute value of any entry of D.*

Proof. Without loss of generality, assume that all the rows of D are independent. (If not, choose a basis for the row space of D and delete the other rows.) Now, renumber the columns of D, if necessary, so that the first k columns form a non-singular matrix B. Set $f_{k+1} = f_{k+2} = \cdots = f_n = -1$. For $i \in [k]$, define $\lambda_i \overset{\text{def}}{=\!=} \sum_{j=k+1}^{n} d_{ij} = \lambda_i$ and $\lambda \overset{\text{def}}{=\!=} (\lambda_1, \lambda_2, \ldots, \lambda_k)^T$. Since B is non-singular, there is a solution to $Bf' = \lambda$. Now verify that the concatenated vector $f \overset{\text{def}}{=\!=} (f', f_{k+1}, f_{k+2}, \ldots, f_n)$ is $\ker(D)$. By Cramer's rule, f' is a rational vector. Further, for each $i \in [k]$, f'_i has a numerator which is a $(k \times k)$ determinant with one column given by λ and the rest columns of B. Since $\|\lambda\|_1 \leq nd$ and each entry of B is at most d in absolute value, we get that $|\text{numerator}| \leq ((nd)d^{k-1})k!$ which is at most $n(dk)^k$. Now notice that $f \cdot \det(B)$ is the vector which satisfies all the conditions we claimed. $\square$

Now, S defined in Equation (1) is nonempty if and only if $S \cap \{x \mid I_i x_i, i \in [n]\}$ is nonempty for some choice of $\{I_i\}_{i \in [n]}$ with each I_i being chosen from the two element set $\{-1, 1\}$. Thus, it is enough to prove that in each of these 2^n sets, there exists an x if an only if there exists one satisfying $\|x\|_1 \leq 2^{q(n,m)}$ ($q(n,m)$ will be computed later). Note that the addition of the n inequalities makes the rank of the coefficient matrix equal to n. Thus, without loss of generality, we may assume that $\operatorname{rank}(A) = n$, and prove the theorem for S itself. The addition of the n constraints increases the number of rows of A by n, thus A will be assumed to be an $M \times n$ matrix where $M = m + n$. In the rest of the proof, we will assume as hypothesis that S is nonempty. See that there is an x in S such that

$$a^i \cdot x \leq b_i + a$$

holds for at least one $i \in [M]$, where a^i stands for the i^{th} row of A. (To see this, take any $x \in S$ and alter a component of x until the above inequality is satisfied.) Without loss of generality assume $i = 1$. (If not, renumber the rows of A.) Therefore, there is an integer b'_1 with $b_1 \leq b'_1 \leq b_1 + a$ for which

$$S_1 \overset{\text{def}}{=\!=} S \cap \{x \mid a^1 \cdot x = b'_1\} \neq \emptyset.$$

For induction, assume that there are positive integers $b'_1, b'_2, \ldots, b'_k$ such that $b'_i \le b_i + n^2 a(aM)^M$ for all $i \in [k]$. (It will become clear later why this bound is chosen.) Define

$$S_k \stackrel{\text{def}}{=\!=} S \cap \{x \mid a^i \cdot x = b'_i \text{ for all } i \in [k]\} \neq \emptyset.$$

Let A_k denote the first k rows of A. There are two cases to consider.

Case 1: In this case $\operatorname{rank}(A_k) < n$. By using Lemma 1.1, there is a non-zero integer vector $f = (f_1, f_2, \ldots, f_n)$ with $f \in \ker(A_k)$ and $\|f\|_1 \le n(aM)^M$. If x is a solution to $A_k x = (b'_1, b'_2, \ldots, b'_k)^T$ then $x + cf$ is also solution to this system for any $c \in \mathbb{Z}$. We use this observation to prove that the following Lemma 1.2.

Lemma 1.2. *$S_k \neq \emptyset$ implies that there is an x in S_k such that*

$$a^i \cdot x \le b_i + na\|f\|_1 \text{ for some } i \in \{k+1, k+2, \ldots, M\}. \tag{2}$$

Proof. Suppose there is an x in S_k (recall $S_k \neq \emptyset$) not satisfying Equation (2). We will show that we can add a suitable multiple of f to x to get an $(x + cf) \in S$ satisfying Equation (2). Since A is of rank n, $a^j f \neq 0$ for some $j \ge k+1$. Replacing f by $-f$, if necessary, we can assume that $a^j f < 0$. Let

$$\alpha \stackrel{\text{def}}{=\!=} \min_{\{j > i : a^j \cdot f < 0\}} \lfloor \frac{a^j \cdot x - b_j}{|a^j f|} \rfloor. \tag{3}$$

Then it is easily checked that $(x + \alpha f) \in S_k$. If i_1 is the value of i for which the minimum is achieved in Equation (3), then a simple calculation shows that $a^{i_1}(x + \alpha f) \le b_{i_1} + |a^{i_1} \cdot f|$, which is at most $b_{i_1} + na\|f\|_1$ since $|a^i f| \le na\|f\|_1$ for any i. Hence the lemma follows. $\square$

Without loss of generality, assume that the i_1 in the proof of Lemma 1.2 is $k+1$. Thus, there is a b'_{k+1} with $b_{k+1} \le b'_{k+1} \le b_{k+1} + na\|f\|_1$.

$$S_{k+1} \stackrel{\text{def}}{=\!=} S \cap S \cap \{x \mid a^i \cdot x = b'_i \text{ for all } i \in [k+1]\} \neq \emptyset.$$

Since $na\|f\|_1 \le n^2 a(aM)^M$ we have proved the inductive step. Since there are finitely many inequalities and since $\operatorname{rank}(A) = n$, we must finally end in the case where $\operatorname{rank}(A_k) = n$.

Case 2: In this case $\operatorname{rank}(A_k) = n$. There is now at most one rational x satisfying $A_k x = (b'_1, b'_2, \ldots, b'_k)^T$ and by Cramer's rule, the numerators of the x_1 in this x are of magnitude at most

$$(\|b\|_1 + n^2 a(aM)^M) a^{M-1} M! \le (\|b\|_1 + n^2 a(aM)^M)(aM)^M.$$

Thus with the polynomial $q(n, m) \stackrel{\text{def}}{=\!=} \log_2((\|b\|_1 + n^2 a(aM)^M)(aM)^M)$, Theorem 1.1 is true. Note that q is also a polynomial in $\log a$ and $\log((\|b\|_1)$. Thus, q is a polynomial function of the length of the input data.

References

[KM78] Ravindran Kannan and Clyde L. Monma. "On the Computational Complexity of Integer Programming Problems." In: *Optimization and Operations Research*. Ed. by Rudolf Henn, Bernhard Korte, and Werner Oettli. Berlin, Heidelberg: Springer Berlin Heidelberg, 1978, pp. 161–172. ISBN: 978-3-642-95322-4.