SCHOOL OF OPERATIONS RESEARCH
AND INDUSTRIAL ENGINEERING
COLLEGE OF ENGINEERING
CORNELL UNIVERSITY
ITHACA, NEW YORK 14850

TECHNICAL REPORT NO. 690

March 1986

CUTTING-PLANE PROOFS IN POLYNOMIAL SPACE

by

William Cook*

*This research was partially supported by a grant from the Alexander von Humboldt Stiftung and by the Institut fur Okon und Operations Research, University Bonn, W. Germany.

Abstract: Following Chvátal, cutting planes may be viewed as a proof system for establishing that a given system of linear inequalitites has no integral solution. We show that such proofs may be carried out in polynomial workspace.

The integer programming problem is to decide if a given system of linear inequalities has an integral solution. Recent progress on this algorithmic question has involved techniques from the geometry of numbers, in the celebrated paper of Lenstra[21] and in results of Babai[1], Grötschel, Lovász, and Schrijver[14], and Kannan[17]. One of the things that is apparent in these results is the importance of the fact that if a polyhedron contains no integral vectors then there must be some direction in which it is not very "wide". This idea has been developed more fully by Kannan and Lovász[18], who obtained a theorem which provides much more information on the appearance of such polyhedra. These "width" results have consequences for the construction and analysis of proof systems for verifying that a polyhedron contains no integral vectors. Whereas the integer programming problem is directly related to the question of the equality of P and NP, the existence of a polynomial proof system for integer programming is equivalent to NP = co-NP.

One of the fundamental concepts in the theory of integer programming is that of cutting planes, going back to the work of Dantzig, Fulkerson, and Johnson[11] and Gomory[12]. On the practical side, cutting-plane techniques are the basis of very successful algorithms for the solution of large-scale combinatorial and 0-1 programming problems in Crowder, Johnson, and Padberg[9], Crowder and Padberg[10], Grötschel, Jünger, and Reinelt[13], Padberg, van Roy, and Wolsey[23] and elsewhere. While on the theorectical side, Chvátal[3,4,5,6] has shown that the notion of cutting planes leads to many nice results and proofs in combinatorics. We will adopt Chvátal's point of view and consider cutting planes as a proof system, in our case for verifying that polyhedra contain no integral vectors.

Perhaps the best known of all proof systems is the resolution method for proving the unsatisfiability of formulas in the propositional calculus. Haken[15] settled a long-standing open problem by showing that resolution is nonpolynomial. It is easy to see that proving the unsatisfiability of a formula is a special case of proving that a polyhedron contains no integral vectors, and, using Haken's result, it can be shown that cutting planes are a strictly more powerful proof system than the resolution system (see Cook, Coullard, and Turán[7] for a treatment of this and the relationship of cutting planes and extended resolution).

To define Chvátal's[6] concept of a cutting-plane proof, consider a system of linear inequalities

$$(1) \qquad a_i x \le b_i \qquad (i = 1, \ldots, k).$$

If we have nonnegative numbers $y_1, \ldots, y_k$ such that $y_1 a_1 + \cdots + y_k a_k$ is integral, then every integral solution of (1) satisfies the inequality

$$(2) \qquad (y_1 a_1 + \cdots + y_k a_k) \le \gamma$$

for any number γ which is less than or equal to $\lfloor y_1 b_1 + \cdots + y_k b_k \rfloor$ (the number $y_1 b_1 + \cdots + y_k b_k$ rounded down to the nearest integer). We say that the inequality (2) is <u>derived</u> from (1) using the numbers $y_1, \ldots, y_k$. A <u>cutting-plane proof</u> of the fact that the linear system (1) has no integral solution is a list of inequalities $a_{k+i} x \le b_{k+i}$ $(i = 1, \ldots, M)$, together with nonnegative numbers y_{ij} $(i = 1, \ldots, M,\ j = 1, \ldots, k+i-1)$, such that for each i the inequality $a_{k+i} x \le b_{k+i}$ is derived from the inequalities $a_j x \le b_j$ $(j = 1, \ldots, k+i-1)$ using the numbers y_{ij} $(j = 1, \ldots, k+i-1)$ and where the last inequality in the sequence is $0x \le -1$. Results of Chvátal[3] and Schrijver[24] imply that a system of rational linear inequalities has no integral solution if and only if this fact has a cutting-plane proof.

The <u>length</u> of a cutting-plane proof is the number, M, of derived inequalities. Cook, Coullard, and Turán[7] have shown that results on the "width" of polyhedra imply that if a rational linear system has no integral solution then there exists a cutting-plane proof of this with length bounded above by a function depending only on the number of variables in the system. A consequence of this is that in fixed dimension, the total number of binary digits needed to write down a cutting-plane proof that a rational system $Ax \le b$ has no integral solution can be bounded above by a polynomial function of the size, in binary notation, of $Ax \le b$ (see Boyd and Pulleyblank[2] or Cook, Coullard, and Turán[7]). Unfortunately, the bound on the length of the cutting-plane proofs is necessarily exponential in the number of variables, so for varying dimension we have no guarantee that we can write down our cutting-plane proof in polynomial space. (Again, this is possible if and only if NP = co-NP.) Notice, however, that during the course of a proof it may happen that some of the derived inequalities are no longer needed and so could be removed from our workspace. Thus the amount of space we need in order to carry out a proof may be considerably less than the amount of space it would take to write down the entire list of derived inequalities. So perhaps we can still bound the amount of workspace we need by a polynomial function of the size of $Ax \leq b$.

A notion of the amount of space required by general proof systems was developed by Kozen[19,20]. To specialise his definition to cutting-planes we will view our proofs as certain acyclic directed graphs, as suggested by Chvátal[6]. Suppose that $a_{k+i}x \leq b_{k+i}$ $(i = 1,\ldots,M)$, together with nonnegative y_{ij} $(i = 1,\ldots,M,$ $j = 1,\ldots,k+i-1)$, is a cutting-plane proof of the fact that $a_i x \leq b_i$ $(i = 1,\ldots,k)$ has no integral solution. An associated directed graph has nodes $1,2,\ldots,k+M$ and a directed edge from node i to node j if and only if the inequality $a_i x \leq b_i$ is used in the derivation of $a_j x \leq b_j$. (By "used" we mean that a positive multiple of the inequality $a_i x \leq b_i$ is taken in the derivation of $a_j x \leq b_j$.) So to derive inequality $a_j x \leq b_j$, we only need to know the inequalities corresponding to the immediate predecessors of node j in our directed graph. Thus, once we have reached node j, the only previously derived inequalities we need to remember are those for which there is a directed edge going from it to a node greater than j. So the greatest number of inequalities which must be stored during the proof is the maximum number, over all nodes k+i $(i = 1,\ldots,M)$, of directed edges going from nodes $\{1,\ldots,k+i\}$ to nodes $\{k+i+1,\ldots,k+M\}$. As our bound on the space requirement of the proof we take this number multiplied by the maximum size of an inequality used in the proof. (We have not considered the numbers y_{ij} in calculating our bound, since, using linear programming results, these can always be chosen to be of size polynomial in the size of the inequalities used in the derivation and the size of the inequality to be derived - see, for example, Schrijver[25].) With this definition, we will show that there exist cutting-plane proofs with length depending only on the dimension and which can be carried out in polynomial workspace, that is, in an amount of workspace bounded above by a polynomial function of the size of $Ax \leq b$. We refer the reader to the book of Schrijver[25] for results in the theory of polyhedra and integer programming which are used in the proof.

<u>Theorem</u>: Let A be a rational $m \times n$ matrix and b a rational $m \times 1$ vector such that $Ax \leq b$ has no integral solution. Then there exists a cutting-plane proof of $0x \leq -1$ from $Ax \leq b$ with length at most $n^{3n} + 1$ which can be carried out in polynomial workspace.

Proof: As we may scale the inequalities if necessary, we may assume that A and b are integral. We may also assume that n is at least 2, since the result is trivial otherwise. The theorem will be proven by showing that the following result holds for each $k \in \{0,1,\ldots,n\}$:

(3) Let C be a $k \times n$ integral matrix of rank k, let d be a $k \times 1$ integral vector and let $\sigma(A,b,C,d)$ denote the greatest absolute value amongst the entries of A,b,C,d. Then there exists an inequality $c_k x \leq d_k$ with $\{x\colon c_k x \leq d_k\} \cap \{x\colon Ax \leq b,\ Cx = d\} = \phi$ and a cutting-plane proof of $c_k x \leq d_k$ from $(Ax \leq b,\ Cx \leq d)$ of length at most $n^{3(n-k)}-1$ (or 1 if k=n) needing only n-k+1 inequalities, besides $(Ax \leq b,\ Cx \leq d)$, to be stored at any one time and where each inequality in the proof has all coefficients of absolute value at most $n^{3(n-k)+1}\sigma(A,b,C,d)$.

The theorem follows from the case $k=0$, since $\{x\colon c_0 x \leq d_0\} \cap \{x\colon Ax \leq b\} = \phi$ implies, by Farkas' lemma, that $0x \leq -1$ may be derived from $(Ax \leq b,\ c_0 x \leq d_0)$.

To begin with, suppose C is of rank n. If $\{x\colon Ax \leq b,\ Cx = d\} = \phi$, then there is nothing to prove. So we may assume that $\{x\colon Ax \leq b,\ Cx = d\}$ consists of a single vector, say v. Now since $Ax \leq b$ has no integral solution, v must be nonintegral. Thus there exists trivially an inequality $wx \leq \alpha$ which can be derived from $(Ax \leq b,$ $Cx \leq d,\ -Cx \leq -d)$ with $\{x\colon wx \leq \alpha\} \cap \{x\colon Ax \leq b,\ Cx = d\} = \phi$. To obtain an inequality which can be derived from $(Ax \leq b,\ Cx \leq d)$ we will "rotate" $wx \leq \alpha$ in the following way, as in Schrijver[24]. By the definition of a derivation, there exist vectors y^1 and y^2 with $y^1 \geq 0$ and $y^1 A + y^2 C = w$, $y^1 b + y^2 d < \alpha + 1$. Let

$$w' = w - \lfloor y^2 \rfloor C = y^1 A + (y^2 - \lfloor y^2 \rfloor)C$$

$$\alpha' = \alpha - \lfloor y^2 \rfloor d \geq \lfloor y^1 b + (y^2 - \lfloor y^2 \rfloor)d \rfloor$$

where $\lfloor y^2 \rfloor$ denotes the vector $(\lfloor y_1^2 \rfloor, \ldots, \lfloor y_k^2 \rfloor)$. Now since $(y^2 - \lfloor y^2 \rfloor)$ is nonnegative and w' is integral, $w'x \leq \alpha'$ may be derived from $(Ax \leq b,\ Cx \leq d)$. Furthermore, $\{x\colon w'x \leq \alpha',\ Ax \leq b,\ Cx = d\} = \{x\colon wx \leq \alpha,\ Ax \leq b,\ Cx = d\}$. So $w'x \leq \alpha'$ is an appropriate inequality. The only difficulty is that we have not yet given a bound on its size. To do this, we will "reduce" the inequality as follows. By Caratheodory's theorem, there exist nonnegative vectors $\bar{y}^1$ and $\bar{y}^2$ with $\bar{y}^1 A + \bar{y}^2 C = w'$ and $\bar{y}^1 b + \bar{y}^2 d < \alpha' + 1$, such that at most n components of $\bar{y}^1$ and $\bar{y}^2$ are positive. For a vector $u = (u_1, \ldots, u_{\ell}$

let $[u] = ([u_1],\ldots,[u_t])$ where $[u_i] = \lfloor u_i \rfloor - 1$ if u_i is a positive integer and $[u_i] = \lfloor u_i \rfloor$ otherwise. (We use $[u]$ in the following definition, rather than $\lfloor u \rfloor$, since latter in the proof we need to have $u_i - [u_i] > 0$ if $u_i > 0$.) Let

$$c_n = w' - [\bar{y}^1]A - [\bar{y}^2]C = (\bar{y}^1 - [\bar{y}^1])A + (\bar{y}^2 - [\bar{y}^2])C$$
$$d_n = \alpha' - [\bar{y}^1]b - [\bar{y}^2]d \geq \lfloor (\bar{y}^1 - [\bar{y}^1])b + (\bar{y}^2 - [\bar{y}^2])d \rfloor .$$

The inequality $c_n x \leq d_n$ may be derived from $(Ax \leq b,\ Cx \leq d)$ and $\{x\colon c_n x \leq d_n,\ Ax \leq b,\ Cx \leq d\} \subseteq \{x\colon w'x \leq \alpha',\ Ax \leq b,\ Cx \leq d\}$. Also, since $0 \leq \bar{y}^1 - [\bar{y}^1] \leq 1$ and $0 \leq \bar{y}^2 - [\bar{y}^2] \leq 1$ and at most n components of $\bar{y}^1 - [\bar{y}^1]$ and $\bar{y}^2 - [\bar{y}^2]$ are positive, the absolute value of each coefficient in $c_n x \leq d_n$ is at most $n\sigma(A,b,C,d)$. So $c_n x \leq d_n$ is the inequality we seek and, thus, (3) is true when $k = n$.

Now suppose C is of rank $r < n$ and that (3) is true for all $k \geq r+1$. Letting $A^o x \leq b^o$ be those inequalities in $Ax \leq b$ which hold as equality for each vector in $\{x\colon Ax \leq b,\ Cx = d\}$ we have that $M = \{x\colon A^o x = b^o,\ Cx = d\}$ is the affine hull of $\{x\colon Ax \leq b,\ Cx = d\}$. If $(A^o x = b^o,\ Cx = d)$ has no integral solution, then there exist vectors y^o and y such that $y^o A^o + yC$ is integral and $y^o b^o + yd$ is nonintegral (see, for example, Schrijver[25]). Letting $w = y^o A^o + yC$ and $\alpha = \lfloor y^o b^o + yd \rfloor$ we have $\{x\colon wx \leq \alpha,\ Ax \leq b,\ Cx = d\} = \phi$. Also, by Farkas' lemma, $wx \leq \alpha$ may be derived from $(Ax \leq b,\ Cx \leq d,\ -Cx \leq -d)$. So, rotating $wx \leq \alpha$ as above we obtain an inequality $w'x \leq \alpha'$ which may be derived from $(Ax \leq b,\ Cx \leq d)$ such that $\{x\colon w'x \leq \alpha',\ Ax \leq b,\ Cx = d\} = \{x\colon wx \leq \alpha,\ Ax \leq b,\ Cx = d\} = \phi$. Now reducing $w'x \leq \alpha'$ as above, we obtain an inequality $c_r x \leq d_r$ which satisfies the conditions in (3). So we may assume $(A^o x = b^o,\ Cx = d)$ has an integral solution, that is, that M contains integral vectors.

Let s be the dimension of M. We will define an affine transformation T which maps Z^n onto Z^n and M onto $\{x \in Q^n\colon x_{s+1} = 0,\ldots,x_n = 0\}$ so that we may work with polyhedra of full dimension. To do this, let v be an integral vector in M and let $L = \{x-v\colon x \in M\}$ be the linear subspace parallel to M. Consider a basis $h^1,\ldots,h^n$ of the lattice Z^n such that $h^1,\ldots,h^s$ is a basis of the lattice $L \cap Z^n$ and let $T(x)$ be $S(x) - v$ where S is the linear transformation which maps h^i onto e^i, the i^{th}- unit vector, for $i = 1,\ldots,n$.

Denote by P the polyhedron which is the projection, onto the first s coordinates of the image of $\{x\colon Ax \leq b,\ Cx = d\}$ under T, that is, let $P = \{\bar{x} \in Q^s\colon (\bar{x},0) \in T(\{x\colon Ax \leq b,\ Cx = d\})\}$. Since T maps Z^n onto Z^n, we have $P \cap Z^s = \phi$. Thus, as shown by Hastad[16], a result of Lenstra and Schnorr[22] on the product of the covering radius of a lattice and the length of the shortest vector in the dual lattice implies that

• there exists an integral vector $\bar{w} \varepsilon Q^s$ such that $|\bar{w}\bar{x}' - \bar{w}\bar{x}''| < s^{5/2}$ for all vectors $\bar{x}'$, $\bar{x}''$ in P (see also Grötschel, Lovász, and Schrijver[14] and Kannan and Lovász[18]).

We may assume that the components of $\bar{w}$ are relatively prime and hence that the equation $\bar{w}\bar{x} = k$ has integral solutions for all integers k. Let $\bar{\alpha} = \lfloor \max\{\bar{w}\bar{x}: \bar{x} \varepsilon P\} \rfloor$. Since $\{\bar{x} \varepsilon Q^s: \bar{w}\bar{x} = \bar{\alpha}\}$ contains integral vectors, so does the hyperplane $H = T^{-1}(\{(\bar{x},0) \varepsilon Q^n: \bar{w}\bar{x} = \bar{\alpha}\})$. So there exists a vector $w \varepsilon Z^n$ with relatively prime components such that $H = \{x: wx = \alpha\}$ for some integer α. Notice that since $P \subseteq \{\bar{x} \varepsilon Q^s: \bar{w}\bar{x} < \bar{\alpha} + 1\}$ we may assume that $\{x: Ax \le b,\ Cx = d\} \subseteq \{x: wx < \alpha + 1\}$. Furthermore, for any integer k the hyperplane $T^{-1}(\{(\bar{x},0) \varepsilon Q^n: \bar{w}\bar{x} = k\})$ contains integral vectors and so is of the form $\{x: wx = k'\}$ for some integer k'. Thus, the fact that $P \subseteq \{\bar{x} \varepsilon Q^s: \bar{w}\bar{x} > \bar{\alpha} - s^{5/2}\}$ implies that $\{x: Ax \le b,\ Cx = d\} \subseteq \{x: wx > \alpha - s^{5/2}\}$. After rotating and reducing, we will use the hyperplanes $\{x: wx = k'\}$ as cutting planes.

First, since $\{x: Ax \le b,\ Cx = d\} \subseteq \{x: wx < \alpha + 1\}$, Farkas' lemma implies that $wx \le \alpha$ can be derived from $(Ax \le b,\ Cx \le d,\ -Cx \le -d)$. By rotating and reducing as above we obtain an inequality $c_r'x \le d_r'$ which can be derived from $(Ax \le b,\ Cx \le d)$, such that $\{x: Ax \le b,\ Cx = d,\ c_r'x \le d_r'\} \subseteq \{x: Ax \le b,\ Cx = d,\ wx \le \alpha\}$ and the greatest amongst the absolute values of the components of c_r' and d_r' is at most $n\sigma(A,b,C,d)$. It also follows from the rotation and reduction procedures that

$$\{x: Ax \le b,\ Cx = d,\ c_r'x \le d_r' - s^{5/2}\} \subseteq \{x: Ax \le b,\ Cx = d,\ wx \le \alpha - s^{5/2}\}.$$

So $\{x: Ax \le b,\ Cx = d\} \subseteq \{x: c_r'x > d_r' - s^{5/2}\} \subseteq \{x: c_r'x > d_r' - (n-r)^{5/2}\}$.

The dimension of $P \cap \{\bar{x} \varepsilon Q^s: \bar{w}\bar{x} = \bar{\alpha}\}$ is less than the dimension of P, since P is of full dimension. So $\{x: Ax \le b,\ Cx = d,\ c_r'x = d_r'\}$ has dimension less than that of $\{x: Ax \le b,\ Cx = d\}$. (To see this, note that if $wx \le \alpha$ does not hold for each solution of $(Ax \le b,\ Cx = d)$ then we have $\{x: Ax \le b,\ Cx = d\} \not\subseteq \{x: c_r'x = d_r'\}$; and if $wx \le \alpha$ is valid for all solutions of $(Ax \le b,\ Cx = d)$ then $\{x: Ax \le b,\ Cx = d,\ c_r'x = d_r'\} = \{x: Ax \le b,\ Cx = d,\ wx = \alpha\}$, using the fact that in the reduction procedure we have $y_i^1 - \lfloor y_i^1 \rfloor > 0$ if $y_i^1 > 0$.) Thus c_r' is not a linear combination of the rows of C. This implies that there exists an inequality $c_{r+1}x \le d_{r+1}$ with $\{x: Ax \le b,\ Cx = d,\ c_r'x = d_r',\ c_{r+1}x \le d_{r+1}\} = \phi$ and a cutting-plane proof of $c_{r+1}x \le d_{r+1}$ from $(Ax \le b,\ Cx \le d,\ c_r'x \le d_r')$ of length at most $\max\{1,\ n^{3(n-r-1)} - 1\}$ which requires only n-r inequalities, besides $(Ax \le b,\ Cx \le d,\ c_r'x \le d_r')$, to be stored at any one time and with each inequality in the proof having all coefficients of absolute value at most $n^{3(n-r-1)+1}(n\sigma(A,b,C,d))$, since we have assumed that (3) is true for all $k \ge r+1$. Let $c_r''x \le d_r''$ be obtained by summing $c_r'x \le d_r'$ and the inequalities $Cx \le d$, that is, $c_r'' = c_r' + \mathbf{1}C$, $d_r'' = d_r' + \mathbf{1}d$, where $\mathbf{1}$ is the vector of all 1's. We have that

$$\{x\colon Ax \le b,\ Cx \le d,\ c_r'x \le d_r',\ c_r''x = d_r''\} = \{x\colon Ax \le b,\ Cx = d,\ c_r'x = d_r'\}.$$

So $\{x\colon Ax \le b,\ Cx \le d,\ c_r'x \le d_r',\ c_r''x = d_r'',\ c_{r+1}x \le d_{r+1}\} = \phi$ and hence $c_r''x \le d_r'' - 1$ may be derived from $(Ax \le b,\ Cx \le d,\ c_r'x \le d_r',\ c_{r+1}x \le d_{r+1})$. Notice that $\{x\colon Ax \le b,\ Cx = d\} \subseteq \{x\colon c_r''x > d_r'' - (n-r)^{5/2}\}$ and that the numbers appearing in $c_r''x \le d_r'' - 1$ have absolute value at most $2n\sigma(A,b,C,d)$.

So far we have a cutting-plane proof of $c_r''x \le d_r'' - 1$ from $(Ax \le b,\ Cx \le d)$. If $\{x\colon Ax \le b,\ Cx = d,\ c_r''x \le d_r'' - 1\} = \phi$ we are finished. Otherwise, we can find, as above, a cutting-plane proof of the inequality $c_r'''x \le d_r''' - 2$ from $(Ax \le b,\ Cx \le d)$, where $c_r'''x \le d_r'''$ is obtained by summing $c_r''x \le d_r''$ and the inequalities $Cx \le d$. Repeating this at most $(n-r)^{5/2}$ times, we obtain a cutting-plane proof of an inequality $c_rx \le d_r$ from $(Ax \le b,\ Cx \le d)$ with $\{x\colon Ax \le b,\ Cx = d,\ c_rx \le d_r\} = \phi$. The absolute values of the coefficients of $c_rx \le d_r$ are at most $((n-r)^{5/2} + 1)\sigma(A,b,C,d)$, which is less than $n^3\sigma(A,b,C,d)$. So the greatest absolute value amongst the coefficients of the inequalities in the cutting-plane proof is at most $n^{3(n-r)+1}\sigma(A,b,C,d)$. The length of the cutting-plane proof is at most $(n-r)^{5/2}(\max\{1, n^{3(n-r-1)} - 1\}) + (n-r)^{5/2} + 1 \le n^{3(n-r)} - 1$. Finally, the proof requires at most $n-r+1$ inequalities, besides $(Ax \le b,\ Cx \le d)$, to be stored at any one time. So (3) holds in the case $k = r$, which completes the proof of the theorem. //

<u>Remarks</u>: 1) For bounded polyhedra, this theorem without the restriction on the lengths of the proofs may also be derived from Chvátal's[3] technique, since, as observed by Coullard[8], the cutting-plane proofs given in [3] require only polynomial workspace. The restriction on the length does not follow in this way since the number of derived inequalities in these proofs depends on the least integer N such that $\{x\colon Ax \le b\} \subseteq \{x\colon |x_i| \le N,\ i = 1,\dots,n\}$ and so may be arbitrarily high, even in the 2-dimensional case. //

2) Chvátal[6] defines cutting-plane proofs in general as a method for showing that every integral solution of $Ax \le b$ satisfies another specified inequality $wx \le \beta$, by requiring that the last inequality in the proof be $wx \le \beta$, rather than $0x \le -1$. Such a cutting-plane proof always exists if either $\{x\colon Ax \le b\}$ is bounded, as shown by Chvátal[3], or if A and b are rational and $Ax \le b$ has at least one integral solution,

as shown by Schrijver[24]. The lengths of these proofs, even when the inequalities have only two variables, may necessarily be arbitrarily long (see the example of J.A. Bondy given in Chvátal[3]). But, as the proof of our theorem only requires that ($Ax \leq b$, $wx = t$) have no integral solution in order to obtain a cutting-plane proof of $wx \leq t-1$, if A and b are rational then in either Chvátal's case or Schrijver's case there exist proofs which can be carried out in polynomial workspace. //

Acknowledgements

The author would like to thank Professor Gy. Turán for many valuable conversation which initiated the research reported here, and also to thank Professor L. Lovász for valuable discussions on proofs of the main result.

References

[1] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem", to appear in Combinatorica.

[2] S.C. Boyd and W.R. Pulleyblank, "Facet generating techniques", in preparation.

[3] V. Chvátal, "Edmonds polytopes and a hierarchy of combinatorial problems", Discrete Math. 4 (1973) 305-337.

[4] V. Chvátal, "Edmonds polytopes and weakly hamiltonian graphs", Math. Prog. 5 (1973) 29-40.

[5] V. Chvátal, "Cutting planes in combinatorics", Report No. 84325-OR, Inst. für Ökon. u. Op. Res., Uni. Bonn, W. Germany, 1984.

[6] V. Chvátal, "Cutting-plane proofs and the stability number of a graph", Report No. 84326-OR, Inst. für Ökon. u. Op. Res., Uni. Bonn, W. Germany, 1984.

[7] W. Cook, C.R. Coullard, and Gy. Turán, "On the complexity of cutting-plane proofs", Report No. 85377-OR, Inst. für Ökon. u. Op. Res., Uni. Bonn, W. Germany, 1985.

[8] C.R. Coullard, personal communication.

[9] H. Crowder, E.L. Johnson, and M.W. Padberg, "Solving large scale zero-one linear programming problems", Operations Research 31 (1983) 803-834.

[10] H.P. Crowder and M.W. Padberg, "Solving large scale symmetric travelling salesman problems to optimality", Management Sci. 26 (1980) 495-509.

[11] G.B. Dantzig, D.R. Fulkerson, and S.M. Johnson, "Solution of a large-scale traveling salesman problem", JORSA 2 (1954) 393-410.

[12] R.E. Gomory, "An algorithm for integer solutions to linear programs", in: R.L. Graves and P. Wolfe (eds.), Recent Advances in Mathematical Programming (McGraw-Hill, New York, 1963) 269-302.

[13] M. Grötschel, M. Jünger, and G. Reinelt, "A cutting plane algorithm for the linear ordering problem", Operations Research 32 (1984) 1195-1220.

[14] M. Grötschel, L. Lovász, and A. Schrijver, The Ellipsoid Method and Combinatorial Optimization (Springer, Berlin), to appear.

[15] A. Haken, "The intractability of resolution", Theorectical Comp. Sci. 39 (1985) 297-308.

[16] J. Hastad, communicated by R. Kannan.

[17] R. Kannan, "Improved algorithms for integer programming and related lattice problems", 15th ACM Symp. on the Theory of Computing (1983) 193-206.

[18] R. Kannan and L. Lovász, to appear.

[19] D. Kozen, "Lower bounds for natural proof systems", Proc. 18th IEEE Symp. on Foundations of Computer Science (1977) 254-266.

[20] D. Kozen, "Pebblings, edgings, and equational logic", Proc. 16th ACM Symp. on the Theory of Computing (1984) 428-435.

[21] H.W. Lenstra, "Integer programming with a fixed number of variables", Math. of Op. Res. 8 (1983) 538-548.

[22] H.W. Lenstra and C.P. Schnorr, "On the successive minima of a pair of polar lattices", to appear.

[23] M.W. Padberg, T.J. van Roy, and L.A. Wolsey, "Valid linear inequalities for for fixed charge problems", Operations Research 33 (1985) 842-861.

[24] A. Schrijver, "On cutting planes", Ann. of Discrete Math. 9 (1980) 291-296.

[25] A. Schrijver, Theory of Linear and Integer Programming (Wiley, Chichester, 198