RC22575 (W0209-110) September 27, 2002
OTHER

IBM Research Report

Exponential Lower Bounds on the Lengths of Some Classes of Branch-and-Cut Proofs

Sanjeeb Dash
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Exponential Lower Bounds on the Lengths of Some Classes of Branch-and-Cut Proofs*

Sanjeeb Dash
IBM Research Division
T. J. Watson Research Center

September 27, 2002

Abstract

Branch-and-cut methods are among the most important techniques for solving integer programming problems. They can also be used to prove that all solutions of an integer program satisfy a given linear inequality. We examine the complexity of branch-and-cut proofs in the context of 0-1 integer programs. We prove an exponential lower bound on the length of branch-and-cut proofs which use 0-1 branching and lift-and-project cuts (called simple disjunctive cuts by some authors), Gomory-Chvátal cuts, and cuts arising from the N_0 matrix-cut operator of Lovász and Schrijver. A consequence of the lower-bound result in this paper is that branch-and-cut methods of the type described above have exponential running time in the worst case.

Key words. Cutting planes, cutting-plane proofs, branch-and-cut proofs, proof complexity.

1 Introduction

Branch-and-cut algorithms, which combine linear programming based branch-and-bound with cutting planes, are currently the most important methods for integer programming . Such methods have been used with great success over the last decade in solving both specific combinatorial optimization problems – such as the traveling salesman problem – and general integer programs arising in practical situations. Earlier, branch-and-cut implementations typically employed problem specific cutting planes (e.g., comb inequalities for TSP instances), but recently, general cutting planes such as disjunctive cuts (Balas 1979), Gomory mixed integer cuts (Gomory 1960), and MIR cuts (Nemhauser and Wolsey 1990) have become important components in branch-and-cut. See Balas, Ceria, Cornuéjols and Nataraj (1996), Bixby, Fenelon, Gu, Rothberg and Wunderling (2000), and Marchand and Wolsey (2001).

Different types of complexity properties of branch-and-cut methods have been studied by various authors. Three types of complexity issues which have recently been addressed are:

(i) Given an arbitrary point, how difficult is it to find a violated inequality from a given class of cutting planes ?

*This work was supported in part by ONR Grant N00014-01-1-0058.

(ii) Given a class of cutting planes, what is the rank of the linear programming relaxation for a problem with respect to the closure operation (for the class of cuts) ?

(iii) What is the worst-case time complexity of a given branch-and-cut method ?

See Cornuéjols and Li (2002), Caprara and Letchford (2002), and Eisenbrand (1999) for recent work on the first aspect. See Eisenbrand and Schulz (1999), Goemans and Tunçel (2001) and Laurent (2001) for studies of rank. Here we study the time-complexity of branch-and-cut methods, and the sizes of proofs or certificates generated by such methods.

In spite of the many successful applications of branch-and-cut, such methods are unlikely to have polynomial time-complexity as the integer programming problem is NP-hard. Some special classes of branch-and-cut algorithms are known to have exponential time-complexity; however, not many results of this type are known. Jeroslow (1974) showed that any branch-and-bound procedure for the 0-1 integer program $\max\{x_1 \mid x_1+\cdots+x_n = n/2, x_1, \ldots, x_n \in \{0,1\}\}$ where n is an odd integer, requires at least $2^{(n+1)/2}$ iterations. Chvátal (1980) showed that every (LP based) branch-and-bound procedure requires an exponential number of nodes for almost every problem in a certain class of 0-1 knapsack problems. Gu, Nemhauser and Savelsbergh (1999) strengthened Chvátal's result by presenting a class of 0-1 knapsack problems such that any branch-and-cut method based on lifted-cover inequalities requires exponentially many nodes. Chvátal, Cook and Hartmann (1989) proved exponential lower bounds on the number of cutting-planes generated by a class of (Gomory-Chvátal) cutting-plane algorithms for the traveling salesman problem; their bounds are however exponential in the number of variables, but not in the number of constraints. Pudlák (1997) provided the first true exponential lower bound on the complexity of cutting-plane algorithms based on Gomory-Chvátal cuts; he showed that such algorithms must generate exponentially many cuts in order to establish the infeasibility of some 0-1 integer programs.

Chvátal (1973) introduced the notion of a *cutting-plane proof*; this can be viewed as a way of writing down a certificate of optimality or infeasibility generated by a cutting-plane algorithm. This notion is further developed in Chvátal (1984, 1985); it can trivially be extended to the notion of *branch-and-cut proofs*. An important common thread through the results in the previous paragraph is this: each result essentially shows the non-existence of "short" or polynomial-size branch-and-cut proofs of a certain type (e.g., proofs having only Gomory-Chvátal cuts). Such results are obviously more general than complexity bounds on a single algorithm. For example, Pudlak's result shows that not only does Gomory's algorithm (1958) take exponential time in the worst case, but so does every other algorithm which sequentially generates Gomory-Chvátal cuts.

We need to clarify a point here. A simple example by Bondy (see Schrijver 1986) shows that for $\max\{x_1 \mid x_1 + kx_2 \leq k, x_1 - kx_2 \leq 0, x_1, x_2 \text{ integral}\}$ where k is a positive integer, at least $k/2$ Gomory-Chvátal cuts are required to establish that integral solutions satisfy $x_1 \leq 0$ (i.e., the optimal value is 0). On the other hand, we can indirectly verify that the optimal value is 0 by showing that no integral solutions satisfy $x_1 \geq 1$; a single cut is enough for this. More generally, for any cutting-plane proof of $c^T x \leq d$, there is a always a cutting plane proof of the same length showing that no integral solutions satisfy $c^T x \geq d + 1$, whereas the converse is not true. (See Cook, Coullard and Turán 1987 for a discussion of *indirect* cutting-plane proofs). In this sense cutting-plane proofs of infeasibility are more general than cutting-plane proofs of optimality. Bondy's example easily yields exponential lower bounds (the number of cuts is exponential in the encoding size) for proofs of the second type, whereas Pudlák's result is the first exponential bound for proofs of the first type and is far more difficult.

The main reason for studying sizes of cutting-plane proofs of infeasibility (i.e., the number of bits needed to write down the proof) is because of the connection to the $NP \neq coNP$ question. The problem of determining if $Ax \leq b$ has a 0-1 solution for arbitrary A and b is NP-complete; not only do we expect that no polynomial-time algorithm exists, we expect that polynomial size cutting-plane proofs of infeasibility do not always exist for $Ax \leq b$ with no 0-1 solutions. This is because of the belief that $NP \neq coNP$, or that there is no "good characterization" of the integer feasibility of an arbitrary set of linear inequalities. A discussion of cutting-plane proofs in the context of complexity theory can be found in Cook, Coullard and Turán (1987), Cook (1990), Pudlák (1999) and Bonet, Pitassi and Raz (1997).

In this paper we study branch-and-cut proofs of infeasibility of 0-1 integer programs. We extend the notion of cutting-plane proofs given in Chvátal (1973) – we refer to the proofs there as Gomory-Chvátal cutting-plane proofs or *G-C proofs* – and study cutting-plane proofs based on lift-and-project cuts (Balas, Ceria and Cornuéjols 1993), Gomory-Chvátal cuts, and the cuts described in Lovász and Schrijver (1991). We also consider branch-and-cut proofs which use the cutting planes above along with branching on the 0-1 variables. When these proofs are restricted to using the weakest version of matrix cuts described in Lovász and Schrijver (1991), we call them *L-M-G proofs* and *L-M-G branch-and-cut proofs*. Extending Pudlák's (1997) ideas, we prove an exponential lower bound on the lengths (and therefore on the sizes) of L-M-G branch-and-cut proofs. Thus, we show that any branch-and-cut algorithm which uses branching on the variables and the cuts above has exponential worst-case complexity.

The paper is organised as follows. In Section 2, we describe the different cuts we use in this paper, and state some of their properties. The material after Theorem 2.3 is somewhat technical; we recommend that the reader refer to it while going through Section 4 and Section 5. In Section 3 we discuss the notion of branch-and-cut proofs. In Section 4, we discuss interpolation and monotone interpolation and their usefulness in establishing lower bounds on the lengths of cutting-plane proofs. We also present Pudlák's exponential bound for G-C proofs. In Section 6, an exponential lower bound on the lengths of lift-and-project cutting-plane proofs is proved. We then use this result to obtain the main result of the paper, an exponential lower bound on the lengths of L-M-G branch-and-cut proofs for 0-1 integer programs. We also answer a question posed by Pudlák (1999) on matrix-cut based proofs. We will assume familiarity with linear programming theory; see Schrijver (1986) for basic results in this area.

2 Some Classes of Cutting Planes

Two widely studied classes of general cutting planes are Gomory-Chvátal cutting planes (Gomory 1958, Chvátal 1973) and lift-and-project cuts (Balas, Ceria and Cornuéjols 1993). Gomory-Chvátal cuts are defined for general integer programs, whereas lift-and-project cuts are defined only for 0-1 integer programs (which is the case we are interested in here). Lift-and-project cuts — also called simple disjunctive cuts in Cornuéjols and Li (2001) — are special cases of the disjunctive cuts of Balas (1979), the matrix cuts of Lovász and Schrijver (1991), and the RLT framework of Sherali and Adams (1990). Split cuts, defined in Cook, Kannan and Schrijver (1990), generalize both Gomory-Chvátal cuts and lift-and-project cuts (and are also called disjunctive cuts). In this paper we study properties of algorithms and certificates (cutting-plane proofs) which use the above cutting planes.

Let $Q_n = [0,1]^n$ be the 0-1 cube in R^n. If the dimension is obvious from the context, we denote the 0-1 cube by Q. Let $a_i^T x \le b_i$ $(i = 1, \dots, m)$ be a system of rational linear inequalities in R^n (we generally assume linear inequalities are rational). Assume that the inequalities $0 \le x_j \le 1$ $(j = 1, \dots, n)$ are included in the above system. Let $P \subseteq Q$ be defined by

$$P = \{x \mid a_i^T x \le b_i,\ i = 1, \dots, m\}, \tag{1}$$

and let P_I stand for the convex hull of 0-1 points in P.

If $c^T x \le d$ is a linear inequality valid for P and c is integral, then $c^T x \le \lfloor d \rfloor$ is valid for all 0-1 points in P, and is called a *Gomory-Chvátal cutting plane* for P (abbreviated as a *G-C cut*). If an inequality $a^T x \le b$ is valid for both $P \cap \{x \mid c^T x \le d\}$ and $P \cap \{x \mid c^T x \ge d + 1\}$ for some integral c and d, then $a^T x \le b$ is called a *split cut.* A G-C cut is obviously a special type of split cut. The *Chvátal closure* of P is the set of points satisfying all G-C cuts for P and is denoted by P'. The *split closure* of P is defined similarly in terms of split cuts, and is denoted by $sc(P)$.

In what follows, we write $a^T x \le b$ as $b - a^T x \ge 0$. All points in P satisfy

$$\begin{aligned} (b_i - a_i^T x)\, x_j &\ge 0, \qquad i = 1, \dots, m, j = 1, \dots, n, \\ (b_i - a_i^T x)(1 - x_j) &\ge 0, \quad\ i = 1, \dots, m, j = 1, \dots, n, \end{aligned} \tag{2}$$

obtained by multiplying the inequalities in (1) with the inequalities defining Q. Also, 0-1 points in P satisfy

$$x_j^2 - x_j = 0,\ j = 1, \dots, n. \tag{3}$$

Adding non-negative multiples of the inequalities in (2) and arbitrary multiples of the equations (3) yields inequalities valid for all 0-1 points in P. A linear inequality of this form is a cutting plane for P, and is called an N-cut.

Formally, an inequality $c^T x \le d$ or $d - c^T x \ge 0$ is called an N*-cut* for P if

$$\begin{aligned} d - c^T x = \ & \sum_{i,j} \alpha_{ij}(b_i - a_i^T x) x_j + \\ & \sum_{i,j} \beta_{ij}(b_i - a_i^T x)(1 - x_j) + \\ & \sum_j \lambda_j (x_j^2 - x_j), \end{aligned} \tag{4}$$

where $\alpha_{ij} \ge 0, \beta_{ij} \ge 0$ and $\lambda_j \in R$ for $i = 1, \dots, m, j = 1, \dots, n$. A weakening of N-cuts, called N_0*-cuts*, can be obtained if in (4) we insist that $x_i x_j$ and $x_j x_i$ are distinct terms, for all i, j with $i \ne j$. That is, we do not combine $x_i x_j$ and $x_j x_i$ terms. A *lift-and-project cut* for P with respect to a variable x_k is a linear inequality of the form

$$\alpha(b_1 - a_1^T x)x_k + \beta(b_2 - a_2^T x)(1 - x_k) + \lambda(x_k^2 - x_k), \tag{5}$$

where $a_1^T x \le b_1$ and $a_2^T x \le b_2$ are valid for P, λ is some real number and α and β are non-negative reals. Thus a lift-and-project cut is a special type of N_0-cut.

N-cuts and N_0-cuts are examples of matrix cuts; see Lovász and Schrijver (1991) and Lovász (1994). N-cuts are also described in Sherali and Adams (1990). Lovász and Schrijver (1991) define N_+-cuts, which are stronger than the previous two classes. An inequality $d - c^T x \geq 0$ is called an N_+-*cut* for P if it is formed by adding $n+1$ squares of linear functions (i.e., terms of the form $(g_k + h_k^T x)^2$) to the sum in (4). Note that every inequality defining P is an N-cut, as is $1 \geq 0$ and any non-negative linear combination of N-cuts; this is true as well for N_0-cuts and N_+-cuts.

Of course, a notion of closure, similar to Chvátal closure, can be defined in the context of matrix cuts. The sets $N(P)$ and $N_+(P)$ are defined as follows:

$$N(P) \text{ is the set of points satisfying all } N\text{-cuts for } P, \tag{6}$$

$$N_+(P) \text{ is the set of points satisfying all } N_+\text{-cuts for } P. \tag{7}$$

$N_0(P)$ is defined similarly in terms of N_0-cuts; these sets have alternative projection representations. $N(P)$ and $N_0(P)$ are polytopes, whereas $N_+(P)$ is generally non-polyhedral. P_k is the polytope obtained from P by adding all lift-and-project cuts with respect to the variable x_k. Observe that every inequality valid for $N(P)$ is an N-cut for P. This is true even if $N(P) = \emptyset$; similar properties hold for $N_0(P), N_+(P)$ and P_k. We refer to N_0, N and N_+ as the matrix-cut operators.

The Chvátal closure can be iterated to obtain P_I from P; see Chvátal (1973), Schrijver (1980), and Eisenbrand and Schulz (1999). Lift-and-project cuts can also be generated iteratively.

Theorem 2.1 *(Balas 1979). If $i_1, i_2, \ldots, i_n$ is any permutation of $\{1, 2, \ldots, n\}$ and P is a polytope in Q_n, then $(\cdots((P_{i_1})_{i_2})\cdots)_{i_n} = P_I$.*

A proof can be found in Balas, Ceria and Cornuéjols (1993).

The matrix-cut operators can be iterated to obtain approximations of P_I which are strictly contained in P (if $P \neq P_I$). Let $N^0(P) = P$ and $N^{t+1}(P) = N(N^t(P))$ if t is a non-negative integer. Let $N_0^t(P)$ and $N_+^t(P)$ be similarly defined. Lovász and Schrijver (1991) establish the following facts (Theorem 2.2 can be derived from Theorem 2.1).

Theorem 2.2 *Let $P \subseteq Q_n$ be a polytope. Then $N_0^n(P) = P_I$.*

Theorem 2.3 *(Lovász and Schrijver 1991). Let $P = \{x \mid Ax \leq b\}$ be a polytope contained in Q_n. For any fixed value of t, it is possible to optimize linear functions over both $N_0^t(P)$ and $N^t(P)$ in time bounded by a polynomial function of the encoding size of $Ax \leq b$.*

Theorem 2.2 remains true if N_0 is replaced by N or N_+, as both of these operators yield smaller convex sets than N_0. In the case of N_+, it is possible to approximate the maximum or minimum of a linear function over $N_+(P)$ to within a prescribed error tolerance in polynomial time.

The next result can be found in Cook and Dash (2001); an analogous property holds for Chvátal closures (Schrijver 1980).

Lemma 2.4 *If F is a face of a polytope $P \subseteq Q$, then $N(F) = N(P) \cap F$. This equation is also valid for the N_+ and N_0 operators.*

Lemma 2.4 is useful in many contexts. Let F be a face of a polytope P and let $c^T x \leq d$ be an N-cut for F. From Lemma 2.4, $N(F)$ is a face of $N(P)$. As $N(P)$ is a polytope, we can "rotate" $c^T x \leq d$ to get an inequality $(c')^T x \leq d'$ valid for $N(P)$, and hence an N-cut for P, such that

$$F \cap \{x \mid c^T x \leq d\} = F \cap \{x \mid (c')^T x \leq d'\}. \tag{8}$$

Compare this with Lemma 6.33 in Cook, Cunningham, Pulleyblank, and Schrijver (1998) (the same result for P'). We may not be able to "rotate" $c^T x \leq d$ in the case of $N_+(P)$ as it may not be a polytope. Lemma 2.4 also implies:

$$F \text{ is a face of } Q \Rightarrow N(P \cap F) = N(P) \cap F. \tag{9}$$

Lemma 2.5 and Lemma 2.6 combine results from Lovász and Schrijver (1991) and Balas, Ceria and Cornuéjols (1993) and give useful properties of $N_0(P)$.

Lemma 2.5 *Assume that $a^T x \leq b$ is valid for $P \cap \{x \mid x_i = 0\}$ and $P \cap \{x \mid x_i = 1\}$, where P is a polytope, and $1 \leq i \leq n$. Then $a^T x \leq b$ is valid for P_i and $N_0(P)$.*

Proof: It is easy to see that there are non-negative numbers α and β, such that

$$\begin{aligned} &a^T x - \alpha x_i \leq b \text{ is valid for } P, \\ &a^T x - \beta(1 - x_i) \leq b \text{ is valid for } P. \end{aligned}$$

Multiplying the first inequality by $1 - x_i$ and the second by x_i, replacing x_i^2 by x_i and adding, we see that $a^T x \leq b$ is a lift-and-project cut with respect to the variable x_i. □

Lemma 2.6 *If $P \subseteq Q_n$ is a polytope, then $P_i = conv((P \cap \{x \mid x_i = 0\}) \cup (P \cap \{x \mid x_i = 1\}))$ for $i = 1, \ldots, n$, and $N_0(P) = \cap_i P_i$.*

We now state some well-known properties of symmetric positive semidefinite matrices which we need; see Horn and Johnson (1985). We denote the fact that a matrix A is positive semidefinite by $A \succeq 0$. A *principal submatrix* of a matrix is a square submatrix obtained by deleting some rows and the corresponding columns from the matrix. If $A \succeq 0$, then every principal submatrix of A is positive semidefinite. If a matrix A has a block-diagonal decomposition, then $A \succeq 0 \Leftrightarrow$ every block is positive semidefinite. For example,

$$\text{if } A = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}, \text{ then } A \succeq 0 \Leftrightarrow A_1 \succeq 0, A_2 \succeq 0 \ . \tag{10}$$

A useful characterization of positive semidefinite matrices, involving Schur complements, is:

Proposition 2.7 *Let A be a non-singular matrix, and let B and C be matrices.*

$$\textit{If } D = \begin{bmatrix} A & B \\ B^T & C \end{bmatrix}, \textit{ then } D \succeq 0 \Leftrightarrow C - B^T A^{-1} B \succeq 0 \ .$$

We now proceed to formalize the intuitively obvious idea that given two independent systems of inequalities, if a cutting plane is derived from the combined system, then it is implied by cutting planes derived separately from the two systems. We first give a very concise description of some results from Lovász and Schrijver (1991). For a vector $z \in R^n$, define $\overline{z}$ as the vector $(1 \ \ z^T)^T$, and assume the coordinates of $\overline{z}$ are indexed from 0 onwards. Thus, $\overline{z}_0 = 1$ and $\overline{z}_i = z_i$ for $i = 1, \ldots, n$. Also assume $(n+1) \times (n+1)$ matrices are indexed from (0,0) onwards, and that e_i is the ith unit vector in R^{n+1}. Observe that if z is a 0-1 solution of (1), then $M = \overline{z}\overline{z}^T$ satisfies:

$$\text{(i) } (b_i \text{ -}a_i^T)Me_0 \geq 0 \text{ and } (b_i \text{ -}a_i^T)M(e_0 - e_i) \geq 0 \ (i = 1, \ldots, m, \ j = 1, \ldots, n),$$
$$\text{(ii) } M_{i0} = M_{ii} \ (i = 1, \ldots, n), \ \text{(iii) } M = M^T, \ \text{and (iv) } M \succeq 0.$$

Lovász and Schrijver (1991) provided the following characterizations of $N_+(P)$ and $N(P)$ (dual to (6) and (7)):

$$N(P) = \{x \mid \overline{x} = Me_0, \text{ where } M \text{ satisfies (i) - (iii) above}\}, \tag{11}$$
$$N_+(P) = \{x \mid \overline{x} = Me_0, \text{ where } M \text{ satisfies (i) - (iv) above}\}. \tag{12}$$

The set of matrices satisfying conditions (i) - (iii) (as in (11)) is called $M(P)$, and $M_+(P)$ is the set of matrices satisfying (i) - (iv) above. $N_0(P)$ can be defined similarly: $x \in N_0(P) \Leftrightarrow \overline{x} = Me_0$ for some M satisfying (i) and (ii) (the set of such matrices is $M_0(P)$). The next result is essential for some of the lower bounds we prove later on.

Lemma 2.8 *Let $P_1 = \{(x, y) \mid Ax \leq e\}$ and $P_2 = \{(x, y) \mid By \leq f\}$ be two polytopes contained in Q. Then $N_+(P_1 \cap P_2) = N_+(P_1) \cap N_+(P_2)$. An identical result holds for N and N_0.*

Proof: For any two polytopes P_1 and P_2, it is true that $N_+(P_1 \cap P_2) \subseteq N_+(P_1) \cap N_+(P_2)$. Let P_1 and P_2 satisfy the conditions of the lemma. To prove the reverse inclusion, assume that

$$z = \begin{pmatrix} x \\ y \end{pmatrix} \in N_+(P_1) \cap N_+(P_2) \ . \tag{13}$$

Then there are symmetric matrices $X \in M_+(P_1)$ and $Y \in M_+(P_2)$ such that $\overline{z} = Xe_0 = Ye_0$, where

$$X = \begin{pmatrix} 1 & x^T & y^T \\ x & X_{11} & X_{12}^T \\ y & X_{12} & X_{22} \end{pmatrix} \text{ and } Y = \begin{pmatrix} 1 & x^T & y^T \\ x & Y_{11} & Y_{12}^T \\ y & Y_{12} & Y_{22} \end{pmatrix}. \tag{14}$$

Also $X, Y \succeq 0$. As X and Y are positive semidefinite,

$$\begin{pmatrix} 1 & x^T \\ x & X_{11} \end{pmatrix} \succeq 0 \text{ and } \begin{pmatrix} 1 & y^T \\ y & Y_{22} \end{pmatrix} \succeq 0 \ ; \tag{15}$$

the above matrices are principal submatrices of X and Y. We can conclude that $X_{11} - xx^T$ and $Y_{22} - yy^T$ are both positive semidefinite. This is true because of Proposition 2.7 (set $A = 1$).

Now, let Z be the matrix defined by

$$Z = \begin{pmatrix} 1 & x^T & y^T \\ x & X_{11} & xy^T \\ y & yx^T & Y_{22} \end{pmatrix}. \tag{16}$$

It is not difficult to verify that Z is contained in $M(P_1 \cap P_2)$. Also, observe that $Z - \overline{z}\overline{z}^T$ is a block-diagonal matrix with non-zero blocks $X_{11} - xx^T$ and $Y_{22} - yy^T$. Therefore $Z - \overline{z}\overline{z}^T$ is positive semidefinite by (10); this implies that $Z \succeq 0$. Since $\overline{z} = Ze_0$, we have shown that $z \in N_+(P_1 \cap P_2)$, and the result follows for the semidefinite operator.

Observe that in (14), if we start out with X in $M(P_1)$ and Y in $M(P_2)$, then Z yields the result for $N(P)$. Now let X and Y belong to $M_0(P_1)$ and $M_0(P_2)$ respectively. Then X and Y are as in (14), except that they are non-symmetric and X_{12}^T is replaced by X_{21}, and Y_{12}^T by Y_{21}. The matrix Z above, formed from X and Y, belongs to $M_0(P_1 \cap P_2)$, and the result for $N_0(P)$ follows. □

3 Cutting-Plane Proofs and Branch-and-Cut Proofs

Traditionally, the phrase "cutting-plane proof" refers to a proof using G-C cuts. We refer to such proofs as *Gomory-Chvátal cutting-plane proofs* (or as *G-C proofs* for shortness' sake). By a cutting-plane proof, we mean one which uses any of the cutting planes discussed in Section 2.

Let $Ax \leq b$ denote the following linear system in R^n:

$$a_i^T x \leq b_i \ (i = 1, \ldots, m). \tag{17}$$

Assume $c^T x \leq d$ is valid for all 0-1 solutions of $Ax \leq b$. An *N-cutting-plane proof* of $c^T x \leq d$ from $Ax \leq b$ is a sequence,

$$a_{m+k}^T x \leq b_{m+k} \ (k = 1, \ldots, M), \tag{18}$$

with $c^T x \leq d$ the last inequality in the sequence, and a collection of numbers

$$\alpha_{jl}^k, \beta_{jl}^k \geq 0 \ (k = 1, \ldots, M, \ j = 1, \ldots, m + k - 1, \ l = 1, \ldots, n) \tag{19}$$

such that, for $k = 1, \ldots, M$, $a_{m+k}^T x \leq b_{m+k}$ is derived as in (4) using α_{jl}^k and β_{jl}^k from

$$a_j^T x \leq b_j \ (j = 1, \ldots, m + k - 1).$$

Informally, an inequality in the sequence is an N-cut for the previous inequalities in the sequence. The *length* of the cutting-plane proof is M and its *size* is the sum of the sizes of the inequalities and numbers $\alpha_{jl}^k, \beta_{jl}^k$ in the proof. (The size of a proof is the number of bits required to write it down). If an inequality belongs to or is implied by $Ax \leq b$, we say it has an N-cutting-plane proof of length 0 from $Ax \leq b$. We can assume that inequalities in (17) and (18) are integral. Proofs using lift-and-project cuts, N_0-cuts, or N_+-cuts are defined in a similar fashion. An N-cutting-plane proof will be abbreviated as an *N-proof.* We analogously define *N_+-proofs.*

If an inequality $c^T x \leq d$ has an N-proof from P, then $c^T x \leq d$ is valid for P_I. Conversely, an inequality valid for P_I has an N-proof from P; this follows from Theorem 2.2 and the fact that $N(P)$ is a polytope whenever P is. Because of this property the set of N-proofs is said to be *complete* or to define a complete proof system. Similarly, each class of cutting planes in Section 2 defines a complete proof system. If P_I is empty, we refer to a cutting-plane proof of $0^T x \leq -1$ as a *cutting-plane proof of infeasibility.*

We can use both G-C cuts and N_+-cuts in a cutting-plane proof; such a proof will be called an N_*-proof. We also define $N_\#$-proofs and L-M-G proofs ; in the first class, each cut is either an N-cut or a G-C cut and in the second proof system, every cut is either a lift-and-project cut, or an N_0-cut or a G-C cut.

An important property of G-C cuts is the following: if $c^T x \leq \lfloor d \rfloor$ is a G-C cut for $Ax \leq b$, then

$$\exists \lambda \in R^{n+1} \text{ such that } \lambda \geq 0, \ c^T = \lambda^T A, \ \lambda^T b \leq d. \tag{20}$$

(We say that $c^T x \leq \lfloor d \rfloor$ is derived from $Ax \leq b$ with multipliers λ). Thus, each inequality in a G-C proof is derived only from $n+1$ or fewer previous inequalities. A similar property holds for matrix cuts.

Lemma 3.1 *If $c^T x \leq d$ is an N-cut derived as in (4), then $c^T x \leq d$ can be obtained with at most $\frac{1}{2}n(n+1)+1$ of the numbers α_{ij} and β_{ij} nonzero.*

Proof: Let $c^T x \leq d$ be an N-cut obtained as in (4). Let $p_{ij} = (b_i - a_i^T x)x_j$ and $q_{ij} = (b_i - a_i^T x)(1 - x_j)$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Then

$$d - c^T x = \sum_{i,j} \alpha_{ij} p_{ij} + \sum_{i,j} \beta_{ij} q_{ij} + \sum_j \lambda_j (x_j^2 - x_j)$$

for some values of $\alpha_{ij}, \beta_{ij} \geq 0$ and some λ_j. Let p'_{ij} stand for p_{ij} with x_j^2 replaced by x_j and let q'_{ij} be derived from q_{ij} in a similar manner. Then

$$d - c^T x = \sum_{i,j} \alpha_{ij} p'_{ij} + \sum_{i,j} \beta_{ij} q'_{ij}.$$

As the quadratic inequalities p'_{ij} and q'_{ij} lie in a $\frac{1}{2}n(n+1)+1$ dimensional space, Carathéodory's Theorem implies the desired result. $\square$

Lemma 3.1 remains true with N-cuts replaced by N_+-cuts. Both can be refined slightly; see Lemma 3.3 in Dash (2001).

It follows from the work of Cook, Coullard and Turán (1987) that a G-C proof of infeasibility can be transformed into a G-C proof of the same length with polynomially bounded size (in the length of the proof, and the encoding size of the problem). Hence, strong (exponential) lower bounds on the sizes of G-C proofs are equivalent to strong bounds on the lengths of such proofs (we do not know if the same is true for matrix-cuts). Chvátal, Cook and Hartmann (1989) proved that the length of G-C proofs can be exponential in the dimension of the problem; they obtained (essentially) a lower bound of $2^n/n$ on the length of G-C proofs of infeasibility of the following system of inequalities:

$$P_n = \{x \in Q_n \mid \sum_{i \in J} x_i + \sum_{i \notin J} (1 - x_i) \geq \frac{1}{2}, \text{ for all } J \subseteq \{1, \ldots, n\}\}. \tag{21}$$

Applying the technique used in Chvátal, Cook and Hartmann (1989), a lower bound of $2^n/n^2$ can be established on the lengths of N-proofs of infeasibility of P_n. However, as P_n has 2^n inequalities, the above lower bounds are not exponential in the size of P_n; we shall see true exponential bounds for L-M-G proofs in the next section.

The branch-and-cut method can be used to prove that a given inequality is satisfied by all 0-1 solutions of (17); this yields the notion of a "branch-and-cut proof". We define the length of a branch-and-cut proof to be the sum of the number of cuts and the number of non-leaf nodes (or the number of times we branch) in the proof. We will mainly deal with *branch-and-cut proofs of infeasibility* where $0^T x \leq -1$ is the last inequality in each branch. See Cook, Coullard and Turán (1987) for a discussion of the relationship of (cutting-plane) proofs of infeasibility to proofs of more general inequalities.

Cook and Hartmann (1990) presented, in the context of the traveling salesman problem, an exponential lower bound on the length of branch-and-cut proofs using Gomory-Chvátal cuts (the

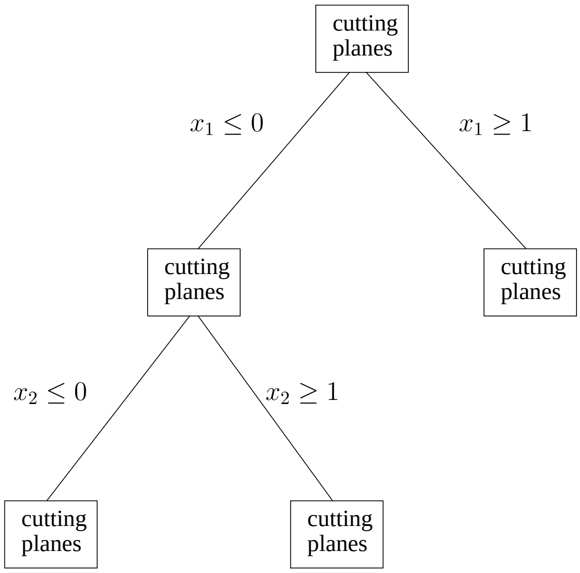

Figure 1: A branch-and-cut tree

actual result is more general). However, in their result, the lower bounds are exponential in the dimension of the problem (the number of cities squared), but not in the number of inequalities defining the problem (the standard linear programming relaxation of the TSP). Gu, Nemhauser, and Savelsbergh (1999) provided an exponential lower bound on the length of certain classes of branch-and-cut proofs of optimality for knapsack problems. The cutting planes they consider do not however form a complete system (thus any number of such cuts will not suffice); they show that exponentially many nodes have to be evaluted to prove optimality. We study branch-and-cut proofs which use the cutting-plane classes described in Section 2.

4 Interpolation and Cutting-Plane Proofs

The problem of determining if a system of linear inequalities $Ax \leq b$ has a 0-1 solution is NP-complete. Therefore, every algorithm which finds a 0-1 solution, or provides a certificate that no 0-1 solution exists, is expected to have super-polynomial time complexity. In fact, many believe that polynomial-size certificates of infeasibility (in the encoding size of A, b) do not always exist; this is the same as saying that $NP \neq coNP$. This question is far from being solved. However there has been progress in studying various restricted classes of certificates – formally, proofs in some proof system – and in showing exponential worst case complexity (size) for some classes. Achieving this goal for all proof systems would show that $NP \neq coNP$, and therefore that $P \neq NP$. (Note that exponential length branch-and-cut proofs have exponential size; we will focus on the lengths of such proofs).

Most of the literature on this subject deals with propositional proof systems, which are methods of writing down certificates of unsatisfiability of instances of SAT, i.e., of boolean formulae $\psi : \{0,1\}^n \rightarrow \{0,1\}$ in conjunctive normal form. Branch-and-cut proof systems, which we study here, can be viewed as propositional proof systems: ψ is satisfiable if and only if an associated linear system $A_\psi x \leq b_\psi$ has a 0-1 solution. A well-known propositional proof system is the *resolution proof system.* It is shown in Cook, Coullard and Turán (1987) that G-C proofs form a stronger proof system than resolution proofs. A similar statement is true for lift-and-project proofs (see Pudlák 1999) and N_0-proofs.

See Beame and Pitassi (1998) for a nice survey on propositional proof complexity; see also Pudlák (1999). Some of the methods developed to establish exponential worst-case complexity for proofs in various proof systems are the *bottleneck counting method* of Haken (1985), the *restriction method* of Ajtai (1994), and the *interpolation method.* Krajíček (1994, 1997) proposed the idea of using *effective interpolation* to etablish lower bounds on the lengths of proofs in different proof systems. This idea was first used by Razborov (1995), and independently, by Bonet, Pitassi, and Raz (1997), to prove exponential lower bounds for some proof systems (the latter paper contains bounds for a special case of G-C proofs). Both of these papers use a restriction of interpolation called *monotone interpolation.* Pudlák (1997) derived exponential lower bounds for lengths of G-C proofs using a generalization of monotone interpolation. We now discuss this technique in the context of cutting-plane proofs.

We will be interested only in infeasible 0-1 integer programs; we will use the phrase "integer program" to mean a problem without an objective function where we want to find 0-1 solutions of linear inequality systems. Assume that the following integer program in the disjoint sets of variables x, y and z is infeasible:

$$\begin{aligned} Ax + Cz &\leq e, \\ By + Dz &\leq f, \\ x, y, z &\text{ are 0-1 }. \end{aligned} \tag{22}$$

Then $0^T x + 0^T y + 0^T z \leq -1$ has a G-C proof $\mathcal{P}$ from (22). Let z' denote some 0-1 assignment to z. The system

$$\begin{aligned} Ax &\leq e - Cz', \\ By &\leq f - Dz', \\ x, y &\text{ are 0-1 }, \end{aligned} \tag{23}$$

obtained from (22), is still infeasible. Now, $\mathcal{P}$ can be modified to a proof $\mathcal{P}'$ of infeasibility of (23), with the same length and the property that (let $\mathcal{P}_i$ stand for the ith inequality in $\mathcal{P}$):

$$\text{if } \mathcal{P}_i \text{ is } a^T x + b^T y + c^T z \leq d \text{ then } \mathcal{P}'_i \text{ is } a^T x + b^T y \leq d - c^T z', \tag{24}$$

$$\mathcal{P}'_i \text{ is derived with the same multipliers as } \mathcal{P}_i. \tag{25}$$

In (23) we have two linear systems, with no variables in common, and at least one of the two has no 0-1 solutions. If $Ax \leq e - Cz'$ has no 0-1 solutions, then we can certainly construct a G-C proof of infeasibility (in the variables x). Can such a G-C proof be derived from the proof $\mathcal{P}'$? Pudlák (1997) showed that $\mathcal{P}'$ can be "split" in the following sense:
Given any z', it is possible to construct in polynomial time (in the size of $\mathcal{P}$), two G-C proofs, one involving x alone and the other involving only y, such that either the last inequality in the first proof is $0^T x \leq -1$ or the last in the second proof is $0^T y \leq -1$.
Hence, associated with each G-C proof $\mathcal{P}$, there is an algorithm $\mathcal{F}_{\mathcal{P}}(z)$, with running time bounded by a polynomial function of the size of $\mathcal{P}$, which takes as input a 0-1 z' and decides which of the two systems in (23) has no 0-1 solutions. This is called *effective interpolation* and $\mathcal{F}_{\mathcal{P}}(z)$ is called an *interpolating algorithm.*

Interpolating algorithms $\mathcal{F}_{\mathcal{P}}$ derived from different proof systems use restricted sets of boolean or arithmetic operations, and this allows their complexity to be analyzed in some cases. Strong lower bounds on the complexity of $\mathcal{F}_{\mathcal{P}}$ for various proof systems (including G-C proofs $\mathcal{P}$) have primarily been derived from Razborov's (1985) beautiful result on monotone circuit complexity, and an important extension proved independently by Pudlák (1997) and Cook and Haken (1999). (A result similar to Razborov's was proved independently by Andreev 1985). These results are stated in terms of monotone boolean circuits, and we will briefly dwell on this topic.

A boolean circuit can be thought of as a description of the elementary steps in an algorithm. It is often represented by a directed acyclic graph with three types of nodes: input nodes – nodes with no incoming arcs, a single output node – the only node with no outgoing arcs, and computation nodes (also called gates), each of which is labelled by one of the boolean functions $\wedge, \vee$, and $\neg$. For nodes i and j, an arc ij means that the value computed at i is used as an input to the gate or function at node j. A computation is represented by placing 0-1 values on the input gates, and then recursively applying the gates to inputs on incoming arcs, till the function at the output node is evaluated. Thus, an algorithm $\mathcal{A}$ can be represented by a class $\{C_n \mid n \geq 1\}$, where C_n is a boolean circuit with n input gates. For input size n, the running time of the algorithm equals the number of gates in C_n (called the *size* of C_n, denote this by $|C_n|$). If there is a polynomial $p(n)$ such that $|C_n| \leq p(n)$ for all $n \geq 0$, then $\mathcal{A}$ is a polynomial-time algorithm.

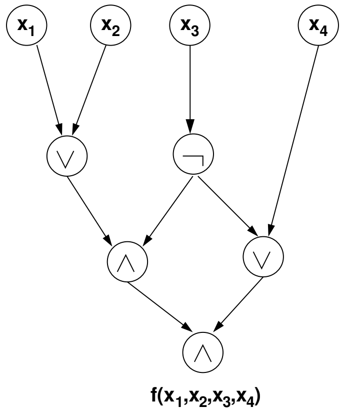

Figure 2: A boolean circuit

We define a *monotone function* to be a real-valued non-decreasing function $f : R^n \to R$, that is, if $x \leq y$ with x, y in R^n, then $f(x) \leq f(y)$. We refer to an application of a monotone function to given inputs as a "monotone computation", and define a monotone algorithm to be one whose elementary steps are monotone computations. Examples of monotone unary and binary functions (we call these *monotone operations*) are

$$tx, \quad r + x, \quad x + y, \quad \lfloor x \rfloor, \quad thr(x, -1) \tag{26}$$

where t is a non-negative constant, x and y are real variables, and r is a real constant; $thr(x, -1)$ is a *threshold function* which returns 0, if $x \leq -1$, and returns 1 otherwise. The functions $\wedge$ and $\vee$ are monotone operations, when their domain is restricted to $\{0, 1\}$. A *monotone boolean* *circuit* is one which uses only $\wedge$ gates and $\vee$ gates; a *monotone real circuit* is one with arbitary monotone operations as gates. We will only consider monotone circuits with 0-1 inputs and outputs.

Many important problems in the complexity class NP can be represented by monotone boolean functions (with 0-1 inputs and outputs). For example, consider $CLIQUE_{k,n}$ (say k is fixed), the function which takes as input n-node graphs (represented by incidence vectors of their edges) and returns 1 if the graph has a clique of size $\geq k$, and 0 otherwise. This is obviously monotone, as adding edges to a graph (changing some zeros to ones in the incidence vector) causes the maximum clique size to increase, and removing edges results in the maximum clique size decreasing. It turns out that every monotone boolean function can be computed by a monotone boolean circuit; Razborov showed that in contrast to the non-monotone case, strong lower bounds can be obtained on the sizes of monotone boolean circuits. Alon and Boppana (1987) strengthened his lower bound result.

Theorem 4.1 *(Razborov 1985, Alon and Boppana 1987) Let C_n be a monotone boolean circuit which takes as input graphs on n nodes (given as incidence vectors of edges), and returns 1 if the input graph contains a clique of size $k = n^{2/3}$, and 0 if the graph contains a coloring of size $k-1$ (and returns 0 or 1 for all other graphs). Then*

$$|C_n| \geq 2^{\Omega((n/\log n)^{1/3})}. \tag{27}$$

Thus any monotone boolean circuit computing $CLIQUE_{k,n}$, with k given as above, has exponentially many gates. This result is essentially true for monotone real circuits as well (Cook and Haken proved a slightly different statement).

Theorem 4.2 *(Pudlák 1997, Cook and Haken 1999) Let D_n be a monotone real circuit which has the same inputs and outputs as in Theorem 4.1. Then D_n must have exponentially many gates (the lower bound for $|C_n|$ given in Theorem 4.1 is also valid for $|D_n|$).*

Theorem 4.2 is the main result used in Pudlák's exponential lower bound on the complexity of G-C proofs, and for our bounds in the case of lift-and-project cuts. To use Theorem 4.2, Pudlák defined a system of inequalities, having the same form as (22), which in a sense encodes the problem of Theorem 4.1. We use a slightly modified inequality system, defined in the following way. Let $k = n^{2/3}$. Consider the set of nodes $N = \{1, \ldots, n\}$, with N^2 standing for $\{ij \mid 1 \leq i < j \leq n\}$. Let z be an $\binom{n}{2}$-vector of 0-1 variables, such that every 0-1 assignment to z corresponds to the incidence vector of a graph on n nodes. Let x be the 0-1 vector of variables $(x_i \mid i = 1, \ldots, n)$ and let y be the 0-1 vector of variables $(y_{ij} \mid i = 1, \ldots, n, j = 1, \ldots, k-1)$. We want to impose the conditions:

$$\text{the set of nodes } \{i \mid x_i = 1\} \text{ forms a clique of size } \geq k,$$

$$\text{for all } j \in \{1, \ldots, k-1\}, \text{ the set } \{i \mid y_{ij} = 1\} \text{ is a stable set.}$$

Thus, the variables y_{ij} define a mapping of nodes in a graph to $k-1$ colors in a proper colouring. To this end, add the inequalities

$$\sum_i x_i \geq k, \tag{28}$$

$$x_i + x_j \leq 1 + z_{ij}, \quad \forall i, j \in N^2, \tag{29}$$

$$\sum_j y_{ij} = 1, \quad \forall i \in N, \tag{30}$$

$$y_{is} + y_{js} \leq 2 - z_{ij}, \quad \forall i, j \in N^2 \text{ and } \forall s \in \{1, \ldots, k-1\}. \tag{31}$$

Let $Ax + Cz \leq e$ stand for the inequalities (28) and (29), and let $By + Dz \leq f$ stand for the inequalities (30) and (31). Let (22) stand for the above systems of inequalities along with the condition that x, y, z are 0-1 (more precisely, there is such a system for every n). Then any 0-1 solution of (22) corresponds to a graph which has both a clique of size k, and a coloring of size $k-1$. As this is not possible, (22) is infeasible. Note that (22) has $O(n^3)$ variables and constraints; for technical purposes we will also need the fact that $C \leq 0$. Now, because of Theorem 4.2, every monotone real circuit which takes a graph on n nodes as input (in the form of a 0-1 vector z') and decides whether $Ax \leq e - Cz'$ has no 0-1 solution or $By \leq f - Dz'$ has no 0-1 solution, has exponential size.

Pudlák showed that in the case of G-C proofs $\mathcal{P}$, a polynomial-time interpolating algorithm $\mathcal{F}_{\mathcal{P}}$, which uses monotone operations only (and can be mapped to a monotone real circuit), can be derived. This is called *monotone interpolation* and leads to exponential lower bounds on the complexity of G-C proofs. We now give Pudlák's (1997) monotone interpolation result for G-C proofs. We use a similar approach for our bound on L-M-G proofs later on.

Assume that the following integer program, in n variables and m inequalities, is infeasible:

$$Ax \leq e, \quad x \text{ is 0-1}, \tag{32}$$

$$By \leq f, \quad y \text{ is 0-1}, \tag{33}$$

and assume that x and y have no variables in common. For convenience, we assume that the initial inequalities in every cutting-plane proof of infeasibility from the above system are precisely the inequalities in the system.

Proposition 4.3 *(Pudlák 1997) Let $\mathcal{R}$ be a G-C proof of $0^T x + 0^T y \leq -1$ from (32) and (33). In polynomial time (in the size of $\mathcal{R}$), a G-C proof of infeasibility of either (32), or of (33), can be constructed from $\mathcal{R}$. Further, whether (32) has no 0-1 solution or (33) has no 0-1 solution can be determined using polynomially many monotone operations.*

Proof: Let $a_i^T x + b_i^T y \leq d_i$ be the ith inequality in $\mathcal{R}$ and call this $\mathcal{R}_i$. Now, $\mathcal{R}_1, \ldots, \mathcal{R}_m$ are just (32) and (33) and $\mathcal{R}_k$ (for some k) is precisely $0^T x + 0^T y \leq -1$. We can assume that $\mathcal{R}$ has integral inequalities. We say that $\mathcal{R}_i$ is derived from $\mathcal{R}_1, \ldots, \mathcal{R}_{i-1}$ if

$$a_i^T x + b_i^T y = \sum_j \lambda_{ij}(a_j^T x + b_j^T y) \text{ and } d_i = \lfloor \sum_j \lambda_{ij} d_j \rfloor,$$

where $\lambda_{ij} \geq 0$ for $j = 1, \ldots, i-1$.

We construct a sequence of inequalities $\mathcal{S}$ involving only x, and another sequence $\mathcal{T}$, involving only y, such that $\mathcal{S}_i$ and $\mathcal{T}_i$ together imply $\mathcal{R}_i$. Let I_i stand for $\{1, \ldots, i-1\}$. For $i = 1, \ldots, m$, if $\mathcal{R}_i$ involves only x, then set $\mathcal{S}_i$ to $\mathcal{R}_i$ and $\mathcal{T}_i$ to $0^T y \leq 0$, otherwise set $\mathcal{S}_i$ to $0^T x \leq 0$ and $\mathcal{T}_i$ to $\mathcal{R}_i$. Define subsequent terms of $\mathcal{S}$ and $\mathcal{T}$ as follows: for $i = m+1, \ldots, k$, if $\mathcal{R}_i$ is derived from $\mathcal{R}_j\,(j \in I_i)$ with the numbers $\lambda_{ij} \geq 0\,(j \in I_i)$, then let $\mathcal{S}_i$ be derived from $\mathcal{S}_j\,(j \in I_i)$ and let $\mathcal{T}_i$

be derived from $\mathcal{T}_j$ $(j \in I_i)$, with the same numbers λ_{ij}. If the right-hand sides of $\mathcal{S}_i$ and $\mathcal{T}_i$ are g_i and h_i respectively, we can conclude that

$$\mathcal{S}_i \equiv a_i^T x \leq g_i \quad \text{and} \quad \mathcal{T}_i \equiv b_i^T y \leq h_i \quad \text{with} \quad g_i + h_i \leq d_i. \tag{34}$$

Therefore the last inequalities in $\mathcal{S}$ and $\mathcal{T}$ are, respectively, $0^T x \leq g_k$ and $0^T y \leq h_k$. Since $d_k = -1$, one of g_k and h_k is at most -1, and we have a G-C proof of infeasibility of either (32) or (33). This is a polynomial-time construction.

To prove the second part of the theorem, observe that it suffices to compute $\mathcal{S}$: if $g_k \leq -1$, we know that (32) has no 0-1 solutions and we output 0, otherwise we know that (33) has no 0-1 solutions and we output 1. To compute $\mathcal{S}$, we only have to compute $g_i, i = 1, \ldots, k$, as we already know the left-hand sides of $\mathcal{S}$. Each g_i can be computed from $g_1, \ldots, g_{i-1}$ with at most $2(n+1)$ of the monotone operations in (26); this is because of (20). Finally we apply the threshold function in (26) to g_k. $\square$

Once again let (22) stand for the inequalities (28) - (31). Suppose $\mathcal{P}$ is a G-C proof of $0^T x + 0^T y + 0^T z \leq -1$ from (22). Now define a monotone interpolating algorithm $\mathcal{F}_{\mathcal{P}}(z)$ in the following way.

1. If z' is a 0-1 assignment to z, first compute the right-hand side of $Ax \leq e - Cz'$. As $C \leq 0$, this can be done with polynomially many monotone operations.

2. Compute $g_1, \ldots, g_k$ as in Proposition 4.3, and return $thr(g_k, -1)$.

Now, if $\mathcal{P}$ has length L, for every 0-1 z' $\mathcal{F}_{\mathcal{P}}$ decides whether z' has a clique of size k or a coloring of size $k-1$ with only $O(Ln^4)$ monotone operations. Then Theorem 4.2 implies the following.

Theorem 4.4 *(Pudlák 1997) Every G-C proof of unsatisfiability of the inequalities (28) - (31) has exponential length.*

We would like to use similar techniques for other cutting-plane systems. To this end, note that $\mathcal{F}_{\mathcal{P}}$ uses a number of properties of G-C cuts: properties (24) and (25) (we refer to these as properties (A) and (B)) and also the properties:

(C) *if $a^T x + b^T y \leq d$ is a G-C cut for $Ax \leq e, By \leq f$, and x, y have no variables in common, then there exist G-C cuts $a^T x \leq g$ and $b^T y \leq h$, such that $g + h \leq d$ and g and h can be computed in polynomial time,*

(D) *g can be computed from $Ax \leq e$ using polynomially many monotone operations.*

Though property (C) is trivially true in the case of G-C cuts, showing it for the other classes of cuts is not completely straightforward. We will see in the next section that most of the classes of cuts given in Section 2 satisfy properties (A), (B) and (C) (with some caveats); these three properties imply the existence of the effective interpolation property. The main difficulty is in showing property (D); this is required for monotone interpolation and exponential lower bounds, at least in the above framework.

It follows from results in Chvátal (1973) that G-C proofs simulate branch-and-bound proofs of infeasibility. More precisely,

Proposition 4.5 *(Chvátal 1973). If a 0-1 integer program has a branch-and-bound proof of infeasibility with k nodes (including leaf nodes), then it has a G-C proof of infeasibility with length k.*

This immediately implies that every branch-and-bound proof of infeasibility of (28) - (31) has exponential length. We will generalize Proposition 4.5 in the next section.

5 Bounds for other proof systems

In this section we present the main result of this paper, which is that L-M-G branch-and-cut proofs of infeasibility of the system (28) - (31) have exponential length. We will approach this result by first showing that some stronger proof systems have the effective interpolation property.

Pudlák showed that $N_{\#}$-proofs have the effective interpolation property; this however does not yield an exponential lower bound on the complexity of these proofs. Recall from Section 3 that these proofs combine N-cuts and G-C cuts. The main part of his result involves showing that N-cuts have property (C).

Proposition 5.1 *(Pudlák 1999) Let $\mathcal{R}$ be an $N_{\#}$-proof of $0^T x \leq -1$ from (32) and (33). In polynomial time (in the size of $\mathcal{R}$), an $N_{\#}$-proof of infeasibility of either (32), or of (33), can be constructed from $\mathcal{R}$.*

We now proceed to extend the above result to N_+-proofs (more precisely N_*-proofs) thus answering a question which is mentioned as being unsolved by Pudlák (1999, page 11).

Proposition 5.2 *Let $\mathcal{R}$ be an N_*-proof of $0^T x \leq -1$ from (32) and (33). In polynomial time (in the size of $\mathcal{R}$), an N_*-proof of infeasibility of either (32), or of (33), can be constructed from $\mathcal{R}$.*

Proof: We can assume that all inequalities in $\mathcal{R}$ are integral and N_+-cuts for the previous ones in $\mathcal{R}$. G-C cuts can be handled as in Proposition 4.3.

Let $\mathcal{R}$ be as in Proposition 4.3 (only $\mathcal{R}$ is an N_+-proof of infeasibility). We construct two N_+-proofs $\mathcal{S}$ and $\mathcal{T}$ with the same length as $\mathcal{R}$. Let the first m terms in $\mathcal{S}$ and $\mathcal{T}$ be as in Proposition 4.3. By definition, if $\mathcal{R}_j$ is $a_j^T x + b_j^T y \leq d_j$ and $i = m+1$, then for all $j < i$

$$\mathcal{S}_j \equiv a_j^T x \leq g_j \text{ and } \mathcal{T}_j \equiv b_j^T y \leq h_j \text{ with } g_j + h_j \leq d_j. \tag{35}$$

Assume that we have obtained $\mathcal{S}_j$ and $\mathcal{T}_j$ satisfying (35) for all $j < i$, where i is some number greater than m. Let P_1 be the polytope defined by $\mathcal{S}_1, \ldots, \mathcal{S}_{i-1}$. Similarly, let P_2 be defined by $\mathcal{T}_1, \ldots, \mathcal{T}_{i-1}$. Now, if P is defined by $\mathcal{R}_1, \ldots, \mathcal{R}_{i-1}$, then $P_1 \cap P_2 \subseteq P$.

It follows that $a_i^T x + b_i^T y \leq d_i$ is valid for $N_+(P_1 \cap P_2)$. By Lemma 2.8 and Carathéodory's Theorem, we have

$$a_i^T x + b_i^T y = \sum_{j \in J} \alpha_j p_j^T x + \sum_{k \in K} \beta_k q_k^T y \text{ and } \sum_{j \in J} \alpha_j r_j + \sum_{k \in K} \beta_k s_k \leq d_i, \tag{36}$$

where $p_j^T x \leq r_j$ $(j \in J)$ are $N_+(P_1)$-cuts and $q_k^T x \leq s_k$ $(k \in K)$ are $N_+(P_2)$-cuts and $\alpha_j \geq 0$ and $\beta_k \geq 0$ for all $j \in J$ and $k \in K$. Adding separately the $N_+(P_1)$-cuts and the $N_+(P_2)$-cuts, we see that there are there are real numbers g_i' and h_i' such that

$$a_i^T x \leq g_i' \text{ is an } N_+(P_1)\text{-cut and } b_i^T y \leq h_i' \text{ is an } N_+(P_2)\text{-cut}, \tag{37}$$

and $g_i' + h_i' \leq d_i$. The numbers g_i' and h_i' can be computed as

$$g_i' = \max\{a_i^T x \,|\, (x,y) \in N_+(P_1)\}, \quad h_i' = \max\{b_i^T y \,|\, (x,y) \in N_+(P_2)\}. \tag{38}$$

To get the ith terms of $\mathcal{S}$ and $\mathcal{T}$, we compute g_i' and h_i' as in (38), by solving two semidefinite programs (see Theorem 2.3 and the discussion following it). As these are not necessarily integers, we round them down to get g_i and h_i; we have completed the construction of the ith terms in $\mathcal{S}$ and $\mathcal{T}$. Repeating this process we get, as the last terms in $\mathcal{S}$ and $\mathcal{T}$, $0^T x \leq g_k$ and $0^T x \leq h_k$ where at least one of g_k or h_k is bounded above by -1. □

In the proof above, if we replace $N_+(P)$ by $N(P)$, we get Pudlák's result, Proposition 5.1, by combining with Proposition 4.3. We can also use $N_0(P)$ instead of $N_+(P)$ and get a result analogous to Proposition 5.1 in the case where we have proofs using N_0-cuts and G-C cuts. Proposition 5.2 essentially shows that N_+-cuts have property (C). We now present an effective interpolation property for N_*-proofs.

Theorem 5.3 *Let (22) stand for the system (28) - (31). If $\mathcal{P}$ is an N_*-proof of infeasibility of (22), then there is an algorithm $\mathcal{F}_{\mathcal{P}}(z)$ with the following properties:*
(i) if z' is a 0-1 vector, then $\mathcal{F}_{\mathcal{P}}$ computes 0 if $Ax \leq e - cz'$ is infeasible, and 1 otherwise;
(ii) $\mathcal{F}_{\mathcal{P}}$ performs monotone computations only;
(iii) The running-time of $\mathcal{F}_{\mathcal{P}}$ is bounded above by a polynomial function of the length of $\mathcal{P}$.

Proof: Let $\mathcal{P}$ be an N_*-proof of $0^T x + 0^T y + 0^T z \leq -1$ from (22). By Lemma 2.4, if $\mathcal{P}'$ is defined by (24) then $\mathcal{P}'$ is an N_*-proof of the infeasibility of (23). In fact, properties (A) and (B) follow directly from definition: an N_+-cut is a linear combination of quadratic terms, just replace z by z' in every quadratic term. Now, let $\mathcal{R}$ denote $\mathcal{P}'$; as in Proposition 5.2, obtaining the N_*-proof $\mathcal{S}$ suffices to decide whether $Ax \leq e - Cz'$ is feasible or not. We proceed as in the case of G-C proofs and first compute $e - Cz'$ and then the numbers $g_1, g_2, \ldots, g_k$ described in Proposition 5.2, and finally $thr(g_k, -1)$ to get $\mathcal{F}_{\mathcal{P}}(z')$.

The numbers $g_1, g_2, \ldots, g_k$ can be obtained by monotone *computations.* To see this, observe that the following computation

$$\max\{a_i^T x \,|\, x \in N_+(P)\},$$
$$P = \{x \in Q \,|\, a_1^T x \leq g_1, \ldots, a_{i-1}^T x \leq g_{i-1}\}, \tag{39}$$

performed in (38), is monotone in the inputs $g_1, g_2, \ldots, g_{i-1}$. If the numbers $g_1, \ldots, g_{i-1}$ are increased, then P is larger, and so is $N_+(P)$, and the maximum in (39) increases.

Finally, assume (22) has m inequalities and n variables. Computing $e - Cz'$ requires at most $2mn$ monotone operations ($C \leq 0$). The numbers $g_1, g_2, \ldots, g_k$ each require a monotone computation of the form (39). Hence, the number of monotone computation steps is at most $2nL$, where L is the length of $\mathcal{P}$ (here $m \leq L$). □

Theorem 5.3 does not yield an exponential lower bound on the length of N_*-proofs as all monotone computations do not have a bounded number of inputs (they are not monotone operations, for example). But we can prove:

Theorem 5.4 *Let $\mathcal{I}_n$ stand for the inequalities (28) - (31). Every lift-and-project proof of infeasibility of $\mathcal{I}_n$ has exponential length (in n).*

Proof: Let $\mathcal{O}$ be a lift-and-project proof of length L of the infeasibility of $\mathcal{I}_n$ for a given integer n. Note that $\mathcal{I}_n$ has fewer than $p(n) = cn^3$ variables and constraints for some constant $c > 0$. Every $\mathcal{O}_i$ is a lift-and-project cut (say with respect to the variable x_k; this variable changes with i) for $\mathcal{O}_1, \ldots, \mathcal{O}_{i-1}$. Therefore $\mathcal{O}_i$ is equal to $\alpha q_1 + \beta q_2 + \lambda(x_k^2 - x_k)$ for some $\alpha, \beta \geq 0$ and some λ, where q_1 and q_2 are inequalities implied by $\mathcal{O}_1, \ldots, \mathcal{O}_{i-1}$. Define a sequence $\mathcal{P}$ of length at most $3L$ by

$$\mathcal{P}_{3i-2} \equiv q_1,\ \mathcal{P}_{3i-1} \equiv q_2,\ \mathcal{P}_{3i} \equiv \mathcal{O}_i. \tag{40}$$

As lift-and-project cuts are also N_0-cuts, $\mathcal{P}$ is an N_0-cutting-plane proof of $0^T x + 0^T y + 0^T z \leq -1$ with the special property that each inequality is either a non-negative linear combination of $p(n) + 1$ previous inequalities in $\mathcal{P}$ ($\mathcal{I}_n$ has at most $p(n)$ variables) or is an N_0-cut derived from at most two previous inequalities.

If in Theorem 5.3, we replace N_* by N_0, we get an interpolating algorithm $\mathcal{F}_{\mathcal{P}}$ which performs only monotone operations. To see this, let z' be some 0-1 assignment to z, and let $\mathcal{R} \equiv \mathcal{P}'$ where $\mathcal{P}'$ is defined as in (24). As in the proof of Proposition 5.2 define the proofs $\mathcal{S}$ and $\mathcal{T}$ from $\mathcal{R}$ with the following property. If $\mathcal{R}_i = \lambda_1 \mathcal{R}_1 + \cdots + \lambda_{i-1}\mathcal{R}_{i-1}$ for non-negative numbers $\lambda_1, \ldots, \lambda_{i-1}$, then $\mathcal{S}_i$ equals $\lambda_1 \mathcal{S}_1 + \cdots + \lambda_{i-1}\mathcal{S}_{i-1}$ and $\mathcal{T}_i$ equals $\lambda_1 \mathcal{T}_1 + \cdots + \lambda_{i-1}\mathcal{T}_{i-1}$. If $\mathcal{R}_i$ is the inequality $a_i^T x + b_i^T y \leq d_i$ and is an N_0-cut derived from two previous inequalities, say $\mathcal{R}_j$ and $\mathcal{R}_l$, then $\mathcal{S}_i$ is the inequality $a_i^T x \leq g_i$ such that

$$g_i = \max\{a_i^T x \mid x \in N_0(P)\},$$

$$P = \{x \in Q \mid a_j^T x \leq g_j,\ a_l^T x \leq g_l\}. \tag{41}$$

Similarly $\mathcal{T}_i$ is the inequality $b_i^T y \leq h_i$ derived as an N_0-cut from $b_j^T y \leq h_j$ and $b_l^T y \leq h_l$; also $g_i + h_i \leq d_i$. Hence, if $\mathcal{P}$ has k inequalities, then either $g_k \leq -1$ or $h_k \leq -1$. Also, $g_1, g_2, \ldots, g_k$ can be computed by monotone operations only. Either g_i is the non-negative linear combination of $p(n) + 1$ previous numbers from $g_1, \ldots, g_{i-1}$ (this requires $2(p(n) + 1)$ monotone operations) or g_i is computed as in (41), which is a monotone operation. Combining the facts above, we can construct a real monotone circuit D_n, as in Theorem 4.2, with $O(Ln^3)$ gates. Hence L is exponential (the bound in (27) divided by n^3) and the result follows. $\square$

Theorem 5.4 implies that every cutting-plane algorithm based only on lift-and-project cuts requires exponential time (in the worst-case) to solve $\mathcal{I}_n$. For example, the algorithm given in Theorem 3.1 of Balas, Ceria, Cornuéjols (1993), which the authors call the "specialized cutting plane algorithm", has exponential time complexity. The next result implies that N_0-cutting-plane proofs of the infeasibility of $\mathcal{I}_n$, given in Theorem 5.4, must have exponential length.

Lemma 5.5 *Let $\mathcal{P}$ be an N_0-proof of $c^T x \leq d$, from some polytope in Q_n, of length L. There is a lift-and-project cutting-plane proof of $c^T x \leq d$ of length at most $(n+2)L$.*

Proof: Let $a^T x \leq b$ be an inequality in the proof. Let $P = \{x \mid Ax \leq b\}$ be the polytope defined by the inequalities used in deriving $a^T x \leq b$ as an N_0-cut. By Lemma 2.6, $N_0(P) = \cap_i P_i$, where P_i is the lift-and-project operator with respect to the variable x_i. Therefore $N_0(P)$ is completely defined by the inequalities defining the polytopes P_i. Hence, by Carathéodory's Theorem, $a^T x \leq b$ is a nonnegative linear combination of $n + 1$ inequalities $g_1^T x \leq h_1, \ldots, g_{n+1}^T x \leq h_{n+1}$, where for $i = 1, \ldots, n + 1$, $g_i^T x \leq h_i$ is valid for some P_k ($1 \leq k \leq n$). It follows that $a^T x \leq b$ is a nonnegative linear combination of $n + 1$ lift-and-project cuts for P. Let $\mathcal{R}$ be a sequence of inequalities such that $a^T x \leq b$ in $\mathcal{P}$ is replaced by the inequalities $g_1^T x \leq h_1, \ldots, g_{n+1}^T x \leq h_{n+1}$ and $a^T x \leq b$ (in order). In $\mathcal{R}$, every inequality is either a nonnegative linear combination of previous inequalities or a lift-and-project cut derived from previous inequalities; hence $\mathcal{R}$ is a lift-and-project cutting-plane proof of length at most $(n+2)L$. $\square$

Combining Theorem 4.2, Proposition 4.3, Theorem 5.4 and Lemma 5.5, we get the following theorem.

Theorem 5.6 *Let $\mathcal{I}_n$ be as in Theorem 5.4. Then any cutting-plane proof of infeasibility which uses only N_0-cuts, lift-and-project cuts and G-C cuts must have exponential length, i.e., length at least $e(n)/h(n)$ where $e(n)$ is the exponential function in Theorem 4.1, and $h(n)$ is some polynomial function of n.*

We refer to the cutting-plane proofs in Theorem 5.6 as L-M-G proofs. To get an exponential lower bound on the length of branch-and-cut proofs for $\mathcal{I}_n$, we prove the following lemma.

Lemma 5.7 *Let $P \subseteq Q_n$ be a polytope which does not contain 0-1 points. Let $\mathcal{P}$ be an L-M-G branch-and-cut proof of $0^T x \leq -1$ from P, with m cutting planes and k branches. Then there is an L-M-G cutting-plane proof of $0^T x \leq -1$ with length exactly $m+k$.*

Proof: As discussed earlier, every lift-and-project cut is an N_0-cut; so we can assume that the cuts in the proof are either N_0-cuts or Gomory-Chvátal cuts. Assume $\mathcal{P}$ has exactly one branch and s inequalities in the left branch and t inequalities in the right branch. Further assume that the very first step in the branch-and-cut proof consists of branching on the variable x_1. In the the left branch, we impose the condition $x_1 = 0$ and in the right branch the condition $x_1 = 1$.

Let the inequalities in the left branch be $a_1^T x \leq b_1, a_2^T x \leq b_2, \ldots$. Let $a_1^T x \leq b_1$ be an N_0-cut for P and the inequality $x_1 = 0$. We can assume that $a_1^T x \leq b_1$ is an N_0-cut for $P \cap \{x \,|\, x_1 = 0\}$, i.e., $a_1^T x \leq b_1$ is an $N_0(P \cap \{x \,|\, x_1 = 0\})$-cut. From Lemma 2.4 and the subsequent discussion, we know that $a_1^T x \leq b_1$ can be "rotated" to get an N_0-cut for P of the form $a_1^T x + \alpha_1 x_1 \leq b_1$ for some number α_1. To continue this process, for $i = 2, \ldots, s$ do the following: if $a_i^T x \leq b_i$ is an N_0-cut from P, $x_1 = 0$, and the inequalities $a_1^T x \leq b_1, \ldots, a_{i-1}^T x \leq b_{i-1}$, let P_{i-1} equal P intersected with the inequalities $a_1^T x + \alpha_1 x_1 \leq b_1, \ldots, a_{i-1}^T x + \alpha_{i-1} x_1 \leq b_{i-1}$. Then $a_i^T x \leq b_i$ is an $N_0(P_{i-1} \cap \{x \,|\, x_1 = 0\})$-cut and can be rotated to get an $N_0(P_{i-1})$-cut of the form $a_i^T x + \alpha_i x_1 \leq b_i$. This rotation process can also be performed if $a_i^T x \leq b_i$ is a Gomory-Chvátal cut. Similarly an inequality $c_i^T \leq d_i$ in the right branch gets rotated to $c_i^T x + \beta_i(1 - x_1) \leq d_i$ for some β_i.

The last inequality in the left branch is mapped to $0^T x + \alpha_s x_1 \leq -1$ and the last inequality in the right branch is mapped to $0^T x + \beta_t(1 - x_1) \leq -1$. Multiplying the first of these two inequalities by $(1 - x_1)$ and the second by x_1, replacing x_1^2 by x_1, and adding, we get the inequality $0^T x \leq -1$ as an N_0-cut. Observe that we have removed a branch and replaced it by an N_0-cut, to get a cutting-plane proof of infeasibility of length $s + t + 1$.

If a branch-and-cut proof has many branches, we can start from the lowermost branches, and recursively eliminate the branches by adding an extra N_0-cut for every branch eliminated. This completes the proof. $\square$

The exponential lower bounds on the length of L-M-G branch-and-cut proofs follows immediately from Theorem 5.6.

Theorem 5.8 *Every L-M-G branch-and-cut proof of infeasibility of $\mathcal{I}_n$ given in Theorem 5.4 has exponential length.*

6 Some open questions

The main open question we would like to set down here is:

Question 6.1 *Do N_+-proofs of infeasibility have exponential size in the worst-case ? What about cutting-plane proofs using split cuts ? What about proofs of the system $\mathcal{I}_n$ given in Proposition 5.4 ?*

The first part of Question 6.1 is presented as an unsolved question in Beame and Pitassi (1998) and Pudlák (1999). This question is also examined in Grigoriev, Hirsch and Pasechnick (2002), who show that an extension of the N_+-proof system is strong in the sense that there are short proofs for $\mathcal{I}_n$ in this extended system. Proving exponential bounds on the lengths of such proofs will obviously yield similar bounds on their sizes; note that we do not know if the sizes and lengths of N_+-proofs and split proofs are polynomially related as in the case of G-C proofs.

Let $Ax \leq b$ define a polyhedron P contained in the n-dimensional 0-1 cube. Suppose $c^T x \leq d$ is valid for P_I. As the Chvátal rank of P is bounded by $3n^2 \log n$ (see Eisenbrand and Schulz 1999), there is a Gomory-Chvátal cutting-plane proof of $c^T x \leq d$, from $Ax \leq b$, of length bounded above by $n^{O(n^2 \log n)}$. This follows from results in Chvátal, Cook and Hartmann (1989). An interesting question is the following.

Question 6.2 *If $c^T x \leq d$ is an N-cut (N_+-cut) for $Ax \leq b$, a polytope in Q_n, does there always exist a Gomory-Chvátal cutting-plane proof of $c^T x \leq d$ from $Ax \leq b$ with length bounded by a polynomial function of n ?*

If the answer to this question is positive, we will say that the Chvátal proof system (defined by Gomory-Chvátal cuts) *polynomially simulates* the N-cut proof system. Let $f(n)$ be the bound in question 6.2; if we replace N-cuts by N_+-cuts, let the bound be $f_+(n)$. We do not know the answer to the above question, i.e., we do not know if either of $f(n)$ or $f_+(n)$ is a polynomial.

However, we can say the following.

Proposition 6.3 *If $f(n)$ is a polynomial function, then the Chvátal rank of polytopes in Q_n, will be bounded above by $nf(n)$, also a polynomial in n. Further, there will exist infeasible integer programs, with polynomially many (in n) variables, but requiring an exponential length N-cutting-plane proof.*

This is easy to see. Firstly, for any polytope P, $P^{(f(n))}$ is contained in $N(P)$. Further, if $f(n)$ is polynomial, then a polynomial-length N-proof can be translated into a polynomial-length Chvátal-proof, and, if the final inequality is $0^T x \leq -1$, into a polynomial-size Chvátal-proof by results in Cook, Coullard, and Turán (1987). Then Pudlák's result, that for an infinite class of integer programs, every Chvátal-proof of infeasibility must have exponentially length (and size), would imply the second statement.

We can then say that $f(n) > 1$ as there are examples of polytopes with Chvátal rank greater than n (see Eisenbrand and Schulz 1999). Also

$$f_+(n) \geq \lceil \log_2(n-1) \rceil;$$

this follows from Hartmann (1988, Theorem 3.1.1), where the Chvátal rank of the fractional stable set polytope of the complete graph is shown to equal the right-hand side of the above equation (the N_+-rank is 1 in this case).

Consider the reverse problem.

Question 6.4 *Is it possible to polynomially simulate Gomory-Chvátal cuts by N-cuts or N_+-cuts.*

Again letting $g(n)$ ($g_+(n)$) stand for the maximum length of an N-cut (N_+-cut) based proof of a Gomory-Chvátal cut, it turns out that $g(n)$ or $g_+(n)$ is at least n. This is because given $x_1 + \cdots + x_n \geq \frac{1}{2}$, any N_+-proof of $x_1 + \cdots + x_n \geq 1$ has length at least n (see Cook and Dash 2001), but $x_1+\cdots+x_n \geq 1$ is a G-C cut. (In fact n N_+-cuts are enough to derive $x_1+\cdots+x_n \geq 1$; combining this with the polynomial simulation of resolution by Gomory-Chvátal cutting planes given in Cook, Coullard, and Turán 1987, we have a polynomial simulation of resolution by N-cuts or N_+-cuts.)

Let GC_2 stand for the restriction of the G-C proof system, where only division by 2 is allowed. This means that while taking nonnegative combinations of inequalities, we are only allowed to multiply inequalities with multiples of $\frac{1}{2}$. Buss and Clote (1996) proved the following interesting result.

Proposition 6.5 *GC_2 polynomially simulates the G-C proof system for 0-1 integer programs.*

This means that Question 6.4 is equivalent to

Question 6.6 *Given an inequality $c^T x \geq d - \frac{1}{2}$ where c and d are integral, does there exist a polynomial-length N-proof (or N_+-proof) of the inequality $c^T x \geq d$?*

We believe that any N_+-proof of $x_1 + \cdots + x_n \geq \lfloor \frac{n}{2} \rfloor$, from

$$x_1 + \cdots + x_n \geq \lfloor \frac{n}{2} \rfloor - \frac{1}{2},$$

is exponential in n. We have not been able to demonstrate this fact. An almost identical conjecture is stated in Grigoriev, Hirsch, and Pasechnik (2002).

Acknowledgements

I would like to thank Bill Cook for suggesting the problems dealt with in this paper, and George Nemhauser for pointing out the result on simulation of branch-and-cut proofs of infeasibility by G-C proofs given in Chvátal (1973). I would also like to thank Oktay Günlük for suggesting the simplified version of Pudlák's inequalities given in (28) - (31).

References

[1] Ajtai, M. 1994. The complexity of the pigeonhole principle. *Combinatorica* **14** 417–433.

[2] Alon, N., R. Boppana. 1987. The monotone circuit complexity of Boolean functions, *Combinatorica* **7** 1–22.

[3] Andreev, A. E. 1985. On a method for obtaining lower bounds for the complexity of individual monotone functions. *Soviet Mathematics - Doklady* **31** 530–534.

[4] Balas, E. 1979. Disjunctive programming. *Annals of Discrete Mathematics* **5** 3–51.

[5] Balas, E., S. Ceria, G. Cornuéjols. 1993. A lift-and-project cutting plane algorithm for mixed 0-1 programs. *Mathematical Programming* **58** 295–324.

[6] Balas, E., S. Ceria, G. Cornuéjols, G. Natraj. 1996. Gomory cuts revisited. *Operations Research Letters* **19** 1–9.

[7] Beame, P., T. Pitassi. 1998. Propositional proof complexity: past, present, and future. *Bulletin of the European Association for Theoretical Computer Science* **65** 66–89.

[8] Bixby, R. E., M. Fenelon, Z. Gu, E. Rothberg, R. Wunderling. 2000. MIP: Theory and practice – closing the gap. M. J. D. Powell, S. Scholtes, eds., *System Modelling and Optimization: Methods, Theory, and Applications*, Kluwer Academic Publishers, 19–49.

[9] Bonet, M., T. Pitassi, R. Raz. 1997. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic* **62** 708–728.

[10] Boppana, R., M. Sipser. 1990. The complexity of finite functions. *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity*, MIT Press/Elsevier, 757–804.

[11] Caprara, A., A. Letchford. On the separation of split cuts and related inequalities, to appear in *Mathematical Programming.*

[12] Chvátal, V. 1973. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics* **4** 305–337.

[13] Chvátal, V. 1984. Cutting-plane proofs and the stability number of a graph, Report Number 84326-OR, Insitut für Ökonometrie und Operations Research, Universität Bonn, Bonn, Germany.

[14] Chvátal, V. 1985. Cutting planes in combinatorics. *European Journal of Combinatorics* **6** 217-226.

[15] Chvátal, V., W. Cook, M. Hartmann. 1989. On cutting plane proofs in combinatorial optimization. *Linear Algebra and its Applications* **114/115** 455–499.

[16] Cook, S. A., A. Haken. 1999. An exponential lower bound for the size of monotone real circuits. *Journal of Computer and System Sciences* **58** 326–335.

[17] Cook, W., C. R. Coullard, Gy. Turán. 1987. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics* **18** 25–38.

[18] Cook, W., Cunningham, W., Pulleyblank, W., Schrijver, A.: 1998. Combinatorial Optimization, Wiley, New York.

[19] Cook, W., S. Dash. 2001. On the matrix-cut rank of polyhedra. *Mathematics of Operations Research* **26** 19–30.

[20] Cook, W., M. Hartmann. 1990. On the complexity of branch and cut methods for the traveling salesman problem. P. D. Seymour, W. Cook, eds., *Polyhedral Combinatorics, Vol. 1, DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 75–82.

[21] Cornuéjols. G., Y. Li. 2001. Elementary closures for integer programs. *Operations Research Letters* **28** 1–8.

[22] Cornuéjols, G., Y. Li. 2002. A connection between cutting plane theory and the geometry of numbers. *Mathematical Programming, Series A* **93** 123–127.

[23] Dash, S. 2001. *On the matrix cuts of Lovász and Schrijver and their use in integer programming*, Ph.D. Thesis, Rice University, Houston, Texas.

[24] Eisenbrand, F. 1999. On the membership problem for the elementary closure of a polyhedron. *Combinatorica* **19** 297–300.

[25] Eisenbrand, F., A. S. Schultz. 1999. Bounds on the Chvátal rank of polytopes in the 0/1-cube. G. Cornuéjols, R. E. Burkard, G. J. Woeginger, eds., *Integer Programming and Combinatorial Optimization, 7th International IPCO Conference* , Springer, Berlin, 137–150.

[26] Grigoriev, D., E. A. Hirsch, D. V. Pasechnik. 2002. Complexity of semi-algebraic proofs. *Lecture Notes in Computer Science*, Vol. 2285, 419–430.

[27] Goemans, M. X., L. Tunçel. 2001. When does the positive semidefiniteness constraint help in lifting procedures ? *Mathematics of Operations Research* **26** 796–815.

[28] Gomory, R. E. 1958. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society* **64** 275–278.

[29] Gomory, R. E. 1960. An algorithm for the mixed integer problem, RM-2597, The Rand Corporation.

[30] Haken, A. 1985. The intractability of resolution. *Theoretical Computer Science* **39** 297–308.

[31] Hartmann, M. 1988. *Cutting Planes and the complexity of the integer hull*, Ph.D. Thesis, Department of Operations Research and Industrial Engineering, Cornell University, Ithaca, New York.

[32] Horn, R. A., C. R. Johnson. 1985. Matrix Analysis, Cambridge University Press.

[33] Jeroslow, R. G. 1974. Trivial integer programs unsolvable by branch-and-bound. Mathematical Programming **6** 105–109.

[34] Krajíček, J. 1994. Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic* **59** 73–86.

[35] Krajíček, J. 1997. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic* **62** 457–486.

[36] Laurent, M. 2001. Tighter linear and semidefinite relaxations for max-cut based on the Lovász-Schrijver lift-and-project procedure. *SIAM Journal on Optimization* **12** 345–375.

[37] Lovász, L. 1994. Stable sets and polynomials. *Discrete Mathematics* **124** 137–153.

[38] Lovász, L., A. Schrijver. 1991. Cones of matrices and set-functions and 0-1 optimization. *SIAM Journal on Optimization* **1** 166–190.

[39] Marchand, H., L. A. Wolsey. 2001. Aggregation and Mixed Integer Rounding to solve MIPs. *Operations Research* **49** 363–371.

[40] Nemhauser, G., L. A. Wolsey. 1990. A recursive procedure to generate all cuts for 0-1 mixed integer programs. *Mathematical Programming* **46** 379–390.

[41] Pudlák, P. 1997. Lower bounds for resolution and cutting plane proofs and monotone computations. *Journal of Symbolic Logic* **62** 981–998.

[42] Pudlák, P. 1999. On the complexity of propositional calculus. *Sets and Proofs, Invited papers from Logic Colloquium 1997*, Cambridge University Press, 197–218.

[43] Razborov, A. A. 1985. Lower bounds for the monotone complexity of some boolean functions. *Dokladi Akademii Nauk SSSR* **281** 798–801 (in Russian). English translation in: *Soviet Mathematics - Doklady* **31** (1985) 354–357.

[44] Razborov, A. A. 1995. Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic. *Izvestiiya of the RAN* **59** 201–224.

[45] Schrijver, A. 1980. On cutting planes. M. Deza, I. G. Rosenberg, eds., *Combinatorics 79 Part II, Annals of Discrete Mathematics 9*, North Holland, Amsterdam, 291–296.

[46] Schrijver, A. 1986. *Theory of Linear and Integer Programming*, Wiley, Chichester, U.K.

[47] Sherali, H. D., W. P. Adams. 1990. A hierarchy of relaxations between the continuous and convex representations for zero-one programming problems. *SIAM Journal on Discrete Mathematics* **3** 411–430.