Cutting planes, connectivity, and threshold logic

Samuel R. Buss* Peter Clote†

March 6, 2002

Abstract

Originating from work in operations research the cutting plane refutation system CP is an extension of resolution, where unsatisfiable propositional logic formulas in conjunctive normal form are recognized by showing the non-existence of boolean solutions to associated families of linear inequalities. Polynomial size CP proofs are given for the undirected s-t connectivity principle. The subsystems CP_q of CP, for $q \geq 2$, are shown to be polynomially equivalent to CP, thus answering problem 19 from the list of open problems of [8]. We present a normal form theorem for CP_2-proofs and thereby for arbitrary CP-proofs. As a corollary, we show that the coefficients and constant terms in arbitrary cutting plane proofs may be exponentially bounded by the number of steps in the proof, at the cost of an at most polynomial increase in the number of steps in the proof. The extension $CPLE^+$, introduced in [9] and there shown to p-simulate Frege systems, is proved to be polynomially equivalent to Frege systems. Lastly, since linear inequalities are related to threshold gates, we introduce a new threshold logic and prove a completeness theorem.
Mathematics Subject Classification: 03B05, 03F07, 03F20, 90C10.

1 Introduction

The cutting plane system CP [12, 13] is a refutation system for propositional logic formulas in conjunctive normal form CNF. In CP, the truth values TRUE and FALSE are interpreted by 1 and 0 and propositional formulas are expressed by systems of linear inequalities. An unsatisfiable CNF formula such as

$$(x \vee y) \wedge (\overline{x} \vee y) \wedge (x \vee \overline{y}) \wedge (\overline{x} \vee \overline{y})$$

*Supported in part by NSF grant DMS-9205181 and by US-Czech Science and Technology Grant 93-205. Mailing address: sbuss@ucsd.edu, Department of Mathematics, University of California at San Diego, La Jolla CA 92093.

†Partially supported by NSF grant CCR-9102896 and by US-Czech Science and Technology Grant 93-205. Mailing address: clote@cs.bc.edu, Department of Computer Science, Boston College, Chestnut Hill MA 02167.

is represented by the family

$$x + y \geq 1 \tag{1}$$
$$1 - x + y \geq 1 \tag{2}$$
$$x + 1 - y \geq 1 \tag{3}$$
$$1 - x + 1 - y \geq 1 \tag{4}$$

of linear inequalities, one for each conjunct.

The inference rules of CP include addition of linear inequalities and division of an inequality by a positive integer (a formal definition of CP is given later). Adding equations (1) and (2) we have

$$1 + 2y \geq 2$$

hence

$$2y \geq 1$$

and dividing by 2 and rounding up we have

$$y \geq \lceil 1/2 \rceil = 1.$$

Now adding equations (3) and (4) we have

$$3 - 2y \geq 2$$

hence

$$1 \geq 2y$$

and dividing by 2 and rounding down we have

$$0 = \lfloor 1/2 \rfloor \geq y.$$

But then $0 \geq y$ and $y \geq 1$ which is a contradiction.

It is perhaps not surprising that CP is more "efficient" than resolution, since cutting plane expressions have considerably more expressive power that the clauses of resolution. To give a representative example of the efficiency of CP over resolution, consider a combinatorial principle called the pigeonhole principle.

The *pigeonhole principle*, PHP_n, is

$$\bigwedge_{0 \leq i \leq n} \bigvee_{0 \leq j < n} p_{i,j} \supset \bigvee_{0 \leq i < i' \leq n} \bigvee_{0 \leq j < n} (p_{i,j} \wedge p_{i',j})$$

and states that there is no injection from $\{0, \ldots, n\}$ into $\{0, \ldots, n-1\}$. Its negation can be formulated by a propositional CNF formula denoted $\neg PHP_n$ of size $O(n^3)$. Work of Haken [14] and W. Cook et al. [12] established an exponential size gap between CP and resolution.

Specifically, if the *size* of a proof is the total number of symbols appearing in the proof, then while *every* resolution refutation of $\neg PHP_n$ must be of size $2^{\Omega(n)}$ [14] there exists a CP refutation of $\neg PHP_n$ of size $O(n^4)$ [12, 9]. In fact, every depth d Frege proof[1] of $\neg PHP_n$ must be of size at least $2^{\Omega(n^{1/6^d})}$ [3].

In this paper, we further investigate the cutting plane refutation system; the outline of the paper is as follows. Section 2 gives the basic definitions for cutting plane proofs. In sections 3, 4 and 5, we give polynomial size cutting plane proofs of the unique endnode principle and the *s-t* connectivity principle for graphs of valence 2. In section 6, we consider the subsystems CP_k of CP in which the division rule is restricted to be division by k, for $k \geq 2$. Somewhat surprisingly, we show that the subsystem CP_k of CP is equivalent within a polynomial factor to CP, thus answering question 19 on the list of open problems from [8]. In section 7, we present a normal form for CP_2 proofs, which in conjunction with the results of section 6 is a normal form for all cutting plane proofs. In section 8 we extend the construction of the normal form for CP_2 to arbitrary CP proofs; as a consequence we prove that the coefficients and constant terms in a cutting plane proof may be exponentially bounded by the number of steps in a cutting plane proof at the cost of increasing the number of steps by at most a polynomial amount. Sections 6, 7 and 8 may be read independently of sections 3-5. Next, in section 9, the extension $CPLE^+$ is proved to be polynomially equivalent to Frege systems. Lastly, in section 10, since linear inequalities are related to threshold gates, we introduce a new threshold logic and prove a completeness theorem.

2 Preliminaries

We begin by defining the class $\mathcal{E}$ of CP expressions.

Definition 1 If $a \in \mathbf{Z}$ and $i \in \mathbf{N}$, then $a \in \mathcal{E}$ and $(a \cdot x_i) \in \mathcal{E}$. If $E, F \in \mathcal{E}$ and $a \in \mathbf{Z}$, then $a \cdot E$ and $E + F$ belong to $\mathcal{E}$. A positive integer c *divides* an expression $E = \sum a_i \cdot E_i$ of $\mathcal{E}$, denoted $c|E$, if $c|a_i$ all i. The *quotient* of E by c is that expression $E' = \sum b_i \cdot E_i$ of $\mathcal{E}$, where $b_i = a_i/c$. Formulas of CP are of the form $E \geq F$, where $E, F \in \mathcal{E}$. The cutting plane system CP has five rules of inference — *transitivity, simplification, addition, multiplication, division*, given as follows.

- transitivity

$$\frac{E \geq F \qquad F \geq G}{E \geq G}$$

[1] i.e. usual Hilbert-style proof using axioms and modus ponens, where all formulas involve at most d alternations of $\wedge$, $\vee$.

- simplification: addition is commutative and associative; multiplication is commutative, associative and distributive over addition; common expressions may be combined [i.e. $a \cdot E + b \cdot E$ may be replaced by $(a+b) \cdot E$]; integer sums and products may be evaluated; an expression may be moved to the opposite side of the inequality sign, provided the sign of the coefficient is changed; $0 \cdot E$ may be replaced by 0.
- addition
$$\frac{E \geq F \qquad G \geq H}{E + G \geq F + H}$$
- multiplication — for $c \in \mathbf{N}$,
$$\frac{E \geq F}{c \cdot E \geq c \cdot F}$$
- division: for $c \in \mathbf{N}$, $c > 0$, $b \in \mathbf{Z}$, if $c|E$ with quotient E', then
$$\frac{E \geq b}{E' \geq \lceil b/c \rceil.}$$

In order to prove a formula A in disjunctive normal form, one expresses the negation $B = \neg A$ in conjunctive normal form as $\bigwedge_{i \in I} \bigvee_{j \in J} c_{i,j}$ where the $c_{i,j}$ are *literals*; i.e. propositional variables x or negations $\overline{x}$ of propositional variables. To express clauses in B as cutting plane formulas, we let propositional variables x be represented by integer variables x, let negated propositional variables, $\overline{x}$, be represented by $1 - x$, and let disjunctions be represented by summations. Formally, the cutting plane representation of a clause is defined by letting $R(x) = x$ and $R(\overline{x}) = 1 - x$, and the *representation* $R(\bigvee_{j \in J} c_j)$ of literals c_j defined to equal the linear inequality $\sum_{j \in J} R(c_j) \geq 1$. Finally the *representation* of the formula B in conjunctive normal form $\bigwedge_{i \in I} \bigvee_{j \in J} c_{i,j}$ is the set

$$\{R(\bigvee_{j \in J} c_{i,j}) : i \in I\}$$

of linear inequalities.

The intent of cutting plane proofs is to restrict attention to boolean solutions $x \in \{0, 1\}$ of families of linear inequalities with integer coefficients. We define a cutting plane *axiom* to be an inequality of the form $1 \geq 0$, $1 \geq 1$, and $x \geq x$, $x \geq 0$, $1 \geq x$ where x is a propositional variable. A formula B in conjunctive normal form has a cutting plane refutation, if there is a sequence $s_0, \ldots, s_m$ of linear inequalities, such that

- s_m is $0 \geq 1$,

- for all $i \leq m$, either s_i is a cutting plane axiom $1 \geq 0$, $1 \geq 1$, $x \geq 0$, $x \geq x$, $1 \geq x$ for propositional variable x in B, or of the form $R(\bigvee_{j\in J} c_{i,j})$ for one of the conjuncts of B, or there exist $j, k < i$ such that s_i is obtained from s_j, s_k by the transitivity, simplification, addition, multiplication or division rule.

A formula A is said to have a cutting plane proof if its negation $\neg A$ has a cutting plane refutation.

For an arbitrary proof system (semantic tableaux, resolution, cutting planes, constant depth Frege, Frege, extended Frege, etc.), the size of a proof is the total number of symbols in the proof (integers, including those in subscripts of variables, are represented in binary).

The following definitions are due to Cook and Reckhow in [11]. Let TAUT denote the collection of propositional tautologies.

Definition 2 Let Σ be a finite alphabet and TAUT $\subseteq \Sigma^*$. A proof system is a polynomial time computable function $f : \Sigma^* \to$ TAUT which is onto.

Definition 3 If $f : \Sigma_1^* \to$ TAUT and $g : \Sigma_2^* \to$ TAUT are proof systems, then g *p*-simulates f if there is a polynomial time computable function $h : \Sigma_1^* \to \Sigma_2^*$ such that $g(h(x)) = f(x)$ for all $x \in \Sigma_1^*$.

If the associated function h is polynomially bounded but not necessarily polynomial time computable, then we have the weaker notion of *simulation*. More formally,

Definition 4 Let $\mathcal{P}_1$, $\mathcal{P}_2$ be arbitrary proof systems for propositional logic. The system $\mathcal{P}_1$ *simulates* system $\mathcal{P}_2$, iff there is a polynomial $p(x)$ such that for any proof Q of formula A in $\mathcal{P}_2$, there is a proof P of (the formula corresponding to) A in $\mathcal{P}_1$ and the $size(P) \leq p(size(Q))$.

3 Nonunique endnode principle

A graph G is stipulated by a non-empty vertex set V and an edge set $E \subseteq V \times V$. A graph is *simple* if it contains no loops (i.e. for any $x \in V$, $(x, x) \notin E$), and is *undirected* if for any $(x, y) \in E$, it is the case that $(y, x) \in E$. An *endnode* $x \in V$ of an undirected graph G is a vertex for which there is a unique vertex $y \in V$ such that $(x, y), (y, x) \in E$.

The *valence* (or *degree*) of a node x of a simple undirected graph is the number of edges to which x is incident. The *valence* of a finite simple undirected graph G is the maximum valence of its nodes. Note that a graph of valence k may possess certain nodes of valence smaller than k. A graph is k-regular if all its nodes have valence k. The *nonunique endnode principle* informally states that no finite simple undirected graph of valence 2 can have a unique endnode. Its negation, the *unique endnode principle*, states that there exists a finite simple undirected graph of valence 2 having a unique endnode. An easy inductive proof establishes the nonunique endnode principle. The unique endnode principle for graphs whose vertex set is $\{0, \dots, n-1\}$ can be formulated in propositional logic by the conjunction of (5) through (10) below.[2]

$$\neg r_{i,i}, \text{for all } 0 \le i < n \tag{5}$$

$$\neg r_{i,j} \vee r_{j,i}, \text{for all } 0 \le i, j < n \tag{6}$$

$$\bigvee_{0 \le j < n} r_{0,j} \tag{7}$$

$$\neg r_{0,j} \vee \neg r_{0,j'}, \text{for all } 0 < j < j' < n \tag{8}$$

$$\bigvee_{0 < j < j' < n} (r_{i,j} \wedge r_{i,j'}), \text{for all } 0 < i < n \tag{9}$$

$$\neg r_{i,j} \vee \neg r_{i,j'} \vee \neg r_{i,j''}, \text{for all } 0 < i < n \text{ and } 0 \le j < j' < j'' < n \tag{10}$$

Note that, because of (9), the conjunction of (5) through (10) is not in conjunctive normal form. Nevertheless, we can present an equivalent formulation of this principle within the cutting plane system by the following equalities (11) through (14).

$$r_{i,i} = 0, \text{for all } 0 \le i < n \tag{11}$$

$$r_{i,j} = r_{j,i}, \text{for all } 0 \le i, j < n \tag{12}$$

$$\sum_{0 \le j < n} r_{0,j} = 1 \tag{13}$$

$$\sum_{0 \le j < n} r_{i,j} = 2, \text{for all } 0 < i < n. \tag{14}$$

Since the symbol '=' is not part of the syntax of the CP system, each of the above equations (11) through (14) really abbreviates two inequalities; e.g., (13) abbreviates

$$\sum_{0 \le j < n} r_{0,j} \ge 1 \qquad \text{and} \qquad 1 \ge \sum_{0 \le j < n} r_{0,j}.$$

The family of linear inequalities represented by (11) through (14) will be denoted as UEP_n. We will prove that UEP_n has a cutting plane refutation of size $n^{O(1)}$.

[2]The unique endnode principle is very closely related to the search problems in the class PPA introduced by Papadimitriou [18]. In a nutshell, the class PPA contains search problems where, given one node of degree one, it is required to find another node which does not have degree two. In [4], it is shown that the unique endnode principle is equivalent to the mod 2 counting principle in the setting of constant depth Frege proofs.

For $0 \leq k < n$, let

$$B_k = \sum_{i<j\leq k<n} r_{i,j} \tag{15}$$

$$S_k = \sum_{i\leq k<j<n} r_{i,j} \tag{16}$$

Thus B_k is the number of edges $r_{i,j}$ for $i < j$ *both* of whose endpoints are bounded by k, while S_k is the number of edges $r_{i,j}$ for $i < j$ whose endpoints *straddle* k.

Claim For $0 \leq k < n$, $2 \cdot B_k + S_k = 2k + 1$.

Proof. By induction on k. The base case, $k = 0$, holds since by (11), $B_0 = 0$, and by (13), $S_0 = 1$, so that $2 \cdot B_0 + S_0 = 1$. Assume by the induction hypothesis that $2 \cdot B_\ell + S_\ell = 2\ell + 1$ holds for $\ell < n - 1$. By definition, $2 \cdot B_{\ell+1} + S_{\ell+1}$ is given by

$$2 \sum_{i<j\leq \ell+1} r_{i,j} + \sum_{i\leq \ell+1<j} r_{i,j}$$

which is

$$2(\sum_{i<j\leq \ell} r_{i,j} + \sum_{i\leq \ell} r_{i,\ell+1}) + \sum_{i\leq \ell, \ell+1<j} r_{i,j} + \sum_{\ell+1<j} r_{\ell+1,j}$$

hence is

$$2(\sum_{i<j\leq \ell} r_{i,j} + \sum_{i\leq \ell} r_{i,\ell+1}) + \sum_{i\leq \ell<j} r_{i,j} - \sum_{i\leq \ell} r_{i,\ell+1} + \sum_{\ell+1<j} r_{\ell+1,j}.$$

By rearranging, this yields

$$2 \sum_{i<j\leq \ell} r_{i,j} + \sum_{i\leq \ell} r_{i,\ell+1} + \sum_{i\leq \ell<j} r_{i,j} + \sum_{\ell+1<j} r_{\ell+1,j}$$

and since by (12) $r_{\ell+1,j} = r_{j,\ell+1}$ and by (11) $r_{\ell+1,\ell+1} = 0$, we obtain

$$2 \sum_{i<j\leq \ell} r_{i,j} + \sum_{i\leq \ell<j} r_{i,j} + \sum_{0\leq i<n} r_{\ell+1,i}.$$

By (14) and the induction hypothesis, this yields

$$2\ell + 1 + 2 = 2(\ell + 1) + 1$$

Setting $k = n - 1$ we have

$$2B_{n-1} + S_{n-1} = 2n - 1.$$

But by its definition, $S_{n-1} = 0$, so that $2B_{n-1} = 2n-1$. The left side is odd and the right side is even, yielding the desired contradiction. This, when properly formalized (as in the related $CPLE$ proof of s-t undirected connectivity given in detail below), furnishes a cutting plane refutation of the system (11) through (14) of size polynomial in n. Hence we have the following theorem.

Theorem 5 *There are polynomial size CP proofs of the unique endnode principle UEP_n.*

4 s-t connectivity

The s-t connectivity principle, as formalized below by P. Pudlák, is the following statement. Let G be a finite simple *undirected* graph all of whose nodes have degree 2, except for two specially designated nodes s,t, each of which has degree 1. Then there is a path in G from s to t.

Let $\neg STC_n$ be the conjunction of the following propositional formulas.

$$q_0 \tag{17}$$

$$\overline{p_{ii}}, \text{ for all } 0 \leq i \leq n \tag{18}$$

$$\bigvee_{0 \leq j \leq n} p_{0j} \tag{19}$$

$$\bigvee_{0 \leq j \leq n} p_{nj} \tag{20}$$

$$\overline{p_{ij}} \vee p_{ji}, \text{ for all } 0 \leq i, j \leq n \tag{21}$$

$$\bigvee_{0 \leq j < j' \leq n} (p_{ij} \wedge p_{ij'}), \text{ for all } 0 < i < n \tag{22}$$

$$\overline{p_{0j}} \vee \overline{p_{0j'}}, \text{ for all } 0 \leq j < j' \leq n \tag{23}$$

$$\overline{p_{nj}} \vee \overline{p_{nj'}}, \text{ for all } j < j' \leq n \tag{24}$$

$$(\overline{p_{ij}} \vee \overline{p_{ij'}}) \vee \overline{p_{ij''}}, \text{ for all } 0 \leq i \leq n \text{ and } 0 \leq j < j' < j'' \leq n \tag{25}$$

$$(\overline{q_i} \vee \overline{p_{ij}}) \vee q_j, \text{for all } 0 \leq i, j \leq n \tag{26}$$

$$\overline{q_n} \tag{27}$$

The above formalization can be explained as follows. The propositional atom q_i means that vertex i is connected to vertex 0, while p_{ij} means that there is a *directed* edge from vertex i to j. Thus equation (25) states that if there is a directed edge from i to j then there is a directed edge from j to i; i.e. the graph is *undirected*. Thus any truth value assignment to the atoms for which conditions (17) through (25) hold gives rise to an undirected finite simple graph. Condition (26) states that if i is connected to 0 and there is an edge from i to j, then j is connected to 0. Condition (27) states that vertex n is not connected to vertex 0.

As in the propositional formalization of the unique endnode principle, $\neg STC_n$ is not in conjunctive normal form. However, by introducing new atoms r_{ij} to abbreviate $q_i \wedge p_{ij}$, we can provide polynomial size refutations of $\neg STC_n$ in $CPLE$, the cutting plane system with limited extension, which will be defined momentarily. Informally, the idea of the proof is to reduce $\neg STC_n$ to UEP_n.

Namely, as before, one proves that for $0 \le k < n$,

$$2B_k + S_k = 2Q_k + 1$$

where $Q_k = \sum_{0 \le i \le k} q_i$ is the number of vertices i for which $0 \le i \le k$ and q_i holds.

We now introduce the refutation system $CPLE$ of cutting planes with limited extension. The idea of $CPLE$ is to allow the introduction of new propositional variables *only* for subformulas of the initial formula to be refuted. By contrast, cutting planes with a general extension rule is equivalent to extended resolution (see [12]).

Definition 6 By induction on formula A, we define the set $LE[A]$ of linear inequalities associated with A.

- If A is the propositional variable x_i, then
  $LE[A] = \{p_A \ge 0, 1 \ge p_A, p_A \ge p_A, 1 \ge 1, 1 \ge 0\}$
- If A is $\neg B$, then
  $LE[A] = \{p_A \ge 0, p_A + p_B \ge 1, 1 \ge p_A, 1 \ge p_A + p_B, p_A \ge p_A\} \cup LE[B]$.
- If A is $B \wedge C$, then
  $LE[A] = \{p_A \ge 0, p_A \ge p_B + p_C - 1, 1 \ge p_A, p_B \ge p_A, p_C \ge p_A, p_A \ge p_A\} \cup LE[B] \cup LE[C]$.
- If A is $B \vee C$, then
  $LE[A] = \{p_A \ge 0, p_B + p_C \ge p_A, 1 \ge p_A, p_A \ge p_B, p_A \ge p_C, p_A \ge p_A\} \cup LE[B] \cup LE[C]$.

The acronym LE stands for limited extension, a concept related to Tseitin's notion of the extension rule for resolution. The system $CPLE$ has, as before, the rules for transitivity, simplification, addition, multiplication and division. A $CPLE$ refutation of the formula B (not necessarily in conjunctive normal form) is a sequence $s_0, \ldots, s_m$ of linear inequalities, such that

- s_m is $0 \ge 1$,
- for all $i \le m$, either $s_i \in LE[B] \cup \{p_B \ge 1\}$, or there exist $j, k < i$ such that s_i is obtained from s_j, s_k by the simplification, addition, multiplication or division rule.

We sometimes speak of $C \in LE[B]$ as an *axiom* and of $p_B \ge 1$ as the *hypothesis* in a refutation of B. The formula A is said to have a $CPLE$ proof, if its negation $\neg A$ has a $CPLE$ refutation.

Theorem 7 *There are polynomial size CPLE proofs of STC_n.*

This proof of Theorem 7 is in the appendix.

5 Undirected and directed s-t connectivity

It is well-known that there is sometimes a difference in the computational complexity (or definability) of undirected versus directed graph properties. In particular, Ajtai and Fagin [2] proved that connectivity for undirected graphs is not definable in monadic second order logic, whereas connectivity for directed graphs is so definable. In this section, we investigate the *proof theoretic* strength of the undirected and directed forms of s-t connectivity. We observe that undirected s-t connectivity trivially implies directed s-t connectivity, and the latter is equivalent (by constant depth polynomial size Frege proofs) to the pigeonhole principle. Moreover, the nonunique endnode principle of the previous section is easily seen to be equivalent (by constant depth polynomial size Frege proofs) to the undirected s-t connectivity principle. In [4], the nonunique endnode principle is shown to be equivalent (by constant depth polynomial size Frege proofs) to Ajtai's parity principle. By [1, 3] the parity principle is strictly stronger than the pigeonhole principle. Thus it follows from this section that the undirected s-t connectivity principle is strictly stronger than the directed s-t connectivity principle, with respect to constant depth polynomial size Frege proofs.

$STC(P,Q)$ or s-t connectivity for undirected graphs of valence 2 is the bounded first order statement in predicates P, Q given as follows.

1. $Q(s)$, meaning s is red.
2. $\neg Q(t)$, meaning t is not red.
3. $\exists j \leq n(j \neq s \wedge P(s,j))$, meaning at least one edge incident to s.
4. $\exists j \leq n(j \neq t \wedge P(t,j))$, meaning at least one edge incident to t.
5. $\forall i, j \leq n(P(i,j) \leftrightarrow P(j,i))$, meaning G undirected.
6. $\forall i \leq n\ \exists j, j' \leq n(i \neq s \wedge i \neq t \rightarrow j \neq j' \wedge P(i,j) \wedge P(i,j'))$, meaning at least 2 edges incident to every vertex different from s, t.
7. $\forall j, j' \leq n(j \neq j' \rightarrow \neg P(s,j) \vee \neg P(s,j'))$, meaning s incident to at most one edge.
8. $\forall j, j' \leq n(j \neq j' \rightarrow \neg P(t,j) \vee \neg P(t,j'))$, meaning t incident to at most one edge.
9. $\forall i, j, k, l \leq n(j, k, l \text{ distinct } \wedge i \neq s \wedge i \neq t \rightarrow \neg P(i,j) \vee \neg P(i,k) \vee \neg P(i,l))$, meaning vertices different than s, t incident to at most 2 edges.
10. $\forall i(\neg P(i,i))$, meaning no loops at vertices.
11. $\forall i, j \leq n(Q(i) \wedge P(i,j) \rightarrow Q(j))$, meaning any vertex connected by an edge to a red vertex is red.

12. $s = 0$

13. $t = n$

Let $\theta(P, Q, n)$ [resp. $\theta'(P, Q, n, s, t)$] be the conjunction of the above formulas [resp. with the exception of $s = 0$, $t = n$]. Then $STC(P, Q)$ [resp. $STC'(P, Q)$] is the formula $\forall n \neg \theta(P, Q, n)$ [resp. $\forall n \forall s, t \leq n(\neg \theta'(P, Q, n, s, t)$]. Let $\alpha(P, Q, n, s, t)$ denote the conjunction of (1) through (10). $STC(P, Q)$ states that any undirected graph on nodes $\{0, \ldots, n\}$ for which $0, n$ have valence 1 and all other nodes valence 2 must have a path from 0 to n. Thus $STC(P, Q)$ expresses s-t connectivity where $s = 0$, $t = n$, while $STC'(P, Q)$ expresses s-t connectivity without postulating the values of s, t. Note that for given P, Q, n, the values s and t in $\alpha(P, Q, n, s, t)$ must be unique — it is not possible for two distinct pairs (s, t) and (s', t') to satisfy the above conditions.

Recall that $I\Delta_0$ is the first order theory of arithmetic in the language $0, 1, +, \cdot, \leq$ with the usual axioms describing a discretely ordered semi-ring together with the scheme of induction

$$\Phi(0) \wedge (\forall x)(\Phi(x) \to \Phi(x+1)) \to (\forall x)(\Phi(x))$$

for all formulas Φ which are Δ_0 (where all quantifiers are *bounded*, i.e. of the form $(\exists x < t)$, $(\forall x < t)$ for some term t). In [20], J. Paris and A. Wilkie observed that if $I\Delta_0 \vdash \Phi(x)$, then there are constant depth polynomial size Frege proofs of the tautologies $\widetilde{\Phi}_n$. See as well [17] for details about the translation $\widetilde{\Phi}_n$.

Proposition 8 *$I\Delta_0(P, Q, P', Q') \vdash STC(P, Q) \leftrightarrow STC'(P', Q')$.*

Proof. ($\Leftarrow$) clear.
($\Rightarrow$) Suppose that $\neg STC'(P', Q')$, so that $\exists s, t \leq n(s \neq t \wedge \theta'(P', Q', n, s, t))$. Given P', Q' define $P(i, j)$ to be

$$\begin{aligned} i \neq j \wedge \exists s, t \leq n(\alpha(P', Q', n, s, t) \wedge \ & i = s \wedge j = t \to P'(0, n) \wedge \\ & i = t \wedge j = s \to P'(n, 0) \wedge \\ & i = s \wedge j \neq t \to P'(0, j) \wedge \\ & i = t \wedge j \neq s \to P'(n, j) \wedge \\ & i \neq t \wedge j = s \to P'(i, 0) \wedge \\ & i \neq s \wedge j = t \to P'(i, n) \wedge \\ & \{i, j\} \cap \{s, t\} = \emptyset \to P'(i, j)). \end{aligned}$$

Similarly define $Q(i)$ to be

$$\begin{aligned} \exists s, t \leq n \ \ & (\alpha(P', Q', n, s, t) \wedge \\ & i = 0 \to Q(i) \leftrightarrow Q'(s) \wedge \\ & i = n \to Q(i) \leftrightarrow Q'(t) \wedge \\ & i = s \to Q(i) \leftrightarrow Q'(0) \wedge \\ & i = t \to Q(i) \leftrightarrow Q'(n)). \end{aligned}$$

P, Q are Δ_0 definable in P', Q' and simply correspond to the interchange of $0, s$ and n, t. By hypothesis, $\theta'(P', Q', n, s, t)$ so by construction $\theta'(P, Q, n, 0, n)$. Thus $\theta(P, Q, n)$ and so $\neg STC(P, Q)$. $\Box$

$DSTC(P, Q, R)$, directed s-t connectivity for directed graphs of valence 2, is given as follows.

14. $\forall i, j \leq n(P(i, j) \wedge R(i, j) \rightarrow \neg R(j, i))$
15. $\forall i, j \leq n(P(i, j) \wedge \neg R(i, j) \rightarrow R(j, i))$
16. $\forall i, j \leq n(P(i, j) \wedge R(i, j) \wedge P(j, k) \rightarrow R(j, k))$
17. $\forall i, j \leq n(P(i, j) \wedge \neg R(i, j) \wedge P(j, k) \rightarrow \neg R(j, k))$

Let $\varphi[P, Q, R](n)$ be the conjunction of (1) through (17). $DSTC(P, Q, R)$ is the formula $\forall n \neg\varphi(P, Q, R, n)$. The idea is that (14)-(17) describe an orientation or direction for the edges: $P(i, j) \wedge R(i, j)$ describes the edge $i \rightarrow j$, while $P(i, j) \wedge \neg R(i, j)$ describes the edge $i \leftarrow j$. One can show, as before that $DSTC(P, Q, R)$ and an analogous statement $DSTC'(P', Q', R') \equiv_{df} \forall n \neg\varphi'(P', Q', R', n)$ (without specifying s to be 0 and t to be n) are equivalent over $I\Delta_0(P, Q, R, P', Q', R')$.

Proposition 9 *$I\Delta_0(P, Q, P', Q', R') \vdash STC(P, Q) \rightarrow DSTC(P', Q', R')$.*

Proof. Trivial.

Definition 10 $PHP^{onto}(F, n)$ is the statement

$$[\forall i \leq n\ \exists j < n\ F(i, j) \wedge \forall j < n\ \exists i \leq n\ F(i, j)$$

$$\wedge \forall i \leq n\ \forall j, j' < n(j \neq j' \rightarrow \neg F(i, j) \vee \neg F(i, j'))]$$

$$\rightarrow \exists j < n\ \exists i, i' \leq n(i \neq i' \wedge F(i, j) \wedge F(i', j))$$

where F is a binary predicate symbol. $PHP^{onto}(F)$ is $\forall n\ PHP^{onto}(F, n)$.

Proposition 11 *$I\Delta_0(P, Q, R, F) \vdash PHP^{onto}(F) \leftrightarrow DSTC(P, Q, R)$.*

Proof. ($\Rightarrow$) Suppose $DSTC(P, Q, R)$ does not hold. Let n be such that $\varphi(P, Q, n)$. Define $f : \{0, \ldots, n\} \rightarrow \{0, \ldots, n-1\}$ by

$$f(i) = \begin{cases} i & \text{if } \neg Q(i) \\ j & \text{if } Q(i) \wedge P(i, j) \wedge R(i, j). \end{cases}$$

Assuming $\varphi(P, Q, n)$, then for any i such that $Q(i)$, there is a unique j such that $Q(i) \wedge P(i, j) \wedge R(i, j)$. Thus f is well-defined. Let $F(i, j) \leftrightarrow_{df} f(i) = j$. Then as f is a 1-1 mapping from $n + 1$ into n, $\neg PHP^{onto}(F)$ holds.

($\Leftarrow$) Suppose $\neg PHP^{onto}(F, n)$ holds for some n. Define the relation G on $\{n + 1, \ldots, 2n + 1\} \rightarrow \{n, \ldots, 2n - 1\}$ by $G(n + 1 + i, n + j) \equiv_{df} F(i, j)$.

Let $P(i,j) \equiv_{df} F(i,j) \vee G(i,j) \vee F(j,i) \vee G(j,i)$
$R(i,j) \equiv_{df} P(i,j) \wedge (F(i,j) \vee G(i,j))$
$Q(i) \quad \equiv_{df} i \leq n.$

Then $\varphi'(P,Q,R,2n+1)$ holds, so $DSTC'(P,Q,R)$ fails and hence $DSTC(P,Q,R)$ fails. $\Box$

Corollary 12 *STC_n requires exponential size constant depth Frege proofs.*

Proof. A subexponential size constant depth Frege proof of STC_n would yield a subexponential size constant depth Frege proof of PHP_n^{onto}, contradicting [3]. $\Box$

From the previous section there are polynomial size $CPLE$ proofs of STC_n, hence by [13] polynomial size Frege proofs of STC_n.

6 The Systems CP_q

For an integer $q \geq 2$, the proof system CP_q is obtained from CP by restricting the division rule to division by q. The systems CP_q are quite strong, and will be shown to be p-equivalent to CP. To illustrate the idea of the proof, we present the following example of how CP_2 can simulate division by three.

Example 13 To simulate division by 3 applied to

(28) $$6x + 15y \geq 7$$

within CP_2, first write the coefficient of each variable with 3 as explicit factor. This gives

(29) $$3(2x) + 3(5y) \geq 7.$$

The least power of 2 greater than 3 is 2^2 or 4. Using $x \geq 0$, $y \geq 0$ obtain $2x \geq 0$, $5y \geq 0$ which when added to (29) gives

(30) $$2^2(2x) + 2^2(5y) \geq 7.$$

Two applications of division by 2 yields

(31) $$2x + 5y \geq 2.$$

Adding (29) and (31) gives

(32) $$2^2(2x) + 2^2(5y) \geq 9$$

and two applications of division by 2 yields the desired inequality

(33) $$2x + 5y \geq 3$$

which one would obtain from (28) by division by 3.

Theorem 14 *Let $q > 1$. Then CP_q p-simulates CP.*

Since CP trivially p-simulates CP_q, we have that CP and CP_q are p-equivalent systems, for any fixed $q > 1$.

Proof. Fix $q > 1$. We must prove that an arbitrary instance of the division rule in a CP-proof can be simulated by a polynomial size CP_q proof. For the purposes of this proof, we modify slightly the syntax of cutting plane proofs as follows. Firstly, we allow only inequalities of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \geq b,$$

where $a_1, \ldots, a_n$ and b are integers. With this restricted syntax for inequalities appearing in cutting plane proofs, the transitivity and simplification rules are unneeded. The addition, multiplication and division rules still apply in the obvious way and these are the only rules of inference. The axioms for this restricted cutting plane syntax are $-x_i \geq -1$ and $x_i \geq 0$. A cutting plane refutation now is defined to be a sequence of inequalities obtained via these axioms and rules of inference and ending with a formula $0 \geq 1$. It is easy to verify (and we leave the verification to the reader) that any cutting plane refutation of the type we defined in section 2 above can be converted into a cutting plane refutation in this restricted syntax system. For the rest of this section, we work with the restricted cutting plane system, which we also denote CP.

Suppose a cutting plane proof contains a division inference

$$\frac{c\alpha \geq M}{\alpha \geq \lceil \frac{M}{c} \rceil} \tag{34}$$

where, of course, $c > 1$. We must prove that this can be efficiently simulated using division by q; so we shall describe a short CP_q proof of $\alpha \geq \lceil \frac{M}{c} \rceil$ from the hypothesis

$$c \cdot \alpha \geq M \tag{35}$$

Choose p so that $q^{p-1} < c \leq q^p$. Without loss of generality, we may assume that $q^p/2 < c$; if this does not hold, then find a suitable multiple $m \cdot c$ of c such that $q^p/2 < m \cdot c \leq q^p$ and multiply the hypothesis inequality (35) by m and use division by $m \cdot c$ in place of c.

The expression α is a linear combination $\sum_{i=1}^{n} a_ix_i$ with integer coefficients. Let s_0 equal the sum of the *negative* coefficients of α. From the axioms $x_i \geq 0$ and $-x_i \geq -1$, we can derive

$$\alpha \geq s_0 \tag{36}$$

without any use of the division rule. Inductively define s_i by

$$s_{i+1} \ = \ \left\lceil \frac{(q^p - c)s_i + M}{q^p} \right\rceil .$$

Assuming that $\alpha \geq s_i$ has already been derived, we show that CP_q can derive $\alpha \geq s_{i+1}$ with a short proof. First, by combining the inequality (35) with $\alpha \geq s_i$, CP_q can derive

$$q^p \cdot \alpha \geq (q^p - c)s_i + M$$

with no use of division. Then, with p uses of division by q, CP_q can derive $\alpha \geq s_{i+1}$.

Since we have

$$s_{i+1} \geq \frac{q^p - c}{q^p} s_i + \frac{c}{q^p}\left(\frac{M}{c}\right)$$

and $c > q^p/2$, it is immediate that $\frac{M}{c} - s_{i+1} \leq \frac{1}{2}\left(\frac{M}{c} - s_i\right)$. Since s_i is an integer, it follows that if $M/c - s_i < 1/c$, then $s_i = \lceil M/c \rceil$. Therefore, $s_i = \lceil M/c \rceil$ after $i = \log(M - c \cdot s_0)$ iterations. This completes the simulation of the inference (34) in CP_q; namely, the CP_q-proof derives $\alpha \geq s_i$ for $i = 0, 1, \ldots, \log(M - c \cdot s_0)$. The fact that this CP_q-proof has length polynomially bounded by the number of symbols in inequality (35) is easily checked. $\Box$

7 A normal form for cutting plane proofs

In this section, we present a normal form for CP_2-proofs. In view of Theorem 14 which implies that CP_2 p-simulates CP, this also gives a normal form for arbitrary cutting plane proofs. Our original motivation for discovering the normal form for CP_2-proofs was an attempt to show that the coefficients of inequalities in cutting plane proofs can be bounded by a polynomial of the number of inferences in the proof (provided that the set of inequalities being refuted contains only small coefficients). Unfortunately, we have not achieved this goal; instead, we only obtain exponential bounds on the values of coefficients in the cutting plane proofs (the proof for general CP-proofs is in section 8). In fact it remains an open problem whether cutting plane proofs with coefficients represented in unary notation can p-simulate cutting plane proofs with coefficients represented in the usual binary notation. However, the normal form for CP_2-proofs that we present below does give a partial result in this direction.

For this section and the next section, we shall again slightly modify the syntax of cutting plane proofs: we now assume that all inequalities in the proof are of the form

$$a_1x_1 + a_2x_2 + \cdots a_nx_n + a_{n+1} \geq 0$$

where the a_i's are integers. We'll use letters E and F, often with subscripts and superscripts to denote expressions of the form shown in the lefthand side of the inequality; thus, all inequalities in the proof are of the form $E \geq 0$. The rules of inference are still the addition rule, the multiplication rule and the division rule. For the division rule, each of the coefficients $a_1, \ldots, a_n$ in the inequality in the hypothesis must be multiples of the divisor c, and the constant coefficient, a_{n+1}, is rounded down, not up, since it is on the lefthand side of the inequality. The initial inequalities include $x_i \geq 0$ and $-x_i + 1 \geq 0$ in addition to the inequalities which are being refuted. The last line of a cutting plane proof is now $-1 \geq 0$.

We are now ready to describe the normal form for CP_2-proofs. Assume we are given a CP_2-proof P. Firstly, we can, w.l.o.g., view P as consisting of the lines

$$\begin{array}{l} E_1 \geq 0, \quad E_2 \geq 0, \quad \ldots \quad , E_p \geq 0, \\ \qquad F_{p+1} \geq 0, \quad E_{p+1} \geq 0, \quad F_{p+2} \geq 0, \quad E_{p+2} \geq 0, \\ \qquad \ldots, \quad F_m \geq 0, \quad E_m \geq 0, \quad F_{m+1} \geq 0, \end{array}$$

where the following conditions hold. Firstly, $E_1 \geq 0$ through $E_p \geq 0$ are the initial inequalities (axioms and hypotheses). Secondly, F_{m+1} is just -1. Thirdly, each F_{i+1} is a nonnegative linear combination of $E_1, \ldots, E_i$; i.e.,

$$F_{i+1} = b_1^i E_1 + b_2^i E_2 + \cdots + b_i^i E_i, \tag{37}$$

with each b_j^i a nonnegative integer. Finally, for $i > p$, $E_i \geq 0$ is obtained from $F_i \geq 0$ by division by two.

Given the proof P containing the lines $E_i \geq 0$ and $F_i \geq 0$ as above, we now describe how to form a CP_2-proof P' in the normal form. P' will contain lines $E'_i \geq 0$ and $F'_i \geq 0$ which correspond to the lines in P. For $1 \leq i \leq p$, E'_i is equal to E_i. For $i > p$, the lines $E'_i \geq 0$ will be obtained from $F'_i \geq 0$ by division by two. It remains to describe the lines $F'_i \geq 0$. Recall that F_i was computed according to (37) above. We compute F'_{p+1} as

$$F'_{p+1} = \sum_{i=1}^{p} (b_i^p \bmod 2) E_i.$$

Note the coefficients of variables which appear in F'_{p+1} are even, since they were even in F_{p+1}. Therefore, it is valid to use the division by two rule to obtain $E'_{p+1} \geq 0$ from $F'_{p+1} \geq 0$.

Now we claim that E_{p+1} is a nonnegative linear combination of $E'_1, \ldots, E'_{p+1}$. Indeed,

$$E_{p+1} = E'_{p+1} + \sum_{i=1}^{p} \lfloor b_i^p / 2 \rfloor E'_i.$$

We continue this process inductively to define F'_i and E'_i for $p + 1 \leq i \leq m$. We always maintain the inductive condition that E_i is a nonnegative linear combination of $E'_1, \ldots, E'_i$; therefore, F_{i+1} is equal to a nonlinear combination of these, say,

$$F_{i+1} = b_1 E'_1 + b_2 E'_2 + \cdots + b_i E'_i.$$

Then F'_{i+1} is defined to equal

$$F'_{i+1} = \sum_{j=1}^{i} (b_j \bmod 2) E'_j.$$

Once F'_i and E'_i have been obtained, for all $i = 1, \ldots, m$; we have that -1 is a nonnegative linear combination of $E'_1, \ldots, E'_m$. Of course, this nonnegative linear combination may involve large coefficients. However, these large coefficients can be avoided as follows. Suppose $\sum_{i=1}^{m} c_i E'_i = -1$ with the c_i's nonnegative integers. Since the c_i's are obtainable as solutions to a linear programming problem with the constraints $c_i \geq 0$, we may assume the sizes of the c_i's are polynomially bounded by m and the sizes of the coefficients and constant terms in the E'_i's. This is an elementary fact about linear programming; in fact, letting C equal the maximum of the absolute values of the coefficients and constant terms in the E'_i's, we have that $|c_i| \leq m! \cdot C^m$, for all i. (For a proof of this see, e.g., [19, Lemma 2.1]). Let J be such that each $|c_i| < 2^J$; thus, $J = O(m(\log m + \log C))$. Instead of deriving $-1 \geq 0$ as a single nonnegative linear combination of the inequalities $E'_i \geq 0$; we use J steps, with $j = J, J-1, \ldots, 2, 1, 0$, to successively derive $G_j \geq 0$ where

$$G_j = \sum_{i=1}^{m} \lfloor c_i / 2^j \rfloor E'_i.$$

However, the G_j's are not derived according to the formula defining them; instead, the $G_{j-1} \geq 0$ is derived from $G_j \geq 0$ and from the inequalities E'_i using the fact that G_{j-1} equals twice G_j plus a 0/1 linear combination of the E'_i's; namely,

$$G_{j-1} = 2 \cdot G_j + \sum_{i=1}^{m} \left(\lfloor c_i / 2^{j-1} \rfloor \bmod 2 \right) E'_i.$$

Since G_0 is just -1, we obtain a CP_2 derivation P' of $-1 \geq 0$.

To analyze the size of the coefficients appearing in P'; first note the absolute values of the coefficients in the G_j's must be $\leq m \cdot C$; since otherwise, it would be impossible to end up with the final summation G_0 equal to -1. To bound the size of the coefficients in E'_i, we let B be the maximum of the absolute values of the coefficients and constant terms in the hypotheses $E_1 \geq 0, \ldots, E_p \geq 0$, and let $A = B \cdot p$.

Lemma 15 *Let $i > p$. The constant term and every coefficient of E'_i has absolute value $\leq \frac{11}{8} A \cdot (1.5)^{i-p-3}$. Thus $C \leq A \cdot 1.5^{m-p} = p \cdot B \cdot 1.5^{m-p}$.*

The lemma is proved by induction on i. In the base case $i = p+1$, since F'_{p+1} is a 0/1-linear combination of the p expressions $E_1, \ldots, E_p$ and since E_{p+1} is $F_{p+1}/2$, we have that each coefficient of E'_{p+1} is $\leq A/2$ in absolute value. By similar reasoning, each coefficient in E'_{p+2} has absolute value $\leq (A+A/2)/2 \leq 3A/4$; and likewise each coefficient in E'_{p+3} has absolute value $\leq (A+A/2+3A/4)/2 = \frac{11}{8}A$. For the induction step, with $i \geq p+3$, E'_{i+1} is a 0/1-linear combination of $E'_1, \ldots, E'_i$. Therefore, each coefficient in E'_{i+1} has absolute value bounded by

$$A \cdot \frac{11}{8}\left(\left(\frac{2}{3}\right)^{i-p-3} + \frac{1}{2}\left(\frac{2}{3}\right)^{i-p-3}\right) = \frac{11}{8} \cdot A \cdot \left(\frac{2}{3}\right)^{i-p-2} \qquad \square$$

To count the number of lines in P', note that each F'_i can be obtained by $\leq i+2$ additions and thus with $O(m)$ lines. The complete derivation of the inequalities $E'_1 \geq 0, \ldots, E'_m \geq 0$ therefore takes $O(m^2)$ lines. The final portion of P' derives each of the J inequalities $G_i \geq 0$ with $O(m)$ steps. By the above estimate on J and by Lemma 15,

$$J = O(m(\log m + (m-p)(\log B + \log p))) = O(m^2 \log B).$$

Therefore, the final portion of P' has $O(m^3 \log B)$ lines, so P' has $O(m^3 \log B)$ lines in total.

8 Bounds on coefficients in general CP proofs

Let Σ be a set of linear inequalities: following the convention of the previous section, we assume all inequalities are of the form $E \geq 0$, where E is a linear polynomial of variables $x_1, \ldots, x_n$. We let $||E||$ denote the maximum of the absolute values of the constant term and the coefficients appearing in E. For the rest of this section, we let B denote the maximum value of $||E||$ for inequalities $E \geq 0$ in Σ.

The construction in section 7 and the size analysis of Lemma 15 proved that if a CP_2-proof P refuting Σ has M lines, then there is another CP_2-proof P', also refuting Σ, in which each coefficient and constant term has absolute value bounded by $O(M^2 \cdot B \cdot (1.5)^M)$ such that the number of steps in P' is $O(M^3 \log B)$. Also, by the construction of section 6, every general CP-proof can be converted into a polynomial size CP_2-proof. Therefore it is reasonable to expect that whenever P is a general CP-proof refuting Σ, then there is a CP-proof P', also refuting Σ, such that the both the number of lines of P' and the sizes of constant terms and coefficients in P' are polynomially bounded by M and $\log B$.

Unfortunately, the construction in section 6, which converted a general CP-proof into a CP_2-proof, can cause a superpolynomial increase in the number of lines in the proof when the coefficients and divisors are very big. So we must give a new proof to establish the following lemma.

Lemma 16 *Let Σ and $B > 0$ be as above. Let P be an M line CP-proof refuting Σ. Then there is a CP-proof P', also refuting Σ, such that P' has*

$O(M^3 \log B)$ lines and such that each coefficient and each constant term appearing in P' has absolute value equal to $O(M^2 \cdot B \cdot 2^M)$.

Note, that as a corollary to Lemmas 15 and 16, we can also take P' to be a CP_2-proof with slightly worse upper bounds.

Proof. The proof is very similar to the construction of the CP_2-proof in normal form in the previous section; so we shall sketch only the principal ideas of the proof. As before, we can view the CP-proof P as a sequence of inequalities

$$\begin{aligned} &E_1 \geq 0, \quad E_2 \geq 0, \quad \dots \quad , E_p \geq 0, \\ &\quad F_{p+1} \geq 0, \quad E_{p+1} \geq 0, \quad F_{p+2} \geq 0, \quad E_{p+2} \geq 0, \\ &\quad \dots, \quad F_m \geq 0, \quad E_m \geq 0, \quad F_{m+1} \geq 0. \end{aligned}$$

where each F_i is a nonnegative linear combination of $E_1, \dots, E_{i-1}$, but now each E_i, with $i > p$, is obtained from F_i by division by some integer $c_i \geq 2$. Similarly to the earlier construction, form P' with inequalities $E'_i \geq 0$ and $F'_i \geq 0$. We still have E_i is equal to E_i for $i \leq p$, and also, for $i > p$, $E'_i \geq 0$ is obtained from F'_i be division by c_i. Now, however, each

$$F'_{i+1} = \sum_{j=1}^{i} b_j \cdot E'_j$$

for some integers b_j, which depend on i, such that $0 \leq b_j < c_i$. The proof that P' can be constructed this way is essentially the same as before. And the final part of P' that derives $G_i \geq 0$ is constructed exactly as before.

Redoing the analysis of Lemma 15, we find that $||E_{p+i+1}||$ can be bounded by

$$\frac{1}{c_i}\left[(c_i - 1)\left(p \cdot B + \sum_{j=1}^{i} ||E_{p+j}||\right)\right]$$

and then $||E_{p+i+1}|| \leq pB + \sum_{j=1}^{i} ||E_{p+j}||$. Therefore, $||E_{p+i+1}|| \leq pB2^i$. Then P' has all constant terms and coefficients $\leq MpB2^{m-p} < M^2B2^M$ in absolute value and has

$$O(m(\log m + m \log(pB2^{m-p}))) = O(m^3 \log B) = O(M^3 \log B)$$

many lines. □

9 Frege systems and extended cutting planes

We define the extensions CP^+ and $CPLE^+$ of CP, $CPLE$ obtained by removing a requirement in the division rule. We first define the collection $\mathcal{E}^+$ of all CP^+ expressions.

Definition 17 If $a \in \mathbf{Z}$ and $i \in \mathbf{N}$, then $a \in \mathcal{E}^+$ and $(a \cdot x_i) \in \mathcal{E}^+$. If $E, F \in \mathcal{E}^+$ and $a \in \mathbf{Z}$, then $a \cdot E$ and $E + F$ belong to $\mathcal{E}^+$. If $E \in \mathcal{E}^+$ and $c \in \mathbf{N}$, $c > 0$, then $\lceil E/c \rceil$ belongs to $\mathcal{E}^+$.

Though not formally part of the syntax, the floor operator $\lfloor E/c \rfloor$ could be defined by $-\lceil -E/c \rceil$. A positive integer c *divides* an expression $E = \sum a_i \cdot E_i$ of $\mathcal{E}^+$, denoted $c|E$, if $c|a_i$ all i. The *quotient* of E by c is that expression $E' = \sum b_i \cdot E_i$ of $\mathcal{E}^+$, where $b_i = a_i/c$.

We define the modified rule of simplification to admit, in addition to the other cases of simplification, the following replacements and inferences. For E, F, G expressions in $\mathcal{E}^+$, and $c > 0$ in $\mathbf{N}$, if $c|E$ with quotient E' then $\lceil \frac{E+F}{c} \rceil$ may be replaced by $E' + \lceil \frac{F}{c} \rceil$, and $\lceil \frac{E}{c} \rceil$ may be replaced by E'. As well we admit the following simplification inference.

$$\frac{1 \geq E}{\lceil E/c \rceil \geq E}$$

Modified division is given by the following:

For $c > 0$ in $\mathbf{N}$ and $E, F \in \mathcal{E}^+$,

$$\frac{E \geq F}{\lceil \frac{E}{c} \rceil \geq \lceil \frac{F}{c} \rceil}$$

The systems CP^+ and $CPLE^+$ are respectively defined from CP and $CPLE$ by modifying the substitution and division rules as indicated above.

Theorem 18 *Frege systems p-simulate $CPLE^+$.*

Proof. We give only a proof sketch, basing the essential ideas on Goerdt's [13] p-simulation of CP by Frege systems. We begin by an overview of Goerdt's simulation. Let $C = \bigwedge_{i-1}^{n} C_i$ be a formula in conjunctive formal form where each C_i is $\bigvee_{j=1}^{m_i} D_{ij}$. Let $I_1, \ldots, I_M$ be a CP refutation of C; i.e. axioms $\sum_{j=1}^{m_i} R(D_{ij}) \geq 1$ are allowed for $1 \leq i \leq n$.

Goerdt constructs a Frege formula $Rep(I_k)$ for each inequality I_k and proves within a Frege system $\mathcal{F}$ that

$$\begin{gathered}
\vdash_{\mathcal{F}} C \supset Rep(I_1) \\
\vdash_{\mathcal{F}} C \supset Rep(I_2) \\
\vdots \\
\vdash_{\mathcal{F}} C \supset Rep(I_M) \\
\vdash_{\mathcal{F}} C \supset \textsc{false}
\end{gathered}$$

where FALSE represents the false formula $x_0 \wedge \neg x_0$. Standard techniques then show $\vdash_{\mathcal{F}} \neg C$. What has just been sketched is an effective translation process, which given a CP refutation of C yields a Frege proof of $\neg C$.

Goerdt's techniques are easily adapted to provide a p-simulation of $CPLE$. Before indicating how to extend these techniques to $CPLE^+$, we review some of the machinery introduced in [13].

An integer $m = \sum_{i=0}^{T-1} m_i \cdot 2^i$, $0 \leq m_i \leq 1$, has propositional representation $\vec{m} = (F^0, \ldots, F^{T-1})$ where $F^i = \text{TRUE} = x_0 \vee \neg x_0$ if $m_i = 1$ and $F^i = \text{FALSE} = x_0 \wedge \neg x_0$ otherwise. Integers can be given a positive or negative sign by

$$+\vec{F} = (F^0, \ldots, F^{T-1}, \text{TRUE})$$
$$-\vec{F} = (F^0, \ldots, F^{T-1}, \text{FALSE}).$$

Inequality $\vec{F} \geq \vec{G}$ is then defined in $\mathcal{F}$, along with

$$Add(\vec{F}, \vec{G}) = (Add^0(\vec{F}, \vec{G}), \ldots, Add^{T-1}(\vec{F}, \vec{G}))$$

where $Add^i(\vec{F}, \vec{G})$ is TRUE iff the i^{th} bit of the sum of the integers designated by formula vectors $\vec{F}, \vec{G}$ is 1. Using carry-save addition, as in [5], the formula $ItAdd(\vec{F^0}, \vec{F^1}, \ldots, \vec{F^{n-1}})$ is defined, which represents the sum $f_0 + f_1 + \cdots + f_{n-1}$ where f_i is the integer denoted by the formula vector $\vec{F_i}$ of length T, and n is a power of 2, $n \leq T$.

Taking into account iterated addition for all positive terms and separately for all negative terms, the representing formula $Rep(I)$ for cutting plane inequality $\sum a_i \cdot x_i - \sum b_i \cdot x_i \geq m$ for $a_i, b_i \in \mathbf{N}$ is given by

$$AddSi(+ItAdd(\vec{a} \cdot \vec{x}),\ -ItAdd(\vec{b} \cdot \vec{x})) \geq \vec{m}$$

where $AddSi$ is an extension of Add which allows addition of two signed integers.

The formula

$$Mult(\vec{F}, \vec{G}) = (Mult^0(\vec{F}, \vec{G}), \ldots, Mult^{2T-1}(\vec{F}, \vec{G}))$$

is defined where $Mult^i(\vec{F}, \vec{G})$ is TRUE iff the i^{th} bit of $f \cdot g$ is 1 where f [resp. g] is the integer denoted by the formula vector $\vec{F} = (F_0, F_1, \ldots, F_{T-1})$ [resp. $\vec{G} = (G_0, G_1, \ldots, G_{T-1})$].

Goerdt proves that all the above formulas are of size polynomial in T and that, provably in the Frege system $\mathcal{F}$, the usual properties of addition, multiplication, distribution of addition over multiplication, etc. all hold. For conjunctive normal form formula C, Goerdt now shows by induction on the number of inferences $I_1, I_2, \ldots, I_M$ in a cutting plane refutation that $\vdash_{\mathcal{F}} C \supset Rep(I_1), \ldots \vdash_{\mathcal{F}} C \supset Rep(I_M), \vdash_{\mathcal{F}} C \supset \text{FALSE}$.

To extend Goerdt's technique, we must construct a propositional formula to express $\lceil \frac{E_1 + \cdots + E_m}{n} \rceil$. This is done as follows. Theorem 136 on p.112 of [15] yields the following. Suppose $q \in \mathbf{N}$, $q \geq 2$ is of the form $2^\mu Q$, where Q is not divisible by 2 and let p satisfy $0 < p/q < 1$, $\gcd(p, q) = 1$. Let ν be the order of 2, mod Q; i.e. ν is the least positive integer satisfying $2^\nu \equiv 1 \pmod{Q}$. Then the binary expansion of $\frac{p}{q}$ has μ non-recurring bits and ν recurring bits.

Now for $q = 2^\mu Q$ and ν the order of 2 modulo Q, the binary representation of $\frac{1}{q}$ is $0\,.\,r_1 \dots r_\mu \overline{s_1 \dots s_\nu}$ where the bar indicates infinitely many repetitions of the indicated block $s_1, \dots, s_\nu$. Given $a \in \mathbf{N}$ where $|a| = n$, let k be the least positive integer satisfying $\mu + k \cdot \nu > n + \mu + \nu$. Let $\mathrm{inv}(q, k)$ have binary representation $0\,.\,r_1 \dots r_\mu \overline{s_1 \cdots s_\nu}^{\,k}$, where the bar with superscript k indicates k repetitions of the block $s_1, \dots, s_\nu$. It follows that $0 \leq \frac{1}{q} - \mathrm{inv}(q, k) < \frac{1}{2^{n+\mu+\nu}}$, so that

$$\begin{aligned} 0 &\leq \frac{a}{q} - a \cdot \mathrm{inv}(q, k) \\ &\leq a \cdot (\frac{1}{q} - \mathrm{inv}(q, k)) \\ &\leq \frac{a}{2^{n+\mu+\nu}} \\ &\leq \frac{2^n}{2^{n+\mu+\nu}} = \frac{1}{2^{\mu+\nu}}. \end{aligned}$$

Thus the first $\mu + \nu$ bits (to the right of the decimal) of $a \cdot \mathrm{inv}(q, k)$ agree with those of $\frac{a}{q}$. By the previously mentioned theorem of [15], for all p satisfying $0 < \frac{p}{q} < 1$, $\gcd(p, q) = 1$, it is the case that $\frac{p}{q}$ has at most μ non-recurring bits and ν recurring bits to the right of the decimal. As well, if $\frac{p}{q} \geq 1$ or $\gcd(p, q) \neq 1$ then $\frac{p}{q} = K + \frac{p'}{q'}$ when $0 < \frac{p'}{q'} < 1$ and $\gcd(p', q') = 1$. Letting $q = 2^\mu Q, q' = 2^{\mu'} Q'$ and ν be the order of 2 modulo Q, and ν' be the order of 2 modulo Q', it is easy to show that $\mu' \leq \mu$ and $\nu' \leq \nu$. For instance, to see that $\nu' \leq \nu$ note that $2^\nu \equiv 1 \pmod{Q}$ so that $Q \mid 2^\nu - 1$; since $Q' \mid Q$ it follows that $Q' | 2^\nu - 1$ so $2^\nu \equiv 1 \pmod{Q'}$. The order of 2 modulo Q' is the least positive ν' satisfying $2^{\nu'} \equiv 1 \pmod{Q'}$. Hence $\nu' \leq \nu$. It is similarly easy to see that $\mu' \leq \mu$.

From this discussion, it follows that if the binary expansion of $a \cdot \mathrm{inv}(q, k)$ is $b_{m-1} \cdots b_1 b_0 . c_1 c_2 \cdots c_{\mu+\nu}$ and if $c_1 = 1$ or $c_2 = 1$ or $\dots$ or $c_{\mu+\nu} = 1$ then $\lceil \frac{a}{q} \rceil = \left(\sum_{i<m} b_i \cdot 2^i\right) + 1$ otherwise $\lceil \frac{a}{q} \rceil = \sum_{i<m} b_i \cdot 2^i$.

We now sketch polynomial size formulas to express $\lceil \frac{\vec{F}}{q} \rceil$, where $\vec{F}$ is a formula vector $(F_0, \dots, F_{T-1})$ representing an integer of length T.

Temporarily we abbreviate the expression $Mult^i(\vec{x}, \mathrm{inv}(q, \vec{\mu}, \nu, k))$ by $Mult^i$ for any $i < T + \mu + k \cdot \nu$. Define $Quot^i_{q,\mu,\nu,k}(x_0, \dots, x_{T-1})$ by

$$\begin{gathered} (\textstyle\bigwedge_{j<\mu+k\cdot\nu} \neg Mult^j \wedge Mult^{i+\mu+k\cdot\nu}) \vee \\ (\textstyle\bigvee_{j<\mu+k\cdot\nu} Mult^j \wedge [(\bigvee_{i'<i} \neg Mult^{i'+\mu+k\cdot\nu} \wedge Mult^{i+\mu+k\cdot\nu}) \vee \\ (\textstyle\bigwedge_{i'<i} Mult^{i'+\mu+k\cdot\nu} \wedge \neg Mult^{i+\mu+k\cdot\nu})]) \end{gathered}$$

The previous informal discussion provides the intuition behind the definition of the formula $Quot^i_{q,\mu,\nu,k}(x_0, \dots, x_{T-1})$. Namely one forms the product P of the integer x, represented by formula vector $\vec{x}$, with the integer $\mathrm{inv}(q, \mu, \nu, k) =$

$\mathrm{inv}(q, k) \cdot 2^{\mu+k\cdot\nu}$, represented by the formula vector $\mathrm{inv}(q, \vec{\mu}, \nu, k)$. Then we divide by $2^{\mu+k\cdot\nu}$ and check to see if any bits to the right of the decimal point are 1. If not, then the i^{th} bit of $\left\lceil \frac{x}{q} \right\rceil$ is the $i + \mu + k \cdot \nu - th$ bit of P. If so, then the i^{th} bit of $\left\lceil \frac{x}{q} \right\rceil$ is equal to the i^{th} bit of $\left\lfloor \frac{P}{2^{\mu+k\cdot\nu}} \right\rfloor + 1$. Clearly the formula $Quot^i_{q,\mu,\nu,k}(x_0, \ldots, x_{T-1})$ is of size polynomial in T, μ, ν, k. If the size of a given $CPLE^+$ refutation $I_1, \ldots, I_M$ is S, then to propositionally represent all expressions of the form $\left\lceil \frac{x}{q} \right\rceil$ occurring in the refutation sequence, it suffices to take $k = S$ in $Quot^i_{q,\mu,\nu,k}(x_0, \ldots, x_{T-1})$, and as $T \leq S$, it follows that all propositional formulas representing $C \supset Rep(I_j)$ are of size polynomial in S.

We can simulate in a Frege system the general division rule

$$\frac{E_1 \geq E_2}{\lceil \frac{E_1}{q} \rceil \geq \lceil \frac{E_2}{q} \rceil}$$

by extending Goerdt's [13] Frege system simulation of the multiplication rule

$$\frac{E_1 \geq E_2}{C \cdot E_1 \geq C \cdot E_2}$$

for fixed positive integer C. [Goerdt's proof was for the case of CP expressions, whereas E_1, E_2 are $CPLE$ expressions.] Since $Quot^i_{q,\mu,\nu,k}$ is defined in terms of $Mult^j(\vec{x}, inv(q, \vec{\mu}, \nu k))$ the propositional representation

$$\frac{C \supset Rep(E_1 \geq E_2)}{C \supset Rep(\lceil \frac{E_1}{q} \rceil \geq \lceil \frac{E_2}{q} \rceil})$$

has polynomial size Frege proofs. The same type of argument can be used to provide polynomial size Frege proofs of proportional representations of the simplification rules of $CPLE^+$

$$\frac{\lceil E+F \rceil \geq G}{\lceil E \rceil + \lceil F \rceil \geq G}$$

$$\frac{E \geq 0}{E \geq \lceil \frac{E}{C} \rceil}$$

$$\frac{1 \geq E}{\lceil \frac{E}{C} \rceil \geq E}$$

for $C \in \mathbf{N}^+$.

This concludes the sketch of proof of theorem 18. $\Box$

In [9], the second author showed that $CPLE^+$ p-simulates constant depth Frege systems. As observed by first author, this proof can be extended to prove that $CPLE^+$ p-simulates Frege systems (details will appear in the journal version of [9]). It thus follows that $CPLE^+$ and Frege systems are polynomially equivalent.

10 Threshold logic

In this section, we introduce propositional threshold logic and prove a completeness theorem. It is hoped that certain lower bound results for threshold circuits may be extended to yield lower bounds for proof size of propositional threshold logic and *a fortiori* for cutting planes.

Krajíček has introduced a different system FC of propositional threshold logic [17].

Definition 19 *Propositional threshold logic* is given as follows. Formula depth and size are defined inductively by:

i. a propositional variable x_i, $i \in \mathbf{N}$, is a formula of depth 0 and size 1.[3]

ii. if F is a formula then $\neg F$ is a formula of depth $1 + dp(F)$ and size $1 + size(F)$.

iii. if $F_1, \ldots, F_n$ are formulas and $1 \leq k \leq n$ then $T_k^n(F_1, \ldots, F_n)$ is a formula of depth $1 + max\{depth(F_i) : 1 \leq i \leq n\}$ and size $(n + k) + 1 + \sum_{1 \leq i \leq n} size(F_i)$.

Propositional threshold logic can be viewed as an extension of propositional logic in the connectives $\neg, \wedge, \vee$, the latter two connectives being defined by

$$\begin{aligned} \bigvee_{1 \leq i \leq n} F_i &\equiv T_1^n(F_1, \ldots, F_n) \\ \bigwedge_{1 \leq i \leq n} F_i &\equiv T_n^n(F_1, \ldots, F_n) \end{aligned}$$

A *cedent* is any sequence $F_1, \ldots, F_n$ of formulas separated by commas. Cedents are sometimes designated by $\Gamma, \Delta, \ldots$ (capital Greek letters). A *sequent* is given by $\Gamma \vdash \Delta$, where Γ, Δ are arbitrary cedents. The size [resp. depth] of a cedent $F_1, \ldots, F_n$ is $\sum_{1 \leq i \leq n} size(F_i)$ [resp. $\max_{1 \leq i \leq n}(depth(F_i))$]. The size [resp. depth] of a sequent $\Gamma \vdash \Delta$ is $size(\Gamma) + size(\Delta)$ [resp. $\max(depth(\Gamma), depth(\Delta))$]. The intended interpretation of the sequent $\Gamma \vdash \Delta$ is $\wedge\Gamma \rightarrow \vee\Delta$.

An *initial sequent* is of the form $F \vdash F$ where F is any formula of propositional threshold logic. The rules of inference of PTK, the sequent calculus of propositional threshold logic, are as follows.[4] By convention, $T_m^n(A_1, \ldots, A_n)$ is only defined if $1 \leq m \leq n$.

[3] One could as well allow propositional constants 1 (TRUE) and 0 (FALSE) of depth 0 and size 1.

[4] Gentzen's original sequent calculus for first order logic was called LK (*Logischer Kalkül*). The propositional sequent calculus with connectives $\neg$, $\vee$, $\wedge$ has sometimes been called PK (propositional Kalkül), so our *propositional threshold Kalkül* is denoted PTK.

structural rules

$$\text{weak left: } \frac{\Gamma, \Delta \vdash \Gamma'}{\Gamma, A, \Delta \vdash \Gamma'} \qquad \text{weak right: } \frac{\Gamma \vdash \Gamma', \Delta'}{\Gamma \vdash \Gamma', A, \Delta'}$$

$$\text{contract left: } \frac{\Gamma, A, A, \Delta \vdash \Gamma'}{\Gamma, A, \Delta \vdash \Gamma'} \qquad \text{contract right: } \frac{\Gamma \vdash \Gamma', A, A, \Delta'}{\Gamma \vdash \Gamma', A, \Delta'}$$

$$\text{permute left: } \frac{\Gamma, A, B, \Delta \vdash \Gamma'}{\Gamma, B, A, \Delta \vdash \Gamma'} \qquad \text{permute right: } \frac{\Gamma \vdash \Gamma', A, B, \Delta'}{\Gamma \vdash \Gamma', B, A, \Delta'}$$

cut rule

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

logical rules

$$\neg\text{-left: } \frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \qquad \neg\text{-right: } \frac{\Gamma \vdash A, \Delta}{\neg A, \Gamma \vdash \Delta}$$

$$\wedge\text{-left: } \frac{A_1, \dots, A_n, \Gamma \vdash \Delta}{T_n^n(A_1, \dots, A_n), \Gamma \vdash \Delta} \quad \text{for } n \geq 1$$

$$\wedge\text{-right: } \frac{\Gamma \vdash A_1, \Delta \qquad \cdots \qquad \Gamma \vdash A_n, \Delta}{\Gamma \vdash T_n^n(A_1, \dots, A_n), \Delta} \quad \text{for } n \geq 1$$

$$\vee\text{-left: } \frac{A_1, \Gamma \vdash \Delta \qquad \cdots \qquad A_n, \Gamma \vdash \Delta}{T_1^n(A_1, \dots A_n), \Gamma \vdash \Delta} \quad \text{for } n \geq 1$$

$$\vee\text{-right: } \frac{\Gamma \vdash A_1, \dots, A_n, \Delta}{\Gamma \vdash T_1^n(A_1, \dots, A_n), \Delta} \quad \text{for } n \geq 1$$

$$T_k^n\text{-left: } \frac{T_k^{n-1}(A_2, \dots, A_n), \Gamma \vdash \Delta \qquad A_1, T_{k-1}^{n-1}(A_2, \dots, A_n), \Gamma \vdash \Delta}{T_k^n(A_1, \dots, A_n), \Gamma \vdash \Delta} \quad \text{for } 2 \leq k < n$$

$$T_k^n\text{-right: } \frac{\Gamma \vdash A_1, T_{k-1}^{n-1}(A_2,\dots,A_n), \Delta \qquad \Gamma \vdash T_k^{n-1}(A_2,\dots,A_n), \Delta}{\Gamma \vdash T_k^n(A_1,\dots,A_n), \Delta} \quad \text{for } 2 \le k < n$$

Theorem 20 *PTK is sound.*

Proof. A *truth evaluation* is a mapping $\nu : \{x_i : i \in \mathbf{N}\} \to \{0,1\}$. By induction on formula depth, it is clear how to extend the truth evaluation ν to assign a truth value for each formula of propositional threshold logic. A formula is *valid* if it is true in every truth evaluation. Now by induction on the number of inferences in an PTK proof, it is straightforward to show that every theorem of PTK is valid. Thus PTK is sound. □

Theorem 21 *PTK is complete.*

Proof. Suppose that $\wedge\Gamma \to \vee\Delta$ is valid. We construct a finite tree T, each node of which is labeled by sequents, the root of T being labeled by $\Gamma \vdash \Delta$. The tree T is constructed so that

i. if $\Gamma'' \vdash \Delta''$ is a child of $\Gamma' \vdash \Delta'$ then $size(\Gamma'' \vdash \Delta'') < size(\Gamma' \vdash \Delta')$,

ii. if $\Gamma'' \vdash \Delta''$ is a child of $\Gamma' \vdash \Delta'$ and ν is a truth evaluation such that $\nu(\Gamma'' \vdash \Delta'') = 0$, then $\nu(\Gamma' \vdash \Delta') = 0$,

iii. if $\Gamma_1 \vdash \Delta_1, \dots, \Gamma_n \vdash \Delta_n$ are all the children of $\Gamma' \vdash \Delta'$, each of which has a proof in PTK, then there is a proof of $\Gamma' \vdash \Delta'$ in PTK,.

iv. each leaf of T is of the form $\Gamma' \vdash \Delta'$ where Γ', Δ' contain only propositional variables, and moreover some propositional variable x appears both in Γ' and in Δ'.

Given an already defined node $\Gamma' \vdash \Delta'$ of T, let F be the first formula of that sequent which is not a propositional variable. If F appears in Γ', then for notational simplicity we write Γ' as F, Π rather than Π, F, Π' when F is not necessarily the first formula of cedent Γ'. Similarly for Δ'.

<u>Case 1</u> F is $\neg A$, occurring in Γ'.

$$\frac{\Pi \vdash A, \Lambda}{\neg A, \Pi \vdash \Lambda}$$

<u>Case 2</u> F is $\neg A$, occurring in Δ'.

$$\frac{A, \Pi \vdash \Lambda}{\Pi \vdash \neg A, \Lambda}$$

Case 3 $\quad$ F is $T^n_k(A_1,\ldots,A_n)$, occurring in Γ'.

$$\frac{T^{n-1}_k(A_2,\ldots,A_n),\Pi\vdash\Lambda \qquad A,T^{n-1}_{k-1}(A_2,\ldots,A_n),\Pi\vdash\Lambda}{T^n_k(A_1,\ldots,A_n),\Pi\vdash\Lambda}$$

Case 4 $\quad$ F is $T^n_k(A_1,\ldots,A_n)$, occurring in Δ'.

$$\frac{\Pi\vdash A_1,T^{n-1}_k(A_2,\ldots,A_n),\Lambda \qquad \Pi\vdash T^{n-1}_{k-1}(A_2,\ldots,A_n),\Lambda}{\Pi\vdash T^n_k(A_1,\ldots,A_n),\Lambda}$$

Conditions (i),(ii) are straightforward to check and left to the reader. Condition (iii) for cases 1-4 follows immediately from the relevant logical rules. If condition (iv) does not hold, then there is a leaf of tree T labeled by a sequent $\Gamma'\vdash\Delta'$ whose cedents consist only of propositional variables, but which have no variable in common. Define the truth assignment ν by

$$\nu(x)=\begin{cases}1 & \text{if } x \text{ does not occur in } \Delta'\\ 0 & \text{otherwise}\end{cases}$$

Then $\nu(\Gamma'\vdash\Delta')=0$, and by iterating condition (ii) along the branch consisting of all nodes of tree T between leaf $\Gamma'\vdash\Delta'$ and root $\Gamma\vdash\Delta$, it follows that $\nu(\Gamma\vdash\Delta)=0$. But this contradicts the assumption that $\Gamma\vdash\Delta$ is valid. □

Remark 22 Since the above proof does not use the cut rule, it follows that cuts may be eliminated from proofs in PTK. Also note that cut-free PTK proofs satisfy the *subformula property*; namely, every formula in a cut-free PTK proof is a subformula of a formula in the endsequent.

The structural rules, cut rule, $\neg$ rules, $\wedge$ rules and $\vee$ rules are the same as for PTK. However, in place of the T^n_k rules of PTK, PTK' has the following rules.

$$T^n_k\text{-left1:}\ \frac{T^n_k(A_1,\ldots,A_n),\Gamma\vdash\Delta}{T^n_{k+\ell}(A_1,\ldots,A_n),\Gamma\vdash\Delta}\ \text{for } 1\le k<k+\ell\le n$$

$$T^n_k\text{-left2:}\ \frac{T^n_k(A_1,\ldots,A_n),\Gamma\vdash\Delta}{T^{n+m}_{k+m}(A_1,\ldots,A_n,B_1,\ldots,B_m),\Gamma\vdash\Delta}\ \text{for } 1\le k\le n<n+m$$

$$T^n_k\text{-left3:}\ \frac{\neg A_1,\ldots,\neg A_n,T^m_k(B_1,\ldots,B_m),\Gamma\vdash\Delta}{\neg A_1,\ldots,\neg A_n,T^{m+n}_k(A_1,\ldots,A_n,B_1,\ldots,B_m),\Gamma\vdash\Delta}\ \text{for } 1\le k\le m<m+n$$

$$T^n_k\text{-right1:}\ \frac{\Gamma\vdash T^n_k(A_1,\ldots,A_n),\Delta}{\Gamma\vdash T^{n+m}_k(A_1,\ldots,A_n,B_1,\ldots,B_m),\Delta}\ \text{for } 1\le k\le n<n+m$$

T_k^n-right2: $\dfrac{\Gamma \vdash T_k^n(A_1,\ldots,A_n),\Delta \qquad \Gamma \vdash T_\ell^m(B_1,\ldots,B_m),\Delta}{\Gamma \vdash T_{k+\ell}^{n+m}(A_1,\ldots,A_n,B_1,\ldots,B_m),\Delta}$ for $1 \leq k \leq m < m+n$

Theorem 23 *PTK' is sound.*

Proof. As in the proof of soundness of PTK. $\square$

Theorem 24 *PTK' is complete.*

Proof. As in the proof of completeness of PTK, suppose that $\wedge\Gamma \to \vee\Delta$ is valid. As before, construct a finite tree T, each node of which is labeled by sequents, the root of T being labeled by $\Gamma \vdash \Delta$, such that T satisfies the previous conditions (i) through (iv).

Given an already defined node $\Gamma' \vdash \Delta'$ of T, let F be the first formula of that sequent which is not a propositional variable. If F appears in Γ', then for notational simplicity we write Γ' as F, Π rather than Π, F, Π' when F is not necessarily the first formula of cedent Γ'. Similarly for Δ'.

<u>Case 1</u> F is $\neg A$, occurring in Γ'.

$$\frac{\Pi \vdash A, \Lambda}{\neg A, \Pi \vdash \Lambda}$$

<u>Case 2</u> F is $\neg A$, occurring in Δ'.

$$\frac{A, \Pi \vdash \Lambda}{\Pi \vdash \neg A, \Lambda}$$

<u>Case 3</u> F is $T_1^n(A_1,\ldots,A_n)$, occurring in Γ'.

$$\frac{A_1, \Pi \vdash \Lambda \qquad \cdots \qquad A_n, \Pi \vdash \Lambda}{T_1^n(A_1,\ldots,A_n), \Pi \vdash \Lambda}$$

<u>Case 4</u> F is $T_1^n(A_1,\ldots,A_n)$, occurring in Δ'.

$$\frac{\Pi \vdash A_1, \ldots A_n, \Lambda}{\Pi \vdash T_1^n(A_1,\ldots,A_n), \Lambda}$$

<u>Case 5</u> F is $T_n^n(A_1,\ldots,A_n)$, occurring in Γ'.

$$\frac{A_1, \ldots, A_n, \Pi \vdash \Lambda}{T_n^n(A_1,\ldots,A_n), \Pi \vdash \Lambda}$$

<u>Case 6</u> F is $T_n^n(A_1,\ldots,A_n)$, occurring in Δ'.

$$\frac{\Pi \vdash A_1, \Lambda \qquad \cdots \qquad \Pi \vdash A_n, \Lambda}{\Pi \vdash T_n^n(A_1,\ldots,A_n), \Lambda}$$

Case 7 $\quad F$ is $T^n_k(A_1,\ldots,A_n)$, occurring in Γ', where $1<k<n$.

$$\frac{T^{n-1}_k(A_2,\ldots,A_n),\Pi\vdash\Lambda \qquad A_1,T^{n-1}_{k-1}(A_2,\ldots,A_n),\Pi\vdash\Lambda}{T^n_k(A_1,\ldots,A_n),\Pi\vdash\Lambda}$$

Case 8 $\quad F$ is $T^n_k(A_1,\ldots,A_n)$, occurring in Δ', where $1<k<n$.

$$\frac{\Pi\vdash A_1,T^{n-1}_k(A_2,\ldots,A_n),\Lambda \qquad \Pi\vdash T^{n-1}_{k-1}(A_2,\ldots,A_n),\Lambda}{\Pi\vdash T^n_k(A_1,\ldots,A_n),\Lambda}$$

Conditions (i),(ii) are straightforward to check and left to the reader. Condition (iii) for cases 1-6 follows immediately from the relevant logical rules. The following is a proof for case 7.

$$\frac{\dfrac{\dfrac{T^{n-1}_k(A_2,\ldots,A_n),\Pi\vdash\Lambda}{\neg A_1,T^{n-1}_k(A_2,\ldots,A_n),\Pi\vdash\Lambda}}{\neg A_1,T^n_k(A_1,\ldots,A_n),\Pi\vdash\Lambda} \qquad \dfrac{A_1,T^{n-1}_{k-1}(A_2,\ldots,A_n),\Pi\vdash\Lambda}{A_1,T^n_k(A_1,\ldots,A_n),\Pi\vdash\Lambda}}{T^2_1(\neg A_1,A_1),T^n_k(A_1,\ldots,A_n),\Pi\vdash\Lambda}$$

Now one can prove $A_1\vdash A_1$

$$\frac{T^n_k(A_1,\ldots,A_n),\Pi\vdash\neg A_1,A_1,\Lambda}{T^n_k(A_1,\ldots,A_n),\Pi\vdash T^2_1(\neg A_1,A_1),\Lambda}$$

Applying the cut rule to the endsequents of these two proofs yields the desired

$$T^n_k(A_1,\ldots,A_n),\Pi\vdash\Lambda$$

The following is a proof of case 8.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Pi\vdash A_1,T^{n-1}_k(A_2,\ldots,A_n),\Lambda}{\Pi\vdash T^1_1(A_1),T^{n-1}_k(A_2,\ldots,A_n),\Lambda} \qquad \dfrac{\Pi\vdash T^{n-1}_{k-1}(A_2,\ldots,A_n),\Lambda}{\Pi\vdash T^{n-1}_{k-1}(A_2,\ldots,A_n),T^{n-1}_k(A_2,\ldots,A_n),\Lambda}}{\Pi\vdash T^n_k(A_1,\ldots,A_n),T^{n-1}_k(A_2,\ldots,A_n),\Lambda}}{\Pi\vdash T^n_k(A_1,\ldots,A_n),T^n_k(A_2,\ldots,A_n),\Lambda}}{\Pi\vdash T^n_k(A_1,\ldots,A_n),\Lambda}$$

This completes the verification of condition (iii). If condition (iv) does not hold, then as before, define a truth evaluation ν so that $\nu(\Gamma\vdash\Delta)=0$, contradicting the assumption. $\Box$

Remark 25 Unlike the proof of completeness of PTK, the cut rule was used in the previous proof. It is unclear whether PTK' enjoys cut elimination or the subformula property.

The systems FC ([17]), PTK and PTK' all p-simulate each other within a polynomial size factor and constant depth factor. For lack of space, we only state the results below (detailed proofs can be found in [6]).

Definition 26 Translate the FC formula A by the PTK' formula $\overline{A}$ as follows:

FC formula	PTK' formula
x	x
$\bigwedge_{i=1}^{n} A_i$	$T_n^n(\overline{A_1}, \ldots, \overline{A_n})$
$\bigvee_{i=1}^{n} A_i$	$T_1^n(\overline{A_1}, \ldots, \overline{A_n})$
$A \supset B$	$T_1^2(\neg\overline{A}, \overline{B})$
$A \equiv B$	$T_2^2(\overline{A \supset B}, \overline{B \supset A})$
$C_{n,k}(A_1, \ldots, A_n), 0 < k < n$	$T_2^2(T_k^n(\overline{A_1}, \ldots, \overline{A_n}), \neg T_{k+1}^n(\overline{A_1}, \ldots, \overline{A_n}))$
$C_{n,n}(A_1, \ldots, A_n)$	$T_n^n(\overline{A_1}, \ldots, \overline{A_n})$
$C_{n,0}(A_1, \ldots, A_n)$	$\neg T_1^n(\overline{A_1}, \ldots, \overline{A_n})$

Definition 27 Translate the PTK formula A by the FC formula $\tilde{A}$ as follows:

PTK formula	FC formula
x	x
$\neg A$	$\neg\tilde{A}$
$T_k^n(A_1, \ldots, A_n)$	$\bigvee_{i=k}^{n} C_{n,i}(\tilde{A}_1, \ldots, \tilde{A}_n)$

A PTK sequent $\Gamma \vdash \Delta$, which is equivalent to the formula

$$\bigwedge_{i=1}^{n} A_i \supset \bigvee_{j=1}^{m} B_j$$

is translated by the FC formula

$$\bigwedge_{i=1}^{n} \tilde{A}_i \supset \bigvee_{j=1}^{m} \tilde{B}_j.$$

Proposition 28 *Suppose that $\langle P_n : n \geq 1 \rangle$ is a family of PTK proofs, where P_n is a depth $d(n)$, size $s(n)$ proof of ϕ_n. Then there exists a constant c for which there exists a family $\langle P'_n : n \geq 1 \rangle$ of FC proofs, where P'_n is a depth $c + d(n)$, size $s(n)^c$ proof of $\tilde{\phi}_n$.*

Proposition 29 *Suppose that $\langle P_n : n \geq 1 \rangle$ is a family of PTK' proofs, where P_n is a depth $d(n)$, size $s(n)$ proof of ϕ_n. Then there exists a constant c for which there exists a family $\langle P'_n : n \geq 1 \rangle$ of PTK proofs, where P'_n is a depth $c + d(n)$, size $s(n)^c$ proof of ϕ_n.*

Proposition 30 *Suppose that $\langle P_n : n \geq 1 \rangle$ is a family of FC proofs, where P_n is a depth $d(n)$, size $s(n)$ proof of ϕ_n. Then there exists a constant c for which there exists a family $\langle P'_n : n \geq 1 \rangle$ of PTK' proofs, where P'_n is a depth $c + d(n)$, size $c \cdot s(n)$ proof of ϕ_n.*

11 Appendix.

Here we present the proof of Theorem 7.
Proof. Using limited extension, for $0 \leq i, j \leq n$ introduce new atoms r_{ij} to abbreviate $q_i \wedge p_{ij}$.

Let

$$\begin{aligned} B_s &= \textstyle\sum_{0 \leq i < j \leq s} r_{ij} \\ S_s &= \textstyle\sum_{0 \leq i \leq s < j} r_{ij} \\ Q_s &= \textstyle\sum_{0 \leq i \leq s} q_i \end{aligned}$$

Then $B_0 = 0$, $S_0 = 1$, and by induction on s it will be shown that

$$S_s + 2B_s = 2Q_s - 1.$$

Since $S_n = 0$ it follows that

$$2B_n = 2Q_n - 1.$$

But the left side is even and the right side is odd, a contradiction. We shall formalize this argument in $CPLE$; for space reasons we omit some of the details.

Claim. $r_{ij} = r_{ji}$

Proof. By hypothesis we have

$$\overline{p_{ij}} \vee p_{ji} \text{ for } 0 \leq i, j \leq n$$

hence

$$1 - p_{ij} + p_{ji} \geq 1$$

and so

$$p_{ji} \geq p_{ij}.$$

Similarly $p_{ij} \geq p_{ji}$. From $\overline{q_i} \vee \overline{p_{ij}} \vee q_j$ we have

$$\begin{aligned} &1 - q_i + 1 - p_{ij} + q_j \geq 1 \\ &1 + q_j \geq q_i + p_{ij} \end{aligned}$$

Now

1. $r_{ij} \geq r_{ij}$
2. $1 \geq 1$
3. $r_{ij} + (1 - r_{ij}) \geq 1$, addition of (1), (2) and simplification
4. $q_i \geq r_{ij}$
5. $p_{ij} \geq r_{ij}$
6. $q_i + (1 - r_{ij}) \geq 1$, addition of (3), (4) and simplification
7. $p_{ij} + (1 - r_{ij}) \geq 1$, addition of (3), (5) and simplification
8. $q_i + p_{ij} + 2(1 - r_{ij}) \geq 2$, addition of (6) (7)
9. $q_i + p_{ij} - 1 + 2(1 - r_{ij}) \geq 1$, simplification of (8)
10. $q_j \geq q_i + p_{ij} - 1$
11. $q_j + 2(1 - r_{ij}) \geq 1$, addition of (9), (10) and simplification
12. $p_{ji} \geq p_{ij}$
13. $p_{ji} + (1 - r_{ij}) \geq 1$, addition of (12), (7) and simplification
14. $q_j + p_{ji} + 3(1 - r_{ij}) \geq 2$, addition of (11), (13)
15. $r_{ji} \geq q_j + p_{ji} - 1$
16. $r_{ji} + 3(1 - r_{ij}) \geq 1$, addition of (15), (14) and simplification
17. $r_{ji} \geq 0$
18. $2r_{ji} \geq 0$, multiplication of (17) by 2
19. $3r_{ji} + 3(1 - r_{ij}) \geq 1$, addition of (16) (18)
20. $r_{ji} + (1 - r_{ij}) \geq 1$, division of (19) by 3
21. $r_{ji} \geq r_{ij}$, simplification of (20). $\square$

Following our earlier proof outline, we intend to show that $S_s + 2B_s = 2Q_s - 1$ for $0 \leq s \leq n$. To this end, it first must be shown that

$$\sum_{j=1}^{n} r_{0j} = 1$$

$$\sum_{j=0}^{n-1} r_{nj} = 0$$

and for fixed $0 < i < n$

$$\sum_{0 \le j \le n, j \ne i} r_{ij} = 2q_i.$$

The $CPLE$ proofs of these three equalities actually consist of proving six inequalities; namely, the following six claims:

Claim. $\sum_{j=1}^{n} r_{0j} \ge 1$

Claim. $1 \ge \sum_{j=1}^{n} r_{0j}$

Claim. $\sum_{j=0}^{n-1} r_{nj} \ge 0$

Claim. $0 \ge \sum_{j=0}^{n-1} r_{nj}$

Claim. $\sum_{j \ne i} r_{ij} \ge 2q_i$, for $0 < i < n$.

Claim. $2q_i \ge \sum_{j \ne i} r_{ij}$, for $0 < i < n$

The proof of $r_{ji} \ge r_{ij}$ was already given in complete detail; the $CPLE$ proofs of the above six claims are of similar length and detail. We therefore omit their proofs for space reasons and leave it to the reader to supply the details of these $CPLE$ proofs.

Claim. For $0 \le s \le n$, $S_s + 2B_s = 2Q_s - 1$.

Proof. By induction on s. If $s = 0$, then it follows from earlier claim ($\sum_{j \ne 0} r_{0j} = 1$, $0 \ge r_{00}$) that

$$S_0 = 1, \quad B_0 = 0, \quad Q_0 = 1$$

hence

$$S_0 + 2B_0 = 2Q_0 - 1.$$

Suppose the claim holds for s. Now by regrouping, $S_{s+1} + 2B_{s+1}$ is the sum

$$2 \sum_{i<j \le s} r_{ij} + \sum_{i \le s < j} r_{ij} + (2 \sum_{i<s+1} r_{i,s+1} - \sum_{i \le s} r_{i,s+1} + \sum_{j>s+1} r_{s+1,j})$$

Using an earlier claim that $r_{s+1,j} = r_{j,s+1}$, the expression in parentheses is equal to

$$\sum_{j \le s} r_{s+1,j} + \sum_{j>s+1} r_{s+1,j} = \sum_{j \ne s+1} r_{s+1,j}.$$

By an earlier claim,

$$\sum_{j \ne s+1} r_{s+1,j} = 2q_{s+1}.$$

Thus

$$S_{s+1} + 2B_{s+1} = S_s + 2B_s + 2q_{s+1} = 2Q_s + 2q_{s+1} = 2Q_{s+1}$$

This inductive step establishes the claim. $\square$
Now taking $s = n$, we have

$$S_n + 2B_n = 2Q_n - 1.$$

But as $S_n = 0$, we have

$$2B_n = 2Q_n - 1.$$

Dividing the inequality

$$2B_n \geq 2Q_n - 1$$

by 2, we have

$$B_n \geq Q_n.$$

Similarly, dividing the inequality

$$2Q_n \geq 2B_n + 1$$

by 2 yields

$$Q_n \geq B_n + 1.$$

From the above inequalities it follows that

$$B_n \geq B_n + 1$$

hence $0 \geq 1$, the desired contradiction. That completes the construction of the polynomial size $CPLE$ proofs of STC_n. $\square$

References

[1] M. Ajtai. Parity and the pigeonhole principle. In S.R. Buss and P.J. Scott, editors, *Feasible Mathematics*, pages 1–24. Birkhäuser, 1990.

[2] M. Ajtai and R. Fagin. Reachability is harder for directed than for undirected finite graphs, *Journal of Symbolic Logic*, 55:113–150, 1990.

[3] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, P. Pudlák, and A. Woods. Exponential lower bounds for the pigeonhole principle. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, Victoria*, 1992.

[4] P. Beame, S. Cook., C. Papadimitriou and T. Pitassi. The relative complexity of NP search problems. Manuscript, November 1993.

[5] S. Buss. The propositional pigeonhole principle has polynomial size Frege proofs. *Journal of Symbolic Logic*, 52:916 – 927, 1987.

[6] S. Buss and P. Clote. Threshold logic proof systems. Manuscript, May 1995.

[7] S. Buss and G. Turán. Resolution proofs of generalized pigeonhole principles. *Theoretical Computer Science*, 62:311 – 317, 1988.

[8] P. Clote and J. Krajíček, eds. *Arithmetic, Proof Theory and Computational Complexity*. Oxford University Press, 1993. 428 pages.

[9] P. Clote. Cutting planes and constant depth Frege proofs. In *Proceedings of 7th Annual IEEE Symposium on Logic in Computer Science*, 1992. pp. 296–307.

[10] P. Clote. Cutting plane and Frege proofs. To appear in *Information and Computation*.

[11] S. A. Cook and R. Reckhow. On the relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36 – 50, 1977.

[12] W. Cook, C.R. Coullard, and G. Turan. On the complexity of cutting plane proofs. *Discrete Applied Mathematics*, 18:25–38, 1987.

[13] A. Goerdt. Cutting plane versus frege proof systems. In Egon Börger, editor, *Computer Science Logic 1990*, volume 552, pages 174–194, 1992. Springer Lecture Notes in Computer Science.

[14] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297 – 305, 1985.

[15] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford, Clarendon Press, 1979. Fifth edition.

[16] R. Impagliazzo, T. Pitassi and A. Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Proceedings of 9th Annual IEEE Symposium on Logic in Computer Science*, 1994. pp. 220–228.

[17] J. Krajíček. On Frege and extended Frege systems. In P. Clote and J. Remmel, editors, *Feasible Mathematics II*, pages 284—319. Birkhäuser, 1994.

[18] C.H. Papadimitriou. On the complexity of the parity argument and other inefficient proofs of existence. *J. Comput. System Sci.* 48 (1994) 498-532.

[19] C. H. Papadimitriou and K. Steiglitz. *Combinatorial Optimization*. Prentice-Hall, 1982.

[20] J. B. Paris and A. J. Wilkie. Counting problems in bounded arithmetic. In C. A. di Prisco, editor, *Methods in Mathematical Logic*, pages 317 – 340. 1983. Springer Lecture Notes in Mathematics 1130.

[21] A. Urquhart. Hard examples for resolution. *Journal of the Association of Computing Machinery*, 34(1):209 – 219, 1987.