A note on Degen's generalization of the pigeonhole principle, st-connectivity, and odd charged graphs

Peter Clote* Anton Setzer †

21 October 1996

1 Introduction

As witnessed by this proceedings, there is currently much interest in the analysis of proof size for tautology families in certain proof systems for propositional logic. The reason is twofold: (1) the analysis of proof systems leads to a better understanding of efficiency issues for theorem provers and (2) the development of new combinatorial methods in establishing proof size lower bounds for propositional proof systems may help in better understanding and solving difficult problems in complexity theory (it is well-known that $NP = co - NP$ if and only if there is a sound, complete propositional proof system which furnishes polynomial size proofs for all tautologies).

In this paper, we consider several proof systems (resolution, cutting planes, and a multiplicative extension of cutting planes), and analyze the proof size of certain combinatorial statements related to the pigeonhole principle and to graph theoretic principles.

The well-known pigeonhole principle PHP_k is given by

$$\bigwedge_{0\leq i\leq k} \bigvee_{0\leq j<k} p_{i,j} \rightarrow \bigvee_{0\leq i<i'\leq k} \bigvee_{0\leq j<k} (p_{i,j} \wedge p_{i',j}).$$

In [7], W. Degen gave a natural generalization of the pigeonhole principle, which states that for positive integers m, k if f is a function mapping $\{0,\ldots,m\cdot k\}$ into $\{0,\ldots,k-1\}$ then there is $j<k$ for which $f^{-1}(j)$ has size greater than m. Formulated in propositional logic, this is given by a family $\{D_{m,k} : m,k \in \mathbf{N} - \{0\}\}$ where $D_{m,k}$ is

$$\bigwedge_{0\leq i\leq m\cdot k} \bigvee_{0\leq j<k} p_{i,j} \rightarrow \bigvee_{0\leq j<k} \bigvee_{I\in\binom{m\cdot k+1}{m+1}} \bigwedge_{i\in I} p_{i,j}.$$

W. Degen showed that for m fixed, over ZF set theory without the axiom of choice, the set theoretic analogue of $\{D_{m,k} : k\in\mathbf{N}\}$ is properly weaker than the set theoretic analogue of $\{D_{m+1,k} : k \in \mathbf{N}\}$. The pigeonhole principle, Ajtai's parity principle, and various modular counting principles have been investigated in boolean circuit complexity and in propositional proof theory, the idea being that counting is

*Part of this research supported by NSF CCR-9408090 and US-Czech Science and Technology Grant 93-205.
Mailing address: Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstraße 67, D-80538 München, GERMANY, clote@informatik.uni-muenchen.de
Key words and phrases: boolean circuit, monotonic circuit, propositional logic, connectivity, charged graph.
†Mailing address: Mathematisches Institut, Ludwig-Maximilians-Universität München, Theresienstraße 39, D-80333 München, Germany setzer@rz.mathematik.uni-muenchen.de

a difficult notion to capture in finite depth circuits or proofs. Motivated by Degen's surprising hierarchy result in set theory, we investigated his principle in propositional logic. This paper establishes that Degen's principle is of the same strength as the pigeonhole principle. Additionally, we consider a propositional logic formulation of st-connectivity, and using the Karchmer-Wigderson lower bound for monotonic circuits, furnish an example where tree-like resolution is weaker than resolution (by a different proof, a separation between tree-like resolution and resolution was first given by Tseitin). Finally, we prove some fragmentary results concerned with Tseitin's odd-charged graph tautologies, and with a monotonic polynomial calculus for monotonic Gentzen sequent calculus.

2 Preliminaries

We refer the reader to Krajíček's book [11] for any undefined terminology. Resolution is a sound, complete refutation system for conjunctive normal form (CNF) formulas – *sound*, in that if CNF formula ϕ has a resolution refutation, then ϕ is unsatisfiable, and *complete*, in that every unsatisfiable CNF formula has a resolution refutation. CNF formulas are represented in resolution by a set of clauses containing literals (a literal is a propositional variable or its negation), where the clause $\{\alpha_1, \ldots, \alpha_n\}$ represents $\alpha_1 \vee \cdots \vee \alpha_n$. The resolution rule allows the derivation of clause $C \cup D$ from the clauses $C \cup \{x\}$ and $D \cup \{\overline{x}\}$. A resolution derivation from $C_1, \ldots, C_n$ is a sequence of clauses $D_1, \ldots, D_m$, such that every D_i is either one of the C's, or obtained from D_j, D_k for $j, k < i$ by the resolution rule. A resolution refutation of clauses $C_1, \ldots, C_n$ is a derivation of the empty clause from $C_1, \ldots, C_n$. By abuse of notation, we say that a disjunctive normal form formula has a resolution proof, if its negation (a CNF formula) has a resolution refutation. A resolution derivation is tree-like if every clause is used at most once in an application of the resolution rule (multiple resolutions on the same clause require multiple derivations of that clause).

The cutting plane proof system, CP, is a sound and complete refutation system for CNF formulas. Propositional variable x_i is represented by itself; $\neg x_i$ is represented by $1 - x_i$; a disjunction $\bigvee_{i \in I} \alpha_i$ of literals is represented by $\sum_{i \in I} R(\alpha_i) \geq 1$, where $R(\alpha_i)$ represents the literal α_i; finally, a CNF formula $\bigwedge_{i \in I} \bigvee_{j \in J_i} \alpha_{i,j}$ is represented by the family

$$\sum_{j \in J_i} R(\alpha_{i,j}) \geq 1$$

of linear inequalities. Without loss of generality, we assume all linear inequalities are of the form $\sum a_i \cdot x_i \geq A$ where $a_i, A \in \mathbf{Z}$. The a_i are the coefficients of the propositional variables, and for lack of a better term, we call A the integer sum. The *axioms* of CP are $x_i \geq 0$, $-x_i \geq -1$. The *rules of inference* of CP are

- addition $\dfrac{\sum a_i \cdot x_i \geq A \qquad \sum b_i \cdot x_i \geq B}{\sum (a_i + b_i) \cdot x_i \geq A + B}$

- division $\dfrac{\sum (c \cdot a_i) \cdot x_i \geq A}{\sum a_i \cdot x_i \geq \lceil \frac{A}{c} \rceil}$

where integer $c > 1$,

$$\bullet \text{ multiplication } \frac{\sum a_i \cdot x_i \geq A}{\sum (c \cdot a_i) \cdot x_i \geq c \cdot A}$$

where integer $c > 1$.

A derivation D for inequalities I from inequalities $I_1, \ldots, I_m$ is a sequence $D = (D_0, \ldots, D_n)$ such that for all $i \leq n$ either D_i is an axiom, or one of $I_i, \ldots, I_m$ or inferred from D_j, D_k for $j, k < i$ by means of a rule of inference. A *refutation* of $I_1, \ldots, I_m$ is a derivation of $0 \geq 1$ from $I_1, \ldots, I_m$. As in the case of resolution, by abuse of terminology, we say that a disjunctive normal form formula has a CP proof if its negation has a CP refutation. The *size* of a CP refutation is the sum over all inequalities $\sum a_i \cdot x_i \geq A$ occurring in the refutation of $\sum |a_i| + |A|$, where $|A|$ indicates the length of the binary representation of A. It is easy to see [6] that CP is a sound extension of resolution, hence complete.

3 Cutting plane proofs of Degen's principle

By $E_{m,k}$ we denote the CP inequalities corresponding to the CNF formula $\neg D_{m,k}$. Thus $E_{m,k}$ is

$$\sum_{j=0}^{k-1} p_{i,j} \geq 1$$

for $0 \leq i \leq m \cdot k$, together with

$$-p_{i_1,j} - p_{i_2,j} - \cdots - p_{i_{k+1},j} \geq -m$$

for $0 \leq j < k$ and $0 \leq i_1 < i_2 < \cdots < i_{m+1} \leq m \cdot k$.

Theorem 1 *There are $O(k^5)$ size CP refutations of $E_{2,k}$.*

Proof By assumption from $E_{2,k}$, for all $0 \leq i_1 < i_2 < i_3 \leq 2k$ and all $0 \leq r < k$,

$$2 \geq p_{i_1,r} + p_{i_2,r} + p_{i_3,r}.$$

Claim 2 *For all $0 \leq i_1 < i_2 < i_3 < i_4 \leq 2k$ and all $0 \leq r < k$,*

$$2 \geq p_{i_1,r} + p_{i_2,r} + p_{i_3,r} + p_{i_4,r}.$$

Proof of claim: Fix i_1, i_2, i_3, i_4 and r, and temporarily, set $a = p_{i_1,r}$, $b = p_{i_2,r}$, $c = p_{i_3,r}$, $d = p_{i_4,r}$. By assumption from $E_{2,k}$, we have

$$\begin{aligned} 2 &\geq a + b + c \\ 2 &\geq b + c + d \\ 2 &\geq a + b + d \\ 2 &\geq a + c + d \end{aligned}$$

and so by addition

$$8 \geq 3a + 3b + 3c + 3d$$

and hence by division by 3

$$2 = \lfloor 8/3 \rfloor \geq a + b + c + d.$$

□

For later generalization, note that the pattern of the previous inequalities is of the following form:

$$\begin{array}{cccc} + & + & + & - \\ - & + & + & + \\ + & - & + & + \\ + & + & - & + \end{array}$$

where + [resp. $-$] indicates presence [resp. absence] of the corresponding element (i.e. in the first row, there is a, b, c but no d present). In this manner, with $O(k^5)$ (i.e. order $k \cdot \binom{2k+1}{4}$) many proof lines we can show that

$$2 \geq p_{i_1,r} + \cdots + p_{i_4,r}$$

for all rows $0 \leq r < k$ and all 4-tuples $0 \leq i_1 < i_2 < i_3 < i_4 \leq 2 \cdot k$ from that row. In a similar manner, we could show by a proof of $O(k^{s+1})$ lines, that $2 \geq p_{i_1,r} + \cdots + p_{i_s,r}$, for all rows $0 \leq r < k$ and all distinct s-tuples $i_1, \ldots, i_s$. However, the overall proof would then be of $\sum_{i=5}^{2k+1} O(k^i)$ lines, hence of exponential size. For that reason, in the following claim, we consider sets $i_1, \ldots, i_s$ of a particular form. Define integers $x_1, \ldots, x_m$ to be *consecutive* if for all $1 \leq j < m$, $x_{j+1} = x_j + 1$.

Claim 3 *Assume that $3 \leq s \leq 2k$ and for all $0 \leq i_1 < \cdots < i_s \leq 2k$ such that $i_2, \ldots, i_s$ are consecutive, and for all $0 \leq r < k$, it is the case that*

$$2 \geq p_{i_1,r} + \cdots p_{i_s,r}.$$

Then for all $0 \leq i_1 < \cdots < i_{s+1} \leq 2k$ such that $i_2, \ldots, i_{s+1}$ are consecutive, and for all $0 \leq r < k$, it is the case that

$$2 \geq p_{i_1,r} + \cdots p_{i_{s+1},r}.$$

Proof of claim: Fix $0 \leq i_1 < \cdots < i_{s+1}$ and r. By assumption

$$\begin{array}{rcl} 2 & \geq & p_{i_1,r} + \cdots + p_{i_s,r} \\ 2 & \geq & p_{i_2,r} + \cdots + p_{i_{s+1},r} \\ 2 & \geq & p_{i_1,r} + p_{i_3,r} + \cdots + p_{i_{s+1},r} \\ 2 & \geq & p_{i_1,r} + p_{i_2,r} + p_{i_{s+1},r} \end{array}$$

Note that the pattern in the previous inequalities is of the following form:

$$\begin{array}{cccccc} + & + & + & \cdots & + & - \\ - & + & + & \cdots & + & + \\ + & - & + & \cdots & + & + \\ + & + & - & \cdots & - & + \end{array}$$

The first three inequalities hold by the assumption in the claim, and the fourth (which contains only 3 terms) holds by assumption of $E_{2,k}$. By addition, we have

$$8 \geq 3p_{i_1,r} + \cdots + 3p_{i_{s+1},r}$$

and hence by division by 3

$$2 = \lfloor 8/3 \rfloor \geq p_{i_1,r} + \cdots + p_{i_{s+1},r}.$$

□

By induction on s, using the base case $2 \geq p_{i_1,r} + p_{i_2,r}$ for all $0 \leq r < k$ and $0 \leq i_1 < i_2 \leq 2 \cdot k$ (given by $E_{2,k}$), and applying Claim 3 in the inductive case, it follows that for all $0 \leq r < k$,

$$2 \geq p_{0,r} + \cdots + p_{2k,r}.$$

Adding all k inequalities (one for each $0 \leq r < k$), we have

$$2k \geq \sum_{i=0}^{2k} \sum_{j=0}^{k-1} p_{i,j}.$$

However, by hypothesis $E_{2,k}$, for each fixed $0 \leq i \leq 2k$, $\sum_{j=0}^{k-1} p_{i,j} \geq 1$, and by addition of these $2k+1$ inequalities (one for each $0 \leq i \leq 2k$), we have

$$\sum_{i=0}^{2k} \sum_{j=0}^{k-1} p_{i,j} \geq 2k+1.$$

Thus we arrive at the contradiction $2k \geq 2k+1$. Rewriting the above proof in the required normal form $\sum a_{i,j} \cdot p_{i,j} \geq A$ we obtain a derivation of $0 \geq 1$ from $E_{2,k}$.

What is the size of this CP refutation? In Claim 3, for each fixed $s \geq 3$, there are at most $O(2k)$ choices of $0 \leq i_1 \leq 2k$ and (by consecutivity) at most $O(2k)$ choices of the remaining consecutive $0 \leq i_2, \ldots, i_{s+1} \leq 2k$ with $i_1 < i_2$. There are k many values of $0 \leq r < k$, so altogether this makes $O(k^3)$ proof lines for establishing the claim in going from s to $s+1$. As $s \leq 2k$, the entire proof requires $O(k^4)$ lines. The coefficients of the propositional variables have size bounded by 2 (the largest coefficient is 3). Except in the last two steps, where at most $2k+1$ inequalities are added (producing sums $2k$ and $2k+1$), all sums are bounded by 8. Each inequality (proof line) has size $O(k)$, since coefficients of the variables are bounded by a constant, the integer sum is bounded by $2k+1$, and there are at most $O(k)$ variables per inequality. Thus the proof size is $O(k^4 \cdot k)$ or $O(k^5)$. ∎

Theorem 4 *For $m \geq 2$, there are $O(n^{m+3})$ size CP refutations of $E_{m,k}$, where the constant in the O-notation depends on m, and $O(n^{m+4})$ size CP refutations, where the constant is independent of n, m.*

Proof We generalize the proof of the previous theorem.

Claim 5 *Assume that $3 \leq s \leq mk$ and for all $0 \leq i_1 < \cdots < i_s \leq mk$ such that $i_m, \ldots, i_s$ are consecutive, and for all $0 \leq r < k$, it is the case that*

$$m \geq p_{i_1,r} + \cdots + p_{i_s,r}.$$

Then for all $0 \leq i_1 < \cdots < i_{s+1} \leq mk$ such that $i_m, \ldots, i_{s+1}$ are consecutive, and for all $0 \leq r < k$, it is the case that

$$m \geq p_{i_1,r} + \cdots + p_{i_{s+1},r}.$$

Proof of claim: Fix $i_1 < \cdots < i_{s+1}$ and r. We have the following $m+2$ inequalities:

$$\begin{array}{rcl}
m & \geq & p_{i_1,r} + \cdots + p_{i_s,r} \\
m & \geq & p_{i_2,r} + \cdots + p_{i_{s+1},r} \\
m & \geq & p_{i_1,r} + p_{i_3,r} + \cdots + p_{i_{s+1},r} \\
m & \geq & p_{i_1,r} + p_{i_2,r} + p_{i_4,r} + \cdots + p_{i_{s+1},r} \\
m & \geq & p_{i_1,r} + \cdots + p_{i_3,r} + p_{i_5,r} + \cdots + p_{i_{s+1},r} \\
m & \geq & p_{i_1,r} + \cdots + p_{i_4,r} + p_{i_6,r} + \cdots + p_{i_{s+1},r} \\
 & \vdots & \\
m & \geq & p_{i_1,r} + \cdots + p_{i_{m-1},r} + p_{i_{m+1},r} + \cdots + p_{i_{s+1},r} \\
m & \geq & p_{i_1,r} + \cdots + p_{i_m,r} + p_{i_{s+1},r}
\end{array}$$

The pattern of terms in the $m+2$ inequalities above is of the form:

$$
\begin{array}{ccccccccc}
+ & + & + & \cdots & + & + & + & + & - \\
- & + & + & \cdots & + & + & + & + & + \\
+ & - & + & \cdots & + & + & + & + & + \\
+ & + & - & \cdots & + & + & + & + & + \\
. & . & . & \cdots & . & . & . & . & . \\
. & . & . & \cdots & . & . & . & . & . \\
. & . & . & \cdots & . & . & . & . & . \\
+ & + & + & \cdots & + & - & + & + & + \\
+ & + & + & \cdots & + & + & - & - & +
\end{array}
$$

Removal of any of the first $m-1$ summands in the term $p_{i_1,r}+\cdots+p_{i_{s+1},r}$ produces a term where $p_{i_m,r},\ldots,p_{i_{s+1},r}$ are consecutive. This observation, with the assumption in the claim, justifies the first $m+1$ inequalities. The last inequality (which contains only $m+1$ terms) holds by assumption of $E_{m,k}$. By addition, we have

$$m\cdot(m+2)\geq(m+1)\cdot(p_{i_1,r}+\cdots+p_{i_{s+1},r})$$

and hence by division by $m+1$

$$m=\lfloor\frac{m(m+2)}{m+1}\rfloor\geq p_{i_1,r}+\cdots+p_{i_{s+1},r}.$$

□

Adding k inequalities $m\geq p_{0,r}+\cdots+p_{mk,r}$, we have $mk\geq\sum_{i=0}^{mk}\sum_{j=0}^{k-1}p_{i,j}$. Similarly adding the $mk+1$ inequalities $p_{i,0}+\cdots+p_{i,k-1}\geq 1$, we have $\sum_{i=0}^{mk}\sum_{j=0}^{k-1}p_{i,j}\geq mk+1$. Finally, we have the desired contradiction $mk\geq mk+1$.

Let $n=mk$. In Claim 5, for each fixed $3\leq s\leq mk$, there are at most $O(n^m)$ choices of $0\leq i_1<\cdots<i_s\leq mk$ for which $i_m,\ldots,i_s$ are consecutive (such sequences are stipulated by choice of $i_1,\ldots,i_m$). There are k many values of $0\leq r<k$, so altogether this makes $O(n^{m+1})$ proof lines for establishing the claim in going from s to $s+1$. As $s\leq mk$, the entire proof requires $O(n^{m+2})$ lines. In each proof line (inequality), there are at most $mk+1$ variables (hence $O(k)$, if m is held as a constant), while the coefficients of the variables are bounded by $m+1$, and the integer sum (except in the last steps where k inequalities are added together) are bounded by $m(m+2)$. In the last steps involving addition of k inequalities, the integer sum is bounded by $mk+1$, hence the size of each inequality (proof line) in the proof is bounded by $O(n)$ if m is held as a constant. It follows that the proof size is $O(n^{m+2}\cdot n)$ or $O(n^{m+3})$, where the constant in the O-notation depends only on m. The previous considerations yield that the proof size is $O(n^{m+3}\cdot\log m)$ or $O(n^{m+4})$, where the constant in the O-notation is an absolute constant independent of n,m. ∎

Corollary 6 *There are polynomial size CP refutations of* $\{E_{m,k}:m\geq 2,k\geq 1\}$.

Proof Each application of Claim 3 requires $m+1$ additions and one division. Taking this into account, as in the previous analysis, there are then $O(m\cdot n^{m+3})$ proof lines, each of size $O(\log m)$, so the refutation size of $E_{m,k}$ is $O(n^{m+4})$, where the constant in the O-notation is independent of n,m,k. On the other hand, the size of $E_{n,k}$ is $O(n^{m+1})$. Thus the refutation size is polynomial in the size of the formula being refuted. ∎

Let $[n]^r$ [resp. $[X]^r$] denote the set of r-element subsets of $\{0,\ldots,n-1\}$ [resp. X]. The Erdös-Rado partition calculus notation $n\rightarrow(m)_k^r$ means that for any partition $f : [n]^r \to \{0, \ldots, k-1\}$, there is a size m subset X of $\{0, \ldots, n-1\}$ on which f is constant; i.e. $f([X]^r)$ has cardinality 1. Using the Erdös-Rado partition calculus notation, PHP_n can be written as

$$n + 1 \to (2)^1_n$$

and Degen's principle as

$$mk + 1 \to (m+1)^1_k.$$

Question 7 *Are there polynomial size CP proofs of versions of Ramsey's theorem*

$$n + 1 \to (m)^r_k$$

for appropriate n, m, r, k?

In [3], V. Chvatal gave a cutting planes proof of the instance

$$\begin{array}{lcl} 15 & \not\to & (3)^1_2 \\ 16 & \to & (3)^1_2 \end{array}$$

of Ramsey's theorem, and claimed that a general form of Ramsey's theorem could be proved in cutting planes. Since no details were given, it is unclear whether Chvatal's intended proof was indeed polynomial size. In [13], P. Pudlák has shown the existence of polynomial size constant depth Frege proofs of an appropriate formulation of Ramsey's theorem. It appears unlikely that CP (or $CPLE$, an extension of cutting planes with limited extension, see [2]) can polynomially simulate constant depth Frege systems. Hence it would be of interest to extend the counting arguments within CP to prove Ramsey's theorem and stronger combinatorial theorems.

4 Polynomial equivalence over resolution between Degen's principle and the pigeonhole principle

Denote the cardinality of a finite set S by $||S||$.

Definition 8 *The proof system Q* p-simulates *the proof system P if there is a polynomial time computable function f such that for all x, y, if x is a P-proof of y then $f(x, y)$ is a Q-proof of (the translation of) of y. Proof systems P, Q are* p-equivalent *if each p-simulates the other.*

In this section, we show that over resolution, the clausal form of Degen's principle

$$(\forall f : \{0, \ldots, mk\} \to \{0, \ldots, k-1\})(\exists i < k)(||f^{-1}(i)|| \geq m + 1)$$

is p-equivalent to the clausal form of the pigeonhole principle

$$(\forall f : \{0, \ldots, mk\} \to mk)(\exists i < mk)(||f^{-1}(i)|| \geq 2).$$

The idea of proof by contrapositives is quite simple. To show $\neg D_{m,k} \Rightarrow \neg PHP_{mk}$, suppose that $f : \{0, \ldots, mk\} \to \{0, \ldots, k-1\}$ violates Degen's principle; i.e. $(\forall r < k)||(f^{-1}(r)|| \leq m)$. Define $g : \{0, \ldots, mk\} \to \{0, \ldots, mk-1\}$ as follows: $g(x) = i \cdot k + j$ if

$$[||\{x' < x : f(x') = f(x)\}|| = i] \wedge f(x) = j.$$

Since f violates Degen's principle, it follows that g is injective, so g violates the pigeonhole principle. To show $\neg PHP_{mk} \Rightarrow \neg D_{m,k}$, suppose that $f : \{0, \ldots, mk\} \to \{0, \ldots, mk-1\}$ is injective. It follows that $g(x) := f(x) \bmod k$ violates Degen's principle. In this section, the previous argument of equivalence is formalized within resolution. As a corollary, we obtain another proof of the main result of the previous section: polynomial size CP proofs of $D_{m,k}$. Namely CP p-simulates resolution, so by the main result of this section, there are polynomial size CP proofs of Degen's principle from the pigeonhole principle. Since it is well-known that there are polynomial size CP proofs of PHP_{mk}, the corollary follows.

Throughout this section, fix k, m and let $n = mk$. For ease of notation, non-negative integers will be considered as von Neumann ordinals, so that $n = \{0, \ldots, n-1\}$. In the following definitions, the reader should bear in mind that in the sketch proof that $\neg D_{m,k} \Rightarrow \neg PHP_{mk}$, the p's encode f, and the q's encode g; i.e. $p_{i,j} = 1$ iff $f(i) = j$ and $q_{i,j} = 1$ iff $g(i) = j$.

Definition 9 *The set of defining clauses for $p \equiv \bigwedge_{i \in I} q_i$ is defined as*

$$\{\{\overline{p}, q_i\} : i \in I\} \cup \{\{\overline{q}_i : i \in I\} \cup \{p\}\}$$

The set of defining clauses for $p \equiv \bigvee_{i \in I} q_i$ is defined as

$$\{\{\overline{p}\} \cup \{q_i : i \in I\}\} \cup \{\{\overline{q}_i, p\} : i \in I\}$$

Definition 10 *1. $\mathcal{S}_i^l := \{S \subset i \mid ||S|| = l\}$.*

2. $\mathcal{S}_i := \bigcup_{l<m} \mathcal{S}_i^l$.

3. If $||S|| < m - 1$, then let $Def(p_{i,j}^S)$ be the set of defining clauses for

$$p_{i,j}^S \equiv p_{i,j} \wedge \bigwedge_{i' \in S} p_{i',j} \wedge \bigwedge_{i' \in (i \setminus S)} \overline{p}_{i',j}.$$

If $||S|| = m - 1$, let $Def(p_{i,j}^S)$ be the set of defining clauses for

$$p_{i,j}^S \equiv p_{i,j} \wedge \bigwedge_{i' \in S} p_{i',j}.$$

In words, $Def(p_{i,j}^S)$ says that i is the $||S|| + 1$-st pigeon to be mapped to j, so $g(i) = ||S|| \cdot k + j$ in our earlier sketch argument.

4.

$$Def(p^S, k, m) := \bigcup_{i \leq n} \bigcup_{j<k} \bigcup_{S \in \mathcal{S}_i} Def(p_{i,j}^S).$$

5. $C_{m,k}$ is the set of clauses expressing the refutable version of Degen's principle

$$(\exists f : \{0, \ldots, n\} \to k)(\forall i < k)(||f^{-1}(i)|| \leq m)$$

so that

$$C_{m,k} := C_{m,k}^0 \cup C_{m,k}^1$$

with

$$C_{m,k}^0 := \{\{p_{i,j} : j < k\} : i \leq n\}$$

and

$$C_{m,k}^1 := \{\{\overline{p}_{i,j} : i \in S\} : j < k, S \in \mathcal{S}_{n+2}^{m+1}\}.$$

Lemma 11 *If $i \leq n$, $j < k$, $S \in \mathcal{S}_i$, then*

$$C_{m,k}^0, Def(p^S, k, m) \vdash \{\{\overline{p}_{i,j}\} \cup \{\overline{p}_{i',j} : i' \in S\} \cup \{p_{i,j}^{S'} : S \subset S' \in \mathcal{S}_i\}\}.$$

For all possible choices of i, j, S altogether we need $\leq (n+1)^{m+3}$ resolution steps.

Proof In words, the assertion of the lemma is that *if* $p_{i,j}$ holds and $p_{i',j}$ holds for all $i' \in S$, *then* $g(i) = ||S'|| \cdot k + j$ holds for some $S \subset S'$. By induction on $(m-1) - ||S||$.
The base case $||S|| = m-1$ follows from $Def(p^S_{i,j})$. For the induction step, assume $||S|| = l < m-1$, and that the theorem is proven for $||S|| = l+1$. By $Def(p^S, k, m)$ we have

$$\{\overline{p}_{i,j}\} \cup \{\overline{p}_{i',j} : i' \in S\} \cup \{p_{i',j} : i' \in (i \setminus S)\} \cup \{p^S_{i,j}\}$$

which asserts that

$$[(f^{-1}(j) \cap i) = S \wedge f(i) = j] \rightarrow p^S_{i,j}.$$

By the induction hypothesis, for $i_0 \in (i \setminus S)$,

$$\{\overline{p}_{i,j}, \overline{p}_{i_0,j}\} \cup \{\overline{p}_{i',j} : i' \in S\} \cup \{p^{S'}_{i,j} : S \cup \{i_0\} \subset S' \in \mathcal{S}_i\}$$

and so with $i - ||S||$ resolution steps we conclude the assertion.

To compute the number of resolution steps, note that for every $i \leq n$, $j < k$, $l < m$, $S \in \mathcal{S}^l_i$, $i - ||S|| \leq n$ steps are required, and $||\mathcal{S}^l_i|| = \binom{i}{l} \leq (n+1)^m$, therefore altogether at most $k \cdot (n+1) \cdot m \cdot (n+1)^m \cdot (n+1) = km(n+1)^{m+2} \leq (n+1)^{m+3}$ steps are required. ∎

Definition 12

$$Def(q, k, m) := \bigcup_{i \leq n} \bigcup_{j < n} Def(q_{i,j})$$

where for $i \leq n$, $l < m$, $j < k$ $Def(q_{i,j})$ is the set of defining clauses for

$$q_{i,lk+j} \equiv \bigvee_{S \in \mathcal{S}^l_i} p^S_{i,j}$$

Lemma 13 *For $i \leq n$*

$$\{p_{i,j} : j < k\}, Def(p^S, k, m), Def(q, k, m) \vdash \{q_{i,j} : j < n\}$$

for all i altogether in $\leq 3(n+1)^{m+3}$ steps.

Proof By lemma 11, for each fixed i we have

$$\{\overline{p}_{i,j}\} \cup \{p^S_{i,j} : S \in \mathcal{S}_i\}.$$

From this and

$$\{p_{i,j} : j < k\}$$

in k resolution steps we deduce

$$\{p^S_{i,j} : S \in \mathcal{S}_i, j < k\}.$$

By $Def(q, k, m)$

$$\{\overline{p}^S_{i,j}, q_{i,k \cdot ||S|| + j}\}.$$

In $\sum_{i \leq n} \sum_{l < m} ||\mathcal{S}^l_i||$ resolution steps we conclude

$$\{q_{i,j} : j < n\}.$$

Number of steps needed: For lemma 11 there are at most $(n+1)^{m+3}$ steps, additionally at most $k \cdot (n+1) \cdot (k + (n+1)^{m+1} \cdot m)$, so altogether at most $3(n+1)^{m+3}$ steps. ∎

Lemma 14 *Assume $i < i' \leq n$, $j < k$, $S \in \mathcal{S}_i^l$, $S' \in \mathcal{S}_{i'}^l$. If $l < m-1$, then*

$$Def(p^S, k, m) \vdash \{\overline{p}_{i,j}^S, \overline{p}_{i',j}^{S'}\}$$

and if $l = m-1$, then

$$Def(p^S, k, m), C_{m,k}^1 \vdash \{\overline{p}_{i,j}^S, \overline{p}_{i',j}^{S'}\}.$$

For all possible i, i', j, S together, at most $(n+1)^{2m+3}(m+2)$ steps are needed.

Proof Case $l < m-1$:
If $S = S'$, then $i \notin S'$. By $Def(p^S, k, m)$, we have $\{\overline{p}_{i,j}^S, p_{i,j}\}$, $\{\overline{p}_{i',j}^{S'}, \overline{p}_{i,j}\}$, by resolution $\{\overline{p}_{i,j}^S, \overline{p}_{i',j}^{S'}\}$. From $S \neq S'$, it follows that $S \not\subset S'$, $i_0 \in (S \setminus S')$ for some i_0, $\{\overline{p}_{i,j}^S, p_{i_0,j}\}$, $\{\overline{p}_{i',j}^{S'}, \overline{p}_{i_0,j}\}$, so by resolution $\{\overline{p}_{i,j}^S, \overline{p}_{i',j}^{S'}\}$.
Case $l = m-1$:
By $C_{m,k}^1$,

$$\{\overline{p}_{i_0,j} : i_0 \in S\} \cup \{\overline{p}_{i,j}, \overline{p}_{i',j}\},$$

by $Def(p^S, k, m)$, for $i_0 \in S$, $\{\overline{p}_{i,j}^S, p_{i_0,j}\}$, $\{\overline{p}_{i,j}^S, p_{i,j}\}$, $\{\overline{p}_{i',j}^{S'}, p_{i',j}\}$, by $m+2$ resolution steps $\{\overline{p}_{i,j}^S, \overline{p}_{i',j}^{S'}\}$.

Number of steps needed: there are at most $\sum_{i<i'\leq n} \sum_{j<k} \sum_{l<m} \sum_{S \in \mathcal{S}_i^l} \sum_{S \in \mathcal{S}_{i'}^l} (m+2) \leq km(m+2)(n+1)^{2m+2} \leq (n+1)^{2m+3}(m+2)$ steps.

Lemma 15 *If $i < i' \leq n$, $j < n$,*

$$Def(p^S, k, m), Def(q, k, m), C_{m,k}^1 \vdash \{\overline{q}_{i,j}, \overline{q}_{i',j}\}.$$

All proofs together need (if $k \geq 2$) at most $(n+1)^{2m+4}$ steps.

Proof By lemma 14, if $l < m$, $j < k$, $S \in \mathcal{S}_i^l$, $S' \in \mathcal{S}_{i'}^l$ it follows that $\{\overline{p}_{i,j}^S, \overline{p}_{i',j}^{S'}\}$, further by $Def(q, k, m)$ in $||\mathcal{S}_i||$ resolution steps

$$\{\overline{q}_{i,kl+j}\} \cup \{p_{i,j}^S : S \in \mathcal{S}_i^l\},$$

therefore

$$\{\overline{q}_{i,kl+j}, \overline{p}_{i',j}^{S'}\},$$

by $Def(q, k, m)$

$$\{\overline{q}_{i',kl+j}\} \cup \{p_{i',j}^{S'} : S' \in \mathcal{S}_{i'}^l\},$$

by $||\mathcal{S}_{i'}^l||$ steps $\{\overline{q}_{i,kl+j}, \overline{q}_{i',kl+j}\}$.

Number of Steps: steps from lemma 14 at most $(m+2)(n+1)^{2m+3}$ steps, additionally

$$\sum_{i<i'\leq n} \sum_{j<k} \sum_{l<m} (||\mathcal{S}_i|| \cdot ||\mathcal{S}_{i'}||) \leq (n+1)^2 \cdot k \cdot m \cdot (n+1)^{2m} \leq (n+1)^{2m+3}$$

steps, altogether at most $(n+1)^{2m+3} \cdot (m+3)$ steps. ∎

This completes the formalization in resolution of $\neg D_{m,k} \Rightarrow \neg PHP_{mk}$. The formalization in resolution of the converse is straightforward and left to the reader. From the analysis of resolution steps and consideration of the number of variables which can appear in any clause, we deduce that $D_{m,k} \equiv PHP_{mk}$ has resolution proofs of size polynomial in the size of $D_{m,k}$ and PHP_{mk}.

Note that the proof of equivalence really uses extended resolution, since we introduced polynomially (in n) many new literals $p_{i,j}^S$ and $q_{i,lk+j}$. The $p_{i,j}^S$ were defined in terms of the original $p_{i,j}$, and the $q_{i,lk+j}$ were defined in terms of the $p^S_{i,j}$; thus the depth of the extension is 2, and all definitions involve polynomially (in n) many literals. By substituting the defining clauses appropriately, from a derivation of the empty clause from $\neg PHP_{mk}$ we can obtain a derivation of the empty clause from $\neg D_{m,k}$. It is in this sense we mean that over resolution PHP_{mk} and $D_{m,k}$ are polynomially equivalent.

Since cutting planes p-simulates resolution, it follows that $D_{m,k} \equiv PHP_{mk}$ has polynomial size cutting planes proofs (more precisely, cutting planes with extension, where the depth of the extension is 2, and all extending inequalities involve polynomially (in n) many literals; see [5] for information on cutting planes with extension). Since PHP_{mk} is well-known to have cutting planes proofs of size polynomial in mk, we have an alternative proof of the main result of the previous section.

5 *st*-Connectivity

Graph connectivity has been studied under various guises by many authors (Floyd-Warshall's $O(n^2 \log n)$ algorithm for transitive closure, the well-known observation that the so-called directed *graph accessibility problem* GAP is complete for nondeterministic logarithmic space, Borodin's observation that LOGSPACE is contained in AC^1, etc.). In [10], M. Karchmer and A. Wigderson gave a significant size lower bound for boolean circuits computing *st-connectivity*, the problem whether there is a path from designated nodes s to t in an undirected graph.

Theorem 16 (Karchmer-Wigderson [10]) *Monotonic fan-in 2 depth of st-connectivity is* $\Theta(\log^2 n)$.

In [18], I. Wegener proved the monotonic analogue of Spira's theorem which relates depth and size of monotonic formulas: a problem P has depth $O(d)$ monotonic formulas if and only if P has size $2^{O(d)}$ monotonic circuits (see Boppana-Sipser [1] for an overview of boolean circuit complexity). Wegener's result, with the previous theorem, implies the following.

Corollary 17 (Karchmer-Wigderson [10]) *Monotonic formula size of st-connectivity is* $\Theta(n^{\log n})$.

Another application of the previous theorem, not used in this paper, is the following result.

Theorem 18 (Clote [4]) *The monotonic depth for fan-in 2 circuits recognizing whether a 2-CNF formula is refutable is* $\Theta(\log^2 n)$.

There are various possible formulations of st-connectivity in propositional logic.

Definition 19 (st-connectivity (Form 1)) *Assume that G is a finite undirected graph, with two designated vertices s, t of degree 1, while all other vertices have degree 2. Then there is a path from s to t.*

This notion of st-connectivity, proposed by P. Pudlák, was investigated by S. Buss and P. Clote in [2] (this version of st-connectivity for *directed graphs* was there shown to be equivalent (over constant depth, polynomial size Frege systems) to the onto version of the pigeonhole principle, and polynomial size CP proofs were given for st-connectivity for undirected graphs). An alternate, weaker form of st-connectivity is now defined.

Definition 20 (st-connectivity (Form 2)) *Assume that G is a finite undirected graph with two distinct, designated vertices s, t. Then either there is a path from s to t, or there is a partition of the vertices of G into two classes, where s and t lie in different classes and no edge goes between vertices lying in different classes.*

We will show that there are polynomial size resolution proofs for st-connectivity (Form 2), though of course, since st-connectivity (Form 1) implies the pigeonhole principle, there is an exponential lower bound for resolution proof size for st-connectivity (Form 1). The formalization in resolution of Definition 20 is now given. The formula $A(\vec{p},\vec{q})$ is the conjunction of the following clauses:

1. $q_{0,0}$
2. $q_{n+1,n+1}$
3. $\overline{q}_{i,j}, \overline{q}_{i,k}$, for all $j \neq k$ in $\{0,\ldots,n+1\}$.
4. $q_{i,0},\ldots,q_{i,n+1}$, for all $i \in \{1,\ldots,n\}$.
5. $\overline{q}_{i,j}, \overline{q}_{i+1,k}, p_{j,k}$, for all $j \neq k$ in $\{0,\ldots,n+1\}$.
6. $\overline{p}_{i,j}, p_{j,i}$, for all $i \neq j$ in $\{0,\ldots,n+1\}$.

The idea is that the p's express the edge relation of G ($p_{i,j} = 1$ iff there is a directed edge from i to j), and that the q's define a path from $s = 0$ to $t = n+1$. We allow multiple occurrences of the same vertex along a path.

The formula $B(\vec{p},\vec{r})$ is the conjunction of the following clauses:

1. $\overline{r}_0$
2. r_{n+1}
3. $\overline{r}_i, \overline{p}_{i,j}, r_j$, for all $i \neq j$ in $\{0,\ldots,n+1\}$.

The idea is that the p's express the edge relation of G, and the r's express the partition: those vertices i in the same partition class as s (we identify s with 0) satisfy $\overline{r}_i$, while those in the same class as t (we identify t with $n+1$) satisfy r_i.

The resolution formulation of st-connectivity (Form 2) is the conjunction of both $A(\vec{p},\vec{q})$, which expresses that either G is not an undirected graph, or there is a path from s to t, and $B(\vec{p},\vec{r})$, which states that there is a partition of G's vertices, with s,t in different classes, and for which no edge of G goes between vertices in different classes. Note that all occurrences of $\vec{p}$ in the clauses B are negative.

J. Krajíček [12] proved an interesting interpolation result, which relates monotonic circuit lower bounds with lower bounds resolution proofs (P. Pudlák [14] extended this to an interpolation result relating monotonic real circuit lower bounds with lower bounds for cutting plane proofs).

Theorem 21 (Krajíček [12]) *Suppose that propositional variables $\vec{p}$ are positive in $A(\vec{p},\vec{q})$, or that $\vec{p}$ are negative in $B(\vec{p},\vec{r})$, and that there is a resolution refutation P of $A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})$ of depth d and size s. Then there is a monotonic boolean circuit C of depth d and size $O(s)$ for which*

$$C(\vec{p}) = \begin{cases} 0 & \textit{if } A(\vec{p},\vec{q}) \textit{ is refutable} \\ 1 & \textit{else if } B(\vec{p},\vec{r}) \textit{ is refutable} \end{cases}$$

Moreover, if P is a proof tree, then the circuit C has fan-out 1.

By Theorem 21 and Corollary 17 we have the following.

Theorem 22 *All tree-like resolution proofs of st-connectivity (Form 2) have size $\Omega(n^{\log n})$.*

The separation between tree-like resolution and resolution is a corollary of the following.

Theorem 23 *There are polynomial size resolution proofs of st-connectivity (Form 2).*

Proof We begin by the following claim.
Claim: For $1 \le i \le n+1$, there is a resolution proof of $\overline{q}_{i,j}, \overline{r}_j$

The proof of the claim is by induction on i. For the base case of $i = 1$, note that

$$\frac{\dfrac{\dfrac{\overline{q}_{0,0}, \overline{q}_{1,k}, p_{0,k} \qquad \dfrac{\overline{r}_k \overline{p}_{k,0}, r_0 \qquad \overline{p}_{0,k}, p_{k,0}}{\overline{r}_k, \overline{p}_{0,k}, r_0}}{\overline{q}_{0,0}, \overline{q}_{1,k}, \overline{r}_k, r_0} \qquad q_{0,0}}{\overline{q}_{1,k}, \overline{r}_k, r_0} \qquad \overline{r}_0}{\overline{q}_{1,k}, \overline{r}_k}$$

The resolution proof for the base case is $O(n)$ size. Now, the induction hypothesis is

$$\overline{q}_{i,j}, \overline{r}_j.$$

We have the following auxiliary result.

$$\frac{\overline{q}_{i,j}, \overline{r}_j \qquad \dfrac{\overline{q}_{i,j}, \overline{q}_{i+1,k}, p_{j,k} \qquad \dfrac{\overline{p}_{j,k}, p_{k,j} \qquad \overline{r}_k, \overline{p}_{k,j}, r_j}{\overline{r}_k, \overline{p}_{j,k}, r_j}}{\overline{q}_{i,j}, \overline{q}_{i+1,k}, \overline{r}_k, r_j}}{\overline{q}_{i,j}, \overline{q}_{i+1,k}, \overline{r}_k}$$

Now

$$\frac{\dfrac{q_{i,0}, q_{i,1}, \dots, q_{i,n+1} \qquad \overline{q}_{i,0}, \overline{q}_{i+1,k}, \overline{r}_k}{q_{i,1}, q_{i,2}, \dots, q_{i,n+1}, \overline{q}_{i+1,k}, \overline{r}_k} \qquad \overline{q}_{i,1}, \overline{q}_{i+1,k}, \overline{r}_k}{q_{i,2}, \dots, q_{i,n+1}, \overline{q}_{i+1,k}, \overline{r}_k}$$

Inductively continuing in this manner, we obtain

$$\overline{q}_{i+1,k}, \overline{r}_k.$$

This completes the inductive case. For i, k fixed, there are $O(n)$ additional resolution steps, with overall size $O(n^2)$.

Taking $i = n+1$, it follows that

$$\overline{q}_{n+1,k}, \overline{r}_k$$

for all k, so that

$$\frac{\dfrac{\overline{q}_{n+1,n+1}, \overline{r}_{n+1} \qquad q_{n+1,n+1}}{\overline{r}_{n+1}} \qquad r_{n+1}}{\emptyset}$$

We have thus derived the empty clause by a proof of size $O(n^4)$ from the assum ptions. ∎

Corollary 24 *Tree-like resolution does not polynomially simulate resolution.*

See A. Urquhart's survey article [17] for discussion of Tseitin's original argument.

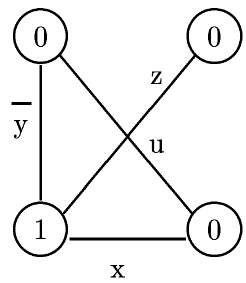

Figure 1: Odd-charged graph with edges labeled by literals

6 Tseitin's odd-charged graphs

In [15], Tseitin associated propositional formulas with labeled undirected graphs, and developed a technique for obtaining lower bounds for regular resolution refutations (regular resolution allows, on any branch of the refutation tree, at most one resolution on any particular variable).

Suppose that G is a finite, undirected graph, whose vertices are labeled by $0, 1$ and whose edges are labeled by distinct propositional literals (if literal α labels edge e, then neither α nor $\overline{\alpha}$ can label another edge). The label on a vertex is said to be its charge. The graph G is said to be odd-charged, if the sum modulo 2 of the vertex labels is 1. Figure 1 is an example.

Associate with G its charge equations, i.e. for vertex v the equation $EQ(v)$ states that the sum modulo 2 of the literals incident to v equals the charge on v. For the example in Figure 1, here are the charge equations:

1. $\overline{y} \oplus u = 0$
2. $\overline{y} \oplus x \oplus z = 1$
3. $z = 0$
4. $x \oplus u = 0$

The Tseitin clauses $F(G)$ associated with graph G are the clauses corresponding to the CNF formulation of the charge equations. With this example, we have:

1. $\{\overline{u}, \overline{y}\}, \{u, y\}$
2. $\{x, y, \overline{z}\}, \{x, \overline{y}, z\}, \{\overline{x}, y, z\}, \{\overline{x}, \overline{y}, \overline{z}\}$
3. $\{\overline{z}\}$
4. $\{x, \overline{u}\}, \{\overline{x}, u\}$

The rule for producing clauses from a charge equation is to place an odd [resp. even] number of negations on the associated literals, if the charge is 0 [resp. 1]. Clearly, there are 2^{d-1} clauses associated with the charge equation for vertex v if the degree of v is d (note that half of the 2^d truth assignments satisfy the charge equation). When considering proof size, we are thus only interested in graph families of bounded degree. The key property of odd-charged graphs is given by the following.

Fact 25 (Tseitin [15, 17]) *The connected graph G is odd-charged if and only if the clauses $F(G)$ are unsatisfiable.*

In [15], Tseitin developed recurrence relations for regular resolution refutation size, depending on a connectivity parameter for the graphs, and thus proved an exponential lower bound for regular resolution refutations for $F(L_n)$, where L_n is the odd-charged $n \times n$ lattice. In [16], A. Urquhart employed A. Haken's lower bound technique [8] to prove an exponential lower bound for Tseitin tautologies associated with particular expander graphs. Two interesting questions remain in this area:

1. Are there polynomial size CP refutations for Urquhart's formulas [16]?
2. For which families of graphs of bounded degree are there superpolynomial lower bounds for resolution [resp. regular resolution] refutations of Tseitin formulas?

Despite Tseitin's recurrence relations, it seems to be an interesting open problem to determine which graph theoretic properties lead to polynomial size regular resolution proofs.

Lemma 26 *Let u, v be two nodes of a charged, labeled, undirected graph G, which are joined by an edge in G labeled by x. Let G' be obtained from G by contracting the edge $\{u, v\}$. In other words, define $V(G') = V(G) - \{u, v\} \cup \{w\}$ where $w \notin V(G)$ is a new node, and*

$$E(G') = E(G) - \{e : u \in e \text{ or } v \in e\} \cup \{\{r, w\} : \{r, u\} \in E(G) \text{ or } \{r, v\} \in E(G)\}.$$

The charge on every node in $V(G') - \{w\}$ is the same as the charge of that node in G, while the charge on w is defined to be

$$change(u) \oplus charge(v).$$

Then there are $2^{dg(u)+dg(v)-3}$ resolution steps to derive the clauses associated with the charge equation $EQ(w)$ in G' from the charge equations $EQ(u)$, $EQ(v)$ in G.

The proof of this lemma follows from a simple computation, where positive [resp. negative] occurrences of the edge literal x in $EQ(u)$ are resolved against negative [resp. positive] occurrences of x in $EQ(v)$. The formal proof is left to the reader.

Definition 27 *The graph H is a minor of the graph G, if H can be obtained from G by the operations of deleting an isolated vertex, removing an edge, contracting an edge.*

Edge deletions and their relation to regular resolution were first discussed by Tseitin [15, 17], and were the basis of his recurrence relations. Isolated vertices play no role in Tseitin's formulas, as there is no charge equation for such vertices. Finally, edge contractions can be handled by the previous lemma. From this discussion, it is clear that a precise relation between $F(G)$ and $F(H)$ can be worked out, if H is a minor of G. Moreover, a simple computation, contracting edges beginning with those adjacent to the leaves, shows that the Tseitin formulas $F(G_n)$ have linear size regular resolution refutations, for families $\{G_n : n \in \mathbf{N}\}$ of bounded degree odd-charged trees. This follows from the next proposition.

Proposition 28 *Let T be a rooted, odd-charged binary tree with n nodes and degree bound e. Then there are regular resolution refutations of $F(T)$ consisting of at most $n(2^e - 1)$ steps.*

Proof Contract edges, beginning with the leaves of T. By Lemma 26, the number of resolution steps required to contract the edge connecting a leaf (of degree 1) with its parent is 2^{e-1}. For that parent, there are respectively 2^{e-2}, 2^{e-3}, etc. many

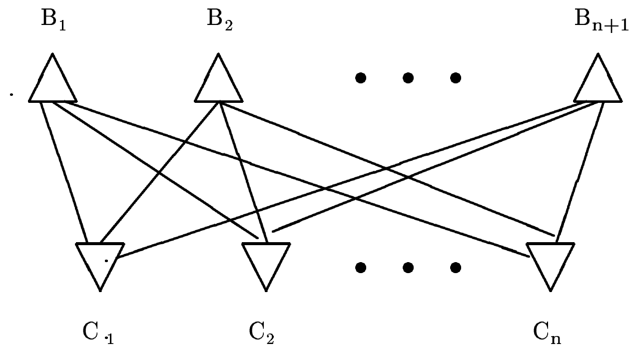

Figure 2: Global view of Tseitin graph representing PHP_n

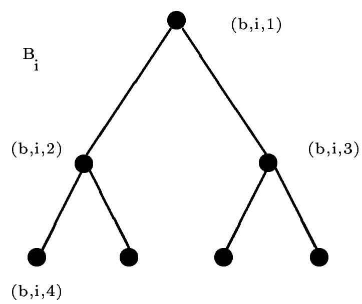

Figure 3: Local view of Tseitin graphs for the B's

steps in contracting sibling leaves with the same parent. Thus an upper bound for the number of resolution steps required to derive the empty clause is the number of internal nodes of T times $\sum_{i=0}^{e-1} 2^i$, so bounded by $n(2^e - 1)$. ∎

Hence, it seems possible that one could classify via graph theoretic properties those families of bounded degree connected graphs whose associated Tseitin formulas have polynomial size regular resolution refutations. Noting the correspondence in regular resolution with operations in the definition of graph minor, certain techniques may be applicable from the Robertson-Seymour theorem that the collection of all finite graphs is well quasi-ordered under graph minors.

As a small step in this direction, we describe degree 3 graphs whose Tseitin formulas correspond to the pigeonhole principle, and for which there are no polynomial size resolution (or even constant depth Frege) proofs. As shown in Figure 2, the graph G_n consists of $n+1$ top trees B_i, and n bottom trees C_j, both indicated by triangles. B_i is responsible for mapping the i-th pigeon, and C_j is responsible for the j-th hole. The jth leaf of B_i is connected with the ith leaf of C_j. The B's themselves are shown in Figure 3 and the C's are shown in Figure 4. The trees B_i have n leaves each, therefore $2n-1$ nodes, whereas the trees C_i have $n+1$ leaves and $2n+1$ nodes. The jth leaf of B_i has number $\text{leaf}_B(j) := n-1+j$ and the ith leaf of C_j has number $\text{leaf}_C(i) := n+i$. Therefore G_n has vertices

$$\{\langle b,i,j\rangle : 1 \le i \le n+1, 1 \le j \le 2n-1\} \cup \{\langle c,i,j\rangle : 1 \le i \le n, 1 \le j \le 2n+1\}$$

and edges from the following three sets:

$$\{\{\langle b,i,\lfloor j/2\rfloor\rangle, \langle b,i,j\rangle\} : 1 \le i \le n+1, 2 \le j \le 2n-1\}$$

and

$$\{\{\langle c,i,\lfloor j/2\rfloor\rangle, \langle c,i,j\rangle\} : 1 \le i \le n, 2 \le j \le 2n+1\}$$

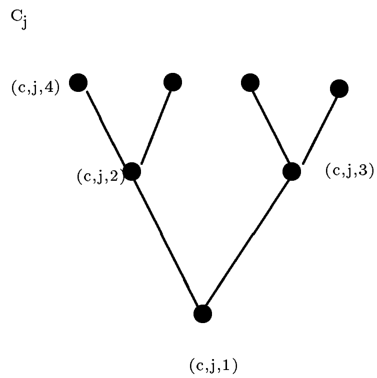

Figure 4: Local view of Tseitin graphs for C's

and

$$\{\{\langle b, i, \text{leaf}_B(j)\rangle, \langle c, j, \text{leaf}_C(i)\rangle\} : 1 \leq i \leq n+1, 1 \leq j \leq n\}.$$

We assign propositional variables to the edges of G_n as follows: $p_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle}$ labels the edge from $\lfloor j/2 \rfloor$ to j in the tree B_i; $q_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle}$ labels the edge from $\lfloor j/2 \rfloor$ to j in the tree C_i; and $r_{\langle i, \text{leaf}_B(j)\rangle, \langle j, \text{leaf}_C(i)\rangle}$ is responsible for connecting leaf j of B_i to leaf i of C_j. Here, the propositional variable sets are given as follows:

$$\{p_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle} : 1 \leq i \leq n+1, 2 \leq j \leq 2n-1\}$$

and

$$\{q_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle} : 1 \leq i \leq n, 2 \leq j \leq 2n+1\}$$

and

$$\{r_{\langle i, \text{leaf}_C(j)\rangle, \langle j, \text{leaf}_B(i)\rangle} : 1 \leq i \leq n+1, 1 \leq j \leq n\}.$$

Let each of $\langle b, i, 1\rangle$ for $1 \leq i \leq n+1$, and $\langle c, j, 1\rangle$ for $1 \leq j \leq n$ have charge 1, and all other nodes have charge 0. The edges of G_n are labeled in the obvious manner (eg. $\{\langle b, i, \lfloor j/2 \rfloor\rangle, \langle b, i, j\rangle\}$ is labeled by $p_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle}$ etc.). Therefore G has odd charge $2n+1$ and we have the following charge equations:

(1) $$p_{\langle i,1\rangle, \langle i,2\rangle} \oplus p_{\langle i,1\rangle, \langle i,3\rangle} = 1$$

for all $1 \leq i \leq n+1$,

(2) $$q_{\langle i,1\rangle, \langle i,2\rangle} \oplus q_{\langle i,1\rangle, \langle i,3\rangle} = 1$$

for all $1 \leq i \leq n$,

(3) $$p_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle} \oplus p_{\langle i,j\rangle, \langle i,2j\rangle} \oplus p_{\langle i,j\rangle, \langle i,2j+1\rangle} = 0$$

for all $1 \leq i \leq n+1, 2 \leq j \leq n-1$,

(4) $$q_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i,j\rangle} \oplus q_{\langle i,j\rangle, \langle i,2j\rangle} \oplus q_{\langle i,j\rangle, \langle i,2j+1\rangle} = 0$$

for all $1 \leq i \leq n, 2 \leq j \leq n$,

(5) $$p_{\langle i, \lfloor \frac{leaf_B(j)}{2} \rfloor\rangle, \langle i, \text{leaf}_B(j)\rangle} \oplus r_{\langle i, \text{leaf}_B(j)\rangle, \langle j, \text{leaf}_C(i)\rangle} = 0$$

for all $1 \leq i \leq n+1$, and $1 \leq j \leq n$,

(6) $$r_{\langle i, \mathrm{leaf}_B(j)\rangle, \langle j, \mathrm{leaf}_C(i)\rangle} \oplus q_{\langle j, \lfloor \frac{\mathrm{leaf}_C(i)}{2} \rfloor\rangle, \langle j, \mathrm{leaf}_C(i)\rangle} = 0$$

for all $1 \leq i \leq n+1$, and $1 \leq j \leq n$.

The set of G_n's vertices has cardinality $(n+1)(2n-1)+n(2n+1) = 0(n^2)$ and each node has degree at most 3.

We claim that there are polynomial size resolution derivations of $F(G_n)$ from $\neg PHP_n$ – recall that the Tseitin formula $F(G_n)$ is refutable, whereas PHP_n is a tautology.

To this end, for $1 \leq i \leq n+1, 2 \leq j \leq 2n-1$ let

(7) $$p_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i, j\rangle} \equiv \bigvee_{\{1 \leq k \leq n : j \sqsubseteq \mathrm{leaf}_B(k)\}} P_{i,k}$$

where $u \sqsubseteq v$ means that u is a prefix of v (integer u is a prefix of integer v if the binary representation of u is a prefix of the binary representation of v). The idea is that the leaves of the tree B_{i_0} are labeled by $P_{i_0,1}, P_{i_0,2}, \ldots, P_{i_0,n}$ and that an edge $p_{\langle i, \lfloor j/2 \rfloor\rangle, \langle i, j\rangle}$ between node $\langle b, i, \lfloor j/2 \rfloor\rangle$ and node $\langle b, i, j\rangle$ of B_{i_0} has the value 1 iff $\langle b, i, \lfloor j/2 \rfloor\rangle$ is the ancestor of a leaf bearing the value 1. For $1 \leq j \leq n, 2 \leq i \leq 2n+1$ let

(8) $$q_{\langle j, \lfloor i/2 \rfloor\rangle, \langle j, i\rangle} \equiv \bigvee_{\{1 \leq k \leq n+1 : i \sqsubseteq \mathrm{leaf}_C(k)\}} P_{k,j}$$

Similarly, the idea is that the leaves of the tree C_{j_0} are labeled by $P_{1,j_0}, P_{2,j_0}, \ldots, P_{n+1,j_0}$ and that an edge $q_{\langle j, \lfloor i/2 \rfloor\rangle, \langle j, i\rangle}$ between internal nodes of C_{j_0} has the value 1 iff $\langle c, j, \lfloor i/2 \rfloor\rangle$ is the ancestor of a leaf bearing the value 1. For $1 \leq i \leq n+1, 1 \leq j \leq n$ let

(9) $$r_{\langle i, \mathrm{leaf}_B(j)\rangle, \langle j, \mathrm{leaf}_C(i)\rangle} \equiv P_{i,j}.$$

The function of the r's is to connect up leaves of the B's with those of the C's, where leaf the j-th leaf of B_i (labeled by $P_{i,j}$) is connected to the i-th leaf of C_j. Finally, let $DEF(G_n)$ be the resolution clauses corresponding (as in Section 4) to the above definitions.

Definition 29 *The negation of the onto-version of the pigeonhole principle, denoted $\neg PHP_n^{onto}$, states that there is a bijection from $\{1, \ldots, n+1\}$ onto $\{1, \ldots, n\}$, and is given by the following clauses:*

$$\{\{P_{i,1}, \cdots, P_{i,n}\} : 1 \leq i \leq n+1\} \cup \{\{\overline{P}_{i,j}, \overline{P}_{i',j}\} : 1 \leq i < i' \leq n+1, 1 \leq j \leq n\}$$

together with

$$\{\{P_{1,j}, \cdots, P_{n+1,j}\} : 1 \leq j \leq n\} \cup \{\{\overline{P}_{i,j}, \overline{P}_{i,j'}\} : 1 \leq i \leq n+1, 1 \leq j < j' \leq n\}.$$

Note that the onto version of the pigeonhole principle requires a bijection (not simply injection) from the domain of size $n+1$ to range of size n. In contrast to the formalization of PHP_n, we have $1 \leq i \leq n+1$ and $1 \leq j \leq n$ to allow a simple correspondence with the trees B_i and C_j.

Theorem 30 *There are polynomial size resolution derivations of $F(G_n)$ from $DEF(G_n)$ and $\neg PHP_n^{onto}$.*

Proof For $1 \leq j \leq n$, by Equation (7)

$$p_{\langle i, \lfloor \frac{\mathrm{leaf}_B(j)}{2} \rfloor, \rangle, \langle i, \mathrm{leaf}_B(j) \rangle} \equiv P_{i,j}$$

and by Equation (9)

$$r_{\langle i, \mathrm{leaf}_B(j) \rangle, \langle j, \mathrm{leaf}_C(i) \rangle} \equiv p_{\langle i, \lfloor \frac{\mathrm{leaf}_B(j)}{2} \rfloor \rangle, \langle i, \mathrm{leaf}_B(j) \rangle}.$$

This proves Equation (5). Equation (6) is similarly derived. Thus we've established the charge equations for the connection between appropriate trees B_i to C_j.

Fix $1 \leq i \leq n+1$. Equations (1) and (3) respectively correspond to the charge equation at the root and the charge equations at non-root internal nodes of the tree B_i. Consider first Equation (1). To simplify notation, write d resp. e in place of $p_{\langle i,1 \rangle, \langle i,2 \rangle}$ resp. $p_{\langle i,1 \rangle, \langle i,3 \rangle}$, and let $P_a, P_{a+1}, \ldots, P_b$ resp. $P_{b+1}, \ldots, P_c$ denote the leaf labels in B_i below d resp. e (hence the P's correspond to appropriate $P_{i,j}$'s). With this notation, Equation (7) states that $d \equiv P_a \vee \cdots \vee P_b$ and $e \equiv P_{b+1} \vee \cdots \vee P_c$, so from its clausal form in $DEF(G_n)$,

$$\{\overline{d}, P_a, \ldots, P_b\}.$$

Repeatedly resolve this clause against clauses

$$\{\overline{P}_a, \overline{P}_{b+1}\}, \{\overline{P}_{a+1}, \overline{P}_{b+1}\}, \{\overline{P}_{a+2}, \overline{P}_{b+1}\}, \ldots, \{\overline{P}_b, \overline{P}_{b+1}\}$$

(these clauses come from $\neg PHP_n^{onto}$) to obtain $\{\overline{d}, \overline{P}_{b+1}\}$. In a similar fashion, obtain $\{\overline{d}, \overline{P}_{b+2}\}$, $\{\overline{d}, \overline{P}_{b+3}\}, \ldots$, $\{\overline{d}, \overline{P}_c\}$. From $DEF(G_n)$, we have $\{\overline{e}, P_{b+1}, \ldots, P_c\}$, so by repeated resolution against the previous clauses, we obtain $\{\overline{d}, \overline{e}\}$.

From $\neg PHP_n^{onto}$, we have $\{P_a, \ldots, P_c\}$, and from $DEF(G_n)$ we have $\{\overline{P}_a, d\}, \ldots$, $\{\overline{P}_b, d\}$ and $\{\overline{P}_{b+1}, e\}, \ldots$, $\{\overline{P}_c, e\}$. Repeatedly resolving the former against the latter, we obtain $\{d, e\}$. Now $\{d, e\}$ and $\{\overline{d}, \overline{e}\}$ form the clausal representation of the charge equation (1) $d \oplus e = 1$. In a similar fashion (using the onto part of the formulation of the pigeonhole principle) one can prove Equation (2). This concludes the derivation of charge equations for roots of the B_i and C_j.

Consider now Equation (3). To simplify notation, write d, e, f resp. for $p_{\langle i, \lfloor j/2 \rfloor \rangle, \langle i,j \rangle}$, $p_{\langle i,j \rangle, \langle i,2j \rangle}$, $p_{\langle i,j \rangle, \langle i,2j+1 \rangle}$, and let $P_a, \ldots, P_b$ resp. $P_{b+1}, \ldots, P_c$ denote the leaves of tree B_i respectively below e, f. Thus the leaves below d are $P_a, \ldots, P_c$. The clausal representation of Equation (3) has the following clauses:

1. $\{\overline{d}, e, f\}$
2. $\{d, \overline{e}, f\}$
3. $\{d, e, \overline{f}\}$
4. $\{\overline{d}, \overline{e}, \overline{f}\}$.

The first clause is simple to obtain. From $DEF(G_n)$ we have $\{\overline{d}, P_a, \ldots, P_c\}$ and $\{\overline{P}_a, e\}$, $\{\overline{P}_{a+1}, e\}, \ldots$, $\{\overline{P}_b, e\}$ and $\{\overline{P}_{b+1}, f\}$, $\{\overline{P}_{b+2}, f\}, \ldots$, $\{\overline{P}_c, f\}$. By resolution of the former against the latter, we have $\{\overline{d}, e, f\}$. The second and third clauses are similarly derived. To obtain the fourth clause, proceed as follows. By $DEF(G_n)$, we have $\{\overline{e}, P_a, \ldots, P_b\}$ and from $\neg PHP_n^{onto}$ we have $\{\overline{P}_a, \overline{P}_{b+1}\}$, $\{\overline{P}_{a+1}, \overline{P}_{b+1}\}, \ldots$, $\{\overline{P}_b, \overline{P}_{b+1}\}$ and so by resolution we obtain $\{\overline{e}, \overline{P}_{b+1}\}$. Similarly, we obtain $\{\overline{e}, \overline{P}_{b+2}\}, \ldots$, $\{\overline{e}, \overline{P}_c\}$, and in an analogous fashion $\{\overline{f}, \overline{P}_a\}, \ldots$, $\{\overline{f}, \overline{P}_b\}$. By $DEF(G_n)$, we have $\{\overline{d}, P_a, \ldots, P_c\}$ and so by repeated resolution against the preceding clauses, we derive $\{\overline{d}, \overline{e}, \overline{f}\}$, as required. This establishes Equation (3). The derivation of Equation (4) is analogous. This completes our treatment of the charge equations for non-root internal nodes of trees B_i and C_j.

Thus we have a resolution derivation of $F(G_n)$ from $DEF(G_n)$ and $\neg PHP_n^{onto}$. Straightforward estimation shows that the sketched resolution proof is of polynomial size. ∎

Corollary 31 *There is an exponential lower bound for resolution (even constant depth Frege) refutations of $F(G_n)$.*

The corollary is immediate, since it is well-known that $\neg PHP_n^{onto}$ has an exponential size lower bound for resolution (and constant depth Frege) refutations. See [11] for details.

From this construction, one might think that for every unsatisfiable propositional formula H there is a related odd charged graph G, for which $H \to F(G)$ has a polynomial size resolution (or constant depth Frege) derivation. This however is false, unless $NP = co - NP$.

Proposition 32 *For any polynomials p, q there exists an unsatisfiable propositional formula H such that for all odd charged graphs G of size at most $q(|H|)$, there is a resolution (or constant depth Frege, or Frege, etc.) derivation of $H \to F(G)$, where $F(G)$ is the Tseitin formula related to G.*

Proof If not, then we have an NP-procedure to test whether a formula ϕ is a tautology: $\phi \in \text{TAUT}$ iff $\neg\phi \notin \text{SAT}$ iff there is odd charged G of size $q(|\phi|)$ and a resolution (or constant depth Frege, or Frege, etc.) derivation of $\neg\phi \to F(G)$. ∎

7 A Generalization of Cutting Planes to Polynomial Inequalities

In this section, we indicate a fragmentary result, which we pursued to shed light on the following open question, which the we first learned from A. Carbone. In this section, we assume familiarity with Gentzen sequent calculus for propositional formulas, which is here denoted PK for Propositional Kalkül (see [11] for a reference).

Let MPK, Monotonic Propositional Kalkül, be the monotonic version of Gentzen's sequent calculus for propositional formulas, where the only logical connectives are $\wedge$, $\vee$ (no negations), and the rules of inference are the usual rules, without the rules for introducing the negation on the left and right. By monotonic formula, we mean a sequent $\Gamma \Rightarrow \Delta$, where Γ, Δ are cedents of formulas not containing negation, and $\Rightarrow$ is the Gentzen sequent arrow (not implication). The pigeonhole principle can be so represented, as follows:

$$\bigwedge_{0 \le i \le k} \bigvee_{0 \le j < k} p_{i,j} \Rightarrow \bigvee_{0 \le i < i' \le k} \bigvee_{0 \le j < k} (p_{i,j} \wedge p_{i',j}).$$

The proof of completeness of PK for all propositional tautologies easily yields the completeness of MPK for monotonic tautologies. In boolean circuit complexity theory, it is well-known that there are monotonic problems having polynomial size circuits, but requiring exponential size monotonic circuits.

In analogy to this there is the following.

Question 33 *Does there exist a family of monotonic formulas, having polynomial size proofs in PK, but requiring superpolynomial size MPK proofs?*

P. Pudlák's interpolation theorem for CP, together with his extension of Razborov's exponential monotonic circuit size lower bound for clique to arbitrary monotone real circuits in [14], led to an exponential lower bound for CP.[1] The full strength of the circuit lower bound is not exploited in Pudlák's application to cutting planes. In particular, *provided* one shows an interpolation for a stronger proof system P whose operations involve real operations, one could obtain a lower bound for P.

Our goal in this section is to introduce a monotonic polynomial calculus, extending CP, and implying MPK, and to establish an interpolation result for the resulting calculus. This would then lead to the separation between monotonic Gentzen and Gentzen sequent calculus on a monotonic formula. We state our monotonic polynomial calculus, and state the p-simulation of MPK; however, we don't know whether one can prove an interpolation result for this logic. Does interpolation for MPK imply or is it implied by some complexity assumption?

We are going to introduce a calculus MP_1, which will extend CP by allowing the stronger multiplication rule:

- polynomial multiplication $\dfrac{0 \leq p \qquad p \leq q \qquad 0 \leq p' \qquad p' \leq q'}{p \cdot p' \leq q \cdot q'}$

Further, since all propositional variables x_i are 0 or 1, we have $x_i^2 = x_i$ and can identify all polynomials having monomials which only differ in the exponents greater than equal to 1 of propositional variables. If $\approx$ is the equivalence relation given by this identification, we have additionally the rule

- $\approx \dfrac{p' \approx p \qquad p \leq q \qquad q \approx q'}{p' \leq q'}$

In MP_1, one *cannot* move expressions from one side of the inequality to the other, in introducing a minus sign — if so, one could simulate the Gentzen negation rules. We'll soon see that additional rules are needed. Let as first introduce an intermediate system MP_0.

Definition 34 *Let* $\min(x,y) = x \cdot y$*, and* $\max(x,y) = x + y - x \cdot y$*. Further, let* $\approx$ *be the least equivalence relation on polynomials in the propositional variables* x_i*, such that for* $x_i^2 \approx x_i$ *and, if* $p \approx p'$*, then* $p + q \approx p' + q$ *and* $p \cdot q \approx p' \cdot q$*.*

The system MP_0 *has axioms* $0 \leq q$*,* $q \leq 1$ *and* $q \leq q$*, where* q *is* 0*,* 1 *or a propositional variable and the following rules of inference:*

- *transitivity* $\dfrac{p \leq q \qquad q \leq r}{p \leq r}$

- min *left* $\dfrac{p \leq q}{\min(r,p) \leq q}$

- max *left* $\dfrac{p \leq r \qquad q \leq r}{\max(p,q) \leq r}$

- min *right* $\dfrac{r \leq p \qquad r \leq q}{r \leq \min(p,q)}$

- max *right* $\dfrac{p \leq q}{p \leq \max(q,r)}$

[1] In [9] A. Haken and S.A. Cook give an exponential lower bound for monotonic real circuit recognition of a clique-related problem, the *broken mosquito screen* problem. Earlier bounds for restricted versions of cutting planes were given by Bonet, Goerdt, Impagliazzo, Krajíček, and Razborov.

$$\bullet \approx \frac{p' \approx p \qquad p \leq q \qquad q \approx q'}{p' \leq q'}$$

Remark 35 *The following properties follow:*

1. max *and* min *are commutative and associative i.e.* $\max(p,q) = \max(q,p)$, $\max(\max(p,q),r) = \max(p, \max(q,r))$ *etc.*

2. *Let P be the least set of polynomials containing* 0, 1, *propositional variables and closed under* max, min *and* $\approx$. *Then, if MP_1 derives $p \leq q$, then $p, q \in P$.*

3. *If $p \in P$, then $p^2 \approx p$.*

4. *If $p \in P$, then $0 \leq p$ and $p \leq 1$.*

5. *For $p, q, r \in P$ we have the distributive laws* $\max(\min(p,q),r) \approx \min(\max(p,r), \max(q,r))$ *and* $\min(\max(p,q),r) \approx \max(\min(p,r), \min(q,r))$.

6. *If $p \in P$, then* $\min(p,p) \approx p \approx \max(p,p)$

Proposition 36 *The system MP_0 p-simulates MPK, where $\Gamma \Rightarrow \Delta$ is translated in MP_0 by $p \leq q$, where p [resp. q] is a polynomial expressing $\bigwedge \Gamma$ [resp. $\bigvee \Delta$], and $\wedge$ corresponds to* min, $\vee$ *to* max.

Proof By the remark we have Gentzen's exchange and contraction rules. Left weakening and $\wedge$-left follow from min-left rule and associativity of min; right weakening and $\vee$-right follow from max-right rule and associativity. The $\wedge$-right rule is simulated using min-right rule and distributivity; the $\vee$-left rule follows by max-left and distributivity. We sketch how to handle the cut rule. Assume that

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

Let p, q, r be polynomials, using the translation mentioned above, respectively representing Γ, Δ, A.

1. $p \leq r + q - rq$, from assumption that $\Gamma \vdash A, \Delta$.

2. $p \leq p$, axiom.

3. $p \leq pr + pq - pqr$, by min-right.

4. $q \leq q$, axiom

5. $pq \leq q$, by min-left.

6. $pr \leq q$, from assumption that $\Gamma, A \vdash \Delta$.

7. $pq + pr - pqr \leq q$, by max-left, $\approx$ and transitivity.

8. $p \leq q$, transitivity.

∎

With the rules of MP_1 we have introduced above (plus transitivity and the axioms of MP_0) we can simulate the min-left and min-right rules, using, that all polynomials occurring in derivations or MP_0 are in P and therefore we have $r \leq 1$ and $r \approx r^2$. Here we use, that the minimum is multiplication and we have a rule for it. However we couldn't prove (and this is probably not possible) closure under the max-left rule with the rules we have. In a non-monotonic extension, where we can shift expressions from one side of the inequality sign to the other, we have closure under it as sign by the following derivation:

$$\text{max-right}\ \frac{\dfrac{p \le r}{1-r \le 1-p} \qquad \dfrac{q \le r}{1-r \le 1-q}}{\dfrac{1-r \le \max(1-p,1-q)}{\min(p,q) = 1-\max(1-p,1-q) \le r}}$$

In the calculus MP_1 this is not possible. Therefore we need rules, which simulate derivations, which we get by moving a polynomial to the other side. For this purpose we interchange first the expressions on both sides of the equality sign in the multiplication rule:

$$\frac{1-p \le 1 \qquad 1-q \le 1-p \qquad 1-p' \le 1 \qquad 1-q' \le 1-p'}{1-(q \cdot q') \le 1-(p \cdot p')}$$

and replace now $1-p$ by p, etc. and get the rule

$$\frac{p \le 1 \qquad q \le p \qquad p' \le 1 \qquad q' \le p'}{\max(q,q') = 1-((1-q)\cdot(1-q')) \le 1-((1-p)\cdot(1-p')) = \max(p,p')}$$

We have now the following calculus:

Definition 37 *The system MP_1 has the axioms of MP_0, and as rules of inference the transitivity-rule and $\approx$-rule of MP_0 and additionally*

- *addition* $\dfrac{p \le q \qquad p' \le q'}{p+p' \le q+q'}$
- *multiplication* $\dfrac{p \le q \quad p' \le q' \qquad 0 \le p \quad 0 \le p'}{p \cdot p' \le q \cdot q'}$
- max $\dfrac{p \le q \quad p' \le q' \qquad q \le 1 \quad q' \le 1}{\max(p,p') \le \max(q,q')}$

Proposition 38 *MP_1 p-simulates MP_0*

Proof: If $p \in P$ we can derive in MP_1 $0 \le p$, $p \le 1$. Now the multiplication rule simulate the min-rules and the new max-rule simulate max-rules of MP_0. ∎

Note the for this simulation, the addition rule was not necessary. On the other hand, in the presence of multiplication and addition rule, using, that for propositional variables we can easily show $x_i \le x_i^2 \le x_i$, that if $r \approx r'$, then $r \le r'$ and $r' \le r$ and omit the $\approx$-rules. Further one might consider the division rules from cutting planes, which (if m is a monomial, i.e. a product of propositional variables or 1, A and c are integer and $c \ge 2$) read now as

- division by integer $\dfrac{c \cdot p \le c \cdot q + A \cdot m}{p \le q + \lfloor \frac{A}{c} \rfloor \cdot m} \qquad \dfrac{c \cdot p + A \cdot m \le c \cdot q}{p + \lceil \frac{A}{c} \rceil \cdot m \le q}$

- polynomial division $\dfrac{p \cdot q \le p \cdot q' \qquad p \ge 1}{q \le q'}$

Many questions here remain open. We briefly considered the substitution rule

- substitution $\dfrac{p \le q}{Q(x/p) \le Q(x/q)}$

where $Q(x)$ is a polynomial monotonic in x (i.e. Q may have other variables, and as a multivariate polynomial $Q(0) \le Q(1)$). A.A. Razborov (personal correspondence) raised the question whether MP_0 with substitution is polynomially equivalent to extended Frege systems, since the substitution rule is a kind of extension rule. It would be interesting to know whether MPK p-simulates MP_0.

8 Acknowledgements

We would like to thank A. Haken, J. Krajíček, P. Pudlák and A.A. Razborov for comments, and especially W. Degen, for relating his hierarchy results concerning the Degen principle, and for a preliminary copy of [7]. Thanks to J. Krajíček and P. Pudlák for a preliminary copy of their unpublished typescripts. Special thanks to J. Johannsen for sending his unpublished manuscript, which raised the question of how Degen's principle relates to the pigeonhole principle, over constant depth Frege systems. In his manuscript, Johanssen made some observations concerning $I\Delta_0$ provability that $D_{m+1,k} \to D_{m,k}$; since it follows from this paper, that $I\Delta_0$ proves the equivalence of the pigeonhole principle and Degen's principle, we have answered Johannsen's principal question. The resolution proofs were typeset using LaTeXmacros developed by S. Buss.

References

[1] R. Boppana and M. Sipser. The complexity of finite functions. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume A, pages 759–804. Elsevier, MIT Press, 1990. Elsevier (Amsterdam), MIT Press (Cambridge).

[2] S.R. Buss and P. Clote. Cutting planes, connectivity, and threshold logic. *Archive for Mathematical Logic*, 35:33–62, 1966.

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

[4] P. Clote. Note on monotonic complexity of $2-REF$. *Information Processing Letters*, 57:117–123, 1996.

[5] P. Clote. Cutting plane and Frege proofs. *Information and Computation*, 121(1):103–122, 1995.

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

[7] J.W. Degen. Pigeonhole principles and choice principles. Typescript, Universität Erlangen-Nürnberg, 1995.

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

[9] A. Haken and S.A. Cook. An exponential lower bound for the size of monotonic real circuits. Typeset manuscript, December 23, 1995.

[10] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *J. Discrete Mathematics*, 3, 1990. 255–265.

[11] J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Cambridge University Press, 1995.

[12] J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. Typeset manuscript, submitted, 1995.

[13] P. Pudlák. Ramsey's theorem in bounded arithmetic. In E. Börger, editor, *Proceedings of* Computer Science Logic 1990. Springer Lecture Notes in Computer Science **553**, 1992.

[14] P. Pudlák. Lower bounds for resolution and cutting planes proofs and monotone computations. Typeset manuscript, 1995.

[15] G. S. Tseitin. On the complexity of derivation in propositional calculus. In J. Siekmann and G. Wrigtson, editors, *Automation of Reasoning*, volume 2, pages 466 – 483. Springer Verlag, 1983.

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

[17] A. Urquhart. The complexity of propositional proofs. *The Bulletin of Symbolic Logic*, 1:425–467, 1995.

[18] I. Wegener. *Complexity of Boolean Functions.* Teubner-Wiley, 1987.