DIMACS Series in Discrete Mathematics
and Theoretical Computer Science
Volume **00**, 19xx

Equational Calculi and Constant Depth Propositional Proofs

Jan Johannsen

ABSTRACT. We define equational calculi for proving equations between functions in the complexity classes $ACC(2)$ and TC^0, and we show that proofs in these calculi can be simulated by polynomial size, constant depth proofs in Frege systems with counting modulo 2 and threshold connectives respectively.

Introduction

To motivate our work, we give a brief overview of the theory of propositional proof systems, for a more detailed exposition see e.g. the recent survey [**18**]. A propositional proof system is a polynomial time computable function whose range is the set of propositional tautologies. The usual proof systems fall under this definition if we associate with them the function mapping a valid proof to the tautology proved by it, and every other string to some fixed tautology.

A proof system is *polynomially bounded* if for every tautology A, there is a proof in it of length polynomial in the length of A. The existence of a polynomially bounded proof system is equivalent to $NP = co\text{-}NP$, hence the quest for lower bounds on the length of propositional proofs can be considered an approach to this problem from computational complexity theory.

A proof system P_1 *polynomially simulates* P_2, if for each proof p in P_2, there is a proof in P_1 of the same tautology whose length is polynomial in the length of p. Two proof systems are *polynomially equivalent* if they polynomially simulate each other.

A *Frege system* is a usual proof system for tautologies in a language with finitely many connectives, given by finitely many axiom schemes and inference rules, which are implicationally complete in the sense that if the formulas $B_1, \dots, B_m$ semantically entail A, then there must be a proof of A from the hypotheses $B_1, \dots, B_m$. All Frege systems are polynomially equivalent [**14**]. An *extended Frege system* is a Frege system extended by the substitution rule. An important open question is whether Frege systems are polynomially bounded, or whether they can polynomially simulate extended Frege systems.

In a *constant depth Frege system*, the depth of formulas appearing in proofs is required to be bounded by a constant, where the depth of formulas is measured as

1991 *Mathematics Subject Classification.* Primary 03F20; Secondary 03F30, 68Q15.

This paper is in final form and no version of it will be submitted elsewhere for publication.

if the binary connectives were of unbounded arity. Constant depth Frege systems and some extensions of these by additional, non-schematic axioms (like pigeonhole and counting principles) are known not to be polynomially bounded [**1, 4, 2, 5, 3**].

A recurring theme in the theory of propositional proof systems is the correspondence of certain proof systems to certain complexity classes. So e.g. extended Frege systems correspond to P, Frege systems to NC^1 and constant depth Frege systems to AC^0.

The first of these correspondences was made precise by S. Cook in his classic paper [**13**], where he defined an equational calculus PV for proving equations between polynomial time computable functions, based on Cobham's characterization of this class as a function algebra [**12**]. He then showed that proofs in PV can be simulated by polynomial size families of extended Frege proofs.

In the same vein, P. Clote [**10**] defined calculi ALV and AV for equations between functions in NC^1 and AC^0 resp., and showed that proofs in these calculi can be simulated by polynomial size Frege proofs and constant depth Frege proofs respectively.

Recently, extensions of Frege systems by modular counting [**3**] and threshold connectives [**15, 7**] were introduced, where constant depth proofs in these intuitively correspond to the circuit complexity classes $ACC(m)$ and TC^0. We support this intuition by defining equational calculi $A2V$ for functions in $ACC(2)$ and TV for functions in TC^0 and showing that proofs in these calculi can be simulated by polynomial size, constant depth proofs in the corresponding proof systems.

Two propositional proof systems

Let PK denote the propositional part of the classical sequent calculus LK, with the connectives $\wedge$, $\vee$ and $\neg$. It is well-known that PK is polynomially equivalent to any Frege system [**14**]. Moreover the mutual simulations do not increase the depth of formulas occurring in a proof by more than a constant, provided that the Frege system has the same underlying set of connectives.

We extend PK by the binary connective $\oplus$ (exclusive disjunction) and the following inference rules for its introduction:

$$\oplus\text{-left1}: \frac{\Gamma \Longrightarrow A, \Delta \quad \Gamma \Longrightarrow B, \Delta}{A \oplus B, \Gamma \Longrightarrow \Delta} \qquad \oplus\text{-left2}: \frac{A, \Gamma \Longrightarrow \Delta \quad B, \Gamma \Longrightarrow \Delta}{A \oplus B, \Gamma \Longrightarrow \Delta}$$

$$\oplus\text{-right1}: \frac{\Gamma \Longrightarrow A, \Delta \quad B, \Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow A \oplus B, \Delta} \qquad \oplus\text{-right2}: \frac{A, \Gamma \Longrightarrow \Delta \quad \Gamma \Longrightarrow B, \Delta}{\Gamma \Longrightarrow A \oplus B, \Delta}$$

We call this extension $PK\oplus$. Define the formulas $\bigoplus^n(A_1, \dots, A_n)$ for $n \geq 2$ inductively by $\bigoplus^2(A, B) := A \oplus B$ and

$$\bigoplus^{n+1}(A_1, \dots, A_{n+1}) := A_1 \oplus \bigoplus^n(A_2, \dots, A_{n+1}) \ .$$

Let $B(p_1, \dots, p_n)$ be a formula built up from the variables $p_1, \dots, p_n$ using only one kind of binary connective, and let $A_1, \dots, A_n$ be formulas with an outermost connective of a different kind. If d is the maximum of the depths of the formulas A_i, then $B(A_1, \dots, A_n)$ is a formula of depth $d + 1$. With this notion of depth, $PK\oplus$ is polynomially equivalent to a Frege system with Mod_2 connectives $F(Mod_2)$ as introduced e.g. in [**3**] and to the Frege system with biconditional considered in [**17**]. In both cases, the mutual simulations do not increase the formula-depth in a proof by more than a constant.

Propositional threshold logic, as introduced in [**7**], has the unary connective $\neg$ and for each $n \geq 1$ and $1 \leq k \leq n$ the n-ary threshold connective T_k^n, where $T_k^n(A_1, \dots, A_n)$ is intended to be true if at least k of the A_i are true. The depth of a threshold logic formula is simply its syntactic depth, and its size is the sum of the sizes of the variables and connectives in it, where the variables and $\neg$ are of size 1 and T_k^n is of size $n + k + 1$. Note that n-ary conjunction and disjunction are the special cases T_n^n and T_1^n of threshold connectives.

The sequent calculus PTK for propositional threshold logic has the initial sequents $A \Longrightarrow A$, the usual structural rules, cut rule and rules for negation plus the following versions of the rules for conjunction

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

$$\wedge\text{-right}: \quad \frac{\Gamma \Longrightarrow A_1, \Delta \quad \cdots \quad \Gamma \Longrightarrow A_n, \Delta}{\Gamma \Longrightarrow T_n^n(A_1, \dots, A_n), \Delta}$$

and the dual rules for disjunction. Additionally, for $n \geq 3$ there are the following rules for T_k^n with $1 < k < n$:

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

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

The correctness and completeness of PTK was proved in [**7**]. Furthermore it was proved in [**8**] that PTK is polynomially equivalent to a Frege system with threshold connectives FC introduced in [**15**], and that the mutual simulations increase the formula-depth in a proof at most by a constant.

The sequent calculus PTK^* is defined exactly like PTK, but where the rules T_k^n-right and T_k^n-left are replaced by the rules

$$T_k^n\text{-right1}: \quad \frac{\Gamma \Longrightarrow A_1, \Delta \qquad \Gamma \Longrightarrow T_{k-1}^{n-1}(A_2, \dots, A_n), \Delta}{\Gamma \Longrightarrow T_k^n(A_1, \dots, A_n), \Delta}$$

$$T_k^n\text{-right2}: \quad \frac{\Gamma \Longrightarrow T_k^{n-1}(A_2, \dots A_n), \Delta}{\Gamma \Longrightarrow T_k^n(A_1, \dots, A_n), \Delta}$$

$$T_k^n\text{-left1}: \quad \frac{A_1, \Gamma \Longrightarrow \Delta \qquad T_k^{n-1}(A_2, \dots, A_n), \Gamma \Longrightarrow \Delta}{T_k^n(A_1, \dots, A_n), \Gamma \Longrightarrow \Delta}$$

$$T_k^n\text{-left2}: \quad \frac{T_{k-1}^{n-1}(A_2, \dots A_n), \Gamma \Longrightarrow \Delta}{T_k^n(A_1, \dots, A_n), \Gamma \Longrightarrow \Delta}\,.$$

It is easily shown that PTK and PTK^* are polynomially equivalent, and that the mutual simulations do not increase the formula-depth.

Function algebras and equational calculi

Let $BASE$ denote the set of functions consisting of the constant 0, s_0, s_1, $mod2$, len, $trunc$ and $\#$, where $s_0(x) = 2x$, $s_1(x) = 2x + 1$, $mod2(x) := x \bmod 2$, $len(x) := |x| = \lceil \log_2(x + 1) \rceil$, $trunc(x, y) := \lfloor \frac{x}{2^{|y|}} \rfloor$ and $x \# y := 2^{|x| \cdot |y|}$, together with the projections π_k^n for $1 \leq k \leq n \in \mathbb{N}$, where $\pi_k^n(x_1, \dots, x_n) := x_k$.

Let g be an n-ary function and h_0, h_1 be $n + 1$-ary functions with $h_i(\bar{x}, y) \leq 1$ for $i = 0, 1$. Then the $n + 1$-ary function f is defined by concatenation recursion on notation (CRN) from g and h_0, h_1 if f is the unique function satisfying

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, 2y) &= 2f(\bar{x}, y) + h_0(\bar{x}, y) \qquad \text{for } y > 0 \\ f(\bar{x}, 2y+1) &= 2f(\bar{x}, y) + h_1(\bar{x}, y) \end{aligned}$$

The following characterization of the functions in AC^0 was given in [**9**]:

PROPOSITION 1. *AC^0 is the smallest class of functions containing the $BASE$ functions and closed under composition and CRN.*

Let $count(x)$ be the number of bits equal to 1 in the binary representation of x, and let $parity(x) := count(x) \bmod 2$. The following characterizations of the functions in $ACC(2)$ and TC^0 can be extracted from the proofs of Thm. 2.1 and 2.2 in [**11**]:

PROPOSITION 2. *$ACC(2)$ is the smallest class of functions that contains the $BASE$ functions and parity and is closed under composition and CRN, and TC^0 is the smallest class of functions containing the $BASE$ functions and count and closed under composition and CRN.*

Based on the characterization given in Prop. 1, the equational calculus AV was defined in [**10**]. It has an infinite set of variables denoted $x, y, \ldots$, possibly with subscripts. Function symbols and terms of AV are defined inductively as follows:

- The constant 0 and the variables are terms.
- s_0, s_1, tr, $mod2$, S and len are unary function symbols, $trunc$ and $\#$ are binary function symbols and $cond$ is a ternary function symbol. These are the *primitive* function symbols of AV.
- If t is a term whose free variables are among $x_1, \ldots, x_n$, then $[\lambda x_1 \ldots x_n.t]$ is an n-ary function symbol.
- If g is an n-ary function symbol and h_0, h_1 are $(n+1)$-ary function symbols, then $CR[g, h_0, h_1]$ is an $(n+1)$-ary function symbol.
- If f is an n-ary function symbol and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

For sake of readability, the function symbol $\#$ is written infix, and we write $|t|$ for $len(t)$, 1 for $s_1(0)$ and $t0$ and $t1$ for $s_0(t)$ and $s_1(t)$ respectively. The function symbol $mod2$ is denoted *parity* in [**10**]. Furthermore, AV as defined there has an additional function symbol *pad*, which is redundant since it can be defined as $CR[[\lambda x.x], [\lambda xy.0], [\lambda xy.0]]$. AV has a set of axioms that are sufficient to evaluate every closed term to a normal form built up from 0, s_0 and s_1 only. Some of these axioms of AV are

$$s_0(0) = 0, \quad mod2(x0) = 0,\ mod2(x1) = 1, \quad S(x0) = x1,\ S(x1) = s_0(S(x)),$$
$$cond(0, y, z) = y,\ cond(x0, y, z) = cond(x, y, z),\ cond(x1, y, z) = z,$$
$$[\lambda \bar{x}.t](\bar{x}) = t$$
$$CR[g, h_0, h_1](\bar{x}, y0) = cond(y, g(\bar{x}), cond(h_0(\bar{x}, y0), \tilde{c}0, \tilde{c}1))$$
$$CR[g, h_0, h_1](\bar{x}, y1) = cond(h_1(\bar{x}, y1), \tilde{c}0, \tilde{c}1)$$

where in the last two lines $\tilde{c}$ is an abbreviation for $CR[g, h_0, h_1](\bar{x}, y)$. The rules of AV are the ususal rules of equational logic (symmetry, transitivity, congruence and substitution) and a special rule of induction on notation:

$$\frac{\begin{array}{cc} \multicolumn{2}{c}{t_1[0] = t_2[0]} \\ t_1[x0] = v_0[t_1[x]] & t_2[x0] = v_0[t_2[x]] \\ t_1[x1] = v_1[t_1[x]] & t_2[x1] = v_1[t_2[x]] \end{array}}{t_1[x] = t_2[x]}$$

By Prop. 1, the function symbols in AV represent exactly the functions in AC^0. Based on Prop. 2, we define the equational calculi $A2V$ and TV whose function symbols represent exactly the functions in $ACC(2)$ and TC^0 respectively. They are defined like AV, but have additional primitive function symbols with axioms on them. $A2V$ has the additional unary function symbol *parity* with the axioms

$$(\dagger) \qquad \begin{gathered} parity(0) = 0\ ,\ \ parity(x0) = parity(x)\ , \\ parity(x1) = cond(parity(x), 1, 0)\ . \end{gathered}$$

TV has the additional unary function symbol *count* with the axioms

$$(\ddagger) \qquad count(0) = 0\,,\ count(x0) = count(x)\,,\ count(x1) = S(count(x))\,.$$

The simulation

For every equation $t = u$ of AV, a family of propositional tautologies $|t = u|^n$ for $n \geq 0$ is defined, where $|t = u|^b$ expresses the fact that the equality $t = u$ holds for all values of the variables whose lengths are bounded by b. We shall only sketch this definition, the reader is referred to [**10**] for the complete definition.

First, for every function symbol f a bounding polynomial $bound_f$ is defined, e.g. we define

$$\begin{gathered} bound_{s_0}(b) = bound_{s_1}(b) = bound_S(b) = b + 1\ , \\ bound_{cond}(b_1, b_2, b_3) = b_2 + b_3\ . \end{gathered}$$

This definition is extended inductively to arbitrary terms by

$$\begin{gathered} bound_0 = 0\ , \qquad bound_x(b) = b\ , \\ bound_{f(t_1(\bar{x}),\dots,t_m(\bar{x}))}(\bar{b}) = bound_f(bound_{t_1(\bar{x})}(\bar{b}), \dots, bound_{t_m(\bar{x})}(\bar{b}))\ . \end{gathered}$$

The polynomial $bound_{t(\bar{x})}(\bar{b})$ has the property that for values of the variables whose lengths are bounded by $\bar{b}$, the value of $t(\bar{x})$ is bounded in length by $bound_{t(\bar{x})}(\bar{b})$.

For every variable x of AV let $Q_i[x]$ and $P_i[x]$ be propositional variables who are intended to say $|x| > i$ and "the ith bit in x is 1" respectively. Furthermore let P be a variable that is different from all these, and let $\bot$ and $\top$ abbreviate $P \wedge \neg P$ and $P \vee \neg P$ respectively. Then for each term t whose variables are among the $x_1, \dots, x_m$ and non-negative integers i and $b_1, \dots, b_m$ two propositional formulas $q_i^{b_1,\dots,b_m}[t]$ and $p_i^{b_1,\dots,b_m}[t]$ in these variables are defined. The intended meaning of these formulas is $|t| > i$ and "the ith bit in t is 1", provided that $|x_j| \leq b_j$ for each $j \leq m$.

These formulas are defined inductively. First we define $q_i[0] = p_i[0] = \bot$, and for a variable x

$$q_i^b[x] = \begin{cases} Q_i[x] & \text{if } i < b \\ \bot & \text{else} \end{cases} \qquad p_i^b[x] = \begin{cases} P_i[x] & \text{if } i < b \\ \bot & \text{else} \end{cases} \ .$$

Then the formulas $q_i^{\bar{b}}[t]$ and $p_i^{\bar{b}}[t]$ are defined for terms consisting of a primitive function symbol applied to variables, e.g.

$$q_i^b[x0] = \begin{cases} q_0^b[x] & \text{if } i = 0 \\ q_{i-1}^b[x] & \text{else} \end{cases} \qquad p_i^b[x0] = \begin{cases} \bot & \text{if } i = 0 \\ p_{i-1}^b[x] & \text{else} \end{cases}$$

$$q_i^b[x1] = \begin{cases} \bot & \text{if } i = 0 = b \\ \top & \text{if } i = 0 < b \\ q_{i-1}^b[x] & \text{else} \end{cases} \qquad p_i^b[x1] = \begin{cases} \bot & \text{if } i = 0 = b \\ \top & \text{if } i = 0 < b \\ p_{i-1}^b[x] & \text{else} \end{cases}$$

$$q^{b_1,b_2,b_3}[cond(x,y,z)] = (\neg q_0^{b_1}[x] \wedge q_i^{b_2}[y]) \vee (q_0^{b_1}[x] \wedge q_i^{b_3}[z])$$

$$p^{b_1,b_2,b_3}[cond(x,y,z)] = (\neg q_0^{b_1}[x] \wedge p_i^{b_2}[y]) \vee (q_0^{b_1}[x] \wedge p_i^{b_3}[z])$$

$$q_i^b[S(x)] = \begin{cases} q_i^b[x] \vee \bigwedge_{j<i} p_j^b[x] & \text{if } i < b \\ \bot & \text{else} \end{cases}$$

$$p_i^b[S(x)] = \begin{cases} (p_i^b[x] \wedge \bigvee_{j<i} \neg p_j^b[x]) \vee (\neg p_i^b[x] \wedge \bigwedge_{j<i} p_j^b[x]) & \text{if } i > 0 \\ \neg p_i^b[x] & \text{else} \end{cases}$$

Now let $t = f(t_1(\bar{x}), \dots, t_m(\bar{x}))$, and let σ be the substitution replacing $Q_j[y_k]$ by $q_j^{\bar{b}}[t_k(\bar{x})]$ and $P_j[y_k]$ by $p_j^{\bar{b}}[t_k(\bar{x})]$ for each $j \leq m$, then we define

$$q_i^{\bar{b}}[t] := \sigma\big(\, q_i^{bound_{t_1(\bar{x})}(\bar{b}),\dots,bound_{t_m(\bar{x})}(\bar{b})}[f(y_1,\dots,y_m)]\,\big)$$

and $p_i^{\bar{b}}[t]$ analogously. The definition of $q_i^b[f(\bar{x})]$ and $p_i^b[f(\bar{x})]$ for compound function symbols is quite involved and is omitted here for sake of brevity.

For a variable x the formula $con^b[x]$ is defined as

$$\bigwedge_{i=0}^{b-2} q_{i+1}^b[x] \to q_i^b[x] \;\wedge\; \bigwedge_{i=0}^{b-1} p_i^b[x] \to q_i^b[x] \;\wedge\; \bigwedge_{i=1}^{b} len_i^b[x] \to p_{i-1}^b[x]$$

where $len_i^b[x]$ is defined as $q_{i-1}^b[x] \wedge \neg q_i^b[t]$. The formula $|t = u|_k^{\bar{b}}$ is

$$\bigwedge_{i=1}^{m} con^{b_i}[x_i] \to \bigwedge_{i=0}^{k-1} (q_i^{\bar{b}}[t] \leftrightarrow q_i^{\bar{b}}[u]) \wedge (p_i^{\bar{b}}[t] \leftrightarrow p_i^{\bar{b}}[u])$$

where the variables of t and u are among $x_1, \dots, x_m$. Finally, let $maxb_{t,u}(\bar{b})$ be an abbreviation for $\max(bound_t(\bar{b}), bound_u(\bar{b}))$, then we let

$$|t = u|^b := |t = u|_{maxb_{t,u}(b,\dots,b)}^{b,\dots,b} .$$

Now we are ready to state the following theorem, which was proved in [**10**].

Theorem 3. *If $AV \vdash t = u$, then the tautologies $|t = u|^n$ for $n \geq 0$ have polynomial size, constant depth Frege proofs.*

We shall now extend the translation defined above in such a way that equations in the languages of $A2V$ and TV are mapped to families of tautologies in the languages of $PK\oplus$ and PTK respectively.

The definition of the bounding polynomials $bound_t$ is extended by the clauses for the additional function symbols

$$bound_{parity}(b) = 1 \qquad bound_{count}(b) = b .$$

The definition of the formulas $q_i^{\bar{b}}[t]$ and $p_i^{\bar{b}}[t]$ is also extended by clauses for the additional primitive function symbols. For the additional function symbol *parity* of $A2V$ we define

$$q_0^b[parity(x)] = p_0^b[parity(x)] = \begin{cases} \bot & \text{if } b = 0 \\ p_0^b[x] & \text{if } b = 1 \\ \bigoplus^b(p_0^b[x], \dots, p_{b-1}^b[x]) & \text{else} \end{cases} ,$$

$$q_i^b[parity(x)] = p_i^b[parity(x)] = \bot \quad \text{for } i > 0.$$

For the additional function symbol *count* of TV we first define the PTK-formula $cnt_i^b[x]$

$$cnt_i^b[x] = \begin{cases} \neg T_1^b(p_0^b[x], \dots, p_{b-1}^b[x]) & \text{if } i = 0 \\ T_i^b(p_0^b[x], \dots, p_{b-1}^b[x]) \wedge \neg T_{i+1}^b(p_0^b[x], \dots, p_{b-1}^b[x]) & \text{if } 1 \le i < b \\ T_b^b(p_0^b[x], \dots, p_{b-1}^b[x]) & \text{if } i = b \\ \bot & \text{else} \end{cases} ,$$

and then

$$q_i^b[count(x)] = \begin{cases} T_{2^i}^b(p_0^b[x], \dots, p_{b-1}^b[x]) & \text{if } 2^i \le b \\ \bot & \text{else} \end{cases} ,$$

$$p_i^b[count(x)] = \bigvee_{\substack{j \le b \\ j \ni i}} cnt_j^b[x] ,$$

where $j \ni i$ means that the ith bit in j is 1. With these additional clauses, the families $|t = u|^n$ for equations $t = u$ of $A2V$ and TV are defined as above, and we can state our main theorem.

THEOREM 4. *If $A2V \vdash t = u$, then the tautologies $|t = u|^n$ for $n \ge 0$ have polynomial size, constant depth proofs in $PK\oplus$. If $TV \vdash t = u$, then the tautologies $|t = u|^n$ for $n \ge 0$ have polynomial size, constant depth proofs in PTK^*.*

By the above mentioned equivalences it follows that proofs in $A2V$ and TV can be simulated by polynomial size, constant depth proofs in $F(Mod_2)$ and FC respectively.

PROOF. Since both $PK\oplus$ and PTK^* can polynomially simulate a Frege system, where the simulations increase the depth at most by a constant, there are polynomial size, constant depth proofs of $|t = u|^n$ for every axiom $t = u$ of AV by Thm. 3. In Lemmas 5 and 6 below, we shall show that the translations of the additional axioms of $A2V$ and TV have polynomial size, constant depth proofs in $PK\oplus$ and PTK^*, respectively.

To complete the proof, it remains to show that for the rules of the equational calculi $A2V$ and TV, we get a polynomial size, constant depth proof of the conclusion from polynomial size, constant depth proofs of the premises, in both $PK\oplus$ and PTK^*.

Since the rules of $A2V$ and TV are the same as those of AV and constant depth Frege proofs of polynomial size can be simulated by polynomial size, constant depth proofs in $PK\oplus$ and PTK^*, the proof of this for the case of AV in [**10**] can be adapted to our case. The only change necessary is the incorporation of the additional function symbols in those places where the proof uses induction on the complexity of a term in AV. It is possible, although tedious, to show that these inductive arguments remain valid for terms in $A2V$ and TV. □

It remains to prove the promised lemmas, which will almost take the rest of the paper.

LEMMA 5. *The translations of the axioms (†) of $A2V$ have polynomial size, constant depth proofs in $PK\oplus$.*

PROOF. The formulas $|parity(0) = 0|^n$ do not depend on n and are true, hence they obviously have polynomial size, constant depth proofs in $PK\oplus$.

Now we have to prove in $PK\oplus$ the formulas $|parity(x0) = parity(x)|_1^b$. The formulas $q_0^b[parity(x0)]$ and $p_0^b[parity(x0)]$ are both

$$\bigoplus^{b+1}(p_0^{b+1}[x0], \dots, p_b^{b+1}[x0]) \;=\; \bigoplus^{b+1}(\bot, P_0[x], \dots, P_{b-1}[x]) \;,$$

and the formulas $q_0^b[parity(x)]$ and $p_0^b[parity(x0)]$ are both $\bigoplus^b(P_0[x], \dots, P_{b-1}[x])$. Thus we prove both required equivalences without using the assumption $con^b[x]$ by giving short proofs of

$$\bigoplus^{k+1}(\bot, A_1, \dots, A_k) \;\leftrightarrow\; \bigoplus^k(A_1, \dots, A_k)$$

for propositional variables $A_1, \dots, A_k$. These proofs have a constant number of steps, hence are of linear size, since we defined $\bigoplus^{k+1}$ by association to the left.

Finally we have to give proofs of $|parity(x1) = cond(parity(x), 1, 0)|_1^b$. The formulas $q_0^b[parity(x1)]$ and $p_0^b[parity(x1)]$ are by definition both

$$\bigoplus^{b+1}(\top, P_0[x], \dots, P_{b-1}[x]) \;,$$

and the formulas $q_0^b[cond(parity(x), 1, 0)]$ and $p_0^b[cond(parity(x), 1, 0)]$ are

$$\big(\neg q_0^b[parity(x)] \wedge \top\big) \vee \big(q_0^b[parity(x)] \wedge \bot\big) \;. \tag{1}$$

Their equivalence can again be proved without use of the assumption $con^b[x]$. The formulas (1) are shown to be equivalent to $\neg q_0^b[parity(x)]$ by short, constant depth proofs without use of the $\oplus$-rules, hence it remains to prove

$$\bigoplus^{k+1}(\top, A_1, \dots, A_k) \;\leftrightarrow\; \neg\bigoplus^k(A_1, \dots, A_k)$$

for propositional variables $A_1, \dots, A_k$. These equivalences are again easily seen to have short proofs in $PK\oplus$. □

LEMMA 6. *The translations of the axioms (‡) of TV have polynomial size, constant depth proofs in PTK^*.*

PROOF. The formulas $|count(0) = 0|^n$ are again true formulas that do not depend on n, hence there are trivially polynomial size, constant depth proofs in PTK^* of them.

We have to give PTK^*-proofs of the formulas $|count(x0) = count(x)|_{b+1}^b$. So under the hypothesis $con^b[x]$, which will in fact not be needed, we have to deduce

$$q_i^b[count(x0)] \;\leftrightarrow\; q_i^b[count(x)] \qquad \text{and} \qquad p_i^b[count(x0)] \;\leftrightarrow\; p_i^b[count(x)]$$

for every $i \le b$. For i with $2^i \le b + 1$, the formula $q_i^b[count(x0)]$ is defined as $T_{2^i}^{b+1}(p_0^{b+1}[x0], \dots, p_b^{b+1}[x0])$, which is $T_{2^i}^{b+1}(\bot, P_0[x], \dots, P_{b-1}[x])$. On the other hand, $q_i^b[count(x)]$ is $T_{2^i}^b(P_0[x],\dots,P_{b-1}[x])$ for i with $2^i \leq b$, and $\bot$ for $2^i > b$. Furthermore, the formulas $p_i^b[count(x0)]$ and $p_i^b[count(x)]$ are

$$\bigvee_{\substack{j\leq b+1\\ j\ni i}} cnt_j^{b+1}[x0] \qquad \text{and} \qquad \bigvee_{\substack{j\leq b\\ j\ni i}} cnt_j^b[x]\ .$$

To show their equivalence, we have to prove $cnt_j^b[x] \leftrightarrow cnt_j^{b+1}[x0]$ for every $j \leq b$ and $\neg cnt_{b+1}^{b+1}[x0]$ in PTK^*. All the required formulas are deduced by short, constant depth proofs from

$$T_k^{m+1}(\bot, A_1,\dots,A_m) \leftrightarrow T_k^m(A_1,\dots,A_m)$$

for $k \leq m$ and $\neg T_{m+1}^{m+1}(\bot, A_1,\dots,A_m)$, for variables $A_1,\dots,A_m$. Short proofs of these equivalences are easily given using the rules for T_k^n.

The most difficult part is to give proofs of $|count(x1) = S(count(x))|_{b+1}^b$. First we will give proofs of the equivalences $q_i^b[count(x1)] \leftrightarrow q_i^b[S(count(x))]$ for $i \leq b$ without using the assumption $con^b[x]$.

The formula $q_i^b[count(x1)]$ is by definition $T_{2^i}^{b+1}(\top, P_0[x],\dots,P_{b-1}[x])$ if $2^i \leq b+1$ and $\bot$ else, and the formula $q_i^b[S(count(x))]$ is

$$q_i^b[count(x)] \vee \bigwedge_{j<i} \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x]\ .$$

hence we have to show

$$\text{(I)} \qquad T_{2^i}^{b+1}(\top,\tilde{P}[x]) \leftrightarrow T_{2^i}^b(\tilde{P}[x]) \vee \bigwedge_{j<i} \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x] \qquad \text{for } 2^i \leq b,$$

$$\text{(II)} \qquad T_{2^i}^{b+1}(\top,\tilde{P}[x]) \leftrightarrow \bigwedge_{j<i} \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x] \qquad \text{for } 2^i = b+1,$$

$$\text{(III)} \qquad \neg \bigwedge_{j<i} \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x] \qquad \text{for } 2^i > b+1,$$

where $\tilde{P}[x]$ is short for $P_0[x],\dots,P_{b-1}[x]$. For this, we shall need short proofs of the sequents

$$\text{(2)} \qquad T_j^k(A_1,\dots,A_k) \implies T_{j-1}^k(A_1,\dots,A_k)$$

for every $1 < j \leq k$ and variables $A_1,\dots,A_k$. These are easily deduced using the rules T_k^n-left2 and T_k^n-right2. By use of (2), one can give proofs of the sequents $cnt_\mu^b[x], cnt_\nu^b[x] \implies$ for every $\mu < \nu \leq b$, of size $O(b(\nu-\mu))$.

We treat (II) first. The direction from left to right of the equivalence is obtained by a $\wedge$-right inference from the sequents

$$T_{2^i}^{b+1}(\top,\tilde{P}[x]) \implies \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x] \qquad \text{for } j < i,$$

which we get by weakening and $\vee$-right from $T_{2^i}^{b+1}(\top,\tilde{P}[x]) \implies cnt_b^b[x]$, since $b = 2^i - 1$, and hence $b \ni j$ for every $j < i$. These last sequents are by definition

$T_{b+1}^{b+1}(\top, \tilde{P}[x]) \implies T_b^b(\tilde{P}[x])$ and are easily deduced by the $\wedge$-rules. For the other direction, we have to give proofs of

$$\bigwedge_{j<i} \bigvee_{\substack{k \leq b \\ k \ni j}} cnt_k^b[x] \implies P_\ell[x]$$

for each $\ell \leq b-1$, from which together with $\implies \top$ we obtain the desired sequent by a $\wedge$-right inference. The sequent above is obtained by $\wedge$-left and a cut from $cnt_b^b[x] \implies P_\ell[x]$, which are easily easily derived as $b = 2^i - 1$, and

$$\bigvee_{\substack{k \leq b \\ k \ni 0}} cnt_k^b[x]\,,\ \ldots\,,\ \bigvee_{\substack{k \leq b \\ k \ni (i-1)}} cnt_k^b[x] \implies cnt_b^b[x]\,. \tag{3}$$

Each of the disjunctions on the left has $\lceil \frac{b+1}{2} \rceil$ terms. This sequent is deduced by two applications of $\vee$-left from $\lceil \frac{b+1}{2} \rceil^2$ sequents of the form

$$cnt_\mu^b[x]\,,\ cnt_\nu^b[x]\,,\ \bigvee_{\substack{k \leq b \\ k \ni 2}} cnt_k^b[x]\,,\ \ldots\,,\ \bigvee_{\substack{k \leq b \\ k \ni (i-1)}} cnt_k^b[x] \implies cnt_b^b[x]\,.$$

For $\mu \neq \nu$, these sequents have short proofs using (2), and the remaining ones with $\mu = \nu$ are again obtained by $\vee$-left from $\lceil \frac{b+1}{2} \rceil$ premises of the form

$$cnt_\nu^b[x]\,,\ cnt_\nu^b[x]\,,\ cnt_{\mu'}^b[x]\,,\ \bigvee_{\substack{k \leq b \\ k \ni 3}} cnt_k^b[x]\,,\ \ldots\,,\ \bigvee_{\substack{k \leq b \\ k \ni (i-1)}} cnt_k^b[x] \implies cnt_b^b[x]$$

for each such ν. But there are only $\lceil \frac{b+1}{4} \rceil$ values of ν for which $cnt_\nu^b[x]$ occurs in the first *and* second disjunction in (3). Again, most of these sequents have short proofs using (2), except for the $\lceil \frac{b+1}{8} \rceil$ of them with $\mu' = \nu$. After $i-1$ iterations of this process, the only remaining sequent to be deduced is the trivial

$$cnt_b^b[x]\,,\ \ldots\,,\ cnt_b^b[x] \implies cnt_b^b[x]\,,$$

since $b = 2^i - 1$ is the only value $k \leq b$ for which $k \ni j$ holds for every $j < i$. The size of these derivations can be calculated as follows: Each of the short proofs using (2) is of size $O(b^2)$, hence the whole proof is of size

$$O(b^2) \cdot \left\lceil \frac{b+1}{2} \right\rceil \cdot \sum_{1 \leq j < i} \left\lceil \frac{b+1}{2^j} \right\rceil \;=\; O(b^4)\,.$$

For case (III), we have to deduce the sequent

$$\bigvee_{\substack{k \leq b \\ k \ni 0}} cnt_k^b[x]\,,\ \ldots\,,\ \bigvee_{\substack{k \leq b \\ k \ni (i-1)}} cnt_k^b[x] \implies \quad .$$

A proof of this is constructed analogously to the proof of (3) above, where this time there is no sequent remaining after the $i-1$ steps, since there is no value $k \leq b$ for which $k \ni j$ holds for every $j < i$.

For case (I), observe that the following sequent is easily deduced:

$$T_{2^i-1}^b(\tilde{P}[x]) \implies T_{2^i}^b(\tilde{P}[x]), cnt_{2^i-1}^b[x]\,.$$

Since $2^i - 1 \ni j$ for every $j < i$, we get from this like in the proof of the first direction of (II)

$$T^b_{2^i-1}(\tilde{P}[x]) \Longrightarrow T^b_{2^i}(\tilde{P}[x]), \bigwedge_{j<i} \bigvee_{\substack{k \leq b \\ k \ni j}} cnt^b_k[x] \ ,$$

from which we obtain the left-to-right direction of (I) by $T^{b+1}_{2^i}$-left2. For the other direction, we first need proofs of

$$\bigwedge_{j<i} \bigvee_{\substack{k \leq b \\ k \ni j}} cnt^b_k[x] \Longrightarrow T^b_{2^i-1}(\tilde{P}[x]) \ . \tag{4}$$

These proofs can again be constructed by the method given for (3) in (II), since every value k for which $k \ni j$ for each $j < i$ is at least $k \geq 2^i - 1$. Now from (4) and $\Longrightarrow \top$ one gets by a $T^{b+1}_{2^i}$-right1

$$\bigwedge_{j<i} \bigvee_{\substack{k \leq b \\ k \ni j}} cnt^b_k[x] \Longrightarrow T^{b+1}_{2^i}(\top, \tilde{P}[x])$$

and from this and $T^b_{2^i}(\tilde{P}[x]) \Longrightarrow T^{b+1}_{2^i}(\top, \tilde{P}[x])$, a $\vee$-left yields the right-to-left direction of (I), which completes the proof of $q^b_i[count(x1)] \leftrightarrow q^b_i[S(count(x)]$.

Now we give proofs $p^b_i[count(x1)] \leftrightarrow p^b_i[S(count(x)]$, again without using the assumption $con^b[x]$. For this, we first need short proofs of the equivalence

$$cnt^b_j[x] \leftrightarrow cnt^{b+1}_{j+1}[s_1(x)] \ , \tag{5}$$

which can easily be given using (2). For $i = 0$, by definition we have to prove the equivalence

$$\bigvee_{\substack{j \leq b \\ j \ni 0}} cnt^b_j[x1] \leftrightarrow \neg \bigvee_{\substack{j \leq b \\ j \ni 0}} cnt^b_j[x] \ .$$

For the left-to-right direction, by (5) it is sufficient to deduce

$$\bigvee_{\substack{j \leq b \\ j \text{ odd}}} cnt^b_j[x] \ , \ \bigvee_{\substack{j \leq b \\ j \text{ even}}} cnt^b_j[x] \Longrightarrow \ ,$$

which is obtained by two applications of $\vee$-left from $\lceil \frac{b+1}{2} \rceil^2$ premises of the form $cnt^b_\mu, cnt^b_\nu \Longrightarrow$ for $\mu \leq b$ odd and $\nu \leq b$ even. These premises have, as noted above, short proofs using (2). For the other direction, we first show by induction that there are proofs of the sequents

$$T^b_k(\tilde{P}[x]) \Longrightarrow cnt^b_k[x], \ldots, cnt^b_b[x] \tag{6}$$

for every $k \leq b$ of size $O(b(b-k+1))$. This is trivial for $k = b$, and a proof of the sequent (6) for $k-1$ is easily given using (6) for k. This yields a proof of size $O(b^2)$ of the sequent

$$\Longrightarrow cnt^b_0[x], cnt^b_1[x], \ldots, cnt^b_b[x] \ .$$

Using the equivalence (5), we can deduce from this

$$\Longrightarrow \bigvee_{\substack{j \leq b \\ j \text{ odd}}} cnt^b_j[x] \ , \ \bigvee_{\substack{j \leq b+1 \\ j \text{ odd}}} cnt^{b+1}_j[x1] \ ,$$

which yields the desired right-to-left direction and thus completes the case $i = 0$.

For $i > 0$, the formula $p_i^b[S(count(x))]$ is

$$\big(\, p_i^b[count(x)] \wedge \bigvee_{j<i} \neg p_j^b[count(x)] \,\big) \vee \big(\, \neg p_i^b[count(x)] \wedge \bigwedge_{j<i} p_j^b[count(x)] \,\big) \ ,$$

thus the left-to-right direction of $p_i^b[count(x1)] \leftrightarrow p_i^b[S(count(x))]$ follows by a short, constant depth proof using (5) from the two sequents

$$\bigvee_{\substack{j\leq b\\(j+1)\ni i}} cnt_j^b[x]\,,\, p_i^b[count(x)] \implies \neg \bigwedge_{j<i} p_j^b[count(x)] \tag{7}$$

$$\bigvee_{\substack{j\leq b\\(j+1)\ni i}} cnt_j^b[x]\,,\, \neg p_i^b[count(x)] \implies \bigwedge_{j<i} p_j^b[count(x)]\ . \tag{8}$$

Recalling the definition of $p_j^b[count(x)]$, we see that the sequent (7) is obtained from at most $\lceil \frac{b+1}{2} \rceil$ sequents of the form

$$cnt_\nu^b[x]\,,\, \bigvee_{\substack{j\leq b\\ j\ni 0}} cnt_j^b[x]\,,\, \ldots\,,\, \bigvee_{\substack{j\leq b\\ j\ni i}} cnt_j^b[x] \implies\ ,$$

where ν is such that $(\nu+1) \ni i$. Since $\nu \ni k$ for all $k \leq i$ would imply $(\nu + 1) \not\ni i$, the formula $cnt_\nu^b[x]$ cannot appear in all of the disjunctions. Let k_0 be such that $\nu \not\ni k_0$, then we obtain the sequent above from at most $\lceil \frac{b+1}{2} \rceil$ sequents of the form

$$cnt_\nu^b[x]\,,\, cnt_\kappa^b[x]\,,\, \bigvee_{\substack{j\leq b\\ j\ni 0}} cnt_j^b[x]\,,\ldots\,,\, \bigvee_{\substack{j\leq b\\ j\ni i}} cnt_j^b[x] \implies\ ,$$

for each κ with $\kappa \ni k_0$ and hence $\kappa \neq \nu$, which have short constant depth PTK^*-proofs. Next (8) is obtained from at most $\lceil \frac{b+1}{2} \rceil$ sequents of the form

$$cnt_\nu^b[x] \implies \bigvee_{\substack{j\leq b\\ j\ni i}} cnt_j^b[x]\,,\, \bigwedge_{j<i} \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x] \tag{9}$$

with $(\nu + 1) \ni i$. Now if $\nu \ni i$, then (9) is obtained by weakening and $\vee$-right from an axiom since $cnt_\nu^b[x]$ appears in the first disjunction. Otherwise $\nu \ni j$ must hold for every $j < i$, hence we get (9) from i sequents

$$cnt_\nu^b[x] \implies \bigvee_{\substack{j\leq b\\ j\ni i}} cnt_j^b[x]\,,\, \bigvee_{\substack{k\leq b\\ k\ni j}} cnt_k^b[x]$$

for $j < i$, which can then be obtained as above since $cnt_\nu^b[x]$ must appear in the second disjunction.

Finally the right-to-left direction $p_i^b[S(count(x))] \to p_i^b[count(x1)]$ is deduced by short proofs using (5) from the two sequents

$$p_i^b[count(x)] \implies \bigwedge_{j<i} p_j^b[count(x)]\,,\, \bigvee_{\substack{j\leq b\\(j+1)\ni i}} cnt_j^b[x] \tag{10}$$

$$p_0^b[count(x)]\,,\ldots\,,\, p_{i-1}^b[count(x)] \implies p_i^b[count(x)]\,,\, \bigvee_{\substack{j\leq b\\(j+1)\ni i}} cnt_j^b[x]\ . \tag{11}$$

The sequent (10) is obtained by $\vee$-left and $\wedge$-right from $i \cdot \lceil \frac{b}{2} \rceil$ sequents of the form

$$cnt^b_\nu[x] \Longrightarrow \bigvee_{\substack{k \le b \\ k \ni j}} cnt^b_k[x]\,, \quad \bigvee_{\substack{j \le b \\ (j+1) \ni i}} cnt^b_j[x]$$

for ν with $\nu \ni i$ and $j < i$. Now if ν is such that $(\nu + 1) \ni i$, then $cnt^b_\nu[x]$ appears in the second disjunction. Otherwise it must be the case that $\nu \ni j$ for every $j < i$, hence $cnt^b_\nu[x]$ appears in the first disjunction. In both cases the sequent above is deduced by weakenings and $\vee$-right from an initial sequent.

By the method used for (3) above, (11) can be deduced using (2) from the sequents

$$cnt^b_\nu[x], \ldots , cnt^b_\nu[x] \Longrightarrow \bigvee_{\substack{j \le b \\ j \ni i}} cnt^b_j[x]\,, \quad \bigvee_{\substack{j \le b \\ (j+1) \ni i}} cnt^b_j[x]$$

for every ν with $\nu \ni k$ for every $k < i$. Now if $\nu \ni i$, then $cnt^b_\nu[x]$ appears in the first disjunction, and otherwise $(\nu + 1) \ni i$, hence $cnt^b_\nu[x]$ appears in the second disjunction, hence in either case this sequent is easily deduced. $\square$

Conclusion

We have presented equational calculi that prove equations between functions in $ACC(2)$ and TC^0, and shown that proofs in these can be simulated by polynomial size, constant depth proofs in Frege systems extended by modulo 2 counting and threshold connectives, respectively. It seems to be straightforward to define analogous calculi for the classes $ACC(m)$ for $m > 2$ and show these can be simulated by constant depth proofs in $F(Mod_m)$ in the same way. Besides supporting the intuitive correspondence between these complexity classes and proof systems, this provides us with a tool for proving the existence of polynomial size, constant depth proofs in these proof systems.

Actually, the relationship between PV and extended Frege proofs is much tighter than those presented in [**10**] and the present paper, in that extended Frege proofs are the maximal proof system among those whose correctness can be proved in PV. It should be possible, although tedious, to establish a similarly close connection between ALV from [**10**] and Frege proofs, using the fact that evaluation of boolean formulas can be done in NC^1 [**6**] (cf. also [**16**] for an effort in this direction).

To establish such a tight connection between TV, $A2V$ and AV and their corresponding proof systems, we have to overcome the obstacle that evaluation of boolean formulas is complete for NC^1, hence it is not possible in AC^0 and $ACC(2)$, and in TC^0 only if $TC^0 = NC^1$. Therefore it is not clear if the correctness of proofs can be expressed in these calculi.

The following remedy was suggested by P. Clote: The evaluation of threshold formulas of a fixed maximal depth d should be possible in TC^0, and by formalizing that we could then express the correctness of PTK-proofs of depth d by TV-terms. Then TV should be able to prove the correctness of PTK-proofs of depth d, for every d. A similar relationship might hold between $A2V$ and $F(Mod_2)$-proofs, as well as AV and Frege proofs.

References

1. Miklos Ajtai, *The complexity of the pigeonhole principle*, 29th Sympos. on Foundations of Computer Science, IEEE, 1988, pp. 346–355.
2. ______, *Parity and the pigeonhole principle*, Feasible Mathematics (Samuel R. Buss and Philip J. Scott, eds.), Birkhäuser, Boston, 1990, pp. 1–24.
3. Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák, *Lower bounds on Hilbert's Nullstellensatz and propositional proofs*, Proc. London Math. Soc. **73** (1996), 1–26.
4. Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, Pavel Pudlák, and Alan Woods, *Exponential lower bound for the pigeonhole principle*, Proc. 24th Sympos. Theory of Computing, 1992, pp. 200–221.
5. Paul Beame and Toniann Pitassi, *An exponential separation between the matching principle and the pigeonhole principle*, Proc. LICS '93, 1993, pp. 308–319.
6. Samuel R. Buss, *The Boolean formula value problem is in $ALOGTIME$*, Proceedings of the 19th Sympos. Theory of Computing, ACM, 1987, pp. 123–131.
7. Samuel R. Buss and Peter Clote, *Cutting planes, connectivity and threshold logic*, Arch. Math. Logic **35** (1995), 34 ff.
8. ______, *Threshold logic proof systems*, unpublished manuscript, 1995.
9. Peter Clote, *Sequential, machine independent characterizations of the parallel complexity classes $ALogTIME$, AC^k, NC^k and NC*, Feasible Mathematics (Samuel R. Buss and Philip J. Scott, eds.), Birkhäuser, Boston, 1990, pp. 49–69.
10. ______, *$ALOGTIME$ and a conjecture of S. A. Cook*, Ann. Math. Artificial Intelligence **6** (1992), 57–106.
11. Peter Clote and Gaisi Takeuti, *First order bounded arithmetic and small boolean circuit complexity classes*, Feasible Mathematics II (Peter Clote and Jeffrey Remmel, eds.), Birkhäuser, Boston, 1995, pp. 154–218.
12. Alan Cobham, *The intrinsic computational difficulty of functions*, Proc. 2nd International Congress on Logic, Methodology and Philosophy of Science, 1965, pp. 24–30.
13. Stephen A. Cook, *Feasible constructive proofs and the propositional calculus*, Proc. 7th Sympos. Theory of Computing, 1975, pp. 83–97.
14. Stephen A. Cook and Robert A. Reckhow, *The relative efficiency of propositional proof systems*, J. Symbolic Logic **44** (1979), 36–50.
15. Jan Krajíček, *On Frege and Extended Frege proof systems*, Feasible Mathematics II (Peter Clote and Jeffrey Remmel, eds.), Birkhäuser, Boston, 1995, pp. 284–319.
16. François Pitt, *A quantifier-free theory based on a string algebra for NC^1*, this volume.
17. Alasdair Urquhart, *Hard examples for resolution*, J. Assoc. Comput. Mach. **34** (1987), 209–219.
18. ______, *The complexity of propositional proofs*, Bull. Symbolic Logic **1** (1995), 425–467.

Informatik 1, Universität Erlangen-Nürnberg, Erlangen, Germany

Current address: Department of Mathematics, University of California, San Diego, La Jolla, California 92093-0112

E-mail address: `johannsn@math.ucsd.edu`