tba

Arnold Beckmann

Department of Computer Science
University of Wales Swansea
UK

5 April 2008
Workshop in Honour of Wilfried Buchholz' 60th Birthday
Munich

Proof Notations for Bounded Arithmetic

Arnold Beckmann (joint work with Klaus Aehlig)

Department of Computer Science
University of Wales Swansea
UK

5 April 2008
Workshop in Honour of Wilfried Buchholz' 60th Birthday
Munich

Outline of talk

Language of Bounded Arithmetic (BA)

Language of first order arithmetic similar to Peano Arithmetic

Non-logical symbols:

$$\{0, 1, +, \cdot, \leq\} \quad + \quad \{|.|, \#, \dots\}$$

$$\begin{aligned} |x| &= \text{length of binary representation of } x \\ x\#y &= 2^{|x|\cdot|y|} \text{ produces polynomial growth rate} \end{aligned}$$

Language of Bounded Arithmetic (BA)

Language of first order arithmetic similar to Peano Arithmetic

Non-logical symbols:

$$\{0, 1, +, \cdot, \leq\} \quad + \quad \{|.|, \#, \dots\}$$

$$\begin{aligned} |x| &= \text{length of binary representation of } x \\ x\#y &= 2^{|x|\cdot|y|} \text{ produces polynomial growth rate} \end{aligned}$$

Bounded Formulas:

$\hat{\Sigma}^b_1$: $\exists x_1 \leq s_1 \; \forall y \leq |t| \; \varphi(x_1, y)$

$\hat{\Sigma}^b_2$: $\exists x_1 \leq s_1 \; \forall x_2 \leq s_2 \; \exists y \leq |t| \; \varphi(x_1, x_2, y)$

$\vdots$

with quantifier-free φ

Bounded Arithmetic theories

Induction:

$$\Phi\text{-Ind}: \quad \varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(x)$$

$$\Phi\text{-LInd}: \quad \varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(|x|)$$

where $\varphi \in \Phi$

Bounded Arithmetic theories

Induction:

$$\Phi\text{-Ind}: \quad \varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(x)$$

$$\Phi\text{-LInd}: \quad \varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(|x|)$$

where $\varphi \in \Phi$

BASIC $=$ a set of open formulas defining the non-logical symbols.

Theories: Pick a set of formulas and an induction scheme, form the theory BASIC $+$ all instances of induction for formulas from the set just picked.

Examples:

$$S^1_2 = \text{BASIC} + \hat{\Sigma}^b_1\text{-LInd}$$

$$S^2_2 = \text{BASIC} + \hat{\Sigma}^b_2\text{-LInd}$$

Definable functions

f is $\hat{\Sigma}^{\mathrm{b}}_1$-definable in S^1_2 iff there exists $\varphi \in \hat{\Sigma}^{\mathrm{b}}_1$ such that

- $f(x) = y \iff \mathbb{N} \models \varphi(x, y)$
- $S^1_2 \vdash \forall x \exists y \varphi(x, y)$

Definable functions

f is $\hat{\Sigma}^{b}_{1}$-definable in S^1_2 iff there exists $\varphi \in \hat{\Sigma}^{b}_{1}$ such that

- $f(x) = y \iff \mathbb{N} \vDash \varphi(x, y)$
- $S^1_2 \vdash \forall x \exists y \varphi(x, y)$

Theorem (Buss '86)

f is $\hat{\Sigma}^{b}_{1}$-definable in S^1_2 iff $f \in FP$

Definable functions – the general case

f is $\hat{\Sigma}^{\mathrm{b}}_i$-definable in T
iff
there exists $\varphi \in \hat{\Sigma}^{\mathrm{b}}_i$
such that

- $f(x) = y$
  $\iff$
  $\mathbb{N} \models \varphi(x, y)$
- $T \vdash \forall x \exists y \varphi(x, y)$

bounded arithmetic theories		polynomial time hierarchy of functions
$\vdots$		$\vdots$
S^3_2	$\hat{\Sigma}^{\mathrm{b}}_3$	$FP^{\Sigma^p_2}$
S^2_2	$\hat{\Sigma}^{\mathrm{b}}_2$	$FP^{\Sigma^p_1}$
S^1_2	$\hat{\Sigma}^{\mathrm{b}}_1$	FP

Definable search problems

Theorem (Buss '86)

$\hat{\Sigma}^{\mathrm{b}}_{i}$*-definable functions in* $S^i_2 = FP^{\Sigma^p_{i-1}}$

Definable search problems

Theorem (Buss '86)

$\hat{\Sigma}^{\mathrm{b}}_i$*-definable functions in* $S^i_2 = FP^{\Sigma^p_{i-1}}$

Theorem (Krajíček'93)

$\hat{\Sigma}^{\mathrm{b}}_{i+1}$*-definable multi-functions in* $S^i_2 = FP^{\Sigma^p_i}[wit, O(\log n)]$

Definable search problems

Theorem (Buss '86)

$\hat{\Sigma}^b_i$-*definable functions in* $S^i_2 = FP^{\Sigma^p_{i-1}}$

Theorem (Krajíček'93)

$\hat{\Sigma}^b_{i+1}$-*definable multi-functions in* $S^i_2 = FP^{\Sigma^p_i}[wit, O(\log n)]$

Theorem (Buss, Krajíček'94)

$\hat{\Sigma}^b_{i-1}$-*definable multi-functions in* $S^i_2 =$ *projection of* $PLS^{\Sigma^p_{i-2}}$

Independence results

Main open problem for bounded arithmetic:

Does the hierarchy of bounded arithmetic theories collapse?

Independence results

Main open problem for bounded arithmetic:

Does the hierarchy of bounded arithmetic theories collapse?

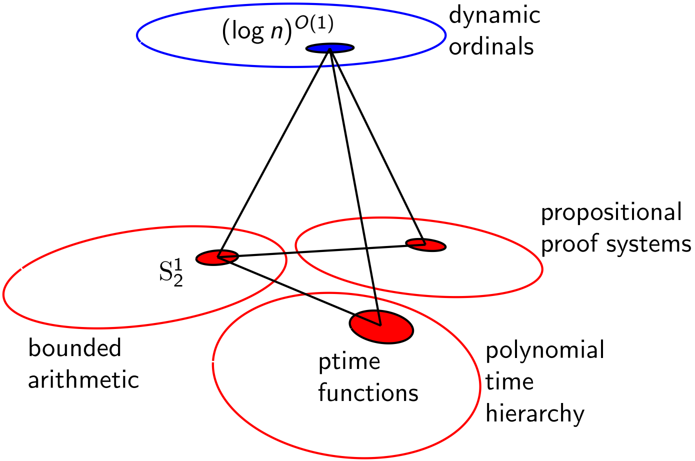
Theorem (Krajíček, Pudlák, Takeuti '91, Krajíček '93)

If the levels of the polynomial time hierarchy of predicates (PH) are separated, then the levels of bounded arithmetic theories (BA) are separated as well.
In particular, if $\Sigma^p_{i+2} \neq \Pi^p_{i+2}$, then $\mathrm{S}^i_2 \neq \mathrm{S}^{i+1}_2$.

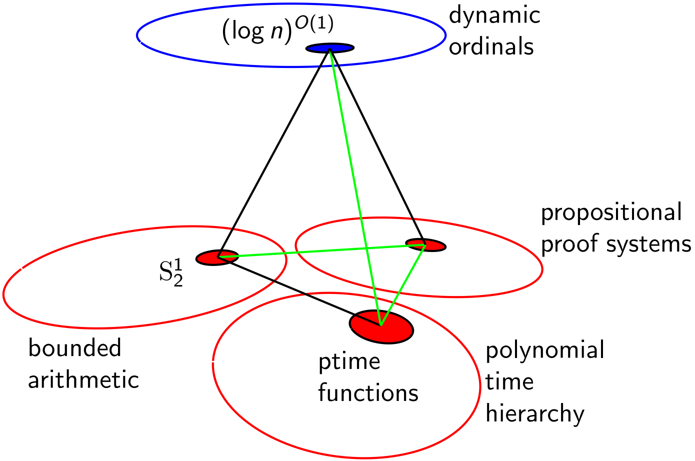
Theorem (Buss '95, Zambella '96)

BA collapses iff PH collapses provable in BA

Dynamic ordinals – a picture



Dynamic ordinals – a picture



Proposed future work at MFO'05:

> *Adapt finitary notations for infinitary derivations to Bounded Arithmetic setting.*

Wilfried Buchholz. Notation systems for infinitary derivations. *Archive for Mathematical Logic*, 30:277–296, 1991.

Proposed future work at MFO'05:

> *Adapt finitary notations for infinitary derivations to Bounded Arithmetic setting.*

Wilfried Buchholz. Notation systems for infinitary derivations. *Archive for Mathematical Logic*, 30:277–296, 1991.

Klaus Aehlig and **Arnold Beckmann.** On the computational complexity of cut-reduction. Accepted for publication at LICS 2008.

Full version available as Technical Report CSR15-2007, Department of Computer Science, Swansea University, December 2007. `http://arxiv.org/abs/0712.1499`.

Finitary Proof System $\mathrm{BA}^\star$

$$(\mathrm{Ax}_\Delta) \quad \frac{}{\Delta} \quad \text{if } \bigvee \Delta \in \mathrm{BASIC}$$

$$(\bigwedge_{A_0 \wedge A_1}) \quad \frac{A_0 \qquad A_1}{A_0 \wedge A_1} \qquad (\bigvee^k_{A_0 \vee A_1}) \quad \frac{A_k}{A_0 \vee A_1} \quad (k \in \{0,1\})$$

$$(\bigwedge^y_{(\forall x)A}) \quad \frac{A_x(y)}{(\forall x)A} \qquad (\bigvee^t_{(\exists x)A}) \quad \frac{A_x(t)}{(\exists x)A}$$

$$(\mathrm{IND}^{y,t}_F) \quad \frac{\neg F, F_y(\mathsf{s}\, y)}{\neg F_y(0), F_y(2^{|t|})}$$

$$(\mathrm{IND}^{y,n,i}_F) \quad \frac{\neg F, F_y(\mathsf{s}\, y)}{\neg F_y(\underline{n}), F_y(\underline{n+2^i})} \quad (n, i \in \mathbb{N})$$

$$(\mathrm{Cut}_C) \quad \frac{C \qquad \neg C}{\emptyset}$$

Proof Notations for Bounded Arithmetic

$\mathcal{H}_{\mathrm{BA}}$: set of closed $\mathrm{BA}^{\star}$-derivations

For $h \in \mathcal{H}_{\mathrm{BA}}$ define, following translation into propositional logic

$\mathsf{tp}(h)$: denoted last inference

$h[j]$: denoted jth subderivation

$|h|$: size $=$ number of inference symbols occurring in h

$\mathsf{o}(h)$: height of denoted derivation tree

Using auxiliary induction inference symbols $(\mathrm{IND}_F^{y,n,i})$ we can ensure

$$|h[i]| \leq |h|$$

Abstract notation for cut-elimination

Let I, E and R be new symbols.

"Cut elimination closure" $\widetilde{\mathcal{H}_{\mathrm{BA}}}$: inductively defined to extend $\mathcal{H}_{\mathrm{BA}}$ and contain $\mathsf{I}d$, $\mathsf{E}d$, and $\mathsf{R}de$.

Size: $|\mathsf{I}d| = |\mathsf{E}d| = 1 + |d|$, $|\mathsf{R}de| = 1 + |d| + |e|$.

Height: $o(\mathsf{I}d) = o(d)$, $o(\mathsf{R}de) = o(d) + o(e)$, $o(\mathsf{E}d) = 2^{o(d)} - 1$.

Abstract notation for cut-elimination

Let I, E and R be new symbols.

"Cut elimination closure" $\widetilde{\mathcal{H}_{\mathrm{BA}}}$: inductively defined to extend $\mathcal{H}_{\mathrm{BA}}$ and contain $\mathsf{I}d$, $\mathsf{E}d$, and $\mathsf{R}de$.

Size: $|\mathsf{I}d| = |\mathsf{E}d| = 1 + |d|$, $|\mathsf{R}de| = 1 + |d| + |e|$.

Height: $o(\mathsf{I}d) = o(d)$, $o(\mathsf{R}de) = o(d) + o(e)$, $o(\mathsf{E}d) = 2^{o(d)} - 1$.

Relation $\longrightarrow$ is inductively defined as follows.

$$\frac{d' = d[i] \text{ in } \mathcal{H}_{\mathrm{BA}},\ i \in \mathbb{N}}{d \longrightarrow d'} \qquad \frac{d \longrightarrow d'}{\mathsf{I}d \longrightarrow \mathsf{I}d'} \qquad \frac{e \longrightarrow e'}{\mathsf{R}de \longrightarrow \mathsf{R}de'}$$

$$\frac{d \longrightarrow d'}{\mathsf{E}d \longrightarrow \mathsf{E}d'} \qquad \frac{}{\mathsf{R}de \longrightarrow \mathsf{I}d} \qquad \frac{d \longrightarrow d' \qquad d \longrightarrow d''}{\mathsf{E}d \longrightarrow \mathsf{R}(\mathsf{E}d')(\mathsf{E}d'')}$$

Definition

Define *size function* $\vartheta\colon \widetilde{\mathcal{H}_{\mathrm{BA}}} \to \mathbb{N}$ by induction on inductive definition of $\widetilde{\mathcal{H}_{\mathrm{BA}}}$:

$$\begin{aligned}
\vartheta(d) &= |d|, \text{ provided } d \in \mathcal{H}_{\mathrm{BA}} \\
\vartheta(\mathsf{I}d) &= \vartheta(d) + 1 \\
\vartheta(\mathsf{R}de) &= \max\{|d|{+}1{+}\vartheta(e)\ ,\ \vartheta(d){+}1\} \\
\vartheta(\mathsf{E}d) &= o(d)(\vartheta(d) + 2)
\end{aligned}$$

Definition

Define *size function* $\vartheta \colon \widetilde{\mathcal{H}_{\mathrm{BA}}} \to \mathbb{N}$ by induction on inductive definition of $\widetilde{\mathcal{H}_{\mathrm{BA}}}$:

$$\begin{aligned}
\vartheta(d) &= |d|, \text{ provided } d \in \mathcal{H}_{\mathrm{BA}} \\
\vartheta(\mathsf{I}d) &= \vartheta(d) + 1 \\
\vartheta(\mathsf{R}de) &= \max\{|d|+1+\vartheta(e)\ ,\ \vartheta(d)+1\} \\
\vartheta(\mathsf{E}d) &= o(d)(\vartheta(d) + 2)
\end{aligned}$$

Proposition

For every $d \in \widetilde{\mathcal{H}_{\mathrm{BA}}}$ we have $|d| \leq \vartheta(d)$.

Theorem

If $d \in \widetilde{\mathcal{H}_{\mathrm{BA}}}$ and $d \to d'$, then $\vartheta(d) \geq \vartheta(d')$.

Computational Content of Bounded Arithmetic Proofs

Assume $\mathrm{S}^2_2 \vdash (\forall x)(\exists y)\varphi(x,y)$. Fix $h \in \mathrm{BA}^\star$ such that end-sequent of h is $(\exists y)\varphi(x,y)$ and all formulas in h are in $\hat{\Sigma}^{\mathrm{b}}_2 \cup \hat{\Pi}^{\mathrm{b}}_2$. Then

$$\mathrm{o}(h[x/\underline{a}]) = \mathcal{O}(\log\log a)$$

(this coincides with the dynamic ordinal analysis of S^2_2.)

Computational Content of Bounded Arithmetic Proofs

Assume $\mathrm{S}^2_2 \vdash (\forall x)(\exists y)\varphi(x,y)$. Fix $h \in \mathrm{BA}^\star$ such that end-sequent of h is $(\exists y)\varphi(x,y)$ and all formulas in h are in $\hat{\Sigma}^b_2 \cup \hat{\Pi}^b_2$. Then

$$\mathrm{o}(h[x/\underline{a}]) = \mathcal{O}(\log\log a)$$

(this coincides with the dynamic ordinal analysis of S^2_2.)

We want to define a search problem on the translated propositional derivation, where we follow a path guaranteeing that the sequents are of the form $(\exists y)\varphi(\underline{a},y),\Gamma$ where all formulas in Γ are false. As the derivation tree is well-founded, this search must end with a $\bigvee^k_{(\exists y)\varphi(\underline{a},y)}$-inference for which $\varphi(\underline{a},\underline{k})$ is true, then we are done.

Computational Content of Bounded Arithmetic Proofs

Assume $\mathrm{S}^2_2 \vdash (\forall x)(\exists y)\varphi(x,y)$. Fix $h \in \mathrm{BA}^\star$ such that end-sequent of h is $(\exists y)\varphi(x,y)$ and all formulas in h are in $\hat{\Sigma}^{\mathrm{b}}_2 \cup \hat{\Pi}^{\mathrm{b}}_2$. Then

$$\mathrm{o}(h[x/\underline{a}]) = \mathcal{O}(\log\log a)$$

(this coincides with the dynamic ordinal analysis of S^2_2.)

We want to define a search problem on the translated propositional derivation, where we follow a path guaranteeing that the sequents are of the form $(\exists y)\varphi(\underline{a},y),\Gamma$ where all formulas in Γ are false. As the derivation tree is well-founded, this search must end with a $\bigvee^k_{(\exists y)\varphi(\underline{a},y)}$-inference for which $\varphi(\underline{a},\underline{k})$ is true, then we are done.

To define such a path, we have to make decisions: In case Cut_C we have to decide whether C is true or not, and in case $\bigvee^k_{(\exists y)\varphi(\underline{a},y)}$ we have to decide whether we found a witness or not. To obtain optimal results, all decisions should have same complexity $\mathcal{C}$.

A general local search problem

Define local search problem L: On instance $a \in \mathbb{N}$

possible solutions $F(a)$: all $h \in \widetilde{\mathcal{H}_{\mathrm{BA}}}$ with

$\Gamma(h) \subseteq \{(\exists y)\varphi(\underline{a}, y)\} \cup \Delta$ for some $\Delta \subseteq \mathcal{C} \cup \neg\mathcal{C}$ such that all $A \in \Delta$ are closed and false,

$\mathcal{C}\text{-crk}(h) \leq 1$,

$\mathrm{o}(h) \leq \mathrm{o}(h_a)$,

$\vartheta(h) \leq \vartheta(h_a)$, ...

A general local search problem

Define local search problem L: On instance $a \in \mathbb{N}$

possible solutions $F(a)$: all $h \in \widetilde{\mathcal{H}_{\mathrm{BA}}}$ with
$\Gamma(h) \subseteq \{(\exists y)\varphi(\underline{a}, y)\} \cup \Delta$ for some $\Delta \subseteq \mathcal{C} \cup \neg\mathcal{C}$ such that all $A \in \Delta$ are closed and false,
$\mathcal{C}\text{-crk}(h) \leq 1$,
$\mathrm{o}(h) \leq \mathrm{o}(h_a)$,
$\vartheta(h) \leq \vartheta(h_a)$, ...

initial value function: $i(a) := h_a$.

cost function: $c(a, h) := \mathrm{o}(h)$.

neighbourhood function: $N(a, h) = h[j]$ if j'th minor premise of last rule is in $F(a)$, and h otherwise.

A general local search problem

Define local search problem L: On instance $a \in \mathbb{N}$

possible solutions $F(a)$: all $h \in \widetilde{\mathcal{H}_{\mathrm{BA}}}$ with
$\Gamma(h) \subseteq \{(\exists y)\varphi(\underline{a}, y)\} \cup \Delta$ for some $\Delta \subseteq \mathcal{C} \cup \neg\mathcal{C}$ such that all $A \in \Delta$ are closed and false,
$\mathcal{C}\text{-crk}(h) \leq 1$,
$\mathrm{o}(h) \leq \mathrm{o}(h_a)$,
$\vartheta(h) \leq \vartheta(h_a)$, ...

initial value function: $i(a) := h_a$.

cost function: $c(a, h) := \mathrm{o}(h)$.

neighbourhood function: $N(a, h) = h[j]$ if j'th minor premise of last rule is in $F(a)$, and h otherwise.

Solution to L on a is any h with $N(a, h) = h$.

$\hat{\Sigma}^b_1$-definable multi-functions in S^2_2

$\hat{\Sigma}^b_1$-definable multi-functions in S^2_2

As $\varphi \in \hat{\Pi}^b_0$, let $\mathcal{C} := \hat{\Pi}^b_0$ and consider $h_a := \mathrm{EE}h[x/\underline{a}]$.
$\mathrm{o}(h_a) = 2^{(\log a)^{\mathcal{O}(1)}}$, $\vartheta(h_a) = (\log a)^{\mathcal{O}(1)}$.

$\hat{\Sigma}^b_1$-definable multi-functions in S^2_2

As $\varphi \in \hat{\Pi}^b_0$, let $\mathcal{C} := \hat{\Pi}^b_0$ and consider $h_a := \mathsf{EE}h[x/\underline{a}]$.
$\mathrm{o}(h_a) = 2^{(\log a)^{\mathcal{O}(1)}}$, $\vartheta(h_a) = (\log a)^{\mathcal{O}(1)}$.

This search problem defines a PLS-problem, which coincides with the description given by [Buss and Krajíček'94].

Theorem (Buss, Krajíček'94)

$\hat{\Sigma}^b_{i-1}$-definable multi-functions in S^i_2 = projection of $PLS^{\Sigma^p_{i-2}}$

$\hat{\Sigma}^b_2$-definable functions in S^2_2

$\hat{\Sigma}^b_2$-definable functions in S^2_2

As $\varphi \in \hat{\Pi}^b_1$, let $\mathcal{C} := \hat{\Pi}^b_1$ and consider $h_a := \mathsf{E}h[x/\underline{a}]$.
$o(h_a) = (\log a)^{\mathcal{O}(1)}$.

$\hat{\Sigma}^{\mathrm{b}}_2$-definable functions in S^2_2

As $\varphi \in \hat{\Pi}^{\mathrm{b}}_1$, let $\mathcal{C} := \hat{\Pi}^{\mathrm{b}}_1$ and consider $h_a := \mathsf{E}h[x/\underline{a}]$.
$\mathrm{o}(h_a) = (\log a)^{\mathcal{O}(1)}$.

This can be seen to define a function in $\mathrm{FP}^{\mathsf{NP}}$, which coincides with the description given by [Buss '86].

Theorem (Buss '86)

$\hat{\Sigma}^{\mathrm{b}}_i$-definable functions in $S^i_2 = FP^{\Sigma^p_{i-1}}$

$\hat{\Sigma}^b_3$-definable functions in S^2_2

$\hat{\Sigma}^b_3$-definable functions in S^2_2

As $\varphi \in \hat{\Pi}^b_2$, let $\mathcal{C} := \hat{\Pi}^b_2$ and consider $h_a := h[x/\underline{a}]$.
$o(h_a) = \mathcal{O}(\log \log a)$.

$\hat{\Sigma}^b_3$-definable functions in S^2_2

As $\varphi \in \hat{\Pi}^b_2$, let $\mathcal{C} := \hat{\Pi}^b_2$ and consider $h_a := h[x/\underline{a}]$.
$o(h_a) = \mathcal{O}(\log \log a)$.

This can be seen to define a multi-function in $\mathrm{FP}^{\hat{\Sigma}^b_2}[wit, O(\log n)]$, which coincides with the description given by [Krajíček'93].

Theorem (Krajíček'93)

$\hat{\Sigma}^b_{i+1}$-definable multi-functions in S^i_2 $= FP^{\Sigma^p_i}[wit, O(\log n)]$

Future Work

Find characterisations for all combinations of Bounded Arithmetic theories and levels of definability.

Future Work

Find characterisations for all combinations of Bounded Arithmetic theories and levels of definability.

The End

References

Klaus Aehlig and Arnold Beckmann. On the computational complexity of cut-reduction. Accepted for publication at LICS 2008. Full version available as Technical Report CSR15-2007, Department of Computer Science, Swansea University, December 2007. `http://arxiv.org/abs/0712.1499`.

Arnold Beckmann. Dynamic ordinal analysis. *Arch. Math. Logic*, 42:303–334, 2003.

Arnold Beckmann. Generalised dynamic ordinals–universal measures for implicit computational complexity. In *Logic Colloquium '02*, vol. 27 of *Lect. Notes Log.*, pp. 48–74. Assoc. Symbol. Logic, 2006.

Wilfried Buchholz. Notation systems for infinitary derivations. *Archive for Mathematical Logic*, 30:277–296, 1991.

Samuel R. Buss. *Bounded arithmetic*, vol. 3 of *Stud. Proof Theory, Lect. Notes*. Bibliopolis, Naples, 1986.

Samuel R. Buss and Jan Krajíček. An application of boolean complexity to separation problems in bounded arithmetic. *Proceedings of the London Mathematical Society*, 69:1–21, 1994.

S. R. Buss. Relating the bounded arithmetic and the polynomial time hierarchies. *APAL*, 75:67–77, 1995.

Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52:143–153, 1991.

Jan Krajíček. Fragments of bounded arithmetic and bounded query classes. *Transactions of the American Mathematical Society*, 338:587–98, 1993.

D. Zambella. Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, 61:942–966, 1996.