Theories for Subexponential-size Bounded-depth Frege Proofs

Kaveh Ghasemloo and Stephen Cook

Department of Computer Science
University of Toronto
Canada

CSL 2013

Propositional vs Uniform Proof Complexity

- Propositional proof complexity studies the lengths of proofs of tautology families in proof systems such as Frege and bdFrege (bounded-depth Frege).

Propositional vs Uniform Proof Complexity

- Propositional proof complexity studies the lengths of proofs of tautology families in proof systems such as Frege and bdFrege (bounded-depth Frege).
- Uniform proof complexity studies the power of weak formal theories such as VNC^1 and V^0.

Propositional vs Uniform Proof Complexity

- Propositional proof complexity studies the lengths of proofs of tautology families in proof systems such as Frege and bdFrege (bounded-depth Frege).
- Uniform proof complexity studies the power of weak formal theories such as VNC^1 and V^0.
- Both proof systems and theories are often associated with complexity classes.
  - Frege systems and VNC^1 are associated with the complexity class NC^1
  - bdFrege and V^0 are associated with the complexity class AC^0.

Complexity Classes, Theories, and Proof Systems

A three-way connection $\langle$ C, VC, C-Frege $\rangle$

- Complexity class C, theory VC, and proof system C-Frege
- The provably total functions in VC are those in C

Complexity Classes, Theories, and Proof Systems

A three-way connection $\langle$ C, VC, C-Frege $\rangle$

- Complexity class C, theory VC, and proof system C-Frege
- The provably total functions in VC are those in C
- C-Frege is the strongest propositional proof system whose soundness is provable in VC

Complexity Classes, Theories, and Proof Systems

A three-way connection $\langle$ C, VC, C-Frege $\rangle$

- Complexity class C, theory VC, and proof system C-Frege
- The provably total functions in VC are those in C
- C-Frege is the strongest propositional proof system whose soundness is provable in VC
- The Σ_0^B theorems of VC translate to a family $\{\varphi_n\}_n$ of propositional tautologies which have polynomial size C-Frege proofs.
  Example: VNC^1 proves the Pigeonhole Principle: "For all n, $n+1$ pigeons cannot be assigned to n holes with at most one pigeon per hole."
  The corresponding tautologies $\{\varphi_n\}_n$ have polysize Frege proofs.

Complexity Classes, Theories, and Proof Systems

A three-way connection ⟨ C, VC, C-Frege ⟩

- Complexity class C, theory VC, and proof system C-Frege
- The provably total functions in VC are those in C
- C-Frege is the strongest propositional proof system whose soundness is provable in VC
- The Σ_0^B theorems of VC translate to a family $\{\varphi_n\}_n$ of propositional tautologies which have polynomial size C-Frege proofs.
  Example: VNC^1 proves the Pigeonhole Principle: "For all n, $n+1$ pigeons cannot be assigned to n holes with at most one pigeon per hole."
  The corresponding tautologies $\{\varphi_n\}_n$ have polysize Frege proofs.

Examples

- ⟨ NC^1, VNC^1, Frege ⟩
- ⟨ AC^0, V^0, bdFrege ⟩
- ⟨ P, VP, eFrege ⟩

Motivatation for our paper

1. Theorem[FPS'12]: Frege proofs can be converted to bdFrege proofs of subexponential size.
2. That is, given $0 < \varepsilon < 1$ and a family $\{\varphi_n\}_n$ of tautologies and a family $\{\pi_n\}_n$ of Frege proofs such that π_n proves φ_n and has size $n^{O(1)}$, there exists a family $\{\pi'_n\}_n$ of Frege proofs such that π'_n proves φ_n and has size $2^{O(n^{\varepsilon})}$ and all cut formulas have depth $O(1)$.
3. We want a uniform version of this.

Motivatation for our paper

1. Theorem[FPS'12]: Frege proofs can be converted to bdFrege proofs of subexponential size.
2. That is, given $0 < \varepsilon < 1$ and a family $\{\varphi_n\}_n$ of tautologies and a family $\{\pi_n\}_n$ of Frege proofs such that π_n proves φ_n and has size $n^{O(1)}$, there exists a family $\{\pi'_n\}_n$ of Frege proofs such that π'_n proves φ_n and has size $2^{O(n^\varepsilon)}$ and all cut formulas have depth $O(1)$.
3. We want a uniform version of this.
4. i.e. we want a triple $\langle C_\varepsilon, VC_\varepsilon, C_\varepsilon\text{-}Frege\rangle$ where C_ε-*Frege* is as in item 2 above.

Motivatation for our paper

1. Theorem[FPS'12]: Frege proofs can be converted to bdFrege proofs of subexponential size.
2. That is, given $0 < \varepsilon < 1$ and a family $\{\varphi_n\}_n$ of tautologies and a family $\{\pi_n\}_n$ of Frege proofs such that π_n proves φ_n and has size $n^{O(1)}$, there exists a family $\{\pi'_n\}_n$ of Frege proofs such that π'_n proves φ_n and has size $2^{O(n^\varepsilon)}$ and all cut formulas have depth $O(1)$.
3. We want a uniform version of this.
4. i.e. we want a triple $\langle C_\varepsilon, VC_\varepsilon, C_\varepsilon\text{-}\mathit{Frege}\rangle$ where C_ε-*Frege* is as in item 2 above.
5. Note that bdFrege and C_ε-*Frege* are *proof classes* rather than proof systems.
   A Proof class associates families of proofs with families of formulas.

What is the triple $\langle C_\varepsilon, VC_\varepsilon, C_\varepsilon\text{-}Frege\rangle$ for subexponential bdFrege?

- Here $\varepsilon = 1/d$ where $d > 1$ is an integer.
- Let $C_\varepsilon = \mathrm{AltTime}(O(1), O(n^\varepsilon))$
  (problems computable by uniform size $2^{O(n^\varepsilon)}$ bounded-depth circuit families).
- $\mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq C_\varepsilon$

What is the triple $\langle C_\varepsilon, VC_\varepsilon, C_\varepsilon\text{-}Frege\rangle$ for subexponential bdFrege?

- Here $\varepsilon = 1/d$ where $d > 1$ is an integer.
- Let $C_\varepsilon = \mathrm{AltTime}(O(1), O(n^\varepsilon))$
  (problems computable by uniform size $2^{O(n^\varepsilon)}$ bounded-depth circuit families).
- $\mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq C_\varepsilon$
- What is the theory VC_ε.?
  (We want the provably total functions of VC_ε to be those in C_ε.)

What is the triple $\langle C_\varepsilon, VC_\varepsilon, C_\varepsilon\text{-}Frege\rangle$ for subexponential bdFrege?

- Here $\varepsilon = 1/d$ where $d > 1$ is an integer.
- Let $C_\varepsilon = \mathrm{AltTime}(O(1), O(n^\varepsilon))$
(problems computable by uniform size $2^{O(n^\varepsilon)}$ bounded-depth circuit families).
- $\mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq C_\varepsilon$
- What is the theory VC_ε.?
(We want the provably total functions of VC_ε to be those in C_ε.)
- Major Obstacle: In general the provably total functions in a theory VC are closed under compostion. But the subexponential functions are not closed under composition.
- For example the composition of $n \mapsto 2^{n^{\frac{1}{2}}}$ with $n \mapsto n^2$ is 2^n.

What is the triple $\langle C_\varepsilon, VC_\varepsilon, C_\varepsilon\text{-}Frege\rangle$ for subexponential bdFrege?

- Here $\varepsilon = 1/d$ where $d > 1$ is an integer.
- Let $C_\varepsilon = \mathrm{AltTime}(O(1), O(n^\varepsilon))$
  (problems computable by uniform size $2^{O(n^\varepsilon)}$ bounded-depth circuit families).
- $\mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq C_\varepsilon$
- What is the theory VC_ε.?
  (We want the provably total functions of VC_ε to be those in C_ε.)
- Major Obstacle: In general the provably total functions in a theory VC are closed under compostion. But the subexponential functions are not closed under composition.
- For example the composition of $n \mapsto 2^{n^{\frac{1}{2}}}$ with $n \mapsto n^2$ is 2^n.
- We'll get to this in a moment.

We follow the framework in [Cook-Nguyen '10]

Program in Chapter 9

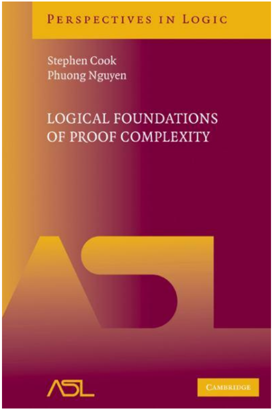
1. Presents a general method for associating a theory VC with a complexity classes C, including theories

$$\mathrm{V}^0 \subseteq \mathrm{VNC}^1 \subseteq \mathrm{VL} \subseteq \mathrm{VNL} \subseteq \mathrm{VP}$$

for classes

$$\mathrm{AC}^0 \subseteq \mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq \mathrm{P}$$

2. Theories have two sorts: Natural numbers $x, y, z, \ldots$ and bit strings $X, Y, Z, \ldots$.
3. Function symbols 0, 1, $+$, $\cdot$, $|\,|$ (length)
4. Relation symbols $=$, $\leq$, and $\in$ (membership/bit).



Two-sorted relations and formulas

- (Uniform)
  $\mathrm{AC}^0 = \mathrm{FO} = \mathrm{AltTime}(O(1), O(\lg n)) = \mathrm{DepthSize}(O(1), n^{O(1)})$.
- A relation $R(\vec{x}, \vec{X})$ is in AC^0 as above, where number arguments $\vec{x}$ are presented in unary.

Two-sorted relations and formulas

- (Uniform)
  $\mathrm{AC}^0 = \mathrm{FO} = \mathrm{AltTime}(O(1), O(\lg n)) = \mathrm{DepthSize}(O(1), n^{O(1)})$.
- A relation $R(\vec{x}, \vec{X})$ is in AC^0 as above, where number arguments $\vec{x}$ are presented in unary.
- Σ_0^B is the class of formulas with no string quantifiers, and with all number quantifers bounded.
- Σ_0^B Representation Theorem: A relation $R(\vec{x}, \vec{X})$ is in AC^0 iff it is represented by a Σ_0^B formula $\varphi(\vec{x}, \vec{X})$.

Two-sorted relations and formulas

- (Uniform)
  $\mathrm{AC}^0 = \mathrm{FO} = \mathrm{AltTime}(O(1), O(\lg n)) = \mathrm{DepthSize}(O(1), n^{O(1)})$.
- A relation $R(\vec{x}, \vec{X})$ is in AC^0 as above, where number arguments $\vec{x}$ are presented in unary.
- Σ_0^B is the class of formulas with no string quantifiers, and with all number quantifers bounded.
- Σ_0^B Representation Theorem: A relation $R(\vec{x}, \vec{X})$ is in AC^0 iff it is represented by a Σ_0^B formula $\varphi(\vec{x}, \vec{X})$.
- Σ_i^B and Π_i^B are classes of bounded formulas with limits on alternations of the string quantifiers.
- $\exists^B \Phi$ consists of formulas starting with bounded existential string quantifiers followed by a formula in Φ.

Introducing io-typed theories ioVC to limit composition

- Introduce two types of variables: input type and output type
- input type: a, b, c denote numbers, A, B, C denote strings.
  output type: x, y, z denote numbers, X, Y, Z denote strings.

Introducing io-typed theories ioVC to limit composition

- Introduce two types of variables: input type and output type
- input type: a, b, c denote numbers, A, B, C denote strings.
  output type: x, y, z denote numbers, X, Y, Z denote strings.
- For fast growing f, the arugments of f have input type and are small, while the value of f has output type and might be large.

Introducing io-typed theories ioVC to limit composition

- Introduce two types of variables: input type and output type
- input type: a, b, c denote numbers, A, B, C denote strings.
  output type: x, y, z denote numbers, X, Y, Z denote strings.
- For fast growing f, the arugments of f have input type and are small, while the value of f has output type and might be large.
- For each $0 < \varepsilon < 1$, the functions with growth rate $2^{O(n^\varepsilon)}$ are closed under composition with linear functions, so we allow linear terms to be input type.

Introducing io-typed theories ioVC to limit composition

- Introduce two types of variables: input type and output type
- input type: a, b, c denote numbers, A, B, C denote strings.
  output type: x, y, z denote numbers, X, Y, Z denote strings.
- For fast growing f, the arugments of f have input type and are small, while the value of f has output type and might be large.
- For each $0 < \varepsilon < 1$, the functions with growth rate $2^{O(n^{\varepsilon})}$ are closed under composition with linear functions, so we allow linear terms to be input type.
- All terms (including input type terms) have output type.

Introducing io-typed theories ioVC to limit composition

- Introduce two types of variables: input type and output type
- input type: a, b, c denote numbers, A, B, C denote strings.
  output type: x, y, z denote numbers, X, Y, Z denote strings.
- For fast growing f, the arugments of f have input type and are small, while the value of f has output type and might be large.
- For each $0 < \varepsilon < 1$, the functions with growth rate $2^{O(n^{\varepsilon})}$ are closed under composition with linear functions, so we allow linear terms to be input type.
- All terms (including input type terms) have output type.
- Example input type term:

$$a + b + 1 + \mathrm{pd}(c) + |A| + |B|$$

(No output type variables allowed.)

Theory io2Basic: Axioms have output type variables

Table: io2Basic

B1	$x + 1 \neq 0$	B7	$x \leq y \wedge y \leq x \rightarrow x = y$
B2	$x + 1 = y + 1 \rightarrow x = y$	B8	$x \leq x + y$
B3	$x + 0 = x$	B9	$0 \leq x$
B4	$x + (y + 1) = (x + y) + 1$	B10	$x \leq y \vee y \leq x$
B5	$x \cdot 0 = 0$	B11	$x \leq y \leftrightarrow x < y + 1$
B6	$x \cdot (y + 1) = x \cdot y + x$	B12	$\mathrm{pd}(0) = 0 \wedge (x \neq 0 \rightarrow \mathrm{pd}(x) + 1 = x)$
L	$y \in X \rightarrow y < \lvert X \rvert$		

$X = Y$ abbreviates $(|X| = |Y| \wedge \forall x \leq |X| \; x \in X \leftrightarrow x \in Y)$.

Theory ioV^0 for AC^0

ioV^0 extends io2Basic by adding the substring function $X[y, z]$ and the following axioms:

Theory ioV^0 for AC^0

ioV^0 extends io2Basic by adding the substring function $X[y,z]$ and the following axioms:

- $x \in X[y,z] \leftrightarrow x < z \wedge y + x \in X$
- $|X[y,z]| = z$

Theory ioV^0 for AC^0

ioV^0 extends io2Basic by adding the substring function $X[y,z]$ and the following axioms:

- $x \in X[y,z] \leftrightarrow x < z \wedge y + x \in X$
- $|X[y,z]| = z$
- Ind: $0 \in X, \forall y < z \ (y \in X \to y + 1 \in X) \Rightarrow z \in X$
- φ-CA (Comprehension): $\exists Y = z \ \forall x < z \ \left(x \in Y \leftrightarrow \varphi(x, \vec{a}, \vec{A})\right)$
  where $\varphi(x, \vec{a}, \vec{A})$ is in Σ_0^B

Theory ioV^0 **for** AC^0

ioV^0 extends io2Basic by adding the substring function $X[y, z]$ and the following axioms:

- $x \in X[y, z] \leftrightarrow x < z \wedge y + x \in X$
- $|X[y, z]| = z$
- Ind: $0 \in X, \forall y < z\ (y \in X \rightarrow y + 1 \in X) \Rightarrow z \in X$
- φ-CA (Comprehension): $\exists Y = z\ \forall x < z\ \left(x \in Y \leftrightarrow \varphi(x, \vec{a}, \vec{A})\right)$

  where $\varphi(x, \vec{a}, \vec{A})$ is in Σ_0^B
- $\mathrm{oiConv}_{\mathrm{num}}$: $\exists b \leq a\ \ b = \min(a, x)$
- $\mathrm{oiConv}_{\mathrm{str}}$: $\exists B = a\ \ B = X[y, a]$

Theory ioV^0 for AC^0

ioV^0 extends io2Basic by adding the substring function $X[y,z]$ and the following axioms:

- $x \in X[y,z] \leftrightarrow x < z \wedge y + x \in X$
- $|X[y,z]| = z$
- Ind: $0 \in X, \forall y < z\ (y \in X \to y+1 \in X) \Rightarrow z \in X$
- φ-CA (Comprehension): $\exists Y = z\ \forall x < z\ \left(x \in Y \leftrightarrow \varphi(x, \vec{a}, \vec{A})\right)$
  where $\varphi(x, \vec{a}, \vec{A})$ is in Σ_0^B
- $\mathrm{oiConv}_{\mathrm{num}}$: $\exists b \le a\ \ b = \min(a, x)$
- $\mathrm{oiConv}_{\mathrm{str}}$: $\exists B = a\ \ B = X[y, a]$

Theorem: The $\exists^B \Sigma_0^B$ definable functions in ioV^0 coincide with the AC^0 functions.

Theory $\mathrm{ioVNC}^1 = \mathrm{ioV}^0 + \Sigma_0^B(\mathrm{MBBFE})\text{-CA}$

Theory $\mathrm{ioVNC}^1 = \mathrm{ioV}^0 + \Sigma_0^B(\mathrm{MBBFE})\text{-CA}$

$\Sigma_0^B(\mathrm{MBBFE})$-CA is the following axiom schema:

$$\exists Y = 2s\ \exists Z = 2s\ [\forall x < 2s\ (x \in Z \leftrightarrow \varphi(x, \vec{a}, \vec{A}))\wedge \\ \text{“}Y \text{ is the computation of } Z\text{”}]$$

where s has output type and $\varphi \in \Sigma_0^B$ and “Y is the computation of Z” stands for

$$\forall z < s\ [z{+}s \in Y \leftrightarrow z \in Z]\wedge[(z \in Z \rightarrow (z \in Y \leftrightarrow 2z \in Y \wedge 2z+1 \in Y))\wedge$$

$$(z \notin Z \rightarrow (z \in Y \leftrightarrow 2z \in Y \vee 2z+1 \in Y))]$$

We think of φ as specifying the bit graph of an AC^0 function whose output Z is as an instance of MBBFE: its first half specifies the gates of the formula and its second half specifies the inputs to the formula.

Theory $\mathrm{ioVNC}^1 = \mathrm{ioV}^0 + \Sigma_0^B(\mathrm{MBBFE})$-CA

$\Sigma_0^B(\mathrm{MBBFE})$-CA is the following axiom schema:

$$\exists Y = 2s \;\; \exists Z = 2s \;\; [\forall x < 2s \;\; (x \in Z \leftrightarrow \varphi(x, \vec{a}, \vec{A})) \wedge \text{“}Y \text{ is the computation of } Z\text{”}]$$

where s has output type and $\varphi \in \Sigma_0^B$ and “Y is the computation of Z” stands for

$$\forall z < s \;\; [z+s \in Y \leftrightarrow z \in Z] \wedge [(z \in Z \to (z \in Y \leftrightarrow 2z \in Y \wedge 2z+1 \in Y)) \wedge$$

$$(z \notin Z \to (z \in Y \leftrightarrow 2z \in Y \vee 2z+1 \in Y))]$$

We think of φ as specifying the bit graph of an AC^0 function whose output Z is as an instance of MBBFE: its first half specifies the gates of the formula and its second half specifies the inputs to the formula.

Theorem: The $\exists^B \Sigma_0^B$ definable functions of ioVNC^1 are precisely the NC^1 functions.

Theory n^{ε}-ioV$^{\infty}$ (This is $\mathsf{VC}_{\varepsilon}$)

Theory n^{ε}-ioV$^{\infty}$ (This is VC$_{\varepsilon}$)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^{ε} (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^{\varepsilon} = y \leftrightarrow y^{d} \leq x < (y+1)^{d}$.

Theory n^{ε}-ioV$^{\infty}$ (This is VC$_{\varepsilon}$)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^{ε} (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^{\varepsilon} = y \leftrightarrow y^{d} \leq x < (y+1)^{d}$.

We call a formula $\Sigma^{B}_{\infty}(n^{\varepsilon})$ iff it is bounded and all of its string quantifiers are bounded by linear terms in n^{ε} (n is the max size of its free variables).

Theory n^ε-ioV^∞ (This is VC_ε)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^ε (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^\varepsilon = y \leftrightarrow y^d \leq x < (y+1)^d$.

We call a formula $\Sigma^B_\infty(n^\varepsilon)$ iff it is bounded and all of its string quantifiers are bounded by linear terms in n^ε (n is the max size of its free variables).
Definition: n^ε-$\mathrm{ioV}^\infty = \mathrm{ioV}^0 + \Sigma^B_\infty(n^\varepsilon)$-Comprehension

Theory n^{ε}-ioV^{∞} (This is $\mathrm{VC}_{\varepsilon}$)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^{ε} (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^{\varepsilon} = y \leftrightarrow y^{d} \leq x < (y+1)^{d}$.

We call a formula $\Sigma^{B}_{\infty}(n^{\varepsilon})$ iff it is bounded and all of its string quantifiers are bounded by linear terms in n^{ε} (n is the max size of its free variables).
Definition: n^{ε}-$\mathrm{ioV}^{\infty} = \mathrm{ioV}^{0} + \Sigma^{B}_{\infty}(n^{\varepsilon})$-Comprehension
We take the provably total functions in n^{ε}-ioV^{∞} to be the Φ-definable functions, where $\Phi = \exists^{B}\Sigma^{B}_{\infty}(n^{\varepsilon})$.

Theory n^ε-ioV^∞ (This is VC_ε)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^ε (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^\varepsilon = y \leftrightarrow y^d \leq x < (y+1)^d$.

We call a formula $\Sigma^B_\infty(n^\varepsilon)$ iff it is bounded and all of its string quantifiers are bounded by linear terms in n^ε (n is the max size of its free variables).
Definition: n^ε-$\mathrm{ioV}^\infty = \mathrm{ioV}^0 + \Sigma^B_\infty(n^\varepsilon)$-Comprehension
We take the provably total functions in n^ε-ioV^∞ to be the Φ-definable functions, where $\Phi = \exists^B\Sigma^B_\infty(n^\varepsilon)$.

Theorem

The provably total functions of the theory n^ε-ioV^∞ are exactly those of polynomial growth rate whose graphs are in $\mathrm{AltTime}(O(1), O(n^\varepsilon))$, where n is the size of the arguments.

Theory n^{ε}-ioV$^{\infty}$ (This is VC$_{\varepsilon}$)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^{ε} (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^{\varepsilon} = y \leftrightarrow y^{d} \leq x < (y+1)^{d}$.

We call a formula $\Sigma^{B}_{\infty}(n^{\varepsilon})$ iff it is bounded and all of its string quantifiers are bounded by linear terms in n^{ε} (n is the max size of its free variables).
Definition: $n^{\varepsilon}\text{-ioV}^{\infty} = \text{ioV}^{0} + \Sigma^{B}_{\infty}(n^{\varepsilon})$-Comprehension
We take the provably total functions in n^{ε}-ioV$^{\infty}$ to be the Φ-definable functions, where $\Phi = \exists^{B}\Sigma^{B}_{\infty}(n^{\varepsilon})$.

Theorem

The provably total functions of the theory n^{ε}-ioV$^{\infty}$ are exactly those of polynomial growth rate whose graphs are in $\text{AltTime}(O(1), O(n^{\varepsilon}))$, *where n is the size of the arguments.*

Theorem: The theories n^{ε}-ioV$^{\infty}$ contain the theory ioVNC^{1}.

Theory n^{ε}-ioV$^{\infty}$ (This is VC$_{\varepsilon}$)

Here $\varepsilon = 1/d$, where $d > 1$ is a constant. The theory includes the function x^{ε} (actually $\lfloor x^{\frac{1}{d}} \rfloor$) with defining axiom $x^{\varepsilon} = y \leftrightarrow y^d \leq x < (y+1)^d$.

We call a formula $\Sigma_{\infty}^{B}(n^{\varepsilon})$ iff it is bounded and all of its string quantifiers are bounded by linear terms in n^{ε} (n is the max size of its free variables).
Definition: n^{ε}-ioV$^{\infty}$ = ioV^0 + $\Sigma_{\infty}^{B}(n^{\varepsilon})$-Comprehension
We take the provably total functions in n^{ε}-ioV$^{\infty}$ to be the Φ-definable functions, where $\Phi = \exists^B \Sigma_{\infty}^{B}(n^{\varepsilon})$.

Theorem

The provably total functions of the theory n^{ε}-ioV$^{\infty}$ are exactly those of polynomial growth rate whose graphs are in AltTime$(O(1), O(n^{\varepsilon}))$, *where n is the size of the arguments.*

Theorem: The theories n^{ε}-ioV$^{\infty}$ contain the theory ioVNC^1.
Proof Idea: The $\Sigma_{\infty}^{B}(n^{\varepsilon})$-Comprehension axiom can formalize Buss's Prover-Challenger game to solve the MBBFE problem.

Proof Systems for Quantified Propositional Calculus

Proof Systems for Quantified Propositional Calculus

1. System G for quantified propositional calculus is based on Gentzen's sequent calculus.

Proof Systems for Quantified Propositional Calculus

1. System G for quantified propositional calculus is based on Gentzen's sequent calculus.
2. System PK (equivalent to Frege systems) is G restricted to quantifier-free formulas.

Proof Systems for Quantified Propositional Calculus

1. System G for quantified propositional calculus is based on Gentzen's sequent calculus.
2. System PK (equivalent to Frege systems) is G restricted to quantifier-free formulas.
3. For $d > 1$, system d-PK (equivalent to d-Frege) is PK with cuts restricted to depth d formulas.

Proof Systems for Quantified Propositional Calculus

1. System G for quantified propositional calculus is based on Gentzen's sequent calculus.
2. System PK (equivalent to Frege systems) is G restricted to quantifier-free formulas.
3. For $d > 1$, system d-PK (equivalent to d-Frege) is PK with cuts restricted to depth d formulas.
4. We say a formula family $\{\varphi_n\}_n$ has polysize bdFrege proofs if there are constants d and m such that each φ_n has a d-Frege proof of size $O(|\varphi_n|^m)$.

Proof Class n^{ε}-bdG_{∞} (Quantified version of C_{ε}-Frege)

Definition

n^{ε}-bdG_{∞} is the class of bdG_{∞} proof families with cuts restricted to $\mathsf{bd}\Sigma^{\mathsf{q}}_{\infty}$ formulas with an absolute upper bound on the number of quantifier alternations, and the total number of eigenvariables in each sequent does not exceed n^{ε}, where n is the size of the proven formula.

Proof Class n^{ε}-bdG_{∞} (Quantified version of C_{ε}-Frege)

Definition

n^{ε}-bdG_{∞} is the class of bdG_{∞} proof families with cuts restricted to $\mathsf{bd}\Sigma^{\mathsf{q}}_{\infty}$ formulas with an absolute upper bound on the number of quantifier alternations, and the total number of eigenvariables in each sequent does not exceed n^{ε}, where n is the size of the proven formula.

Remark: It follows that the total number of quantified variables in any formula in any proof does not exceed n^{ε}, assuming that this is true of formulas that are proved.

Translating two-sorted terms to sequences of propositional formulas

The *translation context* $\sigma : Var \to \mathbb{N}$ assigns number (size) to each variable. $\sigma(x)$ is the value of x and $\sigma(X)$ is the length of X. σ naturally extends to assign a size to every term.

Table: Extended Translation Context σ and Translation of Terms

$\sigma(0) = 0$ $\sigma(1) = 1$ $\sigma(t+s) = \sigma(t) + \sigma(s)$ $\sigma(t \cdot s) = \sigma(t) \cdot \sigma(s)$ $\sigma(\mathrm{pd}(t)) = \mathrm{pd}(\sigma(t))$ $\sigma(\lvert T \rvert) = \sigma(T)$ $\sigma(f(\vec{t}, \vec{T})) = f^\sigma(\sigma(\vec{t}), \sigma(\vec{T}))$ $\sigma(F(\vec{t}, \vec{T})) = F^\sigma(\sigma(\vec{t}), \sigma(\vec{T}))$	$[\![n]\!]_\sigma = (\top, \overbrace{\bot, \dots, \bot}^{n \text{ times}}), \quad n \in \mathbb{N}$ $[\![t]\!]_\sigma = [\![\sigma(t)]\!]_\sigma$ $[\![X]\!]_\sigma = (p^X_{\sigma(X)-1}, \dots, p^X_0)$ $[\![F(\vec{t}, \vec{T})]\!]_\sigma = (F_{\sigma(F(\vec{t},\vec{T}))-1}([\![\vec{t}]\!]_\sigma, [\![\vec{T}]\!]_\sigma)$

Translating two-sorted formulas to quantified propositional formulas

Table: Translation of Formulas

$[\![s = t]\!]_\sigma = \begin{cases} \top & [\![s]\!]_\sigma = [\![t]\!]_\sigma \\ \bot & o.w. \end{cases}$ $[\![s \leq t]\!]_\sigma = \begin{cases} \top & [\![s]\!]_\sigma \leq [\![t]\!]_\sigma \\ \bot & o.w. \end{cases}$ $[\![t \in T]\!]_\sigma = ([\![T]\!]_\sigma)_{[\![t]\!]_\sigma}$	$[\![\bot]\!]_\sigma = \bot$ $[\![\top]\!]_\sigma = \top$ $[\![\neg\varphi]\!]_\sigma = \neg[\![\varphi]\!]_\sigma$ $[\![\psi \wedge \varphi]\!]_\sigma = [\![\psi]\!]_\sigma \wedge [\![\varphi]\!]_\sigma$ $[\![\psi \vee \varphi]\!]_\sigma = [\![\psi]\!]_\sigma \vee [\![\varphi]\!]_\sigma$ $[\![\exists x \leq t \;\; \varphi]\!]_\sigma = \bigvee_{i \leq \sigma(t)} [\![x \leq t \wedge \varphi]\!]_{\sigma[x \mapsto i]}$ $[\![\forall x \leq t \;\; \varphi]\!]_\sigma = \bigwedge_{i \leq \sigma(t)} [\![x \leq t \to \varphi]\!]_{\sigma[x \mapsto i]}$ $[\![\exists X = t \;\; \varphi]\!]_\sigma = \exists[\![X]\!]_\tau \;\; [\![X = t \wedge \varphi]\!]_\tau$ $[\![\forall X = t \;\; \varphi]\!]_\sigma = \forall[\![X]\!]_\tau \;\; [\![X = t \to \varphi]\!]_\tau.$ where $\tau = \sigma[X \mapsto \sigma(t)]$

Translating Proofs to Propositional Proofs

Old results (e.g. [Cook/Nguyen])

Theorem

If $\varphi \in \Sigma_0^B$ is provable in V^0 *(resp.* VNC^1*) then* $\{\llbracket\varphi\rrbracket_{\vec{n}}\}_{\vec{n}}$ *has polynomial-size* bdFrege *(resp.* Frege*) proofs.*

New results:

Theorem

If $\varphi \in \Sigma_0^B$ is provable in n^{ε}-ioV^{∞} *(i.e.* $\mathrm{VC}_{\varepsilon}$*) then* $\{\llbracket\varphi\rrbracket_{\vec{n}}\}_{\vec{n}}$ *has polynomial-size* n^{ε}-bdG_{∞} *proofs.*

Corollary

If $\varphi \in \Sigma_0^B$ is provable in n^{ε}-ioV^{∞} *(i.e.* $\mathrm{VC}_{\varepsilon}$*) then* $\{\llbracket\varphi\rrbracket_{\vec{n}}\}_{\vec{n}}$ *has size* $2^{O(n^{\varepsilon})}$ bdFrege *proofs.*

Main Results

Theorem

ioVNC^1 *proves the soundness of Frege.*

Corollary

$\mathrm{n}^{\varepsilon}\text{-}\mathrm{ioV}^{\infty}$ *proves the soundness of Frege*

Corollary

Frege proofs can be effectively translated to polynomial size $\mathrm{n}^{\varepsilon}\text{-}\mathrm{bdG}_{\infty}$ *proofs, and to size* $2^{O(n^{\varepsilon})}$ *size* bdFrege *proofs.*

Main Results

Theorem

ioVNC^1 *proves the soundness of Frege.*

Corollary

$\mathrm{n}^{\varepsilon}\text{-}\mathrm{ioV}^{\infty}$ *proves the soundness of Frege*

Corollary

Frege proofs can be effectively translated to polynomial size $\mathrm{n}^{\varepsilon}\text{-}\mathrm{bdG}_{\infty}$ *proofs, and to size* $2^{O(n^{\varepsilon})}$ *size* bdFrege *proofs.*

See our websites for updated versions of these results.

Main Results

Theorem

ioVNC^1 *proves the soundness of Frege.*

Corollary

$\mathrm{n}^{\varepsilon}\text{-}\mathrm{ioV}^{\infty}$ *proves the soundness of Frege*

Corollary

Frege proofs can be effectively translated to polynomial size $\mathrm{n}^{\varepsilon}\text{-}\mathrm{bdG}_{\infty}$ *proofs, and to size* $2^{O(n^{\varepsilon})}$ *size* bdFrege *proofs.*

See our websites for updated versions of these results.
THANK YOU