# A Second Order Theory for $\mathbf{TC}^0$

Kazuhiro Ishida

Mathematical Institute, Tohoku University

December 10, 2011

# Outline

1. What is Bounded Reverse Mathematics?
2. Weaker complexity classes than **P**
3. Introduction to second order theories for complexity classes
4. An example of Bounded Reverse Mathematics
5. A new second order theory for $\mathbf{TC}^0$

# What is Bounded Reverse Mathematics?

# What is Bounded Reverse Mathematics?

Questions [Cook]

Given a theorem , what is the least complexity class containing enough concepts to prove the theorem?

That is, we construct second order theories for complexity classes and we check whether the theorem can prove in the theory, or not.
I will introduce some example later.

# Weaker complexity classes than **P**

# Complexity classes

To define weaker complexity classes than **P**, we need to define the computational model "Boolean circuit".

**Def (Boolean circuit)**

For all $n \in \mathbb{N}$, Boolean circuit $C_n$ is a directed acyclic graph with $n$-input and 1-output. All non-input vertices are called gates and labeled with one of $\vee$, $\wedge$, $\neg$. The size of $C_n$, denoted by $|C_n|$, is the number of vertices in it. And, the depth of a circuit is the length of the longest directed path from an input node to the output node.

**Def**

Let T: $\mathbb{N} \to \mathbb{N}$ be a function. A family of $T(n)$-size circuit is a sequence $\{C_n\}_{n \in \mathbb{N}}$ of Boolean circuits, where $C_n$ has $n$-input, a 1-output and its size $|C_n| \leq T(n)$ for all $n$.

# Complexity classes

**Def**

- $\mathbf{AC}^0$ ($\mathbf{NC}^1$) : A class of relations which are accepted by a family $\{C_n\}_{n\in\mathbb{N}}$ of circuits of size $n^{\mathcal{O}(1)}$ and depth $\mathcal{O}(1)$ ($\mathcal{O}(\log n)$), with unbounded (bounded) fan-in $\wedge$, $\vee$-gates.
- $\mathbf{TC}^0$ ($\mathbf{AC}^0(m)$) : A class of relations which are accepted by a family $\{C_n\}_{n\in\mathbb{N}}$ of circuits of size $n^{\mathcal{O}(1)}$ and depth $\mathcal{O}(1)$, with majority gate (modulo $m$ gate).

Remark: A majority gate outputs 1 iff at least half of its input are 1 and a modulo $m$ gate outputs 1 iff the number of one input is 1 mod $m$.

# Uniformity

Now, for complexity classes defined as above, there is some problem. We want to discuss only computable problems, but much weak complexity class $\mathbf{AC}^0$ defined as above can compute incomputable set.
Let A$\subseteq \mathbb{N}$ be incomputable set. Then, we define a family of Boolean circuits as follows.

$$C_n = \begin{cases} 1 & \text{if } n \in \text{A} \\ 0 & \text{o.w} \end{cases}$$

This family of Boolean circuits computes imcomputable set. In order to avoid such a situation, we should give to the condition ”uniformity” a family of Boolean circuits.

# Inclusive relation of these complexity classes

**Def**

A circuits family $\{C_n\}_{n\in\mathbb{N}}$ is **DLOGTIME**-uniform if there is a **DLOGTIME** TM that on input $1^n$ outputs the description of the circuit $C_n$.

For uniform complexity classes, the next fact follows.

**Fact**

$\mathbf{AC}^0 \subsetneq \mathbf{AC}^0(2) \subsetneq \mathbf{AC}^0(3) \subsetneq \mathbf{AC}^0(6) \subseteq \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP}$

It is not known yet whether $\mathbf{AC}^0(6) = \mathbf{TC}^0 = \cdots = \mathbf{P} = \mathbf{NP}$.

Another benefit of constructing second order theories for complexity classes is that we may be able to show separation of these classes by comparing the strength of such a theory.

# Introduction to second order theories for complexity classes

# Introduction to theories for complexity classes

| | | | | | |
|---|---|---|---|---|---|
| stronger | $\mathbf{P}$ | $\Longleftrightarrow$ | $\mathbf{VP}$, $\mathbf{V}^1$ | $\Longleftrightarrow$ | eFrege |
| | $\mathbf{NC}^1$ | $\Longleftrightarrow$ | $\mathbf{VNC}^1$ | $\Longleftrightarrow$ | Frege |
| $\Uparrow$ | $\mathbf{TC}^0$ | $\Longleftrightarrow$ | $\mathbf{VTC}^0$ | $\Longleftrightarrow$ | $\mathbf{TC}^0$-Frege |
| | $\mathbf{AC}^0(m)$ | $\Longleftrightarrow$ | $\mathbf{V}^0(m)$ | $\Longleftrightarrow$ | $\mathbf{AC}^0(m)$-Frege |
| weaker | $\mathbf{AC}^0$ | $\Longleftrightarrow$ | $\mathbf{V}^0$ | $\Longleftrightarrow$ | $\mathbf{AC}^0$-Frege |
| | | Definable | | Translation | |

# Introduction to theories for complexity classes

We define a class of $\mathcal{L}$-formulas the follows, where $\mathcal{L} = [0, 1, +, \cdot, |\,|, =_1, =_2, \leq, \in]$ and $|\,|$ means length function. And, we use the abbreviation "$X(t) \equiv t \in X$", where $t$ is a number term.

Def

$\Sigma_0^B$ is the set of $\mathcal{L}$-formulas whose only quantifiers are bounded number quantifiers. $\Sigma_1^B$ is the set of $\mathcal{L}$-formulas of the form $\exists \vec{X} \leq \vec{t} \varphi(\vec{X})$, where $\varphi \in \Sigma_0^B$.

# Introduction to theories for complexity classes

**Def**

Let $\mathcal{T}$ be a theory with $\mathcal{L}' \supseteq \mathcal{L}$ and $\Phi$ be a set of $\mathcal{L}'$-formulas. A function is $\Phi$-definable in $\mathcal{T}$ if there is a $\Phi$-formula $\varphi$ such that $\varphi$ represents the function and we can prove in $\mathcal{T}$ that value of the function exists uniquely for all $\vec{x}, \vec{X}$.

In particular, we say that a function is provably total in $\mathcal{T}$ if it is $\Sigma^1_1$-definable in $\mathcal{T}$.

The bit graph $B_F$ of a string function $F$ is defined by $B_F(i, \vec{x}, \vec{Y}) \leftrightarrow F(\vec{x}, \vec{Y})(i)$. If **C** is a complexity class , then the functions class **FC** consists of all p-bounded number functions whose graphs are in **C**, together with all p-bounded string functions whose bit graphs are in **C**.

# Introduction to a theories for complexity classes

Our goal is to prove the next theorem.

**Thm (Definable theorem)**

Let **C** be a complexity class. Then a function is in **FC** iff it is provably total in **VC**. Also, a relation is in **C** iff it is $\Delta_1^1$-definable in **VC**.

The following corollary can be proved using Parikh's theorem.

**Coro**

Let **C** be a complexity class. Then a function is in **FC** iff it is $\Sigma_1^B$-definable in **VC**. Also, a relation is in **C** iff it is $\Delta_1^B$-definable in **VC**.

# Axiom of the second order theory for $\mathbf{AC}^0$

$\mathbf{V}^0$ is the theory over $\mathcal{L}$ with the follows axioms.

Def

B1 $x+1 \neq 0$

B2 $x+1=y+1 \supset x=y$

B3 $x+0=x$

B4 $x+(y+1)=(x+y)+1$

B5 $x \cdot 0=0$

B6 $x(y+1)=(x \cdot y)+x$

B7 $(x \leq y \wedge y \leq x) \supset x=y$

B8 $x \leq x+y$

B9 $0 \leq x$

B10 $x \leq y \vee y \leq x$

B11 $x \leq y \leftrightarrow x<y+1$

B12 $x \neq 0 \supset \exists y \leq x(y+1=x)$

L1 $X(y) \supset y<|X|$

L2 $y+1=|X| \supset X(y)$

SE $[|X|=|Y| \wedge \forall i<|X|(X(i) \leftrightarrow Y(i))] \supset X=Y$

$\Sigma_0^B$-COMP$\equiv \exists X \leq y \forall z<y(X(z) \leftrightarrow \varphi(z))$, where $\varphi(z)$ is any formula in $\Sigma_0^B$, and X doesn't occur free in $\varphi(z)$.

# Properties of $\mathbf{V}^0$

**Fact1**

- A relation is in $\mathbf{AC}^0$ iff it is represented by some $\Sigma_0^B$-formula.
- $\mathbf{V}^0 \nvdash \Sigma_0^B$-REPL axiom, where $\Sigma_0^B$-REPL$\equiv (\forall x \leq b \exists X \leq c\varphi(x, X)) \supset \exists Z \leq \langle b, c\rangle \forall x \leq b(|Z^{[x]}| \leq c \wedge \varphi(x, Z^{[x]}))$.

We can define binary addition $X + Y$ in $\mathbf{V}^0$ and prove the following fact.

**Fact2**

The following can prove in $\mathbf{V}^0(\emptyset, S, +)$.

- $X + \emptyset = X$
- $X + S(Y) = S(X + Y)$
- $X + Y = Y + X$
- $(X + Y) + Z = X + (Y + Z)$

# Axiom of the second order theories for complexity classes

Now, we define another second order theory for a complexity class. Such a theory will construct by using a complete ploblem for the complexity class.

Def

- For A,B$\subseteq \{0,1\}^*$, A is **AC**$^0$-reducible to B iff there is a function f$\in$ **AC**$^0$ such that the conditions "$x \in$ A$\Leftrightarrow f(x) \in$ B" follows for every $x \in \{0,1\}^*$.
- Let **C** be a complexity class. For A$\subseteq \{0,1\}^*$, A is complete for **C** over **AC**$^0$-reducibility iff A satisfies the condition "A$\in$ **C**" and "for every B$\in$ **C**, B is **AC**$^0$-reducible to A".

Remark: Since we consider a weaker complexity classes than **P**, polynomial time reducibility is meaningless.

# Axiom of the second order theories for complexity class

Now, we define two $\mathbf{AC}^0$ functions. We define the pairing function $\langle x, y\rangle = (x + y)(x + y + 1) + 2y$.

Def

- The function $\mathrm{Row}(x, Z)$, written by $Z^{[x]}$, has the bit-defining axiom, where $Z(x, i)$ means $Z(\langle x, i\rangle)$.

$$|Z^{[x]}| \leq |Z| \wedge (Z^{[x]}(i) \leftrightarrow i < |Z| \wedge Z(x, i))$$

- The function $\mathrm{Seq}(x, Z)$, written by $(Z)^x$, has the defining axiom.

$$y = (Z)^x \leftrightarrow (y < |Z| \wedge Z(x, y) \wedge \forall z < y \neg Z(x, z)) \vee (\forall z < |Z| \neg Z(x, z) \wedge y = |Z|)$$

# Axiom of the second order theory for $\mathbf{TC}^0$

**Def**

$\mathbf{VTC}^0$ is the theory over $\mathcal{L}$ with axioms of $\mathbf{V}^0$ and NUMONES$\equiv$ $\exists Y \leq 1 + \langle x, x\rangle \delta_{NUM}(x, X, Y)$, where $\delta_{NUM}(x, X, Y)$ is the following formula.

$$(Y)^0 = 0 \wedge \forall z < x(X(z) \supset (Y)^{z+1} = (Y)^z + 1) \wedge (\neg X(z) \supset (Y)^{z+1} = (Y)^z)$$

**Thm, [1]**

A function is in $\mathbf{FTC}^0$ iff it is provably total in $\mathbf{VTC}^0$ iff it is $\Sigma^B_1$-definable in $\mathbf{VTC}^0$.

# Properties of $\mathbf{VTC}^0$

We can define string multiplication in $\mathbf{VTC}^0$ and prove the facts in $\mathbf{VTC}^0$.

**Fact**

The following can prove in $\mathbf{VTC}^0(\emptyset, S, \times)$.

- Adding $n$ string
- $X \times Y = Y \times X$
- $X \times (Y + Z) = X \times Y + X \times Z$
- $X \times \emptyset = \emptyset$
- $X \times S(Y) = (X \times Y) + X$
- $(X \times Y) \times Z = X \times (Y \times Z)$

But, we don't know whether we can define the string division function $\lfloor X / Y \rfloor$ in $\mathbf{VTC}^0$.

# Example of Bounded Reverse Mathematics

# Example of Bounded Reverse Mathmatics

**Def**

$\mathbf{PHP}(a, X) \equiv \forall i \leq a \exists j < a X(i,j) \supset \exists i \leq a \exists k \leq a \exists j < a (i < k \wedge X(i,j) \wedge X(k,j))$, where $a$ means the number of holes and $X(i,j)$ holds iff pigeon $i$ gets placed in hole $j$ (for $0 \leq i \leq a,\ 0 \leq j < a$).

**Fact**

$\mathbf{VTC}^0 \vdash \mathbf{PHP}(a, X)$

We prove by contradiction. We follow the cook's proof.
Assume that $\forall x \leq a \exists y < a X(x,y) \wedge \forall x \leq a \forall z \leq a \forall y < a ((x \neq z \wedge X(x,y)) \supset \neg X(z,y))$.
Let $P = \{0, 1, \cdots, a\}$ be the set of pigeons and
$\varphi(x,y) \equiv x \leq a \wedge y < a \wedge X(x,y) \wedge \forall v < y \neg X(x,v)$.
By assumption, $\mathbf{VTC}^0 \vdash \forall x \leq a \exists! y < a \varphi(x,y) \wedge \forall x \leq a \forall z \leq a \forall y < a ((x \neq z \wedge \varphi(x,y)) \supset \neg \varphi(z,y))$.

# Proof of $\mathbf{VTC}^0 \vdash \mathbf{PHP}(a, X)$

Let $H$ be the image of $P$: $|H| \leq a \wedge (H(y) \leftrightarrow \exists x \leq a\varphi(x, y))$. We can show existence of this set by using $\Sigma_0^B$-COMP. Clealy, $\varphi$ defines a bijection between $P$ and $H$. We need numones to prove the claim "if $\varphi$ is the bijection then numones$(a + 1, P)$=numones$(a + 1, H)$" . However, $\mathbf{VTC}^0 \vdash$ numones$(a + 1, P) = a + 1$ and $\mathbf{VTC}^0 \vdash$ numones$(a + 1, H) \leq a$, contradiction.□

Fact, [Jan Krajíček, 1992]

$\mathbf{V}^0 \nvdash \mathbf{PHP}(a, X)$

# A new second order theory for $\mathbf{TC}^0$

# A complete problem for $\mathbf{TC}^0$

We define new second order theory using another complete probem for $\mathbf{TC}^0$. Fix a morphism $h : \Sigma^* \to \Delta^*$, where $\Sigma$ and $\Delta$ are finite sets of alphabets. We says $h$ is isometric if for any $\sigma$, $\tau$, $|\sigma| = |\tau| \Rightarrow |h(\sigma)| = |h(\tau)|$.

**Def**

The decision problem $\mathbf{eval}_h(b, j, v)$ asks whether $b$ is the $j$-th symbol in $h(v)$.

**Thm, [Pierre McKenzie, 2002]**

- If $h$ is isometric then $\mathbf{eval}_h$ is in $\mathbf{AC}^0$.
- If $h$ is nonisometric then $\mathbf{eval}_h$ is $\mathbf{TC}^0$- complete.

# Axiom of new second order theory for $\mathbf{TC}^0$

Let $\Sigma$ be $\{0,1\}$ and $h$ be $h(0)=0$ and $h(1)=10$.

Def

**TEVAL**$_h$ is the theory over $\mathcal{L}$ with axioms of $\mathbf{V}^0$ and EVAL$_h$ $\equiv \exists Z \leq 1+|X|^2+|X|\delta_{\mathbf{eval}_h}(X,Z)$, where $\delta_{\mathbf{eval}_h}(X,Z)$ is the following formula.

$$Z^{[0]} = \langle\,\rangle \wedge \forall z < |X|(Z^{[z+1]} = Z^{[z]}(h(X(z))))$$

We can show the theorem.

Thm

A function is in $\mathbf{FTC}^0$ iff it is provably total in **TEVAL**$_h$ iff it is $\Sigma_1^B$-definable in **TEVAL**$_h$.

# Future work

I am interested in the following things.

- Given a theorem about an algebraic equations, elementary number theory, and Galois theory, how much complicated concepts does it need to prove the theorem?
- Is the string division function $\lfloor X / Y \rfloor$ definable in $\mathbf{VTC}^0$?

Reference


1. Stephen Cook, Phuong Nguyen 『Logical foundations of proof complexity』 2010
2. Klaus-Jörn and Pierre McKenzie『On the Complexity of Free Monoid Morphisms』2002


# Thank you for your attention!