数理解析研究所講究録
976巻 1997年 27-33

COUNTING SMALL SETS IN WEAK BOUNDED ARITHMETIC

SATORU KURODA (黒田 覚)

Graduate School of Human Informatics, Nagoya University
(名古屋大学大学院人間情報学研究科)

ABSTRACT. We define a weak first order theory for AC^0 with an auxiliary axiom scheme which counts the cardinality of small sets defined by some AC^0 relation. The main result is that definable functions of this theory is exactly those which are AC^0 reducible to the binary counting function. Our tool is Herbrand-type witnessing method for universal theories.

1.INTRODUCTION

One of the main concern in the research of circuit complexity is whether the hierarchy of circuit complexity classes AC^k and NC^k is proper. The role played by AC^0 in this hierarchy is much like that played by the class of PTIME predicates in the polynomial hierarchy. But unlike the case of $PTIME$, it is already known that AC^0 is strictly included in NC^1 and this is the only separation result known so far. AC^0 is so weak a class that it cannot even compute simple arithmetical functions such as multiplication or the parity function.

Fragments of bounded arithmetic for these circuit complexity classes are defined by Clote and Takeuti, Allen, Ferreira etc. Among them, Clote and Takeuti [4] and Ferreira [5] defined theories for AC^0.

In [5], Ferreira defined a string language theory $Th-FO$, which corresponds to AC^0 using the descriptive characterization of this class by Immerman [6] and gave a model theoretical study of the relation between this theory and $I\Delta_0$.

In this note, we concentrate on the complexity theoretical study of such a class for AC^0. We first define the theory AC^0 CA similar to Ferreira's $Th-FO$, but unlike his theory our theory is based on the arithmetical language setting and the recursion theoretic characterization of AC^0 given by Clote [3]. Then we treat the counting axiom scheme (denoted by count) which states that the number of elements in any small sets can be counted. We define $\mathrm{COUNT}(\Sigma_0^b)$ to be the theory AC^0 CA extended by counting axioms for all Σ_0^b definable small sets and show that definable functions of $\mathrm{COUNT}(\Sigma_0^b)$ is precisely those computable by constant-depth polynomial size circuits which consist of NOT gate, unbounded-fanin AND and OR gates and gates which count the number of 1's in input bits.

The function

$$\mathrm{bc}(x) = \text{the number of 1's in the binary expansion of } x$$

is one of those functions which are not in AC^0 but very close to AC^0, such as multiplication or majority function. For example the class of functions which are reducible to majority function via AC^0-reduction form a new class called TC^0 which is placed between AC^0 and NC^1. Our characterization of definable functions of the theory $COUNT(\Sigma_0^b)$ is similar to TC^0 which is defined for binary counting in place of the majority function. In [2] Chandra, Stockmeyer and Vishkin proved that binary counting is equivalent to multiplication and majority under AC^0 reduction. Furthermore, S.Buss [1] proved that even the graph of multiplication is equivalent to binary counting. Hence making AC^0 closure of any one of these functions yields the class TC^0. So our result is an alternative characterization of TC^0 and we believe that our approach gives a framework for the proof theoretical study of the strength of the funcition bc and other equivalent functions comparing to AC^0 and also the study of counting axiom in view of computational complexity.

2.Definitions and Basic Results

We assume that readers are familiar with basic notions about bounded arithmetic and circuit complexity. See Clote and Takeuti [4] for the details of these notions.We consider only logtime uniform circuits, hence for example, we simply call AC^0 the class of functions computable by some logtime uniform family of unbouded fan-in, constant depth, polynomial size circuits. AC^0 has the following recursion theoretic characterization due to Clote [3].

Definition 2.1. INITIAL is the following set of functions: $Z(x) = 0$, $S(x) = x+1$, $P_i^n(x_1, \cdots, x_n) = x_i$, $s_0(x) = 2x$, $s_1(x) = 2x+1$, $|x| = \lfloor \log_2(x+1) \rfloor$, $x\#y = 2^{|x|\cdot|y|}$, $\mathrm{Bit}(x,i) = \lfloor x/2^i \rfloor \mod 2$ (the i-th bit of the binary expansion of x).

Definition 2.2. A function f is defined by *Concatenation Recursion on Notation (CRN)* from g,h_0 and h_1 if

$$\begin{aligned} f(0,\vec{x}) &= g(\vec{x}) \\ f(2n,\vec{x}) &= s_{h_0(n,\vec{x})}(f(n,\vec{x})) \quad (n>0) \\ f(2n+1,\vec{x}) &= s_{h_1(n,\vec{x})}(f(n,\vec{x})) \quad (n \geq 0), \end{aligned}$$

provided that $h_i(n,\vec{x}) \leq 1$ for $i = 0, 1$.

Proposition 2.1. *(Clote [3])* AC^0 *is the smallest class of functions containing INITIAL and closed under composition and CRN operation.*

Based on this result, we define the theory AC^0 CA as follows. Let $\mathcal{L}_{AC}$ be the language consisting of symbols for all AC^0 functions.

Definition 2.3. AC^0 CA is the $\mathcal{L}_{AC}$-theory consisting of the following axioms:

(1) defining axioms for all $f \in \mathcal{L}_{AC}$,
(2) PIND for all Σ_0^b formula,

where PIND for φ (denoted by PIND(φ)) is the following weak form of induction:

$$\varphi(0) \wedge \forall x(\varphi(\lfloor \tfrac{1}{2}x \rfloor) \rightarrow \varphi(x)) \rightarrow \forall x \varphi(x).$$

Theorem 2.1. AC^0 CA *is an universal theory.*

Theorem 2.1 was proved in [7].

The notion of essentially sharply boundedness (esb) is crucial in defining functions in our weak fragments for small size circuits. This is defined as follows:

Definition 2.4. Let T be a theory. A formula φ is esb in T if it belongs to the smallest class $\mathcal{F}$ satisfying the following conditions:

(1) every atomic formula is in $\mathcal{F}$.

(2) $\mathcal{F}$ is closed under boolean connectives and sharply bounded quantifications.

(3) If $\varphi_0, \varphi_1 \in \mathcal{F}$ and

$$T \vdash \exists x \leq s(\vec{a})\varphi_0(\vec{a}, x)$$
$$T \vdash \forall x, y \leq s(\vec{a})(\varphi_0(\vec{a}, x) \wedge \varphi_0(\vec{a}, y) \rightarrow x = y)$$

then $\exists x \leq s(\vec{a})(\varphi_0(\vec{a}, x) \wedge \varphi_1(\vec{a}, x))$ and $\forall x \leq s(\vec{a})(\varphi_0(\vec{a}, x) \rightarrow \varphi_1(\vec{a}, x))$ are in $\mathcal{F}$.

Definition 2.5. A function f is esb definable in theory T if it is defined by some esb formula provably in T.

The following holds for our base theory :

Theorem 2.2. *Let φ be esb in* AC^0 CA *then there exists a quantifier-free formula φ^* such that*

$$\mathrm{AC}^0 \mathrm{CA} \vdash \varphi \leftrightarrow \varphi^*$$

See Clote and Takeuti [4] for more discussions about esb definability.

From Theorem 2.1 and 2.2 we obtain the following witnessing theorem using Herbrand's theorem for universal theories.

Theorem 2.3. *A function f is in* AC^0 *if and only if it is esb definable in* AC^0 CA.

Our main concern in this paper is to characterize the computational strength of the following function bc in terms of proof theoretical notions.

Definition 2.6. The binary counting function bc is defined inductively as follows:

$$\begin{aligned} \mathrm{bc}(0) &= 0 \\ \mathrm{bc}(2n) &= \mathrm{bc}(n) \quad \text{if } n \neq 0 \\ \mathrm{bc}(2n+1) &= \mathrm{bc}(n) + 1 \end{aligned}$$

Definition 2.7. $\mathrm{AC}^0(\mathrm{bc})$ is the smallest class of functions containing INITIAL and bc and closed under composition and CRN operation.

Chandra, Stockmeyer and Vishkin proved that bc is as hard as computing multiplicaton, i.e.

Theorem 2.4. *(Chandra-Stockmeyer-Vishkin [2]) bc, majority and multiplication are all equivalent under* AC^0 *reduction.*

Definition 2.7. TC^0 is the set of functions computable by a family of unbouded fan-in, constant depth circuits formed from and, or, not and majority gates.

So we obtain the following characterization of TC^0 from Theorem 2.3.

Definition 2.8. Let $AC^0\,CA(\cdot)$ be the theory $AC^0\,CA$ extended by a symbol for multiplication plus its defining axioms.

Theorem 2.5. TC^0 *is the class of fucntions which are esb definable in* $AC^0\,CA(\cdot)$.

By the result of Chandra-Stockmeyer-Vishkin $AC^0(bc)$ is equal to TC^0. In the next section we give an alternative characterization of TC^0 using the function bc.

3.AC^0 AND BINARY COUNTING

As mentioned in Introduction, we present a framework for the study of binary counting function bc.

First we define the axiom to count the cardinality of small sets.

Proposition 3.1. *The followings are functions in* $AC^0\,CA$.

$$\begin{aligned}
\mathrm{Seq}(w) &\Leftrightarrow w \textit{ is a code of a sequence whose length and} \\
&\qquad \textit{the length of each elements are sharply bounded} \\
\mathrm{Len}(w) &= \textit{the length of a sequence } w \\
\beta(w,i) &= \textit{the } i\textit{-th element of } w \\
w * x &= \textit{concatenation of a sequence } w \textit{ and an element } x. \\
\mathrm{SqBd}(x,y) &= \textit{the bound for a sequence whose length is } |x| \textit{ and} \\
&\qquad \textit{each element is of length } |y|
\end{aligned}$$

Proof. See Clote and Takeuti [4].

Definition 3.1. For formula φ, the counting axiom scheme count(φ) is the following axiom scheme:

$$\begin{aligned}
\forall n \exists x < |n| \exists f < \mathrm{SqBd}(n,n)[&\mathrm{Seq}(f) \wedge \mathrm{Len}(f) = x \\
&\wedge \forall i < \mathrm{Len}(f)\varphi(\beta(f,i)) \\
&\wedge \forall y < |n|(\varphi(y) \rightarrow \exists! i < x \beta(f,i) = y) \\
&\wedge \forall i,j < x(i < j \rightarrow \beta(f,i) < \beta(f,j))]
\end{aligned}$$

$\mathrm{COUNT}(\Sigma_0^b)$ is the theory $AC^0\,CA$ extended by the counting axiom scheme for all Σ_0^b formulae.

Intuitive meaning of this axiom is that for each n there exist a number x and a sequence f such that f is a strictly increasing enumeration of the set

$$\{y < |n| : \varphi(y)\}$$

and x is the cardinality of this set.

First we show that every function in $AC^0(bc)$ is esb definable in $\mathrm{COUNT}(\Sigma_0^b)$.

Lemma 3.1. bc *is esb definable in* COUNT(Σ_0^b).

Proof. Define

$$\begin{aligned} y = \mathrm{bc}(x) \Leftrightarrow \exists f < \mathrm{SqBd}(x,x) \\ & [\mathrm{Seq}(f) \wedge \mathrm{Len}(f) = y \\ & \wedge \forall i < \mathrm{Len}(f)(\mathrm{Bit}(\beta(f,i),x) = 1) \\ & \wedge \forall z < |x|(\mathrm{Bit}(z,x) = 1 \rightarrow \exists! i < y \beta(f,i) = z) \\ & \wedge \forall i,j < y(i < j \rightarrow \beta(f,i) < \beta(f,j))] \end{aligned}$$

Denote this formula by $\exists f < \mathrm{SqBd}(x,x)\Phi(x,y,f)$. Note that this formula is strict-Σ_1^b.

Claim 1. COUNT(Σ_0^b) *proves*

$$\Phi(x,y,f) \wedge \Phi(2x,z,g) \rightarrow y = z \wedge f = g$$

and

$$\Phi(x,y,f) \wedge \Phi(2x+1,z,g) \rightarrow y+1 = z \wedge f * |x| = g$$

Proof of Claim 1. In both case it is easy to show by LIND on i that

$$\forall i < \mathrm{Len}(f)(\beta(f,i) = \beta(g,i))$$

and the claim follows easily from this fact.

By Claim 1 we have that the above definition of bc satisfies Definition 2.6. So it suffices to show that the formula $\exists f < \mathrm{SqBd}(x,x)\Phi(x,y,f)$ is esb in COUNT(Σ_0^b). This is equivalent to showing that

$$\mathrm{COUNT}(\Sigma_0^b) \vdash \forall x \exists! y \exists! f < \mathrm{SqBd}(x,x)\Phi(x,y,f).$$

The existence of y and f is an immediate consequence of count($\mathrm{Bit}(i,x) = 1$). The uniqueness

$$\Phi(x,y,f) \wedge \Phi(x,z,g) \rightarrow y = z \wedge f = g$$

is proved by PIND on x using Claim 1 as follows.

If $x = 0$ then it must be that $y = f = 0$, so y and f are uniquely determined. Suppose for induction step $\Phi(2x,y,f) \wedge \Phi(2x,z,g)$ holds. By count(Σ_0^b) there exist y' and z' such that $\Phi(x,y',f')$ and by inductive hypothesis, such y' and f' must be unique. So we have $\Phi(x,y',f') \wedge \Phi(2x,y,f)$ and $\Phi(x,y',f') \wedge \Phi(2x,z,g)$. Hence by Claim 1 $y = y' \wedge f = f'$ and $z = y' \wedge g = f'$. So $y = z \wedge f = g$ and we are done. The case for $2x+1$ is similar.

Hence we have proved that bc is esb definable in COUNT(Σ_0^b). Q.E.D.

Remark. Although it seems that the condition "f is unique" in the axiom count is redundant, we used it to show the uniqueness condition in the previous lemma. It is an open question whether this condition can be omitted from the axiom count.

Theorem 3.1. *If $f \in \mathrm{AC}^0(\mathrm{bc})$ then f is esb definable in $\mathrm{COUNT}(\Sigma^b_0)$.*

Proof. Immediate from Lemma 3.1 and the definability of AC^0 functions in AC^0 CA. Q.E.D.

By Theorem 2.4 bc is not in AC^0 and hence it is not esb definable in AC^0 CA. So we have

Corollary 3.1. *$\mathrm{COUNT}(\Sigma^b_0)$ is not conservative over AC^0 CA.*

Now our goal is to show the reverse of Theorem 3.1, namely,

Theorem 3.2. *If φ is esb in $\mathrm{COUNT}(\Sigma^b_0)$ such that*

$$\mathrm{COUNT}(\Sigma^b_0) \vdash \forall x \exists! y \phi(x, y)$$

then there exists a function $f \in \mathrm{AC}^0(\mathrm{bc})$ such that

$$\mathbb{N} \models \forall x \phi(x, f(x)).$$

As with the case for AC^0 CA, we use Herbrand's theorem for universal theories. Most of the cases are given by the proof for AC^0 CA except for the axiom $\mathrm{count}(\Sigma^b_0)$.

Definition 3.2. Let AC^0 CA(bc) be the theory AC^0 CA extended by the function symbols for bc together with its defining axioms (Definition 2.6).

Lemma 3.2. *For each $\varphi \in \Sigma^b_0$ in the language $\mathcal{L}_{\mathrm{AC}}$ there exist $\mathrm{AC}^0(\mathrm{bc})$ functions F and G such that*

$$\begin{aligned}\mathrm{AC}^0\ \mathrm{CA}(\mathrm{bc}) \vdash \forall n[&F(n) < |n| \wedge G(n) < \mathrm{SqBd}(n, n)\\ &\wedge \mathrm{Seq}(G(n)) \wedge \mathrm{Len}(G(n)) = F(n)\\ &\wedge \forall i < \mathrm{Len}(G(n))\varphi(\beta(G(n), i))\\ &\wedge \forall y < |n|(\varphi(y) \to \exists! i < F(n)\beta(G(n), i) = y)\\ &\wedge \forall i, j < F(n)(i < j \to \beta(G(n), i) < \beta(G(n), j))]\end{aligned}$$

holds.

Proof. Let $\varphi \in \Sigma^b_0$. First let B_φ be the function defined by CRN as follows:

$$B_\varphi(0) = 0$$

$$B_\varphi(s_i(n)) = \begin{cases} s_0(B_\varphi(n)) & \text{if } \varphi(n) \\ s_1(B_\varphi(n)) & \text{if } \neg\varphi(n) \end{cases}$$

for $i = 0, 1$. Then B_φ satisfies

$$\forall i < |n|[\mathrm{Bit}(i, B_\varphi(n)) \leftrightarrow \varphi(i)].$$

So let $F(n) = \mathrm{bc}(B_\varphi(n))$. Then clearly $F \in \mathrm{AC}^0(\mathrm{bc})$. To define G, let C be the function computing the i-th $x < n$ that satisfies φ. This function is defined as

$$C(i, n) = \mu x \leq |n|(F(x) \geq i).$$

Since sharply bounded μ-operator is AC^0 computable, $C \in \mathrm{AC}^0(\mathrm{bc})$. Now let

$$G(n) = \langle C(1, n), C(2, n) \ldots, C(F(n), n)\rangle.$$

As the code of short sequence is computable by some AC^0 circuit, F and G are in $\mathrm{AC}^0(\mathrm{bc})$. And it is easy to check that these functions satisfy the desired condition. Q.E.D.

Corollary 3.2. $\mathrm{AC}^0\,\mathrm{CA}$ *proves all consequences of* $\mathrm{COUNT}(\Sigma_0^b)$.

Proof of Theorem 3.2. Let φ be an esb formula which satisfies the condition. Then by Corollary 3.2 it is also esb in $\mathrm{AC}^0\,\mathrm{CA}(\mathrm{bc})$. As $\mathrm{AC}^0\,\mathrm{CA}(\mathrm{bc})$ is an universal theory, it is easy to show using Herbrand's theorem that φ is provably equivalent to some quantifier-free formula ψ. So we have

$$\mathrm{AC}^0\,\mathrm{CA}(\mathrm{bc}) \vdash \forall x \exists y \psi(x, y).$$

Hence again by Herbrand's theorem there exists a function $f \in \mathrm{AC}^0(\mathrm{bc})$ such that

$$\mathbb{N} \models \forall x \psi(x, f(x)).$$

This implies the consequence of the theorem. Q.E.D.

References

[1] S.Buss, *The Graph of Multiplication is Equivalent to Counting*, Information Processing Letters **14** (1992), 199–201.

[2] A.K.Chandra,L.Stockmeyer and U.Vishkin, *Constant depth reducibility*, SIAM Journal on Computing, **13** (1984), 423–439.

[3] P.Clote, *Sequential, Machine independent characterizations of the parallel complexity classes* ALOGTIME, AC^k, NC^k *and* NC., Feasible Mathematics (1990), Birkhaüser, 47–96.

[4] P.Clote and G.Takeuti, *Feasible Mathematics II*, Birkhaüser, 1995, pp. 154–218.

[5] F.Ferreira, *On End-Extensions of Models of* $\neg\exp$, Mathematcal Logic Quarterly **42** (1996), 1–18.

[6] N.Immerman, *Descriptive and computational complexity*, Computational Complexity Theory, AMS Short Course Lecture Notes **38** (1989), 75–91.

[7] S.Kuroda, *On a theory for* AC^0 *and the strength of induction scheme, submitted.*