

A Bounded Arithmetic Theory for Constant Depth Threshold Circuits

Jan Johannsen

IMMD 1, Universität Erlangen-Nürnberg, Germany
email: johannsen@informatik.uni-erlangen.de

Abstract. We define an extension \bar{R}_2^0 of the bounded arithmetic theory R_2^0 and show that the class of functions Σ_1^b -definable in \bar{R}_2^0 coincides with the computational complexity class TC^0 of functions computable by polynomial size, constant depth threshold circuits.

1 Introduction

The theories S_2^i , for $i \in \mathbb{N}$, of Bounded Arithmetic were introduced by Buss [3]. The language of these theories is the language of Peano Arithmetic extended by symbols for the functions $\lfloor \frac{1}{2}x \rfloor$, $|x| := \lceil \log_2(x+1) \rceil$ and $x \# y := 2^{\lfloor x \rfloor \cdot |y|}$. A quantifier of the form $\forall x \leq t$, $\exists x \leq t$ with x not occurring in t is called a *bounded quantifier*. Furthermore, a quantifier of the form $\forall x \leq |t|$, $\exists x \leq |t|$ is called *sharply bounded*. A formula is called (sharply) bounded if all quantifiers in it are (sharply) bounded.

The class of bounded formulae is divided into an hierarchy analogous to the arithmetical hierarchy: The class of sharply bounded formulae is denoted Σ_0^b or Π_0^b . For $i \in \mathbb{N}$, Σ_{i+1}^b (resp. Π_{i+1}^b) is the least class containing Π_i^b (resp. Σ_i^b) and closed under conjunction, disjunction, sharply bounded quantification and bounded existential (resp. universal) quantification.

Now the theory S_2^i is defined by a finite set *BASIC* of quantifier-free axioms plus the scheme of *polynomial induction*

$$A(0) \wedge \forall x (A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x)$$

for every Σ_i^b -formula $A(x)$ (Σ_i^b -*PIND*).

For a class of formulae Γ , a number-theoretic function f is said to be Γ -definable in a theory T if there is a formula $A(\bar{x}, y) \in \Gamma$, describing the graph of f in the standard model, and a term $t(\bar{x})$, such that T proves

$$\begin{aligned} & \forall \bar{x} \exists y \leq t(\bar{x}) A(\bar{x}, y) \\ & \forall \bar{x}, y_1, y_2 A(\bar{x}, y_1) \wedge A(\bar{x}, y_2) \rightarrow y_1 = y_2 \end{aligned}$$

The main result of [3] relates the theories S_2^i to the Polynomial Time Hierarchy *PH* of Computational Complexity Theory (cf. [9]):

The class of functions that are Σ_{i+1}^b -definable in S_2^{i+1} coincides with $FP^{\Sigma_i^P}$, the class of functions computable in polynomial time with an oracle from the i th level of the PH.

In particular, the functions Σ_1^b -definable in S_2^1 are precisely those computable in polynomial time.

The theories R_2^i were defined in various disguises by several authors [1, 10, 5]. Their language is the same as that of S_2^i extended by additional function symbols for subtraction $-$ and $MSP(x, i) := \lfloor \frac{x}{2^i} \rfloor$. They are axiomatized by an extended set *BASIC* of quantifier-free axioms plus the scheme of *polynomial length induction*

$$A(0) \wedge \forall x (A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(|x|)$$

for every Σ_i^b -formula $A(x)$ (Σ_i^b -LPIND).

R_2^1 is related to the complexity class *NC*, the class of functions computable in polylogarithmic parallel time with a polynomial amount of hardware:

The Σ_1^b -definable functions of R_2^1 are exactly those in *NC*.

In [10] it was shown that R_2^0 is equivalent to S_2^0 in the extended language, which is trivially equivalent to the theory given by the *BASIC* axioms and the scheme of *length induction*

$$A(0) \wedge \forall x (A(x) \rightarrow A(Sx)) \rightarrow \forall x A(|x|)$$

for every Σ_0^b -formula $A(x)$ (Σ_0^b -LIND).

TC^0 denotes the class of functions computable by uniform polynomial size, constant depth families of threshold circuits (cf. [2]). This class can be viewed as the smallest reasonable complexity class, e.g. it is the smallest class known to contain all arithmetical operations: integer multiplication is complete for it under a very weak form of reducibility.

Let B be the set of functions containing all projections, the constant 0, $s_0(x) := 2x$, $s_1(x) := 2x+1$, $Bit(x, i)$ giving the value of the i th bit in the binary representation of x , $\#$ and multiplication. The class TC^0 was characterized in [6] as the smallest class of functions that contains the initial functions in B and is closed under composition and the operation of *concatenation recursion on notation* (CRN), where a function f is defined by CRN from g and h_0, h_1 if

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, s_0(y)) &= 2 \cdot f(\bar{x}, y) + h_0(\bar{x}, y) \quad \text{for } y > 0 \\ f(\bar{x}, s_1(y)) &= 2 \cdot f(\bar{x}, y) + h_1(\bar{x}, y) \end{aligned}$$

provided that $h_i(\bar{x}, y) \leq 1$ for all \bar{x}, y and $i = 0, 1$. It follows from this characterization by methods from [4] that the characteristic function of any predicate defined by a Σ_0^b -formula in the language of R_2^0 is in TC^0 , and that TC^0 is

closed under *sharply bounded minimization*, i.e. if $g \in TC^0$, then f defined by $f(x) := \mu i \leq |x| g(i) = 0$ is also in TC^0 .

We shall define an extension \bar{R}_2^0 of R_2^0 the Σ_1^b -definable functions of which are exactly the functions in TC^0 . In [6], an arithmetical theory TTC^0 is presented that also characterizes TC^0 . We shall compare our work to this in the final section of the paper.

2 Definition of \bar{R}_2^0

Before the theory \bar{R}_2^0 can be defined, we have to develop R_2^0 a little. To be able to talk about the bits of a number, we first define $Mod2(x) := x \dot{-} 2 \cdot \lfloor \frac{1}{2}x \rfloor$ and then $Bit(x, i) := Mod2(MSP(x, i))$. In R_2^0 , a number is uniquely determined by its bits, as the extensionality axiom

$$|a| = |b| \wedge \forall i < |a| (Bit(a, i) = Bit(b, i)) \rightarrow a = b$$

can be proved in R_2^0 (see [7] for a proof).

We shall need the possibility to define a number by specifying its bits. So for a class of formulae Γ , let the Γ -comprehension scheme be the axiom scheme

$$\exists y < 2^{|t|} \forall i < |t| (Bit(y, i) = 1 \leftrightarrow A(i))$$

for every formula $A(i) \in \Gamma$.

Next we need the possibility of coding pairs and short sequences. The coding used is based on the one presented in [5], but we need a refined analysis to show its accessibility in R_2^0 .

First let $\bar{sg}(x) := 1 \dot{-} x$, and then $[x \leq y] := \bar{sg}(x \dot{-} y)$. Obviously, $[x \leq y] = 1$ iff $x \leq y$ and $[x \leq y] = 0$ else. Further let $[x < y] := [Sx \leq y]$, and then define

$$\max(x, y) := [x \leq y] \cdot y + [y < x] \cdot x .$$

Let now $x \frown y := x \cdot 2^{|y|} + y$, then we define

$$\langle x, y \rangle := (2^{|\max(x, y)|} + x) \frown (2^{|\max(x, y)|} + y) .$$

We go on to define $DMSB(x) := x \dot{-} 2^{\lfloor \frac{1}{2}x \rfloor}$, $front(x) := MSP(x, \lfloor \frac{1}{2}|x| \rfloor)$ and $back(x) := x \dot{-} front(x) \cdot 2^{|front(x)|}$, and finally

$$(x)_1 := DMSB(front(x)) \quad \text{and} \quad (x)_2 := DMSB(back(x)) .$$

Using extensionality, one can prove in R_2^0 that $(\langle x, y \rangle)_1 = x$ and $(\langle x, y \rangle)_2 = y$, hence these functions form a pairing system. The pairing function is not surjective, but its range can be described by

$$pair(x) := x > 2 \wedge Mod2(|x|) = 0 \wedge Bit(x, \lfloor \frac{1}{2}|x| \rfloor \dot{-} 1) = 1 .$$

Inductively we can define $(x)_i^{(2)} := (x)_i$ for $i = 1, 2$, and for $n \geq 2$ and $j \leq n$

$$\begin{aligned}\langle x_1, \dots, x_n, x_{n+1} \rangle &:= \langle \langle x_1, \dots, x_n \rangle, x_{n+1} \rangle \\ (x)_j^{(n+1)} &:= ((x)_1)_j^{(n)} \\ (x)_{n+1}^{(n+1)} &:= (x)_2\end{aligned}$$

Note that all the functions defined up to now are *terms* in the language of R_2^0 . Furthermore, they are all in TC^0 , since the function symbols in the language represent functions in TC^0 .

We define a restricted form of division for small numbers by the formula

$$z = \text{LenDiv}(x, y) :\leftrightarrow (y = 0 \wedge z = 0) \vee (y > 0 \wedge z \cdot y \leq |x| \wedge (Sz) \cdot y > |x|),$$

then in R_2^0 we can prove $\forall x, y \exists z \leq |x| z = \text{LenDiv}(x, y)$ as follows: Consider the following instance of $\Sigma_0^b\text{-LIND}$:

$$b \cdot 0 < S|a| \wedge \forall x (b \cdot x < S|a| \rightarrow b \cdot Sx < S|a|) \rightarrow \forall x b \cdot |x| < S|a|$$

Since $b > 0 \rightarrow \neg \forall x b \cdot |x| < S|a|$ is provable, and $b \cdot 0 \geq S|a|$ can be refuted, we get from the contrapositive of the above

$$b > 0 \rightarrow \exists x (b \cdot x \leq |a| \wedge b \cdot Sx > |a|)$$

from which the claim follows easily. The uniqueness of a z with $z = \text{LenDiv}(x, y)$ is also easily proved in R_2^0 .

Now the formula $z = \text{LenDiv}(x, y)$ is Σ_0^b , and z is always bounded by $|x|$, hence we can extend the language by a function symbol for LenDiv such that any sharply bounded formula in the extended language is equivalent to a Σ_0^b -formula in the original language.

Let $\text{LenMod}(x, y) := |x| \dot{-} y \cdot \text{LenDiv}(x, y)$. For readability, we write $\lfloor \frac{|x|}{y} \rfloor$ for $\text{LenDiv}(x, y)$ and $|x| \bmod y$ for $\text{LenMod}(x, y)$. Let furthermore $\text{LSP}'(x, y) := x \dot{-} \text{MSP}(x, |y|) \cdot 2^{|y|}$; we also write $\text{LSP}(x, |y|)$ for this, where $\text{LSP}(x, i)$ is intended to be the number consisting of the rightmost i bits of x , i.e. $x \bmod 2^i$. Now we define a coding for sequences of numbers of length less than $|a|$ by

$$\text{Seq}_a(w) :\leftrightarrow |w| \bmod |a| = 0 \wedge \forall i < \lfloor \frac{|w|}{|a|} \rfloor \text{Bit}(w, (i+1) \cdot |a|) = 1$$

$$\text{Len}_a(w) := \lfloor \frac{|w|}{|a|} \rfloor$$

$$\beta_a(w, i) := \text{DMSB}(\text{LSP}(\text{MSP}(w, (i \dot{-} 1) \cdot |a|), |a|))$$

Note that $\beta_a(w, i)$ is a term, and $\text{Seq}_a(w)$ as well as any sharply bounded formula containing Len_a are equivalent to a Σ_0^b -formula. Finally we define

$$\text{Seq}(w) :\leftrightarrow \text{pair}(w) \wedge \text{Seq}_{(w)_1}((w)_2)$$

$$\text{Len}(w) := \text{Len}_{(w)_1}((w)_2)$$

$$\beta(w, i) := \beta_{(w)_1}((w)_2, i)$$

The remarks above concerning β_a , Seq_a and Len_a also apply to β , Seq and Len . Finally we need a term $SqBd(x, y)$ such that a sequence of length $|x|$ all of whose entries are bounded by y has a code less than $SqBd(x, y)$. For this we can set $SqBd(x, y) := 4(x\#2y)^2$.

By using sharply bounded minimization, one sees that the functions $LenDiv$ and $LenMod$, and hence also the sequence coding operations, are in TC^0 .

Now for a class of formulae Γ , the Γ -replacement axiom scheme is

$$\forall x \leq |s| \exists y \leq t(x) A(x, y) \rightarrow \exists w < SqBd(2s, t(|s|)) [Seq(w) \wedge \wedge Len(w) = |s| + 1 \wedge \forall x \leq |s| \beta(w, Sx) \leq t(x) \wedge A(x, \beta(w, Sx))] ,$$

for every formula $A(x, y) \in \Gamma$.

Finally, the theory \bar{R}_2^0 is defined as R_2^0 extended by the schemes of Σ_0^b -comprehension and Σ_0^b -replacement. A result in [7] shows that this extension is proper.

3 Definability of TC^0 -functions

For every Σ_1^b -formula $A(\bar{a})$ we define a formula $WITNESS_A(w, \bar{a})$ (to be read as “ w witnesses $A(\bar{a})$ ”) inductively as follows: If $A(\bar{a})$ is a Σ_0^b -formula, then

$$WITNESS_A(w, \bar{a}) := A(\bar{a}).$$

If $A(\bar{a}) \equiv B(\bar{a}) \circ C(\bar{a})$ for $\circ \in \{ \wedge, \vee \}$, then

$$WITNESS_A(w, \bar{a}) := WITNESS_B((w)_1, \bar{a}) \circ WITNESS_C((w)_2, \bar{a}).$$

If $A(\bar{a}) \equiv \exists x \leq t(\bar{a}) B(\bar{a}, x)$ and $A(\bar{a})$ is not a Σ_0^b -formula, then

$$WITNESS_A(w, \bar{a}) := (w)_2 \leq t(\bar{a}) \wedge WITNESS_B((w)_1, \bar{a}, (w)_2).$$

If $A(\bar{a}) \equiv \forall x \leq |s(\bar{a})| B(\bar{a}, x)$ and $A(\bar{a})$ is not a Σ_0^b -formula, then

$$WITNESS_A(w, \bar{a}) := Seq(w) \wedge Len(w) = |s(\bar{a})| + 1 \wedge \wedge \forall x \leq |s(\bar{a})| WITNESS_B(\beta(w, x + 1), \bar{a}, x).$$

If $A(\bar{a}) \equiv \neg B(\bar{a})$ and $A(\bar{a})$ is not a Σ_0^b -formula, then let $A^*(\bar{a})$ be a formula logically equivalent to $A(\bar{a})$ obtained by pushing the negation side inside by de Morgan’s rules, and let

$$WITNESS_A(w, \bar{a}) := WITNESS_{A^*}(w, \bar{a}).$$

Clearly, $WITNESS_A(w, \bar{a})$ is equivalent Σ_0^b -formula for every Σ_1^b -formula $A(\bar{a})$.

Proposition 1. *For every Σ_1^b -formula $A(\bar{a})$ there is a term $t_A(\bar{a})$ such that:*

(i) $\bar{R}_2^0 \vdash WITNESS_A(w, \bar{a}) \rightarrow A(\bar{a})$

(ii) $\bar{R}_2^0 \vdash A(\bar{a}) \rightarrow \exists w \leq t_A(\bar{a}) \text{ WITNESS}_A(w, \bar{a})$

This is proved by a straightforward induction on the complexity of the formula $A(\bar{a})$. For part (ii), in the case where $A(\bar{a})$ starts with a sharply bounded universal quantifier, Σ_0^b -replacement is needed.

Proposition 2. *The Σ_1^b -replacement axioms are provable in \bar{R}_2^0 .*

Proof. By Prop. 1, every Σ_1^b -formula $A(x, y)$ is equivalent in \bar{R}_2^0 to a formula of the form $\exists z \leq u(x, y) B(x, y, z)$ for some term $u(x, y)$ and $B(x, y, z) \in \Sigma_0^b$, hence it suffices to deduce the replacement axiom for such a formula.

From the premise of the replacement axiom for this formula we can now easily conclude $\forall x \leq |s| \exists p \leq \langle t(x), u(x, t(x)) \rangle B(x, (p)_1, (p)_2)$, and an application of Σ_0^b -replacement yields

$$\begin{aligned} \exists v \leq SqBd(2s, \langle t(|s|), u(|s|, t(|s|)) \rangle) [Seq(v) \wedge Len(v) = |s| + 1 \wedge \\ \wedge \forall x \leq |s| \beta(v, Sx) \leq \langle t(x), u(x, t(x)) \rangle \wedge B(x, (\beta(v, Sx))_1, (\beta(v, Sx))_2)] . \quad (*) \end{aligned}$$

Next we need the following

Lemma 3. *For every term $t(x)$ the following is provable in \bar{R}_2^0 :*

$$\begin{aligned} \forall v Seq(v) \rightarrow \\ \exists w [Seq(w) \wedge Len(w) = Len(v) \wedge \forall i \leq Len(w) \beta(w, Si) = t(\beta(v, Si))] . \end{aligned}$$

This lemma, which is easily proved by Σ_0^b -replacement, for $t(x) = (x)_1$ applied to the v from (*) yields a sequence as required in the conclusion of the replacement axiom. \square

Now we are ready to show

Theorem 4. *Every function in TC^0 is Σ_1^b -definable in \bar{R}_2^0 .*

Proof. It is trivial that the Σ_1^b -definable functions in \bar{R}_2^0 comprise the initial functions in B and are closed under composition, hence it remains to prove that they are closed under CRN.

So let f be defined by CRN from g, h_0 and h_1 , let g and h_i be Σ_1^b -defined by the formulae $C(\bar{x}, y)$ and $B_i(\bar{x}, y, z)$ resp. and the terms $s(\bar{x})$ and $t_i(\bar{x}, y)$, for $i = 0, 1$.

First we show the existence of the sequence of those values of the functions h_i that are needed in the computation of $f(x, y)$ by CRN, i.e. we prove in \bar{R}_2^0

$$\begin{aligned} \exists w \leq SqBd(2y, m(\bar{x}, y)) Seq(w) \wedge Len(w) = |y| + 1 \wedge \\ \wedge \forall i \leq |y| [(Bit(y, i) = 0 \wedge B_0(\bar{x}, MSP(y, |y| \dot{-} i), \beta(w, i + 1))) \vee \\ \vee (Bit(y, i) = 1 \wedge B_1(\bar{x}, MSP(y, |y| \dot{-} i), \beta(w, i + 1)))] , \end{aligned}$$

where $m(\bar{x}, y) := \max(t_0(\bar{x}, y), t_1(\bar{x}, y))$. This follows by Σ_1^b -replacement from

$$\forall i < |y| \exists z \leq m(\bar{x}, y) \left[(Bit(y, i) = 0 \wedge B_0(\bar{x}, MSP(y, |y| \dot{-} i), z)) \vee \right. \\ \left. \vee (Bit(y, i) = 1 \wedge B_1(\bar{x}, MSP(y, |y| \dot{-} i), z)) \right],$$

which is easily obtained from the existence conditions in the Σ_1^b -definitions of h_0 and h_1 .

Now we show that for every sequence w and number a there is a number consisting of a concatenated with the least significant bits of the terms of w , i.e.

$$\forall a, w \text{ Seq}(w) \rightarrow \exists z \leq 1\#aw \left[|z| = |a| + Len(w) \wedge \right. \\ \wedge \forall i < |z| \left(i < Len(w) \wedge Bit(z, i) = Mod2(\beta(w, i + 1)) \right) \\ \left. \vee \left(i \geq Len(w) \wedge Bit(z, i) = Bit(a, i \dot{-} Len(w)) \right) \right]$$

which is easily deduced in \bar{R}_2^0 by use of Σ_0^b -comprehension. Setting $g(\bar{x})$ for a and the sequence from above for w yields the existence condition for a Σ_1^b -definition of f , with the bounding term $1\#s(\bar{x}) \cdot SqBd(2y, m(\bar{x}, y))$. The uniqueness is easily proved by use of extensionality. \square

4 Witnessing

The converse of Thm. 4 is proved by a witnessing argument as in [3]. For this, \bar{R}_2^0 has to be formulated in a sequent calculus with special rules for the introduction of bounded quantifiers, the *BASIC*, comprehension and replacement axioms as initial sequents and the Σ_0^b -LIND rule

$$\frac{A(b), \Gamma \Longrightarrow \Delta, A(Sb)}{A(0), \Gamma \Longrightarrow \Delta, A(|t|)}.$$

where the free variable b must not occur in the conclusion, except possibly in the term t .

Since the formulae in the initial sequents are all Σ_1^b , we can, by a standard cut elimination argument, assume that every formula appearing in the proof of a Σ_1^b -statement is in $\Sigma_1^b \cup \Pi_1^b$. Therefore we can prove the following witnessing theorem by induction on the length of a proof:

Theorem 5. *Let Γ, Δ be sequences of Σ_1^b -formulae and Π, Λ sequences of Π_1^b -formulae such that*

$$\bar{R}_2^0 \vdash \Gamma, \Pi \Longrightarrow \Delta, \Lambda =: \mathcal{S},$$

let furthermore all free variables in \mathcal{S} be among the \bar{a} . Let $G := \bigwedge \Gamma \wedge \bigwedge \neg \Lambda$ and $H := \bigvee \Delta \vee \bigvee \neg \Pi$. Then there is a function $f \in TC^0$ such that

$$\mathbb{N} \models \text{WITNESS}_G(w, \bar{a}) \rightarrow \text{WITNESS}_H(f(w, \bar{a}), \bar{a})$$

Proof. The induction base has four cases: A logical axiom $A \implies A$, where A is an atomic formula, is trivially witnessed, and likewise the initial sequents stemming from the *BASIC* axioms. A function witnessing a Σ_0^b -comprehension axiom

$$\exists y < 2^{|t|} \forall i < |t| (Bit(y, i) = 1 \leftrightarrow A(i))$$

can be defined by CRN from the characteristic function of the predicate $A(i)$, which is in TC^0 since $A(i)$ is a Σ_0^b -formula.

A witness for the left hand side of a Σ_0^b -replacement axiom

$$\forall x \leq |s| \exists y \leq t(x) A(x, y) \implies \exists w < SqBd(2s, t(|s|)) [Seq(w) \wedge \\ \wedge Len(w) = |s| + 1 \wedge \forall x \leq |s| \beta(w, Sx) \leq t(x) \wedge A(x, \beta(w, Sx))] ,$$

is a sequence of length $|s|+1$ whose i th term is a pair $\langle \ell_i, r_i \rangle$, where ℓ_i is a witness for $A(i-1, r_i)$. Similar to Lemma 3 we obtain the sequence $R := \langle r_i \rangle_{i \leq |s|+1}$. This sequence satisfies the matrix $B(w) := [\dots]$ of the right hand side of the replacement axiom, and since $B(w)$ is equivalent to a Σ_0^b -formula, this can be witnessed by any value. Thus $\langle 0, R \rangle$ witnesses $\exists w \leq SqBd(2s, t(|s|)) B(w)$.

In the induction step there is a case distinction corresponding to the last inference in the proof. In the cases of bounded quantifier inferences, we further have to distinguish whether the principal formula of the inference is Σ_0^b or not. Most of the cases are straightforward or easily adapted from existing witnessing proofs like the proof of the main theorem in [3].

The only more difficult cases are ($\forall \leq$: *right*) where the principal formula is not Σ_0^b , and *LIND*. W.l.o.g. we can assume that a ($\forall \leq$: *right*) inference is of the form

$$\frac{b \leq |t|, \Gamma \implies \Delta, A(b)}{\Gamma \implies \Delta, \forall x \leq |t| A(x)}$$

with Γ, Δ consisting of Σ_1^b -formulae. Then the induction hypothesis yields a function $f \in TC^0$ such that $f(w, b)$ witnesses $\forall \Delta \vee A(b)$ provided that w witnesses $b \leq |t| \wedge \bigwedge \Gamma$.

We need a function g such that $g(w)$ witnesses $\forall \Delta \vee \forall x \leq |t| A(x)$ whenever w witnesses $\bigwedge \Gamma$. Let now $w' := \langle 0, (w)_1^{(|\Gamma|)}, \dots, (w)_{|\Gamma|}^{(|\Gamma|)} \rangle$ and let

$$g(w) := \left\langle (f(w', 0))_1^{(|\Delta|+1)}, \dots, (f(w', 0))_{|\Delta|}^{(|\Delta|+1)}, s(w, t) \right\rangle$$

where $s(w, t)$ is a code for the sequence $\langle (f(w, i))_{|\Delta|+1}^{(|\Delta|+1)} \rangle_{i \leq |t|}$. The function s can be defined by use of CRN, and thus g is in TC^0 . Now it is easily verified that g has the desired witnessing property.

Finally we consider a *LIND*-inference of the form

$$\frac{A(b), \Gamma \implies \Delta, A(Sb)}{A(0), \Gamma \implies \Delta, A(|t|)} ,$$

with Γ, Δ as above. Since $A(b)$ is Σ_0^b , by induction there is $f \in TC^0$ such that for each w, b with w witnessing $A(b) \wedge \bigwedge \Gamma$, either $f(w, b)$ witnesses $\bigvee \Delta$ or $A(Sb)$ holds. Now define

$$g(w) := f(w, \mu y \leq |t| \text{WITNESS}_{\bigvee \Delta}(f(w, y))),$$

then for w witnessing $A(0) \wedge \bigwedge \Gamma$, either $g(w)$ witnesses $\bigvee \Delta$ and we are done, or for every $y \leq |t|$ $f(w, y)$ does not witness $\bigvee \Delta$. Since w also witnesses $A(y) \wedge \bigwedge \Gamma$, we can conclude $A(Sy)$ from this for every such y , hence we can conclude $A(|t|)$ inductively from $A(0)$ then. Since $A(|t|)$ is Σ_0^b , it is then trivially witnessed. \square

From this witnessing theorem we obtain the converse of Thm. 4:

Corollary 6. *Every function Σ_1^b -definable in \bar{R}_2^0 is in TC^0 .*

Proof. If f is Σ_1^b -definable in \bar{R}_2^0 , there is a Σ_1^b -formula $A(\bar{a}, b)$ and a term $t(\bar{a})$ such that \bar{R}_2^0 proves $\exists y \leq t(\bar{a}) A(\bar{a}, y)$. Then by Thm. 5 there is a function $g \in TC^0$ such that $g(\bar{a})$ witnesses this. But then $(g(\bar{a}))_2$ satisfies $A(\bar{a}, (g(\bar{a}))_2)$ for every \bar{a} , and hence $f(\bar{a}) = (g(\bar{a}))_2$, and thus $f \in TC^0$. \square

Together with Thm. 4 we get the characterization of the functions in TC^0 :

Theorem 7. *The Σ_1^b -definable functions in \bar{R}_2^0 are exactly those in TC^0 .*

5 Conclusion

We have characterized the class TC^0 as the Σ_1^b -definable functions in \bar{R}_2^0 . From this characterization, we can conclude things like

$$\text{If } \bar{R}_2^0 = R_2^1, \text{ then } TC^0 = NC, \text{ and } \bar{R}_2^0 = S_2^1 \text{ implies } TC^0 = FP.$$

or, viewed from a different perspective:

Under the hypothesis that $TC^0 \neq FP$ (or $TC^0 \neq NC$), S_2^1 (resp. R_2^1) is not conservative over \bar{R}_2^0 w.r.t. $\forall \Sigma_1^b$ -sentences.

In [6], a theory TTC^0 is defined that also yields a characterization of TC^0 . For the purpose of comparison, we recall the definition of TTC^0 : The language is the same as that of \bar{R}_2^0 . To state its axioms we first need a technical definition:

A formula A is called *essentially sharply bounded*, or *esb*, in a theory T , if A is in the smallest class Γ of formulae s.t.

- (i) every atomic formula is in Γ .
- (ii) Γ is closed under propositional connectives and sharply bounded quantification.
- (iii) if $A(\bar{x}, y)$ and $B(\bar{x}, y)$ are in Γ , and $\forall y, z \leq t(\bar{x}) A(\bar{x}, y) \wedge A(\bar{x}, z) \rightarrow y = z$ and $\forall \bar{x} \exists y \leq t(\bar{x}) A(\bar{x}, y)$ are provable in T , then the formulae

$$\exists y \leq t(\bar{x}) A(\bar{x}, y) \wedge B(\bar{x}, y) \quad \text{and} \quad \forall y \leq t(\bar{x}) A(\bar{x}, y) \rightarrow B(\bar{x}, y)$$

are in Γ .

Now the theory TTC^0 is given by the *BASIC* axioms, *esb-LIND* and the *esb*-comprehension scheme, i.e. TTC^0 is the least theory T that contains the basic axioms and has the property that whenever $A(x)$ is *esb* in T , then

$$A(0) \wedge \forall x (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(|x|)$$

and

$$\exists y < 2^{|t|} \forall i < |t| (Bit(y, i) = 1 \leftrightarrow A(i))$$

are axioms of T .

The theory TTC^0 characterizes TC^0 in the following way: TC^0 coincides with the class of *esb*-definable functions in TTC^0 . Compared to this characterization, the one in the present paper is, in the author's opinion, much more natural.

First, the notion of Σ_1^b -definability is a more useful one than that of *esb*-definability, since it delineates the functions in TC^0 among a probably larger class of functions (those whose graph is in *NP* vs. those whose graph is in TC^0). This might be easily remedied since it could be the case that the Σ_1^b -definable functions of (some extension of) TTC^0 also coincide with TC^0 .

But second, the theory TTC^0 itself has a quite cumbersome definition. We think that the axiomatization of a theory should be such that the set of axioms is easily decidable. This is not the case with TTC^0 : It seems that for a $\forall\Sigma_1^b$ -sentence, determining whether it is an axiom of TTC^0 is as difficult as deciding its provability in TTC^0 .

There is of course the possibility that TTC^0 is equivalent to \bar{R}_2^0 , but this seems to be unlikely, or at least difficult to prove, in view of the following fact: A crucial step in the obvious proof of equivalence would be to show that every *esb*-formula is equivalent to a Σ_0^b -formula in TTC^0 . Now the *esb*-formulae in TTC^0 describe exactly the predicates in TC^0 . But in [8] it was shown that the class of predicates definable by Σ_0^b -formulae in (a variant of) the language of R_2^0 is a proper subclass of P . Hence a proof of equivalence as above would separate TC^0 from P , and thus solve a difficult open problem in Complexity Theory.

References

1. B. Allen. Arithmetizing uniform *NC*. *Annals of Pure and Applied Logic*, 53:1–50, 1991.
2. D. A. M. Barrington, N. Immermann, and H. Straubing. On uniformity within NC^1 . *Journal of Computer and System Sciences*, 41:274–306, 1990.
3. S. R. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.
4. P. Clote. On polynomial size Frege proofs of certain combinatorial principles. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, volume 23 of *Oxford Logic Guides*, pages 162–184. Clarendon Press, Oxford, 1993.
5. P. Clote and G. Takeuti. Bounded arithmetic for *NC*, *ALogTIME*, *L* and *NL*. *Annals of Pure and Applied Logic*, 56:73–117, 1992.
6. P. Clote and G. Takeuti. First order bounded arithmetic and small boolean circuit complexity classes. In P. Clote and J. Remmel, editors, *Feasible Mathematics II*, pages 154–218. Birkhäuser, Boston, 1995.

7. J. Johannsen. A note on sharply bounded arithmetic. *Archive for Mathematical Logic*, 33:159–165, 1994.
8. S.-G. Mantzavis. Circuits in bounded arithmetic part I. *Annals of Mathematics and Artificial Intelligence*, 6:127–156, 1992.
9. L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1976.
10. G. Takeuti. *RSUV* isomorphisms. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, volume 23 of *Oxford Logic Guides*, pages 364–386. Clarendon Press, Oxford, 1993.