A Bounded Arithmetic Theory for Constant Depth Threshold Circuits*

Jan Johannsen

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

Summary. We define an extension $\bar{R}^0_2$ of the bounded arithmetic theory R^0_2 and show that the class of functions Σ^b_1-definable in $\bar{R}^0_2$ coincides with the computational complexity class TC^0 of functions computable by polynomial size, constant depth threshold circuits.

1. Introduction

The theories S^i_2, for $i \in \mathrm{N}$, 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 $x \# y := 2^{|x| \cdot |y|}$. 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^b_0 or Π^b_0. For $i \in \mathrm{N}$, Σ^b_{i+1} (resp. Π^b_{i+1}) is the least class containing Π^b_i (resp. Σ^b_i) and closed under conjunction, disjunction, sharply bounded quantification and bounded existential (resp. universal) quantification.

Now the theory S^i_2 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^b_i-formula $A(x)$ (Σ^b_i-$PIND$).

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

$$\forall \bar{x} \, \exists y \leq t(\bar{x}) \, A(\bar{x}, y)$$

$$\forall \bar{x}, y_1, y_2 \, A(\bar{x}, y_1) \wedge A(\bar{x}, y_2) \rightarrow y_1 = y_2$$

The main result of [3] relates the theories S^i_2 to the Polynomial Time Hierarchy PH of Computational Complexity Theory (cf. [9]):

* This paper is in its final form, and no version of it will be submitted for publication elsewhere

The class of functions that are Σ^b_{i+1}-definable in S^{i+1}_2 coincides with $FP^{\Sigma^P_i}$, the class of functions computable in polynomial time with an oracle from the ith level of the PH.

In particular, the functions Σ^b_1-definable in S^1_2 are precisely those computable in polynomial time.

The theories R^i_2 were defined in various disguises by several authors [1, 10, 5]. Their language is the same as that of S^i_2 extended by additional function symbols for subtraction $\dot{-}$ 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^b_i-formula $A(x)$ (Σ^b_i-$LPIND$).

R^1_2 is related to the complexity class NC, the class of functions computable in polylogarithmic parallel time with a polynomial amount of hardware:

The Σ^b_1-definable functions of R^1_2 are exactly those in NC.

In [10] it was shown that R^0_2 is equivalent to S^0_2 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^b_0-formula $A(x)$ (Σ^b_0-$LIND$).

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 ith 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

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

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

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

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

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

Note that all the functions defined up to now are *terms* in the language of R^0_2. 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

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

then in R^0_2 we can prove $\forall x, y \, \exists z \leq |x| \; z = LenDiv(x,y)$ as follows: Consider the following instance of Σ^b_0-$LIND$:

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

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 $z = LenDiv(x,y)$ is also easily proved in R^0_2.

Now the formula $z = LenDiv(x,y)$ is Σ^b_0, 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^b_0-formula in the original language.

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

$$\begin{aligned}Seq_a(w) &:\leftrightarrow |w| \mathbf{mod} |a| = 0 \wedge \forall i < \lfloor \tfrac{|w|}{|a|} \rfloor \, Bit(w, (i+1) \cdot |a|) = 1 \\ Len_a(w) &:= \lfloor \tfrac{|w|}{|a|} \rfloor \\ \beta_a(w,i) &:= DMSB(LSP(MSP(w, (i \dot{-} 1) \cdot |a|), |a|))\end{aligned}$$

Note that $\beta_a(w,i)$ is a term, and $Seq_a(w)$ as well as any sharply bounded formula containing Len_a are equivalent to a Σ^b_0-formula. Finally we define

$$\begin{aligned}Seq(w) &:\leftrightarrow pair(w) \wedge Seq_{(w)_1}((w)_2) \\ Len(w) &:= Len_{(w)_1}((w)_2) \\ \beta(w,i) &:= \beta_{(w)_1}((w)_2, i)\end{aligned}$$

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

$$\forall x \le |s|\, \exists y \le t(x)\, A(x,y) \rightarrow \exists w < SqBd(2s, t(|s|))\, \big[Seq(w) \wedge$$

$$\wedge\, Len(w) = |s| + 1 \wedge \forall x \le |s|\, \beta(w, Sx) \le t(x) \wedge A(x, \beta(w, Sx))\big] \;,$$

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

Finally, the theory $\bar{R}^0_2$ is defined as R^0_2 extended by the schemes of Σ^b_0-comprehension and Σ^b_0-replacement. A result in [7] shows that this extension is proper.

3. Definability of TC^0-functions

For every Σ^b_1-formula $A(\bar{a})$ we define a formula $\textsc{Witness}_A(w,\bar{a})$ (to be read as "w witnesses $A(\bar{a})$") inductively as follows: If $A(\bar{a})$ is a Σ^b_0-formula, then

$$\textsc{Witness}_A(w,\bar{a}) \quad :\equiv A(\bar{a}).$$

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

$$\textsc{Witness}_A(w,\bar{a}) \quad :\equiv \textsc{Witness}_B((w)_1,\bar{a}) \circ \textsc{Witness}_C((w)_2,\bar{a}).$$

If $A(\bar{a}) \equiv \exists x \le t(\bar{a})\, B(\bar{a},x)$ and $A(\bar{a})$ is not a Σ^b_0-formula, then

$$\textsc{Witness}_A(w,\bar{a}) \quad :\equiv (w)_2 \le t(\bar{a}) \wedge \textsc{Witness}_B((w)_1,\bar{a},(w)_2).$$

If $A(\bar{a}) \equiv \forall x \le |s(\bar{a})|\, B(\bar{a},x)$ and $A(\bar{a})$ is not a Σ^b_0-formula, then

$$\begin{aligned}\textsc{Witness}_A(w,\bar{a}) \quad :\equiv\; & Seq(w) \wedge Len(w) = |s(\bar{a})| + 1 \wedge \\ & \wedge \forall x \le |s(\bar{a})|\, \textsc{Witness}_B(\beta(w,x+1),\bar{a},x).\end{aligned}$$

If $A(\bar{a}) \equiv \neg B(\bar{a})$ and $A(\bar{a})$ is not a Σ^b_0-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

$$\textsc{Witness}_A(w,\bar{a}) \quad :\equiv \textsc{Witness}_{A^*}(w,\bar{a}).$$

Clearly, $\textsc{Witness}_A(w,\bar{a})$ is equivalent Σ^b_0-formula for every Σ^b_1-formula $A(\bar{a})$.

Proposition 3.1. *For every Σ^b_1-formula $A(\bar{a})$ there is a term $t_A(\bar{a})$ such that:*

1. $\bar{R}^0_2 \vdash \text{WITNESS}_A(w,\bar{a}) \to A(\bar{a})$
2. $\bar{R}^0_2 \vdash A(\bar{a}) \to \exists w \le t_A(\bar{a})\ \text{WITNESS}_A(w,\bar{a})$

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^b_0-replacement is needed.

Proposition 3.2. *The Σ^b_1-replacement axioms are provable in $\bar{R}^0_2$.*

Proof. By Prop. 3.1, every Σ^b_1-formula $A(x,y)$ is equivalent in $\bar{R}^0_2$ to a formula of the form $\exists z \le u(x,y)\ B(x,y,z)$ for some term $u(x,y)$ and $B(x,y,z) \in \Sigma^b_0$, 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 $\forall x \le |s|\ \exists p \le \langle t(x), u(x,t(x))\rangle\ B(x,(p)_1,(p)_2)$, and an application of Σ^b_0-replacement yields

$$(*) \exists v \le SqBd(2s, \langle t(|s|), u(|s|, t(|s|))\rangle)\ \big[Seq(v) \wedge Len(v) = |s| + 1 \wedge$$

$$\wedge\ \forall x \le |s|\ \beta(v,Sx) \le \langle t(x), u(x,t(x))\rangle \wedge B(x, (\beta(v,Sx))_1, (\beta(v,Sx))_2)\big]\ .$$

Next we need the following

Lemma 3.1. *For every term $t(x)$ the following is provable in $\bar{R}^0_2$:*

$$\forall v\ Seq(v) \to$$

$$\exists w\ \big[Seq(w) \wedge Len(w) = Len(v) \wedge \forall i \le Len(w)\ \beta(w,Si) = t(\beta(v,Si))\big]\ .$$

This lemma, which is easily proved by Σ^b_0-replacement, for $t(x) = (x)_1$ applied to the v from $(*)$ yields a sequence as required in the conclusion of the replacement axiom. □

Now we are ready to show

Theorem 3.1. *Every function in TC^0 is Σ^b_1-definable in $\bar{R}^0_2$.*

Proof. It is trivial that the Σ^b_1-definable functions in $\bar{R}^0_2$ 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^b_1-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 $\bar{R}^0_2$

$$\exists w \le SqBd(2y, m(\bar{x},y))\ Seq(w) \wedge Len(w) = |y| + 1 \wedge$$

$$\wedge\ \forall i \le |y|\ \big[\big(Bit(y,i) = 0 \wedge B_0(\bar{x}, MSP(y, |y| \dot{-} i), \beta(w, i+1))\big) \vee$$

$$\vee\ \big(Bit(y,i) = 1 \wedge B_1(\bar{x}, MSP(y, |y| \dot{-} i), \beta(w, i+1))\big)\big]\ ,$$

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

$$\begin{aligned} \forall i < |y|\, \exists z \leq m(\bar{x},y)\, [\ & \big(Bit(y,i) = 0 \wedge B_0(\bar{x}, MSP(y, |y| \dot{-} i), z)\big) \vee \\ \vee\ & \big(Bit(y,i) = 1 \wedge B_1(\bar{x}, MSP(y, |y| \dot{-} i), z)\big)\,]\,, \end{aligned}$$

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.

$$\begin{aligned} \forall a, w\ Seq(w) \rightarrow\ & \exists z \leq 1\#aw\, \big[\,|z| = |a| + Len(w) \wedge \\ \wedge\, \forall i < |z|\ & \big(i < Len(w) \wedge Bit(z,i) = Mod2(\beta(w, i+1))\big) \\ \vee\ & \big(i \geq Len(w) \wedge Bit(z,i) = Bit(a, i \dot{-} Len(w))\big)\,\big] \end{aligned}$$

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. □

4. Witnessing

The converse of Thm. 3.1 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 4.1. *Let Γ, Δ be sequences of Σ_1^b-formulae and Π, Λ sequences of Π_1^b-formulae such that*

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

let furthermore all free variables in S be among the $\bar{a}$. Let $G :\equiv \bigwedge \Gamma \wedge \bigwedge \neg\Lambda$ and $H :\equiv \bigvee \Delta \vee \bigvee \neg\Pi$. 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 $A \Longrightarrow A$, 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

$$\forall x \leq |s|\, \exists y \leq t(x)\, A(x,y) \Longrightarrow \exists w < SqBd(2s, t(|s|))\, \big[Seq(w) \wedge$$

$$\wedge\, Len(w) = |s| + 1 \wedge \forall x \leq |s|\, \beta(w, Sx) \leq t(x) \wedge A(x, \beta(w, Sx))\big]\ ,$$

is a sequence of length $|s| + 1$ whose ith 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 3.1 we obtain the sequence $R := \langle r_i \rangle_{i \leq |s|+1}$. This sequence satisfies the matrix $B(w) := [\ldots]$ 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

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

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 $\bigvee \Delta \vee A(b)$ provided that w witnesses $b \leq |t| \wedge \bigwedge \Gamma$.

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

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

where $s(w,t)$ is a code for the sequence $\langle \big(f(w,i)\big)_{|\Delta|+1}^{(|\Delta|+1)} \rangle_{i \leq |t|}$. 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

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

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. □

From this witnessing theorem we obtain the converse of Thm. 3.1:

Corollary 4.1. *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. 4.1 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 $f \in TC^0$. □

Together with Thm. 3.1 we get the characterization of the functions in TC^0:

Theorem 4.2. *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

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

1. every atomic formula is in Γ.
2. Γ is closed under propositional connectives and sharply bounded quantification.

3. 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. Mantzivis. 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.