

On the Δ_1^b -Bit-Comprehension Rule

Jan Johannsen^{1,*} and Chris Pollett²

¹ Dept. of Mathematics
U.C. San Diego,
La Jolla, CA, USA

johannsn@math.ucsd.edu
² Dept. of Mathematics and Computer Science
Clark University
Worcester, MA, USA
cpollett@aleph0.clark.edu

Summary. The theory Δ_1^b -CR of Bounded Arithmetic axiomatized by the Δ_1^b -bit-comprehension rule is defined and shown to be strongly related to the complexity class TC^0 . The Σ_1^b -definable functions of Δ_1^b -CR are those in uniform TC^0 , and the Σ_2^b -definable functions are computable by counterexample computations using TC^0 -functions. The latter is used to show that a collapse of stronger theories to Δ_1^b -CR implies that NP is contained in non-uniform TC^0 .

1 Introduction

The Δ_1^b -bit-comprehension rule roughly states the following: Given a length n and a predicate $A(x)$ that has been proven to be Δ_1^b , i.e., equivalent to both an NP -(Σ_1^b -) and a co - NP -(Π_1^b -) predicate, there is a number w of length n such that for every $i < n$, the i th bit of w is set if and only if $A(i)$ holds. One can think of w as coding the set of small i such that $A(i)$ holds.

We consider the theory of Bounded Arithmetic Δ_1^b -CR that has this rule as its main axiom. This theory is related to the computational complexity class TC^0 of functions computable by constant-depth threshold circuits. We show that the theory C_2^0 of [9], whose Σ_1^b -definable functions are TC^0 , is $\forall\Sigma_1^b$ -conservative over Δ_1^b -CR.

Theories of Bounded Arithmetic that correspond to the complexity class TC^0 have been described earlier by the authors [9, 8] as well as by Clote and Takeuti [7]. So why do we come up with yet another one? We think there are two reasons that make Δ_1^b -CR more interesting than the previous theories for TC^0 .

First, one can argue that it is the weakest natural theory whose Σ_1^b -definable functions are TC^0 , as the closure of the Σ_1^b -definable functions under concatenation recursion on notation (CRN) is essentially the same as Δ_1^b -comprehension.

Second, we will show that Δ_1^b -CR has a tighter connection to TC^0 than the previously considered theories: The Σ_2^b -theorems of Δ_1^b -CR can be witnessed by counterexample computations (a concept introduced by [13, 11] that we will define

* Supported by DFG grant No. Jo 291/1-1.

below) where the Student has the computational capabilities of TC^0 . Similar to the results of [12], this will allow us to show that a collapse of stronger theories, S_2^1 or R_2^1 , to \mathcal{A}_1^b -CR implies that every NP-predicate can be decided by non-uniform TC^0 -circuits.

2 Uniform and Non-Uniform TC^0

A *threshold circuit* is a circuit built up from boolean variables and their negations by threshold gates of the form $T_k(x_1, \dots, x_m)$, where the boolean function T_k is defined by

$$T_k(x_1, \dots, x_m) := \begin{cases} 1 & \text{if } \#\{i; x_i = 1\} \geq k \\ 0 & \text{otherwise} \end{cases} .$$

If the variables in the circuit are x_1, \dots, x_n , then it computes a boolean function $\{0, 1\}^n \rightarrow \{0, 1\}$. More generally, we can let it compute a function $\{0, 1\}^n \rightarrow \{0, 1\}^m$ by allowing several outputs.

A boolean function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is computed by a circuit family $\langle C_n; n \in \mathbb{N} \rangle$ if for each n , C_n computes $f|_{\{0,1\}^n}$. The non-uniform class TC^0 is defined as the class of functions computable by a family of threshold circuits of polynomial size and constant depth, i.e., there are a polynomial $p(n)$ and a constant d such that for all n , $size(C_n) \leq p(n)$ and $depth(C_n) \leq d$.

Non-uniform circuit families can compute functions that are not computable. For example, let K be an undecidable set of natural numbers, then the characteristic function of $\{1^k; k \in K\}$ is computable by a trivial circuit family of linear size and depth 1. To overcome this sometimes unwanted feature, circuit families are required to satisfy certain uniformity conditions. For TC^0 -circuits, the most suitable uniformity notion is DLogTime-uniformity, see [3] for the somewhat involved definition.

DLogTime-uniform TC^0 is a fairly natural complexity class: it is characterized by first-order logic with majority quantifiers on ordered finite models [3] in Descriptive Complexity Theory, or by acceptance in time $O(\log(n))$ on so-called Threshold Turing Machines [2], or by the machine-independent characterization below, which is most convenient for our purposes. Whenever we speak of TC^0 in the following without further qualification, we mean DLogTime-uniform TC^0 .

For a complexity class C , the class $C/poly$ is defined as follows: A predicate $A(x)$ is in $C/poly$ if there is a predicate $B(x, y) \in C$ and a polynomially bounded *advice function*, i.e., a function f such that $|f(n)| \leq p(n)$ for some polynomial $p(n)$, and for which it holds that

$$\forall x A(x) \leftrightarrow B(x, f(|x|)) .$$

Advice functions are used to inject non-uniformity into uniform complexity classes. For example, it is well-known that $P/poly$ is equal to the class of predicates

computable by non-uniform circuits of polynomial size. Analogously we have the following:

Proposition 1. $TC^0/poly$ is the same as non-uniform TC^0 .

Proof (Sketch). For each d , there is an interpreter in TC^0 that takes as inputs a threshold circuit C of depth d and an input a to C , and outputs the value computed by C on input a . Let a non-uniform threshold circuit family $\langle C_n; n \in \mathbb{N} \rangle$ of depth d and size $O(p(n))$ computing $A(x)$ be given. Then $A(x) \in TC^0/poly$ is seen as follows: $B(x, y)$ is the interpreter for threshold circuits of depth d , and the advice $f(n)$ is an encoding of the circuit C_n . Obviously $B(x, f(|x|))$ is equivalent to $A(x)$.

On the other hand, let $A(x) \in TC^0/poly$ given by predicate $B(x, y)$ and advice function f . Then a circuit computing $A(x)$ for inputs x of length n is constructed from the circuit computing $B(x, y)$ for inputs x of length n and y of length $|f(n)|$, by plugging into y constant subcircuits computing the bits of $f(n)$. \square

Next we give the machine-independent characterization of TC^0 mentioned above:

Definition 1. Suppose $h_0(n, \mathbf{x}), h_1(n, \mathbf{x}) \leq 1$. A function f is defined by concatenation recursion on notation (CRN) from g, h_0 , and h_1 if

$$\begin{aligned} f(0, \mathbf{x}) &= g(\mathbf{x}) \\ f(2n, \mathbf{x}) &= 2 \cdot f(n, \mathbf{x}) + h_0(n, \mathbf{x}), \text{ provided } n \neq 0 \\ f(2n+1, \mathbf{x}) &= 2 \cdot f(n, \mathbf{x}) + h_1(n, \mathbf{x}) \end{aligned}$$

Let $i_k^n(x_1, \dots, x_n) := x_k$, $s_0(x) := 2x$, $s_1(x) = 2x + 1$, $|x| := \lceil \log_2(x+1) \rceil$, $x \# y := 2^{|x|+|y|}$ and $Bit(x, i) := \lfloor \frac{x}{2^i} \rfloor \bmod 2$. The following characterization of the number-theoretic functions in TC^0 was given in [7]:

Proposition 2. The class TC^0 is the smallest class of functions that contains $0, i_k^n, s_0, s_1$, multiplication $\cdot, \#, |x|$, Bit and which is closed under composition and CRN.

3 Theories of Bounded Arithmetic

We briefly review the necessary background on Bounded Arithmetic, for more information see [4] or [10]. The language L_2 of Bounded Arithmetic comprises the usual signature of arithmetic $0, S, +, -, \cdot, \leq$, together with function symbols for $\lfloor \frac{1}{2}x \rfloor$, $MSP(x, i) := \lfloor x/2^i \rfloor$, $|x|$ and $\#$.

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, the quantifier is called *sharply bounded* if the bounding term t is of the form $|s|$ for some term s . A formula is called (sharply) bounded if all quantifiers in it are (sharply) bounded.

We denote the class of quantifier-free formulas in L_2 by *open*. The class of sharply bounded formulas 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.

We say that a function $f(\mathbf{x})$ is Σ_i^b -definable in a theory T if there is a Σ_i^b -formula $A(\mathbf{x}, y)$ and a term $t(\mathbf{x})$ such that

$$\begin{aligned} \mathbb{N} & \models \forall \mathbf{x} A(\mathbf{x}, f(\mathbf{x})) \\ T & \vdash \forall \mathbf{x} \exists y \leq t(\mathbf{x}) A(\mathbf{x}, y) \\ T & \vdash \forall \mathbf{x}, y, z A(\mathbf{x}, y) \wedge A(\mathbf{x}, z) \rightarrow y = z . \end{aligned}$$

BASIC denotes a set of quantifier-free axioms specifying the interpretations of the function symbols of L_2 . It can most conveniently be taken as the set *BASIC* from [4] together with the axioms for *MSP* and $\dot{-}$ from [14].

For a class of formulas Φ , the axiom schema Φ -*LIND* is

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

for each $A(x) \in \Phi$, and Φ -*LLIND* is

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

for $A(x) \in \Phi$. In general, for $m \geq 1$, Φ -*L^mIND* is

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

for $A(x) \in \Phi$, where $|x|_1 := |x|$ and $|x|_{m+1} := \||x|_m|$.

The theory S_2^j is the theory axiomatized by the *BASIC* axioms and Σ_i^b -*LIND*, and R_2^j is the theory given by *BASIC* and Σ_i^b -*LLIND*.

Definition 2. Given a term $t \in L_2$ we define a monotonic L_2 -term t^* as follows: If t is constant or a variable, then $t = t^*$. If t is $f(s)$, where f is a unary function symbol, then t^* is $f(s^*)$. If t is $s_1 \circ s_2$ for \circ a binary operation other than $\dot{-}$ or *MSP*, then t^* is $s_1^* \circ s_2^*$. Lastly, if t is $s_1 \dot{-} s_2$ or *MSP*(s_1, s_2), then t^* is s_1^* .

It is easily proved in *BASIC* + *open-LIND* that t^* is monotonic, and $t \leq t^*$. The following terms will be used frequently below. Let

$$\begin{aligned} 2^{|x|} & := 1\#x \\ \text{mod}2(x) & := x \dot{-} 2 \cdot \lfloor \frac{1}{2}x \rfloor \\ \text{Bit}(x, i) & := \text{mod}2(\text{MSP}(x, i)) \\ 2^{\min(x, |y|)} & := \text{MSP}(2^{|y|}, |y| \dot{-} x) \\ \text{LSP}(x, i) & := x \dot{-} 2^{\min(i, |x|)} \cdot \text{MSP}(x, i) \\ \beta_a(w, i) & := \text{MSP}(\text{LSP}(w, Si \cdot |a|), i \cdot |a|) \end{aligned}$$

so that $LSP(x, |y|)$ returns the number consisting of the last $|y|$ bits of x , and if w codes a sequence $\langle b_1, \dots, b_\ell \rangle$ with $|b_i| \leq |a|$ for all i , then $\beta_a(w, i) = b_i$. The code for this sequence is simply the number w whose binary representation consists of a 1 followed by the binary representations of the b_i concatenated, each padded with zeroes to be of exact length $|a|$. If we set $bd(a, s) := 2(2a\#2s)$, then $bd(a, s)$ is thus a bound on the code for a sequence of length $|s|$ with each item bounded by a .

We also define a pairing operation that does not rely on an explicitly mentioned bound. Let $B = 2^{|\max(x,y)|}$. Pairs are coded as $\langle x, y \rangle := (B + y) \cdot 2B + (B + x)$. The terms $(w)_1 := \beta_{\lfloor \frac{1}{2}|w| \rfloor - 1}(0, \beta_{\lfloor \frac{1}{2}|w| \rfloor}(0, w))$ and $(w)_2 := \beta_{\lfloor \frac{1}{2}|w| \rfloor - 1}(0, \beta_{\lfloor \frac{1}{2}|w| \rfloor}(1, w))$, project out the left and right coordinates from an ordered pair. To check if w is a pair we use the formula

$$ispair(w) := Bit(w, \lfloor \frac{1}{2}|w| \rfloor - 1) = 1 \wedge 2 \cdot |\max((w)_1, (w)_2)| + 2 = |w|.$$

For a class of formulas Φ , the replacement scheme $BB\Phi$ is

$$\begin{aligned} \forall x \leq |s| \exists y \leq t(x) A(x, y) \rightarrow \\ \exists w < bd(t^*(|s|), s) \forall x \leq |s| \beta_{t^*(|s|)}(w, x) \leq t(x) \wedge A(x, \beta_{t^*(|s|)}(w, x)) \end{aligned}$$

for each $A(x, y) \in \Phi$.

The theory C_2^0 is defined as $BASIC + open-LIND + BB\Sigma_0^b$. The following theorem summarizes some relations between Σ_i^b -definability in the theories defined and computational complexity.

- Theorem 1.** – *The Σ_i^b -definable functions in S_2^i are exactly those in $FP^{\Sigma_{i-1}^p}$, for each $i \geq 1$ [4].*
- *The Σ_1^b -definable functions in R_2^1 are exactly those in NC [1, 5].*
 - *The Σ_1^b -definable functions in C_2^0 are exactly those in TC^0 [8, 9].*

The comprehension axiom for formula $A(x)$, denoted $COMP_A(a)$, is the formula

$$\exists y < 2^{|a|} \forall x < |a| (Bit(y, x) = 1 \leftrightarrow A(x)).$$

The Δ_1^b -comprehension rule, Δ_1^b-COMP , is the following inference rule

$$\frac{A(x) \leftrightarrow B(x)}{COMP_A(t)},$$

where $A(x)$ is Σ_1^b and $B(x)$ is Π_1^b , and t is an arbitrary L_2 -term. Note that this rule is different from the possibly stronger Δ_1^b -comprehension *axiom*

$$\forall x (A(x) \leftrightarrow B(x)) \rightarrow COMP_A(a),$$

thus it is essential that in a sequent calculus context, the rule must not have any side formulas.

Definition 3. Let Δ_1^b -CR be the theory axiomatized by BASIC, open-LIND and the Δ_1^b -COMP rule.

In [9], it is proved that C_2^0 proves the Δ_1^b -COMP axiom, therefore Δ_1^b -CR is a subtheory of C_2^0 . But we will show that C_2^0 is not much stronger:

Theorem 2. C_2^0 is $\forall\Sigma_1^b$ -conservative over Δ_1^b -CR.

This implies immediately:

Corollary 1. The Σ_1^b -definable functions of Δ_1^b -CR are precisely TC^0 .

Hence $S_2^1 = \Delta_1^b$ -CR implies $P = TC^0$, and $R_2^1 = \Delta_1^b$ -CR implies $NC = TC^0$. We will show that the connection between the theory Δ_1^b -CR and TC^0 is still tighter: the Σ_2^b -theorems of Δ_1^b -CR can be witnessed by a type of interactive TC^0 -computations to be defined below. This will allow us to show that the equality of Δ_1^b -CR to either of the stronger theories S_2^1 or R_2^1 implies a further collapse of complexity classes:

Theorem 3. If $S_2^1 = \Delta_1^b$ -CR or $R_2^1 = \Delta_1^b$ -CR, then NP is contained in non-uniform TC^0 .

The method could further be generalized to show that $NP \subseteq$ non-uniform TC^0 follows from Δ_1^b -CR $\vdash \Sigma_1^b$ - L^m IND for any $m > 0$.

The following further axiom schemes will be used below. The Σ_1^b -length-maximization scheme, Σ_1^b -LMAX, is the axiom

$$\exists x \leq a A(x) \rightarrow \exists x \leq a (A(x) \wedge \forall y \leq a (|y| > |x| \rightarrow \neg A(y)))$$

for every Σ_1^b -formula $A(x)$. Similarly, the Σ_1^b -double-length-maximization scheme, Σ_1^b -LLMAX, is the axiom

$$\exists x \leq a A(x) \rightarrow \exists x \leq a (A(x) \wedge \forall y \leq a (||y|| > ||x|| \rightarrow \neg A(y)))$$

for every Σ_1^b -formula $A(x)$. The following proposition is well-known.

Proposition 3. $S_2^1 \vdash \Sigma_1^b$ -LMAX and $R_2^1 \vdash \Sigma_1^b$ -LLMAX. In fact, Σ_1^b -LMAX is equivalent to Σ_1^b -LIND and Σ_1^b -LLMAX is equivalent to Σ_1^b -LLIND over BASIC + open-LIND.

4 Proof of Conservativity

The following two lemmas are well-known and easily proved by the method of [6]:

Lemma 1. The Σ_0^b -predicates are computable in TC^0 . In particular, the L_2 -base functions are in TC^0 .

Lemma 2. *Let f be a function in TC^0 . Then the function*

$$\mu j < |x| (f(j, x) = 0)$$

is also in TC^0 .

Lemma 3. $\lfloor |a|/|b| \rfloor$ *is contained in TC^0 .*

Proof. By Lemma 2 and Lemma 1 we can define

$$\lfloor |a|/|b| \rfloor := \mu n \leq |a| (|a| < (n+1)|b|).$$

Suppose $g(n, \mathbf{x}) \leq t(\mathbf{x})$ and s, t are L_2 -terms. Then a *length-sum* is a sum of the form

$$\sum_{n=0}^{\lfloor s \rfloor} g(n, \mathbf{x}) \cdot 2^{n \cdot \lfloor t^* \rfloor}.$$

Lemma 4. TC^0 *is closed under length-sums.*

Proof. Suppose we want to define the length-sum

$$f(a, x) := \sum_{n=0}^{\lfloor a \rfloor} h(n, x) 2^{n \cdot \lfloor s^*(x) \rfloor}$$

using CRN where $h(n, x) \leq s(x)$ are functions in TC^0 . We use CRN to compute the bits of f from the most significant bit to the least significant bit. The function

$$t(i, a, x) := |a| \dot{-} \lfloor |i|/|s^*(x)| \rfloor$$

allows us to determine which term in f we are computing the bits from. The function

$$p(i, x) := |s^*(x)| \dot{-} (|i| \dot{-} \lfloor |i|/|s^*(x)| \rfloor |s^*(x)|) \dot{-} 1$$

gives us the position within a term. Define the function f' by CRN in the following way:

$$\begin{aligned} f'(0, a, x) &= \text{Bit}(p(0, x), h(t(0, a, x), x)) \\ f'(2i+1, a, x) &= f'(2i, a, x) = 2f'(i, a, x) + \text{Bit}(p(i, x), h(t(i, a, x), x)). \end{aligned}$$

Then the desired $f(a, x)$ is $f'(2^{\lfloor a/|s^*(x)| + |h(|a|, x)| - 2}, a, x)$. The expression in the first component of f' is easily defined using \cdot , $\#$, and MSP . \square

Lemma 5. Δ_1^b -CR *proves the Δ_1^b -LIND axioms, and Δ_1^b -CR proves the bit-extensionality axiom:*

$$|a| = |b| \wedge \forall i < |a| (\text{Bit}(a, i) = \text{Bit}(b, i)) \rightarrow a = b.$$

Proof. If A is Δ_1^b in Δ_1^b -CR, then Δ_1^b -CR proves the *LIND* axiom for A since Δ_1^b -CR proves $COMP_A(a)$ and Δ_1^b -CR proves *LIND* on x for the formula $Bit(y, x) = 1$. The second statement is easily proved by *LIND* on x in the following Σ_0^b -formula:

$$\forall i < |a| (i \leq x \rightarrow Bit(a, i) = Bit(b, i)) \rightarrow LSP(a, x) = LSP(b, x) .$$

We are now ready to show the functions in TC^0 are Σ_1^b -definable in Δ_1^b -CR.

Theorem 4. Δ_1^b -CR can Σ_1^b -define the functions in TC^0 .

Proof. The base functions symbols are obviously Σ_1^b -definable in Δ_1^b -CR, and closure under composition is straightforward. So it suffices to show the Σ_1^b -definable functions of Δ_1^b -CR are closed under CRN.

Suppose that f is defined by CRN from $g(x)$ and $h_0(n, x), h_1(n, x)$, where g, h_0, h_1 are Σ_1^b -defined in Δ_1^b -CR. Define $t(a, x)$ to be

$$\sum_{n=0}^{|a|} cond(Bit(|a| \dot{-} n, a), h_0(n, x), h_1(n, x)) \cdot 2^n ,$$

then $f(a, x) = g(x) \cdot 2^{t(a, x)} + t(a, x)$. It suffices to show the length-sum $t(a, x)$ is Σ_1^b -definable, since then $f(a, x)$ will be by composition.

Notice $k(n, x, a) := cond(Bit(|a| \dot{-} n, a), h_0(n, x), h_1(n, x))$ is Σ_1^b -defined in Δ_1^b -CR. Let $A_k(n, a, x, y)$ be its defining formula. Given the other parameters, Δ_1^b -CR proves the value y is unique and bounded by 1. Therefore Δ_1^b -CR $\vdash A_k(n, x, a, 1) \leftrightarrow \neg A_k(n, x, a, 0)$ and $A_k(n, x, a, 1)$ is true iff $k(n, x, a) = 1$ so $k(n, x, a) = 1$ is a Δ_1^b -property in Δ_1^b -CR. We want to define the sum $\sum_{n=0}^{|a|-1} k(n, x, a) \cdot 2^n$. Δ_1^b -COMP on $k(n, x, a) = 1$ implies

$$(\exists w \leq s)(\forall n \leq |a|)(Bit(n, w) = 1 \leftrightarrow k(n, x, a) = 1) ,$$

the value w is the desired sum and it can be proven unique using extensionality. \square

Remark 1. Given two Σ_1^b -defined in Δ_1^b -CR functions f, g , the property $f(x) = g(x)$ will be Δ_1^b in Δ_1^b -CR. Using this, Δ_1^b -LIND, and extensionality it is not hard to show Δ_1^b -CR proves simple properties of both the μ -operation and length-sums. For instance, Δ_1^b -CR proves that if $h(n, x) \leq s(x)$ then

$$\beta_{|s^*(x)|}(j, \sum_{n=0}^{|a|} h(n, x) 2^{n|s^*(x)|}) = h(j, x)$$

for $j \leq |a|$.

To prove the conservativity result, we formalize the witnessing proof for C_2^0 in Δ_1^b -CR. First we define a witness bounding term and witness predicate for Σ_1^b -formulas as follows:

- If $A(\mathbf{a}) \in \Sigma_0^b$ then $t_A = 0$ and $Wit_A(w, \mathbf{a}) := A(\mathbf{a}) \wedge w = 0$.
- If $A(\mathbf{a})$ is of the form $B \circ C$ where \circ is \wedge or \vee then $t_A := 4 \cdot (2^{|\max(t_B, t_C)|})^2$ and

$$Wit_A(w, \mathbf{a}) := \text{ispair}(w) \wedge (Wit_B((w)_1, \mathbf{a}) \circ Wit_C((w)_2, \mathbf{a}))$$

- If $A(\mathbf{a})$ is of the form $\exists x \leq t B(x, \mathbf{a})$ where $B(x, \mathbf{a}) \in \Sigma_0^b$ then $t_A := t$ and

$$Wit_A(w, \mathbf{a}) := w \leq t \wedge B(w, \mathbf{a}) .$$

- If $A(\mathbf{a})$ is of the form $\exists x \leq t B(x, \mathbf{a})$ where $B(x, \mathbf{a}) \in \Sigma_1^b \setminus \Sigma_0^b$, then $t_A := 4 \cdot (2^{|\max(t, t_B)|})^2$ and

$$Wit_A(w, \mathbf{a}) := \text{ispair}(w) \wedge (w)_1 \leq t \wedge Wit_B((w)_2, (w)_1, \mathbf{a}) .$$

- If $A(\mathbf{a})$ is of the form $\forall x \leq |s| B(x, \mathbf{a})$ where $B(x, \mathbf{a}) \in \Sigma_1^b \setminus \Sigma_0^b$, then $t_A := bd(t_B^*(|s|), s)$ and

$$Wit_A(w, \mathbf{a}) := w \leq t_A \wedge \forall x \leq |s| Wit_B(\beta_{t_A}(x, w), x, \mathbf{a}) .$$

The following lemma is true for this witness predicate:

Lemma 6. *If $A(\mathbf{a}) \in \Sigma_1^b$, then:*

- (a) Wit_A is a Σ_0^b -predicate.
- (b) $\Delta_1^b\text{-CR} \vdash \exists w \leq t_A(\mathbf{a}) Wit_A(w, \mathbf{a}) \rightarrow A(\mathbf{a})$.

Proof. Part (a) follows from the definition of witness and since β and the pairing functions are defined by L_2 -terms. Part (b) is easily proved by induction on the complexity of A . \square

To prove the witnessing theorem, we formalize C_2^0 in a sequent calculus LKB that has special rules for the introduction of bounded quantifiers (see [4]). In this formalization, *open-LIND* and $BB\Sigma_0^b$ are given as inference rules, which are shown in the proof below.

Theorem 5. *Suppose*

$$C_2^0 \vdash \Gamma \Longrightarrow \Delta$$

where Γ and Δ are cedents of Σ_1^b -formulas. Let \mathbf{a} be the free variables in this sequent. Then there is a TC^0 function f which is Σ_1^b -defined in $\Delta_1^b\text{-CR}$ such that:

$$\Delta_1^b\text{-CR} \vdash Wit_{\bigwedge \Gamma}(w, \mathbf{a}) \rightarrow Wit_{\bigvee \Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

Proof. This is proved by induction on the number of sequents in a C_2^0 proof of $\Gamma \Longrightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are Σ_1^b . Most of the cases are similar to previous witnessing arguments so we only show the $(\forall : \text{right})$ case, *open-LIND* case and the $BB\Sigma_0^b$ case.

(\forall :right case) Suppose we have the inference:

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

By the induction hypothesis there is a TC^0 function g such that

$$\Delta_1^b\text{-CR} \vdash \text{Wit}_{b \leq t} \wedge \bigwedge_{\Gamma} (w, \mathbf{a}, b) \rightarrow \text{Wit}_{A \vee \bigvee_{\Delta}} (g(w, \mathbf{a}, b), \mathbf{a}, b).$$

By cut-elimination, $\forall x \leq t A(x)$ is a Σ_1^b -formula, so t must be of the form $t = |s|$. There are two cases: where A is Σ_0^b and where A is $\Sigma_1^b \setminus \Sigma_0^b$. In the first case, let y be $\mu i \leq |s| \neg A(i)$ and define f to be $g(\langle 0, w \rangle, \mathbf{a}, y)$. The 0 in the ordered pair is since $\text{Wit}_{b \leq t}(w, b) = b \leq t \wedge w = 0$. This is in TC^0 by Lemma 1 and Lemma 2 and it is not hard to show that

$$\Delta_1^b\text{-CR} \vdash \text{Wit}_{\Gamma}(w, \mathbf{a}) \rightarrow \text{Wit}_{\forall x \leq |s| A \vee \bigvee_{\Delta}} (f(w, \mathbf{a}), \mathbf{a}).$$

In the second case, since Wit_A is a Σ_0^b -formula, its characteristic function χ_{Wit_A} is in TC^0 . Let k be the function

$$k(w, \mathbf{a}) = \mu j \leq |s| [\neg \text{Wit}_A(\langle g(\langle 0, w \rangle, \mathbf{a}, j) \rangle_1, \mathbf{a}, j)].$$

Let $t' := (t_A(t))^*$ where $t_{A(x)}$ is from Lemma 6. Now define $f(w, \mathbf{a})$ from k as follows

$$f(w, \mathbf{a}) = \begin{cases} \langle \sum_{j=0}^{|s|} (g(\langle 0, w \rangle, \mathbf{a}, j))_1 \cdot 2^{j \cdot |t'|}, 0 \rangle & \text{if } k(w, \mathbf{a}) = |s| + 1 \\ \langle 0, (g(\langle 0, w \rangle, \mathbf{a}, k(w, \mathbf{a})))_2 \rangle & \text{otherwise} \end{cases},$$

then using the remark after Theorem 4

$$\Delta_1^b\text{-CR} \vdash \text{Wit}_{\Gamma}(w, \mathbf{a}) \rightarrow \text{Wit}_{\forall x \leq |s| A \vee \bigvee_{\Delta}} (f(w, \mathbf{a}), \mathbf{a}).$$

(open-LIND case) Suppose we have the inference

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

where A is an open formula and s is a term in L_2 . By the induction hypothesis there is a TC^0 function g such that

$$\Delta_1^b\text{-CR} \vdash \text{Wit}_{A(b) \wedge \bigwedge_{\Gamma}} (w, b, \mathbf{a}) \rightarrow \text{Wit}_{A(Sb) \vee \bigvee_{\Delta}} (g(w, b, \mathbf{a}), b, \mathbf{a}).$$

From our definition of the Wit predicate and Lemma 1, we know TC^0 contains the predicate $\text{Wit}_{\bigvee_{\Delta}}$. Define

$$f(w, \mathbf{a}) := g(w, (\mu y < |s|) (\neg \text{Wit}_{\bigvee_{\Delta}} (\langle g(w, y, \mathbf{a}) \rangle_2, y, \mathbf{a})), \mathbf{a}).$$

Notice $Wit_A(v, b, \mathbf{a}) := A \wedge v = 0$ as A is open, so the value of a witness to A does not depend on b . So it will witness $A(b)$ for all $b \leq |s|$. Using this, the idea is $f(w, \mathbf{a})$ runs g on the least value y less than $|s|$ that produces a witness for A . If no such value exists then it must be the case that $A(|s|)$ holds and so, as A is open, the cedent is trivially witnessed. From this it is not hard to show:

$$\Delta_1^b\text{-CR} \vdash Wit_{A(0)} \wedge \bigwedge_{\Gamma} (w, \mathbf{a}) \rightarrow Wit_{A(|s|)} \vee \bigvee_{\Delta} (f(w, \mathbf{a}), \mathbf{a}).$$

($BB\Sigma_0^b$:case) Suppose we have the inference:

$$\frac{\Gamma \implies \forall x \leq |s| \exists y \leq t A(x, y), A}{\Gamma \implies \exists v \leq bd(t^*(|s|), s) \forall x \leq |s| (\beta_{t^*(|s|)}(x, v) \leq t \wedge A(x, \beta_{t^*(|s|)}(x, v))), A}$$

where s, t are terms in L_2 and $A(x, y) \in \Sigma_0^b$. By the induction hypothesis there is a TC^0 function g such that

$$\Delta_1^b\text{-CR} \vdash Wit \bigwedge_{\Gamma} (w, \mathbf{a}, b) \rightarrow Wit_{\forall x \leq |s| \exists y \leq t A} \vee \bigvee_{\Delta} (g(w, \mathbf{a}), \mathbf{a}).$$

For this case, it suffices to notice that the predicates

$$Wit_{\forall x \leq |s| \exists y \leq t A}$$

and

$$Wit_{\exists v \leq bd(t^*(|s|), s) \forall x \leq |s| (\beta_{t^*(s(|x|))}(x, v) \leq t \wedge A)}$$

are the same. Hence, if we let $f = g$ then

$$\Delta_1^b\text{-CR} \vdash Wit \bigwedge_{\Gamma} (w, \mathbf{a}, b) \rightarrow Wit_{\exists w \leq bd(t^*, s) \forall x \leq |s| A} \vee \bigvee_{\Delta} (f(w, \mathbf{a}), \mathbf{a}).$$

This completes the cases and the proof. \square

Now Thm. 2 follows from this witnessing theorem as follows: Suppose C_2^0 proves a Σ_1^b -formula $A(x)$. Then by Theorem 5, taking Γ to be the empty cedent, $\Delta_1^b\text{-CR} \vdash Wit_A(g(x), \mathbf{x})$, where g is a TC^0 function. By Lemma 6, we have $\Delta_1^b\text{-CR} \vdash A(x)$. \square

5 Counterexample Computations with TC^0 functions

In this section we view binary relations $R(x, y)$ in TC^0 as *optimization problems*: given x , the task is to find a solution y of maximal length $|y| \leq |x|$ such that $R(x, y)$ holds. We consider a particular way of solving such optimization problems, viz. *counterexample computations* as introduced implicitly in [12] and made explicit in [13, 11].

A counterexample computation is performed by two agents: Student, who has limited computational power, and Teacher who has unlimited knowledge.


```

y := f1(a)
if length(y) ≥ 1 and R(a, y) then
  output ⟨1, (y)1⟩
  stop
fi
for j from 2 to k do
  y := fj(a, b1, . . . , bj-1)
  if length(y) ≥ j and R(a, y) then
    output ⟨j, (y)j⟩
    stop
  fi
od

```

Algorithm W. b_j is defined as $\langle w(x_1), \dots, w(x_j) \rangle$.

For a fixed length n , let $V_1 := \{x \in A : |x| = n\}$, and for each $x \in V_1$, let $w(x)$ be a canonical witness. Algorithm W below computes a pair $\langle j, w \rangle$ from an input $a = \langle x_1, \dots, x_k \rangle \in V_1^k$ such that w witnesses x_j . Since there is a sequence of witnesses $b_0 = \langle w(x_1), \dots, w(x_k) \rangle$ of length k , a length maximal b with $R(a, b)$ has to be of length k . By our assumption of $\Omega(TC^0)$, such a length maximal b is computed by one of the $f_j(a, b_1, \dots, b_{j-1})$, so Algorithm W halts at one of the **stop** instructions for every $a \in V_1^k$.

For a set $Q \subseteq V_1$ with $|Q| = k - 1$ and $v \in V_1 \setminus Q$ we define Q helps v if for some ordering $a := \langle x_1, \dots, x_{j-1}, v, x_{j+1}, \dots, x_k \rangle$ of $Q \cup \{v\}$, Algorithm W on input a outputs a pair $\langle j, w \rangle$ such that w witnesses v .

As there is only a constant number $k!$ of orderings of $Q \cup \{v\}$, there is a function in TC^0 that, given Q, v and canonical witnesses for the elements of Q , uses Algorithm W to decide whether Q helps v , and if so computes a witness $w(Q, v)$ for v .

There are at least $\binom{|V_1|}{k}$ pairs $\langle Q, v \rangle$ such that Q helps v , but there are only $\binom{|V_1|}{k-1}$ possible sets Q of size $k - 1$. Hence there is a set $Q_1 \subseteq V_1$ such that Q_1 helps at least $\frac{|V_1| - k + 1}{k}$ different elements of V_1 .

Inductively we define $V_{i+1} := \{v \in V_i : Q_i \text{ does not help } v\}$, and by the same argument as above, if $|V_{i+1}| > k$ then there is a set $Q_{i+1} \subseteq V_{i+1}$ that helps at least $\frac{|V_{i+1}| - k + 1}{k}$ elements of $V_{i+1} \setminus Q_{i+1}$.

Let t be the least j such that $|V_j| \leq k$, then since $|V_{i+1}| < \left(\frac{k-1}{k}\right)^i |V_1| + k$ we get $t = \lceil \log_{k/(k-1)} |V_1| \rceil = O(n)$. For $i < t$ let S_i be the sequence of pairs $\langle x, w(x) \rangle$ for $x \in Q_i$, and let S_t be the sequence of pairs $\langle x, w(x) \rangle$ for $x \in V_t$. Finally, let the advice $h(n)$ be $S := \langle S_1, \dots, S_t \rangle$. Note that $|S| = O(kn^2)$.

Finally, Algorithm G computes a witness for $v \in V_1$ from inputs v and S . By the remark above, lines 5–6 of Algorithm G can be implemented in TC^0 , and hence the function g computed by Algorithm G is in TC^0 . By construction $g(x, h(|x|))$ witnesses x iff there is a witness for x , hence the equivalence (1) holds. \square

```

if  $v$  occurs in  $S$  then
    output  $w(v)$       (* also occurs in  $S$  next to  $v$  *)
else
    for  $j \in \{1, \dots, t-1\}$  do in parallel
        if  $Q_j$  helps  $v$  then
             $w_j := w(Q_j, v)$ 
        od
    output  $w_j$  with  $j < t$  minimal
fi
    
```

Algorithm G.

We now consider a variant where the measure to be maximized is $\|y\|$ instead of $|y|$. Principle $\Omega^*(TC^0)$ is thus exactly the same as $\Omega(TC^0)$, only with the relation $R^*(x, y, z)$ replaced by $R^{**}(x, y, z)$, which is defined as

$$\|y\| \leq \|x\| \wedge (y > 0 \rightarrow R(x, y)) \wedge (\|y\| < \|z\| \leq \|x\| \rightarrow \neg R(x, z)) .$$

Proposition 5. $\Omega^*(TC^0)$ implies $NP \subseteq \text{non-uniform } TC^0$.

Proof. Modify the proof of Prop. 4 as follows: Let $\ell := 2^{k-1}$. Algorithm W is replaced by Algorithm W*, which gets input $a = \langle x_1, \dots, x_\ell \rangle \in V_1^\ell$. Now again

```

 $y := f_1(a)$ 
if  $\text{length}(y) \geq 1$  and  $R(a, y)$  then
    output  $\langle 1, (y)_1 \rangle$ 
    stop
fi
for  $j$  from 2 to  $k$  do
     $y := f_j(a, b_1, \dots, b_{j-1})$ 
    if  $\text{length}(y) \geq 2^{j-1}$  and  $R(a, y)$  then
         $w := \langle (y)_{2^{j-2}+1}, \dots, (y)_{2^{j-1}} \rangle$ 
        output  $\langle j, w \rangle$ 
        stop
    fi
od
    
```

Algorithm W*. b_j is defined as $\langle w(x_1), \dots, w(x_{2^{j-1}}) \rangle$.

there is a sequence of witnesses $b_0 = \langle w(x_1), \dots, w(x_\ell) \rangle$ of length ℓ , and hence $|b_0| = n\ell$, so $\|b_0\| = k + |n|$. Hence any sequence b with $R(a, b)$ and $\|b\|$ maximal has to be of length ℓ , and by the assumption $\Omega^*(TC^0)$, such a maximal b is found by one of the $f_j(a, b_1, \dots, b_{j-1})$.

For $Q \subseteq V_1$ with $|Q| = \ell - 1$ and $v \in V_1 \setminus Q$, define Q helps v if for some ordering $a := \langle x_1, \dots, x_{m-1}, v, x_{m+1}, \dots, x_\ell \rangle$ of $Q \cup \{v\}$, Algorithm W* on input a outputs a pair $\langle j, w \rangle$ such that either $j = m = 1$ and w witnesses v ,

or $2^{j-2} < m \leq 2^{j-1}$ and w is a sequence of length 2^{j-2} such that $(w)_{m-2^{j-2}}$ witnesses v .

The definition of the advice S is as before, only with k replaced by ℓ everywhere. So Algorithm G on input v and S will still output a witness for v if there is one. \square

6 KPT witnessing for Δ_1^b -CR

In [12] it was shown that the $\exists\forall\Sigma_{i+1}^b$ -theorems of T_2^i can be witnessed by counterexample computations using $FP^{\Sigma_i^p}$ -functions and constantly many counterexamples. For this to be true for $i = 0$, T_2^0 needs to be defined as having function symbols for all functions in FP .

Analogously, we now show that the $\exists\forall\Delta_1^b$ -theorems of Δ_1^b -CR can be witnessed by counterexample computations using TC^0 -functions and constantly many counterexamples. This will be the main tool for proving Thm. 3, but the witnessing theorem and its proof might be of independent interest.

Theorem 6. *Assume Δ_1^b -CR $\vdash \exists x \forall y A(a, x, y)$, where A is Δ_1^b w.r.t. Δ_1^b -CR. Then there are $k \in \mathbb{N}$ and functions $f_1, \dots, f_k \in TC^0$, that are Σ_1^b -definable in Δ_1^b -CR, s.t. Δ_1^b -CR proves*

$$A(a, f_1(a), b_1) \vee A(a, f_2(a, b_1), b_2) \vee \dots \vee A(a, f_k(a, b_1, \dots, b_{k-1}), b_k) .$$

Proof. Let $\{f_n; n \geq 1\}$ be an enumeration of all functions in TC^0 s.t. f_n is n -ary and every function in TC^0 occurs in the list infinitely often (possibly with dummy arguments). Assume that A is Δ_1^b w.r.t. Δ_1^b -CR and Δ_1^b -CR $\vdash \exists x \forall y A(a, x, y)$, but the conclusion of the theorem does not hold. Then by compactness there is a model

$$M \models \Delta_1^b\text{-CR} + \{\neg A(c, f_1(c), d_1), \dots, \neg A(c, f_n(c, d_1, \dots, d_{n-1}), d_n), \dots\}$$

for new constants c, d_1, d_2, \dots

Define $M^* := \{f_1(c), f_2(c, d_1), \dots, f_n(c, d_1, \dots, d_{n-1}), \dots\}$. By the construction of the enumeration f_n , $\mathbb{N} \cup \{c, d_1, d_2, \dots\} \subseteq M^*$, and M^* is closed under all functions in TC^0 .

We first show $M^* \preceq_{\Sigma_0^b} M$, i.e., for every Σ_0^b -formula $B(\mathbf{x})$ and all parameters $\mathbf{a} \in M^*$,

$$M \models B(\mathbf{a}) \text{ iff } M^* \models B(\mathbf{a}) .$$

This is proved by induction on the complexity of $B(\mathbf{x})$. The only interesting case is to show that for $B(\mathbf{x}) = \exists y \leq |t(\mathbf{x})| A(\mathbf{x}, y)$, $M \models B(\mathbf{a})$ implies $M^* \models B(\mathbf{a})$. Consider the function $f(\mathbf{x}) = \mu y \leq |t(\mathbf{x})| A(\mathbf{x}, y)$. This function is in TC^0 ,

hence $f(\mathbf{a}) \in M^*$, and if $M \models B(\mathbf{a})$, then $M \models A(\mathbf{a}, f(\mathbf{a}))$, therefore $M^* \models A(\mathbf{a}, f(\mathbf{a}))$ holds by the induction hypothesis.

Hence if $A(x)$ is Π_1^b and $B(x)$ is Σ_1^b and $\mathbf{a} \in M^*$, then $M \models A(\mathbf{a})$ implies $M^* \models A(\mathbf{a})$ and $M^* \models B(\mathbf{a})$ implies $M \models B(\mathbf{a})$.

Let $\Delta_1^b\text{-CR}_0$ denote *BASIC* + *open-LIND*, and inductively define $\Delta_1^b\text{-CR}_{i+1}$ to be the closure of $\Delta_1^b\text{-CR}_i$ under unnested applications of $\Delta_1^b\text{-COMP}$, and Γ_i to be the set of formulas that are Δ_1^b w.r.t. $\Delta_1^b\text{-CR}_i$. Hence $\Delta_1^b\text{-CR}_{i+1}$ is axiomatized by all theorems of $\Delta_1^b\text{-CR}_i$ and the axioms COMP_A for all formulas $A \in \Gamma_i$, $\Delta_1^b\text{-CR} = \bigcup_i \Delta_1^b\text{-CR}_i$ and the set of formulas that are Δ_1^b w.r.t. $\Delta_1^b\text{-CR}$ is $\Gamma := \bigcup_i \Gamma_i$.

We shall show by simultaneous induction that for all i , $M^* \models \Delta_1^b\text{-CR}_i$ and $M^* \preceq_{\Gamma_i} M$. Obviously $M^* \models \text{BASIC}$. Now let $M^* \models B(0) \wedge \neg B(|a|)$ for some open formula $B(x)$ and $a \in M^*$. Then also $M \models B(0) \wedge \neg B(|a|)$, hence there is a least $b \in M$ such that $M \models b < |a| \wedge B(b) \wedge \neg B(b+1)$. Since the function $f(x) := \mu y < |x| \neg B(y+1)$ is in TC^0 , $f(a) = b \in M^*$, and $M^* \models B(b) \wedge \neg B(b+1)$. This shows $M^* \models \text{open-LIND}$ and thus $M^* \models \Delta_1^b\text{-CR}_0$.

Now assume that $M^* \models \Delta_1^b\text{-CR}_i$, and let $B(x) \in \Gamma_i$. This means there are a Σ_1^b -formula $B^\Sigma(x)$ and a Π_1^b -formula $B^\Pi(x)$ such that

$$\Delta_1^b\text{-CR}_i \vdash B^\Sigma(x) \leftrightarrow B(x) \leftrightarrow B^\Pi(x).$$

Let $\mathbf{a} \in M^*$, then we have

$$M \models B(\mathbf{a}) \implies M \models B^\Pi(\mathbf{a}) \xrightarrow{(\dagger)} M^* \models B^\Pi(\mathbf{a}) \xrightarrow{(*)} M^* \models B(\mathbf{a})$$

$$M^* \models B(\mathbf{a}) \xrightarrow{(*)} M^* \models B^\Sigma(\mathbf{a}) \xrightarrow{(\dagger)} M \models B^\Sigma(\mathbf{a}) \implies M \models B(\mathbf{a})$$

The implications marked $(*)$ hold since $M^* \models \Delta_1^b\text{-CR}_i$, and those marked (\dagger) hold by $M^* \preceq_{\Sigma_0^b} M$. Hence we have shown $M^* \preceq_{\Gamma_i} M$.

Again, let $B(x) \in \Gamma_i$, and $a \in M^*$. Then the characteristic function of B , χ_B , is in TC^0 , and from it we can define a function f_B using CRN that satisfies

$$M \models \forall x < |a| (Bit(f_B(a), x) = 1 \leftrightarrow \chi_B(x) = 1).$$

Since $\chi_B(x) = 1$ is in Γ_i , this formula is also in Γ_i , and hence it also holds in M^* , and furthermore

$$M^* \models \forall x < |a| (\chi_B(x) = 1 \leftrightarrow B(x)),$$

since this formula is in Γ_i and holds in M . Hence $M^* \models \text{COMP}_B$, and we have shown that $M^* \models \Delta_1^b\text{-CR}_{i+1}$.

By induction, $M^* \models \Delta_1^b\text{-CR}$ and $M^* \preceq_{\Gamma} M$. Finally, we show that

$$M^* \models \forall x \exists y \neg A(c, x, y),$$

which contradicts the assumption that $\Delta_1^b\text{-CR} \vdash \exists x \forall y A(a, x, y)$, and thus proves the theorem. Indeed, for $a = f_n(c, d_1, \dots, d_{n-1}) \in M^*$, let $b = d_n$, then by construction $M \models \neg A(c, a, b)$, and since $M^* \preceq_{\Gamma} M$, also $M^* \models \neg A(c, a, b)$. \square

Note that the proof does not show that M^* satisfies the Δ_1^b -comprehension axiom, but only the Δ_1^b -COMP rule.

Corollary 2. *If $S_2^1 = \Delta_1^b$ -CR, then $\Omega(TC^0)$ holds, and $R_2^1 = \Delta_1^b$ -CR implies $\Omega^*(TC^0)$.*

Proof. Let $R(x, y)$ be a predicate in TC^0 , then $R(x, y)$ is Δ_1^b w.r.t. Δ_1^b -CR, and hence also $R^*(x, y, z)$ and $R^{**}(x, y, z)$ are Δ_1^b w.r.t. Δ_1^b -CR. Now we have

$$\begin{array}{ll} S_2^1 \vdash \exists y \forall z R^*(a, y, z) & \text{by } \Sigma_1^b\text{-LMAX} \\ R_2^1 \vdash \exists y \forall z R^{**}(a, y, z) & \text{by } \Sigma_1^b\text{-LLMAX} \end{array}$$

and thus if $S_2^1 = \Delta_1^b$ -CR, then Δ_1^b -CR $\vdash \exists y \forall z R^*(a, y, z)$, and by Thm. 6 there are $k \in \mathbb{N}$ and functions $f_1, \dots, f_k \in TC^0$ such that

$$R^*(a, f_1(a), b_1) \vee R^*(a, f_2(a, b_1), b_2) \vee \dots \vee R^*(a, f_k(a, b_1, \dots, b_{k-1}), b_k),$$

i.e., principle $\Omega(TC^0)$ holds. By the same argument with R^{**} instead of R^* , if $R_2^1 = \Delta_1^b$ -CR then $\Omega^*(TC^0)$ holds. \square

Corollary 2 together with Prop. 4 and 5 prove Thm. 3. The proof of Thm. 6 suggests some open question:

- First, is Δ_1^b -CR = Δ_1^b -CR $_i$ for some i ?
- For $f \in TC^0$, is there a relationship between the minimal i s.t. f is Σ_1^b -definable in Δ_1^b -CR $_i$ and the nesting depth of CRN required to define f in the function algebra? Note that the proof of Thm. 4 actually shows every function in TC^0 that can be defined by i nested applications of CRN is Σ_1^b -definable in Δ_1^b -CR $_i$.
- Moreover, is there a relation between either of these complexity measures and the depth of a TC^0 circuit family computing f ?

References

1. B. Allen. Arithmetizing uniform NC. *Annals of Pure and Applied Logic*, 53:1–50, 1991.
2. E. Allender. The permanent requires large uniform threshold circuits. To appear in *Chicago Journal of Theoretical Computer Science*. Preliminary Version appeared in COCOON'96, 1998.
3. D. A. M. Barrington, N. Immermann, and H. Straubing. On uniformity within NC¹. *Journal of Computer and System Sciences*, 41:274–306, 1990.
4. S. R. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.
5. P. Clote. A first order theory for the parallel complexity class NC. Technical Report BCCS-89-01, Boston College, January 1989.
6. 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.

7. 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.
8. J. Johannsen. A bounded arithmetic theory for constant depth threshold circuits. In P. Hájek, editor, *GÖDEL '96*, pages 224–234, 1996. Springer Lecture Notes in Logic 6.
9. J. Johannsen and C. Pollett. On proofs about threshold circuits and counting hierarchies (extended abstract). In *Proc. 13th IEEE Symposium on Logic in Computer Science*, pages 444–452, 1998.
10. J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Cambridge University Press, 1995.
11. J. Krajíček, P. Pudlák, and J. Sgall. Interactive computations of optimal solutions. In B. Rován, editor, *Mathematical Foundations of Computer Science*, pages 48–60. Springer, 1990.
12. J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52:143–153, 1991.
13. P. Pudlák. Some relations between subsystems of arithmetic and complexity of computations. In Y. N. Moschovakis, editor, *Logic from Computer Science*, pages 499–519. Springer, New York, 1992.
14. 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.