On the $\Delta^b_1$-Bit-Comprehension Rule

Jan Johannsen\textsuperscript{1,*} and Chris Pollett\textsuperscript{2}

\begin{itemize}
  \item \textsuperscript{1} Dept. of Mathematics
  \textsuperscript{}U.C. San Diego
  johannsn@math.ucsd.edu
  \item \textsuperscript{2} Dept. of Mathematics and Computer Science
  Clark University
cpollett@aleph0.clark.edu
\end{itemize}

Abstract. The theory $\Delta^b_1$-CR of Bounded Arithmetic axiomatized by the $\Delta^b_1$-bit-comprehension rule is defined and shown to be strongly related to the complexity class $TC^0$. The $\Sigma^b_1$-definable functions of $\Delta^b_1$-CR are those in uniform $TC^0$, and the $\Sigma^b_2$-definable functions are computable by counterexample computations using $TC^0$-functions. The latter is used to show that a collapse of stronger theories to $\Delta^b_1$-CR implies that $NP$ is contained in non-uniform $TC^0$.

1 Introduction

The $\Delta^b_1$-bit-comprehension rule roughly states the following: Given a length $n$ and a predicate $A(x)$ that has been proven to be $\Delta^b_1$, i.e. equivalent to both an $NP$- ($\Sigma^b_1$-) and a $co-NP$- ($\Pi^b_1$-) 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 $\Delta^b_1$-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 $C^b_0$ of [9], whose $\Sigma^b_1$-definable functions are $TC^0$, is $\forall \Sigma^b_2$-conservative over $\Delta^b_1$-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 $\Delta^b_1$-CR more interesting than the previous theories for $TC^0$.

First, one can argue that it is the weakest natural theory whose $\Sigma^b_1$-definable functions are $TC^0$, as the closure of the $\Sigma^b_1$-definable functions under concatenation recursion on notation (CRN) is essentially the same as $\Delta^b_1$-comprehension.

Second, we will show that $\Delta^b_1$-CR has a tighter connection to $TC^0$ than the previously considered theories: The $\Sigma^b_2$-theorems of $\Delta^b_1$-CR can be witnessed by counterexample computations (a concept introduced by [13, 11] that we will define below) where the Student has the computational capabilities of $TC^0$.

\* Supported by DFG grant No. Jo 291/1-1
Similar to the results of [12], this will allow us to show that a collapse of stronger theories, $S^1_2$ or $R^1_2$ to $\Delta^1_2$-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 $T_k(x_1, \ldots, x_m)$, where the boolean function $T_k$ is defined by

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

If the variables in the circuit are $x_1, \ldots, x_n$, 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 $n$, $\text{size}(C_n) \leq p(n)$ and $\text{depth}(C_n) \leq d$.

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 $\{k^k : k \in K\}$ 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 $D\text{LogTime}$-uniformity, see [3] for the somewhat involved definition.

$D\text{LogTime}$-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 polynomial-time 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 $D\text{LogTime}$-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

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

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 $TC_0^0$ 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 $(C_n; n \in \mathbb{N})$ of depth $d$ and size $O(p(n))$ computing $A(x)$ be given. Then $A(x) \in TC_0^0/poly$ 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 $A(x) \in TC_0^0/poly$ 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 $f(n)$.

Next we give the machine-independent characterization of $TC_0^0$ mentioned above:

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

\[
\begin{align*}
    f(0, x) &= g(x) \\
    f(2n, x) &= 2 \cdot f(n, x) + h_0(n, x), \text{ provided } n \neq 0 \\
    f(2n + 1, x) &= 2 \cdot f(n, x) + h_1(n, x)
\end{align*}
\]

Let $i^n_k(x_1, \ldots, x_n) := x_k$, $s_0(x) := 2x$, $s_1(x) = 2x + 1$, $|x| := \lceil \log_2 (x + 1) \rceil$, $x \# y := 2^{|x|} \cdot 2^{|y|}$ and $\text{Bit}(x, i) := \left\lfloor \frac{x}{2^i} \right\rfloor \mod 2$. The following characterization of the number-theoretic functions in $TC_0^0$ was given in [7]:

Proposition 2. The class $TC_0^0$ is the smallest class of functions that contains $0$, $i^n_k$, $s_0$, $s_1$, multiplication $\cdot$, $\#$, $|x|$, $\text{Bit}$ 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 $\Sigma_n^b$ or $B_n^b$. For $i \in \mathbb{N}$, $\Sigma_n^b$ (resp. $B_n^b$) is the least class containing $B_0^b$ (resp. $\Sigma_0^b$) and closed under conjunction, disjunction, sharply bounded quantification and bounded existential (resp. universal) quantification.
We say that a function $f(x)$ is $\Sigma^b_1$-definable in a theory $T$ if there is a $\Sigma^b_1$-formula $A(x, y)$ and a term $t(x)$ such that

$$\mathbb{N} \models \forall x \ A(x, f(x))$$
$$T \vdash \forall x \ A(x, y)$$
$$T \vdash \forall x, y, z \ A(x, y) \land A(x, z) \rightarrow y = z.$$  

$\text{BASIC}$ 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 $\text{BASIC}$ from [4] together with the axioms for $\text{MSP}$ and $\text{LLIND}$ from [14].

For a class of formulas $\Phi$, the axiom schema $\Phi\text{LLIND}$ is

$$A(0) \land \forall x \ A(x, A(Sx)) \rightarrow \forall x \ A([x])$$

for each $A(x) \in \Phi$, and $\Phi\text{LLIND}$ is

$$A(0) \land \forall x \ A(x, A(Sx)) \rightarrow \forall x \ A([x])$$

for $A(x) \in \Phi$. In general, for $m \geq 1$, $\Phi\text{-L}^m\text{IND}$ is

$$A(0) \land \forall x \ A(x, A(Sx)) \rightarrow \forall x \ A([x])$$

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

The theory $S^2_2$ is the theory axiomatized by the $\text{BASIC}$ axioms and $\Sigma^b_2\text{-LIN D}$, and $S^2_2$ is the theory given by $\text{BASIC}$ and $\Sigma^b_2\text{-LIN D}$.

**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 a binary operation other than $\text{or}$ or $\text{MSP}$, then $t^*$ is $s^*_1 \circ s^*_2$. Lastly, if $t$ is $s_1 \text{ or } s_2$ or $\text{MSP}(s_1, s_2)$, then $t^*$ is $s^*_1$.

It is easily proved in $\text{BASIC} + \text{open-LIND}$ that $t^*$ is monotonic, and $t \leq t^*$.

The following terms will be used frequently below. Let

- $2^{[y]} := 1 \# x$
- $\text{mod2}(x) := x \div 2 \cdot \lfloor \frac{1}{2} \rfloor$
- $\text{Bit}(x, i) := \text{mod2}(\text{MSP}(x, i))$
- $2^{\min(x, [y])} := \text{MSP}(2^{[y]}, [y], x)$
- $LSP(x, i) := x \div 2^{\min([y], [x])} \cdot \text{MSP}(x, i)$
- $\beta_0(w, i) := \text{MSP}(LSP(w, Si \cdot [a], i \cdot [a])$

so that $LSP(x, [y])$ returns the number consisting of the last $[y]$ bits of $x$, and if $w$ codes a sequence $\langle b_1, \ldots, b_i \rangle$ with $|b_i| \leq |a|$ for all $i$, then $\beta_0(w, i) = b_i$. 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 $|a|$ 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 $(x, y) := (B + y) \times 2B + (B + x)$. The terms $(w)_1 := \beta_{\frac{1}{2}(|s|+1)}^{-1}(0, \beta_{\frac{1}{2}(|s|+1)}(0, w))$ and $(w)_2 := \beta_{\frac{1}{2}(|s|+1)}^{-1}(0, \beta_{\frac{1}{2}(|s|+1)}(1, w))$, project out the left and right coordinates from an ordered pair. To check if $w$ is a pair we use the formula

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

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

$$\forall x \leq |s| \exists y \leq t(x) A(x, y) \rightarrow \\
\exists y < bd(t(|s|), s) \forall x \leq |s| [\beta_{\tau(|s|)}((w, x) \leq t(x) \land A(x, \beta_{\omega(|s|)}((w, x))]
$$

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

The theory $C^0_2$ is defined as $BASIC + open\text{-}LIND + BBSigma^0_2$. The following theorem summarizes some relations between $\Sigma^0_1$-definability in the theories defined and computational complexity.

**Theorem 1.** — The $\Sigma^0_1$-definable functions in $S^2_2$ are exactly those in $FP_{\Sigma^0_1}$,

- The $\Sigma^0_1$-definable functions in $R^0_2$ are exactly those in $NC$ [1, 5],
- The $\Sigma^0_1$-definable functions in $C^0_2$ are exactly those in $TC^0 [8, 9]$.

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

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

The $\Delta^0_1$-comprehension rule, $\Delta^0_1\text{-COMP}$, is the following inference rule

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

where $A(x)$ is $\Sigma^0_1$ and $B(x)$ is $\Pi^0_1$, and $t$ is an arbitrary $L_2$-term. Note that this rule is different from the possibly stronger $\Delta^0_1$-comprehension axiom

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

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

**Definition 3.** Let $\Delta^0_1\text{-CR}$ be the theory axiomatized by $BASIC$, open-LIND and the $\Delta^0_1\text{-COMP}$ rule.

In [9], it is proved that $C^0_2$ proves the $\Delta^0_1\text{-COMP}$ axiom, therefore $\Delta^0_1\text{-CR}$ is a subtheory of $C^0_2$. But we will show that $C^0_3$ is not much stronger:
Theorem 2. $C^0_2$ is $\forall \Sigma^1_1$-conservative over $\Delta^1_1$-$CR$.

This implies immediately:

Corollary 1. The $\Sigma^1_1$-definable functions of $\Delta^1_1$-$CR$ are precisely $TC^0$.

Hence $S^0_2 = \Delta^1_1$-$CR$ implies $P = TC^0$, and $R^1_2 = \Delta^1_1$-$CR$ implies $NC = TC^0$.

We will show that the connection between the theory $\Delta^1_1$-$CR$ and $TC^0$ is still tighter: the $\Sigma^1_1$-theorems of $\Delta^1_1$-$CR$ 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 $\Delta^1_1$-$CR$ to either of the stronger theories $S^0_2$ or $R^1_2$ implies a further collapse of complexity classes:

Theorem 3. If $S^0_2 = \Delta^1_1$-$CR$ or $R^1_2 = \Delta^1_1$-$CR$, 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 $\Delta^1_1$-$CR \vdash \Sigma^0_1$-$LMIND$ for any $m > 0$.

The following further axiom schemes will be used below. The $\Sigma^0_1$-length-maximization scheme, $\Sigma^0_1$-$LMAX$, is the axiom

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

for every $\Sigma^0_1$-formula $A(x)$. Similarly, the $\Sigma^0_1$-double-length-maximizations scheme, $\Sigma^0_1$-$LLMAX$, is the axiom

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

for every $\Sigma^0_1$-formula $A(x)$. The following proposition is well-known.

Proposition 3. $S^0_2 \vdash \Sigma^0_1$-$LMAX$ and $R^1_2 \vdash \Sigma^0_1$-$LLMAX$. In fact, $\Sigma^0_1$-$LMAX$ is equivalent to $\Sigma^0_1$-$LIND$ and $\Sigma^0_1$-$LLMAX$ is equivalent to $\Sigma^0_1$-$LLIND$ 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 $\Sigma^0_1$-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. $||a||/||b||$ is contained in $TC^0$. 
We are now ready to show the functions in $TC$ function allows us to determine which term in $f$ gives us the position within a term. Define the function $Pr$.

By Lemma 2 and Lemma 1 we can define

$$||a||/||b|| := mn \leq |a| \cdot (|a| < (n + 1)||b||).$$

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

$$\sum_{n=0}^{\infty} g(n, x) \cdot 2^n \cdot |s|.$$

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

Proof. Suppose we want to define the length-sum

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

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

$$t(i, a, x) := |a| - |i|/|s^*(x)||$$

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

$$p(i, x) := |s^*(x)| - (|i| - |i|/|s^*(x)||) |s^*(x)| - 1$$

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

$$f'(0, a, x) = Bit(p(0, x), h(t(0, a, x), x))$$
$$f'(2i + 1, a, x) = f'(2i, a, x) = 2f'(i, a, x) + Bit(p(i, x), h(t(i, a, x), x)).$$

Then the desired $f(a, x)$ is $f'(2^n |s^*(x)| + |i|/|s^*(x)|| - 2, a, x)$. The expression in the first component of $f'$ is easily defined using $\wedge$, $\#$, and $MSP$. 

Lemma 5. $\Delta^0_1$-CR proves the $\Delta^0_1$-$LIND$ axioms, and $\Delta^0_1$-CR proves the bit-extensionality axiom:

$$|a| = |b| \iff \forall i < |a| \left( Bit(a, i) = Bit(b, i) \right) \rightarrow a = b.$$ 

Proof. If $A$ is $\Delta^0_1$ in $\Delta^0_1$-CR, then $\Delta^0_1$-CR proves the $LIND$ axiom for $A$ since $\Delta^0_1$-CR proves $COMP_A(a)$ and $\Delta^0_1$-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 $\Sigma^0_1$-formula:

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

We are now ready to show the functions in $TC^0$ are $\Sigma^0_1$-definable in $\Delta^0_1$-CR.
Theorem 4. $\Delta^1_1\text{-CR}$ can $\Sigma^1_1$-define the functions in $TC^0$.

Proof. The base functions symbols are obviously $\Sigma^1_1$-definable in $\Delta^1_1\text{-CR}$ and closure under composition is straightforward. So it suffices to show the $\Sigma^1_1$-definable functions of $\Delta^1_1\text{-CR}$ 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 $\Sigma^1_1$-defined in $\Delta^1_1\text{-CR}$. Define $t(a, x)$ to be

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

then $f(a, x) = g(x) \cdot 2^{1[|a|+x]} + t(a, x)$. It suffices to show the length-sum $t(a, x)$ is $\Sigma^1_1$-definable, since then $f(a, x)$ will be by composition.

Notice $k(n, x, a) := \text{cond}(\text{Bit}(|a| - n, a), h_0(n, x), h_1(n, x))$ is $\Sigma^1_1$-defined in $\Delta^1_1\text{-CR}$. Let $A_k(n, a, x, y)$ be its defining formula. Given the other parameters, $\Delta^1_1\text{-CR}$ proves the value $y$ is unique and bounded by 1. Therefore $\Delta^1_1\text{-CR}$ $\vdash A_k(n, x, a, 1) \iff \neg A_k(n, x, a, 0)$ and $A_k(n, x, a, 1)$ is true if $k(n, x, a) = 1$ so $k(n, x, a) = 1$ is a $\Delta^1_1$-property in $\Delta^1_1\text{-CR}$. We want to define the sum $\sum_{n=0}^{[a]} k(n, x, a) \cdot 2^n$. $\Delta^1_1\text{-COMPO}$ on $k(n, x, a) = 1$ implies

$$(\exists w \leq s)(\forall n \leq |a|)(\text{Bit}(n, w) = 1 \iff k(n, w, a) = 1),$$

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

Remark 1. Given two $\Sigma^1_1$-defined in $\Delta^1_1\text{-CR}$ functions $f, g$, the property $f(x) = g(x)$ will be $\Delta^1_1$ in $\Delta^1_1\text{-CR}$. Using this, $\Delta^1_1\text{-LIND}$, and extensionality it is not hard to show $\Delta^1_1\text{-CR}$ proves simple properties of both the $\mu$-operation and length-sums. For instance, $\Delta^1_1\text{-CR}$ proves that if $h(n, x) \leq s(x)$ then

$$\beta_{1, 1}(j, \sum_{n=0}^{[a]} h(n, x) \cdot 2^{|y| \cdot [x]|}) = h(j, x)$$

for $j \leq |a|$.

To prove the conservativity result, we formalize the witnessing proof for $C^2_\Delta$ in $\Delta^1_1\text{-CR}$. First we define a witness bounding term and witness predicate for $\Sigma^1_1$-formulas as follows:

- If $A(a) \in \Sigma^0_1$ then $t_A = 0$ and $\text{Wit}_A(w, a) := A(a) \land w = 0$.
- If $A(a)$ is of the form $B \circ C$ where $\circ$ is $\land$ or $\lor$ then $t_A := 4 \cdot (2^{\text{max}(B, C)})^2$ and

$$\text{Wit}_A(w, a) := \text{ispair}(w) \land (\text{Wit}_B((w)_1, a) \circ \text{Wit}_C((w)_2, a))$$

- If $A(a)$ is of the form $\exists x \leq t B(x, a)$ where $B(x, a) \in \Sigma^0_1$ then $t_A := t$ and

$$\text{Wit}_A(w, a) := w \leq t \land B(w, a).$$
The following lemma is true for this witness predicate:

**Lemma 6.** If \( A(a) \in \Sigma^1_1 \), then:

(a) \( \text{Wit}_A \) is a \( \Sigma^1_1 \)-predicate.

(b) \( \Delta^1_1 \text{-CR} \vdash \exists w \leq t_A(a) \, \text{Wit}_A(w, a) \rightarrow A(a) \).

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

To prove the witnessing theorem, we formalize \( C^0_2 \) in a sequent calculus \( LKB \) that has special rules for the introduction of bounded quantifiers (see [4]). In this formalization, \( \text{open-LIND} \) and \( BB \Sigma^1_0 \) are given as inference rules, which are shown in the proof below.

**Theorem 5.** Suppose

\[
C^0_2 \vdash \Gamma \Rightarrow \Delta
\]

where \( \Gamma \) and \( \Delta \) are cedents of \( \Sigma^1_1 \)-formulas. Let \( a \) be the free variables in this sequent. Then there is a \( TC^0 \) function \( f \) which is \( \Sigma^1_1 \)-defined in \( \Delta^1_1 \text{-CR} \) such that:

\[
\Delta^1_1 \text{-CR} \vdash \text{Wit}_\Lambda \, \Gamma(w, a) \rightarrow \text{Wit}_\Delta(f(w, a), a).
\]

*Proof.* This is proved by induction on the number of sequents in a \( C^0_2 \) proof of \( \Gamma \Rightarrow \Delta \). By cut elimination, we can assume all the sequents in the proof are \( \Sigma^1_1 \). Most of the cases are similar to previous witnessing arguments so we only show the \((\forall \mathbin{\text{right case}}\) case, open-LIND case and the \( BB \Sigma^1_0 \) case.

\((\forall \mathbin{\text{right case}}\) Suppose we have the inference:

\[
\frac{b \leq t, \, \Gamma \Rightarrow A(b), \, \Delta}{\Gamma \Rightarrow \forall x \leq t \, A(x), \, \Delta}
\]

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

\[
\Delta^1_1 \text{-CR} \vdash \text{Wit}_{b \leq t \, \Lambda \, \Gamma(w, a, b)} \rightarrow \text{Wit}_{\Lambda \, \forall \, \Delta \, (g(w, a, b), a, b)}.
\]

By cut-elimination, \( \forall x \leq t \, A(x) \) is a \( \Sigma^1_1 \)-formula, so \( t \) must be of the form \( t = [s] \). There are two case: where \( A \) is \( \Sigma^1_0 \) and where \( A \) is \( \Sigma^1_1 \setminus \Sigma^1_0 \). In the first case, let \( y \) be \( \mu i \leq [s] \, \neg A(i) \) and define \( f \) to be \( g([0], w, a, y) \). The \( 0 \) in the ordered pair is
since $Wit_{b \leq t}(w, b) = b \leq t \land w = 0$. This is in $TC^0$ by Lemma 1 and Lemma 2 and it is not hard to show that

$$\Delta^0_1-CR \vdash Wit_T(w, a) \rightarrow Wit_{\forall x \leq t} A \lor \bigvee A(f(w, a), a).$$

In the second case, since $Wit_A$ is a $\Sigma^0_0$-formula, its characteristic function $\chi_{Wit_A}$ is in $TC^0$. Let $k$ be the function

$$k(w, a) = \mu j \leq |s| [\neg Wit_A((g(0, w), a))_1, a, j].$$

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

$$f(w, a) = \begin{cases} \left(\sum_{j=0}^{k(w, a)} (g(0, w), a, j) \right) \cdot 2^j \oplus 0, & \text{if } k(w, a) = |s| + 1 \\ \left(0, (g(0, w), a, k(w, a))_2\right), & \text{otherwise} \end{cases}$$

then using the remark after Theorem 4

$$\Delta^0_1-CR \vdash Wit_T(w, a) \rightarrow Wit_{\forall x \leq t} A \lor \bigvee A(f(w, a), a).$$

(open-LIND case) Suppose we have the inference

$$A(b), \Gamma \Rightarrow A(Sb), \Delta$$

$$A(0), \Gamma \Rightarrow A\{s\}, \Delta$$

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

$$\Delta^0_1-CR \vdash Wit_{A(b)} \land \bigwedge \forall r(w, b, a) \rightarrow Wit_{A(Sb)} \lor \bigvee A(g(w, b, a), b, a).$$

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

$$f(w, a) := g(w, \mu y < |s|) (\neg Wit\Delta((g(w, y, a)))_2, y, a).$$

Notice $Wit_{A(b)}(w, b, a) := A \land v = 0$ 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 $f(w, a)$ runs $g$ on the least value $v$ less than $|s|$ that produces a witness for $\Delta$. 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:

$$\Delta^0_1-CR \vdash Wit_{A(b)} \land \bigwedge \forall r(w, a) \rightarrow Wit_{A(Sb)} \lor \bigvee A(f(w, a), a).$$

(BB$\Sigma^0_2$ case) Suppose we have the inference:

$$\Gamma \Rightarrow \forall x \leq |s| \exists y \leq t A(x, y), \Delta$$

$$\Gamma \Rightarrow \exists x \leq k d(t_A|s|, s) \forall x \leq |s| [A(x, \beta x|t| t(x, v)) \leq t \land A(x, t(x, v))], \Delta$$

where $s, t$ are terms in $L_2$ and $A(x, y) \in \Sigma^0_2$. By the induction hypothesis there is a $TC^0$ function $g$ such that

$$\Delta^0_1-CR \vdash Wit_{\forall x \leq |s| \exists y \leq t} A \lor \bigvee \Delta(g(w, a), a).$$
For this case, it suffices to notice that the predicates

\[ W\forall x\exists y \{\exists z \leq t \cdot z \cdot A \} \]

and

\[ W\exists x \leq b \{\forall x \cdot \forall y \exists z \in [0, t] \cdot (x, y) \cdot z \cdot A \} \]

are the same. Hence, if we let \( f = g \) then

\[ \Delta^1_0 \neg \text{CR} \vdash W\forall z A(f(w, a, b) \rightarrow W\exists x \leq b \{ \forall z \geq |x| \cdot w \cdot A \} \vee \neg f(w, a, b) \}. \]

This completes the cases and the proof. \( \square \)

Now Thm. 2 follows from this witnessing theorem as follows: Suppose \( C^0_2 \) proves a \( \Sigma^0_2 \)-formula \( A(x) \). Then by Theorem 5, taking \( \Gamma \) to be the empty cedenent, \( \Delta^1_0 \neg \text{CR} \vdash W\forall x A(g(x), x) \), where \( g \) is a \( TC^0 \) function. By Lemma 6, we have \( \Delta^1_0 \neg \text{CR} \vdash A(x) \). \( \square \)

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. In order to find a maximal solution, Student can ask questions of the form “Is \( y \) a maximal solution?”, to which Teacher can either reply “yes” or provide a counterexample, i.e., a better solution.

There are two natural measures of complexity for counterexample computations: the computational power of Student, and the number of counterexamples. Note that every optimization problem can be solved with \( O(|x|) \) many counterexamples by the trivial Student, who just repeats each counterexample provided as his next question.

Here we are interested in the case where Student has the computational capabilities of \( TC^0 \) and the number of counterexamples is bounded by a constant. We will show that the hypothesis that every optimization problem in \( TC^0 \) can be computed in this way, formalized by principle \( \Omega(\neg \text{TC}^0) \) below, implies that every \( NP \) predicate is computable by non-uniform \( TC^0 \) circuits.

For an optimization problem \( R(x, y) \) let \( R^\star(x, y, z) \) be defined by

\[ |y| \leq |x| \land (y > 0 \rightarrow R(x, y)) \land (|y| < |x| \leq |x| \rightarrow \neg R(x, z)) , \]

so that \( \forall y R^\star(x, y, z) \) expresses that \( y = 0 \) or \( y \) is a maximal solution.

**Principle \( \Omega(\neg \text{TC}^0) \):** for every predicate \( R(x, y) \in TC^0 \) there are \( k \in \mathbb{N} \) and functions \( f_1, \ldots, f_k \in TC^0 \), such that
Either $\forall z \ R^*(a, f_1(a), z)$ or if $b_1$ is such that $\neg R^*(a, f_1(a), b_1)$, then either $\forall z \ R^*(a, f_2(a, b_1), z)$ or if $b_2$ is such that $\neg R^*(a, f_2(a, b_1), b_2)$, ... then $\forall z \ R^*(a, f_1(a, b_1, \ldots, b_{k-1}), z)$.

**Proposition 4.** $\Omega(TC^0)$ implies $NP \subseteq$ non-uniform $TC^0$.

**Proof.** Let $A$ be $NP$-complete under $TC^0$-reductions, and be given by $x \in A \iff \exists w \leq x B(x, w)$ with $B \in TC^0$. We say that $w$ witnesses $x$ if $w \leq x \land B(x, w)$ holds.

We will construct an advice function $h$ with $|h(n)| \leq n^{O(1)}$ and $g \in TC^0$ such that $g(x, h(|x|))$ witnesses $x$ for all $x \in A$, i.e.,

$$x \in A \iff B(x, g(x, h(|x|))).$$

(1)

and hence $A \in TC^0/poly$, assuming $\Omega(TC^0)$.

Let the relation $R(a, b)$ be defined by

- $a$ and $b$ code sequences, and $\text{length}(a) \geq \text{length}(b)$
- and for all $i \leq \text{length}(b)$ : $(b)_i$ witnesses $(a)_i$.

Obviously $R \in TC^0$, so by $\Omega(TC^0)$ there are functions $f_1, \ldots, f_k$ that for a sequence $a = \langle x_1, \ldots, x_m \rangle$ interactively compute a maximal sequence $b$ of witnesses for an initial segment of $a$.

For a fixed length $n$, let $V_1 := \{ x \in A \mid |x| = n \}$, 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 $a = \langle x_1, \ldots, x_k \rangle \in V_1^k$ such that $w$ witnesses $x_j$. Since there is a

$$y := f_1(a)$$

if $\text{length}(y) \geq 1$ and $R(a, y)$ then

- output $\langle 1, \langle y \rangle \rangle$
- stop

for $j$ from 2 to $k$ do

$$y := f_2(a, b_1, \ldots, b_{j-1})$$

if $\text{length}(y) \geq j$ and $R(a, y)$ then

- output $\langle j, \langle y \rangle \rangle$
- stop

od

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

sequence of witnesses $b_0 = \langle w(x_1), \ldots, w(x_k) \rangle$ 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 $f_j(a, b_1, \ldots, b_{j-1})$, so Algorithm W halts at one of the stop instructions for every $a \in V_1^j$.

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 $a := \langle x_1, \ldots, x_j, v, x_{j+1}, \ldots, x_k \rangle$ of $Q \cup \{v\}$, Algorithm W on input $a$ outputs a pair $(j, w)$ 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 $(Q, v)$ 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 $V_{i+1} := \{ v \in V_i : Q_i$ 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 $V_{i+1}$.

Let $t$ be the least $j$ such that $|V_j| \leq k$, then since $|V_{j+1}| < \left(\frac{j+1}{j}\right)^j |V_j| + k$ we get $t = \lceil \log_{j/(j-1)} |V_1| \rceil = O(n)$. For $i < t$ let $S_i$ be the sequence of pairs $(x, w(x))$ for $x \in Q_i$, and let $S_t$ be the sequence of pairs $(x, w(x))$ for $x \in V_t$. Finally, let the advice $h(n)$ be $S := \langle S_1, \ldots, S_t \rangle$. 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 $TC^0$.

\[
\text{Algorithm G.}
\]

and hence the function $g$ computed by Algorithm G is in $TC^0$. By construction $g(x, h([z]))$ witnesses $x$ iff there is a witness for $x$, hence the equivalence (1) holds.

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

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

**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 $a = \langle x_1, \ldots, x_\ell \rangle \in V_1^\ell$. Now again

\[
y := f_1(a)
\]

if $\text{length}(y) \geq 1$ and $R(a, y)$ then
  output $\langle 1, \langle y \rangle_1 \rangle$
  stop
fi
for $j$ from 2 to $k$ do
  $y := f_j(a, b_1, \ldots, b_{j-1})$
  if $\text{length}(y) \geq 2^{j-1}$ and $R(a, y)$ then
    $w := \langle \langle y \rangle_{j-2+1}, \ldots, \langle y \rangle_{j-1} \rangle$
    output $\langle j, w \rangle$
    stop
  fi
od

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

there is a sequence of witnesses $b_0 = \langle w(x_1), \ldots, w(x_\ell) \rangle$ of length $\ell$, 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 $\ell$, and by the assumption $\Omega^*(TC^0)$, such a maximal $b$ is found by one of the $f_j(a, b_1, \ldots, b_{j-1})$.

For $Q \subseteq V_1$ with $|Q| = \ell - 1$ and $v \in V_1 \setminus Q$, define $Q$ helps $v$ if for some ordering $a := \langle x_1, \ldots, x_{m-1}, v, x_{m+1}, \ldots, x_\ell \rangle$ of $Q \cup \{v\}$, Algorithm $W^*$ on input $a$ outputs a pair $(j, w)$ 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 $(w)_{m-2j+3}$ witnesses $v$.

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

6 KPT witnessing for $\Delta^b_1$-CR

In [12] it was shown that the $\exists \forall \Sigma^b_{i+1}$-theorems of $T^i_2$ can be witnessed by counterexample computations using $FP^{\Sigma^b_{i+1}}$-functions and constantly many counterexamples. For this to be true for $i = 0$, $T^0_2$ needs to be defined as having function symbols for all functions in $FP$.

Analogously, we now show that the $\exists \forall \Delta^b_1$-theorems of $\Delta^b_1$-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 $\Delta^b_1$-CR + $\exists \forall A(a, x, y)$, where $A$ is $\Delta^b_1$ w.r.t. $\Delta^b_1$-CR. Then there are $k \in \mathbb{N}$ and functions $f_1, \ldots, f_k \in TC^0$, that are $\Sigma^b_1$-definable in
Consider the function \( \Delta_1^1 \). Let \( \{ f_n \mid n \geq 1 \} \) be an enumeration of all functions in \( TC^0 \). Let \( f_n \) be \( n \)-ary and every function in \( TC^0 \) occurs in the list infinitely often (possibly with dummy arguments). Assume that \( A \) is \( \Delta_1^1 \) w.r.t. \( \Delta_1^1 \)-CR and \( \Delta_1^1 \)-CR proves \( \exists y \forall x A(a, x, y) \), but the conclusion of the theorem does not hold. Then by compactness there is a model
\[
M \models \Delta_1^1 \text{-CR} + \{ \neg A(c, f_1(c), d_1), \ldots, \neg A(c, f_n(c, d_1, \ldots, d_{n-1}), d_n), \ldots \}
\]
for new constants \( c, d_1, d_2, \ldots \).

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

We first show \( M^* \models \Sigma_1^1 \)-model \( M \), i.e., for every \( \Sigma_1^1 \)-formula \( B(x) \) and all parameters \( a \in M^* \),
\[
M \models B(a) \text{ iff } M^* \models B(a) .
\]

This is proved by induction on the complexity of \( B(x) \). The only interesting case is to show that \( B(x) = \forall y \exists z A(x, y, z) \). If \( M \models B(a) \) implies \( M^* \models B(a) \). Consider the function \( f(x) = \langle y, z \rangle A(x, y, z) \). This function is in \( TC^0 \), hence \( f(a) \in M^* \), and if \( M \models B(a) \), then \( M \models A(a, f(a)) \), therefore \( M^* \models A(a, f(a)) \) holds by the induction hypothesis.

Hence if \( A(x) \) is \( \Pi_1^1 \) and \( B(x) \) is \( \Sigma_1^1 \) and \( a \in M^* \), then \( M \models A(a) \) implies \( M^* \models A(a) \) and \( M^* \models B(a) \) implies \( M \models B(a) \).

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

We shall show by simultaneous induction that for all \( i \), \( M^* \models \Delta_1^1 \)-CR\(_i\) and \( M^* \models \Pi_1^1 \)-model \( M \). Obviously \( M^* \models \Pi_1^1 \)-model. Now let \( M^* \models B(0) \wedge \neg B(\bar{a}) \) for some open formula \( B(x) \) and \( a \in M^* \). Then also \( M \models B(0) \wedge \neg B(\bar{a}) \), hence there is a least \( b \in M \) such that \( M \models b < \bar{a} \wedge B(b) \wedge \neg B(b+1) \). Since the function \( f(x) := \langle y, z \rangle A(x, y, z) \) is in \( TC^0 \), \( f(a) \in M^* \), and \( M^* \models B(0) \wedge \neg B(b+1) \).

This shows \( M^* \models \Pi_1^1 \)-LIND and thus \( M^* \models \Delta_1^1 \)-CR\(_0\).

Now assume that \( M^* \models \Delta_1^1 \)-CR\(_0\), and let \( B(x) \in \Gamma \). This means there are \( \Sigma_1^1 \)-formula \( B^\Sigma(x) \) and a \( \Pi_1^1 \)-formula \( B^H(x) \) such that
\[
\Delta_1^1 \text{-CR}_0 \vdash B^\Sigma(x) \iff B(x) \iff B^H(x) .
\]

Let \( a \in M^* \), then we have
\[
M \models B(a) \iff M \models B^H(a) \iff M^* \models B^H(a) \iff M^* \models B(a) ,
\]
\[
M^* \models B(a) \iff M^* \models B^\Sigma(a) \iff M \models B^\Sigma(a) \iff M \models B(a) .
\]
The implications marked (⋆) hold since \( M^* \models \Delta_1^1-CR_i \), and those marked (†) hold by \( M^* \preceq_{\Sigma^1_2} M \). Hence we have shown \( M^* \preceq_{\Sigma^1_2} M \).

Again, let \( B(x) \in \Gamma_i \) and \( a \in M^* \). Then the characteristic function of \( B \), \( \chi_B \), is in \( TC^0 \), and from it we can define a function \( f_B \) using \( CRN \) that satisfies
\[
M \models \forall x < |a| \left( B(x) = 1 \iff \chi_B(x) = 1 \right).
\]
Since \( \chi_B(x) = 1 \) is in \( \Gamma_i \), this formula is also in \( \Gamma_i \), and hence it also holds in \( M^* \), and furthermore
\[
M^* \models \forall x < |a| \left( \chi_B(x) = 1 \iff B(x) \right),
\]
since this formula is in \( \Gamma_i \) and holds in \( M \). Hence \( M^* \models \text{COMP} \), and we have shown that \( M^* \models \Delta_1^1-CR_{i+1} \).

By induction, \( M^* \models \Delta_1^1-CR \) and \( M^* \preceq_{\Sigma^1_2} M \). Finally, we show that
\[
M^* \models \forall x \exists y \neg A(c, x, y),
\]
which contradicts the assumption that \( \Delta_1^1-CR \vdash \exists x \forall y A(a, x, y) \), and thus proves the theorem. Indeed, for \( a = f(c, d_1, \ldots, d_{n-1}) \in M^* \), let \( b = d_n \), then by construction \( M \models \neg A(c, a, b) \), and since \( M^* \preceq_{\Sigma^1_2} M \), also \( M^* \models \neg A(c, a, b) \).

Note that the proof does not show that \( M^* \) satisfies the \( \Delta_1^1 \)-comprehension axiom, but only the \( \Delta_1^1 \)-COMP rule.

**Corollary 2.** If \( S^1_i = \Delta_0^1-CR \) then \( \Omega(TC^0) \) holds, and \( R^1_2 = \Delta_0^1-CR \) implies \( \Omega(TC^0) \).

**Proof.** Let \( R(x, y) \) be a predicate in \( TC^0 \), then \( R(x, y) \) is \( \Delta_0^1 \) w.r.t. \( \Delta_1^1-CR \), and hence also \( R^*(x, y, z) \) and \( R^{**}(x, y, z) \) are \( \Delta_0^1 \) w.r.t. \( \Delta_1^1-CR \). Now we have
\[
S^1_2 \vdash \exists y \forall z R^*(a, y, z) \quad \text{by } \Sigma^1_1\text{-LMAX}
\]
\[
R^1_2 \vdash \exists y \forall z R^{**}(a, y, z) \quad \text{by } \Sigma^1_1\text{-LMAX}
\]
and thus if \( S^1_2 = \Delta_1^1-CR \), then \( \Delta_1^1-CR \vdash \exists y \forall z R^*(a, y, z) \), and by Thm. 6 there are \( k \in \mathbb{N} \) and functions \( f_1, \ldots, f_k \in TC^0 \) such that
\[
R^*(a, f_1(a), b_1) \lor R^*(a, f_2(a, b_1), b_2) \lor \cdots \lor R^*(a, f_k(a, b_1, \ldots, b_{k-1}), b_k),
\]
i.e., principle \( \Omega(TC^0) \) holds. By the same argument with \( R^{**} \) instead of \( R^* \), if \( R^1_2 = \Delta_1^1-CR \) then \( \Omega(TC^0) \) holds.

**Corollary 2** together with Prop. 4 and 5 proves Thm. 3. The proof of Thm. 6 suggests some open questions:

- First, is \( \Delta_i^1-CR = \Delta_i^1-CR_i \) for some \( i \)?
- For \( f \in TC^0 \), is there a relationship between the minimal \( i \) s.t. \( f \) is \( \Sigma^1_1 \)-definable in \( \Delta_i^1-CR \) 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 \( \Sigma^1_1 \)-definable in \( \Delta_i^1-CR_i \).
- Moreover, is there a relation between either of these complexity measures and the depth of a \( TC^0 \) circuit family computing \( f \)?
References