# Total Search Problems in Bounded Arithmetic and Improved Witnessing

Arnold Beckmann and Jean-José Razafindrakoto

Department of Computer Science, College of Science, Swansea University
a.beckmann@swansea.ac.uk, jjrazaf@icloud.com

**Abstract.** We define a new class of total search problems as a subclass of Megiddo and Papadimitriou's class of total $\mathsf{NP}$ search problems, in which solutions are verifiable in $\mathsf{AC}^0$. We denote this class $\forall\exists\mathsf{AC}^0$. We show that all total $\mathsf{NP}$ search problems are equivalent, wrt. $\mathsf{AC}^0$-many-one reductions, to search problems in $\forall\exists\mathsf{AC}^0$. Furthermore, we show that $\forall\exists\mathsf{AC}^0$ contains well-known problems such as the Stable Marriage and the Maximal Independent Set problems. We introduce the class of Inflationary Iteration problems in $\forall\exists\mathsf{AC}^0$, and show that it characterizes the provably total $\mathsf{NP}$ search problems of the bounded arithmetic theory corresponding to polynomial-time. Cook and Nguyen introduced a generic way of defining a bounded arithmetic theory $\mathsf{VC}$ for complexity classes $\mathsf{C}$ which can be obtained using a complete problem. For such $C$ we will define a new class $\mathsf{KPT}[\mathsf{C}]$ of $\forall\exists\mathsf{AC}^0$ search problems based on Student-Teacher games in which the student has computing power limited to $\mathsf{AC}^0$. We prove that $\mathsf{KPT}[\mathsf{C}]$ characterizes the provably total $\mathsf{NP}$ search problems of the bounded arithmetic theory corresponding to $\mathsf{C}$. All our characterizations are obtained via "new-style" witnessing theorems, where reductions are provable in a theory corresponding to $\mathsf{AC}^0$.

## 1 Introduction

The two-sorted bounded arithmetic theories $\mathsf{VC}$ [8] are well-known for their proof theoretic strength corresponding to complexity classes $\mathsf{C}$, for many $\mathsf{C}$ between $\mathsf{AC}^0$ and $\mathsf{PH}$. It is a fundamental open question in computer science whether any two complexity classes within the following sequence

$$\mathsf{AC}^0(6) \subseteq \mathsf{TC}^0 \subseteq \mathsf{NC}^1 \subseteq \mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{NC} \subseteq \mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PH},$$

are equal or not, a question which is a weaker version of the $\mathsf{P}$ versus $\mathsf{NP}$ question. Likewise, it is a fundamental open problem whether any of the corresponding bounded arithmetic theories are distinct. The difference in working with bounded arithmetic theories instead directly with computational classes is that the theories may possibly be shown to be distinct by combining logical considerations of provability along with computational complexity considerations. Another motivation for studying bounded arithmetic theories lies in their relation to propositional proof complexity, in that proving in bounded arithmetic theories corresponds to uniform provability in corresponding propositional proof systems [8]. In this paper, we give characterizations of the total search problems with $\mathsf{AC}^0$ graphs which are definable in bounded arithmetic theories $\mathsf{VC}$ for many $\mathsf{C}$ between $\mathsf{AC}^0$ and $\mathsf{P}$, where necessary reductions are proven in the weakest theory of bounded arithmetic $\mathsf{V}^0$ related to $\mathsf{AC}^0$ reasoning. In particular, we give improved "new-style" witnessing theorems for such theories.

A classical way to associate a theory $\mathcal{T}$ with a complexity class $\mathsf{C}$ is to show that the provably total functions in $\mathcal{T}$ are precisely the functions in the function class $\mathsf{FC}$ associated with $\mathsf{C}$. This assertion splits into two parts: the first, usually easier part shows that all function in $\mathsf{FC}$ can be suitably defined and proven total in $\mathcal{T}$ (and thus are called provably total); the second, usually more involved part often employs a witnessing theorem. Witnessing theorems in their original form were introduced by Buss [5] to show that existential statements with parameters provable in a bounded arithmetic theory $\mathcal{T}$ can be witnessed by functions from a corresponding function class, and that this witnessing property is provable in $\mathcal{T}$. For example, one result of Buss [5], adapted to the two-sorted bounded arithmetic theory $\mathsf{V}^1$, shows that given a $\forall\Sigma_1^B$-consequence of $\mathsf{V}^1$ we can find a polynomial time computable function witnessing the existential quantifier, where the correctness of the witnessing function is provable in $\mathsf{V}^1$. $\Sigma_1^B$ formulas have a certain syntactic form starting with a bounded existential quantifier — such formulas express exactly $\mathsf{NP}$ properties over the domain of natural numbers. We will denote the set of $\forall\Sigma_1^B$-consequences of a theory $\mathcal{T}$ by $\forall\Sigma_1^B(\mathcal{T})$.

Cook and Nguyen [8] have a generic way of defining a bounded arithmetic theory $\mathsf{VC}$ for those complexity classes $\mathsf{C}$ which can be obtained using a complete problem. They show that the set of provably total functions in $\mathsf{VC}$ corresponds to $\mathsf{FC}$. Their approach is to construct a universal conservative extension $\overline{\mathsf{VC}}$ of $\mathsf{VC}$, where the terms of $\overline{\mathsf{VC}}$ represent precisely functions in $\mathsf{FC}$. They then apply Herbrand's theorem to obtain their desired correspondence. The correctness of witnessing functions is proved in $\mathsf{VC}$.

Recently the focus has turned to "new-style" witnessing theorems, in which the correctness of the witnessing function is proved in a weaker theory than the one proving the $\forall\Sigma_1^{\mathrm{B}}$-statement [2–4, 15, 24]. Furthermore, the focus has shifted to search problems, i.e. multifunctions, instead of functions. The class $\mathsf{TFNP}$ [20] of total $\mathsf{NP}$ search problems, whose solutions are verifiable in polynomial-time, has been extensively studied from the point of view of complexity theory and contains a host of important problems like the Polynomial Local Search problems $\mathsf{PLS}$ [13]. For the theories $\mathsf{V}^i$ corresponding to the $i$-th level of the polynomial time hierarchy $\mathsf{PH}$, a host of characterizations of $\forall\Sigma_1^B(\mathsf{V}^i)$ have been given in terms of subclasses of $\mathsf{TFNP}$, using $\mathsf{V}^1$-provability for correctness of witnessing functions. For instance, Buss and Krajíček [6] characterized $\forall\Sigma_1^B(\mathsf{V}^2)$ in terms of $\mathsf{PLS}$; Krajíček, Skelley and Thapen [17] characterized $\forall\Sigma_1^B(\mathsf{V}^3)$ in terms of colored $\mathsf{PLS}$ (denoted $\mathsf{CPLS}$), and, for $0 < i$, Beckmann and Buss [2,3] characterized $\forall\Sigma_1^B(\mathsf{V}^{i+1})$ in terms of some relativized notion of $\mathsf{PLS}$ called $\Pi_i^p$-$\mathsf{PLS}$ with $\Pi_0^p$-goals, which we denote $\Pi_i^p$-$\mathsf{PLS}$ for the purpose of this introduction.

The aim of this paper is to provide characterizations of $\forall\Sigma_1^B(\mathsf{VC})$, for $\mathsf{C}$ below $\mathsf{P}$, and $\forall\Sigma_1^B(\mathsf{V}^1)$ in terms of subclasses of $\mathsf{TFNP}$, using new-style witnessing theorems in which the correctness of witnessing functions is provable in $\mathsf{V}^0$ — these new-style witnessing theorems are similar to the ones in [2–4,15,24], except for the correctness of witnessing functions that is now proved over a weaker theory. To achieve our aim, we define the class of *total* $\mathsf{N}$-$\mathsf{AC}^0$ *search problem* as those total $\mathsf{NP}$ search problems for which solutions are verifiable in $\mathsf{AC}^0$ rather than in $\mathsf{P}$. We denote this class as $\forall\exists\mathsf{AC}^0$. From the point of view of bounded arithmetic, $\forall\exists\mathsf{AC}^0$ can be identified with the set of all true $\forall\Sigma_1^B$-sentences. We will show that $\forall\exists\mathsf{AC}^0$ is equivalent to $\mathsf{TFNP}$ under $\mathsf{AC}^0$-many-one reductions, and that it contains many well-known problems like the problem of finding an inverse of a square matrix, the Stable Marriage problem, or the Maximal Independent Set problem.

Each known characterization of $\forall\Sigma_1^B(\mathsf{V}^i)$ as a subclass $\mathcal{S}$ of $\mathsf{TFNP}$, which can be found in the literature, is given in the form of a generic search principle $\mathcal{S}'(F_1,\ldots,F_n)$ such that $\mathcal{S}$ is obtained by instantiating $F_1,\ldots,F_n$ in $\mathcal{S}'$ with all possible choices of functions from $\mathsf{FP}$. It is then natural to consider $\mathsf{AC}^0$-$\mathcal{S}$ obtained by instantiating $\mathcal{S}'$ with functions from $\mathsf{FAC}^0$, and study the question whether $\mathsf{AC}^0$-$\mathcal{S}$ still characterizes $\forall\Sigma_1^B(\mathsf{V}^i)$ under $\mathsf{AC}^0$-many-one reducibility, provable in $\mathsf{V}^0$. For many characterisations, it is the case: Cook and Nguyen [8] showed that $\mathsf{AC}^0$-$\mathsf{PLS}$ characterizes $\forall\Sigma_1^B(\mathsf{V}^2)$ under $\mathsf{AC}^0$-many-one reducibility, provable in $\mathsf{V}^0$. Furthermore, it is shown in [23] that $\mathsf{AC}^0$-($\Pi_i^p$-$\mathsf{PLS}$) characterizes $\forall\Sigma_1^B(\mathsf{V}^{i+1})$ under $\mathsf{AC}^0$-many-one reducibility, provable in $\mathsf{V}^0$. From that latter result and the fact that $\mathsf{CPLS}$ characterizes $\forall\Sigma_1^B(\mathsf{V}^3)$, it follows directly that $\mathsf{AC}^0$-$\mathsf{CPLS}$ is $\mathsf{AC}^0$-many-one reducible to $\mathsf{AC}^0$-($\Pi_1^p$-$\mathsf{PLS}$). However, it is an open problem whether the other direction holds. We conjecture that $\mathsf{AC}^0$-$\mathsf{CPLS}$, based on $\mathsf{CPLS}$ in its literal form as defined in [17], is not $\mathsf{AC}^0$-many-one reducible to $\mathsf{AC}^0$-($\Pi_1^p$-$\mathsf{PLS}$) — we note here that proving this conjecture implies $\mathsf{P} \neq \mathsf{NP}$.

The outline of the paper is as follows: The next section is a preliminary section providing the necessary background. In Section 3, we introduce the class $\forall\exists\mathsf{AC}^0$ as a subclass of $\mathsf{TFNP}$, and show that it is equivalent to $\mathsf{TFNP}$ w.r.t. $\mathsf{AC}^0$-many-one reducibility, and that it contains a variety of well-known problems.

In Section 4, we define a class of total $\mathsf{N}$-$\mathsf{AC}^0$ search problems which we call $\mathsf{KPT}[\mathsf{C}]$. The class $\mathsf{KPT}[\mathsf{C}]$ is a class of total search problems motivated by the KPT witnessing theorem [16], where the process of finding a solution to an instance of a problem in $\mathsf{KPT}[\mathsf{C}]$ is carried out cooperatively between a student S and a teacher T: the student computes a potential solution, that either T accepts or rejects, and in the case that T rejects, then T must come up with a counterexample that S can then use in order to compute the next candidate solution. We use $\mathsf{KPT}[\mathsf{C}]$ in order to characterize $\forall\Sigma_1^B(\mathsf{VC})$, where the reduction is provable in $\mathsf{V}^0$, using a new-style witnessing theorem for $\mathsf{VC}$.

For $\forall\Sigma_1^B(\mathsf{V}^1)$, we introduce, in Section 5, a class of total $\mathsf{N}$-$\mathsf{AC}^0$ search problems that we call *Inflationary Polynomial Local Search* ($\mathsf{IPLS}$). The class $\mathsf{IPLS}$ is $\mathsf{AC}^0$-$\mathsf{PLS}$, but with some restriction on its neighborhood function in that this function must be inflationary. We show that $\mathsf{IPLS}$ has a complete problem class that we call Inflationary Iteration ($\mathsf{IITER}$), which is based on the iteration principle [7] (which can be viewed as the problem of finding a sink in an exponentially large directed acyclic graph). We show that $\mathsf{IITER}$ characterizes $\forall\Sigma_1^B(\mathsf{V}^1)$, where the reduction is provable in $\mathsf{V}^0$, using a new-style witnessing theorem for $\mathsf{V}^1$.

**Acknowledgement:** We would like to thank Noahi Eguchi. Our characterisation of $\forall\Sigma_1^B(\mathsf{V}^1)$ using inflationary iteration grew out of discussions with him on his attempt to capture $\mathsf{P}$ via a two-sorted theory using axioms on inductive definitions [10].

## 2 Preliminaries

We assume familiarity with bounded arithmetic in either its one-sorted [5] or two-sorted [8] setting, but we will quickly review all necessary notation and results used in this paper. We assume a basic understanding of complexity classes between $\mathsf{AC}^0$ and $\mathsf{P}$. For circuit complexity classes covered here, the uniformity we implicitly use is first-order uniformity [12, 21]. Overall, our exposition follows [8].

*The Language of Two-sorted Bounded Arithmetic.* In the two-sorted setting, there are two kinds of variables: *number variables* $x, y, z, \ldots$ of the first sort, intended to range over $\mathbb{N}$, and *string variables* $X, Y, Z, \ldots$ of the second sort, intended to range over finite subsets of $\mathbb{N}$. We interpret finite subsets of $\mathbb{N}$ as bit strings. The base language $\mathcal{L}_A^2$ consists of the usual symbols $0, 1, +, \cdot, \leq$ of arithmetic on $\mathbb{N}$, the function $|X|$ (whose intended meaning is 0 if $X$ is empty, and 1 plus the maximal element in $X$, otherwise), the set membership relation $\in$, and the relations $=_1$ and $=_2$, which are intended to be the equality on numbers and strings respectively. Since there will be no confusion, the subscripts in $=_i$ will often be omitted. We will usually write $X(i)$ for $i \in X$ and this is understood to denote the $i$-th bit in $X$.

*Terms* over $\mathcal{L}_A^2$ are built in the usual way. Note that the only string terms are string variables. If $\mathcal{L}_A^2$ is extended with additional string function symbols, then other string terms are built as usual. *Formulae* over $\mathcal{L}_A^2$ are built using $\wedge, \vee, \neg$, number quantifiers (i.e., $\exists x$ and $\forall x$) and string quantifiers (i.e., $\exists X$ and $\forall X$). *Bounded number quantifiers* are defined as usual, whereas the *bounded string quantifer* $(\exists X{\leq}t)\varphi$ stands for $\exists X(|X|{\leq}t \wedge \varphi)$ and $(\forall X{\leq}\, t)\varphi$ stands for $\forall X(|X|{\leq}t \supset \varphi)$, where $\varphi \supset \psi$ stands for $\neg\varphi \vee \psi$, and where $X$ does not appear in $t$.

The class $\Sigma_0^B$ (or $\Pi_0^B$) consists of those $\mathcal{L}_A^2$-formulae with no string quantifiers and only bounded number quantifiers. Inductively, $\Sigma_{i+1}^B$ consists of those formulae of the form $(\exists X_1{\leq}t_1)\ldots(\exists X_k{\leq}t_k)\varphi$, where $\varphi \in \Pi_i^B$, and $\Pi_{i+1}^B$ consists of those formulae of the form $(\forall X_1{\leq}t_1)\ldots(\forall X_k{\leq}t_k)\varphi$, where $\varphi \in \Sigma_i^B$. In general, we write $\Sigma_i^B(\mathcal{L})$ to denote the class $\Sigma_i^B$ that allows function and predicate symbols from $\mathcal{L} \cup \mathcal{L}_A^2$. Finally, a formula is in $\Sigma_1^1$ if it is of the form $(\exists X_1)\ldots(\exists X_k)\varphi$, where $\varphi \in \Sigma_0^B$.

*Two-sorted Complexity Classes.* Two-sorted complexity classes consist of relations $R(\boldsymbol{x}, \boldsymbol{X})$ that are taking arguments of both sorts, where the string arguments $\boldsymbol{X}$ are the main inputs and $\boldsymbol{x}$ only play an auxiliary role. However, for our purpose, it is convenient to assume that $R$ only takes a single string argument, as we can always pair $\boldsymbol{x}, \boldsymbol{X}$ into one single string $X$. The following fact will be frequently used:

**Theorem 1 ($\Sigma_0^B$ Representation Theorem [25]).** *A relation is in* $\mathsf{AC}^0$ *if, and only if, it is represented by some* $\Sigma_0^B$*-formula.*

For each two-sorted complexity $\mathsf{C}$ of interest, there is a corresponding function class $\mathsf{FC}$. For a string function $F(X)$ to be in $\mathsf{FC}$, $F(X)$ needs to be *p-bounded* (i.e., $|F(X)|$ is bounded by some polynomial in $|X|$) and its *bit graph* (i.e., the relation $B_F(i, X)$ that holds if, and only if, the $i$-th bit of $F(X)$ is 1) is in $\mathsf{C}$.

*Two-sorted Bounded Arithmetic Theories.* The theory $\mathsf{BASIC}$ consists of some finite set of axioms defining the non-logical symbols in $\mathcal{L}_A^2$. Then, for $i = 0, 1$, the theory $\mathsf{V}^i$ is $\mathsf{BASIC}$ plus the $\Sigma_i^B$*-comprehension axiom scheme*, denoted $\Sigma_i^B$-$\mathsf{COMP}$, which is $(\exists X{\le}y)(\forall z < y)[X(z) \leftrightarrow \varphi(z)]$, where $\varphi \in \Sigma_i^B$ and $X$ does not occur free in $\varphi$. For $\Phi = \Sigma_i^B$, the following axiom schemes are provable in $\mathsf{V}^i$:

$$\begin{array}{ll} \Phi\text{-}\mathsf{IND}: & [\varphi(0) \wedge \forall x(\varphi(x) \supset \varphi(x+1))] \supset \forall x \varphi(x), \\ \Phi\text{-}\mathsf{MAX}: & \varphi(0) \supset (\exists x{\le}y)(\varphi(x) \wedge (\forall z{\le}y)(x < z \supset \neg\varphi(z))). \end{array}$$

We will usually be working with a universal conservative extension $\overline{\mathsf{V}}^0$ of $\mathsf{V}^0$, whose language $\mathcal{L}_{\overline{\mathsf{V}}^0}$ has a symbol for each function in $\mathsf{FAC}^0$.

A string function $F(X)$ is *provably total in a theory* $\mathcal{T}$ if its graph $Y = F(X)$ is represented by a $\Sigma_1^B$-formula $\varphi(X, Y)$ and $\mathcal{T}$ proves $\forall X \exists! Y \varphi(X, Y)$.

For certain complexity classes $\mathsf{C}$ within $\mathsf{P}$, Cook and Nguyen [8] showed how to construct a theory $\mathsf{VC}$ corresponding to $\mathsf{FC}$ (i.e., the provably total functions in $\mathsf{VC}$ are precisely those in $\mathsf{FC}$). Before we give the definition of $\mathsf{VC}$, let us first review the notion of $\mathsf{AC}^0$*-reduction.*

A relation $R$ is $\mathsf{AC}^0$*-reducible* to a collection $\mathcal{L}$ of functions if there is a sequence of string functions $G_1, \ldots, G_n$ such that each $G_i$ is p-bounded and its bit graph is represented by a $\Sigma_0^B(\mathcal{L} \cup \{G_1, \ldots, G_{i-1}\})$-formula and $R$ is represented by a $\Sigma_0^B(\mathcal{L} \cup \{G_1, \ldots, G_n\})$-formula.

For a two-sorted complexity class $\mathsf{C}$ of interest, fix a function $F$ so that $\mathsf{C}$ is the class of all relations that are $\mathsf{AC}^0$-reducible to $\{F\}$ (we keep $F$ fixed in what follows) and so that there is a $\Sigma_0^B$-formula $\delta_F(X, Y)$ and some $\mathcal{L}_A^2$-term $t(X)$ such that the graph $Y = F(X)$ of $F$ is represented by $|Y|{\le}t(X) \wedge \delta_F(X, Y)$. Furthermore, assume that $\mathsf{V}^0$ proves the uniqueness of the value of $F$. Let the *aggregate function* $F^*(b, X)$ of $F(X)$ be the function that gathers the values of $F$ for a polynomially long sequence of arguments. Thus, $F^*$ is defined so that

$$\forall i{<}b, F^*(b, X)^{[i]} = F(X^{[i]}),$$

where $X^{[i]}(j)$ holds if and only if $j < |X| \wedge X(i, j)$ holds — we obtain arrays of more than one dimension by using a suitable pairing function $\langle x, y \rangle$ on numbers $x, y$, e.g. $X(i, j)$ stands for $X(\langle i, j \rangle)$. Let $G_F(b, X, Y)$ be a $\Sigma_0^B$-formula that represents the graph of $F^*(b, X)$. The theory $\mathsf{VC}$ is then $\mathsf{V}^0$ plus the $\Sigma_1^B$-statement $(\exists Y \leq \langle b, t\rangle) G_F(b, X, Y)$.

*Two-sorted Search Problems.* A *total search problem* (or simply a *search problem*) is a binary relation $R(X, Y)$ such that $\forall X \exists Y R(X, Y)$ holds (we also call $R$ the *graph* of the search problem). The search task associated with $R$ is the following: given an *instance* $X$ of $R$, find a *solution* $Y$ such that $R(X, Y)$ holds.

The class $\mathsf{TFNP}$ [20] consists of those search problems $R(X, Y)$ such that $R$ is polynomial-time computable and $|Y|$ is bounded by a polynomial in $|X|$.

Let $R$ be a search problem. $R$ is *provably total in a theory* $\mathcal{T}$ if the graph of $R$ is represented by a $\Sigma_1^B$-formula $\varphi(X, Y)$ and $\mathcal{T}$ proves $\forall X \exists Y \varphi(X, Y)$.

Let $\mathsf{C}$ be a complexity class. Then a search problem $R$ is $\mathsf{C}$-*many-one reducible* to a search problem $Q$, denoted $R \leq_m^{\mathsf{C}} Q$, if there are functions $F, G \in \mathsf{FC}$ such that $Q(F(X), Y)$ implies $R(X, G(X, Y))$, for all $X, Y$. For two classes $\Gamma$ and $\Delta$ of search problems, we say that $\Gamma$ is $\mathsf{C}$-many-one reducible to $\Delta$, denoted $\Gamma \leq_m^{\mathsf{C}} \Delta$, if for all $R \in \Gamma$, there is some $Q \in \Delta$ such that $R \leq_m^{\mathsf{C}} Q$. We say that $\Gamma$ and $\Delta$ are $\mathsf{C}$-*equivalent* if $\Gamma \leq_m^{\mathsf{C}} \Delta$ and $\Delta \leq_m^{\mathsf{C}} \Gamma$. Finally, we say that $\Gamma$ is $\mathsf{C}$-many-one complete for $\Delta$ if $\Gamma \subseteq \Delta$ and $\Delta \leq_m^{\mathsf{C}} \Gamma$.

## 3 The Class $\forall\exists\mathsf{AC}^0$

**Definition 2.** *A search problem $R$ is said to be in $\forall\exists\mathsf{AC}^0$ if $R$ can be expressed as a $\mathsf{TFNP}$ problem with $\mathsf{AC}^0$ graph.*

We observe that $\forall\exists\mathsf{AC}^0$ is $\mathsf{AC}^0$-many-one equivalent to $\mathsf{TFNP}$. To see this, note that the statement “string $W$ is a valid encoding of the full computation of a fixed polynomial-time Turing machine on a given input” can be expressed by a $\Sigma_0^B$-formula. From that, and the $\Sigma_0^B$ representation theorem, we can turn $R$ into a $\forall\exists\mathsf{AC}^0$ problem $Q$, whose solution can then be mapped into a solution for $R$.

Another motivation for studying $\forall\exists\mathsf{AC}^0$ is the fact that it contains a host of well-known problems. As already noted in the introduction, Cook and Nguyen [8] show that $\mathsf{PLS}$ is equivalent to $\mathsf{AC}^0$-$\mathsf{PLS}$. Another example [8] stems from linear algebra: $(\star)$ given an $n \times n$ matrix $A$ over some field, find an $n \times n$ matrix $B \neq 0$ such that $AB = I \vee AB = 0$. Observe that the provability of $(\star)$ in $\mathsf{VNC}^1$ is still an open problem.

In what follows, we demonstrate that the Stable Marriage problem and the Maximal Independent Set problem are $\forall\exists\mathsf{AC}^0$ problems.

*The Stable Marriage Problem.* The Stable Marriage problem (SM) was first introduced by Gale and Shapley [11]. Besides having practical applications, SM is of importance for the $\mathsf{NC}$ vs $\mathsf{P}$ question: It has been shown that SM is complete for Subramanian's complexity class $\mathsf{CC}$ [19], a subclass of $\mathsf{P}$ based on comparator circuits. Furthermore, Cook, Filmus and Lê [9] gave strong evidence that $\mathsf{CC}$ and $\mathsf{NC}$, which is also a subclass of $\mathsf{P}$, are incomparable.

An instance of size $n$ of SM involves two sets of $n$ men and $n$ women. Associated with each person $p$ is a strictly ordered preference list $l = q_1, \dots, q_n$ containing all the members of the opposite sex: person $p$ prefers person $q$ to $r$ if, and only if, there is a $q_i$ and a $q_j$ in $l$ such that $q_i = q$ and $q_j = r$ and $i < j$.

Given an instance of SM, a *matching* $M$ is a bijection between the sets of men and women. A man $m$ and a woman $w$ are called *partners in* $M$ if, and only if, they are matched in $M$; we write $p_M(m)$ to denote the partner of $m$ in $M$ (similarly for $p_M(w)$). A matching $M$ is called *unstable* if there is a man $m$ and a woman $w$ such that $m$ and $w$ are not partners in $M$, but $m$ prefers $w$ to $p_M(m)$ and $w$ prefers $m$ to $p_M(w)$; otherwise, $M$ is called *stable*.

The search task associated with SM is as follows: given an instance of SM, find a matching that is stable. Gale and Shapley showed that such a stable matching always exists. Hence, SM is a total search problem.

We argue that the SM search problem is in $\forall\exists\mathsf{AC}^0$. Let $\{0, 1, \dots, n{-}1\}$ corresponds to the set of men and $\{n, n{+}1, \dots, 2n{-}1\}$ to the set of women. Then a preference list for a person $p$ can be encoded in bounded arithmetic as a three-dimensional array $L(p, j, q_j)$, which holds if and only if $q_j$ sits at $j$-th position in person $p$'s preference list. A matching can be encoded as a two-dimensional array $M(p, q)$ with size bounded by $\langle n, n\rangle$. It is easy to see that the statement "$M$ is a stable matching for $(n, L)$" can be expressed as a $\Sigma_0^B$-formula. Thus, by the representation theorem for $\Sigma_0^B$, SM is a $\forall\exists\mathsf{AC}^0$ search problem.

*The Maximal Independent Set Problem.* Another example for a problem in $\forall\exists\mathsf{AC}^0$ is the Maximal Independent Set problem (MIS), which is a fundamental problem in Graph Theory since several important problems can be reduced to it. For instance, Karp and Widgerson [14] show that the maximal set packing and the maximal matching problems are $\mathsf{NC}^1$-reducible to MIS, and that the 2-satisfiability problem is $\mathsf{NC}^2$-reducible to MIS. In terms of its complexity, Luby [18] and, independently, Alon et al. [1] proved the existence of $\mathsf{NC}^2$-algorithms that solve MIS. However, it is still open whether MIS can be solved by an $\mathsf{NC}^1$-algorithm.

Let $G$ be a graph. An *independent set* in $G$ is a set of vertices such that no two of them are adjacent. A *maximal independent set* $I$ in $G$ is an independent set such that for every vertex $v$ in $G$, either $v$ belongs to $I$ or $v$ has at least one neighbor vertex that belongs to $I$.

The MIS problem is the following computational problem: given a graph $G$, find a maximal independent set in $G$. MIS is a total search problem, since for a given graph $G$, a maximal independent set $I$ is always guaranteed to exist.

The MIS problem is in $\forall\exists\mathsf{AC}^0$. For that, we specify a graph $G$ by a pair $(n, E)$, where $0, 1, \dots, n{-}1$ are the vertices in $G$ and $E(u, v)$ holds if, and only if, there is an edge between vertex $u$ and $v$ in $G$. Then the statement "$U$ is a maximal independent set in $G$" can be written as a $\Sigma_0^B$-formula. Note that the size of $U$ is bounded by $n$.

## 4 The Class $\mathsf{KPT}[\mathsf{C}]$ and $\mathsf{VC}$

For this section, we fix a function $F(X)$ in $\mathsf{FC}$ so that $\mathsf{C}$ is the $\mathsf{AC}^0$-closure of $F$. Let $G_F(b, X, Y)$ be a $\Sigma_0^B$-formula that states that $Y$ is the value for the aggregate function $F^*(b, X)$ of $F(X)$. In the following we will identify $F$ with $F^*$ — it will be clear from the context which of the two is meant.

The following lemma is an application of the KPT witnessing theorem [16]. It says that if the theory $\mathsf{VC}$ proves $\forall X \exists Y \varphi(X, Y)$, where $\varphi$ is a $\Sigma_0^B$-formula, then for a given $X$, we can construct a witness for $\exists Y \varphi(X, Y)$ in a collaborative fashion by using $F$ and some $\mathsf{AC}^0$-functions $F_1(X), \ldots, F_k(X, Z_1, \ldots, F_{k-1})$.

**Lemma 3.** *Let $\varphi(X, Y)$ be a $\Sigma_0^B$-formula and $\theta(X, Y, Z)$ denote*

$$G_F(|Y^{[1]}|, Y^{[2]}, Z) \supset \varphi(X, Y^{[0]}).$$

*Suppose that the theory $\mathsf{VC}$ proves $\forall X \exists Y \varphi(X, Y)$. Then there exist some $\mathsf{AC}^0$-functions $F_1(X), \ldots, F_k(X, Z_1, \ldots, Z_{k-1})$ such that $\overline{\mathsf{V}}^0$ proves*

$$\bigvee_{i=1}^{k} \theta(X, F_i(X, Z_1, \ldots, Z_{i-1}), Z_i). \tag{1}$$

*Proof.* The theory $\mathsf{VC}$ is defined as $\mathsf{V}^0$ plus a $\forall \Sigma_1^B$ sentence expressing the existence of a solution of a complete problem in $\mathsf{C}$. Applying the deduction theorem of first-order logic to a $\mathsf{VC}$ proof of $\forall X \exists Y \varphi(X, Y)$ and working in a conservative extension $\overline{\mathsf{V}}^0$ of $\mathsf{V}^0$, we obtain a $\overline{\mathsf{V}}^0$ proof of a statement to which the KPT witnessing theorem is applicable. □

We can think of Lemma 3 as a game about the formula

$$\exists Y \forall Z \theta(X, Y, Z) \tag{2}$$

between a student E and a teacher U, where E's role is to find a witness $Y$ to the existential quantifier in (2), but has computing power limited to $\mathsf{FAC}^0$, whereas U's role is to find a counterexample $Z$ to the universal quantifier in (2), if it exists. More precisely, the game starts with E producing a potential witness $Y_1 = F_1(X)$, which U either approves or rejects – U approves $Y_1$ if $\forall Z \theta(X, Y_1, Z)$ is true, otherwise U rejects $Y_1$ and has to provide a counterexample $Z_1$ such that $\neg\theta(X, Y_1, Z_1)$ holds, that is to say, $Z_1 = F(|Y_1^{[1]}|, Y_1^{[2]})$ and $\neg\varphi(X, Y_1^{[0]})$ is true. If U rejects $Y_1$ by producing a counterexample $Z_1$, then E can use $Z_1$ in order to compute the next potential witness $Y_2 = F_2(X, Z_1)$. Again, either U approves or rejects $Y_2$. As before, if U rejects $Y_2$, then he has to provide E with a counterexample $Z_2$. This process will continue for at most $k$ steps, after which E finds a witness to the existential quantifier in (2). Note that E cannot compute $F$, since $F$ is beyond E's computing power.

In the student-teacher game interpretation of Lemma 3, the student is always guaranteed to find a value $Y$ such that $\forall Z \theta(X, Y, Z)$ holds after at most $k$

steps. However, if $\varphi(X,Y)$ and $F_1(X),\ldots,F_k(X,Z_1,\ldots,F_k)$ were to be picked arbitrarily, then there is no guarantee that the student would still win, that is to say that he would find a value $Y$ that satisfies $\forall Z\theta(X,Y,Z)$. This is because, for an arbitrary $X$, it is not always the case that there is a $Y$ such that $\varphi(X,Y)$ is true. Also, even if $\forall X\exists Y\varphi(X,Y)$ happened to be true, nothing tells us that $\forall Z\theta(X,F_j(X,Z_1,\ldots,Z_{j-1}),Z)$ will hold, for some $F_j$ in $F_1,\ldots,F_k$. The class $\mathsf{KPT}[\mathsf{C}]$ will be defined with the student-teacher game interpretation of Lemma 3 in mind, but where $\varphi$ and $F_1,\ldots,F_k$ are given arbitrarily. Therefore, some care needs to be taken when defining $\mathsf{KPT}[\mathsf{C}]$ in order to ensure its totality. More precisely, if in case there is no $F_j$ in $F_1,\ldots,F_k$ such that $\forall Z\theta(X,F_j(X,Z_1,\ldots,Z_{j-1}),Z)$ holds, then we will just force part of the formula that defines the graph of a $\mathsf{KPT}[\mathsf{C}]$ search problem to be trivially true.

In the following, we write $\hat{F}_i(X,W)$ for $F_i(X,W^{[1]},\ldots,W^{[i-1]})$.

**Definition 4.** *A* $\mathsf{KPT}[\mathsf{C}]$ *search problem* $Q(X,W)$ *is specified by a* $k\in\mathbb{N}$, *a* $\Sigma_0^B$-*formula* $\varphi(X,Y)$ *and* $\mathsf{AC}^0$-*functions* $F_1(X),\ldots,F_k(X,Z_1,\ldots,Z_{k-1})$. *A string* $W$ *is a solution to an instance* $X$ *of* $Q$ *if, and only if, the following hold:*

1. *For all* $i$ *from* 1 *to* $k$,
$$G_F(|\hat{F}_i(X,W)^{[1]}|,\hat{F}_i(X,W)^{[2]},W^{[i]}). \tag{3}$$
2. *There exists an* $i$ *between* 1 *and* $k$ *such that the following holds:*
$$[W^{[0]}=\hat{F}_i(X,W)^{[0]}\wedge[i<k\supset\varphi(X,W^{[0]})]\wedge\bigwedge_{j<i}\neg\varphi(X,\hat{F}_j(X,W)^{[0]}). \tag{4}$$

*We will call* $\varphi$ *and* $F_1,\ldots,F_k$ *the* components *of* $Q$.

We will explain (3) and (4) here. The formula in (3) says that $W^{[i]}$ stores the counterexample $F(|\hat{F}_i(X,W)^{[1]}|,\hat{F}_i(X,W)^{[2]})$ given by the teacher to the student – in fact, note that even if $\varphi(X,\hat{F}_i(X,W)^{[0]})$ is true, then $W^{[i]}$ always stores $F(|\hat{F}_i(X,W)^{[1]}|,\hat{F}_i(X,W)^{[2]})$. Next, the formula in (4) guarantees the totality of $Q$. If there is no $F_j$ in $F_1,\ldots,F_k$ such that $\varphi(X,\hat{F}_j(X,W)^{[0]})$ is true, then the above formula trivially holds by taking $i=k$ and $W^{[0]}$ to be equal to $\hat{F}_i(X,W)^{[0]}$, and in case there is an $F_i$ in $F_1,\ldots,F_k$ such that $\varphi(X,\hat{F}_i(X,W)^{[0]})$ is true, then the formula in (4) tells us that $i$ is the least value in $\{1,\ldots,k\}$ such that $\varphi(X,\hat{F}_i(X,W)^{[0]})$ is true. Finally, using the $\Sigma_0^B$ representation theorem, it is easy to see that the graph of a $\mathsf{KPT}[\mathsf{C}]$ search problem is in $\mathsf{AC}^0$.

**Lemma 5.** *Let* $Q$ *be a* $\mathsf{KPT}[\mathsf{C}]$ *search problem. Then* $\mathsf{VC}$ *proves that* $Q$ *is total.*

*Proof.* The proof is a straightforward case analysis. □

The next theorem is a converse of Lemma 5.

**Theorem 6 (New-style Witnessing Theorem for** $\mathsf{VC}$**).** *Let* $\varphi(X,Y)$ *be a* $\Sigma_1^1$-*formula such that* $\mathsf{VC}$ *proves* $\forall X\exists Y\varphi(X,Y)$. *Then there is a* $\mathsf{KPT}[\mathsf{C}]$ *search problem* $Q$ *and an* $\mathsf{AC}^0$-*function* $H$ *such that* $\overline{\mathsf{V}}^0$ *proves*
$$Q(X,W)\supset\varphi(X,H(X,W)). \tag{5}$$

*Proof.* W.l.o.g. we can assume that $\varphi \in \Sigma_0^B$. By Lemma 3, we obtain some $\mathsf{AC}^0$-functions $F_1(X), \ldots, F_k(X, Z_1, \ldots, Z_k)$ such that $\overline{\mathsf{V}}^0$ proves

$$\forall X \forall Z_1 \ldots \forall Z_k \bigvee_{i=1}^{k} \theta(X, F_i(X, Z_1, \ldots, Z_{i-1}), Z_i), \tag{6}$$

where $\theta(X, Y, Z)$ is the formula $G_F(|Y^{[1]}|, Y^{[2]}, Z) \supset \varphi(X, Y^{[0]})$. Define a $\mathsf{KPT}[\mathsf{C}]$ search problem $Q$ using $\varphi$ and $F_1, \ldots, F_k$.

Arguing in $\overline{\mathsf{V}}^0$, we want to show (5). Suppose that $Q(X, W)$ holds. Then (4) is true for some $i \leq k$. If $i < k$, then $\varphi(X, W^{[0]})$ follows directly. Otherwise, $i = k$, and we have that

$$\bigwedge_{j<k} \neg\varphi(X, F_j(X, W^{[1,\ldots,j-1]})^{[0]})$$

holds. Combining this with (6), it is easy to see that $\varphi(X, F_k(X, W^{[1,\ldots,k-1]})^{[0]})$ and $W^{[0]} = F_k(X, W^{[1,\ldots,k-1]})^{[0]}$. By letting $H(X, W) = W^{[0]}$ the assertion follows. □

Combining Lemma 5, Theorem 6 and the fact that $\overline{\mathsf{V}}^0$ is a universal conservative extension of $\mathsf{V}^0$, we obtain the following theorem:

**Theorem 7.** $\mathsf{KPT}[\mathsf{C}]$ *is* $\mathsf{AC}^0$*-many-one complete for the provably total* $\mathsf{NP}$*search problems in* $\mathsf{VC}$*. Furthermore, the reduction is provable in the theory* $\mathsf{V}^0$*.*

## 5 The Class of Inflationary Iteration Problems and $\mathsf{V}^1$

Finite subsets of $\mathbb{N}$ can be viewed as finite binary strings with no leading zeros by letting an element in the set indicate whether the corresponding bit in the string is set to one. Using this identification of strings with finite sets, we define the notion of an "inflationary" string function:

**Definition 8.** *A string function $F(X, Z)$ is said to be* inflationary *if, and only if, for all $X, Z$, we have that $Z \subseteq F(X, Z)$.*

The complexity class $\mathsf{PLS}$ [13] is based on the principle that every finite directed acyclic graph has a sink. Additionally, if the local search function is given by an inflationary $\mathsf{FAC}^0$-function, then we obtain the class $\mathsf{IPLS}$:

**Definition 9.** *An* $\mathsf{IPLS}$ *problem $Q(X, Y)$ is specified by the following:*

1. *An* $\mathsf{AC}^0$*-relation $F_Q(X, Y)$ and an $\mathcal{L}_A^2$-term $t(X)$ such that the following conditions hold:*

$$F_Q(X, \emptyset),$$
$$F_Q(X, Z) \supset |Z| \leq t(X).$$

*The set of all $Y$ with $F_Q(X, Y)$ is the set of all* candidate solutions *for $Q$ on instance $X$.*

*2. An* $\mathsf{FAC}^0$*-function* $P_Q(X, Y)$*, which computes the* profit *of* $Y$*, and an inflationary* $\mathsf{FAC}^0$*-function* $N_Q(X, Y)$*, which computes the* neighbor *of* $Y$*, such that for any* $Y$ *that satisfies* $F_Q(X, Y)$*, the following holds:*

$$[N_Q(X, Y) = Y] \vee [F_Q(X, N_Q(X, Y)) \wedge P_Q(X, Y) < P_Q(X, N_Q(X, Y))].$$

*where* $X < Y$ *is the less than relation on strings. A solution to an instance* $X$ *of* $Q$ *is any string* $Y$ *such that*

$$F_Q(X, Y) \wedge N_Q(X, Y) = Y$$

*holds. We will usually refer to* $F_Q, P_Q, N_Q$ *and* $t$ *as the* components *of* $Q$*.*

Any $\mathsf{IPLS}$ problem is a total search problem. Moreover, checking if a string is a solution to an instance of an $\mathsf{IPLS}$ problem is an $\mathsf{AC}^0$-property. Thus every $\mathsf{IPLS}$ problem is a $\forall\exists\mathsf{AC}^0$ search problem.

We will next introduce the class $\mathsf{IITER}$, which is based on the iteration principle [7]. The iteration principle is also based on the fact that every finite directed acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ has a sink. In an exponential sized graph $\mathcal{G}$, it may take exponentially many steps to find a sink following a path through the graph. However, if the edge relation is given by an inflationary function, paths are bound to be of polynomial length.

**Definition 10.** *An* $\mathsf{IITER}$ $Q_F(X, Y)$ *is specified by an inflationary* $\mathsf{FAC}^0$*-function* $F(X, Y)$ *and an* $\mathcal{L}_A^2$*-term* $t(X)$*. A solution to an instance* $X$ *of* $Q_F$ *is a string* $Y$ *satisfying the formula* $\psi_F(X, Y)$*, which is (omitting the parameter* $X$*) given as follows:*

$$\begin{aligned}&[Y = \emptyset \wedge F(Y) = Y] \vee \\ &\qquad [|Y| \leq t \wedge Y < F(Y) \wedge [t < |F(Y)| \vee F(F(Y)) \leq F(Y)]]. \qquad (7)\end{aligned}$$

*We will usually refer to* $F$ *and* $t$ *as the components of* $Q_F$*. We say that a string* $Y$ *is a* candidate solution *to* $Q_F$ *on instance* $X$ *if* $Y$ *satisfies the following condition:*

$$|Y| \leq t \wedge (Y = \emptyset \vee Y < F(X, Y)). \qquad (8)$$

It is known that the iteration principle is $\mathsf{AC}^0$-many-one complete for $\mathsf{PLS}$ [8,22]. In what follows, we show that $\mathsf{IITER}$ is $\mathsf{AC}^0$-many-one complete for $\mathsf{IPLS}$.

**Lemma 11.** *Every* $\mathsf{IITER}$ *problem is an* $\mathsf{IPLS}$ *problem.*

*Proof.* The proof is a direct adaptation of the one for [8, Lemma VIII.5.7]. □

**Lemma 12.** *Every* $\mathsf{IPLS}$ *problem is* $\mathsf{AC}^0$*-many-one reducible to an* $\mathsf{IITER}$ *problem.*

*Proof.* The proof is easier than the one for [8, Theorem VIII.5.8]. Observe that $X \subseteq Y$ implies $X \leq Y$. Given a $\mathsf{IPLS}$ problem $Q$ with components $F_Q, N_Q, P_Q$ and $t$, we can define an $\mathsf{IITER}$ problem $Q_F$ using $N_Q$ on $F_Q$ and $t$. Given an instance $X$, it is easy to see that a solution $Y$ to $Q_F$ is one step beyond a solution to $Q$, the latter being given by $N_Q(X, Y)$. □

From Lemmas 11 and 12, we immediately obtain the following corollary:

**Corollary 13.** $\mathsf{IITER}$ *is* $\mathsf{AC}^0$*-many-one complete for* $\mathsf{IPLS}$. □

**Theorem 14.** *Let $Q$ be an* $\mathsf{IITER}$ *problem. Then $Q$ is provably total in* $\mathsf{V}^1$.

*Proof.* Let $Q$ be an $\mathsf{IITER}$ problem with components $F$ and $t$. Let $\mathrm{numones}(y, Y)$ be the function that computes the total number of elements in $Y$ that are strictly less than $y$. The function numones is a polytime function definable in $\mathsf{V}^1$. Consider $\eta(X, Z)$ to be the formula $Z = \emptyset \vee Z < F(X, Z)$ and $\bar{\eta}(X, z)$ to be

$$\exists Z \leq t(X)[z = \mathrm{numones}(Z) \wedge \eta(X, Z)].$$

Then $\eta$ is in $\Sigma_0^{\mathrm{B}}$, and $\bar{\eta}$ equivalent to a formula in $\Sigma_1^{\mathrm{B}}$. Using maximisation on $z$, which is available in $\mathsf{V}^1$, we obtain a $Z$ with maximal number of elements amongst those satisfying $\eta$. It is easy to see that this $Z$ is a solution to $Q$. □

The converse of Theorem 14 is the new-style witnessing theorem for $\mathsf{V}^1$.

**Theorem 15 (New-style Witnessing Theorem for $\mathsf{V}^1$).** *Suppose that $\varphi(X, Y)$ is a $\Sigma_1^1$-formula such that*

$$\mathsf{V}^1 \vdash \forall X \exists Y \varphi(X, Y).$$

*Then there is an* $\mathsf{IITER}$ *problem $Q_F$ with graph $\psi_F(X, Y)$ (as in (7)), and an* $\mathsf{FAC}^0$*-function $G(X, Y)$, such that*

$$\overline{\mathsf{V}}^0 \vdash \psi_F(X, Y) \supset \varphi(X, G(X, Y)). \tag{9}$$

*Proof (Proof Idea).* The idea of this proof is to construct the required search problem by induction on an appropriate sequent calculus derivation of the original statement. For this we will have to redefine $\mathsf{V}^1$ in terms of an appropriate induction scheme, and use a corresponding inference rule in the definition of the sequent calculus. The main step in the construction is to deal with applications of this induction rule. From an $\mathsf{IITER}$ problem given for the premise of the induction rule, we obtain one for the conclusion by iterating the former polynomially many times, creating in each step an additional entry in a polynomially long board in order to guarantee the result to be inflationary.

Further details can be found in Appendix A. □

Combining Theorems 14 and 15 and the fact that $\overline{\mathsf{V}}^0$ is a universal conservative extension of $\mathsf{V}^0$, we obtain the following corollary:

**Corollary 16.** $\mathsf{IITER}$ *is* $\mathsf{AC}^0$*-many-one complete for the provably total* $\mathsf{NP}$*search problems in* $\mathsf{V}^1$*. Furthermore, the reduction is provable in the theory* $\mathsf{V}^0$. □

## References

1. Alon, N., Babai, L., Itai, A.: A fast and simple randomized parallel algorithm for the maximal independent set problem. J. Algorithms 7(4), 567–583 (Dec 1986), http://dx.doi.org/10.1016/0196-6774(86)90019-2
2. Beckmann, A., Buss, S.R.: Polynomial local search in the polynomial hierarchy and witnessing in fragments of bounded arithmetic. J. Math. Log. 9(1), 103–138 (2009), http://dx.doi.org/10.1142/S0219061309000847
3. Beckmann, A., Buss, S.R.: Characterising definable search problems in bounded arithmetic via proof notations. In: Ways of proof theory, Ontos Math. Log., vol. 2, pp. 65–133. Ontos Verlag, Heusenstamm (2010)
4. Beckmann, A., Buss, S.R.: Improved witnessing and local improvement principles for second-order bounded arithmetic. ACM Trans. Comput. Log. 15(1), Art. 2, 35 (2014), http://dx.doi.org/10.1145/2559950
5. Buss, S.R.: Bounded arithmetic, Studies in Proof Theory. Lecture Notes, vol. 3. Bibliopolis, Naples (1986)
6. Buss, S.R., Krajíček, J.: An application of Boolean complexity to separation problems in bounded arithmetic. Proc. London Math. Soc. (3) 69(1), 1–21 (1994), http://dx.doi.org/10.1112/plms/s3-69.1.1
7. Chiari, M., Krajíček, J.: Witnessing functions in bounded arithmetic and search problems. J. Symbolic Logic 63(3), 1095–1115 (1998), http://dx.doi.org/10.2307/2586729
8. Cook, S., Nguyen, P.: Logical Foundations of Proof Complexity. Cambridge University Press, New York, NY, USA, 1st edn. (2010)
9. Cook, S.A., Filmus, Y., Lê, D.T.M.: The complexity of the comparator circuit value problem. ACM Trans. Comput. Theory 6(4), Art. 15, 44 (2014), http://dx.doi.org/10.1145/2635822
10. Eguchi, N.: Characterising Complexity Classes by Inductive Definitions in Bounded Arithmetic. ArXiv e-prints (Jun 2013)
11. Gale, D., Shapley, L.S.: College admissions and the stability of marriage. Amer. Math. Monthly 120(5), 386–391 (2013), http://dx.doi.org/10.4169/amer.math.monthly.120.05.386, reprint of MR1531503
12. Immerman, N.: Descriptive complexity. Graduate Texts in Computer Science, Springer-Verlag, New York (1999), http://dx.doi.org/10.1007/978-1-4612-0539-5
13. Johnson, D.S., Papadimitriou, C.H., Yannakakis, M.: How easy is local search? J. Comput. System Sci. 37(1), 79–100 (1988), http://dx.doi.org/10.1016/0022-0000(88)90046-3, 26th IEEE Conference on Foundations of Computer Science (Portland, OR, 1985)
14. Karp, R.M., Wigderson, A.: A fast parallel algorithm for the maximal independent set problem. J. Assoc. Comput. Mach. 32(4), 762–773 (1985), http://dx.doi.org/10.1145/4221.4226
15. Kołodziejczyk, L.A., Nguyen, P., Thapen, N.: The provably total NP search problems of weak second order bounded arithmetic. Ann. Pure Appl. Logic 162(6), 419–446 (2011), http://dx.doi.org/10.1016/j.apal.2010.12.002
16. Krajíček, J., Pudlák, P., Takeuti, G.: Bounded arithmetic and the polynomial hierarchy. Ann. Pure Appl. Logic 52(1-2), 143–153 (1991), http://dx.doi.org/10.1016/0168-0072(91)90043-L, international Symposium on Mathematical Logic and its Applications (Nagoya, 1988)
17. Krajíček, J., Skelley, A., Thapen, N.: NP search problems in low fragments of bounded arithmetic. J. Symbolic Logic 72(2), 649–672 (2007), http://dx.doi.org/10.2178/jsl/1185803628

18. Luby, M.: A simple parallel algorithm for the maximal independent set problem. In: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing. pp. 1–10. STOC '85, ACM, New York, NY, USA (1985), http://doi.acm.org/10.1145/22145.22146
19. Mayr, E.W., Subramanian, A.: The complexity of circuit value and network stability. J. Comput. System Sci. 44(2), 302–323 (1992), http://dx.doi.org/10.1016/0022-0000(92)90024-D
20. Megiddo, N., Papadimitriou, C.H.: On total functions, existence theorems and computational complexity. Theoret. Comput. Sci. 81(2, Algorithms Automat. Complexity Games), 317–324 (1991), http://dx.doi.org/10.1016/0304-3975(91)90200-L
21. Mix-Barrington, D.A., Immerman, N., Straubing, H.: On uniformity within nc1. J. Comput. Syst. Sci. 41(3), 274–306 (Dec 1990), http://dx.doi.org/10.1016/0022-0000(90)90022-D
22. Morioka, T.: Classification of search problems and their definability in bounded arithmetic (2001)
23. Razafindrakoto, J.J.: Witnessing theorems in bounded arithmetic and applications (2016), http://cs.swan.ac.uk/∼csjjr/Papers/thesis.pdf, thesis (Ph.D.)–Swansea University
24. Thapen, N.: Higher complexity search problems for bounded arithmetic and a formalized no-gap theorem. Arch. Math. Logic 50(7-8), 665–680 (2011), http://dx.doi.org/10.1007/s00153-011-0240-0
25. Zambella, D.: Notes on polynomially bounded arithmetic. J. Symbolic Logic 61(3), 942–966 (1996), http://dx.doi.org/10.2307/2275794

## Appendix A Proof of Theorem 15

In what follows, when we say that a theory $\mathcal{T}$ proves a sequent

$$\varphi_1, \dots, \varphi_k \longrightarrow \psi_1, \dots \psi_l,$$

we mean that $\mathcal{T}$ proves

$$\bigwedge_{i=1}^{k} \varphi_i \supset \bigvee_{j=1}^{l} \psi_j.$$

Buss [5] originally proved his witnessing theorem for $\mathsf{V}^1$ via a witnessing lemma. Here, we do the same; that is to say, we use a new-style witnessing lemma in order to prove Theorem 15.

**Lemma 17 (New-style Witnessing Lemma for $\mathsf{V}^1$).** *Suppose that the theory $\mathsf{V}^1$ proves a sequent $\Gamma(A) \longrightarrow \Delta(A)$ of the form*

$$\dots, \exists X_i \phi'_i(X_i), \dots, \Lambda \longrightarrow \Pi, \dots, \exists Y_j \psi'_j(Y_j), \dots \tag{10}$$

*where $\phi'_i, \psi'_j, \Lambda$ and $\Pi$ are $\Sigma^B_0$-formulae. Then there is an $\mathsf{IITER}$ problem $Q_F$ with graph $\psi_F$ and $\mathsf{FAC}^0$-functions $\boldsymbol{G}$ such that $\overline{\mathsf{V}}^0$ proves the sequent $\Gamma' \longrightarrow \Delta'$, which is*

$$\dots, \phi'_i(\beta_i), \dots, \Lambda, \psi_F(A, \boldsymbol{\beta}, \gamma) \longrightarrow \Pi, \dots, \psi'_j(G_j(A, \boldsymbol{\beta}, \gamma)), \dots \tag{11}$$

We will use a version of the sequent calculus to prove this lemma. Given a sequent calculus proof $\pi$ of (10) we try to show the conclusion of Lemma 17 by structural induction on the depth of a sequent $S$ in $\pi$. If we use directly a sequent calculus for $\mathsf{V}^1$, we have the issue that the $\Sigma_1^B$-$\mathsf{COMP}$ axiom is in general not equivalent to a $\Sigma_1^B$-formula. As a result, the proof $\pi$ may contain formulae that are not $\Sigma_1^1$. To circumvent this obstacle, we need to work with a slightly different theory $\widetilde{\mathsf{V}}^1$ equivalent to $\mathsf{V}^1$. For that, first consider the following definition:

**Definition 18 (Cook, Nguyen [8]).** *Let $\psi(X)$ be an $\mathcal{L}_A^2$-formula. Then $\psi$ is a* single-$\Sigma_1^1$-formula *if $\psi$ is of the form $\exists Y \varphi(X, Y)$, where $\varphi$ is a $\Sigma_0^B$-formula. If $\psi$ is of the form $(\exists Y {\leq} t)\varphi(X, Y)$, where $\varphi$ is a $\Sigma_0^B$-formula and $t$ is an $\mathcal{L}_A^2$-term not involving $Y$, then $\psi$ is a* single-$\Sigma_1^B$-formula.

**Definition 19 (Cook, Nguyen [8]).** *The theory $\widetilde{\mathsf{V}}^1$ is axiomatized by the axioms of $\mathsf{V}^0$ plus the single-$\Sigma_1^B$-$\mathsf{IND}$ axiom scheme.*

Below, we merely state that $\widetilde{\mathsf{V}}^1 = \mathsf{V}^1$ without proof. A full proof of it can be found in [8, Theorem VI.4.8].

**Theorem 20 (Cook, Nguyen [8]).** *The theories $\widetilde{\mathsf{V}}^1$ and $\mathsf{V}^1$ are the same.*

The sequent calculus $\mathsf{LK}$-$\widetilde{\mathsf{V}}^1$ for $\widetilde{\mathsf{V}}^1$ is essentially the sequent calculus $\mathsf{LK}$-$\mathsf{V}^0$ for $\mathsf{V}^0$ (c.f. [8]) augmented with the *single-$\Sigma_1^B$-$\mathsf{IND}$ rule*, which is

$$\frac{\chi(b), \Gamma \longrightarrow \Delta, \chi(b+1)}{\chi(0), \Gamma \longrightarrow \Delta, \chi(t)},$$

where $\chi \in \Sigma_1^{\mathrm{B}}$, and $b$ is an eigenvariable and cannot appear in the lower sequent.

The sequent calculus $\mathsf{LK}$-$\widetilde{\mathsf{V}}^1$ satisfies the following property, whose proof can be found in [8]:

**Theorem 21 (Cook, Nguyen [8]).** *Suppose that $\widetilde{\mathsf{V}}^1$ proves a sequent $\Gamma \longrightarrow \Delta$ consisting only of single-$\Sigma_1^1$-formulae. Then there is an $\mathsf{LK}$-$\widetilde{\mathsf{V}}^1$ proof $\pi$ of $\Gamma \longrightarrow \Delta$ such that every formula in $\pi$ is a single-$\Sigma_1^1$-formula.*

We are now ready to prove Lemma 17. The proof technique we use to prove Lemma 17 is similar to the one used for Theorem VI.4.1 in [8, page 154] (which is a witnessing theorem for $\mathsf{V}^1$), which adopts the same proof technique as Buss (cf. [5, Theorem 5]).

*Proof (of the New-style Witnessing Lemma for $\mathsf{V}^1$, Lemma 17).* Since $\widetilde{\mathsf{V}}^1$ and $\mathsf{V}^1$ are the same, it follows that $\widetilde{\mathsf{V}}^1$ proves (10). By Theorem 21, let $\pi$ be an $\mathsf{LK}$-$\widetilde{\mathsf{V}}^1$ proof of (10) such that every formula in $\pi$ is a single-$\Sigma_1^1$-formula. We show that $\overline{\mathsf{V}}^0$ proves the conclusion of Lemma 17 by induction on the depth of a sequent $S$ in $\pi$. The inductive proof splits into cases, depending on whether $S$ is an initial sequent or generated by the use of an inference rule. The most crucial case is the case of the single-$\Sigma_1^B$-$\mathsf{IND}$ rule.

Suppose that $S$ is obtained by the application of the single-$\Sigma_1^B$-$\mathsf{IND}$ rule. Then $S$ is the bottom sequent of

$$\frac{\psi(b), \mathit{\Lambda} \longrightarrow \mathit{\Pi}, \psi(b+1)}{\psi(0), \mathit{\Lambda} \longrightarrow \mathit{\Pi}, \psi(t)}$$

where (omitting the parameters $A$) $\psi(b)$ is of the form $(\exists X{\le}r(b))\psi_0(b,X)$ and

$$\mathit{\Pi} = \mathit{\Pi}', \exists Y_1\psi_1'(Y_1), \ldots, \exists Y_l\psi_l'(Y_l).$$

Here $\mathit{\Pi}', \psi_1', \ldots, \psi_l'$ is a sequence of $\mathit{\Sigma}_0^B$-formulae. Let $\eta(b,\beta)$ denote the formula $|\beta| \le r(b) \wedge \psi_0(b,\beta)$. By the induction hypothesis, let $Q_{F_1}$ be an $\mathsf{IITER}$ problem specified by $F_1$ and $t_1$, with graph $\psi_{F_1}$, and $G_1^1, \ldots, G_l^1$ and $G_{l+1}^1$ be the witnessing functions for the formulae in $\mathit{\Pi}, \psi(b+1)$ such that $\overline{\mathsf{V}}^0$ proves the following (omitting the parameters $A$, $\boldsymbol{\lambda}$, where $\boldsymbol{\lambda}$ are witnesses for the formulae in $\mathit{\Lambda}$):

$$\eta(b,\beta), \mathit{\Lambda}', \psi_{F_1}(b,\beta,\gamma) \longrightarrow \mathit{\Pi}''(G_j^1(b,\beta,\gamma)), \eta(b+1, G_{l+1}^1(b,\beta,\gamma)) \tag{12}$$

where $\mathit{\Lambda}'$ is the result of witnessing $\mathit{\Sigma}_1^1$-formulae in $\mathit{\Lambda}$ and leaving the rest unchanged and $\mathit{\Pi}''(G_j^1(b,\beta,\gamma)) = \mathit{\Pi}', \psi_1'(G_1^1(b,\beta,\gamma)), \ldots, \psi_l'(G_l^1(b,\beta,\gamma))$. Our goal is to constuct an $\mathsf{IITER}$ problem $Q_F$ (with graph $\psi_F$) and $\mathsf{FAC}^0$-functions $G_1, \ldots, G_l$ and $G_{l+1}$ such that $\overline{\mathsf{V}}^0$ proves the following:

$$\eta(0,\beta_0), \mathit{\Lambda}', \psi_F(\beta_0,\gamma) \longrightarrow \mathit{\Pi}''(G_j(\beta_0,\gamma)), \eta(t, G_{l+1}(\beta_0,\gamma)). \tag{13}$$

The intuitive idea behind the definition of $Q_F$ is that, assuming that $\eta(0,\beta_0)$ is true, we will repeatedly use $Q_{F_1}$ and $G_{l+1}^1$ in order to generate witnesses $\beta_1, \ldots, \beta_n$ for $\psi(1), \ldots, \psi(n)$, respectively, for $n \le t$. If $n < t$, then $Q_{F_1}$ failed to generate a witness to $\psi(n+1)$. Therefore, assuming that the hypothesis for (13) is true and using (12), we obtain our desired goal.

In what follows, the *string concatenation* function $X *_z Y$ is an $\mathsf{FAC}^0$ string function that concatenates the first $z$ bits of $X$ with $Y$ and can be recursively extended in the natural way. Omitting the subscripts to $*$, we write $Y_0 * \ldots * y * \ldots * Y_k$ for $Y_0 * \ldots * Y * \ldots * Y_k$, where $Y$ is the string representing the unary notation of the number value $y$.

We assume that the search variable for $Q_F$ is of the form

$$\gamma = \langle A, \beta_0, \boldsymbol{\lambda}\rangle *_s S_0 *_{2s} S_1 *_{3s} \ldots *_{(m+1)s} S_m,$$

where $s$ ($s$ is obtained from $t$ and the bounding term $r$, in the induction-formula $\psi$, and the bounding term $t_1$ for $Q_{F_1}$) is a suitable $\mathcal{L}_A^2$-term that bounds $|\langle A, \beta_0, \boldsymbol{\lambda}\rangle|, |S_0|, \ldots, |S_m|$; the symbol $S_i$ denotes $i * \beta_i * \gamma_i * 1$ and $m \le t$. Note here that, even though we omitted the subscripts to $*$ in $S_i$, they are somehow implicit. Let us now define the transition function $F$ for $Q_F$. In the following, we again omit the parameters $A, \boldsymbol{\lambda}$ for $F$. As usual, we will drop the subscripts to $*$ in $F(\beta_0,\gamma)$. If $\gamma = \emptyset$, then

$$F(\beta_0,\gamma) = \langle A, \beta_0, \boldsymbol{\lambda}\rangle * 0 * \beta_0 * \emptyset * 1. \tag{14}$$

Assume now that $\gamma \ne \emptyset$ and suppose that $m < t$ and $\eta(m,\beta_m)$ is true. Then there are two cases to consider. First, if $|\gamma_m| \le t_1 \wedge \gamma_m < F_1(m,\beta_m,\gamma_m) \wedge \neg\psi_{F_1}(m,\beta_m,\gamma_m)$ is true, then

$$F(\beta_0,\gamma) = \langle A, \beta_0, \boldsymbol{\lambda}\rangle * S_0 * \ldots * S_{m-1} * m * \beta_m * F_1(m,\beta_m,\gamma_m) * 1. \tag{15}$$

Second, if $|\gamma_m| \leq t_1 \wedge \gamma_m < F_1(m, \beta_m, \gamma_m) \wedge \psi_{F_1}(m, \beta_m, \gamma_m)$, then

$$F(\beta_0, \gamma) = \langle A, \beta_0, \boldsymbol{\lambda} \rangle * S_0 * \ldots * S_m * (m+1) * G^1_{l+1}(m, \beta_m, \gamma_m) * \emptyset * 1. \tag{16}$$

In all other cases, $F(\beta_0, \gamma) = \gamma$. Let $t_{Q_F}$ be $(t+2) \cdot s$ and $Q_F$ be specified by $F$ and $t_{Q_F}$. Finally, we define the $\mathsf{FAC}^0$-functions $G_i$, for $i = 1, \ldots, l+1$, as follows:

$$G_j(\beta_0, \gamma) = \begin{cases} \beta_0 & \text{if } t = 0 \\ G^1_j(m, \beta_m, \gamma_m) & \text{otherwise,} \end{cases}$$

The fact that $\overline{\mathsf{V}}^0$ proves (13) follows from (13)'s assumptions, from the following claim, the induction hypothesis and the definition of $G_j$ above. As a side remark, note that if $t = 0$, then $\overline{\mathsf{V}}^0$ proves (13) trivially.

*Claim.* We reason in $\overline{\mathsf{V}}^0$. Suppose that $t \neq 0$, $\eta(0, \beta_0)$ is true and $\gamma = \langle A, \beta_0, \boldsymbol{\lambda} \rangle * S_0 * \ldots * S_m$ is a solution to $Q_F(\beta_0)$, where $S_i$ is again of the form $i * \beta_i * \gamma_i * 1$. Then $\eta(m, \beta_m)$ is true; $\gamma_m$ is a solution to $Q_{F_1}(m, \beta_m)$; and either $\neg\eta(m+1, G^1_{l+1}(m, \beta_m, \gamma_m))$ or $\eta(t, G_{l+1}(\beta_0, \gamma))$ is true.

*Proof of Claim.* Since $\gamma$ is a solution to $Q_F(\beta_0)$, then we have two possibilities: either $\gamma = \emptyset$ and $F(\beta_0, \gamma) = \gamma$, or

$$|\gamma| \leq t_{Q_F} \wedge \gamma < F(\beta_0, \gamma) \wedge [|F(\beta_0, \gamma)| > t_{Q_F} \vee F(\beta_0, F(\beta_0, \gamma)) = F(\beta_0, \gamma)].$$

Note that, by the definition of $F$, $\emptyset$ cannot be a solution to $Q_F(\beta_0)$ and $|F(\beta_0, \gamma)| \leq t_{Q_F}$. Therefore, we have that

$$\gamma \neq \emptyset \wedge \gamma < F(\beta_0, \gamma) = F(\beta_0, F(\beta_0, \gamma)). \tag{17}$$

The only way for (17) to hold is if (16) is true. This implies that $\eta(m, \beta_m)$ holds and $\psi_{F_1}(m, \beta_m, \gamma_m)$ is true; that is to say, $\gamma_m$ is a solution $Q_{F_1}(m, \beta_m)$. Hence, we are left with proving the following:

$$\neg\eta(m+1, G^1_{l+1}(m, \beta_m, \gamma_m)) \vee \eta(t, G_{l+1}(\beta_0, \gamma)).$$

If $m+1 = t$, then we are done. So, assume that $m+1 < t$. For the sake of contradiction, assume that $\eta(m+1, G^1_{l+1}(m, \beta_m, \gamma_m))$ holds. This means that $F(\beta_0, \gamma) < F(\beta_0, F(\beta_0, \gamma))$, which is a contradiction. Thus, we are done with the proof of the claim. □

This finishes the proof of Lemma 17.