Closure properties of weak systems of bounded arithmetic

Antonina Kolokolova

University of Toronto & Mathematical Institute, Prague
kol@cs.toronto.edu

Abstract. In this paper we study the properties of systems of bounded arithmetic capturing small complexity classes and state conditions sufficient for such systems to capture the corresponding complexity class tightly. Our class of systems of bounded arithmetic is the class of second-order systems with comprehension axiom for a syntactically restricted class of formulas $\Phi \subset \Sigma_1^B$ based on a logic in the descriptive complexity setting. This work generalizes the results of [CK03] and [CK04].[1]
We show that if the system 1) extends V_0 (second-order version of $I\Delta_0$), 2) Δ_1-defines all functions with bitgraphs from Φ, and 3) proves witnessing for all theorems from Φ, then the class of Σ_1^B-definable functions of the resulting system is exactly the class expressed by Φ in the descriptive complexity setting, provably in this system.

1 Introduction

There has been a lot of research in descriptive complexity and bounded arithmetic, as well as their connections with complexity theory. However the question of direct relationship between these two fields did not receive much attention. The language of bounded arithmetic is richer than that of many logics, but often logics capture complexity classes over languages that include some arithmetic predicates (order, plus and times, or, equivalently, BIT predicate).

Bounded arithmetic studies the complexity of proving properties of these classes of formulas, whereas descriptive complexity is concerned with their expressive power. The most important distinction between different systems of bounded arithmetic is the strength of their induction (or comprehension) axiom schemes. This leads to the following question: how does the expressive power of the class of formulas in the induction axioms of a system relate to the power of the resulting system?

We answer this question for several second-order logics capturing small complexity classes. Restricting our attention to small classes allows us to use definability by `NP` predicates (bounded Σ_1) for the definition of capture in the bounded arithmetic setting: we consider exactly the functions defined by `NP` predicates that are provably total in our systems. The provability of existence

[1] More detailed presentation of most of this work can be found in my PhD thesis, [Kol04], available on ECCC.

and uniqueness of a value for such functions depends on the power of the systems, and gives us the main measure of that power. In most other systems of arithmetic, functions are introduced either by their recursion-theoretic characterization (see [Cob65] for the original such result or [Zam96]). Since we know the exact expressive power of the formulas in comprehension, and are trying to define the same function class, we introduce function symbols by setting their bitgraphs to be formulas from the comprehension scheme. We still need to prove the existence and uniqueness, but having comprehension over function definitions makes proofs much easier.

More precisely, let C be a complexity class, and let Φ_C be a class of formulas that captures C in the descriptive complexity setting. Define a theory of bounded arithmetic V-Φ_C to be Robinson's Q together with comprehension over bounded Φ_C. We would like to know under which conditions V-Φ_C captures C in the sense that provably total functions of V-Φ_C are functions computable in C. Our main contribution is to pinpoint some sufficient conditions for such capture. The following is an informal statement of our main result (weaker form).

Claim: *Consider a class of formulas $\Phi_C \subset \Sigma_1^B$ capturing C in the descriptive complexity setting, and a system of arithmetic V-Φ_C that has comprehension (induction) over Φ_C. Suppose that Φ_C is closed under first-order operations provably in V-Φ_C. Also, suppose that for every formula $\phi \in \Phi_C$ which is a theorem of V-Φ_C there is a function F computable in C which takes as its input the values of the free variables of ϕ and witnesses existential quantifiers of ϕ. Then V-Φ_C captures C, that is, the class of provably total functions of V-Φ_C is the class of functions computable in C.*

For conventional systems of bounded arithmetic, such as ones considered by Clote and Takeuti in [CT95], it was shown that the class of provably total functions of a system coincides with the function class in the complexity-theoretic sense. Under our conditions this is provable within the system itself, provided that the function class is introduced by bitgraphs of the functions. Therefore, more work is needed to prove the conditions, however the result is stronger. Hopefully, this can make our framework useful for proving independence results for weak theories of arithmetic.

Systems that provably capture complexity classes are V_1-Horn capturing $\mathtt{P}$ from [CK01,CK03], V-Krom capturing $\mathtt{NL}$ from [CK04] and V^0 capturing $\mathtt{AC}^0$ from [Coo02]. As an example of a system that captures a complexity class, but not (known to be) provably, we present a system of arithmetic V-SymKrom. It is based on symmetric second-order 2-CNF formulas (with $\oplus$ instead of $\vee$ between literals). This system can prove that its class of Σ_1^B-definable functions is the $\mathtt{AC}^0$ closure of $\mathtt{SL}$ functions. By the recent Reingold's result [Rei04], $\mathtt{SL} = \mathtt{L}$ and so symmetric 2-SAT is solvable in logspace; therefore, $\mathtt{AC}^0(\mathtt{SL}) = \mathtt{SL} = \mathtt{L}$. However, this proof, and even the proof that $\mathtt{SL}$ is closed under complementation by Nisan and Ta-Shma [NTS95], rely on algebraic properties on expander graphs. In their current form, these proofs are not formalizable using $\mathtt{SL}$-reasoning: to talk about algebra, we need at least polynomial time. It is a very interesting open question whether there is a combinatorial version of Reingold's proof that is formalizable in a system for L, and whether our theory for SL is fully conservative over a system for L.

2 Descriptive complexity framework

The name "descriptive complexity" refers to the study of expressive power of logics: fixing a formula, we look at the complexity of evaluating this formula on different finite structures. It is more common to call this area "finite model theory"; however, here we stay with the term "descriptive complexity" to emphasize the complexity theory connection and the richness of the underlying vocabulary. Please see [EF95], [Imm99], and [Lib04] for the background.

We will assume, following [Imm99], that all logics we consider are over the vocabulary $\tau = \{\min, \max, +, \times, \leq\}$ (we do not include BIT operator since it can be defined from $+, \times$ in the weakest of our systems; see [Coo02] for details). For many results it is sufficient to assume only the presence of order and successor relations in the vocabulary (these are the assumptions of [Grä91,Grä92]); however it is more convenient to work with a vocabulary containing all basic arithmetic operations. We refer to structures where the arithmetic symbols of the vocabulary get the standard interpretation as "arithmetic structures". The way we connect logics with complexity classes is stated in this definition (following [Lib04]):

Definition 1 (Capture by a logic). *Let C be a complexity class, L a logic and K a class of finite structures. Then L captures C on K if*

1. *For every L-sentence ϕ and every $\mathcal{A} \in K$, testing if $\mathcal{A} \models \phi$ with ϕ fixed and an encoding of $\mathcal{A}$ as an input can be done in C.*
2. *For every collection K' of structures closed under isomorphism, if this collection is decidable in C then there is a sentence $\phi_{K'}$ of L such that $\mathcal{A} \models \phi_{K'}$ iff $\mathcal{A} \in K'$, for every $\mathcal{A} \in K$.*

For our purposes, we fix K to be the arithmetic structures. In particular, the universe of a structure is always considered to be $\{0, \ldots, n-1\}$.

Many capture results are obtained by extending first-order logic with additional operators, such as fixed-point operators. We find it more convenient to work with restrictions of second-order logics rather than extensions of first-order. However, in many cases we can switch to the extended first-order logic framework by adding a defining axiom for a new operator, where the defining axiom is a second-order formula. We use this for NL and SL theories, in order to introduce respective transitive closure operators.

Definition 2. *We will use the term* restricted $SO\exists$ *to refer to formulas of the form*

$$\exists P_1 \ldots P_k \forall x_1 \ldots x_l \psi(\bar{P}, \bar{x}, \bar{a}, \bar{Y}), \tag{1}$$

where k, l are constants, and ψ is a (sub)class of CNF closed under conjunction. Here, when defining a subclass of CNF we only treat quantified second-order variables $\bar{P}$ as literals.

Note that there are no occurrences of existential first-order quantifiers in restricted $SO\exists$ formulas. This is because even when the class of ψ is restricted to 2CNF with at most one occurrence of a positive literal, with presence of an existential quantifier it is possible to capture all of $SO\exists$ [Grä91,Grä92]. Universal first-order and quantifier-free formulas are restricted $SO\exists$.

Schaefer's classes ([Sch78]) provide several restrictions on CNF that correspond to different complexity classes. Grädel in [Grä91,Grä92] described how to use some of them to capture complexity classes by restricted second-order formulas. Here we use systems based on the following restrictions of ψ:

Definition 3. *A formula $\psi(\bar{x}, \bar{P}, \bar{a}, \bar{Y})$ is* Horn *with respect to the second-order variables $P_1, ..., P_k$ if ψ is quantifier-free in conjunctive normal form and in every clause there is at most one positive literal of the form $P_i(\bar{x})$. It is* Krom *with respect to $\bar{P}$ if ψ is a CNF with at most two occurrences of a P-literal per clause. It is* SymKrom *if it is Krom with $\oplus$ instead of $\vee$ in every clause (so every clause is of the form $(\phi_i \to L_i \oplus L'_i)$, where the only P-literals are L_i and L'_i).*

Following Grädel, we can define classes $SO\exists$ Horn and $SO\exists$ Krom to be restricted $SO\exists$, in which ψ is Horn with respect to $\bar{P}$ for $SO\exists$ Horn and Krom with respect to $\bar{P}$ for $SO\exists$ Krom, respectively. $SO\exists$ SymKrom is defined analogously.

The following descriptive complexity characterizations provide classes of formulas on which our systems can be based. However, not all of them result in systems tightly capturing the corresponding complexity class.

Theorem 1 (Capturing complexity classes by logics). *Over arithmetic structures,*

- *First-order logic captures uniform* $\mathtt{AC}^0$ *([Imm82,BIS90]).*
- *Second-order existential logic captures* `NP` *([Fag74]), and in general levels of SO hierarchy correspond to levels of PH ([Sto77]).*
- *Second-order Horn, Krom and SymKrom capture* `P`, `NL` *and* `SL`, *respectively ([Grä91,Grä92]).*

In case of restricted second-order formulas, the formula evaluation direction of the capture proof consists of the following steps. First, the formula is brought into propositional form by making a copy of its quantifier-free part for every possible tuple of values of quantified first-order variables. Then first-order terms and free second-order terms are evaluated. Second-order terms of the form $P_i(t(\bar{x}))$, where P_i is quantified and $t(\bar{x})$ is a term, are assigned propositional variables so that $P_i(t(\bar{x}))$ and $P_i(t'(\bar{x}))$ are assigned to the same variable whenever $t(\bar{x})$ evaluates to the same value as $t'(\bar{x})$, on possibly different tuples $\bar{x}$. Now the problem is reduced to testing satisfiability of the resulting propositional formula.

3 Bounded arithmetic framework

In descriptive complexity, a language in the traditional complexity theory setting is thought of as interpretations of a unary predicate X (representing a binary string) in a set of structures. A class of recursively enumerable languages then naturally corresponds to a class of formulas: each language in the class corresponds to a formula which has, as its set of models, the structures with X interpreted as strings from the language. In the bounded arithmetic setting, the relationship with complexity classes is slightly different. Here, we consider representations of languages in the standard model of arithmetic $\mathbb{N}_2$, defined below. Instead of a set of structures with one predicate getting different interpretation we are talking about one fixed structure and different (second-order) elements of it satisfying the formula.

The language of our systems of arithmetic is $\mathcal{L}_A^2 = \{0, 1, +, \cdot, |\ |; <, =, \in\}$, a natural second-order extension of the language of Peano Arithmetic $\mathcal{L}_A = \{0, 1, +, \cdot; <, =\}$. Let $\mathbb{N}_2$ be a standard structure with natural numbers and finite sets of natural numbers in the universe; our first-order objects (denoted by lower-case letters) are natural numbers; second-order objects (denoted by upper-case letters) are binary strings or, equivalently, (finite) sets of numbers. Treating a second-order variable X as a set, its upper bound ("length") $|X|$ is defined to be the largest element $y \in X$ plus one, or 0 if X is an empty set.

Arithmetic terms are constructed using $+$ and $\times$ from first-order variables, constants 0 and 1, and terms of the form $|X|$ where X is a second-order variable. The atomic formulas of $\mathcal{L}_A^2$ have one of the forms $s = t, s \leq t, t \in X$, where s and t are terms and X is a second-order variable. We usually write $X(t)$ instead of $t \in X$. Formulas are built from atomic formulas using the propositional connectives $\wedge, \vee, \neg$, the first-order quantifiers $\forall x, \exists x$ and the second-order quantifiers $\forall X, \exists X$.

Bounded first-order quantifiers get their usual meaning: $\forall x \leq t\phi$ stands for $\forall x(x \leq t \rightarrow \phi)$ and $\exists x \leq t\phi$ stands for $\exists x(x \leq t \wedge \phi)$. Second-order quantified variables are strings of bounded length; the notation $\exists Z \leq b$ corresponds to $\exists Z\ |Z| \leq b$.

Definition 4. *Σ_0^B and Π_0^B both denote the class of bounded formulas with no second-order quantifiers. We define inductively Σ_{i+1}^B as the least class of formulas containing Π_i^B and closed under disjunction, conjunction, and bounded existential second-order quantification. The class Π_{i+1}^B is defined dually. We use notation $\Sigma_0^B(\Phi)$ to refer to the closure of Φ under Σ_0^B operations: that is, under $\vee, \wedge, \neg$ and bounded first-order $\forall$ and $\exists$.*

3.1 Translation

Let Φ be a descriptive logic over a vocabulary τ. For every $\phi \in \Phi$, we can define a translation ϕ^* into $\mathcal{L}_A^2$ with the following properties:

1. Every interpreted symbol from τ that occurs in $\mathcal{L}_A^2$ gets the standard interpretation. Successor, min, etc are translated into appropriate arithmetic operations such as $+1$ for successor, 0 for min.
2. Translate max as n for a free variable n. For every quantified first-order variable, set $n+1$ (more generally, a polynomial of n) as a bound. Note that then $|X| = n + 1$ for a unary second-order predicate.

3. Translate uninterpreted relational symbols of τ occurring in ϕ as free second-order variables of ϕ^*. If a variable is k-ary, use a pairing function to encode the relational symbol as a unary second-order variable. Then any occurrence of $R(x_1,\ldots,x_k)$ becomes $R^*(\langle x_1,\ldots,x_k\rangle)$, where $\langle x_1,\ldots,x_k\rangle$ is a value obtained by applying the pairing function to $x_1,\ldots,x_k$.

Under this translation, a restricted second-order formula becomes a restricted Σ^B_1 formula with the same restriction on the quantifier-free part. The resulting Φ^* represents in the standard model the same complexity class as is captured by Φ.

3.2 Systems of bounded arithmetic

B1: $x+1\neq 0$	B2: $x+1=y+1\rightarrow x=y$	B4: $x+(y+1)=(x+y)+1$
B3: $x+0=x$	B5: $x\cdot 0=0$	B6: $x\cdot(y+1)=(x\cdot y)+x$
B7: $0\leq x$	B9: $x\leq y\wedge y\leq z\rightarrow x\leq z$	B10: $(x\leq y\wedge y\leq x)\rightarrow x=y$
B8: $x\leq x+y$	B11: $x\leq y\vee y\leq x$	B12: $x\leq y\leftrightarrow x<y+1$
L1: $X(y)\rightarrow y<\lvert X\rvert$	L2: $y+1=\lvert X\rvert\rightarrow X(y)$	B13: $x\neq 0\rightarrow\exists y(y+1=x)$

Table 1. The 2-BASIC axioms

Now, for a set of formulas Φ, a system V-Φ is axiomatized by 2-BASIC axioms listed in table above together with a comprehension scheme of the form

$$\exists Z\leq b\forall i<b(Z(i)\leftrightarrow\phi(i,\bar{a},\bar{X})), \qquad (\Phi\text{-comp})$$

where $\phi\in\Phi$.

To agree with the common notation, we abbreviate V-Σ^B_i as V^i, $i\geq 0$. These theories are axiomatized by the 2-BASIC together with a comprehension scheme for Σ^B_i formulas. For $i\geq 1$, V^i is RSUV isomorphic to the first-order theory S^i_2. The system V^0 corresponds to the complexity class uniform $\mathtt{AC}^0$.

4 Definability in V-Φ.

4.1 Basic properties of V^0 and V-Φ.

The system V^0 is robust enough to prove many natural properties. In particular, induction on the length of string (and thus on Σ^B_0 combinations of Φ) is a theorem of V-Φ extending V^0. Also, V^0 proves properties of the pairing function and simultaneous comprehension over several variables, resulting in an array (so several existential second-order quantifiers can be treated as one). We use $P^{[b]}$ to denote the "b-th row" when P is being used as a 2-dimensional array. If $\phi(P)$ is a formula with no occurrence of $|P|$, then $\phi(P^{[b]})$ is obtained from $\phi(P)$ by replacing every atomic formula $P(t)$ by $P(b,t)$.

The following property, Replacement, plays a major role in our definability proofs. It is a theorem for V^1 and stronger theories, however weaker theories do not prove full Σ_1^B replacement under cryptographic assumptions by [CT04]. In this case, we prove it for restricted Σ_1^B formulas.

Lemma 1 (Replacement). *Let Φ be a class of restricted Σ_1^B formulas. Then for every formula $\exists \bar{P}\phi(y, \bar{P}) \in \Phi$, where ϕ can have additional free variables, V-Φ proves*

$$\forall y < t \exists \bar{P}\phi(y, \bar{P}) \leftrightarrow \exists \bar{P} \forall y < t \phi(y, \bar{P}^{[y]}) \qquad \text{(Replacement)}$$

where $\bar{P}^{[y]}$ is $P_1^{[y]}, ..., P_k^{[y]}$.

Proof. The proof is a generalization of a proof of Replacement in [CK03]. Here we are heavily relying on lack of existential first-order quantifiers and closure under conjunctions of the quantifier-free parts of Φ-formulas.

4.2 Function classes

Our complexity classes, both in the descriptive complexity setting and in bounded arithmetic, are relational. However, in bounded arithmetic we would like to be able to talk about functions. We can use relations as graphs to define number functions and as bit graphs to define string functions. The following definition is very general, but sometimes does not produce a robust function class: for example, there is nothing in this definition that would force the functions to be closed under composition. In order to make the function classes defined this way meaningful, we will need additional restrictions.

Definition 5. *Let C be a complexity class. We define the corresponding class FC of functions of C as follows: A string function $F : \mathbb{N}^k \times (\{0,1\}^*)^l \to \{0,1\}^*$ is in FC iff there is a relation R in C and a polynomial p such that $F(\bar{x}, \bar{Y})(i) \leftrightarrow i < p(\bar{x}, |\bar{Y}|) \wedge R(i, \bar{x}, \bar{Y})$ for all $i \in \mathbb{N}$. A number function $f(\bar{x}, \bar{Y})$ is in the class FC if there is a string function in $F(\bar{x}, \bar{Y}) \in FC$ such that $f(\bar{x}, \bar{Y}) = |F(\bar{x}, \bar{Y})|$. If formula class Φ represents C, then R can be replaced by a formula $\phi \in \Phi$ representing R.*

For string functions, we are only concerned with the bits with indices smaller than $p(\bar{x}, \bar{Y})$. Therefore, a string corresponding to the value of a function will be of length less than $p(\bar{x}, \bar{Y})$. In particular, by the length axioms, all bits with indices larger than $p(\bar{x}, \bar{Y})$ are 0.

This definition of FC does not directly impose any "robustness" conditions. A robust function class should at least be closed under function composition. To allow for that, we define an $\mathtt{AC}^0$ closure of FC as follows.

Definition 6. *A (string) function $F(\bar{x}, \bar{Y})$ is $\mathtt{AC}^0$ reducible to $\mathcal{L}$ (denoted $F \in \mathtt{AC}^0(\mathcal{L})$) iff there is a sequence $F_1 \dots F_n$ of string functions such that $F_n = F$ and F_i is in $\Sigma_0^B(\mathcal{L} \cup \{F_1 \dots F_{i-1}\})$ for $i = 1, \dots, n$. If for any $F \in \mathtt{AC}^0(\mathcal{L})$, $F \in \mathcal{L}$ we say that $\mathcal{L}$ is closed under $\mathtt{AC}^0$ reductions.*

In case FC is definable by formulas from Φ, the definition naturally generalizes to $\mathtt{AC}^0(\Phi)$.

A power of a system of arithmetic can be defined either as a class of Δ_1^B-definable relations of the system, or a class of Σ_1^B-definable functions the system proves total.

Definition 7. *A relation $R(\bar{x},\bar{Y})$ is Δ_1^B-definable in V-Φ iff there exists formulas $\phi,\tilde{\phi} \in \Sigma_1^B$ such that $R(\bar{x},\bar{Y})$ is represented by $\phi(\bar{x},\bar{Y})$ and $V\text{-}\Phi \vdash \phi(\bar{x},\bar{Y}) \leftrightarrow \neg\tilde{\phi}(\bar{x},\bar{Y})$. A string function F is Σ_1^B-definable in V-Φ if it has a defining axiom $Z = F(\bar{x},\bar{Y}) \leftrightarrow \phi(Z,\bar{x},\bar{Y})$), with $\phi \in \Sigma_1^B$ such that $V\text{-}\Phi \vdash \forall\bar{x}\forall\bar{Y}\exists!Z\phi(Z,\bar{x},\bar{Y})$).*

Using definition 7, we can state the definition of "capture" in the bounded arithmetic setting. This gives us a way of measuring the power of a system of arithmetic.

Definition 8 (Capture in bounded arithmetic). *A system of arithmetic T* captures *a complexity class C if the class of Σ_1^B-definable functions of T is exactly FC.*

Note that this is quite different from the descriptive complexity notion of "capture" from definition 1. The reason we are using the same word is that in both cases we are relating a logic (system of arithmetic) and a complexity class; "capture" here is a generic name for such a connection.

4.3 Properties

The first property that we consider is (provable) closure under $\mathtt{AC}^0$ reductions. Although at the end this property is not essential, it greatly simplifies proofs and is satisfied by most of our systems. The provability part is necessary for the bounded arithmetic setting.

*Property 1 (***Closure***).* Let Φ represent a complexity class C and let FC be as in the definition 5. Then the *closure property* holds if Φ is closed under $\mathtt{AC}^0$ reductions. In particular, FC is closed under composition and substitution of a term for a variable. In addition, Φ is *strongly* closed if for every $\phi^* \in \Sigma_0^B(\Phi)$ there exists $\phi \in \Phi$ such that $V\text{-}\Phi \vdash \phi^* \leftrightarrow \phi$.

If this property holds, the corresponding C must be closed under complementation and Φ extends Σ_0^B (that is, defines all of first-order). For some Φ, notably restricted Σ_1^B, it is not syntactically true that $\Sigma_0^B \subseteq \Phi$, but it can be proved that for any Σ_0^B formula there is an equivalent formula of Φ.

In order for a logic to translate into a "nice" system of arithmetic, the logic has to be in some sense "natural". That is, its properties such as closure under composition and complementation have to be provable using only simple concepts. Moreover, it should be easy to verify whether a given formula holds on a structure. More formally, we need the following property:

Property 2 (**Constructiveness**). Let Φ be a class of restricted Σ_1^B formulas, and let Φ represent C. This Φ has the *constructiveness property* if the following two conditions hold. Firstly, every $\phi \in \Phi$ defines a relation R that is Δ_1^B-definable in V-Φ, with ϕ being its Σ_1^B definition. That is, for every $\phi \in \Phi$ there exists $\tilde{\phi} \in \Sigma_1^B$ such that $V\text{-}\Phi \vdash \phi(\bar{a}, \bar{Y}) \leftrightarrow \neg\tilde{\phi}(\bar{a}, \bar{Y})$. Secondly, there are witnessing functions $\bar{F}$ with bit graphs in $\Sigma_0^B(\Phi)$ such that $\bar{F}(\bar{a}, \bar{Y})$ witness the existential quantifiers of the prenex form of $\phi \vee \tilde{\phi}$.

Remark 1. If, additionally, Φ is strongly closed, that is, has the property 1, then the conclusion of the constructiveness property can be stated simpler as follows.

For every $\phi \equiv \exists \bar{P} \psi(\bar{P}, \bar{a}, \bar{Y}) \in \Phi$ such that $V\text{-}\Phi \vdash \phi$ there are functions $\bar{F}$ witnessing $\bar{P}$ such that bitgraphs of $\bar{F}$ are in Φ. It is enough to consider ϕ-theorems of V-Φ because if Φ is closed, then $\tilde{\phi} \in \Phi$ and so is $\phi \vee \tilde{\phi}$. Also, the assumption that bitgraphs of $\bar{F}$ are in $\Sigma_0^B(\Phi)$ becomes bitgraphs $\in \Phi$.

4.4 Main results

Now we are ready to state the main theorem of this paper.

Theorem 2 (Definability theorem). *Suppose that Φ is restricted Σ_1^B or Σ_0^B, constructive, and represents a complexity class C. Then all functions from FC are Σ_1^B-definable in V-Φ and all Σ_1^B-definable functions of V-Φ are in $\mathtt{AC}^0(FC)$.*

Suppose, additionally, that Φ is strongly closed. Then the class of Σ_1^B-definable functions of V-Φ coincides with FC provably in V-Φ.

We will refer to the first statement as "weak definability" and the second statement as "strong definability".

The proof of this theorem consists of two parts. First, we show that FC is Σ_1^B-definable in V-Φ provided that Φ is constructive in V-Φ. Here, replacement lemma plays major role.

The second part we call *generalized witnessing theorem*.

Theorem 3 (Generalized witnessing theorem). *Let Φ be a class of restricted Σ_1^B formulas representing C. Suppose that Φ is constructive. Then Σ_1^B-theorems of V-Φ can be witnessed by functions from $\mathtt{AC}^0(FC)$ provably in V-Φ. That is, if $V\text{-}\Phi \vdash \exists Z \phi(\bar{x}, \bar{Y}, Z)$, where $\phi \in \Sigma_1^B$, then there is a string function $F(\bar{x}, \bar{Y})$ in $\mathtt{AC}^0(FC)$ such that*

$$V\text{-}\Phi, AX(F) \vdash \phi(\bar{x}, \bar{Y}, F(\bar{x}, \bar{Y})),$$

where $AX(F)$ is a defining axiom for F. If Φ is strongly closed and constructive, then V-Φ proves that the defining axiom for F is equivalent to a formula from Φ.

The witnessing theorem looks similar to the constructiveness property, but they talk about different classes of formulas. Whereas constructiveness is concerned with witnessing an existential quantifier in a $\phi \in \Phi$ (or finding a counterexample to ϕ), the witnessing theorem describes the power of a system in terms of the strength of Σ_1^B-theorems that the system in question can prove.

The theorem 3 is a generalization of the witnessing theorem for V^0 as presented in [Coo02] (hence the name "Generalized witnessing"). The proof uses proof-theoretic techniques. Taking a Σ_1^B theorem of V-Φ, we analyze its anchored proof in a second-order version of quantified Gentzen calculus LK^2. To ensure that every line in the proof has only Σ_1^B formulas, we replace the comprehension axiom of V-Φ by a statement of the form $\exists Z < t \forall i \leq t(\phi(i) \wedge Z(i)) \vee (\tilde{\phi}(i) \wedge \neg Z(i))$, $\phi \in \Phi$, where $\tilde{\phi}$ is a Σ_1^B formula equivalent to the negation of ϕ, provided by the constructiveness property.

5 Applications of the Strong Definability theorem.

Three examples when Theorem 2 applies are V^0 itself, V_1-Horn and V-Krom.

Example 1([Coo02,Zam96,Coo04]) Functions bit-definable by Σ_0^B formulas in V^0 are $\mathtt{AC}^0$ functions, and Σ_0^B formulas correspond to the first-order logic which captures $\mathtt{AC}^0$ in the descriptive sense ([BIS90]). The constructiveness property is satisfied trivially, since Σ_0^B is closed under complementation syntactically and there are no quantifiers to witness. It was shown in [Zam96,Coo04] that $\mathtt{AC}^0$ functions are closed under composition and thus under $\mathtt{AC}^0$ reductions. Therefore, theorem 2 applies, so the class of Σ_1^B-definable functions of V^0 is $F\mathtt{AC}^0$.

Example 2 ([CK01,CK03]) The class of Σ_1^B-Horn formulas comes from $SO\exists$-Horn formulas capturing $\mathtt{P}$ in the descriptive setting. The resulting system V_1-Horn defines polynomial-time functions by Σ_1^B-Horn formulas, and is equivalent in power to Zambella's $\mathtt{P}$-def (and thus PV). In this case, the Theorem 2 holds with $\Phi = \Sigma_1^B$-Horn and $FC = FP$. So by the definability theorem Σ_1^B-definable functions of V_1-Horn are precisely polynomial-time functions. The bulk of work is a formalization of the satisfiability algorithm for propositional Horn formulas, which is needed already to prove closure of Σ_1^B-Horn formulas under complementation. This algorithm is constructive; therefore, a satisfying assignment (or, equivalently, values for quantified second-order variables) can be constructed as part of the algorithm. This gives the constructiveness property.

Note that if the conditions do not hold, then the class of witnessing functions can be smaller than representable by formulas in the comprehension axiom. An example of that is the theory V^1, with comprehension over $\mathtt{NP}$ predicates. By a second-order version of Buss' witnessing theorem [Zam96,Coo02], the class of Σ_1^B-definable functions of V^1 is $\mathtt{P}$. But not every Σ_1^B formula is Δ_1^B-definable in V^1. Moreover, even if $\mathtt{NP} = co\mathtt{NP}$ and for every Σ_1^B formula there is an equivalent Π_1^B formula, it might not be the case that these equivalences are provable in V^1.

Example 3([CK04]) Now take the class of Σ_1^B-Krom formulas, a translated version of Grädel's $SO\exists$-Krom (second-order 2CNF). It is possible to formalize Immerman-Szelepcsényi's proof of closure of $\mathtt{NL}$ under complementation in the resulting theory V-Krom ([CK04]). Also, proving that transitive closure function is Σ_1^B-definable in V-Krom results in a proof of constructiveness for V-Krom: values for quantified second-order variables are expressed as Σ_0^B combination of transitive closure function calls.

The next example, a system of arithmetic for SL, presents a case when we were not able to prove the strong version of the properties; this led to the formulation of the weaker properties.

6 Weak case of the definability theorem

A class of Σ_1^B-SymKrom formulas is very similar to Σ_1^B-Krom, except it is based on symmetric 2CNF (that is, 2CNF with XOR instead of disjunctions). From the same Grädel's paper as before, [Grä92], we know that $SO\exists$-SymKrom captures SL. We define V-SymKrom to be V-Φ with $\Phi \equiv \Sigma_1^B$-SymKrom.

It seems that showing that a system V-SymKrom would capture FSL should be straightforward. However, the methods used to prove closure of SL under complementation (Nisan and Ta-Shma, [NTS95]), and, recently, that SL = L (Reingold, [Rei04]) use properties of expander graphs and rely on algebraic methods for the proofs. But those are not known to be formalizable in less complexity than P. Therefore, it seems only possible to prove a weak version of theorem 2, that is that every SL function is definable in V-SymKrom and every Σ_1^B-definable function of V-SymKrom is in $\mathtt{AC}^0(F\mathtt{SL})$. By Reingold's result, the class of Σ_1^B-definable functions of V-SymKrom is thus all logspace functions, but this is not known to be provable in V-SymKrom itself, as opposed to the cases of $\mathtt{AC}^0$, NL and P. It might still be possible that such a theory for SL is not fully conservative over a theory for L.

6.1 Symmetric transitive closure

To simplify proofs, we introduce symmetric transitive closure operator by the following axiom:

$$STC_{x,y}\phi(x,y,\bar{a},\bar{Y})[a,b,n] \leftrightarrow \forall R(CondS(\phi,R,n) \to R(a,b)), \qquad \text{(AxSTC)}$$

where

$$CondS(\phi,R,n) \equiv \forall x,y,z < n(R(x,x) \wedge (\phi(x,y) \to (R(y,z) \leftrightarrow R(x,z))))$$

Note that if ϕ is quantifier-free except for bounded existential first-order quantifiers, then negation of $STC_{x,y}\phi(x,y)[a,b,n]$ is equivalent to a Σ_1^B-SymKrom formula. Therefore, V-SymKrom proves induction on Σ_0^B combinations of STC functions.

By the same reasoning as for V-Krom in [CK04], STC defined in this manner is reflexive, transitive and robust against adding an edge on the left versus on the right (that is, conditions with $\phi(x,y) \to (R(x,z) \leftrightarrow R(y,z))$ and $\phi(y,z) \to (R(x,z) \leftrightarrow R(x,y))$ are equivalent). It is also provable in V-SymKrom that STC is symmetric: $STC(a,b,n) \leftrightarrow STC(b,a,n)$.

To see that $V^0 \subset V$-SymKrom, we encode a first-order formula as a graph and apply the STC operator to it. A first-order existential quantifier in $\exists z < n\psi(z)$ is represented by STC applied to the graph with an edge relation defined by

$E(x,y) \leftrightarrow \neg\psi(x) \wedge y = x+1$. That is, a graph is a path from vertex 0 to vertex n with every edge $(z, z+1)$ labeled $\neg\psi(z)$; if $\psi(z)$ holds for some z_0 then the edge (z_0, z_0+1) is absent so the start of the path and the end of it are disconnected. Similarly, a first-order universal quantifier is encoded by a graph with $E(x,y)$ such that $E(s,u) \leftrightarrow E(u,t) \leftrightarrow \neg\psi(u)$. This construction is applied for every block $\exists z < n \forall u < n \psi(z,u)$: such block is encoded as a path with every edge replaced by a "nested diamonds" gadget encoding a universal quantifier. A vertex $\langle n,n\rangle$ is reachable from the vertex $\langle 0,0\rangle$ iff $\exists z < n \forall u < n \psi(z,u)$ holds.

Now we need to show the weak constructiveness property. There are two parts to prove. First, we show how to witness formulas from Σ_1^B-SymKrom using $\Sigma_0^B(STC)$. Second, we give a Σ_1^B predicate equivalent to the negation of STC: since the value of every formula can be expressed using STC, this is sufficient for Δ_1^B-definability of Σ_1^B-SymKrom.

6.2 Constructing a witness for a Σ_1^B-SymKrom formula

Given a formula $\phi^* \equiv \exists P \forall \bar{x} < \bar{n} \psi(P, \bar{x})$, we create a formula $\phi'(u,s,v,s')$ encoding the structure of ψ; this encoding is similar to the encoding used in [CK04] for Σ_1^B-Krom formulas. For every clause, $\phi'(u,s,v,s')$ says that P-literals contain terms evaluating to u and v, with s and s' being 0 if the literal is negated and 1 otherwise. A propositional version of the formula is satisfiable if the corresponding graph is bipartite, that is, $\exists R \forall u,v < b \forall s,s' < 2(\phi'(u,s,v,s') \to \neg R(u,s) \leftrightarrow R(v,s'))$. Now, to use STC to test bipartiteness we use the standard technique of "doubling" the graph, with every vertex having "even" and "odd" version and every edge connecting the literals on opposite sides. There is an odd cycle in the original graph (and thus the formula evaluates to false) iff there is a path from a vertex on one side to the same numbered vertex on the other; this can be expressed using STC. From the witness to the negation of STC we construct a value for P (all literals on the same side as the constant $\top$ are set to true).

6.3 Δ_1^B-definability of STC

Saying that a pair (a,b) is in the symmetric transitive closure of a graph is equivalent to the statement that b is reachable from a in an undirected graph. Therefore, we give a Σ_1^B-predicate $\textsc{ReachCond}(R,E,n+1,a)$ which states that $R(x,i)$ is true iff x is at most distance i from a:

$$\forall x \le n \forall i \le n (R(x,0) \leftrightarrow x = a) \wedge (R(x,i+1) \leftrightarrow (\exists y \le n R(y,i) \wedge (E(y,x) \vee y = x)))$$

Let ϕ be a formula defining an edge relation of a graph. Let

$$UDist_\phi(x,y,d) \equiv STC_{(u,c),(v,c')} \alpha[(x,0),(y,d),(n,n)],$$

where $\alpha(u,c,v,c') \equiv (c' = c+1 \wedge (\phi(u,v) \vee u = v))$. For simplicity, we assume that ϕ is represented by the corresponding graph E, and write $UDist(x,y,d)$ in that case. Then, $R(x,i) \equiv UDist(a,x,i)$ satisfies $\exists R \textsc{ReachCond}(R,E,n+1,a)$, and V-SymKrom $\vdash STC(a,b,n) \leftrightarrow \exists R \textsc{ReachCond}(R,E,n+1,a) \wedge R(b,n)$.

Now, we showed that the weak constructiveness property holds. Therefore, every $\mathtt{SL}$ function is Σ_1^B-definable in V-SymKrom and every Σ_1^B-definable function of V-SymKrom is in $\mathtt{AC}^0(F\mathtt{SL})$ provably in V-SymKrom. We know that $\mathtt{AC}^0(F\mathtt{SL}) = F\mathtt{L}$, that is every $\mathtt{AC}^0(\mathtt{SL})$ function is already computable in logspace, but this is not known to be provable in V-SymKrom. Also, just like V-Krom, V-SymKrom is finitely axiomatizable by finite set of axioms of V^0 together with comprehension over $\neg AxSTC$.

7 Conclusion

In this work we present a general framework for constructing systems of arithmetic with predefined power based on descriptive complexity results. The setback is that whereas for capture results in the descriptive complexity setting it is sufficient to have "some" proof of capture, in our bounded arithmetic framework we need an "easy" proof of capture, getting in return a "provable" capture result. It is interesting to see in which cases the complexity classes behave nicely, like $\mathtt{P}$ or $\mathtt{NL}$, and in which cases, like $\mathtt{SL}$, the proofs use concepts not (known to be) formalizable within the class itself.

A general witnessing theorem applying to slightly different types of theories was presented recently by Cook and Nguyen [NC04a]. Their framework applies to theories equivalent to universal theories. They have a large number of applications, including different theories for $\mathtt{NL}$, $\mathtt{SL}$ and $\mathtt{P}$. However, they do not talk about provable capture.

Yet another property, uniqueness, that can be used instead of constructiveness was suggested to me by Sam Buss. This property states that for every formula from Φ there is an equivalent Σ_1^B formula with at most one witness to the quantifiers. The uniqueness property immediately implies constructiveness.

In general, it seems interesting to study "robustness" of complexity classes, such as provability of their properties. We hope that our framework provides a natural setting for such study.

References

[BIS90] D. M. Barrington, N. Immerman, and H. Straubing. On uniformity within NC^1. *Journal of Computer and System Sciences*, 41(3):274 – 306, 1990.

[CK01] S.A. Cook and A. Kolokolova. A second-order system for polynomial-time reasoning based on Grädel's theorem. In *Proceedings of the Sixteens annual IEEE symposium on Logic in Computer Science*, pages 177–186, 2001.

[CK03] S.A. Cook and A. Kolokolova. A second-order system for polytime reasoning based on Grädel's theorem. *Annals of Pure and Applied Logic*, 124:193–231, 2003.

[CK04] S.A. Cook and A. Kolokolova. Bounded arithmetic of NL. In *Proceedings of the Nineteens annual IEEE symposium on Logic in Computer Science*, pages 398–407, 2004.

[Cob65] A. Cobham. The intrinsic computational difficulty of functions. In Y. Bar-Hillel, editor, *Logic, Methodology and Philosophy of Science*, pages 24–30, Amsterdam, 1965. North-Holland.

[Coo02] S. A. Cook. CSC 2429S: Proof Complexity and Bounded Arithmetic. Course notes, URL: "http://www.cs.toronto.edu/~sacook/csc2429h", Spring 1998-2002.

[Coo04] S. Cook. Theories for complexity classes and their propositional translations. *submitted*, pages 1–36, 2004.

[CT95] P. Clote and G. Takeuti. First order bounded arithmetic and small boolean circuit complexity classes. In *Feasible Mathematics*, volume II. Birkhuser Inc., 1995.

[CT04] Stephen Cook and Neil Thapen. The strength of replacement in weak arithmetic. In *Proceedings of the Nineteens annual IEEE symposium on Logic in Computer Science*, pages 256–264, 2004.

[EF95] H.-D. Ebbinghaus and J. Flum. *Finite model theory.* Springer Verlag, 1995.

[Fag74] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. *Complexity of computation, SIAM-AMC proceedings*, 7:43–73, 1974.

[Grä91] E. Grädel. The Expressive Power of Second Order Horn Logic. In *Proceedings of 8th Symposium on Theoretical Aspects of Computer Science STACS '91, Hamburg 1991*, volume 480 of *LNCS*, pages 466–477. Springer-Verlag, 1991.

[Grä92] E. Grädel. Capturing Complexity Classes by Fragments of Second Order Logic. *Theoretical Computer Science*, 101:35–57, 1992.

[Imm82] N. Immerman. Relational queries computable in polytime. In *14th ACM Symp.on Theory of Computing, Springer Verlag (Heidelberg, FRG and NewYork NY, USA)-Verlag*, pages 147 –152, 1982.

[Imm99] N. Immerman. *Descriptive complexity.* Springer Verlag, New York, 1999.

[Kol04] A. Kolokolova. *Systems of bounded arithmetic from descriptive complexity.* PhD thesis, University of Toronto, October 2004.

[Lib04] L. Libkin. *Elements of Finite Model Theory.* Springer Verlag, 2004.

[NC04a] Phuong Nguyen and Stephen Cook. Theories for TC^0 and other small complexity classes. *submitted*, 2004.

[NC04b] Phuong Nguyen and Stephen Cook. VTC^0: a second-order theory for TC^0. In *Proceedings of the Nineteens annual IEEE symposium on Logic in Computer Science*, pages 378–387, 2004.

[NTS95] Noam Nisan and Amnon Ta-Shma. Symmetric logspace is closed under complement. In *Proc. 27th Ann. ACM Symp. on Theory of Computing (STOC'95)*, pages 140–146, 1995.

[Rei04] O. Reingold. Undirected ST-Connectivity in Log-Space. *Electronic Colloquium on Computational Complexity*, ECCC Report TR04-094, 2004.

[Sch78] T. J. Schaefer. The complexity of satisfiability problems. In *Proceedings of the Tenth Annual ACM Symposium on Theory of Computing*, pages 216–226, 1978.

[Sto77] L. J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.

[Zam96] D. Zambella. Notes on polynomially bounded arithmetic. *The Journal of Symbolic Logic*, 61(3):942–966, 1996.